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

На правах рукописи

Покозий Екатерина Александровна

МЕТОДЫ СПЕЦИФИКАЦИИ И ВЕРИФИКАЦИИ ПАРАЛЛЕЛЬНЫХ МОДЕЛЕЙ С НЕПРЕРЫВНЫМ ВРЕМЕНЕМ

05.13.11 — математическое и программное обеспечение вычислительных машин, комплексов, систем и сетей

Автореферат
диссертации на соискание ученой степени
кандидата физико-математических наук

Новосибирск, 1999

Работа выполнена в Институте систем информатики
Сибирского отделения Российской академии наук

Научный руководитель:	кандидат физико-математических наук, Вирбицкайте И.Б.
Официальные оппоненты:	доктор технических наук, Бандман О.Л. кандидат физико-математических наук, Соколов В.А.
Ведущая организация:	Томский политехнический университет

Защита состоится 7 июня 1999 года в 14 час. 30 мин. на заседании диссертационного совета К0003.93.01 в Институте систем информатики Сибирского отделения РАН по адресу:

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

С диссертацией можно ознакомится в читальном зале библиотеки ВЦ СО РАН (пр. Лаврентьева, 6).

Автореферат разослан "___" апреля 1999 г.

Ученый секретарь
специализированного совета
К0003.93.01
к.ф.-м.н. М.А.Бульонков

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность. Параллельная обработка информации широко используется для увеличения производительности вычислительных систем. Особое место среди параллельных систем занимают системы реального времени, поведение которых в значительной степени зависит от количественных временных характеристик. Процесс проектирования систем такого типа — нетривиальная задача, требующая для своего решения фундаментальных исследований, основанных на различных формальных методах и средствах, которые варьируются в зависимости от класса моделируемых систем, степени детализации их структуры и поведения, а также от характера изучаемых проблем.

Для систем реального времени важны как модели времени, так и модели вычислений. Известны следующие дихотомии при задании временных характеристик: явное/неявное, линейное/ветвистое, ссылками на временные точки/интервалы, в непрерывной/дискретной временной области. Введение временных характеристик привело к появлению многих специализированных моделей вычислений с известными различиями: синхронные/асинхронные, с глобальным/локальным временем, интерливинговые/"истинно" параллельные, соотношением между действиями и временем (действия с нулевыми задержками).

Среди наиболее популярных формализмов систем реального времени встречаются как интерливинговые модели: временные автоматы, временные системы переходов, алгебры временных процессов, так и модели "истинного параллелизма": временные структуры событий, временные причинно-следственные структуры, временные и стохастические сети Петри.

Темпоральные логики являются удобным формализмом для спецификации и верификации свойств параллельных и распределенных систем. В данной проблематике сформировалось два подхода: аксиоматический и алгоритмический. При первом подходе разрабатывается система аксиом, с помощью которой может быть описана как сама система, так и ее свойства. Для верификационных целей используется механический доказыватель теорем. Основу второго подхода составляют алгоритмы проверки на моделях (model checking), объединяющие в себе традиционные и логические методы анализа свойств параллельных/распределенных систем. Основная цель исследований в этой области состоит в том, чтобы сформулировать ясную логическую основу для

создания автоматических систем верификации, синтеза и оптимизации параллельных систем.

Известно, что к сетям Петри могут быть применены эффективные и довольно мощные алгоритмы верификации. Однако исследования по верификации свойств временных сетей Петри значительно менее продвинуты. Известен верификационный алгоритм для временных сетей Петри и темпоральной логики линейного времени.

Интересной задачей является верификация количественных свойств систем реального времени. Для выражения таких свойств удобно использовать темпоральные логики реального времени. Р. Алюром был предложен алгоритм верификации свойств временных автоматов средствами темпоральной логики реального времени TCTL. Однако, применение логик реального времени для верификации свойств временных сетей Петри остается открытым вопросом. Другая проблема верификации реальных систем состоит в том, что приходится анализировать огромное число состояний. Один из способов решения этой проблемы заключается в применении техники "частичных порядков", которая позволяет редуцировать число верифицируемых состояний за счет параллелизма, присущего системе.

Традиционно используемые модели систем реального времени требуют детальной спецификации временных ограничений и при "настройке" системы каждое изменение временных ограничений влечет необходимость нового выполнения верификационного алгоритма. Интересной задачей является создание временной модели, допускающей менее подробную спецификацию временных ограничений. Одним из подходов к решению этой задачи является введение параметров во временные спецификации. В качестве средства описания свойств системы при верификации подобной параметрической модели естественно выбрать формализм, позволяющий выражать свойства с параметрическими временными ограничениями. Таким формализмом является, например, параметрическая темпоральная логика реального времени PTCTL, предложенная Ф. Вангом. Для модификации временных сетей Петри за счет введения параметров задача верификации состоит в нахождении значений параметров, при которых выполнено проверяемое свойство.

Еще одной задачей, возникающей при верификации систем реального времени является проверка свойств параллелизма. Существующие темпоральные логики реального времени имеют интерливинговую семантику и, следовательно, не позволяют напрямую описывать свойства, связанные с параллелизмом. С другой стороны, поскольку временные

сети Петри являются моделью "истинного параллелизма"и позволяют явно выражать параллелизм системы, для их анализа требуется логика, имеющая средства для описания как количественных характеристик, так и параллельных свойств.

Таким образом, в области верификации параллельных систем реального времени актуальными являются, с одной стороны, задачи увеличения выразительной мощности временных моделей и темпоральных логик, с другой — задачи повышения эффективности верификационных алгоритмов.

Цель диссертации. Введение и изучение системы формальных понятий, методов и средств спецификации и анализа поведения систем реального времени, представленных сетями Петри с непрерывным временем. Достижение цели связывается с решением следующих задач:

1. Разработка новых темпоральных языков реального времени с элементами параллелизма, позволяющих специфицировать и верифицировать поведение параллельных/распределенных систем реального времени.
2. Увеличение выразительных мощностей средств описания и изучения систем реального времени посредством введения параметров во временные спецификации.
3. Построение эффективных процедур верификации поведенческих свойств параллельных систем реального времени, представленных в виде различных моделей сетей Петри с непрерывным временем.

Методы исследования. В качестве формальной модели параллелизма используются временные сети Петри, а также их подклассы (временные сети, удовлетворяющие прогресс-условию; безопасные временные сети) и расширения (параметрические временные сети). В рамках данной работы используется такой формализм, как аппарат темпоральных логик. Кроме того, применяются методы теории графов и линейного программирования.

Научная новизна состоит в разработке оригинального подхода к решению задач спецификации и верификации систем реального времени средствами различных логических формализмов. Научную новизну раскрывают следующие результаты:

- Введена и исследована новая модель параллельных систем реального времени — параметрические временные сети, которые

являются модификацией временных сетей Петри за счет введения параметров в спецификации временных ограничений. Достоинство данной модели состоит в том, что не требуется детальная спецификация временных ограничений.

- Предложена новая темпоральная логика реального времени, содержащая средства для описания свойств параллелизма в системах реального времени. Такая логика позволяет адекватно описывать системы, представленные моделями с семантикой "истинного параллелизма".
- Разработаны алгоритмы верификации поведенческих свойств различных временных сетевых моделей с использованием аппарата темпоральных логик реального времени.
- Предложен метод редукции числа верифицируемых сетевых состояний, позволяющий учитывать как параллелизм сети, так и существенность временных ограничений при проверке заданного свойства.

Практическая ценность данных исследований состоит в возможности их использования при создании автоматизированных систем верификации систем реального времени. В частности, результаты диссертационной работы использовались при создании модуля верификации в системе PEP (Programming Environment based on Petri nets), совместно разрабатываемой Институтом информатики Университета г. Хильдесхайма (Германия) и лабораторией теоретического программирования ИСИ СО РАН.

Апробация работы проведена на следующих международных научных конференциях.

1. 4^{th} *Workshop on Logic, language, Information and Computation*, Fortaleza (Ceara), Brazil, August 1997.
2. *Distributed data processing (DDP'98)*, Novosibirsk, Russia, June 1998.
3. *International Workshop on Discrete Event Systems (WODES'98)*, Cagliari, Italy, August 1998.
4. *1st International conference on practical and theoretical programming (UkrProg'98)*, Kiev, Ukraine. September 1998.

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

Публикации. По теме диссертации опубликовано 9 научных работ.

Структура и объем работы. Диссертация состоит из введения, трех глав, заключения и списка литературы из 57 наименований. Основное содержание составляет 71 страницу. Работа включает 11 рисунков.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность рассматриваемых вопросов, формулируются цели и указываются методы исследований, описывается научная новизна результатов, практическая ценность работы, приводится список конференций и семинаров, на которых проведена апробация данных исследований, дается краткий обзор работы по главам.

В **первой главе** предлагается эффективный метод анализа поведенческих свойств временных сетей Петри, основанный на темпоральной логике реального ветвящегося времени TCTL.

В **разделе 1.1** даются определения, связанные с понятием временной сети модели Мерлина.

Временная сеть $\mathcal{N} = (P, T, F, Eft, Lft, m_0)$ характеризуется непересекающимися конечными множествами мест P и переходов T, отношением инцидентности $F \subseteq (P \times T) \cup (T \times P)$, начальной разметкой m_0 и целочисленными временными ограничениями: нижней (Eft) и верхней (Lft) временными границами, сопоставляемыми ее переходам. Ограничимся рассмотрением однобезопасных временных сетей. *Состоянием* временной сети назовем пару, состоящую из разметки (множества мест, содержащих фишки) и множества вещественнозначных счетчиков, сопоставленных с переходами. Во временной сети смена одного состояния другим осуществляется либо при истечении некоторого времени, либо при срабатывании некоторого перехода. Поведение временной сети моделируется путями – последовательностями состояний, связанных срабатыванием переходов или истечением времени.

В **разделе 1.2** приводятся синтаксис и семантика известной темпоральной логики реального времени TCTL, предложенной Р. Алюром. Данная логика является расширением языка ветвящегося времени CTL за счет добавления временных ограничений на его операторы. Семантика TCTL определяется на состояниях и путях временной сети. Будем говорить, что временная сеть $\mathcal{N}$ *удовлетворяет* TCTL-формуле ϕ, если ϕ выполняется в начальном состоянии $\mathcal{N}$.

В **разделе 1.3** разработан и исследован алгоритм, проверяющий, выполняется ли для временной сети некоторое свойство, заданное в виде

TCTL-формулы.

Поскольку понятие временной сети базируется на модели непрерывного времени, то число состояний любой временной сети бесконечно. Чтобы получить конечное представление сетевого поведения, введем понятие обобщенного состояния. Два состояния временной сети принадлежат одному и тому же обобщенному состоянию, если они в некотором смысле эквивалентны, то есть их разметки совпадают и значения соответствующих счетчиков согласованы по целым частям и порядку дробных частей. В качестве конечного представления поведения временной сети $\mathcal{N}$ при анализе TCTL-формулы ϕ строим граф обобщенных состояний $G(\mathcal{N}, \phi)$ с вершинами, соответствующими обобщенным состояниям и дугами, соответствующими срабатыванию переходов или истечению времени. Размер $G(\mathcal{N}, \phi)$ экспоненциален относительно размера $\mathcal{N}$.

Алгоритм верификации TCTL-формулы ϕ на временной сети $\mathcal{N}$ состоит в построении графа обобщенных состояний $G(\mathcal{N}, \phi)$ и пометке его вершин подформулами ϕ или их отрицанием. Чтобы проверить временные ограничения, встречающиеся в ϕ, для каждого ограничения $\sim c$ вводится новая элементарная формула $p_{\sim c}$, истинная тогда и только тогда, когда это ограничение выполнено. Алгоритм пометки вершины v подформулами ϕ рекурсивен. Для элементарных формул и логических связок пометка вершины v определяется естественным образом. Вершина v помечается формулой вида $\forall\phi_1\mathcal{U}_{\sim c}\phi_2$ ($\exists\phi_1\mathcal{U}_{\sim c}\phi_2$), если в $G(\mathcal{N}, \phi)$ для любого пути, начинающегося в v (существует путь, начинающийся в v такой, что), его n-ая вершина помечена формулами ϕ_2 и $p_{\sim c}$ для некоторого $n \geq 1$, а все предшествующие ей вершины помечены формулой ϕ_1. Будем говорить, что временная сеть $\mathcal{N}$ удовлетворяет TCTL-формуле ϕ, если и только если начальная вершина $G(\mathcal{N}, \phi)$ помечена ϕ. Следующая лемма устанавливает корректность алгоритма пометки.

Лемма 1.3.4. Пусть ϕ' — подформула TCTL-формулы ϕ. Предложенный алгоритм помечает вершину v из $G(\mathcal{N}, \phi)$ формулой ϕ' тогда и только тогда, когда ϕ' выполняется на состоянии в $\mathcal{N}$, принадлежащем v.

Далее дана оценка сложности предложенного алгоритма:

Теорема 1.3.2. Существует алгоритм, проверяющий, что временная сеть $\mathcal{N}$ удовлетворяет TCTL-формуле ϕ, который линеен по длине ϕ и размеру $G(\mathcal{N}, \phi)$ (и, следовательно, экспоненциален по размеру $\mathcal{N}$).

Введено понятие временной статтеринг-эквивалентности для графов

обобщенных состояний, позволяющее осуществлять их корректную редукцию. Пусть даны временная сеть $\mathcal{N}$ и TCTL-формула ϕ. Будем говорить, что место в $\mathcal{N}$ *существенно для* ϕ, если в ϕ существует элементарная формула, соответствующая данному месту. Далее, будем говорить, что два графа обобщенных состояний $G' = G(\mathcal{N}, \phi')$ и $G'' = G(\mathcal{N}, \phi'')$ *статтеринг-эквивалентны относительно TCTL-формулы* ϕ, если на множествах их вершин определено отношение *временной статтеринг-эквивалентности:*

1. начальные вершины G' и G'' статтеринг-эквивалентны;
2. вершины v' из G' и v'' из G'' статтеринг-эквивалентны, если
   - их разметки на множестве мест, существенных для ϕ, совпадают и значения их счетчиков согласованы относительно временных ограничений из ϕ;
   - каждой дуге (v', v) из G' соответствует конечный путь в G'', в котором все вершины, кроме последней, статтеринг-эквивалентны v', а последняя вершина статтеринг-эквивалентна v;
   - аналогично предыдущему пункту, меняя местами G' с G'', а также v' с v''.

Теорема 1.3.1. Пусть графы обобщенных состояний $G(\mathcal{N}, \phi')$ и $G(\mathcal{N}, \phi'')$ статтеринг-эквивалентны относительно TCTL-формулы ϕ. Далее, пусть v' и v'' – вершины в $G(\mathcal{N}, \phi')$ и $G(\mathcal{N}, \phi'')$ соответственно. Если вершины v' и v'' статтеринг-эквивалентны, то v' помечена формулой ϕ тогда и только тогда, когда v'' помечена формулой ϕ.

В **разделе 1.4** описано использование техники "частичных порядков" для редукции числа анализируемых обобщенных состояний временной сети. Данный метод редукции использует тот факт, что многие свойства не 'чувствительны' к порядку, в каком выполняются параллельные переходы временной сети, что позволяет избежать конструирования эквивалентных состояний (то есть состояний, достижимых срабатыванием различных интерливинговых последовательностей переходов). Особенность предложенной редукции состоит в учете как параллелизма сети, так и существенности временных ограничений при проверке выполнимости заданного свойства. Будем говорить, что в вершине v графа обобщенных состояний $G(\mathcal{N}, \phi)$ время *существенно* для ϕ, если для некоторого временного ограничения $\sim c$ из ϕ время, соответствующее вершине v, не превышает c. Идея редукции состоит в следующем: для каждой вершины v строящегося редуцированного графа

обобщенных состояний $G_R(\mathcal{N}, \phi)$ при порождении следующих вершин рассматриваются не все срабатывающие переходы (как при построении $G(\mathcal{N}, \phi)$), а их подмножество и, кроме того, истечение времени, если в вершине v время существенно для ϕ. Показано, что редукционная процедура полиномиальна по размеру временной сети.

Теорема 1.4.1. Для заданных временной сети $\mathcal{N}$ и TCTL-формулы ϕ графы обобщенных состояний $G(\mathcal{N}, \phi)$ и $G_R(\mathcal{N}, \phi)$ статтеринг-эквивалентны.

Таким образом, алгоритм пометки для $G(\mathcal{N}, \phi)$ сводится к алгоритму пометки для $G_R(\mathcal{N}, \phi)$.

В конце главы приведены некоторые сведения об экспериментальных результатах, подтверждающие эффективность предложенной редукции.

Во **второй главе** вводится понятие параметрической временной сети, а также предлагается и исследуется метод поведенческого анализа параметрических временных сетей, основанный на параметрической темпоральной логике реального времени PTCTL.

В **разделе 2.1.** вводятся основные определения, касающиеся параметрической временной сети и ее поведения.

Введем конечное множество параметров. *Параметрическая временная сеть* $\mathcal{PN} = (P, T, F, \tau, m_0)$ характеризуется непересекающимися конечными множествами мест P и переходов T, отношением инцидентности $F \subseteq (P \times T) \cup (T \times P)$, начальной разметкой m_0 и функцией τ, сопоставляющей каждому переходу некоторый *временной предикат*, индуктивно определяющийся следующим образом: $\eta = false \mid x \sim \theta \mid \eta_1 \rightarrow \eta_2$, где θ – параметр или натуральное число, x – переход в $\mathcal{PN}$, η_1 и η_2 – временные предикаты и $\sim$ — одно из бинарных отношений $<, \leq, =, \geq, >$. Ограничимся рассмотрением однобезопасных параметрических временных сетей.

Вводится понятие *означивания* как функции, сопоставляющей каждому параметру некоторое натуральное число. Означивание называется *c-ограниченным* для некоторого натурального числа c, если оно сопоставляет каждому параметру значение, не превышающее c. Для заданного означивания χ, обозначим параметрическую временную сеть $\mathcal{PN}$ с означенными посредством χ параметрами через $\mathcal{PN}^{\chi}$. Будем называть *означенной* параметрическую временную сеть, все параметры которой означены посредством некоторого χ. Функционирование модели определяется для означенных параметрических временных сетей. Состояние

означенной параметрической временной сети определяется аналогично состоянию временной сети, определенному в главе 1. Будем говорить, что переход t *готов* в состоянии q означенной параметрической временной сети $\mathcal{PN}$, если в $\mathcal{PN}$ все входные места перехода t имеют фишки. В означенной параметрической временной сети смена одного состояния другим осуществляется либо при истечении некоторого времени, либо при срабатывании некоторого перехода. Пусть q – состояние в $\mathcal{PN}^\chi$. Будем говорить, что в состоянии q переход $t \in T$ *может сработать*, если он готов в q и временной предикат $\tau(t)$ при означивании χ и подстановке вместо переходов соответствующих значений счетчиков – истинен. Будем говорить, что в состоянии q *может пройти время* δ, если для всякого перехода t, готового в q, временной предикат $\tau(t)$ при означивании χ и подстановке вместо переходов соответствующих значений счетчиков будет истинен через некоторое время, не меньшее, чем δ.

В **разделе 2.2** приведены синтаксис и семантика параметрической темпоральной логики реального времени PTCTL (Parametric Timed Computation Tree Logic), предложенной Ф. Вангом. PTCTL является расширением известной логики ветвящегося времени TCTL за счет введения параметрических переменных, представляющих неспецифицированные временные ограничения, в ее операторы. Семантика PTCTL определяется на состояниях и путях означенной параметрической временной сети. Для заданного означивания χ, обозначим PTCTL-формулу ϕ с означенными посредством χ параметрами через ϕ^χ. Будем говорить, что параметрическая временная сеть $\mathcal{PN}$ *удовлетворяет* PTCTL-формуле ϕ при означивании χ, если формула ϕ^χ выполняется в начальном состоянии $\mathcal{PN}^\chi$.

Задача c-ограниченного анализа параметрической временной сети $\mathcal{PN}$ относительно PTCTL-формулы ϕ состоит в нахождении c-ограниченного означивания χ такого, что $\mathcal{PN}$ удовлетворяет формуле ϕ при означивании χ.

В **разделе 2.3** строится конечное представление поведения параметрической временной сети на основе понятия обобщенного состояния.

Для конечного представления поведения означенной параметрической временной сети $\mathcal{PN}^\chi$ при анализе PTCTL-формулы ϕ используется граф обобщенных состояний $G(\mathcal{PN}^\chi, \phi^\chi)$. c-ограниченный граф обобщенных состояний $G(\mathcal{PN}, \phi, c)$ для параметрической временной сети $\mathcal{PN}$ и PTCTL-формулы ϕ строится как объединение графов обобщенных состояний $G(\mathcal{PN}^\chi, \phi^\chi)$ по всем c-ограниченным означиваниям χ. Для определения временной длительности путей в графе вводится

понятие кактус-структуры, которая представляет собой набор простых циклов, связанных с некоторым простым путем. Данное понятие позволяет выразить время произвольного пути в графе обобщенных состояний через времена простых путей и циклов.

В **разделе 2.4** разрабатывается алгоритм решения задачи c-ограниченного анализа параметрической временной сети $\mathcal{PN}$ относительно PTCTL-формулы ϕ, который заключается в построении графа обобщенных состояний $G(\mathcal{PN}, \phi, c)$ и пометке пары (v, ϕ'), где v – вершина $G(\mathcal{PN}, \phi, c)$ и ϕ' – подформула формулы ϕ, некоторой формулой логики первого порядка $L(v, \phi')$, называемой *условием*, с параметрами в качестве свободных переменных. Для c-ограниченного означивания χ, будем говорить, что χ является решением задачи c-ограниченного анализа параметрической временной сети $\mathcal{PN}$ относительно PTCTL-формулы ϕ, если для начальной вершины v_0 из $G(\mathcal{PN}, \phi, c)$ означивание χ удовлетворяет условию $L(v_0, \phi)$. Следующая теорема устанавливает корректность алгоритма пометки:

Теорема 2.4.1. Пусть даны задача c-ограниченного анализа параметрической временной сети $\mathcal{PN}$ относительно PTCTL-формулы ϕ, ϕ' – подформула ϕ, c-ограниченное означивание χ и вершина v в $G(\mathcal{PN}^\chi, \phi^\chi)$. χ удовлетворяет условию $L(v, \phi')$, тогда и только тогда, когда ϕ'^χ выполняется на состоянии в $\mathcal{PN}^\chi$, принадлежащем v.

Далее дана оценка сложности предложенного алгоритма:

Теорема 2.4.2. Существует алгоритм решения задачи c-ограниченного анализа параметрической временной сети $\mathcal{PN}$ относительно PTCTL-формулы ϕ, который линеен по размеру ϕ и дважды экспоненциален по размеру $\mathcal{PN}$.

Третья глава посвящена введению новой темпоральной логики непрерывного времени с элементами параллелизма – TCCTL и ее использованию для спецификации и верификации поведения систем реального времени. Как и в главе 1 в качестве модели систем реального времени рассматриваются однобезопасные временные сети модели Мерлина.

В **разделе 3.1** вводится понятие поддерева на состояниях временной сети для представления параллельного поведения системы. Традиционно для описания поведения временных сетей используют последовательности состояний, называемые путями. Однако, такое представление теряет информацию о параллелизме системы. Введем отношение, сопоставляющее состоянию множество состояний, в которые можно пе-

рейти из него параллельным выполнением некоторого множества переходов. Такое отношение дает возможность различать точки параллельного ветвления и точки недетерминированного выбора. На основе этого отношения вводится понятие поддерева, как одного из возможных поведений системы, учитывающего параллельные выполнения переходов.

В **разделе 3.2** даются синтаксис и семантика новой темпоральной логики реального времени TCCTL (Timed Concurrent Computation Tree Logic), которая является расширением языка ветвящегося времени CCTL, предложенного Пенчеком, за счет добавления временных ограничений на его операторы. Специфику временной области удачно отражает темпоральный оператор $Until$, позволяющий выражать свойства вида "формула ϕ_1 истинна до тех пор, пока не станет истинной формула ϕ_2". Чтобы выражать свойства, связанные с параллелизмом, удобно использовать модификацию темпорального оператора $Next$ для логики непрерывного времени, которая позволяет выражать свойства вида "формула ϕ истинна после срабатывания произвольного перехода". В TCCTL в качестве темпоральных операторов взяты операторы $Next$ (X) и $Until$ $(\mathcal{U})$ с явными временными границами.

Фиксируем временную сеть $\mathcal{N}$. Множества *state-формул* и *tree-формул* определяются взаимно-индуктивно:

1. в качестве множества элементарных state-формул используется множество мест временной сети $\mathcal{N}$;
2. если ϕ_1 и ϕ_2 – state-формулы, то $\neg\phi_1$ и $\phi_1 \wedge \phi_2$ – state-формулы;
3. если ϕ_1 и ϕ_2 – state-формулы, то $\mathbf{A}X_{\sim c}\phi_1$, $\mathbf{E}X_{\sim c}\phi_1$, $\mathbf{A}\phi_1\mathcal{U}_{\sim c}\phi_2$, $\mathbf{E}\phi_1\mathcal{U}_{\sim c}\phi_2$,– tree-формулы;
4. если ϕ_1 и ϕ_2 – tree-формулы, то $\neg\phi_1$ и $\phi_1 \wedge \phi_2$ – tree-формулы;
5. если ϕ_1 – tree-формула, то $\forall\phi_1$ и $\exists\phi_1$ – state-формулы.

Здесь $\mathbf{A}, \mathbf{E}$ – кванторы по путям, $\sim$ — одно из бинарных отношений $<, \leq, =, \geq, >$. State-формулы интерпретируются на состояниях вовременной сети $\mathcal{N}$, в то время как tree-формулы интерпретируются на поддеревьях в $\mathcal{N}$. Кванторы по поддеревьям позволяют выражать свойства, выполненные для всех (для некоторых, в зависимости от квантора) поддеревьев с корнем в рассматриваемом состоянии. Будем говорить, что временная сеть $\mathcal{N}$ *удовлетворяет* state-формуле ϕ, если ϕ выполняется в начальном состоянии $\mathcal{N}$.

В **разделе 3.3** предложен алгоритм, проверяющий, выполняется ли для временной сети некоторое свойство, выраженное на языке TCCTL. В качестве конечного представления поведения временной сети $\mathcal{N}$ при анализе state-формулы ϕ рассматривается структура обобщенных со-

стояний $\mathcal{M}(\mathcal{N}, \phi)$, получающаяся в результате дискретизации множества поддеревьев в $\mathcal{N}$. Размер $\mathcal{M}(\mathcal{N}, \phi)$ экспоненциален относительно размера $\mathcal{N}$. Алгоритм верификации state-формулы ϕ на временной сети $\mathcal{N}$ состоит в построении структуры обобщенных состояний $\mathcal{M}(\mathcal{N}, \phi)$ и пометке вершин $\mathcal{M}(\mathcal{N}, \phi)$ state-подформулами формулы ϕ и дуг $\mathcal{M}(\mathcal{N}, \phi)$ — tree-подформулами формулы ϕ. Идея алгоритма пометки дуг состоит в следующем: дуга из $\mathcal{M}(\mathcal{N}, \phi)$ помечается tree-формулой ϕ' тогда и только тогда, когда она принадлежит некоторому поддереву в $\mathcal{M}(\mathcal{N}, \phi)$, на котором ϕ' истинна. Для проверки истинности tree-формулы на поддереве используется алгоритм, аналогичный алгоритму пометки, описанному в главе 1. В алгоритме пометки вершин наиболее сложным является случай формул с кванторами по поддеревьям. Вершина v помечается state-формулой $\exists\phi$ ($\forall\phi$), если в $\mathcal{M}(\mathcal{N}, \phi)$ не существует дуги, помеченной tree-формулой $\neg\phi$ (существует дуга, начинающаяся в v, помеченная tree-формулой ϕ). Для случаев элементарных формул и логических связок пометка вершины определяется естественным образом. Следующая теорема устанавливает корректность алгоритма пометки.

Теорема 3.3.1. Пусть ϕ' — state-подформула формулы ϕ. Приведенный выше алгоритм помечает вершину v из $\mathcal{M}(\mathcal{N}, \phi)$ формулой ϕ' тогда и только тогда, когда ϕ' выполняется на состоянии в $\mathcal{N}$, принадлежащем v.

Далее дана оценка сложности предложенного алгоритма:

Теорема 3.3.2. Существует алгоритм, проверяющий, что временная сеть $\mathcal{N}$ удовлетворяет state-формуле ϕ, который линеен по размеру ϕ и полиномиален по размеру $\mathcal{M}(\mathcal{N}, \phi)$, а, следовательно, экспоненциален по размеру $\mathcal{N}$.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ

В рамках диссертации были получены следующие результаты.

1. Разработан алгоритм верификации поведенческих свойств безопасных временных сетей на основе темпоральной логики реального времени TCTL, который позволяет проверять не только качественные, но и количественные свойства сети.
   - Построено конечное представление поведения сети в виде графа обобщенных состояний.
   - Предложен алгоритм пометки графа обобщенных состояний TCTL-формулами.

- Продемонстрирована возможность применения техники частичных порядков для повышения эффективности рассматриваемого алгоритма. Одна из отличительных черт предложенного метода состоит в возможности редукции графового представления поведения сети не только за счет ее параллельных переходов, но также и за счет сокращения числа состояний, полученных при истечении времени, не существенного для рассматриваемой TCTL-формулы.
- Введено понятие временной статтеринг-эквивалентности для обоснования корректности предложенной редукции.
- Получены экспериментальные результаты, обосновывающие целесообразность предложенной редукции.

2. Предложена новая модель систем реального времени — параметрические временные сети.
   - Введено понятие параметрической временной сети, обеспечивающее более гибкую спецификацию временных ограничений системы, чем существующие временные модели.
   - Понятие графа обобщенных состояний адаптировано к параметрической природе временных ограничений.
   - Предложен верификационный метод, позволяющий получить информацию для настройки временных ограничений системы на проверяемое свойство.
3. Разработан метод верификации поведенческих свойств временных сетей с использованием аппарата темпорального языка реального ветвящегося времени TCCTL, который позволяет количественные свойства, связанные с параллелизмом системы.
   - Введена и исследована новая темпоральная логика реального времени TCCTL, содержащая средства для описания “истинного параллелизма” в системах реального времени.
   - Предложено понятие поддеревьев на состояниях временной сети для характеристики параллельных выполнений системы.
   - Построено конечное представление поведения сети в виде структуры обобщенных состояний, позволяющее различать в выполнениях системы точки параллельного ветвления и точки недетерминированного выбора.
   - Предложен алгоритм анализа структуры обобщенных состояний средствами TCCTL.
4. Дана оценка сложности предложенных алгоритмов и доказана

их корректность.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Вирбицкайте И.Б., Покозий Е.А., Использование техники частичных порядков для верификации временных сетей Петри. *Программирование,* N 1, 1999, 28–41.
2. Вирбицкайте И.Б., Покозий Е.А., Метод параметрической верификации поведения временных сетей Петри. *Программирование,* N 4, 1999, 55–68.
3. Покозий Е.А., Поведенческий анализ параметрических временных сетей Петри. UkrProg'98 (1st International conference on practical and theoretical programming), сентябрь 1998, Киев, Украина, 111–119.
4. Покозий Е.А., Метод верификации свойств параллелизма временных сетей Петри. *Препринт* **61**, ИСИ, Новосибирск, 1999, 22 стр.
5. Pokozy, E.A., Towards behaviour analysis of parametric time Petri nets. Proc. *International Workshop on Discrete Event Systems (WODES'98)*, August 1998, Cagliari, Italy. The IEE Publisher, London, 1998, 517–518.
6. Pokozy, E.A., Behaviour analysis of parametric time Petri nets. *Joint Novosibirsk Computing Center and Institute of Informatics Systems Bulletin, Series Computer Science*, V. 9, Novosibirsk (1999), 73–89.
7. Virbitskaite, I.B., Pokozy, E.A., Model Checking of Time Petri Nets. *Joint Novosibirsk Computing Center and Institute of Informatics Systems Bulletin, Series Computer Science*, V. 7, Novosibirsk (1997), 85–95.
8. Virbitskaite, I.B., Pokozy, E.A., Towards Efficient Verification of Time Petri Nets. Logical Journal of IGPL **5(6)** Oxford University Press (1997) 921–924.
9. Virbitskaite, I.B., Pokozy, E.A., A partial order algorithm for verifying time Petri nets. Proc. *International Workshop on Discrete Event Systems (WODES'98)*, August 1998, Cagliari, Italy. The IEE Publisher, London, 1998, 514–516.

Подписано в печать 28.04.99 Объем 1 уч.-изд.л.
Формат бумаги 60×90 1/16 Тираж 100 экз.

Отпечатано на ризографе “AL-Group”.
630090, Новосибирск-90, пр. акад. Лаврентьева, 6.