И.Б.Бурдонов, А.С. Косачев.
Удаление из спецификации неконформных трасс.
Препринт Института Системного Программирования РАН, 2011 г., №23.
218 стр.

Оглавление

И.Б.Бурдонов, А.С. Косачев.
Удаление из спецификации неконформных трасс.
Препринт Института Системного Программирования РАН, 2011 г., №23.
218 стр.

Удаление из спецификации неконформных трасс

Игорь Бурдонов <igor@ispras.ru>, Александр Косачев <kos@ispras.ru>

Аннотация. Работа посвящена оптимизации тестирования, понимаемого как проверка соответствия (конформности) реализации заданной спецификации в процессе тестовых экспериментов. Тесты генерируются по трассам спецификации. Однако, как показано в данной работе, некоторые трассы спецификации могут не встречаться ни в одной конформной реализации. Тесты, сгенерированные по таким неконформным трассам, заведомо «лишние». Поэтому в целях оптимизации тестирования возникает задача удаления из спецификации неконформных трасс. Для этого предлагается соответствующее преобразование спецификации (которое мы назвали ∇-пополнением) с дополнительным требованием: не изменяется класс конформных реализаций и сохраняется возможность тестировать все те реализации, которые можно было тестировать по исходной спецификации. Предлагаемые алгоритмы пригодны для широкого класса отношений конформности, параметризуемых той или иной семантикой взаимодействия, основанной на тестовых воздействиях и наблюдениях. Для конечной семантики и конечной исходной спецификации эти алгоритмы выполняют требуемое преобразование за конечное время, и результатом является конечная спецификация.

Ключевые слова: Семантика взаимодействия, отказы, разрушение, дивергенция, конформность, безопасное тестирование, трассы, LTS, генерация тестов.

1. Теория конформности

1.1. Семантика взаимодействия и безопасное тестирование

Верификация конформности понимается как проверка соответствия исследуемой системы заданным требованиям. В модельном мире система отображается в реализационную модель (реализацию), требования – в спецификационную модель (спецификацию), а их соответствие – в бинарное отношение конформности. Если требования выражены в терминах взаимодействия системы с окружающим миром, возможно тестирование как проверка конформности в процессе тестовых экспериментов, когда тест подменяет собой окружение системы. В этом случае само отношение

конформности и его тестирование основаны на той или иной модели взаимодействия.

Мы рассматриваем семантики взаимодействия, которые определяются только внешним, наблюдаемым поведением системы и не учитывают её внутреннее устройство, которое на уровне модели отображается понятием *состояния*. Мы можем наблюдать только такое поведение реализации, которое, во-первых, «спровоцировано» тестом (управление) и, во-вторых, наблюдаемо во внешнем взаимодействии. Такое взаимодействие может моделироваться с помощью, так называемой, машины тестирования [7],[9],[10],[32],[33],[37]. Она представляет собой «чёрный ящик», внутри которого находится реализация (Рис. 1.). Управление сводится к тому, что оператор машины, выполняя тест (понимаемый как инструкция оператору), нажимает кнопки на клавиатуре машины, «разрешая» реализации выполнять те или иные действия, которые могут им наблюдаться. Наблюдения (на «дисплее» машины) бывают двух типов: наблюдение некоторого *внешнего (наблюдаемого) действия*, разрешённого оператором и выполняемого реализацией, и наблюдение *отказа* как отсутствия каких бы то ни было наблюдаемых действий из числа тех, что разрешены нажатой кнопкой.

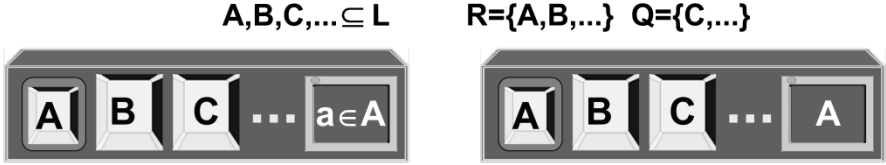


Рис. 1. Машина тестирования

Подчеркнём, что при управлении оператор разрешает реализации выполнять именно множество действий, а не обязательно одно действие. Будем считать, что каждой кнопке соответствует своё множество разрешаемых действий, и оператор нажимает только одну кнопку. После наблюдения (действия или отказа) кнопка отжимается, и все внешние действия запрещаются. Далее оператор может нажать другую (или ту же самую) кнопку.

Тестовые возможности определяются тем, какие «кнопочные» множества есть в машине, а также для каких кнопок возможно наблюдение отказа. Тем самым, семантика взаимодействия определяется алфавитом внешних действий **L** и двумя наборами кнопок машины тестирования: с наблюдением соответствующих отказов – семейство $\mathbf{R}\subseteq\mathcal{P}(\mathbf{L})$ и без наблюдения отказа – семейство $\mathbf{Q}\subseteq\mathcal{P}(\mathbf{L})$. Предполагается, что $\mathbf{R}\cap\mathbf{Q}=\varnothing$ и $\cup\mathbf{R}\cup\cup\mathbf{Q}=\mathbf{L}$. Такую семантику мы называем **R**/**Q**-семантикой [7],[10],[12],[16],[20],[22],[23].

Кроме внешних действий реализация может совершать внутренние (ненаблюдаемые) действия, обозначаемые символом τ. Эти действия

считаются всегда разрешенными (при нажатии любой кнопки или при отсутствии нажатой кнопки).

Для выполнимости любого действия (как внешнего, так и внутреннего) необходимо, чтобы оно было определено в реализации и разрешено оператором. Если этого условия также и достаточно, то есть любое действие, удовлетворяющее этому условию, может быть выбрано на выполнение, то говорят, что в системе нет приоритетов [33]. Здесь мы ограничимся только системами без приоритетов. Тестирование систем с приоритетами рассмотрено в наших работах [11],[13].

Предполагается, что любая конечная последовательность любых действий (как внешних, так и внутренних) совершается за конечное время, а бесконечная – за бесконечное время. Также предполагается, что «передача» тестового воздействия (нажатие кнопки) от машины тестирования в реализацию и наблюдения от реализации на дисплей машины выполняются за конечное время. Эти предположения гарантируют наблюдение внешнего действия, выполняемого реализацией, через конечное время после нажатия кнопки, разрешающей это действие.

Эти же предположения часто используются для реализации наблюдения **R**-отказа, но в усиленном варианте: время выполнения каждого действия, разрешаемого кнопкой, вместе с возможными предшествующими ему внутренними действиями не только конечно, но и ограничено. В этом случае вводится тайм-аут, истечение которого без наблюдения действия трактуется как отказ. Важно отметить, что это не единственный возможный способ реализации наблюдения отказа.

После нажатия **R**-кнопки через конечное время оператор наблюдает или разрешенное этой кнопкой внешнее действие или соответствующий отказ. Однако при нажатии **Q**-кнопки, если в реализации возможен отказ, то, поскольку этот отказ не наблюдаем, оператор не знает, нужно ли ему ждать наблюдения внешнего действия или такого действия не будет, поскольку возник отказ. Поэтому оператор не может ни продолжать тестирование, ни закончить его.

Бесконечная последовательность τ-действий («зацикливание») называется *дивергенцией* и обозначается символом Δ. Дивергенция сама по себе не опасна, но при попытке выхода из неё, когда оператор нажимает любую (**R**- или **Q**-) кнопку, он не знает, нужно ли ждать наблюдения (внешнего действия или **R**-отказа) или бесконечно долго будут выполняться только внутренние действия. Поэтому оператор не может ни продолжать тестирование, ни закончить его.

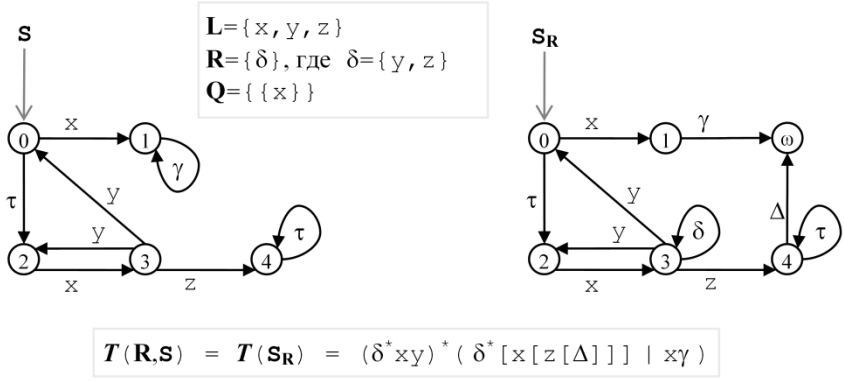
Кроме этого мы вводим [6],[7],[8],[9],[10] специальное, также не регулируемое кнопками, действие, которое называем *разрушением* и обозначаем символом γ. Оно моделирует любое поведение реализации, которое не должно допускаться во время тестирования.

Тестирование, при котором не возникает разрушения, попыток выхода из дивергенции и ненаблюдаемых отказов, называется безопасным [7],[10].[1]

1.2. LTS-модель

В качестве основной модели реализации и спецификации мы используем *систему помеченных переходов* (LTS – Labelled Transition System) – ориентированный граф с выделенной начальной вершиной, дуги которого помечены некоторыми символами. Формально, LTS – это совокупность $\mathbf{S}=\mathrm{LTS}(V_S,\mathbf{L},E_S,s_0)$, где V_S – непустое множество состояний (вершин графа), $\mathbf{L}$ – алфавит внешних действий, $E_S \subseteq V_S \times (\mathbf{L} \cup \{\tau,\gamma\}) \times V_S$ – множество переходов (помеченных дуг графа), $s_0 \in V_S$ – начальное состояние (начальная вершина графа).

Пример LTS приведен на Рис. 2. слева.



$$\boldsymbol{T}(\mathbf{R},\mathbf{S}) = \boldsymbol{T}(\mathbf{S}_\mathbf{R}) = (\delta^* xy)^* (\delta^* [x[z[\Delta]]] \mid x\gamma)$$

*Рис. 2. Пример LTS и ее **R**-трасс*[2]

---

[1] В наших более ранних работах [6][7][9][10] опасной считалась сама дивергенция, а не попытка выхода из нее.

[2] При записи регулярных выражений здесь и ниже в тексте мы для краткости будем опускать знаки конкатенации «·» для последовательностей и множеств последовательностей, запятые «,», разделяющие элементы последовательности, угловые скобки «⟨» и «⟩», отмечающие начало и конец последовательности, а также фигурные скобки «{» и «}» для множеств. Например, регулярное выражение на данном рисунке, записанное в краткой форме как $(\delta^* xy)^* (\delta^* [x[z[\Delta]]] \mid x\gamma)$, в полной форме записывается так:

$(\{\langle\delta\rangle\}^* \cdot \{\langle x,y\rangle\})^* \cdot (\{\langle\delta\rangle\}^* \cdot \{[\langle x\rangle \cdot [\langle z\rangle \cdot [\langle\Delta\rangle]]]\} \mid \{\langle x,\gamma\rangle\})$.

Множество всех LTS в алфавите $\mathbf{L}$ обозначим $\boldsymbol{LTS}(\mathbf{L})$. Также введем обозначения для наличия/отсутствия переходов:

$s—z→s' \triangleq (s,z,s') \in E_s$,

$s—z↛s' \triangleq \neg(s—z→s')$,

$s—z→ \triangleq \exists s'\ s—z→s'$,

$s—z↛ \triangleq \neg(s—z→)$.

Там, где это не приводит к недоразумениям, мы будем использовать запись $s—z→s'$ для обозначения самого перехода (s,z,s'), а не как предикат $(s,z,s') \in E_s$.

Маршрутом LTS называется последовательность смежных переходов: начало каждого перехода, кроме первого, совпадает с концом предыдущего перехода.

Выполнение LTS в машине тестирования сводится к прохождению маршрута, каждый переход которого разрешается нажатой кнопкой с учетом того, что после выполнения перехода по внешнему действию, разрешаемому нажатой кнопкой, эта кнопка автоматически отжимается. При этом τ- и γ-переходы всегда разрешены.

Состояние s' *достижимо из состояния* s, если в s' заканчивается маршрут, начинающийся в состоянии s. *Достижимое состояние* – это состояние, достижимое из начального состояния s_0. Множество состояний, достижимых из состояния s, будем обозначать $\boldsymbol{der}(s)$. Определим $\boldsymbol{der}(\mathbf{S}) \triangleq \boldsymbol{der}(s_0)$.

Простой трассой LTS будем называть последовательность σ пометок на переходах маршрута с пропуском символов τ. Простая трасса в алфавите $\mathbf{L}$ – это последовательность в алфавите $\mathbf{L} \cup \{\gamma\}$. Множество простых трасс, начинающихся (то есть маршруты которых начинаются) в состоянии s будем обозначать $\boldsymbol{T}(s)$. Через $s\ \boldsymbol{after}\ \sigma$ обозначим множество состояний, в которых заканчивается простая трасса σ, начинающаяся в состоянии s, то есть заканчиваются все маршруты с простой трассой σ, начинающиеся в состоянии s. Распространим оператор ***after*** на множество A состояний обычным образом: $A\ \boldsymbol{after}\ \sigma \triangleq \{s\ \boldsymbol{after}\ \sigma \mid s \in A\}$, результатом является множество множеств состояний LTS. По умолчанию, будем считать, что простая трасса начинается в начальном состоянии LTS, и обозначать $\mathbf{S}\ \boldsymbol{after}\ \sigma \triangleq s_0\ \boldsymbol{after}\ \sigma$, $\boldsymbol{T}(\mathbf{S}) \triangleq \boldsymbol{T}(s_0)$.

Введем следующие обозначения для состояний s и s' и трассы σ:

$s \Rightarrow s` \triangleq s` \in (s \ \textit{after} \ \epsilon)$, где ϵ пустая трасса (трасса нулевой длины),

$s = \sigma \Rightarrow s` \triangleq s` \in (s \ \textit{after} \ \sigma)$, $\quad s = \sigma \not\Rightarrow s` \triangleq \neg(s = \sigma \Rightarrow s`)$,

$s = \sigma \Rightarrow \triangleq \exists s` \ s = \sigma \Rightarrow s`$, $\quad s = \sigma \not\Rightarrow \triangleq \neg(s = \sigma \Rightarrow)$.

LTS *детерминирована*, если каждая простая трасса заканчивается не более чем в одном состоянии: $\forall \sigma \ \ |\mathbf{S} \ \textit{after} \ \sigma| \le 1$. Очевидно, что в детерминированной LTS нет τ-переходов из достижимых состояний: $\forall s \in \textit{der}(\mathbf{S}) \ s \text{—}\tau\!\!\not\rightarrow$.

Состояние s *терминально*, если из него не выходят никакие переходы: $\forall z \in \mathbf{L} \cup \{\tau, \gamma\} \ s \text{—}z\!\!\not\rightarrow$.

Состояние s *стабильно*, если из него не выходят τ- и γ-переходы: $s \text{—}\tau\!\!\not\rightarrow$ & $s \text{—}\gamma\!\!\not\rightarrow$. Отказ $P \in \mathcal{P}(\mathbf{L})$ порождается стабильным состоянием, из которого нет переходов по действиям из P: $\forall z \in P \cup \{\tau, \gamma\} \ s \text{—}z\!\!\not\rightarrow$.

Состояние s будем называть *дивергентным* и обозначать $s\uparrow$, если в нем начинается бесконечный τ-маршрут, то есть маршрут, содержащий только τ-переходы; в противном случае состояние *конвергентно*, что обозначается $s\downarrow$.

Если LTS находится в конвергентном состоянии s, когда нажимается кнопка P, то через конечное время либо выполняется переход по действию z, разрешаемому кнопкой P, то есть $z \in P$, либо происходит отказ P. Этот отказ P наблюдается, если $P \in \mathbf{R}$. Поскольку τ-переходы всегда разрешены, может оказаться, что переход по действию z выполняется не из состояния s, а из другого состояния $s`$, достижимого из $s$ по цепочке $\tau$-переходов ($s \Rightarrow s`$). Аналогично, поскольку при возникновении **R**-отказа P LTS должна находиться в стабильном состоянии, это состояние совпадает с состоянием s только в том случае, когда состояние s стабильно, а в противном случае отказ происходит в стабильном состоянии $s`$, достижимом из $s$ по цепочке $\tau$-переходов ($s \Rightarrow s`$).

Если состояние s дивергентно, то после нажатия кнопки P никаких внешних действий и отказов может не быть, если бесконечно долго будут выполняться только τ-переходы.

R-трассой LTS будем называть последовательность наблюдений, которая может быть получена при взаимодействии с LTS в **R**/**Q**-семантике, то есть последовательность не только действий, но и **R**-отказов. При этом нас не будет интересовать поведение LTS после дивергенции или разрушения. Для определения **R**-трасс LTS $\mathbf{S}$ добавим в каждом ее стабильном состоянии виртуальные петли $s \text{—}R\!\rightarrow s$, помеченные **R**-отказами, порождаемыми в этом состоянии, добавим новое терминальное состояние ω, перенаправим в это

состояние все γ-переходы, а также проведем в него Δ-переходы из дивергентных состояний. Формально для любого заданного семейства множеств **R** это преобразование $\mathbf{S}\to\mathbf{S_R}$ дает LTS $\mathbf{S_R}=\mathsf{LTS}(V_S\cup\{\omega\},\mathbf{L}\cup\mathbf{R}\cup\{\Delta\},E_R,s_0)$, где $\omega\notin V_S$, а множество переходов E_R определяется как минимальное множество, порождаемое следующими правилами вывода:

$\forall s,s'\in V_S \quad \forall z\in\mathbf{L}\cup\{\tau\} \quad \forall R\in\mathbf{R}$

$s\text{—}z\to s' \quad \vdash \quad s\text{—}z\to s',$

$\forall z\in R\cup\{\tau,\gamma\} \quad s\text{—}z\not\to \quad \vdash \quad s\text{—}R\to s,$

$s\text{—}\gamma\to \quad \vdash \quad s\text{—}\gamma\to\omega,$

$s\!\uparrow \quad \vdash \quad s\text{—}\Delta\to\omega.$

Пример LTS **S**, LTS $\mathbf{S_R}$ и множества **R**-трасс LTS **S** приведен на Рис. 2. .

R-трасса в алфавите **L** – это простая трасса в алфавите $\mathbf{L}\cup\mathbf{R}\cup\{\Delta\}$, то есть последовательность в алфавите $\mathbf{L}\cup\mathbf{R}\cup\{\Delta,\gamma\}$. **R**-трассой LTS **S** будем называть простую трассу LTS $\mathbf{S_R}$. Множество всех **R**-трасс LTS, начинающихся (то есть маршруты которых начинаются) в состоянии s будем обозначать $\boldsymbol{T}(\mathbf{R},s)$. Множество $\boldsymbol{T}(\mathbf{R},\mathbf{S}) \triangleq \boldsymbol{T}(\mathbf{R},s_0) = \boldsymbol{T}(\mathbf{S_R})$ называется **R**-моделью или просто *трассовой моделью* в алфавите **L**, если семейство **R** подразумевается. Заметим, что $\boldsymbol{T}(\varnothing,s)=\boldsymbol{T}(s)$ и $\boldsymbol{T}(\varnothing,\mathbf{S})=\boldsymbol{T}(\mathbf{S})$.

Для $\mathbf{R}=\mathcal{P}(\mathbf{L})$ **R**-трассы LTS будем называть **F**-трассами или полными трассами, а множество всех таких трасс LTS – **F**-моделью или *полной трассовой моделью* в алфавите **L**. **F**-трасса в алфавите **L** – это $\mathcal{P}(\mathbf{L})$-трасса в алфавите **L**, то есть простая трасса в алфавите $\mathbf{L}\cup\mathcal{P}(\mathbf{L})\cup\{\Delta\}$, то есть последовательность в алфавите $\mathbf{L}\cup\mathcal{P}(\mathbf{L})\cup\{\Delta,\gamma\}$. Обозначим: $\boldsymbol{F}(s) \triangleq \boldsymbol{T}(\mathcal{P}(\mathbf{L}),s)$ – множество полных трасс, начинающихся в состоянии s LTS **S**, $\boldsymbol{F}(\mathbf{S}) \triangleq \boldsymbol{T}(\mathcal{P}(\mathbf{L}),\mathbf{S}) = \boldsymbol{T}(\mathcal{P}(\mathbf{L}),s_0) = \boldsymbol{T}(\mathbf{S}_{\mathcal{P}(\mathbf{L})})$. По умолчанию под трассами будем понимать **F**-трассы.

Для LTS **S** и полной трассы σ операторы s ***after*** σ, **S** ***after*** σ и предикаты $s=\sigma\Rightarrow s'$, $s=\sigma\not\Rightarrow$, $s=\sigma\not\Rightarrow s'$, $s=\sigma\not\Rightarrow$ будем понимать как соответствующие операторы и предикаты для LTS $\mathbf{S}_{\mathcal{P}(\mathbf{L})}$.

Состояния s и s` будем называть *T-эквивалентными* (эквивалентными в трассовом смысле) и обозначать $s \sim_T s`$, если в них начинаются одни и те же полные трассы: $\boldsymbol{F}(s)=\boldsymbol{F}(s`)$. Множества состояний A и A` будем называть *T-эквивалентными* (эквивалентными в трассовом смысле) и обозначать $A \sim_T A`$, если в их состояниях начинаются одни и те же трассы: $\cup\{\boldsymbol{F}(s) \mid s \in A\}=\cup\{\boldsymbol{F}(s`) \mid s` \in A`\}$.

1.3. Трассовая модель

Для взаимодействия, основанного на наблюдениях, единственным результатом тестового эксперимента является чередующаяся последовательность кнопок (тестовых воздействий) и наблюдений, которую будем называть (тестовой) *историей*. История, если она не пустая, должна начинаться с кнопки. Дивергенция и разрушение считаются условно-наблюдаемыми действиями: хотя они не должны возникать при безопасном тестировании, но для полноты моделирования должны присутствовать в историях, отмечая те их них, после которых возможны дивергенция или разрушение. Так как нас не интересует поведение системы после дивергенции или разрушения, символы Δ и γ могут быть только последними элементами историй. Любое другое наблюдение u (внешнее действие или **R**-отказ) разрешается непосредственно предшествующей ему кнопкой P, то есть $u \in P$ или $u=P$ для $P \in \mathbf{R}$. Подпоследовательность истории, состоящая только из наблюдений (включая Δ и γ), как раз и является трассой (этой истории). Заметим, что по этому определению любой префикс истории является историей.

Для систем без приоритетов важны только трассы, поскольку возможность или невозможность появления данного наблюдения после некоторой трассы определяется только тем, что нажимаемая кнопка разрешает данное наблюдение, и не зависит от того, какие еще наблюдения она разрешает или запрещает. Для данной тестируемой системы без приоритетов множество ее историй однозначно восстанавливается по множеству ее трасс. Поэтому трассовая модель как множество трасс, которые можно наблюдать при работе с системой, является наиболее естественной моделью такой системы. В частности, одной и той же трассовой модели может соответствовать несколько LTS с одним и тем же множеством трасс, и эти LTS неразличимы при взаимодействии с ними в **R**/**Q**-семантике.

Конечная последовательность σ длины n в некотором алфавите – это однозначное отображение отрезка натуральных чисел [1..n] в алфавит. Поэтому для трасс, маршрутов (и вообще, любых последовательностей) мы будем использовать обычные для отображений обозначения:

- $|\sigma|$ – мощность множества, которым является последовательность (множества пар «индекс элемента в последовательности, элемент последовательности»), то есть длина последовательности (число

элементов отображения), пустая последовательность ϵ имеет нулевую длину,

- $\boldsymbol{Im}(\sigma)$ – множество (различных) элементов последовательности,
- $\sigma(i)$ – i-ый элемент последовательности,
- $\sigma[i..j]$ – отрезок последовательности, начиная с i-ого и заканчивая j-ым элементом (если $i>j$ или $i>|\sigma|$, отрезок является пустой последовательностью).

На множестве последовательностей будем использовать следующие *префиксные* отношения:

$\mu\le\sigma \triangleq \exists i\ \mu=\sigma[1..i]$, последовательность μ является *префиксом* последовательности σ,

$\mu<\sigma \triangleq \mu\le\sigma\ \&\ \mu\ne\sigma$, последовательность μ является *строгим префиксом* последовательности σ.

$\boldsymbol{p_{re}}$-операцией будем называть операцию взятия префикса последовательности: $\mu\cdot\lambda \text{—}\boldsymbol{p_{re}}\!\!\rightarrow\mu$. Эта операция зависит от двух параметров: $\mu\cdot\lambda$ и μ.

Замыкание последовательности σ по операции $\boldsymbol{p_{re}}$, то есть множество префиксов последовательности σ, обозначим $\boldsymbol{p_{re}}(\sigma)$.

Множество последовательностей, которое вместе с каждой последовательностью σ содержит и все ее префиксы из $\boldsymbol{p_{re}}(\sigma)$, называется *префикс-замкнутым* множеством трасс.

Проекцией последовательности σ на множество A будем называть подпоследовательность, состоящую из тех и только тех элементов последовательности σ, которые принадлежат множеству A. Проекцией множества Σ последовательностей будем называть множество проекций этих последовательностей.

$\sigma{\downarrow}A \triangleq \langle\sigma(i)|i=1..|\sigma|\ \&\ \sigma(i)\in A\rangle$,

$\Sigma{\downarrow}A \triangleq \{\sigma{\downarrow}A|\sigma\in\Sigma\}$.

В частности, **R**-трасса – это проекция тестовой истории на алфавит $\mathbf{L}\cup\mathbf{R}\cup\{\Delta,\gamma\}$.

Подпоследовательность трассы σ, содержащую все действия из трассы и только их, будем называть подтрассой действий и обозначать $\sigma\text{^} \triangleq \sigma{\downarrow}(\mathbf{L}\cup\{\Delta,\gamma\})$.

Для $i=1..|\sigma\text{^}|$ i-ое действие трассы σ, очевидно, равно $\sigma\text{^}(i)$.

Подтрассу отказов после последнего действия (или саму трассу, если в ней нет действий) будем называть *постфиксом отказов* и обозначать $\boldsymbol{p_{ost}}(\sigma) \triangleq \langle \sigma(i)|i=1..|\sigma| \;\&\; \sigma[i..|\sigma|] \in \mathbf{R}^* \rangle$.

Множество отказов, содержащихся в постфиксе отказов трассы σ, будем называть *последним множеством отказов* трассы σ и обозначать $\boldsymbol{Ip}(\sigma) \triangleq \boldsymbol{Im}(\boldsymbol{p_{ost}}(\sigma))$.

Для $i=0..|\sigma\hat{}|$ префикс трассы σ, непосредственно предшествующий $i+1$-ому действию трассы, если $i<|\sigma\hat{}|$, или саму трассу σ, если $i=|\sigma\hat{}|$, будем называть *i-ым префиксом* трассы σ и обозначать

$\sigma^i \triangleq \langle \sigma(j)|j=1..|\sigma| \;\&\; |\sigma[1..j]\hat{}| \le i \rangle$.

Очевидно, что $\sigma\hat{}^i = \sigma^i\hat{}$.

Для трассы σ i-ой *подтрассой отказов* будем называть постфикс отказов i-го префикса трассы, то есть трассу $\boldsymbol{p_{ost}}(\sigma^i)$. Соответственно, i-ым множеством отказов трассы σ будем называть множество отказов в i-ой подтрассе отказов, что совпадает с последним множеством отказов i-го префикса трассы, то есть множество $\boldsymbol{Ip}(\sigma^i)$.

Повторным отказом в трассе σ будем называть такой отказ $P=\sigma(i)$, который принадлежит постфиксу отказов непосредственно предшествующего ему префиксу трассы: $i>0 \;\&\; P \in \boldsymbol{Ip}(\sigma[1..i-1])$.

Определим операции над трассами:

- $\boldsymbol{d}$ – удаление отказа $P \in \mathcal{P}(\mathbf{L})$: $\mu\cdot\langle P\rangle\cdot\lambda \text{—}\boldsymbol{d}\!\to \mu\cdot\lambda$;

  операция зависит от трех параметров: $\mu\cdot\langle P\rangle\cdot\lambda$, μ и $\mathbf{L}$, где $P \in \mathcal{P}(\mathbf{L})$.

- $\boldsymbol{r}$ – повторение отказа $P \in \mathcal{P}(\mathbf{L})$: $\mu\cdot\langle P\rangle\cdot\lambda \text{—}\boldsymbol{r}\!\to \mu\cdot\langle P,P\rangle\cdot\lambda$;

  операция зависит от трех параметров: $\mu\cdot\langle P\rangle\cdot\lambda$, μ и $\mathbf{L}$, где $P \in \mathcal{P}(\mathbf{L})$.

- $\boldsymbol{t}$ – перестановка соседних отказов $P,Q \in \mathcal{P}(\mathbf{L})$: $\mu\cdot\langle P,Q\rangle\cdot\lambda \text{—}\boldsymbol{t}\!\to \mu\cdot\langle Q,P\rangle\cdot\lambda$;

  операция зависит от трех параметров: $\mu\cdot\langle P,Q\rangle\cdot\lambda$, μ и $\mathbf{L}$, где $P,Q \in \mathcal{P}(\mathbf{L})$.

- $\boldsymbol{i}$ – вставка отказа $R \in \mathbf{R}$ в трассу $\mu\cdot\lambda$ после трассы μ при условии, что трасса μ заканчивается отказом и не продолжается во множестве трасс $\boldsymbol{\Sigma}$ дивергенцией, разрушением и действиями из R:

  если $\boldsymbol{p_{ost}}(\mu) \ne \epsilon \;\&\; \mu\cdot\lambda \in \boldsymbol{\Sigma} \;\&\; \forall z \in R \cup \{\Delta,\gamma\}\ \mu\cdot\langle z\rangle \notin \boldsymbol{\Sigma}$, то $\mu\cdot\lambda \text{—}\boldsymbol{i}\!\to \mu\cdot\langle R\rangle\cdot\lambda$;

  операция зависит от пяти параметров: $\mu\cdot\lambda$, μ, R, $\boldsymbol{\Sigma}$, $\mathbf{R}$, где $R \in \mathbf{R}$.

Замыканием трассы σ по операции $\boldsymbol{op} \in \{\boldsymbol{p_{re}},\boldsymbol{d},\boldsymbol{r},\boldsymbol{t}\}$ будем называть множество трасс, получаемых из трассы σ всеми возможными конечными цепочками применения этой операции, и обозначать $\boldsymbol{op}(\sigma)$. Формально:

$\boldsymbol{op}(\sigma) \triangleq \{\sigma` \mid \exists n\ \exists \sigma_1,\sigma_2,\ldots,\sigma_n\ \sigma_n=\sigma` \ \&\ \sigma_1 \text{—}\boldsymbol{op}\text{→} \sigma_2 \text{—}\boldsymbol{op}\text{→} \ldots \text{—}\boldsymbol{op}\text{→} \sigma_n\}$.

Замыканием трассы σ по операции $\boldsymbol{i}$ будем называть множество трасс, получаемых из трассы σ с помощью всех возможных одновременных[3] вставок любого (в том числе нулевого) числа отказов, и обозначать $\boldsymbol{i}(\sigma)$. Формально:

$\boldsymbol{i}(\sigma) \triangleq \{\sigma` \mid \exists n\ \exists \mu_0,\ldots,\mu_n\ \exists R_1,\ldots,R_n\ \sigma=\mu_0\cdot\ldots\cdot\mu_n$

$\&\ \sigma`=\mu_0\cdot\langle R_1\rangle\cdot\mu_1\cdot\ldots\cdot\langle R_n\rangle\cdot\mu_n\ \&\ \forall i\in[1..n]\ \sigma \text{—}\boldsymbol{i}\text{→} \mu_0\cdot\ldots\cdot\mu_{i-1}\cdot\langle R_i\rangle\cdot\mu_i\cdot\ldots\cdot\mu_n\}$.

Там, где множество отказов $\mathbf{R}$ не подразумевается по умолчанию, мы будем обозначать замыкание трассы σ по $\boldsymbol{i}$-операции как $\boldsymbol{i}_{\mathbf{R}}(\sigma)$.

Распространим замыкание по операции $\boldsymbol{op}\in\{\boldsymbol{p}_{re},\boldsymbol{d},\boldsymbol{r},\boldsymbol{t},\boldsymbol{i}\}$ на множество трасс $\boldsymbol{\Sigma}$ обычным образом: для $\boldsymbol{op}\in\{\boldsymbol{p}_{re},\boldsymbol{d},\boldsymbol{r},\boldsymbol{t},\boldsymbol{i}\}$:

$\boldsymbol{op}(\boldsymbol{\Sigma}) \triangleq \{\boldsymbol{op}(\sigma) \mid \sigma\in\boldsymbol{\Sigma}\}$, результатом является множество множеств трасс.

Замыканием трассы σ по последовательности операций $\boldsymbol{op}_1,\ldots,\boldsymbol{op}_k$, где $\{\boldsymbol{op}_1,\ldots,\boldsymbol{op}_k\}\subseteq\{\boldsymbol{p}_{re},\boldsymbol{d},\boldsymbol{r},\boldsymbol{t},\boldsymbol{i}\}$ будем называть множество трасс, получаемых из трассы σ конечным числом применений каждой операции в заданной последовательности операций, и обозначать $\boldsymbol{op}_1\ldots\boldsymbol{op}_k(\sigma)$. Например, $\boldsymbol{p}_{re}(\sigma)$, $\boldsymbol{d}(\sigma)$, $\boldsymbol{rt}(\sigma)$ или $\boldsymbol{drt}(\sigma)$. Поскольку каждая операция преобразует одну трассу во множество трасс, формальное определение такое:

$\boldsymbol{op}_1\boldsymbol{op}_2\ldots\boldsymbol{op}_{k-1}\boldsymbol{op}_k(\sigma) \triangleq \cup\boldsymbol{op}_1(\cup\boldsymbol{op}_2(\ldots\cup\boldsymbol{op}_{k-1}(\boldsymbol{op}_k(\sigma))\ldots))$.

Любая LTS вместе с полной трассой σ содержит и ее $\boldsymbol{p}_{re}\boldsymbol{drti}_{\mathcal{P}(\mathbf{L})}$-замыкание.

Распространим замыкание по последовательности $\boldsymbol{op}_1,\ldots,\boldsymbol{op}_k$ операций на множество трасс Σ обычным образом:

$\boldsymbol{op}_1\ldots\boldsymbol{op}_k(\Sigma) \triangleq \{\boldsymbol{op}_1\ldots\boldsymbol{op}_k(\sigma) \mid \sigma\in\Sigma\}$, результатом является множество множеств трасс.

В [10] доказано, что множество $\mathbf{R}$-трасс $\boldsymbol{\Sigma}$ является трассовой моделью в алфавите $\mathbf{L}$ (то есть множеством $\mathbf{R}$-трасс некоторой LTS в алфавите $\mathbf{L}$) тогда и только тогда, когда оно не пусто, префикс-замкнуто и удовлетворяет следующим требованиям:

T1. <u>допустимость</u>: все трассы $\sigma\in\boldsymbol{\Sigma}$ *допустимы*: дивергенция и разрушение либо не входят в трассу, либо являются последним символом трассы:

[3] Такое определение замыкания по операции $\boldsymbol{i}$ с одновременной вставкой отказов необходимо для правильного определения операции ***Ext*** расширения $\mathbf{R}$-модели до полной трассовой модели, которое дано ниже в этом подразделе.

$\forall i=1..|\sigma|-1\ \sigma(i)\notin\{\Delta,\gamma\}$;

T2. согласованность: все трассы $\sigma\in\mathbf{\Sigma}$ *согласованы*: любая непустая последовательность отказов в трассе не продолжается ни дивергенцией, ни разрушением, ни каким-либо внешним действием, принадлежащим какому-либо отказу, входящему в эту последовательность:

$\forall i\in[2..|\sigma|]\ \forall R\in\boldsymbol{Ip}(\sigma[1..i-1])\ \sigma(i)\notin R\cup\{\Delta,\gamma\}$;

T3. конвергентность: все трассы $\mathbf{\Sigma}$ *конвергентны*: если трасса $\sigma\in\mathbf{\Sigma}$ не содержит и не продолжается разрушением и дивергенцией, то для каждого отказа $R\in\mathbf{R}$ трасса σ продолжается в $\mathbf{\Sigma}$ этим отказом R или каким-либо внешним действием, принадлежащим отказу R:

$\forall R\in\mathbf{R}\ \ \sigma\cdot\langle R\rangle\in\mathbf{\Sigma}\ \vee\ \exists z\in R\ \ \sigma\cdot\langle z\rangle\in\mathbf{\Sigma}$;

T4. замкнутость: $\mathbf{\Sigma}$ замкнуто по ***d***-операции: $\cup\boldsymbol{d}(\mathbf{\Sigma})=\mathbf{\Sigma}$;

T5. полнота: $\mathbf{\Sigma}$ замкнуто по ***i***-операции вставки (**R**-отказов): $\cup\boldsymbol{i}(\mathbf{\Sigma})=\mathbf{\Sigma}$.

Фактически, это утверждение дает интенсиональное определение трассовой модели, в отличие от ее генетического определения как множества трасс LTS. Множество всех трассовых моделей в алфавите $\mathbf{L}$ обозначим $\boldsymbol{MODEL}(\mathbf{L})$.

Если $\mathbf{R}=\mathcal{P}(\mathbf{L})$, то такая трассовая модель называется полной. Полная трассовая модель совпадает с множеством всех полных трасс некоторой LTS. Как показано в [10], для любого $\mathbf{R}\subseteq\mathcal{P}(\mathbf{L})$ проекция полной трассовой модели на алфавит $\mathbf{L}\cup\mathbf{R}\cup\{\Delta,\gamma\}$ является **R**-моделью[4], и любая **R**-модель может быть расширена до такой полной трассовой моделью, что станет ее проекцией на алфавит $\mathbf{L}\cup\mathbf{R}\cup\{\Delta,\gamma\}$. Полная трассовая модель описывает как устроена система «на самом деле», а её **R**-проекция – это «взгляд» на систему, определяемый тестовыми возможностями по управлению и наблюдению, которые описываются **R**/**Q**-семантикой.

Вообще говоря, могут существовать несколько разных полных трассовых моделей, проекции которых на алфавит $\mathbf{L}\cup\mathbf{R}\cup\{\Delta,\gamma\}$ дают одну и ту же **R**-модель. В [10] определено расширение $\boldsymbol{Ext}(\mathbf{N})\ \triangleq\ \cup\boldsymbol{d}(\cup\boldsymbol{i}_{\mathcal{P}(\mathbf{L})}(\cup\boldsymbol{e}(\mathbf{N})))$ **R**-модели $\mathbf{N}$ до полной трассовой модели, то есть $\mathcal{P}(\mathbf{L})$-модели. Здесь под операцией $\boldsymbol{e}$ понимается вставка пустых отказов в трассы после префиксов, которые не заканчиваются и не продолжаются дивергенцией, разрушением и отказами (то есть префикс либо пуст, либо заканчивается действием, и в обоих случаях продолжается только действиями). Затем применяется ***i***-замыкание для всех отказов из $\mathcal{P}(\mathbf{L})$. И в конце делается ***d***-замыкание.

[4] В силу замкнутости трассовой модели, проекция полной трассовой модели на алфавит $\mathbf{L}\cup\mathbf{R}\cup\{\Delta,\gamma\}$ совпадает с подмножеством ее трасс в этом алфавите.

Трассы σ и $\sigma`$ будем называть *T-эквивалентными* и обозначать $\sigma\sim_T\sigma`$, если они имеют одни и те же продолжения в трассовой модели $\mathbf{\Sigma}$: $\{\lambda\,|\,\sigma\cdot\lambda\in\mathbf{\Sigma}\}=\{\lambda\,|\,\sigma`\cdot\lambda\in\mathbf{\Sigma}\}$.

Замечание 1. Две трассы в LTS $\mathbf{S}$ T-эквивалентны тогда и только тогда, когда они заканчиваются в T-эквивалентных множествах состояний: $s_0\ \textbf{\textit{after}}\ \sigma\ \sim_T\ s_0\ \textbf{\textit{after}}\ \sigma` \Leftrightarrow \sigma\sim_T\sigma`$. Если две трассы заканчиваются в одном и том же множестве состояний, то они, очевидно, T-эквивалентны: $s_0\ \textbf{\textit{after}}\ \sigma\ =\ s_0\ \textbf{\textit{after}}\ \sigma` \Rightarrow \sigma\sim_T\sigma`$. Обратное, вообще говоря, не верно: трассы могут заканчиваться в T-эквивалентных, но разных множествах состояний.

1.4. RTS-модель

Трассовая модель имеет то преимущество перед LTS-моделью, что не содержит ничего «лишнего». Если при взаимодействии наблюдаемы только трассы, а не состояния, то существуют разные LTS-модели, неразличимые при взаимодействии с ними. Трассовая модель соответствует, фактически, классу таких неразличимых LTS-моделей. С другой стороны, LTS-модель более «наглядна», чем трассовая модель. Формально это означает, что любой граф с выделенной начальной вершиной и дугами, помеченными символами из алфавита $\mathbf{L}\cup\{\tau,\gamma\}$, является LTS-моделью в алфавите $\mathbf{L}$. В то же время далеко не любое множество $\mathbf{R}$-трасс в алфавите $\mathbf{L}$ (последовательностей в алфавите $\mathbf{L}\cup\mathbf{R}\cup\{\Delta,\gamma\}$) является трассовой моделью, оно должно быть непустым, префикс-замкнутым и должны выполняться указанные выше пять свойств трассовой модели.

Важно также то, что LTS-модель является способом конечного представления регулярных трассовых моделей, то есть регулярных множеств последовательностей, являющихся трассовыми моделями. Этот способ, однако, обладает одним существенным недостатком: LTS-модель, вообще говоря, недетерминирована: трасса может заканчиваться не в одном, а в нескольких состояниях. Работать с такими трассами на LTS неудобно. В то же время этот недетерминизм вовсе не является неизбежным следствием недетерминизма моделируемой системы. Причина недетерминизма LTS-модели в том, что наблюдения делятся на два вида: действия и отказы, которые существенно различным образом отображаются в LTS-модели. Если трасса продолжается как отказом R, так и действием $z\in R$, то эти два продолжения не могут быть определены в одном и том же состоянии LTS-модели.

С другой стороны, для трассовой модели (как и для любого множества последовательностей) всегда существует детерминированный порождающий

ее граф. Поскольку трассовая модель префикс-замкнута, существует такой порождающий ее граф, в котором только одна вершина начальная, и все вершины конечные[5]. Если трассовая модель регулярна, то такой порождающий граф может быть конечным. Порождающий граф, конечно, тоже является LTS, но не в исходном алфавите $\mathbf{L}$, а (для **R**/**Q**-семантики) в алфавите $\mathbf{L}\cup\mathbf{R}\cup\{\Delta\}$.[6] Кроме того, за детерминизм модели приходится чем-то «жертвовать»: не любая LTS в алфавите $\mathbf{L}\cup\mathbf{R}\cup\{\Delta\}$ является графом, порождающим трассовую модель в **R**/**Q**-семантике.

Для дальнейшего нам потребуется LTS, порождающая не все трассы трассовой модели $\mathbf{\Sigma}$, а подмножество $\mathbf{\Sigma}`\subseteq\mathbf{\Sigma}$, $\boldsymbol{d}$-замыкание которого дает всю трассовую модель: $\cup\boldsymbol{d}(\mathbf{\Sigma}`)=\mathbf{\Sigma}$. Дополнительно потребуем, чтобы отказам, повторным в трассах, в порождающей LTS соответствовали переходы-петли.

Определим *RTS-модель* (Refusal Transition System) как детерминированную LTS $\mathbf{S}=\mathrm{LTS}(V_{\mathbf{S}},\mathbf{L}\cup\mathbf{R}\cup\{\Delta\},E_{\mathbf{S}},s_0)$, где $\mathbf{R}\subseteq\mathcal{P}(\mathbf{L})$, с выделенным состоянием $\varpi\in V_{\mathbf{S}}$, которая обладает следующими свойствами: $\forall s,s`\in\boldsymbol{der}(\mathbf{S})\ \ \forall R,R`\in\mathbf{R}$

R1. <u>допустимость</u>: переход по дивергенции или разрушению заканчивается в состоянии ϖ, в этом состоянии не заканчиваются другие переходы, и это состояние терминально:

$$s\text{—}\Delta\to s`\ \Rightarrow\ s`=\varpi,\ \forall z\in\mathbf{L}\cup\mathbf{R}\ \ s\text{—}z\to s`\Rightarrow\ s`\neq\varpi,$$

$$s\text{—}\gamma\to s`\ \Rightarrow\ s`=\varpi,\ \forall z\in\mathbf{L}\cup\mathbf{R}\cup\{\Delta,\gamma\}\ \ \varpi\text{—}z\not\to;$$

R2. <u>согласованность</u>: если в состоянии определен переход-петля по **R**-отказу, то в состоянии не определены переходы по дивергенции, разрушению и действиям, принадлежащим этому отказу:

$$s\text{—}R\to s\ \Rightarrow\ \forall z\in R\cup\{\Delta,\gamma\}\ \ s\text{—}z\not\to;$$

R3. <u>конвергентность</u>: если состояние $s\neq\varpi$, и в нем не определены переходы по дивергенции и разрушению, то для каждого **R**-отказа в s определен переход по этому отказу или по действию из этого отказа:

$$s\neq\varpi\ \&\ s\text{—}\Delta\not\to\ \&\ s\text{—}\gamma\not\to\ \Rightarrow\ s\text{—}R\to\ \vee\ \exists z\in R\ \ s\text{—}z\to;$$

R4. <u>кумулятивность</u>: в конце перехода по отказу определен переход-петля по этому отказу и переходы-петли по всем тем отказам, по которым такие переходы-петли определены в начале перехода:

$$s\text{—}R\to s`\ \Rightarrow\ s`\text{—}R\to s`\ \&\ \forall R`\in\mathbf{R}\ \ (s\text{—}R`\to s\ \Rightarrow\ s`\text{—}R`\to s`);$$

---

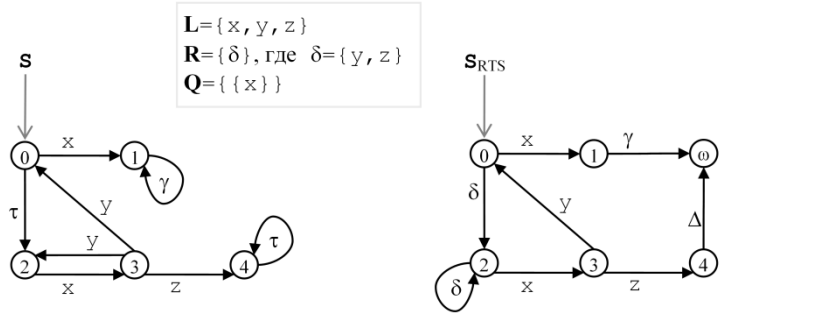
[5] Это условие не только необходимо, но и достаточно для префикс-замкнутости множества последовательностей [9][10].

[6] Для полной трассовой модели $\mathbf{R}=\mathcal{P}(\mathbf{L})$.

R5. полнота: если в состоянии определен переход-петля по **R**-отказу R и не определены переходы по действиям из **R**-отказа $R`$, то в этом состоянии определен переход-петля по $R`$:

$s \text{—} R \to s \;\&\; \forall z \in R` \;\; s \text{—} z \not\to \;\Rightarrow\; s \text{—} R` \to s.$

На Рис. 3. приведен пример RTS $\mathbf{S}_{RTS}$, ***d***-замыкание множества простых трасс которой совпадает с множеством **R**-трасс LTS **S**, взятой с Рис. 2. .



$$\boldsymbol{T}(\mathbf{S}_{RTS}) \;=\; (\delta\delta^*xy)^*(\,\delta\delta^*[x[z[\Delta]]] \mid [x[\gamma]]\,)$$

$$\boldsymbol{d}(\boldsymbol{T}(\mathbf{S}_{RTS})) \;=\; \boldsymbol{T}(\mathbf{R},\mathbf{S}) \;=\; \boldsymbol{T}(\mathbf{S}_{\mathbf{R}}) \;=\; (\delta^*xy)^*(\,\delta^*[x[z[\Delta]]] \mid x\gamma\,)$$

Рис. 3. Пример RTS и ее трасс

Множество всех RTS в алфавите **L** обозначим $\boldsymbol{RTS}(\mathbf{L})$.

Определим преобразование $\boldsymbol{L2R}\colon\ \boldsymbol{LTS}(\mathbf{L}) \to \boldsymbol{RTS}(\mathbf{L})$. Для LTS $\mathbf{S} = \mathrm{LTS}(V_S,\mathbf{L},E_S,s_0)$ множество $\boldsymbol{T}(\mathbf{R},\mathbf{S})$ ее **R**-трасс определяется как множество простых трасс LTS $\mathbf{S}_{\mathbf{R}} = \mathrm{LTS}(V_S \cup \{\omega\}, \mathbf{L} \cup \mathbf{R} \cup \{\Delta\}, E_{\mathbf{R}}, s_0)$. LTS $\mathbf{S}_{\mathbf{R}}$ есть, по сути, граф, порождающий множество $\boldsymbol{T}(\mathbf{R},\mathbf{S})$, в котором начальная вершина – состояние s_0, и все вершины (состояния) конечные. Мы применим обычную процедуру детерминизации порождающего графа, основанную на построении power-графа [27]. Состояниями будут непустые подмножества состояний LTS $\mathbf{S}_{\mathbf{R}}$, начальное состояние s_0 ***after*** ϵ, а переход $A \text{—} z \to B$ для каждого $z \in \mathbf{L} \cup \mathbf{R} \cup \{\Delta,\gamma\}$ определяется тогда, когда во множестве A есть состояние, в котором начинается трасса $\langle z \rangle$, и множество B – это множество конечных состояний всех таких трасс для всех состояний из A. Формально $\boldsymbol{L2R}(\mathbf{S}) = \mathbf{T} = \mathrm{LTS}(V_{\mathbf{T}}, \mathbf{L} \cup \mathbf{R} \cup \{\Delta\}, E_{\mathbf{T}}, t_0)$, где

$V_T = \mathcal{P}(V_S \cup \{\omega\}) \setminus \{\varnothing\}$, $t_0 = s_0$ ***after*** ϵ, а множество переходов E_T определяется как наименьшее множество, порождаемое следующим правилом вывода:

$\forall A, B \in \mathcal{P}(V_S \cup \{\omega\}) \setminus \{\varnothing\}$ $\forall z \in \mathbf{L} \cup \mathbf{R} \cup \{\Delta, \gamma\}$

$B = \cup(A$ ***after*** $\langle z \rangle) \neq \varnothing \quad \vdash A \text{—}z\text{→} B,$

где оператор ***after*** берется по LTS $\mathbf{S_R}$.

Теорема 1: **О преобразовании *L2R*.** Для любой LTS **S** преобразование ***L2R*** дает LTS $\mathbf{T}=\boldsymbol{L2R}(\mathbf{S})$, которая является RTS и множество простых трасс которой совпадает с множеством **R**-трасс исходной LTS: $\boldsymbol{T}(\mathbf{T})=\boldsymbol{T}(\mathbf{R},\mathbf{S})$. При этом если **S** имеет конечное число состояний, то LTS **T** также имеет конечное число состояний.

Доказательство см. на стр.99

Преобразование ***L2R*** дает RTS, множество простых трасс которой является **R**-моделью. Для произвольной RTS множество ее простых трасс, вообще говоря, не является **R**-моделью. Однако мы покажем, что ***d***-замыкание этого множества является **R**-моделью. Для этого мы определим преобразование ***R2L***, которое по RTS строит LTS, множество **R**-трасс которой, то есть **R**-модель, совпадает с ***d***-замыканием множества простых трасс исходной RTS.

Идея преобразования $\boldsymbol{R2L}: \boldsymbol{RTS}(\mathbf{L}) \rightarrow \boldsymbol{LTS}(\mathbf{L})$ заключается в следующем. Каждая непустая цепочка переходов по отказам, начинающаяся в состоянии без петель по отказам, заменяется на τ-переход. Переход по внешнему действию, за которым следует цепочка переходов по отказам, заменяется на переход по этому действию. Переход по разрушению сохраняется, а переход по дивергенции заменяется на τ-петлю. Кроме того, вводится новое начальное состояние ε, и каждая (в том числе, пустая) цепочка переходов по отказам, начинающаяся в начальном состоянии RTS, заменяется на τ-переход из состояния ε. Формально, для RTS $\mathbf{T} = \mathrm{LTS}(V_T, \mathbf{L} \cup \mathbf{R} \cup \{\Delta\}, E_T, t_0)$ LTS $\boldsymbol{R2L}(\mathbf{T}) = \mathbf{S} = \mathrm{LTS}((V_T \cup \{\varepsilon\}) \setminus \{\varpi\}, \mathbf{L}, E_S, \varepsilon)$, где состояние $\varepsilon \notin V_T$, а множество переходов E_S определяется как наименьшее множество, порождаемое следующими правилами вывода:

$\forall A, B \in V_T \quad \forall z \in \mathbf{L} \quad \forall P \in \mathbf{R} \quad \forall \rho \in \mathbf{R}^*$

$t_0 = \rho \Rightarrow B \quad \vdash \varepsilon \text{—}\tau\text{→} B,$

$A = \rho \Rightarrow B \;\&\; \rho \neq \epsilon \;\&\; \forall R \in \mathbf{R}\ A = \langle R \rangle \not\Rightarrow A \quad \vdash A \text{—}\tau\text{→} B,$

$A = \langle z \rangle \cdot \rho \Rightarrow B \quad \vdash A \text{—}z\text{→} B,$

$A \text{—}\gamma\text{→} \varpi \quad \vdash A \text{—}\gamma\text{→} A,$

$A \text{—}\Delta\text{→} \varpi \quad \vdash A \text{—}\tau\text{→} A.$

Теорема 2: **О преобразовании *R2L*.** Для любой RTS **T** преобразование ***R2L*** дает LTS **S**=***R2L***(**T**), множество **R**-трасс которой совпадает с ***d***-замыканием множества простых трасс исходной RTS: ***T***(**R**,**S**)=∪***d***(***T***(**T**)). При этом если **T** имеет конечное число состояний, то LTS **S** имеет такое же число состояний.

Доказательство см. на стр.102

Любая RTS **T** однозначно определяет трассовую **R**-модель (как ***d***-замыкание множества ее простых трасс). Соответственно, может быть несколько разных полных трассовых моделей, построенных как расширение этой **R**-модели. Одной из таких моделей является модель ***Ext***(∪***d***(***T***(**T**))). Легко показать, что эта же полная трассовая модель может быть получена с помощью преобразования ***R2L*** и взятия множества ее полных трасс.

Итак, все три модели: LTS-модель, трассовая модель и RTS-модель эквивалентны в том смысле, что могут быть преобразованы одна в другую с сохранением множества определяемых ими полных трасс.

На Рис. 4. приведены результаты преобразований ***L2R***(**S**) и ***R2L***(***L2R***(**S**)) для LTS **S** с Рис. 2. . Можно увидеть различие между RTS ***L2R***(**S**) и RTS $\mathbf{S}_{RTS}$ с Рис. 3. . Хотя эти RTS определяют одну и ту же трассовую **R**-модель ***T***($\mathbf{S}_R$), множества их простых трасс различны. Для RTS ***L2R***(**S**) множество ее простых трасс уже совпадает с **R**-моделью ***T***($\mathbf{S}_R$), следовательно, ***d***-замкнуто, и его ***d***-замыкание ничего не добавляет. В то же время для RTS $\mathbf{S}_{RTS}$ множество ее простых трасс не является **R**-моделью, но его ***d***-замыкание совпадает с **R**-моделью ***T***($\mathbf{S}_R$).

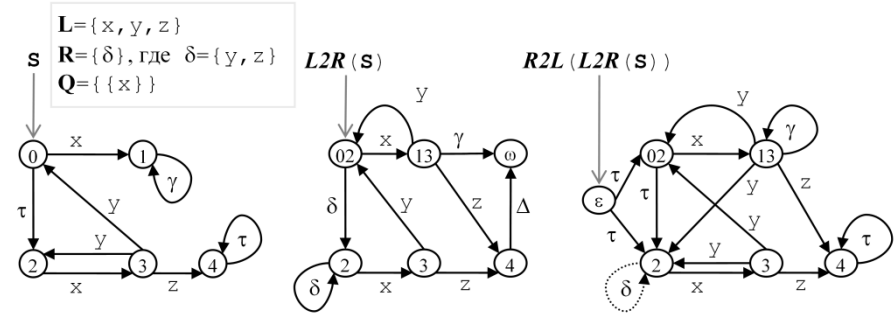


*Рис. 4. Преобразования **L2R** и **R2L***

1.5. Гипотеза о безопасности и безопасная конформность

В силу эквивалентности трассовой, LTS- и RTS-моделей нам достаточно определить гипотезу о безопасности и безопасную конформность только для полных трассовых моделей реализации и спецификации. Когда используется LTS- или RTS-модель, в соответствующих определениях применяется соответствующая этим моделям полная трассовая модель.

Безопасное тестирование, прежде всего, предполагает формальное определение на уровне модели отношения безопасности «кнопка P безопасна в модели M после трассы σ». При безопасном тестировании будут нажиматься только безопасные кнопки. Это отношение различно для реализационной и спецификационной моделей.

Для произвольного множества трасс $\mathbf{N}$ будем говорить, что кнопка P после трассы $\sigma \in \mathbf{N}$ *неразрушающая* и обозначать P ***safe***$_{\gamma\Delta}$ $\mathbf{N}$ ***after*** σ, если ее нажатие не может означать попытку выхода из дивергенции (трасса не продолжается дивергенцией в $\mathbf{N}$) и не может вызывать разрушение (после действия, разрешаемого кнопкой). Формально: $\forall P \in \mathbf{R} \cup \mathbf{Q} \quad \forall \sigma \in \mathbf{N}$

$$P \; \textbf{\textit{safe}}_{\gamma\Delta} \; \mathbf{N} \; \textbf{\textit{after}} \; \sigma \;\triangleq\; \sigma \cdot \langle \Delta \rangle \notin \mathbf{N} \;\;\&\;\; \forall z \in P \;\; \sigma \cdot \langle z, \gamma \rangle \notin \mathbf{N}.$$

В полной трассовой реализации $\mathbf{I}$ отношение безопасности обозначается ***safe in*** и означает, во-первых, что кнопка P после трассы σ *неразрушающая* и, во-вторых, нажатие кнопки не может привести к ненаблюдаемому отказу (если это **Q**-кнопка): $\forall P \in \mathbf{R} \cup \mathbf{Q} \quad \forall \sigma \in \mathbf{I}$

$$P \; \textbf{\textit{safe in}} \; \mathbf{I} \; \textbf{\textit{after}} \; \sigma \;\triangleq\; P \; \textbf{\textit{safe}}_{\gamma\Delta} \; \mathbf{I} \; \textbf{\textit{after}} \; \sigma \;\;\&\;\; (P \in \mathbf{Q} \;\Rightarrow\; \sigma \cdot \langle P \rangle \notin \mathbf{I}).$$

В полной трассовой спецификации $\mathbf{\Sigma}$ отношение безопасности обозначается ***safe by*** и отличается только для **Q**-кнопок: мы не требуем, чтобы после трассы σ не было **Q**-отказа Q, но требуем, чтобы было хотя бы одно действие $z \in Q$. Кроме того, если действие разрешается хотя бы одной неразрушающей кнопкой, то оно должно разрешаться какой-нибудь безопасной кнопкой. Если это неразрушающая **R**-кнопка, то она же и безопасна. Но если все неразрушающие кнопки, разрешающие действие, являются **Q**-кнопками, то хотя бы одна из них должна быть объявлена безопасной.

Такое отношение безопасности всегда существует: достаточно объявить безопасной каждую неразрушающую **Q**-кнопку, разрешающую действие, продолжающее трассу. Однако в целом указанные требования неоднозначно определяют отношение ***safe by***, и при задании спецификации $\mathbf{\Sigma}$ указывается конкретное отношение.

Требования к отношению ***safe by*** записываются так:

$\forall R \in \mathbf{R} \quad \forall z \in \mathbf{L} \quad \forall Q \in \mathbf{Q} \quad \forall \sigma \in \mathbf{\Sigma}$

1) R ***safe by*** $\mathbf{\Sigma}$ ***after*** $\sigma \;\Leftrightarrow\; R$ ***safe***$_{\gamma\Delta}$ $\mathbf{\Sigma}$ ***after*** σ,

2) $\exists U \in \mathbf{R} \cup \mathbf{Q}\ \ U\ \textbf{\textit{safe}}_{\gamma\Delta}\ \Sigma\ \textbf{\textit{after}}\ \sigma\ \ \&\ \ z \in U\ \ \&\ \ \sigma \cdot \langle z \rangle \in \Sigma$

$\Rightarrow\ \exists P \in \mathbf{R} \cup \mathbf{Q}\ \ z \in P\ \ \&\ \ P\ \textbf{\textit{safe by}}\ \Sigma\ \textbf{\textit{after}}\ \sigma$,

3) $Q\ \textbf{\textit{safe by}}\ \Sigma\ \textbf{\textit{after}}\ \sigma\ \Rightarrow\ Q\ \textbf{\textit{safe}}_{\gamma\Delta}\ \Sigma\ \textbf{\textit{after}}\ \sigma\ \ \&\ \ \exists v \in Q\ \ \sigma \cdot \langle v \rangle \in \Sigma$.

Безопасность кнопок определяет безопасность наблюдений. **R**-отказ R безопасен, если после трассы безопасна кнопка R. Действие z безопасно, если оно разрешается некоторой кнопкой, безопасной после трассы:

$z\ \textbf{\textit{safe in}}\ I\ \textbf{\textit{after}}\ \sigma\ \triangleq\ \exists P \in \mathbf{R} \cup \mathbf{Q}\ \ z \in P\ \ \&\ \ P\ \textbf{\textit{safe in}}\ I\ \textbf{\textit{after}}\ \sigma$.

$z\ \textbf{\textit{safe by}}\ \Sigma\ \textbf{\textit{after}}\ \sigma\ \triangleq\ \exists P \in \mathbf{R} \cup \mathbf{Q}\ \ z \in P\ \ \&\ \ P\ \textbf{\textit{safe by}}\ \Sigma\ \textbf{\textit{after}}\ \sigma$.

Теперь мы можем определить *безопасные* **R**-*трассы*. **R**-трасса σ безопасна, если эта трасса есть в модели и 1) модель не разрушается с самого начала (сразу после включения машины ещё до нажатия первой кнопки), то есть в ней нет трассы $\langle \gamma \rangle$, 2) каждый символ трассы безопасен после непосредственно предшествующего ему префикса трассы:

$\sigma \in I\ \ \&\ \ \langle \gamma \rangle \notin I\ \ \&\ \ \forall \mu\ \ \forall u\ \ (\mu \cdot \langle u \rangle \le \sigma\ \Rightarrow\ u\ \textbf{\textit{safe in}}\ I\ \textbf{\textit{after}}\ \mu)$,

$\sigma \in \Sigma\ \ \&\ \ \langle \gamma \rangle \notin \Sigma\ \ \&\ \ \forall \mu\ \ \forall u\ \ (\mu \cdot \langle u \rangle \le \sigma\ \Rightarrow\ u\ \textbf{\textit{safe by}}\ \Sigma\ \textbf{\textit{after}}\ \mu)$.

Для подразумеваемой семантики **R**/**Q** множество безопасных трасс реализации I обозначим $\textbf{\textit{SafeIn}}(I)$. Для подразумеваемых семантики **R**/**Q** и отношения ***safe by*** множество безопасных трасс спецификации Σ обозначим $\textbf{\textit{SafeBy}}(\Sigma)$.

Для любой спецификации Σ в общем случае $\textbf{\textit{SafeIn}}(\Sigma) \ne \textbf{\textit{SafeBy}}(\Sigma)$, но имеет место вложенность $\textbf{\textit{SafeIn}}(\Sigma) \subseteq \textbf{\textit{SafeBy}}(\Sigma)$.

Действительно, если пустая трасса безопасна по ***safe in***, то она безопасна по ***safe by***. Пусть трасса $\sigma \cdot \langle u \rangle \in \textbf{\textit{SafeIn}}(\Sigma)$. Тогда $\sigma \cdot \langle u \rangle \in \Sigma$, $\sigma \in \textbf{\textit{SafeIn}}(\Sigma)$ и наблюдение $u\ \textbf{\textit{safe in}}\ \Sigma\ \textbf{\textit{after}}\ \sigma$. Если u – это **R**-отказ, то $u\ \textbf{\textit{safe by}}\ \Sigma\ \textbf{\textit{after}}\ \sigma$, так как безопасность **R**-кнопок после трасс определяется одинаково для ***safe in*** и ***safe by***. Если u – это действие, то найдется такая кнопка P, что $u \in P$ и $P\ \textbf{\textit{safe in}}\ \Sigma\ \textbf{\textit{after}}\ \sigma$. Но тогда $P\ \textbf{\textit{safe}}_{\gamma\Delta}\ \Sigma\ \textbf{\textit{after}}\ \sigma$, что вместе с $\sigma \cdot \langle u \rangle \in \Sigma$ влечет по второму правилу для ***safe by*** наличие кнопки $P`\ \textbf{\textit{safe by}}\ \Sigma\ \textbf{\textit{after}}\ \sigma$ такой, что $u \in P`$. Следовательно, $u\ \textbf{\textit{safe by}}\ \Sigma\ \textbf{\textit{after}}\ \sigma$ и $\sigma \cdot \langle u \rangle \in \textbf{\textit{SafeBy}}(\Sigma)$.

Замечание 2. Пустая **Q**-кнопка опасна как после любой безопасной по отношению ***safe in*** трассы любой реализации, так и после любой безопасной

по любому отношению ***safe by*** трассы любой спецификации. Такую кнопку никогда нельзя нажимать при безопасном тестировании. Поэтому в дальнейшем будем считать, что такой **Q**-кнопки в семантике нет: $\varnothing \notin \mathbf{Q}$. В то же время пустая **R**-кнопка имеет смысл: она безопасна после любой безопасной трассы, не продолжающейся дивергенцией, а наблюдение пустого **R**-отказа означает, что реализация оказалась в стабильном состоянии.

Замечание 3. Отношение $\boldsymbol{safe}_{\gamma\Delta}$, вообще говоря, не удовлетворяет 3-ему требованию к отношению ***safe by***. Однако, если каждая безопасная по $\boldsymbol{safe}_{\gamma\Delta}$ трасса для каждой неразрушающей (безопасной по $\boldsymbol{safe}_{\gamma\Delta}$) **Q**-кнопки Q продолжается каким-нибудь действием $z \in Q$, то отношение $\boldsymbol{safe}_{\gamma\Delta}$ будет удовлетворять всем трем требованиям к отношению ***safe by***.

Требование безопасности тестирования выделяет класс *безопасно-тестируемых* реализаций, то есть таких, которые могут быть безопасно протестированы для проверки их конформности или неконформности заданной спецификации. Этот класс определяется следующей *гипотезой о безопасности*: реализация $\mathbf{I}$ *безопасно-тестируема* для спецификации $\boldsymbol{\Sigma}$, если:

1) в реализации нет разрушения с самого начала, если этого нет в спецификации,

2) после общей безопасной трассы реализации и спецификации любая кнопка, безопасная в спецификации, безопасна после этой трассы в реализации:

$$\mathbf{I}\ \textit{safe for}\ \boldsymbol{\Sigma} \triangleq (\langle\gamma\rangle \notin \boldsymbol{\Sigma} \Rightarrow \langle\gamma\rangle \notin \mathbf{I})\ \&\ \forall \sigma \in \boldsymbol{SafeBy}(\boldsymbol{\Sigma}) \cap \boldsymbol{SafeIn}(\mathbf{I})\ \ \forall P \in \mathbf{R} \cup \mathbf{Q}$$
$$(P\ \textit{safe by}\ \boldsymbol{\Sigma}\ \textit{after}\ \sigma \Rightarrow P\ \textit{safe in}\ \mathbf{I}\ \textit{after}\ \sigma).$$

После этого можно определить отношение (безопасной) *конформности*: реализация $\mathbf{I}$ *безопасно конформна* (или просто *конформна*) спецификации $\boldsymbol{\Sigma}$, если она безопасна и выполнено *тестируемое условие*: любое наблюдение, возможное в реализации в ответ на нажатие безопасной (в спецификации) кнопки, разрешается спецификацией:

$$\mathbf{I}\ \textit{saco}\ \boldsymbol{\Sigma} \triangleq \mathbf{I}\ \textit{safe for}\ \boldsymbol{\Sigma}$$
$$\&\ \forall \sigma \in \boldsymbol{SafeBy}(\boldsymbol{\Sigma}) \cap \boldsymbol{SafeIn}(\mathbf{I})\ \ \forall P\ \textit{safe by}\ \boldsymbol{\Sigma}\ \textit{after}\ \sigma\ \ \boldsymbol{obs}(\sigma, P, \mathbf{I}) \subseteq \boldsymbol{obs}(\sigma, P, \boldsymbol{\Sigma}),$$

где $\boldsymbol{obs}(\sigma, P, \mathbf{M}) \triangleq \{u \mid \sigma \cdot \langle u \rangle \in \mathbf{M}\ \&\ (u \in P \vee u = P\ \&\ P \in \mathbf{R})\}$ – множество наблюдений, которые можно получить над полной трассовой моделью $\mathbf{M}$ при нажатии кнопки P после трассы σ.

Следует отметить, что гипотеза о безопасности не проверяема при тестировании и является его предусловием; тестирование проверяет тестируемое условие конформности.

Замечание 4. В определении гипотезы о безопасности и конформности вместо условия $\sigma \in \boldsymbol{SafeIn}(\mathbf{I})$ достаточно условия $\sigma \in \mathbf{I}$ [10].

Замечание 5. Из определения отношений безопасности ***safe by*** и ***safe in*** видно, что для фиксированной **R**/**Q**-семантики в определениях отношений ***safe for*** и ***saco*** существенны не множества всех полных трасс спецификации **Σ** и реализации **I**, а их подмножества. Для спецификации **Σ** существенно только подмножество ее **R**-трасс $\mathbf{\Sigma}{\downarrow}(\mathbf{L}\cup\mathbf{R}\cup\{\gamma,\Delta\})$, а для реализации **I** – кроме множества ее **R**-трасс $\mathbf{I}{\downarrow}(\mathbf{L}\cup\mathbf{R}\cup\{\gamma,\Delta\})$, еще их продолжения **Q**-отказами, то есть подмножество множества **R**∪**Q**-трасс $\mathbf{I}{\downarrow}(\mathbf{L}\cup\mathbf{R}\cup\mathbf{Q}\cup\{\gamma,\Delta\})$.

Определенные выше гипотеза о безопасности и конформность называются трассовыми, поскольку они основаны только на полных трассах наблюдений.[7] LTS-спецификация в этих определениях сводится к множеству ее **R**-трасс. Соответственно, RTS-спецификация в этих определениях сводится к ***d***-замыканию множества ее простых трасс, которое является **R**-моделью. Заметим, что в отличие от LTS в алфавите **L**, которую можно рассматривать как спецификацию в любой **R**/**Q**-семантике, где $\cup\mathbf{R}\cup\cup\mathbf{Q}=\mathbf{L}$, RTS-спецификация в алфавите $\mathbf{L}\cup\mathbf{R}\cup\{\Delta\}$ рассматривается только в такой **R`**/**Q`**-семантике, где множество **R`** наблюдаемых отказов фиксировано: **R`**=**R** и $\cup\mathbf{R`}\cup\cup\mathbf{Q`}=\mathbf{L}$.

Тестовой трассой будем называть безопасную трассу или трассу $\sigma\cdot\langle u\rangle$, где трасса σ безопасна в спецификации, а наблюдение u безопасно в спецификации **Σ** после σ (но не обязательно продолжает σ в **Σ**): $\sigma\in\mathbf{SafeBy}(\mathbf{\Sigma})$ & u ***safe by*** **Σ** ***after*** σ. Для подразумеваемых семантики **R**/**Q** и отношения ***safe by*** множество тестовых трасс спецификации обозначим $\mathbf{tt}(\mathbf{\Sigma})$. При безопасном тестировании могут проходиться только тестовые трассы.

1.6. Спецификационные тройки и отношения на тройках

Для трассовых моделей гипотеза о безопасности и конформность задаются *спецификационной тройкой* $\mathbf{T}=(\mathbf{R}/\mathbf{Q},\mathbf{\Sigma},\mathbf{safe\ by})$, то есть семантикой взаимодействия **R**/**Q**, трассовой спецификационной моделью **Σ** в алфавите $\mathbf{L}=\cup\mathbf{R}\cup\cup\mathbf{Q}$ и отношением безопасности кнопок ***safe by***.

Поскольку множества $\mathbf{SafeBy}(\mathbf{\Sigma})$ безопасных трасс и $\mathbf{tt}(\mathbf{\Sigma})$ тестовых трасс спецификации зависят от подразумеваемых семантики и отношения безопасности кнопок, там, где мы будем рассматривать различные

[7] Другим видом конформности является симуляция, основанная, кроме того, на соответствии состояний реализации и спецификации. Вопросы безопасной симуляции и ее тестирования рассмотрены в наших работах [17][18][19].

спецификационные тройки, мы будем обозначать эти множества как $\mathbf{SafeBy(T)}$ безопасных трасс и $\mathbf{tt(T)}$ тестовых трасс, соответственно.

Спецификационная тройка $\mathbf{T=(R/Q,\Sigma,}$***safe by***$\mathbf{)}$ определяет классы безопасно-тестируемых и конформных LTS-реализаций:

$\mathbf{SafeImp(T)} \triangleq \{\mathbf{I}\in\mathbf{MODEL(L)} \mid \mathbf{I}$ ***safe for*** $\mathbf{\Sigma}\}$,

$\mathbf{ConfImp(T)} \triangleq \{\mathbf{I}\in\mathbf{MODEL(L)} \mid \mathbf{I}$ ***saco*** $\mathbf{\Sigma}\}$.

Будем обозначать $\mathbf{T_i=(R_i/Q_i,\Sigma_i,}$***safe by***$_\mathbf{i}\mathbf{)}$. Определим на множестве спецификационных троек отношение предпорядка «вложенность троек» $\mathbf{T_1 \le T_2}$ как равенство классов конформных реализаций и вложенность классов безопасно-тестируемых реализаций.

Замечание 6. Если $\mathbf{T_1 \le T_2}$, тройка $\mathbf{T_2}$ может использоваться вместо тройки $\mathbf{T_1}$, поскольку она позволяет безопасно тестировать все те реализации, которые могли безопасно тестироваться по тройке $\mathbf{T_1}$, хотя, быть может, позволяет тестировать и другие реализации (класс безопасно-тестируемых реализаций может расшириться), но в то же время конформными считаются те и только те реализации, которые конформны для тройки $\mathbf{T_1}$.

Сначала определим этот предпорядок «≤» для троек в одном алфавите $\mathbf{L=\cup R_1\cup\cup Q_1=\cup R_2\cup\cup Q_2}$:

$\mathbf{T_1 \le T_2} \triangleq \mathbf{ConfImp(T_1) = ConfImp(T_2)}\ \&\ \mathbf{SafeImp(T_1) \subseteq SafeImp(T_2)}$.

Если алфавиты спецификационных троек разные, то классы реализаций также рассматриваются в разных алфавитах и, чтобы их сравнивать, нужно привести их к «единому знаменателю». Таким «знаменателем» может служить любой «целевой» класс интересующих нас реализаций: вместо классов конформных и безопасно-тестируемых реализаций рассматриваются их пересечения с этим «целевым» классом реализаций. Для наших целей достаточно в качестве такого «целевого» класса брать класс всех моделей в некотором «целевом» алфавите.

Определим «приведение» к алфавиту $\mathbf{L}$ разрушения, дивергенции, действия, множества действий, семейств кнопок $\mathbf{R_i}$ и $\mathbf{Q_i}$, трассы σ, множества трасс $\mathbf{I}$, семейства $\mathbf{K}$ множеств трасс и LTS $\mathbf{S}=\mathtt{LTS}(\mathtt{V_S},\mathbf{L_i},\mathtt{E_S},\mathtt{s_0})$:

$\gamma_\mathbf{L} \triangleq \gamma$, $\Delta_\mathbf{L} \triangleq \Delta$; если $\mathtt{u}\in\mathbf{L_i}$, то $\mathtt{u}_\mathbf{L} \triangleq \mathtt{u}$; если $\mathtt{U}\subseteq\mathbf{L_i}$, то $\mathtt{U}_\mathbf{L} \triangleq \mathtt{U}\cap\mathbf{L}$;

$\mathbf{R_{iL}} \triangleq \{\mathtt{R}_\mathbf{L} \mid \mathtt{R}\in\mathbf{R_i}\}$; $\mathbf{Q_{iL}} \triangleq \{\mathtt{Q}_\mathbf{L} \mid \mathtt{Q}\in\mathbf{Q_i}\}$;

$\sigma_\mathbf{L} \triangleq \langle\sigma(\mathtt{i})_\mathbf{L} \mid \mathtt{i}=1..|\sigma|\rangle$; $\mathbf{I_L} \triangleq \{\sigma_\mathbf{L} \mid \sigma\in\mathbf{I}\}$; $\mathbf{K_L} \triangleq \{\mathbf{I_L} \mid \mathbf{I}\in\mathbf{K}\}$;

если $\mathtt{E_S}\subseteq\mathtt{V_S}\times(\mathbf{L}\cup\{\tau,\gamma\})\times\mathtt{V_S}$, то $\mathbf{S_L} \triangleq \mathtt{LTS}(\mathtt{V_S},\mathbf{L},\mathtt{E_S},\mathtt{s_0})$.

L-*наблюдением* будем называть действия из алфавита $\mathbf{L}$ (**L**-*действия*), $\mathbf{R_i}$-отказы, а также дивергенцию Δ и разрушение γ, то есть элемент множества $\mathbf{L}\cup\mathbf{R_i}\cup\{\Delta,\gamma\}$. В общем случае $\sigma\in(\mathbf{L_i}\cup\mathbf{R_i}\cup\{\Delta,\gamma\})^*$ и $\sigma_\mathbf{L}\in(\mathbf{L_i}\cup\mathbf{R_{iL}}\cup\{\Delta,\gamma\})^*$, то есть в трассах σ и $\sigma_\mathbf{L}$ могут встречаться

действия не из алфавита **L.** Трассу σ будем называть **L**-*трассой*, если все ее действия из алфавита **L**, кроме, быть может, дивергенции или разрушения в конце трассы: $\sigma\hat{}\in(\mathbf{L}\cup\{\Delta,\gamma\})^*$. Иными словами, **L**-трасса – это трасса $\sigma\in(\mathbf{L}\cup\mathbf{R_i}\cup\{\Delta,\gamma\})^*$, что эквивалентно $\sigma_{\mathbf{L}}\in(\mathbf{L}\cup\mathbf{R_{iL}}\cup\{\Delta,\gamma\})^*$. **L**-трасса – это трасса, состоящая из **L**-наблюдений.

Для заданной спецификационной тройки $\mathbf{T_i}=(\mathbf{R_i}/\mathbf{Q_i},\Sigma_\mathbf{i},\textit{safe by}_\mathbf{i})$ под реализациями по умолчанию считаются модели в алфавите $\mathbf{L_i}=\cup\mathbf{R_i}\cup\mathbf{Q_i}$. Для трассовой реализации **I** в общем случае $\mathbf{I_L}\not\in\textit{MODEL}(\mathbf{L})$, то есть некоторые трассы из **I** могут содержать действия не из алфавита **L**, и, следовательно, $\mathbf{I_L}$ не будет трассовой моделью в алфавите **L.** Для LTS-реализации **S** в общем случае может быть не выполнено условие «приведения» к алфавиту **L,** то есть некоторые переходы из $\mathsf{E_S}$ могут быть помечены действиями не из $\mathbf{L}\cup\{\tau,\gamma\}$. Реализация (LTS или трассовая), все трассы которой являются **L**-трассами, будем называть **L**-*реализацией*. Если реализация является **L**-реализацией, то это такая трассовая реализация **I**, что $\mathbf{I_L}\in\textit{MODEL}(\mathbf{L})$, или такая LTS-реализация **S**, что определена LTS $\mathbf{S_L}\in\textit{LTS}(\mathbf{L})$.

Обозначим множества конформных и безопасно-тестируемых трассовых **L**-реализаций:

$$\textit{ConfImp}(\mathbf{T_i},\mathbf{L}) \triangleq \{\mathbf{I}\in\textit{ConfImp}(\mathbf{T_i})\mid\mathbf{I_L}\in\textit{MODEL}(\mathbf{L})\},$$

$$\textit{SafeImp}(\mathbf{T_i},\mathbf{L}) \triangleq \{\mathbf{I}\in\textit{SafeImp}(\mathbf{T_i})\mid\mathbf{I_L}\in\textit{MODEL}(\mathbf{L})\}.$$

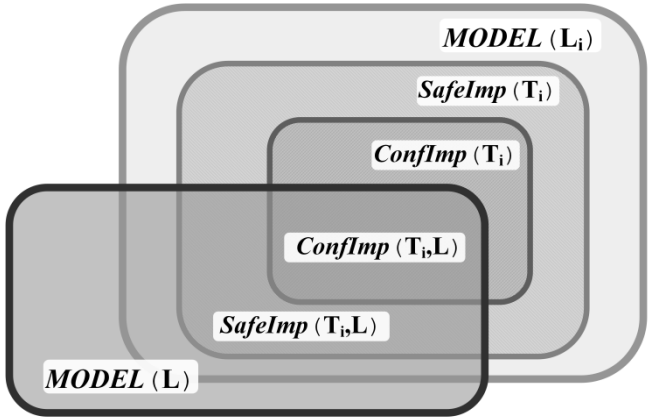


*Рис. 5. Классы безопасно-тестируемых и конформных (**L**-)реализаций*

Множества безопасных и тестовых **L**-трасс для тройки $\mathbf{T_i}$ будем обозначать:

$$\mathit{SafeBy}(\mathbf{T_i},\mathbf{L}) \triangleq \{\sigma\in\mathit{SafeBy}(\mathbf{T_i}) \mid \sigma\hat{}\in\mathbf{L}^*\},$$

$$\mathit{tt}(\mathbf{T_i},\mathbf{L}) \triangleq \{\sigma\in\mathit{tt}(\mathbf{T_i}) \mid \sigma\hat{}\in\mathbf{L}^*\}.$$

Тогда предпорядок вложенности на произвольных спецификационных тройках для целевого алфавита $\mathbf{L}$ определяется так:

$$\mathbf{T_1} \le_{\mathbf{L}} \mathbf{T_2} \triangleq \mathit{ConfImp}(\mathbf{T_1},\mathbf{L})_{\mathbf{L}} = \mathit{ConfImp}(\mathbf{T_2},\mathbf{L})_{\mathbf{L}} \;\&\; \mathit{SafeImp}(\mathbf{T_1},\mathbf{L})_{\mathbf{L}} \subseteq \mathit{SafeImp}(\mathbf{T_2},\mathbf{L})_{\mathbf{L}}.$$

Для заданной тройки $\mathbf{T}$ отношение вложенности определяет верхний конус: $\nabla(\mathbf{T})=\{\mathbf{T_i} \mid \mathbf{T} \le_{\mathbf{L}} \mathbf{T_i}\}$.[8]

Как обычно, отношение предпорядка индуцирует отношения эквивалентности. Две спецификационные тройки *эквивалентны* ($\approx_{\mathbf{L}}$), если они определяют одни и те же классы конформных и безопасно-тестируемых реализаций:

$$\mathbf{T_1} \approx_{\mathbf{L}} \mathbf{T_2} \triangleq \mathbf{T_1} \le_{\mathbf{L}} \mathbf{T_2} \;\&\; \mathbf{T_2} \le_{\mathbf{L}} \mathbf{T_1},$$

что эквивалентно:

$$\mathbf{T_1} \approx_{\mathbf{L}} \mathbf{T_2} \triangleq \mathit{ConfImp}(\mathbf{T_1},\mathbf{L})_{\mathbf{L}} = \mathit{ConfImp}(\mathbf{T_2},\mathbf{L})_{\mathbf{L}} \;\&\; \mathit{SafeImp}(\mathbf{T_1},\mathbf{L})_{\mathbf{L}} = \mathit{SafeImp}(\mathbf{T_2},\mathbf{L})_{\mathbf{L}}.$$

Преобразование f спецификационных троек будем называть вложенным или эквивалентным, если, соответственно: $\mathbf{T} \le_{\mathbf{L}} f(\mathbf{T})$ или $\mathbf{T} \approx_{\mathbf{L}} f(\mathbf{T})$.

Разные семантики определяют, вообще говоря, разные тестовые возможности по управлению реализацией и наблюдению за ее поведением. Однако, если ограничиться реализациями в алфавите $\mathbf{L}$, то разные семантики $\mathbf{R}_1/\mathbf{Q}_1$ и $\mathbf{R}_2/\mathbf{Q}_2$ определяют одни те же тестовые возможности тогда и только тогда, когда кнопки одной семантики отличаются от кнопок другой семантики только «лишними» действиями, то есть действиями, не принадлежащими алфавиту $\mathbf{L}$.

Если $\mathbf{R}_{1\mathbf{L}} = \mathbf{R}_{2\mathbf{L}}$ и $\mathbf{Q}_{1\mathbf{L}} = \mathbf{Q}_{2\mathbf{L}}$, то такие семантики $\mathbf{R}_1/\mathbf{Q}_1$ и $\mathbf{R}_2/\mathbf{Q}_2$, определяющие одни и те же тестовые возможности для реализаций в алфавите $\mathbf{L}$, будем называть $\mathbf{L}$-*эквивалентными* и обозначать $\mathbf{R}_1/\mathbf{Q}_1 \approx_{\mathbf{L}} \mathbf{R}_2/\mathbf{Q}_2$. Подмножество троек из верхнего конуса $\nabla(\mathbf{T})$, семантики которых $\mathbf{L}$-

[8] Обычно (но не всегда) символ «△» используют для обозначения верхнего конуса множества элементов частично-упорядоченного множества, а символ «▽» – для нижнего конуса. В данной работе мы выбрали для верхнего конуса символ «∇» по двум причинам. Во-первых, символ «△» очень похож на символ «Δ», обозначающий дивергенцию, что может ввести читателя в заблуждение. Во-вторых, из мнемонических соображений: мы используем верхний конус не множества элементов, которому соответствует нижняя сторона символа «△», а одного элемента, которому лучше соответствует нижняя вершина символа «∇».

эквивалентны семантике исходной тройке **T**, будем называть **L**-*конусом* и обозначать:

$\nabla(\mathbf{T})_{\mathbf{L}} \triangleq \{\mathbf{T_i} \in \nabla(\mathbf{T}) \mid \mathbf{R_i/Q_i} \approx_{\mathbf{L}} \mathbf{R/Q}\}$.

Для спецификаций из **L**-конуса мы ограничиваемся рассмотрением только **L**-реализаций и **L**-трасс.

2. Генерация тестов

2.1. Актуальные трассы и ошибки

Для тройки $\mathbf{T_i}$ трассу будем называть *актуальной*, если она имеется хотя бы в одной безопасно-тестируемой реализации $\mathbf{I} \in \boldsymbol{SafeImp}(\mathbf{T_i})$. **L**-*актуальной* трассой будем называть **L**-трассу, которая встречается хотя бы в одной безопасно-тестируемой **L**-реализации $\mathbf{I} \in \boldsymbol{SafeImp}(\mathbf{T_i},\mathbf{L})$. Наблюдение $\mathtt{u}$ после актуальной (**L**-актуальной) трассы σ будем называть *актуальным* (**L**-*актуальным*), если оно оставляет трассу $\sigma\cdot\langle\mathtt{u}\rangle$ актуальной (**L**-актуальной). Очевидно, **L**-актуальное наблюдение является **L**-наблюдением.

Замечание 7. **L**-актуальная трасса является актуальной **L**-трассой, но, вообще говоря, не наоборот: актуальная **L**-трасса может не встречаться в безопасно-тестируемых **L**-реализациях. Например, на Рис. 6. для $\mathbf{T_i}=\{\mathbf{R_i}\setminus\mathbf{Q_i}, \boldsymbol{F}(\mathbf{S_0}), \boldsymbol{safe\ in}\}$ и $\mathbf{L_i}=\cup\mathbf{R_i}\cup\cup\mathbf{Q_i}=\{\mathtt{a},\mathtt{b},\mathtt{c},\mathtt{d}\}$ имеем: $\boldsymbol{F}(\mathbf{S_0})$ ***safe for*** $\boldsymbol{F}(\mathbf{S_0})$. **L**-трасса $\langle\{\mathtt{a},\mathtt{b},\mathtt{c}\}\rangle \in \boldsymbol{F}(\mathbf{S_0})$ и поэтому является актуальной **L**-трассой. Однако ни в какой безопасно-тестируемой **L**-реализации эта **L**-трасса встречаться не может, так как в **L**-реализации, поскольку $\mathtt{d} \notin \mathbf{L}$, наличие трассы $\langle\{\mathtt{a},\mathtt{b},\mathtt{c}\}\rangle$ влечет наличие трассы $\langle\{\mathtt{a},\mathtt{d}\}\rangle$. А это нарушает гипотезу о безопасности, поскольку $\{\mathtt{a},\mathtt{d}\} \in \mathbf{Q_i}$ и $\{\mathtt{a},\mathtt{d}\}$ ***safe by*** $\boldsymbol{F}(\mathbf{S_0})$ ***after*** ϵ.

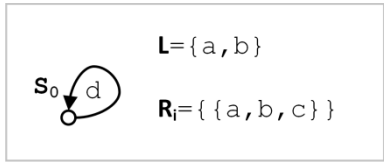


Рис. 6. ***L****-актуальность и* ***L****-конформность*

Любая тестовая трасса, в том числе актуальная (**L**-актуальная), по гипотезе о безопасности безопасна в каждой безопасно-тестируемой реализации

(**L**-реализации), в которой она встречается. Только такие трассы могут наблюдаться при безопасном тестировании безопасно-тестируемых реализаций (**L**-реализаций).

Заметим, что безопасная трасса всегда согласована, но тестовая трасса $\sigma\cdot\langle u\rangle$ может быть несогласованной, если u – действие, запрещенное постфиксом отказов безопасной трассы σ, то есть $u\in\cup\boldsymbol{Ip}(\sigma)$. Несогласованная тестовая трасса неактуальная, поскольку не может встречаться не только в безопасно-тестируемых, но и в любых реализациях. Как будет показано ниже, могут существовать согласованные, в том числе безопасные, но неактуальные тестовые трассы (см. подраздел 2.4). Мы определим необходимые и достаточные условия актуальности как безопасной трассы, так и тестовой, но не безопасной трассы (см. подраздел 3.3).

Тестовую трассу $\sigma\cdot\langle u\rangle$ будем называть *ошибкой* (*ошибочной трассой*), если наблюдение u отсутствует в спецификации после σ: $\sigma\cdot\langle u\rangle\notin\boldsymbol{\Sigma}$. Ошибка $\sigma\cdot\langle u\rangle$ называется *актуальной* (**L**-*актуальной*), если трасса $\sigma\cdot\langle u\rangle$ актуальна (**L**-актуальна). Будем говорить, что *в реализации есть ошибка* $\sigma\cdot\langle u\rangle$, если спецификация определяет ошибку $\sigma\cdot\langle u\rangle$, а в реализации есть трасса $\sigma\cdot\langle u\rangle$. Очевидно, реализация неконформна тогда и только тогда, когда в ней есть некоторая ошибка. Также очевидно, что для проверки конформности достаточно обнаруживать только актуальные ошибки.

2.2. Тесты

В терминах машины тестирования тест – это инструкция оператору машины. В каждом пункте инструкции указывается кнопка, которую оператор должен нажимать, и для каждого наблюдения – пункт инструкции, который должен выполняться следующим, или вердикт (***pass*** или ***fail***), если тестирование нужно закончить. В тесте после кнопки P допускается только такое наблюдение u, которое разрешается кнопкой P, то есть $u\in P\ \vee\ u=P\ \&\ P\in\mathbf{R}$. Среди этих наблюдений обязательно должны быть те, которые могут встречаться в безопасно-тестируемых реализациях после наблюдаемой к этому моменту трассы.

Тест можно понимать как префикс-замкнутое множество конечных историй с назначенными вердиктами, в котором:

1) каждая максимальная история заканчивается наблюдением, и ей приписан вердикт, немаксимальным история вердикты не приписываются;
2) каждая немаксимальная история, заканчивающаяся кнопкой, продолжается во множестве только теми наблюдениями, которые разрешаются этой кнопкой (это следует из определения истории в п.1.3);
3) каждая немаксимальная история, заканчивающаяся кнопкой, обязательно продолжается во множестве всеми актуальными наблюдениями, то есть

теми наблюдениями, которые могут встречаться в безопасно-тестируемых реализациях после трассы этой истории**.**

Тест безопасен тогда и только тогда, когда в каждой его истории каждая кнопка безопасна в спецификации после трассы непосредственно предшествующего этой кнопки префикса истории. Иными словами, тест безопасен тогда и только тогда, когда трассы всех его историй являются тестовыми.

После наблюдения, разрешаемого кнопкой, трасса истории может стать неактуальной (в частности, несогласованной). Безопасный тест будем называть *актуальным* (**L**-*актуальным*), если трассы всех его историй актуальны (**L**-актуальны).

Очевидно, что в любом безопасном тесте есть максимальный (по вложенности) актуальный (**L**-актуальный) подтест, который получается следующей процедурой:

1) Удаляются все истории с не актуальными (не **L**-актуальными) трассами.
2) После этого могут образоваться максимальные истории, заканчивающиеся кнопками. Все такие истории также удаляются.
3) После этого могут образоваться новые максимальные истории, которым назначается вердикт ***pass*****.**

Заметим, что в [7],[9],[10] под тестом (для систем без приоритетов) понималось не множество историй, а множество тестовых трасс. Тест назывался управляемым, если оператор мог однозначно выбрать кнопку, которую нужно нажимать после наблюдения немаксимальной трассы. Поскольку множества наблюдений, разрешаемых разными кнопками, всегда различны, для управляемости теста каждая немаксимальная трасса продолжалась в тесте всеми наблюдениями, разрешаемыми некоторой кнопкой, в том числе несогласованными и неактуальными. Если тест – это множество историй, он автоматически управляем, поскольку оператору прямо указывается кнопка, которую нужно нажимать. Поэтому мы можем обойтись без неактуальных, в частности, несогласованных наблюдений.

Реализация *проходит* тест, если её тестирование с помощью этого теста всегда заканчивается с вердиктом ***pass***. Реализация проходит набор тестов, если она проходит каждый тест из набора. Набор тестов *значимый*, если каждая конформная реализация его проходит; *исчерпывающий*, если каждая неконформная реализация его не проходит; *полный*, если он значимый и исчерпывающий. Для определения конформности или неконформности любой безопасно-тестируемой реализации ставится задача генерации полного набора тестов по спецификации.

Строгим тестом будем называть такой тест, в котором вердикт ***pass*** назначается максимальной истории, если ее трасса есть в спецификации, а вердикт ***fail*** – если нет. Такие тесты, во-первых, значимые (не фиксируют ложных ошибок) и, во-вторых, не пропускают обнаруженных ошибок.

2.3. Примитивные тесты

Полный набор тестов всегда существует, в частности, им является набор всех *примитивных* тестов [10]. Примитивный тест строится по одной выделенной немаксимальной (по префиксному отношению «≤») безопасной **R**-трассе спецификации $\sigma=\langle u_1,u_2,\ldots,u_n\rangle$ (Рис. 7.). Для этого в трассу вставляются кнопки, которые оператор должен нажимать: перед каждым отказом $u_i\in\mathbf{R}$ вставляется кнопка $P_i=u_i$, перед каждым действием $u_i\in\mathbf{L}$ – какая-нибудь безопасная (после соответствующего префикса трассы) кнопка P_i, разрешающая действие u_i, а после всей трассы вставляется любая безопасная после нее кнопка P_{n+1}.

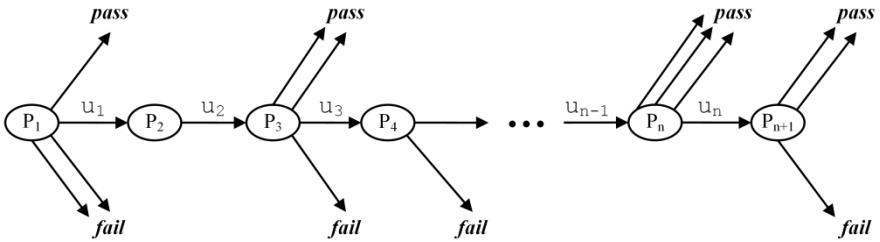


Рис. 7. Примитивный тест

В результате получается тестовая история $T=\langle P_1,u_1,P_2,u_2,\ldots,P_{n+1}\rangle$. Остальные истории $T`$ теста – это строгие префиксы $T`<T$ или имеют вид $T`=\langle P_1,u_1,P_2,u_2,\ldots,P_i,u_i`\rangle$, где $u_i`$ наблюдение, продолжающее трассу $\sigma$ при $i=n+1$, или ответвляющееся от трассы при $i\le n$ и $u_i`\ne u_i$.

Мы будем рассматривать только строгие примитивные тесты, в которых вердикт ***pass*** назначается максимальной истории, если ее трасса есть в спецификации, а вердикт ***fail*** – если нет.

Длиной теста будем называть максимальное число нажатий кнопок (тестовых воздействий) до окончания теста, то есть число $n+1$.

Безопасность трассы σ гарантирует безопасность кнопки $P_i=u_i$ для каждого отказа $u_i\in\mathbf{R}$, и для каждого действия $u_i\in\mathbf{L}$ гарантирует наличие разрешающей его безопасной кнопки P_i, а немаксимальность безопасной трассы σ гарантирует наличие последней кнопки P_{n+1}. Выбор кнопок P_i для $u_i\in\mathbf{L}$ и кнопки P_{n+1} может быть неоднозначным: по одной безопасной

трассе спецификации можно сгенерировать, вообще говоря, несколько разных примитивных тестов.

Если наблюдение, полученное после нажатия непоследней кнопки P_i, совпадает со следующим в трассе σ наблюдением u_i (пройдена немаксимальная в тесте история), тест продолжается. Наблюдение, полученное после нажатия последней кнопки P_{n+1}, и любое наблюдение, «ответвляющееся» от трассы σ, полученное после нажатия непоследней кнопки, всегда заканчивают тестирование (пройдена максимальная в тесте история).

Любой строгий тест T (как множество историй) равен объединению некоторого множества примитивных тестов $T_1,T_2,\ldots$. Каждая максимальная история теста T является максимальной историей хотя бы одного примитивного теста T_i. Поскольку тест T и все примитивные тесты строгие, этой истории в тесте T и в каждом примитивном тесте T_i, где она максимальна, назначен один и тот же вердикт. Если немаксимальная история теста T является максимальной историей в некоторых примитивных тестах T_i, то в каждом таком тесте T_i ей назначен вердикт ***pass***. Тем самым тест T и множество тестов $T_1,T_2,\ldots$ обнаруживают одни и те же ошибки. Поэтому в данной работе мы ограничиваемся рассмотрением только примитивных тестов: по умолчанию под «тестом» будем всегда иметь в виду «примитивный тест».

Примитивный тест также может быть как актуальным, так и неактуальным. Очевидно, что актуальный примитивный тест строится только по актуальной безопасной трассе, но, кроме того, в нем все наблюдения, ответвляющиеся от этой трассы или продолжающие эту трассу, должны быть актуальны.

Для минимизации тестового набора нужно ограничиться только актуальными тестами.

Будем говорить, что набор тестов генерируется по данному набору трасс, если каждый тест из набора тестов генерируется по некоторой трассе из данного набора трасс. Иными словами, набор тестов является подмножеством множества всех тестов, генерируемых по трассам из данного набора трасс. Набор трасс *полный*, если по нему можно сгенерировать полный набор тестов.

Актуальный тест генерируется по немаксимальной безопасной актуальной трассе $\sigma=\langle u_1,u_2,\ldots,u_n\rangle$, и каждое наблюдение $u_i`$, продолжающее трассу при $i=n+1$, или ответвляющееся от трассы при $i\le n$ и $u_i`\ne u_i$, должно быть актуальным.

Если спецификация определяет ошибку $\sigma\cdot\langle u\rangle$, то будем говорить, что тест, соответствующий истории $T=\langle P_1,u_1,P_2,u_2,\ldots,P_{n+1}\rangle$, *обнаруживает ошибку* $\sigma\cdot\langle u\rangle$, если $\sigma=\langle u_1,u_2,\ldots,u_i\rangle$, где $i\le n$, а наблюдение u разрешается кнопкой P_{i+1}, то есть $u\in P_{i+1}$ или $u=P_{i+1}$ для $P_{i+1}\in\mathbf{R}$. Иными словами, ошибка $\sigma\cdot\langle u\rangle$ должна быть трассой некоторой (очевидно, максимальной) истории теста. Поскольку тест строгий, этой истории должен быть приписан вердикт ***fail***. Все актуальные ошибки, очевидно, обнаруживаются всеми актуальными тестами.

Набор актуальных тестов, который обнаруживает все ошибки, определяемые спецификацией, полон. Обратное, вообще говоря, не верно: могут существовать полные наборы актуальных тестов, обнаруживающие не все ошибки; это будет рассмотрено в следующих разделах. Забегая вперед, скажем, что причина этого – в наличии в спецификации безопасных, но неконформных трасс, то есть трасс, которые не могут встречаться ни в одной конформной реализации, в том числе неактуальных трасс. Набор тестов, заканчивающих свою работу с вердиктом ***fail*** сразу после прохождения неконформной трассы σ, может быть полным, но не будет обнаруживать ошибку $\sigma\cdot\langle u\rangle$.

Заметим, что описанный выше способ генерации теста отличается от изложенного в [10]. Там тест генерировался по любой безопасной трассе спецификации Σ (включая максимальные), но после трассы не вставлялась еще одна кнопка и (после нее) разрешаемые ею наблюдения. Из-за этого один тест мог быть сгенерирован по двум разным трассам вида $\sigma\cdot\langle u\rangle$ и $\sigma\cdot\langle u`\rangle$, если находилась кнопка $P$ ***safe by*** $\Sigma$ ***after*** $\sigma$, разрешающая оба наблюдения $u$ и $u`$. При том определении примитивного теста, которое дано в данной работе, множества тестов, генерируемых по разным трассам, не пересекаются.

2.4. Неактуальные безопасные и тестовые трассы

Повторим, что актуальной трассой называется трасса, которая встречается в безопасно-тестируемых реализациях. В [10] показано, что, если в семантике нет **Q**-кнопок, то спецификация удовлетворяет собственной гипотезе о безопасности. Поэтому для таких семантик все безопасные трассы спецификации актуальны. При наличии **Q**-кнопок, вообще говоря, не всякая безопасная трасса спецификации актуальна.

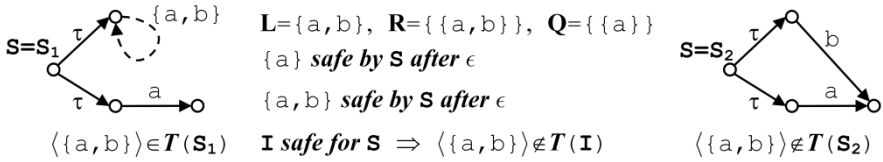


Рис. 8. Неактуальные безопасная и тестовая трассы

Пример приведен на Рис. 8. . Здесь в LTS-спецификации $\mathbf{S_1}$, изображенной слева, **Q**-кнопка {a} безопасна после пустой трассы, а трасса ⟨{a,b}⟩ безопасна. По гипотезе о безопасности в безопасно-тестируемой реализации после пустой трассы не должно быть **Q**-отказа {a}. Однако, если в реализации есть трасса ⟨{a,b}⟩, то хотя бы в одном состоянии после пустой трассы имеется **R**-отказ {a,b}, а тогда в этом состоянии имеется **Q**-отказ {a}. Поэтому в безопасно-тестируемых реализациях не может быть трассы ⟨{a,b}⟩, хотя она является безопасной трассой спецификации.

Понятно, что для генерации тестов достаточно ограничиться только теми безопасными трассами спецификации, которые актуальные.

Точно также тестовая, но отсутствующая в спецификации, трасса может оказаться неактуальной. Прежде всего, все несогласованные тестовые трассы неактуальны. Но могут быть и согласованные неактуальные тестовые трассы. На Рис. 8. в LTS-спецификации $\mathbf{S_2}$, изображенной справа, тестовая трасса ⟨{a,b}⟩ отсутствует в спецификации, согласована, но неактуальна.

2.5. Неконформные безопасные трассы

Для тройки $\mathbf{T_i}$ трассу будем называть *конформной*, если она имеется хотя бы в одной конформной реализации $\mathbf{I}\in\boldsymbol{ConfImp}(\mathbf{T_i})$.

Множество конформных безопасных трасс обозначим:

$$\boldsymbol{conf}(\mathbf{T_i}) \triangleq \{\sigma\in\boldsymbol{SafeBy}(\mathbf{T_i}) \mid \exists \mathbf{I}\in\boldsymbol{ConfImp}(\mathbf{T_i}) \ \&\ \sigma\in\mathbf{I}\}.$$

Его подмножество конформных **L**-трасс – это следующее множество:

$$\{\sigma\in\boldsymbol{SafeBy}(\mathbf{T_i},\mathbf{L}) \mid \exists \mathbf{I}\in\boldsymbol{ConfImp}(\mathbf{T_i}) \ \&\ \sigma\in\mathbf{I}\} = \boldsymbol{conf}(\mathbf{T_i})\cap(\mathbf{L}\cup\mathbf{R_i})^* \subseteq \boldsymbol{conf}(\mathbf{T_i}).$$

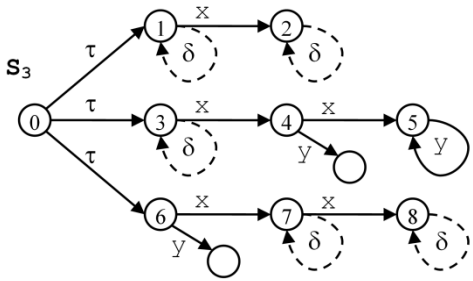
L-*конформной* трассой будем называть **L**-трассу, которая встречается хотя бы в одной конформной **L**-реализации $\mathbf{I}\in\boldsymbol{ConfImp}(\mathbf{T_i},\mathbf{L})$.

Множество **L**-конформных безопасных трасс обозначим:

$$\mathit{conf}(\mathbf{T}_i,\mathbf{L}) \triangleq \{\sigma\in \mathit{SafeBy}(\mathbf{T}_i,\mathbf{L}) \mid \exists \mathbf{I}\in \mathit{ConfImp}(\mathbf{T}_i,\mathbf{L}) \;\&\; \sigma\in\mathbf{I}\} \subseteq \mathit{conf}(\mathbf{T}_i)\cap(\mathbf{L}\cup\mathbf{R}_i)^*$$

Замечание 8. **L**-конформная трасса является конформной **L**-трассой, но, вообще говоря, не наоборот: конформная **L**-трасса может не встречаться в конформных **L**-реализациях. Пример тот же, что на Рис. 6. , который иллюстрировал **L**-актуальность (п.2.1). Для $\mathbf{T}_i=\{\mathbf{R}_i\backslash\mathbf{Q}_i, \mathit{F}(\mathbf{S}_0), \textit{safe in}\}$ и $\mathbf{L}_i=\cup\mathbf{R}_i\cup\cup\mathbf{Q}_i=\{a,b,c,d\}$ имеем: $\mathit{F}(\mathbf{S}_0)$ *saco* $\mathit{F}(\mathbf{S}_0)$, **L**-трасса $\langle\{a,b,c\}\rangle\in\mathit{F}(\mathbf{S}_0)$ и поэтому является конформной **L**-трассой. Однако эта трасса не является **L**-конформной, потому что для тройки $\mathbf{T}_i$ нет конформных **L**-реализаций. Действительно, если бы была конформная **L**-реализация, то в ней $\mathbf{Q}_i$-кнопка $\{a,d\}$ была бы безопасна после пустой трассы (как в спецификации), поэтому пустая трасса продолжалась бы действием $z\in\{a,d\}$, но действие a не конформно, а действие $d\notin\mathbf{L}$.

В [10] показано, что, если в семантике нет **Q**-кнопок, то спецификация безопасно-тестируема и конформна сама себе. Поэтому для таких семантик все безопасные трассы спецификации конформны. При наличии **Q**-кнопок, вообще говоря, не всякая безопасная трасса спецификации конформна.



$\mathbf{L}=\{x,y\}$
$\mathbf{R}=\{\delta\}$, где $\delta=\{y\}$
$\mathbf{Q}=\{\{x\}\}$
$\mathbf{I}$ *saco* $\mathbf{S}_3 \Rightarrow \langle\delta,x,\delta,x\rangle\notin\mathit{T}(\mathbf{I}) \Rightarrow \langle\delta,x,\delta\rangle\notin\mathit{T}(\mathbf{I})$

Рис. 9. Неконформная безопасная трасса $\langle\delta,x,\delta\rangle$

Кроме примера на Рис. 6. , рассмотрим пример на Рис. 9. , являющийся модификацией примера из [7],[9]. Здесь используется семантика отношения ***ioco*** [40],[41], в которой действия делятся на стимулы и реакции; каждый стимул x разрешается одной **Q**-кнопкой $\{x\}$, а все реакции разрешаются одной **R**-кнопкой, обозначаемой δ. В данном примере в алфавите имеется один стимул x и одна реакция y, поэтому $\delta=\{y\}$. Отношение ***ioco*** предполагает всюду-определенность реализации по стимулам, то есть отсутствие в ней **Q**-отказов. Отношение ***saco*** более либерально, но даже для него в LTS-спецификации $\mathbf{S}_3$ кнопка $\{x\}$ по 2-ому правилу отношения ***safe by*** должна быть безопасной после трассы $\langle x\rangle$, так как разрушения и дивергенции нет и есть трасса $\langle x,x\rangle$. Если в реализации есть трасса $\langle\delta,x,\delta\rangle$,

то в ней есть и трасса ⟨x⟩, после которой кнопка {x} по гипотезе о безопасности должна быть безопасной по ***safe in***. А тогда кнопка {x} безопасна по ***safe in*** после трассы ⟨δ,x,δ⟩. Поскольку это **Q**-кнопка, ее безопасность после трассы ⟨δ,x,δ⟩ означает наличие в реализации трассы ⟨δ,x,δ,x⟩. Поскольку δ **R**-кнопка и в спецификации нет разрушения, эта кнопка безопасна после любой безопасной трассы спецификации, в частности после трассы ⟨x,x⟩, а тогда в реализации она безопасна по ***safe in*** после трассы ⟨x,x⟩ и, следовательно, безопасна по ***safe in*** после трассы ⟨δ,x,δ,x⟩. Поскольку кнопка δ разрешает только два наблюдения: y и δ, в реализации должна быть хотя бы одна из трасс ⟨δ,x,δ,x,y⟩ или ⟨δ,x,δ,x,δ⟩. Но тогда в реализации есть хотя бы одна из трасс ⟨x,δ,x,y⟩ или ⟨δ,x,x,δ⟩. Каждая из этих трасс является продолжением безопасной трассы спецификации наблюдением, разрешаемым безопасной кнопкой δ, но отсутствующим в спецификации, что противоречит тестируемому условию конформности. Следовательно, трасса ⟨δ,x,δ⟩, хотя и безопасна в спецификации, но неконформна.

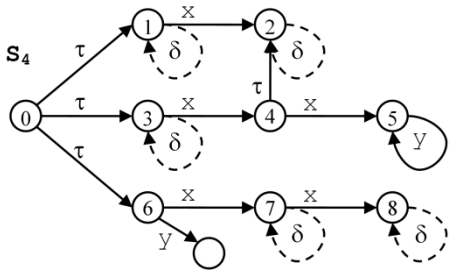
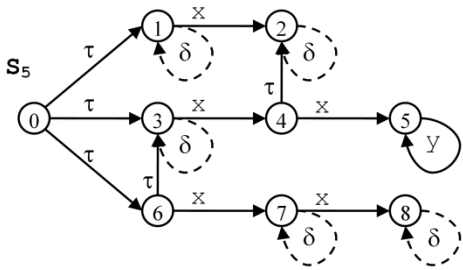


Рис. 10. Неконформная безопасная трасса ⟨δ⟩

Другой пример приведен на Рис. 10. . Этот пример отличается тем, что в состоянии 4 для того, чтобы не было отказа δ, вместо перехода по реакции y вставлен τ-переход. Из-за этого уже более короткая трасса ⟨δ⟩ и, следовательно, все её имеющиеся продолжения неконформны. Это

объясняется тем, что после трассы $\langle\delta\rangle$ в любой реализации должен приниматься стимул x, после которого конформен только отказ δ, а все реакции неконформны. Тем самым, наличие трассы $\langle\delta\rangle$ в конформной реализации влекло бы наличие в ней неконформной трассы $\langle\delta,x,\delta\rangle$.



$\mathbf{L}=\{x, y\}$
$\mathbf{R}=\{\delta\}$, где $\delta=\{y\}\}$
$\mathbf{Q}=\{\{x\}\}$

$\mathbf{I}$ *saco* $\mathbf{S_5} \Rightarrow \langle\delta, x, \delta, x\rangle \notin \boldsymbol{T}(\mathbf{I})$
$\Rightarrow \langle\delta, x, \delta\rangle \notin \boldsymbol{T}(\mathbf{I})$
$\Rightarrow \langle\delta, x\rangle \notin \boldsymbol{T}(\mathbf{I})$
$\Rightarrow \langle\delta\rangle \notin \boldsymbol{T}(\mathbf{I})$
$\Rightarrow \epsilon \notin \boldsymbol{T}(\mathbf{I})$

Рис. 11. Все безопасные трассы неконформны

Третий пример, изображенный на Рис. 11. , является дальнейшей модификацией примера на Рис. 10. : еще в одном состоянии – состоянии 6 – для того, чтобы не было отказа δ, вместо перехода по реакции y вставлен τ-переход. Как и в предыдущем примере в конформной реализации не может быть трассы $\langle\delta\rangle$. В то же время в такой реализации после пустой трассы не должно быть действия y. Следовательно, в конформной реализации не может быть пустой трассы. Поскольку пустая трасса является префиксом любой трассы, в этой спецификации все безопасные трассы неконформны.

2.6. Классификация ошибок и типов тестирования

Ошибку, определенную в подразделе 1.5 как продолжение безопасной в спецификации трассы σ безопасным, но отсутствующим в спецификации, наблюдением u, то есть трассу $\sigma\cdot\langle u\rangle$, будем теперь называть *ошибкой 1-го рода*. Очевидно, она не встречается в конформных реализациях. Эту ошибку будем называть *первичной*, если трасса σ конформна, и *вторичной* – в противном случае.

Наличие в спецификации неконформных безопасных трасс само по себе не создает проблем, но дает возможность оптимизации тестирования. Наличие в реализации неконформной безопасной в спецификации трассы влечет неконформность реализации. *Ошибкой 2-го рода* будем называть неконформную безопасную (в спецификации) трассу. Эту ошибку будем называть *первичной*, если все ее строгие префиксы конформны, и *вторичной* – в противном случае.

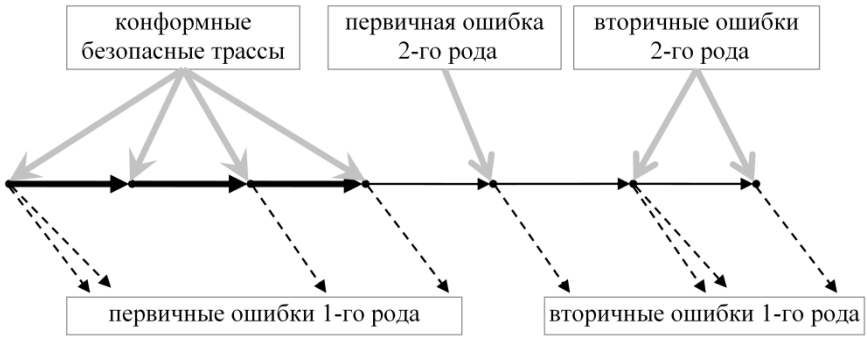


Рис. 12. Типы ошибок

Эта классификация ошибок проиллюстрирована на Рис. 12. .

Посмотрим, как выглядят конформные трассы и актуальные ошибки различных видов в примерах на Рис. 9. , Рис. 10. , Рис. 11. . Неактуальные ошибки в этих примерах являются несогласованными трассами, когда реакция y следует непосредственно после отказа δ, как например, в тестовой трассе $\langle \delta, y \rangle$.

В примере на Рис. 9. все безопасные трассы конформны, кроме трасс, задаваемых регулярным выражением $\delta\delta^* x \delta\delta^*$, которые являются актуальными ошибками 2-го рода. Из них трассы вида $\delta\delta^* x \delta$ являются первичными ошибками, а остальные – вторичными. Актуальными ошибками 1-го рода являются трассы, задаваемые следующими регулярными выражениями: yy, $\delta^* xyy$, $x\delta\delta^* xy$, $\delta\delta^* xx\delta$, $\delta^* xxyy^*\delta$. Все эти ошибки 1-го рода являются первичными.

В примере на Рис. 10. неконформна безопасная трасса $\langle \delta \rangle$, которая является первичной ошибкой 2-го рода. Все ее безопасные в спецификации продолжения также неконформны и являются вторичными ошибками 2-го рода. Актуальными ошибками 1-го рода являются трассы, задаваемые следующими регулярными выражениями: yy, $\delta^* xy$, $x\delta\delta^* xy$, $\delta\delta^* xx\delta$, $\delta^* xxyy^*\delta$. Из них только ошибки yy, xy, $x\delta\delta^* xy$ и $xxyy^*\delta$ являются первичными, а остальные ошибки $\delta\delta^* xy$, $\delta\delta^* xx\delta$, $\delta\delta^* xxyy^*\delta$ являются вторичными.

В примере на Рис. 11. неконформна безопасная пустая трасса, которая, тем самым, является первичной ошибкой 2-го рода. Все остальные безопасные в спецификации трассы являются вторичными ошибками 2-го рода. Все

тестовые, но отсутствующие в спецификации трассы, являются вторичными ошибками 1-го рода.

Для спецификационной тройки $\mathbf{T_i}$ множества определяемых ею трасс обозначим (см. Рис. 13.):

первичные тестовые трассы:

$$\boldsymbol{ptt}(\mathbf{T_i}) \triangleq \{\sigma \in \boldsymbol{tt}(\mathbf{T_i}) \mid \forall \mu < \sigma\ \mu \in \boldsymbol{conf}(\mathbf{T_i})\} = \boldsymbol{perr}(\mathbf{T_i}) \cup \boldsymbol{conf}(\mathbf{T_i}),$$

все ошибки:

$$\boldsymbol{err}(\mathbf{T_i}) \triangleq \boldsymbol{tt}(\mathbf{T_i}) \setminus \boldsymbol{conf}(\mathbf{T_i}) = \boldsymbol{err_1}(\mathbf{T_i}) \cup \boldsymbol{err_2}(\mathbf{T_i}),$$

первичные ошибки:

$$\boldsymbol{perr}(\mathbf{T_i}) \triangleq \boldsymbol{ptt}(\mathbf{T_i}) \setminus \boldsymbol{conf}(\mathbf{T_i}) = \boldsymbol{perr_1}(\mathbf{T_i}) \cup \boldsymbol{perr_2}(\mathbf{T_i}),$$

ошибки 1-го рода:

$$\boldsymbol{err_1}(\mathbf{T_i}) \triangleq \boldsymbol{tt}(\mathbf{T_i}) \setminus \boldsymbol{SafeBy}(\mathbf{T_i}),$$

ошибки 2-го рода:

$$\boldsymbol{err_2}(\mathbf{T_i}) \triangleq \boldsymbol{SafeBy}(\mathbf{T_i}) \setminus \boldsymbol{conf}(\mathbf{T_i}),$$

первичные ошибки 1-го рода:

$$\boldsymbol{perr_1}(\mathbf{T_i}) \triangleq \boldsymbol{err_1}(\mathbf{T_i}) \cap \boldsymbol{ptt}(\mathbf{T_i}) = \{\sigma \in \boldsymbol{err_1}(\mathbf{T_i}) \mid \forall \mu < \sigma\ \mu \in \boldsymbol{conf}(\mathbf{T_i})\},$$

первичные ошибки 2-го рода:

$$\boldsymbol{perr_2}(\mathbf{T_i}) \triangleq \boldsymbol{err_2}(\mathbf{T_i}) \cap \boldsymbol{ptt}(\mathbf{T_i}) = \{\sigma \in \boldsymbol{err_2}(\mathbf{T_i}) \mid \forall \mu < \sigma\ \ \mu \in \boldsymbol{conf}(\mathbf{T_i})\}.$$

Также имеем:

$$\boldsymbol{tt}(\mathbf{T_i}) = \boldsymbol{SafeBy}(\mathbf{T_i}) \cup \boldsymbol{err_1}(\mathbf{T_i}) = \boldsymbol{err}(\mathbf{T_i}) \cup \boldsymbol{conf}(\mathbf{T_i}),$$
$$\boldsymbol{conf}(\mathbf{T_i}) = \boldsymbol{tt}(\mathbf{T_i}) \setminus \boldsymbol{err}(\mathbf{T_i}) = \boldsymbol{SafeBy}(\mathbf{T_i}) \setminus \boldsymbol{err}(\mathbf{T_i}).$$

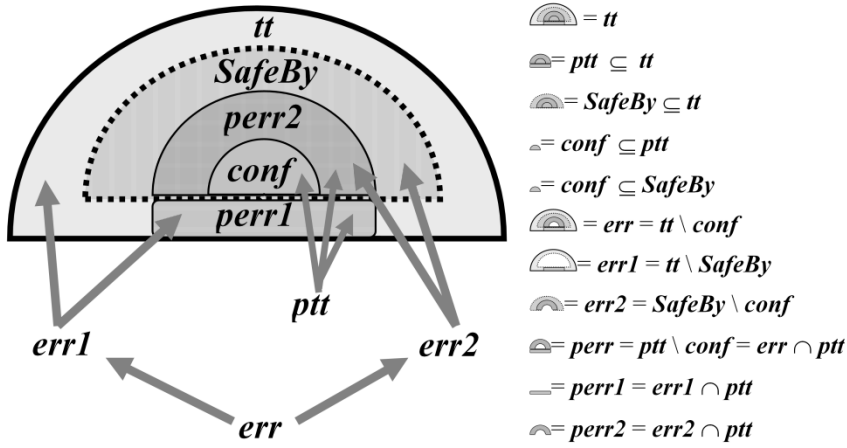


Рис. 13. Множества трасс

L-*ошибкой* будем называть такую тестовую **L**-трассу, которая не является **L**-конформной. Соответствующие множества обозначим:

первичные тестовые **L**-*трассы:*

$$\boldsymbol{ptt}(\mathbf{T_i},\mathbf{L}) \triangleq \{\sigma\in\boldsymbol{tt}(\mathbf{T_i},\mathbf{L}) \mid \forall\mu{<}\sigma\ \mu\in\boldsymbol{conf}(\mathbf{T_i},\mathbf{L})\} = \boldsymbol{perr}(\mathbf{T_i},\mathbf{L})\cup\boldsymbol{conf}(\mathbf{T_i},\mathbf{L}),$$

все **L**-*ошибки:*

$$\boldsymbol{err}(\mathbf{T_i},\mathbf{L}) \triangleq \boldsymbol{tt}(\mathbf{T_i},\mathbf{L})\setminus\boldsymbol{conf}(\mathbf{T_i},\mathbf{L}) = \boldsymbol{err_1}(\mathbf{T_i},\mathbf{L})\cup\boldsymbol{err_2}(\mathbf{T_i},\mathbf{L}),$$

первичные **L**-*ошибки:*

$$\boldsymbol{perr}(\mathbf{T_i},\mathbf{L}) \triangleq \boldsymbol{ptt}(\mathbf{T_i},\mathbf{L})\setminus\boldsymbol{conf}(\mathbf{T_i},\mathbf{L}) = \boldsymbol{perr_1}(\mathbf{T_i},\mathbf{L})\cup \boldsymbol{perr_2}(\mathbf{T_i},\mathbf{L}),$$

L-*ошибки 1-го рода:*

$$\boldsymbol{err_1}(\mathbf{T_i},\mathbf{L}) \triangleq \boldsymbol{tt}(\mathbf{T_i},\mathbf{L})\setminus\boldsymbol{SafeBy}(\mathbf{T_i},\mathbf{L}),$$

L-*ошибки 2-го рода:*

$$\boldsymbol{err_2}(\mathbf{T_i},\mathbf{L}) \triangleq \boldsymbol{SafeBy}(\mathbf{T_i},\mathbf{L})\setminus\boldsymbol{conf}(\mathbf{T_i},\mathbf{L}),$$

первичные **L**-*ошибки 1-го рода:*

$$\boldsymbol{perr_1}(\mathbf{T_i},\mathbf{L}) \triangleq \boldsymbol{err_1}(\mathbf{T_i})\cap\boldsymbol{ptt}(\mathbf{T_i},\mathbf{L}) = \{\sigma\in\boldsymbol{err_1}(\mathbf{T_i},\mathbf{L}) \mid \forall\mu{<}\sigma\ \mu\in\boldsymbol{conf}(\mathbf{T_i},\mathbf{L})\},$$

первичные **L**-*ошибки 2-го рода:*

$$\boldsymbol{perr_2}(\mathbf{T_i},\mathbf{L}) \triangleq \boldsymbol{err_2}(\mathbf{T_i},\mathbf{L})\cap\boldsymbol{ptt}(\mathbf{T_i},\mathbf{L}) = \{\sigma\in\boldsymbol{err_2}(\mathbf{T_i},\mathbf{L}) \mid \forall\mu{<}\sigma\ \mu\in\boldsymbol{conf}(\mathbf{T_i},\mathbf{L})\}.$$

Также имеем:

$$\boldsymbol{tt}(\mathbf{T_i},\mathbf{L}) = \boldsymbol{SafeBy}(\mathbf{T_i},\mathbf{L})\cup \boldsymbol{err_1}(\mathbf{T_i},\mathbf{L}) = \boldsymbol{err}(\mathbf{T_i},\mathbf{L})\cup\boldsymbol{conf}(\mathbf{T_i},\mathbf{L}),$$

$$\boldsymbol{conf}(\mathbf{T_i},\mathbf{L}) = \boldsymbol{tt}(\mathbf{T_i},\mathbf{L})\setminus\boldsymbol{err}(\mathbf{T_i},\mathbf{L}) = \boldsymbol{SafeBy}(\mathbf{T_i},\mathbf{L})\setminus\boldsymbol{err}(\mathbf{T_i},\mathbf{L}).$$

Следует заметить, что род ошибки не является инвариантом при эквивалентных и вложенных преобразованиях спецификационных троек. Более того, при таких преобразованиях может не сохраняться множество актуальных тестовых трасс, тем самым некоторые актуальные ошибки, определяемые одной спецификационной тройкой, могут не быть тестовыми трассами (и, следовательно, ошибками) для другой спецификационной тройки. Однако при таких преобразованиях первичная ошибка не может стать вторичной и наоборот. В следующем разделе мы определим эквивалентное преобразование пополнения, которое дает возможность определять неактуальные и неконформные трассы, тем самым позволяя обнаруживать ошибки 2-го рода.

Если ошибка вторичная, то по определению некоторый ее строгий префикс является первичной ошибкой 2-го рода. Поэтому для полноты тестирования достаточно обнаруживать первичные ошибки 1-го и 2-го родов.

Тестирование, не обнаруживающее ошибки 2-го рода, то есть ориентированное на обнаружение ошибок только 1-го рода (не различая первичные и вторичные ошибки) с генерацией тестов, описанной в подразделе 2.1, будем называть *тестированием 1-го рода. Тестированием 2-го рода* будем называть тестирование, обнаруживающее только первичные ошибки 1-го и 2-го рода, что достаточно для полноты тестирования.

Поскольку род ошибки не является инвариантом при эквивалентных и вложенных преобразованиях спецификационных троек, не является таким инвариантом и тип тестирования.

Понятно, что ошибка 2-го рода влечет наличие в реализации какой-нибудь ошибки 1-го рода, но тестирование 2-го рода, вообще говоря, обнаруживает неконформность быстрее, чем тестирование 1-го рода.

Для примера на Рис. 9. при обнаружении трассы $\langle \delta,x,\delta \rangle$ можно заканчивать тестирование с вердиктом ***fail***, а не ***pass*** как при тестировании 1-го рода. Для примера на Рис. 10. тестирование можно закончить еще раньше: при обнаружении трассы $\langle \delta \rangle$. Наконец, для примера на Рис. 11. тестирование вообще излишне, поскольку пустая трасса неконформна: такая трасса есть в любой реализации, следовательно, для этой спецификации нет конформных реализаций. Этот несколько курьезный пример показывает, насколько полезным может оказаться анализ неконформных трасс. Для спецификации из этого примера полное тестирование 1-го рода будет бесконечным, поскольку имеется цикл по действию y после безопасной трассы $\langle \delta,x,x \rangle$ и, тем самым, имеется бесконечное число безопасных трасс вида $\delta\delta^* xxy^*$ и актуальных, но ошибочных (вторичных 1-го рода) тестовых трасс вида $\delta\delta^* xxy^*\delta$. В то же время тестирование 2-го рода вообще не будет проводиться.

Однако следует отметить, что для обнаружения ошибок 2-го рода требуется анализ конформности безопасных трасс спецификации, что может быть нетривиальной задачей. Например, если в спецификациях на Рис. 9. , Рис. 10. , Рис. 11. переходы по x из состояний 4 и 7 заменяются на цепочки переходов по x длины n, то неконформность трассы $\langle \delta,x,\delta \rangle$ на Рис. 9. , трассы $\langle \delta \rangle$ на Рис. 10. или пустой трассы на Рис. 11. , может быть обнаружена только после анализа двух трасс $\langle \delta,x,x,...,x,y \rangle$ и $\langle x,\delta,x,...,x,\delta \rangle$ длины $n+3$. Общее решение этой проблемы мы рассмотрим в следующих разделах.

После ошибки 1-го рода тест не может продолжаться (любая кнопка может быть опасной в реализации), то есть должен выноситься вердикт. Иными словами, множество ошибок 1-го рода образует антицепь по отношению «≤»

на множестве всех трасс. Строгость теста означает, что при обнаружении ошибки тест выносит вердикт ***fail***, а не вердикт ***pass***. При тестировании 1-го рода это единственный случай вынесения вердикта ***fail***.

При тестировании 2-го рода возможен другой случай, когда после наблюдения u конформная безопасная в спецификации трасса σ становится безопасной, но неконформной трассой $\sigma\cdot\langle u\rangle$, то есть первичной ошибкой 2-го рода. После такой ошибки могут быть безопасные в спецификации кнопки, и тестирование может продолжаться. Однако для полноты тестирования это лишнее, так как любая полученная при этом трасса будет вторичной ошибкой: 2-го или 1-го рода. Поэтому от строгого теста 2-го рода мы потребуем для первичных ошибок 2-го рода вынесения вердикта ***fail***, после чего тест заканчивается. Заметим, что множество первичных ошибок образует антицепь по отношению «≤» на множестве всех трасс.

Для тестирования 2-го рода мы, как и раньше, можем в любом безопасном тесте выделить максимальный (по вложенности) актуальный подтест.

Заметим, что набор тестов 1-го рода, сгенерированный только по конформным трассам спецификации, то есть обнаруживающий только первичные ошибки 1-го рода, вообще говоря, не является полным. Более того, существуют спецификации, для которых в любой безопасно-тестируемой реализации нет первичных ошибок 1-го рода. Это иллюстрируется примером на Рис. 11. , где для спецификации имеется единственная первичная ошибка – пустая трасса, которая является ошибкой 2-го рода.

2.7. Оптимизация тестирования на основе анализа конформности и актуальности трасс

Хотя набор всех примитивных тестов является полным, это не означает, что не существует других, меньших, полных наборов примитивных тестов.

Оптимизация тестирования решает две задачи: 1) упрощение каждого теста удалением из него «лишнего», 2) уменьшение тестового набора удалением из него «лишних» тестов.

Первая задача решается удалением из программы теста реакции на **L**-неактуальные наблюдения, поскольку их все равно не может быть при тестировании безопасно-тестируемых **L**-реализаций. Если сама трасса, по которой генерируется тест, **L**-неактуальна, то такой тест можно удалить целиком, что решает уже вторую задачу, но только отчасти.

Для решения второй задачи мы могли бы использовать тестирование 2-го рода, опирающееся на анализ конформности безопасных трасс исходной спецификации. Тесты генерировались бы только по **L**-конформным трассам этой спецификации. Вместо этого мы определим вложенное преобразование

спецификации, после которого в новой спецификации все безопасные **L**-трассы будут **L**-конформны. Для этой новой спецификации тестирование 1-го и 2-го рода совпадают.

Следует отметить, что это не решает вторую задачу полностью, а является только первым, но необходимым, приближением к ее решению. Дальнейшие виды оптимизаций будут рассмотрены в наших дальнейших работах.

3. Трассовое пополнение трассовой спецификации

3.1. Определение ∇-трасс и ∇-пополнения

В подразделе 0 было сказано, что ошибка, род ошибки и тип тестирования не являются инвариантами при вложенных преобразованиях спецификационных троек. **L**-конус $\nabla(\mathbf{T})_{\mathbf{L}}$ состоит из тех и только тех спецификационных троек, которые определяют те же самые тестовые возможности тестирования для класса **L**-реализаций, что исходная тройка **T** (то есть троек в семантиках, **L**-эквивалентных исходной семантике), и при этом сохраняют класс приведенных к алфавиту **L** конформных **L**-реализаций и не сужают класс приведенных к алфавиту **L** безопасно-тестируемых **L**-реализаций. Если дать определение ошибки через **L**-конус $\nabla(\mathbf{T})_{\mathbf{L}}$, то такая ошибка будет инвариантной.

Пусть задана исходная спецификационная тройка $\mathbf{T}=(\mathbf{R}/\mathbf{Q},\mathbf{\Sigma},\textit{safe by})$ и $\mathbf{L}=\cup\mathbf{R}\cup\cup\mathbf{Q}$.

∇-*тестовой трассой* будем называть приведенную к алфавиту **L** тестовую **L**-трассу какой-нибудь тройки из **L**-конуса $\nabla(\mathbf{T})_{\mathbf{L}}$. ∇-тестовые трассы делятся на ∇-*ошибки*, среди которых выделяются *первичные* ∇-*ошибки*, и ∇-*конформные трассы* в зависимости от того, определяются эти трассы какой-нибудь тройкой из **L**-конуса $\nabla(\mathbf{T})_{\mathbf{L}}$ как ошибки, первичные ошибки или безопасные конформные трассы. Первичные ∇-ошибки и ∇-конформные трассы образуют множество первичных ∇-тестовых трасс. Введем обозначения для всех этих множеств ∇-трасс (см. Рис. 14.):

∇-тестовых: $\nabla\textit{tt}(\mathbf{T}) \triangleq \cup\{\textit{tt}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}} \mid \mathbf{T_i}\in\nabla(\mathbf{T})_{\mathbf{L}}\} = \nabla\textit{err}(\mathbf{T}) \cup \nabla\textit{conf}(\mathbf{T}),$

∇-ошибок: $\nabla\textit{err}(\mathbf{T}) \triangleq \cup\{\textit{err}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}} \mid \mathbf{T_i}\in\nabla(\mathbf{T})_{\mathbf{L}}\} = \nabla\textit{tt}(\mathbf{T}) \setminus \nabla\textit{conf}(\mathbf{T}),$

первичных ∇-ошибок: $\nabla\textit{perr}(\mathbf{T}) \triangleq \cup\{\textit{perr}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}} \mid \mathbf{T_i}\in\nabla(\mathbf{T})_{\mathbf{L}}\} = \{\sigma\in\nabla\textit{err}(\mathbf{T}) \mid \forall\mu<\sigma\ \mu\in\nabla\textit{conf}(\mathbf{T})\},$

∇-конформных: $\nabla\textit{conf}(\mathbf{T}) \triangleq \cup\{\textit{conf}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}} \mid \mathbf{T_i}\in\nabla(\mathbf{T})_{\mathbf{L}}\} = \cup\{(\textit{tt}(\mathbf{T_i},\mathbf{L})\setminus\textit{err}(\mathbf{T_i},\mathbf{L}))_{\mathbf{L}} \mid \mathbf{T_i}\in\nabla(\mathbf{T})_{\mathbf{L}}\} = \cup\{(\textit{SafeBy}(\mathbf{T_i},\mathbf{L})\setminus\textit{err}(\mathbf{T_i},\mathbf{L}))_{\mathbf{L}} \mid \mathbf{T_i}\in\nabla(\mathbf{T})_{\mathbf{L}}\}$

$$= \nabla\mathit{tt}(\mathbf{T}) \setminus \nabla\mathit{err}(\mathbf{T})$$
$$= \nabla\mathit{ptt}(\mathbf{T}) \setminus \nabla\mathit{perr}(\mathbf{T}),$$

первичных ∇-тестовых: $\nabla\mathit{ptt}(\mathbf{T}) \triangleq \cup\{\mathit{ptt}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}} \mid \mathbf{T_i} \in \nabla(\mathbf{T})_{\mathbf{L}}\}$

$$= \nabla\mathit{perr}(\mathbf{T}) \cup \nabla\mathit{conf}(\mathbf{T})$$
$$= \{\sigma \in \nabla\mathit{tt}(\mathbf{T}) \mid \forall \mu{<}\sigma \ \ \mu \in \nabla\mathit{conf}(\mathbf{T})\}.$$

Имеем: $\nabla\mathit{perr}(\mathbf{T}) \subseteq \nabla\mathit{err}(\mathbf{T})$, $\nabla\mathit{ptt}(\mathbf{T}) \subseteq \nabla\mathit{tt}(\mathbf{T})$, $\nabla\mathit{perr}(\mathbf{T}) \cap \nabla\mathit{conf}(\mathbf{T}) = \varnothing$ и $\nabla\mathit{err}(\mathbf{T}) \cap \nabla\mathit{conf}(\mathbf{T}) = \varnothing$.

Замечание 9. Множество первичных ∇-ошибок образует антицепь по отношению «≤» на множестве всех ∇-тестовых трасс. Действительно, все строгие префиксы первичной ∇-ошибки ∇-конформны, а множества первичных ∇-ошибок и ∇-конформных трасс не пересекаются.

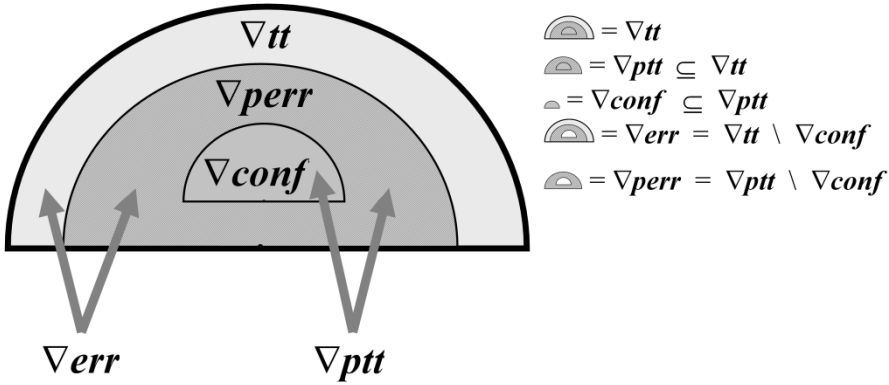


Рис. 14. Множества ∇-трасс

Множество ∇-конформных трасс совпадает с множеством конформных ∇-тестовых трасс.

Действительно, если трасса $\sigma_{\mathbf{L}}$ ∇-конформна, то она ∇-тестовая, но не ∇-ошибка, то есть для некоторой тройки из **L**-конуса трасса σ является тестовой, но не ошибочной **L**-трассой, то есть конформной тестовой **L**-трассой, а тогда трасса $\sigma_{\mathbf{L}}$ конформная ∇-тестовая трасса. Если ∇-тестовая трасса $\sigma_{\mathbf{L}}$ конформна, то трасса σ не может быть ошибкой ни для какой тройки из **L**-конуса, то есть трасса $\sigma_{\mathbf{L}}$ не принадлежит $\nabla\mathit{err}(\mathbf{T})$, следовательно, принадлежит $\nabla\mathit{conf}(\mathbf{T})$, а тогда трасса $\sigma_{\mathbf{L}}$ ∇-конформна.

Будем говорить, что наблюдение ∇-*конформно после* ∇-конформной трассы, если трасса, продолженная этим наблюдением, остается ∇-конформной.

Спецификационную тройку $\mathbf{T_i=(R_i/Q_i,\Sigma_i,}\boldsymbol{safe\ by}_\mathbf{i})$ будем называть ∇-*пополнением* тройки **T**, если выполнены следующие условия:

1) семантики **L**-эквивалентны $\mathbf{R_i/Q_i \approx_L R/Q}$;
2) $\mathbf{T_i} \in \nabla(\mathbf{T})_\mathbf{L}$;
3) все приведенные к алфавиту **L** безопасные **L**-трассы, определяемые тройкой $\mathbf{T_i}$, ∇-конформны: $\boldsymbol{SafeBy}(\mathbf{T_i,L})_\mathbf{L} \subseteq \nabla\boldsymbol{conf}(\mathbf{T})$.

Преобразование $\mathbf{T} \rightarrow \mathbf{T_i}$ будем называть *преобразованием* ∇-*пополнения* (или просто ∇-*пополнением* там, где это не проводит к конфликтам).

Теорема 3: **О свойствах ∇-пополнения.** ∇-пополнение $\mathbf{T_i}$ обладает следующими свойствами:

1) все **L**-ошибки, определяемые тройкой $\mathbf{T_i}$, являются первичные **L**-ошибками 1-го рода: $\boldsymbol{err}(\mathbf{T_i,L})_\mathbf{L} = \boldsymbol{perr}_\mathbf{1}(\mathbf{T_i,L})_\mathbf{L}$.
2) все приведенные к алфавиту **L** **L**-ошибки, определяемые тройкой $\mathbf{T_i}$, являются первичными ∇-ошибками: $\boldsymbol{err}(\mathbf{T_i,L})_\mathbf{L} \subseteq \nabla\boldsymbol{perr}(\mathbf{T})$;
3) все приведенные к алфавиту **L** тестовые **L**-трассы, определяемые тройкой $\mathbf{T_i}$, являются первичными ∇-тестовыми трассами: $\boldsymbol{tt}(\mathbf{T_i,L})_\mathbf{L} \subseteq \nabla\boldsymbol{ptt}(\mathbf{T})$.

Доказательство см. на стр.107

Теорема 4: **О существовании ∇-пополнения.** ∇-пополнение не существует, если для исходной тройки **T** нет конформных реализаций.

Доказательство см. на стр.108

Безопасные трассы ∇-пополнения по определению конформны. Заметим, что опасные трассы ∇-пополнения не обязательно конформны. Более того, в некоторых случаях любое ∇-пополнение содержит неконформные опасные трассы (ниже теорема 7).

∇-пополнение $\mathbf{T_i}$ будем называть *максимальным*, если вместо вложенности имеет место равенство:

1) множество приведенных к алфавиту **L** безопасных **L**-трасс, определяемых тройкой $\mathbf{T_i}$, совпадает с множеством ∇-конформных трасс:
   $\boldsymbol{SafeBy}(\mathbf{T_i,L})_\mathbf{L} = \nabla\boldsymbol{conf}(\mathbf{T})$;
2) множество приведенных к алфавиту **L** **L**-ошибок 1-го рода, определяемых тройкой $\mathbf{T_i}$, совпадает с множеством первичных ∇-ошибок:
   $\boldsymbol{err}_\mathbf{1}(\mathbf{T_i,L})_\mathbf{L} = \nabla\boldsymbol{perr}(\mathbf{T})$;
3) множество приведенных к алфавиту **L** тестовых **L**-трасс, определяемых тройкой $\mathbf{T_i}$, совпадает с множеством первичных ∇-тестовых трасс:
   $\boldsymbol{tt}(\mathbf{T_i,L})_\mathbf{L} = \nabla\boldsymbol{ptt}(\mathbf{T})$.

Очевидно, что для трёх условий максимального ∇-пополнения каждое является следствием двух других.

Наша цель – построить максимальное ∇-пополнение.

3.2. Проблема ∇-пополнения без изменения семантики

Прежде всего, покажем, что в общем случае не существует ∇-пополнения в той же семантике. Для этого рассмотрим пример на Рис. 15. слева. Здесь в LTS $\mathbf{S_6}$ переход по реакции y ведет в начальное состояние LTS $\mathbf{S_5}$, совпадающей со спецификацией из примера на Рис. 11. .

Теорема 5: **О ∇-пополнении в той же семантике.** Для спецификационной тройки $\mathbf{T_6=(R/Q,\Sigma_6,}$***safe by***$\mathbf{)}$ в примере на Рис. 15. существуют конформные реализации, но не существует ∇-пополнения в той же семантике.

Доказательство см. на стр.108

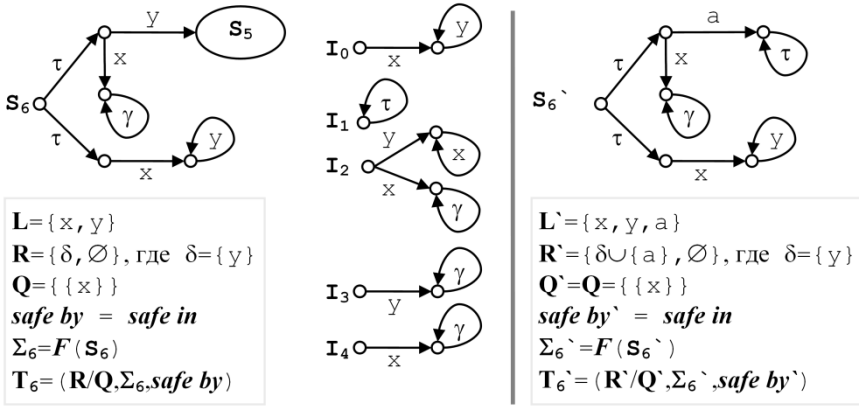


Рис. 15. Отсутствие ∇-пополнения в той же семантике и опасные неконформные трассы ∇-пополнения

Эту теорему можно усилить.

Теорема 6: **О семантиках и ∇-пополнениях в этих семантиках.** Для любой семантики **R/Q**, в которой 1) есть хотя бы две **R**-кнопки $R_1 \neq R_2$ и 2) хотя бы одна **Q**-кнопка Q, разрешающая действие $x \notin R_1 \cup R_2$, существует такая спецификационная тройка $\mathbf{T=(R/Q,\Sigma,}$***safe by***$\mathbf{)}$, для которой существуют конформные реализации, но не существует ∇-пополнения в той же семантике.

Доказательство см. на стр.110

Заметим, что эти условия не выполняется для семантики отношения ***ioco***: хотя каждый стимул x разрешается единственной **Q**-кнопкой {x}, то есть выполняется условие 2, но имеется только одна **R**-кнопка приема всех

реакций, то есть не выполняется условие 1. И действительно, для ***ioco***-семантики удается построить ∇-пополнение без изменения семантики [24].

В следующей теореме будет доказано, что для примера спецификационной тройки **T** на Рис. 15. слева в ∇-пополнении **T`**, изображенном справа, существует опасная трасса $\langle\varnothing,x,\gamma\rangle$, не встречающаяся в конформных реализациях. Более того, будет показано, что такая трасса имеется в любом ∇-пополнении для спецификационной тройки **T.**

Теорема 7: **О неконформных опасных трассах ∇-пополнения.** Существует такая спецификационная тройка, для которой существуют конформные реализации, но в любом ∇-пополнении есть опасные трассы, не встречающиеся в конформных реализациях.

Доказательство см. на стр.110

3.3. Операция $i^{\sim}$. Актуальность трасс

Пусть задана **R**/**Q**-семантика. Определим операцию вставки отказа $R\in\mathbf{R}$ в трассу $\sigma=\mu\cdot\lambda$ после трассы μ при условии, что трасса μ заканчивается отказом, а все действия из R запрещены постфиксом отказов трассы μ:[9]

если $p_{ost}(\mu)\neq\epsilon$ & $R\subseteq\cup Ip(\mu)$, то $\mu\cdot\lambda\text{—}i^{\sim}\!\!\rightarrow\mu\cdot\langle R\rangle\cdot\lambda$.

Как обычно, мы можем определить замыкание трассы σ как по новой операции $i^{\sim}$, так и по набору операций, включающих эту операции. Например, $i^{\sim}(\sigma)$, $di^{\sim}(\sigma)$. Заметим, что, в отличие от операции $i(\sigma)$ операция $i^{\sim}(\sigma)$ не зависит от множества трасс, а только от самой трассы σ. Очевидно, что $i^{\sim}(\sigma)\subseteq i(\sigma)$ и $p_{re}drt(\sigma)\subseteq p_{re}di^{\sim}(\sigma)\subseteq p_{re}di(\sigma)$.

Определим для согласованной и допустимой **R**-трассы σ в алфавите **L** (последовательности в алфавите $\mathbf{L}\cup\mathbf{R}\cup\{\Delta,\gamma\}$) **L**-модель, трассы которой – это все допустимые согласованные трассы вида $\mu\cdot\lambda$, где трасса $\mu\in p_{re}di^{\sim}(\sigma`)$, трасса $\sigma`$ получается из трассы σ вставкой пустого отказа после каждого префикса трассы σ, который не заканчивается и не продолжается в рамках σ отказами, а трасса λ не содержит непустых отказов, то есть $\lambda\in(\mathbf{L}\cup\{\varnothing\})^{*}$, и либо пуста, либо $\mu\cdot\langle\lambda(1)\rangle\notin p_{re}di^{\sim}(\sigma`)$.

Мы определим такую модель как LTS-модель $\mathbf{I}(\sigma)$ (см. Рис. 16.). Пусть подтрасса **L**-действий трассы σ имеет длину n, то есть $n=|\sigma\downarrow\mathbf{L}|$.

Состояниями LTS $\mathbf{I}(\sigma)$ будут все префиксы подтрассы **L**-действий трассы σ, то есть трассы вида $\sigma^{\wedge i}$, где $i=0..n$, а также дополнительное состояние ***t.***

В каждом состоянии $\sigma^{\wedge i}$, кроме последнего состояния $\sigma^{\wedge n}$, проведем следующие переходы:

---

[9] (Полная) трасса σ не обязательно является **R**-трассой, но операция $i^{\sim}$ вставляет только **R**-отказы. Если σ **R**-трасса, то операция $i^{\sim}$ порождает тоже **R**-трассу.

- переход в следующее состояние $\sigma\hat{}^{i+1}$ по следующему действию $\sigma\hat{}(i+1)$;
- переход в состояние ***t*** по каждому другому **L**-действию z, не запрещаемому постфиксом отказов трассы σ^i, то есть по каждому действию $z \in (\mathbf{L} \setminus \{\sigma\hat{}(i+1)\}) \cup \boldsymbol{Ip}(\sigma^i)$.

В последнем состоянии $\sigma\hat{}^n$ проведем следующие переходы:

- переход в состояние ***t*** по каждому **L**-действию z, не запрещаемому постфиксом отказов трассы σ^n при условии, что трасса σ не заканчивается дивергенцией или разрушением;
- переход-петлю по τ, если трасса σ заканчивается дивергенцией;
- переход-петлю по γ, если трасса σ заканчивается разрушением.

Это гарантирует наличие в каждом состоянии $\sigma\hat{}^i$ всех отказов, вложенных в $\cup\boldsymbol{Ip}(\sigma^i)$, и только таких отказов. Кроме того, если трасса σ^i не заканчивается отказом, в состоянии $\sigma\hat{}^i$ реализуется только пустой отказ.

В состоянии ***t*** проведем переходы-петли по всем действиям из **L**.

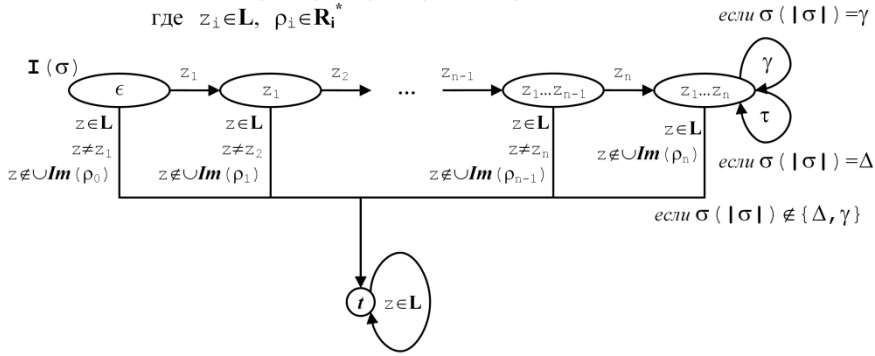


Рис. 16. Построение модели $\boldsymbol{I}(\sigma)$ *по трассе* σ

Формально множество переходов LTS $\mathbf{I}(\sigma)$ определяется как наименьшее множество трасс, порождаемое следующими правилами вывода: $\forall i=0..n$ $\forall z \in \mathbf{L}$

$i<n \quad \vdash \sigma^{\wedge i} — \sigma^{\wedge (i+1)} \rightarrow \sigma^{\wedge i+1}$,

$i<n \ \& \ z \notin \cup \boldsymbol{Ip}(\sigma^i) \ \& \ z \neq \sigma^{\wedge (i+1)} \quad \vdash \sigma^{\wedge i} — z \rightarrow \boldsymbol{t}$,

$|\sigma^{\wedge}| = n \ \& \ z \notin \cup \boldsymbol{Ip}(\sigma^n) \quad \vdash \sigma^{\wedge n} — z \rightarrow \boldsymbol{t}$,

$|\sigma^{\wedge}| \neq n \ \& \ \sigma^{\wedge (n+1)} = \Delta \quad \vdash \sigma^{\wedge n} — \tau \rightarrow \sigma^{\wedge n}$,

$|\sigma^{\wedge}| \neq n \ \& \ \sigma^{\wedge (n+1)} = \gamma \quad \vdash \sigma^{\wedge n} — \gamma \rightarrow \sigma^{\wedge n}$.

Заметим, что $|\sigma^{\wedge}| \neq n$ тогда и только тогда, когда трасса σ заканчивается дивергенцией или разрушением (поскольку $n = |\sigma \downarrow \mathbf{L}|$). В этом случае трасса $\sigma^{\wedge}$ имеет длину $n+1$ и тоже заканчивается дивергенцией или разрушением.

Лемма 1: Для того, чтобы любая модель вместе с трассой σ содержала и трассу μ, необходимо и достаточно, чтобы трасса μ была $\boldsymbol{p_{re}di}^{\sim}$-подтрассой трассы σ, то есть $\mu \in \boldsymbol{p_{re}di}^{\sim}(\sigma)$.

Доказательство см. на стр.111

Исследуем вопрос об **L**-актуальности тестовых трасс.

Лемма 2: Для любой тройки $\mathbf{T_i=(R_i/Q_i,\Sigma_i,}\boldsymbol{safe\ by_i}\mathbf{)}$, семантика которой **L**-эквивалентна семантике исходной тройки $\mathbf{T=(R/Q,\Sigma,}\boldsymbol{safe\ by}\mathbf{)}$, пустая трасса **L**-актуальна.

Доказательство см. на стр.114

Для дальнейшего нам понадобится модифицированнаяя LTS $\mathbf{I}(\sigma)$, которую обозначим $\mathbf{I_1}(\sigma)$ (Рис. 17.). Модификация заключается в следующем: в каждом состоянии $\sigma^{\wedge i}$, где $i<n$, удалим все переходы, ведущие в состояние $\boldsymbol{t}$, и добавим переход $\sigma^{\wedge i} — \tau \rightarrow \boldsymbol{t}$, если трасса σ^i не заканчивается отказом. Очевидно, что после такой модификации в LTS $\mathbf{I_1}(\sigma)$ в каждом состоянии $\sigma^{\wedge i}$ заканчиваются только трассы из $\boldsymbol{di}^{\sim}(\sigma^i)$, а трасса σ сохраняется.

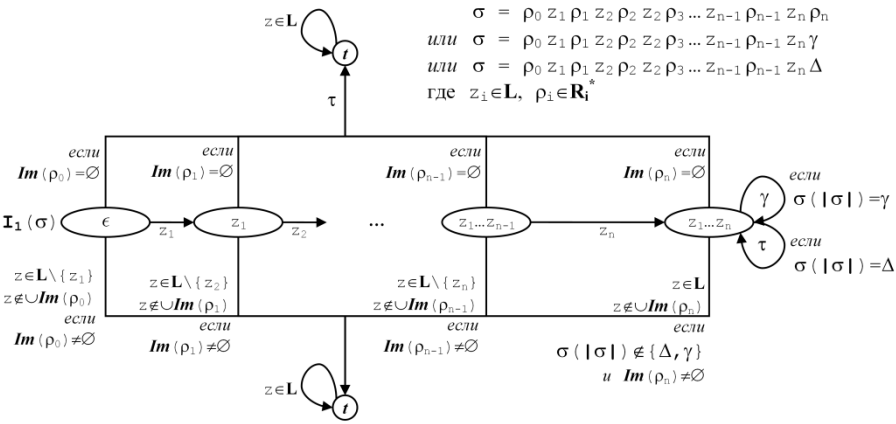


Рис. 17. Построение модели $I_1(\sigma)$ по трассе σ

Теорема 8: **L-актуальные наблюдения.** Пусть задана тройка $T_i=(R_i/Q_i,\Sigma_i,safe\ by_i)$, семантика которой **L**-эквивалентна семантике исходной тройки $T=(R/Q,\Sigma,safe\ by)$. Для того, чтобы наблюдение $u\in L\cup R_i$, безопасное после **L**-актуальной безопасной трассы σ, было **L**-актуальным, необходимо и достаточно, чтобы либо 1) наблюдение u было действием, оставляющим трассу $\sigma\cdot\langle u\rangle$ согласованной, то есть $u\notin\cup Ip(\sigma)$, либо 2) для T_i наблюдение u было R_i-отказом, и каждая кнопка $Q\in Q_i$ такая, что $Q_L\subseteq u_L\cup\cup Ip(\sigma_L)$, опасна после каждой безопасной **L**-трассы μ, для которой $\mu_L\in di\tilde{}(\sigma_L\cdot\langle u_L\rangle)$.

Доказательство см. на стр.114

3.4. ~трассы

∇-трассы (∇-тестовые трассы, ∇-ошибки и т.д.) в подразделе 3.1 определяются через **L**-конус $\nabla(T)_L$. В этом подразделе мы дадим сначала конструктивное определение трасс, которые мы будем называть ~трассами, через трассы исходной спецификационной тройки **T** и в следующих подразделах покажем связь ∇-трасс и ~трасс, определим ~пополнение на основе ~трасс, и далее ∇-пополнение на основе ~пополнения.

Для заданной спецификационной тройки **T** *~безопасными* после трассы σ будем называть:

- **Q**-кнопку $Q \in \mathbf{Q}$, если она безопасна после некоторой ***di~***-подтрассы трассы σ, безопасной в спецификации:

  Q ***safe~by*** Σ ***after*** $\sigma \triangleq \exists \mu \in \boldsymbol{di}^{\sim}(\sigma) \cap \boldsymbol{SafeBy}(\Sigma)$ Q ***safe by*** Σ ***after*** μ;

- пустой **R**-отказ, если $\varnothing \in \mathbf{R}$ и пустой отказ безопасен после некоторой ***di~***-подтрассы трассы σ, безопасной в спецификации:

  $\varnothing$ ***safe~by*** Σ ***after*** $\sigma \triangleq \exists \mu \in \boldsymbol{di}^{\sim}(\sigma) \cap \boldsymbol{SafeBy}(\Sigma)$ $\varnothing$ ***safe by*** Σ ***after*** μ;

- действие $z \in \mathbf{L}$, если оно безопасно после некоторой ***di~***-подтрассы трассы σ, безопасной в спецификации:

  z ***safe~by*** Σ ***after*** $\sigma \triangleq \exists \mu \in \boldsymbol{di}^{\sim}(\sigma) \cap \boldsymbol{SafeBy}(\Sigma)$ z ***safe by*** Σ ***after*** μ;

- непустой **R**-отказ $R \in \mathbf{R} \setminus \{\varnothing\}$, если каждое его действие ~безопасно:

  R ***safe~by*** Σ ***after*** $\sigma \triangleq \forall z \in R$ z ***safe~by*** Σ ***after*** σ;

- **R**-кнопку $R \in \mathbf{R}$, если ~безопасен отказ R.

Заметим, что пустой **R**-отказ безопасен после безопасной трассы тогда и только тогда, когда эта трасса не продолжается дивергенцией.

Для заданной спецификационной тройки наблюдение (действие или **R**-отказ) будем называть *~опасным* после трассы σ, если оно не является *~безопасным* после трассы σ. Также будем считать, что разрушение и дивергенция ~опасны после любой трассы.

Лемма 3: *~безопасность после отказа.* $\forall P \in \mathbf{R} \cup \mathbf{Q}$ $\forall R \in \mathbf{R}$ $\forall \kappa$ $\forall \lambda$

$$(P \textbf{ safe~by } \Sigma \textbf{ after } \kappa\cdot\lambda \Rightarrow P \textbf{ safe~by } \Sigma \textbf{ after } \kappa\cdot\langle R\rangle\cdot\lambda).$$

Доказательство см. на стр.116

Обратная импликация, вообще говоря, не верна. Пример на Рис. 18. .

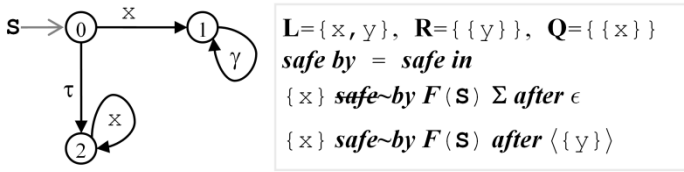


Рис. 18. Пример P ***safe~by*** Σ ***after*** $\kappa\cdot\langle R\rangle\cdot\lambda \not\Rightarrow P$ ***safe~by*** Σ ***after*** $\kappa\cdot\lambda$

Для заданной спецификационной тройки **T** **R**-трассу σ будем называть *~тестовой*, если

1) пустая трасса безопасна для **T**, и
2) каждый символ трассы ~безопасен после непосредственно предшествующего ему префикса.

Из этого следует, что ~тестовая трасса не содержит дивергенции и разрушения. Также из определения непосредственно следует префикс-замкнутость множества ~тестовых трасс.

Определим необходимые условия продолжения ∇-конформной трассы ∇-конформным наблюдением (доказательство необходимости см. ниже лемму 6). Для заданной спецификационной тройки *~конформными* после ~тестовой трассы $\sigma\in(\mathbf{L}\cup\mathbf{R})^*$ будем называть:

1) ~безопасное действие $z\in\mathbf{L}$, если выполнены два дополнительных условия ~конформности:
   a) z не запрещается постфиксом отказов трассы,
   b) каждая безопасная ***di~***-подтрасса, после которой z безопасно, им продолжается:

$$z\ \textbf{\textit{~conf}}\ \Sigma\ \textbf{\textit{after}}\ \sigma\ \triangleq\ z\ \textbf{\textit{safe~by}}\ \Sigma\ \textbf{\textit{after}}\ \sigma$$
$$\&\ z\notin\cup\textbf{\textit{Ip}}(\sigma)$$
$$\&\ \forall\mu\in\textbf{\textit{di~}}(\sigma)\cap\textbf{\textit{SafeBy}}(\Sigma)$$
$$(z\ \textbf{\textit{safe by}}\ \Sigma\ \textbf{\textit{after}}\ \mu\ \Rightarrow\ \mu\cdot\langle z\rangle\in\Sigma);$$

2) ~безопасный непустой **R**-отказ $R\in\mathbf{R}\setminus\{\varnothing\}$, если выполнены два дополнительных условия ~конформности:
   a) каждая **Q**-кнопка, все действия которой запрещены постфиксом отказов трассы $\sigma\cdot\langle R\rangle$, опасна после каждой безопасной ***di~***-подтрассы трассы $\sigma\cdot\langle R\rangle$,
   b) для каждого **R**-отказа, все действия которого запрещены постфиксом отказов трассы $\sigma\cdot\langle R\rangle$, каждая безопасная ***di~***-подтрасса трассы $\sigma\cdot\langle R\rangle$, после которой этот отказ безопасен, им продолжается:

$$R\ \textbf{\textit{~conf}}\ \Sigma\ \textbf{\textit{after}}\ \sigma\ \triangleq\ R\ \textbf{\textit{safe~by}}\ \Sigma\ \textbf{\textit{after}}\ \sigma$$
$$\&\ \forall Q\in\mathbf{Q}\ \ \forall\mu\in\textbf{\textit{di~}}(\sigma\cdot\langle R\rangle)\cap\textbf{\textit{SafeBy}}(\Sigma)$$
$$(Q\subseteq\cup\textbf{\textit{Ip}}(\sigma\cdot\langle R\rangle)\ \Rightarrow\ Q\ \textbf{\textit{safe by}}\ \Sigma\ \textbf{\textit{after}}\ \mu)$$
$$\&\ \forall P\in\mathbf{R}\ \ \forall\mu\in\textbf{\textit{di~}}(\sigma\cdot\langle R\rangle)\cap\textbf{\textit{SafeBy}}(\Sigma)$$
$$(P\subseteq\cup\textbf{\textit{Ip}}(\sigma\cdot\langle R\rangle)\ \&\ P\ \textbf{\textit{safe by}}\ \Sigma\ \textbf{\textit{after}}\ \mu\ \Rightarrow\ \mu\cdot\langle P\rangle\in\Sigma);$$

3) ~безопасный пустой отказ:

$$\varnothing\ \textbf{\textit{~conf}}\ \Sigma\ \textbf{\textit{after}}\ \sigma\ \triangleq\ \varnothing\ \textbf{\textit{safe~by}}\ \Sigma\ \textbf{\textit{after}}\ \sigma.$$

Для заданной спецификационной тройки **T** **R**-трассу σ будем называть ~*конформной*, если

1) пустая трасса безопасна для **T**, и
2) каждое наблюдение в трассе ~конформно после непосредственно предшествующего ему префикса трассы.

Из определения непосредственно следует префикс-замкнутость множества ~конформных трасс.

Поскольку условия ~конформности наблюдения после трассы включают условия ~безопасности наблюдения, ~конформная трасса является ~тестовой. Первичной ~тестовой трассой будем называть ~тестовую трассу, все строгие префиксы которой ~конформны.

Введем обозначения для всех множеств ~трасс:

~тестовых: $\sim\!\boldsymbol{tt}(\mathbf{T})$,

~конформных: $\sim\!\boldsymbol{conf}(\mathbf{T})$,

~ошибок: $\sim\!\boldsymbol{err}(\mathbf{T}) \triangleq \sim\!\boldsymbol{tt}(\mathbf{T}) \setminus \sim\!\boldsymbol{conf}(\mathbf{T})$,

первичных ~ошибок: $\sim\!\boldsymbol{perr}(\mathbf{T}) \triangleq \{\sigma \in \sim\!\boldsymbol{err}(\mathbf{T}) \mid \forall \mu < \sigma \;\; \mu \in \sim\!\boldsymbol{conf}(\mathbf{T})\}$,

первичных ~тестовых: $\sim\!\boldsymbol{ptt}(\mathbf{T}) \triangleq \sim\!\boldsymbol{perr}(\mathbf{T}) \cup \sim\!\boldsymbol{conf}(\mathbf{T})$

$= \{\sigma \in \sim\!\boldsymbol{tt}(\mathbf{T}) \mid \forall \mu < \sigma \;\; \mu \in \sim\!\boldsymbol{conf}(\mathbf{T})\}$.

Эти множества ~трасс изображены на Рис. 19. , который совпадает с Рис. 14. при замене символов "~"↔"∇".

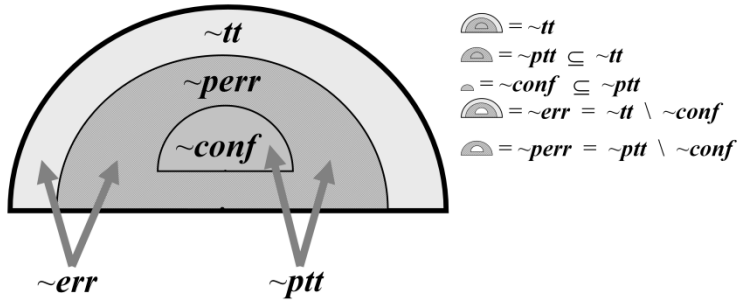


Рис. 19. Множества ~трасс

Лемма 4: $\forall \sigma \in \sim\!\boldsymbol{conf}(\mathbf{T}) \; \forall P \in \mathbf{R} \; (\boldsymbol{Ip}(\sigma) \neq \varnothing \;\&\; P \subseteq \cup \boldsymbol{Ip}(\sigma) \Rightarrow P \sim\!\boldsymbol{conf}\, \boldsymbol{\Sigma}\, \boldsymbol{after}\, \sigma)$.

Доказательство см. на стр.116

В этой лемме условие $\boldsymbol{Ip}(\sigma) \neq \varnothing$ требуется для случая $P = \varnothing$, так как иначе это условие следует из другого условия $P \subseteq \cup \boldsymbol{Ip}(\sigma)$.

Лемма 5: Для любой исходной спецификации: 1) каждая тестовая трасса ~тестовая, 2) безопасная трасса ~конформна тогда и только тогда, когда она актуальна, 3) каждая ошибка 1-го рода $\sigma\cdot\langle u\rangle$ не ~конформна.

Доказательство см. на стр.119

Соотношение ∇-трасс и ~трасс отражает следующее утверждение (необходимость условий ~конформности для ∇-конформности).

Лемма 6: 1) $\nabla\mathit{ptt}(\mathbf{T})\subseteq{\sim}\mathit{ptt}(\mathbf{T})$ и 2) $\nabla\mathit{conf}(\mathbf{T})\subseteq{\sim}\mathit{conf}(\mathbf{T})$.

Доказательство см. на стр.122

3.5. ~Пополнение

Будем называть *~пополнением* тройку $\mathbf{T_i}=(\mathbf{R_i/Q_i},\Sigma_i,\mathit{safe\ by_i})\approx_{\mathbf{L}}\mathbf{T}$ в **L**-эквивалентной семантике $\mathbf{R_i/Q_i}\approx_{\mathbf{L}}\mathbf{R/Q}$, для которой множество приведенных к алфавиту **L** безопасных **L**-трасс совпадает с множеством ~конформных трасс, а множество приведенных к алфавиту **L** тестовых **L**-трасс – с множеством первичных ~тестовых трасс:

$\mathit{SafeBy}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}}={\sim}\mathit{conf}(\mathbf{T})$ и $\mathit{tt}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}}={\sim}\mathit{ptt}(\mathbf{T})$.

Теорема 9: **Основное свойство ~пополнения.** Если существует ~пополнение $\mathbf{T_i}$, то $\mathit{conf}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}}=\nabla\mathit{conf}(\mathbf{T})$ и $\mathit{perr}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}}=\nabla\mathit{perr}(\mathbf{T})$.

Доказательство см. на стр.128

В этом подразделе мы определим **L**-эквивалентную семантику $\mathbf{R}^{\#}/\mathbf{Q}^{\#}\approx_{\mathbf{L}}\mathbf{R/Q}$ и построим ~пополнение $\mathbf{T}^{\sim}=(\mathbf{R}^{\#}/\mathbf{Q}^{\#},\Sigma^{\sim},\mathit{safe}_{\gamma\Delta})$, а в следующем подразделе покажем, что если удалить из $\Sigma^{\sim}$ все безопасные **L**-трассы, не являющиеся **L**-конформными, то получится ∇-пополнение.

Расширим алфавит **L** новыми действиями: для каждой кнопки $P\in\mathbf{R}\cup\mathbf{Q}$ добавим действие, называемое *не-отказ* P и обозначаемое как $\not P$. Везде, где мы будем использовать обозначение $\not P$, мы будем иметь в виду, что $P\in\mathbf{R}\cup\mathbf{Q}$. Предполагается, что $\forall A,B\in\mathbf{R}\cup\mathbf{Q}\ A\neq B\Rightarrow\not A\neq\not B$. В каждую кнопку $P\in\mathbf{R}\cup\mathbf{Q}$ добавляется не-отказ $\not P$. Обозначим кнопки с не-отказами, расширенную семантику (семейства кнопок с не-отказами) и расширенный алфавит: $\forall P\in\mathbf{R}\cup\mathbf{Q}\ P^{\#}\triangleq P\cup\{\not P\}$, $\mathbf{R}^{\#}\triangleq\{R^{\#}\mid R\in\mathbf{R}\}$, $\mathbf{Q}^{\#}\triangleq\{Q^{\#}\mid Q\in\mathbf{Q}\}$, $\mathbf{L}^{+}\triangleq\mathbf{L}\cup\{\not P\mid P\in\mathbf{R}\cup\mathbf{Q}\}$.

Очевидно, что $\mathbf{R}^{\#}/\mathbf{Q}^{\#}\approx_{\mathbf{L}}\mathbf{R/Q}$. Заметим, что отображение «$^{\#}$» для кнопок является взаимно-однозначным. Для **L**-действий определим отображение «$^{\#}$» как тождественное: $\forall z\in\mathbf{L}\ z^{\#}\triangleq z$.

Трассу, полученную из **R**-трассы σ, не заканчивающейся дивергенцией и разрушением, добавлением в каждый встречающийся в ней отказ $R\in\mathbf{R}$ соответствующего не-отказа, то есть заменой R на $R^{\#}$, будем обозначать $\sigma^{\#}$. Формально для $\sigma\in(\mathbf{L}\cup\mathbf{R})^{*}$: $\sigma^{\#} \triangleq \langle\sigma(i)^{\#}|i=1..|\sigma|\rangle$. Везде, где мы будем обозначать трассу как $\sigma^{\#}$, мы будем иметь в виду, что трасса $\sigma\in(\mathbf{L}\cup\mathbf{R})^{*}$ и является согласованной трассой. Она также допустима, поскольку не содержит дивергенции и разрушения. Распространим отображение «$^{\#}$» на множество трасс $\mathbf{N}\subseteq(\mathbf{L}\cup\mathbf{R})^{*}$: $\mathbf{N}^{\#} \triangleq \{\sigma^{\#}|\sigma\in\mathbf{N}\}$, результатом такого отображения является множество трасс. Для трасс и множеств трасс отображение «$^{\#}$» инъективно.

Очевидно, что $\mathbf{L}^{+} = \cup\mathbf{R}^{\#}\cup\cup\mathbf{Q}^{\#}$ и $\mathbf{R}^{\#}\cap\mathbf{Q}^{\#}=\varnothing$, то есть мы можем рассматривать $\mathbf{R}^{\#}/\mathbf{Q}^{\#}$-семантику для алфавита $\mathbf{L}^{+}$.

Также очевидно, что отображение «$_{\mathbf{L}}$» обратно к отображению «$^{\#}$» для кнопок, семейства кнопок, трасс и множества трасс[10]:

$P^{\#}{}_{\mathbf{L}}=P$, $\mathbf{R}^{\#}{}_{\mathbf{L}}=\mathbf{R}$, $\mathbf{Q}^{\#}{}_{\mathbf{L}}=\mathbf{Q}$, $\sigma^{\#}{}_{\mathbf{L}}=\sigma$, $\mathbf{N}^{\#}{}_{\mathbf{L}}=\mathbf{N}$.

~финальной трассой будем называть трассу $\sigma^{\#}$, где σ ~конформная трасса, а также ее продолжения не-отказом $\langle\not R\rangle$, за которым следует либо 1) дивергенция, если кнопка P ~безопасна и не все действия из P запрещены постфиксом отказов трассы или этот постфикс является пустой трассой (это важно для $P=\varnothing$), либо 2) разрушение, если кнопка P ~опасна. Если же кнопка P ~безопасна, но все действия из P запрещены непустым постфиксом отказов трассы, то продолжение этой трассы не-отказом $\langle\not R\rangle$ не является ~финальной трассой.

Формально множество $\mathbf{\Sigma^{01\sim}}$ ~финальных трасс определим как $\mathbf{\Sigma^{01\sim}}=\mathbf{\Sigma^{0\sim}}\cup\mathbf{\Sigma^{1\sim}}$, где $\mathbf{\Sigma^{0\sim}}=\sim\!\boldsymbol{conf}(\mathbf{T})^{\#}$, а $\mathbf{\Sigma^{1\sim}}$ –наименьшее множество, порождаемое следующими правилами вывода: $\forall\sigma\in\sim\!\boldsymbol{conf}(\mathbf{T})\ \ \forall P\in\mathbf{R}\cup\mathbf{Q}$

$\epsilon\notin\sim\!\boldsymbol{conf}(\mathbf{T})$ $\quad\vdash \epsilon\in\mathbf{\Sigma^{1\sim}}\ \&\ \langle\gamma\rangle\in\mathbf{\Sigma^{1\sim}}$,

$P\ \boldsymbol{safe\sim by}\ \mathbf{\Sigma}\ \boldsymbol{after}\ \sigma$ $\quad\vdash \sigma^{\#}\cdot\langle\not R\rangle\in\mathbf{\Sigma^{1\sim}}\ \&\ \sigma^{\#}\cdot\langle\not R,\gamma\rangle\in\mathbf{\Sigma^{1\sim}}$,

$P\ \boldsymbol{safe\sim by}\ \mathbf{\Sigma}\ \boldsymbol{after}\ \sigma\ \&\ (\boldsymbol{Ip}(\sigma)=\varnothing\vee P\not\subseteq\cup\boldsymbol{Ip}(\sigma))$ $\quad\vdash \sigma^{\#}\cdot\langle\not R\rangle\in\mathbf{\Sigma^{1\sim}}\ \&\ \sigma^{\#}\cdot\langle\not R,\Delta\rangle\in\mathbf{\Sigma^{1\sim}}$.

Замечание 10. Очевидно, что $\boldsymbol{Ip}(\sigma)=\varnothing \Leftrightarrow \boldsymbol{Ip}(\sigma^{\#})=\varnothing$
и $\forall A\subseteq\mathbf{L}\quad A\subseteq\boldsymbol{Ip}(\sigma) \Leftrightarrow A\subseteq\boldsymbol{Ip}(\sigma^{\#})$.

Используя определение ~конформной трассы, перепишем определение множества $\mathbf{\Sigma^{01\sim}}$ в следующем виде: $\forall\sigma\ \ \forall u\in\mathbf{R}\cup\mathbf{L}\ \ \forall P\in\mathbf{R}\cup\mathbf{Q}$

1) $\epsilon\notin\boldsymbol{SafeBy}(\mathbf{\Sigma})$ $\quad\vdash \epsilon\in\mathbf{\Sigma^{1\sim}}\ \&\ \langle\gamma\rangle\in\mathbf{\Sigma^{1\sim}}$,

[10] Отображение «$_{\mathbf{L}}$» обратно к отображению «$^{\#}$» только на области значений отображения «$^{\#}$», которое является подмножеством области определения отображения «$_{\mathbf{L}}$».

---

2) $\epsilon\in\boldsymbol{SafeBy}(\boldsymbol{\Sigma})$ $\vdash$ $\epsilon\in\boldsymbol{\Sigma}^{\mathbf{0}\sim}$,

3) $\sigma^{\#}\in\boldsymbol{\Sigma}^{\mathbf{0}\sim}$ & u ~***conf*** $\boldsymbol{\Sigma}$ ***after*** σ $\vdash$ $\sigma^{\#}\cdot\langle\mathsf{u}^{\#}\rangle\in\boldsymbol{\Sigma}^{\mathbf{0}\sim}$,

4) $\sigma^{\#}\in\boldsymbol{\Sigma}^{\mathbf{0}\sim}$ & P ~~***safe~by***~~ $\boldsymbol{\Sigma}$ ***after*** σ $\vdash$ $\sigma^{\#}\cdot\langle\not{\mathsf{P}}\rangle\in\boldsymbol{\Sigma}^{\mathbf{1}\sim}$ & $\sigma^{\#}\cdot\langle\not{\mathsf{P}},\gamma\rangle\in\boldsymbol{\Sigma}^{\mathbf{1}\sim}$,

5) $\sigma^{\#}\in\boldsymbol{\Sigma}^{\mathbf{0}\sim}$ & P ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** σ
& $(\boldsymbol{Ip}(\sigma)=\varnothing\vee\mathsf{P}\not\subseteq\cup\boldsymbol{Ip}(\sigma))$ $\vdash$ $\sigma^{\#}\cdot\langle\not{\mathsf{P}}\rangle\in\boldsymbol{\Sigma}^{\mathbf{1}\sim}$ & $\sigma^{\#}\cdot\langle\not{\mathsf{P}},\Delta\rangle\in\boldsymbol{\Sigma}^{\mathbf{1}\sim}$.

Множество $\boldsymbol{\Sigma}^{\mathbf{01}\sim}$ – это множество $\mathbf{R}^{\#}$-трасс в алфавите $\mathbf{L}^{+}$. Его подмножество $\boldsymbol{\Sigma}^{\mathbf{0}\sim}$ совпадает с подмножеством трасс, не заканчивающихся и не продолжающихся дивергенцией и разрушением. Если $\langle\gamma\rangle\in\boldsymbol{\Sigma}$, то пустая трасса опасна в исходной спецификации $\boldsymbol{\Sigma}$ и множество $\boldsymbol{\Sigma}^{\mathbf{01}\sim}=\boldsymbol{\Sigma}^{\mathbf{1}\sim}=\{\epsilon,\langle\gamma\rangle\}$ состоит из двух ~финальных **L**-трасс. В противном случае множество ~финальных **L**-трасс совпадает с множеством $\boldsymbol{\Sigma}^{\mathbf{0}\sim}$, то есть трасс вида $\sigma^{\#}$.

Будем называть **Q**-*свойством* множества **N** $\mathbf{R}^{\#}$-трасс в алфавите $\mathbf{L}^{+}$ следующее свойство: любая трасса $\sigma^{\#}$ продолжается не-отказом $\not{\mathsf{Q}}$ для любой кнопки $\mathsf{Q}\in\mathbf{Q}$. Формально: $\forall\sigma^{\#}\in\mathbf{N}\ \forall\mathsf{Q}\in\mathbf{Q}\ \ \sigma^{\#}\cdot\langle\not{\mathsf{Q}}\rangle\in\mathbf{N}$.

Будем называть **R**-*свойством* множества **N** $\mathbf{R}^{\#}$-трасс в алфавите $\mathbf{L}^{+}$ следующее свойство: для любой трассы $\sigma^{\#}$ и любой кнопки $\mathsf{R}\in\mathbf{R}$ выполняются следующие свойства:

1) Трасса $\sigma^{\#}$ не продолжается не-отказом $\not{\mathsf{R}}$ тогда и только тогда, когда $\boldsymbol{Ip}(\sigma)\neq\varnothing$ & $\mathsf{R}\subseteq\cup\boldsymbol{Ip}(\sigma)$.
2) Если трасса $\sigma^{\#}$ не продолжается не-отказом $\not{\mathsf{R}}$, то она продолжается отказом $\mathsf{R}^{\#}$.

Формально: $\forall\sigma^{\#}\in\mathbf{N}\ \forall\mathsf{R}\in\mathbf{R}$

$(\sigma^{\#}\cdot\langle\not{\mathsf{R}}\rangle\notin\mathbf{N}\ \Leftrightarrow\ \boldsymbol{Ip}(\sigma)\neq\varnothing\ \&\ \mathsf{R}\subseteq\cup\boldsymbol{Ip}(\sigma))\ \&\ (\sigma^{\#}\cdot\langle\not{\mathsf{R}}\rangle\notin\mathbf{N}\ \Rightarrow\ \sigma^{\#}\cdot\langle\mathsf{R}^{\#}\rangle\in\mathbf{N})$.

Будем называть $\Delta\gamma$-*свойством* множества **N** $\mathbf{R}^{\#}$-трасс в алфавите $\mathbf{L}^{+}$ следующее свойство:

1) $\mathbf{N}=\{\epsilon,\langle\gamma\rangle\}$ либо **N** содержит только трассы вида $\sigma^{\#}$, $\sigma^{\#}\cdot\langle\not{\mathsf{P}}\rangle$, $\sigma^{\#}\cdot\langle\not{\mathsf{P}},\Delta\rangle$ и $\sigma^{\#}\cdot\langle\not{\mathsf{P}},\gamma\rangle$ (где $\mathsf{P}\in\mathbf{R}\cup\mathbf{Q}$);
2) после не-отказа обязательно следует либо дивергенция, либо разрушение, либо и то и другое.

Формально:

1) $\mathbf{N}=\{\epsilon,\langle\gamma\rangle\}\ \vee\ \forall\pi\in\mathbf{N}\setminus(\mathbf{L}\cup\mathbf{R}^{\#})^{*}\ \exists\sigma^{\#}\ \exists\not{\mathsf{P}}\ \ \pi\in\{\sigma^{\#}\cdot\langle\not{\mathsf{P}}\rangle,\sigma^{\#}\cdot\langle\not{\mathsf{P}},\Delta\rangle,\sigma^{\#}\cdot\langle\not{\mathsf{P}},\gamma\rangle\}$,

2) $\forall\sigma^{\#}\in\mathbf{N}\ \forall\Bbbp\ (\sigma^{\#}\cdot\langle\Bbbp\rangle\in\mathbf{N}\ \Rightarrow\ (\sigma^{\#}\cdot\langle\Bbbp,\Delta\rangle\in\mathbf{N}\ \vee\ \sigma^{\#}\cdot\langle\Bbbp,\gamma\rangle\in\mathbf{N}))$.

Иными словами, трасса не содержит и не продолжается дивергенцией или разрушением тогда и только тогда, когда это $\sigma^{\#}$ трасса и $\mathbf{N}\neq\{\epsilon,\langle\gamma\rangle\}$.

Лемма 7: *~финальные трассы: Q- R- и Δγ-свойства.*

Для множества ~финальных трасс выполнены следующие свойства:

1) если трасса $\sigma^{\#}\in\mathbf{\Sigma}^{0\sim}$, кнопка $Q\in\mathbf{Q}$ и $Q\subseteq\cup\boldsymbol{Ip}(\sigma)$, то Q ~~***safe~by***~~ $\mathbf{\Sigma}$ ***after*** σ;

2) **Q**-свойство;

3) **R**-свойство;

4) Δγ-свойство с дополнительным условием: после не-отказа не могут следовать и дивергенция и разрушение:

$\forall\sigma^{\#}\in\mathbf{N}\ \forall\Bbbp\ (\sigma^{\#}\cdot\langle\Bbbp,\Delta\rangle\in\mathbf{N}\ \Rightarrow\ \sigma^{\#}\cdot\langle\Bbbp,\gamma\rangle\notin\mathbf{N})$.

Доказательство см. на стр.130

Лемма 8: Множество $\mathbf{\Sigma}^{01\sim}$ ~финальных трасс обладает всеми свойствами $\mathbf{R}^{\#}$-модели, кроме, быть может, замкнутости (по ***d***-операции).

Доказательство см. на стр.131

Лемма 9: ***d***-замыкание $\cup\boldsymbol{d}(\mathbf{N})$ сохраняет **Q**-свойство и Δγ-свойство множества трасс **N**.

Доказательство см. на стр.132

Заметим, что **R**-свойство может не сохраняться при ***d***-замыкании, но оно нам для ***d***-замыкания и последующего расширения до полной трассовой модели и не понадобится.

Лемма 10: Если множество **N** трасс обладает всеми свойствами трассовой модели, кроме, быть может, замкнутости (по ***d***-операции), то его ***d***-замыкание $\cup\boldsymbol{d}(\mathbf{N})$ является трассовой моделью.

Доказательство см. на стр.133

Лемма 11: Множество $\cup\boldsymbol{d}(\mathbf{\Sigma}^{01\sim})$ 1) является $\mathbf{R}^{\#}$-моделью, 2) обладает **Q**-свойством, 3) обладает Δγ-свойством.

Доказательство см. на стр.133

Согласно замечанию 5 в п.1.5 отношение безопасности кнопок после трасс достаточно определить на $\mathbf{R}^{\#}$-модели $\cup\boldsymbol{d}(\mathbf{\Sigma}^{01\sim})$. Выберем отношение безопасности кнопок $\boldsymbol{safe}_{\gamma\Delta}$, то есть объявим безопасной после трассы каждую неразрушающую кнопку. По замечанию 3 в п.1.5 такое отношение безопасности будет удовлетворять всем требования, предъявляемым к отношению ***safe by***, если каждая безопасная по $\boldsymbol{safe}_{\gamma\Delta}$ трасса для каждой неразрушающей (безопасной по $\boldsymbol{safe}_{\gamma\Delta}$) **Q**-кнопки Q продолжается каким-нибудь действием $z\in Q^{\#}$. Покажем, что это выполнено для $\mathbf{R}^{\#}$-модели $\cup\boldsymbol{d}(\mathbf{\Sigma}^{01\sim})$.

Действительно, по $\Delta\gamma$-свойству $\mathbf{R}^{\#}$-модели $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$ (лемма 11) такими трассами могут быть только трассы вида 1) $\sigma^{\#}$ или 2) $\sigma^{\#}\cdot\langle\not{\mathrm{R}}\rangle$ при условии $\sigma^{\#}\cdot\langle\not{\mathrm{R}},\gamma\rangle\notin\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$. Каждая трасса вида 1 по **Q**-свойству $\mathbf{R}^{\#}$-модели $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$ (лемма 11) продолжается не-отказом $\not{\mathrm{Q}}\in\mathrm{Q}^{\#}$ для любой кнопки $\mathrm{Q}\in\mathbf{Q}$. А трасса вида 2 по $\Delta\gamma$-свойству $\mathbf{R}^{\#}$-модели $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$ (лемма 11) продолжается дивергенцией, следовательно, после нее все кнопки разрушающие.

Обозначим через $\boldsymbol{\Sigma}^{\sim}$ любое расширение $\mathbf{R}^{\#}$-модели $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$ до полной модели, например, с помощью операции ***Ext***: $\boldsymbol{\Sigma}^{\sim}=\boldsymbol{Ext}(\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01\sim}}))$. Теперь спецификационная тройка $\mathbf{T}^{\sim}=(\mathbf{R}^{\#}/\mathbf{Q}^{\#},\boldsymbol{\Sigma}^{\sim},\boldsymbol{safe}_{\gamma\Delta})$ определена корректно.

Замечание 11. Расширение до полной трассовой модели по определению сохраняет множество $\mathbf{R}^{\#}$-трасс. Отсюда также следует, что **Q**-свойство и $\Delta\gamma$-свойство сохраняются, поскольку они касаются только множества $\mathbf{R}^{\#}$-трасс.

Лемма 12: Для исходной спецификации $\boldsymbol{\Sigma}$ необходимым и достаточным условием ~безопасности наблюдения u после трассы σ является существование такой кнопки P, которая разрешает наблюдение u и ~безопасна после этой трассы: $\forall\mathrm{u}\in\mathbf{L}\cup\mathbf{R}$

u ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** $\sigma\ \Leftrightarrow\ \exists\mathrm{P}\in\mathbf{R}\cup\mathbf{Q}\ \ (\mathrm{u}\in\mathrm{P}\vee\mathrm{u}=\mathrm{P}\ \&\ \mathrm{P}\in\mathbf{R})\ \&\ \mathrm{P}$ ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** σ.

Доказательство см. на стр.133

При ***d***-замыкании множества ~финальных трасс, в результате которого получается $\mathbf{R}^{\#}$-модель, некоторые ~финальные **L**-трассы продолжаются новыми **L**-наблюдениями. Однако, как показывает следующая лемма, все они опасны после соответствующих трасс.

Лемма 13: *~финальные трассы: О безопасности L-наблюдений.*

Если трасса $\kappa^{\#}\in\boldsymbol{\Sigma}^{\mathbf{0\sim}}$, **L**-наблюдение $\mathrm{u}^{\#}\in\mathbf{L}\cup\mathbf{R}^{\#}$ и трасса $\kappa^{\#}\cdot\langle\mathrm{u}^{\#}\rangle\in(\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01\sim}}))\setminus\boldsymbol{\Sigma}^{\mathbf{0\sim}}$, то $\mathrm{u}^{\#}$ ***safe***$_{\gamma\Delta}$ $\boldsymbol{\Sigma}^{\sim}$ ***after*** $\kappa^{\#}$.

Доказательство см. на стр.134

Следующая лемма дает простое правило определения безопасности кнопок для множества трасс с $\Delta\gamma$-свойством. Поскольку по лемме 7 множество ~финальных трасс обладает $\Delta\gamma$-свойством, это правило применимо и для множества ~финальных трасс.

Лемма 14: Если множество $\mathbf{N}$ трасс обладает $\Delta\gamma$-свойством, то для того, чтобы кнопка $\mathrm{P}^{\#}$ была безопасна по отношению ***safe***$_{\gamma\Delta}$ после трассы $\sigma^{\#}$, необходимо и достаточно, чтобы $\sigma^{\#}\cdot\langle\not{\mathrm{R}},\gamma\rangle\notin\mathbf{N}$.

Доказательство см. на стр.136

В общем случае для произвольного множества $\mathbf{N}$ трасс кнопка, которая безопасна по $\boldsymbol{safe}_{\gamma\Delta}$ после трассы, может стать опасной по $\boldsymbol{safe}_{\gamma\Delta}$ после этой трассы в результате $\boldsymbol{d}$-замыкания множества $\mathbf{N}$, то есть во множестве $\cup\boldsymbol{d}(\mathbf{N})$. Однако, следующая лемма показывает, что безопасность кнопок по $\boldsymbol{safe}_{\gamma\Delta}$ сохраняется при $\boldsymbol{d}$-замыкании множества ~финальных трасс.

Лемма 15: $\forall\mu^{\#}\in\boldsymbol{\Sigma}^{\mathbf{0}\sim}\ (\mu^{\#}\cdot\langle\text{Ꝑ},\gamma\rangle\notin\boldsymbol{\Sigma}^{\mathbf{1}\sim}\ \Leftrightarrow\ \mu^{\#}\cdot\langle\text{Ꝑ},\gamma\rangle\notin\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}\sim}))$.

Доказательство см. на стр.136

В результате простое правило определения безопасности кнопок после ~финальных трасс (только по множеству ~финальных трасс) сохраняется в итоговой полной трассовой модели $\boldsymbol{\Sigma}^{\sim}$.

Теорема 10: **~финальные трассы: Безопасность кнопок.**

$\forall\mu^{\#}\in\boldsymbol{\Sigma}^{\mathbf{0}\sim}\ \forall P\in\mathbf{R}\cup\mathbf{Q}\ (P^{\#}\ \boldsymbol{safe}_{\gamma\Delta}\ \boldsymbol{\Sigma}^{\sim}\ \boldsymbol{after}\ \mu^{\#}\ \Leftrightarrow\ \mu^{\#}\cdot\langle\text{Ꝑ},\gamma\rangle\notin\boldsymbol{\Sigma}^{\mathbf{1}\sim})$.

Доказательство см. на стр.136

Лемма 16: *~финальные трассы: Безопасность после отказа.*

$\forall P\in\mathbf{R}\cup\mathbf{Q}\ \forall R\in\mathbf{R}\ \forall\kappa\ \forall\lambda$

$(\kappa^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\in\boldsymbol{\Sigma}^{\mathbf{0}\sim}\ \&\ P^{\#}\ \boldsymbol{safe}_{\gamma\Delta}\ \boldsymbol{\Sigma}^{\sim}\ \boldsymbol{after}\ \kappa^{\#}\cdot\lambda^{\#}\ \Rightarrow\ P^{\#}\ \boldsymbol{safe}_{\gamma\Delta}\ \boldsymbol{\Sigma}^{\sim}\ \boldsymbol{after}\ \kappa^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#})$.

Доказательство см. на стр.137

Теорема 11: **~финальные трассы: Безопасные L-трассы.**

Множество $\boldsymbol{SafeBy}(\mathbf{T}^{\sim},\mathbf{L})=\boldsymbol{\Sigma}^{\mathbf{0}\sim}$ и однозначно определяется множеством $\boldsymbol{\Sigma}^{\mathbf{01}\sim}$ ~финальных трасс.

Доказательство см. на стр.137

Теорема 12: **~финальные трассы: L-актуальные наблюдения и трассы.**

1. Для $\mathbf{T}^{\sim}$ все трассы из множества $\boldsymbol{\Sigma}^{\mathbf{0}\sim}$ **L**-актуальны.
2. Для $\mathbf{T}^{\sim}$ **L**-наблюдение $u^{\#}\in\mathbf{L}\cup\mathbf{R}^{\#}$, безопасное после трассы $\sigma^{\#}\in\boldsymbol{\Sigma}^{\mathbf{0}\sim}$, **L**-актуально тогда и только тогда, когда либо 1) $u\in\mathbf{L}$ и $u\notin\cup\boldsymbol{Ip}(\sigma)$, либо 2) $u\in\mathbf{R}$ и для каждой кнопки $Q\in\mathbf{Q}$ такой, что $Q\subseteq u\cup\cup\boldsymbol{Ip}(\sigma)$, трасса $\mu^{\#}\cdot\langle\text{Ꝗ},\gamma\rangle\in\boldsymbol{\Sigma}^{\mathbf{1}\sim}$ для каждой трассы $\mu^{\#}\in\boldsymbol{\Sigma}^{\mathbf{0}\sim}$ такой, что $\mu\in\boldsymbol{di}^{\sim}(\sigma\cdot\langle u\rangle)$.

Доказательство см. на стр.138

Лемма 17: Для спецификационной тройки $\mathbf{T}^{\sim}$ на подмножестве безопасных **L**-трасс отношение $\boldsymbol{safe}_{\gamma\Delta}$ совпадает с отношением ***safe~by*** на этих же трассах, приведенных к алфавиту **L**:

$\forall\sigma^{\#}\in\boldsymbol{SafeBy}(\mathbf{T}^{\sim},\mathbf{L})\ \forall P\in\mathbf{R}\cup\mathbf{Q}\ (P^{\#}\ \boldsymbol{safe}_{\gamma\Delta}\ \boldsymbol{\Sigma}^{\sim}\ \boldsymbol{after}\ \sigma^{\#}\Leftrightarrow P\ \boldsymbol{safe\sim by}\ \boldsymbol{\Sigma}\ \boldsymbol{after}\ \sigma)$.

Доказательство см. на стр.139

Лемма 18: $\boldsymbol{SafeBy}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}}=\sim\boldsymbol{conf}(\mathbf{T})$ и $\boldsymbol{tt}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}}=\sim\boldsymbol{ptt}(\mathbf{T})$.

Доказательство см. на стр.140

Лемма 19: $\mathbf{T}^{\sim}\ \approx_{\mathbf{L}}\ \mathbf{T}$.

Доказательство см. на стр.140

Теорема 13: **О ~пополнении.** Спецификационная тройка $\mathbf{T}^{\sim}$ является ~пополнением тройки **T**.

Доказательство см. на стр.144

3.6. От ~пополнения к ∇-пополнению

∇-*финальной* трассой будем называть **L**-конформную ~финальную трассу σ, а также ее ~финальные не **L**-продолжения, то есть продолжения не-отказами и далее дивергенцией или разрушением. Множество ∇-финальных трасс обозначим как $\mathbf{\Sigma}^{\mathbf{01}\nabla}$ и формально определим:

$\mathbf{\Sigma}^{\mathbf{0}\nabla} \triangleq \boldsymbol{conf}(\mathbf{T}^{\sim},\mathbf{L})$,

$\mathbf{\Sigma}^{\mathbf{1}\nabla} \triangleq \{\sigma\cdot\langle \mathbb{R}\rangle\cdot\lambda \in \mathbf{\Sigma}^{\mathbf{1}\sim} \mid \sigma\in\mathbf{\Sigma}^{\mathbf{0}\nabla} \ \&\ \mathrm{P}\in\mathbf{R}\cup\mathbf{Q}\} \cup \{\sigma\in\mathbf{\Sigma}^{\mathbf{1}\sim} \mid \langle\gamma\rangle\in\mathbf{\Sigma}^{\mathbf{1}\sim}\}$,

$\mathbf{\Sigma}^{\mathbf{01}\nabla} \triangleq \mathbf{\Sigma}^{\mathbf{0}\nabla}\cup\mathbf{\Sigma}^{\mathbf{1}\nabla}$.

Множество $\mathbf{\Sigma}^{\mathbf{01}\nabla}$ – это множество $\mathbf{R}^{\#}$-трасс в алфавите $\mathbf{L}^{+}$. Его подмножество $\mathbf{\Sigma}^{\mathbf{0}\nabla}$ совпадает с подмножеством трасс, не заканчивающихся и не продолжающихся дивергенцией и разрушением.

Если для исходной спецификации **Σ** нет конформных реализаций, то множество $\mathbf{\Sigma}^{\mathbf{01}\nabla}$ ∇-финальных трасс пусто.

Если конформные реализации есть, то возможны два варианта.

1) Если $\langle\gamma\rangle\in\mathbf{\Sigma}$, то пустая трасса опасна в исходной спецификации **Σ**, множество $\mathbf{\Sigma}^{\mathbf{01}\nabla}=\mathbf{\Sigma}^{\mathbf{1}\nabla}=\mathbf{\Sigma}^{\mathbf{01}\sim}=\mathbf{\Sigma}^{\mathbf{1}\sim}=\{\epsilon, \langle\gamma\rangle\}$ состоит из двух ∇-финальных **L**-трасс, а множество **L**-конформных безопасных ~финальных трасс $\boldsymbol{conf}(\mathbf{T}^{\sim},\mathbf{L})=\mathbf{\Sigma}^{\mathbf{0}\nabla}=\varnothing$.
2) Если $\langle\gamma\rangle\notin\mathbf{\Sigma}$, то пустая трасса безопасна в исходной спецификации **Σ**, а множество ∇-финальных **L**-трасс совпадает с множеством **L**-конформных безопасных ~финальных трасс $\boldsymbol{conf}(\mathbf{T}^{\sim},\mathbf{L})=\mathbf{\Sigma}^{\mathbf{0}\nabla}\neq\varnothing$, то есть ∇-финальных трасс вида $\sigma^{\#}$.

Следующая лемма для ∇-финальных трасс аналогична лемме 7 для ~финальных трасс и утверждает, что **Q**-, **R**- и Δγ-свойства сохраняются и для подмножества $\mathbf{\Sigma}^{\mathbf{01}\nabla}\subseteq\mathbf{\Sigma}^{\mathbf{01}\sim}$.

Лемма 20: *∇-трассы: Q- R- и Δγ-свойства.* Множество $\mathbf{\Sigma}^{\mathbf{01}\nabla}$ ∇-финальных трасс обладает следующими свойствами:

1) **Q**-свойство;
2) **R**-свойство;

3) Δγ-свойство с дополнительным условием: после не-отказа не могут следовать и дивергенция и разрушение.

Доказательство см. на стр.145

Следующая лемма для ∇-финальных трасс аналогична лемме 8 для ~финальных трасс и утверждает, что, при условии наличия конформных реализаций для исходной тройки **T**, все свойства $\mathbf{R}^{\#}$-модели, кроме, быть может, замкнутости (по ***d***-операции), сохраняются и для подмножества $\boldsymbol{\Sigma}^{\mathbf{01}^{\nabla}} \subseteq \boldsymbol{\Sigma}^{\mathbf{01}^{\sim}}$.

Заметим, что если для исходной тройки **T** нет конформных реализаций, то множество $\boldsymbol{\Sigma}^{\mathbf{01}^{\nabla}}$ ∇-финальных трасс пусто и, тем самым, его ***d***-замыкание не может быть $\mathbf{R}^{\#}$-моделью, поскольку тоже пусто, хотя обладает всеми остальными свойствами $\mathbf{R}^{\#}$-модели.

Лемма 21: Если для исходной тройки **T** есть конформные реализации, то множество $\boldsymbol{\Sigma}^{\mathbf{01}^{\nabla}}$ ∇-финальных трасс обладает всеми свойствами $\mathbf{R}^{\#}$-модели, кроме, быть может, замкнутости (по ***d***-операции).

Доказательство см. на стр.147

Также при условии наличия конформных реализаций для исходной тройки **T**, следующая лемма для ∇-финальных трасс аналогична лемме 11 для ~финальных трасс и утверждает, что ***d***-замыкание подмножества $\boldsymbol{\Sigma}^{\mathbf{01}^{\nabla}} \subseteq \boldsymbol{\Sigma}^{\mathbf{01}^{\sim}}$ является $\mathbf{R}^{\#}$-моделью и обладает **Q**- и Δγ-свойствами так же, как ***d***-замыкание множества $\boldsymbol{\Sigma}^{\mathbf{01}^{\sim}}$.

Лемма 22: Если для исходной тройки **T** есть конформные реализации, то множество $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}^{\nabla}})$ 1) является $\mathbf{R}^{\#}$-моделью и 2) обладает **Q**-свойством, 3) обладает Δγ-свойством.

Доказательство см. на стр.148

Пусть для исходной тройки **T** есть конформные реализации. Тогда по лемме 22 $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}^{\nabla}})$ является трассовой $\mathbf{R}^{\#}$-моделью. Согласно замечанию 5 в п.1.5 отношение безопасности кнопок после трасс достаточно определить на $\mathbf{R}^{\#}$-модели $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}^{\sim}})$. Выберем отношение безопасности кнопок $\boldsymbol{safe}_{\gamma\Delta}$, то есть объявим безопасной после трассы каждую неразрушающую кнопку. По замечанию 3 в п.1.5 такое отношение безопасности будет удовлетворять всем требования к отношению ***safe by***, если каждая безопасная по $\boldsymbol{safe}_{\gamma\Delta}$ трасса для каждой неразрушающей (безопасной по $\boldsymbol{safe}_{\gamma\Delta}$) **Q**-кнопки $\mathtt{Q}$ продолжается каким-нибудь действием $\mathtt{z} \in \mathtt{Q}^{\#}$. Покажем, что это выполнено для $\mathbf{R}^{\#}$-модели $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}^{\nabla}})$.

Действительно, по Δγ-свойству $\mathbf{R}^{\#}$-модели $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}^{\nabla}})$ (лемма 22) такими трассами могут быть только трассы вида 1) $\sigma^{\#}$ или 2) $\sigma^{\#}\cdot\langle\text{Ꝑ}\rangle$ при условии $\sigma^{\#}\cdot\langle\text{Ꝑ}, \gamma\rangle \notin \cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}^{\nabla}})$. Каждая трасса вида 1 по **Q**-свойству $\mathbf{R}^{\#}$-модели $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}^{\nabla}})$ (лемма 22) продолжается не-отказом $\text{Ꝙ} \in \mathtt{Q}^{\#}$ для любой

кнопки $Q \in \mathbf{Q}$. А трасса вида 2 по $\Delta\gamma$-свойству $\mathbf{R}^{\#}$-модели $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}\nabla})$ (лемма 22) продолжается дивергенцией, следовательно, после нее все кнопки разрушающие.

Обозначим через $\boldsymbol{\Sigma}^{\nabla}$ любое расширение $\mathbf{R}^{\#}$-модели $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}\nabla})$ до полной модели, например, с помощью операции $\boldsymbol{Ext}$: $\boldsymbol{\Sigma}^{\nabla} = \boldsymbol{Ext}(\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}\nabla}))$. Теперь для случая, когда для исходной тройки $\mathbf{T}$ есть конформные реализации, спецификационная тройка $\mathbf{T}^{\nabla}=(\mathbf{R}^{\#}/\mathbf{Q}^{\#},\boldsymbol{\Sigma}^{\nabla},\boldsymbol{safe}_{\gamma\Delta})$ определена корректно.

Замечание 12. Аналогично замечанию 11 расширение до полной трассовой модели сохраняет множество $\mathbf{R}^{\#}$-трасс, что влечет сохранение $\mathbf{Q}$-свойства и $\Delta\gamma$-свойства, поскольку они касаются только множества $\mathbf{R}^{\#}$-трасс.

Поскольку по лемме 20 множество ∇-финальных трасс обладает $\Delta\gamma$-свойством, по лемме 14 мы имеем простое правило определения безопасности кнопок по отношению $\boldsymbol{safe}_{\gamma\Delta}$ на множестве ∇-финальных трасс. Следующая лемма аналогична лемме 15 и показывает, что безопасность кнопок по $\boldsymbol{safe}_{\gamma\Delta}$ сохраняется при $\boldsymbol{d}$-замыкании множества ∇-финальных трасс, то есть безопасность кнопок после ∇-финальных трасс во множестве $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}\nabla})$ определяется по-прежнему только по множеству ∇-финальных трасс $\boldsymbol{\Sigma}^{\mathbf{01}\nabla}$.

Лемма 23: $\forall\mu^{\#}\in\boldsymbol{\Sigma}^{\mathbf{0}\nabla}\ (\mu^{\#}\cdot\langle\not{\mathbf{R}},\gamma\rangle\notin\boldsymbol{\Sigma}^{\mathbf{1}\nabla} \Leftrightarrow \mu^{\#}\cdot\langle\not{\mathbf{R}},\gamma\rangle\notin\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}\nabla}))$.

Доказательство см. на стр.148

Следующая теорема для ∇-финальных трасс аналогична теореме 10 для ~финальных трасс и утверждает, что простое правило определения безопасности кнопок после ∇-финальных трасс (только по множеству ∇-финальных трасс) сохраняется в итоговой полной трассовой модели $\boldsymbol{\Sigma}^{\nabla}$.

Теорема 14: **∇-трассы: Безопасность кнопок.**

$\forall\mu^{\#}\in\boldsymbol{\Sigma}^{\mathbf{0}\nabla}\ \forall P\in\mathbf{R}\cup\mathbf{Q}\ (P^{\#}\ \boldsymbol{safe}_{\gamma\Delta}\ \boldsymbol{\Sigma}^{\nabla}\ \boldsymbol{after}\ \mu^{\#} \Leftrightarrow \mu^{\#}\cdot\langle\not{\mathbf{R}},\gamma\rangle\notin\boldsymbol{\Sigma}^{\mathbf{1}\nabla})$.

Доказательство см. на стр.149

Лемма 24: Отношения $\boldsymbol{safe}_{\gamma\Delta}$ на множестве $\boldsymbol{\Sigma}^{\mathbf{01}\nabla}$ и на множестве $\boldsymbol{\Sigma}^{\mathbf{01}\sim}$ совпадают на подмножестве ∇-финальных $\mathbf{L}$-трасс.

Доказательство см. на стр.149

Следующая теорема для ∇-финальных трасс аналогична теореме 11.

Теорема 15: **∇-трассы: Безопасные L-трассы.** Если для исходной спецификационной тройки $\mathbf{T}$ есть конформные реализации, то множество $\boldsymbol{SafeBy}(\mathbf{T}^{\nabla},\mathbf{L})=\boldsymbol{\Sigma}^{\mathbf{0}\nabla}$ и однозначно определяется множеством ∇-финальных трасс $\boldsymbol{\Sigma}^{\mathbf{01}\nabla}$.

Доказательство см. на стр.150

Следующая теорема для ∇-финальных трасс аналогична теореме 12 для ~финальных трасс.

Теорема 16: **∇-трассы: L-актуальные наблюдения и трассы.**

Если для исходной тройки $\mathbf{T}$ есть конформные реализации, то:

1. Для $\mathbf{T}^{\nabla}$ все трассы из множества $\mathbf{\Sigma}^{\mathbf{0}\nabla}$ **L**-актуальны.
2. Для $\mathbf{T}^{\nabla}$ **L**-наблюдение $u^{\#}\in\mathbf{L}\cup\mathbf{R}^{\#}$, безопасное после трассы $\sigma^{\#}\in\mathbf{\Sigma}^{\mathbf{0}\nabla}$, **L**-актуально тогда и только тогда, когда либо 1) $u\in\mathbf{L}$ и $u\notin\cup\boldsymbol{Ip}(\sigma)$, либо 2) $u\in\mathbf{R}$ и для каждой кнопки $Q\in\mathbf{Q}$ такой, что $Q\subseteq u\cup\cup\boldsymbol{Ip}(\sigma)$, трасса $\mu^{\#}\cdot\langle\Theta,\gamma\rangle\in\mathbf{\Sigma}^{\mathbf{1}\nabla}$ для каждой трассы $\mu^{\#}\in\mathbf{\Sigma}^{\mathbf{0}\nabla}$ такой, что $\mu\in\boldsymbol{di}^{\sim}(\sigma\cdot\langle u\rangle)$.

Доказательство см. на стр.150

Лемма 25: Если для исходной тройки $\mathbf{T}$ есть конформные реализации, то $\boldsymbol{SafeBy}(\mathbf{T}^{\nabla},\mathbf{L})=\boldsymbol{conf}(\mathbf{T}^{\sim},\mathbf{L})$ и $\boldsymbol{err}_1(\mathbf{T}^{\nabla},\mathbf{L})=\boldsymbol{perr}(\mathbf{T}^{\sim},\mathbf{L})$.

Доказательство см. на стр.151

Следующая лемма для ∇-финальных трасс аналогична лемме 19 для ~финальных трасс, но только вместо $\mathbf{T}\approx_{\mathbf{L}}\mathbf{T}^{\sim}$ утверждается $\mathbf{T}\leq_{\mathbf{L}}\mathbf{T}^{\nabla}$.

Лемма 26: Если для исходной тройки $\mathbf{T}$ есть конформные реализации, то $\mathbf{T}^{\nabla}\in\nabla(\mathbf{T})_{\mathbf{L}}$.

Доказательство см. на стр.151

Следующая лемма для ∇-финальных трасс аналогична теореме 13 для ~финальных трасс, но только, если $\mathbf{T}^{\sim}$ является ~пополнением, то $\mathbf{T}^{\nabla}$ является ∇-пополнением, причем максимальным.

Теорема 17: **О ∇-пополнении.** Если для исходной спецификационной тройки $\mathbf{T}$ есть конформные реализации, то тройка $\mathbf{T}^{\nabla}$ является максимальным ∇-пополнением тройки **T**.

Доказательство см. на стр.152

Замечание 13. Тестирование излишне в двух случаях: 1) когда нет конформных реализаций, 2) все реализации конформны. В случае 1 по теореме 4 ∇-пополнение не существует, а в случае 2 оно состоит из двух трасс $\{\epsilon,\langle\gamma\rangle\}$. В обоих случаях (и только в этих случаях) множество $\boldsymbol{conf}(\mathbf{T}^{\sim},\mathbf{L})$ пусто. Эти два случаях различаются между собой наличием или отсутствием разрушения в начале исходной спецификации. Конечно, в случае, когда множество $\boldsymbol{conf}(\mathbf{T}^{\sim},\mathbf{L})$ не пусто, тестирование также может быть излишне, если все безопасно-тестируемые реализации конформны. Например, если в исходной спецификации с самого начала нет разрушения, но есть дивергенция.

3.7. ~пополнение и ∇-пополнение при расширении Ext

Лемма 27: Расширение $Ext(\mathbf{N})$ сохраняет **Q**-свойство множества **N** $\mathbf{R}^{\#}$-трасс.

Доказательство см. на стр.153

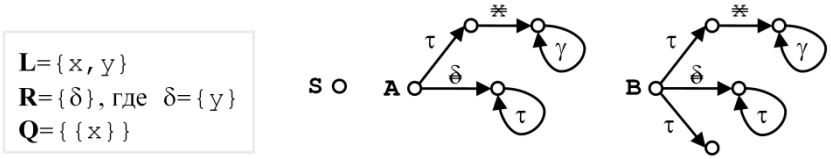
Теорема 18: **О ~пополнении с расширением *Ext*.** При использовании расширения ***Ext*** 1) ~пополнение $\mathbf{\Sigma}^{\sim}$ не содержит $\mathbf{Q}^{\#}$-отказов, и 2) $safe_{\gamma\Delta}$ **=** ***safe in*.**

Доказательство см. на стр.153

Теорема 19: **О ∇-пополнении с расширением *Ext*.** Если для исходной спецификационной тройки **T** есть конформные реализации, то при использовании расширения ***Ext*** 1) ∇-пополнение $\mathbf{\Sigma}^{\nabla}$ не содержит $\mathbf{Q}^{\#}$-отказов, 2) $safe_{\gamma\Delta}$ **=** ***safe in*.**

Доказательство см. на стр.153

Заметим, что $\mathbf{Q}^{\#}$-отказы будут отсутствовать в полной трассовой модели не при любом расширении множеств $\cup d(\mathbf{\Sigma}^{01\sim})$ и $\cup d(\mathbf{\Sigma}^{01\nabla})$. Пример приведен на Рис. 20. . Здесь для ***ioco***-семантики **R**/**Q** изображена LTS-спецификация **S**, состоящая из одного терминального состояния, множество ее полных трасс $F(\mathbf{S})$. Множество ~финальных трасс $F(\mathbf{S})^{01\sim}$ не меняется при ***d***-замыкании $\cup d(F(\mathbf{S})^{01\sim})=F(\mathbf{S})^{01\sim}$. $\mathbf{R}^{\#}$-модель $\cup d(F(\mathbf{S})^{01\nabla}) = \cup d(F(\mathbf{S})^{01\sim})$ задана в виде $\mathbf{R}^{\#}$-трасс LTS **A**. Множество $F(\mathbf{A})$ полных трасс LTS **A** совпадает с ~пополнением спецификации $F(\mathbf{S})$, полученным из $\cup d(F(\mathbf{S})^{01\sim})$ с помощью расширения ***Ext***. В то же время множество $F(\mathbf{B})$ полных трасс LTS **B** также является ~пополнением спецификации $F(\mathbf{S})$, но полученным из $\cup d(F(\mathbf{S})^{01\sim})$ с помощью расширения, отличного от ***Ext***. Можно заметить, что в $F(\mathbf{A})$ трассы не содержат $\mathbf{Q}^{\#}$-отказов, а в $F(\mathbf{B})$ есть трасса $\langle\{x,\not\approx\}\rangle$, где $\{x\}\in\mathbf{Q}$.



$F(\mathbf{A})\downarrow(\mathbf{L}^{\#}\cup\mathbf{R}^{\#}\cup\{\Delta,\gamma\}) = F(\mathbf{B})\downarrow(\mathbf{L}^{\#}\cup\mathbf{R}^{\#}\cup\{\Delta,\gamma\}) = F(\mathbf{S})^{\sim} = F(\mathbf{S})^{\nabla}$
$F(\mathbf{S})^{01\sim} = F(\mathbf{S})^{\sim} = T(\mathbf{R}^{\#},\mathbf{A})$

Рис. 20. $\mathbf{Q}^{\#}$-отказы при расширении до полной трассовой модели

Впервые пополнение, аналогичное ~пополнению, было определено в [10]. Для полной трассовой модели спецификации $\boldsymbol{\Sigma}$ определялось множество ~финальных (они назывались просто финальными) трасс $\boldsymbol{final}(\boldsymbol{\Sigma})$, но не на основе безопасных $\boldsymbol{di}^{\sim}$-подтрасс трасс исходной спецификации как для ~трасс при определении $\boldsymbol{\Sigma}^{\mathbf{01}\sim}$ в 3.5, а на основе безопасных $\boldsymbol{drt}$-подтрасс трасс исходной спецификации. Далее аналогично показывалось, что $\boldsymbol{d}$-замыкание $\cup\boldsymbol{d}(\boldsymbol{final}(\boldsymbol{\Sigma}))$ является $\mathbf{R}^{\#}$-моделью. После этого применялось расширение $\boldsymbol{Ext}$. В результате получалось пополнение: $\boldsymbol{Comp}(\boldsymbol{\Sigma}) \triangleq \boldsymbol{Ext}(\cup\boldsymbol{d}(\boldsymbol{final}(\boldsymbol{\Sigma})))$.

На $\boldsymbol{Comp}(\boldsymbol{\Sigma})$ определялось отношение ***safe by* = *safe in***, которое при отсутствии $\mathbf{Q}^{\#}$-отказов корректно, то есть удовлетворяет всем трем требованиям, предъявляемым к отношению ***safe by***.

В [10] дополнительно доказывалось, что, если полученную спецификацию $\boldsymbol{Comp}(\boldsymbol{\Sigma})$ и отношение ***safe by* = *safe in*** рассматривать не в **L**-эквивалентной семантике $\mathbf{R}^{\#}/\mathbf{Q}^{\#}$, а в (вообще говоря, не **L**-эквивалентной) семантике $\mathbf{R}^{\#}\cup\mathbf{Q}^{\#}/\varnothing$, то такая спецификационная тройка принадлежит **L**-конусу $\nabla(\mathbf{T})_{\mathbf{L}}$ исходной спецификационной тройки **T**, то есть сохраняется класс конформных **L**-реализаций и не сужается класс безопасно-тестируемых **L**-реализаций (хотя может расширяться). Этот результат легко переносится на ~ и ∇-пополнение, но это выходит за рамки данной работы.

3.8. Конструктивное определение конформных трасс

Цель этого подраздела – конструктивно определить множество **L**-конформных ~финальных трасс $\boldsymbol{conf}(\mathbf{T}^{\sim},\mathbf{L})$.

Если $\langle\gamma\rangle\in\boldsymbol{\Sigma}$, то пустая трасса опасна в исходной спецификации $\boldsymbol{\Sigma}$, множество $\boldsymbol{\Sigma}^{\mathbf{01}\nabla}=\boldsymbol{\Sigma}^{\mathbf{1}\nabla}=\boldsymbol{\Sigma}^{\mathbf{01}\sim}=\boldsymbol{\Sigma}^{\mathbf{1}\sim}=\{\epsilon,\langle\gamma\rangle\}$ состоит из двух ∇-финальных **L**-трасс, а множество **L**-конформных безопасных ~финальных трасс $\boldsymbol{conf}(\mathbf{T}^{\sim},\mathbf{L})=\boldsymbol{\Sigma}^{\mathbf{0}\nabla}=\varnothing$.

В дальнейшем будем предполагать, что $\langle\gamma\rangle\notin\boldsymbol{\Sigma}$.

3.8.1. L-неконвергентность и L-неполнота.

Мы покажем, что есть только две причины существования **L**-неконформных трасс: **L**-неконвергентность и **L**-неполнота.

L-неконвергентность означает, что для кнопки $P^{\#}$, безопасной в спецификации после некоторой безопасной трассы $\mu^{\#}$, спецификация не определяет никакого конформного **L**-наблюдения u, то есть такого u, что $u\in P$ или $u=P^{\#}$ (если $P\in\mathbf{R}$).

Заметим, что поскольку в спецификационной модели все трассы конвергентны, спецификация определяет единственное наблюдение – не-отказ $\not\Rightarrow$, который, однако, не является **L**-наблюдением.

Понятно, что, если в какой-нибудь безопасно-тестируемой **L**-реализации имеется такая трасса $\mu^{\#}$, то при тестировании нажатие кнопки $P^{\#}$ после $\mu^{\#}$ может дать только **L**-наблюдение, а все такие наблюдения неконформны. А это означает, что любая **L**-реализация, содержащая трассу $\mu^{\#}$, неконформна. Следовательно, трасса $\mu^{\#}$ **L**-неконформна, хотя имеется в спецификации.

L-неполнота. Пусть для кнопки $P^{\#}$, безопасной в спецификации после некоторой безопасной трассы $\mu^{\#}$, заканчивающейся отказом, спецификация не определяет никакого конформного **L**-действия $z \in P$.

Заметим, что поскольку в спецификационной модели все трассы конвергентны, спецификация определяет в качестве конформного наблюдения либо не-отказ $\not\Rightarrow$, либо отказ $P^{\#}$, либо и то и другое. В первом случае, когда определяется только не-отказ $\not\Rightarrow$, имеем ситуацию **L**-неконвергентности. Во втором случае, когда определяется только отказ $P^{\#}$, по полноте спецификационной модели поведение (множество трасс) спецификации после трасс $\mu^{\#}$ и $\mu^{\#}\cdot\langle P^{\#}\rangle$ одинаковое. По правилам вывода ~финальных трасс не-отказ $\not\Rightarrow$ отсутствует после трассы $\mu^{\#}$ тогда и только тогда, когда $\boldsymbol{Ip}(\mu)\neq\varnothing$ & $P\subseteq\cup\boldsymbol{Ip}(\mu)$.

Остается третий случай: после трассы $\mu^{\#}$ спецификация определяет как не-отказ $\not\Rightarrow$, так и отказ $P^{\#}$. В этом случае поведение (множество трасс) реализации после трасс $\mu^{\#}$ и $\mu^{\#}\cdot\langle P^{\#}\rangle$ может быть различным. В то же время, если **L**-реализация конформна и в ней есть трасса $\mu^{\#}$, то она не может продолжаться неконформными действиями $z \in P$. Поэтому по полноте реализационной модели в ней должна быть трасса $\mu^{\#}\cdot\langle P^{\#}\rangle$, и поведение (множество трасс) реализации после трасс $\mu^{\#}$ и $\mu^{\#}\cdot\langle P^{\#}\rangle$ одинаковое.

Заметим, что, если в спецификации после $\mu^{\#}\cdot\langle P^{\#}\rangle$ есть безопасная **L**-трасса $\lambda^{\#}$, то по ***d***-замкнутости спецификационной модели такая **L**-трасса есть и после трассы $\mu^{\#}$, хотя она может быть опасной. Иными словами, различие поведения спецификации после трасс $\mu^{\#}$ и $\mu^{\#}\cdot\langle P^{\#}\rangle$ может заключаться лишь в том, что в спецификации имеется некоторая трасса $\mu^{\#}\cdot\lambda^{\#}$, но нет трассы $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}$. В этом случае у трассы $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}$ имеется префикс $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_1{}^{\#}$, являющийся ошибкой 1-го рода, определяемой спецификацией.

Если эта трасса $\mu^{\#}\cdot\lambda^{\#}$ безопасна в спецификации, то в любой конформной **L**-реализации, в которой есть трасса $\mu^{\#}\cdot\lambda^{\#}$, должна быть также и трасса $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}$, что противоречит конформности реализации. Следовательно, трасса $\mu^{\#}\cdot\lambda^{\#}$ **L**-неконформна, хотя имеется в спецификации. Такую трассу $\mu^{\#}\cdot\lambda^{\#}$ будем называть **L**-неполной.

3.8.2. Удаление L-неконвергентных и L-неполных трасс.

Определим **L**-неконвергентность и **L**-неполноту формально.

Будем говорить, что **L**-трасса $\mu^{\#}\in\mathbf{N}$ *P-неконвергентна* во множестве трасс **N**, где $P\in\mathbf{R}\cup\mathbf{Q}$, если $\mu^{\#}\cdot\langle\text{Ꝑ},\gamma\rangle\notin\mathbf{N}$, но каждое **L**-наблюдение u, разрешаемое этой кнопкой, то есть $u\in P\cup\{P^{\#}\}$, отсутствуют в **N** после этой трассы:

для $\mu^{\#}\in\mathbf{N}$ и $P\in\mathbf{R}\cup\mathbf{Q}$:

$\mu^{\#}$ P-*неконвергентна в* **N** $\triangleq$ $\mu^{\#}\cdot\langle\text{Ꝑ},\gamma\rangle\notin\mathbf{N}$ & $\forall u\in P\cup\{P^{\#}\}\ \mu^{\#}\cdot\langle u\rangle\notin\mathbf{N}$.

$\mu^{\#}$ P-*конвергентна в* **N** $\triangleq$ $\mu^{\#}\cdot\langle\text{Ꝑ},\gamma\rangle\in\mathbf{N}$ $\vee$ $\exists u\in P\cup\{P^{\#}\}\ \mu^{\#}\cdot\langle u\rangle\notin\mathbf{N}$.

Будем говорить, что **L**-трасса $\mu^{\#}\in\mathbf{N}$ **L**-*неконвергентна* во множестве трасс **N**, если она P-неконвергентна в **N** для какой-нибудь кнопки $P\in\mathbf{R}\cup\mathbf{Q}$:

для $\mu^{\#}\in\mathbf{N}$:

$\mu^{\#}$ **L**-*неконвергентна в* **N** $\triangleq$ $\exists P\in\mathbf{R}\cup\mathbf{Q}$ $\mu^{\#}$ P-*неконвергентна в* **N**.

$\mu^{\#}$ **L**-*конвергентна в* **N** $\triangleq$ $\forall P\in\mathbf{R}\cup\mathbf{Q}$ $\mu^{\#}$ P-*конвергентна в* **N**.

$\mathbf{R}^{\#}$-отказ $P^{\#}\in\mathbf{R}^{\#}$ будем называть *особым после* трассы $\mu^{\#}\in\mathbf{N}$ во множестве трасс **N**, если $\mu^{\#}\cdot\langle\text{Ꝑ},\gamma\rangle\notin\mathbf{N}$, трасса $\mu^{\#}$ заканчивается некоторым отказом и во множестве **N** не продолжается никаким **L**-действием z, разрешаемым этой кнопкой, то есть $z\in P$:

для $\mu^{\#}\in\mathbf{N}$ и $P\in\mathbf{R}$:

$P^{\#}$ *особый после* $\mu^{\#}$ *в* **N** $\triangleq$ $\boldsymbol{Ip}(\mu)\neq\varnothing$ & $\mu^{\#}\cdot\langle\text{Ꝑ},\gamma\rangle\notin\mathbf{N}$ & $\forall z\in P\ \ \mu^{\#}\cdot\langle z\rangle\notin\mathbf{N}$.

L-трассу $\mu^{\#}\cdot\lambda^{\#}\in\mathbf{N}$ будем называть *P-неполной* после $\mu^{\#}\in\mathbf{N}$ во множестве трасс **N**, где $P^{\#}\in\mathbf{R}^{\#}$, если после ее префикса $\mu^{\#}$ есть особый отказ $P^{\#}$, после которого нет трассы $\lambda^{\#}$:

для $\mu^{\#}\cdot\lambda^{\#}\in\mathbf{N}$ и $P\in\mathbf{R}$:

$\mu^{\#}\cdot\lambda^{\#}$ P-*неполна после* $\mu^{\#}$ *в* **N** $\triangleq$ $P^{\#}$ *особый после* $\mu^{\#}$ *в* **N** & $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin\mathbf{N}$.

$\mu^{\#}\cdot\lambda^{\#}$ P-*полна после* $\mu^{\#}$ *в* **N** $\triangleq$ $P^{\#}$ *особый после* $\mu^{\#}$ *в* **N** $\Rightarrow$ $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\in\mathbf{N}$.

L-трасса $\mu^{\#}\cdot\lambda^{\#}\in\mathbf{N}$ **L**-*неполна после* $\mu^{\#}$ во множестве трасс **N**, если она P-неполна после $\mu^{\#}$ в **N** для какой-нибудь **R**-кнопки P:

для $\mu^{\#}\cdot\lambda^{\#}\in\mathbf{N}$:

$\mu^{\#}\cdot\lambda^{\#}$ **L**-*неполна после* $\mu^{\#}$ *в* **N** $\triangleq$ $\exists \mathsf{P}\in\mathbf{R}$ $\mu^{\#}\cdot\lambda^{\#}$ P-*неполна после* $\mu^{\#}$ *в* **N**.

$\mu^{\#}\cdot\lambda^{\#}$ **L**-*полна после* $\mu^{\#}$ *в* **N** $\triangleq$ $\forall \mathsf{P}\in\mathbf{R}$ $\mu^{\#}\cdot\lambda^{\#}$ P-*полна после* $\mu^{\#}$ *в* **N**.

L-трасса $\sigma^{\#}\in$**N** **L**-*неполна* во множестве трасс **N**, если она **L**-неполна после некоторого своего префикса в **N**:

для $\sigma^{\#}\in$**N**:

$\sigma^{\#}$ **L**-*неполна в* **N** $\triangleq$ $\exists \mu^{\#}\le\sigma^{\#}$ $\sigma^{\#}$ **L**-*неполна после* $\mu^{\#}$ *в* **N**.

$\sigma^{\#}$ **L**-*полна в* **N** $\triangleq$ $\forall \mu^{\#}\le\sigma^{\#}$ $\sigma^{\#}$ **L**-*полна после* $\mu^{\#}$ *в* **N**.

Разумеется, если трасса **L**-неконформна, то все её продолжения также **L**-неконформны. Поэтому вместе с каждой **L**-неконвергентной или **L**-неполной трассой мы должны удалить и все их продолжения, в том числе продолжения, не являющиеся **L**-трассами (заканчивающиеся не-отказом или следующими после него дивергенцией или разрушением).

Удаление **L**-неконвергентных и **L**-неполных трасс может привести к появлению новых **L**-неконвергентных и **L**-неполных трасс. Например, пусть удаляется трасса $\mu^{\#}\cdot\langle \mathsf{u}\rangle$. Если после трассы $\mu^{\#}$ наблюдение u является единственным **L**-наблюдением, разрешаемым некоторой безопасной после $\mu^{\#}$ кнопкой $\mathsf{P}^{\#}$, то удаление трассы $\mu^{\#}\cdot\langle \mathsf{u}\rangle$ приведет к тому, что трасса $\mu^{\#}$ становится P-неконвергентной, следовательно, **L**-неконвергентной. Если, кроме u, трасса $\mu^{\#}$ продолжается еще одним **L**-наблюдением – $\mathbf{R}^{\#}$-отказом $\mathsf{P}^{\#}$, то удаление трассы $\mu^{\#}\cdot\langle \mathsf{u}\rangle$ приведет к тому, что отказ $\mathsf{P}^{\#}$ становится особым после трассы $\mu^{\#}$, а это может привести к тому, что некоторые трассы вида $\mu^{\#}\cdot\lambda^{\#}$ становятся P-неполными, следовательно, **L**-неполными.

Поэтому общее определение **L**-неконформных трасс индуктивное.

Замечание 14. Вместо удаления **L**-неполных трасс мы могли бы при генерации полного набора тестов просто учитывать особые отказы. Тест генерировался бы только по такой трассе, у которой нет префикса $\mu^{\#}\cdot\langle \mathsf{u}\rangle$, где u не является особым отказом после $\mu^{\#}$, но после $\mu^{\#}$ существует некоторый особый отказ $\mathsf{P}^{\#}$. Все, что проверяет тест, сгенерированный по трассе $\mu^{\#}\cdot\langle \mathsf{u}\rangle\cdot\lambda^{\#}$, проверяет тест, сгенерированный по трассе $\mu^{\#}\cdot\langle \mathsf{P}^{\#}, \mathsf{u}\rangle\cdot\lambda^{\#}$. Однако такая генерация тестов не является стандартной, в спецификации остаются **L**-неполные и, следовательно, **L**-неконформные трассы, то есть такая спецификация не будет ∇-пополнением.

Пусть задано множество трасс $\mathbf{N}$. Определим подмножество $\boldsymbol{x}(\mathbf{N})$ множества $\mathbf{N}$ следующим образом.

1. Для каждого ординала α определим множество $\boldsymbol{x}_\alpha(\mathbf{N})$.

1.1. Если $\alpha=0$, то:

0. $\vdash \boldsymbol{x}_0(\mathbf{N})=\varnothing$.

1.2. Если $\alpha>0$ не предельный ординал, то $\boldsymbol{x}_\alpha(\mathbf{N})$ определяется как наименьшее множество, порождаемое следующими правилами вывода:

$\forall\sigma\ \forall\mu\ \forall\lambda\ \forall\kappa$

1. $\sigma\in\boldsymbol{x}_{\alpha-1}(\mathbf{N}) \vdash \sigma\in\boldsymbol{x}_\alpha(\mathbf{N})$,

2. $\mu^{\#}\cdot\kappa\in\mathbf{N}\setminus\boldsymbol{x}_{\alpha-1}(\mathbf{N})$
& $\mu^{\#}$ **L**-*неконвергентна в* $\mathbf{N}\setminus\boldsymbol{x}_{\alpha-1}(\mathbf{N}) \vdash \mu^{\#}\cdot\kappa\in\boldsymbol{x}_\alpha(\mathbf{N})$,

3. $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in\mathbf{N}\setminus\boldsymbol{x}_{\alpha-1}(\mathbf{N})$
& $\mu^{\#}\cdot\lambda^{\#}$ **L**-*неполна после* $\mu^{\#}$ *в* $\mathbf{N}\setminus\boldsymbol{x}_{\alpha-1}(\mathbf{N}) \vdash \mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in\boldsymbol{x}_\alpha(\mathbf{N})$.

Или, учитывая определения **L**-неконвергентной и **L**-неполной трасс, в эквивалентном виде:

$\forall\sigma\ \forall\mu\ \forall\lambda\ \forall\kappa\ \forall P$

1. $\sigma\in\boldsymbol{x}_{\alpha-1}(\mathbf{N}) \vdash \sigma\in\boldsymbol{x}_\alpha(\mathbf{N})$,

2. $\mu^{\#}\cdot\kappa\in\mathbf{N}\setminus\boldsymbol{x}_{\alpha-1}(\mathbf{N})$ & $P\in\mathbf{R}\cup\mathbf{Q}$
& $\mu^{\#}\cdot\langle\cancel{P},\gamma\rangle\notin\mathbf{N}\setminus\boldsymbol{x}_{\alpha-1}(\mathbf{N})$
& $\forall u\in P\cup\{P^{\#}\}\ \mu^{\#}\cdot\langle u\rangle\notin\mathbf{N}\setminus\boldsymbol{x}_{\alpha-1}(\mathbf{N}) \vdash \mu^{\#}\cdot\kappa\in\boldsymbol{x}_\alpha(\mathbf{N})$,

3. $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in\mathbf{N}\setminus\boldsymbol{x}_{\alpha-1}(\mathbf{N})$ & $P\in\mathbf{R}$
& $\mu^{\#}\cdot\langle\cancel{P},\gamma\rangle\notin\mathbf{N}\setminus\boldsymbol{x}_{\alpha-1}(\mathbf{N})$
& $\forall z\in P\ \mu^{\#}\cdot\langle z\rangle\notin\mathbf{N}\setminus\boldsymbol{x}_{\alpha-1}(\mathbf{N})$ & $\boldsymbol{Ip}(\mu)\neq\varnothing$
& $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin\mathbf{N}\setminus\boldsymbol{x}_{\alpha-1}(\mathbf{N}) \vdash \mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in\boldsymbol{x}_\alpha(\mathbf{N})$.

1.3. Если α предельный ординал, то $\boldsymbol{x}_\alpha(\mathbf{N})$ определяется как объединение $\boldsymbol{x}_\alpha(\mathbf{N}) = \cup\{\boldsymbol{x}_\beta(\mathbf{N})\mid\beta<\alpha\}$.

2. Определим $\boldsymbol{x}(\mathbf{N})=\boldsymbol{x}_\alpha(\mathbf{N})$, где α такое, что $\boldsymbol{x}_\alpha(\mathbf{N})=\boldsymbol{x}_{\alpha+1}(\mathbf{N})$.

Покажем, что такое α всегда существует.

Действительно, каждое множество можно вполне упорядочить (занумеровать)[11]. Сделаем это для множества $\mathbf{N}$. Существует такой ординал ϕ, который больше, чем все использованные при таком упорядочивании ординалы (в противном случае множество $\mathbf{N}$ было

[11] Мы опираемся на NBG (Нейман, Бернайс, Гедель) аксиоматическую теорию множеств с праэлементами (от немецкого Urelement) [25].

бы взаимно-однозначно сопоставлено классу всех ординалов, который не является множеством). Будем нумеровать трассы в $\boldsymbol{x}_\alpha(\mathbf{N})$ следующим образом. Поскольку $\boldsymbol{x}_0(\mathbf{N})=\varnothing$ по определению, сначала занумеруем все трассы в $\boldsymbol{x}_1(\mathbf{N})$. По свойству вполне-упорядоченного множества будет существовать самый маленький ординал, который мы не использовали. Начиная с этого ординала будем нумеровать все трассы в $\boldsymbol{x}_2(\mathbf{N})\setminus\boldsymbol{x}_1(\mathbf{N})$. И так далее. Каждый раз у нас будут использоваться ординалы, которые меньше ϕ. Значит $\boldsymbol{x}_\phi(\mathbf{N})=\boldsymbol{x}_{\phi+1}(\mathbf{N})$.

Обозначим $\boldsymbol{\Sigma}^{\boldsymbol{x}} = \boldsymbol{\Sigma}^{\mathbf{01\sim}}\setminus\boldsymbol{x}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$ и $\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_\alpha = \boldsymbol{\Sigma}^{\mathbf{01\sim}}\setminus\boldsymbol{x}_\alpha(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$.

Поскольку $\boldsymbol{x}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})\subseteq\boldsymbol{\Sigma}^{\mathbf{01\sim}}$ и $\boldsymbol{x}_\alpha(\boldsymbol{\Sigma}^{\mathbf{01\sim}})\subseteq\boldsymbol{\Sigma}^{\mathbf{01\sim}}$,

имеем $\boldsymbol{x}(\boldsymbol{\Sigma}^{\mathbf{01\sim}}) = \boldsymbol{\Sigma}^{\mathbf{01\sim}}\setminus\boldsymbol{\Sigma}^{\boldsymbol{x}}$ и $\boldsymbol{x}_\alpha(\boldsymbol{\Sigma}^{\mathbf{01\sim}}) = \boldsymbol{\Sigma}^{\mathbf{01\sim}}\setminus\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_\alpha$.

Также $\boldsymbol{\Sigma}^{\boldsymbol{x}}\cap(\mathbf{L}\cup\mathbf{R}^{\#})^* = \boldsymbol{\Sigma}^{\boldsymbol{x}}\cap\boldsymbol{\Sigma}^{\mathbf{0\sim}} = \boldsymbol{\Sigma}^{\mathbf{0\sim}}\setminus\boldsymbol{x}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$ – подмножество **L**-трасс множества $\boldsymbol{\Sigma}^{\boldsymbol{x}}$.

Лемма 28: Пусть $\langle\gamma\rangle\not\in\boldsymbol{\Sigma}$. Множества $\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_\alpha$ и $\boldsymbol{x}_\alpha(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$ для каждого ординала α обладают следующими свойствами:

1) $\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_\alpha\subseteq\boldsymbol{\Sigma}^{\mathbf{01\sim}}$: $\sigma\in\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_\alpha$ влечет $\sigma\in\boldsymbol{\Sigma}^{\mathbf{01\sim}}$;
2) множество $\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_\alpha$ префикс-замкнуто: $\sigma\cdot\kappa\in\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_\alpha$ влечет $\sigma\in\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_\alpha$;
3) множество $\boldsymbol{x}_\alpha(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$ вместе с каждой трассой содержит ее максимальный **L**-префикс: если $\mu^{\#}\cdot\langle\text{Ⓡ}\rangle\cdot\pi\in\boldsymbol{\Sigma}^{\mathbf{01\sim}}$ и $\mu^{\#}\in\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_\alpha$, то $\mu^{\#}\cdot\langle\text{Ⓡ}\rangle\cdot\pi\in\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_\alpha$.

Доказательство см. на стр.153

Лемма 29: Если $\langle\gamma\rangle\not\in\boldsymbol{\Sigma}$, то все трассы множества $\boldsymbol{x}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$ не **L**-конформны.

Доказательство см. на стр.154

Рассмотрим следующее ***d*-*свойство*** множества трасс $\mathbf{N}\subseteq\boldsymbol{\Sigma}^{\mathbf{01\sim}}$: при переходе $\boldsymbol{\Sigma}^{\mathbf{01\sim}}\to\mathbf{N}$ вместе с каждой удаляемой трассой удаляются и все ее надтрассы, то есть трассы, в ***d***-замыкании которых она находится:

если $\mu^{\#}\in\boldsymbol{d}(\sigma^{\#})$, $\mu^{\#}\in\boldsymbol{\Sigma}^{\mathbf{01\sim}}\setminus\mathbf{N}$ и $\sigma^{\#}\in\boldsymbol{\Sigma}^{\mathbf{01\sim}}$, то $\sigma^{\#}\in\boldsymbol{\Sigma}^{\mathbf{01\sim}}\setminus\mathbf{N}$,

что эквивалентно:

если $\mu^{\#}\in\boldsymbol{d}(\sigma^{\#})$, $\mu^{\#}\in\boldsymbol{\Sigma}^{\mathbf{01\sim}}$ и $\sigma^{\#}\in\mathbf{N}$, то $\mu^{\#}\in\mathbf{N}$.

Лемма 30: Если $\langle\gamma\rangle\not\in\boldsymbol{\Sigma}$, то множества $\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_\alpha$ для каждого ординала α и $\boldsymbol{\Sigma}^{\boldsymbol{x}}$ обладают ***d*-свойством**.

Доказательство см. на стр.157

3.8.3. L-реализация I^{∇}, содержащая все L-конформные трассы

Покажем, что все ~финальные **L**-трассы, оставшиеся после удаления **L**-неконвергентных и **L**-неполных трасс, являются **L**-конформными. Если $\langle\gamma\rangle \notin \mathbf{\Sigma}$ и множество $\mathbf{\Sigma}^x$ пусто, то утверждение очевидно, и конформных реализаций нет. В дальнейшем будем предполагать, что $\mathbf{\Sigma}^x \neq \varnothing$. Мы построим конформную **L**-реализацию $\mathbf{I}^{\nabla}$, содержащую все **L**-трассы из $\mathbf{\Sigma}^x$.

Мы определим множество трасс $\mathbf{I}^{\nabla}$ и докажем, что оно обладает следующими свойствами:

1) содержит только **L**-трассы, то есть его трассы не содержат не-отказов,
2) содержит все **L**-трассы из множества $\mathbf{\Sigma}^x$, то есть, $\mathbf{\Sigma}^x \cap \mathbf{\Sigma}^{\mathbf{0}\sim} \subseteq \mathbf{I}^{\nabla}$,
3) является полной трассовой моделью в алфавите $\mathbf{L}^+$,
4) является безопасно-тестируемой реализацией для ~пополнения: $\mathbf{I}^{\nabla}$ ***safe for*** $\mathbf{\Sigma}^{\sim}$.
5) не содержит ошибочных трасс, определяемых ~пополнением, то есть конформно ~пополнению: $\mathbf{I}^{\nabla}$ ***saco*** $\mathbf{\Sigma}^{\sim}$.

Множество $\mathbf{I}^{\nabla}$ определим как ***Ext***-расширение $\mathbf{R}^{\#}$-модели $\mathbf{I}^{\mathbf{R}}$ в алфавите $\mathbf{L}^+$ до полной трассовой модели: $\mathbf{I}^{\nabla} = \boldsymbol{Ext}(\mathbf{I}^{\mathbf{R}})$.

Сначала неформально рассмотрим, как мы будем строить множество $\mathbf{I}^{\mathbf{R}}$.

Прежде всего заметим следующее. Во множестве $\mathbf{\Sigma}^x$ все трассы конвергентны и полны (формально это следует из доказанной ниже теоремы 20 и аналогичного свойства ∇-финальных трасс леммы 21). Однако, если взять подмножество **L**-трасс множества $\mathbf{\Sigma}^x$, то есть множество трасс $\mathbf{\Sigma}^x \cap \mathbf{\Sigma}^{\mathbf{0}\sim}$, то свойства конвергентности и полноты могут быть нарушены.

В то же время из **L**-конвергентности и **L**-полноты **L**-трасс множества $\mathbf{\Sigma}^x$ следует, что эти трассы конвергентны и полны по безопасным кнопкам. Поясним это. Если $\mu^{\#}\cdot\langle \not\Rightarrow, \gamma\rangle \notin \mathbf{\Sigma}^x$, то трасса $\mu^{\#}$ P-конвергентна и, следовательно, конвергентна в $\mathbf{\Sigma}^x \cap \mathbf{\Sigma}^{\mathbf{0}\sim}$ по кнопке $\mathsf{P}^{\#}$: продолжается каким-нибудь **L**-наблюдением $\mathsf{z} \in \mathsf{P} \cup \{\mathsf{P}^{\#}\}$. Если $\mu^{\#}\cdot\langle \not\Rightarrow, \gamma\rangle \notin \mathbf{\Sigma}^x$, трасса $\mu^{\#}$ заканчивается каким-нибудь отказом и не продолжается действиями $\mathsf{z} \in \mathsf{P}$, то любая имеющаяся **L**-трасса $\mu^{\#}\cdot\lambda^{\#}$ P-полна и, следовательно, выполнено требование полноты в $\mathbf{\Sigma}^x \cap \mathbf{\Sigma}^{\mathbf{0}\sim}$ для кнопки $\mathsf{P}^{\#}$: для любой имеющейся **L**-трассы $\mu^{\#}\cdot\lambda^{\#}$ имеется трасса $\mu^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\cdot\lambda^{\#}$.

Следовательно, при построении множества $\mathbf{I}^{\mathbf{R}}$ нам достаточно обеспечить конвергентность и полноту только по опасным кнопкам, то есть когда $\mu^{\#}\cdot\langle \not\Rightarrow, \gamma\rangle \in \mathbf{\Sigma}^x$. Для этого мы добавим к множеству $\mathbf{\Sigma}^x$ некоторое множество трасс $\mathbf{Y}$ так, чтобы обеспечить конвергентность и полноту в ***d***-замыкании

подмножества **L**-трасс полученного множества, то есть во множестве $\cup\boldsymbol{d}((\boldsymbol{\Sigma}^x\cup\mathbf{Y})\cap(\mathbf{L}\cup\mathbf{R}^{\#})^*)$, которое и будет множеством $\mathbf{I}^{\mathbf{R}}$.

Полнота. Если $\mu^{\#}\cdot\langle\text{Ъ},\gamma\rangle\in\boldsymbol{\Sigma}^x$ и трасса $\mu^{\#}$ заканчивается отказом и не продолжается **L**-действиями $z\in P$, но продолжается каким-нибудь таким действием в $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^x)$, то для нее по кнопке $P^{\#}$ не требуется полнота в $\mathbf{I}^{\mathbf{R}}$. Поэтому для полноты трасс из $\boldsymbol{\Sigma}^x$, заканчивающихся отказом, мы должны проверять отсутствие продолжения трассы действием $z\in P$ во множестве $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^x)$, добавляя в этом случае трассу $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}$ во множество $\mathbf{Y}$ для каждой имеющейся трассы $\mu^{\#}\cdot\lambda^{\#}$. После этого все трассы из $\boldsymbol{\Sigma}^x\cup\mathbf{Y}$ будут полны в $\mathbf{I}^{\mathbf{R}}$.

Конвергентность. Пусть для трассы $\mu^{\#}\in\mathbf{I}^{\mathbf{R}}$, заканчивающейся отказом, выполнено требование полноты во множестве $\mathbf{I}^{\mathbf{R}}$: если трасса $\mu^{\#}$ не продолжается действиями из кнопки P, то для любой трассы $\mu^{\#}\cdot\lambda^{\#}$ имеется трасса $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}$. Тогда выполнено и требование конвергентности трассы $\mu^{\#}$ во множестве $\mathbf{I}^{\mathbf{R}}$: для каждой **R**-кнопки R трасса $\mu^{\#}$ либо продолжается действием из R, либо, в противном случае, по полноте продолжается отказом $R^{\#}$.

Поэтому для обеспечения конвергентности достаточно рассматривать только трассы, не заканчивающиеся никаким отказом. Пусть трасса $\mu^{\#}$ не заканчивается никаким отказом, $\mu^{\#}\cdot\langle\text{Ъ},\gamma\rangle\in\boldsymbol{\Sigma}^x$ и трасса $\mu^{\#}$ продолжается каким-нибудь **L**-наблюдением $u\in P\cup\{P^{\#}\}$ в $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^x)$. Тогда трасса $\mu^{\#}$ будет конвергентна по этой кнопке в $\mathbf{I}^{\mathbf{R}}$. Поэтому для конвергентности мы должны проверять отсутствие продолжения трассы наблюдением $u\in P\cup\{P^{\#}\}$ в множестве $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^x)$. Далее, если трасса $\mu^{\#}$ продолжается каким-нибудь отказом в $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^x)$, то она, очевидно, продолжается каким-нибудь отказом $R^{\#}$ в $\boldsymbol{\Sigma}^x$. Если мы обеспечим в $\mathbf{I}^{\mathbf{R}}$ полноту трассы $\mu^{\#}\cdot\langle R^{\#}\rangle$, то, как сказано выше, мы обеспечим конвергентность трассы $\mu^{\#}\cdot\langle R^{\#}\rangle$ и тем самым мы обеспечим конвергентность трассы $\mu^{\#}$.

Следовательно, для обеспечения конвергентности по кнопке $P^{\#}$ нам достаточно рассматривать трассы $\mu^{\#}\in\boldsymbol{\Sigma}^x$, не заканчивающиеся отказами и в $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^x)$ не продолжающиеся никаким действием $z\in P$ и никакими отказами. В этом случае мы должны продолжить трассу $\mu^{\#}$ каким-нибудь наблюдением $u\in P\cup\{P^{\#}\}$. Для того, чтобы при этом получилась модель и не было добавлено

лишних трасс, мы будем добавлять во множество $\mathbf{\Sigma}^x$ те и только те трассы, которые имеют вид $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}$, где трасса $\mu^{\#}\cdot\lambda^{\#}$ уже была в $\mathbf{\Sigma}^x$.

После добавления указанных трасс мы будем делать ***d***-замыкание и докажем, что полученное множество трасс $\mathbf{I}^{\mathbf{R}}=\cup\boldsymbol{d}((\mathbf{\Sigma}^x\cup\mathbf{Y})\cap(\mathbf{L}\cup\mathbf{R}^{\#})^*)$ является $\mathbf{R}^{\#}$-моделью в алфавите $\mathbf{L}^+$.

Теперь определим множество $\mathbf{I}^{\mathbf{R}}$ формально.

Будем говорить, что отказ $P^{\#}$ *необходим после трассы* $\mu^{\#}$, если выполнены следующие условия:

1) отказ $P^{\#}$ опасен после трассы $\mu^{\#}$:

   $\mu^{\#}\cdot\langle \underline{a}, \gamma\rangle\in\mathbf{\Sigma}^x$,

2) трасса $\mu^{\#}$ не продолжается действиями из P в ***d***-замыкании $\mathbf{\Sigma}^x$:

   $\forall z\in P\ \ \mu^{\#}\cdot\langle z\rangle\notin\cup\boldsymbol{d}(\mathbf{\Sigma}^x)$,

3) трасса $\mu^{\#}$ либо заканчивается какими-нибудь отказом, либо не заканчивается отказом и не продолжается в ***d***-замыкании $\mathbf{\Sigma}^x$ никакими отказами:

   $\boldsymbol{Ip}(\mu)\neq\varnothing\ \vee\ (\boldsymbol{Ip}(\mu)=\varnothing\ \&\ \forall R\in\mathbf{R}\ \ \mu^{\#}\cdot\langle R^{\#}\rangle\notin\cup\boldsymbol{d}(\mathbf{\Sigma}^x))$.

Отказы, необходимые после трассы $\mu^{\#}$, – это как раз те отказы, которые мы будем вставлять после трассы $\mu^{\#}$ перед каждым ее продолжением в $\mathbf{\Sigma}^x$ для обеспечения конвергентности и полноты множества $\mathbf{I}^{\mathbf{R}}$.

Будем говорить, что трасса σ *получается вставкой необходимых отказов в трассу* μ, если трассу σ можно представить в виде $\sigma=\mu_0{}^{\#}\cdot\rho^{\#}{}_0\cdot\mu_1{}^{\#}\cdot\rho^{\#}{}_1\cdot\ldots\cdot\mu_n{}^{\#}\cdot\rho^{\#}{}_n\cdot\lambda$, где $\mu=\mu_0{}^{\#}\cdot\mu_1{}^{\#}\cdot\ldots\cdot\mu_n{}^{\#}\cdot\lambda$, трасса $\rho^{\#}{}_i$ состоит из $\mathbf{R}^{\#}$-отказов, то есть $\rho^{\#}{}_i\in\mathbf{R}^{\#*}$, и каждый отказ $P^{\#}\in\boldsymbol{Im}(\rho^{\#}{}_i)$ необходим после трассы $\mu_0{}^{\#}\cdot\mu_1{}^{\#}\cdot\ldots\cdot\mu_i{}^{\#}$.

Определим операцию $\boldsymbol{i}^{\nabla}$ *вставки необходимых отказов в трассу* μ: $\boldsymbol{i}^{\nabla}(\mu)$ – множество всех трасс, которые получаются вставкой необходимых отказов в трассу μ.

Распространим операцию $\boldsymbol{i}^{\nabla}$ на множество трасс $\mathbf{\Sigma}^x$ обычным образом:

$\boldsymbol{i}^{\nabla}(\mathbf{\Sigma}^x)\ =\ \{\boldsymbol{i}^{\nabla}(\mu)\mid\mu\in\mathbf{\Sigma}^x\}$, результатом является множество множеств трасс.

$\cup\boldsymbol{i}^{\nabla}(\mathbf{\Sigma}^x)$ – это множество всех трасс, получаемых из трасс $\mathbf{\Sigma}^x$ всеми возможными вставками необходимых отказов. Множество $\cup\boldsymbol{i}^{\nabla}(\mathbf{\Sigma}^x)\setminus\mathbf{\Sigma}^x$ как раз и будет множеством $\mathbf{Y}$ добавляемых трасс.

Для построения $\mathbf{R}^{\#}$-модели $\mathbf{I}^{\mathbf{R}}$ сначала выполним операцию $\boldsymbol{i}^{\nabla}$. Затем удалим все трассы, содержащие не-отказы, то есть все не $\mathbf{L}$-трассы. Наконец, выполним ***d***-замыкание полученного множества трасс. Заметим еще раз, что вставки необходимых отказов нужны для обеспечения конвергентности и полноты множества $\mathbf{I}^{\mathbf{R}}$.

Определим операцию $\boldsymbol{l}$ удаления не **L**-трасс из множества трасс **N**:

$\boldsymbol{l}(\mathbf{N}) \triangleq \mathbf{N} \cap (\mathbf{L} \cup \mathbf{R}^{\#})^{*}$.

Определим формально множество трасс $\mathbf{I}^{\mathbf{R}} \triangleq \cup \boldsymbol{d}(\boldsymbol{l}(\cup \boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{x})))$.

Лемма 31: Пусть трасса $\sigma^{\#} \in \mathbf{I}^{\mathbf{R}}$. Тогда найдутся такие трассы $\sigma_1{}^{\#}$ и $\sigma_2{}^{\#}$, что 1) $\sigma_2{}^{\#} \in \boldsymbol{\Sigma}^{x}$, $\sigma_1{}^{\#} \in \boldsymbol{i}^{\nabla}(\sigma_2{}^{\#})$ и $\sigma^{\#} \in \boldsymbol{d}(\sigma_1{}^{\#})$, и 2) если трасса $\sigma^{\#}$ для некоторой **R**-кнопки $\mathsf{P} \in \mathbf{R}$ не продолжается действиями $\mathsf{z} \in \mathsf{P}$ во множестве $\mathbf{I}^{\mathbf{R}}$, то трасса $\sigma_2{}^{\#}$ не продолжается действиями $\mathsf{z} \in \mathsf{P}$ во множестве $\cup \boldsymbol{d}(\boldsymbol{\Sigma}^{x})$.

Доказательство см. на стр.161

Лемма 32: Пусть $\boldsymbol{\Sigma}^{x} \neq \varnothing$. Тогда множество $\mathbf{I}^{\mathbf{R}}$ является $\mathbf{R}^{\#}$-моделью в алфавите $\mathbf{L}^{+}$, и его трассы не содержат дивергенции и разрушения.

Доказательство см. на стр.164

Лемма 33: Пусть $\boldsymbol{\Sigma}^{x} \neq \varnothing$. Тогда множество $\mathbf{I}^{\nabla}$ обладает следующими свойствами:

1) содержит только **L**-трассы, то есть его трассы не содержат не-отказов,
2) содержит все **L**-трассы из множества $\boldsymbol{\Sigma}^{x}$, то есть, $\boldsymbol{\Sigma}^{x} \cap \boldsymbol{\Sigma}^{\mathbf{0}\sim} \subseteq \mathbf{I}^{\nabla}$,
3) является полной трассовой моделью в алфавите $\mathbf{L}^{+}$.

Доказательство см. на стр.172

Лемма 34: Любая трасса $\sigma^{\#} \in \mathbf{I}^{\mathbf{R}} \setminus \boldsymbol{\Sigma}^{x}$ имеет префикс вида $\mu^{\#} \cdot \langle \mathsf{u}^{\#} \rangle$, где трасса $\mu^{\#}$ безопасна в ~пополнении, а наблюдение $\mathsf{u}^{\#}$ опасно в ~пополнении после трассы $\mu^{\#}$.

Доказательство см. на стр.173

Следствие. Из этой леммы непосредственно следует, что трасса $\sigma^{\#} \in \mathbf{I}^{\mathbf{R}} \setminus \boldsymbol{\Sigma}^{x}$ не может быть безопасной трассой ~пополнения. Поскольку по теореме 11 $\boldsymbol{SafeBy}(\mathbf{T}^{\sim}, \mathbf{L}) = \boldsymbol{\Sigma}^{\mathbf{0}\sim}$, а $\boldsymbol{x}(\boldsymbol{\Sigma}^{\mathbf{01}\sim}) \subseteq \boldsymbol{\Sigma}^{\mathbf{01}\sim}$, имеем $\sigma^{\#} \notin \boldsymbol{x}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})$. Следовательно, множество $\mathbf{I}^{\mathbf{R}}$ не содержит трасс, которые были удалены при переходе от $\boldsymbol{\Sigma}^{\mathbf{01}\sim}$ к $\boldsymbol{\Sigma}^{x}$: $\mathbf{I}^{\mathbf{R}} \cap \boldsymbol{x}(\boldsymbol{\Sigma}^{\mathbf{01}\sim}) = \varnothing$.

Лемма 35: Пусть $\boldsymbol{\Sigma}^{x} \neq \varnothing$. Тогда $\mathbf{I}^{\nabla}$ ***safe for*** $\boldsymbol{\Sigma}^{\sim}$.

Доказательство см. на стр.174

Лемма 36: Пусть $\boldsymbol{\Sigma}^{x} \neq \varnothing$. Тогда $\mathbf{I}^{\nabla}$ ***saco*** $\boldsymbol{\Sigma}^{\sim}$.

Доказательство см. на стр.175

Таким образом множество $\mathbf{I}^{\nabla}$ является конформной **L**-реализацией, содержащей все **L**-трассы из множества $\boldsymbol{\Sigma}^{x}$.

Лемма 37: Пусть $\boldsymbol{\Sigma}^{x} \neq \varnothing$. Тогда все трассы множества $\boldsymbol{\Sigma}^{x} \cap \boldsymbol{\Sigma}^{\mathbf{0}\sim}$ **L**-конформны.

Доказательство см. на стр.175

Лемма 38: Множество $\boldsymbol{x}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$ является постфикс-замкнутым подмножеством множества $\boldsymbol{\Sigma}^{\mathbf{01\sim}}$ и вместе с каждой трассой содержит ее максимальный **L**-префикс (максимальный префикс, являющийся **L**-трассой).

Доказательство см. на стр.175

Теорема 20: **О конструктивном определении конформных трасс:**
Пусть $\boldsymbol{\Sigma}^{x}\neq\varnothing$. $\boldsymbol{\Sigma}^{x}\cap\boldsymbol{\Sigma}^{\mathbf{0\sim}}=\boldsymbol{\Sigma}^{\mathbf{0}\nabla}$, $\boldsymbol{\Sigma}^{x}\cap\boldsymbol{\Sigma}^{\mathbf{1\sim}}=\boldsymbol{\Sigma}^{\mathbf{1}\nabla}$ и $\boldsymbol{\Sigma}^{x}=\boldsymbol{\Sigma}^{\mathbf{01}\nabla}$.

Доказательство см. на стр.175

Следующая лемма показывает, что **L**-неконформные трассы можно удалять в несколько этапов. Если из множества трасс **N** удалить по правилам вывода **L**-неконформных трасс не все **L**-неконформные трассы, а только некоторое подмножество X таких трасс, то оставшиеся **L**-неконформные трассы множества **N** также удаляются по правилам вывода **L**-неконформных трасс, применяемых к множеству оставшихся трасс **N**\X. Заметим, что каждое применение правила вывода **L**-неконформных трасс добавляет к удаляемым трассам постфикс-замкнутое множество трасс, которое вместе с каждой трассой содержит ее максимальный **L**-префикс (максимальный префикс, являющийся **L**-трассой).

Лемма 39: Если $\mathbf{N}\subseteq\boldsymbol{\Sigma}^{\mathbf{01\sim}}$, $\mathsf{X}\subseteq\boldsymbol{x}(\mathbf{N})$ и множество X постфикс-замкнутое подмножество множества $\boldsymbol{x}(\mathbf{N})$ и вместе с каждой трассой содержит ее максимальный **L**-префикс (максимальный префикс, являющийся **L**-трассой), то $\boldsymbol{x}(\mathbf{N})=\mathsf{X}\cup\boldsymbol{x}(\mathbf{N}\backslash\mathsf{X})$.

Доказательство см. на стр.176

Для дальнейшего нам понадобится отношение «$\preccurlyeq$» на **L**-трассах при заданном множестве $\mathbf{N}\subseteq\boldsymbol{\Sigma}^{\mathbf{01\sim}}$. Отметим, что **L**-трассы, связанные этим отношением не обязательно принадлежат **N**. Для $\mathsf{P}\in\mathbf{R}$ и произвольных **L**-трасс $\mu^{\#}$, $\lambda^{\#}$, $\sigma^{\#}$ и $\sigma`^{\#}$ определим:

$\mu^{\#}\cdot\lambda^{\#}\prec_{1}\mu^{\#}\cdot\langle\mathsf{P}^{\#}\rangle\cdot\lambda^{\#}$ $\triangleq$ $\mathsf{P}^{\#}$ *особый после* $\mu^{\#}$ *в* **N**,

$\sigma^{\#}\preccurlyeq_{1}\sigma`^{\#}$ $\triangleq$ $\sigma^{\#}=\sigma`^{\#}$ $\vee$ $\sigma^{\#}\prec_{1}\sigma`^{\#}$.

Отношение «$\preccurlyeq$» определяется как транзитивное замыкание отношения «$\preccurlyeq_{1}$».

Лемма 40: Отношение «$\preccurlyeq$» является частичным порядком.

Доказательство см. на стр.183

Лемма 41: Если $\sigma^{\#}\preccurlyeq\sigma`^{\#}$, $\sigma^{\#}\in\mathbf{N}$ и $\sigma`^{\#}\notin\mathbf{N}$, то $\sigma^{\#}\in\boldsymbol{x}(\mathbf{N})$.

Доказательство см. на стр.183

4. Конечные: семантика, спецификация, пополнение

Под конечной семантикой будем понимать семантику с конечным алфавитом. Очевидно, что в конечной семантике число кнопок и каждая кнопка тоже конечны.

Под конечной моделью будем понимать такую модель в конечной семантике, которая может быть задана конечным способом. Трассовая **R**-модель $\mathbf{\Sigma}$ – это множество **R**-трасс некоторой LTS $\mathbf{S}$, то есть $\boldsymbol{T}(\mathbf{R},\mathbf{S})=\mathbf{\Sigma}$. Трассовую **R**-модель $\mathbf{\Sigma}$ будем называть конечной, если существует конечный порождающий ее граф, что по сути означает конечность LTS $\mathbf{S_R}$. LTS и RTS конечны, если у них конечное число состояний и переходов.

По теореме 1 и теореме 2 LTS и RTS алгоритмически преобразуются друг в друга (преобразованиями ***L2R*** и ***R2L***) с сохранением соответствующей им трассовой **R**-модели (т.е. множества **R**-трасс этих моделей), причем при таком преобразовании сохраняется конечность числа состояний.

Что касается числа переходов LTS и RTS, то число переходов LTS $\mathbf{S}$ конечно, если конечно число переходов LTS $\mathbf{S_R}$, но обратное, вообще говоря, не верно. Также из конечности числа переходов RTS $\mathbf{T}$ следует конечность числа переходов LTS $\mathbf{S}=\boldsymbol{R2L}(\mathbf{T})$. Однако, для LTS $\mathbf{S}$ с конечным числом переходов RTS $\mathbf{T}=\boldsymbol{L2R}(\mathbf{S})$ (и любая RTS, определяющая после ***d***-замыкания то же множество **R**-трасс), вообще говоря, может иметь бесконечное число переходов. Это различие связано с тем, что в LTS $\mathbf{S}$ переходы по отказам виртуальные, а в LTS $\mathbf{S_R}$ и RTS – явные. В то же время для конечной семантики конечность числа переходов LTS $\mathbf{S}$, LTS $\mathbf{S_R}$ и RTS $\mathbf{T}=\boldsymbol{L2R}(\mathbf{S})$ эквивалентны.

В этом разделе мы не ставим цель исследовать необходимые и достаточные условия, которым должны удовлетворять исходная спецификационная тройка для того, чтобы существовали конечные ~пополнение и ∇-пополнение и/или они могли строиться алгоритмически. Этот вопрос достаточно сложен, а условия алгоритмизации, кроме того, зависят от способа представления бесконечных семантики и/или спецификации, в частности, от задания тех или иных алгоритмов перечисления и разрешения для семантики и спецификации.

В этом разделе мы покажем, что достаточными условиями являются конечность исходной семантики и исходной спецификации, а также ограничение на отношение безопасности ***safe by***, сформулированное в следующем подразделе. Исходную спецификацию будем считать заданной в виде LTS $\mathbf{S}$. Будем строить ~пополнение в виде RTS $\mathbf{S}^{\sim}$ и ∇-пополнение в виде RTS $\mathbf{S}^{\nabla}$. Конечное пополнение можно за конечное время алгоритмически преобразовать (***R2L***) в конечную LTS.

4.1. Ограничение на *safe by*.

Сейчас мы введем ограничение на отношение ***safe by***, которое потребует совпадения множеств безопасных кнопок после безопасных трасс, заканчивающихся в одном множестве состояний LTS-спецификации. Поскольку для конечной спецификации таких множеств состояний конечное число, это позволит нам строить конечное пополнение.

Используем данное в подразделе 1.3 отношение T-эквивалентности трасс (трассы T-эквивалентны, если в спецификации они имеют одинаковые множества продолжений). Если в LTS-модели трассы заканчиваются в одном множестве состояний, то они T-эквивалентны, но обратное, вообще говоря, не верно. Потребуем, чтобы безопасность кнопок определялась одинаково после T-эквивалентных трасс. В трассовой теории это будет означать, по сути, что безопасность кнопок определяется для префикс-замкнутого множества трасс $\mathbf{X}$, которым является множество трасс, продолжающих некоторую безопасную трассу μ.

Обычные отношения безопасности в реализации и спецификации определяют безопасность кнопки в заданном множестве трасс после некоторой его заданной трассы, то есть имеют вид:

«кнопка» ***safe in/by*** *«множество трасс»* ***after*** *«трасса»*.

Отношения безопасности кнопки для префикс-замкнутого множества $\mathbf{X}$ трасс, продолжающих заданную трассу в заданном множестве трасс, будут иметь вид

«кнопка» ***safe in/by*** *«префикс-замкнутое множество продолжений трассы во множестве трасс»*.

Безопасность в трассовой реализации $\mathbf{I}$.

Определим: $\forall P \in \mathbf{R} \cup \mathbf{Q} \quad \forall \mathbf{X}$

$P\ \boldsymbol{safe}_{\gamma\Delta}\ \mathbf{X} \quad \triangleq \quad \langle\Delta\rangle \notin \mathbf{X} \ \&\ \forall u \in P \ \ \langle u,\gamma\rangle \notin \mathbf{X},$

$P\ \boldsymbol{safe\ in}\ \mathbf{X} \quad \triangleq \quad P\ \boldsymbol{safe}_{\gamma\Delta}\ \mathbf{X} \ \&\ (P \in \mathbf{Q} \ \Rightarrow\ \langle P\rangle \notin \mathbf{X}).$

Очевидно, что: $P\ \boldsymbol{safe\ in}\ \mathbf{I}\ \boldsymbol{after}\ \sigma \ =\ P\ \boldsymbol{safe\ in}\ \mathbf{X}$, где $\mathbf{X}=\{\lambda \mid \sigma\cdot\lambda \in \mathbf{I}\}$.

Безопасность в трассовой спецификации $\boldsymbol{\Sigma}$.

Определим: $\forall R \in \mathbf{R} \quad \forall z \in \mathbf{L} \quad \forall Q \in \mathbf{Q} \quad \forall \mathbf{X}$

1) $R\ \boldsymbol{safe\ by}\ \mathbf{X} \ \Leftrightarrow\ R\ \boldsymbol{safe}_{\gamma\Delta}\ \mathbf{X},$

2) $\exists U \in \mathbf{Q} \ \ U\ \boldsymbol{safe}_{\gamma\Delta}\ \mathbf{X} \ \&\ z \in U \ \&\ \langle z\rangle \in \mathbf{X} \ \Rightarrow\ \exists P \in \mathbf{R} \cup \mathbf{Q} \ \ z \in P \ \&\ P\ \boldsymbol{safe\ by}\ \mathbf{X},$

3) $Q\ \boldsymbol{safe\ by}\ \mathbf{X} \ \Rightarrow\ Q\ \boldsymbol{safe}_{\gamma\Delta}\ \mathbf{X} \ \&\ \exists v \in Q \ \ \langle v\rangle \in \mathbf{X}.$

Для ограниченного отношения безопасности в спецификации потребуем:

$P\ \boldsymbol{safe\ by}\ \boldsymbol{\Sigma}\ \boldsymbol{after}\ \sigma \ =\ P\ \boldsymbol{safe\ by}\ \mathbf{X}$, где $\mathbf{X}=\{\lambda \mid \sigma\cdot\lambda \in \boldsymbol{\Sigma}\}$.

В LTS-теории мы будем использовать более *слабое* отношение безопасности, основанное не на множестве продолжений трассы, а на множестве состояний после трассы.

Безопасность в LTS-реализации **I**.

Определим: $\forall P \in \mathbf{R} \cup \mathbf{Q}\ \ \forall a \subseteq V_{\mathbf{I}}$

P ***safe***$_{\gamma\Delta}$ $a \triangleq \forall i \in a\ i{\downarrow}\ \&\ \forall z \in P\ i = \langle z,\gamma \rangle \not\Rightarrow$,

P ***safe in*** $a \triangleq P$ ***safe***$_{\gamma\Delta}$ $a\ \&\ (P \in \mathbf{Q} \Rightarrow \forall i \in a\ i = \langle P \rangle \not\Rightarrow)$.

Очевидно, что: P ***safe in*** $F(\mathbf{I})$ ***after*** $\sigma = P$ ***safe in*** $(\mathbf{I}$ ***after*** $\sigma)$.

По определению: P ***safe***$_{\gamma\Delta}$ $\varnothing$ и P ***safe in*** $\varnothing$.

Безопасность в LTS-спецификации **S**.

Определим: $\forall R \in \mathbf{R}\ \ \forall z \in \mathbf{L}\ \ \forall Q \in \mathbf{Q}\ \ \forall a \subseteq V_{\mathbf{S}}$

1) R ***safe by*** $a \Leftrightarrow R$ ***safe***$_{\gamma\Delta}$ a,

2) $\exists U \in \mathbf{Q}\ \ U$ ***safe***$_{\gamma\Delta}$ $a\ \&\ z \in U\ \&\ \exists s \in a\ s = \langle z \rangle \Rightarrow$

$\Rightarrow \exists P \in \mathbf{R} \cup \mathbf{Q}\ \ z \in P\ \&\ P$ ***safe by*** a,

3) Q ***safe by*** $a \Rightarrow Q$ ***safe***$_{\gamma\Delta}$ $a\ \&\ \exists v \in Q\ \exists s \in a\ s = \langle v \rangle \Rightarrow$.

Для ограниченного отношения безопасности в спецификации потребуем:

P ***safe by*** $F(\mathbf{S})$ ***after*** $\sigma = P$ ***safe by*** $(\mathbf{S}$ ***after*** $\sigma)$.

По определению для $R \in \mathbf{R}$ всегда R ***safe by*** $\varnothing$, а для $Q \in \mathbf{Q}$ Q ~~***safe by***~~ $\varnothing$.

Как обычно, **R**-отказ R безопасен во множестве состояний, если в этом множестве безопасна кнопка R. Действие z безопасно во множестве состояний, если оно разрешается некоторой кнопкой, безопасной в этом множестве состояний:

z ***safe by*** $a \triangleq \exists P \in \mathbf{R} \cup \mathbf{Q}\ \ z \in P\ \&\ P$ ***safe by*** a.

Напомним, что отношение ***after*** распространяется на множество состояний $a \subseteq V_{\mathbf{S}}$ следующим образом: a ***after*** $\sigma = \{s$ ***after*** $\sigma \mid s \in a\}$, результатом является множество множеств состояний.

По определению, $\varnothing$ ***after*** $\sigma = \varnothing$.

Заметим, что для конечной семантики **R**/**Q** и конечной спецификационной модели **S** ограниченное отношение ***safe by*** может быть задано конечным способом: для каждого подмножества состояний (таких подмножеств конечное число, а для определения ***safe by*** достаточно подмножеств в концах трасс) указываются безопасные кнопки как подмножество (конечного) числа кнопок.

Спецификационную тройку $\mathbf{T=(R/Q,\Sigma,}$***safe by***$\mathbf{)}$ будем называть *конечной*, если конечна семантика $\mathbf{R/Q}$, полная трассовая модель $\mathbf{\Sigma}$ задана конечной LTS или RTS, а отношение ***safe by*** ограниченное.

4.2. Трассовое ~пополнение LTS-спецификации

Перепишем определение трассового ~пополнения для случая, когда исходная спецификация задана в виде LTS $\mathbf{S}$ и $\boldsymbol{F}(\mathbf{S})=\mathbf{\Sigma}$. Это определение базируется на определении ~финальных трасс, которое, в свою очередь, базируется на определении отношений ~безопасности и ~конформности наблюдений после трасс. Эти отношения для трассы σ зависят от множества ее $\boldsymbol{di}^{\sim}$-подтрасс, точнее, от того, какие кнопки и наблюдения безопасны после этих подтрасс и какими наблюдениями эти подтрассы продолжаются в исходной спецификации. Для ограниченного отношения ***safe by*** это однозначно определяется множеством состояний после подтрассы.

Теперь вместо каждой трассы μ исходной спецификации мы можем использовать множество $\mathbf{S}$ ***after*** μ состояний в конце этой трассы, которое определяет как безопасность кнопок после трассы, так и продолжения этой трассы в исходной спецификации. Вместо множества трасс $\boldsymbol{di}^{\sim}(\sigma)\cap\boldsymbol{SafeBy}(\boldsymbol{F}(\mathbf{S}))$ будем использовать семейство множеств состояний, которое обозначим: $A_\sigma=\{\mathbf{S}\ \boldsymbol{after}\ \mu \mid \mu\in\boldsymbol{di}^{\sim}(\sigma)\cap\boldsymbol{SafeBy}(\boldsymbol{F}(\mathbf{S}))\}$.

Кроме этого, отношение ~конформности после трассы σ зависит от отказов в конце трассы, точнее, от множества действий в этих отказах. Обозначим $r_\sigma=\{\cup\boldsymbol{Ip}(\sigma) \mid \boldsymbol{Ip}(\sigma)\neq\varnothing\}$. Заметим, что r_σ – это либо пустое множество, либо синглетон, т.е. множество состоящее из одного элемента, этим элементом является множество действий. Также заметим, что $r_\sigma=\{\varnothing\}$, если постфикс отказов трассы σ не пуст, но содержит только пустые отказы, и $r_\sigma=\varnothing$, если постфикс отказов трассы σ пуст. Итак, при построении пополнения вместо трассы σ будем использовать пару (A_σ,r_σ). Напишем определения ~безопасности и ~конформности после такой пары.

<u>~безопасность</u>.

- для $Q\in\mathbf{Q}$: Q ***safe~by*** $A_\sigma \triangleq \exists a\in A_\sigma\ Q$ ***safe by*** a;
- для $\varnothing\in\mathbf{R}$: $\varnothing$ ***safe~by*** $A_\sigma \triangleq \exists a\in A_\sigma\ \varnothing$ ***safe by*** a;
- для $z\in\mathbf{L}$: z ***safe~by*** $A_\sigma \triangleq \exists a\in A_\sigma\ z$ ***safe by*** a;
- для $R\in\mathbf{R}\backslash\{\varnothing\}$: R ***safe~by*** $A_\sigma \triangleq \forall z\in R\ z$ ***safe~by*** A_σ.

<u>Замечание 15.</u> Учитывая лемму 12, $\forall u\in\mathbf{L}\cup\mathbf{R}$

u ***safe~by*** $A_\sigma \Leftrightarrow \exists P\in\mathbf{R}\cup\mathbf{Q}\ (u\in P \vee u=P\ \&\ P\in\mathbf{R})\ \&\ P$ ***safe~by*** A_σ.

<u>~конформность</u>.

- для $z\in\mathbf{L}$: $z \sim\!\!\textit{conf}\ (A_\sigma,r_\sigma) \triangleq z\ \textit{safe}\sim\!\!\textit{by}\ A_\sigma$
  $\&\ z\notin\cup r_\sigma\ \&\ \forall a\in A_\sigma\ (z\ \textit{safe}\sim\!\!\textit{by}\ a \Rightarrow \cup(a\ \textit{after}\ \langle z\rangle)\neq\varnothing)$;
- для $R\in\mathbf{R}\setminus\{\varnothing\}$: $R \sim\!\!\textit{conf}\ (A_\sigma,r_\sigma) \triangleq R\ \textit{safe}\sim\!\!\textit{by}\ A_\sigma$
  $\&\ \forall Q\in\mathbf{Q}\ \forall a\in A_\sigma\ (Q\subseteq\cup r_\sigma\cup R \Rightarrow Q\ \textit{safe by}\ a)$
  $\&\ \forall P\in\mathbf{R}\ \forall a\in A_\sigma\ (P\subseteq\cup r_\sigma\cup R\ \&\ P\ \textit{safe by}\ a \Rightarrow \cup(a\ \textit{after}\ \langle P\rangle)\neq\varnothing)$;
- для $\varnothing\in\mathbf{R}$: $\varnothing \sim\!\!\textit{conf}\ (A_\sigma,r_\sigma) \triangleq \varnothing\ \textit{safe}\sim\!\!\textit{by}\ A_\sigma$.

Теперь определение ~финальных трасс выглядит так:

$\forall\sigma\ \forall u\in\mathbf{R}\cup\mathbf{L}\ \forall P\in\mathbf{R}\cup\mathbf{Q}$

1) $s_0=\langle\gamma\rangle\Rightarrow \vdash \epsilon\in\mathbf{\Sigma^{1\sim}}\ \&\ \langle\gamma\rangle\in\mathbf{\Sigma^{1\sim}}$,
2) $s_0=\langle\gamma\rangle\not\Rightarrow \vdash \epsilon\in\mathbf{\Sigma^{0\sim}}$,
3) $\sigma^{\#}\in\mathbf{\Sigma^{0\sim}}\ \&\ u \sim\!\!\textit{conf}\ (A_\sigma,r_\sigma) \vdash \sigma^{\#}\cdot\langle u^{\#}\rangle\in\mathbf{\Sigma^{0\sim}}$,
4) $\sigma^{\#}\in\mathbf{\Sigma^{0\sim}}\ \&\ P\ \textit{safe}\sim\!\!\textit{by}\ A_\sigma \vdash \sigma^{\#}\cdot\langle\text{Ꝑ}\rangle\in\mathbf{\Sigma^{1\sim}}\ \&\ \sigma^{\#}\cdot\langle\text{Ꝑ},\gamma\rangle\in\mathbf{\Sigma^{1\sim}}$,
5) $\sigma^{\#}\in\mathbf{\Sigma^{0\sim}}\ \&\ P\ \textit{safe}\sim\!\!\textit{by}\ A_\sigma\ \&\ (r_\sigma=\varnothing\vee P\not\subseteq\cup r_\sigma) \vdash \sigma^{\#}\cdot\langle\text{Ꝑ}\rangle\in\mathbf{\Sigma^{1\sim}}\ \&\ \sigma^{\#}\cdot\langle\text{Ꝑ},\Delta\rangle\in\mathbf{\Sigma^{1\sim}}$.

4.3. ~финальная RTS (~пополнение в виде RTS)

По-прежнему будем считать, что исходная спецификационная модель задана в виде LTS $\mathbf{S}$, исходная спецификационная тройка $\mathbf{T=(R/Q,\Sigma,}\textit{safe by}\mathbf{)}$, где $\mathbf{\Sigma=}\boldsymbol{F}\mathbf{(S)}$.

RTS $\mathbf{S^{\sim}}$ будем называть ~пополнением, если множество ее простых трасс совпадает с множеством ~финальных трасс $\boldsymbol{T}\mathbf{(S^{\sim})=\Sigma^{01\sim}}$. Тогда $\cup\boldsymbol{d}\mathbf{(}\boldsymbol{T}\mathbf{(S^{\sim}))=\cup}\boldsymbol{d}\mathbf{(\Sigma^{01\sim})}$ и при любом расширении до полной трассовой модели будет получаться трассовое ~пополнение $\mathbf{\Sigma^{\sim}}$. В результате будет построена спецификационная тройка $\mathbf{T^{\sim}=(R^{\#}/Q^{\#},\Sigma^{\sim},}\textit{safe}_{\gamma\Delta}\mathbf{)}$ ~пополнения.

Для построения RTS $\mathbf{S^{\sim}}$ заметим, что в определении ~финальных трасс в предыдущем подразделе ~финальные продолжения ~финальной $\mathbf{L}$-трассы $\sigma^{\#}$ зависят только от пары (A_σ,r_σ). Нам нужно также выяснить, как для ~конформного наблюдения u связаны пары (A_σ,r_σ) и $(A_{\sigma\cdot\langle u\rangle},r_{\sigma\cdot\langle u\rangle})$.

Для произвольных $A\subseteq\mathcal{P}(V_S)$, $z\in\mathbf{L}$ и $R\in\mathbf{R}$ обозначим:

(A,r) ***safter*** $z \triangleq (\{\cup(a \textit{ after } \langle z\rangle) \mid a\in A \ \&\ z \textit{ safe by } a\}, \varnothing)$,

(A,r) ***safter*** $R \triangleq (\{\cup(a \textit{ after } \rho) \mid a\in A \ \&\ \forall i=1..|\rho|$

$\rho(i)\subseteq\cup r\cup R \ \&\ \rho(i) \textit{ safe by } \cup(a \textit{ after } \rho[1..i-1])\}, \{\cup r\cup R\})$.

Если z действие, и z ~~***safe by***~~ (A,r), то (A,r) ***safter*** $z = (\varnothing,\varnothing)$.

Если z действие, и z ***safe by*** (A,r), но z ~~***conf***~~ (A,r),

то (A,r) ***safter*** $z = (A`,\varnothing)$, где $\varnothing\in A`$.

Если R отказ, и R ~~***safe by***~~ (A,r), то (A,r) ***safter*** $R = (\varnothing,\{\cup r\cup R\})$.

Если R отказ, и R ***safe by*** (A,r), но R ~~***conf***~~ (A,r),

то (A,r) ***safter*** $R = (A`,\{\cup r\cup R\})$, где $\varnothing\in A`$.

Лемма 42: Для произвольных **L**-трассы $\sigma^{\#}$ и наблюдения $u\in\mathbf{L}\cup\mathbf{R}$ имеет место: $(A_{\sigma\cdot\langle u\rangle},r_{\sigma\cdot\langle u\rangle}) = (A_\sigma,r_\sigma)$ ***safter*** u.

Доказательство см. на стр.183

Лемма 43: Условие $R\subseteq\cup r_\sigma$ влечет (A_σ,r_σ) ***safter*** $R = (A_\sigma,r_\sigma)$.

Доказательство см. на стр.184

Мы также хотим при построении RTS $\mathbf{S}^{\sim}$ различить **L**-актуальные и не **L**-актуальные **L**-наблюдения среди безопасных, но не **L**-конформных, **L**-наблюдений после трассы. Следующая лемма аналогична теореме 12 о **L**-актуальности для ~финальных трасс, но только условия **L**-актуальности переформулированы в терминах A_σ и r_σ.

Лемма 44: Наблюдение $u^{\#}\in\mathbf{L}\cup\mathbf{R}^{\#}$, безопасное (по $\textit{safe}_{\gamma\Delta}$) после трассы $\sigma^{\#}\in\mathbf{\Sigma}^{\mathbf{0}\sim}$, **L**-актуально тогда и только тогда, когда либо 1) $u\in\mathbf{L}$ и $u\notin\cup r_\sigma$, либо 2) $u\in\mathbf{R}$ и каждая кнопка $Q\in\mathbf{Q}$ такая, что $Q\subseteq\cup r_{\sigma\cdot\langle u\rangle}$, опасна в исходной спецификации $\mathbf{S}$ в каждом множестве состояний $a\in A_{\sigma\cdot\langle u\rangle}$.

Доказательство см. на стр.184

Согласно этой лемме для проверки **L**-актуальности действия, безопасного после трассы $\sigma^{\#}$, достаточно множества r_σ, а для проверки **L**-актуальности $\mathbf{R}^{\#}$-отказа $R^{\#}$, безопасного после трассы $\sigma^{\#}$, достаточно пары $(A_{\sigma\cdot\langle R\rangle},r_{\sigma\cdot\langle R\rangle})$.

Согласно лемме 42 $(A_{\sigma\cdot\langle R\rangle},r_{\sigma\cdot\langle R\rangle}) = (A_\sigma,r_\sigma)$ ***safter*** R.

Обозначим для $R\in\mathbf{R}$:

R ***act*** $(A,r) \triangleq \forall Q\in\mathbf{Q}\ (Q\subseteq\cup r` \ \&\ a\in A` \Rightarrow Q$ ~~***safe by***~~ $a)$,

где $(A`,r`)=(A,r)$ ***safter*** R.

Обозначим: $\mathcal{R}(\mathbf{L}) \triangleq \{\varnothing\}\cup\{\{x\}\mid x\subseteq\mathbf{L}\}$. Элементы этого множества – это пустое множество и все синглетоны $\{x\}$, где x пробегает все подмножества (в том числе пустое) алфавита действий **L**.

Определим *~финальную* LTS $\mathbf{S}^{\sim}=\mathrm{LTS}(V_{\mathbf{S}^{\sim}},\mathbf{L}^{+}\cup\mathbf{R}^{\#}\cup\{\Delta\},E_{\mathbf{S}^{\sim}},s^{\sim}_{0})$, где множество $V_{\mathbf{S}^{\sim}}$ содержит выделенные состояния γ, Δ, $\Delta`$, ϖ и все возможные пары (A,r), где $A\subseteq\mathcal{P}(V_{\mathbf{S}})$ и $r\in\mathcal{R}(\mathbf{L})$, начальное состояние $s^{\sim}_{0}=(\{\{\mathbf{S}\ \textit{after}\ \epsilon\}\},\varnothing)$, если $s_0=\langle\gamma\rangle\not\Rightarrow$, или $s^{\sim}_{0}=\gamma$, если $s_0=\langle\gamma\rangle\Rightarrow$, а переходы определяются правилами вывода, аналогичными правилам вывода для ~финальных трасс:

$\forall A\subseteq\mathcal{P}(V_{\mathbf{S}})\ \ \forall r\in\mathcal{R}(\mathbf{L})\ \ \forall u\in\mathbf{L}\cup\mathbf{R}\ \ \forall P\in\mathbf{R}\cup\mathbf{Q}\ \ \forall Q\in\mathbf{Q}\ \ \forall R\in\mathbf{R}$

1R) $s_0=\langle\gamma\rangle\Rightarrow$ $\quad\vdash \gamma\text{—}\gamma\to\varpi,$

2R) u ***~conf*** (A,r) $\quad\vdash (A,r)\text{—}u^{\#}\to(A,r)$ ***safter*** $u,$

3R) P ***~~safe~by~~*** A $\quad\vdash (A,r)\text{—}\not{P}\to\gamma\text{—}\gamma\to\varpi,$

4R) Q ***safe~by*** A $\quad\vdash (A,r)\text{—}\not{Q}\to\Delta\text{—}\Delta\to\varpi,$

5R) R ***safe~by*** A & $(r=\varnothing\vee R\not\subseteq\cup r)$ & R ***act*** (A,r) $\vdash (A,r)\text{—}\not{R}\to\Delta\text{—}\Delta\to\varpi,$

6R) R ***safe~by*** A & $(r=\varnothing\vee R\not\subseteq\cup r)$ & R ***~~act~~*** (A,r) $\vdash (A,r)\text{—}\not{R}\to\Delta`\text{—}\Delta\to\varpi.$

Достижимое состояние вида (A,r) будем называть **L**-состоянием.

Замечание 16. По построению для ~финальной LTS выполнено следующее свойство, которое будем называть $\Delta\gamma$-свойством: $\forall a,b\in V_{\mathbf{S}}\ \forall P\in\mathbf{R}\cup\mathbf{Q}\ \forall u$

1) переходы по не-отказам ведут только в состояния γ, Δ, $\Delta`$, и в эти состояния ведут только переходы по не-отказам:

$(a\text{—}\not{P}\to b\Rightarrow b\in\{\gamma,\Delta,\Delta`\})\ \&\ (a\text{—}u\to b\ \&\ b\in\{\gamma,\Delta,\Delta`\}\Rightarrow\exists Q\in\mathbf{R}\cup\mathbf{Q}\ u=\not{Q});$

2) из состояния γ ведет только переход по γ, и переход по γ ведет только из состояния γ в состояние ϖ:

$(\gamma\text{—}u\to\ \Rightarrow\ u=\gamma)\ \&\ (a\text{—}\gamma\to b\ \Rightarrow\ a=\gamma\ \&\ b=\varpi);$

3) из состояний Δ, $\Delta`$ ведут только переходы по $\Delta$, и переход по $\Delta$ ведет только из состояний $\Delta$, $\Delta`$ в состояние ϖ:

$(a\in\{\Delta,\Delta`\}\ \&\ a\text{—}u\to\ \Rightarrow\ u=\Delta)\ \&\ (a\text{—}\Delta\to b\ \Rightarrow\ a\in\{\Delta,\Delta`\}\ \&\ b=\varpi);$

4) в состояние ϖ ведут только переходы по γ и Δ, и состояние ϖ терминально:

$(a\text{—}u\to\varpi\ \Rightarrow\ u\in\{\gamma,\Delta\})\ \&\ \varpi\text{—}u\not\to.$

По построению LTS $\mathbf{S}^{\sim}$ и лемме 42 для любой трассы $\sigma^{\#}$, заканчивающейся в **L**-состоянии (A,r), имеем $A=A_{\sigma}=\{\mathbf{S}\ \textit{after}\ \mu\,|\,\mu\in\textit{di}^{\sim}(\sigma)\cap\textit{SafeBy}(F(\mathbf{S}))\}$

и $r=r_\sigma=\{\cup \boldsymbol{Ip}(\sigma)\,|\,\boldsymbol{Ip}(\sigma)\neq\varnothing\}$. В частности, если $r\neq\varnothing$, то трасса $\sigma^{\#}$ заканчивается отказом.

Теорема 21: **О ~финальной RTS.** 1) Если пустая трасса безопасна в исходной LTS-спецификации **S**, то каждая простая **L**-трасса $\sigma^{\#}$ LTS $\mathbf{S}^{\sim}$ заканчивается в **L**-состоянии (A_σ,r_σ); 2) множество простых трасс LTS $\mathbf{S}^{\sim}$ является множеством ~финальных трасс $\boldsymbol{T}(\mathbf{S}^{\sim})=\boldsymbol{\Sigma}^{\mathbf{01}\sim}$, где $\boldsymbol{\Sigma}=\boldsymbol{F}(\mathbf{S})$; 3) ~финальная LTS $\mathbf{S}^{\sim}$ является RTS.

Доказательство см. на стр.186

Замечание 17. Из теоремы 21 и правил вывода ~финальной RTS следует, что 1) множество простых трасс RTS $\mathbf{S}^{\sim}$, заканчивающихся в **L**-состояниях, совпадает с множеством $\boldsymbol{\Sigma}^{\mathbf{0}\sim}$, а 2) множество простых трасс RTS $\mathbf{S}^{\sim}$, заканчивающихся в остальных состояниях, то есть состояниях γ, Δ, $\Delta`$ и ϖ, совпадает с множеством $\boldsymbol{\Sigma}^{\mathbf{1}\sim}$.

Тем самым, **L**-состояния ~финальной RTS – это все состояния, достижимые по безопасным (в $\mathbf{T}^{\sim}$) простым **L**-трассам, и только они.

Заметим, что простая **L**-трасса никогда не может заканчиваться в состояниях Δ и $\Delta`$, и может заканчиваться в состояниях γ и ϖ только в том случае, когда пустая трасса опасна в исходной LTS-спецификации **S**, то есть $s_0=\langle\gamma\rangle\Rightarrow$. В последнем случае имеются только две ~финальные трассы ϵ и $\langle\gamma\rangle$, которые являются **L**-трассами, но опасны.

Итак, множество простых трасс ~финальной RTS совпадает с множеством ~финальных трасс. Переформулируем в терминах RTS утверждения о безопасности кнопок (теорема 10) и о безопасных **L**-трассах (теорема 11).

Теорема 22: **~финальная RTS: Безопасность кнопок.** В ~финальной RTS $\mathbf{S}^{\sim}$ кнопка $P^{\#}$ безопасна по отношению $\boldsymbol{safe}_{\gamma\Delta}$ после простой трассы, заканчивающейся в **L**-состоянии s, тогда и только тогда, когда $s \not\xrightarrow{P}\gamma$.

Доказательство см. на стр.192

Теорема 23: **~финальная RTS: Безопасные L-трассы.** **L**-трасса из $\boldsymbol{d}$-замыкания множества простых трасс ~финальной RTS $\mathbf{S}^{\sim}$ безопасна по отношению $\boldsymbol{safe}_{\gamma\Delta}$ тогда и только тогда, когда это простая трасса, заканчивающаяся в **L**-состоянии.

Доказательство см. на стр.192

Утверждение о **L**-актуальных наблюдениях и трассах (теорема 12) переформулируем с учетом введенного дополнительного состояния $\Delta`$.

В ~финальной RTS для состояния s обозначим через $\boldsymbol{r}(s)$ пустое множество, если в состоянии s не определены переходы-петли по отказам, или одноэлементное множество, содержащее объединение отказов, по которым в состоянии s определены переходы-петли:

$\boldsymbol{r}(s) \triangleq \{\cup\{R\in\mathbf{R} \mid s\text{—}R^{\#}\!\!\rightarrow s\} \mid \exists R\in\mathbf{R}\ s\text{—}R^{\#}\!\!\rightarrow s\}$.

Лемма 45: Для **L**-состояния (A,r) ~финальной RTS имеет место $\boldsymbol{r}((A,r))=r$.

Доказательство см. на стр.193

Теорема 24: **~финальная RTS: Актуальные наблюдения и L-трассы.**

1) Все простые **L**-трассы RTS $\mathbf{S}^{\sim}$ **L**-актуальны.
2) Наблюдение $u^{\#}\in\mathbf{L}\cup\mathbf{R}^{\#}$, безопасное по $\boldsymbol{safe}_{\gamma\Delta}$ в **L**-состоянии s, то есть после любой трассы, заканчивающейся в этом состоянии, **L**-актуально тогда и только тогда, когда либо 1) $u\in\mathbf{L}$ & $u\notin\cup\boldsymbol{r}(s)$, либо 2) $u\in\mathbf{R}$ & $s\text{—}\underline{u}\!\!\rightarrow\Delta`$.

Доказательство см. на стр.194

Заметим, что для $u\in\mathbf{R}$ из $u^{\#}\ \boldsymbol{safe}_{\gamma\Delta}\ s$ следует $s\text{—}\underline{u}\!\!\rightarrow\gamma$. Поэтому условие $s\text{—}\underline{u}\!\!\rightarrow\Delta`$ эквивалентно условию $s\text{—}\underline{u}\!\!\rightarrow \vee\ s\text{—}\underline{u}\!\!\rightarrow\Delta$.

Теорема 25: **О конечности ~финальной RTS.** Для конечной спецификационной тройки $\mathbf{T}=(\mathbf{R}/\mathbf{Q},\boldsymbol{F}(\mathbf{S}),\boldsymbol{safe\ by})$ ~финальная RTS $\mathbf{S}^{\sim}$ конечна, и ее можно алгоритмически построить за конечное время. Спецификационная тройка ~пополнения $\mathbf{T}^{\sim}=(\mathbf{R}^{\#}/\mathbf{Q}^{\#},\mathbf{\Sigma}^{\sim},\boldsymbol{safe}_{\gamma\Delta})$, где $\mathbf{\Sigma}=\boldsymbol{F}(\mathbf{S})$, конечна.

Доказательство см. на стр.195

Для дальнейшего нам понадобится еще ряд определений и утверждений о ~финальной RTS.

Лемма 46: В $\mathbf{S}^{\sim}$ для каждого **L**-состояния (A,r) имеет место:

$A=\{\cup(x\ \boldsymbol{after}\ \rho) \mid x\in A\ \&\ \forall i=1..|\rho|$
$(r\neq\varnothing\ \&\ \rho(i)\subseteq\cup r\ \&\ \rho(i)\ \boldsymbol{safe\ by}\ \cup(x\ \boldsymbol{after}\ \rho[1..i-1]))\}$.

Доказательство см. на стр.196

Замечание 18. Из этой леммы непосредственно следует, что в $\mathbf{S}^{\sim}$ для каждого **L**-состояния (A,r) каждое множество состояний из A имеет вид $\cup(x\ \boldsymbol{after}\ \rho)$. Поскольку $(\cup(x\ \boldsymbol{after}\ \rho))\ \boldsymbol{after}\ \epsilon = \cup(x\ \boldsymbol{after}\ \rho)$, каждое множество состояний из A замкнуто по τ-переходам, то есть $A=\{\cup(x\ \boldsymbol{after}\ \epsilon) \mid x\in A\}$.

Лемма 47: В $\mathbf{S}^{\sim}$ для каждого **L**-состояния a и каждой кнопки $P\in\mathbf{R}$ имеет место $a\text{—}\underline{P}\!\!\rightarrow \Leftrightarrow a\text{—}P^{\#}\!\!\rightarrow a$.

Доказательство см. на стр.197

Определим отношение:

$(A,r)\le(A`,r`) \triangleq A\subseteq A` \;\&\; (r\neq\varnothing \Rightarrow r`\neq\varnothing) \;\&\; \cup r\subseteq\cup r`,$

где A, $A`$, $r$ и $r`$ семейства множеств.

В частности, такое отношение определено на множестве **L**-состояний ~финальной RTS.

Лемма 48: Отношение «≤» является частичным порядком.

Доказательство см. на стр.197

Лемма 49: В $\mathbf{S}^{\sim}$ для любых **L**-состояний a и b, и любой кнопки $P\in\mathbf{R}\cup\mathbf{Q}$ имеет место $a\text{—}\not{P}\!\!\rightarrow \;\&\; a\le b \Rightarrow b\text{—}\not{P}\!\!\rightarrow$.

Доказательство см. на стр.197

Лемма 50: В $\mathbf{S}^{\sim}$ для любых **L**-состояний a и b, и любой кнопки $P\in\mathbf{R}\cup\mathbf{Q}$ имеет место $b\text{—}\not{P}\!\!\rightarrow\gamma \;\&\; a\le b \Rightarrow a\text{—}\not{P}\!\!\rightarrow\gamma$.

Доказательство см. на стр.198

Лемма 51: В $\mathbf{S}^{\sim}$ для любых **L**-состояний a и b, и любой трассы отказов $\rho\in\mathbf{R}^{*}$ имеет место $a=\rho^{\#}\Rightarrow b \Rightarrow a\le b$.

Доказательство см. на стр.198

Лемма 52: В $\mathbf{S}^{\sim}$ для любых **L**-состояний a и b, и любого **L**-наблюдения $u\in\mathbf{L}\cup\mathbf{R}$ имеет место $a\le b \;\&\; a\text{—}u^{\#}\!\rightarrow a` \;\&\; b\text{—}u^{\#}\!\rightarrow b` \Rightarrow a`\le b`$.

Доказательство см. на стр.199

Рассмотрим произвольную LTS в алфавите $\mathbf{L}^{+}\cup\mathbf{R}^{\#}\cup\{\Delta\}$ и ее состояние s.

Будем говорить, что *кнопка* $P^{\#}$ *γ-опасна в* s, если $\langle\not{P},\gamma\rangle\in\boldsymbol{T}(s)$, иначе *кнопка* $P^{\#}$ *γ-безопасна в* s.

Будем говорить, что *отказ* $P^{\#}$ *γ-опасен в* s, если кнопка $P^{\#}$ *γ-опасна в* s, иначе *отказ* $P^{\#}$ *γ-безопасен в* s.

Для *действия* $z\in\mathbf{L}$ будем говорить, что z *γ-опасно в* s, если в этом состоянии γ-опасна каждая кнопка, которой это действие принадлежит, иначе *действие* z *γ-безопасно в* s.

Заметим, что для ~финальной RTS отношение $P^{\#}$ *γ-безопасна в* s эквивалентно отношению $P\ \boldsymbol{safe}_{\gamma\Delta}\ \{s\}$ для любой LTS, множество $\mathbf{R}^{\#}$-трасс которой, совпадает с множеством трасс ~финальной RTS (например, для LTS $\boldsymbol{R2L}(\mathbf{S}^{\sim})$).

Лемма 53: В $\mathbf{S}^{\sim}$ для любых **L**-состояний a и b, и любого **L**-наблюдения $u\in\mathbf{L}\cup\mathbf{R}$ имеет место $b\text{—}u^{\#}\!\rightarrow \;\&\; a\le b \Rightarrow u^{\#}$ *γ-опасно в* $a \vee a\text{—}u^{\#}\!\rightarrow$.

Доказательство см. на стр.200

4.4. Построение ∇-пополнения в виде RTS

По-прежнему будем считать, что исходная спецификационная модель задана в виде LTS $\mathbf{S}$, исходная спецификационная тройка $\mathbf{T=(R/Q,\Sigma,}\boldsymbol{safe\ by}\mathbf{)}$, где $\mathbf{\Sigma=}\boldsymbol{F}\mathbf{(S)}$.

Если из начального состояния исходной спецификации $\mathbf{S}$ достижимо разрушение, то есть $s_0=\langle\gamma\rangle\Rightarrow$, то начальное состояние ~финальной RTS $\tilde{s}_0=\gamma$, все реализации конформны, тестирование излишне и ∇-пополнение строить не нужно.

В дальнейшем будем считать, что $s_0=\langle\gamma\rangle\not\Rightarrow$ в исходной спецификации $\mathbf{S}$.

RTS $\mathbf{S}^\nabla$ будем называть ∇-пополнением, если множество ее простых трасс совпадает с множеством ∇-финальных трасс $\boldsymbol{T}(\mathbf{S}^\nabla)=\mathbf{\Sigma}^{\mathbf{01}\nabla}$. Тогда $\cup\boldsymbol{d}(\boldsymbol{T}(\mathbf{S}^\nabla))=\cup\boldsymbol{d}(\mathbf{\Sigma}^{\mathbf{01}\nabla})$ и при любом расширении до полной трассовой модели будет получаться трассовое ∇-пополнение $\mathbf{\Sigma}^\nabla$. В результате будет построена спецификационная тройка $\mathbf{T}^\nabla=(\mathbf{R}^\#/\mathbf{Q}^\#,\mathbf{\Sigma}^\nabla,\boldsymbol{safe}_{\gamma\Delta})$ ∇-пополнения.

Согласно теореме 20, для этого нам нужно из множества простых трасс ~финальной RTS удалить все трассы из множества $\boldsymbol{x}(\mathbf{\Sigma})$. Как показано в подразделе 3.8 есть две причины **L**-неконформности: **L**-неконвергентность и **L**-неполнота. Мы рассмотрим два последовательных преобразования $\boldsymbol{C_1}$ и $\boldsymbol{C_2}$, первое из которых удаляет **L**-неконвергентные трассы, а второе – **L**-неполные трассы. В обоих случаях удаляемое множество трасс является постфикс-замкнутым подмножеством множества $\boldsymbol{x}(\mathbf{N})$ и вместе с каждой трассой содержит ее максимальный **L**-префикс (максимальный префикс, являющийся **L**-трассой). Поэтому, согласно лемме 39, после этого достаточно снова удалить все **L**-неконвергентные трассы и **L**-неполные трассы. Однако, вторые уже удалены операцией $\boldsymbol{C_2}$. Мы покажем, что после последовательности операций $\boldsymbol{C_1,C_2}$ не появляются новые **L**-неконвергентные трассы. Тем самым будет показано, что удалены все трассы из $\boldsymbol{x}(\mathbf{\Sigma})$ и только они.

4.4.1. Операция C_1 – удаление L-неконвергентных трасс.

Состояние a будем называть P-*неконвергентным*, где $P\in\mathbf{R}\cup\mathbf{Q}$, если это **L**-состояние (достижимое состояние вида (A,r)) и в нем не-отказ $\not\Rightarrow$ неразрушающий, и нет переходов по **L**-наблюдениям, разрешаемым кнопкой $P^\#$:

a P-*неконвергентно* $\triangleq$ a **L**-состояние $\&\ a\not\Rightarrow\gamma\ \&\ \forall u\in P\cup\{P\}\ a\not\xrightarrow{u^\#}$.

a P-*конвергентно* $\triangleq$ a P-~~*неконвергентно*~~.

Состояние a будем называть **L**-*неконвергентным*, если оно P-неконвергентно для некоторой кнопки $P \in \mathbf{R} \cup \mathbf{Q}$:

a **L**-*неконвергентно* $\triangleq \exists P \in \mathbf{R} \cup \mathbf{Q}$ a P-*неконвергентно*.

a **L**-*конвергентно* $\triangleq$ a **L**-~~*неконвергентно*~~.

Определим операцию c_1 как удаление всех переходов во все **L**-неконвергентные состояния. Операцию C_1 определим как повторение c_1 до тех пор, пока удаляются какие-то переходы. Поскольку число переходов в конечной RTS конечно, такое определение операции C_1 корректно. Обозначим $\mathbf{S}^{\sim 1} = C_1(\mathbf{S}^{\sim})$. Заметим, что $\mathbf{S}^{\sim 1}$, очевидно, является LTS. Ниже мы покажем, что она является также RTS.

Формальное определение $c_1(\mathbf{S}^{\sim}) = \mathrm{LTS}(V_{\mathbf{S}^{\sim}}, \mathbf{L}^{+} \cup \mathbf{R}^{\#} \cup \{\Delta\}, E, s^{\sim}_0)$, где $E = E_{\mathbf{S}^{\sim}} \setminus X$, а X определяется как наименьшее множество, порождаемое следующим правилом вывода: $\forall a, b \in V_{\mathbf{S}^{\sim}}$ $\forall u \in \mathbf{L} \cup \mathbf{R}$

$a \text{—} u^{\#} \rightarrow b$ & b **L**-*неконвергентно* $\vdash (a, u^{\#}, b) \in X$.

Обозначим $c_1^{\,n}(\mathbf{S}^{\sim}) \triangleq c_1(c_1(\ldots(c_1(\mathbf{S}^{\sim}))\ldots))$, где операция c_1 повторяется n раз, и $C_1(\mathbf{S}^{\sim}) \triangleq c_1^{\,k}(\mathbf{S}^{\sim})$, где $c_1^{\,k}(\mathbf{S}^{\sim}) = c_1^{\,k+1}(\mathbf{S}^{\sim})$.

Лемма 54: Операция $c_1^{\,n}$ для любого n обладает следующими свойствами:

1) Не появляются новых **L**-состояний (достижимых состояний вида (A,r)).
2) Не добавляются переходы и трассы, в частности: $T(c_1^{\,n}(\mathbf{S}^{\sim})) \subseteq \Sigma^{01\sim}$ и $T(\mathbf{S}^{\sim 1}) \subseteq \Sigma^{01\sim}$.
3) Не удаляются переходы-петли в остающихся **L**-состояниях, то есть состояниях вида (A,r), которые остаются достижимыми.
4) Сохраняется $\Delta\gamma$-свойство (замечание 16).
5) Если выполнено $\Delta\gamma$-свойство, то не удаляются переходы по не-отказам в остающихся **L**-состояниях, то есть состояниях вида (A,r), которые остаются достижимыми.

Доказательство см. на стр.200

Лемма 55: Все состояния LTS $\mathbf{S}^{\sim 1}$ **L**-конвергентны.

Доказательство см. на стр.201

Лемма 56: LTS $c_1^{\,n}(\mathbf{S}^{\sim})$ является RTS.

Доказательство см. на стр.202

Лемма 57: *О конечности RTS* $\mathbf{S}^{\sim 1}$. Для конечной спецификационной тройки $\mathbf{T} = (\mathbf{R}/\mathbf{Q}, F(\mathbf{S}), \textit{safe by})$ RTS $\mathbf{S}^{\sim 1}$ конечна, и ее можно алгоритмически построить за конечное время.

Доказательство см. на стр.203

Лемма 58: Операция c_1^n удаляет только те трассы, которые принадлежат $x(\Sigma^{01\sim})$, то есть $\Sigma^{01\sim}\setminus T(c_1^n(S^\sim))\subseteq x(\Sigma^{01\sim})$. Множество $\Sigma^{01\sim}\setminus T(c_1^n(S^\sim))$ удаляемых трасс является постфикс-замкнутым подмножеством множества $\Sigma^{01\sim}$ и вместе с каждой трассой содержит ее максимальный **L**-префикс (максимальный префикс, являющийся **L**-трассой).

Доказательство см. на стр.204

Следующая лемма аналогична лемме 47 для ~финальной RTS.

Лемма 59: В $c_1^n(S^\sim)$ для каждого **L**-состояния a и каждой кнопки $P\in\mathbf{R}$ имеет место $a\text{—}\not P\!\!\rightarrow \Leftrightarrow a\text{—}P^{\#}\!\!\rightarrow a$.

Доказательство см. на стр.204

Поскольку RTS $c_1^n(S^\sim)$ имеет то же множество состояний, что RTS $S^\sim$ (хотя, возможно, другое множество достижимых состояний), отношение «≤», определенное на состояниях RTS $S^\sim$, сохраняется и для состояний RTS $c_1^n(S^\sim)$. Следующие леммы аналогичны леммам 49÷53.

Лемма 60: В $c_1^n(S^\sim)$ для любых **L**-состояний a и b, и любой кнопки $P\in\mathbf{R}\cup\mathbf{Q}$ имеет место $a\text{—}\not P\!\!\rightarrow \;\&\; a\le b \Rightarrow b\text{—}\not P\!\!\rightarrow$.

Доказательство см. на стр.204

Лемма 61: В $c_1^n(S^\sim)$ для любых **L**-состояний a и b, и любой кнопки $P\in\mathbf{R}\cup\mathbf{Q}$ имеет место $b\text{—}\not P\!\!\rightarrow\gamma \;\&\; a\le b \Rightarrow a\text{—}\not P\!\!\rightarrow\gamma$.

Доказательство см. на стр.205

Лемма 62: В $c_1^n(S^\sim)$ для любых **L**-состояний a и b, и любой трассы отказов $\rho\in\mathbf{R}^*$ имеет место $a=\rho^{\#}\Rightarrow b \Rightarrow a\le b$.

Доказательство см. на стр.205

Лемма 63: В $c_1^n(S^\sim)$ для любых **L**-состояний a и b, и любого **L**-наблюдения $u\in\mathbf{L}\cup\mathbf{R}$ имеет место $a\le b \;\&\; a\text{—}u^{\#}\!\!\rightarrow a` \;\&\; b\text{—}u^{\#}\!\!\rightarrow b` \Rightarrow a`\le b`$.

Доказательство см. на стр.205

Лемма 64: В $c_1^n(S^\sim)$ для любых **L**-состояний a и b, и любого **L**-наблюдения $u\in\mathbf{L}\cup\mathbf{R}$ имеет место $b\text{—}u^{\#}\!\!\rightarrow \;\&\; a\le b \Rightarrow u^{\#}$ *γ-опасно в* $a \vee a\text{—}u^{\#}\!\!\rightarrow$.

Доказательство см. на стр.205

Если в результате преобразования C_1 начальное состояние RTS $S^{\sim 1}$ оказалось **L**-неконвергентным, то это означает, что все ~финальные трассы **L**-

неконформны. В этом случае тестирование излишне и ∇-пополнение строить не нужно.

В дальнейшем будем считать, что начальное состояние RTS $\mathbf{S}^{\sim 1}$ L-конвергентно.

4.4.2. Операция C_2 – удаление L-неполных трасс.

Переход по отказу $s \text{—} P^{\#} \rightarrow s'$ будем называть *особым переходом*, если:

1) этот переход ведёт в другое состояние,
2) в состоянии s есть переход-петля по какому-нибудь отказу и
3) в состоянии s нет переходов по действиям из P:

$s \text{—} P^{\#} \rightarrow s'$ *особый* $\triangleq s' \neq s \;\&\; \exists R \in \mathbf{R}\; s \text{—} R^{\#} \rightarrow s \;\&\; \forall z \in P\; s \text{—} z \not\rightarrow$.

Лемма 65: В $\mathbf{S}^{\sim 1}$ отказ $P^{\#}$ особый после трассы $\mu^{\#}$ тогда и только тогда, когда трасса $\mu^{\#}$ заканчивается в **L**-состоянии, в котором есть переход-петля или особый переход по отказу $P^{\#}$.

Доказательство см. на стр.207

Трассу $\rho^{\#}$ будем называть *особой в состоянии* s и обозначать $\rho^{\#}$ *особая в* s, если в этом состоянии есть маршрут с этой трассой, состоящий из особых переходов. Заметим, что особая трасса является трассой особых отказов, но не любая трасса особых отказов является особой трассой, а только такая, которая является трассой маршрута, в котором все переходы особые, то есть нет петель по особым отказам.

Трасса особая в состоянии s *максимальна*, если она не является строгим префиксом никакой трассы особой в s, то есть заканчивается в состоянии, в котором нет особых переходов. Будем обозначать: $\rho^{\#}$ *максимальная особая в* s.

Лемма 66: В $\mathbf{S}^{\sim 1}$ все трассы, являющиеся максимальными особыми в одном и том же достижимом **L**-состоянии s, заканчиваются в одном и том же **L**-состоянии s'.

Доказательство см. на стр.208

Определим операцию C_2: $\mathbf{S}^{\nabla} = C_2(\mathbf{S}^{\sim 1}) = LTS(V_{\mathbf{S}}{}^{\nabla}, \mathbf{L}^{+} \cup \mathbf{R}^{\#} \cup \{\Delta\}, E_{\mathbf{S}}{}^{\nabla}, s^{\nabla}{}_0)$, где множество состояний $V_{\mathbf{S}}{}^{\nabla} = (V_{\mathbf{S}^{\sim}} \times V_{\mathbf{S}^{\sim}}) \cup \{\gamma, \Delta, \Delta', \varpi\}$ содержит выделенные состояния $\gamma, \Delta, \Delta', \varpi$ и множество всех пар (a,b), где a,b – состояния $\mathbf{S}^{\sim}$, начальное состояние $s^{\nabla}{}_0 = (s^{\sim}{}_0, s^{\sim}{}_0)$, где $s^{\sim}{}_0$ – начальное состояние $\mathbf{S}^{\sim}$,

множество переходов $E_{\mathbf{S}}{}^{\nabla}$ определяется как наименьшее множество, порождаемое следующими правилами вывода[12]:

[12] В левой части правил указываются переходы в RTS $\mathbf{S}^{\sim 1}$.

$\forall a,b,a`,b`,b_u \in V_{\mathbf{S}^{\sim}}\ \ \forall u \in \mathbf{L} \cup \mathbf{R}\ \ \forall \rho$

1. $a \text{—} u^{\#} \rightarrow a`\ \ \&\ \ b \text{—} u^{\#} \rightarrow b_u\ \ \&\ \ b_u = \rho \Rightarrow b`$

$\&\ \ \rho$ *максимальная особая в* $b_u \qquad \vdash\ (a,b) \text{—} u^{\#} \rightarrow (a`,b`),$

2. $a \text{—} \not{\rho} \rightarrow \gamma \text{—} \gamma \rightarrow \varpi \qquad \vdash\ (a,b) \text{—} \not{\rho} \rightarrow \gamma \text{—} \gamma \rightarrow \varpi,$

3. $a \text{—} \not{\rho} \rightarrow \Delta \text{—} \Delta \rightarrow \varpi \qquad \vdash\ (a,b) \text{—} \not{\rho} \rightarrow \Delta \text{—} \Delta \rightarrow \varpi,$

4. $a \text{—} \not{\rho} \rightarrow \Delta` \text{—} \Delta \rightarrow \varpi \qquad \vdash\ (a,b) \text{—} \not{\rho} \rightarrow \Delta` \text{—} \Delta \rightarrow \varpi.$

L-состояниями LTS $\mathbf{S}^{\nabla}$ будем называть достижимые состояния вида (a,b), то есть состояния отличные от состояний γ, Δ, $\Delta`$ и ϖ.

Замечание 19. Из правил вывода непосредственно следует выполнение $\Delta\gamma$-свойства в $\mathbf{S}^{\nabla}$.

Лемма 67: В $\mathbf{S}^{\nabla}$ для каждого **L**-состояния (a,b) в состоянии b в $\mathbf{S}^{\sim 1}$ нет особых переходов и $a \le b$.

Доказательство см. на стр.211

Лемма 68: В $\mathbf{S}^{\nabla}$ для каждого **L**-состояния (a,b) правило вывода **1** эквивалентно следующему правилу вывода:

1a. $u^{\#}$ *γ-безопасно в* $a\ \ \&\ \ b \text{—} u^{\#} \rightarrow b_u\ \ \&\ \ b_u = \rho \Rightarrow b`$

$\&\ \ \rho$ *максимальная особая в* $b_u \qquad \vdash\ (a,b) \text{—} u^{\#} \rightarrow (a`,b`).$

Доказательство см. на стр.212

Лемма 69: В $\mathbf{S}^{\nabla}$ 1) каждое **L**-состояние (a,b) **L**-конвергентно и 2) все простые **L**-трассы **L**-конвергентны.

Доказательство см. на стр.212

Лемма 70: LTS $\mathbf{S}^{\nabla}$ является RTS.

Доказательство см. на стр.213

RTS $\mathbf{S}^{\nabla}$ будем называть ∇-финальной RTS.

Лемма 71: Если в $\mathbf{S}^{\nabla}$ **L**-трасса заканчивается в состоянии (a,b), то в $\mathbf{S}^{\sim 1}$ такая трасса тоже есть и она заканчивается в состоянии a.

Доказательство см. на стр.215

Лемма 72: Если **L**-трасса $\sigma^{\#}$ имеется в $\mathbf{S}^{\nabla}$, то все ее продолжения неотказами и далее разрушением или дивергенцией одинаковы в $\mathbf{S}^{\sim 1}$ и в $\mathbf{S}^{\nabla}$.

Доказательство см. на стр.216

Лемма 73: Преобразование C_2 не добавляет новых трасс: $T(S^{\nabla}) \subseteq T(S^{-1})$.

Доказательство см. на стр.216

Лемма 74: Если трасса $\sigma^{\#}$ в S^{∇} заканчивается в состоянии (a,b), то в S^{-1} существует такая трасса $\sigma`^{\#}$, которая заканчивается в состоянии $b$, и $\sigma^{\#} \preccurlyeq \sigma`^{\#}$.

Доказательство см. на стр.216

Лемма 75: Преобразование C_2 удаляет только те **L**-трассы, которые принадлежат $x(T(S^{-1}))$.

Доказательство см. на стр.216

Лемма 76: 1) Преобразование C_2 удаляет только те трассы, которые принадлежат $x(T(S^{-1}))$, то есть $T(S^{-1}) \setminus T(S^{\nabla}) \subseteq x(T(S^{-1}))$. 2) Множество $T(S^{-1}) \setminus T(S^{\nabla})$ удаляемых трасс является постфикс-замкнутым подмножеством множества $T(S^{-1})$ и вместе с каждой трассой содержит ее максимальный **L**-префикс (максимальный префикс, являющийся **L**-трассой).

Доказательство см. на стр.217

Лемма 77: Для любого **L**-состояния (a,b) в S^{∇}:

$(a,b) \text{—} P^{\#} \rightarrow (a`,b`)$ *особый* $\Rightarrow a \le a` \ \&\ b = b`$.

Доказательство см. на стр.218

Лемма 78: Для любого **L**-состояния (a,b) в S^{∇}, любого **L**-состояния $a`$ в S^{-1} и любого $u \in \mathbf{L} \cup \mathbf{R}$:

$a \le a` \ \&\ (a,b) \text{—} u^{\#} \rightarrow (a_u, b_u) \Rightarrow \exists a_u` \ (a`,b) \text{—} u^{\#} \rightarrow (a_u`, b_u) \ \&\ a_u \le a_u`$.

Доказательство см. на стр.218

Лемма 79: В S^{∇} все простые **L**-трассы **L**-полны.

Доказательство см. на стр.219

Теорема 26: **О ∇-финальной RTS:** $T(S^{\nabla}) = \Sigma^{x} = \Sigma^{01\nabla}$.

Доказательство см. на стр.220

Теорема 27: **∇-финальная RTS: О безопасности кнопок.** В S^{∇} кнопка $P^{\#}$ безопасна по отношению $safe_{\gamma\Delta}$ после простой **L**-трассы, заканчивающейся в состоянии s, тогда и только тогда, когда $s \text{—} P \not\rightarrow \gamma$.

Доказательство см. на стр.220

Теорема 28: **∇-финальная RTS: Безопасные L-трассы.** В S^{∇} **L**-трасса безопасна по отношению $safe_{\gamma\Delta}$ тогда и только тогда, когда это простая трасса.

Доказательство см. на стр.221

Лемма 80: **Свойство $\mathbf{R}^{\#}$-петель:** В $\mathbf{S}^{\nabla}$ для **L**-состояния (a,b) имеет место $\cup\boldsymbol{r}((a,b))=\cup\boldsymbol{Ip}(\sigma)$ для любой трассы $\sigma^{\#}$, заканчивающейся в состоянии (a,b).

Доказательство см. на стр.221

Лемма 81: В $\mathbf{S}^{\nabla}$ для любой трассы $\sigma^{\#}$, заканчивающейся в состоянии (a,b), условие **L**-актуальности $\mathbf{R}^{\#}$-отказа $P^{\#}$, безопасного по $\boldsymbol{safe}_{\gamma\Delta}$ после трассы $\sigma^{\#}$, эквивалентно $(a,b)\text{—}\not{P}\not\to\Delta`$.

Доказательство см. на стр.222

Теорема 29: **∇-финальная RTS: L-актуальные наблюдения и трассы.**

1. Все **L**-трассы из $\boldsymbol{T}(\mathbf{S}^{\nabla})$ **L**-актуальны.
2. **L**-наблюдение $u^{\#}\in\mathbf{L}\cup\mathbf{R}^{\#}$, безопасное по $\boldsymbol{safe}_{\gamma\Delta}$ в **L**-состоянии s, то есть после любой трассы, заканчивающейся в этом состоянии, **L**-актуально тогда и только тогда, когда либо 1) $u\in\mathbf{L}$ и $u\notin\cup\boldsymbol{r}(s)$, либо 2) $u\in\mathbf{R}$ & $s\text{—}\not{u}\not\to\Delta`$.

Доказательство см. на стр.223

Заметим, что из $u^{\#}\ \boldsymbol{safe}_{\gamma\Delta}\ s$ следует $s\text{—}\not{u}\not\to\gamma$. Поэтому условие $s\text{—}\not{u}\not\to\Delta`$ эквивалентно условию $s\text{—}\not{u}\not\to\ \vee\ s\text{—}\not{u}\to\Delta$.

Теорема 30: **О конечности ∇-финальной RTS.** Для конечной спецификационной тройки $\mathbf{T}=(\mathbf{R}/\mathbf{Q},\boldsymbol{F}(\mathbf{S}),\boldsymbol{safe\ by})$ RTS $\mathbf{S}^{\nabla}$ конечна, и ее можно алгоритмически построить за конечное время. Спецификационная тройка $\mathbf{T}^{\nabla}=(\mathbf{R}^{\#}/\mathbf{Q}^{\#},\boldsymbol{\Sigma}^{\nabla},\boldsymbol{safe}_{\gamma\Delta})$ является конечным максимальным ∇-пополнением тройки **T**.

Доказательство см. на стр.223

4.4.3. Особые отказы и зависимость между ошибками.

Здесь мы рассмотрим оптимизацию генерации тестов, основанную на учете особых отказов. В спецификации $\mathbf{S}^{\nabla}$ отказ $R^{\#}$ особый после трассы $\sigma^{\#}$ заканчивающейся в состоянии s, если в этом состоянии имеется переход-петля $s\text{—}R^{\#}\to s$, или особый переход $s\text{—}R^{\#}\to s`$ в состояние $s`\neq s$.

Прежде всего, заметим, что для полноты тестового набора достаточно генерировать тесты только по тем простым трассам RTS $\mathbf{S}^{\nabla}$, маршруты которых не содержат петель по отказам. Действительно, если в $\mathbf{S}^{\nabla}$ простая трасса $\sigma^{\#}$ заканчивается в состоянии s, где имеется петля по отказу $R^{\#}$, то (в силу детерминизма RTS) трассы $\sigma^{\#}$ и $\sigma^{\#}\cdot\langle R^{\#}\rangle$ T-эквивалентны (см.

замечание 1): они имеют в $\mathbf{S}^{\nabla}$ одинаковые множества продолжений. Поэтому спецификация определяет ошибку $\sigma^{\#}\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$ тогда и только тогда, когда она определяет ошибку $\sigma^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$. Следовательно, достаточно искать только ошибки вида $\sigma^{\#}\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$ и не искать ошибки вида $\sigma^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$.

Если же трасса $\sigma^{\#}$ заканчивается в состоянии s, где имеется переход $s\text{—}R^{\#}\rightarrow s`$ по отказу $R^{\#}$, но ведущий в другое состояние $s`\neq s$, то по лемме 80 $R\not\subseteq\cup\boldsymbol{Ip}(\sigma)$. В этом случае трассы $\sigma^{\#}$ и $\sigma^{\#}\cdot\langle R^{\#}\rangle$, вообще говоря, не T-эквивалентны. Спецификация может определять ошибку $\sigma^{\#}\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$, но не определять ошибку $\sigma^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$; в спецификации может даже не быть трассы $\sigma^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}$. Также и наоборот: спецификация может определять ошибку $\sigma^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$, но не определять ошибку $\sigma^{\#}\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$, хотя по ***d***-замкнутости спецификации должна быть трасса $\sigma^{\#}\cdot\lambda^{\#}$. Во-первых, трасса $\sigma^{\#}\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$ может не быть тестовой трассой и, следовательно, ошибкой (трасса $\sigma^{\#}\cdot\lambda^{\#}$ может не быть безопасной трассой, или наблюдение $u^{\#}$ может быть опасным после безопасной трассы $\sigma^{\#}\cdot\lambda^{\#}$). Во-вторых, трасса $\sigma^{\#}\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$ может быть простой трассой спецификации $\mathbf{S}^{\nabla}$ и, следовательно, не быть ошибкой. Тем самым, вообще говоря следует искать ошибки как вида $\sigma^{\#}\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$, так и вида $\sigma^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$.

Особый случай – когда переход $s\text{—}R^{\#}\rightarrow s`$ особый. В этом случае по **L**-полноте, если спецификация определяет ошибку $\sigma^{\#}\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$, то она определяется и ошибку $\sigma^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$. Наоборот, если имеется ошибка $\sigma^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$, то трасса $\sigma^{\#}\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$ не может быть простой трассой спецификации $\mathbf{S}^{\nabla}$, но она может не быть ошибкой, если не является тестовой трассой (трасса $\sigma^{\#}\cdot\lambda^{\#}$ не безопасная трасса, или наблюдение $u^{\#}$ опасно после безопасной трассы $\sigma^{\#}\cdot\lambda^{\#}$). Тем самым, в этом особом случае достаточно искать только ошибки вида $\sigma^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$, и не искать ошибки вида $\sigma^{\#}\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$.

Если в состоянии s имеется особый переход по отказу $R^{\#}$, то мы всегда должны выбирать этот переход, то есть генерировать тест по трассе $\sigma^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$, а не трассе $\sigma^{\#}\cdot\lambda^{\#}\cdot\langle u^{\#}\rangle$. В состоянии s может быть несколько особых переходов, но по лемме 66 все максимальные особые маршруты (состоящие из особых отказов), начинающиеся в состоянии s, заканчиваются в одном и том же состоянии. Нам достаточно выбирать любой такой маршрут,

и трассу $\sigma^{\#}$ продолжать трассой $\rho^{\#}$ этого маршрута, то есть генерировать тест по трассе вида $\sigma^{\#}\cdot\rho^{\#}\cdot\lambda^{\#}$. В целом достаточно генерировать тесты только по таким трассам, в которых после каждого префикса следует трасса максимального особого маршрута. Иными словами, тест генерируется только по трассе такого маршрута, в котором после каждого префикса следует максимальный особый маршрут (возможно, пустой).

В целом можно сказать: полный набор тестов может обнаруживать не все ошибки, определяемые спецификацией, даже если такой спецификацией является RTS $\mathbf{S}^{\nabla}$, в которой все безопасные трассы **L**-конформны. Анализ этой проблемы должен опираться на (множественную) зависимость между ошибками.

Будем говорить, что из множества ошибок A следует множество ошибок B, если в каждой безопасно-тестируемой **L**-реализации, в которой есть какая-нибудь ошибка из A, имеется также какая-нибудь ошибка из B. Набор тестов полный, очевидно, если из множества обнаруживаемых им ошибок следует множество всех ошибок, определяемых спецификацией. Задача построения полного набора тестов с минимальным (например, по отношению вложенности) множеством обнаруживаемых ошибок выходит за рамки данной работы и является предметом дальнейших исследований.

4.5. О безопасных трассах конформных реализаций.

Итак, мы построили максимальное ∇-пополнение в виде RTS-спецификации $\mathbf{S}^{\nabla}$: множество ее простых **L**-трасс, приведенных к алфавиту **L**, совпадает с множеством ∇-конформных трасс: $(\boldsymbol{T}(\mathbf{S}^{\nabla})\cap(\mathbf{L}\cup\mathbf{R}^{\#})^{*})_{\mathbf{L}} = \nabla\boldsymbol{conf}(\mathbf{T})$.

Напомним, что ∇-конформная трасса (трасса из $\nabla\boldsymbol{conf}(\mathbf{T})$) – это такая трасса $\sigma_{\mathbf{L}}$, которая получается приведением к алфавиту **L** трассы σ, которая, во-первых, **L**-конформна, то есть встречается в некоторой конформной **L**-реализации, и, во-вторых, является безопасной трассой некоторой спецификации из **L**-конуса $\nabla(\mathbf{T})_{\mathbf{L}}$. Такая трасса σ безопасна (по ***safe in***) в каждой конформной (даже в каждой безопасно-тестируемой) **L**-реализации, в которой она встречается.

Обратное, вообще говоря, не верно: может существовать такая трасса σ, которая **L**-конформна, то есть встречается в некоторой конформной **L**-реализации, и безопасна в каждой конформной **L**-реализации, в которой она встречается, но трасса $\sigma_{\mathbf{L}}\notin\nabla\boldsymbol{conf}(\mathbf{T})$. В этом случае для каждой спецификационной тройки $\mathbf{T_i}\in\nabla(\mathbf{T})_{\mathbf{L}}$ можно рассмотреть максимальный префикс μ трассы σ такой, что $\mu_{\mathbf{L}}\in\boldsymbol{conf}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}}$, то есть в этой спецификации есть безопасная трасса μ_i такая, что $\mu_{i\mathbf{L}}=\mu_{\mathbf{L}}$. Поскольку такой

префикс μ строгий, за ним в трассе σ имеется наблюдение u. Поскольку семантики спецификационных троек из **L**-конуса **L**-эквивалентны, семантика $\mathbf{R_i \backslash Q_i}$ определяет (быть может не единственное) соответствующее наблюдение u_i такое, что $u_{iL}=u_L$. Для каждого такого наблюдения u_i должно быть $\mu_i \cdot \langle u_i \rangle \notin \mathbf{\Sigma_i}$. Понятно, что это наблюдение u_i должно быть опасным в спецификации $\mathbf{\Sigma_i}$ после μ_i, так как в противном случае спецификация определяла бы ошибку $\mu_i \cdot \langle u_i \rangle$, что противоречит **L**-конформности трассы σ.

Для исходной тройки **T** обозначим множество трасс, которые встречаются в конформных реализациях и безопасны во всех конформных реализациях, в которых они встречаются:

$$\mathbf{\mathit{Safe}(T)} \triangleq \{\sigma \in \cup \mathbf{\mathit{ConfImp}(T)} \mid \forall \mathbf{I} \in \mathbf{\mathit{ConfImp}(T)}\ (\sigma \in \mathbf{I} \Rightarrow \sigma \in \mathbf{\mathit{SafeIn}(I)})\}$$

$$= \cup\{\mathbf{\mathit{SafeIn}(I)} \mid \mathbf{I} \in \mathbf{\mathit{ConfImp}(T)}\} \setminus \cup\{\mathbf{I} \backslash \mathbf{\mathit{SafeIn}(I)} \mid \mathbf{I} \in \mathbf{\mathit{ConfImp}(T)}\}$$

Тогда можно записать: $\nabla \mathbf{\mathit{conf}(T)} \subseteq \mathbf{\mathit{Safe}(T)}$.

Пример трассы $\sigma_0 \in \mathbf{\mathit{Safe}(T)} \setminus \nabla \mathbf{\mathit{conf}(T)}$ приведен на Рис. 21. . Здесь $\sigma_0 = \langle \{a\}, \{b\} \rangle$. Для семантики **R**/**Q**, где **R**={{y},{a},{b}} и **Q**={{x}}, единственно возможным отношением ***safe by*** является отношение, которое объявляет **Q**-кнопку {x} безопасной после трассы тогда и только тогда, когда трасса продолжается неразрушающим действием x. В LTS-спецификации $\mathbf{S_7}$ действие x не является разрушающим ни в каком состоянии. В этой LTS использована LTS $\mathbf{S_5}$ из примера на Рис. 11. , все трассы которой неконформны. Из-за этого в RTS $\mathbf{S_7}^{\sim}$ переходы, показанные пунктиром, ведут в **L**-неконвергентное состояние – начальное состояние RTS $\mathbf{S_5}^{\sim}$. Удаляя эти переходы, получаем RTS $\mathbf{S_7}^{\nabla}$ (**L**-неполных трасс не возникает, поэтому операция $\boldsymbol{C_2}$ не меняет множества трасс). В этой RTS трасса $\sigma_0^{\#}$ опасна: после трассы $\langle \{a\}^{\#} \rangle$ наблюдение $\{b\}^{\#}$ опасно, поскольку после перехода по $\{a\}^{\#}$ имеется переход по ~~{b}~~, ведущий в состояние γ. Имеем $\sigma_0 \notin \nabla \mathbf{\mathit{conf}(T_7)}$.

LTS $\mathbf{I_1}$ – пример безопасно-тестируемой, но неконформной реализации (в ней имеется ошибка $\langle y \rangle$). В этой LTS после трассы $\langle \{a\} \rangle$ наблюдение {b} опасно, поскольку переход по действию b разрушающий.

В то же время в любой конформной реализации после трассы $\langle \{a\} \rangle$ кнопка {y} должна быть безопасна, а единственным конформным наблюдением по этой кнопке является отказ {y}. Следовательно, в любой конформной реализации отказ {y} вставляется ***i***-операцией после трассы $\langle \{a\} \rangle$ в любую трассу вида $\langle \{a\} \rangle \cdot \lambda$. Поэтому, если бы кнопка {b} была в

конформной реализации опасна после трассы ⟨{a}⟩, то была бы трасса ⟨{a},b,γ⟩, а тогда была бы и трасса ⟨{a},{y},b,γ⟩, что противоречит гипотезе о безопасности, поскольку в спецификации кнопка {b} безопасна после трассы ⟨{a},{y}⟩. Следовательно, в любой конформной реализации, в которой есть трасса σ_0, эта трасса безопасна по ***safe in***. Имеем: $\sigma_0 \in$ ***Safe***(**T**).

L={x,y,a,b} **R**={{y},{a},{b}} **Q**={{x}}

{x} ***safe by*** $\mathbf{S}_7$ ***after*** μ ⇔ μ·⟨x⟩∈***T***($\mathbf{S}_7$)

⟨y⟩∈***T***($\mathbf{I}_1$) ⇒ $\mathbf{I}_1$ ~~***saco***~~ $\mathbf{S}_5$ $\mathbf{I}_2$ ***saco*** $\mathbf{S}_5$

В RTS $\mathbf{S}_7^{\sim}$ опущены:
- петли по отказам, требуемые свойством кумулятивности RTS,
- переходы по не-отказам в состояние Δ и
- переходы по ~~(x)~~ в состояние γ из всех состояний, где нет перехода по x.

RTS $\mathbf{S}_7^{\nabla}$ получается из $\mathbf{S}_7^{\sim}$ удалением переходов, показанных пунктиром.

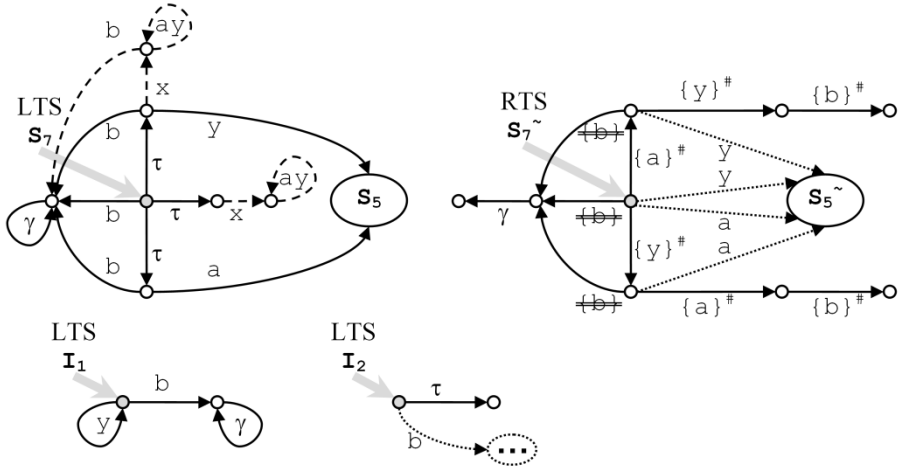


Рис. 21. Пример трассы ⟨{a},{b}⟩∈***Safe(T)*** \ ∇***conf(T)***

Аналогичную ситуацию имеем с трассой σ_1=⟨{a},x,{b}⟩, если в LTS $\mathbf{S}_7$ добавить переходы, показанные штрихом.

Эти две трассы σ_0 и σ_1 на Рис. 21. демонстрируют два случая, когда в конформной реализации отказ оказывается безопасным по ***safe in*** после

трассы и вставляется после нее ***i***-операцией, хотя в спецификации отказ опасен после этой трассы. Это связано с наличием особых отказов, когда после трассы $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}$ с особым отказом $P^{\#}$ некоторый отказ $R^{\#}$ безопасен, а после этой же трассы без особого отказа, то есть после трассы $\mu^{\#}\cdot\lambda^{\#}$ отказ $R^{\#}$ опасен. Такой отказ $R^{\#}$ может быть опасен после трассы $\mu^{\#}\cdot\lambda^{\#}$ только в такой безопасно-тестируемой реализации, которая неконформна. Именно поэтому при построении в 3.8.3 конформной реализации $\mathbf{I}^{\nabla}$, содержащей все ∇-конформные трассы, мы такие **R**-отказы делали безопасными и вставляли их в трассы как необходимые отказы. Иными словами, поскольку эта реализация конформна, множество $\boldsymbol{SafeIn}(\mathbf{I}^{\nabla})$ ее безопасных трасс включает не только множество $\nabla\boldsymbol{conf}(\mathbf{T})$ ∇-конформных трасс, но и множество $\boldsymbol{Safe}(\mathbf{T})$ (а также, быть может, некоторые дополнительные безопасные трассы).

5. Заключение

5.1. Итоги

Итогом этой работы является алгоритм построения по конечной исходной спецификационной тройке $\mathbf{T}=(\mathbf{R}/\mathbf{Q},\Sigma,\boldsymbol{safe\ by})$ спецификационной модели, заданной в виде конечной RTS $\mathbf{S}^{\nabla}$, и соответствующей конечной тройки $\mathbf{T}^{\nabla}=(\mathbf{R}^{\#}/\mathbf{Q}^{\#},\Sigma^{\nabla},\boldsymbol{safe}_{\gamma\Delta})$.

Это дает целый ряд свойств полезных для оптимизированной генерации полного тестового набора. Напомним, что полный набор тестов достаточно генерировать по безопасным **L**-конформным трассам. В каждом тесте после получения трассы, нажимается кнопка, безопасная после этой трассы, и для каждого **L**-актуального наблюдения, определяемого этими трассой и кнопкой, в тесте должен либо выноситься вердикт, либо продолжаться тестирование (если такое наблюдение продолжает трассу, по которой сгенерирован тест).

1. **Все безопасные L-трассы L-конформны**.
2. **Безопасные L-трассы**. В RTS $\mathbf{S}^{\nabla}$ такими трассами являются простые трассы, заканчивающиеся в **L**-состояниях, то есть состояниях, отличных от состояний $\gamma,\Delta,\Delta`,\varpi$.
3. **Детерминизм**. RTS детерминирована, следовательно, каждая трасса, по которой нужно генерировать тесты, заканчивается в одном состоянии.
4. **Безопасные кнопки**. Кнопка $P^{\#}$ безопасна после **L**-трассы, заканчивающейся в состоянии a, тогда и только тогда, когда $a\ \mathbf{P}\not\rightarrow\gamma$.
5. **Актуальные наблюдения**. **L**-наблюдение $u^{\#}\in\mathbf{L}\cup\mathbf{R}^{\#}$, безопасное после трассы, заканчивающейся в состоянии a, **L**-актуально тогда и только тогда, когда либо 1) $u\in\mathbf{L}$ & $u\notin\cup\boldsymbol{r}(s)$, либо 2) $u\in\mathbf{R}$ & $s\ \mathbf{u}\not\rightarrow\Delta`$.

6. **Оптимизация «особые отказы»**. Для того, чтобы полностью выполнить оптимизацию «особые отказы» достаточно каждый тест генерировать только по такой трассе, маршрут которой, во-первых, не проходит через петли по отказам, и, во-вторых, продолжается после каждого своего префикса максимальным особым маршрутом (возможно, пустым).

5.2. Направления дальнейших исследований

5.2.1. Критерии «правильных» спецификаций

Конечная RTS-спецификация $\mathbf{S}^{\nabla}$ может быть построена из любой исходной спецификации, заданной в виде конечной LTS (или RTS) **S**. В связи с этим возникает естественная задача сформулировать критерии, которым должна удовлетворять исходная RTS-спецификация **S**, чтобы ее преобразование в RTS $\mathbf{S}^{\nabla}$ не требовалось. Конечно, в качестве такого критерия можно использовать преобразование исходной RTS **S** в RTS $\mathbf{S}^{\nabla}$, а затем проверку «эквивалентности» построенной и исходной RTS. Понятно, что такой критерий мало пригоден как практическое руководство разработчику спецификаций.

Целью дальнейших исследований мог бы стать поиск таких практически удобных, легко проверяемых критериев, которые показывали бы, что спецификация обладает указанными в п.5.1 (или аналогичными) свойствами, и которыми мог бы непосредственно руководствоваться разработчик спецификаций. Проблема здесь в том, что проверка наличия или отсутствия в спецификации **L**-неконформных трасс, скорее всего, принципиально не может быть простой для LTS- или RTS-модели. Причина в том, что эти модели построены на локальных описаниях переходов из того или иного состояния, а анализ безопасных **L**-неконформных трасс требует глобального учета множества различных состояний и переходов. Возможно, здесь потребуется какая-то новая модель, в идеале модель должна быть такой, чтобы в ней вообще нельзя было описать **L**-неконформные безопасные трассы.

5.2.2. Бесконечные и конечные полные наборы тестов

Если полный набор тестов для данной спецификации бесконечен, то задача генерации тестов сводится к перечислению тестов этого набора. При таком перечислении каждый тест должен быть получен через конечный интервал времени после предыдущего (или от начала генерации для первого теста). Все возможные оптимизации генерации тестов могут уменьшать только этот конечный интервал, но общее время генерации тестов все равно остается бесконечным.

Поэтому, в первую очередь, ставится задача определения условий на спецификацию, при которых существует конечный полный набор тестов. Заметим, что для некоторых спецификаций могут существовать как бесконечные, так и конечные полные наборы тестов, что делает решение этой задачи еще более актуальным.

5.2.3. Минимальные множества ошибок

Как уже замечено в п.4.4.3 полный набор тестов может обнаруживать не все ошибки, определяемые спецификацией, даже если такой спецификацией является RTS $\mathbf{S}^{\nabla}$, в которой все безопасные трассы **L**-конформны. Анализ этой проблемы должен опираться на (множественную) зависимость между ошибками. Задача заключается, в первую очередь, в нахождении конструктивных критериев зависимости между множествами ошибок.

После этого необходимо решить задачу конструктивного построения минимального (по вложенности множеств) множества ошибок, из которого следовало бы множество всех ошибок, определяемых спецификацией. Условия существования конечного полного набора тестов, фактически, сводятся к условиям существования конечного минимального множества ошибок.

Таких минимальных, в том числе конечных, множеств ошибок может быть несколько (может не существовать наименьшего множества ошибок). Выбор того или иного минимального множества ошибок для генерации набора тестов, их обнаруживающего, может определяться дополнительными критериями. Примерами таких критериев могут быть число трасс, суммарная длина трасс, взвешенная суммарная длина трасс (когда для каждого тестового воздействия задан его «вес»), и т.п.

5.2.4. Pass-тесты и конечность времени генерации тестов

Бесконечный набор тестов требует, естественно, бесконечного времени генерации. Конечный набор тестов хотелось бы генерировать за конечное время. Как это сделать?

Проблема в том, что конечность минимального множества ошибок не означает конечности множества безопасных трасс, а генерация тестов основана как раз на перечислении этого множества трасс и фильтрации получающихся тестов. Отбрасываются те тесты, которые можно было бы завершить раньше: как только исчезает неопределенность в возможном вердикте. Это такие «лишние» тесты, в которых после нажатия последней кнопки возможен только вердикт ***fail*** или только вердикт ***pass***.

fail-тесты. Если после получения трассы σ и нажатия некоторой кнопки p возможен только вердикт ***fail***, то это означает, что трасса σ **L**-неконформна. За счет **L**-неконформных трасс множество всех ошибок, определяемых спецификацией, может быть бесконечным, хотя минимальное множество ошибок конечно. Поэтому тесты нужно генерировать только по **L**-

конформным трассам, а для этого их надо выделить и перечислять только такие трассы для генерации тестов. Эта задача решена в настоящей работе с помощью вложенного преобразования исходной спецификации **S** в RTS-спецификацию $\mathbf{S}^{\nabla}$, в которой все безопасные трассы **L**-конформны. Для спецификации $\mathbf{S}^{\nabla}$ тестирования 1-го и 2-го рода совпадают. Тесты генерируются только по **L**-конформным трассам, а получение **L**-неконформного **L**-наблюдения означает вердикт ***fail***.

pass-тесты. Если в спецификации трасса σ, по которой генерировался тест, продолжается каждым **L**-актуальным наблюдением из множества $P_{\mathbf{L}}\cup\{P\}$ для $P\in\mathbf{R}$ или из множества $P_{\mathbf{L}}$ для $P\in\mathbf{Q}$, то после получения трассы σ и нажатия кнопки P возможен только вердикт ***pass***. Такой тест тоже оказывается «лишним»: нужно генерировать тест по максимальному префиксу трассы σ, после которого нет однозначности вердикта. Заметим, что, вообще говоря, если тест «лишний» по вердикту ***pass***, то это не значит, что «лишние» все его продолжения. Поэтому при генерации тестов можно просто отфильтровывать такие ***pass***-тесты.

Особый случай возникает тогда, когда после любого продолжения λ такого, что трасса $\sigma\cdot\lambda$ безопасна, любое безопасное **L**-актуальное наблюдение имеется в спецификации. Иными словами, после трассы σ спецификация допускает произвольное, с учетом безопасности, поведение **L**-реализации. Такие трассы σ будем называть демоническими[13]. Поскольку безопасное продолжение демонической трассы по определению демоническое, фильтрация будет работать «вхолостую» на всех демонических трассах, префиксом которых является данная демоническая трасса σ. Вместо этого нужно было бы просто прекратить генерировать тесты по трассам вида $\sigma\cdot\lambda$. Особенно это важно в том случае, когда существует конечный полный набор тестов, но демонических трасс бесконечно много: без учета демонических трасс генерация этого конечного набора тестов потребует бесконечного времени, впустую потраченного на фильтрацию. Это может быть даже в том случае, когда множество всех ошибок, определяемых спецификацией, конечно, но множество **L**-конформных трасс спецификации бесконечно.

Возникает задача предварительного выделения среди всех безопасных трасс спецификации $\mathbf{S}^{\nabla}$ недемонических трасс и перечисления только таких трасс для генерации тестов.

[13] Название «демоническое» выбрано по аналогии с «демоническим» пополнением спецификации, определяющим произвольное поведение [29][30][34][38].

Можно высказать следующую гипотезу: Если существует конечный полный набор тестов для класса всех безопасно-тестируемых реализаций, то для конечной спецификации в конечной семантике его можно построить алгоритмически за конечное время с помощью трех оптимизаций, основанных на 1) удалении **L**-неконформных трасс (чему посвящена данная работа), 2) учете демонических трасс и 3) множественном следовании ошибок (выделении конечного минимального множества ошибок).

5.2.5. Минимизация покрытия ошибок тестами

Генерация (примитивных) тестов, описанная в данной работе, предполагает генерацию по одной трассе всех возможных тестов. В то же время каждый тест, как правило, обнаруживает не одну, а множество ошибок, в том числе принадлежащих выбранному минимальному множеству ошибок, на обнаружение которых нацелена генерация тестов. Множества ошибок, обнаруживаемых разными тестами, сгенерированными по разным трассам или даже по одной и той же трассе, могут пересекаться. Поэтому возникает задача минимизация покрытия тестами (точнее, множествами обнаруживаемых ими ошибок) выбранного минимального множества ошибок.

5.2.6. Целевые подклассы реализаций

До сих пор речь шла о генерации полного набора тестов для класса всех безопасно-тестируемых реализаций. Если тестирование нацелено на обнаружение ошибок в том или ином подклассе реализаций, то возникают дополнительные возможности оптимизации тестирования. В частности, для таких целевых подклассов могут существовать конечные полные наборы тестов, хотя для всего класса безопасно-тестируемых реализаций все полные наборы тестов бесконечные. Например, одним из естественных целевых подклассов реализаций является множество LTS-реализаций ограниченного размера (с ограниченным числом состояний и переходов) [26],[28],[35].

Иногда говорят о классе ошибок, на обнаружение которых нацелены тесты. Понятно, что это эквивалентно генерации полных наборов тестов для подкласса реализаций, в которых нет других ошибок. Такие тесты, конечно, применимы и для других безопасно-тестируемых реализаций, но для них они только значимые, но не полные.

5.2.7. Конечность времени тестирования: ограничения на недетерминизм

Одной из проблем тестирования (даже для конечного полного набора тестов) является бесконечность времени тестирования, которая возникает из-за недетерминизма реализации. В то же время при некоторых ограничениях на возможный недетерминизм реализаций полное тестирование может быть конечным. Например, часто ограничиваются подклассом детерминированных реализаций [39]. Другим примером может служить более широкий подкласс реализаций с ограниченным недетерминизмом [14],[15],[21].

5.2.8. Дополнительные тестовые возможности: опрос состояния реализации

До сих пор мы предполагали, что тестовые возможности не выходят за рамки машины тестирования: мы можем только нажимать кнопки (осуществлять тестовые воздействия) и наблюдать выполняемые реализацией внешние действия или наблюдаемые отказы. Дополнительные тестовые возможности могут позволить дополнительную оптимизацию тестирования.

Одним из примеров такой тестовой возможности является опрос текущего состояния реализации («status message» [36]). Разумеется, этот опрос можно формализовать в машине тестирования, введя соответствующую кнопку и действия-ответы как все возможные состояния реализации. Однако сам по себе опрос состояния мало помогает, если его тоже нужно тестировать. Поэтому обычно предполагается, что опрос состояния достоверен («reliable status message» [36]): реализация в каждом своем состоянии сообщает именно его.

Если опрос состояния реализации достоверен, удается провести полное тестирование любой конечной реализации за конечное время [1],[2],[3],[4],[5],[14],[15],[21],[31].

6. Доказательства утверждений

6.1. Доказательство теоремы 1

1. Сначала покажем, что $\mathbf{T}$ – это RTS.

1.1. $\mathbf{T}$ – это LTS.

По построению множество состояний $V_{\mathbf{T}}$ не пусто, например, содержит состояния $\{s_0\}$ и $\{\omega\}$.

Поэтому $\mathbf{T}$ – это LTS.

1.2. Детерминированность.

По построению LTS $\mathbf{T}$ – это детерминированная LTS в алфавите $\mathbf{L}\cup\mathbf{R}\cup\{\Delta\}$.

Обозначим $\varpi=\{\omega\}$.

Нам осталось показать, что для LTS $\mathbf{T}$ выполнены все свойства **R1**÷**R5** RTS-модели.

1.3. **R1** Допустимость.

В LTS $\mathbf{S_R}$ переходы по дивергенции и разрушению заканчиваются в терминальном состоянии ω, в котором не заканчиваются никакие другие переходы.

То же самое, очевидно, будет иметь место в LTS **T** для состояния $\varpi=\{\omega\}$.

1.4. **R2** Согласованность.

Переход-петля по отказу $A—R\rightarrow A$ определяется в LTS **T** тогда и только тогда, когда в LTS $\mathbf{S_R}$ в каждом состоянии $s\in A$ определен переход-петля $s—R\rightarrow s$.

Но тогда в LTS $\mathbf{S_R}$ в каждом состоянии $s\in A$ нет переходов по дивергенции, разрушению и действиям из R.

Следовательно, это имеет место и в LTS **T** для состояния A.

1.5. **R3** Конвергентность.

Пусть в LTS **T** состояние $A\neq\varpi$.

Тогда, поскольку A не пусто, в нем должно найтись состояние $s\neq\omega$.

Если в LTS **T** в состоянии A не определены переходы по дивергенции и разрушению, то в LTS $\mathbf{S_R}$ в состоянии $s\in A$ не могут начинаться трассы $\langle\gamma\rangle$ и $\langle\Delta\rangle$.

Следовательно, в LTS **S** найдется такое стабильное состояние $s`\in A$, что $s\Rightarrow s`$.

В таком состоянии $s`$ для каждого **R**-отказа R в LTS $\mathbf{S_R}$ должен быть определен переход по отказу R или по действию $z\in R$.

Тем самым, такой переход будет определен и в LTS **T** в состоянии A.

1.6. **R4** Кумулятивность.

Если в LTS **T** определен переход по отказу $A—R\rightarrow B$, то B – это непустое множество состояний из A, в которых в LTS $\mathbf{S_R}$ определены переходы-петли по отказу R.

А тогда в LTS **T** есть переход $B—R\rightarrow B$.

Если в LTS **T** в состоянии A имеется переход-петля по отказу $A—R`\rightarrow A$, то в LTS $\mathbf{S_R}$ в каждом состоянии из A определен переход-петля по отказу R, в том числе в состояниях из $B\subseteq A$.

Следовательно, в LTS **T** есть переход $B—R`\rightarrow B$.

1.7. **R5** Полнота.

Если в LTS **T** определен переход-петля по отказу $A—R\rightarrow A$, то все состояния из A стабильны в **S**.

Если в A не определены переходы по действиям из **R**-отказа $R`$, то в LTS $\mathbf{S_R}$ таких переходов нет ни в одном состоянии $s\in A$.

Следовательно, в LTS $\mathbf{S_R}$ в каждом таком состоянии $s \in A$ есть переход-петля по отказу $R`$.

Тем самым, в LTS $\mathbf{T}$ есть переход $A \text{—} R` \rightarrow A$.

2. Второе условие $\boldsymbol{T}(\mathbf{T}) = \boldsymbol{T}(\mathbf{R},\mathbf{S})$ выполнено по определению преобразования ***L2R*** как детерминизации [27] LTS $\mathbf{S_R}$, множество простых трасс которой равно множеству **R**-трасс LTS $\mathbf{S}$ по определению множества **R**-трасс LTS. Мы докажем это утверждение независимо.

2.1. Действительно, пустая трасса принадлежит как $\mathbf{T}$, так и $\mathbf{S_R}$, причем $\mathbf{T}\ \boldsymbol{after}\ \epsilon = \{\mathbf{S_R}\ \boldsymbol{after}\ \epsilon\}$.

Далее применяем индукцию.

2.2. Сначала покажем, что

если $\sigma \in \boldsymbol{T}(\mathbf{S_R}) \cap \boldsymbol{T}(\mathbf{T})$, $\sigma \cdot \langle u \rangle \in \boldsymbol{T}(\mathbf{S_R})$ и $(\mathbf{T}\ \boldsymbol{after}\ \sigma) = \{\mathbf{S_R}\ \boldsymbol{after}\ \sigma\}$,

то $\sigma \cdot \langle u \rangle \in \boldsymbol{T}(\mathbf{T})$ и $(\mathbf{T}\ \boldsymbol{after}\ \sigma \cdot \langle u \rangle) = \{\mathbf{S_R}\ \boldsymbol{after}\ \sigma \cdot \langle u \rangle\}$.

Действительно, в этом случае

$\cup((\mathbf{S_R}\ \boldsymbol{after}\ \sigma)\ \boldsymbol{after}\ \langle u \rangle) = (\mathbf{S_R}\ \boldsymbol{after}\ \sigma \cdot \langle u \rangle) \neq \varnothing$,

что влечет наличие в LTS $\mathbf{T}$ перехода $(\mathbf{S_R}\ \boldsymbol{after}\ \sigma) \text{—} u \rightarrow \cup((\mathbf{S_R}\ \boldsymbol{after}\ \sigma)\ \boldsymbol{after}\ \langle u \rangle) = (\mathbf{S_R}\ \boldsymbol{after}\ \sigma \cdot \langle u \rangle)$.

Отсюда и из детерминизма LTS $\mathbf{T}$ имеем $\sigma \cdot \langle u \rangle \in \boldsymbol{T}(\mathbf{T})$ и $(\mathbf{T}\ \boldsymbol{after}\ \sigma \cdot \langle u \rangle) = \{\mathbf{S_R}\ \boldsymbol{after}\ \sigma \cdot \langle u \rangle\}$, что и требовалось доказать.

2.3. Теперь покажем, что

если $\sigma \in \boldsymbol{T}(\mathbf{S_R}) \cap \boldsymbol{T}(\mathbf{T})$, $\sigma \cdot \langle u \rangle \in \boldsymbol{T}(\mathbf{T})$ и $(\mathbf{T}\ \boldsymbol{after}\ \sigma) = \{\mathbf{S_R}\ \boldsymbol{after}\ \sigma\}$,

то $\sigma \cdot \langle u \rangle \in \boldsymbol{T}(\mathbf{S_R})$ и $(\mathbf{T}\ \boldsymbol{after}\ \sigma \cdot \langle u \rangle) = \{\mathbf{S_R}\ \boldsymbol{after}\ \sigma \cdot \langle u \rangle\}$.

Действительно, в этом случае в LTS $\mathbf{T}$ есть переход $(\mathbf{S_R}\ \boldsymbol{after}\ \sigma) \text{—} u \rightarrow \cup((\mathbf{S_R}\ \boldsymbol{after}\ \sigma)\ \boldsymbol{after}\ \langle u \rangle) = (\mathbf{S_R}\ \boldsymbol{after}\ \sigma \cdot \langle u \rangle)$,

что влечет $(\mathbf{S_R}\ \boldsymbol{after}\ \sigma \cdot \langle u \rangle) \neq \varnothing$.

Отсюда $\sigma \cdot \langle u \rangle \in \boldsymbol{T}(\mathbf{S_R})$, и в силу детерминизма LTS $\mathbf{T}$ имеем $(\mathbf{T}\ \boldsymbol{after}\ \sigma \cdot \langle u \rangle) = \{\mathbf{S_R}\ \boldsymbol{after}\ \sigma \cdot \langle u \rangle\}$, что и требовалось доказать.

3. Покажем, что RTS $\mathbf{T}$ имеет конечное число состояний, если LTS $\mathbf{S}$ имеет конечное число состояний.

Действительно, если LTS $\mathbf{S}$ имеет $|V_S| = n$ состояний,

то LTS $\mathbf{S_R}$ имеет $|V_S \cup \{\omega\}| = n+1$ состояние,

и LTS $\mathbf{T}$ имеет $|V_T| = |\mathcal{P}(V_S \cup \{\omega\}) \setminus \{\varnothing\}| = 2^{n+1}-1$ состояний.

6.2. Доказательство теоремы 2

1. Сначала покажем, что $\mathbf{S}$ – это LTS.

   Для этого достаточно показать, что множество ее состояний не пусто.

   А это следует из того, что $V_S = (V_T \cup \{\varepsilon\}) \setminus \{\varpi\}$, а $\varepsilon \neq \varpi$ (так как $\varpi \in V_T$ и $\varepsilon \notin V_T$).

2. Теперь покажем, что $T(\mathbf{R},\mathbf{S}) = \cup d(T(\mathbf{T}))$.

2.1. Сначала покажем, что $T(\mathbf{R},\mathbf{S}) \supseteq \cup d(T(\mathbf{T}))$.

Поскольку множество $\mathbf{R}$-трасс $T(\mathbf{R},\mathbf{S})$ замкнуто по операции d, достаточно показать, что $T(\mathbf{R},\mathbf{S}) \supseteq T(\mathbf{T})$.

Мы покажем, что, кроме того, для каждой трассы $\sigma \in T(\mathbf{T})$, не заканчивающейся дивергенцией и разрушением, имеет место $(\mathbf{T}\ \textit{after}\ \sigma) \subseteq (\mathbf{S}\ \textit{after}\ \sigma)$.

Будем вести доказательство индукцией по простой трассе RTS $\mathbf{T}$.

Пустая трасса ϵ, очевидно, имеется в LTS $\mathbf{S}$.

Поскольку в RTS $t_0 \Rightarrow t_0$, по правилам вывода в LTS $\varepsilon \text{—}\tau\text{→} t_0$,

что влечет $\{t_0\} \subseteq (\mathbf{S}\ \textit{after}\ \epsilon)$.

Поскольку RTS $\mathbf{T}$ детерминирована, $(\mathbf{T}\ \textit{after}\ \epsilon) = \{t_0\}$.

Следовательно, $(\mathbf{T}\ \textit{after}\ \epsilon) \subseteq (\mathbf{S}\ \textit{after}\ \epsilon)$.

Пусть $\sigma \cdot \langle u \rangle \in T(\mathbf{T})$ и для любой трассы $\mu < \sigma \cdot \langle u \rangle$ трасса $\mu \in T(\mathbf{R},\mathbf{S})$ и $(\mathbf{T}\ \textit{after}\ \mu) \subseteq (\mathbf{S}\ \textit{after}\ \mu)$.

Нужно показать, что $\sigma \cdot \langle u \rangle \in T(\mathbf{R},\mathbf{S})$ и

если $u \neq \gamma$ и $u \neq \Delta$, то $(\mathbf{T}\ \textit{after}\ \sigma \cdot \langle u \rangle) \subseteq (\mathbf{S}\ \textit{after}\ \sigma \cdot \langle u \rangle)$.

2.1.1. Пусть $u = \gamma$. Нужно показать, что $\sigma \cdot \langle \gamma \rangle \in T(\mathbf{R},\mathbf{S})$.

В силу детерминизма RTS имеется состояние A такое, что $\{A\} = (\mathbf{T}\ \textit{after}\ \sigma)$.

Тогда в RTS $A \text{—}\gamma\text{→} \varpi$.

Поскольку по предположению шага индукции $A \in (\mathbf{S}\ \textit{after}\ \sigma)$,

по правилам вывода в LTS $A \text{—}\gamma\text{→} A$,

что влечет $\sigma \cdot \langle \gamma \rangle \in T(\mathbf{R},\mathbf{S})$.

2.1.2. Пусть $u = \Delta$. Нужно показать, что $\sigma \cdot \langle \Delta \rangle \in T(\mathbf{R},\mathbf{S})$.

В силу детерминизма RTS имеется состояние A такое, что $\{A\}=(\mathbf{T}\ \textit{after}\ \sigma)$.

Тогда в RTS $A\text{—}\Delta\rightarrow\varpi$.

Поскольку по предположению шага индукции $A\in(\mathbf{S}\ \textit{after}\ \sigma)$,

по правилам вывода в LTS $A\text{—}\tau\rightarrow A$,

что влечет $\sigma\cdot\langle\Delta\rangle\in\boldsymbol{T}(\mathbf{R},\mathbf{S})$.

2.1.3. Пусть $u\in\mathbf{L}$.

Нужно показать, что $\sigma\cdot\langle u\rangle\in\boldsymbol{T}(\mathbf{R},\mathbf{S})$ и $(\mathbf{T}\ \textit{after}\ \sigma\cdot\langle u\rangle)\subseteq(\mathbf{S}\ \textit{after}\ \sigma\cdot\langle u\rangle)$.

В силу детерминизма RTS имеется состояние A такое, что $\{A\}=(\mathbf{T}\ \textit{after}\ \sigma)$.

Тогда в RTS $A\text{—}u\rightarrow$, то есть существует состояние B такое, что $A\text{—}u\rightarrow B$.

Поскольку по предположению шага индукции $A\in(\mathbf{S}\ \textit{after}\ \sigma)$,

по правилам вывода в LTS $A\text{—}u\rightarrow B$,

что влечет $\{B\}=(\mathbf{T}\ \textit{after}\ \sigma\cdot\langle u\rangle)\subseteq(\mathbf{S}\ \textit{after}\ \sigma\cdot\langle u\rangle)$ и $\sigma\cdot\langle u\rangle\in\boldsymbol{T}(\mathbf{R},\mathbf{S})$.

2.1.4. Пусть $u\in\mathbf{R}$.

В силу детерминизма RTS имеется состояние C такое, что $\{C\}=(\mathbf{T}\ \textit{after}\ \sigma)$.

Тогда в RTS $C\text{—}u\rightarrow$, то есть существует состояние D такое, что $C\text{—}u\rightarrow D$.

Трассу σ можно представить в виде $\sigma=\mu\cdot\boldsymbol{p}_{ost}(\sigma)$.

В силу детерминизма RTS имеется состояние B такое, что $\{B\}=(\mathbf{T}\ \textit{after}\ \mu)$.

Тогда в RTS $B=\boldsymbol{p}_{ost}(\sigma)\Rightarrow C$ (если $\boldsymbol{p}_{ost}(\sigma)=\epsilon$, то $B=C$).

Следовательно, в RTS $B=\boldsymbol{p}_{ost}(\sigma)\cdot\langle u\rangle\Rightarrow D$, и в силу детерминизма RTS $\{D\}=(\mathbf{T}\ \textit{after}\ \sigma\cdot\langle u\rangle)$.

По предположению шага индукции $\{B\}=(\mathbf{T}\ \textit{after}\ \mu)\subseteq(\mathbf{S}\ \textit{after}\ \mu)$ и $\mu\in\boldsymbol{T}(\mathbf{R},\mathbf{S})$.

По кумулятивности RTS для каждого отказа $P \in \boldsymbol{Ip}(\sigma \cdot \langle u \rangle)$ в RTS имеет место $D \text{—} P \rightarrow D$,

что по правилам вывода влечет в LTS стабильность состояния D.

По согласованности RTS для каждого отказа $P \in \boldsymbol{Ip}(\sigma \cdot \langle u \rangle)$ и каждого действия $z \in P$ в RTS имеет место $D \text{—} z \not\rightarrow$,

что влечет $D = \langle z \cdot \rho \rangle \not\Rightarrow$ для каждого $\rho \in \mathbf{R}^*$.

Отсюда по правилам вывода в LTS в состоянии D порождаются все отказы $P \in \boldsymbol{Ip}(\sigma \cdot \langle u \rangle)$,

то есть в LTS $D = \boldsymbol{p}_{ost}(\sigma) \cdot \langle u \rangle \Rightarrow D$.

2.1.4.1. Пусть $\mu = \epsilon$.

Тогда $B = t_0$ и, следовательно, в RTS $t_0 = \boldsymbol{p}_{ost}(\sigma) \cdot \langle u \rangle \Rightarrow D$,

что по правилам вывода влечет в LTS $\varepsilon \text{—} \tau \rightarrow D$.

Отсюда в LTS, поскольку $D = \boldsymbol{p}_{ost}(\sigma) \cdot \langle u \rangle \Rightarrow D$,

имеем $\{D\} = (\mathbf{T}\ \boldsymbol{after}\ \sigma \cdot \langle u \rangle) \subseteq (\mathbf{S}\ \boldsymbol{after}\ \sigma \cdot \langle u \rangle)$ и $\sigma \cdot \langle u \rangle \in \boldsymbol{T}(\mathbf{R},\mathbf{S})$.

2.1.4.2. Пусть $\mu \neq \epsilon$.

Тогда трассу μ можно представить в виде $\mu = \lambda \cdot \langle z \rangle$, где $z \in \mathbf{L}$,

что влечет для некоторого состояния A в RTS $t_0 = \lambda \Rightarrow A$ и $A \text{—} z \rightarrow B$,

что, поскольку в RTS $B = \boldsymbol{p}_{ost}(\sigma) \cdot \langle u \rangle \Rightarrow D$,

влечет в RTS $A = \langle z \rangle \cdot \boldsymbol{p}_{ost}(\sigma) \cdot \langle u \rangle \Rightarrow D$.

Отсюда в LTS по предположению шага индукции $\varepsilon = \lambda \Rightarrow A$,

по правилам вывода $A \text{—} z \rightarrow D$,

что влечет $\varepsilon = \lambda \cdot \langle z \rangle \Rightarrow D$.

А тогда в LTS, поскольку $D = \boldsymbol{p}_{ost}(\sigma) \cdot \langle u \rangle \Rightarrow D$,

имеем $\{D\} = (\mathbf{T}\ \boldsymbol{after}\ \sigma \cdot \langle u \rangle) \subseteq (\mathbf{S}\ \boldsymbol{after}\ \sigma \cdot \langle u \rangle)$ и $\sigma \cdot \langle u \rangle \in \boldsymbol{T}(\mathbf{R},\mathbf{S})$.

2.2. Теперь покажем, что $\boldsymbol{T}(\mathbf{R},\mathbf{S}) \subseteq \cup \boldsymbol{d}(\boldsymbol{T}(\mathbf{T}))$.

Пустая трасса ϵ имеется в RTS и, следовательно, $\epsilon \in \cup \boldsymbol{d}(\boldsymbol{T}(\mathbf{T}))$.

По правилам вывода в LTS только пустая трасса ϵ заканчивается в состоянии ε. Поэтому нам достаточно доказать, что для любой трассы

$\mu\in\boldsymbol{T}(\mathbf{R},\mathbf{S})$, заканчивающаяся в LTS в состоянии $s\neq\varepsilon$, найдется такая простая трасса σ RTS, что $\mu\in\boldsymbol{d}(\sigma)$. Мы докажем более сильное утверждение, дополнительно потребовав, чтобы трасса σ в RTS тоже заканчивалась в состоянии s.

Будем вести доказательство индукцией по трассе LTS $\mathbf{S}$.

По правилам вывода в LTS пустая трасса ϵ заканчивается в состоянии $s\neq\varepsilon$ только тогда, когда в RTS $t_0=\rho\Rightarrow s$, где $\rho\in\mathbf{R}^*$.

Имеем: $\rho\in\boldsymbol{T}(\mathbf{T})$, $s\in(\mathbf{T}\ \boldsymbol{after}\ \rho)$ и $\epsilon\in\boldsymbol{d}(\rho)$.

По правилам вывода в LTS в состоянии ε заканчивается только пустая трасса. Поэтому нам достаточно показать следующее:

Если $\mu\cdot\langle u\rangle\in\boldsymbol{T}(\mathbf{R},\mathbf{S})$, $\mu\in\cup\boldsymbol{d}(\boldsymbol{T}(\mathbf{T}))$

и $\forall s\in(\mathbf{S}\ \boldsymbol{after}\ \mu)\backslash\{\varepsilon\}\ \exists\sigma\in\boldsymbol{T}(\mathbf{T})\ \{s\}=(\mathbf{T}\ \boldsymbol{after}\ \sigma)\ \&\ \mu\in\boldsymbol{d}(\sigma)$,

то $\sigma\cdot\langle u\rangle\in\boldsymbol{T}(\mathbf{T})$ и, если $u\neq\gamma$ и $u\neq\Delta$,

то $\forall s_u\in(\mathbf{S}\ \boldsymbol{after}\ \mu\cdot\langle u\rangle)\ \exists\sigma_u\in\boldsymbol{T}(\mathbf{T})\ \{s_u\}=(\mathbf{T}\ \boldsymbol{after}\ \sigma_u)\ \&$ $\mu\cdot\langle u\rangle\in\boldsymbol{d}(\sigma_u)$.

2.2.1. Пусть $u=\gamma$. Нужно показать, что $\sigma\cdot\langle\gamma\rangle\in\boldsymbol{T}(\mathbf{T})$.

Имеем для некоторого состояния $s\in(\mathbf{S}\ \boldsymbol{after}\ \mu)\backslash\{\varepsilon\}$ в LTS $s\text{—}\gamma\rightarrow$.

По предположению шага индукции найдется трасса $\sigma\in\boldsymbol{T}(\mathbf{T})$ такая, что $\{s\}=(\mathbf{T}\ \boldsymbol{after}\ \sigma)$ и $\mu\in\boldsymbol{d}(\sigma)$.

Тогда по правилам вывода в RTS $s\text{—}\gamma\rightarrow$,

что влечет $\sigma\cdot\langle\gamma\rangle\in\boldsymbol{T}(\mathbf{T})$.

2.2.2. Пусть $u=\Delta$. Нужно показать, что $\sigma\cdot\langle\Delta\rangle\in\boldsymbol{T}(\mathbf{T})$.

Действительно, в LTS некоторое состояние $s\in(\mathbf{S}\ \boldsymbol{after}\ \mu)\backslash\{\varepsilon\}$ дивергентно, то есть в нем начинается бесконечная цепочка τ-переходов.

В LTS τ-переход из состояния, отличного от ε, порождается двумя правилами:

1) $A=\rho\Rightarrow B\ \&\ \rho\neq\epsilon\ \&\ \forall R\in\mathbf{R}\ A=\langle R\rangle\not\Rightarrow A$, 2) $A\text{—}\Delta\rightarrow\varpi$.

2.2.2.1. Правило 1: $A=\rho\Rightarrow B\ \&\ \rho\neq\epsilon\ \&\ \forall R\in\mathbf{R}\ A=\langle R\rangle\not\Rightarrow A$.

Тогда, поскольку $\rho \neq \epsilon$, найдется такой **R**-отказ R,

что по кумулятивности RTS $B \text{—} R \rightarrow B$,

а тогда по правилам вывода в LTS из состояния B нет τ-переходов.

Поэтому τ-переход бесконечной цепочки не может образоваться по первому правилу.

2.2.2.2. Правило 2: $A \text{—} \Delta \rightarrow \varpi$.

По согласованности RTS переход по дивергенции может быть только таком состоянии A, в котором нет петель по отказам.

А тогда по кумулятивности RTS в состоянии A не заканчиваются никакие переходы по отказам,

что для LTS означает, что в состоянии A не заканчиваются никакие τ-переходы, кроме τ-петли.

Отсюда $A=s$ и $s \text{—} \Delta \rightarrow \varpi$.

По предположению шага индукции найдется трасса $\sigma \in \boldsymbol{T}(\mathbf{T})$ такая,

что $\{s\}=(\mathbf{T}\ \boldsymbol{after}\ \sigma)$ и $\mu \in \boldsymbol{d}(\sigma)$.

Имеем $\sigma \cdot \langle \Delta \rangle \in \boldsymbol{T}(\mathbf{T})$.

2.2.3. Пусть $u \in \mathbf{L}$.

Нужно показать, что $\sigma \cdot \langle u \rangle \in \boldsymbol{T}(\mathbf{T})$ и

$\forall s_u \in (\mathbf{S}\ \boldsymbol{after}\ \mu \cdot \langle u \rangle)\ \exists \sigma_u \in \boldsymbol{T}(\mathbf{T})\ \{s_u\}=(\mathbf{T}\ \boldsymbol{after}\ \sigma_u)\ \&\ \mu \cdot \langle u \rangle \in \boldsymbol{d}(\sigma_u)$.

Действительно, для некоторого состояния $s \in (\mathbf{S}\ \boldsymbol{after}\ \mu) \setminus \{\varepsilon\}$ в LTS $s \text{—} u \rightarrow s_u$.

По предположению шага индукции найдется трасса $\sigma \in \boldsymbol{T}(\mathbf{T})$ такая, что $\{s\}=(\mathbf{T}\ \boldsymbol{after}\ \sigma)$ и $\mu \in \boldsymbol{d}(\sigma)$.

Тогда по правилам вывода в RTS $s=\langle u \rangle \cdot \rho \Rightarrow s_u$,

что влечет $\sigma \cdot \langle u \rangle \in \boldsymbol{T}(\mathbf{T})$, $\sigma_u=\sigma \cdot \langle u \rangle \cdot \rho \in \boldsymbol{T}(\mathbf{T})$, $\{s_u\}=(\mathbf{T}\ \boldsymbol{after}\ \sigma_u)$ и $\mu \cdot \langle u \rangle \in \boldsymbol{d}(\sigma_u)$.

2.2.4. Пусть $u \in \mathbf{R}$.

Тогда для некоторого состояния $s \in (\mathbf{S}\ \boldsymbol{after}\ \mu) \setminus \{\varepsilon\}$ в LTS $s=\langle u \rangle \Rightarrow s_u$, где $s_u=s$, то есть $s \text{—} \tau \not\rightarrow$ & $\forall z \in u\ \ s \text{—} z \not\rightarrow$.

По предположению шага индукции найдется трасса $\sigma \in \boldsymbol{T}(\mathbf{T})$ такая, что $\{s\}=(\mathbf{T}\ \boldsymbol{after}\ \sigma)$ и $\mu \in \boldsymbol{d}(\sigma)$.

Поскольку в LTS $\forall z \in u\ \ s \text{—} z \not\rightarrow$,

по правилам вывода в RTS $\forall z \in u\ \ s \text{—} z \not\rightarrow$.

В RTS по конвергентности $s \text{—} u \rightarrow s`$.

Если бы в RTS в состоянии s не было петель по отказам,

то по правилам вывода в LTS был бы переход $s \text{—} \tau \rightarrow s`$, что не верно.

Значит в RTS в состоянии s есть петля по отказу,

а тогда, поскольку в RTS $\forall z \in u\ \ s \text{—} z \not\rightarrow$,

по полноте RTS $s = s`$.

В результате в RTS $s \text{—} u \rightarrow s$,

что влечет $\sigma \cdot \langle u \rangle \in \boldsymbol{T}(\mathbf{T})$, $\sigma_u = \sigma \cdot \langle u \rangle \in \boldsymbol{T}(\mathbf{T})$, $\{s_u\} = \{s\} = (\mathbf{T}\ \textbf{\textit{after}}\ \sigma_u)$ и $\mu \cdot \langle u \rangle \in \boldsymbol{d}(\sigma_u)$.

3. Покажем, что если $\mathbf{T}$ имеет конечное число состояний, то LTS $\mathbf{S}$ имеет такое же число состояний.

   Пусть RTS $\mathbf{T}$ имеет конечное число $|V_T| = n$ состояний.

   Тогда по определению LTS $\mathbf{S}$ имеет такое же $|(V_T \cup \{\varepsilon\}) \setminus \{\varpi\}| = n$ число состояний.

6.3. Доказательство теоремы 3

1. По определению ∇-пополнения все безопасные **L**-трассы ∇-пополнения после приведения к алфавиту $\mathbf{L}$ ∇-конформны и, следовательно, конформны для исходной тройки $\mathbf{T}$.

   А, поскольку $\mathbf{T_i} \in \nabla(\mathbf{T})_\mathbf{L}$, такие трассы **L**-конформны для $\mathbf{T_i}$.

   Отсюда непосредственно следует, что все **L**-ошибки являются первичными **L**-ошибками 1-го рода.

2. По доказанному **L**-ошибка является первичной **L**-ошибкой в ∇-пополнении.

   А тогда, поскольку ∇-пополнение принадлежит **L**-конусу исходной спецификации, эта ошибка является первичной ∇-ошибкой.

3. Тестовая **L**-трасса – это безопасная **L**-трасса или **L**-ошибка 1-го рода.

   Поскольку безопасная **L**-трасса ∇-пополнения ∇-конформна,

   она является ∇-тестовой трассой.

   Также по доказанному **L**-ошибка 1-го рода является первичной ∇-ошибкой и, следовательно, является ∇-тестовой трассой.

   Тем самым тестовая **L**-трасса является первичной ∇-тестовой трассой.

6.4. Доказательство теоремы 4

Действительно, если для исходной тройки $\mathbf{T}$ нет конформных реализаций, то пустая трасса определяется исходной тройкой как первичная ошибка 2-го рода.

Поскольку $\mathbf{T}\in\nabla(\mathbf{T})_{\mathbf{L}}$, в ∇-пополнении, если бы оно существовало, пустая трасса должна была бы быть ошибкой.

А тогда по теореме 3 (утверждение 1) пустая трасса должна была бы быть ошибкой 1-го рода, что невозможно для пустой трассы.

6.5. Доказательство теоремы 5

Конформная реализация существует, например, ею является реализация $\mathbf{I_0}$.

Допустим, что существует спецификационная тройка $\mathbf{T_i}=(\mathbf{R/Q},\Sigma_i,\textit{safe by}_i)$ такая, что в спецификации Σ_i все безопасные трассы конформны и $\mathbf{T_6} \le_L \mathbf{T_i}$.

1. Покажем, что $\epsilon\in\textit{SafeBy}(\mathbf{T_i})$ и $\varnothing\ \textit{safe by}_i\ \Sigma_i\ \textit{after}\ \epsilon$.

   Допустим, это не так.

   Рассмотрим реализацию $\mathbf{I_1}$.

   Поскольку $\varnothing\ \textit{safe by}\ \Sigma_6\ \textit{after}\ \epsilon$, но $\varnothing\ \textit{safe in}\ F(\mathbf{I_1})\ \textit{after}\ \epsilon$, имеем $F(\mathbf{I_1})\ \textit{safe for}\ \Sigma_6$.

   Следовательно, $F(\mathbf{I_1})\ \textit{saco}\ \Sigma_6$.

   По допущению возможны два варианта.

1.1. Пустая трасса опасна в Σ_i, то есть $\epsilon\notin\textit{SafeBy}(\mathbf{T_i})$.

   Тогда все реализации конформны спецификации Σ_i, в том числе $F(\mathbf{I_1})\ \textit{saco}\ \Sigma_i$, что противоречит $\mathbf{T_6} \le_L \mathbf{T_i}$.

1.2. Пустая трасса безопасна $\epsilon\in\textit{SafeBy}(\mathbf{T_i})$, но после нее в Σ_i опасна пустая кнопка $\varnothing\ \textit{safe by}_i\ \Sigma_i\ \textit{after}\ \epsilon$.

   Тогда после пустой трассы в Σ_i опасны все кнопки, и тогда конформны все реализации, в которых нет разрушения с самого начала, в том числе $F(\mathbf{I_1})\ \textit{saco}\ \Sigma_i$, что противоречит $\mathbf{T_6} \le_L \mathbf{T_i}$.

Единственным наблюдением, возможным после пустой **R**-кнопки является пустой отказ. Поэтому $\varnothing\ \textit{safe by}_i\ \Sigma_i\ \textit{after}\ \epsilon$ влечет $\langle\varnothing\rangle\in\textit{SafeBy}(\mathbf{T_i})$.

2. Покажем, что $\{x\}\ \textit{safe by}_i\ \Sigma_i\ \textit{after}\ \epsilon$ и $\{x\}\ \textit{safe by}_i\ \Sigma_i\ \textit{after}\ \langle\varnothing\rangle$.

   Допустим, это не так.

   Рассмотрим реализацию $\mathbf{I_2}$.

   Имеем $F(\mathbf{I_2})\ \textit{safe for}\ \Sigma_6$.

   Но по допущению $F(\mathbf{I_2})\ \textit{safe for}\ \Sigma_i$, что противоречит $\mathbf{T_6} \le_L \mathbf{T_i}$.

3. Покажем, что δ ***safe by***$_i$ $\mathbf{\Sigma_i}$ ***after*** $\langle\varnothing\rangle$.

   Допустим, это не так.

   Тогда, так как δ **R**-кнопка, в $\mathbf{\Sigma_i}$ должна быть трасса $\langle\varnothing,\mathtt{y},\gamma\rangle$,

   что по замкнутости модели влечет наличие трассы $\langle\mathtt{y},\gamma\rangle$,

   то есть δ ~~***safe by***$_i$~~ $\mathbf{\Sigma_i}$ ***after*** ϵ.

   Рассмотрим реализацию $\mathbf{I_3}$.

   Поскольку δ ***safe by*** $\mathbf{\Sigma_6}$ ***after*** ϵ, но δ ~~***safe in***~~ $\boldsymbol{F}(\mathbf{I_3})$ ***after*** ϵ, имеем $\boldsymbol{F}(\mathbf{I_3})$ ~~***safe for***~~ $\mathbf{\Sigma_6}$.

   Но, поскольку по допущению δ ~~***safe by***~~$_i$ $\mathbf{\Sigma_i}$ ***after*** $\langle\varnothing\rangle$ и по следствию из допущения δ ~~***safe by***~~$_i$ $\mathbf{\Sigma_i}$ ***after*** ϵ, $\boldsymbol{F}(\mathbf{I_3})$ ***saco*** $\mathbf{\Sigma_i}$, что противоречит $\mathbf{T_6} \le_L \mathbf{T_i}$.

4. Покажем, что $\mathtt{y} \notin \boldsymbol{obs}(\langle\varnothing\rangle,\delta,\mathbf{\Sigma_i})$.

   Допустим, это не так.

   Тогда в $\mathbf{\Sigma_i}$ есть трасса $\langle\mathtt{y}\rangle$.

   Но поскольку $\mathbf{\Sigma_i}$ ∇-пополнение, в ней нет неконформных трасс, следовательно, трасса $\langle\mathtt{y}\rangle$ должна быть конформна в $\mathbf{\Sigma_i}$, то есть встречаться в некоторой конформной $\mathbf{\Sigma_i}$ реализации **I**.

   Поскольку в $\mathbf{S_5}$ все трассы неконформны, трасса $\langle\mathtt{y}\rangle$ неконформна в $\mathbf{\Sigma_6}$.

   Но тогда реализация **I** неконформна $\mathbf{\Sigma_6}$, что противоречит $\mathbf{T_6} \le_L \mathbf{T_i}$.

Тем самым, единственным наблюдением, возможным в $\mathbf{\Sigma_i}$ после трассы $\langle\varnothing\rangle$ при нажатии **R**-кнопки δ является отказ δ.

Поэтому $\langle\varnothing,\delta\rangle \in \boldsymbol{SafeBy}(\mathbf{T_i})$.

5. Покажем, что $\{\mathtt{x}\}$ ***safe by***$_i$ $\mathbf{\Sigma_i}$ ***after*** $\langle\varnothing,\delta\rangle$.

   Допустим, это не так.

   Рассмотрим реализацию $\mathbf{I_4}$.

   Поскольку $\{\mathtt{x}\}$ ***safe by*** $\mathbf{\Sigma_6}$ ***after*** $\langle\delta\rangle$, но $\{\mathtt{x}\}$ ~~***safe in***~~ $\boldsymbol{F}(\mathbf{I_4})$ ***after*** $\langle\delta\rangle$, имеем $\boldsymbol{F}(\mathbf{I_4})$ ~~***safe for***~~ $\mathbf{\Sigma_6}$.

Но, поскольку по п.2 $\{x\}$ ***safe by***$_i$ Σ_i ***after*** ϵ и $\{x\}$ ***safe by***$_i$ Σ_i ***after*** $\langle\varnothing\rangle$ и по допущению $\{x\}$ ***safe by***$_i$ Σ_i ***after*** $\langle\varnothing,\delta\rangle$, $F(\mathbf{I}_4)$ ***saco*** Σ_i, что противоречит $\mathbf{T}_6 \le_L \mathbf{T}_i$.

Поскольку $\{x\}$ **Q**-кнопка, из ее безопасности после трассы $\langle\varnothing,\delta\rangle$ следует (по 3-ему правилу для ***safe by***) наличие в Σ_i трассы $\langle\varnothing,\delta,x\rangle$ и отсутствие трассы $\langle\varnothing,\delta,x,\gamma\rangle$.

В то же время, поскольку действие x разрешается только **Q**-кнопкой $\{x\}$, доказанное в п. 2 условие $\{x\}$ ***safe by***$_i$ Σ_i ***after*** $\langle\varnothing\rangle$ влечет

либо 1) отсутствие трассы $\langle\varnothing,x\rangle$,

либо 2) наличие трассы $\langle\varnothing,x,\gamma\rangle$.

Первое по замкнутости трассовой модели противоречит наличию в Σ_i трассы $\langle\varnothing,\delta,x\rangle$.

Второе, поскольку трасса $\langle\varnothing\rangle$ не продолжается по п.4 реакциями (y) из кнопки δ, влечет по полноте трассовой модели наличие трассы $\langle\varnothing,\delta,x,\gamma\rangle$, что противоречит отсутствию этой трассы в Σ_i.

Мы пришли к противоречию, и, следовательно, для спецификационной тройки $\mathbf{T}_6$ не существует спецификационная тройка $\mathbf{T}_i=(\mathbf{R}/\mathbf{Q},\Sigma_i,$***safe by***$_i)$ такая, что спецификация Σ_i не содержит неактуальных и неконформных трасс и $\mathbf{T}_6 \le_L \mathbf{T}_i$.

6.6. Доказательство теоремы 6

Пример на Рис. 15. слева легко применяется для любой семантики, в которой

1) есть хотя бы две **R**-кнопки $R_1 \neq R_2$ и

2) хотя бы одна **Q**-кнопка Q, разрешающая действие $x \notin R_1 \cup R_2$.

Достаточно через y обозначить действие, которое разрешается одной из этих **R**-кнопок (для определенности, R_2) и не разрешается другой **R**-кнопкой (соответственно, R_1).

Тогда в доказательстве теоремы 5 вместо отказа $\{x\}$ пишем кнопку Q, вместо отказа $\varnothing$ – отказ R_1, а вместо отказа δ – отказ R_2.

6.7. Доказательство теоремы 7

Для примера на Рис. 15. слева существует ∇-пополнение (на Рис. 15. справа) $\mathbf{T}_6\text{`}=(\mathbf{R}\text{`}/\mathbf{Q}\text{`},F(\mathbf{S}_6\text{`}),$***safe by***`$)$ в расширенном алфавите $\mathbf{L}\text{`}=\mathbf{L}\cup\{a\}$ и расширенной семантике, в которой **R**-отказ δ заменяется на отказ $\delta\cup\{a\}$: $\mathbf{R}\text{`}=\{\delta\cup\{a\},\varnothing\}$, $\mathbf{Q}\text{`}=\mathbf{Q}=\{\{x\}\}$, где $\delta=\{y\}$.

Спецификационная модель ∇-пополнения $\mathbf{S_6}$`. В этой модели есть трасса ⟨∅,x,γ⟩, которая не может встречаться в конформных реализациях, поскольку в таких реализациях после пустого отказа обязательно должен быть отказ δ, а после него действие x должно быть безопасно.

Покажем, что эта ситуация имеет место для любого ∇-пополнения $\mathbf{T_i}$.

Для тройки $\mathbf{T_i}$ рассмотрим реализации $\mathbf{I_2}$ и $\mathbf{I_4}$ в алфавите $\mathbf{L_i}$.

После приведения к алфавиту **L** они становятся реализациями для исходной тройки.

В $\mathbf{T_i}$ действие x должно быть опасным после трассы ⟨∅⟩, так как в противном случае реализация $\mathbf{I_2}$ не будет безопасно-тестируемой для $\mathbf{T_i}$, но реализация $\mathbf{I_{2L}}$ безопасно-тестируема для исходной тройки $\mathbf{T_6}$, что противоречит не сужению класса безопасно-тестируемых **L**-реализаций при ∇-пополнении.

Также в $\mathbf{T_i}$ действие x должно быть безопасно после трассы ⟨δ⟩, так как иначе реализация $\mathbf{I_4}$ будет конформна для $\mathbf{T_i}$, но реализация $\mathbf{I_{4L}}$ не безопасно-тестируема и, следовательно, не конформна для $\mathbf{T_6}$, что противоречит сохранению класса конформных **L**-реализаций при ∇-пополнении.

Но тогда, поскольку в $\mathbf{T_6}$ действие x разрешается единственной **Q**-кнопкой {x}, в $\mathbf{T_i}$ действие x должно разрешаться только такими **Q**-кнопками Q, что Q∩**L**={x}. Поэтому в $\mathbf{T_i}$ должна быть трасса ⟨δ,x⟩, что влечет в ней наличие трассы ⟨∅,x⟩.

Следовательно, поскольку в $\mathbf{T_i}$ действие x опасно после трассы ⟨∅⟩, оно разрушающее после трассы ⟨∅⟩, то есть в $\mathbf{T_i}$ имеется трасса ⟨∅,x,γ⟩.

Но эта опасная трасса отсутствует в любой реализации конформной исходной тройке $\mathbf{T_6}$.

6.8. Доказательство леммы 1

1. Достаточность.

   Пусть $\mu \in \boldsymbol{p_{re}di}^{\sim}(\sigma)$.

   Поскольку $\boldsymbol{p_{re}di}^{\sim}(\sigma) \subseteq \boldsymbol{p_{re}di}(\sigma)$, а модель $\boldsymbol{p_{re}di}$-замкнута, достаточность условия доказана.

2. Необходимость.

Если трасса σ не является допустимой и согласованной трассой, то никакая модель не содержит трассу σ, и утверждение леммы очевидно.

Пусть трасса σ допустима и согласована, но $\mu \notin \boldsymbol{p_{re}di}^{\sim}(\sigma)$.

Нам достаточно построить LTS-модель $\mathbf{I}$, в которой будет трасса σ и не будет трассы μ.

Возьмем за основу LTS-модель $\mathbf{I}(\sigma)$.

Трассу μ можно представить в виде $\mu=\mu_1 \cdot \langle u \rangle \cdot \mu_2$,

где μ_1 максимальный префикс трассы μ, принадлежащий $\boldsymbol{p_{re}di}^{\sim}(\sigma)$

(такой префикс всегда существует, так как $\epsilon \in \boldsymbol{p_{re}di}^{\sim}(\sigma)$).

Поскольку дивергенция и разрушение могут быть только в конце допустимой трассы σ, из условия $\mu_1 \in \boldsymbol{p_{re}di}^{\sim}(\sigma)$ следует, что, если трасса μ_1 заканчивается дивергенцией или разрушением, то трасса $\mu=\mu_1 \cdot \langle u \rangle \cdot \mu_2$ не допустима (после дивергенции или разрушения имеется наблюдение u). А такой трассы не может быть в модели, в частности, ее нет в модели $\mathbf{I}(\sigma)$, и утверждение доказано.

В дальнейшем будем считать, что трасса μ_1 не заканчивается дивергенцией или разрушением.

Пусть подтрасса действий трассы μ_1 имеет длину i.

Тогда трасса μ_1 заканчивается в LTS $\mathbf{I}(\sigma)$ в состоянии $\sigma^{\wedge i}$ и, поскольку LTS по построению детерминирована (в каждом состоянии определено не более одного перехода по каждому действию, и нет τ-переходов, кроме, быть может, τ-петли), только в этом состоянии.

Рассмотрим все возможные случаи в зависимости от того, каким наблюдением является наблюдение u. В каждом из этих случаев мы при необходимости так модифицируем LTS, чтобы она, во-первых, по-прежнему содержала трассу σ, во-вторых, трасса μ_1 по-прежнему заканчивалась в состоянии $\sigma^{\wedge i}$, и, в-третьих, в состоянии $\sigma^{\wedge i}$ не было трассы $\langle u \rangle$.

2.1. $u \neq \varnothing$ непустой отказ.

Модификации LTS не требуется, поэтому трасса σ сохраняется в LTS.

Поскольку $\mu_1 \cdot \langle u \rangle \notin \boldsymbol{p_{re}di}^{\sim}(\sigma)$, отказ u не вложен в $\cup \boldsymbol{Ip}(\sigma^i)$.

Поэтому в состоянии $\sigma^{\wedge i}$ есть переход по действию из $u \setminus \cup \boldsymbol{Ip}(\sigma^i)$, поскольку u – это непустой отказ, который не вложен в $\cup \boldsymbol{Ip}(\sigma^i)$.

Следовательно, в состоянии $\sigma^{\wedge i}$ нет отказа u и, следовательно, нет трассы $\langle u \rangle$.

2.2. $u=\varnothing$ пустой отказ.

Возможны два подслучая.

2.2.1. $i<n$ или $i=n$ и $|\sigma^{\wedge}|=n$.

Модификация: добавим переход-петлю $\sigma^{\wedge}{}^{i}\!\!-\!\!\tau\!\!\rightarrow\!\sigma^{\wedge}{}^{i}$.

Трасса σ останется в LTS, трасса μ_1 по-прежнему будет заканчивается только в состоянии $\sigma^{\wedge}{}^{i}$, но в этом состоянии не будет пустого отказа и, следовательно, не будет трассы $\langle u\rangle$.

2.2.2. $i=n$ и $|\sigma^{\wedge}|\neq n$.

Модификации LTS не требуется, поэтому трасса σ сохраняется в LTS.

В состоянии $\sigma^{\wedge}{}^{n}$ имеется τ-петля или γ-петля, следовательно, нет пустого отказа и трассы $\langle u\rangle$.

2.3. u действие и $u\in\cup\boldsymbol{Ip}(\sigma^{i})$.

Модификации LTS не требуется, поэтому трасса σ сохраняется в LTS.

Поскольку $u\in\cup\boldsymbol{Ip}(\sigma^{i})$, в состоянии $\sigma^{\wedge}{}^{i}$ нет перехода по действию u и, следовательно, нет трассы $\langle u\rangle$.

2.4. u действие и $u\notin\cup\boldsymbol{Ip}(\sigma^{i})$.

Тогда возможны два подслучая.

2.4.1. $i<n$ или $i=n$ и $|\sigma^{\wedge}|=n$.

Поскольку $u\notin\cup\boldsymbol{Ip}(\sigma^{i})$, в рассматриваемом случае имеется переход $\sigma^{\wedge}{}^{i}\!\!-\!\!u\!\!\rightarrow\!\boldsymbol{t}$.

Модификация: удалим этот переход.

Трасса σ останется в LTS, трасса μ_1 по-прежнему будет заканчивается только в состоянии $\sigma^{\wedge}{}^{i}$, но в этом состоянии не будет перехода по действию u и, следовательно, не будет трассы $\langle u\rangle$.

2.4.2. $i=n$ и $|\sigma^{\wedge}|\neq n$.

Модификации LTS не требуется, поэтому трасса σ сохраняется в LTS.

В состоянии $\sigma^{\wedge}{}^{n}$ имеется только τ-петля или γ-петля, следовательно, нет перехода по действию u и нет трассы $\langle u\rangle$.

2.5. $u=\gamma$ или $u=\Delta$.

Тогда возможны два подслучая.

2.5.1. $i<n$ или $i=n$ и $|\sigma^{\wedge}|=n$.

Модификации LTS не требуется, поэтому трасса σ сохраняется в LTS.

В состоянии $\sigma^{\wedge}i$ нет дивергенции и разрушения, следовательно, нет перехода по действию u и нет трассы $\langle u\rangle$.

2.5.1.1. $i=n$ и $|\sigma^{\wedge}|\neq n$.

Модификации LTS не требуется, поэтому трасса σ сохраняется в LTS.

В состоянии $\sigma^{\wedge}n$ есть дивергенция или разрушение $u`$.

Если $u\neq u`$, то в состоянии $\sigma^{\wedge}i$ нет дивергенции и разрушения, следовательно, нет перехода по действию u и нет трассы $\langle u\rangle$.

Если же $u=u`$, то $\mu_1\cdot\langle u\rangle\in \boldsymbol{p_{re}di}^{\sim}(\sigma)$, что противоречит тому, что μ_1 максимальный префикс трассы μ, принадлежащий $\boldsymbol{p_{re}di}^{\sim}(\sigma)$.

6.9. Доказательство леммы 2

Из определения отношения ***safe for*** следует, что, если в реализации нет достижимых дивергенции и разрушения и $\mathbf{Q_i}$-отказов, то она безопасно-тестируема для тройки $\mathbf{T_i}$.

Такая реализация всегда существует. Например, достаточно рассмотреть LTS-реализацию в алфавите $\mathbf{L}$, в которой в начальном состоянии определены переходы-петли по всем действиям из алфавита $\mathbf{L}$, и других переходов нет.

6.10. Доказательство теоремы 8

1. Необходимость.

Допустим противное.

Тогда в некоторой безопасно-тестируемой для тройки $\mathbf{T_i}$ трассовой $\mathbf{L}$-реализации $\mathbf{I}$ есть трасса $\sigma_{\mathbf{L}}\cdot\langle u_{\mathbf{L}}\rangle$, но условие теоремы не выполнено.

Трасса $\sigma_{\mathbf{L}}\cdot\langle u_{\mathbf{L}}\rangle$ согласована как трасса модели $\mathbf{I}$.

Поэтому нарушение условия теоремы возможно только в том случае, когда u отказ, но существуют такие кнопка $Q\in\mathbf{Q_i}$ и трасса $\mu\in(\mathbf{L}\cup\mathbf{R_i})^{*}\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma_i})$,

что $Q_{\mathbf{L}}\subseteq u_{\mathbf{L}}\cup\cup\boldsymbol{Ip}(\sigma_{\mathbf{L}})$, $\mu_{\mathbf{L}}\in\boldsymbol{di}^{\sim}(\sigma_{\mathbf{L}}\cdot\langle u_{\mathbf{L}}\rangle)$ и Q ***safe by*** $\boldsymbol{\Sigma_i}$ ***after*** μ.

Тогда $\sigma_{\mathbf{L}}\cdot\langle u_{\mathbf{L}}\rangle\in\mathbf{I}$ и $Q_{\mathbf{L}}\subseteq u_{\mathbf{L}}\cup\cup\boldsymbol{Ip}(\sigma_{\mathbf{L}})$ влечет $\sigma_{\mathbf{L}}\cdot\langle u_{\mathbf{L}}, Q_{\mathbf{L}}\rangle\in\mathbf{I}$.

Далее $\mu_{\mathbf{L}}\in\boldsymbol{di}^{\sim}(\sigma_{\mathbf{L}}\cdot\langle u_{\mathbf{L}}\rangle)$ влечет $\mu_{\mathbf{L}}\cdot\langle Q_{\mathbf{L}}\rangle\in\boldsymbol{di}^{\sim}(\sigma_{\mathbf{L}}\cdot\langle u_{\mathbf{L}}, Q_{\mathbf{L}}\rangle)$.

А тогда по лемме 1 $\mu_{\mathbf{L}}\cdot\langle Q_{\mathbf{L}}\rangle\in\mathbf{I}$.

Отсюда, поскольку $\mathbf{I}$ $\mathbf{L}$-реализация, $\mu\cdot\langle Q\rangle\in\mathbf{I}$,

что влечет Q ~~***safe in***~~ $\mathbf{I}$ ***after*** μ,

что противоречит гипотезе о безопасности.

2. Достаточность.

Поскольку трасса σ безопасная, а наблюдение u безопасно после σ, трасса $\sigma\cdot\langle u\rangle$ тестовая и, следовательно, допустимая.

По условию теоремы эта трасса также согласованная.

Поэтому мы можем рассмотреть реализацию $\mathbf{I_1}(\sigma_L\cdot\langle u_L\rangle)$.

В этой реализации в состоянии $(\sigma_L\cdot\langle u_L\rangle)^n$ заканчиваются только трассы из $\boldsymbol{di}\tilde{}(\sigma_L\cdot\langle u_L\rangle)$, и реализация содержит трассу $\sigma_L\cdot\langle u_L\rangle$.

Покажем, что такая реализация $\mathbf{I_1}(\sigma_L\cdot\langle u_L\rangle)$ безопасно-тестируема для тройки $\mathbf{T_i}$.

Действительно, в этой реализации нет дивергенции и разрушения, поскольку $u\in\mathbf{L}\cup\mathbf{R_i}$, то есть u_L не является дивергенцией или разрушением.

Поэтому опасность могут представлять собой только ненаблюдаемые отказы.

В состоянии $\boldsymbol{t}$ проведены переходы-петли по всем действиям из $\mathbf{L}$, поэтому в нем есть только пустой отказ, но он не является $\mathbf{Q}$-отказом.

Поскольку любой $\mathbf{Q_i}$-отказ в пересечении с $\mathbf{L}$ дает $\mathbf{Q}$-отказ, в состоянии $\boldsymbol{t}$ нет $\mathbf{Q_i}$-отказов.

Если бы ненаблюдаемый отказ, нарушающий гипотезу о безопасности, порождался не последним состоянием $(\sigma_L\cdot\langle u_L\rangle)^i$, где $i<n=|\sigma_L\cdot\langle u_L\rangle|$, то, поскольку такой отказ имеется в любой реализации после соответствующего префикса трассы σ_L, никакая безопасно-тестируемая реализация не могла бы содержать этот префикс, что противоречит тому, что любой строгий префикс трассы σ_L актуален, то есть встречается в некоторой безопасно-тестируемой реализации.

Следовательно, такой нарушающий гипотезу о безопасности ненаблюдаемый отказ Q_L может порождаться только последним состоянием $(\sigma_L\cdot\langle u_L\rangle)^n$.

Тогда u – это отказ,

$Q_L\subseteq u_L\cup\cup\boldsymbol{Ip}(\sigma_L)$

и для некоторой трассы $\mu\in(\mathbf{L}\cup\mathbf{R_i})^*\cap\boldsymbol{SafeBy}(\mathbf{\Sigma_i})$ такой,

что Q ***safe by*** $\mathbf{\Sigma_i}$ ***after*** μ и

в реализации $\mathbf{I_1}(\sigma_{\mathbf{L}}\cdot\langle u_{\mathbf{L}}\rangle)$ трасса μ заканчивается в состоянии $(\sigma_{\mathbf{L}}\cdot\langle u_{\mathbf{L}}\rangle)^{\wedge n}$.

Но, как сказано выше, тогда $\mu_{\mathbf{L}}\in \boldsymbol{di}^{\sim}(\sigma_{\mathbf{L}}\cdot\langle u_{\mathbf{L}}\rangle)$, а тогда нарушается условие теоремы.

Мы пришли к противоречию, следовательно, гипотеза о безопасности не нарушается, и реализация $\mathbf{I_1}(\sigma_{\mathbf{L}}\cdot\langle u_{\mathbf{L}}\rangle)$ безопасно-тестируемая для тройки $\mathbf{T_i}$.

Поскольку это **L**-реализация и содержит трассу $\sigma_{\mathbf{L}}\cdot\langle u_{\mathbf{L}}\rangle$, трасса $\sigma_{\mathbf{L}}\cdot\langle u_{\mathbf{L}}\rangle$ **L**-актуальная, что и требовалось доказать.

6.11. Доказательство леммы 3

1. Если $P\in\mathbf{Q}$, то

   P ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** $\kappa\cdot\lambda$

   $\Rightarrow\ \exists\mu\in \boldsymbol{di}^{\sim}(\kappa\cdot\lambda)\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma})\ \ P$ ***safe by*** $\boldsymbol{\Sigma}$ ***after*** μ

   $\Rightarrow\ \exists\mu\in \boldsymbol{di}^{\sim}(\kappa\cdot\langle R\rangle\cdot\lambda)\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma})\ \ P$ ***safe by*** $\boldsymbol{\Sigma}$ ***after*** μ

   $\Rightarrow\ P$ ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** $\kappa\cdot\langle R\rangle\cdot\lambda$.

2. Если $P=\varnothing$, то

   P ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** $\kappa\cdot\lambda$

   $\Rightarrow\ \exists\mu\in \boldsymbol{di}^{\sim}(\kappa\cdot\lambda)\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma})\ \ P$ ***safe by*** $\boldsymbol{\Sigma}$ ***after*** μ

   $\Rightarrow\ \exists\mu\in \boldsymbol{di}^{\sim}(\kappa\cdot\langle R\rangle\cdot\lambda)\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma})\ \ P$ ***safe by*** $\boldsymbol{\Sigma}$ ***after*** μ

   $\Rightarrow\ P$ ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** $\kappa\cdot\langle R\rangle\cdot\lambda$.

3. Если $P\in\mathbf{R}\backslash\{\varnothing\}$, то

   P ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** $\kappa\cdot\lambda$

   $\Rightarrow\ \forall z\in P\ \ z$ ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** $\kappa\cdot\lambda$

   $\Rightarrow\ \forall z\in P\ \ \exists\mu\in \boldsymbol{di}^{\sim}(\kappa\cdot\lambda)\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma})\ \ z$ ***safe by*** $\boldsymbol{\Sigma}$ ***after*** μ

   $\Rightarrow\ \forall z\in P\ \ \exists\mu\in \boldsymbol{di}^{\sim}(\kappa\cdot\langle R\rangle\cdot\lambda)\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma})\ \ z$ ***safe by*** $\boldsymbol{\Sigma}$ ***after*** μ

   $\Rightarrow\ \forall z\in P\ \ z$ ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** $\kappa\cdot\langle R\rangle\cdot\lambda\ \Rightarrow\ P$ ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** $\kappa\cdot\langle R\rangle\cdot\lambda$.

6.12. Доказательство леммы 4

Пусть $P\in\mathbf{R}$, $\boldsymbol{Ip}(\sigma)\neq\varnothing$ и $P\subseteq\cup\boldsymbol{Ip}(\sigma)$.

Нужно доказать, что P ***~conf*** $\boldsymbol{\Sigma}$ ***after*** σ.

Рассмотрим два возможных случая в зависмости от того $P=\varnothing$ или $P\neq\varnothing$.

1. $P=\varnothing$.

   В этом случае условие P ***~conf*** $\boldsymbol{\Sigma}$ ***after*** σ

эквивалентно условию $\varnothing$ ***safe~by*** Σ ***after*** σ.

Так как $\mathit{Ip}(\sigma)\neq\varnothing$, трассу σ можно представить в виде $\sigma=\kappa\cdot\langle R\rangle$, где $P\in\mathbf{R}$.

Поскольку $\sigma\in\sim\mathit{conf}(\mathbf{T})$, имеем $R\sim\mathit{conf}\,\Sigma\ \mathit{after}\ \kappa$,

что влечет R ***safe~by*** Σ ***after*** κ.

Рассмотрим два возможных подслучая: $R=\varnothing$ и $R\neq\varnothing$.

1.1. $R=\varnothing$.

Тогда $\varnothing$ ***safe~by*** Σ ***after*** κ,

что влечет $\exists\mu\in\mathit{di}\tilde{}(\kappa)\cap\mathit{SafeBy}(\Sigma)$ $\varnothing$ ***safe by*** Σ ***after*** μ,

что, поскольку $\mathit{di}\tilde{}(\kappa)\subseteq\mathit{di}\tilde{}(\kappa\cdot\langle R\rangle)$ и $\sigma=\kappa\cdot\langle R\rangle$,

влечет $\exists\mu\in\mathit{di}\tilde{}(\sigma)\cap\mathit{SafeBy}(\Sigma)$ $\varnothing$ ***safe by*** Σ ***after*** μ,

что влечет $\varnothing$ ***safe~by*** Σ ***after*** σ, что и требовалось доказать.

1.2. $R\neq\varnothing$.

Тогда R ***safe~by*** Σ ***after*** κ

влечет $\forall z\in R$ z ***safe~by*** Σ ***after*** σ, что, поскольку $R\neq\varnothing$,

влечет $\exists z\in R$ z ***safe~by*** Σ ***after*** σ,

что влечет $\exists Q\in\mathbf{R}\cup\mathbf{Q}$ $z\in Q$ & Q ***safe~by*** Σ ***after*** σ,

что влечет $\exists\mu\in\mathit{di}\tilde{}(\kappa)\cap\mathit{SafeBy}(\Sigma)$ Q ***safe by*** Σ ***after*** μ,

что влечет $\exists\mu\in\mathit{di}\tilde{}(\kappa)\cap\mathit{SafeBy}(\Sigma)$ Q $\mathit{safe}_{\gamma\Delta}$ Σ ***after*** μ,

что влечет $\exists\mu\in\mathit{di}\tilde{}(\kappa)\cap\mathit{SafeBy}(\Sigma)$ $\mu\cdot\langle\Delta\rangle\notin\Sigma$,

что влечет $\exists\mu\in\mathit{di}\tilde{}(\kappa)\cap\mathit{SafeBy}(\Sigma)$ $\varnothing$ $\mathit{safe}_{\gamma\Delta}$ Σ ***after*** μ,

что влечет $\exists\mu\in\mathit{di}\tilde{}(\kappa)\cap\mathit{SafeBy}(\Sigma)$ $\varnothing$ ***safe by*** Σ ***after*** μ,

что, поскольку $\mathit{di}\tilde{}(\kappa)\subseteq\mathit{di}\tilde{}(\kappa\cdot\langle R\rangle)$ и $\sigma=\kappa\cdot\langle R\rangle$,

влечет $\exists\mu\in\mathit{di}\tilde{}(\sigma)\cap\mathit{SafeBy}(\Sigma)$ $\varnothing$ ***safe by*** Σ ***after*** μ,

что влечет $\varnothing$ ***safe~by*** Σ ***after*** σ, что и требовалось доказать.

2. $P\neq\varnothing$.

В этом случае условие $P\sim\mathit{conf}\,\Sigma\ \mathit{after}\ \sigma$ эквивалентно конъюнкции следующих условий:

1) P ***safe~by*** Σ ***after*** σ,

2) $\forall Q\in\mathbf{Q}$ $\forall\mu\in\mathit{di}\tilde{}(\sigma\cdot\langle P\rangle)\cap\mathit{SafeBy}(\Sigma)$

$(Q\subseteq\cup\mathit{Ip}(\sigma\cdot\langle P\rangle)\ \Rightarrow\ Q\ \sout{\mathit{safe\ by}}\ \Sigma\ \mathit{after}\ \mu)$,

3) $\forall R\in\mathbf{R}\ \ \forall\mu\in\boldsymbol{di}^{\sim}(\sigma\cdot\langle P\rangle)\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma})$

$(R\subseteq\cup\boldsymbol{Ip}(\sigma\cdot\langle P\rangle)\ \ \&\ \ R\ \boldsymbol{safe\ by}\ \boldsymbol{\Sigma}\ \boldsymbol{after}\ \mu\ \Rightarrow\ \mu\cdot\langle R\rangle\in\boldsymbol{\Sigma})$.

Докажем выполнение этих условий.

2.1. Докажем выполнение условия 1.

Поскольку $P\subseteq\cup\boldsymbol{Ip}(\sigma)$, $\forall z\in P\ \exists R_z\in\mathbf{R}\ \ z\in R_z\ \&\ R_z\in\boldsymbol{Ip}(\sigma)$.

Тогда для каждого такого $z\in P$ трассу σ можно представить в виде $\sigma=\kappa\cdot\langle R_z\rangle\cdot\rho$, где $\rho\in\mathbf{R}^*$.

Поскольку $\sigma\in\sim\boldsymbol{conf}(\mathbf{T})$, имеем $R_z\sim\boldsymbol{conf}\ \boldsymbol{\Sigma}\ \boldsymbol{after}\ \kappa$,

что влечет $R_z\ \boldsymbol{safe\sim by}\ \boldsymbol{\Sigma}\ \boldsymbol{after}\ \kappa$,

что, поскольку $z\in R_z$ и, следовательно, $R_z\neq\varnothing$,

влечет $z\ \boldsymbol{safe\sim by}\ \boldsymbol{\Sigma}\ \boldsymbol{after}\ \kappa$,

что влечет $\exists Q\in\mathbf{R}\cup\mathbf{Q}\ \ z\in Q\ \&\ Q\ \boldsymbol{safe\sim by}\ \boldsymbol{\Sigma}\ \boldsymbol{after}\ \kappa$,

что влечет $\exists Q\in\mathbf{R}\cup\mathbf{Q}\ \ z\in Q\ \&\ \exists\mu\in\boldsymbol{di}^{\sim}(\kappa)\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma})$ $Q\ \boldsymbol{safe\ by}\ \boldsymbol{\Sigma}\ \boldsymbol{after}\ \mu$,

что, поскольку $\boldsymbol{di}^{\sim}(\kappa)\subseteq\boldsymbol{di}^{\sim}(\kappa\cdot\langle R\rangle\cdot\rho)$, $\rho\in\mathbf{R}^*$ и $\sigma=\kappa\cdot\langle R\cdot\rho\rangle$,

влечет $\exists Q\in\mathbf{R}\cup\mathbf{Q}\ \ z\in Q\ \&\ \exists\mu\in\boldsymbol{di}^{\sim}(\sigma)\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma})\ \ Q\ \boldsymbol{safe\ by}\ \boldsymbol{\Sigma}\ \boldsymbol{after}\ \mu$,

что влечет $\exists Q\in\mathbf{R}\cup\mathbf{Q}\ \ z\in Q\ \&\ Q\ \boldsymbol{safe\sim by}\ \boldsymbol{\Sigma}\ \boldsymbol{after}\ \sigma$,

что влечет $z\ \boldsymbol{safe\sim by}\ \boldsymbol{\Sigma}\ \boldsymbol{after}\ \sigma$.

Поскольку это верно для каждого $z\in P$,

имеем $P\ \boldsymbol{safe\sim by}\ \boldsymbol{\Sigma}\ \boldsymbol{after}\ \sigma$, что и требовалось доказать.

2.2. Докажем выполнение условий 2 и 3.

Пусть $Q\in\mathbf{R}\cup\mathbf{Q}$, $\mu\in\boldsymbol{di}^{\sim}(\sigma\cdot\langle P\rangle)\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma})$ и $Q\subseteq\cup\boldsymbol{Ip}(\sigma\cdot\langle P\rangle)$.

Нам нужно доказать:

2) если $Q\in\mathbf{Q}$, то $Q\ \boldsymbol{safe\ by}\ \boldsymbol{\Sigma}\ \boldsymbol{after}\ \mu$;

3) если $Q\in\mathbf{R}$ и $Q\ \boldsymbol{safe\ by}\ \boldsymbol{\Sigma}\ \boldsymbol{after}\ \mu$, то $\mu\cdot\langle Q\rangle\in\boldsymbol{\Sigma}$.

Поскольку $P\subseteq\cup\boldsymbol{Ip}(\sigma)$ и $P\neq\varnothing$,

трассу σ можно представить в виде $\sigma=\kappa\cdot\langle P_1\rangle\cdot\rho$,

где $P_1\in\mathbf{R}\backslash\{\varnothing\}$ и $\rho\in\{\varnothing\}^*$.

Поскольку $P\subseteq\cup\boldsymbol{Ip}(\sigma)$ и $\rho\in\{\varnothing\}^*$,

условие $Q\subseteq\cup\boldsymbol{Ip}(\sigma\cdot\langle P\rangle)$ влечет $Q\subseteq\cup\boldsymbol{Ip}(\kappa\cdot\langle P_1\rangle)$.

Поскольку $\mu\in\boldsymbol{di}^{\sim}(\sigma\cdot\langle P\rangle)$, а $P\subseteq\cup\boldsymbol{Ip}(\sigma)$, имеем $\mu\in\boldsymbol{di}^{\sim}(\sigma)$.

А тогда, поскольку $\sigma=\kappa\cdot\langle P_1\rangle\cdot\rho$, где $\rho\in\{\varnothing\}^*$, имеем $\mu\in\boldsymbol{di}^{\sim}(\kappa\cdot\langle P_1\rangle)$.

Итак, $\mu \in \boldsymbol{di}^{\sim}(\kappa \cdot \langle P_1 \rangle) \cap \boldsymbol{SafeBy}(\Sigma)$ и $Q \subseteq \cup \boldsymbol{Ip}(\kappa \cdot \langle P_1 \rangle)$.

Поскольку $\kappa \cdot \langle P_1 \rangle \cdot \rho = \sigma \in \sim \boldsymbol{conf}(\mathbf{T})$, должно быть P_1 $\boldsymbol{\sim conf\ \Sigma\ after}$ κ.

А тогда, поскольку $P_1 \neq \varnothing$, должны быть выполнены условия 2 и 3 для отказа P_1 после трассы κ:

2) если $Q \in \mathbf{Q}$, то Q ~~***safe by***~~ $\boldsymbol{\Sigma\ after}$ μ;

3) если $Q \in \mathbf{R}$ и Q $\boldsymbol{safe\ by\ \Sigma\ after}$ μ, то $\mu \cdot \langle R \rangle \in \boldsymbol{\Sigma}$.

Что и требовалось доказать.

6.13. Доказательство леммы 5

1. Покажем, что каждая тестовая трасса ~тестовая.

Пусть трасса σ тестовая.

По определению ~тестовой трассы нам нужно показать, что

1) пустая трасса безопасна в спецификации,

2) если $\mu \cdot \langle u \rangle \le \sigma$, то наблюдение u ~безопасно после μ.

Пустая трасса безопасна в спецификации, поскольку трасса σ тестовая.

Докажем свойство 2.

1.1. Пусть u действие.

Тогда нужно показать, что оно безопасно после некоторой $\boldsymbol{di}^{\sim}$-подтрассы $\mu` \in \boldsymbol{di}^{\sim}(\mu) \cap \boldsymbol{SafeBy}(\Sigma)$.

Поскольку это верно для самой трассы μ, являющейся одной из таких $\boldsymbol{di}^{\sim}$-подтрасс, утверждение доказано.

1.2. Пусть u непустой отказ.

Тогда нужно показать, что каждое действие $z \in u$ ~безопасно после μ.

Поскольку u безопасно после трассы μ, каждое действие $z \in u$ безопасно после μ, что по доказанному п.1.1 влечет ~безопасность z после μ, а это влечет ~безопасность отказа u.

Утверждение доказано.

1.3. Пусть u пустой отказ.

Тогда нужно показать, что хотя бы после одной $\boldsymbol{di}^{\sim}$-подтрассы $\mu` \in \boldsymbol{di}^{\sim}(\mu) \cap \boldsymbol{SafeBy}(\Sigma)$ в спецификации нет дивергенции.

Поскольку u безопасно после трассы μ, после μ нет дивергенции, и трасса μ является одной из таких $\boldsymbol{di}^{\sim}$-подтрасс, а это влечет ~безопасность пустого отказа u.

Утверждение доказано.

2. Покажем, что безопасная трасса ~конформна тогда и только тогда, когда она актуальна.

2.1. Сначала покажем, что каждая актуальная безопасная трасса ~конформна.

Пусть трасса σ актуальная безопасная трасса.

Тогда она тестовая и по доказанному п.1 ~тестовая.

Нам осталось показать, что

если $\mu\cdot\langle u\rangle\le\sigma$, то наблюдение u ~конформно после μ.

2.1.1. Пусть u действие.

Тогда нужно показать выполнение дополнительных условий a) и b) в п.1 определения ~конформности.

a) $u\notin\cup\boldsymbol{Ip}(\mu)$.

Это следует из того, что трасса $\mu\cdot\langle u\rangle$ – безопасная и, следовательно, согласованная трасса спецификации.

b) Каждая подтрасса $\mu`\in\boldsymbol{di}^{\sim}(\mu)\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma})$, после которой $u$ безопасно, им продолжается, то есть $u$ ***safe by*** $\boldsymbol{\Sigma}$ ***after*** $\mu` \Rightarrow \mu`\cdot\langle u\rangle\in\boldsymbol{\Sigma}$.

Действительно, по лемме 1 $\mu\cdot\langle u\rangle\in\boldsymbol{\Sigma}$ влечет $\mu`\cdot\langle u\rangle\in\boldsymbol{\Sigma}$ для каждой трассы $\mu`$.

2.1.2. Пусть u непустой отказ.

Тогда нужно показать выполнение дополнительных условий a) и b) в п.2 определения ~конформности.

a) Каждая кнопка $Q\in\boldsymbol{Q}$ такая, что $Q\subseteq\cup\boldsymbol{Ip}(\mu\cdot\langle u\rangle)$, опасна после каждой подтрассы $\mu`\in\boldsymbol{di}^{\sim}(\mu\cdot\langle u\rangle)\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma})$.

Допустим, это не верно.

Тогда после некоторой трассы $\mu`$ кнопка Q безопасна в спецификации.

Поскольку трасса σ актуальная, ее префикс $\mu\cdot\langle u\rangle$ тоже актуален и, следовательно, встречается в некоторой безопасно-тестируемой реализации.

Но тогда в этой реализации по свойствам полной трассовой модели есть трасса $\mu\cdot\langle u,Q\rangle$ и по лемме 1 в этой реализации есть трасса $\mu`\cdot\langle Q\rangle\in\boldsymbol{di}^{\sim}(\mu\cdot\langle u,Q\rangle)$, что противоречит гипотезе о безопасности.

b) Для каждой кнопки $R \in \mathbf{R}$ такой, что $R \subseteq \cup \boldsymbol{Ip}(\mu \cdot \langle u \rangle)$, каждая подтрасса $\mu` \in \boldsymbol{di\tilde{}}(\mu \cdot \langle u \rangle) \cap \boldsymbol{SafeBy}(\boldsymbol{\Sigma})$, после которой кнопка R безопасна, продолжается отказом R.

Действительно, $\mu \cdot \langle u \rangle \in \boldsymbol{\Sigma}$ влечет по свойствам полной трассовой модели $\mu \cdot \langle u, R \rangle \in \boldsymbol{\Sigma}$,

что по лемме 1 влечет $\mu` \cdot \langle R \rangle \in \boldsymbol{\Sigma}$ для каждой трассы $\mu`$.

2.1.3. Пусть u пустой отказ.

Тогда, поскольку он ~безопасен, он ~конформен после трассы μ.

2.2. Теперь покажем, что каждая безопасная неактуальная трасса σ не ~конформна.

Действительно, поскольку трасса σ безопасная, она тестовая и, следовательно, по доказанному ~тестовая.

Поскольку условия ~конформности включают в себя условия актуальности по теореме 8, для неактуальной трассы σ эти условия не выполнены, поэтому эта трасса не ~конформная.

3. Покажем, что каждая ошибка 1-го рода $\sigma \cdot \langle u \rangle$ не ~конформна.

По доказанному, если трасса σ не актуальная трасса, то она не ~конформна и, следовательно, трасса $\sigma \cdot \langle u \rangle$ не ~конформна.

Теперь пусть трасса $\sigma \cdot \langle u \rangle$ ошибка 1-го рода, где σ актуальная трасса.

Тогда трасса $\sigma \cdot \langle u \rangle$ тестовая и, следовательно, трасса σ безопасная.

По доказанному трасса σ ~конформная, а $\sigma \cdot \langle u \rangle$ ~тестовая.

Нам надо показать, что наблюдение u не ~конформно после μ.

3.1. Пусть u действие.

Тогда оно безопасно после трассы σ, но трасса σ не продолжается им, то есть нарушено дополнительное условие b) в п.1 определения ~конформности.

3.2. Пусть u непустой отказ.

Тогда он безопасен после трассы σ, но трасса σ не продолжается им, то есть нарушено дополнительное условие b) в п.2 определения ~конформности.

3.3. Пусть u пустой отказ.

Тогда из его безопасности после трассы σ следует отсутствие дивергенции после трассы σ.

А тогда по конвергентности модели трасса σ продолжается пустым отказом в спецификации.

Иными словами, этого случая не бывает.

6.14. Доказательство леммы 6

Если для тройки $\mathbf{T}$ пустая трасса опасна в спецификации,
то нет ~тестовых и ~конформных трасс.

В этом случае также **L**-реализация, состоящая из одной трассы $\langle\gamma\rangle$, безопасно-тестируемая.

Для любой тройки, в спецификации которой пустая трасса безопасна,
эта реализация не является безопасно-тестируемой.

Следовательно, в любой тройке из **L**-конуса (не сужающей класс безопасно-тестируемых реализаций) пустая трасса опасна.

А тогда нет ни одной ∇-тестовой и, тем более, ∇-конформной трассы.

Теперь будем предполагать, что пустая трасса безопасна для тройки $\mathbf{T}$.

Будем доказывать индукцией по трассе σ следующее утверждение:

1) $\sigma\in\nabla\boldsymbol{ptt}(\mathbf{T}) \Rightarrow \sigma\in\sim\boldsymbol{ptt}(\mathbf{T})$,
2) $\sigma\in\nabla\boldsymbol{conf}(\mathbf{T}) \Rightarrow \sigma\in\sim\boldsymbol{conf}(\mathbf{T})$.

Поскольку безопасная пустая трасса ~конформная и, следовательно, первичная ~тестовая, для нее утверждение доказано.

Пусть трасса σ ∇-конформна и ~конформна.

1. Сначала докажем, что, если трасса $\sigma\cdot\langle u\rangle$ ∇-тестовая, то она ~тестовая.

   Поскольку трасса σ ∇-конформная, а трасса $\sigma\cdot\langle u\rangle$ ∇-тестовая,

   существует тройка $\mathbf{T}`\in\nabla(\mathbf{T})_{\mathbf{L}}$,

   в спецификации которой есть безопасная трасса $\sigma`$ такая, что $\sigma`_{\mathbf{L}}=\sigma$,

   и есть наблюдение $u`$, безопасное после $\sigma`$, такое, что $u`_{\mathbf{L}}=u$.

   Также существует конформная реализация $\mathbf{I}$ в алфавите **L**, содержащая трассу σ.

1.1. Рассмотрим случай, когда u действие.

   Тогда $u=u`$.

   Нужно показать, что действие u ~безопасно после трассы σ.

1.1.1. Пусть $u\in\cup\boldsymbol{Ip}(\sigma)$.

   Тогда трассу σ можно представить в виде $\sigma=\sigma_1\cdot\langle R\rangle\cdot\rho$, где $R\in\mathbf{R}$, $u\in R$ и $\rho\in\mathbf{R}^*$.

   Поскольку трасса σ ~конформна, отказ R ~безопасен после σ_1.

Но тогда все его действия, в том числе u, ~безопасны после σ_1.

Это значит, что действие u безопасно в исходной спецификации после некоторой трассы $\mu \in \boldsymbol{di}^{\sim}(\sigma_1)$.

Поскольку $\rho \in \mathbf{R}^*$, $\boldsymbol{di}^{\sim}(\sigma_1) \subseteq \boldsymbol{di}^{\sim}(\sigma)$, следовательно, $\mu \in \boldsymbol{di}^{\sim}(\sigma)$.

А тогда u ~безопасно после σ.

1.1.2. Пусть теперь $u \notin \cup \boldsymbol{Ip}(\sigma)$.

Допустим, что действие u ~опасно после трассы σ.

Поскольку трасса σ встречается в модели $\mathbf{I}$, она допустима и согласована.

А тогда, поскольку $u \notin \cup \boldsymbol{Ip}(\sigma)$, трасса $\sigma \cdot \langle u \rangle$ тоже допустима и согласована, и, поскольку u действие, допустима и согласована трасса $\sigma \cdot \langle u, \gamma \rangle$.

Поэтому мы можем взять в качестве реализации LTS $\mathbf{I}_1(\sigma \cdot \langle u, \gamma \rangle)$.

В этой реализации в каждом состоянии $(\sigma \cdot \langle u \rangle)^{\wedge i}$ заканчиваются только трассы из $\boldsymbol{di}^{\sim}((\sigma \cdot \langle u \rangle)^i)$, и реализация содержит трассу $\sigma \cdot \langle u, \gamma \rangle$.

Покажем, что реализация $\mathbf{I}_1(\sigma \cdot \langle u, \gamma \rangle)$ безопасно-тестируема для исходной тройки $\mathbf{T}$.

Действительно, в реализации $\mathbf{I}_1(\sigma \cdot \langle u, \gamma \rangle)$ любой $\mathbf{Q}$-отказ Q не может быть в состоянии $\boldsymbol{t}$, то есть может быть только в состоянии вида $(\sigma \cdot \langle u \rangle)^{\wedge i} = (\sigma^{\wedge} \cdot \langle u \rangle)^i$, где $i = 0..n$.

Но в состоянии $(\sigma^{\wedge} \cdot \langle u \rangle)^n$ имеется только γ-петля.

Следовательно, отказ Q может быть только в состоянии вида $(\sigma^{\wedge} \cdot \langle u \rangle)^i$, где $i < n$, а в этом случае $(\sigma^{\wedge} \cdot \langle u \rangle)^i = \sigma^{\wedge i}$.

В этом состоянии заканчиваются только трассы $\mu \in \boldsymbol{p}_{re}\boldsymbol{di}^{\sim}(\sigma)$.

Отказ Q имеется после этой трассы только при условии $Q \subseteq \cup \boldsymbol{Ip}(\mu)$.

По лемме 1 такая подтрасса μ будет и в реализации $\mathbf{I}$, поскольку в ней есть трасса σ, и в $\mathbf{I}$ тоже после μ будет $\mathbf{Q}$-отказ Q.

Следовательно, если μ безопасна в исходной спецификации,
то такой $\mathbf{Q}$-отказ не может быть безопасным в исходной спецификации после μ,

так как это противоречило бы безопасно-тестируемости конформной реализации $\mathbf{I}$ для исходной тройки $\mathbf{T}$.

Мы показали, что нарушение гипотезы о безопасности не может происходить из-за $\mathbf{Q}$-отказов, то есть может быть только из-за дивергенции или разрушения.

Но в реализации $\mathbf{I_1}(\sigma\cdot\langle u,\gamma\rangle)$ нет дивергенции, а разрушение встречается только после трасс из множества $\boldsymbol{di}^{\sim}(\sigma\cdot\langle u\rangle)$.

Это значит, что гипотеза о безопасности для исходной тройки $\mathbf{T}$ может быть нарушена только в том случае, когда после некоторой трассы $\mu\in\boldsymbol{di}^{\sim}(\sigma)\cap\boldsymbol{SafeBy}(\mathbf{T})$ в спецификации безопасна кнопка, разрешающая действие u.

Но тогда действие u было бы ~безопасно после трассы σ, что противоречит допущению.

Мы показали, что реализация $\mathbf{I_1}(\sigma\cdot\langle u,\gamma\rangle)$ безопасно-тестируема для исходной тройки $\mathbf{T}$.

Однако реализация $\mathbf{I_1}(\sigma\cdot\langle u,\gamma\rangle)$ не удовлетворяет гипотезе о безопасности для тройки $\mathbf{T}`$, поскольку реализация содержит трассу $\sigma\cdot\langle u,\gamma\rangle$, а поскольку эта тройка определяет трассу $\sigma`\cdot\langle u\rangle$, где $\sigma`_{\mathbf{L}}=\sigma$, как тестовую.

А это противоречит условию не сужения класса безопасно-тестируемых реализаций для тройки $\mathbf{T}`\in\nabla(\mathbf{T})_{\mathbf{L}}$.

Мы пришли к противоречию и, следовательно, наше допущение не верно, и действие u ~безопасно после трассы σ.

1.2. Рассмотрим случай, когда u непустой $\mathbf{R}$-отказ.

Тогда $u=u`\cap\mathbf{L}$.

Докажем, что отказ u ~безопасен после трассы σ.

Действительно, поскольку трасса $\sigma`\cdot\langle u`\rangle$ тестовая для тройки $\mathbf{T}`$,

для этой тройки являются тестовыми все трассы вида $\sigma`\cdot\langle z\rangle$, где $z\in u$.

Но тогда по доказанному п.1.1 все эти действия z ~безопасны после трассы σ.

А это и означает ~безопасность непустого $\mathbf{R}$-отказа u после трассы σ.

1.3. Рассмотрим случай, когда $u=\varnothing$ пустой $\mathbf{R}$-отказ.

Тогда $\varnothing=u`\cap\mathbf{L}$.

Докажем, что пустой отказ ~безопасен после трассы σ.

1.3.1. Пусть трасса σ заканчивается отказом, то есть имеет вид $\sigma=\sigma_1\cdot\langle R\rangle$, где $R\in\mathbf{R}$.

1.3.1.1. Пусть $R=\varnothing$ пустой отказ.

Тогда, поскольку трасса σ ~конформна,

пустой отказ ~безопасен после σ_1.

А это означает, что некоторая трасса $\mu\in \boldsymbol{di}^{\sim}(\sigma_1)\cap \boldsymbol{SafeBy}(\mathbf{T})$ в спецификации не продолжается дивергенцией.

Поскольку $\sigma=\sigma_1\cdot\langle R\rangle$, имеем $\mu\in \boldsymbol{di}^{\sim}(\sigma)$,

что означает ~безопасность пустого отказа и после трассы σ.

1.3.1.2. Пусть R непустой отказ.

Тогда, поскольку трасса σ ~конформна,

найдется действие $z\in R$, которое ~безопасно после σ_1.

А это означает, что после некоторой трассы $\mu\in \boldsymbol{di}^{\sim}(\sigma_1)\cap \boldsymbol{SafeBy}(\mathbf{T})$ действие z безопасно в спецификации.

Но тогда трасса μ не продолжается в спецификации дивергенцией.

Поскольку $\sigma=\sigma_1\cdot\langle R\rangle$, имеем $\mu\in \boldsymbol{di}^{\sim}(\sigma)$,

что означает ~безопасность пустого отказа и после трассы σ.

1.3.2. Пусть трасса σ не заканчивается отказом.

Допустим, что пустой отказ ~опасен после трассы σ.

Поскольку трасса σ встречается в модели $\mathbf{I}$,

она допустима и согласована.

А тогда, поскольку трасса σ не заканчивается отказом,

трасса $\sigma\cdot\langle\Delta\rangle$ тоже допустима и согласована.

Поэтому мы можем взять в качестве реализации LTS $\mathbf{I_1}(\sigma\cdot\langle\Delta\rangle)$.

Покажем, что она безопасно-тестируема для исходной тройки $\mathbf{T}$.

Аналогично п.1.1.2 нарушение гипотезы о безопасности не может происходить из-за **Q**-отказов.

Действительно, в LTS $\mathbf{I_1}(\sigma\cdot\langle\Delta\rangle)$ любой **Q**-отказ Q не может быть в состоянии $\boldsymbol{t}$, то есть может быть только в состоянии вида $(\sigma\cdot\langle\Delta\rangle)^{\wedge i}=(\sigma^{\wedge}\cdot\langle\Delta\rangle)^i$, где $i=0..n$ и $n=|\sigma^{\wedge}\cdot\langle\Delta\rangle\downarrow\mathbf{L}|$.

А это состояния вида $\sigma^{\wedge i}$.

В этом состоянии заканчиваются только трассы $\mu\in \boldsymbol{p_{re}di}^{\sim}(\sigma)$.

Отказ Q имеется после этой трассы только при условии $Q\subseteq\cup\boldsymbol{Ip}(\mu)$.

По лемме 1 такая подтрасса μ будет и в реализации $\mathbf{I}$,

поскольку в ней есть трасса σ, и в $\mathbf{I}$ тоже после μ будет **Q**-отказ Q.

Следовательно, если μ безопасна в исходной спецификации,

то такой **Q**-отказ не может быть безопасным в исходной спецификации после μ,

так как это противоречило бы безопасно-тестируемости конформной реализации $\mathbf{I}$ для исходной тройки **T**.

Мы показали, что нарушение гипотезы о безопасности не может происходить из-за **Q**-отказов, то есть может быть только из-за дивергенции или разрушения.

В LTS $\mathbf{I_1}(\sigma\cdot\langle\Delta\rangle)$ нет разрушения, а дивергенция встречается только после трасс из множества $\boldsymbol{di}^{\sim}(\sigma)$.

Это значит, что гипотеза о безопасности для исходной тройки **T** может быть нарушена только в том случае, когда некоторая трасса $\mu\in\boldsymbol{di}^{\sim}(\sigma)\cap\boldsymbol{SafeBy}(\mathbf{T})$ в спецификации не продолжается дивергенцией.

Но тогда пустой отказ был бы ~безопасен после трассы σ, что противоречит допущению.

Мы показали, что реализации $\mathbf{I_1}(\sigma\cdot\langle\Delta\rangle)$ безопасно-тестируема для исходной тройки **T**.

Однако реализация $\mathbf{I_1}(\sigma\cdot\langle\Delta\rangle)$ не удовлетворяет гипотезе о безопасности для тройки $\mathbf{T}`$, поскольку эта тройка определяет трассу $\sigma`\cdot\langle u`\rangle$ как тестовую.

А это противоречит условию не сужения класса безопасно-тестируемых реализаций для тройки $\mathbf{T}`\in\nabla(\mathbf{T})_{\mathbf{L}}$.

Мы пришли к противоречию и, следовательно, наше допущение не верно, и пустой отказ ~безопасен после трассы σ.

2. Теперь докажем, что, если трасса $\sigma\cdot\langle u\rangle$ ∇-конформна, то она ~конформная.

   Поскольку трасса $\sigma\cdot\langle u\rangle$ ∇-конформная,

   существует тройка $\mathbf{T}`\in\nabla(\mathbf{T})_{\mathbf{L}}$,

   в спецификации которой есть безопасная трасса $\sigma`\cdot\langle u`\rangle$ такая,

   что $\sigma`_{\mathbf{L}}=\sigma$ и $u`_{\mathbf{L}}=u$.

   Также существует конформная реализация $\mathbf{I}$ в алфавите **L**,

   содержащая трассу $\sigma\cdot\langle u\rangle$.

2.1. Рассмотрим случай, когда u действие.

Тогда $u=u`$.

Поскольку мы уже доказали, что действие u ~безопасно после трассы σ, нам нужно показать, что оно удовлетворяет дополнительным условиям ~конформности.

2.1.1. Условие a: u не запрещается постфиксом отказов трассы.

Поскольку трасса $\sigma\cdot\langle u\rangle$ встречается в модели $\mathbf{I}$,

выполнено условие согласованности этой трассы $u\notin\cup\boldsymbol{Ip}(\sigma)$.

2.1.2. Условие b: каждая подтрасса $\mu\in\boldsymbol{di}^{\sim}(\sigma)\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma})$, после которой действие u безопасно, продолжается этим действием.

Действительно, если бы для какой-то трассы μ это было не так, то существовала бы кнопка P, безопасная в $\boldsymbol{\Sigma}$ после μ и разрешающая действие u, и трасса μ не продолжалась бы в $\boldsymbol{\Sigma}$ действием u.

По лемме 1 из наличия в реализации $\mathbf{I}$ трассы $\sigma\cdot\langle u\rangle$ следует наличие в ней трассы $\mu\cdot\langle u\rangle\in\boldsymbol{di}^{\sim}(\sigma\cdot\langle u\rangle)$.

Поскольку реализация $\mathbf{I}$ конформна, она безопасно-тестируема для исходной тройки $\mathbf{T}$, следовательно, кнопка P безопасна в $\mathbf{I}$ после μ.

Но при нажатии этой кнопки в реализации $\mathbf{I}$ может наблюдаться действие u, которого нет после μ в спецификации $\boldsymbol{\Sigma}$.

А это противоречит тестируемому условию конформности $\mathbf{I}$.

2.2. Рассмотрим случай, когда u непустой **R**-отказ.

Тогда $u=u`\cap\mathbf{L}$.

Поскольку мы уже доказали, что отказ u ~безопасен после трассы σ, нам нужно показать, что он удовлетворяет дополнительным условиям ~конформности.

2.2.1. Условие a: каждая кнопка $Q\in\mathbf{Q}$ такая, что $Q\subseteq\cup\boldsymbol{Ip}(\sigma\cdot\langle u\rangle)$, опасна в исходной спецификации после каждой трассы $\mu\in\boldsymbol{di}^{\sim}(\sigma\cdot\langle u\rangle)\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma})$.

Действительно, по лемме 1 из наличия в реализации $\mathbf{I}$ трассы $\sigma\cdot\langle u\rangle$ следует наличие в ней трассы μ, которая также продолжается отказом Q.

Если бы кнопка Q была в исходной спецификации безопасна после трассы μ, то реализация $\mathbf{I}$ не удовлетворяла бы гипотезе о

безопасности для исходной спецификации, что противоречит конформности реализации $\mathbf{I}$.

2.2.2. Условие b: для каждого **R**-отказа $R \subseteq \cup \boldsymbol{Ip}(\sigma \cdot \langle u \rangle)$ каждая подтрасса $\mu \in \boldsymbol{di}^{\sim}(\sigma \cdot \langle u \rangle) \cap \boldsymbol{SafeBy}(\boldsymbol{\Sigma})$, после которой R безопасен, им продолжается.

Действительно, по лемме 1 из наличия в реализации $\mathbf{I}$ трассы $\sigma \cdot \langle u \rangle$ следует наличие в ней каждой трассы $\mu \in \boldsymbol{di}^{\sim}(\sigma \cdot \langle u \rangle) \cap \boldsymbol{SafeBy}(\boldsymbol{\Sigma})$, которая продолжается отказом R.

Если бы в исходной спецификации кнопка R была безопасна после некоторой трассы μ, которая не продолжалась бы отказом R, то реализация $\mathbf{I}$ не удовлетворяла бы тестируемому условию конформности для исходной спецификации.

2.3. Рассмотрим случай, когда $u = \varnothing$ пустой **R**-отказ.

Тогда $\varnothing = u` \cap \mathbf{L}$.

Мы уже доказали, что пустой отказ ~безопасен после трассы σ.

Поскольку для ~конформности пустого отказа дополнительных условий нет, он ~конформен после трассы σ.

Лемма доказана.

6.15. Доказательство теоремы 9

1. Покажем, что $\boldsymbol{conf}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}} \subseteq \nabla \boldsymbol{conf}(\mathbf{T})$.

По определению $\nabla \boldsymbol{conf}(\mathbf{T}) = \cup\{\boldsymbol{conf}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}} \mid \mathbf{T_i} \in \nabla(\mathbf{T})_{\mathbf{L}}\}$,

Далее $\mathbf{T_i} \approx_{\mathbf{L}} \mathbf{T}$ влечет $\mathbf{T_i} \in \nabla(\mathbf{T})_{\mathbf{L}}$.

Поэтому $\boldsymbol{conf}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}} \subseteq \nabla \boldsymbol{conf}(\mathbf{T})$.

2. Покажем, что $\nabla \boldsymbol{conf}(\mathbf{T}) \subseteq \boldsymbol{conf}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}}$ (см. Рис. 22.).

По определению ~пополнения $\mathbf{T_i}$ имеем $\boldsymbol{SafeBy}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}} = {\sim}\boldsymbol{conf}(\mathbf{T})$.

По лемме 6 $\nabla \boldsymbol{conf}(\mathbf{T}) \subseteq {\sim}\boldsymbol{conf}(\mathbf{T})$.

Следовательно, $\nabla \boldsymbol{conf}(\mathbf{T}) \subseteq \boldsymbol{SafeBy}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}}$.

По определению $\nabla \boldsymbol{err}(\mathbf{T}) = \cup\{\boldsymbol{err}(\mathbf{T_j},\mathbf{L})_{\mathbf{L}} \mid \mathbf{T_j} \in \nabla(\mathbf{T})_{\mathbf{L}}\}$.

Далее $\mathbf{T_i} \approx_{\mathbf{L}} \mathbf{T}$ влечет $\mathbf{T_i} \in \nabla(\mathbf{T})_{\mathbf{L}}$.

Следовательно, $\boldsymbol{err}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}} \subseteq \nabla \boldsymbol{err}(\mathbf{T})$.

Далее, поскольку $\boldsymbol{SafeBy}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}} \setminus \boldsymbol{conf}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}} \subseteq \boldsymbol{err}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}}$,

имеем $\boldsymbol{SafeBy}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}} \setminus \boldsymbol{conf}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}} \subseteq \nabla \boldsymbol{err}(\mathbf{T})$.

Поскольку $\nabla \boldsymbol{err}(\mathbf{T}) \cap \nabla \boldsymbol{conf}(\mathbf{T}) = \varnothing$ и $\nabla \boldsymbol{conf}(\mathbf{T}) \subseteq \boldsymbol{SafeBy}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}}$,

то $\nabla \boldsymbol{conf}(\mathbf{T}) \subseteq \boldsymbol{conf}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}}$.

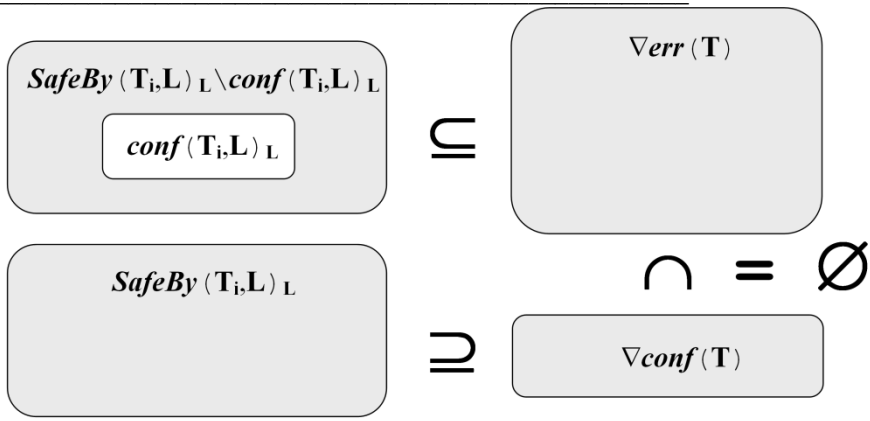


Рис. 22. $\nabla conf(T) \subseteq conf(T_i,L)_L$

3. Покажем, что $perr(T_i,L)_L \subseteq \nabla perr(T)$.
   По определению $\nabla perr(T) = \cup\{perr(T_i,L)_L \mid T_i \in \nabla(T)_L\}$,
   Далее $T_i \approx_L T$ влечет $T_i \in \nabla(T)_L$.
   Поэтому $perr(T_i,L)_L \subseteq \nabla perr(T)$.
4. Покажем, что $\nabla perr(T) \subseteq perr(T_i,L)_L$.
   По определению ~пополнения T_i имеем $tt(T_i,L)_L = {\sim}ptt(T)$.
   По лемме 6 $\nabla ptt(T) \subseteq {\sim}ptt(T)$.
   Следовательно, $\nabla ptt(T) \subseteq tt(T_i,L)_L$.
   По определению $\nabla ptt(T) = \nabla perr(T) \cup \nabla conf(T)$.
   Также $\nabla perr(T) \cap \nabla conf(T) = \varnothing$.
   Следовательно, $\nabla perr(T) = \nabla ptt(T) \setminus \nabla conf(T)$.
   Следовательно, $\nabla perr(T) \subseteq tt(T_i,L)_L \setminus \nabla conf(T)$.
   Поскольку мы уже доказали, что $\nabla conf(T) = conf(T_i,L)_L$,
   имеем $\nabla perr(T) \subseteq tt(T_i,L)_L \setminus conf(T_i,L)_L = err(T_i,L)_L$.
   Пусть трасса $\sigma \in \nabla perr(T)$.
   Если бы трасса $\sigma \in err(T_i,L)_L \setminus perr(T_i,L)_L$, то у нее был бы строгий префикс, являющийся ошибкой и, следовательно, был бы строгий префикс μ, являющийся первичной ошибкой: $\mu < \sigma$ и $\mu \in perr(T_i,L)_L$.
   Но по доказанному $perr(T_i,L)_L \subseteq \nabla perr(T)$, значит $\mu \in \nabla perr(T)$.

Тогда у первичной ∇-ошибки σ быд бы строгий префикс μ, являющийся первичной ∇-ошибкой, чего быть не может, поскольку по замечанию 9 первичные ∇-ошибки образуют антицепь по отношению «≤».

Следовательно, $\sigma \in \boldsymbol{err}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}}$ и $\sigma \notin \boldsymbol{err}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}} \setminus \boldsymbol{perr}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}}$,

что влечет $\sigma \in \boldsymbol{perr}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}}$.

Тем самым, $\nabla\boldsymbol{perr}(\mathbf{T}) \subseteq \boldsymbol{err}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}}$ влечет $\nabla\boldsymbol{perr}(\mathbf{T}) \subseteq \boldsymbol{perr}(\mathbf{T_i},\mathbf{L})_{\mathbf{L}}$.

6.16. Доказательство леммы 7

1. Покажем, что если трасса $\sigma^{\#} \in \boldsymbol{\Sigma^{0\sim}}$, кнопка $Q \in \mathbf{Q}$ и $Q \subseteq \cup\boldsymbol{Ip}(\sigma)$, то Q ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** σ.

   Допустим, что утверждение не верно:

   $\sigma^{\#} \in \boldsymbol{\Sigma^{0\sim}}$, $Q \in \mathbf{Q}$, $Q \subseteq \cup\boldsymbol{Ip}(\sigma)$, но Q ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** σ.

   Тогда по определению ~безопасности **Q**-кнопки после некоторой трассы $\mu \in \boldsymbol{di^{\sim}}(\sigma) \cap \boldsymbol{SafeBy}(\boldsymbol{\Sigma})$ **Q**-кнопка Q безопасна.

   Но тогда, поскольку $Q \subseteq \cup\boldsymbol{Ip}(\sigma)$, трасса σ заканчивается отказом, для которого нарушается условие ~конформности, что противоречит $\sigma^{\#} \in \boldsymbol{\Sigma^{0\sim}}$.

2. Докажем выполнение **Q**-свойства: $\forall\sigma^{\#} \in \boldsymbol{\Sigma^{0\sim}}\ \forall Q \in \mathbf{Q}\ \ \sigma^{\#}\cdot\langle\cancel{Q}\rangle \in \boldsymbol{\Sigma^{1\sim}}$.

   Если ~финальная трасса не заканчивается и не продолжается дивергенцией и разрушением, то это трасса $\sigma^{\#} \in \boldsymbol{\Sigma^{0\sim}}$.

2.1. Пусть Q ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** σ.

   Тогда по правилам вывода $\sigma^{\#}\cdot\langle\cancel{Q}\rangle \in \boldsymbol{\Sigma^{1\sim}}$.

2.2. Пусть Q ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** σ.

   Тогда по доказанному утверждению 1 данной леммы $Q \not\subseteq \cup\boldsymbol{Ip}(\sigma)$.

   А тогда по правилам вывода $\sigma^{\#}\cdot\langle\cancel{Q}\rangle \in \boldsymbol{\Sigma^{1\sim}}$.

3. Докажем выполнение **R**-свойства: $\forall\sigma^{\#} \in \boldsymbol{\Sigma^{0\sim}}\ \forall R \in \mathbf{R}$

   $(\sigma^{\#}\cdot\langle\cancel{R}\rangle \notin \boldsymbol{\Sigma^{1\sim}} \Leftrightarrow \boldsymbol{Ip}(\sigma) \neq \varnothing\ \&\ R \subseteq \cup\boldsymbol{Ip}(\sigma))\ \&$

   $(\boldsymbol{Ip}(\sigma) \neq \varnothing\ \&\ R \subseteq \cup\boldsymbol{Ip}(\sigma) \Rightarrow \sigma^{\#}\cdot\langle R^{\#}\rangle \in \boldsymbol{\Sigma^{0\sim}})$.

   Сначала покажем, что если $\sigma^{\#}\cdot\langle\cancel{R}\rangle \notin \boldsymbol{\Sigma^{1\sim}}$, то $\boldsymbol{Ip}(\sigma) \neq \varnothing\ \&\ R \subseteq \cup\boldsymbol{Ip}(\sigma)$.

   Это непосредственно следует из правил вывода.

   Теперь покажем, что если $\boldsymbol{Ip}(\sigma) \neq \varnothing\ \&\ R \subseteq \cup\boldsymbol{Ip}(\sigma)$,

   то 1) $\sigma^{\#}\cdot\langle\cancel{R}\rangle \notin \boldsymbol{\Sigma^{1\sim}}$ и 2) $\sigma^{\#}\cdot\langle R^{\#}\rangle \in \boldsymbol{\Sigma^{0\sim}}$.

   Поскольку $\boldsymbol{Ip}(\sigma) \neq \varnothing\ \&\ R \subseteq \cup\boldsymbol{Ip}(\sigma)$, по лемме 4 R ~***conf*** $\boldsymbol{\Sigma}$ ***after*** σ.

   Условие R ~***conf*** $\boldsymbol{\Sigma}$ ***after*** σ влечет R ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** σ,

   Что влечет по правилам вывода $\sigma^{\#}\cdot\langle\cancel{R}\rangle \notin \boldsymbol{\Sigma^{1\sim}}$, то есть выполнение условия 1.

Также условие $R \sim_{\boldsymbol{conf}\,\Sigma\,\boldsymbol{after}}\,\sigma$ по правилам вывода влечет $\sigma^{\#}\cdot\langle R^{\#}\rangle\in\boldsymbol{\Sigma^{0\sim}}$, то есть выполнение условия 2.

4. Выполнение $\Delta\gamma$-свойства с дополнительным условием непосредственно следует из правил вывода.

6.17. Доказательство леммы 8

Если $\langle\gamma\rangle\in\boldsymbol{\Sigma}$, то $\boldsymbol{\Sigma^{01\sim}}=\{\epsilon,\langle\gamma\rangle\}$ и проверка выполнения свойств трассовой модели тривиальна. Далее будет предполагать, что $\langle\gamma\rangle\notin\boldsymbol{\Sigma}$.

1. Непустота и префикс-замкнутость множества $\boldsymbol{\Sigma^{01\sim}}$ непосредственно следуют из правил вывода.
2. Допустимость.

   Если трасса $\sigma^{\#}\in\boldsymbol{\Sigma^{0\sim}}$, то трасса σ ~конформная, и она по определению не содержит дивергенции и разрушения.

   Трассы множества $\boldsymbol{\Sigma^{1\sim}}$ по правилам вывода могут содержать дивергенцию и разрушение только как последние символы.
3. Согласованность.

   Если трасса σ ~конформна, то она согласована, так как,

   во-первых, по определению ~конформности действия после трассы это действие не запрещается постфиксом отказов трассы, и,

   во-вторых, дивергенция и разрушение не являются ~конформными продолжениями.

   Согласованность трасс из множества $\boldsymbol{\Sigma^{0\sim}}$ следует из согласованности ~конформных трасс.

   Покажем, что продолжение трассы $\sigma^{\#}\in\boldsymbol{\Sigma^{0\sim}}$ не-отказом $\boldsymbol{\Rightarrow}$ также согласовано: если $\boldsymbol{\Rightarrow}\in\cup\boldsymbol{Ip}(\sigma^{\#})$, то $\sigma^{\#}\cdot\langle\boldsymbol{\Rightarrow}\rangle\notin\boldsymbol{\Sigma^{1\sim}}$.

   Действительно, если $\boldsymbol{\Rightarrow}\in\cup\boldsymbol{Ip}(\sigma^{\#})$, то $\boldsymbol{Ip}(\sigma^{\#})\neq\varnothing$ & $P^{\#}\in\boldsymbol{Ip}(\sigma^{\#})$, что влечет $\boldsymbol{Ip}(\sigma)\neq\varnothing$ & $P\subseteq\cup\boldsymbol{Ip}(\sigma)$. А тогда по **R**-свойству (лемма 7) $\sigma^{\#}\cdot\langle\boldsymbol{\Rightarrow}\rangle\notin\boldsymbol{\Sigma^{1\sim}}$.

   Дивергенции и разрушению в ~финальных трассах могут предшествовать только не-отказы, то есть не отказы.
4. Конвергентность.

   ~финальная трасса, не содержащая и не продолжающаяся во множестве ~финальных трасс разрушением и дивергенцией, – это трасса $\sigma^{\#}\in\boldsymbol{\Sigma^{0\sim}}$.

   Рассмотрим произвольный отказ $R\in\mathbf{R}$.

Нам достаточно показать, что во множестве $\boldsymbol{\Sigma}^{01\sim}$ трасса $\sigma^{\#}$ продолжается отказом $R^{\#}$ или не-отказом $\not R$, поскольку $\not R \in R^{\#}$.

Но это следует из **R**-свойства (лемма 7): $\sigma^{\#}\cdot\langle \not R\rangle \notin \boldsymbol{\Sigma}^{1\sim} \Rightarrow \sigma^{\#}\cdot\langle R^{\#}\rangle \in \boldsymbol{\Sigma}^{0\sim}$.

5. Полнота (замкнутость по ***i***-операции).

Пусть имеется ~финальная трасса вида

$\sigma_1=\mu^{\#}\cdot\lambda^{\#}$, или

$\sigma_2=\mu^{\#}\cdot\lambda^{\#}\cdot\langle \not p\rangle$, или

$\sigma_3=\mu^{\#}\cdot\lambda^{\#}\cdot\langle \not p,\gamma\rangle$, или

$\sigma_4=\mu^{\#}\cdot\lambda^{\#}\cdot\langle \not p,\Delta\rangle$ (заметим, что $(\mu\cdot\lambda)^{\#}=\mu^{\#}\cdot\lambda^{\#}$).

Пусть также трасса $\mu^{\#}$ заканчивается отказом, и для некоторого отказа $R^{\#}\in\mathbf{R}^{\#}$ не продолжается во множестве ~финальных трасс никакими действиями из $R^{\#}$.

Нужно показать, что также ~финальна трасса

$\sigma_1`=\mu^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}$, или

$\sigma_2`=\mu^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\cdot\langle \not p\rangle$, или

$\sigma_3`=\mu^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\cdot\langle \not p,\gamma\rangle$, или

$\sigma_4`=\mu^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\cdot\langle \not p,\Delta\rangle$, соответственно.

Трасса $\mu^{\#}$ не продолжается не-отказом $\not R$, поскольку $\not R\in R^{\#}$.

Следовательно, по **R**-свойству (лемма 7) $R\subseteq\cup\boldsymbol{Ip}(\mu)$.

Отсюда следует, что,

во-первых, $\boldsymbol{di}^{\sim}(\mu\cdot\langle R\rangle\cdot\lambda)=\boldsymbol{di}^{\sim}(\mu\cdot\lambda)$ и,

во-вторых, $P\subseteq\cup\boldsymbol{Ip}(\mu\cdot\langle R\rangle\cdot\lambda) \Leftrightarrow P\subseteq\cup\boldsymbol{Ip}(\mu\cdot\lambda)$.

Эти условия однозначно определяют наличие или отсутствие продолжения ~финальной **L**-трассы наблюдением, не-отказом и далее дивергенцией или разрушением.

Поэтому из наличия ~финальной трассы σ_i следует наличие ~финальной трассы $\sigma_i`$.

6.18. Доказательство леммы 9

Прежде всего, заметим, что, если $\pi\in\boldsymbol{d}(\sigma^{\#})$, то существует такая трасса $\mu\in(\mathbf{L}\cup\mathbf{R})^{*}$, что $\pi=\mu^{\#}$.

1. Покажем сохранение **Q**-свойства.

Пусть $Q\in\mathbf{Q}$ и $\mu^{\#}\in\boldsymbol{d}(\sigma^{\#})$.

Тогда по **Q**-свойству множества $\sigma^{\#}\cdot\langle \not Q\rangle\in\mathbf{N}$.

А тогда, поскольку $\mu^{\#}\in\boldsymbol{d}(\sigma^{\#})$ влечет $\mu^{\#}\cdot\langle\text{Ǫ}\rangle\in\boldsymbol{d}(\sigma^{\#}\cdot\langle\text{Ǫ}\rangle)$, что влечет $\mu^{\#}\cdot\langle\text{Ǫ}\rangle\in\cup\boldsymbol{d}(\mathbf{N})$.

2. Покажем сохранение $\Delta\gamma$-свойства.

Пусть $\cup\boldsymbol{d}(\mathbf{N})\neq\{\epsilon,\langle\gamma\rangle\}$, то, очевидно, $\mathbf{N}\neq\{\epsilon,\langle\gamma\rangle\}$.

А тогда по $\Delta\gamma$-свойству множества $\mathbf{N}$ оно содержит только трассы вида $\sigma^{\#}$, $\sigma^{\#}\cdot\langle\text{Ꝑ}\rangle$, $\sigma^{\#}\cdot\langle\text{Ꝑ},\Delta\rangle$ и $\sigma^{\#}\cdot\langle\text{Ꝑ},\gamma\rangle$.

Очевидно, что $\cup\boldsymbol{d}(\mathbf{N})$ тоже содержит только трассы такого вида.

Если $\sigma^{\#}\cdot\langle\text{Ꝑ}\rangle\in\cup\boldsymbol{d}(\mathbf{N})$, то, очевидно, найдется такая трасса $\sigma`^{\#}\cdot\langle\text{Ꝑ}\rangle\in\mathbf{N}$, что $\sigma^{\#}\in\boldsymbol{d}(\sigma`^{\#})$.

Но тогда по $\Delta\gamma$-свойству множества $\mathbf{N}$ имеет место $\sigma`^{\#}\cdot\langle\text{Ꝑ},\Delta\rangle\in\mathbf{N}$ или $\sigma`^{\#}\cdot\langle\text{Ꝑ},\gamma\rangle\in\mathbf{N}$.

Но тогда $\sigma^{\#}\cdot\langle\text{Ꝑ},\Delta\rangle\in\cup\boldsymbol{d}(\mathbf{N})$ или $\sigma^{\#}\cdot\langle\text{Ꝑ},\gamma\rangle\in\cup\boldsymbol{d}(\mathbf{N})$.

6.19. Доказательство леммы 10

Сохранение свойств префикс-замкнутости, допустимости, согласованности, конвергентности и полноты при ***d***-замыкании доказывается тривиально.
Свойство ***d***-замкнутости после ***d***-замыкания также, очевидно, выполняется.

6.20. Доказательство леммы 11

Утверждение 1 непосредственно следует из лемм 8 и 10,
а утверждения 2 и 3 – из лемм 7 и 9.

6.21. Доказательство леммы 12

1. Необходимость.

Пусть u ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** σ.

1.1. Пусть $\mathsf{u}\in\mathbf{R}$.

Тогда для кнопки $\mathsf{P}=\mathsf{u}$ имеем P ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** σ.

1.2. Пусть $\mathsf{u}\in\mathbf{L}$.

Тогда по определению ~безопасности действия имеем u ***safe by*** $\boldsymbol{\Sigma}$ ***after*** μ для некоторой трассы $\mu\in\boldsymbol{di}^{\sim}(\sigma)\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma})$.

Но тогда для некоторой кнопки $\mathsf{P}\in\mathbf{R}\cup\mathbf{Q}$ такой, что $\mathsf{u}\in\mathsf{P}$,
имеет место P ***safe by*** $\boldsymbol{\Sigma}$ ***after*** μ.

1.2.1. Пусть $\mathsf{P}\in\mathbf{Q}$.

Тогда по определению ~безопасности **Q**-кнопки P ***safe by*** Σ ***after*** μ влечет P ***safe~by*** Σ ***after*** σ.

1.2.2. Пусть $P \in \mathbf{R}$.

Тогда P ***safe by*** Σ ***after*** μ влечет $\forall z \in P$ z ***safe by*** Σ ***after*** μ,

что влечет по определению ~безопасности действия

$\forall z \in P$ z ***safe~by*** Σ ***after*** σ,

что влечет по определению ~безопасности **R**-кнопки P ***safe by*** Σ ***after*** σ.

2. Достаточность.

Пусть $u \in P$ или $u = P$ и $P \in \mathbf{R}$, и P ***safe~by*** Σ ***after*** σ.

2.1. Пусть $u = P$.

Тогда u ***safe~by*** Σ ***after*** σ.

2.2. Пусть $u \in P$ и $P \in \mathbf{R}$.

Тогда по определению ~безопасности **R**-кнопки

$\forall z \in P$ z ***safe~by*** Σ ***after*** σ,

в том числе u ***safe~by*** Σ ***after*** σ.

2.3. Пусть $u \in P$ и $P \in \mathbf{Q}$.

Тогда по определению ~безопасности **Q**-кнопки Q ***safe by*** Σ ***after*** μ для некоторой трассы $\mu \in \boldsymbol{di}^{\sim}(\sigma) \cap \boldsymbol{SafeBy}(\Sigma)$.

Но тогда u ***safe by*** Σ ***after*** μ,

что по определению ~безопасности действия влечет u ***safe~by*** Σ ***after*** σ.

6.22. Доказательство леммы 13

1. Сначала докажем следующее вспомогательное утверждение:

Если наблюдение u ~конформно после трассы σ, но не ~конформно после трассы $\kappa \in \boldsymbol{d}(\sigma)$, то оно не ~безопасно после трассы κ:

$\kappa \in \boldsymbol{d}(\sigma)$ & u ***~conf*** Σ ***after*** σ & u ~~***~conf***~~ Σ ***after*** κ $\Rightarrow$ u ~~***safe~by***~~ Σ ***after*** κ.

Допустим обратное: u ***safe~by*** Σ ***after*** κ.

Поскольку u ~~***~conf***~~ Σ ***after*** κ, для наблюдения u после трассы σ имеет место нарушение дополнительных условий ~конформности.

1.1. Пусть u действие.

Тогда либо

a) $u \notin \cup \boldsymbol{Ip}(\sigma)$, либо

b) для некоторой трассы $\mu \in \boldsymbol{di}^{\sim}(\kappa) \cap \boldsymbol{SafeBy}(\Sigma)$ имеет место u ***safe by*** Σ ***after*** μ, но $\mu \cdot \langle u \rangle \notin \Sigma$.

Тогда, поскольку $\kappa \in \boldsymbol{d}(\sigma)$, имеем $\mu \in \boldsymbol{di}^{\sim}(\sigma)$ и, следовательно, нарушены условия ~конформности действия u после трассы σ, что противоречит u ***~conf*** Σ ***after*** σ.

1.2. Пусть u непустой **R**-отказ.

Тогда либо

a) для некоторой трассы $\mu \in \boldsymbol{di}^{\sim}(\kappa \cdot \langle u \rangle) \cap \boldsymbol{SafeBy}(\Sigma)$ и некоторой **Q**-кнопки $Q \subseteq \cup \boldsymbol{Ip}(\sigma \cdot \langle u \rangle)$ имеет место Q ***safe by*** Σ ***after*** μ, либо

b) для некоторой трассы $\mu \in \boldsymbol{di}^{\sim}(\kappa \cdot \langle u \rangle) \cap \boldsymbol{SafeBy}(\Sigma)$ и некоторой **R**-кнопки $R \subseteq \cup \boldsymbol{Ip}(\sigma \cdot \langle u \rangle)$ имеет место R ***safe by*** Σ ***after*** μ, но $\mu \cdot \langle R \rangle \notin \boldsymbol{\Sigma}$.

Тогда, поскольку $\kappa \in \boldsymbol{d}(\sigma)$ и, следовательно, $\kappa \cdot \langle u \rangle \in \boldsymbol{d}(\sigma \cdot \langle u \rangle)$, имеем $\mu \in \boldsymbol{di}^{\sim}(\sigma \cdot \langle u \rangle)$ и, следовательно, нарушены условия ~конформности непустого **R**-отказа u после трассы σ, что противоречит u ***~conf*** Σ ***after*** σ.

1.3. Пусть u пустой **R**-отказ.

Тогда дополнительных условий нет.

Итак, мы пришли к противоречию и, следовательно, наше допущение не верно, и вспомогательное утверждение доказано.

2. Теперь докажем основное утверждение.

Пусть трасса $\kappa^{\#} \in \boldsymbol{\Sigma^{0\sim}}$, наблюдение $u^{\#} \in \mathbf{L} \cup \mathbf{R}^{\#}$ и трасса $\kappa^{\#} \cdot \langle u^{\#} \rangle \in (\cup \boldsymbol{d}(\boldsymbol{\Sigma^{01\sim}})) \setminus \boldsymbol{\Sigma^{0\sim}}$.

Нам нужно показать, что $u^{\#}$ ***safe***$_{\gamma\Delta}$ $\Sigma^{\sim}$ ***after*** $\kappa^{\#}$.

Поскольку $\kappa^{\#} \cdot \langle u^{\#} \rangle \in \cup \boldsymbol{d}(\boldsymbol{\Sigma^{01\sim}})$,

найдется такая трасса $\sigma^{\#} \cdot \langle u^{\#} \rangle \in \boldsymbol{\Sigma^{0\sim}}$, что $\kappa^{\#} \cdot \langle u^{\#} \rangle \in \boldsymbol{d}(\sigma^{\#} \cdot \langle u^{\#} \rangle)$.

Поскольку также $\kappa^{\#} \cdot \langle u^{\#} \rangle \notin \boldsymbol{\Sigma^{0\sim}}$,

по правилам вывода имеем: u ***~conf*** Σ ***after*** σ, но u ~~***~conf***~~ Σ ***after*** κ.

По вспомогательному утверждению u ~~***safe~by***~~ Σ ***after*** κ.

Отсюда по лемме 12 для каждой кнопки $P \in \mathbf{R} \cup \mathbf{Q}$, разрешающей наблюдение u, имеет место P ~~***safe~by***~~ Σ ***after*** κ.

Тогда по правилам вывода для каждой кнопки P, разрешающей наблюдение u, имеет место $\kappa^{\#}\cdot\langle\not{P},\gamma\rangle\in\mathbf{\Sigma^{1\sim}}$.

Отсюда для каждой кнопки P, разрешающей наблюдение u, имеет место $P^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{\Sigma^{\sim}}$ ***after*** $\kappa^{\#}$.

Отсюда $u^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{\Sigma^{\sim}}$ ***after*** $\kappa^{\#}$, что и требовалось доказать.

6.23. Доказательство леммы 14

1. Необходимость.

Пусть $\sigma^{\#}\in\mathbf{N}$, $P\in\mathbf{R}\cup\mathbf{Q}$ и $P^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{N}$ ***after*** σ.

Имеем: $P^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{N}$ ***after*** σ $\Rightarrow$ $\sigma^{\#}\cdot\langle\Delta\rangle\notin\mathbf{N}$ & $\forall z\in P^{\#}$ $\sigma^{\#}\cdot\langle z,\gamma\rangle\notin\mathbf{N}$.

Поскольку $\not{P}\in P^{\#}$, имеем $\sigma^{\#}\cdot\langle\not{P},\gamma\rangle\notin\mathbf{N}$.

2. Достаточность.

Обратно, пусть $\sigma^{\#}\cdot\langle\not{P},\gamma\rangle\notin\mathbf{N}$.

Тогда по $\Delta\gamma$-свойству $\sigma^{\#}\cdot\langle\Delta\rangle\notin\mathbf{N}$ & $\forall z\in P$ $\sigma^{\#}\cdot\langle z,\gamma\rangle\notin\mathbf{N}$.

А тогда, поскольку $P^{\#}=P\cup\{\not{P}\}$ и $\sigma^{\#}\cdot\langle\not{P},\gamma\rangle\notin\mathbf{N}$,

имеем $\sigma^{\#}\cdot\langle\Delta\rangle\notin\mathbf{N}$ & $\forall z\in P^{\#}$ $\sigma^{\#}\cdot\langle z,\gamma\rangle\notin\mathbf{N}$.

что влечет $P^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{N}$ ***after*** σ.

6.24. Доказательство леммы 15

1. Покажем, что $\mu^{\#}\cdot\langle\not{P},\gamma\rangle\notin\cup\boldsymbol{d}(\mathbf{\Sigma^{01\sim}})$ $\Rightarrow$ $\mu^{\#}\cdot\langle\not{P},\gamma\rangle\notin\mathbf{\Sigma^{1\sim}}$.

Это следует из того, что $\mathbf{\Sigma^{1\sim}}\subseteq\cup\boldsymbol{d}(\mathbf{\Sigma^{01\sim}})$.

2. Покажем, что $\mu^{\#}\cdot\langle\not{P},\gamma\rangle\notin\mathbf{\Sigma^{1\sim}}$ $\Rightarrow$ $\mu^{\#}\cdot\langle\not{P},\gamma\rangle\notin\cup\boldsymbol{d}(\mathbf{\Sigma^{01\sim}})$.

Допустим утверждение не верно: $\mu^{\#}\cdot\langle\not{P},\gamma\rangle\notin\mathbf{\Sigma^{1\sim}}$, но $\mu^{\#}\cdot\langle\not{P},\gamma\rangle\in\cup\boldsymbol{d}(\mathbf{\Sigma^{01\sim}})$.

Тогда найдется такая трасса $\sigma^{\#}\in\mathbf{\Sigma^{0\sim}}$, что $\sigma^{\#}\cdot\langle\not{P},\gamma\rangle\in\mathbf{\Sigma^{1\sim}}$ и $\mu\in\boldsymbol{d}(\sigma)$.

Далее $\mu^{\#}\cdot\langle\not{P},\gamma\rangle\notin\mathbf{\Sigma^{1\sim}}$ влечет по правилам вывода P ***safe~by*** $\mathbf{\Sigma}$ ***after*** μ,

а $\sigma^{\#}\cdot\langle\not{P},\gamma\rangle\in\mathbf{\Sigma^{1\sim}}$ влечет P ***safe~by*** $\mathbf{\Sigma}$ ***after*** σ.

Однако по лемме 3 это противоречит $\mu\in\boldsymbol{d}(\sigma)$.

Мы пришли к противоречию и, следовательно, $\mu^{\#}\cdot\langle\not{P},\gamma\rangle\notin\cup\boldsymbol{d}(\mathbf{\Sigma^{01\sim}})$,

что и требовалось доказать.

6.25. Доказательство теоремы 10

$P^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{\Sigma^{\sim}}$ ***after*** $\mu^{\#}$

$\Leftrightarrow$ по замечанию 11 и лемме 14

$\mu^{\#}\cdot\langle\not\Rightarrow,\gamma\rangle\notin\boldsymbol{\Sigma^{\sim}}$

$\Leftrightarrow$ по замечанию 11

$\mu^{\#}\cdot\langle\not\Rightarrow,\gamma\rangle\notin\cup\boldsymbol{d}(\boldsymbol{\Sigma^{01\sim}})$

$\Leftrightarrow$ по лемме 15

$\mu^{\#}\cdot\langle\not\Rightarrow,\gamma\rangle\notin\boldsymbol{\Sigma^{1\sim}}$.

6.26. Доказательство леммы 16

$P^{\#}$ $\boldsymbol{safe}_{\gamma\Delta}$ $\boldsymbol{\Sigma^{\sim}}$ ***after*** $\kappa^{\#}\cdot\lambda^{\#}$

$\Rightarrow$ по определению $\boldsymbol{safe}_{\gamma\Delta}$, поскольку $\not\Rightarrow\in P^{\#}$,

$\kappa^{\#}\cdot\lambda^{\#}\cdot\langle\not\Rightarrow,\gamma\rangle\notin\boldsymbol{\Sigma^{\sim}}$

$\Rightarrow$ по замкнутости трассовой модели $\boldsymbol{\Sigma^{\sim}}$

$\kappa^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\cdot\langle\not\Rightarrow,\gamma\rangle\notin\boldsymbol{\Sigma^{\sim}}$

$\Rightarrow$ поскольку $\boldsymbol{\Sigma^{1\sim}}\subseteq\boldsymbol{\Sigma^{\sim}}$

$\kappa^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\cdot\langle\not\Rightarrow,\gamma\rangle\notin\boldsymbol{\Sigma^{1\sim}}$

$\Rightarrow$ так как $\kappa^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\in\boldsymbol{\Sigma^{0\sim}}$, по теореме 10

$P^{\#}$ $\boldsymbol{safe}_{\gamma\Delta}$ $\boldsymbol{\Sigma^{\sim}}$ ***after*** $\kappa^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}$).

6.27. Доказательство теоремы 11

1. Пусть пустая трасса опасна в исходной спецификации $\boldsymbol{\Sigma}$.

   Тогда по правилам вывода множество $\langle\gamma\rangle\in\boldsymbol{\Sigma^{01\sim}}$, следовательно, $\langle\gamma\rangle\in\boldsymbol{\Sigma^{\sim}}$.

   В этом случае в $\boldsymbol{\Sigma^{\sim}}$ нет безопасных трасс, и пустое множество $\boldsymbol{SafeBy}(\boldsymbol{T^{\sim}},\boldsymbol{L})$ однозначно определяется множеством ~финальных трасс $\{\epsilon,\langle\gamma\rangle\}$.

2. Пусть пустая трасса безопасна в исходной спецификации $\boldsymbol{\Sigma}$.

2.1. Сначала покажем, что безопасность ~финальных **L**-трасс однозначно определяется множеством ~финальных трасс.

   По теореме 10 после трассы $\sigma^{\#}\in\boldsymbol{\Sigma^{0\sim}}$ кнопка $P^{\#}$ безопасна тогда и только тогда, когда $\sigma^{\#}\cdot\langle\not\Rightarrow,\gamma\rangle\notin\boldsymbol{\Sigma^{1\sim}}$, что однозначно определяется множеством ~финальных трасс.

2.2. Теперь покажем, что все ~финальные **L**-трассы безопасны по отношению $\boldsymbol{safe}_{\gamma\Delta}$: $\boldsymbol{\Sigma^{0\sim}}\subseteq\boldsymbol{SafeBy}(\boldsymbol{T^{\sim}},\boldsymbol{L})$.

Для этого нужно показать, что

1) пустая трасса безопасна в ~пополнении, и

2) для любой ~финальной **L**-трассы $\sigma^{\#}\cdot\langle u^{\#}\rangle$

наблюдение $u^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{\Sigma^{\sim}}$ ***after*** $\sigma^{\#}$.

2.2.1. Пустая трасса безопасна в ~пополнении, поскольку она безопасна в исходной спецификации и, следовательно, по правилам вывода $\langle\gamma\rangle\notin\mathbf{\Sigma^{1\sim}}$, что влечет $\langle\gamma\rangle\notin\mathbf{\Sigma^{\sim}}$.

2.2.2. Покажем, что для ~финальной **L**-трассы $\sigma^{\#}\cdot\langle u^{\#}\rangle$ имеет место $u^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{\Sigma^{\sim}}$ ***after*** $\sigma^{\#}$.

По правилам вывода u ***~conf*** $\mathbf{\Sigma}$ ***after*** σ

и, следовательно, u ***safe~by*** $\mathbf{\Sigma}$ ***after*** σ.

По лемме 12 u ***safe~by*** $\mathbf{\Sigma}$ ***after*** σ влечет существование такой кнопки P,

которая разрешает наблюдение u и P ***safe~by*** $\mathbf{\Sigma}$ ***after*** σ.

Тогда кнопка $P^{\#}$ разрешает наблюдение $u^{\#}$

и по правилам вывода $\sigma^{\#}\cdot\langle\text{Д},\gamma\rangle\notin\mathbf{\Sigma^{1\sim}}$.

Отсюда по теореме 10 для кнопки P имеем $P^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{\Sigma^{\sim}}$ ***after*** $\sigma^{\#}$.

Тем самым, $u^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{\Sigma^{\sim}}$ ***after*** $\sigma^{\#}$.

2.3. Теперь покажем, что все **L**-трассы безопасные по отношению по отношению ***safe***$_{\gamma\Delta}$, являются ~финальными. $\mathbf{SafeBy(T^{\sim},L)\subseteq\Sigma^{0\sim}}$.

Поскольку $\mathbf{SafeBy(T^{\sim},L)}$ содержит только $\mathbf{R}^{\#}$-трассы, являющиеся **L**-трассами, нам надо показать, что каждая не ~финальная $\mathbf{L\text{-}R}^{\#}$-трасса $\kappa^{\#}$ во множестве $\mathbf{\cup d(\Sigma^{01\sim})}$ опасна по отношению ***safe***$_{\gamma\Delta}$.

Такая трасса $\kappa^{\#}$ добавляется в $\mathbf{\cup d(\Sigma^{01\sim})}$ при ***d***-замыкании.

Нам достаточно доказать опасность трассы $\kappa^{\#}$ минимальной длины.

Поскольку пустая трасса безопасна в $\mathbf{\Sigma}$, она ~конформна и, следовательно, ~финальна.

Следовательно, трасса $\kappa^{\#}$ минимальной длины имеет вид $\kappa^{\#}=\kappa_1{}^{\#}\cdot\langle u^{\#}\rangle$, где трасса $\kappa_1{}^{\#}$ ~финальна.

Тогда по лемме 13 $u^{\#}$ ~~***safe***~~$_{\gamma\Delta}$ $\mathbf{\Sigma^{\sim}}$ ***after*** $\kappa_1{}^{\#}$, что влечет опасность трассы $\kappa^{\#}$.

6.28. Доказательство теоремы 12

1. Докажем утверждение 1: все трассы из множества $\mathbf{\Sigma^{0\sim}}$ **L**-актуальны.

Это непосредственно следует из того, что все трассы из множества $\mathbf{\Sigma^{0\sim}}$ являются ~конформными трассами, а условие ~конформности включает в себя условие **L**-актуальности из теоремы 8.

2. Докажем утверждение 2: **L**-наблюдение $u^{\#}\in\mathbf{L}\cup\mathbf{R}^{\#}$, безопасное после трассы $\sigma^{\#}\in\mathbf{\Sigma^{0\sim}}$, **L**-актуально тогда и только тогда, когда либо 1) $u\in\mathbf{L}$ и $u\notin\cup\boldsymbol{Ip}(\sigma)$, либо 2) $u\in\mathbf{R}$ и для каждой кнопки $Q\in\mathbf{Q}$ такой, что $Q\subseteq u\cup\cup\boldsymbol{Ip}(\sigma)$, трасса $\mu^{\#}\cdot\langle\cancel{Q},\gamma\rangle\in\mathbf{\Sigma^{1\sim}}$ для каждой трассы $\mu^{\#}\in\mathbf{\Sigma^{0\sim}}$ такой, что $\mu\in\boldsymbol{di}^{\sim}(\sigma\cdot\langle u\rangle)$.

   По доказанному утверждению 1 трасса $\sigma^{\#}\in\mathbf{\Sigma^{0\sim}}$ **L**-актуальна.

   По теореме 8 для того, чтобы наблюдение $u^{\#}\in\mathbf{L}\cup\mathbf{R}^{\#}$, безопасное после **L**-актуальной трассы $\sigma^{\#}$, было **L**-актуальным,
   необходимо и достаточно, чтобы либо
   1) $u\in\mathbf{L}$ и $u\notin\cup\boldsymbol{Ip}(\sigma)$, либо
   2) $u\in\mathbf{R}$ и для каждой кнопки $Q\in\mathbf{Q}$ такой, что $Q\subseteq u\cup\cup\boldsymbol{Ip}(\sigma)$, кнопка $Q^{\#}$ была опасна после каждой безопасной в **L**-трассы $\mu^{\#}$, для которой $\mu\in\boldsymbol{di}^{\sim}(\sigma\cdot\langle u\rangle)$.

   По теореме 11 трасса $\mu^{\#}$ является безопасной **L**-трассой тогда и только тогда, когда $\mu^{\#}\in\mathbf{\Sigma^{0\sim}}$.

   По теореме 10 кнопка $Q^{\#}$ опасна после трассы μ тогда и только тогда, когда трасса $\mu^{\#}\cdot\langle\cancel{Q},\gamma\rangle\in\mathbf{\Sigma^{1\sim}}$.

   Отсюда непосредственно следует утверждение 2 теоремы.

6.29. Доказательство леммы 17

Если пустая трасса опасна в исходной спецификации **Σ**,
то в $\mathbf{\Sigma^{\sim}}$ нет безопасных трасс по правилам вывода.

В противном случае по теореме 11 безопасные **L**-трассы $\mathbf{\Sigma^{\sim}}$ – это ее ~финальные **L**-трассы, то есть трассы из множества $\mathbf{\Sigma^{0\sim}}=\sim\boldsymbol{conf}(\mathbf{T})^{\#}$.

Рассмотрим **L**-трассу $\sigma^{\#}$, которая ~финальна, то есть трасса σ ~конформна.

По правилам вывода для трассы $\sigma\in\sim\boldsymbol{conf}(\mathbf{T})$ и любой кнопки $P\in\mathbf{R}\cup\mathbf{Q}$ имеет место:

$$P\ \boldsymbol{safe\sim by}\ \mathbf{\Sigma}\ \boldsymbol{after}\ \sigma\ \Leftrightarrow\ \sigma^{\#}\cdot\langle\cancel{P},\gamma\rangle\in\mathbf{\Sigma^{1\sim}}.$$

L-трассы из $\mathbf{\Sigma^{\sim}}$ не продолжаются дивергенцией и разрушением, поэтому:

$$\sigma^{\#}\cdot\langle\cancel{P},\gamma\rangle\in\mathbf{\Sigma^{1\sim}}\ \Leftrightarrow\ P^{\#}\ \boldsymbol{safe}_{\gamma\Delta}\ \mathbf{\Sigma^{\sim}}\ \boldsymbol{after}\ \sigma^{\#}.$$

В результате:

P ***safe~by*** Σ ***after*** σ $\Leftrightarrow$ $\mathsf{P}^{\#}$ $\boldsymbol{safe}_{\gamma\Delta}$ $\Sigma^{\sim}$ ***after*** $\sigma^{\#}$.

6.30. Доказательство леммы 18

1. Сначала покажем выполнение равенства $\boldsymbol{SafeBy}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}}=\sim\boldsymbol{conf}(\mathbf{T})$.

   Если пустая трасса опасна в исходной спецификации Σ,

   то ~конформных трасс нет и в $\Sigma^{\sim}$ нет безопасных трасс.

   В противном случае по правилам вывода множество ~финальных **L**-трасс, приведенное к алфавиту **L**, совпадает с множеством ~конформных трасс:

   $\Sigma^{0\sim}=\sim\boldsymbol{conf}(\mathbf{T})^{\#}$, то есть $\Sigma^{0\sim}{}_{\mathbf{L}}=\sim\boldsymbol{conf}(\mathbf{T})$.

   По теореме 11 множество ~финальных **L**-трасс совпадает с множеством безопасных трасс $\Sigma^{\sim}$:

   $\Sigma^{0\sim}=\boldsymbol{SafeBy}(\mathbf{T}^{\sim},\mathbf{L})$.

   Тем самым, $\boldsymbol{SafeBy}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}}=\sim\boldsymbol{conf}(\mathbf{T})$.
2. Теперь выполнение равенства $\boldsymbol{tt}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}}=\sim\boldsymbol{ptt}(\mathbf{T})$ следует из леммы 17.

6.31. Доказательство леммы 19

1. Сначала покажем, что ~пополнение не сужает класс безопасно-тестируемых реализаций: $\boldsymbol{SafeImp}(\mathbf{T}) \subseteq \boldsymbol{SafeImp}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}}$.

   Допустим, это не так.

   Тогда существуют

   такая реализация $\mathbf{I}\in\boldsymbol{SafeImp}(\mathbf{T})$,

   такая трасса $\sigma\in\mathbf{I}$, что $\sigma^{\#}\in\boldsymbol{SafeBy}(\mathbf{T}^{\sim},\mathbf{L})$,

   и такая кнопка $\mathsf{P}\in\mathbf{R}\cup\mathbf{Q}$, что $\mathsf{P}^{\#}$ $\boldsymbol{safe}_{\gamma\Delta}$ $\Sigma^{\sim}$ ***after*** $\sigma^{\#}$,

   но P ~~***safe in***~~ $\mathbf{I}$ ***after*** σ.

   По лемме 17 условие $\mathsf{P}^{\#}$ $\boldsymbol{safe}_{\gamma\Delta}$ $\Sigma^{\sim}$ ***after*** $\sigma^{\#}$ эквивалентно условию P ***safe~by*** Σ ***after*** σ.

1.1. Пусть P – это **Q**-кнопка или пустая **R**-кнопка.

   Тогда условие P ***safe~by*** Σ ***after*** σ означает,

   что для некоторой трассы $\mu\in\boldsymbol{di}^{\sim}(\sigma)$ имеет место P ***safe by*** Σ ***after*** μ.

   В то же время условие P ~~***safe in***~~ $\mathbf{I}$ ***after*** σ означает наличие в реализации $\mathbf{I}$ хотя бы одного из следующих продолжений трассы σ: дивергенции, разрушающего действия или ненаблюдаемого отказа.

   Но тогда по лемме 1 такое продолжение есть и после трассы μ, что влечет P ~~***safe in***~~ $\mathbf{I}$ ***after*** μ.

   Тем самым, нарушается гипотеза о безопасности для спецификации Σ, что противоречит $\mathbf{I}\in\boldsymbol{SafeImp}(\mathbf{T})$.

1.2. Пусть P – это непустая **R**-кнопка.

Тогда условие P ***safe~by*** Σ ***after*** σ означает,
что каждое действие $z \in P$ ~безопасно после σ,
то есть безопасно в Σ после некоторой трассы $\mu_z \in \widetilde{di}(\sigma)$,
что означает наличие такой кнопки $P_z \in \mathbf{R} \cup \mathbf{Q}$,
что $z \in P_z$ и P_z ***safe by*** Σ ***after*** μ_z.
В то же время условие P ~~***safe in***~~ I ***after*** σ означает, что
трасса σ продолжается дивергенцией
или некоторое действие $z \in P$ разрушающее после трассы σ.
Но тогда по лемме 1 трасса μ_z тоже
продолжается дивергенцией
или это действие z разрушающее после трассы μ_z,
что в обоих случаях влечет z ~~***safe in***~~ I ***after*** μ_z.
Отсюда следует, что P_z ~~***safe in***~~ I ***after*** μ_z.
Тем самым, нарушается гипотеза о безопасности для спецификации Σ,
что противоречит $\mathrm{I} \in \mathit{SafeImp}(\mathbf{T})$.

2. Теперь покажем, что ~пополнение не расширяет класс безопасно-тестируемых реализаций: $\mathit{SafeImp}(\mathbf{T}) \supseteq \mathit{SafeImp}(\mathbf{T}\widetilde{\ },\mathbf{L})_{\mathbf{L}}$.
   Допустим, это не так.
   Тогда существуют
   такая «новая» реализация $\mathrm{I} \in \mathit{SafeImp}(\mathbf{T}\widetilde{\ },\mathbf{L})$,
   такая трасса $\sigma \in \mathit{SafeBy}(\mathbf{T})$
   и такая кнопка $P \in \mathbf{R} \cup \mathbf{Q}$,
   что $\sigma \in \mathbf{I_L}$, P ***safe by*** Σ ***after*** σ,
   но P ~~***safe in***~~ $\mathbf{I_L}$ ***after*** σ, что эквивалентно $P^{\#}$ ~~***safe in***~~ I ***after*** $\sigma^{\#}$.

2.1. Покажем, что всегда можно выбрать такую трассу σ актуальной.
   Если σ не актуальная, то, поскольку по лемме 2 пустая трасса актуальная, у трассы σ найдется неактуальный префикс $\mu \cdot \langle u \rangle$, где μ актуальная трасса.

   Поскольку $\mu \cdot \langle u \rangle$ как префикс безопасной трассы σ, является тестовой трассой, по теореме 8 (для $\mathbf{T_i}=\mathbf{T}$) u отказ, и найдется такая трасса $\mu` \in \widetilde{di}(\mu \cdot \langle u \rangle) \cap \mathit{SafeBy}(\mathbf{T})$ и $\mathbf{Q}$-кнопка $Q \subseteq u \cup \cup \mathit{Ip}(\mu)$, что $Q$ ***safe by*** $\Sigma$ ***after*** $\mu`$.

Но $\sigma \in \mathbf{I}_{\mathbf{L}}$ влечет $\mu \cdot \langle u \rangle \in \mathbf{I}_{\mathbf{L}}$,

что вместе с $Q \subseteq u \cup \cup \boldsymbol{Ip}(\mu)$ влечет $\mu \cdot \langle u, Q \rangle \in \mathbf{I}_{\mathbf{L}}$.

А тогда, поскольку $\mu` \in \boldsymbol{di}^{\sim}(\mu \cdot \langle u \rangle)$ влечет $\mu` \cdot \langle Q \rangle \in \boldsymbol{di}^{\sim}(\mu \cdot \langle u, Q \rangle)$,

имеем по лемме 1 $\mu` \cdot \langle Q \rangle \in \mathbf{I}_{\mathbf{L}}$,

что влечет Q ***~~safe in~~*** $\mathbf{I}_{\mathbf{L}}$ ***after*** $\mu`$.

Тем самым, вместо трассы σ и кнопки P мы можем взять актуальную трассу $\mu`$ ($\mu` \in \mathbf{I}_{\mathbf{L}}$, так как $\mu` \cdot \langle Q \rangle \in \mathbf{I}_{\mathbf{L}}$) и кнопку Q.

2.2. Итак, будем считать, что σ актуальная безопасная трасса.

Тогда по лемме 5 трасса σ ~конформна,

следовательно, трасса $\sigma^{\#}$ безопасная трасса ~пополнения.

2.2.1. Пусть P – это **Q**-кнопка или пустая **R**-кнопка.

Тогда, поскольку $\sigma \in \boldsymbol{di}^{\sim}(\sigma)$,

из условия P ***safe by*** $\boldsymbol{\Sigma}$ ***after*** σ следует P ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** σ.

2.2.2. Пусть P – это непустая **R**-кнопка.

Тогда для каждого действия $z \in P$ имеем z ***safe by*** $\boldsymbol{\Sigma}$ ***after*** σ.

Отсюда, поскольку $\sigma \in \boldsymbol{di}^{\sim}(\sigma)$,

имеем z ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** σ для каждого $z \in P$,

что влечет P ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** σ.

А тогда в обоих случаях по лемме 17

условие P ***safe~by*** $\boldsymbol{\Sigma}$ ***after*** σ влечет $P^{\#}$ $\boldsymbol{safe}_{\gamma\Delta}$ $\boldsymbol{\Sigma}^{\sim}$ ***after*** $\sigma^{\#}$.

Однако, поскольку $P^{\#}$ ***~~safe in~~*** $\mathbf{I}$ ***after*** $\sigma^{\#}$,

имеет место нарушение гипотезы о безопасности для ~пополнения,

что противоречит $\mathbf{I} \in \boldsymbol{SafeImp}(\mathbf{T}^{\sim}, \mathbf{L})$.

3. Покажем, что ~пополнение не сужает класс конформных реализаций: $\boldsymbol{ConfImp}(\mathbf{T}) \subseteq \boldsymbol{ConfImp}(\mathbf{T}^{\sim}, \mathbf{L})_{\mathbf{L}}$.

Допустим, это не так.

Тогда существуют

такая реализация $\mathbf{I} \in \boldsymbol{ConfImp}(\mathbf{T})$

и такая трасса $\sigma^{\#} \cdot \langle u^{\#} \rangle \in \boldsymbol{err}_{\mathbf{1}}(\mathbf{T}^{\sim}, \mathbf{L})$,

что $\sigma \cdot \langle u \rangle \in \mathbf{I}$.

Тогда существует такая кнопка $P \in \mathbf{R} \cup \mathbf{Q}$,

что $P^{\#}$ $\boldsymbol{safe}_{\gamma\Delta}$ $\boldsymbol{\Sigma}^{\sim}$ ***after*** $\sigma^{\#}$,

а кнопка P разрешает наблюдение u, то есть $u \in P$ или $P \in \mathbf{R}$ и $u = P$.

Поскольку трасса $\sigma^{\#}\cdot\langle u^{\#}\rangle$ **L**-трасса,

из условий $\sigma^{\#}\cdot\langle u^{\#}\rangle\in \boldsymbol{err_1}(\mathbf{T}^{\sim},\mathbf{L})=\boldsymbol{tt}(\mathbf{T}^{\sim},\mathbf{L})\setminus\boldsymbol{SafeBy}(\mathbf{T}^{\sim},\mathbf{L})$,

а также по лемме 18 $\boldsymbol{SafeBy}(\mathbf{T}^{\sim},\mathbf{L})=\sim\boldsymbol{conf}(\mathbf{T})^{\#}$ и $\boldsymbol{tt}(\mathbf{T}^{\sim},\mathbf{L})=\sim\boldsymbol{ptt}(\mathbf{T})^{\#}$

следует, что u ***safe*~*by*** $\boldsymbol{\Sigma}$ ***after*** σ,

но u ~~$\sim\boldsymbol{conf}$~~ $\boldsymbol{\Sigma}$ ***after*** σ.

Следовательно, не выполняются дополнительные условия ~конформности действия после трассы.

Рассмотрим два возможных случая.

3.1. $u\in P$ действие.

a) $u\in\cup\boldsymbol{Ip}(\sigma)$.

Это противоречит условию $\sigma\cdot\langle u\rangle\in\mathbf{I}$,

поскольку в модели все трассы согласованные.

b) Существует такая трасса $\mu\in\boldsymbol{di}^{\sim}(\sigma)\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma})$, что u ***safe by*** $\boldsymbol{\Sigma}$ ***after*** μ и $\mu\cdot\langle u\rangle\notin\boldsymbol{\Sigma}$.

Тогда для некоторой кнопки $P`\in\mathbf{R}\cup\mathbf{Q}$

имеет место $P`$ ***safe by*** $\boldsymbol{\Sigma}$ ***after*** $\mu$ и $u\in P`$.

Поскольку $\mu\in\boldsymbol{di}^{\sim}(\sigma)$ влечет $\mu\cdot\langle u\rangle\in\boldsymbol{di}^{\sim}(\sigma)\cdot\langle u\rangle$, по лемме 1 из $\sigma\cdot\langle u\rangle\in\mathbf{I}$ следует $\mu\cdot\langle u\rangle\in\mathbf{I}$.

Но это противоречит условию $\mathbf{I}\in\boldsymbol{ConfImp}(\mathbf{T})$, поскольку $\mu\cdot\langle u\rangle\notin\boldsymbol{\Sigma}$.

3.2. $P\in\mathbf{R}$ и $u=P$ отказ.

a) Существуют такая трасса $\mu\in\boldsymbol{di}^{\sim}(\sigma\cdot\langle u\rangle)\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma})$ и такая кнопка $Q\in\mathbf{Q}$, что $Q\subseteq\cup\boldsymbol{Ip}(\sigma\cdot\langle u\rangle)$ и Q ***safe by*** $\boldsymbol{\Sigma}$ ***after*** μ.

Поскольку $\sigma\cdot\langle u\rangle\in\mathbf{I}$ и $Q\subseteq\cup\boldsymbol{Ip}(\sigma\cdot\langle u\rangle)$, то

$\mu\in\boldsymbol{di}^{\sim}(\sigma\cdot\langle u\rangle)$ влечет $\mu\cdot\langle Q\rangle\in\boldsymbol{p_{re}di}^{\sim}(\sigma\cdot\langle u,Q\rangle)$.

Следовательно, по лемме 1 $\mu\cdot\langle Q\rangle\in\mathbf{I}$.

Тем самым, $\mathbf{I}\notin\boldsymbol{SafeImp}(\mathbf{T})$,

что противоречит условию $\mathbf{I}\in\boldsymbol{ConfImp}(\mathbf{T})$.

b) Существуют такая трасса $\mu\in\boldsymbol{di}^{\sim}(\sigma\cdot\langle u\rangle)\cap\boldsymbol{SafeBy}(\boldsymbol{\Sigma})$ и такая кнопка $R\in\mathbf{R}$, что $R\subseteq\cup\boldsymbol{Ip}(\sigma\cdot\langle u\rangle)$, R ***safe by*** $\boldsymbol{\Sigma}$ ***after*** μ, но $\mu\cdot\langle R\rangle\notin\boldsymbol{\Sigma}$.

Поскольку $\sigma\cdot\langle u\rangle\in\mathbf{I}$ и $R\subseteq\cup\boldsymbol{Ip}(\sigma\cdot\langle u\rangle)$, то

$\mu\in\boldsymbol{di}^{\sim}(\sigma\cdot\langle u\rangle)$ влечет $\mu\cdot\langle R\rangle\in\boldsymbol{p}_{re}\boldsymbol{di}^{\sim}(\sigma\cdot\langle u,R\rangle)$.

Следовательно, по лемме 1 $\mu\cdot\langle R\rangle\in\mathbf{I}$.

Но это противоречит условию $\mathbf{I}\in\boldsymbol{ConfImp}(\mathbf{T})$, поскольку $\mu\cdot\langle R\rangle\notin\boldsymbol{\Sigma}$.

4. Покажем, что ~пополнение не расширяет класс конформных реализаций: $\boldsymbol{ConfImp}(\mathbf{T})\supseteq\boldsymbol{ConfImp}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}}$.

   Допустим, это не так.

   Тогда существуют

   такая реализация $\mathbf{I}\in\boldsymbol{ConfImp}(\mathbf{T}^{\sim},\mathbf{L})$

   и такая трасса $\sigma^{\#}\cdot\langle u^{\#}\rangle\in\mathbf{I}$,

   что $\sigma\cdot\langle u\rangle\in\boldsymbol{err}_1(\mathbf{T})$.

   Мы всегда можем выбрать трассу σ актуальной.

   Тогда по лемме 5 трасса $\sigma\in\sim\boldsymbol{conf}(\mathbf{T})$ (утверждение 2),

   а трасса $\sigma\cdot\langle u\rangle\in\sim\boldsymbol{tt}(\mathbf{T})$ ~тестовая (утверждение 1),

   но $\sigma\cdot\langle u\rangle\notin\sim\boldsymbol{conf}(\mathbf{T})$ (утверждение 3).

   Отсюда следует, что $\sigma\cdot\langle u\rangle\in\sim\boldsymbol{ptt}(\mathbf{T})\setminus\sim\boldsymbol{conf}(\mathbf{T})$.

   По лемме 18 $\boldsymbol{SafeBy}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}}=\sim\boldsymbol{conf}(\mathbf{T})$ и $\boldsymbol{tt}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}}=\sim\boldsymbol{ptt}(\mathbf{T})$, поэтому

   $\sigma\cdot\langle u\rangle\in\boldsymbol{tt}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}}\setminus\boldsymbol{SafeBy}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}}$

   $\subseteq\ (\boldsymbol{tt}(\mathbf{T}^{\sim},\mathbf{L})\setminus\boldsymbol{SafeBy}(\mathbf{T}^{\sim},\mathbf{L}))_{\mathbf{L}}\ =\ \boldsymbol{err}_1(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}}$.

   Это означает, что $\sigma^{\#}\cdot\langle u^{\#}\rangle$ является $\mathbf{L}$-ошибкой 1-го рода для $\mathbf{T}^{\sim}$.

   Но, поскольку $\sigma^{\#}\cdot\langle u^{\#}\rangle\in\mathbf{I}$, это противоречит условию $\mathbf{I}\in\boldsymbol{ConfImp}(\mathbf{T}^{\sim},\mathbf{L})$.

   Мы пришли к противоречию и, следовательно, наше допущение не верно, а утверждение доказано.

6.32. Доказательство теоремы 13

По определению операции «$^{\#}$» $\mathbf{R}^{\#}/\mathbf{Q}^{\#}\ \approx_{\mathbf{L}}\ \mathbf{R}/\mathbf{Q}$.

По лемме 11 $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})$ $\mathbf{R}^{\#}$-модель,

следовательно, $\boldsymbol{\Sigma}^{\sim}$ по ее определению является полной трассовой моделью.

По определению отношения $\boldsymbol{safe}_{\gamma\Delta}$, оно удовлетворяет всем трем требованиям, предъявляемым к отношению ***safe by***,

поскольку по лемме 7 выполнено $\mathbf{Q}$-свойство.

Тем самым, $\mathbf{T}^{\sim}=(\mathbf{R}^{\#}/\mathbf{Q}^{\#},\boldsymbol{\Sigma}^{\sim},\boldsymbol{safe}_{\gamma\Delta})$ является спецификационной тройкой в $\mathbf{L}$-эквивалентной семантике.

По лемме 19 $\mathbf{T}^{\sim} \approx_{\mathbf{L}} \mathbf{T}$.

По лемме 18 $\boldsymbol{SafeBy}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}}=\sim\boldsymbol{conf}(\mathbf{T})$ и $\boldsymbol{tt}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}}=\sim\boldsymbol{ptt}(\mathbf{T})$.

Тем самым, по определению ~пополнения тройка $\mathbf{T}^{\sim}$ является ~пополнением.

6.33. Доказательство леммы 20

Если для исходной тройки $\mathbf{T}$ нет конформных реализаций, множество $\boldsymbol{\Sigma}^{\mathbf{01}\nabla}$ ∇-финальных трасс пусто, и утверждение леммы очевидно.

1. **Q**-свойство: $\forall\sigma^{\#}\in\boldsymbol{\Sigma}^{\mathbf{01}\nabla}\ \ \forall \mathtt{Q}\in\mathbf{Q}\ \ \sigma^{\#}\cdot\langle\cancel{\mathtt{Q}}\rangle\in\boldsymbol{\Sigma}^{\mathbf{01}\nabla}$.

   Пусть $\sigma^{\#}\in\boldsymbol{\Sigma}^{\mathbf{01}\nabla}$.

   Тогда по определению ∇-финальных трасс $\sigma^{\#}\in\boldsymbol{\Sigma}^{\mathbf{01}\sim}$.

   Тогда по лемме 7 (утверждение 2) $\forall \mathtt{Q}\in\mathbf{Q}\ \ \sigma^{\#}\cdot\langle\cancel{\mathtt{Q}}\rangle\in\boldsymbol{\Sigma}^{\mathbf{01}\sim}$.

   Тогда по определению ∇-финальных трасс $\sigma^{\#}\cdot\langle\cancel{\mathtt{Q}}\rangle\in\boldsymbol{\Sigma}^{\mathbf{01}\nabla}$.

2. **R**-свойство: $\forall\sigma^{\#}\in\boldsymbol{\Sigma}^{\mathbf{01}\nabla}\ \ \forall \mathtt{R}\in\mathbf{R}\ \ (\sigma^{\#}\cdot\langle\cancel{\mathtt{R}}\rangle\notin\boldsymbol{\Sigma}^{\mathbf{01}\nabla}\ \Leftrightarrow\ \boldsymbol{Ip}(\sigma)\neq\varnothing$
   $\&\ \mathtt{R}\subseteq\cup\boldsymbol{Ip}(\sigma))\ \ \&\ \ (\sigma^{\#}\cdot\langle\cancel{\mathtt{R}}\rangle\notin\boldsymbol{\Sigma}^{\mathbf{01}\nabla}\ \Rightarrow\ \sigma^{\#}\cdot\langle\mathtt{R}^{\#}\rangle\in\boldsymbol{\Sigma}^{\mathbf{01}\nabla})$.

   Пусть $\sigma^{\#}\in\boldsymbol{\Sigma}^{\mathbf{01}\nabla}$.

   Тогда по определению ∇-финальных трасс $\sigma^{\#}\in\boldsymbol{\Sigma}^{\mathbf{01}\sim}$.

   Тогда по **R**-свойству (лемма 7)

   $\forall\mathtt{R}\in\mathbf{R}\ \ (\sigma^{\#}\cdot\langle\cancel{\mathtt{R}}\rangle\notin\boldsymbol{\Sigma}^{\mathbf{01}\sim}\ \Leftrightarrow\ \boldsymbol{Ip}(\sigma)\neq\varnothing\ \ \&\ \mathtt{R}\subseteq\cup\boldsymbol{Ip}(\sigma))$

   $\&\ \ (\sigma^{\#}\cdot\langle\cancel{\mathtt{R}}\rangle\notin\boldsymbol{\Sigma}^{\mathbf{01}\sim}\ \Rightarrow\ \sigma^{\#}\cdot\langle\mathtt{R}^{\#}\rangle\in\boldsymbol{\Sigma}^{\mathbf{01}\sim})$.

   Для $\sigma^{\#}\in\boldsymbol{\Sigma}^{\mathbf{01}\nabla}$ по определению ∇-финальных трасс

   $\sigma^{\#}\cdot\langle\cancel{\mathtt{R}}\rangle\notin\boldsymbol{\Sigma}^{\mathbf{01}\sim}\ \Leftrightarrow\ \sigma^{\#}\cdot\langle\cancel{\mathtt{R}}\rangle\notin\boldsymbol{\Sigma}^{\mathbf{01}\nabla}$.

   Тем самым, $\forall\mathtt{R}\in\mathbf{R}\ \ (\sigma^{\#}\cdot\langle\cancel{\mathtt{R}}\rangle\notin\boldsymbol{\Sigma}^{\mathbf{01}\nabla}\ \Leftrightarrow\ \boldsymbol{Ip}(\sigma)\neq\varnothing\ \ \&\ \mathtt{R}\subseteq\cup\boldsymbol{Ip}(\sigma))$.

   Также $\sigma^{\#}\cdot\langle\cancel{\mathtt{R}}\rangle\notin\boldsymbol{\Sigma}^{\mathbf{01}\nabla}\ \Rightarrow\ \sigma^{\#}\cdot\langle\mathtt{R}^{\#}\rangle\in\boldsymbol{\Sigma}^{\mathbf{01}\sim}$.

   Нам надо показать, что $\sigma^{\#}\cdot\langle\mathtt{R}^{\#}\rangle\in\boldsymbol{\Sigma}^{\mathbf{01}\nabla}$.

   Для этого достаточно показать, что отказ $\mathtt{R}^{\#}$ оставляет трассу $\sigma^{\#}\cdot\langle\mathtt{R}^{\#}\rangle$ **L**-конформной для $\mathbf{T}^{\sim}$.

   Действительно, поскольку $\sigma^{\#}\cdot\langle\cancel{\mathtt{R}}\rangle\notin\boldsymbol{\Sigma}^{\mathbf{01}\nabla}$ влечет $\sigma^{\#}\cdot\langle\cancel{\mathtt{R}}\rangle\notin\boldsymbol{\Sigma}^{\mathbf{01}\sim}$,

   по теореме 10 $\mathtt{R}^{\#}\ \boldsymbol{safe}_{\gamma\Delta}\ \boldsymbol{\Sigma}^{\sim}\ \boldsymbol{after}\ \sigma^{\#}$.

Однако, поскольку $R \subseteq \cup \boldsymbol{Ip}(\sigma)$, то, если бы $\sigma^{\#}\cdot\langle R^{\#}\rangle \notin \boldsymbol{\Sigma}^{01^{\nabla}}$, у трассы $\sigma^{\#}$ не было бы **L**-конформных продолжений, разрешаемых безопасной для $\mathbf{T}^{\sim}$ кнопкой $R^{\#}$.

Поскольку трасса $\sigma^{\#}$ **L**-конформна, она встречается в некоторой **L**-конформной реализации **I**.

По гипотезе о безопасности в реализации **I** после трассы $\sigma^{\#}$ должна быть безопасна кнопка $R^{\#}$.

По конвергентности реализации **I** в ней после трассы $\sigma^{\#}$ имеется хотя бы одно **L**-наблюдение.

Но тогда это **L**-наблюдение не **L**-конформно, что противоречит **L**-конформности реализации **I**.

3. $\Delta\gamma$-свойство:

   1) $\boldsymbol{\Sigma}^{01^{\nabla}}=\{\epsilon, \langle\gamma\rangle\}$

      $\vee\ \forall\pi\in\boldsymbol{\Sigma}^{01^{\nabla}}\setminus(\mathbf{L}\cup\mathbf{R}^{\#})^{*}\ \exists\sigma^{\#}\ \exists\not{R}\ \pi\in\{\sigma^{\#}\cdot\langle\not{R}\rangle, \sigma^{\#}\cdot\langle\not{R}, \Delta\rangle, \sigma^{\#}\cdot\langle\not{R}, \gamma\rangle\}$,

   2) $\forall\sigma^{\#}\in\boldsymbol{\Sigma}^{01^{\nabla}}\ \forall\not{R}$

      $(\sigma^{\#}\cdot\langle\not{R}\rangle\in\boldsymbol{\Sigma}^{01^{\nabla}}\ \Rightarrow\ (\sigma^{\#}\cdot\langle\not{R}, \Delta\rangle\in\boldsymbol{\Sigma}^{01^{\nabla}}\ \vee\ \sigma^{\#}\cdot\langle\not{R}, \gamma\rangle\in\boldsymbol{\Sigma}^{01^{\nabla}}))$.

3.1. Покажем выполнение 1-ой части $\Delta\gamma$-свойства.

3.1.1. По определению ∇-финальных трасс, если пустая трасса опасна в исходной спецификации **Σ**, то $\boldsymbol{\Sigma}^{01^{\nabla}}=\{\epsilon, \langle\gamma\rangle\}$.

3.1.2. Теперь рассмотрим случай, когда пустая трасса безопасна в исходной спецификации **Σ**.

Пусть $\pi\in\boldsymbol{\Sigma}^{01^{\nabla}}\setminus(\mathbf{L}\cup\mathbf{R}^{\#})^{*}$.

Тогда по определению ∇-финальных трасс $\pi=\sigma^{\#}\cdot\langle\not{R}\rangle\cdot\lambda\in\boldsymbol{\Sigma}^{1^{\sim}}$, где $\sigma^{\#}\in\boldsymbol{\Sigma}^{0^{\nabla}}$ и $P\in\mathbf{R}\cup\mathbf{Q}$.

Поскольку $\sigma^{\#}\in\boldsymbol{\Sigma}^{0^{\nabla}}$ влечет $\sigma^{\#}\in\boldsymbol{\Sigma}^{0^{\sim}}$, по $\Delta\gamma$-свойству (лемма 7) множества $\boldsymbol{\Sigma}^{01^{\sim}}$ имеем $\lambda\in\{\epsilon, \langle\Delta\rangle, \langle\gamma\rangle\}$.

Следовательно, $\pi\in\{\sigma^{\#}\cdot\langle\not{R}\rangle, \sigma^{\#}\cdot\langle\not{R}, \Delta\rangle, \sigma^{\#}\cdot\langle\not{R}, \gamma\rangle\}$.

3.2. Покажем выполнение 2-ой части $\Delta\gamma$-свойства.

Пусть $\sigma^{\#}\in\boldsymbol{\Sigma}^{01^{\nabla}}$ и $\sigma^{\#}\cdot\langle\not{R}\rangle\in\boldsymbol{\Sigma}^{01^{\nabla}}$ для некоторого не-отказа $\not{R}$.

Тогда по определению ∇-финальных трасс $\sigma^{\#}\in\boldsymbol{\Sigma}^{01^{\sim}}$ и $\sigma^{\#}\cdot\langle\not{R}\rangle\in\boldsymbol{\Sigma}^{01^{\sim}}$.

Следовательно, по $\Delta\gamma$-свойству (лемма 7) множества $\boldsymbol{\Sigma}^{01^{\sim}}$ имеем

$\sigma^{\#}\cdot\langle\not{R}, \Delta\rangle\in\boldsymbol{\Sigma}^{01^{\sim}}\ \vee\ \sigma^{\#}\cdot\langle\not{R}, \gamma\rangle\in\boldsymbol{\Sigma}^{01^{\sim}}$.

Но тогда, поскольку $\sigma^{\#}\in\boldsymbol{\Sigma}^{01^{\nabla}}$, по определению ∇-финальных трасс имеем

$\sigma^{\#}\cdot\langle \text{R}, \Delta\rangle \in \mathbf{\Sigma}^{\mathbf{01}\nabla} \ \vee \ \sigma^{\#}\cdot\langle \text{R}, \gamma\rangle \in \mathbf{\Sigma}^{\mathbf{01}\nabla}$.

3.3. Покажем выполнение дополнительного условия: после не-отказа не могут следовать и дивергенция и разрушение.

По лемме 7 это условие выполнено для ~финальных трасс. А тогда по определению ∇-финальных трасс оно выполнено и для них.

6.34. Доказательство леммы 21

Если $\langle\gamma\rangle \in \mathbf{\Sigma}$, то $\mathbf{\Sigma}^{\mathbf{01}\nabla} = \mathbf{\Sigma}^{\mathbf{01}\sim} = \{\epsilon, \langle\gamma\rangle\}$ и проверка выполнения свойств трассовой модели тривиальна. Далее будет предполагать, что $\langle\gamma\rangle \notin \mathbf{\Sigma}$.

1. Непустота множества $\mathbf{\Sigma}^{\mathbf{01}\nabla} \neq \varnothing$.

   Так как $\langle\gamma\rangle \notin \mathbf{\Sigma}$, то $\epsilon \in \mathbf{\Sigma}^{\mathbf{01}\sim}$.

   По условию леммы трасса ϵ конформна.

   Поэтому $\epsilon \in \mathbf{\Sigma}^{\mathbf{01}\nabla}$.

2. Префикс-замкнутость множества $\mathbf{\Sigma}^{\mathbf{01}\nabla}$ следует из его определения и префикс-замкнутости множества $\boldsymbol{conf}(\mathbf{T}^{\sim}, \mathbf{L})$ и множества $\mathbf{\Sigma}^{\mathbf{01}\sim}$ (лемма 8).

3. Допустимость и согласованность.

   Это свойства отдельных трасс.

   Поскольку $\mathbf{\Sigma}^{\mathbf{01}\nabla} \subseteq \mathbf{\Sigma}^{\mathbf{01}\sim}$, и эти свойства выполнены для трасс из $\mathbf{\Sigma}^{\mathbf{01}\sim}$ (лемма 8), они сохраняются для трасс из $\mathbf{\Sigma}^{\mathbf{01}\nabla}$.

4. Конвергентность.

   Поскольку по $\Delta\gamma$-свойству множества $\mathbf{\Sigma}^{\mathbf{01}\sim}$ ~финальных трасс (лемма 7) подмножество его трасс, не содержащих и не продолжающихся в нем дивергенцией и разрушением, это множество $\mathbf{\Sigma}^{\mathbf{0}\sim}$, то по определению ∇-финальная трасса, не содержащая и не продолжающаяся во множестве $\mathbf{\Sigma}^{\mathbf{01}\nabla}$ разрушением и дивергенцией, – это трасса $\sigma^{\#} \in \mathbf{\Sigma}^{\mathbf{0}\nabla}$.

   Рассмотрим произвольный отказ $R \in \mathbf{R}$.

   Нам достаточно показать, что во множестве $\mathbf{\Sigma}^{\mathbf{01}\nabla}$ трасса $\sigma^{\#}$ продолжается отказом $R^{\#}$ или не-отказом R, поскольку $\text{R} \in R^{\#}$.

   Но это следует из **R**-свойства множества $\mathbf{\Sigma}^{\mathbf{01}\nabla}$ (лемма 20).

5. Полнота (замкнутость по ***i***-операции).

   Пусть имеется ∇-финальная трасса вида

   $\sigma_1 = \mu^{\#}\cdot\lambda^{\#}$, или

$\sigma_2=\mu^{\#}\cdot\lambda^{\#}\cdot\langle\not\Rightarrow\rangle$, или

$\sigma_3=\mu^{\#}\cdot\lambda^{\#}\cdot\langle\not\Rightarrow,\gamma\rangle$, или

$\sigma_4=\mu^{\#}\cdot\lambda^{\#}\cdot\langle\not\Rightarrow,\Delta\rangle$ (заметим, что $(\mu\cdot\lambda)^{\#}=\mu^{\#}\cdot\lambda^{\#}$).

Пусть также трасса $\mu^{\#}$ заканчивается отказом, и для некоторого отказа $R^{\#}\in\mathbf{R}^{\#}$ не продолжается во множестве ∇-финальных трасс никакими действиями из $R^{\#}$.

Нужно показать, что также ∇-финальна трасса

$\sigma_1`=\mu^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}$, или

$\sigma_2`=\mu^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\cdot\langle\not\Rightarrow\rangle$, или

$\sigma_3`=\mu^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\cdot\langle\not\Rightarrow,\gamma\rangle$, или

$\sigma_4`=\mu^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda^{\#}\cdot\langle\not\Rightarrow,\Delta\rangle$, соответственно.

Трасса $\mu^{\#}$ не продолжается не-отказом $\not\Rightarrow$, поскольку $\not\Rightarrow\in R^{\#}$.

Следовательно, по **R**-свойству (лемма 20) $R\subseteq\cup\boldsymbol{Ip}(\mu)$.

Поскольку множество ~финальных трасс замкнуто по ***i***-операции (лемма 8) и $\boldsymbol{i}\tilde{}\subseteq\boldsymbol{i}$, трассы $\sigma_i`$ ~финальны.

По доказанному трасса $\sigma_1`$ ~финальна.

Покажем, что она также **L**-конформна.

Действительно, **L**-конформность трассы σ_1 означает, что она встречается в некоторой конформной **L**-реализации.

Но из ***i***-замкнутости любой реализации и $\boldsymbol{i}\tilde{}\subseteq\boldsymbol{i}$ следует, что трасса $\sigma_1`$ также встречается в этой конформной **L**-реализации, то есть **L**-конформна.

Тем самым, трасса $\sigma_1`$ ∇-финальна.

По доказанному трассы $\sigma_i`$, где $i>1$, ~финальны.

Также они принадлежат множеству $\boldsymbol{\Sigma^{1\tilde{}}}$, и продолжают ∇-финальную трассу $\sigma_1`$ не-отказом $\not\Rightarrow$ и далее, быть может, дивергенцией и разрушением.

По определению множества $\boldsymbol{\Sigma^{1\nabla}}$ такие трассы $\sigma_i`$ также ∇-финальны.

6.35. Доказательство леммы 22

Утверждение 1 непосредственно следует из лемм 21 и 10,
а утверждения 2 и 3 – из лемм 20 и 9.

6.36. Доказательство леммы 23

1. Покажем, что $\mu^{\#}\cdot\langle\not\Rightarrow,\gamma\rangle\notin\cup\boldsymbol{d}(\boldsymbol{\Sigma^{01\nabla}})\ \Rightarrow\ \mu^{\#}\cdot\langle\not\Rightarrow,\gamma\rangle\notin\boldsymbol{\Sigma^{1\nabla}}$.

   Это следует из того, что $\boldsymbol{\Sigma^{1\nabla}}\ \subseteq\ \cup\boldsymbol{d}(\boldsymbol{\Sigma^{01\nabla}})$.

2. Покажем, что $\mu^{\#}\cdot\langle \not\Rightarrow,\gamma\rangle \notin \mathbf{\Sigma^{1\nabla}} \Rightarrow \mu^{\#}\cdot\langle \not\Rightarrow,\gamma\rangle \notin \cup\boldsymbol{d}(\mathbf{\Sigma^{01\nabla}})$.

   Действительно, по определению $\mathbf{\Sigma^{1\nabla}}$, поскольку $\mu^{\#}\in\mathbf{\Sigma^{0\nabla}}$, имеем

   $\mu^{\#}\cdot\langle \not\Rightarrow,\gamma\rangle \notin \mathbf{\Sigma^{1\nabla}} \Rightarrow \mu^{\#}\cdot\langle \not\Rightarrow,\gamma\rangle \notin \mathbf{\Sigma^{1\sim}}$.

   По лемме 15 $\mu^{\#}\cdot\langle \not\Rightarrow,\gamma\rangle \notin \mathbf{\Sigma^{1\sim}} \Rightarrow \mu^{\#}\cdot\langle \not\Rightarrow,\gamma\rangle \notin \cup\boldsymbol{d}(\mathbf{\Sigma^{01\sim}})$.

   Поскольку $\mathbf{\Sigma^{01\nabla}} \subseteq \mathbf{\Sigma^{01\sim}}$, имеем $\cup\boldsymbol{d}(\mathbf{\Sigma^{01\nabla}}) \subseteq \cup\boldsymbol{d}(\mathbf{\Sigma^{01\sim}})$, поэтому

   $\mu^{\#}\cdot\langle \not\Rightarrow,\gamma\rangle \notin \cup\boldsymbol{d}(\mathbf{\Sigma^{01\sim}}) \Rightarrow \mu^{\#}\cdot\langle \not\Rightarrow,\gamma\rangle \notin \cup\boldsymbol{d}(\mathbf{\Sigma^{01\nabla}})$.

6.37. Доказательство теоремы 14

$\mathrm{P}^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{\Sigma}^{\nabla}$ ***after*** $\mu^{\#}$

$\Leftrightarrow$ по замечанию 12 и по лемме 14

$\mu^{\#}\cdot\langle \not\Rightarrow,\gamma\rangle \notin \mathbf{\Sigma}^{\nabla}$

$\Leftrightarrow$ по замечанию 12

$\mu^{\#}\cdot\langle \not\Rightarrow,\gamma\rangle \notin \cup\boldsymbol{d}(\mathbf{\Sigma^{01\nabla}})$

$\Leftrightarrow$ по лемме 23

$\mu^{\#}\cdot\langle \not\Rightarrow,\gamma\rangle \notin \mathbf{\Sigma^{1\nabla}}$.

6.38. Доказательство леммы 24

Если для исходной тройки **T** нет конформных реализаций, множество $\mathbf{\Sigma^{01\nabla}}$ ∇-финальных трасс пусто, тем более пусто его подмножество ∇-финальных **L**-трасс, и утверждение леммы очевидно.

1. Пусть пустая трасса опасна в исходной спецификации **Σ**.

   Тогда $\mathbf{\Sigma^{01\nabla}}=\mathbf{\Sigma^{01\sim}}=\{\epsilon,\langle\gamma\rangle\}$ и утверждение леммы очевидно.

2. Пусть пустая трасса безопасна в исходной спецификации **Σ**.

   Тогда множество ∇-финальных **L**-трасс – это множество $\mathbf{\Sigma^{0\nabla}}\neq\varnothing$.

   Пусть $\sigma^{\#}\in\mathbf{\Sigma^{0\nabla}}$.

   По теореме 10 (о безопасности кнопок)

   $\mathrm{P}^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{\Sigma}^{\sim}$ ***after*** $\sigma^{\#}$ $\Leftrightarrow$ $\sigma^{\#}\cdot\langle \not\Rightarrow,\gamma\rangle \notin \mathbf{\Sigma^{1\sim}}$.

   По определению ∇-финальных трасс для $\sigma^{\#}\in\mathbf{\Sigma^{0\nabla}}$ имеет место

   $\sigma^{\#}\cdot\langle \not\Rightarrow,\gamma\rangle \notin \mathbf{\Sigma^{1\sim}} \Leftrightarrow \sigma^{\#}\cdot\langle \not\Rightarrow,\gamma\rangle \notin \mathbf{\Sigma^{1\nabla}}$.

   Поскольку $\sigma^{\#}\in\mathbf{\Sigma^{0\nabla}}$, по теореме 14 $\sigma^{\#}\cdot\langle \not\Rightarrow,\gamma\rangle \notin \mathbf{\Sigma^{1\nabla}} \Leftrightarrow \mathrm{P}^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{\Sigma}^{\nabla}$ ***after*** $\sigma^{\#}$.

   Тем самым, $\mathrm{P}^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{\Sigma}^{\sim}$ ***after*** $\sigma^{\#}$ $\Leftrightarrow$ $\mathrm{P}^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{\Sigma}^{\nabla}$ ***after*** $\sigma^{\#}$.

6.39. Доказательство теоремы 15

1. Пусть пустая трасса опасна в исходной спецификации $\boldsymbol{\Sigma}$.

   Тогда ∇-финальные **L**-трассы – это пустая трасса ϵ и трасса $\langle\gamma\rangle$.

   Множество $\boldsymbol{SafeBy}(\mathbf{T}^{\nabla},\mathbf{L})=\varnothing$

   и однозначно определяется множеством ∇-финальных трасс $\{\epsilon, \langle\gamma\rangle\}$.

2. Пусть пустая трасса безопасна в исходной спецификации $\boldsymbol{\Sigma}$.

   Тогда по теореме 11 множество безопасных по отношению $\boldsymbol{safe}_{\gamma\Delta}$ **L**-трасс спецификации $\boldsymbol{\Sigma}^{\sim}$ совпадает с множеством ~финальных **L**-трасс.

   По определению ∇-финальных трасс они являются ~финальными трассами.

   Отсюда, поскольку по лемме 24 отношения $\boldsymbol{safe}_{\gamma\Delta}$ на множестве $\boldsymbol{\Sigma}^{\mathbf{01}^{\nabla}}$ и на множестве $\boldsymbol{\Sigma}^{\mathbf{01}^{\sim}}$ совпадают на подмножестве ∇-финальных **L**-трасс, следует, что множество $\boldsymbol{SafeBy}(\mathbf{T}^{\nabla},\mathbf{L})$ безопасных **L**-трасс спецификации $\boldsymbol{\Sigma}^{\nabla}$ совпадает с множеством ∇-финальных **L**-трасс $\boldsymbol{\Sigma}^{\mathbf{0}^{\nabla}}$.

   Множество $\boldsymbol{SafeBy}(\mathbf{T}^{\nabla},\mathbf{L})$ однозначно определяется множеством $\boldsymbol{\Sigma}^{\mathbf{01}^{\nabla}}$ ∇-финальных трасс по теореме 14.

6.40. Доказательство теоремы 16

1. Утверждение 1.

   Непосредственно следует из того, что $\boldsymbol{\Sigma}^{\mathbf{0}^{\nabla}}\subseteq\boldsymbol{\Sigma}^{\mathbf{0}^{\sim}}$,

   а по теореме 12 трассы из $\boldsymbol{\Sigma}^{\mathbf{0}^{\sim}}$ **L**-актуальны.

2. Утверждение 2.

   Безопасные наблюдения могут быть только в том случае,

   когда нет трассы $\langle\gamma\rangle$.

   По лемме 24 отношения $\boldsymbol{safe}_{\gamma\Delta}$ на множестве $\boldsymbol{\Sigma}^{\mathbf{01}^{\nabla}}$ и на множестве $\boldsymbol{\Sigma}^{\mathbf{01}^{\sim}}$ совпадают на подмножестве $\boldsymbol{\Sigma}^{\mathbf{0}^{\nabla}}$ ∇-финальных **L**-трасс.

   По теореме 12 безопасное наблюдение $u^{\#}\in\mathbf{L}\cup\mathbf{R}^{\#}$ **L**-актуально после трассы $\sigma^{\#}\in\boldsymbol{\Sigma}^{\mathbf{0}^{\sim}}$ тогда и только тогда, когда либо

   1) $u\in\mathbf{L}$ и $u\notin\cup\boldsymbol{Ip}(\sigma)$, либо

   2) $u\in\mathbf{R}$ и для каждой кнопки $Q\in\mathbf{Q}$ такой, что $Q\subseteq u\cup\cup\boldsymbol{Ip}(\sigma)$, трасса $\mu^{\#}\cdot\langle\Theta, \gamma\rangle\in\boldsymbol{\Sigma}^{\mathbf{1}^{\sim}}$ для каждой трассы $\mu^{\#}\in\boldsymbol{\Sigma}^{\mathbf{0}^{\sim}}$ такой, что $\mu\in\boldsymbol{di}^{\sim}(\sigma\cdot\langle u\rangle)$.

   По определению ∇-финальных трасс,

   если нет трассы $\langle\gamma\rangle$ и трасса $\mu^{\#}\in\boldsymbol{\Sigma}^{\mathbf{0}^{\nabla}}$,

   то $\mu^{\#}\in\boldsymbol{\Sigma}^{\mathbf{0}^{\sim}}$

   и трасса $\mu^{\#}\cdot\langle\Theta, \gamma\rangle\in\boldsymbol{\Sigma}^{\mathbf{1}^{\sim}}$ тогда и только тогда, когда $\mu^{\#}\cdot\langle\Theta, \gamma\rangle\in\boldsymbol{\Sigma}^{\mathbf{1}^{\nabla}}$.

Отсюда следует утверждение 2 теоремы.

6.41. Доказательство леммы 25

По определению $\mathbf{\Sigma}^{\mathbf{0}\nabla}=\boldsymbol{conf}(\mathbf{T}^{\sim},\mathbf{L})$.

По теореме 15 $\mathbf{\Sigma}^{\mathbf{0}\nabla}=\boldsymbol{SafeBy}(\mathbf{T}^{\nabla},\mathbf{L})$.

Тем самым, $\boldsymbol{SafeBy}(\mathbf{T}^{\nabla},\mathbf{L})=\boldsymbol{conf}(\mathbf{T}^{\sim},\mathbf{L})$.

Отсюда и по лемме 24 $\boldsymbol{err}_1(\mathbf{T}^{\nabla},\mathbf{L})=\boldsymbol{perr}(\mathbf{T}^{\sim},\mathbf{L})$.

6.42. Доказательство леммы 26

1. Сначала покажем, что класс безопасно-тестируемых **L**-реализаций не сужается: $\boldsymbol{SafeImp}(\mathbf{T}) \subseteq \boldsymbol{SafeImp}(\mathbf{T}^{\nabla},\mathbf{L})_{\mathbf{L}}$.

   Поскольку по лемме 19 $\mathbf{T}^{\sim} \approx_{\mathbf{L}} \mathbf{T}$, нам достаточно показать, что класс безопасно-тестируемых **L**-реализаций не сужается при переходе от $\mathbf{T}^{\sim}$ к $\mathbf{T}^{\nabla}$: $\boldsymbol{SafeImp}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}} \subseteq \boldsymbol{SafeImp}(\mathbf{T}^{\nabla},\mathbf{L})_{\mathbf{L}}$.

   По лемме 25 $\boldsymbol{SafeBy}(\mathbf{T}^{\nabla},\mathbf{L})=\boldsymbol{conf}(\mathbf{T}^{\sim},\mathbf{L})$ и $\boldsymbol{err}_1(\mathbf{T}^{\nabla},\mathbf{L})=\boldsymbol{perr}(\mathbf{T}^{\sim},\mathbf{L})$.

   Поскольку $\boldsymbol{conf}(\mathbf{T}^{\sim},\mathbf{L}) \subseteq \boldsymbol{tt}(\mathbf{T}^{\sim},\mathbf{L})$ и $\boldsymbol{perr}(\mathbf{T}^{\sim},\mathbf{L}) \subseteq \boldsymbol{tt}(\mathbf{T}^{\sim},\mathbf{L})$,

   а $\boldsymbol{tt}(\mathbf{T}^{\nabla},\mathbf{L})=\boldsymbol{SafeBy}(\mathbf{T}^{\nabla},\mathbf{L}) \cup \boldsymbol{err}_1(\mathbf{T}^{\nabla},\mathbf{L})$,

   имеем $\boldsymbol{tt}(\mathbf{T}^{\nabla},\mathbf{L}) \subseteq \boldsymbol{tt}(\mathbf{T}^{\sim},\mathbf{L})$.

   Отсюда, очевидно, следует $\boldsymbol{SafeImp}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}} \subseteq \boldsymbol{SafeImp}(\mathbf{T}^{\nabla},\mathbf{L})_{\mathbf{L}}$.
2. Теперь покажем, что класс конформных **L**-реализаций не расширяется: $\boldsymbol{ConfImp}(\mathbf{T}) \supseteq \boldsymbol{ConfImp}(\mathbf{T}^{\nabla},\mathbf{L})_{\mathbf{L}}$.

   Поскольку по лемме 19 $\mathbf{T}^{\sim} \approx_{\mathbf{L}} \mathbf{T}$,

   нам достаточно показать, что класс конформных **L**-реализаций не расширяется при переходе от $\mathbf{T}^{\sim}$ к $\mathbf{T}^{\nabla}$:

   $\boldsymbol{ConfImp}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}} \supseteq \boldsymbol{ConfImp}(\mathbf{T}^{\nabla},\mathbf{L})_{\mathbf{L}}$.

   Допустим противное.

   Тогда найдется такая реализация $\mathbf{I} \in \boldsymbol{ConfImp}(\mathbf{T}^{\nabla},\mathbf{L})_{\mathbf{L}}$, что $\mathbf{I} \notin \boldsymbol{ConfImp}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}}$.

   Тогда (используя понятие тестирования 2-го рода) найдутся

   трасса $\sigma \in \mathbf{I}$, кнопка $P \in \mathbf{R} \cup \mathbf{Q}$ и наблюдение u такие, что

   $\sigma \cdot \langle u \rangle \in \mathbf{I}$ & $(u \in P \vee u = P$ & $P \in \mathbf{R})$,

   а также $\sigma \in \boldsymbol{conf}(\mathbf{T}^{\sim},\mathbf{L})$, $P^{\#}$ $\boldsymbol{safe}_{\gamma\Delta}$ $\mathbf{\Sigma}^{\sim}$ $\boldsymbol{after}$ σ,

   но $\sigma \cdot \langle u \rangle \in \boldsymbol{perr}(\mathbf{T}^{\sim},\mathbf{L})$.

По лемме 25 имеем: $\sigma \in \mathit{SafeBy}(\mathbf{T}^{\nabla},\mathbf{L})$ и $\sigma\cdot\langle u\rangle \in \mathit{err}_1(\mathbf{T}^{\nabla},\mathbf{L})$.

По лемме 24 $P^{\#}\ \mathit{safe}_{\gamma\Delta}\ \boldsymbol{\Sigma}^{\nabla}\ \mathit{after}\ \sigma$.

Но это (используя понятие тестирования 1-го рода) противоречит $\mathbf{I} \in \mathit{ConfImp}(\mathbf{T}^{\nabla},\mathbf{L})_{\mathbf{L}}$.

3. Наконец, покажем, что класс конформных **L**-реализаций не сужается: $\mathit{ConfImp}(\mathbf{T}) \subseteq \mathit{ConfImp}(\mathbf{T}^{\nabla},\mathbf{L})_{\mathbf{L}}$.

По лемме 19 $\mathbf{T}^{\sim} \approx_{\mathbf{L}} \mathbf{T}$,

поэтому достаточно показать, что класс конформных **L**-реализаций не сужается при переходе от $\mathbf{T}^{\sim}$ к $\mathbf{T}^{\nabla}$:

$\mathit{ConfImp}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}} \subseteq \mathit{ConfImp}(\mathbf{T}^{\nabla},\mathbf{L})_{\mathbf{L}}$.

Допустим противное.

Тогда найдется такая реализация $\mathbf{I} \in \mathit{ConfImp}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}}$, что $\mathbf{I} \notin \mathit{ConfImp}(\mathbf{T}^{\nabla},\mathbf{L})_{\mathbf{L}}$.

Тогда (используя понятие тестирования 1-го рода) найдутся

трасса $\sigma \in \mathbf{I}$, кнопка $P \in \mathbf{R} \cup \mathbf{Q}$ и наблюдение u такие, что

$\sigma\cdot\langle u\rangle \in \mathbf{I}$ & $(u \in P \vee u = P$ & $P \in \mathbf{R})$,

а также $\sigma \in \mathit{SafeBy}(\mathbf{T}^{\nabla},\mathbf{L})$, $P^{\#}\ \mathit{safe}_{\gamma\Delta}\ \boldsymbol{\Sigma}^{\nabla}\ \mathit{after}\ \sigma$,

но $\sigma\cdot\langle u\rangle \in \mathit{err}_1(\mathbf{T}^{\nabla},\mathbf{L})$.

По лемме 25 имеем: $\sigma \in \mathit{conf}(\mathbf{T}^{\sim},\mathbf{L})$ и $\sigma\cdot\langle u\rangle \in \mathit{perr}(\mathbf{T}^{\sim},\mathbf{L})$.

По лемме 24 $P^{\#}\ \mathit{safe}_{\gamma\Delta}\ \boldsymbol{\Sigma}^{\sim}\ \mathit{after}\ \sigma$.

Но это (используя понятие тестирования 2-го рода) противоречит $\mathbf{I} \in \mathit{ConfImp}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}}$.

6.43. Доказательство теоремы 17

По определению операции «$^{\#}$» $\mathbf{R}^{\#}/\mathbf{Q}^{\#} \approx_{\mathbf{L}} \mathbf{R}/\mathbf{Q}$.

Поскольку для исходной тройки $\mathbf{T}$ есть конформные реализации, по лемме 22, множество $\cup\mathit{d}(\boldsymbol{\Sigma}^{\mathbf{01}\nabla})$ является трассовой $\mathbf{R}^{\#}$-моделью.

Следовательно, $\boldsymbol{\Sigma}^{\nabla}$ является полной трассовой моделью.

По лемме 20 выполнено **Q**-свойство, поэтому отношение $\mathit{safe}_{\gamma\Delta}$ удовлетворяет всем трем требованиям, предъявляемым к отношению ***safe by***.

Следовательно, $\mathbf{T}^{\nabla}$ спецификационная тройка в **L**-эквивалентной семантике.

По лемме 26 $\mathbf{T}^{\nabla} \in \nabla(\mathbf{T})_{\mathbf{L}}$.

По лемме 25 $\mathit{SafeBy}(\mathbf{T}^{\nabla},\mathbf{L}) = \mathit{conf}(\mathbf{T}^{\sim},\mathbf{L})$ и $\mathit{err}_1(\mathbf{T}^{\nabla},\mathbf{L}) = \mathit{perr}(\mathbf{T}^{\sim},\mathbf{L})$.

По теореме 13 $\mathbf{T}^{\sim}$ является ~пополнением тройки $\mathbf{T}$.

По теореме 9 $\mathit{conf}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}} = \nabla\mathit{conf}(\mathbf{T})$ и $\mathit{perr}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}} = \nabla\mathit{perr}(\mathbf{T})$.

Следовательно: $\mathit{SafeBy}(\mathbf{T}^{\nabla},\mathbf{L})_{\mathbf{L}} = \nabla\mathit{conf}(\mathbf{T})$ и $\mathit{err}_1(\mathbf{T}^{\nabla},\mathbf{L})_{\mathbf{L}} = \nabla\mathit{perr}(\mathbf{T})$.

Тем самым, для $\mathbf{T}^{\nabla}$ выполнены все свойства максимального ∇-пополнения.

6.44. Доказательство леммы 27

Q-свойство, очевидно, сохраняется при вставке пустых отказов, при ***i***-замыкании, и, по доказанному в лемме 9 при ***d***-замыкании.

Поскольку расширение $\boldsymbol{Ext}(\mathbf{N})=\cup\boldsymbol{d}(\cup\boldsymbol{i}_{\mathcal{P}(\mathbf{L})}(\cup\boldsymbol{e}(\mathbf{N})))$,

Q-свойство сохраняется при расширении $\boldsymbol{Ext}(\mathbf{N})$.

6.45. Доказательство теоремы 18

1. По лемме 11 $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$ обладает **Q**-свойством.
2. Поэтому, поскольку $\boldsymbol{\Sigma}^{\sim}=\boldsymbol{Ext}(\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01\sim}}))$, по лемме 27 $\boldsymbol{\Sigma}^{\sim}$ обладает **Q**-свойством.
3. Отсюда следует утверждение 1, поскольку $\mathbf{Q}^{\#}$-отказы могут вставляться только ***i***-операцией после трасс, не продолжающихся действиями из этих отказов.

   Отсюда с учетом определения $\boldsymbol{safe}_{\gamma\Delta}$ следует утверждение 2.

6.46. Доказательство теоремы 19

1. По лемме 22 $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}\nabla})$ обладает **Q**-свойством.
2. Отсюда по лемме 27 $\boldsymbol{\Sigma}^{\nabla}$ обладает **Q**-свойством.
3. Отсюда непосредственно следует утверждение 1, и с учетом определения $\boldsymbol{safe}_{\gamma\Delta}$ следуют утверждение 2.

6.47. Доказательство леммы 28

1) Покажем, что $\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha}\subseteq\boldsymbol{\Sigma}^{\mathbf{01\sim}}$.

   Поскольку $\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha}=\boldsymbol{\Sigma}^{\mathbf{01\sim}}\backslash\boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$, имеем $\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha}\subseteq\boldsymbol{\Sigma}^{\mathbf{01\sim}}$.

2) Покажем, что множество $\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha}$ префикс-замкнуто.

   Множество $\boldsymbol{\Sigma}^{\mathbf{01\sim}}$ префикс-замкнуто по лемме 8.

   Для непредельного ординала α по правилам вывода **0÷3** вместе с каждой трассой, помещаемой в $\boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$, туда помещаются и все ее продолжения, а для предельного ординала α по определению $\boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})=\cup\{\boldsymbol{x}_{\beta}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})\mid\beta<\alpha\}$.

   Поэтому множество $\boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$ удаляемых трасс является постфикс-замкнутым подмножеством префикс-замкнутого множества $\boldsymbol{\Sigma}^{\mathbf{01\sim}}$.

   Поэтому разность $\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha}=\boldsymbol{\Sigma}^{\mathbf{01\sim}}\backslash\boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$ префикс-замкнута.

3) Множество $\boldsymbol{x}_\alpha(\boldsymbol{\Sigma}^{01\sim})$ вместе с каждой трассой содержит ее максимальный **L**-префикс.

   $\mu^{\#}\cdot\kappa\in\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_\alpha$ влечет $\mu^{\#}\in\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_\alpha$, поскольку множество $\boldsymbol{\Sigma}^{01\sim}$ префикс-замкнуто по лемме 8 и для непредельного ординала α по правилам вывода **0÷3** вместе с каждой трассой, помещаемой в $\boldsymbol{x}_\alpha(\boldsymbol{\Sigma}^{01\sim})$, туда помещаются и все ее продолжения, а для предельного ординала α по определению $\boldsymbol{x}_\alpha(\boldsymbol{\Sigma}^{01\sim})=\cup\{\boldsymbol{x}_\beta(\boldsymbol{\Sigma}^{01\sim})\,|\,\beta<\alpha\}$.

4) Если $\mu^{\#}\cdot\langle\text{Ⓡ}\rangle\cdot\pi\in\boldsymbol{\Sigma}^{01\sim}$ и $\mu^{\#}\in\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_\alpha$, то $\mu^{\#}\cdot\langle\text{Ⓡ}\rangle\cdot\pi\in\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_\alpha$, поскольку для непредельного ординала α по правилам вывода **0÷3** вместе с каждой трассой, помещаемой в $\boldsymbol{x}_\alpha(\boldsymbol{\Sigma}^{01\sim})$, туда помещается и ее максимальный **L**-префикс, а для предельного ординала α по определению $\boldsymbol{x}_\alpha(\boldsymbol{\Sigma}^{01\sim})=\cup\{\boldsymbol{x}_\beta(\boldsymbol{\Sigma}^{01\sim})\,|\,\beta<\alpha\}$.

6.48. Доказательство леммы 29

Поскольку по определению $\boldsymbol{x}(\boldsymbol{\Sigma}^{01\sim})=\boldsymbol{x}_\alpha(\boldsymbol{\Sigma}^{01\sim})$ для некоторого ординала α, нам достаточно доказать утверждение леммы для каждого ординала: все трассы множества $\boldsymbol{x}_\alpha(\boldsymbol{\Sigma}^{01\sim})$ не **L**-конформны для каждого ординала α.

Будем доказывать не **L**-конформность всех трасс из каждого множества $\boldsymbol{x}_\alpha(\boldsymbol{\Sigma}^{01\sim})$ трансфинитной индукцией.

Поскольку $\boldsymbol{x}_0(\boldsymbol{\Sigma}^{01\sim})=\varnothing$, для ординала $\alpha=0$ утверждение очевидно.

Пусть утверждение верно для каждого ординала $\beta<\alpha$, и докажем его для ординала $\alpha>0$.

1. Пусть α непредельный ординал.

   Нам достаточно доказать, что каждая трасса из множества $\boldsymbol{x}_\alpha(\boldsymbol{\Sigma}^{01\sim})\setminus\boldsymbol{x}_{\alpha-1}(\boldsymbol{\Sigma}^{01\sim})$ не **L**-конформна.

   Такая трасса получается по правилам вывода **2** или **3**.

1.1. Пусть трасса $\mu^{\#}\cdot\kappa$ получается по правилу вывода **2** как P-неконвергентная трасса:

   $\mu^{\#}\cdot\kappa\in\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha-1}$ & $\mathsf{P}\in\mathbf{R}\cup\mathbf{Q}$ & $\mu^{\#}\cdot\langle\text{Ⓡ},\gamma\rangle\notin\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha-1}$ & $\forall\mathsf{z}\in\mathsf{P}\cup\{\mathsf{P}^{\#}\}\ \mu^{\#}\cdot\langle\mathsf{z}\rangle\notin\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha-1}$.

   По лемме 28 (1) $\mu^{\#}\cdot\kappa\in\boldsymbol{\Sigma}^{01\sim}$, что влечет для **L**-трассы $\mu^{\#}\in\boldsymbol{\Sigma}^{0\sim}$,

   что по теореме 11 влечет

   безопасность трассы $\mu^{\#}$ в ~финальной спецификации.

   По лемме 28 (2) $\mu^{\#}\in\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha-1}$,

   что вместе с $\mu^{\#}\cdot\langle\text{Ⓡ},\gamma\rangle\notin\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha-1}$ влечет по лемме 28 (3) $\mu^{\#}\cdot\langle\text{Ⓡ},\gamma\rangle\notin\boldsymbol{\Sigma}^{01\sim}$.

   А тогда по теореме 10

   кнопка $\mathsf{P}^{\#}$ безопасна после трассы $\mu^{\#}$ в ~финальной спецификации.

   Допустим утверждение не верно и трасса $\mu^{\#}\cdot\kappa$ **L**-конформна.

Тогда существует конформная **L**-реализация, содержащая трассу $\mu^{\#}\cdot\kappa$.

По префикс-замкнутости трассовой модели,

в этой реализации есть и трасса $\mu^{\#}$.

По гипотезе о безопасности кнопка $P^{\#}$ должна быть безопасна (по ***safe in***) после трассы $\mu^{\#}$ в этой реализации.

Условие $\mu^{\#}\cdot\langle z\rangle\notin\boldsymbol{\Sigma}^{x}_{\alpha-1}=\boldsymbol{\Sigma}^{01\sim}\setminus\boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{01\sim})$ эквивалентно дизъюнкции двух условий

1) $\mu^{\#}\cdot\langle z\rangle\notin\boldsymbol{\Sigma}^{01\sim}$ и

2) $\mu^{\#}\cdot\langle z\rangle\in\boldsymbol{x}_{\alpha-1}(\boldsymbol{\Sigma}^{01\sim})$.

Кнопка $P^{\#}$ безопасна после безопасной трассы $\mu^{\#}$ в ~финальной спецификации, следовательно, каждое наблюдение $z\in P\cup\{P^{\#}\}$ безопасно в спецификации после трассы $\mu^{\#}$.

1.1.1. Случай 1: $\mu^{\#}\cdot\langle z\rangle\notin\boldsymbol{\Sigma}^{01\sim}$.

Наблюдение z после трассы $\mu^{\#}$ отсутствует в $\boldsymbol{\Sigma}^{01\sim}$ и, следовательно,

по лемме 13 оно либо опасно в ~финальной спецификации, что неверно, либо отсутствует в ней, но тогда оно не конформно и, следовательно, не **L**-конформно.

1.1.2. Случай 2: $\mu^{\#}\cdot\langle z\rangle\in\boldsymbol{x}_{\alpha-1}(\boldsymbol{\Sigma}^{01\sim})$.

Наблюдение z не **L**-конформно после трассы $\mu^{\#}$ по предположению шага индукции.

Итак, в обоих случаях в конформной реализации после трассы $\mu^{\#}$ нет конформных **L**-наблюдений, разрешаемых безопасной кнопкой $P^{\#}$, чего быть не может.

Мы пришли к противоречию, следовательно, наше допущение не верно, и утверждение в рассматриваемом случае 1.1 доказано.

1.2. Пусть трасса $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa$ получается по правилу вывода **3** как P-неполная трасса после $\mu^{\#}$:

$\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in\boldsymbol{\Sigma}^{x}_{\alpha-1}$ & $P\in\mathbf{R}$ & $\mu^{\#}\cdot\langle\text{Р},\gamma\rangle\notin\boldsymbol{\Sigma}^{x}_{\alpha-1}$

& $\forall z\in P\ \mu^{\#}\cdot\langle z\rangle\notin\boldsymbol{\Sigma}^{x}_{\alpha-1}$ & $\boldsymbol{Ip}(\mu)\neq\varnothing$

& $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin\boldsymbol{\Sigma}^{x}_{\alpha-1}$.

По лемме 28 (3) $\mu^{\#}\cdot\langle\text{Р},\gamma\rangle\notin\boldsymbol{\Sigma}^{x}_{\alpha-1}$ влечет $\mu^{\#}\cdot\langle\text{Р},\gamma\rangle\notin\boldsymbol{\Sigma}^{01\sim}$.

А тогда по теореме 10 кнопка $P^{\#}$ безопасна после трассы $\mu^{\#}$ в ~финальной спецификации.

Допустим утверждение не верно и трасса $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa$ **L**-конформна.

Тогда существует конформная **L**-реализация, содержащая трассу $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa$.

По префикс-замкнутости реализационной модели,

в ней есть трасса $\mu^{\#}\cdot\lambda^{\#}$ и ее префикс $\mu^{\#}$.

По гипотезе о безопасности кнопка $P^{\#}$ должна быть безопасна (по ***safe in***) после трассы $\mu^{\#}$ в этой реализации.

Как и в доказанном случае 1.1 каждое действие $z\in P$ не **L**-конформно, и, следовательно, его не может быть в конформной **L**-реализации после трассы $\mu^{\#}$.

Но тогда по полноте реализационной модели наличие в ней трассы $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa$ влечет наличие в ней трассы $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\cdot\kappa$ и, следовательно, по префикс-замкнутости реализационной модели ее префикса $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}$.

Условие $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin\boldsymbol{\Sigma}^{x}{}_{\alpha-1}=\boldsymbol{\Sigma}^{01\sim}\backslash\boldsymbol{x}_{\alpha-1}(\boldsymbol{\Sigma}^{01\sim})$ эквивалентно дизъюнкции двух условий

1) $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin\boldsymbol{\Sigma}^{01\sim}$ и

2) $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\in\boldsymbol{x}_{\alpha-1}(\boldsymbol{\Sigma}^{01\sim})$.

1.2.1. Случай 1: $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin\boldsymbol{\Sigma}^{01\sim}$.

Мы можем выбрать наибольший префикс $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_1{}^{\#}$ трассы $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}$, имеющийся в $\boldsymbol{\Sigma}^{01\sim}$, после которого в трассе $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}$ следует наблюдение u, отсутствующее в $\boldsymbol{\Sigma}^{01\sim}$.

Трасса $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_1{}^{\#}$ безопасна в спецификации по теореме 11, а наблюдение u безопасно после этой трассы в спецификации по лемме 16, поскольку трасса $\mu^{\#}\cdot\lambda^{\#}$ безопасна и, следовательно, безопасен ее префикс $\mu^{\#}\cdot\lambda_1{}^{\#}$ и после этого префикса безопасно наблюдение u, а эта трасса $\mu^{\#}\cdot\lambda_1{}^{\#}$ получается из трассы $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_1{}^{\#}$ удалением отказа $P^{\#}$.

Но тогда наблюдение u после трассы $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_1{}^{\#}$ отсутствует не только в $\boldsymbol{\Sigma}^{01\sim}$, но и в ~финальной спецификации по лемме 13, поэтому оно не конформно и, следовательно, не **L**-конформно.

Тем самым, не **L**-конформна трасса $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}$.

1.2.2. Случай 2: $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\in\boldsymbol{x}_{\alpha-1}(\boldsymbol{\Sigma}^{01\sim})$.

Трасса $\mu^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\cdot\lambda^{\#}$ не **L**-конформна по предположению шага индукции.

Итак, в обоих случаях в конформной реализации имеется не **L**-конформная трасса $\mu^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\cdot\lambda^{\#}$, чего быть не может.

Мы пришли к противоречию, следовательно, наше допущение не верно, и утверждение в рассматриваемом случае 1.2 доказано.

Тем самым, оно доказано в случае 1 (непредельный ординал).

2. Пусть α предельный ординал.

Тогда для любой трассы $\sigma\in \boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})$ найдется такой ординал $\beta<\alpha$, что $\sigma\in \boldsymbol{x}_{\beta}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})$.

Отсюда по предположению шага индукции трасса σ не **L**-конформна.

6.49. Доказательство леммы 30

1. Сначала докажем утверждение для множества $\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha}$ для каждого ординала α, учитывая, что $\boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})=\boldsymbol{\Sigma}^{\mathbf{01}\sim}\setminus\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha}$: если $\sigma^{\#}\in \boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})$, $\sigma`^{\#}\in\boldsymbol{\Sigma}^{\mathbf{01}\sim}$ и $\sigma^{\#}\in \boldsymbol{d}(\sigma`^{\#})$, то $\sigma`^{\#}\in \boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})$.

Будем вести доказательство трансфинитной индукцией.

Поскольку $\boldsymbol{x}_{0}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})=\varnothing$, для $\alpha=0$ утверждение очевидно.

Пусть утверждение верно для каждого ординала $\beta<\alpha$, и докажем его для ординала α.

1.1. Пусть α непредельный ординал.

Нам достаточно доказать, что если $\sigma^{\#}\in \boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})\setminus \boldsymbol{x}_{\alpha-1}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})$ и $\sigma^{\#}\in \boldsymbol{d}(\sigma`^{\#})$, то $\sigma`^{\#}\in \boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})$.

Если $\sigma`^{\#}\notin\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha-1}$, то условие $\sigma`^{\#}\in\boldsymbol{\Sigma}^{\mathbf{01}\sim}$ влечет $\sigma`^{\#}\in \boldsymbol{x}_{\alpha-1}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})$, что по правилу вывода **1** влечет $\sigma`^{\#}\in \boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})$.

Поэтому в дальнейшем будем считать, что $\sigma`^{\#}\in\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha-1}$.

Такая трасса $\sigma^{\#}$ получается по правилам вывода **2** или **3**.

1.1.1. Пусть трасса $\sigma^{\#}=\mu^{\#}\cdot\kappa$ получается по правилу вывода **2** для P-неконвергентного префикса $\mu^{\#}$:

$\mu^{\#}\cdot\kappa\in\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha-1}$ & $\mathsf{P}\in\mathbf{R}\cup\mathbf{Q}$ & $\mu^{\#}\cdot\langle \mathsf{P}, \gamma\rangle\notin\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha-1}$ & $\forall \mathsf{Z}\in\mathsf{P}\cup\{\mathsf{P}^{\#}\}$ $\mu^{\#}\cdot\langle \mathsf{Z}\rangle\notin\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha-1}$.

Тогда трассу $\sigma`^{\#}$ можно представить в виде $\sigma`^{\#}=\mu`^{\#}\cdot\kappa`$, где $\mu^{\#}\in \boldsymbol{d}(\mu`^{\#})$.

Мы докажем выполнение для кнопки P и трассы $\mu`^{\#}\cdot\kappa`\in\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha-1}$ следующих условий правила вывода **2**:

1) $\mu`^{\#}\cdot\langle \not\Rightarrow, \gamma\rangle \notin \boldsymbol{\Sigma}^{x}{}_{\alpha-1}$,

2) $\forall z \in P \cup \{P^{\#}\}\ \ \mu`^{\#}\cdot\langle z\rangle \notin \boldsymbol{\Sigma}^{x}{}_{\alpha-1}$.

1.1.1.1. Докажем, что $\mu`^{\#}\cdot\langle \not\Rightarrow, \gamma\rangle \notin \boldsymbol{\Sigma}^{x}{}_{\alpha-1}$.

По лемме 28 (2) $\mu^{\#} \in \boldsymbol{\Sigma}^{x}{}_{\alpha-1}$,

что вместе с $\mu^{\#}\cdot\langle \not\Rightarrow, \gamma\rangle \notin \boldsymbol{\Sigma}^{x}{}_{\alpha-1}$ влечет по лемме 28 (3) $\mu^{\#}\cdot\langle \not\Rightarrow, \gamma\rangle \notin \boldsymbol{\Sigma}^{01\sim}$.

Поэтому по теореме 10 кнопка $P^{\#}$ безопасна в ~пополнении после трассы $\mu^{\#}$.

А тогда, поскольку $\mu^{\#} \in \boldsymbol{d}(\mu`^{\#})$, по лемме 16 кнопка $P^{\#}$ безопасна после трассы $\mu`^{\#}$ в ~пополнении, откуда по теореме 10 следует, что $\mu`^{\#}\cdot\langle \not\Rightarrow, \gamma\rangle \notin \boldsymbol{\Sigma}^{01\sim}$, что влечет $\mu`^{\#}\cdot\langle \not\Rightarrow, \gamma\rangle \notin \boldsymbol{\Sigma}^{x}{}_{\alpha-1} = \boldsymbol{\Sigma}^{01\sim} \setminus \boldsymbol{x}_{\alpha-1}(\boldsymbol{\Sigma}^{01\sim})$.

1.1.1.2. Докажем, что $\forall z \in P \cup \{P^{\#}\}\ \ \mu`^{\#}\cdot\langle z\rangle \notin \boldsymbol{\Sigma}^{x}{}_{\alpha-1}$.

Условие $\mu^{\#}\cdot\langle z\rangle \notin \boldsymbol{\Sigma}^{x}{}_{\alpha-1} = \boldsymbol{\Sigma}^{01\sim} \setminus \boldsymbol{x}_{\alpha-1}(\boldsymbol{\Sigma}^{01\sim})$ эквивалентно дизъюнкции двух условий

1) $\mu^{\#}\cdot\langle z\rangle \notin \boldsymbol{\Sigma}^{01\sim}$ и

2) $\mu^{\#}\cdot\langle z\rangle \in \boldsymbol{x}_{\alpha-1}(\boldsymbol{\Sigma}^{01\sim})$.

Кнопка $P^{\#}$ безопасна после безопасной трассы $\mu^{\#}$ в ~пополнении, следовательно, каждое наблюдение $z \in P \cup \{P^{\#}\}$ безопасно в ~пополнении после трассы $\mu^{\#}$.

1.1.1.2.1. Случай 1: $\mu^{\#}\cdot\langle z\rangle \notin \boldsymbol{\Sigma}^{01\sim}$.

Наблюдение z после трассы $\mu^{\#}$ отсутствует в $\boldsymbol{\Sigma}^{01\sim}$ и, следовательно, по лемме 13 оно либо опасно в ~финальной спецификации, что неверно, либо отсутствует в ней $\mu^{\#}\cdot\langle z\rangle \notin \boldsymbol{\Sigma}^{\sim}$.

Поэтому по ***d***-замкнутости трассовой модели должно быть $\mu`^{\#}\cdot\langle z\rangle \notin \boldsymbol{\Sigma}^{\sim}$, что влечет $\mu`^{\#}\cdot\langle z\rangle \notin \boldsymbol{\Sigma}^{01\sim}$,

что влечет $\mu`^{\#}\cdot\langle z\rangle \notin \boldsymbol{\Sigma}^{x}{}_{\alpha-1} = \boldsymbol{\Sigma}^{01\sim} \setminus \boldsymbol{x}_{\alpha-1}(\boldsymbol{\Sigma}^{01\sim})$.

1.1.1.2.2. Случай 2: $\mu^{\#}\cdot\langle z\rangle \in \boldsymbol{x}_{\alpha-1}(\boldsymbol{\Sigma}^{01\sim})$.

Поскольку $\mu^{\#} \in \boldsymbol{d}(\mu`^{\#})$ влечет $\mu^{\#}\cdot\langle z\rangle \in \boldsymbol{d}(\mu`^{\#}\cdot\langle z\rangle)$,

по предположению шага индукции $\mu`^{\#}\cdot\langle z\rangle \in \boldsymbol{x}_{\alpha-1}(\boldsymbol{\Sigma}^{01\sim})$,

что влечет $\mu`^{\#}\cdot\langle z\rangle \notin \boldsymbol{\Sigma}^{x}{}_{\alpha-1} = \boldsymbol{\Sigma}^{01\sim} \setminus \boldsymbol{x}_{\alpha-1}(\boldsymbol{\Sigma}^{01\sim})$.

Итак, мы показали, что $\forall z \in P \cup \{P^{\#}\}\ \ \mu`^{\#}\cdot\langle z\rangle \notin \boldsymbol{\Sigma}^{x}{}_{\alpha-1}$.

Тем самым, мы доказали, что для отказа P и трассы $\mu`^{\#}\cdot\kappa`\in\boldsymbol{\Sigma}^{\boldsymbol{x}}_{\alpha-1}$ выполнены условия правила вывода **2**, поэтому $\sigma`^{\#}=\mu`^{\#}\cdot\kappa`\in\boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$, что и требовалось доказать.

1.1.2. Пусть трасса $\sigma^{\#}=\mu^{\#}\cdot\lambda^{\#}\cdot\kappa$ получается по правилу вывода **3** для префикса $\mu^{\#}\cdot\lambda^{\#}$ P-неполного после $\mu^{\#}$:

$\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in\boldsymbol{\Sigma}^{\boldsymbol{x}}_{\alpha-1}$ & $P\in\mathbf{R}$ & $\mu^{\#}\cdot\langle\not\mathbb{R},\gamma\rangle\notin\boldsymbol{\Sigma}^{\boldsymbol{x}}_{\alpha-1}$

& $\forall z\in P\ \mu^{\#}\cdot\langle z\rangle\notin\boldsymbol{\Sigma}^{\boldsymbol{x}}_{\alpha-1}$ & $\boldsymbol{Ip}(\mu)\neq\varnothing$

& $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin\boldsymbol{\Sigma}^{\boldsymbol{x}}_{\alpha-1}$.

Тогда трассу $\sigma`^{\#}$ можно представить в виде $\sigma`^{\#}=\mu`^{\#}\cdot\lambda`^{\#}\cdot\kappa`$, где $\mu^{\#}\in\boldsymbol{d}(\mu`^{\#})$ и $\lambda^{\#}\in\boldsymbol{d}(\lambda`^{\#})$.

Рассмотрим два случая в зависимости от того, P-конвергентна трасса $\mu^{\#}$ или нет во множестве $\boldsymbol{\Sigma}^{\boldsymbol{x}}_{\alpha-1}$.

1.1.2.1. Трасса $\mu^{\#}$ P-неконвергентна в $\boldsymbol{\Sigma}^{\boldsymbol{x}}_{\alpha-1}$.

Тогда по доказанному в 1.1.1 $\sigma`^{\#}\in\boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$, что и требовалось доказать.

1.1.2.2. Трасса $\mu^{\#}$ P-конвергентна в $\boldsymbol{\Sigma}^{\boldsymbol{x}}_{\alpha-1}$.

Тогда $\mu^{\#}\cdot\langle P^{\#}\rangle\in\boldsymbol{\Sigma}^{\boldsymbol{x}}_{\alpha-1}$.

1.1.2.2.1. Докажем, что $\mu`^{\#}\cdot\langle\not\mathbb{R},\gamma\rangle\notin\boldsymbol{\Sigma}^{\boldsymbol{x}}_{\alpha-1}$.

По лемме 28 (1) $\mu^{\#}\cdot\langle P^{\#}\rangle\in\boldsymbol{\Sigma}^{\boldsymbol{x}}_{\alpha-1}$ влечет $\mu^{\#}\cdot\langle P^{\#}\rangle\in\boldsymbol{\Sigma}^{\mathbf{01\sim}}$.

Следовательно, по правилам вывода ~финальных трасс $\mu^{\#}\cdot\langle\not\mathbb{R},\gamma\rangle\notin\boldsymbol{\Sigma}^{\mathbf{01\sim}}$.

А тогда аналогично 1.1.1.1 $\mu`^{\#}\cdot\langle\not\mathbb{R},\gamma\rangle\notin\boldsymbol{\Sigma}^{\boldsymbol{x}}_{\alpha-1}$.

1.1.2.2.2. Поскольку мы уже доказали, что $\mu^{\#}\cdot\langle\not\mathbb{R},\gamma\rangle\notin\boldsymbol{\Sigma}^{\mathbf{01\sim}}$, то аналогично 1.1.1.2 $\forall z\in P$ $\mu`^{\#}\cdot\langle z\rangle\notin\boldsymbol{\Sigma}^{\boldsymbol{x}}_{\alpha-1}$.

Итак у нас выполнены часть условий P-неконвергентности трассы $\mu`^{\#}$ или $P$-неполноты трассы $\mu`^{\#}\cdot\lambda`^{\#}$ после трассы $\mu`^{\#}$:

$\mu`^{\#}\cdot\langle\not\mathbb{R},\gamma\rangle\notin\boldsymbol{\Sigma}^{\boldsymbol{x}}_{\alpha-1}$ и $\forall z\in P$ $\mu`^{\#}\cdot\langle z\rangle\notin\boldsymbol{\Sigma}^{\boldsymbol{x}}_{\alpha-1}$.

Далее возможны два случая (1.1.2.2.3 и 1.1.2.2.4) в зависимости от того, продолжается трасс: $\mu`^{\#}$ отказом $P^{\#}$ в $\boldsymbol{\Sigma}^{\boldsymbol{x}}_{\alpha-1}$, или нет.

1.1.2.2.3. Случай 1: $\mu`^{\#}\cdot\langle P^{\#}\rangle\notin\boldsymbol{\Sigma}^{\boldsymbol{x}}_{\alpha-1}$.

В этом случае для трассы $\mu`^{\#}\cdot\lambda`^{\#}\cdot\kappa`$ и кнопки $P^{\#}$ после $\mu`^{\#}$ выполнены все условия P-неконвергентности трассы $\mu`^{\#}$, то есть условия правила вывода **2**:

$\mu`^{\#}\cdot\langle P, \gamma\rangle \notin \boldsymbol{\Sigma}^{x}_{\alpha-1}$ & $\forall z \in P$ $\mu`^{\#}\cdot\langle z\rangle \notin \boldsymbol{\Sigma}^{x}_{\alpha-1}$ & $\mu`^{\#}\cdot\langle P^{\#}\rangle \notin \boldsymbol{\Sigma}^{x}_{\alpha-1}$.

Следовательно, $\sigma`^{\#} \in \boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{01\sim})$, что и требовалось доказать.

1.1.2.2.4. Случай 2: $\mu`^{\#}\cdot\langle P^{\#}\rangle \in \boldsymbol{\Sigma}^{x}_{\alpha-1}$.

Покажем P-неполноту трассы $\mu`^{\#}\cdot\lambda`^{\#}$ после трассы $\mu`^{\#}$, то есть выполнение для (особого) отказа $P^{\#}$ и трассы $\mu`^{\#}\cdot\lambda`^{\#}\cdot\kappa` \in \boldsymbol{\Sigma}^{x}_{\alpha-1}$ всех условий правила вывода **3**. С учетом уже доказанных условий нам осталось показать следующие условия:

1) $\boldsymbol{Ip}(\mu`) \neq \varnothing$,

2) $\mu`^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda`^{\#} \notin \boldsymbol{\Sigma}^{x}_{\alpha-1}$.

Первое условие следует из условия $\boldsymbol{Ip}(\mu) \neq \varnothing$.

Докажем выполнение второго условия.

Здесь возможны два варианта в зависимости от того, имелась ли трасса $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}$ в $\boldsymbol{\Sigma}^{01\sim}$, или нет.

1.1.2.2.4.1. $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#} \in \boldsymbol{\Sigma}^{01\sim}$.

Тогда, поскольку $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#} \notin \boldsymbol{\Sigma}^{x}_{\alpha-1}$,

имеем $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#} \in \boldsymbol{x}_{\alpha-1}(\boldsymbol{\Sigma}^{01\sim})$.

Отсюда, поскольку $\mu^{\#} \in \boldsymbol{d}(\mu`^{\#})$ и $\lambda^{\#} \in \boldsymbol{d}(\lambda`^{\#})$

имеем $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#} \in \boldsymbol{d}(\mu`^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda`^{\#})$.

Отсюда по предположению шага индукции

$\mu`^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda`^{\#} \in \boldsymbol{x}_{\alpha-1}(\boldsymbol{\Sigma}^{01\sim})$.

Отсюда по правилу вывода **1** имеем $\mu`^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda`^{\#} \in \boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{01\sim})$.

Следовательно, $\mu`^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda`^{\#} \notin \boldsymbol{\Sigma}^{x}_{\alpha-1}$.

1.1.2.2.4.2. $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#} \notin \boldsymbol{\Sigma}^{01\sim}$.

Выберем наибольший префикс $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_1{}^{\#}$ трассы $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}$, имеющийся в $\boldsymbol{\Sigma}^{01\sim}$, после которого в трассе $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}$ следует наблюдение u, отсутствующее в $\boldsymbol{\Sigma}^{01\sim}$.

Трасса $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_1{}^{\#}$ безопасна в спецификации по теореме 11, а наблюдение u безопасно после этой трассы в спецификации по лемме 16, поскольку трасса $\mu^{\#}\cdot\lambda^{\#}$ безопасна и, следовательно,

безопасен ее префикс $\mu^{\#}\cdot\lambda_1{}^{\#}$ и после этого префикса безопасно наблюдение u, а эта трасса $\mu^{\#}\cdot\lambda_1{}^{\#}$ получается из трассы $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_1{}^{\#}$ удалением отказа $P^{\#}$.

Но тогда по лемме 13 наблюдение u после трассы $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_1{}^{\#}$ либо опасно, что неверно, либо отсутствует не только в $\boldsymbol{\Sigma^{01\sim}}$, но и в ~пополнении $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_1{}^{\#}\cdot\langle u\rangle\notin\boldsymbol{\Sigma^{\sim}}$, что влечет $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin\boldsymbol{\Sigma^{\sim}}$, что влечет $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin\cup\boldsymbol{d}(\boldsymbol{\Sigma^{01\sim}})$.

Поэтому по ***d***-замкнутости трассовой модели должно быть $\mu`^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda`^{\#}\notin\cup\boldsymbol{d}(\boldsymbol{\Sigma^{01\sim}})$,

что влечет $\mu`^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda`^{\#}\notin\boldsymbol{\Sigma^{01\sim}}$,

что влечет $\mu`^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda`^{\#}\notin\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha-1}=\boldsymbol{\Sigma^{01\sim}}\setminus\boldsymbol{x}_{\alpha-1}(\boldsymbol{\Sigma^{01\sim}})$.

Итак, мы показали выполнение для (особого) отказа $P^{\#}$ и трассы $\mu`^{\#}\cdot\lambda`^{\#}\cdot\kappa`\in\boldsymbol{\Sigma}^{\boldsymbol{x}}{}_{\alpha-1}$ всех условий правила вывода **3**.

Следовательно, $\sigma`^{\#}=\mu`^{\#}\cdot\lambda`^{\#}\cdot\kappa`\in\boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma^{01\sim}})$, что и требовалось доказать.

Итак, для всех случаев мы показали, что $\sigma`^{\#}=\mu`^{\#}\cdot\lambda`^{\#}\cdot\kappa`\in\boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma^{01\sim}})$.

Тем самым, утверждение доказано для непредельного ординала.

1.2. Пусть α предельный ординал.

Тогда для любой трассы $\sigma^{\#}\in\boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma^{01\sim}})$ найдется такой ординал $\beta<\alpha$, что $\sigma^{\#}\in\boldsymbol{x}_{\beta}(\boldsymbol{\Sigma^{01\sim}})$.

Отсюда по предположению шага индукции,

если $\sigma^{\#}\in\boldsymbol{d}(\sigma`^{\#})$, то $\sigma^{\#}`\in\boldsymbol{x}_{\beta}(\boldsymbol{\Sigma^{01\sim}})$,

что по правилу вывода **1** влечет $\sigma^{\#}`\in\boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma^{01\sim}})$.

2. Утверждение для множества $\boldsymbol{\Sigma}^{\boldsymbol{x}}$ непосредственно следует из утверждения 1 и определения $\boldsymbol{x}(\boldsymbol{\Sigma}^{\boldsymbol{x}})=\boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{\boldsymbol{x}})$, где α такое, что $\boldsymbol{x}_{\alpha}(\boldsymbol{\Sigma}^{\boldsymbol{x}})=\boldsymbol{x}_{\alpha+1}(\boldsymbol{\Sigma}^{\boldsymbol{x}})$.

6.50. Доказательство леммы 31

1. Докажем утверждение 1: Пусть трасса $\sigma^{\#}\in\mathbf{I}^{\mathbf{R}}$. Тогда найдутся такие трассы $\sigma_1{}^{\#}$ и $\sigma_2{}^{\#}$, что $\sigma_2{}^{\#}\in\boldsymbol{\Sigma}^{\boldsymbol{x}}$, $\sigma_1{}^{\#}\in\boldsymbol{i}^{\nabla}(\sigma_2{}^{\#})$ и $\sigma^{\#}\in\boldsymbol{d}(\sigma_1{}^{\#})$.

Если $\sigma^{\#}\in\mathbf{I}^{\mathbf{R}}$, то найдется такая трасса $\sigma_1{}^{\#}\in\boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{\boldsymbol{x}}))$, что $\sigma^{\#}\in\boldsymbol{d}(\sigma_1{}^{\#})$.

Поскольку операция $\boldsymbol{l}$ не добавляет новых трасс, $\sigma_1{}^{\#}\in\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{\boldsymbol{x}})$.

Следовательно, найдется такая трасса $\sigma_2{}^{\#}\in\boldsymbol{\Sigma}^{\boldsymbol{x}}$, что $\sigma_1{}^{\#}\in\boldsymbol{i}^{\nabla}(\sigma_2{}^{\#})$.

2. Докажем утверждение 2: Пусть трасса $\sigma^{\#}\in\mathbf{I}^{\mathbf{R}}$ для некоторой **R**-кнопки $P\in\mathbf{R}$ не продолжается действиями $z\in P$ во множестве $\mathbf{I}^{\mathbf{R}}$, $\sigma_2{}^{\#}\in\boldsymbol{\Sigma}^{x}$, $\sigma_1{}^{\#}\in\boldsymbol{i}^{\nabla}(\sigma_2{}^{\#})$ и $\sigma^{\#}\in\boldsymbol{d}(\sigma_1{}^{\#})$. Тогда трасса $\sigma_2{}^{\#}$ не продолжается действиями $z\in P$ во множестве $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{x})$.

   Поскольку трасса $\sigma^{\#}$ не продолжается действиями $z\in P$ во множестве $\mathbf{I}^{\mathbf{R}}$, $\sigma^{\#}\in\boldsymbol{d}(\sigma_1{}^{\#})$ и $\sigma_1{}^{\#}\in\boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{x}))$, трасса $\sigma_1{}^{\#}$ не продолжается действиями $z\in P$ во множестве $\boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{x}))$.

   Поскольку операция $\boldsymbol{l}$ удаляет только **L**-трассы, а для любого действия $z\in P$ трасса $\sigma_1{}^{\#}\cdot\langle z\rangle$ является **L**-трассой, трасса $\sigma_1{}^{\#}$ не продолжается действиями $z\in P$ во множестве $\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{x})$.

   Допустим утверждение 2 не верно: $\sigma_2{}^{\#}\cdot\langle z\rangle\in\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{x})$ для некоторого $z\in P$.

   Тогда найдется такая трасса $\sigma_2{}`{}^{\#}\cdot\langle z\rangle\in\boldsymbol{\Sigma}^{x}$, что $\sigma_2{}^{\#}\in\boldsymbol{d}(\sigma_2{}`{}^{\#})$.

   Покажем, что трассу $\sigma_2{}`{}^{\#}$ можно выбрать такой, чтобы нашлась такая трасса $\sigma_1{}`{}^{\#}\in\boldsymbol{i}^{\nabla}(\sigma_2{}`{}^{\#})$, что $\sigma_1{}^{\#}\in\boldsymbol{d}(\sigma_1{}`{}^{\#})$.

   Для этого достаточно показать, что любой отказ, вставляемый при переходе от трассы $\sigma_2{}^{\#}$ к трассе $\sigma_1{}^{\#}$, либо может быть вставлен в соответствующее место трассы $\sigma_2{}`{}^{\#}\cdot\langle z\rangle$ и при этом получится трасса из $\boldsymbol{\Sigma}^{x}$, либо необходим после соответствующего префикса трассы $\sigma_2{}`{}^{\#}$, то есть может быть вставлен в трассу $\sigma_2{}`{}^{\#}\cdot\langle z\rangle$ операцией $\boldsymbol{i}^{\nabla}$.

   Пусть $\sigma_1{}^{\#}=\mu_1{}^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda_1{}^{\#}$ и $\sigma_2{}^{\#}=\mu_2{}^{\#}\cdot\lambda_2{}^{\#}$, где $\mu_1{}^{\#}\in\boldsymbol{i}^{\nabla}(\mu_2{}^{\#})$ и $\mu_1{}^{\#}\cdot\lambda_1{}^{\#}\in\boldsymbol{i}^{\nabla}(\mu_2{}^{\#}\cdot\lambda_2{}^{\#})$, то есть отказ $R^{\#}\in\mathbf{R}^{\#}$ вставляется в трассу $\sigma_2{}^{\#}$ после трассы $\mu_2{}^{\#}$. Следовательно, выполнены условия необходимости отказа $R^{\#}$ после трассы $\mu_2{}^{\#}$:

   1) $\mu_2{}^{\#}\cdot\langle \mathbf{R}, \gamma\rangle\in\boldsymbol{\Sigma}^{x}$,
   2) $\forall z\in R\ \ \mu_2{}^{\#}\cdot\langle z\rangle\notin\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{x})$,
   3) $\boldsymbol{Ip}(\mu_2)\neq\varnothing\ \vee\ (\boldsymbol{Ip}(\mu_2)=\varnothing\ \&\ \forall T\in\mathbf{R}\ \ \mu_2{}^{\#}\cdot\langle T^{\#}\rangle\notin\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{x}))$.

   Трассу $\sigma_2{}`{}^{\#}$ можно представить в виде $\sigma_2{}`{}^{\#}=\mu_2{}`{}^{\#}\cdot\lambda_2{}`{}^{\#}$, где $\mu_2{}^{\#}\in\boldsymbol{d}(\mu_2{}`{}^{\#})$ и $\lambda_2{}^{\#}\in\boldsymbol{d}(\lambda_2{}`{}^{\#})$.

   Нам достаточно показать, что либо $\mu_2{}`{}^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda_2{}`{}^{\#}\cdot\langle z\rangle\in\boldsymbol{\Sigma}^{x}$, либо $\mu_2{}`{}^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda_2{}`{}^{\#}\cdot\langle z\rangle\in\boldsymbol{i}^{\nabla}(\mu_2{}`{}^{\#}\cdot\lambda_2{}`{}^{\#}\cdot\langle z\rangle)$.

   Так как $\mu_2{}^{\#}\in\boldsymbol{d}(\mu_2{}`{}^{\#})$, условие 2 необходимости отказа $R^{\#}$ после трассы $\mu_2{}^{\#}$ выполнено и для трассы $\mu_2{}`{}^{\#}$: трасса $\mu_2{}`{}^{\#}$ не продолжается действиями из R в $\boldsymbol{d}$-замыкании $\boldsymbol{\Sigma}^{x}$.

   Рассмотрим два возможных случая (2.1 и 2.2).

2.1. Трасса $\mu_2`^{\#}$ не заканчивается отказами: $\boldsymbol{Ip}(\mu_2`)=\varnothing$.

Тогда, поскольку $\mu_2{}^{\#}\in\boldsymbol{d}(\mu_2`^{\#})$, трасса $\mu_2{}^{\#}$ тоже не заканчивается отказами: $\boldsymbol{Ip}(\mu_2)=\varnothing$.

Поскольку $\boldsymbol{Ip}(\mu_2)=\varnothing$, из условия 3 необходимости необходимости отказа $R^{\#}$ после трассы $\mu_2{}^{\#}$ следует, что трасса $\mu_2{}^{\#}$ не продолжается никакими отказами в $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^x)$.

Отсюда, поскольку $\mu_2{}^{\#}\in\boldsymbol{d}(\mu_2`^{\#})$, трасса $\mu_2`^{\#}$ тоже не продолжается никакими отказами в $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^x)$.

Тем самым, выполнено условие 3 необходимости отказа $R^{\#}$ после трассы $\mu_2`^{\#}$.

Условие 2 необходимости отказа $R^{\#}$ после трассы $\mu_2`^{\#}$ означает, что трасса $\mu_2`^{\#}$ не продолжается действиями $z\in R$ во множестве $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^x)$, тем более она не продолжается этими действиями в подмножестве $\boldsymbol{\Sigma}^x$.

Поскольку трасса $\mu_2`^{\#}$ не продолжается никакими отказами во множестве $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^x)$, она не продолжается отказом $R^{\#}$ в подмножестве $\boldsymbol{\Sigma}^x$.

Следовательно, трасса $\mu_2`^{\#}$ не продолжается никакими **L**-наблюдениями, разрешаемыми кнопкой $R^{\#}$, во множестве $\boldsymbol{\Sigma}^x$.

Поэтому, если бы условие 1 необходимости отказа $R^{\#}$ после трассы $\mu_2`^{\#}$ не было выполнено, то есть было бы $\mu_2{}^{\#}\cdot\langle\boldsymbol{R}, \gamma\rangle\notin\boldsymbol{\Sigma}^x$, то были бы выполнены все условия R-неконвергентности трассы $\mu_2`^{\#}$, чего быть не может, поскольку в $\boldsymbol{\Sigma}^x$ все трассы **L**-конвергентны.

Следовательно, условие 1 необходимости отказа $R^{\#}$ после трассы $\mu_2`^{\#}$ выполнено.

Итак, у нас выполнены все три условия необходимости отказа $R^{\#}$ после трассы $\mu_2`^{\#}$.

Следовательно, условие $\mu_2`^{\#}\cdot\lambda_2`^{\#}\cdot\langle z\rangle\in\boldsymbol{\Sigma}^x$

влечет требуемое условие $\mu_2`^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda_2`^{\#}\cdot\langle z\rangle\in\boldsymbol{i}^{\nabla}(\mu_2`^{\#}\cdot\lambda_2`^{\#}\cdot\langle z\rangle)$.

2.2. Трасса $\mu_2`^{\#}$ заканчивается отказами: $\boldsymbol{Ip}(\mu_2`)\neq\varnothing$.

Тогда выполнено условие 3 необходимости отказа $R^{\#}$ после трассы $\mu_2`^{\#}$.

Рассмотрим два случая (2.2.1 и 2.2.2).

2.2.1. $\mu_2`\cdot\langle \not{R}, \gamma\rangle \in \Sigma^x$.

Этот случай означает, что выполнено условие 1 необходимости отказа $R^\#$ после трассы $\mu_2`^\#$.

Тем самым выполнены все три условия необходимости отказа $R^\#$ после трассы $\mu_2`^\#$.

Следовательно, условие $\mu_2`^\#\cdot\lambda_2`^\#\cdot\langle z\rangle \in \Sigma^x$

влечет требуемое условие $\mu_2`^\#\cdot\langle R^\#\rangle\cdot\lambda_2`^\#\cdot\langle z\rangle \in i^\nabla(\mu_2`^\#\cdot\lambda_2`^\#\cdot\langle z\rangle)$.

2.2.2. $\mu_2`\cdot\langle \not{R}, \gamma\rangle \notin \Sigma^x$.

Также, поскольку выполнено условие 2 необходимости отказа $R^\#$ после трассы $\mu_2`^\#$, то есть трасса $\mu_2`^\#$ не продолжается действиями $z\in R$ во множестве $\cup d(\Sigma^x)$, то эта трасса не продолжается этими действиями в подмножестве Σ^x: $\forall z\in R\ \ \mu_2`^\#\cdot\langle z\rangle \notin \Sigma^x$.

Итак, $R^\#\in \mathbf{R}^\#$, $\mu_2`\cdot\langle \not{R}, \gamma\rangle \notin \Sigma^x$, $\forall z\in R\ \ \mu_2`^\#\cdot\langle z\rangle \notin \Sigma^x$, $Ip(\mu_2`)\neq\varnothing$, что означает, что отказ $R^\#$ особый после трассы $\mu_2`^\#$.

Поэтому, поскольку в Σ^x все трассы **L**-полны, условие $\mu_2`^\#\cdot\lambda_2`^\#\cdot\langle z\rangle = \sigma_2`^\#\cdot\langle z\rangle \in \Sigma^x$ влечет $\mu_2`^\#\cdot\langle R^\#\rangle\cdot\lambda_2`^\#\cdot\langle z\rangle \in \Sigma^x$, что и требовалось доказать.

Итак, мы показали, что либо $\mu_2`^\#\cdot\langle R^\#\rangle\cdot\lambda_2`^\#\cdot\langle z\rangle \in \Sigma^x$, либо $\mu_2`^\#\cdot\langle R^\#\rangle\cdot\lambda_2`^\#\cdot\langle z\rangle \in i^\nabla(\mu_2`^\#\cdot\lambda_2`^\#\cdot\langle z\rangle)$.

Следовательно, мы показали, что трассу $\sigma_2`^\#$ можно выбрать такой, чтобы нашлась такая трасса $\sigma_1`^\#\in i^\nabla(\sigma_2`^\#)$, что $\sigma_1{}^\#\in d(\sigma_1`^\#)$.

Но $\sigma_2`^\#\cdot\langle z\rangle \in \Sigma^x$ влечет $\sigma_1`^\#\cdot\langle z\rangle \in \cup i^\nabla(\Sigma^x)$, что влечет $\sigma_1`^\#\cdot\langle z\rangle \in l(\cup i^\nabla(\Sigma^x))$, что влечет $\sigma^\#\cdot\langle z\rangle \in \mathbf{I}^\mathbf{R}$, что неверно.

Следовательно, наше допущение, что для некоторого $z\in P$ имеет место $\sigma_2{}^\#\cdot\langle z\rangle \in \cup d(\Sigma^x)$, не верно, и лемма доказана.

6.51. Доказательство леммы 32

По построению множество $\mathbf{I}^\mathbf{R}$ содержит трассы в алфавите $\mathbf{L}\cup\mathbf{R}^\#$: множество Σ^x содержит **L**-трассы и трассы с не-отказами, операция i^∇ добавляет **L**-трассы и трассы с не-отказами, операция l удаляет трассы с не-отказами, операция d, примененная к множеству **L**-трасс, добавляет только **L**-трассы, поэтому остаются только **L**-трассы, то есть трассы в алфавите $\mathbf{L}\cup\mathbf{R}^\#$.

Поэтому, если мы докажем, что множество $\mathbf{I}^\mathbf{R}$ является $\mathbf{R}^\#$-моделью, то это будет $\mathbf{R}^\#$-модель в алфавите $\mathbf{L}^+$.

Сначала покажем, что трассы множества $\mathbf{I^R}$ не содержат дивергенции и разрушения.

Действительно, по $\Delta\gamma$-свойству множества $\mathbf{\Sigma^{01\sim}}$ дивергенция и разрушение могут быть только после не-отказов.

Поскольку по лемме 28 (1) $\mathbf{\Sigma^x \subseteq \Sigma^{01\sim}}$, в трассах множества $\mathbf{\Sigma^x}$ дивергенция и разрушение также могут быть только после не-отказов.

Операция $\boldsymbol{i}^\nabla$ только вставляет в уже существующие трассы отказы после их **L**-префиксов, то есть не вставляет отказов после не-отказов. Поэтому в трассах множества $\cup\boldsymbol{i}^\nabla(\mathbf{\Sigma^x})$ дивергенция и разрушение также могут быть только после не-отказов.

Далее, поскольку **L**-трассы не содержат не-отказов, после операции $\boldsymbol{l}$ (удаление не **L**-трасс) не остается трасс с дивергенцией и разрушением.

Операция $\boldsymbol{d}$-замыкания не добавляет дивергенцию и разрушение, если их не было.

Тем самым, трассы множества $\mathbf{I^R} = \cup\boldsymbol{d}(\boldsymbol{l}(\cup\boldsymbol{i}^\nabla(\mathbf{\Sigma^x})))$ не содержат дивергенции и разрушения.

1. Непустота.

   Из условия $\mathbf{\Sigma^x \neq \varnothing}$ и префикс-замкнутости множества $\mathbf{\Sigma^x}$ (лемма 28 (2)) следует, что $\epsilon \in \mathbf{\Sigma^x}$, поскольку пустая трасса является префиксом любой трассы.

   А тогда, поскольку операции $\boldsymbol{i}^\nabla$, $\boldsymbol{l}$ и $\boldsymbol{d}$ не удаляют **L**-трассы, а пустая трасса является **L**-трассой, имеем $\epsilon \in \cup\boldsymbol{d}(\boldsymbol{l}(\cup\boldsymbol{i}^\nabla(\mathbf{\Sigma^x}))) = \mathbf{I^R}$.

   Тем самым, $\mathbf{I^R \neq \varnothing}$.

2. Префикс-замкнутость.

   По лемме 28 (2) множество $\mathbf{\Sigma^x}$ префикс-замкнуто.

   Операция $\cup\boldsymbol{i}^\nabla$, примененная к префикс-замкнутому множеству, дает префикс-замкнутое множество, поскольку, если трасса σ получается вставкой необходимых отказов в трассу μ, то любой префикс трассы σ также получается вставкой необходимых отказов в некоторый префикс трассы μ.

   Операция $\boldsymbol{l}$ (удаление не **L**-трасс), примененная к префикс-замкнутому множеству, дает префикс-замкнутое множество, поскольку префикс **L**-трассы является **L**-трассой.

   $\boldsymbol{d}$-замыкание префикс-замкнутого множества префикс-замкнуто, поскольку, если трасса σ получается удалением каких-то отказов из

трассы μ, то любой префикс трассы σ также получается удалением соответствующих отказов из некоторого префикса трассы μ.

Следовательно, множество $\mathbf{I^R} = \cup\boldsymbol{d}(\boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{x})))$ префикс-замкнуто.

3. Допустимость.

По доказанному выше трассы из множества $\mathbf{I^R}$ не содержат дивергенции и разрушения, а все такие трассы допустимы.

4. Согласованность.

По лемме 8 трассы из множества $\boldsymbol{\Sigma}^{\mathbf{01\sim}}$ согласованы.

Тем самым, согласованы трассы его подмножества $\boldsymbol{\Sigma}^{x} = \boldsymbol{\Sigma}^{\mathbf{01\sim}}\backslash x(\boldsymbol{\Sigma}^{\mathbf{01\sim}})$.

Отказ $\mathsf{P}^{\#}$ необходим после трассы $\mu^{\#}$, если, в частности, трасса $\mu^{\#}$ не продолжается действиями из P в ***d***-замыкании $\boldsymbol{\Sigma}^{x}$. Поэтому после операции $\cup\boldsymbol{i}^{\nabla}$ трасса σ может быть несогласованной только в том случае, когда она имеет вид $\sigma=\mu^{\#}\cdot\langle\mathsf{P}^{\#}\rangle\cdot\rho^{\#}\cdot\langle\not\mathsf{R}\rangle\cdot\lambda$, где $\rho^{\#}$ трасса отказов.

Тем самым, после операции $\cup\boldsymbol{i}^{\nabla}$ несогласованными могут быть только трассы, содержащие не-отказы, то есть не **L**-трассы.

Такие несогласованные не **L**-трассы будут удалены последующей операцией ***l*** (удаление не **L**-трасс), после которой останутся только согласованные трассы.

При ***d***-замыкании согласованность трасс, очевидно, сохраняется.

Поэтому все трассы множества $\mathbf{I^R} = \cup\boldsymbol{d}(\boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{x})))$ согласованы.

5. Конвергентность.

Если трасса продолжается действием $\mathsf{z}\in\mathsf{P}$ для некоторой **R**-кнопки P во множестве $\mathbf{I^R}$, то она конвергентна по этой кнопке.

Рассмотрим трассу $\sigma^{\#}\in\mathbf{I^R}$, которая не продолжается действиями $\mathsf{z}\in\mathsf{P}$ для некоторой **R**-кнопки P во множестве $\mathbf{I^R}$. Поскольку после операции ***l*** нет дивергенции, разрушения и не-отказов, нам достаточно доказать, что трасса $\sigma^{\#}$ продолжается в $\mathbf{I^R}$ $\mathbf{R}^{\#}$-отказом $\mathsf{P}^{\#}$.

Тогда по лемме 31 найдутся такие трассы $\sigma_1{}^{\#}$ и $\sigma_2{}^{\#}$, что $\sigma_2{}^{\#}\in\boldsymbol{\Sigma}^{x}$, $\sigma_1{}^{\#}\in\boldsymbol{i}^{\nabla}(\sigma_2{}^{\#})$ и $\sigma^{\#}\in\boldsymbol{d}(\sigma_1{}^{\#})$, и трасса $\sigma_2{}^{\#}$ не продолжается действиями $\mathsf{z}\in\mathsf{P}$ во множестве $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{x})$.

Рассмотрим два возможных случая (5.1 и 5.2).

5.1. $\sigma_2{}^{\#}\cdot\langle\not\mathsf{R},\gamma\rangle\notin\boldsymbol{\Sigma}^{x}$.

Тогда выполнены все, кроме одного, условия P-неконвергентности трассы $\sigma_2{}^{\#}$ в $\boldsymbol{\Sigma}^{x}$: $\mathsf{P}\in\mathbf{R}\cup\mathbf{Q}$ & $\sigma_2{}^{\#}\in\boldsymbol{\Sigma}^{x}$ & $\sigma_2{}^{\#}\cdot\langle\not\mathsf{R},\gamma\rangle\notin\boldsymbol{\Sigma}^{x}$ & $\forall\mathsf{z}\in\mathsf{P}$ $\sigma_2{}^{\#}\cdot\langle\mathsf{z}\rangle\notin\boldsymbol{\Sigma}^{x}$.

Не выполнено может быть только условие $\sigma_2{}^{\#}\cdot\langle\mathsf{P}^{\#}\rangle\notin\boldsymbol{\Sigma}^{x}$.

Но, поскольку все **L**-трассы в $\boldsymbol{\Sigma}^x$ **L**-конвергентны, это условие и не должно быть выполнено: $\sigma_2{}^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\in\boldsymbol{\Sigma}^x$.

А тогда $\sigma_1{}^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\in\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^x)$,

что влечет $\sigma_1{}^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\in\boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^x))$,

что влечет $\sigma^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\in\cup\boldsymbol{d}(\boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^x)))=\mathbf{I}^{\mathbf{R}}$, что и требовалось доказать.

5.2. $\sigma_2{}^{\#}\cdot\langle \not{\mathsf{R}}, \gamma\rangle\in\boldsymbol{\Sigma}^x$.

Тогда возможны два случая (5.2.1 и 5.2.2).

5.2.1. Выполнено 3-е условие необходимости отказа $\mathsf{P}^{\#}$ после трассы $\sigma_2{}^{\#}$:

$\boldsymbol{Ip}(\mu)\neq\varnothing \ \vee\ (\boldsymbol{Ip}(\mu)=\varnothing \ \&\ \forall \mathsf{R}\in\mathbf{R}\ \ \mu^{\#}\cdot\langle \mathsf{R}^{\#}\rangle\notin\boldsymbol{\Sigma}^x)$.

В этом случае выполнены также первые два условия необходимости отказа $\mathsf{P}^{\#}$ после трассы $\sigma_2{}^{\#}$:

1) $\sigma_2{}^{\#}\cdot\langle \not{\mathsf{R}}, \gamma\rangle\in\boldsymbol{\Sigma}^x$,

2) $\forall \mathsf{z}\in\mathsf{P}\ \ \sigma_2{}^{\#}\cdot\langle \mathsf{z}\rangle\notin\cup\boldsymbol{d}(\boldsymbol{\Sigma}^x)$.

Следовательно, отказ $\mathsf{P}^{\#}$ необходим после трассы $\sigma_2{}^{\#}$.

Поэтому $\sigma_1{}^{\#}\in\boldsymbol{i}^{\nabla}(\sigma_2{}^{\#})$ влечет $\sigma_1{}^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\in\boldsymbol{i}^{\nabla}(\sigma_2{}^{\#})$,

что влечет $\sigma_1{}^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\in\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^x)$,

что влечет $\sigma_1{}^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\in\boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^x))$,

что влечет $\sigma^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\in\cup\boldsymbol{d}(\boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^x)))=\mathbf{I}^{\mathbf{R}}$, что и требовалось доказать.

5.2.2. Не выполнено 3-е условие необходимости отказа $\mathsf{P}^{\#}$ после трассы $\sigma_2{}^{\#}$: $\boldsymbol{Ip}(\sigma_2)=\varnothing \ \&\ \exists \mathsf{R}\in\mathbf{R}\ \ \sigma_2{}^{\#}\cdot\langle \mathsf{R}^{\#}\rangle\in\boldsymbol{\Sigma}^x$.

Условие $\forall \mathsf{z}\in\mathsf{P}\ \ \sigma_2{}^{\#}\cdot\langle \mathsf{z}\rangle\notin\cup\boldsymbol{d}(\boldsymbol{\Sigma}^x)$ влечет

выполнение условия $\forall \mathsf{z}\in\mathsf{P}\ \ \sigma_2{}^{\#}\cdot\langle \mathsf{R}^{\#}\rangle\cdot\langle \mathsf{z}\rangle\notin\cup\boldsymbol{d}(\boldsymbol{\Sigma}^x)$.

Рассмотрим два возможных случая (5.2.2.1 и 5.2.2.2).

5.2.2.1. $\sigma_2{}^{\#}\cdot\langle \mathsf{R}^{\#}\rangle\cdot\langle \not{\mathsf{R}}, \gamma\rangle\notin\boldsymbol{\Sigma}^x$.

Тогда выполнены все, кроме одного, условия P-неконвергентности трассы $\sigma_2{}^{\#}\cdot\langle \mathsf{R}^{\#}\rangle$ в $\boldsymbol{\Sigma}^x$: $\mathsf{P}\in\mathbf{R}\cup\mathbf{Q}\ \ \&\ \ \sigma_2{}^{\#}\cdot\langle \mathsf{R}^{\#}\rangle\in\boldsymbol{\Sigma}^x\ \ \&$
$\sigma_2{}^{\#}\cdot\langle \mathsf{R}^{\#}\rangle\cdot\langle \not{\mathsf{R}}, \gamma\rangle\notin\boldsymbol{\Sigma}^x\ \ \&\ \ \forall \mathsf{z}\in\mathsf{P}\ \ \sigma_2{}^{\#}\cdot\langle \mathsf{R}^{\#}\rangle\cdot\langle \mathsf{z}\rangle\notin\boldsymbol{\Sigma}^x$.

Не выполнено может быть только условие $\sigma_2^{\#}\cdot\langle R^{\#}\rangle\cdot\langle P^{\#}\rangle\notin\boldsymbol{\Sigma}^{x}$.

Но, поскольку все **L**-трассы в $\boldsymbol{\Sigma}^{x}$ **L**-конвергентны, это условие и не должно быть выполнено: $\sigma_2^{\#}\cdot\langle R^{\#}\rangle\cdot\langle P^{\#}\rangle\in\boldsymbol{\Sigma}^{x}$.

Поскольку $\sigma_1^{\#}\in\boldsymbol{i}^{\nabla}(\sigma_2^{\#})$ влечет $\sigma_1^{\#}\cdot\langle R^{\#}\rangle\cdot\langle P^{\#}\rangle\in\boldsymbol{i}^{\nabla}(\sigma_2^{\#}\cdot\langle R^{\#}\rangle\cdot\langle P^{\#}\rangle)$,

имеем $\sigma_1^{\#}\cdot\langle R^{\#}\rangle\cdot\langle P^{\#}\rangle\in\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{x})$,

что влечет $\sigma_1^{\#}\cdot\langle R^{\#}\rangle\cdot\langle P^{\#}\rangle\in\boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{x}))$,

что влечет $\sigma^{\#}\cdot\langle R^{\#}\rangle\cdot\langle P^{\#}\rangle\in\cup\boldsymbol{d}(\boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{x})))=\mathbf{I}^{\mathbf{R}}$,

что влечет $\sigma^{\#}\cdot\langle P^{\#}\rangle\in\cup\boldsymbol{d}(\boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{x})))=\mathbf{I}^{\mathbf{R}}$, что и требовалось доказать.

5.2.2.2. $\sigma_2^{\#}\cdot\langle R^{\#}\rangle\cdot\langle \not{P}, \gamma\rangle\in\boldsymbol{\Sigma}^{x}$.

Тогда выполнены все три условия необходимости отказа $P^{\#}$ после трассы $\sigma_2^{\#}\cdot\langle R^{\#}\rangle$:

1) $\sigma_2^{\#}\cdot\langle R^{\#}\rangle\cdot\langle \not{P}, \gamma\rangle\in\boldsymbol{\Sigma}^{x}$,

2) $\forall z\in P\ \ \sigma_2^{\#}\cdot\langle R^{\#}\rangle\cdot\langle z\rangle\notin\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{x})$,

3) $\boldsymbol{Ip}(\sigma_2\cdot\langle R\rangle)\neq\varnothing$.

Следовательно, отказ $P^{\#}$ необходим после трассы $\sigma_2^{\#}\cdot\langle R^{\#}\rangle$.

Поэтому условие $\sigma_1^{\#}\cdot\langle R^{\#}\rangle\in\boldsymbol{i}^{\nabla}(\sigma_2^{\#}\cdot\langle R^{\#}\rangle)$

влечет $\sigma_1^{\#}\cdot\langle R^{\#}\rangle\cdot\langle P^{\#}\rangle\in\boldsymbol{i}^{\nabla}(\sigma_2^{\#}\cdot\langle R^{\#}\rangle)$,

что влечет $\sigma_1^{\#}\cdot\langle R^{\#}\rangle\cdot\langle P^{\#}\rangle\in\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{x})$,

что влечет $\sigma_1^{\#}\cdot\langle R^{\#}\rangle\cdot\langle P^{\#}\rangle\in\boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{x}))$,

что влечет $\sigma^{\#}\cdot\langle R^{\#}\rangle\cdot\langle P^{\#}\rangle\in\cup\boldsymbol{d}(\boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{x})))$,

что влечет $\sigma^{\#}\cdot\langle P^{\#}\rangle\in\cup\boldsymbol{d}(\boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{x})))=\mathbf{I}^{\mathbf{R}}$, что и требовалось доказать.

6. Замкнутость.

d-замыкание множества трасс ***d***-замкнуто по определению.

Поэтому множество $\mathbf{I}^{\mathbf{R}}=\cup\boldsymbol{d}(\boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{x})))$ ***d***-замкнуто.

7. Полнота.

Пусть трасса $\mu^{\#}\in\mathbf{I}^{\mathbf{R}}$ заканчивается отказом, то есть $\boldsymbol{Ip}(\mu)\neq\varnothing$, кнопка $P\in\mathbf{R}$, $\forall z\in P\ \ \mu^{\#}\cdot\langle z\rangle\notin\mathbf{I}^{\mathbf{R}}$ и $\mu^{\#}\cdot\lambda^{\#}\in\mathbf{I}^{\mathbf{R}}$.

Нужно доказать, что $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\in\mathbf{I}^{\mathbf{R}}$.

Если $\sigma^{\#}=\mu^{\#}\cdot\lambda^{\#}\in\mathbf{I}^{\mathbf{R}}$, то по лемме 31 (1) найдутся такие трассы $\sigma_1{}^{\#}$ и $\sigma_2{}^{\#}$, что $\sigma_2{}^{\#}\in\boldsymbol{\Sigma}^{\boldsymbol{x}}$, $\sigma_1{}^{\#}\in\boldsymbol{i}^{\nabla}(\sigma_2{}^{\#})$ и $\sigma^{\#}\in\boldsymbol{d}(\sigma_1{}^{\#})$.

Тогда трассу $\sigma_1{}^{\#}$ можно представить в виде $\sigma_1{}^{\#}=\mu_1{}^{\#}\cdot\lambda_1{}^{\#}$, где $\mu^{\#}\in\boldsymbol{d}(\mu_1{}^{\#})$ и $\lambda^{\#}\in\boldsymbol{d}(\lambda_1{}^{\#})$.

Также трассу $\sigma_2{}^{\#}$ можно представить в виде $\sigma_2{}^{\#}=\mu_2{}^{\#}\cdot\lambda_2{}^{\#}$, где $\mu_1{}^{\#}\in\boldsymbol{i}^{\nabla}(\mu_2{}^{\#})$ и $\lambda_1{}^{\#}\in\boldsymbol{i}^{\nabla}(\lambda_2{}^{\#})$.

Поскольку лемме 28 (2) множество $\boldsymbol{\Sigma}^{\boldsymbol{x}}$ префикс-замкнуто, $\sigma_2{}^{\#}\in\boldsymbol{\Sigma}^{\boldsymbol{x}}$ и $\sigma_2{}^{\#}=\mu_2{}^{\#}\cdot\lambda_2{}^{\#}$, имеем $\mu_2{}^{\#}\in\boldsymbol{\Sigma}^{\boldsymbol{x}}$.

Поскольку выполнены условия $\forall z\in P\ \ \mu^{\#}\cdot\langle z\rangle\notin\mathbf{I}^{\mathbf{R}}$, а также $\mu^{\#}\in\boldsymbol{d}(\mu_1{}^{\#})$ и $\mu_1{}^{\#}\in\boldsymbol{i}^{\nabla}(\mu_2{}^{\#})$, по лемме 31 (2) трасса $\mu_2{}^{\#}$ не продолжается действиями $z\in P$ во множестве $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\boldsymbol{x}})$.

Условие $\boldsymbol{Ip}(\mu)\neq\varnothing$ влечет $\boldsymbol{Ip}(\mu_1)\neq\varnothing$, что влечет либо $\boldsymbol{Ip}(\mu_2)\neq\varnothing$, либо $\boldsymbol{Ip}(\mu_2)=\varnothing$. Рассмотрим два этих случая (7.1 и 7.2).

7.1. $\boldsymbol{Ip}(\mu_2)\neq\varnothing$.

Здесь возможны два подслучая (7.1.1 и 7.1.2) в зависимости от того $\mu_2{}^{\#}\cdot\langle\not{\mathrm{P}},\gamma\rangle\notin\boldsymbol{\Sigma}^{\boldsymbol{x}}$ или $\mu_2{}^{\#}\cdot\langle\not{\mathrm{P}},\gamma\rangle\in\boldsymbol{\Sigma}^{\boldsymbol{x}}$.

7.1.1. $\mu_2{}^{\#}\cdot\langle\not{\mathrm{P}},\gamma\rangle\notin\boldsymbol{\Sigma}^{\boldsymbol{x}}$.

В этом случае выполнены все условия того, что отказ $P^{\#}$ является особым отказом после трассы $\mu_2{}^{\#}$.

Поскольку $\mu_2{}^{\#}\cdot\lambda_2{}^{\#}=\sigma_2{}^{\#}\in\boldsymbol{\Sigma}^{\boldsymbol{x}}$, а все трассы множества $\boldsymbol{\Sigma}^{\boldsymbol{x}}$ **L**-полны, должно быть $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_2{}^{\#}\in\boldsymbol{\Sigma}^{\boldsymbol{x}}$.

Мы докажем, что $\mu_1{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_1{}^{\#}\in\boldsymbol{i}^{\nabla}(\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_2{}^{\#})$.

Для этого достаточно доказать, что если трасса $\lambda_2{}^{\#}$ может быть представлена в виде $\lambda_2{}^{\#}=\lambda_{21}{}^{\#}\cdot\lambda_{22}{}^{\#}$ и некоторый $\mathbf{R}^{\#}$-отказ $R^{\#}$ необходим после трассы $\mu_2{}^{\#}\cdot\lambda_{21}{}^{\#}$, то либо в $\boldsymbol{\Sigma}^{\boldsymbol{x}}$ существует трасса $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda_{22}{}^{\#}$, либо отказ $R^{\#}$ необходим после трассы $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}$.

Поскольку отказ $R^{\#}$ необходим после трассы $\mu_2{}^{\#}\cdot\lambda_{21}{}^{\#}$, эта трасса не продолжается действиями из R в $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\boldsymbol{x}})$.

Но тогда трасса $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}$ также не продолжается действиями из R в $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\boldsymbol{x}})$.

Рассмотрим два варианта (7.1.1.1 и 7.1.1.2) в зависимости от того, $\boldsymbol{Ip}(\mu_2\cdot\langle P\rangle\cdot\lambda_{21})\neq\varnothing$ или $\boldsymbol{Ip}(\mu_2\cdot\langle P\rangle\cdot\lambda_{21})=\varnothing$.

7.1.1.1. $\boldsymbol{Ip}(\mu_2\cdot\langle P\rangle\cdot\lambda_{21})\neq\varnothing$.

Здесь возможны два подварианта (7.1.1.1.1 и 7.1.1.1.2) в зависимости от того $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}\cdot\langle \not{R}, \gamma\rangle\notin\boldsymbol{\Sigma}^{x}$ или $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}\cdot\langle \not{R}, \gamma\rangle\in\boldsymbol{\Sigma}^{x}$.

7.1.1.1.1. $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}\cdot\langle \not{R}, \gamma\rangle\notin\boldsymbol{\Sigma}^{x}$.

Тогда выполнены все условия того, что отказ $R^{\#}$ особый после трассы $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}$.

Поскольку $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}\cdot\lambda_{22}{}^{\#}=\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_2{}^{\#}\in\boldsymbol{\Sigma}^{x}$, а все трассы множества $\boldsymbol{\Sigma}^{x}$ **L**-полны, должно быть $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}\cdot\langle R^{\#}\rangle\cdot\lambda_{22}{}^{\#}\in\boldsymbol{\Sigma}^{x}$, что и требовалось доказать.

7.1.1.1.2. $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}\cdot\langle \not{R}, \gamma\rangle\in\boldsymbol{\Sigma}^{x}$.

Тогда выполнены все условия необходимости отказа $R^{\#}$ после трассы $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}$, что и требовалось доказать.

7.1.1.2. $\boldsymbol{Ip}(\mu_2\cdot\langle P\rangle\cdot\lambda_{21})=\varnothing$.

Это условие влечет $\boldsymbol{Ip}(\mu_2\cdot\lambda_{21})=\varnothing$.

Тогда, поскольку отказ $R^{\#}$ необходим после трассы $\mu_2{}^{\#}\cdot\lambda_{21}{}^{\#}$, эта трасса не продолжается никакими отказами в $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{x})$.

Отсюда следует, что трасса $\mu_2\cdot\langle P\rangle\cdot\lambda_{21}$ не продолжается никакими отказами в $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{x})$.

Здесь возможны два подварианта (7.1.1.2.1 и 7.1.1.2.2) в зависимости от того $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}\cdot\langle \not{R}, \gamma\rangle\notin\boldsymbol{\Sigma}^{x}$ или $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}\cdot\langle \not{R}, \gamma\rangle\in\boldsymbol{\Sigma}^{x}$.

7.1.1.2.1. $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}\cdot\langle \not{R}, \gamma\rangle\notin\boldsymbol{\Sigma}^{x}$.

Тогда выполнены все, кроме одного, условия R-неконвергентности трассы $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}$ в $\boldsymbol{\Sigma}^{x}$: $R\in\mathbf{R}\cup\mathbf{Q}$ & $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}\in\boldsymbol{\Sigma}^{x}$ & $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}\cdot\langle \not{R}, \gamma\rangle\notin\boldsymbol{\Sigma}^{x}$ & $\forall z\in R\ \ \mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}\cdot\langle z\rangle\notin\boldsymbol{\Sigma}^{x}$.

Не выполнено может быть только условие $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}\cdot\langle R^{\#}\rangle\notin\boldsymbol{\Sigma}^{x}$.

Но, поскольку все **L**-трассы в $\boldsymbol{\Sigma}^{x}$ **L**-конвергентны, это условие и не должно быть выполнено: $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda_{21}{}^{\#}\cdot\langle R^{\#}\rangle\in\boldsymbol{\Sigma}^{x}$.

Но это противоречит тому, что трасса $\mu_2{\cdot}\langle \mathsf{P}\rangle{\cdot}\lambda_{21}$ не продолжается никакими отказами в $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^x)$.

Следовательно, рассматриваемый подвариант невозможен.

7.1.1.2.2. $\mu_2{}^{\#}{\cdot}\langle \mathsf{P}^{\#}\rangle{\cdot}\lambda_{21}{}^{\#}{\cdot}\langle \not{\mathsf{R}}, \gamma\rangle \in \boldsymbol{\Sigma}^x$.

Тогда выполнены все условия необходимости отказа $\mathsf{R}^{\#}$ после трассы $\mu_2{\cdot}\langle \mathsf{P}\rangle{\cdot}\lambda_{21}$, что и требовалось доказать.

Итак, мы доказали, что $\mu_1{}^{\#}{\cdot}\langle \mathsf{P}^{\#}\rangle{\cdot}\lambda_1{}^{\#} \in \boldsymbol{i}^{\nabla}(\mu_2{}^{\#}{\cdot}\langle \mathsf{P}^{\#}\rangle{\cdot}\lambda_2{}^{\#})$.

Тогда $\mu_1{}^{\#}{\cdot}\langle \mathsf{P}^{\#}\rangle{\cdot}\lambda_1{}^{\#} \in \cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^x)$,

что влечет $\mu_1{}^{\#}{\cdot}\langle \mathsf{P}^{\#}\rangle{\cdot}\lambda_1{}^{\#} \in \boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^x))$,

что влечет $\mu^{\#}{\cdot}\langle \mathsf{P}^{\#}\rangle{\cdot}\lambda^{\#} \in \cup\boldsymbol{d}(\boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^x))) = \mathbf{I}^{\mathbf{R}}$, что и требовалось доказать.

7.1.2. $\mu_2{}^{\#}{\cdot}\langle \not{\mathsf{R}}, \gamma\rangle \in \boldsymbol{\Sigma}^x$.

Тогда выполнены все условия необходимости отказа $\mathsf{P}^{\#}$ после трассы μ_2, что и требовалось доказать.

А тогда условие $\mu_1{}^{\#}{\cdot}\lambda_1{}^{\#} \in \boldsymbol{i}^{\nabla}(\mu_2{}^{\#}{\cdot}\lambda_2{}^{\#})$

влечет $\mu_1{}^{\#}{\cdot}\langle \mathsf{P}^{\#}\rangle{\cdot}\lambda_1{}^{\#} \in \boldsymbol{i}^{\nabla}(\mu_2{}^{\#}{\cdot}\lambda_2{}^{\#})$.

Тогда $\mu_1{}^{\#}{\cdot}\langle \mathsf{P}^{\#}\rangle{\cdot}\lambda_1{}^{\#} \in \cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^x)$,

что влечет $\mu_1{}^{\#}{\cdot}\langle \mathsf{P}^{\#}\rangle{\cdot}\lambda_1{}^{\#} \in \boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^x))$,

что влечет $\mu^{\#}{\cdot}\langle \mathsf{P}^{\#}\rangle{\cdot}\lambda^{\#} \in \cup\boldsymbol{d}(\boldsymbol{l}(\cup\boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^x))) = \mathbf{I}^{\mathbf{R}}$, что и требовалось доказать.

7.2. $\boldsymbol{Ip}(\mu_2) = \varnothing$.

Поскольку $\boldsymbol{Ip}(\mu) \neq \varnothing$ и $\mu^{\#} \in \boldsymbol{d}(\mu_1{}^{\#})$, должно быть $\boldsymbol{Ip}(\mu_1) \neq \varnothing$.

Но тогда отказы в конце трассы $\mu_1{}^{\#}$ вставлены при переходе от $\mu_2{}^{\#}$ к $\mu_1{}^{\#}$, то есть хотя бы один отказ необходим после $\mu_2{}^{\#}$.

Тогда, поскольку $\boldsymbol{Ip}(\mu_2) = \varnothing$, трасса $\mu_2{}^{\#}$ не продолжается в $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^x)$ никакими отказами.

Также повторим, что трасса $\mu_2{}^{\#}$ не продолжается в $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^x)$ действиями из P.

Рассмотрим два подслучая () в зависимости от того $\mu_2^{\#}\cdot\langle \not{\text{P}}, \gamma\rangle \notin \boldsymbol{\Sigma}^{\boldsymbol{x}}$ или $\mu_2^{\#}\cdot\langle \not{\text{P}}, \gamma\rangle \in \boldsymbol{\Sigma}^{\boldsymbol{x}}$.

7.2.1. $\mu_2^{\#}\cdot\langle \not{\text{P}}, \gamma\rangle \notin \boldsymbol{\Sigma}^{\boldsymbol{x}}$.

Поскольку трасса $\mu_2^{\#}$ не продолжается в $\cup \boldsymbol{d}(\boldsymbol{\Sigma}^{\boldsymbol{x}})$ никакими отказами, она не продолжается никакими отказами в $\boldsymbol{\Sigma}^{\boldsymbol{x}}$, в том числе и отказом $\text{P}^{\#}$.

Но тогда выполнены все условия P-неконвергентности трассы $\mu_2^{\#}$ в $\boldsymbol{\Sigma}^{\boldsymbol{x}}$, чего быть не может, поскольку все трассы в в $\boldsymbol{\Sigma}^{\boldsymbol{x}}$ **L**-конвергентны.

Следовательно, этот подслучай невозможен.

7.2.2. $\mu_2^{\#}\cdot\langle \not{\text{P}}, \gamma\rangle \in \boldsymbol{\Sigma}^{\boldsymbol{x}}$.

Тогда выполнены все условия необходимости отказа $\text{P}^{\#}$ после трассы μ_2.

А тогда условие $\mu_1^{\#}\cdot\lambda_1^{\#} \in \boldsymbol{i}^{\nabla}(\mu_2^{\#}\cdot\lambda_2^{\#})$

влечет $\mu_1^{\#}\cdot\langle \text{P}^{\#}\rangle\cdot\lambda_1^{\#} \in \boldsymbol{i}^{\nabla}(\mu_2^{\#}\cdot\lambda_2^{\#})$.

Тогда $\mu_1^{\#}\cdot\langle \text{P}^{\#}\rangle\cdot\lambda_1^{\#} \in \cup \boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{\boldsymbol{x}})$,

что влечет $\mu_1^{\#}\cdot\langle \text{P}^{\#}\rangle\cdot\lambda_1^{\#} \in \boldsymbol{l}(\cup \boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{\boldsymbol{x}}))$,

что влечет $\mu^{\#}\cdot\langle \text{P}^{\#}\rangle\cdot\lambda^{\#} \in \cup \boldsymbol{d}(\boldsymbol{l}(\cup \boldsymbol{i}^{\nabla}(\boldsymbol{\Sigma}^{\boldsymbol{x}}))) = \mathbf{I}^{\mathbf{R}}$, что и требовалось доказать.

Итак, мы доказали, что $\mu^{\#}\cdot\langle \text{P}^{\#}\rangle\cdot\lambda^{\#} \in \mathbf{I}^{\mathbf{R}}$. Тем самым доказано выполнение свойства полноты в $\mathbf{I}^{\mathbf{R}}$.

Лемма доказана.

6.52. Доказательство леммы 33

1. Множество $\mathbf{I}^{\nabla}$ содержит только **L**-трассы по построению: множество $\boldsymbol{\Sigma}^{\boldsymbol{x}}$ содержит **L**-трассы и трассы с не-отказами, операция $\boldsymbol{i}^{\nabla}$ добавляет **L**-трассы и трассы с не-отказами, операция $\boldsymbol{l}$ удаляет трассы с не-отказами, операция $\boldsymbol{d}$, примененная к множеству **L**-трасс, добавляет только **L**-трассы.
2. Множество $\mathbf{I}^{\nabla}$ содержит все **L**-трассы из множества $\boldsymbol{\Sigma}^{\boldsymbol{x}}$ по построению: операция $\boldsymbol{i}^{\nabla}$ не удаляет трассы из $\boldsymbol{\Sigma}^{\boldsymbol{x}}$, операция $\boldsymbol{l}$ удаляет только не **L**-трассы, а операция $\boldsymbol{d}$ не удаляет трассы.
3. Множество $\mathbf{I}^{\nabla}$ является полной трассовой моделью в алфавите $\mathbf{L}^{+}$, поскольку она является расширением до полной трассовой модели множества $\mathbf{I}^{\mathbf{R}}$, которое по лемме 32 является $\mathbf{R}^{\#}$-моделью в алфавите $\mathbf{L}^{+}$.

6.53. Доказательство леммы 34

Пусть трасса $\sigma^{\#}\in\mathbf{I}^{\mathbf{R}}\backslash\mathbf{\Sigma}^{x}$.

Тогда по лемме 31 (1) найдутся такие трассы $\sigma_1{}^{\#}$ и $\sigma_2{}^{\#}$, что $\sigma_2{}^{\#}\in\mathbf{\Sigma}^{x}$, $\sigma_1{}^{\#}\in\boldsymbol{i}^{\nabla}(\sigma_2{}^{\#})$ и $\sigma^{\#}\in\boldsymbol{d}(\sigma_1{}^{\#})$.

Рассмотрим два случая.

1. Все отказы, которые были вставлены при переходе от $\sigma_2{}^{\#}$ к $\sigma_1{}^{\#}$, удалены при переходе от $\sigma_1{}^{\#}$ к $\sigma^{\#}$.

   Тогда $\sigma^{\#}\in\boldsymbol{d}(\sigma_2{}^{\#})$.

   Тогда либо $\sigma^{\#}\in\mathbf{\Sigma}^{\mathbf{01\sim}}$, либо $\sigma^{\#}\notin\mathbf{\Sigma}^{\mathbf{01\sim}}$.

1.1. $\sigma^{\#}\in\mathbf{\Sigma}^{\mathbf{01\sim}}$.

   Тогда по лемме о ***d***-свойстве (лемма 30) $\sigma^{\#}\in\mathbf{\Sigma}^{x}$, что не верно.

   Этого случая быть не может.

1.2. $\sigma^{\#}\notin\mathbf{\Sigma}^{\mathbf{01\sim}}$.

   Поскольку $\sigma_2{}^{\#}\in\mathbf{\Sigma}^{x}$, по лемме 28 (1) имеем $\sigma_2{}^{\#}\in\mathbf{\Sigma}^{\mathbf{01\sim}}$.

   Поскольку $\sigma^{\#}\in\boldsymbol{d}(\sigma_2{}^{\#})$, имеем $\sigma^{\#}\in\cup\boldsymbol{d}(\mathbf{\Sigma}^{\mathbf{01\sim}})$.

   Следовательно, $\sigma^{\#}\in\cup\boldsymbol{d}(\mathbf{\Sigma}^{\mathbf{01\sim}})\backslash\mathbf{\Sigma}^{\mathbf{01\sim}}$.

   По теореме 11 все трассы из $\cup\boldsymbol{d}(\mathbf{\Sigma}^{\mathbf{01\sim}})\backslash\mathbf{\Sigma}^{\mathbf{01\sim}}$ являются опасными трассами ~пополнения.

   Следовательно, трасса $\sigma^{\#}$ имеет префикс $\mu^{\#}\cdot\langle u^{\#}\rangle$, где трасса $\mu^{\#}$ безопасна в ~пополнении, а наблюдение $u^{\#}$ опасно в ~пополнении после трассы $\mu^{\#}$, что и требовалось доказать.

2. Трасса $\sigma^{\#}$ содержит отказ, вставленный при переходе от $\sigma_2{}^{\#}$ к $\sigma_1{}^{\#}$.

   Выберем первый такой отказ $P^{\#}\in\mathbf{R}^{\#}$.

   Тогда у трасс $\sigma^{\#}$, $\sigma_1{}^{\#}$ и $\sigma_2{}^{\#}$ есть префиксы $\mu^{\#}\cdot\langle P^{\#}\rangle\le\sigma^{\#}$, $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\le\sigma_1{}^{\#}$ и $\mu_2{}^{\#}\le\sigma_2{}^{\#}$ такие, что $\mu_2{}^{\#}\in\mathbf{\Sigma}^{x}$, $\mu_2{}^{\#}\cdot\langle P^{\#}\rangle\in\boldsymbol{i}^{\nabla}(\mu_2{}^{\#})$ и $\mu^{\#}\cdot\langle P^{\#}\rangle\in\boldsymbol{d}(\mu_2{}^{\#}\cdot\langle P^{\#}\rangle)$, и отказ $P^{\#}$ необходим после трассы $\mu_2{}^{\#}$.

   Условие $\mu^{\#}\cdot\langle P^{\#}\rangle\in\boldsymbol{d}(\mu_2{}^{\#}\cdot\langle P^{\#}\rangle)$ влечет $\mu^{\#}\in\boldsymbol{d}(\mu_2{}^{\#})$.

   Тогда по первому из условий необходимости отказа $\mu_2{}^{\#}\cdot\langle \text{P}, \gamma\rangle\in\mathbf{\Sigma}^{x}$.

   Тогда $\mu_2{}^{\#}\cdot\langle \text{P}, \gamma\rangle\in\mathbf{\Sigma}^{\mathbf{01\sim}}$ по лемме 28 (1),

   что по теореме 10 (безопасность кнопок в ~финальных трассах) влечет $P^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{\Sigma}^{\sim}$ ***after*** $\mu_2{}^{\#}$.

Поскольку $\mu_2^{\#} \in \boldsymbol{\Sigma}^{\mathbf{0}\sim}$ и $\mu^{\#} \in \boldsymbol{d}(\mu_2^{\#})$, по лемме 16 (безопасность после отказа в ~финальных трассах) $P^{\#}$ ***safe***$_{\gamma\Delta}$ $\boldsymbol{\Sigma}^{\sim}$ ***after*** $\mu^{\#}$.

Далее либо $\mu^{\#} \in \boldsymbol{\Sigma}^{\mathbf{01}\sim}$, либо $\mu^{\#} \notin \boldsymbol{\Sigma}^{\mathbf{01}\sim}$.

2.1. $\mu^{\#} \in \boldsymbol{\Sigma}^{\mathbf{01}\sim}$.

По теореме 11 $\boldsymbol{SafeBy}(\mathbf{T}^{\sim},\mathbf{L}) = \boldsymbol{\Sigma}^{\mathbf{0}\sim}$, следовательно, трасса $\mu^{\#}$ безопасна в ~пополнении.

Поскольку также $\mu^{\#} \cdot \langle P^{\#} \rangle \le \sigma^{\#}$ и $P^{\#}$ ***safe***$_{\gamma\Delta}$ $\boldsymbol{\Sigma}^{\sim}$ ***after*** $\mu^{\#}$, трасса $\sigma^{\#}$ имеет префикс $\mu^{\#} \cdot \langle P^{\#} \rangle$, где трасса $\mu^{\#}$ безопасна в ~пополнении, а наблюдение $P^{\#}$ опасно в ~пополнении после трассы $\mu^{\#}$, что и требовалось доказать.

2.2. $\mu^{\#} \notin \boldsymbol{\Sigma}^{\mathbf{01}\sim}$.

Поскольку $\mu_2^{\#} \in \boldsymbol{\Sigma}^{x}$, по лемме 28 (1) имеем $\mu_2^{\#} \in \boldsymbol{\Sigma}^{\mathbf{01}\sim}$.

Поскольку $\mu^{\#} \in \boldsymbol{d}(\mu_2^{\#})$, имеем $\mu^{\#} \in \cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})$.

Следовательно, $\mu^{\#} \in \cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}\sim}) \setminus \boldsymbol{\Sigma}^{\mathbf{01}\sim}$.

По теореме 11 все трассы из $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}\sim}) \setminus \boldsymbol{\Sigma}^{\mathbf{01}\sim}$ являются опасными трассами ~пополнения.

Следовательно, трасса $\mu^{\#}$ имеет префикс $\kappa^{\#} \cdot \langle u^{\#} \rangle$, где трасса $\kappa^{\#}$ безопасна в ~пополнении, а наблюдение $u^{\#}$ опасно в ~пополнении после трассы $\kappa^{\#}$.

Поскольку $\mu^{\#} \cdot \langle P^{\#} \rangle \le \sigma^{\#}$, а $\kappa^{\#} \cdot \langle u^{\#} \rangle \le \mu^{\#}$, трасса $\kappa^{\#} \cdot \langle u^{\#} \rangle$ является также префиксом трассы $\sigma^{\#}$, что и требовалось доказать.

6.54. Доказательство леммы 35

По лемме 32 трассы множества $\mathbf{I}^{\mathbf{R}}$ не содержат дивергенции и разрушения.

Тогда трассы множества $\mathbf{I}^{\nabla} = \boldsymbol{Ext}(\mathbf{I}^{\mathbf{R}})$ также не содержат дивергенции и разрушения.

Следовательно, гипотеза о безопасности может быть нарушена только из-за ненаблюдаемых отказов.

Пусть $\mathbf{R}^{\#}$-трасса $\sigma^{\#}$ безопасна в спецификации $\boldsymbol{\Sigma}^{\sim}$, имеется в реализации $\mathbf{I}^{\nabla}$, а отказ $Q^{\#} \in \mathbf{Q}^{\#}$ безопасен после $\sigma^{\#}$ в $\boldsymbol{\Sigma}^{\sim}$.

Нам нужно доказать, что $Q^{\#}$ ***safe in*** $\mathbf{I}^{\nabla}$ ***after*** $\sigma^{\#}$.

Условия $\sigma^{\#} \in \boldsymbol{SafeBy}(\mathbf{T}^{\sim},\mathbf{L})$ и $\sigma^{\#} \in \mathbf{I}^{\nabla}$ влекут по лемме 34 $\sigma^{\#} \in \boldsymbol{\Sigma}^{x}$.

Тогда по лемме 28 (1) $\sigma^{\#} \in \boldsymbol{\Sigma}^{\mathbf{01}\sim}$.

Поэтому по теореме 10 (безопасность кнопок в ~финальных трассах) условие $Q^{\#}$ ***safe***$_{\gamma\Delta}$ $\boldsymbol{\Sigma}^{\sim}$ ***after*** $\sigma^{\#}$ влечет $\sigma^{\#} \cdot \langle \cancel{\theta}, \gamma \rangle \notin \boldsymbol{\Sigma}^{\mathbf{01}\sim}$,

что по лемме 28 (1) влечет $\sigma^{\#} \cdot \langle \cancel{\theta}, \gamma \rangle \notin \boldsymbol{\Sigma}^{x}$.

Все трассы в $\mathbf{\Sigma}^{x}$ **L**-конвергентны.

Поскольку $\sigma^{\#}\in\mathbf{\Sigma}^{x}$, она **L**-конвергентна и, следовательно, Q-конвергентна.

А тогда, поскольку $\sigma^{\#}\cdot\langle \mathbf{\Theta}, \gamma\rangle\notin\mathbf{\Sigma}^{x}$, должно найтись такое наблюдение $u\in Q\cup\{Q^{\#}\}$, что $\sigma^{\#}\cdot\langle u\rangle\in\mathbf{\Sigma}^{x}$.

По правилам вывода ~финальных трасс в этих трассах нет $\mathbf{Q}^{\#}$-отказов, следовательно, их нет в трассах из $\mathbf{\Sigma}^{x}$, поскольку $\mathbf{\Sigma}^{x}\subseteq\mathbf{\Sigma}^{01\sim}$ по лемме 28 (1).

Следовательно, $u\in Q$.

Но тогда $\sigma^{\#}\cdot\langle u\rangle\in\mathbf{I}^{\nabla}$, что влечет $Q^{\#}$ ***safe in*** $\mathbf{I}^{\nabla}$ ***after*** $\sigma^{\#}$, что и требовалось доказать.

6.55. Доказательство леммы 36

По лемме 35 $\mathbf{I}^{\nabla}$ ***safe for*** $\mathbf{\Sigma}^{\sim}$. Докажем, что $\mathbf{I}^{\nabla}$ ***saco*** $\mathbf{\Sigma}^{\sim}$.

Пусть трасса $\sigma^{\#}$ безопасна в $\mathbf{\Sigma}^{\sim}$, наблюдение u безопасно в $\mathbf{\Sigma}^{\sim}$ после трассы $\sigma^{\#}$, и трасса $\sigma^{\#}\cdot\langle u\rangle\in\mathbf{I}^{\nabla}$.

Тогда по лемме 34 $\sigma^{\#}\cdot\langle u\rangle\in\mathbf{\Sigma}^{x}$,

что по лемме 28 (1) влечет $\sigma^{\#}\cdot\langle u\rangle\in\mathbf{\Sigma}^{01\sim}$,

что влечет $\sigma^{\#}\cdot\langle u\rangle\in\mathbf{\Sigma}^{\sim}$, что и требовалось доказать.

6.56. Доказательство леммы 37

По лемме 33 множество $\mathbf{I}^{\nabla}$ является **L**-реализацией, содержащей все **L**-трассы из множества $\mathbf{\Sigma}^{x}$.

По лемме 36 эта реализация конформна.

Следовательно, все ее трассы **L**-конформны, в том числе все **L**-трассы из множества $\mathbf{\Sigma}^{x}$, то есть трассы из множества $\mathbf{\Sigma}^{x}\cap\mathbf{\Sigma}^{0\sim}$.

6.57. Доказательство леммы 38

Утверждение леммы непосредственно следует из правил вывода.

6.58. Доказательство теоремы 20

1. Покажем, что $\mathbf{\Sigma}^{x}\cap\mathbf{\Sigma}^{0\sim}=\mathbf{\Sigma}^{0\nabla}$.

   По теореме 11 $\mathbf{SafeBy}(\mathbf{T}^{\sim},\mathbf{L})=\mathbf{\Sigma}^{0\sim}$,

   а по определению $\mathbf{conf}(\mathbf{T_i},\mathbf{L})$ имеем $\mathbf{conf}(\mathbf{T_i},\mathbf{L})\subseteq\mathbf{SafeBy}(\mathbf{T}^{\sim},\mathbf{L})$.

   Следовательно, $\mathbf{conf}(\mathbf{T_i},\mathbf{L})\subseteq\mathbf{\Sigma}^{0\sim}$.

Отсюда по лемме 29 $\boldsymbol{conf}(\mathbf{T}^{\sim},\mathbf{L})\subseteq\boldsymbol{\Sigma}^{\mathbf{0}\sim}\setminus\boldsymbol{x}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})$.

Поскольку $\boldsymbol{\Sigma}^{x}=\boldsymbol{\Sigma}^{\mathbf{01}\sim}\setminus\boldsymbol{x}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})$, имеем $\boldsymbol{\Sigma}^{x}\cap\boldsymbol{\Sigma}^{\mathbf{0}\sim}=\boldsymbol{\Sigma}^{\mathbf{0}\sim}\setminus\boldsymbol{x}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})$,

тем самым, $\boldsymbol{conf}(\mathbf{T}^{\sim},\mathbf{L})\subseteq\boldsymbol{\Sigma}^{x}\cap\boldsymbol{\Sigma}^{\mathbf{0}\sim}$.

По лемме 37 $\boldsymbol{\Sigma}^{x}\cap\boldsymbol{\Sigma}^{\mathbf{0}\sim}\subseteq\boldsymbol{conf}(\mathbf{T}^{\sim},\mathbf{L})$.

Тем самым, $\boldsymbol{\Sigma}^{x}\cap\boldsymbol{\Sigma}^{\mathbf{0}\sim}=\boldsymbol{conf}(\mathbf{T}^{\sim},\mathbf{L})$.

По определению $\boldsymbol{\Sigma}^{\mathbf{0}\nabla}=\boldsymbol{conf}(\mathbf{T}^{\sim},\mathbf{L})$.

Следовательно, $\boldsymbol{\Sigma}^{x}\cap\boldsymbol{\Sigma}^{\mathbf{0}\sim}=\boldsymbol{\Sigma}^{\mathbf{0}\nabla}$.

2. Покажем, что $\boldsymbol{\Sigma}^{x}\cap\boldsymbol{\Sigma}^{\mathbf{1}\sim}=\boldsymbol{\Sigma}^{\mathbf{1}\nabla}$.

Поскольку $\boldsymbol{\Sigma}^{x}\neq\varnothing$, должно быть $\langle\gamma\rangle\notin\boldsymbol{\Sigma}$.

А тогда по определению ∇-финальных трасс

$\boldsymbol{\Sigma}^{\mathbf{1}\nabla}=\{\sigma\cdot\langle\text{Ⓟ}\rangle\cdot\lambda\in\boldsymbol{\Sigma}^{\mathbf{1}\sim}\mid\sigma\in\boldsymbol{\Sigma}^{\mathbf{0}\nabla}\ \&\ \mathsf{P}\in\mathbf{R}\cup\mathbf{Q}\}$.

Далее $\boldsymbol{\Sigma}^{x}\cap\boldsymbol{\Sigma}^{\mathbf{1}\sim}=(\boldsymbol{\Sigma}^{\mathbf{01}\sim}\setminus\boldsymbol{x}(\boldsymbol{\Sigma}^{\mathbf{01}\sim}))\cap\boldsymbol{\Sigma}^{\mathbf{1}\sim}$.

Отсюда по лемме 38 $\boldsymbol{\Sigma}^{x}\cap\boldsymbol{\Sigma}^{\mathbf{1}\sim}=\{\sigma\cdot\langle\text{Ⓟ}\rangle\cdot\lambda\in\boldsymbol{\Sigma}^{\mathbf{1}\sim}\mid\sigma\in\boldsymbol{\Sigma}^{x}\cap\boldsymbol{\Sigma}^{\mathbf{0}\sim}\ \&\ \mathsf{P}\in\mathbf{R}\cup\mathbf{Q}\}$.

Поскольку по доказанному $\boldsymbol{\Sigma}^{x}\cap\boldsymbol{\Sigma}^{\mathbf{0}\sim}=\boldsymbol{\Sigma}^{\mathbf{0}\nabla}$, имеем $\boldsymbol{\Sigma}^{x}\cap\boldsymbol{\Sigma}^{\mathbf{1}\sim}=\boldsymbol{\Sigma}^{\mathbf{1}\nabla}$.

3. Покажем, что $\boldsymbol{\Sigma}^{x}=\boldsymbol{\Sigma}^{\mathbf{01}\nabla}$.

Имеем $\boldsymbol{\Sigma}^{x}\subseteq\boldsymbol{\Sigma}^{\mathbf{01}\sim}$ по лемме 28 (1).

А тогда, поскольку $\boldsymbol{\Sigma}^{\mathbf{01}\nabla}=\boldsymbol{\Sigma}^{\mathbf{0}\nabla}\cup\boldsymbol{\Sigma}^{\mathbf{1}\nabla}$, а по доказанному $\boldsymbol{\Sigma}^{x}\cap\boldsymbol{\Sigma}^{\mathbf{0}\sim}=\boldsymbol{\Sigma}^{\mathbf{0}\nabla}$ и $\boldsymbol{\Sigma}^{x}\cap\boldsymbol{\Sigma}^{\mathbf{1}\sim}=\boldsymbol{\Sigma}^{\mathbf{1}\nabla}$, имеем $\boldsymbol{\Sigma}^{x}=\boldsymbol{\Sigma}^{\mathbf{01}\nabla}$.

6.59. Доказательство леммы 39

1. Сначала докажем, что $\boldsymbol{x}_{\alpha}(\mathbf{N}\setminus\mathsf{X})\subseteq\boldsymbol{x}(\mathbf{N})\setminus\mathsf{X}$, используя трансфинитную индукцию.

1.1. Для ординала $\alpha=0$ утверждение верно, так как $\boldsymbol{x}_{0}(\mathbf{N}\setminus\mathsf{X})=\varnothing\subseteq\boldsymbol{x}(\mathbf{N})\setminus\mathsf{X}$.

1.2. Пусть утверждение верно для всех ординалов $\beta<\alpha$ и докажем его для ординала α.

1.2.1. Сначала докажем утверждение для предельного ординала α.

По определению $\boldsymbol{x}_{\alpha}(\mathbf{N}\setminus\mathsf{X})=\cup\{\boldsymbol{x}_{\beta}(\mathbf{N}\setminus\mathsf{X})\mid\beta<\alpha\}$.

Поскольку для $\beta<\alpha$ по предположению шага индукции, $\boldsymbol{x}_{\beta}(\mathbf{N}\setminus\mathsf{X})\subseteq\boldsymbol{x}(\mathbf{N})\setminus\mathsf{X}$,

имеем:

$\boldsymbol{x}_{\alpha}(\mathbf{N}\setminus\mathsf{X})$

$=\ \cup\{\boldsymbol{x}_{\beta}(\mathbf{N}\setminus\mathsf{X})\mid\beta<\alpha\}$

$\subseteq\ \cup\{\boldsymbol{x}(\mathbf{N})\setminus\mathsf{X}\mid\beta<\alpha\}$

$=\boldsymbol{x}(\mathbf{N})\setminus\mathsf{X}$.

1.2.2. Докажем утверждение для непредельного ординала α.

Пусть трасса $\sigma\in\boldsymbol{x}_\alpha(\mathbf{N}\backslash X)$.

Нам надо показать, что $\sigma\in\boldsymbol{x}(\mathbf{N})\backslash X$.

Возможны три варианта в зависимости от того, по какому правилу вывода трасса σ попала во множество $\boldsymbol{x}_\alpha(\mathbf{N}\backslash X)$.

1.2.2.1. Правило вывода **1**.

Условие этого правила: $\sigma\in\boldsymbol{x}_{\alpha-1}(\mathbf{N}\backslash X)$.

Тогда по предположению шага индукции $\sigma\in\boldsymbol{x}(\mathbf{N})\backslash X$.

1.2.2.2. Правило вывода **2** для P-неконвергентной трассы: $\sigma=\mu^{\#}\cdot\kappa$.

Условие этого правила:

$\mu^{\#}\cdot\kappa\in(\mathbf{N}\backslash X)\backslash\boldsymbol{x}_{\alpha-1}(\mathbf{N}\backslash X)$ & $P\in\mathbf{R}\cup\mathbf{Q}$ & $\mu^{\#}\cdot\langle\not{\mathrm{R}},\gamma\rangle\notin(\mathbf{N}\backslash X)\backslash\boldsymbol{x}_{\alpha-1}(\mathbf{N}\backslash X)$

& $\forall z\in P\cup\{P^{\#}\}$ $\mu^{\#}\cdot\langle z\rangle\notin(\mathbf{N}\backslash X)\backslash\boldsymbol{x}_{\alpha-1}(\mathbf{N}\backslash X)$.

Допустим, утверждение леммы не верно, то есть $\mu^{\#}\cdot\kappa\notin\boldsymbol{x}(\mathbf{N})$.

1.2.2.2.1. Если $\mu^{\#}\cdot\kappa\in(\mathbf{N}\backslash X)\backslash\boldsymbol{x}_{\alpha-1}(\mathbf{N}\backslash X)$, то $\mu^{\#}\cdot\kappa\in\mathbf{N}$.

Тогда $\mu^{\#}\cdot\kappa\in\mathbf{N}\backslash\boldsymbol{x}(\mathbf{N})$.

1.2.2.2.2. Если $\mu^{\#}\cdot\langle\not{\mathrm{R}},\gamma\rangle\notin(\mathbf{N}\backslash X)\backslash\boldsymbol{x}_{\alpha-1}(\mathbf{N}\backslash X)$, то возможны три варианта:

1.2.2.2.2.1. $\mu^{\#}\cdot\langle\not{\mathrm{R}},\gamma\rangle\notin\mathbf{N}$.

Тогда $\mu^{\#}\cdot\langle\not{\mathrm{R}},\gamma\rangle\notin\mathbf{N}\backslash\boldsymbol{x}(\mathbf{N})$.

1.2.2.2.2.2. $\mu^{\#}\cdot\langle\not{\mathrm{R}},\gamma\rangle\in X$.

Тогда, поскольку $X\subseteq\boldsymbol{x}(\mathbf{N})$, $\mu^{\#}\cdot\langle\not{\mathrm{R}},\gamma\rangle\notin\mathbf{N}\backslash\boldsymbol{x}(\mathbf{N})$.

1.2.2.2.2.3. $\mu^{\#}\cdot\langle\not{\mathrm{R}},\gamma\rangle\in\boldsymbol{x}_{\alpha-1}(\mathbf{N}\backslash X)$.

Тогда по предположению шага индукции $\mu^{\#}\cdot\langle\not{\mathrm{R}},\gamma\rangle\in\boldsymbol{x}(\mathbf{N})\backslash X$.

Тогда $\mu^{\#}\cdot\langle\not{\mathrm{R}},\gamma\rangle\in\boldsymbol{x}(\mathbf{N})$.

Тогда $\mu^{\#}\cdot\langle\not{\mathrm{R}},\gamma\rangle\notin\mathbf{N}\backslash\boldsymbol{x}(\mathbf{N})$.

1.2.2.2.3. Если $\mu^{\#}\cdot\langle z\rangle\notin(\mathbf{N}\backslash X)\backslash\boldsymbol{x}_{\alpha-1}(\mathbf{N}\backslash X)$ для произвольного $z\in P$, то возможны три варианта:

1.2.2.2.3.1. $\mu^{\#}\cdot\langle z\rangle\notin\mathbf{N}$.

Тогда $\mu^{\#}\cdot\langle z\rangle\notin\mathbf{N}\backslash\boldsymbol{x}(\mathbf{N})$.

1.2.2.2.3.1.1 $\mu^{\#}\cdot\langle z\rangle\in X$.

Тогда, поскольку $X\subseteq \boldsymbol{x}(\mathbf{N})$, $\mu^{\#}\cdot\langle z\rangle\notin \mathbf{N}\setminus\boldsymbol{x}(\mathbf{N})$.

1.2.2.2.3.1.2 $\mu^{\#}\cdot\langle z\rangle\in \boldsymbol{x}_{\alpha-1}(\mathbf{N}\setminus X)$.

Тогда по предположению шага индукции $\mu^{\#}\cdot\langle z\rangle\in \boldsymbol{x}(\mathbf{N})\setminus X$.

Тогда $\mu^{\#}\cdot\langle z\rangle\in \boldsymbol{x}(\mathbf{N})$.

Тогда $\mu^{\#}\cdot\langle z\rangle\notin \mathbf{N}\setminus\boldsymbol{x}(\mathbf{N})$.

Итак, мы имеем:

$P\in\mathbf{R}\cup\mathbf{Q}$ & $\mu^{\#}\cdot\kappa\in\mathbf{N}\setminus\boldsymbol{x}(\mathbf{N})$ & $\mu^{\#}\cdot\langle \text{Р}\!\!\!/, \gamma\rangle\notin\mathbf{N}\setminus\boldsymbol{x}(\mathbf{N})$

& $\forall z\in P\cup\{P^{\#}\}\ \mu^{\#}\cdot\langle z\rangle\notin\mathbf{N}\setminus\boldsymbol{x}(\mathbf{N})$.

По определению $\boldsymbol{x}(\mathbf{N})$ существует такой ординал β, что $\boldsymbol{x}(\mathbf{N})=\boldsymbol{x}_{\beta}(\mathbf{N})$ и $\boldsymbol{x}_{\beta}(\mathbf{N})=\boldsymbol{x}_{\beta+1}(\mathbf{N})$.

Следовательно:

$P\in\mathbf{R}\cup\mathbf{Q}$ & $\mu^{\#}\cdot\kappa\in\mathbf{N}\setminus\boldsymbol{x}_{\beta}(\mathbf{N})$ & $\mu^{\#}\cdot\langle \text{Р}\!\!\!/, \gamma\rangle\notin\mathbf{N}\setminus\boldsymbol{x}_{\beta}(\mathbf{N})$

& $\forall z\in P\cup\{P^{\#}\}\ \mu^{\#}\cdot\langle z\rangle\notin\mathbf{N}\setminus\boldsymbol{x}_{\beta}(\mathbf{N})$.

Но тогда $\mu^{\#}\cdot\kappa\notin\boldsymbol{x}_{\beta}(\mathbf{N})$ и по правилу вывода **2** $\mu^{\#}\cdot\kappa\in\boldsymbol{x}_{\beta+1}(\mathbf{N})$.

Но это противоречит равенству $\boldsymbol{x}_{\beta}(\mathbf{N})=\boldsymbol{x}_{\beta+1}(\mathbf{N})$.

Следовательно, наше допущение не верно, и $\mu^{\#}\cdot\kappa\in\boldsymbol{x}(\mathbf{N})$, что и требовалось доказать.

1.2.2.3. Правило вывода **3** для P-неполной трассы после $\mu^{\#}$: $\sigma=\mu^{\#}\cdot\lambda^{\#}\cdot\kappa$.

Условие этого правила для (особого) отказа $P^{\#}$:

$P\in\mathbf{R}$ & $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in(\mathbf{N}\setminus X)\setminus\boldsymbol{x}_{\alpha-1}(\mathbf{N}\setminus X)$ & $\boldsymbol{Ip}(\mu)\neq\varnothing$

& $\mu^{\#}\cdot\langle \text{Р}\!\!\!/, \gamma\rangle\notin(\mathbf{N}\setminus X)\setminus\boldsymbol{x}_{\alpha-1}(\mathbf{N}\setminus X)$ & $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin(\mathbf{N}\setminus X)\setminus\boldsymbol{x}_{\alpha-1}(\mathbf{N}\setminus X)$

& $\forall z\in P$ $\mu^{\#}\cdot\langle z\rangle\notin(\mathbf{N}\setminus X)\setminus\boldsymbol{x}_{\alpha-1}(\mathbf{N}\setminus X)$.

Допустим, утверждение леммы не верно, то есть $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\notin\boldsymbol{x}(\mathbf{N})$.

1.2.2.3.1. Если $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in(\mathbf{N}\setminus X)\setminus\boldsymbol{x}_{\alpha-1}(\mathbf{N}\setminus X)$, то $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in\mathbf{N}$.

Тогда $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in\mathbf{N}\setminus\boldsymbol{x}(\mathbf{N})$.

1.2.2.3.2. Аналогично 1.2.2.2.2 $\mu^{\#}\cdot\langle \text{Р}\!\!\!/, \gamma\rangle\notin\mathbf{N}\setminus\boldsymbol{x}(\mathbf{N})$.

1.2.2.3.3. Аналогично 1.2.2.2.3: $\forall z\in P$ $\mu^{\#}\cdot\langle z\rangle\notin\mathbf{N}\setminus\boldsymbol{x}(\mathbf{N})$.

1.2.2.3.4. Если $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin(\mathbf{N}\setminus X)\setminus\boldsymbol{x}_{\alpha-1}(\mathbf{N}\setminus X)$, то возможны три варианта:

1.2.2.3.4.1. $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin\mathbf{N}$.

Тогда $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin\mathbf{N}\setminus\boldsymbol{x}(\mathbf{N})$.

1.2.2.3.4.2. $\mu^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\cdot\lambda^{\#}\in \mathsf{X}$.

Тогда, поскольку $\mathsf{X}\subseteq \boldsymbol{x}(\mathbf{N})$, $\mu^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\cdot\lambda^{\#}\notin \mathbf{N}\backslash\boldsymbol{x}(\mathbf{N})$.

1.2.2.3.4.3. $\mu^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\cdot\lambda^{\#}\in \boldsymbol{x}_{\alpha-1}(\mathbf{N}\backslash\mathsf{X})$.

Тогда по предположению шага индукции $\mu^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\cdot\lambda^{\#}\in \boldsymbol{x}(\mathbf{N})\backslash\mathsf{X}$.

Тогда $\mu^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\cdot\lambda^{\#}\in \boldsymbol{x}(\mathbf{N})$. Тогда $\mu^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\cdot\lambda^{\#}\notin \mathbf{N}\backslash\boldsymbol{x}(\mathbf{N})$.

Итак, мы имеем:

$\mathsf{P}\in\mathbf{R}$ & $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in\mathbf{N}\backslash\boldsymbol{x}(\mathbf{N})$ & $\boldsymbol{Ip}(\mu)\neq\varnothing$

& $\mu^{\#}\cdot\langle \mathsf{P}, \gamma\rangle\notin\mathbf{N}\backslash\boldsymbol{x}(\mathbf{N})$ & $\mu^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\cdot\lambda^{\#}\notin\mathbf{N}\backslash\boldsymbol{x}(\mathbf{N})$

& $\forall \mathsf{z}\in\mathsf{P}$ $\mu^{\#}\cdot\langle \mathsf{z}\rangle\notin\mathbf{N}\backslash\boldsymbol{x}(\mathbf{N})$.

По определению $\boldsymbol{x}(\mathbf{N})$ существует такой ординал φ, что $\boldsymbol{x}(\mathbf{N})=\boldsymbol{x}_{\varphi}(\mathbf{N})$ и $\boldsymbol{x}_{\varphi}(\mathbf{N})=\boldsymbol{x}_{\varphi+1}(\mathbf{N})$.

Следовательно:

$\mathsf{P}\in\mathbf{R}$ & $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in\mathbf{N}\backslash\boldsymbol{x}_{\varphi}(\mathbf{N})$ & $\boldsymbol{Ip}(\mu)\neq\varnothing$

& $\mu^{\#}\cdot\langle \mathsf{P}, \gamma\rangle\notin\mathbf{N}\backslash\boldsymbol{x}_{\varphi}(\mathbf{N})$ & $\mu^{\#}\cdot\langle \mathsf{P}^{\#}\rangle\cdot\lambda^{\#}\notin\mathbf{N}\backslash\boldsymbol{x}_{\varphi}(\mathbf{N})$

& $\forall \mathsf{z}\in\mathsf{P}$ $\mu^{\#}\cdot\langle \mathsf{z}\rangle\notin\mathbf{N}\backslash\boldsymbol{x}_{\varphi}(\mathbf{N})$.

Но тогда $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\notin\boldsymbol{x}_{\varphi}(\mathbf{N})$ и по правилу вывода **3** $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in\boldsymbol{x}_{\varphi+1}(\mathbf{N})$.

Но это противоречит равенству $\boldsymbol{x}_{\varphi}(\mathbf{N})=\boldsymbol{x}_{\varphi+1}(\mathbf{N})$.

Следовательно, наше допущение не верно, и $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in\boldsymbol{x}(\mathbf{N})$, что и требовалось доказать.

Шаг индукции для непредельного ординала доказан.

Шаг индукции доказан.

Вложенность $\boldsymbol{x}_{\alpha}(\mathbf{N}\backslash\mathsf{X})\subseteq\boldsymbol{x}(\mathbf{N})\backslash\mathsf{X}$ доказана.

2. Теперь докажем, что $\boldsymbol{x}(\mathbf{N}\backslash\mathsf{X})\supseteq\boldsymbol{x}_{\alpha}(\mathbf{N})\backslash\mathsf{X}$, используя трансфинитную индукцию.

2.1. Для ординала $\alpha=0$ утверждение верно,
так как $\boldsymbol{x}_{0}(\mathbf{N})\backslash\mathsf{X}=\varnothing\backslash\mathsf{X}=\varnothing\subseteq\boldsymbol{x}(\mathbf{N}\backslash\mathsf{X})$.

2.2. Пусть утверждение верно для всех ординалов $\beta<\alpha$ и докажем его для ординала α.

2.2.1. Сначала докажем утверждение для предельного ординала α.
По определению $\boldsymbol{x}_{\alpha}(\mathbf{N})=\cup\{\boldsymbol{x}_{\beta}(\mathbf{N})\mid\beta<\alpha\}$.

Поскольку для $\beta<\alpha$ по предположению шага индукции, $\boldsymbol{x}(\mathbf{N}\backslash X)\supseteq\boldsymbol{x}_\beta(\mathbf{N})\backslash X$,

имеем:

$\boldsymbol{x}_\alpha(\mathbf{N})\backslash X$

$= \cup\{\boldsymbol{x}_\beta(\mathbf{N})\,|\,\beta<\alpha\}\backslash X$

$= \cup\{\boldsymbol{x}_\beta(\mathbf{N})\backslash X\,|\,\beta<\alpha\}$

$\subseteq \cup\{\boldsymbol{x}(\mathbf{N}\backslash X)\,|\,\beta<\alpha\} = \boldsymbol{x}(\mathbf{N}\backslash X)$.

2.2.2. Докажем утверждение для непредельного ординала α.

Пусть трасса $\sigma\in\boldsymbol{x}_\alpha(\mathbf{N})\backslash X$.

Нам надо показать, что $\sigma\in\boldsymbol{x}(\mathbf{N}\backslash X)$.

Возможны три варианта в зависимости от того, по какому правилу вывода трасса σ попала во множество $\boldsymbol{x}_\alpha(\mathbf{N})$.

2.2.2.1. Правило вывода **1**: $\sigma=\mu$.

Условие этого правила: $\mu\in\boldsymbol{x}_{\alpha-1}(\mathbf{N})$.

Тогда по предположению шага индукции $\mu\in\boldsymbol{x}(\mathbf{N}\backslash X)$.

2.2.2.2. Правило вывода **2** для P-неконвергентной трассы: $\sigma=\mu^{\#}\cdot\kappa$.

Условие этого правила: $\mu^{\#}\cdot\kappa\in\mathbf{N}\backslash\boldsymbol{x}_{\alpha-1}(\mathbf{N})$ & $\mu^{\#}\cdot\langle\text{Р},\gamma\rangle\notin\mathbf{N}\backslash\boldsymbol{x}_{\alpha-1}(\mathbf{N})$ & $\forall z\in P\cup\{P^{\#}\}\ \mu^{\#}\cdot\langle z\rangle\notin\mathbf{N}\backslash\boldsymbol{x}_{\alpha-1}(\mathbf{N})$.

Допустим, утверждение леммы не верно, то есть $\mu^{\#}\cdot\kappa\notin\boldsymbol{x}(\mathbf{N}\backslash X)$.

2.2.2.2.1. Если $\mu^{\#}\cdot\kappa\in\mathbf{N}\backslash\boldsymbol{x}_{\alpha-1}(\mathbf{N})$, то $\mu^{\#}\cdot\kappa\in\mathbf{N}$.

Поскольку $\mu^{\#}\cdot\kappa=\sigma\in\boldsymbol{x}_\alpha(\mathbf{N})\backslash X$, $\mu^{\#}\cdot\kappa\in\mathbf{N}\backslash X$.

Поскольку $\mu^{\#}\cdot\kappa\notin\boldsymbol{x}(\mathbf{N}\backslash X)$, имеем $\mu^{\#}\cdot\kappa\in(\mathbf{N}\backslash X)\backslash\boldsymbol{x}(\mathbf{N}\backslash X)$.

2.2.2.2.2. Если $\mu^{\#}\cdot\langle\text{Р},\gamma\rangle\notin\mathbf{N}\backslash\boldsymbol{x}_{\alpha-1}(\mathbf{N})$, то возможны два варианта:

2.2.2.2.2.1. $\mu^{\#}\cdot\langle\text{Р},\gamma\rangle\notin\mathbf{N}$.

Тогда $\mu^{\#}\cdot\langle\text{Р},\gamma\rangle\notin(\mathbf{N}\backslash X)\backslash\boldsymbol{x}(\mathbf{N}\backslash X)$.

2.2.2.2.2.2. $\mu^{\#}\cdot\langle\text{Р},\gamma\rangle\in\boldsymbol{x}_{\alpha-1}(\mathbf{N})$.

Тогда по предположению шага индукции $\mu^{\#}\cdot\langle\text{Р},\gamma\rangle\in\boldsymbol{x}(\mathbf{N}\backslash X)$.

Тогда $\mu^{\#}\cdot\langle\text{Р},\gamma\rangle\notin(\mathbf{N}\backslash X)\backslash\boldsymbol{x}(\mathbf{N}\backslash X)$.

2.2.2.2.3. Если $\mu^{\#}\cdot\langle z\rangle\notin\mathbf{N}\backslash\boldsymbol{x}_{\alpha-1}(\mathbf{N})$ для произвольного $z\in P$, то возможны два варианта:

2.2.2.2.3.1. $\mu^{\#}\cdot\langle z\rangle\notin\mathbf{N}$.

Тогда $\mu^{\#}\cdot\langle z\rangle\notin(\mathbf{N}\backslash X)\backslash\boldsymbol{x}(\mathbf{N}\backslash X)$.

2.2.2.2.3.1.1 $\mu^{\#}\cdot\langle z\rangle\in \boldsymbol{x}_{\alpha-1}(\mathbf{N})$.

Тогда по предположению шага индукции $\mu^{\#}\cdot\langle z\rangle\in \boldsymbol{x}(\mathbf{N}\backslash X)$.

Тогда $\mu^{\#}\cdot\langle z\rangle\notin(\mathbf{N}\backslash X)\backslash\boldsymbol{x}(\mathbf{N}\backslash X)$.

Итак, мы имеем:

$P\in\mathbf{R}\cup\mathbf{Q}$ & $\mu^{\#}\cdot\kappa\in(\mathbf{N}\backslash X)\backslash\boldsymbol{x}(\mathbf{N}\backslash X)$ & $\mu^{\#}\cdot\langle \text{Р}, \gamma\rangle\notin(\mathbf{N}\backslash X)\backslash\boldsymbol{x}(\mathbf{N}\backslash X)$

& $\forall z\in P\cup\{P^{\#}\}\ \mu^{\#}\cdot\langle z\rangle\notin(\mathbf{N}\backslash X)\backslash\boldsymbol{x}(\mathbf{N}\backslash X)$.

По определению $\boldsymbol{x}(\mathbf{N}\backslash X)$ существует такой ординал β, что $\boldsymbol{x}(\mathbf{N}\backslash X)=\boldsymbol{x}_{\beta}(\mathbf{N}\backslash X)$ и $\boldsymbol{x}_{\beta}(\mathbf{N}\backslash X)=\boldsymbol{x}_{\beta+1}(\mathbf{N}\backslash X)$.

Следовательно:

$P\in\mathbf{R}\cup\mathbf{Q}$ & $\mu^{\#}\cdot\kappa\in(\mathbf{N}\backslash X)\backslash\boldsymbol{x}_{\beta}(\mathbf{N}\backslash X)$ & $\mu^{\#}\cdot\langle \text{Р}, \gamma\rangle\notin(\mathbf{N}\backslash X)\backslash\boldsymbol{x}_{\beta}(\mathbf{N}\backslash X)$

& $\forall z\in P\cup\{P^{\#}\}\ \mu^{\#}\cdot\langle z\rangle\notin(\mathbf{N}\backslash X)\backslash\boldsymbol{x}_{\beta}(\mathbf{N}\backslash X)$.

Но тогда $\mu^{\#}\cdot\kappa\notin\boldsymbol{x}_{\beta}(\mathbf{N}\backslash X)$ и по правилу вывода **2** $\mu^{\#}\cdot\kappa\in\boldsymbol{x}_{\beta+1}(\mathbf{N}\backslash X)$.

Но это противоречит равенству $\boldsymbol{x}_{\beta}(\mathbf{N}\backslash X)=\boldsymbol{x}_{\beta+1}(\mathbf{N}\backslash X)$.

Следовательно, наше допущение не верно, и $\mu^{\#}\cdot\kappa\in\boldsymbol{x}(\mathbf{N}\backslash X)$, что и требовалось доказать.

2.2.2.3. Правило вывода **3** для P-неполной трассы после $\mu^{\#}$: $\sigma=\mu^{\#}\cdot\lambda^{\#}\cdot\kappa$.

Условие этого правила для (особого) отказа $P^{\#}$:

$P\in\mathbf{R}$ & $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in\mathbf{N}\backslash\boldsymbol{x}_{\alpha-1}(\mathbf{N})$ & $\boldsymbol{Ip}(\mu)\neq\varnothing$

& $\mu^{\#}\cdot\langle \text{Р}, \gamma\rangle\notin\mathbf{N}\backslash\boldsymbol{x}_{\alpha-1}(\mathbf{N})$ & $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin\mathbf{N}\backslash\boldsymbol{x}_{\alpha-1}(\mathbf{N})$

& $\forall z\in P$ $\mu^{\#}\cdot\langle z\rangle\notin\mathbf{N}\backslash\boldsymbol{x}_{\alpha-1}(\mathbf{N})$.

Допустим, утверждение леммы не верно, то есть $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\notin\boldsymbol{x}(\mathbf{N}\backslash X)$.

2.2.2.3.1. Если $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in\mathbf{N}\backslash\boldsymbol{x}_{\alpha-1}(\mathbf{N})$, то $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in\mathbf{N}$.

Поскольку $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa=\sigma\in\boldsymbol{x}_{\alpha}(\mathbf{N})\backslash X$, $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in\mathbf{N}\backslash X$.

Поскольку $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\notin\boldsymbol{x}(\mathbf{N}\backslash X)$, имеем $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in(\mathbf{N}\backslash X)\backslash\boldsymbol{x}(\mathbf{N}\backslash X)$.

2.2.2.3.2. Аналогично 2.2.2.2.2 $\mu^{\#}\cdot\langle \text{Р}, \gamma\rangle\notin(\mathbf{N}\backslash X)\backslash\boldsymbol{x}(\mathbf{N}\backslash X)$.

2.2.2.3.3. Аналогично 2.2.2.2.3: $\forall z\in P$ $\mu^{\#}\cdot\langle z\rangle\notin(\mathbf{N}\backslash X)\backslash\boldsymbol{x}(\mathbf{N}\backslash X)$.

2.2.2.3.4. Если $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin\mathbf{N}\backslash\boldsymbol{x}_{\alpha-1}(\mathbf{N})$, то возможны два варианта:

2.2.2.3.4.1. $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin\mathbf{N}$.

Тогда $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin(\mathbf{N}\setminus X)\setminus\boldsymbol{x}(\mathbf{N}\setminus X)$.

2.2.2.3.4.2. $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\in\boldsymbol{x}_{\alpha-1}(\mathbf{N})$.

Тогда по предположению шага индукции $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\in\boldsymbol{x}(\mathbf{N}\setminus X)$.

Тогда $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin(\mathbf{N}\setminus X)\setminus\boldsymbol{x}(\mathbf{N}\setminus X)$.

Итак, мы имеем:

$P\in\mathbf{R}$ & $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in(\mathbf{N}\setminus X)\setminus\boldsymbol{x}(\mathbf{N}\setminus X)$ & $\boldsymbol{Ip}(\mu)\neq\varnothing$

& $\mu^{\#}\cdot\langle\not{P},\gamma\rangle\notin(\mathbf{N}\setminus X)\setminus\boldsymbol{x}(\mathbf{N}\setminus X)$ & $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin(\mathbf{N}\setminus X)\setminus\boldsymbol{x}(\mathbf{N}\setminus X)$

& $\forall z\in P\ \ \mu^{\#}\cdot\langle z\rangle\notin(\mathbf{N}\setminus X)\setminus\boldsymbol{x}(\mathbf{N}\setminus X)$.

По определению $\boldsymbol{x}(\mathbf{N}\setminus X)$ существует такой ординал ψ, что $\boldsymbol{x}(\mathbf{N}\setminus X)=\boldsymbol{x}_{\psi}(\mathbf{N}\setminus X)$ и $\boldsymbol{x}_{\psi}(\mathbf{N}\setminus X)=\boldsymbol{x}_{\psi+1}(\mathbf{N}\setminus X)$.

Следовательно:

$P\in\mathbf{R}$ & $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in(\mathbf{N}\setminus X)\setminus\boldsymbol{x}_{\psi}(\mathbf{N}\setminus X)$ & $\boldsymbol{Ip}(\mu)\neq\varnothing$

& $\mu^{\#}\cdot\langle\not{P},\gamma\rangle\notin(\mathbf{N}\setminus X)\setminus\boldsymbol{x}_{\psi}(\mathbf{N}\setminus X)$ & $\mu^{\#}\cdot\langle P^{\#}\rangle\cdot\lambda^{\#}\notin(\mathbf{N}\setminus X)\setminus\boldsymbol{x}_{\psi}(\mathbf{N}\setminus X)$

& $\forall z\in P\ \ \mu^{\#}\cdot\langle z\rangle\notin(\mathbf{N}\setminus X)\setminus\boldsymbol{x}_{\psi}(\mathbf{N}\setminus X)$.

Но тогда $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\notin\boldsymbol{x}_{\psi}(\mathbf{N}\setminus X)$ и по правилу вывода **3** $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in\boldsymbol{x}_{\psi+1}(\mathbf{N}\setminus X)$.

Но это противоречит равенству $\boldsymbol{x}_{\psi}(\mathbf{N}\setminus X)=\boldsymbol{x}_{\psi+1}(\mathbf{N}\setminus X)$.

Следовательно, наше допущение не верно, и $\mu^{\#}\cdot\lambda^{\#}\cdot\kappa\in\boldsymbol{x}(\mathbf{N}\setminus X)$, что и требовалось доказать.

Шаг индукции для непредельного ординала доказан.

Шаг индукции доказан.

Вложенность $\boldsymbol{x}(\mathbf{N}\setminus X)\supseteq\boldsymbol{x}_{\alpha}(\mathbf{N})\setminus X$ доказана.

3. Теперь докажем утверждение леммы: $X\cup\boldsymbol{x}(\mathbf{N}\setminus X)=\boldsymbol{x}(\mathbf{N})$.

Мы имеем для каждого ординала α:

$\boldsymbol{x}_{\alpha}(\mathbf{N}\setminus X)\subseteq\boldsymbol{x}(\mathbf{N})\setminus X$ и $\boldsymbol{x}(\mathbf{N}\setminus X)\supseteq\boldsymbol{x}_{\alpha}(\mathbf{N})\setminus X$.

По определению $\boldsymbol{x}(\mathbf{N})$ существует такой ординал φ, что $\boldsymbol{x}(\mathbf{N})=\boldsymbol{x}_{\varphi}(\mathbf{N})$ и $\boldsymbol{x}_{\varphi}(\mathbf{N})=\boldsymbol{x}_{\varphi+1}(\mathbf{N})$.

По определению $\boldsymbol{x}(\mathbf{N}\setminus X)$ существует такой ординал ψ, что $\boldsymbol{x}(\mathbf{N}\setminus X)=\boldsymbol{x}_{\psi}(\mathbf{N}\setminus X)$ и $\boldsymbol{x}_{\psi}(\mathbf{N}\setminus X)=\boldsymbol{x}_{\psi+1}(\mathbf{N}\setminus X)$.

Выберем из ординалов φ и ψ наибольший ординал, который обозначим π. Очевидно, что $\boldsymbol{x}(\mathbf{N})=\boldsymbol{x}_{\varphi}(\mathbf{N})=\boldsymbol{x}_{\varphi+1}(\mathbf{N})$ влечет $\boldsymbol{x}(\mathbf{N})=\boldsymbol{x}_{\varphi}(\mathbf{N})=\boldsymbol{x}_{\pi}(\mathbf{N})$, и $\boldsymbol{x}(\mathbf{N}\setminus X)=\boldsymbol{x}_{\psi}(\mathbf{N}\setminus X)=\boldsymbol{x}_{\psi+1}(\mathbf{N}\setminus X)$ влечет $\boldsymbol{x}(\mathbf{N}\setminus X)=\boldsymbol{x}_{\psi}(\mathbf{N}\setminus X)=\boldsymbol{x}_{\pi}(\mathbf{N}\setminus X)$.

Тогда $\boldsymbol{x}_{\pi}(\mathbf{N}\setminus X)\subseteq\boldsymbol{x}(\mathbf{N})\setminus X$ и $\boldsymbol{x}(\mathbf{N}\setminus X)\supseteq\boldsymbol{x}_{\pi}(\mathbf{N})\setminus X$.

Тогда $\boldsymbol{x}(\mathbf{N}\setminus X)\subseteq\boldsymbol{x}(\mathbf{N})\setminus X$ и $\boldsymbol{x}(\mathbf{N}\setminus X)\supseteq\boldsymbol{x}(\mathbf{N})\setminus X$.

Тем самым, $\boldsymbol{x}(\mathbf{N}\backslash X)=\boldsymbol{x}(\mathbf{N})\backslash X$.

Отсюда, поскольку $X\subseteq\boldsymbol{x}(\mathbf{N})$, имеем $\boldsymbol{x}(\mathbf{N})=X\cup\boldsymbol{x}(\mathbf{N}\backslash X)$.

Лемма доказана.

6.60. Доказательство леммы 40

По определению отношение «$\preccurlyeq$» обладает свойствами рефлексивности и транзитивности. Нам осталось показать его антисимметричность:

$\sigma^{\#}\preccurlyeq\sigma`^{\#}\ \&\ \sigma`^{\#}\preccurlyeq\sigma^{\#}\ \Rightarrow\ \sigma^{\#}=\sigma`^{\#}$.

Действительно, условие $\sigma^{\#}\preccurlyeq\sigma`^{\#}\ \&\ \sigma`^{\#}\preccurlyeq\sigma^{\#}$ влечет

существование последовательности $\sigma^{\#}=\sigma_1{}^{\#}\preccurlyeq_1\ldots\preccurlyeq_1\sigma_n{}^{\#}=\sigma`^{\#}\preccurlyeq_1\ldots\preccurlyeq_1\sigma_m{}^{\#}=\sigma^{\#}$.

Но, поскольку $\sigma^{\#}\preccurlyeq_1\sigma`^{\#}$ по определению означает $\sigma^{\#}=\sigma`^{\#}\ \vee\ \sigma^{\#}\prec_1\sigma`^{\#}$, а из $\sigma_i{}^{\#}\prec_1\sigma_{i+1}{}^{\#}$ следует, что трасса $\sigma_{i+1}{}^{\#}$ длиннее трассы $\sigma_i{}^{\#}$,
такая последовательность возможна только в том случае,
когда $\sigma^{\#}=\sigma_1{}^{\#}=\ldots=\sigma_n{}^{\#}=\sigma`^{\#}=\ldots=\sigma_m{}^{\#}=\sigma^{\#}$, что влечет $\sigma^{\#}=\sigma`^{\#}$.

6.61. Доказательство леммы 41

Из условий леммы следует, что найдутся такие n и m, что

$\sigma^{\#}=\sigma_0{}^{\#}\preccurlyeq_1\sigma_1{}^{\#}\preccurlyeq_1\ldots\preccurlyeq_1\sigma_{n-1}{}^{\#}\preccurlyeq_1\sigma_n{}^{\#}\preccurlyeq_1\ldots\preccurlyeq_1\sigma_m{}^{\#}=\sigma`^{\#}$, где $\sigma_{n-1}{}^{\#}\in\mathbf{N}$ и $\sigma_n{}^{\#}\notin\mathbf{N}$.

Тогда по правилу вывода **3** имеем:
$\sigma_{n-1}{}^{\#}\in\boldsymbol{x}_1(\mathbf{N})$, $\sigma_{n-2}{}^{\#}\in\boldsymbol{x}_2(\mathbf{N})$, … , $\sigma_1{}^{\#}\in\boldsymbol{x}_{n-1}(\mathbf{N})$, $\sigma_0{}^{\#}\in\boldsymbol{x}_n(\mathbf{N})$.
Поскольку $\sigma^{\#}=\sigma_0{}^{\#}$, имеем $\sigma^{\#}\in\boldsymbol{x}_n(\mathbf{N})$.
Поскольку $\boldsymbol{x}_n(\mathbf{N})\subseteq\boldsymbol{x}(\mathbf{N})$, имеем $\sigma^{\#}\in\boldsymbol{x}(\mathbf{N})$.

6.62. Доказательство леммы 42

1. Пусть $u\in\mathbf{L}$.

   Тогда

   $A_{\sigma\cdot\langle u\rangle}\ =\ \{\mathbf{S}\ \textit{after}\ \mu_u\mid\mu_u\in\widetilde{\textit{di}}(\sigma\cdot\langle u\rangle)\cap\textit{SafeBy}(\boldsymbol{F}(\mathbf{S}))\}$

   $=\ \{\cup((\mathbf{S}\ \textit{after}\ \mu)\ \textit{after}\ \langle u\rangle)$

   $\mid\ \mu\in\widetilde{\textit{di}}(\sigma)\cap\textit{SafeBy}(\boldsymbol{F}(\mathbf{S}))\ \ \&\ u\ \textit{safe by}\ \boldsymbol{F}(\mathbf{S})\ \textit{after}\ \mu\}$

   $=\ \{\cup(a\ \textit{after}\ \langle u\rangle)\ \mid\ a\in A_\sigma\ \ \&\ u\ \textit{safe by}\ a\}$.

Также $r_{\sigma\cdot\langle u\rangle}=\varnothing$.

Тем самым, $(A_{\sigma\cdot\langle u\rangle},r_{\sigma\cdot\langle u\rangle}) = (A_\sigma,r_\sigma)$ ***safter*** u.

2. Пусть $u\in\mathbf{R}$.

Тогда

$A_{\sigma\cdot\langle u\rangle} = \{\mathbf{S}\ \textit{after}\ \mu_u \mid \mu_u\in \textit{di}\tilde{}(\sigma\cdot\langle u\rangle)\cap \textit{SafeBy}(\textit{F}(\mathbf{S}))\}$

$= \{\cup((\mathbf{S}\ \textit{after}\ \mu)\ \textit{after}\ \rho)$
$\mid \mu\in \textit{di}\tilde{}(\sigma)\cap \textit{SafeBy}(\textit{F}(\mathbf{S}))\ \&\ \forall i=1..|\rho|$
$\rho(i)\subseteq\cup r_\sigma\cup R\ \&\ \rho(i)\ \textit{safe by}\ \textit{F}(\mathbf{S})\ \textit{after}\ \mu\cdot\rho[1..i-1]\}$

$= \{\cup(a\ \textit{after}\ \rho)$
$\mid a\in A(\sigma)\ \&\ \forall i=1..|\rho|$
$\rho(i)\subseteq\cup r_\sigma\cup R\ \&\ \rho(i)\ \textit{safe by}\ \cup(a\ \textit{after}\ \rho[1..i-1])\}$.

Также $r_{\sigma\cdot\langle u\rangle}=\{\cup r_\sigma\cup R\}$.

Тем самым, $(A_{\sigma\cdot\langle u\rangle},r_{\sigma\cdot\langle u\rangle}) = (A_\sigma,r_\sigma)$ ***safter*** u.

6.63. Доказательство леммы 43

По лемме 42 имеем (A_σ,r_σ) ***safter*** $R = (A_{\sigma\cdot\langle R\rangle},r_{\sigma\cdot\langle R\rangle})$.

По определению $r_{\sigma\cdot\langle R\rangle}=\{\{\cup \textit{Ip}(\sigma\cdot\langle R\rangle)\}\mid \textit{Ip}(\sigma\cdot\langle R\rangle)\neq\varnothing\}=\{\cup \textit{Ip}(\sigma\cdot\langle R\rangle)\}$.

Если $R\subseteq\cup r_\sigma$, то $r_\sigma\neq\varnothing$ и $r_\sigma=\{\cup \textit{Ip}(\sigma)\}=\{\cup \textit{Ip}(\sigma\cdot\langle R\rangle)\}$.

Следовательно, $r_{\sigma\cdot\langle R\rangle}=r_\sigma$.

По определению $A_{\sigma\cdot\langle R\rangle} = \{\mathbf{S}\ \textit{after}\ \mu\mid\mu\in \textit{di}\tilde{}(\sigma\cdot\langle R\rangle)\cap \textit{SafeBy}(\textit{F}(\mathbf{S}))\}$.

Если $R\subseteq\cup r_\sigma$, то $r_\sigma\neq\varnothing$ и $r_\sigma=\{\cup \textit{Ip}(\sigma)\}$, следовательно, $R\subseteq\cup \textit{Ip}(\sigma)$.

А тогда $\textit{di}\tilde{}(\sigma\cdot\langle R\rangle)=\textit{di}\tilde{}(\sigma)$.

Следовательно, $A_{\sigma\cdot\langle R\rangle} = \{\mathbf{S}\ \textit{after}\ \mu\mid\mu\in \textit{di}\tilde{}(\sigma)\cap \textit{SafeBy}(\textit{F}(\mathbf{S}))\} = A_\sigma$.

6.64. Доказательство леммы 44

1. Случай 1: $u\in\mathbf{L}$.

Утверждение леммы следует из теоремы 12 и равенства $\cup r_\sigma=\cup \textit{Ip}(\sigma)$.

2. Случай 2: $u\in\mathbf{R}$.

Пусть $\sigma^{\#}\in\boldsymbol{\Sigma}^{\boldsymbol{\theta}\tilde{}}$ и $u^{\#}\ \textit{safe}_{\gamma\Delta}\ \boldsymbol{\Sigma}\tilde{}\ \textit{after}\ \sigma^{\#}$.

Поскольку $u\in\mathbf{R}$, имеем $\textit{Ip}(\sigma\cdot\langle u\rangle\neq\varnothing$.

А тогда $r_{\sigma\cdot\langle u\rangle}=\{\cup \textit{Ip}(\sigma\cdot\langle u\rangle)\}=\{u\cup\cup \textit{Ip}(\sigma)\}$.

Следовательно, условие $Q\subseteq u\cup\cup \textit{Ip}(\sigma)$ эквивалентно условию $Q\subseteq\cup r_{\sigma\cdot\langle u\rangle}$.

Допустим, утверждение леммы не верно. Тогда возможны два подслучая.

2.1. Подслучай 1: Наблюдение $u^{\#}$ **L**-актуально после $\sigma^{\#}$, но для некоторого $Q \in \mathbf{Q}$ такого, что $Q \subseteq \cup r_{\sigma\cdot\langle u\rangle}$, и некоторого $a \in A_{\sigma\cdot\langle u\rangle}$ имеет место Q ***safe by*** a.

Поскольку $\sigma^{\#} \in \mathbf{\Sigma^{0\sim}}$, по теореме 12 (1) трасса $\sigma^{\#}$ **L**-актуальна.

А тогда, поскольку наблюдение $u^{\#}$ **L**-актуально после $\sigma^{\#}$,

трасса $\sigma^{\#}\cdot\langle u^{\#}\rangle$ **L**-актуальна.

Тогда эта трасса встречается в некоторой безопасно-тестируемой для ~пополнения **L**-реализации **I**:

$\mathbf{I} \in \mathbf{SafeImp}(\mathbf{T}^{\sim},\mathbf{L})$ и $\sigma^{\#}\cdot\langle u^{\#}\rangle \in \mathbf{I}$.

$\mathbf{I} \in \mathbf{SafeImp}(\mathbf{T}^{\sim},\mathbf{L})$ влечет $\mathbf{I}_{\mathbf{L}} \in \mathbf{SafeImp}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}}$.

По лемме 19 $\mathbf{T}^{\sim} \approx_{\mathbf{L}} \mathbf{T}$, что влечет $\mathbf{SafeImp}(\mathbf{T}^{\sim},\mathbf{L})_{\mathbf{L}} = \mathbf{SafeImp}(\mathbf{T},\mathbf{L})_{\mathbf{L}}$.

Далее $\mathbf{SafeImp}(\mathbf{T},\mathbf{L})_{\mathbf{L}} = \mathbf{SafeImp}(\mathbf{T})$.

Поэтому $\mathbf{I}_{\mathbf{L}} \in \mathbf{SafeImp}(\mathbf{T})$, а $\sigma\cdot\langle u\rangle \in \mathbf{I}_{\mathbf{L}}$, то есть является актуальной трассой для исходной спецификации $\mathbf{\Sigma}$.

По определению $A_{\sigma\cdot\langle u\rangle}$ имеем

$a = (\mathbf{S}\ \mathbf{after}\ \mu)$, где $\mu \in \mathbf{di}^{\sim}(\sigma\cdot\langle u\rangle) \cap \mathbf{SafeBy}(\mathbf{\Sigma})$.

По лемме 1 условия $\mu \in \mathbf{di}^{\sim}(\sigma\cdot\langle u\rangle)$ и $\sigma\cdot\langle u\rangle \in \mathbf{I}_{\mathbf{L}}$ влекут $\mu \in \mathbf{I}_{\mathbf{L}}$, то есть трасса μ является актуальной трассой для исходной спецификации $\mathbf{\Sigma}$.

А тогда, поскольку $\mu \in \mathbf{SafeBy}(\mathbf{\Sigma})$, по лемме 5 (2) трасса μ ~конформна.

Следовательно, $\mu^{\#} \in \mathbf{\Sigma^{0\sim}}$.

Поскольку $a = (\mathbf{S}\ \mathbf{after}\ \mu)$,

условие Q ***safe by*** a влечет Q ***safe by*** $(\mathbf{S}\ \mathbf{after}\ \mu)$.

По определению ограниченного отношения ***safe by***:

Q ***safe by*** $(\mathbf{S}\ \mathbf{after}\ \mu) = Q$ ***safe by*** $\mathbf{\Sigma}$ ***after*** μ.

Тогда по определению ~безопасности кнопок Q ***safe~by*** $\mathbf{\Sigma}$ ***after*** μ.

Тогда по правилу вывода ~финальных трасс $\mu^{\#}\cdot\langle \not{\mathbf{Q}},\gamma\rangle \notin \mathbf{\Sigma^{1\sim}}$.

Поскольку условия $Q \subseteq u \cup \cup \mathbf{Ip}(\sigma)$ и $Q \subseteq \cup r_{\sigma\cdot\langle u\rangle}$ эквивалентны,

$Q \subseteq \cup r_{\sigma\cdot\langle u\rangle}$ влечет $Q \subseteq u \cup \cup \mathit{Ip}(\sigma)$.

Итак мы показали:

$Q \subseteq u \cup \cup \mathit{Ip}(\sigma)$, $\mu \in \mathit{di}^{\sim}(\sigma\cdot\langle u\rangle)$, $\mu^{\#} \in \Sigma^{0\sim}$, $\mu^{\#}\cdot\langle \cancel{Q}, \gamma\rangle \notin \Sigma^{1\sim}$.

Но тогда по теореме 12 (2) наблюдение $u^{\#}$ не **L**-актуально после $\sigma^{\#}$, что противоречит его **L**-актуальности в рассматриваемом подслучае 2.1.

Мы пришли к противоречию, следовательно, подслучая 2.1 не бывает.

2.2. Подслучай 2: Наблюдение $u^{\#}$ не **L**-актуально после $\sigma^{\#}$, но для каждого $Q \in \mathbf{Q}$ такого, что $Q \subseteq \cup r_{\sigma\cdot\langle u\rangle}$, и каждого $a \in A_{\sigma\cdot\langle u\rangle}$ имеет место Q ~~***safe by***~~ a.

Поскольку наблюдение $u^{\#}$ не **L**-актуально после $\sigma^{\#}$, по теореме 12 (2) найдется кнопка $Q \in \mathbf{Q}$ такая, что $Q \subseteq u \cup \cup \mathit{Ip}(\sigma)$, и найдется трасса $\mu \in \mathit{di}^{\sim}(\sigma\cdot\langle u\rangle)$ такая, что $\mu^{\#} \in \Sigma^{0\sim}$ и $\mu^{\#}\cdot\langle \cancel{Q}, \gamma\rangle \notin \Sigma^{1\sim}$.

По правилам вывода ~финальных трасс

условие $\mu^{\#}\cdot\langle \cancel{Q}, \gamma\rangle \notin \Sigma^{1\sim}$ влечет Q ***safe~by*** Σ ***after*** μ.

А тогда по определению ~безопасности **Q**-кнопок найдется трасса $\kappa \in \mathit{di}^{\sim}(\mu) \cap \mathit{SafeBy}(\Sigma)$ такая, что Q ***safe by*** Σ ***after*** κ.

Из $\kappa \in \mathit{di}^{\sim}(\mu)$ и $\mu \in \mathit{di}^{\sim}(\sigma\cdot\langle u\rangle)$ следует, что $\kappa \in \mathit{di}^{\sim}(\sigma\cdot\langle u\rangle)$.

Поскольку также $\kappa \in \mathit{SafeBy}(\Sigma)$, имеем $\kappa \in \mathit{di}^{\sim}(\sigma\cdot\langle u\rangle) \cap \mathit{SafeBy}(\Sigma)$.

А тогда по определению $A_{\sigma\cdot\langle u\rangle}$ имеем $a = (S$ ***after*** $\kappa) \in A_{\sigma\cdot\langle u\rangle}$.

Условие Q ***safe by*** Σ ***after*** κ по определению ограниченного отношения ***safe by*** влечет Q ***safe by*** $(S$ ***after*** $\kappa)$, что эквивалентно Q ***safe by*** a, что противоречит условию рассматриваемого подслучая 2.2.

Мы пришли к противоречию, следовательно, подслучая 2.2 не бывает.

Итак, мы пришли к противоречию в обоих рассматриваемых подслучаях 2.1 и 2.2, следовательно, наше допущение о том, что утверждение леммы не верно в случае 2, не верно и в этом случае лемма также доказана.

6.65. Доказательство теоремы 21

1. Докажем утверждение 1 индукцией по трассе.

Если пустая трасса безопасна в исходной LTS-спецификации **S**, то $s_0 = \langle\gamma\rangle \not\Rightarrow$, а начальное состояние – это состояние $s^{\sim}_0$.

Докажем утверждение для пустой трассы ϵ.

Поскольку в LTS $\mathbf{S}^{\sim}$ по построению нет τ-переходов, пустая трасса заканчивается в состоянии $s^{\sim}_0$.

Имеем $s\tilde{}_0=(\{\{\mathbf{S}\ \textit{after}\ \epsilon\}\},\varnothing)=(A_\epsilon,r_\epsilon)$.

Пусть трасса $\sigma^\#$ заканчивается в состоянии (A_σ,r_σ), и рассмотрим трассу $\sigma^\#\cdot\langle u^\#\rangle$.

Такая трасса может быть получена только по правилу вывода: $\forall u\in\mathbf{L}\cup\mathbf{R}$

2R) $u\sim\textit{conf}\ (A,r)\ \vdash\ (A,r)\text{—}u^\#\!\rightarrow(A,r)\ \textit{safter}\ u$,

По лемме 42 $(A_{\sigma\cdot\langle u\rangle},r_{\sigma\cdot\langle u\rangle})\ =\ (A_\sigma,r_\sigma)\ \textit{safter}\ u$.

Следовательно, трасса $\sigma^\#\cdot\langle u^\#\rangle$ заканчивается в состоянии $(A_{\sigma\cdot\langle u\rangle},r_{\sigma\cdot\langle u\rangle})$, что и требовалось доказать.

2. Докажем утверждение 2.

Мы будем использовать определение ~финальных трасс из подраздела 4.2, когда исходная спецификация задана в виде LTS $\mathbf{S}$.

Рассмотрим два возможных случая в зависимости от того, достижимо или нет разрушение из начального состояния LTS $\mathbf{S}$.

2.1. $s_0=\langle\gamma\rangle\Rightarrow$.

Тогда все трассы LTS $\mathbf{S}\tilde{}$ получаются по правилу вывода:

1R) $s_0=\langle\gamma\rangle\Rightarrow\ \vdash\ \gamma\text{—}\gamma\!\rightarrow\varpi$,

а все трассы $\boldsymbol{\Sigma}^{\mathbf{01}\sim}$ – по правилу вывода:

1) $s_0=\langle\gamma\rangle\Rightarrow\ \vdash\ \epsilon\in\boldsymbol{\Sigma}^{\mathbf{1}\sim}\ \&\ \langle\gamma\rangle\in\boldsymbol{\Sigma}^{\mathbf{1}\sim}$.

В обоих случаях получается одно и то же множество трасс $\{\epsilon,\gamma\}$.

2.2. $s_0=\langle\gamma\rangle\not\Rightarrow$.

Доказательство будем вести индукцией по трассе.

Очевидно, $\epsilon^\#=\epsilon\in\boldsymbol{T}(\mathbf{S}\tilde{})\cap\boldsymbol{\Sigma}^{\mathbf{01}\sim}$.

Пусть трасса $\sigma^\#\in\boldsymbol{T}(\mathbf{S}\tilde{})\cap\boldsymbol{\Sigma}^{\mathbf{01}\sim}$.

Тогда по доказанному утверждению 1 в LTS $\mathbf{S}\tilde{}$ трасса $\sigma^\#$ заканчивается в состоянии (A_σ,r_σ).

Рассмотрим возможные продолжения этой трассы в LTS $\mathbf{S}\tilde{}$ и в $\boldsymbol{\Sigma}^{\mathbf{01}\sim}$.

2.2.1. Продолжение $\mathbf{L}$-наблюдением $u^\#$.

Трасса $\sigma^\#\cdot\langle u^\#\rangle$ получается в LTS $\mathbf{S}\tilde{}$ по правилу вывода: $\forall u\in\mathbf{L}\cup\mathbf{R}$

2R) $u\sim\textit{conf}\ (A_\sigma,r_\sigma)\ \vdash\ (A_\sigma,r_\sigma)\text{—}u^\#\!\rightarrow(A_\sigma,r_\sigma)\ \textit{safter}\ u$,

а в $\boldsymbol{\Sigma}^{\mathbf{01}\sim}$ – по правилу вывода: $\forall u\in\mathbf{R}\cup\mathbf{L}$

3) $\sigma^{\#}\in\boldsymbol{\Sigma^{0\sim}}$ & $u \sim\!\!\boldsymbol{conf}\ (A_\sigma,r_\sigma) \vdash \sigma^{\#}\cdot\langle u^{\#}\rangle\in\boldsymbol{\Sigma^{0\sim}}$,

Тем самым, $\sigma^{\#}\cdot\langle u^{\#}\rangle\in\boldsymbol{T}(\mathbf{S}^{\sim}) \Leftrightarrow \sigma^{\#}\cdot\langle u^{\#}\rangle\in\boldsymbol{\Sigma^{01\sim}}$.

2.2.2. Продолжение не-отказом $\not\Vdash$ и далее разрушением.

Трасса $\sigma^{\#}\cdot\langle\not\Vdash,\gamma\rangle$ вместе с ее префиксом $\sigma^{\#}\cdot\langle\not\Vdash\rangle$ получается в LTS $\mathbf{S}^{\sim}$ по правилу вывода: $\forall P\in\mathbf{R}\cup\mathbf{Q}$

3R) P ***safe~by*** $A_\sigma \vdash (A_\sigma,r_\sigma)\text{---}\not\Vdash\rightarrow\gamma\text{---}\gamma\rightarrow\varpi$,

а в $\boldsymbol{\Sigma^{01\sim}}$ – по правилу вывода: $\forall P\in\mathbf{R}\cup\mathbf{Q}$

4) $\sigma^{\#}\in\boldsymbol{\Sigma^{0\sim}}$ & P ***safe~by*** $A_\sigma \vdash \sigma^{\#}\cdot\langle\not\Vdash\rangle\in\boldsymbol{\Sigma^{1\sim}}$ & $\sigma^{\#}\cdot\langle\not\Vdash,\gamma\rangle\in\boldsymbol{\Sigma^{1\sim}}$.

Тем самым, $\sigma^{\#}\cdot\langle\not\Vdash,\gamma\rangle\in\boldsymbol{T}(\mathbf{S}^{\sim}) \Leftrightarrow \sigma^{\#}\cdot\langle\not\Vdash,\gamma\rangle\in\boldsymbol{\Sigma^{01\sim}}$.

2.2.3. Продолжение не-отказом $\not\Vdash$ и далее дивергенцией.

Трасса $\sigma^{\#}\cdot\langle\not\Vdash,\Delta\rangle$ вместе с ее префиксом $\sigma^{\#}\cdot\langle\not\Vdash\rangle$ получается в LTS $\mathbf{S}^{\sim}$ по правилам вывода: $\forall Q\in\mathbf{Q}$ $\forall R\in\mathbf{R}$

4R) Q ***safe~by*** $A_\sigma \vdash (A_\sigma,r_\sigma)\text{---}\not Q\rightarrow\Delta\text{---}\Delta\rightarrow\varpi$,

5R) R ***safe~by*** A_σ & $(r_\sigma=\varnothing \vee R\not\subseteq\cup r_\sigma)$ & R ***act*** (A_σ,r_σ)

$\vdash (A_\sigma,r_\sigma)\text{---}\not R\rightarrow\Delta\text{---}\Delta\rightarrow\varpi$,

6R) R ***safe~by*** A_σ & $(r_\sigma=\varnothing \vee R\not\subseteq\cup r_\sigma)$ & R ***act*** (A_σ,r_σ)

$\vdash (A_\sigma,r_\sigma)\text{---}\not R\rightarrow\Delta\grave{}\text{---}\Delta\rightarrow\varpi$.

Поскольку $r_\sigma=\{\cup\boldsymbol{Ip}(\sigma)\,|\,\boldsymbol{Ip}(\sigma)\neq\varnothing\}$, для $Q\in\mathbf{Q}$ всегда $Q\not\subseteq\cup r_\sigma$.

Тем самым, общее условие продолжения трассы $\sigma^{\#}$ не-отказом $\not\Vdash$ и далее дивергенцией в LTS $\mathbf{S}^{\sim}$: $\forall P\in\mathbf{R}\cup\mathbf{Q}$

P ***safe~by*** A_σ & $(r_\sigma=\varnothing \vee P\not\subseteq\cup r_\sigma)$.

В $\boldsymbol{\Sigma^{01\sim}}$ трасса $\sigma^{\#}\cdot\langle\not\Vdash,\Delta\rangle$ вместе с ее префиксом $\sigma^{\#}\cdot\langle\not\Vdash\rangle$ получается по правилу вывода: $\forall P\in\mathbf{R}\cup\mathbf{Q}$

5) $\sigma^{\#}\in\boldsymbol{\Sigma^{0\sim}}$ & P ***safe~by*** A_σ & $(r_\sigma=\varnothing \vee P\not\subseteq\cup r_\sigma)$

$\vdash \sigma^{\#}\cdot\langle\not\Vdash\rangle\in\boldsymbol{\Sigma^{1\sim}}$ & $\sigma^{\#}\cdot\langle\not\Vdash,\Delta\rangle\in\boldsymbol{\Sigma^{1\sim}}$.

Тем самым, $\sigma^{\#}\cdot\langle\not\Vdash,\Delta\rangle\in\boldsymbol{T}(\mathbf{S}^{\sim}) \Leftrightarrow \sigma^{\#}\cdot\langle\not\Vdash,\Delta\rangle\in\boldsymbol{\Sigma^{01\sim}}$.

3. Докажем, что ~финальная LTS $\mathbf{S}^{\sim}$ является RTS.

3.1. Детерминизм.

По построению ~финальная LTS детерминирована, поскольку τ-переходов нет, и в каждом состоянии определено не более одного перехода по каждому символу.

3.2. Выделенное состояние ϖ имеется по построению.

Нам осталось показать, что для LTS $\mathbf{S}^{\sim}$ выполнены свойства **R1**÷**R5** RTS-модели.

Доказательство можно вести, опираясь только на правила вывода, но для большей наглядности мы будем использовать уже доказанные детерминированность LTS $\mathbf{S}^{\sim}$ и равенство $\boldsymbol{T}(\mathbf{S}^{\sim})=\boldsymbol{\Sigma}^{01\sim}$. Ниже мы будем пользоваться тем, что по лемме 8 множество $\boldsymbol{\Sigma}^{01\sim}$ ~финальных трасс обладает всеми свойствами $\mathbf{R}^{\#}$-модели, кроме, быть может, замкнутости (по $\boldsymbol{d}$-операции).

По правилам вывода переходов ~финальной LTS 1) любой переход по не-отказу заканчивается в состоянии γ, Δ или Δ', 2) в этих состояниях определены только переходы по разрушению или дивергенции, 3) концом переходов по разрушению и дивергенции является терминальное состояние ϖ. Тем самым, из конца перехода по не-отказу не достижимы состояния вида (A,r). Также только состояние вида (A,r) может быть началом перехода по **L**-наблюдению $u^{\#}\in\mathbf{L}\cup\mathbf{R}^{\#}$. Следовательно, в достижимом начале перехода по **L**-наблюдению $u^{\#}\in\mathbf{L}\cup\mathbf{R}^{\#}$ могут заканчиваться только **L**-трассы.

3.3. Допустимость **R1** выполняется по построению.

3.4. Согласованность **R2**.

Пусть в ~финальной LTS в некотором достижимом состоянии s определен переход-петля $s\text{—}R^{\#}\!\to s$, где $R\in\mathbf{R}$. Нам нужно доказать, что в состоянии s нет перехода по символам γ, Δ и $u\in R^{\#}$.

Поскольку состояние s достижимо, в нем заканчивается некоторая трасса σ, которая по доказанному утверждению 2 ~финальна.

Поскольку $s\text{—}R^{\#}\!\to s$, в состоянии s заканчивается также трасса $\sigma\cdot\langle R^{\#}\rangle$, которая по доказанному утверждению 2 тоже ~финальна.

Для любого имеющегося перехода $s\text{—}u\!\to$ по доказанному утверждению 2 трасса $\sigma\cdot\langle R^{\#}\rangle$ после продолжения символом u остается ~финальной.

Из свойства согласованности ~финальных трасс $\boldsymbol{T}(\mathbf{S}^{\sim})=\boldsymbol{\Sigma}^{01\sim}$ следует, что $u\neq\gamma$, $u\neq\Delta$ и $u\notin R^{\#}$.

Следовательно, в состоянии s нет перехода по символам γ, Δ и $u \in R^{\#}$, что и требовалось доказать.

3.5. Конвергентность **R3**.

Пусть в ~финальной LTS имеется достижимое состояние $s \neq \varpi$, и в нем не определены переходы по дивергенции и разрушению. Нам надо доказать, что для каждого **R**-отказа в s определен переход по этому отказу или по действию из этого отказа.

Поскольку состояние s достижимо, в нем заканчивается некоторая трасса σ, которая по доказанному утверждению 2 ~финальна.

Поскольку ~финальная LTS детерминирована, трасса σ заканчивается только в состоянии s.

Отсюда следует, что поскольку $s \text{—}\Delta\!\!\not\rightarrow$ и $s \text{—}\gamma\!\!\not\rightarrow$, трасса σ по доказанному утверждению 2 не продолжается во множестве ~финальных трасс дивергенцией и разрушением.

Поскольку $s \neq \varpi$, трасса σ не содержит дивергенции и разрушения.

Поэтому по свойству конвергентности ~финальных трасс $T(s^{\sim}) = \Sigma^{01\sim}$ трасса σ для каждого отказа $R \in \mathbf{R}$ продолжается во множестве ~финальных трасс отказом $R^{\#}$, каким-либо действием $z \in R$ или не-отказом $\not R$.

А тогда из доказанного утверждения 2 и детерминированности ~финальной LTS следует, что в состоянии s должен быть переход $s \text{—}R^{\#}\!\rightarrow$, $s \text{—}z\rightarrow$ или $s \text{—}\not R\!\rightarrow$, что и требовалось доказать.

3.6. Кумулятивность **R4**.

Пусть в ~финальной LTS в некотором достижимом состоянии s определен переход $s \text{—}R^{\#}\!\rightarrow s'$, где $R \in \mathbf{R}$. Нам надо доказать, что в состоянии s' определен переход-петля по отказу R и переходы-петли по каждому отказу R', по которому есть переход-петля в состоянии s.

Поскольку состояние s достижимо, в нем заканчивается некоторая трасса, которая по доказанному утверждению 2 ~финальна.

Поскольку это состояние является началом перехода по **L**-наблюдению $s \text{—}R^{\#}\!\rightarrow s'$, по доказанному выше эта трасса является **L**-трассой $\sigma^{\#}$.

Также из достижимости состояния s и наличия перехода $s \text{—}R^{\#}\!\rightarrow s'$ по правилам вывода следует $s_0 = \langle\gamma\rangle\!\not\Rightarrow$, а тогда можно применять доказанное выше утверждение 1.

Поскольку $s \text{—} R^{\#} \rightarrow s`$, в состоянии $s`$ заканчивается **L**-трасса $\sigma^{\#} \cdot \langle R^{\#} \rangle$, которая по доказанному утверждению 2 тоже ~финальна.

Поэтому по доказанному утверждению 1 $s` = (A_{\sigma \cdot \langle R \rangle}, r_{\sigma \cdot \langle R \rangle})$.

Если трасса $\sigma^{\#} \cdot \langle R^{\#} \rangle$ ~финальная **L**-трасса, трасса $\sigma^{\#} \cdot \langle R^{\#}, R^{\#} \rangle$ также ~финальная **L**-трасса (поскольку по лемме 8 множество ~финальных трасс обладает свойствами согласованности его трасс и конвергентности).

А тогда по доказанному утверждению 2 и по детерминированности ~финальной LTS в состоянии $s`$ есть переход по $R^{\#}$, заканчивающийся по доказанному утверждению 1 в состоянии $(A_{\sigma \cdot \langle R,R \rangle}, r_{\sigma \cdot \langle R,R \rangle})$.

Так как $r_{\sigma \cdot \langle R,R \rangle} = r_{\sigma \cdot \langle R \rangle}$ и по правилам вывода ~финальной LTS и лемме 43 $A_{\sigma \cdot \langle R,R \rangle} = A_{\sigma \cdot \langle R \rangle}$, то $s` \text{—} R^{\#} \rightarrow s`$.

Если в ~финальной LTS определен переход $s \text{—} R`^{\#} \rightarrow s$, где $R` \in \mathbf{R}$,

то в состоянии s заканчивается **L**-трасса $\sigma^{\#} \cdot \langle R`^{\#} \rangle$, а тогда в состоянии $s`$ заканчивается **L**-трасса $\sigma^{\#} \cdot \langle R`^{\#}, R^{\#} \rangle$, которая по доказанному утверждению 2 ~финальна, а по доказанному утверждению 1 $s` = (A_{\sigma \cdot \langle R`,R \rangle}, r_{\sigma \cdot \langle R`,R \rangle})$.

Если трасса $\sigma^{\#} \cdot \langle R`^{\#}, R^{\#} \rangle$ ~финальная **L**-трасса, трасса $\sigma^{\#} \cdot \langle R`^{\#}, R^{\#}, R`^{\#} \rangle$ также ~финальная **L**-трасса (поскольку по лемме 8 множество ~финальных трасс обладает свойствами согласованности его трасс и конвергентности).

А тогда по доказанному утверждению 2 и по детерминированности ~финальной LTS в состоянии $s`$ есть переход по $R`^{\#}$, заканчивающийся по доказанному утверждению 1 в состоянии $(A_{\sigma \cdot \langle R`,R,R` \rangle}, r_{\sigma \cdot \langle R`,R,R` \rangle})$.

Так как $r_{\sigma \cdot \langle R`,R,R` \rangle} = r_{\sigma \cdot \langle R`,R \rangle}$ и по правилам вывода ~финальной LTS и лемме 43 $A_{\sigma \cdot \langle R`,R,R` \rangle} = A_{\sigma \cdot \langle R`,R \rangle}$, то $s` \text{—} R`^{\#} \rightarrow s`$.

Мы доказали наличие требуемых переходов-петель $s` \text{—} R^{\#} \rightarrow s`$ и $s` \text{—} R`^{\#} \rightarrow s`$.

3.7. Полнота **R5**.

Пусть в ~финальной LTS в некотором достижимом состоянии s определен переход-петля $s \text{—} R^{\#} \rightarrow s$, где $R \in \mathbf{R}$, и для некоторого отказа $R` \in \mathbf{R}$ в состоянии $s$ нет переходов по действиям $z \in R`$ и не-отказу ~~$R`$~~. Нам надо доказать, что в состоянии $s$ определен переход-петля $s \text{—} R`^{\#} \rightarrow s$.

Поскольку состояние s достижимо, в нем заканчивается некоторая трасса, которая по доказанному утверждению 2 ~финальна.

Поскольку это состояние является началом перехода по **L**-наблюдению $s \text{—} R^{\#} \rightarrow s$, по доказанному выше эта трасса является **L**-трассой $\sigma^{\#}$.

Также из достижимости состояния s и наличия перехода $s \text{—} R^{\#} \rightarrow s$ по правилам вывода следует $s_0 = \langle \gamma \rangle \Rightarrow$, а тогда можно применять доказанное выше утверждение 1.

Поэтому по доказанному утверждению 1 $s = (A_{\sigma}, r_{\sigma})$.

Поскольку в состоянии s нет переходов по действиям $z \in R`$ и не-отказу ~~$R`$~~, по доказанной конвергентности ~финальной LTS $s \text{—} R`^{\#} \rightarrow s`$.

Тогда в ~финальной LTS имеется **L**-трасса $\sigma^{\#} \cdot \langle R`^{\#} \rangle$, которая заканчивается в состоянии $s`$ и по доказанному утверждению 1 $s` = (A_{\sigma \cdot \langle R` \rangle}, r_{\sigma \cdot \langle R` \rangle})$.

Поскольку $s \text{—} R^{\#} \rightarrow s$, в состоянии s заканчивается также трасса $\sigma^{\#} \cdot \langle R^{\#} \rangle$, что влечет $r_{\sigma} = r_{\sigma \cdot \langle R \rangle} \neq \varnothing$.

Поэтому отсутствие перехода по не-отказу ~~$R`$~~ в состоянии $s$ влечет по правилам вывода переходов ~финальной LTS $R` \subseteq \cup r_{\sigma}$.

А в этом случае $r_{\sigma \cdot \langle R` \rangle} = r_{\sigma}$ и по правилам вывода ~финальной LTS и лемме 43 $A_{\sigma \cdot \langle R` \rangle} = A_{\sigma}$, что влечет $s` = s$.

Следовательно, в состоянии s имеется переход петля $s \text{—} R`^{\#} \rightarrow s$, что и требовалось доказать.

6.66. Доказательство теоремы 22

Следует из теоремы 21, замечания 17 и теоремы 10.

6.67. Доказательство теоремы 23

Следует из теоремы 21, замечания 17 и теоремы 11.

6.68. Доказательство леммы 45

По правилам вывода переходов ~финальной LTS состояние вида (A,r) достижимо только в том случае, когда пустая трасса безопасна в исходной LTS-спецификации $\mathbf{S}$.

А тогда по теореме 21 (1) в достижимом состоянии (A,r) заканчивается такая простая $\mathbf{L}$-трасса $\sigma^{\#}$, что $(A,r)=(A_\sigma,r_\sigma)$.

По определению

$\boldsymbol{r}(s) = \{\{\cup\{R\in\mathbf{R}\mid(A_\sigma,r_\sigma)\text{—}R^{\#}\!\to s\}\}\mid\exists R\in\mathbf{R}\ \ s\text{—}R^{\#}\!\to s\}$,

а $r_\sigma=\{\cup\boldsymbol{Ip}(\sigma)\mid\boldsymbol{Ip}(\sigma)\neq\varnothing\}$.

Поэтому $\boldsymbol{r}(s)\neq\varnothing \Rightarrow \exists R\in\mathbf{R}\ \ s\text{—}R^{\#}\!\to s$,

и $r_\sigma\neq\varnothing \Rightarrow \exists R\in\mathbf{R}\ \ R\subseteq\cup r_\sigma$.

Поэтому нам достаточно доказать следующие два утверждения: $\forall R\in\mathbf{R}$

1) $\boldsymbol{r}(s)\neq\varnothing\ \&\ (A_\sigma,r_\sigma)\text{—}R^{\#}\!\to(A_\sigma,r_\sigma) \Rightarrow r_\sigma\neq\varnothing\ \&\ R\subseteq\cup r_\sigma$,

2) $r_\sigma\neq\varnothing\ \&\ R\subseteq\cup r_\sigma \Rightarrow \boldsymbol{r}(s)\neq\varnothing\ \&\ A_\sigma,r_\sigma)\text{—}R^{\#}\!\to(A_\sigma,r_\sigma)$.

1. Пусть $\boldsymbol{r}(s)\neq\varnothing$, $R\in\mathbf{R}$ и $(A_\sigma,r_\sigma)\text{—}R^{\#}\!\to(A_\sigma,r_\sigma)$.

   Нам нужно доказать, что $r_\sigma\neq\varnothing$ и $R\subseteq\cup r_\sigma$.

   Если $(A_\sigma,r_\sigma)\text{—}R^{\#}\!\to(A_\sigma,r_\sigma)$, то в состоянии (A_σ,r_σ) заканчивается также трасса $\sigma^{\#}\cdot\langle R^{\#}\rangle$.

   А тогда по теореме 21 (1) $(A_\sigma,r_\sigma)=(A_{\sigma\cdot\langle R\rangle},r_{\sigma\cdot\langle R\rangle})$,

   что влечет $r_\sigma=r_{\sigma\cdot\langle R\rangle}$,

   что, поскольку $\boldsymbol{Ip}(\sigma\cdot\langle R\rangle)\neq\varnothing$, влечет $r_\sigma\neq\varnothing$ и $\cup\boldsymbol{Ip}(\sigma)=\cup\boldsymbol{Ip}(\sigma\cdot\langle R\rangle)$,

   что влечет $r_\sigma=\{\cup\boldsymbol{Ip}(\sigma)\}$ и $R\subseteq\cup\boldsymbol{Ip}(\sigma)$,

   что влечет $R\subseteq\cup r_\sigma$.

2. Пусть $r_\sigma\neq\varnothing$, $R\in\mathbf{R}$ и $R\subseteq\cup r_\sigma$.

   Нам нужно доказать, что $\boldsymbol{r}(s)\neq\varnothing$ и $(A_\sigma,r_\sigma)\text{—}R^{\#}\!\to(A_\sigma,r_\sigma)$.

   Поскольку $r_\sigma\neq\varnothing$, имеем $\cup\boldsymbol{Ip}(\sigma)\neq\varnothing$ и $r_\sigma=\{\cup\boldsymbol{Ip}(\sigma)\}$.

   Тогда условие $R\subseteq\cup r_\sigma$ влечет $R\subseteq\cup\boldsymbol{Ip}(\sigma)$.

   Условие $\cup\boldsymbol{Ip}(\sigma)\neq\varnothing\ \&\ R\subseteq\cup\boldsymbol{Ip}(\sigma)$ по лемме 4 влечет $R\sim\boldsymbol{conf}\,\boldsymbol{\Sigma}\,\boldsymbol{after}\,\sigma$,

   что влечет $R\sim\boldsymbol{conf}\,(A_\sigma,r_\sigma)$,

что влечет по правилам вывода переходов ~финальной LTS

(A_σ,r_σ)—$R^\#$→(A_σ,r_σ) ***safter*** R.

Условие $R\subseteq\cup r_\sigma$ по лемме 43 влечет (A_σ,r_σ) ***safter*** $R = (A_\sigma,r_\sigma)$,

что влечет (A_σ,r_σ)—$R^\#$→(A_σ,r_σ) и $\boldsymbol{r}(s)\neq\varnothing$, что и требовалось доказать.

6.69. Доказательство теоремы 24

2. Утверждение 1.

Если простая **L**-трасса заканчивается в **L**-состоянии, то по теореме 21 (и замечанию 17) она является ~конформной **L**-трассой (принадлежит множеству $\boldsymbol{\Sigma^{\theta\sim}}$), а тогда по теореме 12 она **L**-актуальна.

Простая **L**-трасса не заканчивается в **L**-состоянии только в том случае, когда имеются только две ~финальные трассы ϵ и $\langle\gamma\rangle$, которые в этом случае **L**-актуальны.

3. Утверждение 2.

Если в исходной спецификации **S** нет безопасных трасс, то по правилам вывода имеются только два достижимых состояния γ и ϖ.

Поэтому, если s **L**-состояние, то $s\notin\{\gamma,\Delta,\Delta`,\varpi\}$ и достижимо.

А тогда в исходной спецификации **S** есть безопасные трассы, и по теореме 21 в таком состоянии s заканчивается некоторая трасса $\sigma^\#\in\boldsymbol{\Sigma^{\theta\sim}}$ и $s=(A_\sigma,r_\sigma)$.

А тогда по лемме 44 наблюдение $u^\#$ **L**-актуально после $\sigma^\#$ тогда и только тогда, когда либо

1) $u\in\mathbf{L}$ и $u\notin\cup r_\sigma$, либо

2) $u\in\mathbf{R}$ и каждая кнопка $Q\in\mathbf{Q}$ такая, что $Q\subseteq\cup r_{\sigma\cdot\langle u\rangle}$, опасна в исходной спецификации **S** в каждом множестве состояний $a\in A_{\sigma\cdot\langle u\rangle}$.

3.1. Покажем, что условие 1 эквивалентно условию $u\in\mathbf{L}$ & $u\notin\cup\boldsymbol{r}(s)$.

Это непосредственно следует из леммы 45.

3.2. Покажем, что условие 2 эквивалентно условию $u\in\mathbf{R}$ & s—$\boldsymbol{u}$↛$\Delta`$.

По определению отношения ***act*** и по лемме 42 условие 2 эквивалентно условию $u\in\mathbf{R}$ & u ***act*** (A_σ,r_σ).

3.2.1. Покажем, что для $u\in\mathbf{R}$ условие u ***act*** (A_σ,r_σ) влечет s—$\boldsymbol{u}$↛$\Delta`$.

Это непосредственно следует из правил вывода ~финальной RTS.

3.2.2. Покажем, что для $u\in\mathbf{R}$ условие s—$\boldsymbol{u}$↛$\Delta`$ влечет u ***act*** (A_σ,r_σ).

По теореме 22 из $u^\#$ ***safe***$_{\gamma\Delta}$ s следует s—$\boldsymbol{u}$↛γ.

Рассмотрим два оставшихся случая 3.2.2.1 и 3.2.2.2.

3.2.2.1. Пусть $s \xrightarrow{u} \not\to$.

Тогда по правилам вывода переходов ~финальной RTS $r_\sigma \neq \varnothing$ & $u \subseteq \cup r_\sigma$.

А тогда $\boldsymbol{Ip}(\sigma) \neq \varnothing$ & $u \subseteq \cup \boldsymbol{Ip}(\sigma)$.

А тогда по лемме 4 $u \sim \boldsymbol{conf}\ \boldsymbol{\Sigma}\ \boldsymbol{after}\ \sigma$.

Следовательно, по правилам вывода ~финальных трасс $\sigma^{\#} \cdot \langle u^{\#} \rangle \in \boldsymbol{\Sigma}^{\boldsymbol{\theta}\sim}$.

А тогда по теореме 12 трасса $\sigma^{\#} \cdot \langle u^{\#} \rangle$ **L**-актуальна,

что влечет **L**-актуальность наблюдения $u^{\#}$ после трассы $\sigma^{\#}$,

что по доказанному выше влечет $u\ \boldsymbol{act}\ (A_\sigma, r_\sigma)$.

3.2.2.2. Пусть $s \xrightarrow{u} \Delta$.

Тогда по правилам вывода переходов ~финальной RTS $u\ \boldsymbol{act}\ (A_\sigma, r_\sigma)$.

Итак в обоих случаях $u\ \boldsymbol{act}\ (A_\sigma, r_\sigma)$, что и требовалось доказать.

6.70. Доказательство теоремы 25

1. Конечность RTS-модели.

   Если число состояний исходной спецификации **S** конечно и равно n, а алфавит **L** содержит конечное число k действий, то число состояний RTS $\mathbf{S}^{\sim}$ вида (A,r) конечно и не превосходит числа $2^n(2^k+1)$, а общее число состояний – числа $4+2^n(2^k+1)$.

   В каждом состоянии RTS $\mathbf{S}^{\sim}$ вида (A,r) по каждому наблюдению $u \in \mathbf{L} \cup \mathbf{R}^{\#}$ определено не более одного перехода, а в каждом из состояний γ, Δ, $\Delta`$, ϖ определено не более одного перехода (переход по разрушению, переход по дивергенции или нет переходов).

   Если семантика конечна, то число наблюдений тоже конечно, следовательно, в каждом состоянии RTS $\mathbf{S}^{\sim}$ определено конечное число переходов, и общее число переходов во всех состояниях конечно.

2. Алгоритмическое построение за конечное время.

   Возможность алгоритмического построения RTS $\mathbf{S}^{\sim}$ непосредственно следует из правил вывода.

   Действительно, для конечной исходной LTS-спецификации и конечной семантики для каждого состояния (A,r) конечны семейство A, каждое множество $a \in A$ и множество $\cup r$.

Отсюда следует, что вычисление ***~conf*** (A,r), P ***safe~by***, (A,r) ***safter*** u и R ***act*** (A,r) можно выполнить за конечное время (для проверки (A,r) ***safter*** u в случае $u \in \mathbf{R}^{\#}$ достаточно рассматривать только такие трассы отказов ρ, в которые каждый отказ входит не более одного раза).

Следовательно, однократное применение каждого правила вывода выполняется за конечное время.

А число таких применений правил вывода конечно, поскольку конечна RTS $\mathbf{S}^{\sim}$.

3. Конечность спецификационной тройки.

Спецификационная тройка ~пополнения конечна, поскольку конечны семантика $\mathbf{R}^{\#}/\mathbf{Q}^{\#}$, RTS $\mathbf{S}^{\sim}$, а отношение $\boldsymbol{safe}_{\gamma\Delta}$, как легко показать, ограниченное на любой LTS-модели, множество $\mathbf{R}^{\#}$-трасс которой совпадает с множеством $\mathbf{R}^{\#}$-трасс RTS $\mathbf{S}^{\sim}$.

6.71. Доказательство леммы 46

Рассмотрим два возможных случая.

1. r=∅.

По правилам вывода переходов ~финальной LTS состояние вида (A,r) достижимо только в том случае, когда пустая трасса безопасна в исходной LTS-спецификации **S**.

А тогда по теореме 21 (1) в достижимом состоянии (A,r) заканчивается такая простая **L**-трасса $\sigma^{\#}$, что $(A,r)=(A_{\sigma},r_{\sigma})$.

А тогда $A_{\sigma}=\{\mathbf{S}\ \boldsymbol{after}\ \mu \mid \mu \in \boldsymbol{di}^{\sim}(\sigma) \cap \boldsymbol{SafeBy}(\Sigma)\}$.

По определению ***after*** имеем $(\mathbf{S}\ \boldsymbol{after}\ \mu)\ \boldsymbol{after}\ \epsilon = \mathbf{S}\ \boldsymbol{after}\ \mu$.

Следовательно, $A=\{\cup(x\ \boldsymbol{after}\ \epsilon) \mid x \in A\}$.

Отсюда, поскольку r=∅,

$A=\{\cup(x\ \boldsymbol{after}\ \rho) \mid x \in A\ \&\ \forall i=1..|\rho|$

$(r \neq \varnothing\ \&\ \rho(i) \subseteq \cup r\ \&\ \rho(i)\ \boldsymbol{safe\ by} \cup(x\ \boldsymbol{after}\ \rho[1..i-1]))\}$,

что и требовалось доказать.

2. r≠∅.

Поскольку состояние (A,r) достижимо, по лемме 45 $\boldsymbol{r}(a)=r$.

Следовательно, для некоторого **R**-отказа $R \subseteq \cup r$ имеется переход-петля $a \text{—} R^{\#} \rightarrow a$.

А тогда (A,r) = (A,r) ***safter*** R.

Следовательно,

$A=\{\cup(x\ \boldsymbol{after}\ \rho) \mid x \in A\ \&\ \forall i=1..|\rho|$

$(\rho(i) \subseteq \cup r \cup R\ \&\ \rho(i)\ \boldsymbol{safe\ by} \cup(x\ \boldsymbol{after}\ \rho[1..i-1]))\}$.

Отсюда, поскольку $R \subseteq \cup r$ и $r \neq \varnothing$,

$A=\{\cup(x \mathbin{\textit{after}} \rho) \mid x \in A \ \&\ \forall i=1..|\rho|$

$(r \neq \varnothing \ \&\ \rho(i) \subseteq \cup r \ \&\ \rho(i) \mathbin{\textit{safe by}} \cup(x \mathbin{\textit{after}} \rho[1..i-1]))\}$,

что и требовалось доказать.

6.72. Доказательство леммы 47

1. Покажем, что $a \mathbf{-P}\!\!\not\to \Rightarrow a -P^{\#}\!\!\to a$.

   По правилам вывода переходов ~финальной RTS, если $a \mathbf{-P}\!\!\not\to$, то **L**-состояние a имеет вид $a=(A,r)$ и $r \neq \varnothing$ & $P \subseteq \cup r$.

   Поскольку a **L**-состояние и $a=(A,r)$, по лемме 45 $r(a)=r$.

   А тогда по согласованности ~финальной RTS (теорема 21 (3)) в состоянии a нет переходов по действиям из $P \subseteq \cup r$.

   Следовательно, учитывая $a \mathbf{-P}\!\!\not\to$, по конвергентности ~финальной RTS (теорема 21 (3)) $a -P^{\#}\!\!\to b$.

   А тогда по определению ***safter***, имеем $b = (A`,r`) = a \mathbin{\textit{safter}} P$.

   Поскольку $P \subseteq \cup r$, по лемме 43 $b=a$.

   Следовательно, $a -P^{\#}\!\!\to a$, что и требовалось доказать.

2. Покажем, что $a \mathbf{-P}\!\!\not\to \Leftarrow a -P^{\#}\!\!\to a$.

   По согласованности ~финальной RTS (теорема 21 (3))

   $a -P^{\#}\!\!\to a$ влечет $a \mathbf{-P}\!\!\not\to$.

6.73. Доказательство леммы 48

Рефлексивность.

Поскольку $A \subseteq A$ & $(r \neq \varnothing \Rightarrow r \neq \varnothing)$ & $\cup r \subseteq \cup r$, имеем $(A,r) \leq (A,r)$.

Транзитивность.

Пусть $(A_1,r_1) \leq (A_2,r_2)$ и $(A_2,r_2) \leq (A_3,r_3)$.

Тогда $A_1 \subseteq A_2$ & $(r_1 \neq \varnothing \Rightarrow r_2 \neq \varnothing)$ & $\cup r_1 \subseteq \cup r_2$

и $A_2 \subseteq A_3$ & $(r_2 \neq \varnothing \Rightarrow r_3 \neq \varnothing)$ & $\cup r_2 \subseteq \cup r_3$.

А тогда $A_1 \subseteq A_3$ & $(r_1 \neq \varnothing \Rightarrow r_3 \neq \varnothing)$ & $\cup r_1 \subseteq \cup r_3$,

что влечет $(A_1,r_1) \leq (A_3,r_3)$.

6.74. Доказательство леммы 49

Пусть $a=(A,r_a)$, $b=(B,r_b)$.

По правилам вывода переходов ~финальной RTS

$a \not\xrightarrow{P} \nrightarrow$ влечет $P \in \mathbf{R}$ & P ***safe~by*** A & $r_a \neq \varnothing$ & $P \subseteq \cup r_a$.

Поскольку $a \leq b$, имеем $A \subseteq B$ & $(r_a \neq \varnothing \Rightarrow r_b \neq \varnothing)$ & $\cup r_a \subseteq \cup r_b$.

Следовательно, $r_b \neq \varnothing$ & $P \subseteq \cup r_b$.

Условие P ***safe~by*** A влечет $\forall z \in P$ z ***safe~by*** A,

что влечет $\forall z \in P$ $\exists x \in A$ z ***safe by*** x,

что, поскольку $A \subseteq B$, влечет $\forall z \in P$ $\exists x \in B$ z ***safe by*** x,

что влечет $\forall z \in P$ z ***safe~by*** B,

что влечет P ***safe~by*** B.

Итак, имеем $P \in \mathbf{R}$ & P ***safe~by*** B & $r_b \neq \varnothing$ & $P \subseteq \cup r_b$.

Отсюда по правилам вывода переходов ~финальной RTS $b \not\xrightarrow{P} \nrightarrow$.

6.75. Доказательство леммы 50

Пусть $a=(A, r_a)$, $b=(B, r_b)$.

Тогда $a \leq b$ влечет $A \subseteq B$.

По правилам вывода переходов ~финальной RTS и определению ~безопасности имеем:

1. Для $P \in \mathbf{Q}$ или $P=\varnothing \in \mathbf{R}$:

   Условие $b \not\xrightarrow{P} \gamma$ влечет P ~~***safe~by***~~ B,

   что влечет $\forall a \in B$ P ~~***safe by***~~ a,

   что, поскольку $A \subseteq B$, влечет $\forall a \in A$ P ~~***safe by***~~ a,

   что влечет P ~~***safe~by***~~ A,

   что влечет $a \not\xrightarrow{P} \gamma$.

2. Для $P \in \mathbf{R}$:

   Условие $b \not\xrightarrow{P} \gamma$ влечет P ~~***safe~by***~~ B,

   что влечет $\exists z \in P$ z ~~***safe by***~~ B,

   что влечет $\exists z \in P$ $\forall a \in B$ z ~~***safe by***~~ a,

   что, поскольку $A \subseteq B$, влечет $\exists z \in P$ $\forall a \in A$ z ~~***safe by***~~ a,

   что влечет $\exists z \in P$ z ~~***safe by***~~ A,

   что влечет P ~~***safe~by***~~ A,

   что влечет $a \not\xrightarrow{P} \gamma$.

6.76. Доказательство леммы 51

Сначала докажем, что $a \leq b$ для одного перехода по отказу.

Пусть $a \xrightarrow{P^{\#}} b$, где $P \in \mathbf{R}$ и $a=(A, r_a)$ и $b=(B, r_b)$.

По определению ***safter*** имеем

$B=\{\cup(x\ \textit{after}\ \rho)\mid x\in A\ \&\ \forall i=1..|\rho|$

$\rho(i)\subseteq\cup r\cup P\ \&\ \rho(i)\ \textit{safe by}\ \cup(x\ \textit{after}\ \rho[1..i-1])\}$

$\supseteq\ \{\cup(x\ \textit{after}\ \epsilon)\mid x\in A\}.$

По замечанию 18 (к лемме 46) $\{\cup(x\ \textit{after}\ \epsilon)\mid x\in A\}=A.$

Следовательно, $A\subseteq B$.

Также по определению ***safter*** имеем $r_b=\{\cup r_a\cup P\}\neq\varnothing$ и $\cup r_a\subseteq\cup r_b$,

что влечет $(r_a\neq\varnothing\ \Rightarrow\ r_b\neq\varnothing)\ \&\ \cup r_a\subseteq\cup r_b$.

Тем самым, $a\leq b$.

Условие $a=\rho^{\#}\Rightarrow b$ влечет наличие цепочки переходов по отказам

$a\text{—}P_1{}^{\#}\!\rightarrow a_1\text{—}P_2{}^{\#}\!\rightarrow a_2\text{—}P_3{}^{\#}\!\rightarrow\ldots a_{n-1}\text{—}P_n{}^{\#}\!\rightarrow a_n=b.$

По доказанному имеем $a\leq a_1\leq a_2\leq\ldots a_{n-1}\leq a_n=b$,

что влечет по транзитивности отношения «≤» (лемма 48) $a\leq b$.

6.77. Доказательство леммы 52

Пусть $a=(A,r_a)$, $b=(B,r_b)$, $a`=(A`,r_a`)$, $b`=(B`,r_b`)$.

Из $a\leq b$ следует $A\subseteq B$ и $(r_a\neq\varnothing\ \Rightarrow\ r_b\neq\varnothing)\ \&\ \cup r_a\subseteq\cup r_b$.

По определению ***safter*** имеем следующее.

1. Пусть $u^{\#}$ действие.

   Тогда $r_a`=r_b`=\varnothing$, поэтому $(r_a`\neq\varnothing\ \Rightarrow\ r_b`\neq\varnothing)\ \&\ \cup r_a`\subseteq\cup r_b`$.

   Также $A`=\{\cup(x\ \textit{after}\ \langle z\rangle)\mid x\in A\ \&\ z\ \textit{safe by}\ x\}$

   и $B`=\{\cup(x\ \textit{after}\ \langle z\rangle)\mid x\in B\ \&\ z\ \textit{safe by}\ x\}$.

   Поэтому условие $A\subseteq B$ влечет $A`\subseteq B`$.

2. Пусть $u^{\#}$ отказ.

   Тогда $r_a`=\{\cup r_a\cup u\}$ и $r_b`=\{\cup r_b\cup u\}$.

   Поэтому $r_b`\neq\varnothing$ и $\cup r_a\subseteq\cup r_b$ влечет $\cup r_a`\subseteq\cup r_b`$,

   что влечет $(r_a`\neq\varnothing\ \Rightarrow\ r_b`\neq\varnothing)\ \&\ \cup r_a`\subseteq\cup r_b`$.

   Также $A`=\{\cup(x\ \textit{after}\ \rho)\mid x\in A\ \&\ \forall i=1..|\rho|$

   $\rho(i)\subseteq\cup r_a\cup u\ \&\ \rho(i)\ \textit{safe by}\ \cup(x\ \textit{after}\ \rho[1..i-1])\}$

   и $B`=\{\cup(x\ \textit{after}\ \rho)\mid x\in B\ \&\ \forall i=1..|\rho|$

   $\rho(i)\subseteq\cup r_b\cup u\ \&\ \rho(i)\ \textit{safe by}\ \cup(x\ \textit{after}\ \rho[1..i-1])\}$.

Поэтому условия $A \subseteq B$ и $r_a \subseteq r_b$ влекут $A` \subseteq B`$.

Итак, в обоих случаях мы показали, что

$A` \subseteq B` \;\&\; (r_a` \neq \varnothing \Rightarrow r_b` \neq \varnothing) \;\&\; \cup r_a` \subseteq \cup r_b`$,

что влечет $a` \leq b`$, что и требовалось доказать.

6.78. Доказательство леммы 53

Пусть $a=(A, r_a)$ и $b=(B, r_b)$.

Условие $a \leq b$ влечет $A \subseteq B \;\&\; (r_a \neq \varnothing \Rightarrow r_b \neq \varnothing) \;\&\; \cup r_a \subseteq \cup r_b$.

По правилам вывода переходов ~финальной RTS,

если в $\mathbf{S}^{\sim}$ $b \text{—} u^{\#} \rightarrow$, то $u \sim_{\boldsymbol{conf}} b$.

Опираясь на определение $u \sim_{\boldsymbol{conf}} b$, рассмотрим три возможных случая.

1. $u \in \mathbf{L}$.

   Тогда u ***safe~by*** $B \;\&\; u \notin \cup r_b \;\&\; \forall x \in B \; (u$ ***safe~by*** $x \Rightarrow \cup (x$ ***after*** $\langle u \rangle) \neq \varnothing)$.

   Поскольку $A \subseteq B \;\&\; \cup r_a \subseteq \cup r_b$, имеем $u \sim_{\boldsymbol{conf}} A$, если u ***safe~by*** A.

2. $u \in \mathbf{R} \setminus \{\varnothing\}$.

   Тогда u ***safe~by*** $B \;\&\; \forall Q \in \mathbf{Q} \;\; \forall x \in B \; (Q \subseteq \cup r_b \cup u \Rightarrow Q$ ~~***safe by***~~ $x)$

   $\&\; \forall P \in \mathbf{R} \;\; \forall x \in B \; (P \subseteq \cup r_b \cup u \;\&\; P$ ***safe by*** $x \Rightarrow \cup (x$ ***after*** $\langle P \rangle) \neq \varnothing)$.

   Поскольку $A \subseteq B \;\&\; \cup r_a \subseteq \cup r_b$, имеем $u \sim_{\boldsymbol{conf}} A$, если u ***safe~by*** A.

3. $u = \varnothing \in \mathbf{R}$.

   Тогда $u \sim_{\boldsymbol{conf}} A$, если u ***safe~by*** A.

Итак, во всех случаях $u \sim_{\boldsymbol{conf}} A$, если u ***safe~by*** A.

По замечанию 15

u ***safe~by*** $A \;\Leftrightarrow\; \exists P \in \mathbf{R} \cup \mathbf{Q} \;\; (u \in P \vee u = P \;\&\; P \in \mathbf{R}) \;\&\; P$ ***safe~by*** A.

Поэтому по правилам вывода переходов ~финальной RTS

u ***safe~by*** A эквивалентно тому, что $u^{\#}$ *γ-безопасно в* a.

Тем самым, если $u^{\#}$ *γ-безопасно в* a, то $u \sim_{\boldsymbol{conf}} A$ и, следовательно, $a \text{—} u^{\#} \rightarrow$, а иначе $u^{\#}$ *γ-опасно в* a.

6.79. Доказательство леммы 54

1. Покажем, что после операции $\boldsymbol{c_1}^n$ не появляется новых **L**-состояний (достижимых состояний вида (A,r)).

   По определению операция $\boldsymbol{c_1}$ не добавляет переходов, поэтому состояние, которое достижимо после операции, было достижимым и до нее. Следовательно, состояние, являющееся **L**-состоянием после операции $\boldsymbol{c_1}$, являлось **L**-состоянием и до операции.

   Поскольку операция $\boldsymbol{c_1}^n$ определена как повторение операции $\boldsymbol{c_1}$, доказываемое свойство верно и для нее.

2. Покажем, что операция c_1^n не добавляет переходы и трассы.

   По определению операция c_1 не добавляет переходы и, следовательно, не добавляет трассы.

   Поскольку операция c_1^n определена как повторение операции c_1, она тоже не добавляет переходы и, следовательно, не добавляет трассы.

3. Покажем, что операция c_1^n не удаляет переходы-петли в остающихся **L**-состояниях, то есть состояниях вида (A,r), которые остаются достижимыми.

   По определению, если операция c_1 удаляет переход в некоторое состояние (**L**-неконвергентное), то она удаляет все переходы в это состояние. Поэтому, если **L**-состояние достижимо после операции c_1, то эта операция не удалила переходы-петли в этом состоянии.

   Поскольку операция c_1^n определена как повторение операции c_1, она тоже не удаляет переходы-петли в остающихся **L**-состояниях.

4. Покажем сохранение $\Delta\gamma$-свойства.

   Состояния γ, Δ, $\Delta`$, ϖ не имеют вида (A,r), поэтому не являются **L**-состояниями и, следовательно, **L**-конвергентны.

   Поскольку операция c_1 не удаляет переходы, ведущие в **L**-конвергентные состояния и не добавляет новых переходов, переходы, ведущие в состояния γ, Δ, $\Delta`$, ϖ, до и после операции c_1 одни и те же. Поскольку также переходы, ведущие из этих состояний, не ведут в другие состояния, эти переходы также до и после операции c_1 одни и те же. Следовательно, $\Delta\gamma$-свойство сохраняется.

   Поскольку операция c_1^n определена как повторение операции c_1, она тоже сохраняет $\Delta\gamma$-свойство.

5. Покажем, что, если выполнено $\Delta\gamma$-свойство, то операция c_1^n не удаляет переходы по не-отказам в остающихся **L**-состояниях, то есть состояниях вида (A,r), которые остаются достижимыми.

   Если выполнено $\Delta\gamma$-свойство, то переходы по не-отказам ведут только в состояния γ, Δ, $\Delta`$, которые, как сказано выше, **L**-конвергентны. Следовательно, эти переходы не удаляются операцией c_1^n.

6.80. Доказательство леммы 55

По определению $\mathbf{S}^{\sim 1}=C_1(\mathbf{S}^{\sim})$ и $c_1(C_1(\mathbf{S}^{\sim}))=C_1(\mathbf{S}^{\sim})$. Последнее возможно только в том случае, когда в $C_1(\mathbf{S}^{\sim})$ все состояния **L**-конвергентны.

6.81. Доказательство леммы 56

По лемме 54 операция c_1^n не добавляет переходы. Поэтому нарушиться могли бы только те свойства, которые требуют наличия тех или иных переходов при некоторых условиях. Такими свойствами являются свойства конвергентности, кумулятивности и полноты.

1. Конвергентность.

   Пусть состояние $s \neq \varpi$ достижимо в $c_1^n(\mathbf{S}^{\sim})$, и в нем не определены переходы по дивергенции и разрушению.

   Поскольку, по лемме 54 операция c_1^n не добавляет переходы, в состоянии s и в $\mathbf{S}^{\sim}$ не было переходов по дивергенции и разрушению.

   Следовательно по правилам вывода переходов ~финальной RTS состояние s было **L**-состоянием в ~финальной RTS.

   А тогда по лемме 47 для каждого $P \in \mathbf{R}$ в состоянии s имелся переход по не-отказу $\not\Vdash$ или переход-петля по отказу $P^{\#}$.

   По замечанию 16 в $\mathbf{S}^{\sim}$ выполнено $\Delta\gamma$-свойство.

   Поэтому по лемме 54 операция c_1^n не удаляет переходы по не-отказам, а также переходы-петли по отказам в остающихся **L**-состояниях.

   Следовательно, в состоянии s в $c_1^n(\mathbf{S}^{\sim})$ имеется переход по не-отказу $\not\Vdash$ или переход-петля по отказу $P^{\#}$.

   Тем самым, конвергентность в LTS $c_1^n(\mathbf{S}^{\sim})$ сохранится.

2. Кумулятивность.

   Это свойство требует наличия в (достижимом) состоянии s, являющемся концом перехода $s` \text{—} P^{\#} \rightarrow s$ по отказу $P^{\#}$ из достижимого состояния $s`$, перехода-петли по этому отказу $P^{\#}$ и переходов-петель по всем тем отказам, по которым такие переходы-петли определены в $s`$.

   Поскольку, по лемме 54 операция c_1^n не добавляет переходы, состояние $s`$, которое достижимо в $c_1^n(\mathbf{S}^{\sim})$, достижимо и в $\mathbf{S}^{\sim}$, где также имеется $s` \text{—} P^{\#} \rightarrow s$. Отсюда следует, что состояние s достижимо в $\mathbf{S}^{\sim}$.

   Поскольку по теореме 21 $\mathbf{S}^{\sim}$ является RTS, в ней выполнено свойство кумулятивности и, следовательно, в достижимом состоянии s был переход-петля по отказу $P^{\#}$ и переходы-петли по всем тем отказам, по которым такие переходы-петли определены в достижимом состоянии $s`$.

   По правилам вывода переходов ~финальной RTS достижимый конец перехода по отказу является **L**-состоянием.

   По лемме 54 операция c_1^n не удаляет переходы-петли в остающихся **L**-состояниях и, следовательно, сохраняются все имевшиеся переходы-петли по отказам в состоянии s.

А новых переходов-петель в состоянии s кумулятивность не требует, так как такие переходы-петли не появляются в состоянии $s`$, поскольку по лемме 54 операция c_1^n не добавляет переходы.

Следовательно, в $c_1^n(\mathbf{S}^\sim)$ в состоянии s имеются все требуемые кумулятивностью переходы-петли по отказам.

Следовательно, кумулятивность в LTS $c_1^n(\mathbf{S}^\sim)$ сохранится.

3. Полнота.

Это свойство требует наличия в достижимом состоянии s, в котором определен переход-петля по отказу $P^\#$, перехода-петли по отказу $P`^\#$ при условии отсутствия в этом состоянии переходов по действиям из $P`^\#$.

Поскольку, по лемме 54 операция c_1^n не добавляет переходы, состояние s, которое достижимо в $c_1^n(\mathbf{S}^\sim)$, достижимо и в $\mathbf{S}^\sim$, и в нем определен переход-петля по отказу $P^\#$.

По правилам вывода переходов ~финальной RTS состояние, в котором имеется переход-петля по отказу, является **L**-состоянием.

Следовательно, состояние s является **L**-состоянием в ~финальной RTS.

По замечанию 16 в $\mathbf{S}^\sim$ выполнено $\Delta\gamma$-свойство.

Поэтому по лемме 54 операция c_1^n не удаляет переходы по не-отказам в остающихся **L**-состояниях.

Следовательно, поскольку в $c_1^n(\mathbf{S}^\sim)$ в состоянии s нет перехода по не-отказу $\overline{P`}\in P`^\#$, в $\mathbf{S}^\sim$ в состоянии s тоже нет этого перехода.

А тогда по лемме 47 в состоянии s имелся в $\mathbf{S}^\sim$ переход-петля по отказу $P`^\#$.

По лемме 54 операция c_1^n не удаляет переходы-петли в остающихся **L**-состояниях.

Следовательно, в $c_1^n(\mathbf{S}^\sim)$ в состоянии s остается переход-петля по отказу $P`^\#$.

Следовательно, полнота в LTS $c_1^n(\mathbf{S}^\sim)$ сохранится.

6.82. Доказательство леммы 57

По теореме 25 RTS $\mathbf{S}^\sim$ конечна, и ее можно алгоритмически построить за конечное время.

Операция C_1, применяемая к конечной RTS $\mathbf{S}^\sim$, очевидно, заканчивается за конечное время.

По лемме 54 операция C_1 не добавляет переходы.

Поэтому RTS $\mathbf{S}^{\sim 1}$ конечна, и ее можно алгоритмически построить за конечное время.

6.83. Доказательство леммы 58

Поскольку RTS детерминирована, если состояние **L**-неконвергентно, то любая трасса, заканчивающаяся в этом состоянии **L**-неконвергентна.

Поэтому из определения операции $c_1^{\,n}$ следует, что удаляются только **L**-неконвергентные трассы.

Тем самым, $\Sigma^{01\sim}\setminus T(c_1^{\,n}(\mathbf{S}^{\sim}))\subseteq x(\Sigma^{01\sim})$.

Также очевидно, что вместе с трассой удаляются и все ее продолжения.

Тем самым, множество $\Sigma^{01\sim}\setminus T(c_1^{\,n}(\mathbf{S}^{\sim}))$ удаляемых трасс является постфикс-замкнутым подмножеством множества $\Sigma^{01\sim}$.

По правилам вывода переходов ~финальной RTS (или по теореме 21 и замечанию 17) простая трасса ~финальной RTS, не являющаяся **L**-трассой, имеет вид $\sigma^{\#}\cdot\langle\text{Ꝑ}\rangle$, $\sigma^{\#}\cdot\langle\text{Ꝑ},\gamma\rangle$ или $\sigma^{\#}\cdot\langle\text{Ꝑ},\Delta\rangle$, где трасса $\sigma^{\#}$ заканчивается в **L**-состоянии.

По замечанию 16 в $\mathbf{S}^{\sim}$ выполнено $\Delta\gamma$-свойство.

Поэтому по лемме 54 операция $c_1^{\,n}$ не удаляет переходы по не-отказам в остающихся **L**-состояниях.

Поскольку состояния γ, Δ, $\Delta`$, ϖ **L**-конвергентны, любая из трасс $\sigma^{\#}\cdot\langle\text{Ꝑ}\rangle$, $\sigma^{\#}\cdot\langle\text{Ꝑ},\gamma\rangle$ или $\sigma^{\#}\cdot\langle\text{Ꝑ},\Delta\rangle$ удаляется только в том случае, когда удаляется трасса $\sigma^{\#}$.

Следовательно, множество $\Sigma^{01\sim}\setminus T(c_1^{\,n}(\mathbf{S}^{\sim}))$ удаляемых трасс вместе с каждой трассой содержит ее максимальный **L**-префикс (максимальный префикс, являющийся **L**-трассой).

6.84. Доказательство леммы 59

По лемме 47 это свойство выполнено для RTS $\mathbf{S}^{\sim}$.

По лемме 54 все **L**-состояния RTS $c_1^{\,n}(\mathbf{S}^{\sim})$ являются **L**-состояниями RTS $\mathbf{S}^{\sim}$.

По замечанию 16 в $\mathbf{S}^{\sim}$ выполнено $\Delta\gamma$-свойство.

Поэтому по лемме 54 операция $c_1^{\,n}$ не удаляет переходы по не-отказам, а также переходы-петли по отказам в достижимых **L**-состояниях, и не добавляет переходы, в том числе, переходы по не-отказам и переходы-петли по отказам.

Следовательно, требуемое свойство сохраняется для RTS $c_1^{\,n}(\mathbf{S}^{\sim})$.

6.85. Доказательство леммы 60

По лемме 49 это свойство выполнено для RTS $\mathbf{S}^{\sim}$.

По лемме 54 все **L**-состояния RTS $c_1^{\,n}(\mathbf{S}^{\sim})$ являются **L**-состояниями RTS $\mathbf{S}^{\sim}$.

По замечанию 16 в $\mathbf{S}^{\sim}$ выполнено $\Delta\gamma$-свойство.

Поэтому по лемме 54 операция c_1^n не удаляет переходы по не-отказам, а также не добавляет такие переходы.

Следовательно, требуемое свойство сохраняется для RTS $c_1^n(\mathbf{S}^\sim)$.

6.86. Доказательство леммы 61

По лемме 50 это свойство выполнено для RTS $\mathbf{S}^\sim$.

По лемме 54 все **L**-состояния RTS $c_1^n(\mathbf{S}^\sim)$ являются **L**-состояниями RTS $\mathbf{S}^\sim$.

По замечанию 16 в $\mathbf{S}^\sim$ выполнено $\Delta\gamma$-свойство.

Поэтому по лемме 54 операция c_1^n не удаляет переходы по не-отказам, а также не добавляет такие переходы.

Следовательно, требуемое свойство сохраняется для RTS $c_1^n(\mathbf{S}^\sim)$.

6.87. Доказательство леммы 62

По лемме 51 это свойство выполнено для RTS $\mathbf{S}^\sim$.

По лемме 54 все **L**-состояния RTS $c_1^n(\mathbf{S}^\sim)$ являются **L**-состояниями RTS $\mathbf{S}^\sim$.

Также по лемме 54 операция c_1^n не добавляет трассы.

Следовательно, требуемое свойство сохраняется для RTS $c_1^n(\mathbf{S}^\sim)$.

6.88. Доказательство леммы 63

По лемме 52 это свойство выполнено для RTS $\mathbf{S}^\sim$.

По лемме 54 все **L**-состояния RTS $c_1^n(\mathbf{S}^\sim)$ являются **L**-состояниями RTS $\mathbf{S}^\sim$.

Также по лемме 54 операция c_1^n не добавляет переходы.

Следовательно, требуемое свойство сохраняется для RTS $c_1^n(\mathbf{S}^\sim)$.

6.89. Доказательство леммы 64

Будем вести доказательство индукцией по n.

Для $n=0$ имеем $c_1^0(\mathbf{S}^\sim)=\mathbf{S}^\sim$, и утверждение верно по лемме 53.

Пусть утверждение доказано для n и докажем его для $n+1$.

Допустим противное.

Тогда в RTS $c_1^{n+1}(\mathbf{S}^\sim)$ $b \text{—} u^{\#} \to b'$ & $a \le b$ & $u^{\#}$ *γ-безопасно в* a & $a \text{—} u^{\#} \not\to$.

По лемме 54 все **L**-состояния RTS $c_1^{n+1}(\mathbf{S}^\sim)$ являются **L**-состояниями RTS $c_1^n(\mathbf{S}^\sim)$, следовательно, состояния a, b и b' являются **L**-состояниями в $c_1^n(\mathbf{S}^\sim)$.

Поскольку по лемме 54 операция c_1 не добавляет переходы, в RTS $c_1^n(\tilde{S})$ также имеется переход $b—u^\#→b`$.

Итак, в $c_1^n(\tilde{S})$ a и b являются **L**-состояниями, $a≤b$, $b—u`^\#→$.

Следовательно, по предположению шага индукции в RTS $c_1^n(\tilde{S})$ имеем

$u^\#$ *γ-опасно в* a ∨ $a—u^\#→a`$.

Поскольку по лемме 54 операция c_1 не удаляет переходы по не-отказам из остающихся **L**-состояний, из того, что в RTS $c_1^{n+1}(\tilde{S})$ наблюдение $u^\#$ *γ-безопасно в* a, следует, что в RTS $c_1^n(\tilde{S})$ также наблюдение $u^\#$ *γ-безопасно в* a.

Следовательно, в RTS $c_1^n(\tilde{S})$ имеется переход $a—u^\#→a`$, и $a`$ является **L**-состоянием в $c_1^n(\tilde{S})$.

Поскольку перехода $a—u^\#→a`$ нет в RTS $c_1^{n+1}(\tilde{S})$, он удаляется операцией $c_1$. Следовательно, состояние $a`$ **L**-неконвергентно в $c_1^n(\tilde{S})$, а тогда оно P-неконвергентно для некоторой кнопки $P∈\mathbf{R}∪\mathbf{Q}$.

Тогда $a`—\not{P}↛γ$.

Из $a≤b$, $b—u^\#→b`$ и $a—u^\#→a`$ следует по лемме 62 $a`≤b`$.

Поскольку $a`$ и $b`$ являются **L**-состояниями в $c_1^n(\tilde{S})$ и $a`—\not{P}↛γ$, по лемме 60 $b`—\not{P}↛γ$.

Поскольку в RTS $c_1^{n+1}(\tilde{S})$ имеется переход $b—u^\#→b`$, состояние $b`$ должно быть **L**-конвергентным, в том числе, P-конвергентным в $c_1^n(\tilde{S})$.

Поэтому найдется такое наблюдение $u`^\#$, разрешаемое кнопкой $P^\#$, что $b`—u`^\#→$.

Итак, в $c_1^n(\tilde{S})$ $a`$ и $b`$ являются **L**-состояниями, $a`≤b`$, $b`—u`^\#→$.

Следовательно, по предположению шага индукции в $c_1^n(\tilde{S})$

$u`^\#$ *γ-опасно в* $a`$ ∨ $a`—u`^\#→$.

Поскольку $a`—\not{P}↛γ$, имеем $u`^\#$ *γ-безопасно в* $a`$. Следовательно, $a`—u`^\#→$, что противоречит $P$-неконвергентности состояния $a`$ в $c_1^n(\tilde{S})$.

Мы пришли к противоречию, следовательно, наше допущение не верно, шаг индукции доказан, и лемма доказана.

6.90. Доказательство леммы 65

1. Покажем, что если в $\mathbf{S^{-1}}$ отказ $P^{\#}$ особый после трассы $\mu^{\#}$, то трасса $\mu^{\#}$ заканчивается в **L**-состоянии, в котором есть переход-петля или особый переход по отказу $P^{\#}$.

   По определению, если отказ $P^{\#}$ особый после трассы $\mu^{\#}$, то выполнено следующее условие:

   $P\in\mathbf{R}\ \&\ \boldsymbol{Ip}(\mu)\neq\varnothing\ \&\ \mu^{\#}\cdot\langle \not{R}, \gamma\rangle\notin \boldsymbol{T}(\mathbf{S^{-1}})\ \&\ \forall z\in P\ \ \mu^{\#}\cdot\langle z\rangle\notin \boldsymbol{T}(\mathbf{S^{-1}})$.

   Если трасса $\mu^{\#}$ заканчивается в состоянии s, то, во-первых, это **L**-состояние, а во-вторых, подусловие $\boldsymbol{Ip}(\mu)\neq\varnothing$, учитывая свойство кумулятивности RTS $\mathbf{S^{-1}}$ (лемма 56), эквивалентно подусловию $\exists P_s\in\mathbf{R}\ \ s\text{—}P_s^{\#}\!\to s$.

   Подусловие $\mu^{\#}\cdot\langle \not{R}, \gamma\rangle\notin \boldsymbol{T}(\mathbf{S^{-1}})$ влечет $s\text{—}\not{R}\!\!\rightarrow\gamma$.

   Подусловие $\forall z\in P\ \ \mu^{\#}\cdot\langle z\rangle\notin \boldsymbol{T}(\mathbf{S^{-1}})$ влечет $\forall z\in P\ \ s\text{—}z\!\!\rightarrow$.

   А тогда, поскольку все **L**-состояния RTS $\mathbf{S^{-1}}$ **L**-конвергентны (лемма 55), должно быть $s\text{—}P^{\#}\!\to s'$ для некоторого состояния s'.

   В целом получаем:

   $P\in\mathbf{R}\ \&\ \exists P_s\in\mathbf{R}\ \ s\text{—}P_s^{\#}\!\to s\ \&\ s\text{—}P^{\#}\!\to s'\ \&\ \forall z\in P\ \ s\text{—}z\!\!\rightarrow$.

   Переход $s\text{—}P^{\#}\!\to s'$ является переходом-петлей, если $s'=s$, и особым переходом в противном случае, что и требовалось доказать.

2. Покажем, что если в $\mathbf{S^{-1}}$ трасса $\mu^{\#}$ заканчивается в **L**-состоянии s, в котором есть переход-петля $s\text{—}P^{\#}\!\to s$ или особый переход $s\text{—}P^{\#}\!\to s'$ по отказу $P^{\#}$, то отказ $P^{\#}$ особый после трассы $\mu^{\#}$.

   Поскольку s **L**-состояние, оно имеет вид $s=(A,r)$.

   Поскольку трасса $\mu^{\#}$ заканчивается в **L**-состоянии s, пустая трасса безопасна в исходной спецификации (иначе нет **L**-состояний) и по теореме 21 имеем $(A,r)=(A_\mu,r_\mu)$ и $r=r_\mu=\{\cup\boldsymbol{Ip}(\mu)\mid\boldsymbol{Ip}(\mu)\neq\varnothing\}$.

   Рассмотрим два возможных случая.

2.1. Имеется переход-петля $s\text{—}P^{\#}\!\to s$.

   В этом случае в RTS $\mathbf{S^{-1}}$ имеет место $\boldsymbol{r}(s)\neq\varnothing$.

   Поскольку по лемме 54 операция $\boldsymbol{C_1}$ не удаляет и не добавляет переходы-петли по отказам в остающихся **L**-состояниях, в RTS $\mathbf{S^{\sim}}$ имеет место $\boldsymbol{r}(s)\neq\varnothing$.

А тогда, поскольку по лемме 45 $\boldsymbol{r}(s)=r$ в RTS $\mathbf{S}^{\sim}$, условие $\boldsymbol{r}(s)\neq\varnothing$ влечет $\boldsymbol{Ip}(\mu)\neq\varnothing$.

По свойству согласованности RTS $\mathbf{S}^{\sim\mathbf{1}}$ (лемма 56) имеем:

$s\text{—}\not{P}\!\!\rightarrow$ и $\forall z\in P\ \ s\text{—}z\!\!\rightarrow$.

Условие $s\text{—}\not{P}\!\!\rightarrow$ влечет $\mu^{\#}\cdot\langle\not{P},\gamma\rangle\notin\boldsymbol{T}(\mathbf{S}^{\sim\mathbf{1}})$.

Условие $\forall z\in P\ \ s\text{—}z\!\!\rightarrow$ влечет $\forall z\in P\ \ \mu^{\#}\cdot\langle z\rangle\notin\boldsymbol{T}(\mathbf{S}^{\sim\mathbf{1}})$.

Итак, имеем:

$P\in\mathbf{R}\ \&\ \boldsymbol{Ip}(\mu)\neq\varnothing\ \&\ \mu^{\#}\cdot\langle\not{P},\gamma\rangle\notin\boldsymbol{T}(\mathbf{S}^{\sim\mathbf{1}})\ \&\ \forall z\in P\ \ \mu^{\#}\cdot\langle z\rangle\notin\boldsymbol{T}(\mathbf{S}^{\sim\mathbf{1}})$,

что означает, что отказ $P^{\#}$ особый после трассы $\mu^{\#}$, что и требовалось доказать.

2.2. Имеется особый переход $s\text{—}P^{\#}\!\!\rightarrow s`$.

По определению особого перехода имеем:

$s`\neq s\ \&\ \exists P_s\in\mathbf{R}\ \ s\text{—}P_s{}^{\#}\!\!\rightarrow s\ \&\ \forall z\in P\ \ s\text{—}z\!\!\rightarrow$.

Условие $\exists P_s\in\mathbf{R}\ \ s\text{—}P_s{}^{\#}\!\!\rightarrow s$ влечет $\boldsymbol{r}(s)\neq\varnothing$ в RTS $\mathbf{S}^{\sim\mathbf{1}}$.

Поскольку по лемме 54 операция $\boldsymbol{C_1}$ не удаляет и не добавляет переходы-петли по отказам в остающихся **L**-состояниях, $\boldsymbol{r}(s)\neq\varnothing$ в RTS $\mathbf{S}^{\sim}$.

А тогда, поскольку по лемме 45 $\boldsymbol{r}(s)=r$ в RTS $\mathbf{S}^{\sim}$, условие $\boldsymbol{r}(s)\neq\varnothing$ влечет $\boldsymbol{Ip}(\mu)\neq\varnothing$.

Поскольку $s\text{—}P^{\#}\!\!\rightarrow s`$, имеем $\mu^{\#}\cdot\langle P^{\#}\rangle\in\boldsymbol{T}(\mathbf{S}^{\sim\mathbf{1}})$.

Тогда по лемме 54 $\mu^{\#}\cdot\langle P^{\#}\rangle\in\boldsymbol{T}(\mathbf{S}^{\sim})$,

что по правилам вывода ~финальных трасс влечет $P\sim\boldsymbol{conf}\ (A_{\mu},r_{\mu})$,

что влечет $P\ \boldsymbol{safe\sim by}\ A_{\mu}$, что влечет $\mu^{\#}\cdot\langle\not{P},\gamma\rangle\notin\boldsymbol{T}(\mathbf{S}^{\sim})$.

А тогда по лемме 54 $\mu^{\#}\cdot\langle\not{P},\gamma\rangle\notin\boldsymbol{T}(\mathbf{S}^{\sim\mathbf{1}})$.

Условие $\forall z\in P\ \ s\text{—}z\!\!\rightarrow$ влечет $\forall z\in P\ \ \mu^{\#}\cdot\langle z\rangle\notin\boldsymbol{T}(\mathbf{S}^{\sim\mathbf{1}})$.

Итак, имеем:

$P\in\mathbf{R}\ \&\ \boldsymbol{Ip}(\mu)\neq\varnothing\ \&\ \mu^{\#}\cdot\langle\not{P},\gamma\rangle\notin\boldsymbol{T}(\mathbf{S}^{\sim\mathbf{1}})\ \&\ \forall z\in P\ \ \mu^{\#}\cdot\langle z\rangle\notin\boldsymbol{T}(\mathbf{S}^{\sim\mathbf{1}})$,

что означает, что отказ $P^{\#}$ особый после трассы $\mu^{\#}$, что и требовалось доказать.

6.91. Доказательство леммы 66

Очевидно, что любая особая трасса, начинающаяся в **L**-состоянии, заканчивается тоже в **L**-состоянии, в том числе и максимальная особая. Нам

нужно доказать, что такие максимальные особые трассы заканчиваются в одном и том же состоянии.

Допустим, утверждение не верно.

Тогда найдется такая трасса $\mu^{\#}$, которая в $\mathbf{S}^{\sim 1}$ заканчивается в **L**-состоянии s, в котором начинаются две максимальные особые трассы, заканчивающиеся в $\mathbf{S}^{\sim 1}$ в разных состояниях.

Назовем *состоянием ветвления* такое состояние, которое достижимо из состояния s по особым трассам, и такое, что через него проходят по крайней мере две максимальные особые трассы, начинающиеся в s и заканчивающиеся в разных состояниях.

Такое состояние ветвления, по-первых, всегда существует, поскольку им является само состояние s, и, во-вторых, является **L**-состоянием.

Рангом состояния ветвления назовем максимальную длину особой трассы, начинающейся в s и заканчивающейся в данном состоянии ветвления.

Ранг состояния ветвления конечен, так как по лемме 57 конечна RTS $\mathbf{S}^{\sim 1}$, а особая трасса не может содержать циклов (в RTS цикл переходов по отказам может состоять только из переходов-петель, а они не являются особыми переходами).

Среди всех состояний ветвления выберем состояние $s`$ с максимальным рангом и особую трассу $\pi_1^{\#}$, начинающуюся в $s$, заканчивающуюся в $s`$ и имеющую этот максимальный ранг.

Поскольку любую особую трассу можно продолжить до максимальной, продолжим трассу $\pi_1^{\#}$ до такой максимальной особой трассы $\rho_1^{\#}$, то есть $\pi_1^{\#} \le \rho_1^{\#}$.

Тогда найдется максимальная особая трасса $\rho_2^{\#}$, которая проходит через состояние $s`$, то есть у нее имеется префикс $\pi_2^{\#} \le \rho_2^{\#}$, который заканчивается в $s`$, и трассы $\rho_1^{\#}$ и $\rho_2^{\#}$ заканчиваются в разных состояниях.

Поскольку $\rho_1^{\#}$ и $\rho_2^{\#}$ максимальные особые трассы и заканчиваются в разных состояниях, ни одна из них не может заканчиваться в состоянии $s`$.

Следовательно, $\pi_1^{\#} < \rho_1^{\#}$ и $\pi_2^{\#} < \rho_2^{\#}$, и существуют следующие после этих префиксов отказы: $\pi_1^{\#} \cdot \langle \mathsf{P}_1^{\#} \rangle \le \rho_1^{\#}$ и $\pi_2^{\#} \cdot \langle \mathsf{P}_2^{\#} \rangle \le \rho_2^{\#}$ такие, что переходы $s` \text{—} \mathsf{P}_1^{\#} \to s_1$ и $s` \text{—} \mathsf{P}_2^{\#} \to s_2$ особые.

Поскольку ранг состояния $s`$ максимальный, должно быть $s_1 \ne s_2$, так как в противном случае состояние $s_1 = s_2$ было бы состоянием ветвления с рангом большим, чем у $s`$, что противоречит максимальности ранга $s`$.

По лемме 54 в $\mathbf{S}^{\sim}$ тоже имеется трасса $\mu^{\#}\cdot\pi_1{}^{\#}$, которая тоже заканчивается в состоянии s_1, и тоже имеются переходы $s\,`\!\!-\!\!-\!P_1{}^{\#}\!\!\rightarrow s_1$ и $s\,`\!\!-\!\!-\!P_2{}^{\#}\!\!\rightarrow s_2$.

Тогда по теореме 21 трассы $\mu^{\#}\cdot\pi_1{}^{\#}\cdot\langle P_1{}^{\#}\rangle$ и $\mu^{\#}\cdot\pi_1{}^{\#}\cdot\langle P_2{}^{\#}\rangle$ ~финальны и являются **L**-трассами.

Тогда, по теореме 11 трасса $\mu^{\#}\cdot\pi_1{}^{\#}\cdot\langle P_2{}^{\#}\rangle$ безопасна.

Тогда $P_2{}^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{\Sigma}^{\sim}$ ***after*** $\mu^{\#}\cdot\pi_1{}^{\#}$.
Тогда по лемме 16 о безопасности после отказа
$P_2{}^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{\Sigma}^{\sim}$ ***after*** $\mu^{\#}\cdot\pi_1{}^{\#}\cdot\langle P_1{}^{\#}\rangle$.

Тогда по теореме 10 о безопасности кнопок $\mu^{\#}\cdot\pi_1{}^{\#}\cdot\langle P_1{}^{\#}\rangle\cdot\langle\not{P}_2,\gamma\rangle\notin\mathbf{\Sigma}^{1\sim}$.

Тогда по теореме 21 в $\mathbf{S}^{\sim}$ $s_1\!\!-\!\!-\!\not{P}_2\!\!\rightarrow\!\!\!\!\!\!\diagup\;\gamma$.

Покажем, что в $\mathbf{S}^{\sim}$ $s_1\!\!-\!\!-\!z\!\!\rightarrow\!\!\!\!\!\!\diagup$ для любого действия $z\in P_2$.

> Действительно, в противном случае по теореме 21 трасса $\mu^{\#}\cdot\pi_1{}^{\#}\cdot\langle P_1{}^{\#}\rangle$ продолжалась бы во множестве ~финальных трасс некоторым действием $z\in P_2$.
>
> А тогда $\mu^{\#}\cdot\pi_1{}^{\#}\cdot\langle z\rangle\in\cup\boldsymbol{d}(\mathbf{\Sigma}^{01\sim})$.
>
> Если бы $\mu^{\#}\cdot\pi_1{}^{\#}\cdot\langle z\rangle\notin\mathbf{\Sigma}^{01\sim}$, то по лемме 13 о безопасности **L**-наблюдений было бы $z^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{\Sigma}^{\sim}$ ***after*** $\mu^{\#}\cdot\pi_1{}^{\#}$.
> Но это противоречит тому, что $z\in P_2$ и $P_2{}^{\#}$ ***safe***$_{\gamma\Delta}$ $\mathbf{\Sigma}^{\sim}$ ***after*** $\mu^{\#}\cdot\pi_1{}^{\#}$.
> Следовательно, $\mu^{\#}\cdot\pi_1{}^{\#}\cdot\langle z\rangle\in\mathbf{\Sigma}^{01\sim}$.
>
> Но тогда по теореме 21 имеется переход $s\,`\!\!-\!\!-\!z\!\!\rightarrow$, что противоречит тому, что переход $s\,`\!\!-\!\!-\!P_2{}^{\#}\!\!\rightarrow s_2$ особый.

Итак, в $\mathbf{S}^{\sim}$ $s_1\!\!-\!\!-\!\not{P}_2\!\!\rightarrow\!\!\!\!\!\!\diagup\;\gamma$ и $s_1\!\!-\!\!-\!z\!\!\rightarrow\!\!\!\!\!\!\diagup$ для любого действия $z\in P_2$.
Тогда по лемме 54 это имеет место и в $\mathbf{S}^{\sim 1}$.

Если бы $s_1\!\!-\!\!-\!P_2{}^{\#}\!\!\rightarrow\!\!\!\!\!\!\diagup$, состояние s_1 было бы **L**-неконвергентно в $\mathbf{S}^{\sim 1}$,
чего быть не может по лемме 55.
Следовательно, в $\mathbf{S}^{\sim 1}$ $s_1\!\!-\!\!-\!P_2{}^{\#}\!\!\rightarrow s_{12}$ и этот переход особый.

В силу симметрии аналогично показывается, что в $\mathbf{S}^{\sim 1}$ $s_2\!\!-\!\!-\!P_1{}^{\#}\!\!\rightarrow s_{21}$ и этот переход особый.
Тогда по лемме 54 в $\mathbf{S}^{\sim}$ тоже $s_1\!\!-\!\!-\!P_2{}^{\#}\!\!\rightarrow s_{12}$ и $s_2\!\!-\!\!-\!P_1{}^{\#}\!\!\rightarrow s_{21}$.

Итак, в $\mathbf{S}^{\sim}$ имеем: $s\,`\!\!-\!\!-\!P_1{}^{\#}\!\!\rightarrow s_1\!\!-\!\!-\!P_2{}^{\#}\!\!\rightarrow s_{12}$ и $s\,`\!\!-\!\!-\!P_2{}^{\#}\!\!\rightarrow s_2\!\!-\!\!-\!P_1{}^{\#}\!\!\rightarrow s_{21}$.

Поскольку в $\mathbf{S^{\sim 1}}$ трасса $\mu^{\#}$ заканчивается в **L**-состоянии s, а трасса $\pi_1{}^{\#}$ начинается в s и заканчивается в $s`$, трасса $\mu^{\#}\cdot\pi_1{}^{\#}$, начинающаяся в начальном состоянии, заканчивается в $s`$, а трассы $\sigma=\mu\cdot\pi_1\cdot\langle P_1, P_2\rangle$ и $\sigma`=\mu\cdot\pi_1\cdot\langle P_2, P_1\rangle$ заканчиваются в состояниях s_{12} и s_{21}, соответственно.

Тогда по теореме 21 $s_{12}=(A_\sigma,r_\sigma)$ и $s_{21}=(A_{\sigma`},r_{\sigma`})$. Далее:

$A_\sigma=\{\mathbf{S}\ \textit{after}\ \lambda\,|\,\lambda\in \textit{di}^{\sim}(\sigma)\cap \textit{SafeBy}(F(\mathbf{S^{\sim 1}}))\}$,

$A_{\sigma`}=\{\mathbf{S}\ \textit{after}\ \lambda\,|\,\lambda\in \textit{di}^{\sim}(\sigma`)\cap \textit{SafeBy}(F(\mathbf{S^{\sim 1}}))\}$,

$r_\sigma=\{\cup \textit{Ip}(\sigma)\,|\,\textit{Ip}(\sigma)\neq\varnothing\}$,

$r_{\sigma`}=\{\cup \textit{Ip}(\sigma`)\,|\,\textit{Ip}(\sigma)\neq\varnothing\}$.

Но, очевидно, $\textit{di}^{\sim}(\sigma)=\textit{di}^{\sim}(\sigma`)$ и $\textit{Ip}(\sigma)=\textit{Ip}(\sigma`)$.

Поэтому $s_{12}=s_{21}$.

Но тогда в состоянии $s_{12}=s_{21}$ в $\mathbf{S^{\sim 1}}$ заканчиваются две особые трассы $\pi_1{}^{\#}\cdot\langle P_1{}^{\#}\rangle\cdot\langle P_2{}^{\#}\rangle$ и $\pi_1{}^{\#}\cdot\langle P_2{}^{\#}\rangle\cdot\langle P_1{}^{\#}\rangle$.

Продолжим эти особые трассы до максимальных: $\pi_1{}^{\#}\cdot\langle P_1{}^{\#}\rangle\cdot\langle P_2{}^{\#}\rangle\le\rho_3{}^{\#}$ и $\pi_1{}^{\#}\cdot\langle P_2{}^{\#}\rangle\cdot\langle P_1{}^{\#}\rangle\le\rho_4{}^{\#}$.

Если бы трассы $\rho_1{}^{\#}$ и $\rho_3{}^{\#}$ заканчивались в $\mathbf{S^{\sim 1}}$ в разных состояниях, то состояние s_1 было бы состоянием ветвления, но его ранг больше ранга состояния $s`$, чего быть не может.

Если бы трассы $\rho_3{}^{\#}$ и $\rho_4{}^{\#}$ заканчивались в $\mathbf{S^{\sim 1}}$ в разных состояниях, то состояние $s_{12}=s_{21}$ было бы состоянием ветвления, но его ранг больше ранга состояния $s`$, чего быть не может.

Если бы трассы $\rho_2{}^{\#}$ и $\rho_4{}^{\#}$ заканчивались в $\mathbf{S^{\sim 1}}$ в разных состояниях, то состояние s_2 было бы состоянием ветвления, но его ранг больше ранга состояния $s`$, чего быть не может.

Но тогда получается, что трассы $\rho_1{}^{\#}$ и $\rho_2{}^{\#}$ заканчиваются в одном состоянии, что тоже не верно.

Мы пришли к противоречию и, следовательно, наше допущение не верно, и утверждение леммы доказано.

6.92. Доказательство леммы 67

1. Покажем, что в состоянии b в $\mathbf{S^{\sim 1}}$ нет особых переходов

   Начальным состоянием RTS $\mathbf{S}^{\nabla}$ является пара $(s^{\sim}_0, s^{\sim}_0)$, где $s^{\sim}_0$ – начальное состояние $\mathbf{S}^{\sim}$.

По определению ~финальной RTS $s\tilde{}_0=(\{\{\mathbf{S}\ \textit{after}\ \epsilon\}\},\varnothing)$.

А по определению ***safter*** в этом случае в состоянии $s\tilde{}_0$ в $\mathbf{S}\tilde{}$ нет переходов-петель по отказам.

Тем самым, в этом состоянии в $\mathbf{S}\tilde{}$ нет особых переходов.

Поскольку по лемме 54 операция C_1 не добавляет переходы, в $\mathbf{S}\tilde{}^{-1}$ в состоянии $s\tilde{}_0$ также нет переходов-петель по отказам и, следовательно, нет особых переходов.

По рефлексивности отношения «≤» (лемма 48) $s\tilde{}_0 \le s\tilde{}_0$.

Для любого другого достижимого в $\mathbf{S}^{\nabla}$ состояния (a,b) в состоянии b в $\mathbf{S}\tilde{}^{-1}$ нет особых переходов по определению (в b заканчивается максимальная трасса особых переходов).

2. Покажем, что $a \le b$.

   Это легко доказывается индукцией по маршруту, ведущему в достижимое состояние из начального состояния.

   База индукции: $s\tilde{}_0 \le s\tilde{}_0$, что доказано выше.

   Доказательство шага индукции непосредственно следует из леммы 63.

6.93. Доказательство леммы 68

Пусть состояние (a,b) достижимо.

Тогда по лемме 67 $a \le b$.

1. Пусть выполнено условие правила **1a**:

   $u^{\#}$ *γ-безопасно в* a & $b — u^{\#} \to b_u$ & $b_u = \rho \Rightarrow b`$ & ρ *максимальная особая в* b_u.

   Тогда по лемме 64 $a — u^{\#} \to a`$.

   Следовательно, выполнено условие правила **1**:

   $a — u^{\#} \to a`$ & $b — u^{\#} \to b_u$ & $b_u = \rho \Rightarrow b`$ & ρ *максимальная особая в* b_u.

2. Наоборот, пусть выполнено условие правила **1**:

   $a — u^{\#} \to a`$ & $b — u^{\#} \to b_u$ & $b_u = \rho \Rightarrow b`$ & ρ *максимальная особая в* b_u.

   Тогда по правилам вывода переходов ~финальной RTS $u^{\#}$ *γ-безопасно в* a.
   Следовательно, выполнено условие правила **1a**:

   $u^{\#}$ *γ-безопасно в* a & $b — u^{\#} \to b_u$ & $b_u = \rho \Rightarrow b`$ & ρ *максимальная особая в* b_u.

6.94. Доказательство леммы 69

1. Сначала покажем, что в $\mathbf{S}^{\nabla}$ каждое **L**-состояние (a,b) **L**-конвергентно.

Допустим противное: некоторая кнопка $P^{\#}$ *γ-безопасна в* (a,b), то есть $(a,b)\text{—}\not{P}\!\!\rightarrow\gamma$, но $\forall u\in P\cup\{P\}\ (a,b)\text{—}u^{\#}\!\!\rightarrow$.

Тогда по правилу вывода **2** $a\text{—}\not{P}\!\!\rightarrow\gamma$.

Тогда $\forall u\in P\cup\{P\}\ u^{\#}$ *γ-безопасно в* a.
Следовательно, используя лемму 68,

по правилу вывода **1a** $\forall u\in P\cup\{P\}\ b\text{—}u^{\#}\!\!\rightarrow$.

Поскольку $a\text{—}\not{P}\!\!\rightarrow\gamma$ и по лемме 67 $a\le b$, имеем по лемме 61 $b\text{—}\not{P}\!\!\rightarrow\gamma$.

А тогда в $\mathbf{S}^{\sim 1}$ достижимое состояние b **L**-неконвергентно, что неверно для рассматриваемого случая, когда начальное состояние RTS $\mathbf{S}^{\sim 1}$ **L**-конвергентно.
Мы пришли к противоречию, и, следовательно, наше допущение не верно, а утверждение леммы верно.

2. Теперь покажем, что в $\mathbf{S}^{\nabla}$ все простые **L**-трассы **L**-конвергентны.

   Простая **L**-трасса $\mu^{\#}$ заканчивается в состоянии вида (a,b), которое по доказанному **L**-конвергентно:

   $\forall P\in\mathbf{R}\cup\mathbf{Q}\ (a,b)\text{—}\not{P}\!\!\rightarrow\gamma\ \vee\ \exists u\in P\cup\{P\}\ (a,b)\text{—}u^{\#}\!\!\rightarrow$.

   Следовательно,

   $\forall P\in\mathbf{R}\cup\mathbf{Q}\ \mu^{\#}\cdot\langle\not{P},\gamma\rangle\in\boldsymbol{T}(\mathbf{S}^{\nabla})\ \vee\ \exists u\in P\cup\{P\}\ \mu^{\#}\cdot\langle u^{\#}\rangle\in\boldsymbol{T}(\mathbf{S}^{\nabla})$,

   что и означает **L**-конвергентность трассы $\mu^{\#}$.

6.95. Доказательство леммы 70

1. Детерминизм.
   LTS $\mathbf{S}^{\nabla}$ детерминирована по правилам вывода и лемме 66.
2. Алфавит.
   LTS $\mathbf{S}^{\nabla}$ определена в алфавите $\mathbf{L}^{+}\cup\mathbf{R}^{\#}\cup\{\Delta\}$.
3. Выделенное состояние ϖ.
   В LTS $\mathbf{S}^{\nabla}$ имеется состояние ϖ по определению.
4. Допустимость следует из правил вывода.
5. Согласованность.
   Пусть в состоянии определен переход-петля по $\mathbf{R}^{\#}$-отказу $(a,b)\text{—}P^{\#}\!\!\rightarrow(a,b)$.

Тогда в этом состоянии нет переходов по разрушению и дивергенции по замечанию 19, поскольку такие переходы ведут только из состояний γ, Δ или $\Delta`$.

По правилам вывода имеем $a \text{—} P^{\#} \rightarrow a$.

А тогда по согласованности $\mathbf{S}^{\sim 1}$ (лемма 56) в a нет действий из $P^{\#}$,

что по правилам вывода влечет отсутствие действий из $P^{\#}$ в (a,b).

6. Конвергентность.

Для каждой кнопки $P \in \mathbf{R}$ либо имеется переход по не-отказу $\underline{\Rightarrow}$ в состояние γ, либо, в противном случае, по **L**-конвергентности (лемма 69) имеется переход по **L**-наблюдению, разрешаемому кнопкой $P^{\#}$.

7. Кумулятивность.

Пусть $(a,b) \text{—} P^{\#} \rightarrow (a`,b`)$, где $P \in \mathbf{R}$.

Нам нужно доказать, что $(a`,b`) \text{—} P^{\#} \rightarrow (a`,b`)$,

а также $\forall R^{\#} \in \mathbf{R}\ ((a,b) \text{—} R^{\#} \rightarrow (a,b) \Rightarrow (a`,b`) \text{—} R^{\#} \rightarrow (a`,b`))$.

Условие $(a,b) \text{—} P^{\#} \rightarrow (a`,b`)$ по правилу вывода **1** влечет

$a \text{—} P^{\#} \rightarrow a` \ \&\ b \text{—} P^{\#} \rightarrow b_P \ \&\ b_P = \rho \Rightarrow b` \ \&\ \rho$ *максимальная особая в* b_P.

Следовательно, по кумулятивности $\mathbf{S}^{\sim 1}$ (лемма 56) имеем

$a` \text{—} P^{\#} \rightarrow a` \ \&\ b` \text{—} P^{\#} \rightarrow b`$,

а также $\forall R^{\#} \in \mathbf{R}$

$((a \text{—} R^{\#} \rightarrow a \Rightarrow a` \text{—} R^{\#} \rightarrow a`) \ \&\ (b \text{—} R^{\#} \rightarrow b \Rightarrow b` \text{—} R^{\#} \rightarrow b`))$.

Тогда по лемме 67 в состоянии $b`$ в $\mathbf{S}^{\sim 1}$ нет особых переходов,

поэтому по правилу вывода **1** имеем $(a`,b`) \text{—} P^{\#} \rightarrow (a`,b`)$.

Также по правилу вывода **1** имеем

$\forall R^{\#} \in \mathbf{R}\ ((a,b) \text{—} R^{\#} \rightarrow (a,b) \Rightarrow a \text{—} R^{\#} \rightarrow a \ \&\ b \text{—} R^{\#} \rightarrow b)$.

А тогда по доказанному $a` \text{—} R^{\#} \rightarrow a` \ \&\ b` \text{—} R^{\#} \rightarrow b`$,

что по правилу вывода **1**

и, поскольку в состоянии $b`$ в $\mathbf{S}^{\sim 1}$ нет особых переходов,

влечет $(a`,b`) \text{—} R^{\#} \rightarrow (a`,b`)$.

8. Полнота.

Пусть $(a,b) \text{—} R^{\#} \rightarrow (a,b)$ и $\forall z \in P^{\#}\ (a,b) \text{—} z \nrightarrow$, где $R, P \in \mathbf{R}$.

Нам нужно доказать, что $(a,b) \text{—} P^{\#} \rightarrow (a,b)$.

По правилу вывода **1** имеем $a \text{—} R^{\#} \rightarrow a$

и, поскольку не бывает циклов из переходов по отказам, отличных от переходов-петель, а переходы-петли не являются особыми переходами,

имеем $b \text{—} R^{\#} \rightarrow b$.

Поскольку $\not\Rightarrow \in P^{\#}$, имеем $(a,b) \text{—} \not\Rightarrow$,

что по правилам вывода **2**,**3**,**4** влечет $a \text{—} \not\Rightarrow$,

что по лемме 59 влечет $a \text{—} P^{\#} \rightarrow a$.

Также $a \text{—} \not\Rightarrow$ влечет $\forall z \in P$ z *γ-безопасно в* a.

А тогда, поскольку $\forall z \in P$ $(a,b) \text{—} z \not\rightarrow$,

используя лемму 68, по правилу вывода **1a** имеем $\forall z \in P$ $b \text{—} z \not\rightarrow$.

По лемме 67 $a \le b$.

Поэтому $a \text{—} \not\Rightarrow$ влечет по лемме 60 $b \text{—} \not\Rightarrow$.

Следовательно, поскольку $\forall z \in P$ $b \text{—} z \not\rightarrow$,

по полноте $\mathbf{S}^{\sim 1}$ (лемма 56) имеем $b \text{—} P^{\#} \rightarrow b$.

А тогда по правилу вывода **1**
и, поскольку по лемме 67 в состоянии b в $\mathbf{S}^{\sim 1}$ нет особых переходов,

имеем $(a,b) \text{—} P^{\#} \rightarrow (a,b)$, что и требовалось доказать.

6.96. Доказательство леммы 71

Доказательство будем вести индукцией по **L**-трассе.

Пустая трасса в $\mathbf{S}^{\nabla}$ заканчивается в состоянии $(s\tilde{}_0, s\tilde{}_0)$, где $s\tilde{}_0$ – начальное состояние $\mathbf{S}^{\sim 1}$, в котором заканчивается пустая трасса в $\mathbf{S}^{\sim 1}$.

Пусть утверждение доказано для трассы $\sigma^{\#}$ и докажем его для трассы $\sigma^{\#} \cdot \langle u^{\#} \rangle$.

Пусть в $\mathbf{S}^{\nabla}$ трасса $\sigma^{\#}$ заканчивается в состоянии (a,b).

Тогда по предположению шага индукции в $\mathbf{S}^{\sim 1}$ трасса $\sigma^{\#}$ заканчивается в состоянии a.

Из наличия в $\mathbf{S}^{\nabla}$ трассы $\sigma^{\#} \cdot \langle u^{\#} \rangle$ в силу детерминизма RTS (лемма 70) следует $(a,b) \text{—} u^{\#} \rightarrow (a`,b`)$.

Нам достаточно показать, что $a \text{—} u^{\#} \rightarrow a`$.

Но это следует из правил вывода.

6.97. Доказательство леммы 72

Утверждение непосредственно следует из леммы 71 и правил вывода преобразования C_2.

6.98. Доказательство леммы 73

Утверждение непосредственно следует из леммы 71 (не добавляются новые **L**-трассы) и леммы 72 (продолжения общих **L**-трасс не-отказами и далее дивергенцией и разрушением одинаковы в $\mathbf{S}^{\sim 1}$ и в $\mathbf{S}^{\nabla}$).

6.99. Доказательство леммы 74

Будем вести доказательство индукцией по трассе $\sigma^{\#}$.

Пустая трасса ϵ заканчивается в $\mathbf{S}^{\nabla}$ в состоянии $(s\tilde{}_0, s\tilde{}_0)$, а в $\mathbf{S}^{\sim 1}$ в состоянии $s\tilde{}_0$.

Очевидно, что $\epsilon \preccurlyeq \epsilon$.

Пусть утверждение доказано для трассы $\sigma^{\#}$ и докажем его для трассы $\sigma^{\#}\cdot\langle u^{\#}\rangle$, где $u \in \mathbf{L} \cup \mathbf{R}$.

Пусть трасса $\sigma^{\#}$ в $\mathbf{S}^{\nabla}$ заканчивается в состоянии (a, b).
Тогда по предположению шага индукции в $\mathbf{S}^{\sim 1}$ существует такая трасса $\sigma`^{\#}$, которая заканчивается в состоянии $b$, и $\sigma^{\#} \preccurlyeq \sigma`^{\#}$.

Из наличия в $\mathbf{S}^{\nabla}$ трассы $\sigma^{\#}\cdot\langle u^{\#}\rangle$ в силу детерминизма RTS (лемма 70) следует $(a, b) — u^{\#} \rightarrow (a`, b`)$.

По правилам вывода преобразования C_2 в $\mathbf{S}^{\sim 1}$ имеется переход $b — u^{\#} \rightarrow b_u$ и $b_u = \rho \Rightarrow b`$, где ρ *максимальная особая в* b_u.

По определению отношения «$\preccurlyeq$» условие $\sigma^{\#} \preccurlyeq \sigma`^{\#}$ влечет $\sigma^{\#}\cdot\langle u^{\#}\rangle \preccurlyeq \sigma`^{\#}\cdot\langle u^{\#}\rangle$.

По лемме 65 в трассе $\sigma`^{\#}\cdot\langle u^{\#}\rangle\cdot\rho$ постфикс ρ – это трасса особых отказов.

Поэтому по определению отношения «$\preccurlyeq$» $\sigma`^{\#}\cdot\langle u^{\#}\rangle \preccurlyeq \sigma`^{\#}\cdot\langle u^{\#}\rangle\cdot\rho$.

По транзитивности отношения «$\preccurlyeq$» (лемма 40) имеем $\sigma^{\#}\cdot\langle u^{\#}\rangle \preccurlyeq \sigma`^{\#}\cdot\langle u^{\#}\rangle\cdot\rho$.

Трасса $\sigma`^{\#}\cdot\langle u^{\#}\rangle$ в $\mathbf{S}^{\nabla}$ заканчивается в состоянии $(a`, b`)$,

а трасса $\sigma`^{\#}\cdot\langle u^{\#}\rangle\cdot\rho$ заканчивается в $\mathbf{S}^{\sim 1}$ в состоянии $b`$.

6.100. Доказательство леммы 75

Пустая трасса имеется как в $\mathbf{S}^{\nabla}$, так и в $\mathbf{S}^{\sim 1}$.

Пусть трасса $\sigma^{\#}$ имеется в $\mathbf{S}^{\nabla}$ и в $\mathbf{S}^{\mathbf{\sim 1}}$, а для **L**-наблюдения $u^{\#}$, где $u \in \mathbf{L} \cup \mathbf{R}$, трасса $\sigma^{\#} \cdot \langle u^{\#} \rangle$ имеется в $\mathbf{S}^{\mathbf{\sim 1}}$, но отсутствует в $\mathbf{S}^{\nabla}$.

Согласно лемме 41, если $\sigma^{\#} \cdot \langle u^{\#} \rangle \preccurlyeq \sigma_u{}^{\#}$, $\sigma^{\#} \cdot \langle u^{\#} \rangle \in \mathbf{S}^{\mathbf{\sim 1}}$ и $\sigma_u{}^{\#} \notin \mathbf{S}^{\mathbf{\sim 1}}$,

то $\sigma^{\#} \cdot \langle u^{\#} \rangle \in \boldsymbol{x}(\mathbf{S}^{\mathbf{\sim 1}})$.

Поэтому нам достаточно найти такую трассу $\sigma_u{}^{\#} \notin \mathbf{S}^{\mathbf{\sim 1}}$, что $\sigma^{\#} \cdot \langle u^{\#} \rangle \preccurlyeq \sigma_u{}^{\#}$.

Пусть трасса $\sigma^{\#}$ в $\mathbf{S}^{\nabla}$ заканчивается в состоянии (a,b).
Тогда по лемме 74 в $\mathbf{S}^{\mathbf{\sim 1}}$ найдется трасса $\sigma`^{\#}$, которая заканчивается в состоянии $b$, и $\sigma^{\#} \preccurlyeq \sigma`^{\#}$.

По лемме 71 трасса $\sigma^{\#}$ в $\mathbf{S}^{\mathbf{\sim 1}}$ заканчивается в состоянии a.

Поскольку трасса $\sigma^{\#} \cdot \langle u^{\#} \rangle$ имеется в $\mathbf{S}^{\mathbf{\sim 1}}$, но отсутствует в $\mathbf{S}^{\nabla}$,

то в $\mathbf{S}^{\mathbf{\sim 1}}$ $a — u^{\#} \rightarrow$, а в $\mathbf{S}^{\nabla}$ $(a,b) — u^{\#} \not\rightarrow$.

А тогда, поскольку в любом состоянии есть максимальная особая трасса, по правилу вывода **1** в $\mathbf{S}^{\mathbf{\sim 1}}$ $b — u^{\#} \not\rightarrow$.

Следовательно, в $\mathbf{S}^{\mathbf{\sim 1}}$ нет трассы $\sigma`^{\#} \cdot \langle u^{\#} \rangle$.

Из $\sigma^{\#} \preccurlyeq \sigma`^{\#}$ следует, что $\sigma^{\#} \cdot \langle u^{\#} \rangle \preccurlyeq \sigma`^{\#} \cdot \langle u^{\#} \rangle$.

Для $\sigma_u{}^{\#} = \sigma`^{\#} \cdot \langle u^{\#} \rangle$ имеем: в $\mathbf{S}^{\mathbf{\sim 1}}$ нет трассы $\sigma_u{}^{\#}$ и $\sigma^{\#} \cdot \langle u^{\#} \rangle \preccurlyeq \sigma_u{}^{\#}$,

что и требовалось показать.

6.101. Доказательство леммы 76

1. Утверждение 1.

   Это утверждение непосредственно следует из леммы 75 (не удаляются «лишние» **L**-трассы) и леммы 72 (продолжения общих **L**-трасс не-отказами и далее разрушением и дивергенцией одинаковы).

2. Утверждение 2.

   Если бы множество удаляемых трасс не было постфикс-замкнутым подмножеством множества $\boldsymbol{T}(\mathbf{S}^{\mathbf{\sim 1}})$, то множество $\boldsymbol{T}(\mathbf{S}^{\nabla})$ оставшихся трасс не было бы префикс-замкнутым.

   Но это противоречит лемме 70.

   Вместе с каждой трассой удаляется ее максимальный **L**-префикс согласно лемме 72 (продолжения общих **L**-трасс не-отказами и далее разрушением и дивергенцией одинаковы).

6.102. Доказательство леммы 77

1. Покажем, что $a \le a`$.

   Поскольку в $\mathbf{S}^{\nabla}$ $(a,b) \text{—} P^{\#} \rightarrow (a`,b`)$,

   то по правилу вывода **1** в $\mathbf{S}^{\sim 1}$ $a \text{—} P^{\#} \rightarrow a`$,

   а тогда по лемме 62 $a \le a`$.

2. Покажем, что $b = b`$.

   Из $a \text{—} P^{\#} \rightarrow a`$ следует, что кнопка $P^{\#}$ *γ-безопасна в* a,

   что влечет в $\mathbf{S}^{\sim 1}$ z *γ-безопасно в* a для всех действий $z \in P$.

   Также $(a,b) \text{—} P^{\#} \rightarrow (a`,b`)$ по правилу вывода **1**

   влечет в $\mathbf{S}^{\sim 1}$ $b \text{—} P^{\#} \rightarrow b`$.

   Поскольку в $\mathbf{S}^{\nabla}$ переход $(a,b) \text{—} P^{\#} \rightarrow (a`,b`)$ особый,

   в состоянии (a,b) отсутствуют переходы по действиям $z \in P$.

   А тогда, поскольку для всех этих действий z *γ-безопасно в* a,

   используя лемму 68, по правилу вывода **1a**

   в $\mathbf{S}^{\sim 1}$ в состоянии b отсутствуют переходы по действиям $z \in P$.

   Далее, поскольку в $\mathbf{S}^{\nabla}$ переход $(a,b) \text{—} P^{\#} \rightarrow (a`,b`)$ особый,

   в $\mathbf{S}^{\nabla}$ имеется петля по отказу $(a,b) \text{—} R^{\#} \rightarrow (a,b)$,

   что влечет по правилу вывода **1** $b \text{—} R^{\#} \rightarrow b_R$ и $b_R = \rho \Rightarrow b$,

   что, поскольку циклов переходов по отказам, кроме переходов-петель, не бывает, а особые переходы не являются переходами-петлями,

   влечет $b \text{—} R^{\#} \rightarrow b$.

   А тогда из доказанных условий для состояния b следует, что,

   если переход $b \text{—} P^{\#} \rightarrow b`$ не является петлей, то он особый.

   Однако последнее невозможно, так как по лемме 67 в состоянии b нет особых переходов.

   Следовательно, $b = b`$.

6.103. Доказательство леммы 78

1. Сначала покажем, что найдется $a_u`$ такое, что в $\mathbf{S}^{\nabla}$ $(a`,b) \text{—} u^{\#} \rightarrow (a_u`, b_u)$.

   Если в $\mathbf{S}^{\nabla}$ $(a,b) \text{—} u^{\#} \rightarrow (a_u, b_u)$, то по правилу вывода **1** в $\mathbf{S}^{\sim 1}$

$a \text{—} u^{\#} \to a_u$, $b \text{—} u^{\#} \to b_u`$ и $b_u` = \rho \Rightarrow b_u$, где ρ *максимальная особая в* $b_u`$.

Из наличия перехода $a \text{—} u^{\#} \to a_u$ следует, что

наблюдение $u^{\#}$ *γ-безопасно в* a.

Поэтому, учитывая, что $a \le a`$, по лемме 61

наблюдение $u^{\#}$ *γ-безопасно в* $a`$.

А тогда, учитывая, что $b \text{—} u^{\#} \to b_u`$ и $b_u` = \rho \Rightarrow b_u$,

где ρ *максимальная особая в* $b_u`$,

используя лемму 68, по правилу вывода **1a**

найдется $a_u`$ такое, что в $\mathbf{S}^{\nabla}$ $(a`, b) \text{—} u^{\#} \to (a_u`, b_u)$.

2. Теперь покажем, что $a_u \le a_u`$.

По доказанному в предыдущем пункте в $\mathbf{S}^{-1}$ $a \text{—} u^{\#} \to a_u$.

Также, поскольку в $\mathbf{S}^{\nabla}$ $(a`, b) \text{—} u^{\#} \to (a_u`, b_u)$,

то по правилу вывода **1** в $\mathbf{S}^{-1}$ $a` \text{—} u^{\#} \to a_u`$.

Также по условию леммы $a \le a`$.

Следовательно, по лемме 63 $a_u \le a_u`$.

6.104. Доказательство леммы 79

Рассмотрим в $\mathbf{S}^{\nabla}$ произвольную трассу $\mu^{\#}$ и отказ $P^{\#} \in \mathbf{R}^{\#}$ особый после $\mu^{\#}$.

Нам нужно доказать, что для любой трассы $\mu^{\#} \cdot \lambda^{\#} \cdot \kappa \in \boldsymbol{T}(\mathbf{S}^{\nabla})$ имеет место $\mu^{\#} \cdot \langle P^{\#} \rangle \cdot \lambda^{\#} \cdot \kappa \in \boldsymbol{T}(\mathbf{S}^{\nabla})$.

В силу леммы 72 это достаточно доказать для случая **L**-трасс, когда $\kappa = \epsilon$.

Пусть трасса $\mu^{\#}$ заканчивается в состоянии (a, b).

Поскольку отказ $P^{\#}$ особый после $\mu^{\#}$, по лемме 65 имеется переход $(a, b) \text{—} P^{\#} \to (a`, b`)$, который является либо переходом-петлей, если $(a, b) = (a`, b`)$, либо особым переходом в противном случае.

Нам нужно доказать, что для любой трассы $\lambda^{\#}$ с началом в состоянии (a, b) имеется трасса $\lambda^{\#}$ с началом в состоянии $(a`, b`)$.

Для случая перехода-петли, когда $(a, b) = (a`, b`)$, утверждение очевидно.

Рассмотрим случай, когда переход $(a,b)\text{—}P^{\#}\rightarrow(a`,b`)$ является особым.

Мы докажем более сильное утверждение:

если трасса $\lambda^{\#}$ с началом в состоянии (a,b) заканчивается в состоянии (a_λ,b_λ), то трасса $\lambda^{\#}$ с началом в состоянии $(a`,b`)$ заканчивается в состоянии $(a`_\lambda,b_\lambda)$ и $a_\lambda\le a_\lambda`$.

Доказательство будем вести индукцией по трассе $\lambda^{\#}$.

Нам достаточно доказать два утверждения:

1) база индукции: для пустой трассы $\lambda^{\#}$: $a\le a`$ и $b=b`$;

2) шаг индукции: если $(a_\lambda,b_\lambda)\text{—}u^{\#}\rightarrow(a_{\lambda u},b_{\lambda u})$ и $a_\lambda\le a_\lambda`$,

то $(a`_\lambda,b_\lambda)\text{—}u^{\#}\rightarrow(a`_{\lambda u},b_{\lambda u})$ и $a_{\lambda u}\le a_{\lambda u}`$.

Утверждение 1 следует из леммы 77, а утверждение 2 – из леммы 78.

6.105. Доказательство теоремы 26

По лемме 73 $\boldsymbol{T}(\mathbf{S}^{\nabla})\subseteq\boldsymbol{T}(\mathbf{S}^{\mathbf{-1}})$.

По лемме 54 $\boldsymbol{T}(\mathbf{S}^{\mathbf{-1}})\subseteq\boldsymbol{\Sigma}^{\mathbf{01}\sim}$.

Отсюда $\boldsymbol{T}(\mathbf{S}^{\nabla})\subseteq\boldsymbol{\Sigma}^{\mathbf{01}\sim}$.

По лемме 58 множество $\boldsymbol{\Sigma}^{\mathbf{01}\sim}\setminus\boldsymbol{T}(\mathbf{S}^{\mathbf{-1}})$ постфикс-замкнуто и $\boldsymbol{\Sigma}^{\mathbf{01}\sim}\setminus\boldsymbol{T}(\mathbf{S}^{\mathbf{-1}})\subseteq\boldsymbol{x}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})$ и вместе с каждой трассой содержит ее максимальный **L**-префикс (максимальный префикс, являющийся **L**-трассой).

Следовательно, по лемме 39 $\boldsymbol{x}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})=(\boldsymbol{\Sigma}^{\mathbf{01}\sim}\setminus\boldsymbol{T}(\mathbf{S}^{\mathbf{-1}}))\cup\boldsymbol{x}(\boldsymbol{T}(\mathbf{S}^{\mathbf{-1}}))$.

По лемме 76 множество $\boldsymbol{T}(\mathbf{S}^{\mathbf{-1}})\setminus\boldsymbol{T}(\mathbf{S}^{\nabla})$ постфикс-замкнуто и $\boldsymbol{T}(\mathbf{S}^{\mathbf{-1}})\setminus\boldsymbol{T}(\mathbf{S}^{\nabla})\subseteq\boldsymbol{x}(\boldsymbol{T}(\mathbf{S}^{\mathbf{-1}}))$ и вместе с каждой трассой содержит ее максимальный **L**-префикс (максимальный префикс, являющийся **L**-трассой).

Следовательно, по лемме 39 $\boldsymbol{x}(\boldsymbol{T}(\mathbf{S}^{\mathbf{-1}}))=(\boldsymbol{T}(\mathbf{S}^{\mathbf{-1}})\setminus\boldsymbol{T}(\mathbf{S}^{\nabla}))\cup\boldsymbol{x}(\boldsymbol{T}(\mathbf{S}^{\nabla}))$.

По лемме 69 и лемме 79 $\boldsymbol{x}(\boldsymbol{T}(\mathbf{S}^{\nabla}))=\varnothing$.

Поэтому $\boldsymbol{x}(\boldsymbol{T}(\mathbf{S}^{\mathbf{-1}}))=\boldsymbol{T}(\mathbf{S}^{\mathbf{-1}})\setminus\boldsymbol{T}(\mathbf{S}^{\nabla})$.

А тогда $\boldsymbol{x}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})=(\boldsymbol{\Sigma}^{\mathbf{01}\sim}\setminus\boldsymbol{T}(\mathbf{S}^{\mathbf{-1}}))\cup(\boldsymbol{T}(\mathbf{S}^{\mathbf{-1}})\setminus\boldsymbol{T}(\mathbf{S}^{\nabla}))$.

Поскольку $\boldsymbol{T}(\mathbf{S}^{\nabla})\subseteq\boldsymbol{T}(\mathbf{S}^{\mathbf{-1}})\subseteq\boldsymbol{\Sigma}^{\mathbf{01}}$, имеем $\boldsymbol{x}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})=\boldsymbol{\Sigma}^{\mathbf{01}\sim}\setminus\boldsymbol{T}(\mathbf{S}^{\nabla})$.

Следовательно, $\boldsymbol{\Sigma}^{\boldsymbol{x}}=\boldsymbol{\Sigma}^{\mathbf{01}\sim}\setminus\boldsymbol{x}(\boldsymbol{\Sigma}^{\mathbf{01}\sim})=\boldsymbol{\Sigma}^{\mathbf{01}\sim}\setminus(\boldsymbol{\Sigma}^{\mathbf{01}\sim}\setminus\boldsymbol{T}(\mathbf{S}^{\nabla}))$.

Поскольку $\boldsymbol{T}(\mathbf{S}^{\nabla})\subseteq\boldsymbol{\Sigma}^{\mathbf{01}}$, имеем $\boldsymbol{\Sigma}^{\boldsymbol{x}}=\boldsymbol{T}(\mathbf{S}^{\nabla})$.

По теореме 20 $\boldsymbol{\Sigma}^{\boldsymbol{x}}=\boldsymbol{\Sigma}^{\mathbf{01}^{\nabla}}$.

Итак, $\boldsymbol{T}(\mathbf{S}^{\nabla})=\boldsymbol{\Sigma}^{\boldsymbol{x}}=\boldsymbol{\Sigma}^{\mathbf{01}^{\nabla}}$, что и требовалось доказать.

6.106. Доказательство теоремы 27

По теореме 26 $\boldsymbol{T}(\mathbf{S}^{\nabla})=\boldsymbol{\Sigma}^{\boldsymbol{x}}$.

По теореме 20 $\boldsymbol{\Sigma}^{\boldsymbol{x}}\cap\boldsymbol{\Sigma}^{\mathbf{0}\sim}=\boldsymbol{\Sigma}^{\mathbf{0}^{\nabla}}$, $\boldsymbol{\Sigma}^{\boldsymbol{x}}\cap\boldsymbol{\Sigma}^{\mathbf{1}\sim}=\boldsymbol{\Sigma}^{\mathbf{1}^{\nabla}}$ и $\boldsymbol{\Sigma}^{\boldsymbol{x}}=\boldsymbol{\Sigma}^{\mathbf{01}^{\nabla}}$.

По теореме 14 $\forall \mu^{\#}\in\mathbf{\Sigma^{0\nabla}}\ \forall P\in\mathbf{R}\cup\mathbf{Q}\ \ (P^{\#}\ \boldsymbol{safe}_{\gamma\Delta}\ \mathbf{\Sigma}^{\nabla}\ \boldsymbol{after}\ \mu^{\#}\ \Leftrightarrow\ \mu^{\#}\cdot\langle\not{\mathrm{R}},\gamma\rangle\notin\mathbf{\Sigma^{1\nabla}})$.

Поэтому $\forall \mu^{\#}\in\boldsymbol{T}(\mathbf{S}^{\nabla})\cap\mathbf{\Sigma^{0\sim}}\ \forall P\in\mathbf{R}\cup\mathbf{Q}$

$(P^{\#}\ \boldsymbol{safe}_{\gamma\Delta}\ \mathbf{\Sigma}^{\nabla}\ \boldsymbol{after}\ \mu^{\#}\ \Leftrightarrow\ \mu^{\#}\cdot\langle\not{\mathrm{R}},\gamma\rangle\notin\boldsymbol{T}(\mathbf{S}^{\nabla})\cap\mathbf{\Sigma^{1\sim}})$.

Трасса $\mu^{\#}\in\boldsymbol{T}(\mathbf{S}^{\nabla})\cap\mathbf{\Sigma^{0\sim}}$ тогда и только тогда, когда это простая **L**-трасса.

Далее, очевидно $\mu^{\#}\cdot\langle\not{\mathrm{R}},\gamma\rangle\notin\boldsymbol{T}(\mathbf{S}^{\nabla})\cap\mathbf{\Sigma^{1\sim}}\ \Leftrightarrow\ S\ \not{=\!=}\!\!\Rightarrow\gamma$.

Отсюда следует утверждение теоремы.

6.107. Доказательство теоремы 28

По теореме 26 $\boldsymbol{T}(\mathbf{S}^{\nabla})=\mathbf{\Sigma}^{x}$.

По теореме 20 $\mathbf{\Sigma}^{x}\cap\mathbf{\Sigma^{0\sim}}=\mathbf{\Sigma^{0\nabla}}$.

В рассматриваемом случае (есть конформные реализации) по теореме 15 $\boldsymbol{SafeBy}(\mathbf{T}^{\nabla},\mathbf{L})=\mathbf{\Sigma^{0\nabla}}$.

Поэтому $\boldsymbol{SafeBy}(\mathbf{T}^{\nabla},\mathbf{L})=\boldsymbol{T}(\mathbf{S}^{\nabla})\cap\mathbf{\Sigma^{0\sim}}$.

Трасса $\mu^{\#}\in\boldsymbol{T}(\mathbf{S}^{\nabla})\cap\mathbf{\Sigma^{0\sim}}$ тогда и только тогда,
когда это простая **L**-трасса (напомним, что мы рассматриваем случай, когда в исходной спецификации нет трассы $\langle\gamma\rangle$).

Отсюда следует утверждение теоремы.

6.108. Доказательство леммы 80

По лемме 71 в $\mathbf{S^{\sim 1}}$ есть трасса $\sigma^{\#}$ и она заканчивается в состоянии a.

По лемме 54 операция $\boldsymbol{C_1}$ не добавляет трассы.

Поэтому в $\mathbf{S}^{\sim}$ тоже есть трасса $\sigma^{\#}$ и она заканчивается в состоянии a.

По лемме 67 $a\le b$ и в состоянии b в $\mathbf{S^{\sim 1}}$ нет особых переходов.

Условие $a\le b$ влечет $\cup\boldsymbol{r}(a)\subseteq\cup\boldsymbol{r}(b)$,
где $\boldsymbol{r}(a)$ и $\boldsymbol{r}(b)$ определяются по RTS $\mathbf{S^{\sim 1}}$.

Из условия $\cup\boldsymbol{r}(a)\subseteq\cup\boldsymbol{r}(b)$ по согласованности RTS $\mathbf{S^{\sim 1}}$ следует, что для любого $\mathbf{R}^{\#}$-отказа $P^{\#}$, по которому есть переход-петля в состоянии a, в состоянии b нет переходов по действиям из P.

Поскольку (a,b) является **L**-состоянием в $\mathbf{S}^{\nabla}$, из правил вывода следует, что b является **L**-состоянием в $\mathbf{S^{\sim 1}}$.

По лемме 55 состояние b **L**-конвергентно и, следовательно, P-конвергентно.

Поэтому $b\ \not{=\!=}\!\!\rightarrow\gamma$ или $b\ {=\!=}\!\!\rightarrow_{P^{\#}}b`$.

Если бы было $b \overset{P}{\not\longrightarrow} \gamma$, то по лемме 61 было бы $a \overset{P}{\not\longrightarrow} \gamma$, что по лемме 59 противоречит $a \overset{P^{\#}}{\longrightarrow} a$. Следовательно, $b \overset{P^{\#}}{\longrightarrow} b`$.

А поскольку в b нет особых переходов, $b \overset{P^{\#}}{\longrightarrow} b$.

Отсюда следует, что $\forall P \in \mathbf{R}\ (a \overset{P^{\#}}{\longrightarrow} a \Rightarrow b \overset{P^{\#}}{\longrightarrow} b)$.

Тогда, так как в b нет особых переходов, по правилам вывода для RTS $\mathbf{S}^{\nabla}$

$\forall P \in \mathbf{R}\ (a \overset{P^{\#}}{\longrightarrow} a \Rightarrow (a,b) \overset{P^{\#}}{\longrightarrow} (a,b))$.

Также по правилам вывода для RTS $\mathbf{S}^{\nabla}$

$\forall P \in \mathbf{R}\ (a \overset{P^{\#}}{\longrightarrow} a \Leftarrow (a,b) \overset{P^{\#}}{\longrightarrow} (a,b))$.

Следовательно, у состояний (a,b) и a одинаковые петли по отказам, что влечет $\cup \boldsymbol{r}((a,b)) = \cup \boldsymbol{r}(a)$.

Но в RTS $\mathbf{S}^{\sim}$ $\cup \boldsymbol{r}(a) = \cup \boldsymbol{Ip}(\sigma)$ по лемме 45 и теореме 21.

Тем самым, в $\mathbf{S}^{\nabla}$ имеет место $\cup \boldsymbol{r}((a,b)) = \cup \boldsymbol{Ip}(\sigma)$.

6.109. Доказательство леммы 81

По лемме 71 в $\mathbf{S}^{\sim 1}$ есть трасса $\sigma^{\#}$ и она заканчивается в состоянии a.

По лемме 54 операция $\boldsymbol{C_1}$ не добавляет трассы.

Поэтому в $\mathbf{S}^{\sim}$ тоже есть трасса $\sigma^{\#}$ и она заканчивается в состоянии a.

По правилам вывода для операции $\boldsymbol{C_2}$ имеем

$(a,b) \overset{P}{\not\rightarrow} \Delta`$ в $\mathbf{S}^{\nabla} \Leftrightarrow a \overset{P}{\not\rightarrow} \Delta`$ в $\mathbf{S}^{\sim 1}$.

По лемме 54 операция $\boldsymbol{C_1}$ не добавляет переходы и не удаляет переходы по не-отказам.

Поэтому $(a,b) \overset{P}{\not\rightarrow} \Delta`$ в $\mathbf{S}^{\nabla} \Leftrightarrow a \overset{P}{\not\rightarrow} \Delta`$ в $\mathbf{S}^{\sim}$.

По теореме 27 о безопасности кнопок в $\mathbf{S}^{\nabla}$ $\mathbf{R}^{\#}$-отказ $P^{\#}$ безопасен по $\boldsymbol{safe}_{\gamma\Delta}$ после трассы $\sigma^{\#}$, которая заканчивается в состоянии (a,b), тогда и только тогда, когда $(a,b) \overset{P}{\not\rightarrow} \gamma$.

По правилам вывода операции $\boldsymbol{C_2}$ имеем $(a,b) \overset{P}{\not\rightarrow} \gamma \Leftrightarrow a \overset{P}{\not\rightarrow} \gamma$.

А по теореме 22 в $\mathbf{S}^{\sim}$ $a \overset{P}{\not\rightarrow} \gamma$ тогда и только тогда, когда $\mathbf{R}^{\#}$-отказ $P^{\#}$ безопасен по $\boldsymbol{safe}_{\gamma\Delta}$ после трассы $\sigma^{\#}$, которая заканчивается в состоянии a.

Тем самым, в $\mathbf{S}^{\nabla}$ $\mathbf{R}^{\#}$-отказ $P^{\#}$ безопасен по $\boldsymbol{safe}_{\gamma\Delta}$ после трассы $\sigma^{\#}$, которая заканчивается в состоянии (a,b) тогда и только тогда он в $\mathbf{S}^{\sim}$ безопасен по $\boldsymbol{safe}_{\gamma\Delta}$ после трассы $\sigma^{\#}$, которая заканчивается в состоянии a.

Поэтому по теореме 24 $a \overset{P}{\not\rightarrow} \Delta`$ в $\mathbf{S}^{\sim}$ тогда и только тогда, когда выполнено условие $\mathbf{L}$-актуальности безопасного по $\boldsymbol{safe}_{\gamma\Delta}$ $\mathbf{R}^{\#}$-отказа $P^{\#}$ после трассы $\sigma^{\#}$.

Отсюда следует утверждение леммы.

6.110. Доказательство теоремы 29

По теореме 26 $\boldsymbol{T}(\mathbf{S}^{\nabla})=\boldsymbol{\Sigma}^{x}$.

По теореме 20 $\boldsymbol{\Sigma}^{x}\cap\boldsymbol{\Sigma}^{\mathbf{0}\sim}=\boldsymbol{\Sigma}^{\mathbf{0}\nabla}$.

По теореме 16

1. Все трассы из множества $\boldsymbol{\Sigma}^{\mathbf{0}\nabla}$ **L**-актуальны.
2. **L**-наблюдение $u^{\#}\in\mathbf{L}\cup\mathbf{R}^{\#}$, безопасное после трассы $\sigma^{\#}\in\boldsymbol{\Sigma}^{\mathbf{0}\nabla}$, **L**-актуально тогда и только тогда, когда либо 1) $u\in\mathbf{L}$ и $u\notin\cup\boldsymbol{Ip}(\sigma)$, либо 2) $u\in\mathbf{R}$ и для каждой кнопки $Q\in\mathbf{Q}$ такой, что $Q\subseteq u\cup\cup\boldsymbol{Ip}(\sigma)$, трасса $\mu^{\#}\cdot\langle\Theta,\gamma\rangle\in\boldsymbol{\Sigma}^{\mathbf{1}\nabla}$ для каждой трассы $\mu^{\#}\in\boldsymbol{\Sigma}^{\mathbf{0}\nabla}$ такой, что $\mu\in\boldsymbol{di}^{\sim}(\sigma\cdot\langle u\rangle)$.

Трассы из множества $\boldsymbol{\Sigma}^{\mathbf{0}\nabla}$ – это **L**-трассы из $\boldsymbol{T}(\mathbf{S}^{\nabla})$.

Отсюда следует первое утверждение теоремы.

Докажем второе утверждение теоремы.

Пусть трасса $\sigma^{\#}$ заканчивается в состоянии $s=(a,b)$.

Тогда по лемме 80 $\cup\boldsymbol{r}(s)=\cup\boldsymbol{Ip}(\sigma)$, а по лемме 81 условие **L**-актуальности $\mathbf{R}^{\#}$-отказа $P^{\#}$ после трассы $\sigma^{\#}$ эквивалентно $(a,b)\text{—}\not\text{P}\!\!\rightarrow\Delta`$.

Отсюда следует второе утверждение теоремы.

6.111. Доказательство теоремы 30

По лемме 57 RTS $\mathbf{S}^{\sim\mathbf{1}}$ конечна, и ее можно алгоритмически построить за конечное время.

По правилам вывода для RTS $\mathbf{S}^{\nabla}$ операция $\boldsymbol{C}_2$, применяемая к конечной RTS $\mathbf{S}^{\sim\mathbf{1}}$, заканчивается за конечное время и результирующая RTS $\mathbf{S}^{\nabla}$ конечна.

Тем самым, RTS $\mathbf{S}^{\nabla}$ конечна, и ее можно алгоритмически построить за конечное время.

Спецификационная тройка $\mathbf{T}^{\nabla}$ является максимальным ∇-пополнением тройки **T** по теореме 17.

Спецификационная тройка $\mathbf{T}^{\nabla}$ конечна, поскольку семантика конечна, $\boldsymbol{\Sigma}^{\nabla}$ – это расширение $\mathbf{R}^{\#}$-модели $\cup\boldsymbol{d}(\boldsymbol{\Sigma}^{\mathbf{01}\nabla})$ до полной модели, $\boldsymbol{T}(\mathbf{S}^{\nabla})=\boldsymbol{\Sigma}^{\mathbf{01}\nabla}$ и RTS $\mathbf{S}^{\nabla}$ конечна, а отношение $\boldsymbol{safe}_{\gamma\Delta}$ ограниченное.

Список литературы

[1] Бурдонов И.Б., Косачев А.С., Кулямин В.В. Неизбыточные алгоритмы обхода ориентированных графов. Детерминированный случай. «Программирование». 2003. No. 5.

[2] Бурдонов И.Б., Косачев А.С., Кулямин В.В. Неизбыточные алгоритмы обхода ориентированных графов. Недетерминированный случай. «Программирование». 2004. No. 1.

[3] Бурдонов И.Б. Обход неизвестного ориентированного графа конечным роботом. «Программирование», 2004, No. 4.

[4] Бурдонов И.Б. Проблема отката по дереву при обходе неизвестного ориентированного графа конечным роботом. «Программирование», 2004, No. 6.

[5] Бурдонов И.Б. Исследование одно/двунаправленных распределённых сетей конечным роботом. Труды Всероссийской научной конференции "Научный сервис в сети ИНТЕРНЕТ". 2004.

[6] Bourdonov I., Kossatchev A., Kuliamin V. Formal Conformance Testing of Systems with Refused Inputs and Forbidden Actions. Proc. of MBT 2006, Vienna, Austria, March 2006.

[7] Бурдонов И.Б., Косачев А.С., Кулямин В.В. Формализация тестового эксперимента. «Программирование», 2007, No. 5.

[8] Бурдонов И.Б., Косачев А.С., Кулямин В.В. Безопасность, верификация и теория конформности. Материалы Второй международной научной конференции по проблемам безопасности и противодействия терроризму, Москва, МНЦМО, 2007.

[9] Бурдонов И.Б., Косачев А.С., Кулямин В.В. Теория соответствия для систем с блокировками и разрушением. «Наука», 2008.

[10] Игорь Бурдонов. Теория конформности (функциональное тестирование программных систем на основе формальных моделей). LAP LAMBERT Academic Publishing, Saarbrucken, Germany, 2011, ISBN 978-3-8454-1747-9, 428 стр. (содержание книги доступно по адресу: http://www.ispras.ru/~RedVerst/RedVerst/Publications/TR-01-2007.pdf)

[11] Бурдонов И.Б., Косачев А.С. Системы с приоритетами: конформность, тестирование, композиция. Труды Института системного программирования РАН, N 14.1, 2008.

[12] Бурдонов И.Б., Косачев А.С. Эквивалентные семантики взаимодействия. Труды Института системного программирования РАН, N 14.1, 2008.

[13] Бурдонов И.Б., Косачев А.С. Системы с приоритетами: конформность, тестирование, композиция. «Программирование», 2009, No. 4.

[14] Бурдонов И.Б., Косачев А.С. Полное тестирование с открытым состоянием ограниченно недетерминированных систем. Труды Института системного программирования РАН, N 17, 2009.

[15] Бурдонов И.Б., Косачев А.С. Полное тестирование с открытым состоянием ограниченно недетерминированных систем. «Программирование», 2009, No. 6.

[16] Бурдонов И.Б., Косачев А.С. Аналитическая верификация конформности. Научный сервис в сети Интернет: масштабируемость, параллельность, эффективность: Труды Всероссийской суперкомпьютерной конференции (21-26 сентября 2009 г., г. Новороссийск). - М.: Изд-во МГУ, 2009.

[17] Бурдонов И.Б., Косачев А.С. Тестирование конформности на основе соответствия состояний. Труды Института системного программирования РАН, N 18, 2010.

[18] Бурдонов И.Б., Косачев А.С. Симуляция систем с отказами и разрушением. 5-ый Международный симпозиум по компьютерным наукам в России. Семинар «Семантика, спецификация и верификация программ: теория и приложения».Казань 2010.

[19] Бурдонов И.Б., Косачев А.С. Тестирование безопасной симуляции. 5-ый Международный симпозиум по компьютерным наукам в России. Семинар «Семантика, спецификация и верификация программ: теория и приложения».Казань 2010.

[20] Бурдонов И.Б., Косачев А.С. Семантики взаимодействия с отказами, дивергенцией и разрушением. Часть 1. Гипотеза о безопасности и безопасная конформность. «Вестник Томского государственного университета. Управление, вычислительная техника и информатика», №4, 2010.

[21] Бурдонов И.Б., Косачев А.С. Семантики взаимодействия с отказами, дивергенцией и разрушением. Часть 2. Условия конечного полного тестирования. «Вестник Томского государственного университета. Управление, вычислительная техника и информатика», №2, 2011.

[22] I.Burdonov, A.Kosachev. Formal conformance verification. Short Papers of the 22nd IFIP ICTSS, Alexandre Petrenko, Adenilso Simao, Jose Carlos Maldonado (eds.), Nov. 08-10, 2010, Natal, Brazil.

[23] Бурдонов И.Б., Косачев А.С. Семантики взаимодействия с отказами, дивергенцией и разрушением. «Программирование», 2010, No. 5.

[24] Бурдонов И.Б., Косачев А.С. Пополнение спецификации для ***ioco***. «Программирование», 2011, No. 1.

[25] Барвайс Дж. и др. Справочная книга по математической логике. Часть 2: теория множеств. М: Наука, 1982.

[26] Василевский М.П. О распознавании неисправностей автомата. Кибернетика, т. 9, № 4, стр. 93–108, 1973.

[27] Хопкрофт Д., Мотвани Р., Ульман Д. Введение в теорию автоматов, языков и вычислений. Изд. дом "Вильямс", 2002.

[28] Aho A.V., Hopcroft J.E. The Design and Analysis of Computer Algorithms, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, 1974.

[29] van der Bijl M., Rensink A., Tretmans J. Compositional testing with ioco. Formal Approaches to Software Testing: Third International Workshop, FATES 2003, Montreal, Quebec, Canada, October 6th, 2003. Editors: Alexandre Petrenko, Andreas Ulrich ISBN: 3-540-20894-1. LNCS volume 2931, Springer, pp. 86-100.

[30] van der Bijl M., Rensink A., Tretmans J. Component Based Testing with ioco. CTIT Technical Report TR-CTIT-03-34, University of Twente, 2003.

[31] Edmonds J. Johnson E.L. Matching. Euler Tours, and the Chinese Postman. Math. Programming 5, 88-124 (1973).

[32] van Glabbeek R.J. The linear time – branching time spectrum. In J.C.M. Baeten and J.W. Klop, editors, CONCUR'90, Lecture Notes in Computer Science 458, Springer-Verlag, 1990, pp 278–297.

[33] van Glabbeek R.J. The linear time - branching time spectrum II; the semantics of sequential processes with silent moves. Proceedings CONCUR '93, Hildesheim, Germany, August 1993 (E. Best, ed.), LNCS 715, Springer-Verlag, 1993, pp. 66-81.

[34] Jard C., Jéron T., Tanguy L., Viho C. Remote testing can be as powerful as local testing. In Formal methods for protocol engineering and distributed systems, FORTE XII/ PSTV XIX' 99, Beijing, China, J. Wu, S. Chanson, Q. Gao (eds.), pp. 25-40, October 1999.

[35] Lee D., Yannakakis M. Testing Finite State Machines: State Identification and Verification. IEEE Trans. on Computers, Vol. 43, No. 3, March 1994, pp. 306-320.

[36] Lee D., Yannakakis M. Principles and Methods of Testing Finite State Machines – A Survey. Proceedings of the IEEE 84, No. 8, 1090–1123, 1996.

[37] Milner R. Modal characterization of observable machine behaviour. In G. Astesiano & C. Bohm, editors: Proceedings CAAP 81, LNCS 112, Springer, pp. 25-34.

[38] De Nicola R., Segala R. A process algebraic view of Input/Output Automata. Theoretical Computer Science, 138:391-423, 1995.

[39] Petrenko A., Yevtushenko N., Bochmann G.v. Testing deterministic implementations from nondeterministic FSM specifications. Selected proceedings of the IFIP TC6 9-th international workshop on Testing of communicating systems, September 1996.

[40] Tretmans J. Conformance testing with labelled transition systems: implementation relations and test generation. Computer Networks and ISDN Systems, v.29 n.1, p.49-79, Dec. 1996.

[41] Tretmans J. Test Generation with Inputs, Outputs and Repetitive Quiescence. In: Software-Concepts and Tools, Vol. 17, Issue 3, 1996.

Nonconforming traces elimination from specification

Igor Burdonov <igor@ispras.ru>, Alexander Kosachev <kos@ispras.ru>

Abstract. The paper describes the optimization of testing as checking the correspondence (conformance) of implementation to the given specification during test experiments. Tests are generated from specification traces. However, as this paper shows, some traces in the specification do not occur in any conforming implementations. Test generated from such nonconforming traces are knowingly "redundant". So, for test optimization purpose, there is a task to eliminate nonconforming traces from specification. To do that, we propose the corresponding transformation of the specification (we call it ∇-completion) with additional requirement: the class of conforming implementations is unchanged and there is still possibility to test all implementations that could be tested against the initial specification. The proposed algorithms are suitable for the wide range of conformance relations parameterized with some interaction semantics based on test stimuli and observations. For finite semantics and finite initial specification, these algorithms perform the required transformation in finite time and result in a finite specification.

Keywords: interaction semantics, refusals, destruction, divergence, conformance, safe testing, traces, LTS, test generation.

И.Б.Бурдонов, А.С. Косачев.
Удаление из спецификации неконформных трасс.
Препринт Института Системного Программирования РАН, 2011 г., №23.
218 стр.

Дополнительно к препринту: **ПОДРОБНОЕ ОГЛАВЛЕНИЕ**