Российская академия наук
Сибирское отделение
Институт систем информатики
им. А. П. Ершова

На правах рукописи

В.Е. Козюра

РАЗВЕРТКИ РАСКРАШЕННЫХ СЕТЕЙ ПЕТРИ И ИХ ПРИМЕНЕНИЕ ДЛЯ ВЕРИФИКАЦИИ МОДЕЛЕЙ РАСПРЕДЕЛЕННЫХ СИСТЕМ

05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Автореферат
Диссертации на соискание ученой степени
кандидата физико-математических наук

Новосибирск 2004

Работа выполнена в Институте систем информатики им. А.П.Ершова Сибирского отделения Российской академии наук

Научный руководитель:	кандидат физико-математических наук Непомнящий В.А.
Официальные оппоненты:	доктор физико-математических наук Ломазова Ирина Александровна кандидат физико-математических наук Викентьев Александр Александрович
Ведущая организация:	Ярославский государственный университет (г. Ярославль)

Защита состоится _____года в ____ час. ____ мин. на заседании диссертационного совета Д003.060.01 при Объединенном институте информатики Сибирского отделения РАН по адресу:

630090, г. Новосибирск, пр. Лаврентьева, 6.

С диссертацией можно ознакомиться в читальном зале Вычислительной математики и информатики Отделения ГПНТБ СО РАН и ИВТ СО РАН (пр. Лаврентьева, 6).

Автореферат разослан _____2004 г.

Ученый секретарь
Специализированного совета
Д003.060.01
д.ф.-м.н. Л. В. Чубаров

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность. Верификация распределенных систем и, в частности, коммуникационных протоколов является быстро развивающейся областью современного программирования. В связи с всевозрастающей ролью сетевых соединений данная область имеет большое практическое значение. Ввиду большой сложности многих реальных распределенных систем вопрос о правильности их работы является нетривиальной задачей. Обнаружение ошибок в рассматриваемых системах математическими методами и доказательная проверка корректности их работы являются основными целями верификации распределенных систем. Естественный подход к проблеме верификации состоит в моделировании распределенных систем конечными автоматами или сетями Петри и в верификации полученных моделей. Среди наиболее важных подходов к верификации сетей Петри можно выделить симуляцию работы сети и анализ ее пространства состояний. При симуляции работа сети изучается пошаговым методом в ручном или полуавтоматическом режимах. Хотя многие ошибки в работе сети могут быть обнаружены на этапе симуляции, доказательная проверка корректности работы сети может быть получена для данного подхода только при полном моделировании работы сети и проведении так называемой проверки моделей. Метод проверки моделей заключается в описании требуемых свойств системы на языках логических спецификаций и доказательстве истинности или ложности данных спецификаций на построенном пространстве состояний системы.

Последние два десятилетия метод проверки моделей активно развивался и показал себя как эффективное и многообещающее средство для верификации распределенных систем. Благодаря своей естественности и возможности быть интегрированным в среду разработки и анализа распределенных систем, метод проверки моделей был принят в качестве одного из стандартов для верификации спецификаций систем, описанных на какомлибо формальном языке. В совокупности с известными, достаточно эффективными алгоритмами для логик с сильной выразительной силой, методы проверки моделей дают нам эффективный метод верификации распределенных систем.

Однако, при полном моделировании работы сети мы сталкиваемся с так называемой проблемой взрыва числа состояний. Эта проблема состоит в том, что при росте размеров рассматриваемой сети ее полная модель достаточно быстро становится необозримо большой. Это не позволяет надеяться на построение полной модели для реальных систем. Отдельным и, как

это следует из вышесказанного, достаточно важным направлением верификации распределенных систем является разработка эффективных методов, направленных на борьбу с проблемой взрыва числа состояний и позволяющих на практике решать задачи верификации распределенных систем. Среди таких методов можно выделить следующие: метод упрямых множеств, использование двоичных разрешающих диаграмм, методы, основанные на частичном порядке, а также использование симметрии и эквивалентности на рассматриваемых моделях.

Одним из относительно новых и интенсивно развивающихся направлений в области создания эффективных методов верификации распределенных систем является метод развертки сетей Петри. Данный метод позволяет во многих случаях существенно уменьшить размер модели, не теряя при этом свойств рассматриваемой сети. Использование разверток для анализа сетей Петри было предложено К.Л. МакМилланом и развито впоследствии такими авторами, как Дж. Эспарца, С. Ремер, К. Хелиянко, В. Бибер, Х. Фляйшхак, Ф. Валнер, и др. Кроме существенных улучшений алгоритмов и критериев построения развертки был разработан метод проверки моделей первоначально Дж. Эспарцой для логики S_4, а впоследствии Ф. Валнером для логики линейного времени LTL. Алгоритмы проверки моделей для логики LTL с использованием разверток были развиты в последующих работах. В работах В. Бибера и Х. Фляйшхака метод развертки и метод проверки моделей Эспарцы был применен к сетям Петри с интервальным временем.

В России также велись исследования по верификации распределенных систем с использованием сетей Петри. Отметим, в частности, работы Н.А. Анисимова по ручному моделированию с использованием сетей Петри, О.Л. Бандман по спецификации поведения сетевых протоколов, И.Б. Вирбицкайте по использованию техники частичного порядка для верификации временных сетей Петри и В.А. Соколова по анализу параллельных программ.

Среди различных расширений стандартных сетей Петри выделяются сети Петри высокого уровня – раскрашенные сети Петри (РСП), для которых развит теоретический аппарат, накоплен значительный опыт использования и реализована система симуляции и анализа Design/CPN. В РСП вместо стандартных фишек используются типизированные знаковые элементы. Это позволяет определять эффективные спецификации симметрии и эквивалентности на РСП и использовать их для сужения пространства состояний. Кроме того, в РСП помимо классической интервальной временной модели описана и используется так называемая модель временных штам-

пов. РСП обладают большей выразительной силой по сравнению со стандартными сетями Петри и позволяют удобно описывать достаточно сложные распределенные системы. Возникает следующая задача: возможно ли применить метод развертки, хорошо зарекомендовавший себя в области стандартных сетей Петри, к раскрашенным сетям Петри?

Единственной работой в данном направлении была работа А. Валмари по применению метода упрямых множеств к РСП. В данной работе Валмари использует полуформальное определение ветвящегося процесса РСП без применения критериев финитизации. В дальнейшем в его работах было показано, как применять метод упрямых множеств для РСП без построения ветвящегося процесса. Задача применения методов развертки РСП и связанных с этим методов анализа была долгое время открытой, т.к. формальное применение методов верификации к РСП связано со следующими трудностями.

- Объект РСП является значительно более сложным по сравнению со стандартными сетями Петри. Определения и понятия в области РСП являются более громоздкими, а многие определения не могут быть непосредственно перенесены из области стандартных сетей Петри на РСП.
- Для раскрашенных сетей Петри была предложена уникальная временная модель с использованием временных штампов. Хотя данная модель позволяет описывать многие временные события естественным образом, использовать ее значительно сложнее, чем классическую интервальную модель времени.
- Формально введенные понятия симметрии и эквивалентности для РСП, позволяющие существенно сужать пространство состояний системы, представляют собой дополнительные трудности при определении новых понятий для РСП.

Из вышесказанного следует, что применение метода проверки моделей к раскрашенным сетям Петри с использованием разверток в качестве моделей является интересной и актуальной задачей в области автоматической верификации распределенных систем.

Цель диссертации состоит в разработке эффективных методов и алгоритмов верификации моделей распределенных систем, базирующихся на раскрашенных сетях Петри. Достижение цели связано с решением следующих задач:

– разработка эффективных методов построения разверток РСП без временных конструкций;

– исследование метода развертки для РСП, расширенных спецификациями эквивалентности и двумя временными конструкциями;

– разработка метода проверки моделей с использованием разверток РСП, расширенных спецификациями эквивалентности и двумя временными конструкциями;

– реализация разработанных методов и проведение экспериментов, подтверждающих, что метод развертки РСП является эффективным и может быть применен для верификации моделей распределенных систем.

Методы исследований базируются как на применении аппарата сетей Петри, так и на алгоритмах и методах проверки моделей. В области сетей Петри используются теория раскрашенных сетей Петри и методы разверток стандартных сетей Петри.

Научная новизна

- Дано определение ветвящегося процесса для раскрашенных сетей Петри и доказано существование максимального ветвящегося процесса. Определены развертки раскрашенных сетей Петри и для них доказаны свойства конечности, безопасности и полноты. Развертка определяется как конечный префикс максимального ветвящегося процесса, полученный с помощью некоторого критерия финитизации. Приведены два алгоритма построения разверток раскрашенных сетей Петри. Первый алгоритм является удобным средством для проведения теоретических рассуждений, в то время как второй алгоритм является эффективным с точки зрения практики. Описаны методы обнаружения тупиковых состояний РСП с использованием разверток.

- Определены развертки раскрашенных сетей Петри, расширенных спецификациями эквивалентности и двумя временными конструкциями – интервальным временем и моделью временных штампов. Использование спецификации эквивалентности позволяет дополнительно сократить размер полученной развертки. Это является существенным вкладом в борьбу с проблемой взрыва числа состояний, так как применения только методов развертки РСП оказывается недостаточно для многих сложных систем. Для полученных разверток доказаны важные свойства, позволяющие использовать развертки при верификации расширенных сетей.
- Для раскрашенных сетей Петри разработан метод проверки моделей с использованием разверток. Метод позволяет эффективно проверять

любые свойства, выразимые в логике линейного времени, для раскрашенных сетей Петри. Корректность полученного алгоритма формально доказана. Кроме стандартных РСП метод проверки моделей также применен к раскрашенным сетям Петри, расширенным спецификациями эквивалентности и временными конструкциями. Доказаны теоремы, гарантирующие корректность применения данного метода к расширенным РСП.

- Реализован блок проверки моделей в системе PNV. Проведена прототипная реализация метода проверки моделей с использованием разверток. Проведен ряд экспериментов с системой PNV и системой проверки моделей с использованием разверток. Проведенные эксперименты показали возможность и целесообразность использования метода проверки моделей, базирующегося на развертках, при верификации распределенных систем, описанных на языке РСП.

Практическая ценность данных исследований заключается в том, что разработанный метод проверки моделей на базе разверток РСП во многих случаях оказался эффективнее известных методов, базирующихся на других формализмах. Введение спецификаций симметрии и эквивалентности позволяет существенно уменьшить размер рассматриваемого пространства состояний. Проведенные эксперименты подтверждают целесообразность использования описанного подхода для верификации моделей распределенных систем.

Апробация работы проведена на следующих международных научных конференциях:

International Conference on Parallel Computing in Electrical Engineering (PARELEC 2002), Warsaw, Poland;

4th International Conference of Perspectives of System Informatics (PSI'01), Novosibirsk, Russia, 2001;

5th International Workshop on Concurrency, Specification and Programming, Warsaw, Poland, 2001;

Четвертый Сибирский Конгресс по Прикладной и Индустриальной Математике (ИНПРИМ - 2000), Новосибирск, Россия, 2000.

Кроме того, полученные результаты обсуждались на семинарах лаборатории теоретического программирования ИСИ СО РАН и кафедры систем информатики НГУ.

Публикации. По теме диссертации опубликовано 10 научных работ.

Структура работы. Диссертация состоит из введения, пяти глав, заключения и списка литературы из 56 наименований. Содержание составляет 85 страниц. Работа включает 26 иллюстраций и 4 таблицы.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность направления исследования диссертационной работы, формулируются цели, характеризуется научная новизна и практическая ценность работы, дается исторический обзор работ, связанных с темой диссертации и приводится краткое описание структуры текста.

В **первой главе** даны предварительные понятия, используемые в работе. В **разд. 1.1** описываются базовые понятия, связанные с сетями Петри и их развертками. В **подразд. 1.1.1** основными являются определения О-сети, являющейся ограниченным вариантом стандартной сети Петри и ветвящегося процесса для стандартной сети Петри. Ветвящийся процесс определяется как пара, состоящая из некоторой О-сети и гомоморфизма из исходной сети Петри в О-сеть, удовлетворяющего условиям сохранения некоторых аспектов поведения исходной сети Петри в рассматриваемой О-сети. В **подразд. 1.1.2** формально определены точки сечения и развертки сетей Петри. Определения точек сечения являются основой для определения критериев финитизации максимального ветвящегося процесса. Развертка сети Петри определяется как конечный префикс ее максимального ветвящегося процесса, полученный с помощью какого-либо критерия финитизации. В разделе описаны некоторые важные свойства полученных разверток. Для описания поведенческих свойств развертки и, в частности, для определения критериев финитизации вводится понятие конфигурации. Конфигурация развертки соответствует последовательности срабатывания исходной сети Петри. Введение понятия конфигурации позволяет рассматривать такие свойства развертки, как безопасность и полнота. Безопасность полученной развертки означает, что любой ее конфигурации соответствует некоторая достижимая разметка сети Петри. Свойство полноты развертки означает, что для любой достижимой разметки исходной сети Петри существует соответствующая ей конфигурация развертки. **Подразд. 1.1.3** посвящен описанию двух различных подходов к обнаружению тупиковых состояний в сетях Петри с использованием разверток. Первый подход был предложен МакМиланом в его работах, посвященных определению основных понятий теории разверток сетей Петри и возможностям их применения для верификации свойств распределенных систем. Во втором подходе поведение сети Петри представляется в виде системы линейных неравенств. Тупиковое

состояние системы соответствует некоторому специальному решению такой системы.

Разд. 1.2 посвящен описанию раскрашенных сетей Петри. В **подразд. 1.2.1** даны основные определения РСП. Модель типов данных РСП базируется на понятии мультимножества и на определенных над ним операторах и функциях. Понятие мультимножества является основой для определения цветовых множеств (или цветов) РСП. В подразделе описывается функционирование полученной РСП и дается определение достижимой разметки. Также приведен алгоритм построения графа достижимости для заданной РСП, рассматриваемого в дальнейшем в качестве пространства состояний при проведении процедуры проверки моделей (см. разд. 1.3). В **подразд. 1.2.2** приводятся определения спецификаций симметрии и эквивалентности на РСП. Спецификация симметрии является частным случаем спецификации эквивалентности и в дальнейших частях работы будет рассмотрена только в контексте более общего случая эквивалентности. В **подразд. 1.2.3** описаны РСП, расширенные двумя временными конструкциями. Первая модель представляет собой классическую дискретную модель интервального времени или так называемую модель времени по Мерлину. В данной модели с каждым переходом связывается интервал срабатывания. Переход может сработать, только, когда его временное значение находится в соответствующем интервале срабатывания. Вторая временная модель представляет собой модель временных штампов, введенную К. Йенсеном специально для РСП. В отличие от интервальной временной модели в модели Йенсена имеется понятие глобальных часов, посредством которых представляется текущее время. Некоторые множества цветов получают дополнительный временной признак. Элемент РСП, принимающий значение из такого множества, дополнительно несет значение, называемое временным штампом. Оно определяет момент времени, раньше которого данный элемент не может использоваться при срабатывании какого-либо перехода.

В **разд. 1.3** описаны методы проверки моделей для двух логических систем: логики линейного времени LTL и логики мю-исчисления. В **подразд. 1.3.1** формально описаны синтаксис и семантика логики LTL. В качестве семантической модели описано множество так называемых w-слов над некоторым специальным алфавитом. Кроме данной классической семантики приведена интерпретация формул LTL на сетях Петри. Описывается подмножество статтерно-эквивалентных формул логики LTL. Это подмножество используется в дальнейшем для проведения проверки моделей на сетях Петри с использованием разверток. **Подразд. 1.3.2** посвящен описанию логики мю-исчисления. Логика мю-исчисления является логикой вет-

вящегося времени и благодаря наличию элементов, соответствующих наибольшей и наименьшей неподвижной точке некоторого логического преобразования, представляет собой логическую систему с большой выразительной силой. В качестве семантической модели логики мю-исчисления рассматриваются структуры Крипке. В **подразд. 1.3.3** приведены классический алгоритм проверки моделей для автоматных сетей и его адаптация для стандартных сетей Петри. В данном подходе логическая формула также представляется в виде автоматной системы (так называемый автомат Бюхи), и суждение об истинности или ложности данной формулы делается на основе произведения системного автомата и автомата Бюхи, представляющего отрицание рассматриваемой формулы. В **подразд. 1.3.4** приведено описание классического алгоритма проверки моделей для логики мю-исчисления. Сложность данного алгоритма является экспоненциальной, что объясняется сложностью вычисления значения формулы мю-исчисления. Хотя в литературе имеется описание алгоритмов, уменьшающих данную сложность, эти улучшения являются несущественными в случаях, рассматриваемых в данной работе.

Во **второй главе** описываются развертки раскрашенных сетей Петри. **Разд. 2.1** посвящен определению ветвящегося процесса РСП и доказательству существования максимального ветвящегося процесса для заданной РСП. Определение ветвящегося процесса в случае РСП оказывается заметно сложнее классического определения для стандартных сетей Петри. В качестве основной конструкции берется О-сеть для стандартной сети Петри. Цветовые элементы отображаются с помощью двух дополнительных функций. Существование максимального ветвящегося процесса для РСП доказывается конструктивно. Приводится алгоритм построения ветвящегося процесса и доказывается соответствие полученной сети определению и ее максимальность. В разделе также описан рассматриваемый в работе подкласс РСП. На рассматриваемые РСП накладываются ограничения конечности множеств дуг и переходов, n-безопасности и конечности множеств цветовых элементов для данной сети. Свойство n-безопасности означает возможность пребывания максимального количества из n элементов в одном месте сети. Конечность множеств цветовых элементов означает конечность мощностей рассматриваемых мультимножеств.

В **разд. 2.2** определяются три типа точек сечения максимального ветвящегося процесса РСП, и дается определение разверток РСП как частей максимального ветвящегося процесса, полученных с помощью одного из критериев финитизации, которые, в свою очередь, опираются на определения точек сечения. При определении критериев финитизации для РСП ис-

пользуются адаптации определений точек сечения из области стандартных сетей Петри. Каждому критерию финитизации соответствует свой тип развертки РСП. Всего в работе рассматривается три различных типа разверток. Так как в качестве О-сети для РСП мы используем обычную (не раскрашенную) сеть, определения конфигураций для РСП получаются естественным образом. Как было сказано выше, возможность такого определения О-сети достигается с помощью введения двух дополнительных функций в определение максимального ветвящегося процесса РСП. Для полученных разверток доказываются свойства конечности, безопасности и полноты. Эти свойства уже были описаны в разд. 1.1 для стандартных сетей Петри. Первое свойство дает нам конечность развертки, полученной для любого критерия финитизации. Второе гарантирует отсутствие в развертках лишней информации о поведении РСП. Третье свойство дает нам существование во всех трех типах развертки полной информации о графе достижимости РСП.

В **разд. 2.3** приводятся два алгоритма построения разверток РСП. Для каждого из алгоритмов приводятся оценки сложности. Первый алгоритм является дальнейшим развитием алгоритма, использовавшегося при доказательстве существования максимального ветвящегося процесса для РСП. В общем случае, сложность этого алгоритма экспоненциальна по размеру полученной развертки. Это происходит из-за большого количества рекурсивных проходов по построенной части развертки. Тем не менее, этот алгоритм имеет достаточно четкую структуру и является удобным при проведении теоретических рассуждений. Второй алгоритм является адаптацией для РСП эффективного алгоритма построения разверток стандартной сети Петри, предложенного в работах А. Кондратьева, М. Кишиневского и др. Оценка сложности данного алгоритма является линейной от произведения числа мест и переходов полученной развертки. При применении данного алгоритма к РСП эта оценка умножается на параметр, связанный с мощностью множества цветов. Кроме алгоритмов раздел также содержит примеры построения разверток для РСП. В качестве примеров рассмотрены задача об обедающих философах, пример РСП, наглядно демонстрирующей различие между рассмотренными критериями финитизации, и пример коммуникационной системы "Отправитель-Получатель". Для примеров “Обедающие философы” и "Отправитель-Получатель" приведены теоретически полученные таблицы роста разверток и соответствующих графов достижимости. Данные результаты показали эффективность использования метода разверток в сравнении с классическими методами анализа полного графа достижимости. Для обоих примеров рост развертки в зависимости от раз-

меров сети существенно меньше роста соответствующего графа достижимости.

Разд. 2.4 содержит описание метода обнаружения тупиковых состояний в РСП. Метод формально описан и доказана теорема о корректности применения данного метода к РСП. Основу данного метода составляет описанное в первой главе представление работы стандартной сети Петри в виде системы неравенств. В данном разделе аналогичная система строится для РСП и с ее помощью либо обнаруживаются тупиковые состояния в рассматриваемой сети, либо доказывается их отсутствие.

В **третьей главе** описывается применение метода развертки к раскрашенным сетям Петри, расширенным спецификациями эквивалентности и двумя временными конструкциями. **Разд. 3.1** описывает построение разверток РСП в случае имеющейся в сети спецификации эквивалентности. Наличие эквивалентности позволяет дополнительно существенно сократить размер развертки и, таким образом, делает пространство поиска значительно меньше. Доказана теорема о полноте и безопасности полученной развертки. На примерах “Обедающие философы” и “Отправитель - Получатель” показывается дополнительное уменьшение развертки при применении данного подхода. В случае “Обедающих философов” рассматривается симметрия по числу философов. Использование развертки с симметрией не является для данного примера более эффективным, чем построение усеченного графа достижимости. В связи с этим представляет интерес следующий более сложный пример системы “Отправитель - Получатель”. Рассматривается абстракция от отправляемых данных, т.е. все данные, отправляемые “Отправителем” “Получателю”, считаются идентичными. Для данного примера использование развертки с абстракцией дает гораздо большее уменьшение размера пространства состояний, чем применение данной абстракции к графу достижимости системы. Так, например, при использовании 20 различных экземпляров данных и 20 составляющих компонентов как в системе “Отправителя”, так и в системе “Получателя”, полный размер графа достижимости составляет $1.73 \cdot 10^{174}$, в то время как размер развертки составляет лишь $1.28 \cdot 10^{11}$. При использовании упомянутой выше спецификации абстракции от данных размер графа достижимости уменьшается до $5.97 \cdot 10^{82}$. Такой размер графа достижимости не позволяет надеяться на проведение полного машинного эксперимента для верификации системы. Размер соответствующей развертки с применением абстракции составляет всего лишь $8.0 \cdot 10^{5}$, что является уже вполне реальным числом для проведения полностью автоматического эксперимента.

В **разд. 3.2** описывается применение метода развертки к РСП с интервальным временем (ИВРСП). В данной временной модели с каждым переходом связывается временной интервал, состоящий из двух натуральных чисел, задающих наиболее раннее и наиболее позднее время срабатывания перехода. Развертка ИВРСП определяется с помощью построения так называемого временного расширения. Временное расширение ИВРСП – это обычная РСП без времени, моделирующая работу временной сети. Для каждого перехода исходной ИВРСП вводятся соответствующие места временного расширения, хранящие значения времени для данного перехода. Таким образом, поведение временной сети удается промоделировать обычной (невременной) РСП. Полученное временное расширение удовлетворяет требованиям конечности, n-безопасности и конечности множеств цветовых элементов и, следовательно, для него существуют конечные, безопасные и полные развертки. Однако такие развертки содержат информацию, не относящуюся непосредственно к исходной ИВРСП. Поэтому вводится определение усеченной развертки, и развертка исходной ИВРСП определяется как усеченная развертка ее временного расширения. Для временного расширения и его усеченной развертки формулируется теорема о корректности рассмотренного подхода к определению разверток ИВРСП.

Разд. 3.3 посвящен определению разверток для РСП с моделью временных штампов (ВРСП). Применяется подход, аналогичный описанному в разд. 3.2. Основная трудность заключается в громоздкости модели временных штампов и, следовательно, в нетривиальности определения временного расширения ВРСП. После определения временного расширения, определяется его усеченная развертка, которая берется в качестве определения для развертки исходной ВРСП. Доказывается теорема о соответствии поведения исходной ВРСП и ее временного расширения. Эта теорема обосновывает корректность описанного подхода к определению разверток ВРСП.

Четвертая глава диссертации посвящена описанию метода проверки моделей с использованием разверток для раскрашенных сетей Петри. Прообразом данного подхода служит алгоритм, описанный в первой главе для стандартных сетей Петри. В **разд. 4.1** излагается семантика формул логики линейного времени для n-безопасных РСП и приводится описание алгоритма проверки моделей для обычных (нерасширенных) РСП. Первоначально, для формулы определяется автоматная РСП и дается формальное определение произведения исходной РСП и автоматной РСП для логического отрицания рассматриваемой формулы. Это произведение также является стандартной РСП, и для него можно построить различные виды разверток. Далее описывается, как построить граф, состоящий из точек сечения раз-

вертки полученного произведения, и доказывается, что содержание в этом графе циклических компонент эквивалентно ложности рассматриваемой формулы для исходной РСП. Это доказательство излагается в отдельной теореме, завершающей рассуждения данного раздела.

Разд. 4.2 посвящен изложению метода проверки моделей для РСП с использованием разверток при наличии на рассматриваемой сети спецификации эквивалентности. Первоначально определяется класс формул, совместимых с рассматриваемой спецификацией эквивалентности. Имея такую формулу, мы можем определить некоторую спецификацию эквивалентности на полученном произведении исходной РСП и автоматной РСП, описывающей отрицание логической формулы. Доказывается теорема, позволяющая использовать развертки с эквивалентностью, описанные в разд. 3.1, рассматриваемого произведения для проведения проверки моделей. Приводится пример, наглядно демонстрирующий существенное уменьшение размера полученной развертки при применении данного метода.

Разд. 4.3 содержит описание метода проверки моделей на временных раскрашенных сетях Петри. Описанный в разд. 4.1 метод переносится как на РСП с интервальной временной структурой, так и на РСП с временными штампами в качестве временной конструкции. Для указанных двух временных расширений РСП определяется семантика логики линейного времени (LTL) и доказываются теоремы, позволяющие использовать развертки временных РСП для проведения процедуры проверки моделей. Напомним, что развертка временной РСП определяется как усеченная развертка соответствующего временного расширения. Таким образом, для доказательства указанных теорем необходимо доказать следующие два утверждения. Во-первых, временное расширение сохраняет свойства, описываемые формулами LTL, т.е. истинность формулы LTL в РСП эквивалентна ее истинности во временном расширении РСП. Во-вторых, что при построении усеченной развертки мы не теряем информацию, связанную с истинностью или ложностью формул линейной логики. Первое утверждение оформлено в виде теоремы, второе, как более локальный факт, в виде утверждения. В этом разделе приводятся формальные доказательства обоих упомянутых утверждений.

В **пятой главе** описываются реализации классического подхода к проверке моделей РСП и метода проверки моделей, основанного на развертках. С каждой из систем проведен ряд экспериментов, результаты которых также изложены в данной главе. **Разд. 5.1** посвящен описанию реализованных систем проверки моделей для РСП. В **подразд. 5.1.1** представлена система верификации PNV (Petri Net Verifier), в которой в качестве логического

языка используется мю-исчисление и в качестве модели – граф достижимости РСП. В качестве метода проверки моделей применен стандартный алгоритм проверки моделей для мю-исчисления, описанный в разд. 4.1. В системе PNV имеется ряд возможностей, не используемых в данной работе. Это перевод спецификации РСП в программу на языке СПЕКТР-2 и создание моделирующей программы на языке C++. В качестве входного языка взят язык Standard ML, предложенный в работах К. Йенсена и принятый в качестве стандарта в системе Design/CPN. Спецификация сети на описанном входном языке подается на транслятор, который преобразует ее в интерпретируемую форму, являющуюся внутренним описанием РСП и использующуюся далее интерпретатором для построения модели. Полученная модель состоит из графа достижимости РСП и описания вершин графа достижимости в терминах разметок РСП. На следующем этапе графа достижимости подается на вход блоку проверки моделей, а описания вершин графа на вход блоку вычисления предикатов. Эти два взаимодействующих блока образуют модуль проверки моделей, на выходе которого мы имеем результат эксперимента. В **подразд. 5.1.2** дается описание реализации системы проверки моделей для логики линейного времени с использованием разверток. Система является прототипной реализацией и в отличие от системы PNV не является полностью автоматической. Целью реализации данной системы было показать возможность реализации эффективного метода проверки моделей для РСП и привести несколько примеров верификации моделей распределенных систем. На вход системе поступает произведение системной РСП и автоматной РСП, представляющей отрицание логической спецификации и критерий финитизации максимального ветвящегося процесса. Для данного произведения система строит соответствующую развертку и граф, состоящий из точек сечения развертки. Структура полученного графа, а именно, наличие или отсутствие в нем сильно связных компонент, является критерием истинности или ложности логической спецификации на рассматриваемой сети.

Разд. 5.2 содержит описание экспериментов, проведенных с двумя, описанными выше, системами. Результаты проведенных экспериментов показали возможность и целесообразность применения метода проверки моделей с использованием разверток для верификации моделей распределенных систем. В **подразд. 5.2.1** рассматривается РСП, представляющая задачу об обедающих философах. Для данной сети рассматриваются свойства прогресса и тупиков. Свойства прогресса описывают динамическое поведение системы, например, возможность сколь угодно частого срабатывания некоторых переходов или недопустимость ситуаций, в которых неко-

торые переходы будут блокированы. Тупиковым называется такое состояние системы, в котором никакое действие не является возможным. Свойства описываются в двух логических системах – логике LTL и логике мю-исчисления. Затем полученные спецификации проверяются как с помощью системы PNV, так и с помощью системы, базирующейся на развертках РСП. В **подразд. 5.2.2** рассматривается верификация модели однобитового коммуникационного протокола (АВР). Протокол состоит из частей "Приемник" и "Передатчик", взаимодействующих посредством двух ненадежных каналов. Ненадежность каналов означает, что любой из отправленных пакетов может быть потерян. Искажения отправленного пакета средой считаются недопустимы. Кроме свойств прогресса и тупиков, описанных выше для случая обедающих философов, для коммуникационного протокола имеет смысл рассматривать, так называемые, свойства безопасности. Свойства безопасности описывают, например, правильный порядок приема сообщений или правильную работу "Приемника" по формированию подтверждений на полученные сообщения. Как свойства прогресса и тупиков, так и свойства безопасности, были описаны в логиках LTL и мю-исчисления и верифицированы как с помощью системы PNV, так и с помощью системы, базирующейся на развертках РСП. В **подразд. 5.2.3** описана и верифицирована модель кольцевого протокола. Протокол описывает взаимодействие нескольких станций, соединенных в кольцо. По кольцу циркулирует фрейм фиксированной длины. Станция, обладающая в данный момент фреймом, имеет возможность отправить или считать некоторый пакет данных. Протокол является полностью детерминированным, что исключает целесообразность использования для него методов, базирующихся на частичном порядке и, в частности, методов развертки. Данный протокол был верифицирован с использованием системы PNV. Для кольцевого протокола, помимо проверки свойств прогресса, тупиков и безопасности, был проведен ряд экспериментов, связанных с обнаруженной в работах группой авторов лаборатории теоретического программирования ИСИ СО РАН неэффективностью работы данного протокола. Эта неэффективность также была установлена в экспериментах с системой PNV и для достаточно общих случаев было показано ее отсутствие при внесении в систему требуемых изменений. В **подразд. 5.2.4** рассматривается модель коммуникационного протокола “Отправитель – Получатель”, в которой передача сообщений производится через специальный буфер. Отправка подтверждений о получении сообщений отсутствует. Для данного протокола проверялись свойства прогресса и безопасности. Проведенные эксперименты показали эффектив-

ность использования метода проверки моделей с использованием разверток для данного примера.

Основные выводы и результаты. В рамках диссертации были получены следующие результаты.

- Дано определение ветвящегося процесса для РСП и доказано существование максимального ветвящегося процесса для РСП, удовлетворяющих некоторым естественным ограничениям. Определены развертки РСП и для них доказаны свойства конечности, безопасности и полноты. Приведены два алгоритма построения разверток РСП. Описаны методы обнаружения тупиков в РСП с использованием разверток.
- Определены развертки раскрашенных сетей Петри, расширенных спецификациями эквивалентности и двумя временными конструкциями – интервальным временем и моделью временных штампов. Для полученных разверток доказаны важные свойства, позволяющие использовать данные развертки при верификации расширенных РСП.
- Для РСП разработан метод проверки моделей с использованием разверток. Корректность полученного алгоритма формально доказана. Алгоритм проверки моделей также применен к РСП, расширенным спецификациями эквивалентности и временными конструкциями.
- Реализован блок проверки моделей в системе PNV. Проведена прототипная реализация метода проверки моделей с использованием разверток. Проведен ряд экспериментов с системой PNV и системой проверки моделей с использованием разверток.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Козюра В.Е. Реализация системы проверки моделей раскрашенных сетей Петри с использованием разверток. — Новосибирск, 2002. — 32 с. – (Препр. / Сиб. отд-ние РАН. ИСИ; № 94).

2. Козюра В.Е., Непомнящий В.А., Новиков Р.М. Верификация раскрашенных сетей Петри методом проверки моделей. — Новосибирск, 2001. — 24 с. – (Препр. / Сиб. отд-ние РАН. ИСИ; № 89).

3. Козюра В.Е., Новиков Р.М. Использование метода проверки моделей для верификации коммуникационных протоколов, представленных раскрашенными сетями Петри // Тез. докл. IV сибирского конгресса по прикладной и индустриальной математике (ИНПРИМ-2000). – Новосибирск, 2000. – Ч. V. - С. 44.

4. Козюра В.Е., Новиков Р.М. Верификация коммуникационных протоколов с использованием системы PNV // Материалы молодежной научн. конф., посвященной 10-летию ИВТ СО РАН, Новосибирск, Академгородок, 25 – 26 декабря, 2000.

5. Kozura V.E. Unfoldings of Coloured Petri Nets. – Novosibirsk, 2000. – 34p. – (Prepr. / SD RAS IIS; № 80).

6. Kozura V.E. Unfoldings of Coloured Petri Nets // Proc. 4th Internat. A.Ershov Memorial Conf. «Perspectives of System Informatics", (PSI'01). – Berlin a.o.: Springer-Verlag, 2001. – P. 268–278. – (Lect. Notes Comput. Sci.; Vol. 2244).

7. Kozura V.E. Unfoldings of Timed Coloured Petri Nets. – Novosibirsk, 2001. – 33p. – (Prepr. / SD RAS IIS; № 82).

8. Kozura V.E. Unfoldings of Timed Coloured Petri Nets // Proc. of the Workshop on Concurrency, Specification and Programming 2001 (CS&P'2001), Warsaw 3–5 October 2001. – P. 128–139.

9. Kozura V.E. LTL model checking of coloured Petri nets based on net unfoldings // Joint Bulletin of NCC & IIS. Ser.: Comput. Sci. – 2001. – №15. – P. 83–101.

10. Kozura V.E., Nepomniaschy V.A., Novikov R.M. Verification of Distributed Systems Modelled by High-level Petri Nets // Proc. Internat. Conf. on Parallel Computing in Electrical Engineering (PARELEC 2002), Warsaw, Poland. –IEEE Computer Society, 2002. – P.61–66.

Личный вклад автора

Все включенные в диссертационную работу теоретические результаты получены автором лично. В практической части личным вкладом является реализация системы проверки моделей в системе PNV и реализация системы проверки моделей с использованием разверток.

В.Е. Козюра

РАЗВЕРТКИ РАСКРАШЕННЫХ СЕТЕЙ ПЕТРИ И ИХ ПРИМЕНЕНИЕ ДЛЯ ВЕРИФИКАЦИИ МОДЕЛЕЙ РАСПРЕДЕЛЕННЫХ СИСТЕМ

Подписано в печать 15.12.03 Объем 1.0 уч.-изд.л.
Формат бумаги 60 × 84 1/16 Тираж 100 экз.

ЗАО РИЦ «Прайс-курьер»
630090, г. Новосибирск, пр. Акад. Лаврентьева, 6, тел. (383-2) 34-22-02