

Мета-модель функциональной спецификации распределенной системы, пригодная для тестирования.

И.Б.Бурдонов, А.С.Косачев, В.В.Кулямин

Мета-модель асинхронного автомата (АА).

Предлагаются имплицитные спецификации автоматов с помощью пред- и постусловий. Спецификация синхронного автомата (СА) состоит из предусловия – предиката от пресостояния и стимула, и постусловия – предиката от пресостояния, стимула, реакции и постсостояния. Если задано разбиение домена автомата – множества допустимых пар (пресостояние, стимул), то может быть задано несколько спецификаций, предусловия которых соответствуют областям разбиения. Часто такое разбиение проводят только по стимулам (без учета пресостояния), например, при объектно-ориентированном подходе отдельная спецификация соответствует одному методу класса.

Спецификация АА с одной входной/выходной очередью отличается тем, что стимулы и реакции специфицируются раздельно. В постусловие спецификации стимула не входит реакция. В пред- и постусловие спецификации реакции не входит стимул. В стационарных состояниях определены только спецификации стимулов. Часто первая реакция, которую выдает автомат в ответ на стимул, всегда выдается и не зависит от получаемых впоследствии стимулов. Такую реакцию мы называемой немедленной реакцией, все остальные – отложенными.

В случае нескольких выходных очередей спецификация реакции включает не только реакцию, но и идентификатор выходной очереди. В этом случае спецификация стимула отличается лишь тем, что она включает не только стимул, но и идентификатор входной очереди. Вместе с тем, при наличии мультипереходов удобнее считать, что автомат имеет одну спецификацию стимула, предусловие и постусловие которой разбиваются на ветви, задаваемые предикатами от пресостояния и стимулов в тех или иных очередях. Эти ветви далее могут дробиться на подветви для выделения областей функционального покрытия домена автомата.

Спецификация распределенной системы (РС) как сети АА должна включать, кроме спецификаций АА-компонентов, спецификацию очередей, включая указание их размера и разделение на внешние входные/выходные и внутренние очереди.

Нестационарное, параллельное и гипер-тестирования

Тестирование РС, моделируемых АА, существенно отличается от тестирования систем, моделируемых СА.

а) Обработка стимула есть протяженный по времени процесс, в котором система проходит ряд промежуточных нестационарных состояний, и ее реакция зависит от поступления других стимулов, принимаемых в этих состояниях.

б) При одновременной подаче стимулов на разные входные точки системы возникают параллельные процессы их обработки, и наблюдаемое суммарное поведение системы зависит от взаимодействия этих процессов.

Таким образом, для РС ставится задача нестационарного (а) и параллельного (б) тестирования. Проблему генерации стимулов и наблюдения реакций при нестационарном и параллельном тестировании можно рассматривать, абстрагируясь от устройства системы и способов, которыми она получает стимулы и выдает реакции.

Нестационарное тестирование основано на понятии сериала – серии (последовательности) стимулов, подаваемых на автомат в стационарном состоянии без промежуточного ожидания реакций и/или перехода в стационарное состояние.

Параллельное тестирование основывается на аксиоме о параллелизме, которая утверждает, что параллельное выполнение эквивалентно некоторому последовательному выполнению. При разных используемых моделях аксиома о параллелизме получает различные точные формулировки. Если аксиома о параллелизме считается правильной, целью параллельного тестирования является проверка

ее выполнения в реализации. В противном случае, поведение системы в ситуациях невыполнения аксиомы может быть специфицировано отдельно, и тогда параллельное тестирование нацелено на воспроизведение именно этих ситуаций.

Для параллельного тестирования вводятся понятия мультистимула как мультимножества стимулов (стимул может иметь несколько вхождений). В соответствии с аксиомой о параллелизме, подача на автомат мультистимула трактуется как подача на него некоторой, неизвестной заранее, серии этих стимулов.

Комбинация нестационарного и параллельного тестирования приводит к понятию мультисериала – произвольной иерархической комбинации мультимножеств и серий, элементами которых являются, соответственно, серии и мультимножества, а атомарными элементами – отдельные стимулы. Мультисериал задает множество стимулов с некоторым частичным порядком на нем. Если $a < b$, то это означает, что стимул a принимается автоматом раньше, чем стимул b ; порядок приема автоматом несравнимых по этому частичному порядку стимулов считается неизвестным.

Дальнейшим обобщением является гипертестирование, основанное на понятии гиперстимула и гиперреакции. Гиперстимул определяется как мультимножество стимулов с произвольным заданным на нем частичным порядком. Соответственно, гиперреакция определяется как множество реакций с произвольным заданным на нем частичным порядком.

Понятия гиперстимула и гиперреакции являются результатом абстрагирования от порядка приема реализационным автоматом подаваемых на него стимулов и выдачи им реакций. Реальные порядки приема стимулов и выдачи реакций являются линейными порядками (сериализациями), не противоречащими частичным порядкам, соответственно, гиперстимула и гиперреакции. При этом предполагаются выполненными следующие три условия:

- а) Стационарность пресостояния – гиперстимул подается на автомат, находящийся в стационарном состоянии.
- б) Допустимость гиперстимула – при любом выполнении автомата, то есть, при любом линейном порядке приема стимулов, не противоречащем частичному порядку гиперстимула, принимаемые стимулы оказываются допустимыми в соответствующих состояниях.
- в) Стационарность постсостояния – при любом выполнении по данному гиперстимулу автомат через конечное число переходов оказывается в стационарном состоянии.

На основе последнего условия при тестировании устанавливается тайм-аут на переход по гиперстимулу, по окончании которого считается, что все реакции приняты, а автомат перешел в стационарное постсостояние. Это постсостояние на следующем шаге интерпретируется как пресостояние, в котором подается следующий гиперстимул.

Для верификации гиперреакции используется модельный автомат. Важно отметить, что нестационарное тестирование не предполагает асинхронности модельного автомата, а параллельное тестирование – наличия нескольких входных очередей в сети автоматов. Модельный автомат может быть даже детерминированным синхронным автоматом. Отличие гиперстимула от обычной последовательности стимулов в том, что мы не знаем, в каком порядке поступают на реализационный автомат стимулы, несравнимые по частичному порядку гиперстимула, и в каком порядке выдаются реакции, несравнимые по частичному порядку гиперреакции. Поэтому при проверке по модели мы должны перебирать все возможные сериализации гиперстимула и гиперреакции и проверять по модели. Если все сериализации отвергаются моделью, фиксируется ошибка в тестируемом автомате.

Входная очередь автомата определяет линейный порядок находящихся в ней стимулов, в соответствии с которым стимулы принимаются автоматом. Поэтому для модельного автомата с n входными очередями гиперстимулу соответствуют все n -ки входных слов, частичный порядок которых не противоречит частичному порядку гиперстимула. Аналогично гиперреакция связана с одной или несколькими выходными очередями модельного автомата.

Задача гипертестирования: в каждом стационарном состоянии подать на тестируемый автомат каждый допустимый в нем гиперстимул, получить гиперреакцию и проверить ее по модели. Для того, чтобы эта задача могла быть решена за конечное время, на практике, конечно, накладываются ограничения на подаваемые гиперстимулы: ограничивается число стимулов или вводится эквивалентность, разбивающая множество гиперстимулов на конечное число классов.

Предварительное стационарное тестирование

Стационарное тестирование – это такое тестирование, при котором один стимул подается на тестируемый автомат в стационарном состоянии, после чего до получения всех реакций и перехода в стационарное постсостояние подача стимулов приостанавливается. Задача стационарного тестирования: в каждом стационарном состоянии, достижимом из начального состояния (предполагаемого стационарным), подать на автомат каждый допустимый в нем стимул. Графу переходов автомата соответствует стационарный граф, вершины которого – стационарные состояния, а переход (v, x, u, v') соответствует последовательности переходов автомата из состояния v в постсостояние v' , состоящей из одного принимающего перехода по приему стимула x в состоянии v и далее последовательности из пустых и посылающих переходов, выдающей последовательность реакций u . Задачу стационарного тестирования можно переопределить как обход по стимулам стационарного графа.

Если каждое стационарное состояние достижимо из начального состояния по стационарному графу, стационарное тестирование дает основу для гипертестирования. В процессе стационарного тестирования строится стационарный граф, по которому при гипертестировании осуществляются переходы в нужные стационарные состояния для подачи в них нужных гиперстимулов.

Реализация гиперстимула и гиперреакции

Предлагается реализация гиперстимула с помощью графа процессов – ациклического графа с одним источником и одним стоком. Внутренние вершины графа соответствуют стимулам гиперстимула. В этом графе выделяется выходящий остов, дуги которого называются процессными, а хорды – сигнальными. Процессам соответствует множество непересекающихся путей остова, покрывающих все процессные дуги и заканчивающихся в листовых вершинах. Сигнальная дуга предназначена для синхронизации процессов. Выполнение процесса означает проход по процессному пути. Проход по дуге (a, b) начинается тогда, когда процесс получает сигналы по всем сигнальным дугам, входящим в ее конечную вершину b , и заключается в том, что процесс a) подает на автомат стимул, записанный в вершине b (если она внутренняя), б) посылает сигналы по всем сигнальным дугам, выходящим из вершины b , в) если b не конец процессного пути, создает процессы, пути которых начинаются в вершине b , в противном случае, терминируется. Главному процессу соответствует путь от источника до стока.

В граф процессов могут добавляться внутренние пустые вершины, то есть, вершины не связанные с подачей стимула на автомат и предназначенные только для синхронизации процессов. Особый интерес представляют графы процессов, в которых все сигналы – это сигналы о терминии процессов, то есть, сигнальные дуги выходят только из конечных вершин процессных путей. Показано, что мультисериалы могут быть реализованы такими графами процессов, но только, в общем случае, при наличии пустых вершин.

Для реализации гиперреакции могут быть предложены два способа. Каждый из них предполагает наличие нескольких потоков реакций; реакции, поступающие в одном потоке, считаются выданными автоматом в том порядке, в каком они оказываются в потоке.

Первый способ – способ размножаемых реакций – предполагает, что реакция может быть выдана автоматом сразу в несколько потоков. Считается, что существует способ отождествления копий одной реакции из разных потоков. Показано, что таким способом может быть реализована любая гиперреакция.

Второй способ – способ временных меток – вместо размножения реакций предполагает их маркировку временными метками. Две реакции сравнимы, если а) они из одного потока или б) из

разных потоков, но разность их временных меток превышает некоторый фиксированный квант времени. Показано, однако, что не любая гиперреакция может быть реализована таким способом.