Е.В. Кузьмин
В.А. Соколов

СТРУКТУРИРОВАННЫЕ СИСТЕМЫ ПЕРЕХОДОВ

Е. В. Кузьмин

В. А. Соколов

СТРУКТУРИРОВАННЫЕ СИСТЕМЫ ПЕРЕХОДОВ

2005

УДК 519.68, 519.69
ББК В18
К 89

Кузьмин Е. В., Соколов В. А. **Структурированные системы переходов.** — М.: ФИЗМАТЛИТ, 2006. — 176 с. — ISBN 5-9221-0692-9.

В монографии рассматривается класс вполне структурированных систем помеченных переходов, представляющих собой формализм для моделирования и анализа корректности параллельных и распределенных систем, таких как вычислительные машины и комплексы с параллельной и распределённой архитектурой, параллельные программы, протоколы передачи данных, модели технологических и бизнес-процессов, при этом основное внимание уделяется разрешимости классических проблем ограниченности, достижимости, покрытия, неизбежности, поддержки управляющего состояния, останова, эквивалентности и других важных семантических и темпоральных свойств.

Для научных работников, преподавателей, аспирантов и студентов, интересующихся формальными методами моделирования, анализа и верификации параллельных и распределенных систем.

Допущено учебно-методическим советом по прикладной математике и информатике УМО по классическому университетскому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальности 010200 «Прикладная математика и информатика» и по направлению 510200 «Прикладная математика и информатика».

Ил. 23. Библиогр. 90 назв.

© ФИЗМАТЛИТ, 2006

ISBN 5-9221-0692-9

© Е. В. Кузьмин, В. А. Соколов, 2006

ОГЛАВЛЕНИЕ

Предисловие 5
Введение 11

Глава 1. **Вполне структурированные системы помеченных переходов** 17
1.1. Предварительные сведения 17
1.1.1. Мультимножества 17
1.1.2. Квазиупорядоченные множества 18
1.1.3. Правильный квазипорядок 19
1.2. Системы помеченных переходов 25
1.2.1. Определение 25
1.2.2. Вполне структурированные системы помеченных переходов 27
1.2.3. Метод насыщения 28
1.2.4. Покрывающее дерево системы переходов 34
1.2.5. Строгая совместимость 37
1.2.6. Совместимость по убыванию 40
1.2.7. Системы переходов автоматного типа 43
1.3. Примеры вполне структурированных систем помеченных переходов 46
1.3.1. Сети Петри 46
1.3.2. Системы с ненадежными каналами 51
1.3.3. Системы переходов, независимых от данных 60

Глава 2. **Счетчиковые машины** 75
2.1. Счетчиковые машины Минского 76
2.2. Счетчиковые машины с потерями 80
2.3. Счетчиковые машины с обнулениями и ошибками проверки на нуль 90
2.4. Недетерминированные счетчиковые машины 102

Глава 3. **Темпоральные свойства систем переходов** . . . 113
3.1. Метод проверки модели 113

3.1.1. Логики ветвящегося времени 116
3.1.2. Логики линейного времени 124
3.1.3. Сравнение логик 127

3.2. Темпоральные свойства систем переходов 138
3.2.1. Системы переходов автоматного типа 138
3.2.2. Системы переходов с сильной и транзитивной совместимостью 155
3.2.3. Дерево разрешимости темпоральных логик 162

Заключение 163
Список литературы 166
Предметный указатель 172
Список обозначений 174

Предисловие

Современный период развития информатики и вычислительной техники характеризуется широким использованием параллельных и распределенных систем, поведение которых отличается высокой степенью сложности. Это обстоятельство выдвигает новые задачи в области моделирования и анализа корректности таких систем. Многие существующие методы и средства анализа параллельных и распределенных систем основаны на использовании помеченных систем переходов с конечным числом состояний. Однако очень часто при исследовании сложных систем приходится строить формальные модели, которые представляют собой системы переходов с бесконечным числом состояний. В этом случае многие средства верификации, производящие полный перебор пространства состояний, становятся неприменимыми.

Тем не менее, для некоторых ограниченных классов систем с бесконечным числом состояний разными авторами были разработаны достаточно эффективные методы верификации (как, например, в работах П. Абдуллы, К. Чёранса, А. Финкеля, Б. Йонссона, Ф. Моллера, Ф. Шнеблена [20, 48, 71]). В частности, оказалось, что метод проверки модели (model checking), широко используемый при автоматической верификации систем с конечным числом состояний, может быть применим для некоторых классов систем с бесконечным числом состояний и подмножеств темпоральных логик.

Примерами формальных моделей, являющихся системами переходов с бесконечным числом состояний и позволяющих описывать параллельные и распределенные системы, являются магазинные автоматы [3, 19], сети Петри [6], BPP (Basic Parallel Processes — базовые параллельные процессы) [37], LCS (Lossy Channel Systems — системы с каналами, теряющими сообщения) [23, 24], Real-Time Automata (автоматы реального времени) [26] и др. Целью данной книги является описание свойств и методов исследования одного такого класса систем переходов — так называемых вполне структурированных систем помеченных

переходов. Это весьма широкий класс систем переходов с бесконечным числом состояний, для которого разрешимость многих свойств следует из существования совместимого с отношением переходов правильного квазипорядка на множестве состояний. При исследовании этих систем переходов основное внимание уделяется разрешимости таких классических проблем, как проблемы ограниченности, достижимости, покрытия, неизбежности, поддержки управляющего состояния, останова, эквивалентности и ряда других важных семантических свойств.

Ранее рядом авторов (А. Буаджани, О. Буркарт, Х. Эспарза, Р. Майр) исследовались вопросы разрешимости задачи проверки модели для некоторых конкретных представителей класса вполне структурированных систем переходов, а именно: магазинных автоматов, сетей Петри, базовых параллельных процессов (Basic Parallel Processes), систем сложения векторов с потерями (Lossy Vector Addition Systems) и различных темпоральных логик линейного времени и ветвящегося времени [32, 29, 45, 46]. В данной монографии при исследовании этих проблем выбран подход на основе максимально возможного обобщения и главное внимание уделяется проблеме разрешимости темпоральных свойств для различных классов вполне структурированных систем помеченных переходов, в частности, для класса вполне структурированных систем переходов автоматного типа. В качестве общего средства для демонстрации неразрешимых проблем для вполне структурированных систем помеченных переходов используются счетчиковые машины.

Следует заметить, что в литературе практически не уделяется внимание системам переходов, независимых от данных (за исключением систем переходов с конечным числом состояний), которые, тем не менее, могут быть достаточно выразительным и интересным средством моделирования. В связи с этим в книге представлен специальный фрагмент алгебры процессов, позволяющий строить формальные модели (параллельных и распределенных систем), которые можно рассматривать как независимые от данных помеченные системы переходов. Примером конкретной реализации этого фрагмента является введенный нами формализм, который называется «взаимодействующие раскрашивающие процессы» (Communicating Colouring Processes). Кроме взаимодействующих раскрашивающих процессов, в качестве

примеров вполне структурированных систем переходов рассмотрены обыкновенные сети Петри и сети Петри с обнуляющими дугами, а также системы с ненадежными каналами, в частности, FIFO-канальные системы с потерями.

Наше внимание к исследованию свойств класса вполне структурированных систем переходов было привлечено работами основоположников этого направления, среди которых в первую очередь хотелось бы отметить наших французских коллег: П. Абдуллу, А. Финкеля и Ф. Шнеблена. Мы особенно признательны Филиппу Шнеблену (Ph. Schnoebelen), который оказал нам существенную помощь на начальном этапе наших исследований в этой области.

Мы благодарим всех участников семинара «Моделирование и анализ информационных систем» и, в частности, Ирину Александровну Ломазову за полезное обсуждение и постоянный интерес к нашей работе, а также наших коллег из Ярославского государственного университета им. П. Г. Демидова, чью поддержку мы постоянно ощущали.

Мы благодарим Ольгу Леонидовну Бандман и Валерия Александровича Непомнящего за труд по прочтению рукописи книги и внимание к нашей работе. И наконец, наша особая благодарность — Николаю Вячеславовичу Шилову за скрупулезный анализ всего содержания книги и всех наших результатов, к некоторым из них он имеет самое непосредственное отношение как соавтор! Его многочисленные замечания и предложения позволили избежать целого ряда неточностей и шероховатостей в формулировках и доказательствах теорем, а также в некоторых случаях помогли в выборе терминологии, так как данная область науки только еще формируется.

Мы с большим удовольствием приводим здесь присланные нам отзывы на рукопись книги, которые, как нам кажется, очень хорошо дополняют наше предисловие.

Главный научный сотрудник Института вычислительной математики и математической геофизики СО РАН О. Л. Бандман:

«Для решения больших задач в настоящее время широко используются многопроцессорные суперкомпьютеры, кластеры и распределенные системы. При этом наблюдается отставание методологии и средств параллельного программирования

от уровня современной вычислительной техники. Преодоление этого отставания связано как с приобретением практического опыта в параллельном программировании, так и с решением ряда теоретических проблем, среди которых не последнюю роль играет исследование поведенческих свойств параллельных процессов. Поэтому поиск математических моделей параллельных процессов, которые бы послужили хорошей практической основой для создания средств проверки параллельных алгоритмов и программ на поведенческую корректность, следует считать весьма актуальной проблемой. К сожалению, несмотря на многочисленность существующих моделей и теоретических результатов по их исследованию, решению этой проблемы в литературе уделяется недостаточно внимания. Поэтому любые новые результаты, расширяющие наши знания о поведенческих свойствах параллельных систем и их алгоритмической разрешимости, являются теоретически ценными.

Монография содержит оригинальные результаты, полученные авторами при исследовании свойств параллельных и распределенных систем с бесконечным числом состояний, представляющих собой вполне структурированные системы помеченных переходов. Авторами предложен и последовательно изложен новый подход к исследованию разрешимости темпоральных и семантических свойств, основанный на свойстве структурированности систем переходов, которое состоит в совместимости с отношением переходов правильного квазипорядка на множестве состояний. Построены и приведены доказательства разрешимости (или неразрешимости) ряда свойств, общих для всего класса вполне структурированных систем переходов, а также для выделенных его подклассов.

Отдельно подробно рассмотрен класс счетчиковых машин Минского, поскольку ряд проблем неразрешимости сводится к соответствующим проблемам для этого класса систем. Особое внимание уделено темпоральным свойствам вполне структурированных систем переходов и методам проверки моделей.

Несмотря на строгий математический стиль, необходимость которого диктуется содержанием, книга написана хорошим и ясным языком. Она может быть полезна студентам, аспирантам и преподавателям по компьютерным наукам, а также разработчикам математического обеспечения в распределенных системах».

Заведующий лабораторией теоретического программирования
Института систем информатики им. А. П. Ершова СО РАН,
В. А. Непомнящий;

старший научный сотрудник Института систем
информатики им. А. П. Ершова СО РАН,
Н. В. Шилов:

«Развитие теории верификации программ — важное направление научных исследований современного программирования. Теория верификации программ включает в себя два направления: теорию тестирования программ и теорию формальной верификации. В свою очередь, теория формальной верификации программ имеет два основных «русла» исследований: дедуктивную верификацию и верификацию на моделях.

Представленная монография посвящена теории верификации свойств на классе моделей программ, который получил название вполне структурированных систем переходов (well-structured transition systems). Среди основоположников исследования этого важного класса моделей программ прежде всего необходимо упомянуть имена следующих французских ученых: П. Абдуллы, А. Финкеля и Ф. Шнеблена.

Рецензируемая книга — это первая работа монографического характера на русском языке, посвященная теории вполне структурированных систем переходов. Она дает полное представление о работах зарубежных авторов по этой теории, а также содержит собственные результаты авторов данной монографии, полученные в период 2001–2004 гг., и состоит из следующих трех глав:

1. Вполне структурированные системы переходов.

2. Счетчиковые машины.

3. Темпоральные свойства систем переходов.

Первая глава посвящена в основном обзору теории и примеров вполне структурированных систем переходов, а также описанию методов анализа базовых свойств таких систем. Вторая глава наряду с известными результатами содержит собственные результаты авторов по моделированию универсальных вычислительных устройств (машин Минского). В третьей главе излагаются результаты по проверке временных (темпоральных)

свойств вполне структурированных систем переходов, которые были прежде получены и опубликованы авторами книги.

Монография характеризуется замкнутостью изложения материала, доступного для освоения читателю с базовой подготовкой по дискретной математике. Фактически читателю достаточно иметь представление о множествах, пропозициональной логике, конечных автоматах и машинах Тьюринга.

Материал книги включает в себя:

- все необходимые определения;
- логически правильно расставленные теоремы и утверждения, снабженные корректными доказательствами;
- список всей необходимой учебной и монографической литературы на русском языке, к которой можно обратиться, если возникли трудности при работе со вспомогательным материалом;
- список основных зарубежных публикаций в журналах и трудах конференций, относящихся к теории вполне структурированных систем переходов.

Следует отметить, что данная монография не имеет аналогов в отечественной литературе, а представленный в ней материал может служить основой специального учебного курса для студентов и аспирантов, специализирующихся по теоретической информатике и ее приложениям к верификации программ».

Авторы благодарят Российский фонд фундаментальных исследований за финансовую поддержку проведения исследований, положенных в основу этой книги (грант №03-01-00804), и поддержку ее публикации (грант №05-07095008).

Введение

В настоящее время большое внимание уделяется моделированию и анализу корректности параллельных и распределенных систем, каковыми являются, например, вычислительные машины и комплексы с параллельной и распределенной архитектурой, параллельные программы, протоколы передачи данных, модели технологических и бизнес-процессов. Под корректностью понимается полное соответствие системы задачам, для которых она создается. Корректность определяется абстрактным образом в соответствии с формальной спецификацией, описывающей желаемое поведение системы. Процесс проверки, соответствует ли поведение системы требованиям, заданным в спецификации, называется *верификацией*.

Обычно в качестве формальных моделей параллельных и распределенных систем выступают помеченные системы переходов, представляющие собой средство технически простое, но очень удобное и достаточно общее для моделирования параллельного поведения.

Многочисленные методы и средства анализа параллельных и распределенных систем основаны на использовании помеченных систем переходов с *конечным* числом состояний. Однако существует большое количество примеров формальных моделей, которые могут быть рассмотрены как системы переходов с *бесконечным* числом состояний. В этом случае многие средства верификации, производящие полный перебор пространства состояний, становятся неприменимыми, так как по своей природе не способны анализировать системы, у которых число состояний бесконечно.

Для того чтобы преодолеть этот недостаток, были разработаны методы, применимые, по крайней мере, для некоторых ограниченных классов систем с бесконечным числом состояний. Можно упомянуть здесь работы, например, П. Абдуллы, К. Чёранса, А. Финкеля, Б. Йонссона, Ф. Моллера, Ф. Шнеблена [20, 48, 71]. Более того, оказалось, что метод проверки

модели, широко используемый при автоматической верификации систем с конечным числом состояний, может быть применен для некоторых классов систем с бесконечным числом состояний и подмножеств темпоральных логик [44, 46, 32, 45, 29].

Проверка модели (model checking) — один из подходов к решению проблемы верификации [35]. В качестве языков спецификации для выражения свойств систем при этом подходе используются темпоральные логики. Задача проверки модели состоит в определении выполнимости для системы, заданной формальным образом (в виде формальной модели), свойства, записанного формулой темпоральной логики.

Исследования систем переходов с бесконечным числом состояний были мотивированы теорией формальных языков и грамматик [58, 19, 3]. Во-первых, в этой теории бесконечные языки описываются конечными грамматиками, а во-вторых, некоторые проблемы для языков, например, проблема эквивалентности регулярных языков, являются разрешимыми. Следовательно, не все проблемы систем переходов с бесконечным числом состояний неразрешимы. По аналогии с теорией формальных языков были введены новые формализмы для описания бесконечных систем переходов.

Классическим примером является магазинный автомат. В теории формальных языков он используется для описания контекстно свободных языков. Но этот автомат может быть также рассмотрен как модель системы переходов с бесконечным числом состояний. Каждое управляющее состояние (множество которых конечно) вместе с содержимым стека (магазина) описывает состояние системы переходов. Поскольку размер стека не ограничен, то может быть бесконечно много различных состояний системы. Состояние меняется, когда автомат принимает терминальный символ. Однако это можно интерпретировать как совершение действия системой и переход ее в другое состояние.

Примерами других формальных моделей (систем переходов с бесконечным числом состояний), позволяющих описывать параллельные и распределенные системы, являются сети Петри [6], базовые параллельные процессы (BPP — Basic Parallel Processes) [37], системы с каналами, теряющими сообщения (LCS — Lossy Channel Systems) [23, 24], автоматы реального времени (Real-Time Automata) [26] и др.

Указанные формализмы, как и многие другие, могут быть рассмотрены как *вполне структурированные системы помеченных переходов* [20, 48].

Вполне структурированные системы помеченных переходов — это весьма широкий класс систем переходов с бесконечным числом состояний, для которых разрешимость многих свойств следует из существования совместимого с отношением переходов правильного квазипорядка на множестве состояний.

Описание свойств и методов исследования этого класса систем переходов и является целью настоящей монографии. Основное внимание уделяется разрешимости таких проблем, как проблемы ограниченности, достижимости, покрытия, неизбежности, поддержки управляющего состояния, останова, эквивалентности и ряда других важных семантических свойств. Важность этих задач при анализе свойств систем с бесконечным числом состояний можно продемонстрировать на примере проблем ограниченности и эквивалентности. Одним из первых вопросов при верификации потенциально бесконечных систем является вопрос, действительно ли поведение той или иной системы порождает бесконечное число состояний. Если ответ отрицательный, то могут быть применимы методы, которые используются для верификации конечных систем. Если же множество состояний действительно бесконечно, остается работать лишь с ограниченной, «видимой» частью поведения системы с применением различных комбинаций методов и техник анализа. Для двух формальных моделей, отличающихся размером спецификации, также представляет интерес вопрос о разрешимости проблемы совпадения (эквивалентности) множеств состояний систем переходов, которые они порождают. И в случае положительного ответа существовала бы возможность замены исследуемой сложной модели на более простую (в смысле объема спецификации).

В качестве общего средства для демонстрации неразрешимых проблем для вполне структурированных систем переходов рассматриваются «слабые» счетчиковые машины. Абстрактная счетчиковая машина — довольно простой и удобный объект для исследования неразрешимых семантических и темпоральных свойств систем переходов. Большое количество формализмов, порождающих вполне структурированные системы переходов, с легкостью могут задавать поведение «слабых» счетчиковых

машин. Но в то же время такие проблемы, как ограниченность и достижимость, для некоторых классов машин являются неразрешимыми. Поэтому все неразрешимые проблемы для того или иного класса «слабых» счетчиковых машин автоматически распространяются на вполне структурированные системы переходов (формальные модели), способные отображать поведение этих машин.

Абстрактные счетчиковые машины строятся с помощью различных ослаблений, например, недетерминизма переходов и отношения потери значений счетчиков, на основе счетчиковых машин Минского, которые являются равномощными универсальным машинам Тьюринга. Отсюда неразрешимость исследуемой проблемы устанавливается методом сведения неразрешимой проблемы машины Минского к данной проблеме. Необходимо отметить, что, если исследуемое для конкретной модели свойство является неразрешимым для класса систем переходов, к которому принадлежит модель, это еще не означает бесполезность проверки его выполнимости. Поскольку доказательство неразрешимости некоторого свойства проводится на одном «плохом» примере для всего класса систем переходов в целом, то в конкретном случае, в конкретной модели с учетом ее особенностей проверка свойства может привести к положительному (или отрицательному) результату, т. е. проверка свойства может быть осуществлена.

Ранее в ряде публикаций таких авторов, как А. Буаджани, О. Буркарт, Х. Эспарза, Р. Майр, из которых, например, можно выделить [32, 29, 45, 46], исследовались вопросы разрешимости задачи проверки модели для некоторых конкретных представителей класса вполне структурированных систем переходов, а именно: магазинных автоматов, сетей Петри, BPP, систем сложения векторов с потерями (LVAS) и различных темпоральных логик линейного времени и ветвящегося времени. В данной же монографии мы исходим из позиции обобщения и акцентируем внимание на проблеме разрешимости темпоральных свойств для различных классов вполне структурированных систем помеченных переходов, в частности, для класса вполне структурированных систем переходов автоматного типа, которые из-за своей специфической структуры можно также отнести и к классу систем переходов, независимых от данных.

В литературе практически не уделяется внимание системам переходов, независимых от данных (за исключением систем переходов с конечным числом состояний). Тем не менее, системы, принадлежащие к этому классу, могут быть достаточно выразительными и нетривиальными. Для демонстрации этого факта в данной монографии представлен специальный фрагмент алгебры процессов, построенный на основе таких хорошо известных алгебр процессов, как CCS (Calculus of Communicating Systems — исчисление взаимодействующих систем) Милнера [69] и SCP (Communicating Sequential Processes — взаимодействующие последовательные процессы) Хоара [57], позволяющий строить формальные модели (параллельных и распределенных систем), которые могут быть рассмотрены как независимые от данных помеченные системы переходов, а точнее, как вполне структурированные системы переходов автоматного типа.

В качестве примера конкретной реализации этого фрагмента представлен формализм, который называется *«взаимодействующие раскрашивающие процессы»* (CCP — Communicating Colouring Processes), позволяющий строить модели распределенных систем, где поведение каждого компонента описывается последовательным процессом и между ними организовано взаимодействие, направленное на обмен и передачу пакетов информации. Формализм CCP принимает во внимание факт передачи данных, а также позволяет отслеживать перемещение данных различного типа между компонентами системы. Но переход из одного состояния в другое не зависит от оперируемых данных, а определяется только управляющими состояниями.

Кроме взаимодействующих раскрашивающих процессов, в качестве примеров вполне структурированных систем переходов рассмотрены обыкновенные сети Петри и сети Петри с обнуляющими дугами, а также системы с ненадежными каналами, в частности, FIFO-канальные системы с потерями. Эти формализмы позволяют продемонстрировать ряд абстрактных свойств на конкретных примерах.

Монография организована следующим образом.

В первой главе приводятся предварительные сведения, на которые мы будем опираться в дальнейшем. Здесь определяются понятия мультимножества и правильных квазипорядков. Затем рассматриваются различные классы вполне структурированных

систем переходов; для них описываются методы анализа разрешимых семантических свойств. В конце главы приводятся примеры формальных моделей параллельных и распределенных систем, порождающих вполне структурированные системы переходов рассматриваемых классов. Глава составлена в основном с использованием материалов из литературных источников [13] и [48].

Важно отметить, что в книге [13] И. А. Ломазовой для моделирования и анализа распределенных систем с объектной структурой предлагается использовать *вложенные сети Петри*, которые также рассматриваются как вполне структурированные системы переходов и являются интересным примером систем переходов с сильной совместимостью по возрастанию отношения квазипорядка (на множестве состояний) с отношением переходов. В нашей монографии не рассматриваются вложенные сети Петри, и авторы отсылают читателя для ознакомления с этим формализмом, являющимся расширением обыкновенных сетей Петри, к работе [13].

Вторая глава посвящена счетчиковым машинам, с помощью которых показываются неразрешимые проблемы для вполне структурированных систем переходов, способных моделировать их поведение.

В третьей главе исследуется разрешимость темпоральных свойств систем переходов. Здесь описывается метод проверки модели и приводится ряд темпоральных логик линейного времени и ветвящегося времени. Базовой темпоральной логикой полагается автоматная логика. Проводится сравнение (по выразительной силе) этой логики с другими приведенными темпоральными логиками. Затем для рассматриваемых классов вполне структурированных систем переходов устанавливаются разрешимые и неразрешимые темпоральные свойства, т. е. устанавливаются подмножества логик, в частности, подмножества автоматной логики, для которых метод проверки модели может быть применим, и неразрешимые подмножества, для которых в общем случае этот метод может оказаться бесполезным. Итогом главы является дерево разрешимости темпоральных логик.

В заключении рассматриваются некоторые вопросы вполне структурированности в общем смысле для систем непомеченных переходов.