Использование контрактных спецификаций для представления требований и функционального тестирования моделей аппаратуры

В.П. Иванников, А.С. Камкин, А.С. Косачев, В.В. Кулямин, А.К. Петренко

Институт системного программирования РАН
109004, Москва, Б. Коммунистическая, 25
E-mail: {ivan, kamkin, kos, kuliamin, petrenko}@ispras.ru

Аннотация. Контрактные спецификации в форме пред- и постусловий широко используются в программной инженерии для формального описания интерфейсов программных компонентов. Такие спецификации, с одной стороны, удобны для разработчиков, поскольку хорошо привязываются к архитектуре системы, с другой стороны, на их основе можно автоматически генерировать тестовые оракулы, проверяющие соответствие поведения целевой системы спецификациям. В работе предлагается использовать контрактные спецификации для представления требований и функционального тестирования моделей аппаратуры, разработанных на таких языках, как VHDL, Verilog, SystemC, SystemVerilog и др. В статье предлагается подход к спецификации таких систем, приводится его сравнение с существующими методами спецификации аппаратуры, описывается опыт практического применения. В качестве основы используется технология тестирования UniTESK, разработанная в Институте системного программирования РАН.

1. Введение

Современный мир не мыслим без огромного разнообразия электронных устройств. Мобильные телефоны, цифровые фотокамеры и переносные компьютеры давно стали неотъемлемыми атрибутами жизни человека. Специальные устройства управляют работой бытовой техники, контролируют бортовые системы самолетов и космических спутников, управляют медицинскими системами жизнеобеспечения. В основе практически всех этих систем лежит полупроводниковая аппаратура — кристаллы интегральных схем, состоящие из миллионов связанных друг с другом микроскопических транзисторов, которые, пропуская и преобразуя электрические токи, реализуют требуемые функции.

Чтобы убедиться, что аппаратура работает *правильно*, то есть реализует именно те *функции*, которые от нее ожидают пользователи, на практике используют *функциональное тестирование*. Требования, предъявляемые к качеству тестирования аппаратных систем, очень высоки. Это связано не только с тем, что аппаратура лежит в основе всех информационных и управляющих вычислительных систем, в том числе достаточно критичных к сбоям и ошибкам. Большое влияние на формирование высоких требований оказывают также экономические факторы. В отличие от программного обеспечения, в котором исправление ошибки стоит сравнительно дешево, ошибка в аппаратуре, обнаруженная несвоевременно, может потребовать перевыпуск и замену продукции, а это сопряжено с очень высокими затратами. Так, известная ошибка в реализации инструкции FDIV микропроцессора

Pentium[1] [1], заключающаяся в неправильном делении некоторых чисел с плавающей точкой, обошлась компании Intel в $475 миллионов [2, 3]. С другой стороны, требования к срокам тестирования также очень высоки. Важно не затягивать процесс и выпустить продукт на рынок своевременно, пока он не потерял актуальность и на него существует спрос.

Как разработать качественный продукт своевременно, используя ограниченные ресурсы? В настоящее время для проектирования электронных устройств используются языки моделирования высокого уровня, которые позволяют значительно ускорить процесс разработки за счет автоматической трансляции описания аппаратуры на *уровне регистровых передач* (*RTL, register transfer level*) в описание аппаратуры на *уровне логических вентелей* (*gate level*). Такие языки называются *языками описания аппаратуры* (*HDL, hardware description languages*), а модели, построенные на их основе — *HDL-моделями* или *RTL-моделями*[2]. Языки описания аппаратуры позволяют значительно повысить продуктивность разработки, но они не страхуют от всех ошибок, поэтому функциональное тестирование по-прежнему остается актуальной и востребованной задачей.

При современной сложности микросхем[3] разработать приемлимый набор тестов вручную за разумное время невозможно. Необходимы технологии автоматизированной разработки тестов. В настоящее время разработка таких технологий и поддерживающих их инструментов выделилась в отдельную ветвь *автоматизации проектирования электроники* (*EDA, electronic design automation*) — *автоматизацию тестирования* (*testbench automation*). Основной задачей тестирования является проверка соответствия поведения системы предъявляемым к ней требованиям. Для возможности автоматизации такой проверки требования к системе должны быть представлены в *машиночитаемой форме*. Такую форму представления требований называют *формальными спецификациями* или просто *спецификациями*.

В работе рассматривается определенный вид спецификаций — *контрактные спецификации* (*contract specifications*). Контрактные спецификации и процесс проектирования на их основе (*DbC, Design-by-Contract*) были введены Бертраном Майером (Bertrand Meyer) в 1986 году в контексте разработки программного обеспечения [4, 5]. Центральная метафора подхода заимствована из бизнеса. Компоненты системы взаимодействуют друг с другом на основе взаимных *обязательств* (*obligations*) и *выгод* (*benefits*). Если компонент предоставляет окружению некоторую функциональность, он может наложить *предусловие* (*precondition*) на ее использование, которое определяет обязательство для клиентских компонентов и выгоду для него. Компонент также может

---

1 Pentium — торговая марка нескольких поколений микропроцессоров семейства x86, выпускаемых компанией Intel с 22 марта 1993 года.

2 Именно такие модели являются предметом исследования настоящей работы.

3 Число транзисторов в современных микросхемах достигает сотней миллионов, а согласно закону Мура (Moore) это число возрастает примерно вдвое через каждые 18-24 месяцев.

гарантировать выполнение некоторого действия с помощью *постусловия* (*postcondition*), которое определяет обязательство для него и выгоду для клиентских компонентов.

Современный стиль проектирования сложных аппаратных систем во многом похож на компонентный подход в программной инженерии. Появляются и развиваются библиотеки готовых компонентов, называемых в электронной промышленности *блоками интеллектуальной собственности* (*IP cores*, *intellectual property cores*), которые можно *многократно* использовать в разных проектах [6]. На данный момент создание действительно сложных аппаратных систем в основном сконцентрировано на интеграции готовых блоков [7]. Отметим, что при таком подходе очень ответственная роль отводится функциональному тестированию, так как отчуждаемые блоки могут использоваться в весьма разных окружениях [7].

Почему в своих исследованиях мы выбрали именно контрактные спецификации? На наш взгляд, подход Design-by-Contract естественным образом вписывается в складывающиеся в настоящее время процессы проектирования аппаратуры, и что не менее важно, контрактные спецификации очень подходят для целей тестирования. Во-первых, они удобны для разработчиков, поскольку хорошо привязываются к архитектуре системы; во-вторых, в силу своего представления они стимулируют усилия по созданию независимых от реализации *критериев корректности целевой системы*; в-третьих, что особенно важно, они позволяют автоматически строить *тестовые оракулы*, проверяющие соответствие поведения целевой системы требованиям, описанным в спецификациях [8].

Несколько слов о том, как организована статья. Во втором, следующем за введением, разделе даются общие сведения о моделях аппаратуры и типичной организации модулей аппаратных систем. В третьем разделе описывается предлагаемый подход к представлению и проверке требований, основанный на контрактных спецификациях. Четвертый раздел содержит краткий обзор технологии тестирования UniTESK и инструмента разработки тестов CTESK, в нем также описан способ использования инструмента для спецификации аппаратуры. В пятом разделе приводится сравнение предлагаемого подхода с существующими методами спецификации. Шестой раздел описывает опыт практического применения подхода. Наконец, в последнем, седьмом разделе делается заключение и очерчиваются направления дальнейших исследований.

2. Модели аппаратуры

Перед тем как описывать предлагаемый подход, рассмотрим особенности моделей аппаратуры, для разработки которых используются такие языки, как VHDL [9], Verilog [10], SystemC [11], SystemVerilog [12] и др. Знание этих особенностей позволит адекватно адаптировать контрактные спецификации в форме пред- и постусловий для для представления требований и функционального тестирования таких систем.

2.1. Особенности моделей аппаратуры

Модели аппаратуры представляют собой системы из нескольких взаимодействующих *модулей*. Как и в языках программирования, модули используются для декомпозиции сложной системы на множество независимых или слабо связанных подсистем. Каждый модуль имеет *интерфейс* — набор *входов* и *выходов*, через которые осуществляется соединение модуля с окружением, и *реализацию*, определяющую способ обработки модулем *входных сигналов*: вычисление значений *выходных сигналов* и изменение *внутреннего состояния*.

Обработка модулем входных сигналов инициируется *событиями* со стороны окружения. Под событиями в моделях аппаратуры понимают любые изменения уровней сигналов. Поскольку обычно рассматривают двоичные сигналы, выделяют два основных вида событий: *фронт сигнала* (*posedge*, *positive edge*) — изменение уровня сигнала с низкого на высокий и срез сигнала (*negedge*, *negative edge*) — изменение уровня сигнала с высокого на низкий[4].

Как правило, каждый модуль состоит из нескольких статически созданных *параллельных процессов*[5], каждый из которых реализует следующий цикл: сначала осуществляется ожидание одного или нескольких событий из заданного набора событий, затем их обработка, после чего цикл повторяется. Набор событий, ожидаемых процессом для обработки, называется *списком чувствительности* (*sensitive list*) процесса. Будем называть процесс *пассивным*, если он находится в состоянии ожидания событий, и *активным* в противном случае.

Важной особенностью моделей аппаратуры является наличие в них понятия *времени*. Время моделируется целочисленной величиной, физический смысл единицы времени можно задавать. Для описания причинно-следственных отношений между событиями, происходящими в одну единицу модельного времени используется понятие *дельта-задержки* (*delta delay*). События, между которыми есть дельта-задержка, выполняются последовательно одно за другим, но в одну и ту же единицу модельного времени.

Для выполнения моделей аппаратуры с целью анализа их поведения обычно используют *симуляцию по событиям* (*event-driven simulation*). В отличие от *симуляции по интервалам времени* (*time-driven simulation*), в которой значения сигналов и внутренние состояния модулей вычисляются через регулярные интервалы времени, в этом способе модель рассматривается только в те моменты времени, когда наступают некоторые события.

Работа *событийного симулятора* (*event-driven simulator*) осуществляется следующим образом. В начале симуляции модельное время устанавливается в ноль. Далее в цикле, пока есть активные процессы[6], выбирается один из них и

---

[4] Мы не рассматриваем здесь разного рода неопределенные значения, часто используемые в моделировании аппаратуры.

[5] В дальнейшем будем называть такие процессы *модельными*, чтобы отличать их от процессов операционной системы.

[6] В начале симуляции активными являются процессы, осуществляющие инициализацию.

выполняется до тех пор, пока он не станет пассивным. После того, как выполнены все активные процессы, симулятор проверяет, есть ли события, запланированные на текущий момент времени через дельта-задержку или на будущие моменты времени. Если такие события есть, симулятор изменяет модельное время на время ближайшего события, реализует события, запланированные на этот момент времени, перевычисляет множество активных процессов, после чего цикл повторяется. Если таких событий нет, симуляция заканчивается.

2.2. Типичная организация модулей аппаратуры

В дальнейшем для удобства будем считать, что спецификация и тестирование моделей аппаратуры осуществляется на уровне отдельных модулей.

В типичном случае работа модуля управляется *сигналом тактового импульса*, который для краткости будем называть *тактовым сигналом* или просто *часами*. Фронты (или срезы) тактового сигнала разбивают непрерывное время на дискретный набор интервалов, называемых *тактами*. Что делать модулю на текущем такте определяется значениями входных сигналов и внутренним состоянием модуля.

Как правило, часть входов модуля определяет *операцию*, которую модулю следует выполнить, такие входы будем называть *управляющими* (*control inputs*); другая часть определяет *аргументы операции*, такие входы будем называть *информационными* (*informative inputs*). Среди операций, реализуемых модулем, обычно присутствует специальная операция *NOP* (*no operation*), означающая бездействие, отсутствие каких либо вычислений. Операция NOP обычно используется для создания временны*х* задержек между другими операциями.

Внутреннее состояние модуля также можно разбить на две составляющие: *управляющую* (*control state*) и *информационную* (*informative state*). Управляющее состояние используется модулем для организации процесса выполнения операций. Как правило, для реализации таких управляющих функций модуля используются подходы на основе конечных автоматов. Информационное состояние представляет собой внутренние данные модуля.

Модули аппаратуры могут быть организованы разными способами. По длительности выполнения модулем операций последние бывают *однотактными* и *многотактными*. По способу организации выполнения операций модули делятся на *модули с поочередным выполнением операций*, *модули с конвейерным выполнением операций* и *модули с параллельным выполнением операций*.

Рассмотрим как осуществляется выполнение модулем однотактной операции. До начала очередного такта окружение устанавливает код операции и аргументы на соответствующих входах модуля. Выполнение модулем операции начинается с началом такта. За этот такт модуль производит необходимые вычисления, изменяет внутреннее состояние и устанавливает значения выходных сигналов, которые окружение может использовать, начиная со следующего такта (Рис. 1).

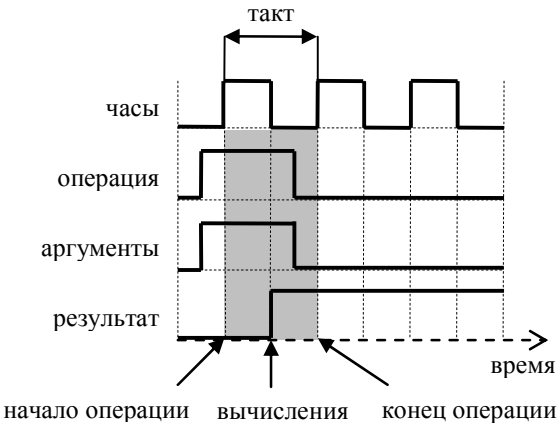

Рис. 1. Временна́я диаграмма сигналов для однотактной операции.

В отличие от однотактной операции, результат многотактной операции вычисляется постепенно такт за тактом. Пусть операция f выполняется модулем за n тактов, тогда на каждом такте $\tau \in \{1, ..., n\}$ модуль выполняет некоторую *микрооперацию* f_τ, а окружение после окончания каждого такта получает некоторый частичный результат. Представление многотактной операции f в виде последовательности микроопераций $(f_1, \ldots, f_n)$ будем называть *временно́й декомпозицией* f.

Теперь несколько слов о способах организации выполнения операций. В модулях с поочередным выполнением операций, как видно из названия, очередную операцию можно подавать на выполнение только после того, как полностью завершена предыдущая. В модулях с конвейерным выполнением операций операции можно подавать последовательно друг за другом, не дожидаясь завершения предыдущей. В модулях с параллельным выполнением операций несколько операций можно подавать одновременно. Модули с поочередным и конвейерным выполнением операций объединим общим термином — *модули с последовательным выполнением операций*, поскольку и в том, и в другом случае операции подаются на выполнение последовательно одна за другой.

В дальнейшем будем считать, что модули организованы таким образом, что одновременно выполняемые операции не вступают друг с другом в *конфликты* (*hazards*), то есть никак не влияют на выполнение друг друга. Если для некоторых операций взаимное влияние все таки возможно, требования должны описывать, как эти операции следует подавать на выполнение, чтобы избежать возникновения конфликтов, например, требования могут указывать число операций NOP, которое всегда следует подавать между определенными инструкциями.

3. Спецификация и проверка требований

Как уже отмечалось во введении, для возможности автоматической проверки соответствия поведения системы требованиям, последние должны быть представлены в *машиночитаемой форме*. Такую форму представления требований

называют *формальными спецификациями* или просто *спецификациями*. В данном разделе описывается предлагаемый подход к представлению и проверке требований к аппаратуре, основанный на *контрактных спецификациях*. Перед описанием подхода рассмотрим какого типа бывают требования к аппаратуре.

3.1. Требования к модулям аппаратуры

В общем случае реализуемые модулем операции являются многотактными, то есть выполняются модулем за несколько тактов. Требования на такие операции бывают двух основных типов: *требования на операцию в целом*, которые не накладывают ограничений на каком именно такте выполняется та или иная микрооперация, и *требования на временну́ю композицию операции*, которые фиксируют на каких тактах какие микрооперации выполняются.

Требования на операцию в целом допускают определенную свободу в реализации модуля. Не важно на каком такте выполняется некоторая микрооперация, важно, чтобы после завершения всей операции, результат этой микрооперации был доступен окружению. В процессе тестирования требования на операцию в целом проверяются после завершения операции.

Требования на временну́ю композицию операции являются более жесткими. В них указаны такты, на которых выполняются микрооперации. Обычно при тестировании имеет смысл проверять не то, что микрооперация была выполнена на определенном такте τ_0, а то, что в конце этого такта соответствующим выходам модуля были присвоены требуемые значения, неважно на каком именно такте $\tau \in \{1, \ldots, \tau_0\}$.

При такой трактовке требования на операцию в целом являются частным случаем требований на временну́ю композицию, поэтому в дальнейшем мы не будем различать эти два типа требований — просто будем считать, что каждому требованию соответствует номер такта, в конце которого его следует проверять.

3.2. Спецификация требований

Предлагаемый подход к представлению требований основан на использовании контрактных спецификаций в форме пред- и постусловий. В отличие от классического Design-by-Contract, когда контракты определяются на уровне операций, мы предлагаем определять контракты для отдельных микроопераций, а контракт для операции в целом получать путем *временно́й композиции* контрактов отдельных микроопераций (Рис. 2.).

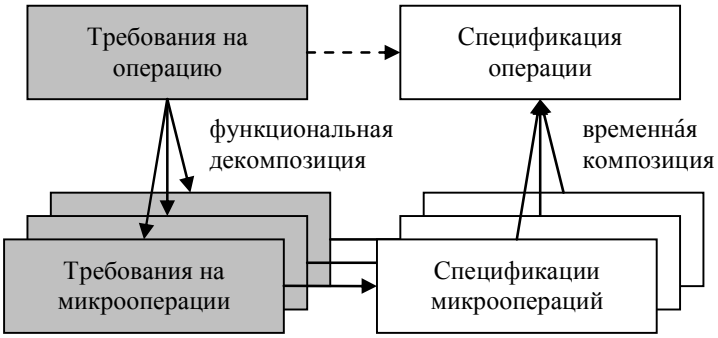

Рис. 2. Построение спецификации отдельной операции.

Под микрооперациями мы здесь понимаем некоторым образом выделенные аспекты функциональности операций, реализуемые за один такт работы модуля, а под временно́й композицией контрактов — спецификацию, в которой для каждой микрооперации указан номер такта, в конце которого должен выполняться соответствующий контракт.

В общих чертах процесс спецификации требований к отдельной операции следующий. Определяется предусловие, ограничивающее ситуации, в которых операцию можно подавать на выполнение. На основе анализа документации производится *функциональная декомпозиция* операции на набор микроопераций. Для каждой микрооперации определяется постусловие, описывающее требования к ней. После этого производится временна́я композиция спецификаций — постусловие каждой микрооперации помечается номером такта, в конце которого оно должно быть выполнено. Таким образом, контракт операции f, для которой выделено n микроопераций, формализуется структурой $C_f=(pre, \{(post_i, \tau_i)_{i=1,n}\})$[7].

Для контракта $C=(pre, \{(post_i, \tau_i)_{i=1,n}\})$ введем следующие обозначения. Через pre_C будем обозначать предусловие операции (pre), через $post_{C,i}$ — постусловие i-ой микрооперации ($post_i$), через $\tau_{C,i}$ — номер такта, в конце которого должно выполняться постусловие i-ой микрооперации (τ_i), через $Post_C(\tau)$ — конъюнкцию постусловий микроопераций, помеченных тактом τ, то есть $\wedge\{ post_{C,i} \mid \tau_{C,i}=\tau \}$.

3.3. Проверка требований

После того как требования к модулю формализованы, проверка поведения модуля на соответствие им может осуществляться в процессе тестирования автоматически.

Предположим, что в некоторый момент времени t тестируемый модуль выполняет m операций $f_1, \ldots, f_m$, которые были поданы на выполнение соответственно $\tau_1, \ldots, \tau_m$ тактов назад ($\tau_i \geq 1$, i=1, …, m). Пусть $C_1, \ldots, C_m$ — контракты операций $f_1, \ldots, f_m$ соответственно, и в моменты подачи операций $f_1, \ldots, f_m$ были выполнены предусловия $pre_{C1}, \ldots, pre_{Cm}$. Тогда для проверки правильности поведения модуля в

[7] Для наглядности мы не вводим модель данных и не уточняем сигнатуры пред- и постусловий.

момент времени t нужно проверить выполнимость предиката $Post_{C1}(\tau_1) \wedge \ldots \wedge Post_{Cm}(\tau_m)$.

Понятно, что для проверки соответствия поведения модуля требованиям также важно уметь строить «хорошие» тестовые последовательности, но рассмотрение этого вопроса выходит за рамки данной работы.

4. Технология тестирования UniTESK

В качестве базового подхода в работе используется технология тестирования UniTESK [13], разработанная в Отделе технологий программирования Института системного программирования РАН [14]. Характерными чертами технологии являются использование контрактных спецификаций в форме пред- и постусловий интерфейсных операций и *инвариантов типов данных* для спецификации требований, а также применение *обобщенных конечно-автоматных моделей* для построения тестовых последовательностей.

4.1. Архитектура тестовой системы UniTESK

Архитектура тестовой системы UniTESK [15] была разработана на основе многолетнего опыта тестирования промышленного программного обеспечения из разных предметных областей и разной степени сложности. Учет этого опыта позволил создать гибкую архитектуру, основанную на следующем разделении задачи тестирования на подзадачи:

- Построение тестовой последовательности, нацеленной на достижение нужного покрытия.
- Создание единичного тестового воздействия в рамках тестовой последовательности.
- Установление связи между тестовой системой и реализацией целевой системы.
- Проверка правильности поведения целевой системы в ответ на единичное тестовое воздействие.

Для решения каждой из этих подзадач предусмотрены специальные компоненты тестовой системы (Рис. 3): для построения тестовой последовательности и создания единичных тестовых воздействий — *обходчик* и *итератор тестовых воздействий*, для проверки правильности поведения целевой системы — *тестовый оракул*, для установления связи между тестовой системой и реализацией целевой системы — *медиатор*. Рассмотрим подробнее каждый из указанных компонентов.

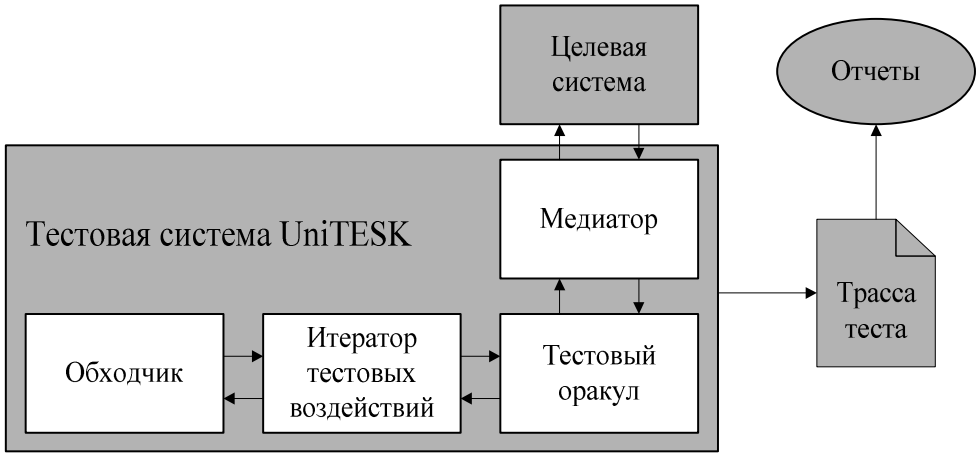

Рис. 3. Архитектура тестовой системы UniTESK.

Обходчик является библиотечным компонентом тестовой системы UniTESK и предназначен вместе с итератором тестовых воздействий для построения тестовой последовательности. В основе обходчика лежит алгоритм обхода графа состояний *обобщенной конечно-автоматной модели* целевой системы (конечного автомата, моделирующего целевую систему на некотором уровне абстракции). Обходчики, реализованные в библиотеках инструментов UniTESK, требуют, чтобы обобщенная конечно-автоматная модель целевой системы, была детерминированной[8] и имела сильно-связный граф состояний.

Итератор тестовых воздействий работает под управлением обходчика и предназначен для перебора в каждом достижимом состоянии конечного автомата допустимых тестовых воздействий. Итератор тестовых воздействий автоматически генерируется из тестового сценария, представляющего собой неявное описание обобщенной конечно-автоматной модели целевой системы.

Тестовый оракул оценивает правильность поведения целевой системы в ответ на единичное тестовое воздействие. Он автоматически генерируется на основе формальных спецификаций, описывающих требования к целевой системе в виде пред- и постусловий интерфейсных операций и инвариантов типов данных.

Медиатор связывает абстрактные формальные спецификации, описывающие требования к целевой системе, с конкретной реализацией целевой системы. Медиатор преобразует единичное тестовое воздействие из спецификационного представления в реализационное, а полученную в ответ реакцию — из реализационного представления в спецификационное. Также медиатор синхронизирует состояние спецификации с состоянием целевой системы.

Трасса теста отражает события, происходящие в процессе тестирования. На основе трассы можно автоматически генерировать различные отчеты, помогающие в анализе результатов тестирования.

---

[8] Исключение составляет обходчик *ndfsm* [18], позволяющий обходить графы состояний для некоторого класса недетерминированных конечных автоматов.

4.2. Инструмент разработки тестов CTESK

Инструмент CTESK [13], используемый в данной работе, является реализацией концепции UniTESK для языка программирования C. Для разработки компонентов тестовой системы в нем используется язык SeC (specification extension of C), являющийся расширением ANSI C. Инструмент CTESK включает в себя транслятор из языка SeC в C, библиотеку поддержки тестовой системы, библиотеку спецификационных типов и генераторы отчетов.

Компоненты тестовой системы UniTESK реализуются в инструменте CTESK с помощью специальных функций языка SeC, к которым относятся:

- *спецификационные функции* — содержат спецификацию непосредственной реакции целевой системы в ответ на единичное тестовое воздействие, а также определение структуры тестового покрытия;
- *функции отложенных реакций* — содержат спецификацию отложенных реакций целевой системы;
- *медиаторные функции* — связывают спецификационные функции с тестовыми воздействиями на целевую систему, а также реакции целевой системы с функциями отложенных реакций;
- *функция вычисления обобщенного состояния* — вычисляет состояние обобщенной конечно-автоматной модели целевой системы;
- *сценарные функции* — описывают набор тестовых воздействий для каждого достижимого обобщенного состояния.

В работах [16, 17] подробно описано, как базовая архитектура тестовой системы UniTESK может быть расширена для функционального тестирования моделей аппаратуры, разработанных на языках Verilog и SystemC. Там же приводятся технические детали, связанные с использованием инструмента CTESK для функционального тестирования моделей аппаратуры.

4.3. Использование CTESK для спецификации аппаратуры

Инструмент разработки тестов CTESK предоставляет достаточно универсальные средства для спецификации систем с асинхронным интерфейсом [18]. Эти средства были адаптированы для спецификации модулей аппаратуры. Рассмотрим процесс разработки спецификаций подробнее.

Для каждой реализуемой модулем операции пишется спецификационная функция, в которой определяется предусловие операции и структура тестового покрытия. Постусловие спецификационной функции обычно возвращает `true`, поскольку все проверки, как правило, определяются в постусловиях микроопераций:

```
// спецификация операции
specification void operation_spec(...)
{
    // предусловие операции
    pre { ... }
    // определение структуры тестового покрытия
    coverage C { ... }
    // постусловие операции обычно возвращает true
    post { return true; }
}
```

Для каждой микрооперации, входящей в состав специфицируемой операции, пишется функция отложенной реакции, в которой определяется ее постусловие. Для удобства тип возвращаемого значения реакции должен содержать аргументы операции, чтобы их можно было использовать в постусловии:

```
// спецификация микрооперации
reaction Operation* micro_return(void)
{
    // постусловие микрооперации
    post { ... }
}
```

Далее определяется *функция временно́й композиции микроопераций*, которая, во-первых, добавляет стимул (операцию вместе с набором аргументов) в *очередь стимулов* с указанием времени, необходимого для обработки стимула (time), во-вторых, для каждой микрооперации добавляет соответствующую реакцию в *очередь реакций* с указанием номера такта относительно текущего, в конце которого следует осуществить проверку реакции ($tick_i$):

```
// временная композиция микроопераций
void operation_time_comp(...)
{
    Operation *descriptor = create_operation(...);

    // добавление стимула в очередь стимулов
    register_stimulus(create_stimulus(time, descriptor)));

    // добавление реакций в очередь реакций
    register_reaction(micro1_return, tick1, descriptor);
    ...
    register_reaction(micron_return, tickn, descriptor);
}
```

Очередь стимулов содержит стимулы, выполняемые в текущий момент времени модулем. Для каждого стимула в очереди хранится время, которое он уже обрабатывается. Очередь реакций содержит еще не завершенные микрооперации. Для каждой микрооперации хранится время, через которое микрооперация будет выполнена и можно будет осуществить проверку реакции. Изменение времени осуществляется *функцией сдвига времени*. После изменения времени вызываются *функции обработки очередей стимулов* и *реакций*. Функция обработки очереди стимулов удаляет из очереди полностью обработанные стимулы. Функция обработки очереди реакций регистрирует отложенные реакции для всех завершившихся микроопераций, которые после этого удаляются из очереди.

Для иллюстрации синтаксиса языка SeC приведем очень простой пример. Рассмотрим устройство, называемое *8-ми битным счетчиком* (Рис. 4).

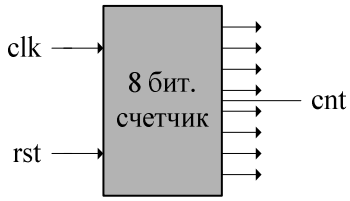

Рис. 4. Схема входов и выходов 8-ми битного счетчика.

Интерфейс счетчика состоит из двух двоичных входов `clk` и `rst` и одного 8-ми битного выходного регистра `cnt`. Если уровень сигнала `rst` низкий, фронт сигнала тактового импульса `clk` увеличивает счетчик `cnt` по модулю 256; иначе, счетчику присваивается значение 0.

Ниже приводится спецификационная функция, описывающая операцию увеличения счетчика, то есть поведение счетчика в ответ на фронт `clk` при низком уровне сигнала `rst`. Поскольку операция является простой, спецификация выполнена без привлечения функций отложенных реакций.

```
// спецификация операции увеличения счетчика
specification void increment_spec(counter_8bit *counter)
    updates cnt = counter->cnt,
            rst = counter->rst
{
    // предусловие операции
    pre { return rst == false; }
    // определение структуры тестового покрытия
    coverage C { return { SingleBranch, "Single branch" }; }
    // постусловие операции
    post { return cnt == (@cnt + 1) % 0xff; }
}
```

5. Сравнение с существующими подходами

В данном разделе приводится сравнение предлагаемого подхода с существующими методами спецификации, поддерживаемыми в современных *языках верификации аппаратуры* (*HVL, hardware verification languages*).

Языки верификации аппаратуры, к которым относятся PSL, OpenVera, SystemVerilog и др. [19], включают в себя конструкции языков описания аппаратуры, языков программирования, а также специальные средства, ориентированные на верификацию. К последним, в частности, относятся средства спецификации поведения, определения структуры тестового покрытия и генерации тестовых данных. Заметим, что мы здесь сравниваем только средства спецификации.

Средства спецификации поведения, используемые в современных языках верификации аппаратуры, базируются на *темпоральной логике линейного времени* (*LTL, linear temporal logic*) и/или *темпоральной логике ветвящегося времени* (*CTL, computation tree logic*) [19]. Языки, по крайней мере по части спецификации, имеют

следующие корни: ForSpec (Intel) [20] (для языков, использующих логику LTL[9]) и Sugar (IBM) [21] (для языков, использующих логику CTL). Ниже приведена диаграмма, показывающая влияние некоторых языков верификации аппаратуры друг на друга.

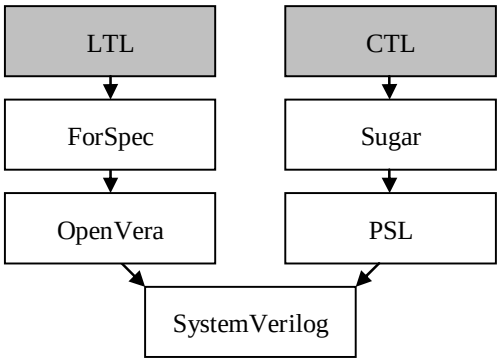

Рис. 5. Влияние языков верификации аппаратуры друг на друга.

Отметим, что логика CTL используется преимущественно для формальной верификации систем. Для целей симуляции и тестирования больший интерес представляет логика линейного времени LTL. Поскольку все языки верификации аппаратуры, использующие LTL, имеют схожие средства спецификации, для сравнения с предлагаемым подходом мы будем использовать только один из них — OpenVera [22]. Данный язык поддерживается многими инструментами, кроме того, он является открытым.

Язык OpenVera был разработан в 1995 году компанией Systems Science. Первоначальное название языка — Vera. В 1998 году компания Synopsys приобрела System Science. В 2001 году Synopsys сделала язык открытым и переименовала его в OpenVera. Для спецификации поведения OpenVera предоставляет специальный язык формулирования *темпоральных утверждений* (*temporal assertions*), который называется OVA (OpenVera assertions) [23, 24].

Язык OVA оперирует с *ограниченными по времени последовательностями событий*, для которых можно обращаться как к прошлому, так и к будущему. Из простых последовательностей можно строить более сложные с помощью *логических связок*, таких как И и ИЛИ, или используя *регулярные выражения*. Язык имеет средства объединения темпоральных утверждений в *параметризованные библиотеки спецификаций*. Проиллюстрируем синтаксис OVA на простом примере.

[9] Вариант логики LTL, используемой в ForSpec, называется FTL (ForSpec temporal logic) [20].

```
// тактовый сигнал
clock negedge(clk)
{
    // граничные значения счетчика
    bool cnt_00: (cnt == 8'h00);
    bool cnt_ff: (cnt == 8'hff);

    // событие переполнения счетчика
    event e_overflow: cnt_ff #1 cnt_00;
}

// утверждение, запрещающее переполнение счетчика
assert a_overflow: forbid(e_overflow);
```

В примере определяется событие переполнения счетчика `e_overflow`, а утверждение `a_overflow` запрещает возникновение такого события.

В подходе OpenVera, как и в других подходах на основе темпоральных логик, упор делается на *временну́ю декомпозицию* операций. Для каждой операции сначала выделяется ее временна́я структура — допустимые последовательности событий и задержки между ними; затем определяются предикаты, описывающие отдельные события; после этого предикаты, относящиеся к одному моменту времени, могут быть некоторым образом сгруппированы (Рис. 6).

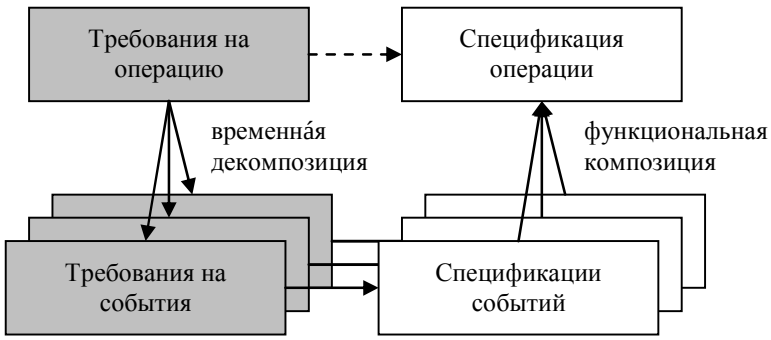

Рис. 6. Построения спецификации в подходах на основе темпоральных логик.

В подходе, предлагаемом нами, основной акцент ставится на *функциональную декомпозицию* операций. Первым делом выделяется функциональная структура операции — набор микроопераций; каждая микрооперация специфицируется; после этого производится временна́я композиция спецификаций (Рис. 2).

Мы полагаем, что функциональная структура операции более устойчива по сравнению с временно́й. Тем самым, подходы, основанные на функциональной декомпозиции операций, позволяют разрабатывать спецификации более устойчивые к изменениям реализации по сравнению с подходами на основе временно́й декомпозиции.

К достоинствам предлагаемого подхода можно отнести наглядность и простоту. Пред- и постусловия обычно понятнее формул темпоральной логики и не требуют от разработчика тестов каких-нибудь специальных знаний.

Отметим также следующее. Контрактные спецификации для описания поведения используют модель состояния целевой системы. Эта модель после некоторого обобщения может быть использована для построения тестовых последовательностей, например, с помощью алгоритмов обхода графов, как это сделано в технологии тестирования UniTESK.

6. Опыт практического применения подхода

Предлагаемый подход был применен на практике при тестировании *буфера трансляции адресов* (*TLB, translation lookaside buffer*) микропроцессора с MIPS64-совместимой архитектурой [25, 26].

Буфер трансляции адресов, входящий в состав большинства современных микропроцессоров, предназначен для кэширования *таблицы страниц* — таблицы операционной системы, хранящей соответствие между номерами *виртуальных* и *физических страниц* памяти. Использование такого буфера позволяет значительно увеличить скорость трансляции адресов. Буфер представляет собой ассоциативную память с фиксированным числом ячеек. Помимо интерфейса для трансляции адресов он предоставляет интерфейс для чтения и изменения содержимого этой памяти.

В общих словах трансляция виртуального адреса осуществляется следующим образом. Если буфер содержит ячейку с нужным номером виртуальной страницы, в определенном выходном регистре модуля формируется соответствующий физический адрес — номер виртуальной страницы меняется на номер физической, а смещение остается прежним; в противном случае, на одном из выходов модуля устанавливается сигнал, говорящий о промахе в буфер.

6.1. Структура и функциональность модуля

Рассмотрим устройство тестируемого буфера трансляции адресов. Память TLB состоит из 64 ячеек, которые составляют *объединенный TLB* (*JTLB, joint TLB*). Кроме того, для повышения производительности модуль содержит два дополнительных буфера: *TLB данных* (*DTLB, data TLB*) и *TLB инструкций* (*ITLB, instruction TLB*). DTLB используется при трансляции адресов данных, ITLB — при трансляции адресов инструкций. Оба буфера содержат по 4 ячейки, их содержимое является подмножеством JTLB, а обновление происходит путем замещения дольше всего не использовавшейся ячейки (LRU, last recently used).

Каждая ячейка TLB условно делится на две секции: *секция-ключ* и *секция-значение*. Секция-ключ включает в себя *спецификатор сегмента памяти* (два старших бита виртуального адреса) (R), *номер виртуальной страницы, деленный на два* (VPN2), *идентификатор процесса* (ASID), *бит глобальной трансляции адресов* (G) и *маску страницы* (MASK). Секция-значение состоит из двух подсекций, каждая из которых содержит *номер физической страницы* (PFN_i), *бит разрешения чтения* (V_i), *бит разрешения записи* (D_i) и *политику кэширования страницы* (C_i). Какая именно подсекция будет использована при трансляции адреса, определяется младшим битом номера виртуальной страницы.

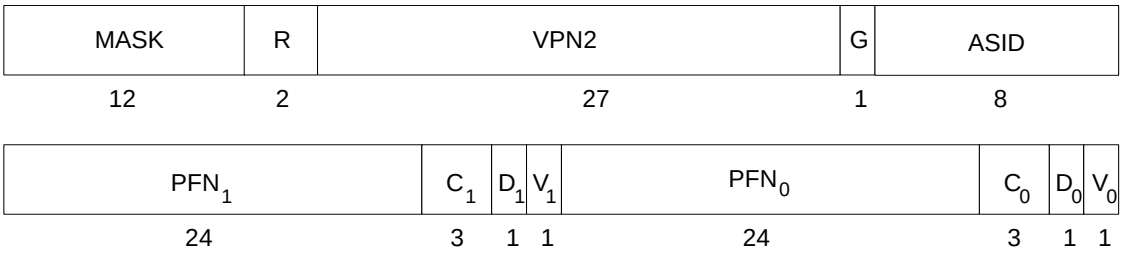

Рис. 7. Структура ячейки TLB (секция-ключ и секция-значение).

Интерфейс тестируемого буфера трансляции адресов состоит из 30 входов (16 входов общего назначения, 3 входа DTLB, 4 входа ITLB, 7 входов JTLB) и 31 выхода (6 выходов общего назначения, 9 выходов DTLB, 8 выходов ITLB, 8 выходов JTLB)[10]. Функциональность модуля включает операции чтения, записи, проверки наличия ячейки в буфере, а также операции трансляции адресов данных и инструкций. RTL-модель модуля разработана на языке Verilog и содержит около 8 000 строк кода.

6.2. Разработка спецификаций модуля

Основные требования к буферу трансляции адресов были получены в письменной форме от разработчиков модуля. В процессе формализации требования уточнялись в результате общения с разработчиками и чтения технической документации. Следует отметить, что все сформулированные разработчиками требования были легко представлены в форме пред- и постусловий.

На первом шаге разработки спецификаций была формально определена модель предметной области. Сначала были выделены базовые понятия, такие как виртуальный и физический адреса, сегмент памяти, режим работы микропроцессора и др. Для этих понятий были определены соответствующие типы данных и вспомогательные функции работы с ними: вычисление сегмента памяти по виртуальному адресу, получение смещения и номера страницы адреса, проверка прав доступа к сегменту памяти при заданном режиме работы микропроцессора и др. Затем постепенно определялись типы данных для более сложных понятий: ячейка TLB, буферы JTLB, DTLB и ITLB; а также соответствующие функции: сопоставление виртуального адреса с ячейкой TLB, поиск ячейки с требуемыми свойствами, трансляция адреса и др. Результатом шага является система типов, полностью описывающая модуль, и набор функций, в терминах которых определяются требования.

Дальнейший процесс был связан со структуризацией требований. Для каждой операции, реализуемой модулем, были выделены микрооперации: по одной микрооперации для операций чтения, записи и проверки наличия ячейки в буфере и по две микрооперации для операций трансляции адресов данных и инструкций. Текстовое описание требований было разбито на атомарные требования, каждое из

[10] При подсчете числа входов и выходов не учитывался интерфейс JTAG (joint test action group) — стандартный интерфейс, используемый для тестирования аппаратуры.

которых было формально описано в виде предиката на основе определенных ранее функций. Декомпозиция реализуемых модулем операций на микрооперации и распределение атомарных требований по предусловиям операций и постусловиям микроопераций отражены в следующей таблице.

Операция	**Микрооперация**	**Число требований**	
		Предусловие	**Постусловие**
Чтение ячейки	—	5	2
Запись ячейки	—	5	4
Проверка наличия ячейки	—	5	3
Трансляция адреса данных	Попадание в DTLB	5	18
	Промах в DTLB		15
Трансляция адреса инструкции	Попадание в ITLB	5	18
	Промах в ITLB		14
Общее число			
5	7	99	
		25	74

6.3. Результаты апробации подхода

Проект продемонстрировал удобство и сравнительно небольшую трудоемкость разработки контрактных спецификаций в форме пред- и постусловий для моделей аппаратуры. Спецификации были разработаны одним человеком приблизительно за 2 недели, а их объем составил около 2 500 строк кода на языке SeC. Значительную долю спецификаций (около 40%), связанную с определением типов данных и функций работы с ними, можно повторно использовать для формального описания буфера трансляции адресов любого MIPS64-совместимого микропроцессора. Разработанные спецификации достаточно модульны, структурированы и наглядны. Их удобно модифицировать — обычно изменения связаны с временно́й композицией микроопераций. Отметим также, что в результате проекта было найдено несколько ошибок в реализации модуля.

7. Заключение

Изначально контрактные спецификации были предложены для описания интерфейсов программных компонентов, но при определенной доработке их вполне можно использовать для описания модулей аппаратуры. Такие спецификации, с одной стороны, удобны для разработчиков, поскольку хорошо привязываются к архитектуре системы, с другой стороны, на их основе можно автоматически генерировать тестовые оракулы, проверяющие соответствие поведения целевой системы требованиям, описанным в спецификациях. Практическая апробация подхода в проекте по тестированию буфера трансляции

адресов микропроцессора показала удобство представления требований к аппаратуре в форме пред- и постусловий и продемонстрировала сравнительно небольшую трудоемкость разработки спецификаций.

На настоящий момент нами получен определенный опыт использования технологии тестирования UniTESK и инструмента CTESK для спецификации и тестирования моделей аппаратуры [16, 17]. Опыт показывает, что некоторые шаги разработки тестов могут быть полностью или частично автоматизированы. Детальное исследование этого вопроса и разработка инструментальной поддержки для автоматизации шагов разработки тестов является основным направлением дальнейшей работы.

Литература

1. *Statistical Analysis of Floating Point Flaw in the Pentium Processor*. Intel Corporation, November 1994.
2. B. Beizer. *The Pentium Bug – An Industry Watershed.* Testing Techniques Newsletter (TTN), TTN Online Edition, September 1995.
3. A. Wolfe. *For Intel, It's a Case of FPU All Over Again*. EE Times, May 1997.
4. B. Meyer. *Design by Contract.* Technical Report TR-EI-12/CO, Interactive Software Engineering Inc., 1986.
5. B. Meyer. *Applying `Design by Contract'*. IEEE Computer, vol. 25, No. 10, October 1992.
6. M. Keating and P. Bricaud. *Reuse Methodology Manual for System-on-a-Chip Designs*. Kluwer Academic Publishers, 2002.
7. В. Немудров, Г. Мартин. *Системы-на-кристалле. Проектирование и развитие*. Москва: Техносфера, 2004.
8. А.В. Баранцев, И.Б. Бурдонов, А.В. Демаков, С.В. Зеленов, А.С. Косачев, В.В. Кулямин, В.А. Омельченко, Н.В. Пакулин, А.К. Петренко, А.В. Хорошилов. *Подход UniTesK к разработке тестов: достижения и перспективы*. (Опубликовано на http://www.citforum.ru/SE/testing/unitesk/)
9. IEEE Standard VHDL Language Reference Manual. IEEE Std 1076-1987.
10. IEEE Standard Hardware Description Language Based on the Verilog Hardware Description Language. IEEE Std 1364-1995.
11. http://www.systemc.org
12. http://www.systemverilog.org
13. http://www.unitesk.com
14. http://www.ispras.ru
15. I. Bourdonov, A. Kossatchev, V. Kuliamin, and A. Petrenko. *UniTesK Test Suite Architecture*. FME'2002. LNCS 2391, Springer-Verlag, 2002.
16. В.П. Иванников, А.С. Камкин, В.В. Кулямин, А.П. Петренко. *Применение технологии UniTESK для функционального тестирования моделей аппаратного обеспечения*. Препринт 8, Институт системного программирования РАН, Москва, 2005. (Опубликовано на http://citforum.ru/SE/testing/unitesk_hard/)
17. A. Kamkin. *The UniTESK Approach to Specification-Based Validation of Hardware Designs*. IEEE-ISoLA'2006: The 2nd International Symposium on Leveraging Applications of Formal Methods, Verification and Validation, November 2006.
18. А.В. Хорошилов. *Спецификация и тестирование систем с асинхронным интерфейсом*. Препринт 12, Институт системного программирования РАН, Москва, 2006. (Опубликовано на http://citforum.ru/SE/testing/asynchronous_interface/)
19. S.A. Edwards. *Design and Verification Languages*. Technical Report, Columbia University, New York, USA, November 2004.

20. R. Armoni, L. Fix, A. Flaisher, R. Gerth, B. Ginsburg, T. Kanza, A. Landver, S. Mador-Haim, E. Singerman, A. Tiemeyer, M. Vardi, and Y. Zbar. *The ForSpec Temporal Logic: A New Temporal Property-Specification Language*. Tools and Algorithms for Construction and Analysis of Systems, 2002.
21. I. Beer, S. Ben-David, C. Eisner, D. Fisman, A. Gringauze, and Y. Rodeh. *The Temporal Logic Sugar*. Lecture Notes in Computer Science, 2001.
22. http://www.open-vera.com
23. *OpenVera® Language Reference Manual: Assertions.* Version 1.4.1, November 2004.
24. *OpenVera® Assertions. Blueprint for Productivity and Product Quality*. March 2003. (Опубликовано на http://www.synopsys.com/products/simulation/ova_wp.html)
25. http://www.mips.com/content/Products/Architecture/MIPS64
26. *MIPS64™ Architecture For Programmers. Revision 2.0.* MIPS Tecnologies Inc., June 9, 2003.