

Минимизация вероятностных моделей программ

А. М. МИРОНОВ

*Институт проблем информатики
Российской академии наук
e-mail: amironov66@gmail.com*

С. Л. ФРЕНКЕЛЬ

*Институт проблем информатики
Российской академии наук
e-mail: fsergei@mail.ru*

УДК 681.3

Ключевые слова: верификация, вероятностные системы переходов, вероятностная темпоральная логика, редукция вероятностных моделей.

Аннотация

Рассматривается задача редукции вероятностных систем переходов с целью понижения сложности верификации таких систем. Верификация вероятностной системы переходов заключается в вычислении истинностных значений формул вероятностной темпоральной логики в начальных состояниях вероятностной системы переходов. Введено понятие эквивалентности состояний вероятностной системы переходов и указан алгоритм удаления эквивалентных состояний, в результате работы которого получается вероятностная система переходов, у которой все свойства, выражаемые формулами вероятностной темпоральной логики, совпадают со свойствами исходной вероятностной системы переходов.

Abstract

A. M. Mironov, S. L. Frenkel, Minimization of probabilistic models of programs, Fundamentalnaya i prikladnaya matematika, vol. 19 (2014), no. 1, pp. 121–163.

In this paper, we consider a problem of reduction of probabilistic transition systems (PTS) in order to reduce the complexity of model checking of such systems. The problem of model checking of a PTS is to calculate truth values of formulas of the probabilistic temporal logic PCTL in an initial state of the PTS. We introduce a concept of equivalence of states of a PTS, and represent an algorithm for removing equivalent states. A result of this algorithm is a PTS such that all its properties expressed by formulas of PCTL coincide with those of the original PTS.

1. Введение

1.1. Постановка задачи, мотивация и научная новизна

В настоящей работе рассматривается задача редукции *вероятностных систем переходов* (ВСП), целью которой является понижение сложности верификации свойств ВСП, выражаемых формулами вероятностной темпоральной логики PCTL.

Фундаментальная и прикладная математика, 2014, том 19, № 1, с. 121–163.
© 2014 Издательский дом «Открытые системы»

ВСП представляют собой один из наиболее широко используемых классов моделей дискретных динамических систем. Понятие ВСП является обобщением понятия цепи Маркова [2], имеющего широкие применения в естественных и гуманитарных науках. Понятие ВСП можно рассматривать также как частный случай понятия вероятностного автомата [1]. Главным отличием понятия ВСП от понятий цепи Маркова и вероятностного автомата является наличие выразительного логического формализма, позволяющего эффективно описывать различные свойства поведения ВСП. В качестве такого формализма выступает вероятностная темпоральная логика PCTL [13, 19], которая представляет собой вероятностный аналог темпоральной логики ветвящегося времени STL [3], использующейся для спецификации свойств параллельных и распределённых программ, и является эффективным инструментом для описания различных свойств дискретных вероятностных динамических систем.

Формулы логики PCTL могут отражать различные вероятностные аспекты поведения анализируемых систем, к числу которых относятся, например,

- частота выполнения тех или иных действий или переходов в анализируемых системах;
- вероятность отказа компонентов анализируемых систем;
- вероятностный характер взаимодействия анализируемой системы с её окружением: частота поступления входных запросов или сообщений, частота получения искажённых сообщений (для протоколов передачи сообщений в компьютерных сетях) и т. п.

В последнее время класс вероятностных моделей находит всё большее применение в различных задачах верификации программных систем. Одной из главных причин актуальности данного класса моделей в задачах верификации программных систем является существенно меньшая (по сравнению с детерминированными моделями) сложность вероятностных моделей анализируемых систем. Тем не менее, несмотря на то, что сложность этих вероятностных моделей может быть меньше сложности исходных детерминированных моделей, процедура их формального анализа может иметь высокую вычислительную трудоёмкость. Поэтому разумно рассматривать вопрос о редукции этих вероятностных моделей, т. е. преобразовании их в вероятностные модели, сохраняющие все свойства исходных моделей, но имеющие меньшую вычислительную трудоёмкость формального анализа по сравнению с формальным анализом исходных вероятностных моделей.

Результат верификации вероятностной модели анализируемой системы может отличаться от свойств исходной системы, и одной из актуальных научных задач является оценка степени расхождения свойств исходной системы и свойств её вероятностной модели. Однако эта задача не является предметом данного исследования. В настоящей работе мы рассматриваем следующую задачу. Мы предполагаем, что вероятностная модель анализируемой системы уже построена, и требуется преобразовать её в такую модель, чтобы задача анализа свойств исходной системы, выражаемых в виде формул вероятностной темпо-

ральной логики, допускала более простое решение для редуцированной модели, а результаты верификации исходной и редуцированной модели были одинаковы.

Некоторые подходы к редукции ВСП изучались в различных работах по вероятностной верификации, однако в этих исследованиях были рассмотрены лишь частные методы редукции ВСП, такие, как редукция частичных порядков [5, 7] и редукция, основанная на понятии симметрии множества состояний ВСП [11, 17]. Данные методы можно эффективно использовать лишь для ВСП достаточно специального вида, как правило, это вероятностные модели параллельных и распределённых программ.

В настоящей работе рассмотрен другой подход к редукции анализируемой вероятностной модели, который кратко может быть описан как удаление избыточных состояний. Данный метод является новым и представляет собой вероятностное обобщение метода минимизации конечных автоматов.

1.2. Исторический обзор и современное состояние дел в области верификации вероятностных систем переходов

Верификация вероятностных систем переходов в настоящее время является одним из наиболее широко используемых методов верификации вычислительных систем. Главным достоинством этого метода является возможность полностью автоматического анализа модели верифицируемой системы. К числу его существенных недостатков относится высокая вычислительная сложность процедуры верификации.

Первые алгоритмы вероятностной верификации были предложены в 1980-е годы в [10, 14, 22]. Данные алгоритмы были предназначены для верификации качественных вероятностных свойств, т. е. таких свойств, которые выполняются с вероятностью 1 или 0. Затем эти алгоритмы были обобщены на случай верификации количественных вероятностных свойств (в спецификации таких свойств могло присутствовать любое значение вероятности). Эти алгоритмы были изложены в [8, 9, 13]. Программные реализации этих алгоритмов были представлены в [6, 12].

Первые промышленные системы вероятностной верификации были разработаны в 2000-х годах [4, 15]. Эти системы вероятностной верификации успешно применяются во многих областях, в том числе в анализе распределённых алгоритмов, телекоммуникационных протоколах, компьютерной безопасности, криптографических протоколах, при моделировании биологических процессов. С использованием этих систем верификации были обнаружены уязвимости и аномальные поведения анализируемых систем (подробнее см. в [16, 20]). При помощи систем вероятностной верификации могут быть вычислены такие характеристики программных систем, как, например, вероятность вторжения злоумышленника в компьютерную сеть, математическое ожидание времени отклика веб-сервиса, а также другие количественные и качественные характеристики.

Наиболее популярной практической системой вероятностной верификации в настоящее время является система PRISM [18, 20], разработанная на факультете компьютерных наук Оксфордского университета (Великобритания) в группе «Количественный анализ и верификация» под руководством Марты Квятковской [21].

1.3. Структура статьи

В разделе 2 мы определяем основное понятие настоящей работы — вероятностную систему переходов (ВСП) — и приводим два простых примера ВСП. В разделе 3 мы вводим представление ВСП в терминах случайных функций и матриц. В разделе 4 мы описываем логику PCTL и определяем её семантику (т. е. правила вычисления значений формул логики PCTL в состояниях ВСП). Раздел 5 является центральным: здесь мы излагаем метод редукции ВСП, для чего вводим понятие эквивалентности состояний и описываем алгоритм вычисления классов эквивалентности на множестве состояний анализируемой ВСП. Также мы излагаем алгоритм преобразования ВСП, связанный с удалением избыточных состояний, и обосновываем его корректность. В разделах 6 и 7 мы рассматриваем практические иллюстрации изложенного метода редукции ВСП. В заключении мы формулируем актуальные проблемы для дальнейших исследований в области вероятностной верификации.

2. Вероятностные системы переходов

2.1. Понятие вероятностной системы переходов

Мы предполагаем, что задано конечное множество AP , элементы которого называются *атомарными утверждениями*. Ниже запись 2^{AP} обозначает множество всех подмножеств AP .

Вероятностная система переходов (ВСП) — это четвёрка D вида

$$D = (S, s^0, P, L), \quad (1)$$

компоненты которой имеют следующий смысл.

1. S — конечное множество, элементы которого называются *состояниями* ВСП D .
2. $s^0 \in S$ — выделенное состояние, называемое *начальным состоянием* ВСП D .
3. P — функция вида

$$P: S \times S \rightarrow [0, 1],$$

называемая *функцией перехода* ВСП D и удовлетворяющая условию

$$\sum_{s' \in S} P(s, s') = 1 \quad \text{для каждого } s \in S.$$

Для каждой пары $(s_1, s_2) \in S \times S$ число $P(s_1, s_2)$ понимается как вероятность того, что если в текущий момент времени D находится в состоянии s_1 , то через один такт времени D будет находиться в состоянии s_2 . Если $P(s_1, s_2) > 0$, то мы будем называть тройку $(s_1, s_2, P(s_1, s_2))$ *переходом* из s_1 в s_2 с вероятностью $P(s_1, s_2)$. Ниже запись $s_1 \xrightarrow{a} s_2$ является другим обозначением перехода (s_1, s_2, a) .

4. L — функция вида

$$L: S \rightarrow 2^{\text{AP}}, \quad (2)$$

называемая *оценкой*, которая имеет следующий смысл: для каждого состояния $s \in S$ и каждого атомарного утверждения $p \in \text{AP}$ утверждение p считается *истинным* в состоянии s , если $p \in L(s)$, и *ложным* в состоянии s , если $p \notin L(s)$.

ВСП удобно рассматривать как помеченный граф, вершинами которого являются состояния, помеченные элементами множества 2^{AP} : каждая вершина $s \in S$ имеет метку $L(s)$. Для каждой пары $(s_1, s_2) \in S \times S$, такой что $P(s_1, s_2) > 0$, граф содержит ребро из s_1 в s_2 с меткой $P(s_1, s_2)$.

2.2. Пути в вероятностных системах переходов

Путь в ВСП (1) — это конечная или бесконечная последовательность состояний

$$\pi = (s_0, s_1, \dots), \quad (3)$$

такая что для каждой пары (s_i, s_{i+1}) соседних состояний в этом пути верно неравенство $P(s_i, s_{i+1}) > 0$. Если последовательность (3) бесконечна, то путь π называется *бесконечным*, в противном случае он называется *конечным*.

При рассмотрении ВСП как графа каждый путь (3) в этой системе можно отождествлять с соответствующей последовательностью рёбер (из s_0 в s_1 , из s_1 в s_2 и т. д.).

Мы будем говорить, что путь π *выходит из состояния* s , если первым состоянием (т. е. состоянием с номером 0) этого пути является s .

Если π — конечный путь вида

$$\pi = (s_0, \dots, s_n), \quad (4)$$

то мы будем говорить, что π — *путь из* s_0 *в* s_n . Мы будем обозначать $s_0 \xrightarrow{*} s_n$ тот факт, что существует путь из s_0 в s_n .

Для каждого пути π вида (3) и каждого $s \in S$ запись $s \in \pi$ означает, что $s = s_i$ для некоторого $i \geq 0$.

Отрезком пути (3) называется произвольная подпоследовательность π' последовательности (3), т. е. произвольный путь вида

$$\pi' = (s_i, s_{i+1}, \dots, s_{i+k}), \quad (5)$$

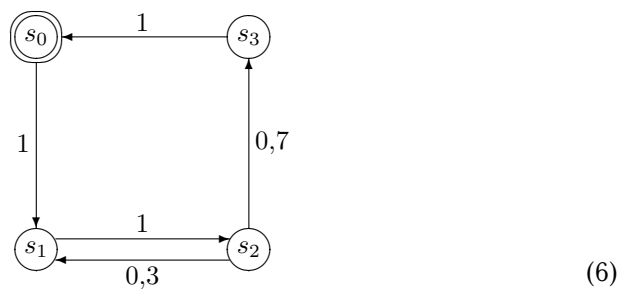
где $k \geq 0$. Число k называется *длиной* отрезка (5). Отрезок (5) обозначается $[s_i, s_{i+k}]$. Отрезок (5) называется *начальным* отрезком пути (3), если $i = 0$.

2.3. Примеры вероятностных систем переходов

Приведём два примера ВСП.

1. Упрощённая модель протокола передачи сообщений через ненадёжный канал (в котором сообщения могут пропадать). Протокол представляет собой систему, состоящую из двух агентов — отправителя и получателя, а также канала, в который помещаются сообщения, пересылаемые от одного агента другому.

Граф, представляющий эту ВСП, имеет следующий вид.

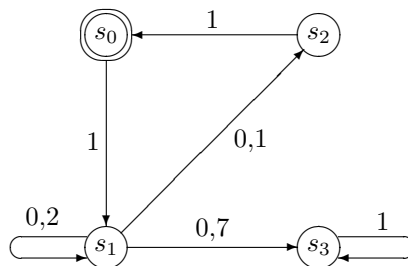


Переходы этой ВСП имеют следующий смысл.

- Переход $s_0 \xrightarrow{1} s_1$ заключается в получении отправителем от внешнего источника сообщения, которое должно быть передано через канал получателю.
- Переход $s_1 \xrightarrow{1} s_2$ заключается в помещении сообщения в канал отправителем.
- Переход $s_2 \xrightarrow{0,3} s_1$ заключается в потере сообщения в канале.
- Переход $s_2 \xrightarrow{0,7} s_3$ заключается в передаче сообщения из канала получателю.
- Переход $s_3 \xrightarrow{1} s_0$ заключается в получении сообщения получателем и посылка им подтверждения отправителю.

2. Упрощённая модель агента, работа которого представляет собой последовательность сеансов. В каждом из этих сеансов агент пытается выполнить некоторое действие. Если действие было выполнено, то он переходит к следующему сеансу, а если не было выполнено, то он завершает свою работу.

Граф, представляющий эту ВСП, имеет следующий вид.



Состояния этой ВСП имеют следующий смысл.

- В состоянии s_0 агент начинает очередной сеанс.
- В состоянии s_1 агент предпринимает попытку выполнения действия (переход $s_1 \xrightarrow{0,2} s_1$ означает, что попытка выполнения действия пока неосуществима).
- В состоянии s_2 агент находится тогда, когда действие было выполнено успешно.
- В состоянии s_3 агент оказывается тогда, когда попытка выполнения действия закончилась неудачей.

3. Матричное представление вероятностных систем переходов

3.1. Случайные функции

Пусть X и Y — два конечных множества.

Случайной функцией (СФ) из X в Y называется произвольная функция f вида

$$f: X \times Y \rightarrow [0, 1], \quad (7)$$

удовлетворяющая условию

$$\sum_{y \in Y} f(x, y) = 1 \quad \text{для каждого } x \in X.$$

Для любых $x \in X$ и $y \in Y$ значение $f(x, y)$ можно интерпретировать как вероятность того, что СФ f отображает x в y .

Случайная функция (7) называется *детерминированной*, если для каждого $x \in X$ существует единственный $y \in Y$, такой что $f(x, y) = 1$. Если f — детерминированная СФ вида (7) и x, y — такие элементы X и Y соответственно, что $f(x, y) = 1$, то мы будем говорить, что f *отображает x в y* .

Если f — СФ из X в Y , то мы будем обозначать этот факт

$$f: X \xrightarrow{\tau} Y.$$

Мы будем называть X *областью определения* СФ f , а Y — *областью значений* СФ f .

Для каждого конечного множества X запись id_X обозначает детерминированную СФ $X \rightarrow X$, которая отображает каждый $x \in X$ в x .

3.2. Матрицы, соответствующие случайным функциям

Если СФ f имеет вид

$$f: X \xrightarrow{\tau} Y$$

и на множествах X и Y заданы упорядочения их элементов, которые имеют вид $(x_1, \dots, x_m)$ и $(y_1, \dots, y_n)$ соответственно, то СФ f можно представить в виде матрицы (обозначаемой тем же символом f)

$$f = \begin{pmatrix} f(x_1, y_1) & \dots & f(x_1, y_n) \\ \dots & \dots & \dots \\ f(x_m, y_1) & \dots & f(x_m, y_n) \end{pmatrix}. \quad (8)$$

Ниже мы будем отождествлять каждую СФ f с соответствующей ей матрицей (8).

Мы будем предполагать, что для каждого конечного множества X , являющегося областью определения или областью значений какой-либо из рассматриваемых СФ, на X задано фиксированное упорядочение его элементов. Таким образом, для каждой рассматриваемой СФ соответствующая ей матрица определена однозначно.

Для каждой СФ

$$f: X \xrightarrow{r} Y$$

и произвольных $x \in X$, $y \in Y$ мы будем называть строку

$$(f(x, y_1), \dots, f(x, y_n))$$

матрицы f *строкой* x и столбец

$$\begin{pmatrix} f(x_1, y) \\ \dots \\ f(x_m, y) \end{pmatrix}$$

матрицы f *столбцом* y .

Если f и g — СФ вида

$$f: X \xrightarrow{r} Y, \quad g: Y \xrightarrow{r} Z,$$

то их *композицией* называется СФ

$$f \cdot g: X \xrightarrow{r} Z,$$

определяемая следующим образом:

$$(f \cdot g)(x) \stackrel{\text{def}}{=} \sum_{y \in Y} f(x, y) \cdot g(y, z) \quad \text{для каждого } x \in X. \quad (9)$$

Согласно определению произведения матриц из (9) следует, что матрица $f \cdot g$ является произведением матриц f и g .

3.3. Матрицы,

соответствующие вероятностным системам переходов

Пусть задана ВСП $D = (S, s^0, P, L)$, и список элементов множества S имеет вид $(s_1, \dots, s_n)$.

Мы будем использовать следующие обозначения.

Через $\mathbf{1}$ обозначается множество, состоящее из одного элемента, который мы будем обозначать e .

Для каждого состояния $s \in S$ запись I_s обозначает детерминированную СФ вида

$$I: \mathbf{1} \xrightarrow{r} S,$$

отображающую элемент $e \in \mathbf{1}$ в состояние s ВСП D .

Для каждого $n \geq 0$ обозначим через P^n СФ вида

$$P^n: S \xrightarrow{r} S,$$

определяемую индуктивно: $P^0 \stackrel{\text{def}}{=} \text{id}_S$, $P^{n+1} \stackrel{\text{def}}{=} P^n \cdot P$ для каждого $n \geq 0$. Нетрудно убедиться, что матрицы, соответствующие СФ P^i , имеют следующий вид: P^0 — единичная матрица и для каждого $n > 0$ матрица P^n является n -й степенью матрицы P .

Для любых $n \geq 0$, $s_1, s_2 \in S$ число $P^n(s_1, s_2)$ можно понимать как вероятность того, что если в текущий момент времени ВСП D находится в состоянии s_1 , то через n тактов времени D будет находиться в состоянии s_2 .

4. Логика PCTL

4.1. Свойства вероятностных систем переходов

Логика PCTL (её название является аббревиатурой англоязычного названия «Probabilistic Computation Tree Logic») — это темпоральная логика, предназначенная для формального описания свойств ВСП. Логика PCTL была введена в [13].

Приведём несколько примеров свойств ВСП, которые могут быть описаны в виде формул логики PCTL.

1. Вероятность доставки сообщения в заданном временном интервале $[t_1, t_2]$ не меньше 0,999.
2. В результате работы алгоритма избрания процесса-лидера избрание такого процесса завершится с вероятностью 1.
3. Вероятность успешной атаки на криптографический протокол не превышает 0,0001 %.

4.2. Формулы логики PCTL

В определении понятия формулы логики PCTL мы будем использовать множество AP атомарных утверждений, введённое в разделе 2.1.

Формулы логики PCTL делятся на два класса: StateFm — *формулы состояний*, PathFm — *формулы путей*. Формулы из классов StateFm и PathFm мы

будем обозначать через φ и α соответственно (возможно, с индексами), а формулу произвольного вида — через f (возможно, с индексом).

Классы StateFm и PathFm определяются следующим образом.
StateFm.

1. Каждое атомарное утверждение p из AP является формулой из StateFm.
2. Символы $\top$ и $\perp$ являются формулами из StateFm. Данные символы обозначают тождественно истинное и тождественно ложное утверждение соответственно.
3. Если φ_1 и φ_2 — формулы из StateFm, то следующие знакосочетания являются формулами из StateFm:

$$\neg\varphi_1, \quad \varphi_1 \wedge \varphi_2, \quad \varphi_1 \vee \varphi_2, \quad \varphi_1 \rightarrow \varphi_2, \quad \varphi_1 \leftrightarrow \varphi_2.$$

4. Если $\triangle$ — функциональный символ, которому соответствует функция (обозначаемая тем же символом) вида

$$\triangle: [0, 1] \times [0, 1] \rightarrow \{0, 1\},$$

a — число из $[0, 1]$ и α — формула из PathFm, то знакосочетание $P_{\triangle a}\alpha$ является формулой из StateFm.

PathFm.

1. Если f — формула логики PCTL, то знакосочетание $\mathbf{X}f$ является формулой из PathFm.
2. Если φ_1 и φ_2 — формулы из StateFm, то следующие знакосочетания являются формулами из PathFm: $\varphi_1 \mathbf{U}^{\leq n} \varphi_2$, где n — натуральное число, $\varphi_1 \mathbf{U} \varphi_2$.
3. Если α — формула из PathFm, то знакосочетание $\neg\alpha$ является формулой из PathFm.

В записи формул из PathFm могут использоваться символы $\mathbf{F}$ и $\mathbf{G}$, которые являются сокращением знакосочетаний $\top\mathbf{U}$ и $\neg\mathbf{F}\neg$ соответственно (т. е., например, знакосочетания $\mathbf{F}\alpha$ и $\mathbf{G}^{\leq n}\alpha$ обозначают формулы $\top\mathbf{U}\alpha$ и $\neg\mathbf{F}^{\leq n}\neg\alpha$ соответственно).

4.3. Значения формул логики PCTL в состояниях вероятностных систем переходов

Пусть $D = (S, s^0, P, L)$ — некоторая ВСП.

Для каждого состояния $s \in S$ и каждой формулы f логики PCTL определено значение формулы f в состоянии s , обозначаемое $s(f)$. Если $f \in \text{StateFm}$, то $s(f) \in \{0, 1\}$ и в случае $s(f) = 1$ формула f считается истинной в s , в случае $s(f) = 0$ формула f считается ложной в s . Если $f \in \text{PathFm}$, то значение $s(f)$ является числом из $[0, 1]$ и интерпретируется как вероятность того, что формула f истинна в состоянии s .

Для каждой формулы f логики PCTL мы будем обозначать через $S(f)$ вектор-столбец

$$\begin{pmatrix} s_1(f) \\ \dots \\ s_n(f) \end{pmatrix}.$$

Значения формул логики PCTL в состояниях ВСП определяются индукцией по структуре формул в соответствии с излагаемыми ниже правилами. В одних правилах мы определяем значение $s(f)$, в других — вектор-столбец $S(f)$ целиком. В этих определениях мы будем использовать следующие обозначения. Для любых векторов

$$U = \begin{pmatrix} u_1 \\ \dots \\ u_n \end{pmatrix}, \quad V = \begin{pmatrix} v_1 \\ \dots \\ v_n \end{pmatrix}$$

из $[0, 1]^n$ записи $\max(U, V)$ и $U \circ V$ обозначают векторы

$$\begin{pmatrix} \max(u_1, v_1) \\ \dots \\ \max(u_n, v_n) \end{pmatrix}$$

и

$$\begin{pmatrix} u_1 \cdot v_1 \\ \dots \\ u_n \cdot v_n \end{pmatrix}$$

соответственно.

Если A и B — матрицы порядков $n \times n$ и $n \times 1$ соответственно с компонентами из $[0, 1]$, то через $[A^* \cdot B]$ обозначается матрицу, получаемая заменой всех ненулевых компонент A и B на 1 и вычислением $\left(\sum_{i \geq 0} A^i\right) \cdot B$, где сложение понимается как дизъюнкция (т. е. сумма $\sum_{i \geq 0} A^i$ является конечной).

Правила определения значений формул логики PCTL в состояниях ВСП имеют следующий вид.

— Для каждого $p \in AP$

$$s(p) \stackrel{\text{def}}{=} \begin{cases} 1, & \text{если } p \in L(s), \\ 0 & \text{иначе.} \end{cases}$$

— $s(\top) \stackrel{\text{def}}{=} 1$, $s(\perp) \stackrel{\text{def}}{=} 0$.

— $s(\neg f) \stackrel{\text{def}}{=} 1 - s(f)$, $s(\varphi_1 \wedge \varphi_2) \stackrel{\text{def}}{=} s(\varphi_1) \cdot s(\varphi_2)$ и т. д. (т. е. значения формул коммутируют с булевыми операциями).

— $s(\mathcal{P}_{\Delta a} \alpha) \stackrel{\text{def}}{=} \Delta(s(\alpha), a)$.

— $S(\mathbf{X}f) \stackrel{\text{def}}{=} P \cdot S(f)$.

- Пусть $\alpha_n = \varphi_1 \mathbf{U}^{\leq n} \varphi_2$ (где $n \geq 0$). Тогда

$$S(\alpha_0) \stackrel{\text{def}}{=} S(\varphi_2),$$

$$S(\alpha_n) \stackrel{\text{def}}{=} \max(S(\varphi_2), S(\varphi_1) \circ S(\mathbf{X}\alpha_{n-1})) \quad \text{для каждого } n > 0.$$

- Пусть $\alpha = \varphi_1 \mathbf{U} \varphi_2$. Тогда $S(\alpha)$ определяется системой линейных уравнений

$$S(\alpha) = \max\left(S(\varphi_2), [P^* \cdot S(\varphi_2)] \circ S(\varphi_1) \circ (P \cdot S(\alpha))\right).$$

4.4. Смысл формул логики PCTL

Формулы логики PCTL представляют собой утверждения, выражающие различные свойства ВСП. Эти свойства могут выражать, например, динамические аспекты поведения ВСП, т. е. описывать зависимость истинности какого-либо утверждения в некотором состоянии s рассматриваемой ВСП от истинности другого утверждения в состояниях, достижимых из s .

Смысл формул состояний логики PCTL непосредственно усматривается из определения значений этих формул в состояниях.

Смысл формул путей логики PCTL можно описать следующим образом.

1. Формулу $\mathbf{X}\varphi$ можно интерпретировать как утверждение «в следующий момент времени будет верно φ », а значение формулы $\mathbf{X}\varphi$ в состоянии s — как вероятность того, что φ будет истинна в произвольном состоянии, в которое можно перейти из s за один такт времени.
2. Значение формулы $\varphi_1 \mathbf{U}^{\leq n} \varphi_2$ в состоянии s можно интерпретировать как вероятность того, что для произвольного пути π , выходящего из s , существует состояние $s' \in \pi$, такое что длина начального отрезка $[s, s']$ пути π не превосходит n и в каждом состоянии этого отрезка, кроме, может быть, s' , верна формула φ_1 , а в состоянии s' верна формула φ_2 .
3. Значение формулы $\varphi_1 \mathbf{U} \varphi_2$ в состоянии s можно интерпретировать так же, как значение предыдущей формулы, без упоминания того, что длина $[s, s']$ не превосходит n .

4.5. Пример формулы логики PCTL, выражающей свойство вероятностной системы переходов

В этом разделе мы приведём пример формулы логики PCTL, выражающей одно из свойств первого протокола из раздела 2.3 (представленного ВСП (6)). Данное свойство заключается в том, что каждое сообщение, полученное отправителем от внешнего источника, будет с вероятностью не меньше 0,9 доставлено получателю не более чем за пять шагов.

Для формального представления этого свойства мы будем предполагать, что среди атомарных утверждений имеются утверждения, комбинации значений которых соответствуют состояниям ВСП. Обозначим эти утверждения записями

p_1 и p_2 и будем считать, что значения p_1 и p_2 в состояниях ВСП (6) определяются следующим образом:

	p_1	p_2
s_0	0	0
s_1	0	1
s_2	1	0
s_3	1	1

В частности, состоянию s_0 соответствует формула $\neg p_1 \wedge \neg p_2$, а состоянию s_3 — формула $p_1 \wedge p_2$. Тогда формула логики PCTL, соответствующая указанному выше свойству, имеет следующий вид:

$$\mathbf{G}\left((\neg p_1 \wedge \neg p_2) \rightarrow \mathcal{P}_{\geq 0,9}(\mathbf{F}^{\leq 5}(p_1 \wedge p_2))\right),$$

где символ $\geq$ обозначает функцию вида

$$\geq: [0, 1] \times [0, 1] \rightarrow \{0, 1\},$$

которая ставит в соответствие паре $(a, b) \in [0, 1] \times [0, 1]$ элемент 1, если $a \geq b$, и 0 иначе.

5. Метод редукции вероятностных систем переходов

5.1. Задача редукции вероятностных систем переходов

Если анализируемая ВСП имеет большой размер, то анализ её свойств, выражаемых формулами логики PCTL (т. е. вычисление значений формул логики PCTL в состояниях этой ВСП), может быть связан с трудновыполнимыми требованиями к вычислительным ресурсам, с использованием которых производится этот анализ. В связи с этим представляет большую актуальность проблема редукции ВСП, т. е. удаления части состояний и переходов анализируемой ВСП с таким расчётом, чтобы получившаяся ВСП была эквивалентна исходной в следующем смысле: для каждой формулы состояний f логики PCTL формула f истинна в начальном состоянии исходной ВСП тогда и только тогда, когда она истинна в начальном состоянии редуцированной ВСП.

Основная идея предлагаемого в настоящей работе метода редукции ВСП основана на понятии эквивалентности состояний ВСП. Мы называем состояния эквивалентными, если значения всех формул логики PCTL в этих состояниях совпадают. Алгоритм редукции ВСП представляет собой вычисление классов эквивалентности состояний анализируемой ВСП и удалении эквивалентных состояний.

5.2. Эквивалентность вероятностных систем переходов

Пусть заданы две ВСП:

$$D_i = (S_i, s_i^0, P_i, L_i) \quad (i = 1, 2). \quad (10)$$

Мы будем называть состояния $s_1 \in S_1$ и $s_2 \in S_2$ *эквивалентными*, если для каждой формулы f логики PCTL верно равенство

$$s_1(f) = s_2(f).$$

Если состояния s_1 и s_2 эквивалентны, то мы будем обозначать этот факт записью $s_1 \sim s_2$.

Мы будем называть ВСП D_1 и D_2 вида (10) *эквивалентными*, если $s_1^0 \sim s_2^0$. Если ВСП D_1 и D_2 эквивалентны, то мы будем обозначать этот факт $D_1 \sim D_2$.

Если ВСП D_1 и D_2 совпадают и S — множество их состояний, то бинарное отношение на S , состоящее из всех пар (s_1, s_2) , таких что $s_1 \sim s_2$, является отношением эквивалентности. Мы будем обозначать это отношение через $\sim$.

Отношение $\sim$ может быть найдено при помощи алгоритма, излагаемого в разделе (5.4). Для обоснования этого алгоритма мы введём необходимые понятия и докажем несколько вспомогательных утверждений.

5.3. Вспомогательные понятия и утверждения

5.3.1. Эквивалентности

и связанные с ними разбиения множества состояний

Пусть заданы ВСП $D = (S, s^0, P, L)$ и некоторое множество Fm формул логики PCTL. Мы будем обозначать $\rho(\text{Fm})$ бинарное отношение на S , определяемое следующим образом:

$$\rho(\text{Fm}) \stackrel{\text{def}}{=} \{(s_1, s_2) \in S^2 \mid s_1(f) = s_2(f) \text{ для каждого } f \in \text{Fm}\}.$$

Нетрудно убедиться, что $\rho(\text{Fm})$ — отношение эквивалентности и

$$\rho(\text{Fm}) = \bigcap_{f \in \text{Fm}} \rho(\{f\}). \quad (11)$$

Если множество Fm конечно и имеет вид $\{f_1, \dots, f_n\}$, то отношение $\rho(\text{Fm})$ мы будем обозначать также $\rho(f_1, \dots, f_n)$.

Лемма 1. Для каждого множества Fm формул логики PCTL существует конечное множество Fm' формул логики PCTL, такое что

$$\rho(\text{Fm}) = \rho(\text{Fm}').$$

Доказательство. Будем строить искомое множество Fm' следующим итеративным алгоритмом.

1. Сначала полагаем $\text{Fm}' \stackrel{\text{def}}{=} \{f\}$, где f — произвольная формула из Fm .

2. Если $\rho(\text{Fm}') = \rho(\text{Fm})$, то алгоритм заканчивает свою работу, иначе найдётся формула $f' \in \text{Fm}$, такая что

$$\rho(\text{Fm}') \neq \rho(\text{Fm}' \cup \{f'\}).$$

Добавляем формулу f' к множеству Fm' и выполняем данный шаг ещё раз.

Отметим, что шаг 2 не может выполняться бесконечно, потому что разбиение, соответствующее отношению эквивалентности $\rho(\text{Fm}' \cup \{f'\})$, является измельчением разбиения, соответствующего отношению эквивалентности $\rho(\text{Fm}')$, и поскольку множество S , на котором заданы эти отношения эквивалентности, является конечным, то таких измельчений не может быть больше, чем $|S|$. $\square$

Лемма 2. Для каждой формулы путей α существует конечное множество Fm формул состояний, такое что $\rho(\alpha) = \rho(\text{Fm})$.

Доказательство. Обозначим через $(a_1, \dots, a_k)$ совокупность всех чисел вида $s(\alpha)$, где $s \in S$. Нетрудно убедиться, что в качестве Fm можно взять множество формул вида

$$\varphi_i \stackrel{\text{def}}{=} \mathcal{P}_{\leq a_i} \alpha \quad (i = 1, \dots, k-1). \quad \square$$

Лемма 3. Пусть задано множество Fm формул логики $PCTL$ и разбиение Σ множества S , соответствующее отношению эквивалентности $\rho(\text{Fm})$, состоит из классов $S_1, \dots, S_k$. Тогда для каждого $j \in \{1, \dots, k\}$ существует формула φ_j^Σ логики $PCTL$, такая что

$$\begin{aligned} s(\varphi_j^\Sigma) &= 1 \quad \text{для каждого } s \in S_j, \\ s(\varphi_j^\Sigma) &= 0 \quad \text{для каждого } s \in S \setminus S_j. \end{aligned} \quad (12)$$

Доказательство. Из лемм 1 и 2 следует, что существует конечное множество $\varphi_1, \dots, \varphi_n$ формул состояний, такое что

$$\rho(\text{Fm}) = \rho(\varphi_1, \dots, \varphi_n). \quad (13)$$

Обозначим φ_{ij} (где $i \in \{1, \dots, n\}$) формулу, определяемую следующим образом:

$$\varphi_{ij} \stackrel{\text{def}}{=} \begin{cases} \varphi_i, & \text{если } s(\varphi_i) = 1 \text{ для каждого } s \in S_j, \\ \neg \varphi_i & \text{иначе.} \end{cases} \quad (14)$$

Искомая формула φ_j^Σ определяется следующим образом:

$$\varphi_j^\Sigma \stackrel{\text{def}}{=} \varphi_{1j} \wedge \dots \wedge \varphi_{nj}. \quad (15)$$

Первое соотношение в (12) следует из того, что, согласно определению (14),

$$s(\varphi_{ij}) = 1 \quad \text{для любых } i = 1, \dots, n, \quad s \in S_j,$$

следовательно,

$$s(\varphi_j^\Sigma) = s(\varphi_{1j} \wedge \dots \wedge \varphi_{nj}) = 1 \quad \text{для каждого } s \in S_j.$$

Второе соотношение в (12) доказывается от противного. Пусть для некоторого $s' \in S \setminus S_j$ верно равенство $s'(\varphi_j^\Sigma) = 1$. Тогда из определения (15) следует, что

$$s'(\varphi_{ij}) = 1 \text{ для каждого } i = 1, \dots, n. \quad (16)$$

Из (16) и (14) следует, что

$$s'(\varphi_i) = s(\varphi_i) \text{ для любых } i = 1, \dots, n, \quad s \in S_j. \quad (17)$$

Из (17) следует, что состояние s' эквивалентно состояниям из класса S_j относительно эквивалентности $\rho(\varphi_1, \dots, \varphi_n)$. Отсюда согласно (13) и определению классов $S_1, \dots, S_k$ следует, что $s' \in S_j$, что противоречит предположению $s' \in S \setminus S_j$. $\square$

Ниже мы будем использовать следующие обозначения. Пусть задано разбиение Σ множества S , которое имеет вид $\{S_1, \dots, S_k\}$.

Мы будем обозначать через π детерминированную СФ

$$\pi: S \xrightarrow[r]{} \Sigma \quad (18)$$

(а также соответствующую матрицу), отображающую каждое состояние $s \in S$ в тот класс разбиения Σ , которому принадлежит s . Для каждого $j = 1, \dots, k$ мы будем обозначать через Σ_j столбец S_j матрицы π .

Нетрудно убедиться, что в этих обозначениях соотношение (12) может быть записано более компактно в виде равенства

$$S(\varphi_j^\Sigma) = \Sigma_j.$$

5.3.2. Разбиения множества состояний, совместимые с функцией перехода

Пусть заданы ВСП $D = (S, s^0, P, L)$ и разбиение Σ множества S .

Мы будем говорить, что разбиение Σ *совместимо* с функцией перехода P , если существует СФ σ , делающая коммутативной диаграмму

$$\begin{array}{ccc} S & \xrightarrow{P} & S \\ \pi \downarrow & & \downarrow \pi \\ \Sigma & \xrightarrow{\sigma} & \Sigma \end{array} \quad (19)$$

Лемма 4. Пусть заданы ВСП $D = (S, s^0, P, L)$ и разбиение $\Sigma = \{S_1, \dots, S_k\}$ множества S . Разбиение Σ совместимо с функцией перехода P тогда и только тогда, когда для каждого $j = 1, \dots, k$ вектор $P \cdot \Sigma_j$ является линейной комбинацией векторов $\Sigma_1, \dots, \Sigma_k$.

Доказательство. Если Σ совместимо с P , то согласно (19) существует матрица σ , обладающая свойством

$$P \cdot \pi = \pi \cdot \sigma. \quad (20)$$

Пусть σ имеет вид

$$\begin{pmatrix} a_{11} & \dots & a_{1k} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kk} \end{pmatrix}.$$

Нетрудно убедиться, что для каждого $j = 1, \dots, k$ столбец S_j левой части (20) равен $P \cdot \Sigma_j$ и столбец S_j правой части (20) равен линейной комбинации

$$\Sigma_1 \cdot a_{1j} + \dots + \Sigma_k \cdot a_{kj}. \quad (21)$$

Обратно, пусть для каждого $j = 1, \dots, k$ вектор $P \cdot \Sigma_j$ представляется в виде линейной комбинации (21). Определим σ как матрицу коэффициентов этих линейных комбинаций. Нетрудно убедиться, что σ удовлетворяет равенству (20).

Докажем, что σ соответствует СФ вида $\Sigma \xrightarrow{r} \Sigma$, т. е. верны утверждения

$$a_{ij} \geq 0 \text{ для любых } i, j = 1, \dots, k, \quad (22)$$

$$\sum_{j=1}^k a_{ij} = 1 \text{ для каждого } i = 1, \dots, k. \quad (23)$$

Докажем (22). Поскольку все компоненты матрицы P и вектора Σ_j неотрицательны, то все компоненты вектора $P \cdot \Sigma_j$ (который совпадает с (21)) тоже неотрицательны. Однако совокупность компонентов вектора (21) совпадает с множеством $\{a_{1j}, \dots, a_{kj}\}$, так как в каждой строке матрицы π один элемент равен 1, а все остальные элементы равны 0 и для каждого $j \in \{1, \dots, k\}$ найдётся $s \in S$, такой что элемент в строке s и столбце S_j матрицы π равен 1.

Утверждение (23) можно переформулировать в виде равенства $\sigma \cdot 1^\downarrow = 1^\downarrow$, где $1^\downarrow$ — вектор-столбец, все компоненты которого равны 1. Данное равенство следует из цепочки равенств

$$\pi \cdot (\sigma \cdot 1^\downarrow) = (\pi \cdot \sigma) \cdot 1^\downarrow = (P \cdot \pi) \cdot 1^\downarrow = P \cdot (\pi \cdot 1^\downarrow) = P \cdot 1^\downarrow = 1^\downarrow$$

и описанного в предыдущем пункте свойства матрицы π . $\square$

Ниже мы будем обозначать через РСТЛ совокупность всех формул логики РСТЛ.

Лемма 5. Для любой ВСП $D = (S, s^0, P, L)$ разбиение Σ множества S , соответствующее эквивалентности $\rho(\text{РСТЛ})$, совместимо с функцией перехода P .

Доказательство. Пусть Σ имеет вид $\{S_1, \dots, S_k\}$ и $\Sigma_1, \dots, \Sigma_k$ — столбцы матрицы π , которая соответствует детерминированной СФ

$$\pi: S \xrightarrow{r} \Sigma.$$

Согласно лемме 3 для каждого $j \in \{1, \dots, k\}$ существует формула φ_j^Σ логики РСТЛ, обладающая свойством (12), т. е. такая, что

$$S(\varphi_j^\Sigma) = \Sigma_j \text{ для каждого } j = 1, \dots, k.$$

Поскольку $\rho(\text{PCTL}) \subseteq \rho(\mathbf{X}\varphi_j^\Sigma)$, то для каждого $j = 1, \dots, k$ вектор

$$S(\mathbf{X}\varphi_j^\Sigma) = P \cdot S(\varphi_j^\Sigma) = P \cdot \Sigma_j \quad (24)$$

имеет одинаковые компоненты, соответствующие состояниям из одного из того же класса разбиения Σ , т. е. вектор $P \cdot \Sigma_j$ является линейной комбинацией векторов $\Sigma_1, \dots, \Sigma_k$. Согласно лемме 4 отсюда следует, что Σ совместимо с функцией перехода P . $\square$

Теорема 1. Пусть заданы ВСП $D = (S, s^0, P, L)$ и множество Fm формул логики PCTL , содержащее все атомарные утверждения из AP . Тогда следующие утверждения эквивалентны:

- 1) разбиение, соответствующее $\rho(\text{Fm})$, совместимо с P ;
- 2) $\rho(\text{Fm}) = \rho(\text{PCTL})$.

Доказательство. Импликация $2) \implies 1)$ следует из леммы 5.

Докажем импликацию $1) \implies 2)$. Поскольку $\text{Fm} \subseteq \text{PCTL}$, то $\rho(\text{PCTL}) \subseteq \rho(\text{Fm})$.

Согласно (11) для доказательства обратного включения достаточно доказать, что для каждой формулы f логики PCTL верно включение

$$\rho(\text{Fm}) \subseteq \rho(f). \quad (25)$$

Докажем это включение индукцией по структуре формулы f .

Если $f \in \text{AP}$, то (25) следует из предположения $\text{AP} \subseteq \text{Fm}$.

Предположим, что для каждой подформулы f' формулы f верно включение (25), в котором f заменено на f' . Докажем, что в этом случае будет верно включение (25).

Пусть f является булевой комбинацией. Рассмотрим, например, случай $f = \neg f'$. Если $(s_1, s_2) \in \rho(\text{Fm})$, то

$$s_1(f) = s_1(\neg f') = 1 - s_1(f') = 1 - s_2(f') = s_2(\neg f') = s_2(f).$$

Другие случаи возможного вида f , когда f является булевой комбинацией, рассматриваются аналогично.

Пусть $f = \mathcal{P}_{\Delta a} \alpha$. Если $(s_1, s_2) \in \rho(\text{Fm})$, то

$$s_1(f) = \Delta(s_1(\alpha), a) = \Delta(s_2(\alpha), a) = s_2(f).$$

Для рассмотрения остальных возможных вариантов вида f мы введём дополнительные обозначения. Обозначим через Σ разбиение, соответствующее отношению эквивалентности $\rho(\text{Fm})$. Пусть Σ состоит из классов $S_1, \dots, S_k$. Заметим, что включение (25) равносильно утверждению

$$s_1(f) = s_2(f) \text{ для любых } j = 1, \dots, k, \quad s_1, s_2 \in S_j. \quad (26)$$

Нетрудно убедиться, что (26) можно переформулировать следующим образом:

$$\text{найдётся } \tilde{S}(f), \text{ такой что } S(f) = \pi \cdot \tilde{S}(f), \quad (27)$$

где π — матрица, соответствующая СФ (18).

Докажем (27) для случая, когда f имеет вид $\mathbf{X}f'$, $\varphi_1 \mathbf{U}^{\leq n} \varphi_2$ и $\varphi_1 \mathbf{U} \varphi_2$.

Пусть $f = \mathbf{X}f'$. По индуктивному предположению

найдётся $\tilde{S}(f')$, такой что $S(f') = \pi \cdot \tilde{S}(f')$.

Следовательно,

$$S(\mathbf{X}f') = P \cdot S(f') = P \cdot \pi \cdot \tilde{S}(f'). \quad (28)$$

По предположению Σ совместимо с P , поэтому существует матрица σ , удовлетворяющая равенству (20). Поэтому цепочку равенств (28) можно продолжить следующим образом:

$$P \cdot \pi \cdot \tilde{S}(f') = \pi \cdot \sigma \cdot \tilde{S}(f'). \quad (29)$$

Из (28) и (29) следует, что в качестве искомого вектор-столбца $\tilde{S}(f)$ в (27) можно взять вектор $\sigma \cdot \tilde{S}(f')$.

Пусть $f = \varphi_1 \mathbf{U}^{\leq n} \varphi_2$. Обозначим эту формулу через α_n .

Докажем индукцией по n , что будет верно утверждение (26), в котором f заменено на α_n .

Если $n = 0$, то по определению

$$S(\alpha_n) = S(\varphi_2)$$

и доказываемое утверждение верно потому, что φ_2 — подформула формулы f .

Если $n > 0$, то по определению

$$S(\alpha_n) = \max(S(\varphi_2), S(\varphi_1) \circ S(\mathbf{X}\alpha_{n-1}))$$

и истинность доказываемого утверждения следует из его истинности для φ_1 , φ_2 , α_{n-1} и $\mathbf{X}\alpha_{n-1}$, а также из определения операций $\max$ и $\circ$ на вектор-столбцах.

Пусть $f = \varphi_1 \mathbf{U} \varphi_2$. Согласно определению вектор-столбец $S(f)$ удовлетворяет соотношению

$$S(f) = \max\left(S(\varphi_2), [P^* \cdot S(\varphi_2)] \circ S(\varphi_1) \circ (P \cdot S(f))\right). \quad (30)$$

Докажем утверждение (27) для данного случая.

По индуктивному предположению будет верно утверждение (27), в котором f заменено на φ_1 или на φ_2 , т. е.

найдётся $\tilde{S}(\varphi_i)$, такой что $S(\varphi_i) = \pi \cdot \tilde{S}(\varphi_i)$ ($i = 1, 2$).

Определим вектор-столбец $\tilde{S}(\varphi)$ как решение системы линейных уравнений

$$\tilde{S}(f) = \max\left(\tilde{S}(\varphi_2), [\sigma^* \cdot \tilde{S}(\varphi_2)] \circ \tilde{S}(\varphi_1) \circ (\sigma \cdot \tilde{S}(f))\right), \quad (31)$$

где σ — матрица, соответствующая той СФ $\sigma: \Sigma \rightarrow \Sigma$, которая делает диаграмму (19) коммутативной.

Утверждение (27) следует из равенств (31) и (20), и из следующих утверждений.

1. Для любых вектор-столбцов V_1 , V_2 длины k верны равенства

$$\pi \cdot \max(V_1, V_2) = \max(\pi \cdot V_1, \pi \cdot V_2), \quad \pi \cdot (V_1 \circ V_2) = (\pi \cdot V_1) \circ (\pi \cdot V_2).$$

Данные равенства непосредственно следуют из определения операций $\max$ и $\circ$ на вектор-столбцах.

2. Для любого вектор-столбца V длины k с неотрицательными компонентами верно равенство

$$\pi \cdot [\sigma^* \cdot V] = [P^* \cdot \pi \cdot V]. \quad (32)$$

Данное равенство обосновывается следующим образом. Из определения матрицы вида $[A^* \cdot B]$ в пункте 4.3 следует, что для каждого $s \in S$ следующие утверждения равносильны:

- 1) элемент s столбца $[P^* \cdot \pi \cdot V]$ (являющегося правой частью равенства (32)) равен 1;
- 2) найдётся $n \geq 0$, такое что элемент s столбца $P^n \cdot \pi \cdot V$ больше 0.

Второе из этих утверждений равносильно следующему:

$$\text{найдётся } n \geq 0, \text{ такое что } I_s \cdot P^n \cdot \pi \cdot V > 0, \quad (33)$$

где I_s — матрица, определённая в пункте 3.3.

Из (20) следует, что (33) можно переписать следующим образом:

$$\text{найдётся } n \geq 0, \text{ такое что } I_s \cdot \pi \cdot \sigma^n \cdot V > 0. \quad (34)$$

С другой стороны, элемент s вектор-столбца $\pi \cdot [\sigma^* \cdot V]$ (являющегося левой частью равенства (32)) равен 1 тогда и только тогда, когда

$$I_s \cdot \pi \cdot [\sigma^* \cdot V] = 1. \quad (35)$$

Равенство (35) эквивалентно следующему утверждению: элемент S_j вектор-столбца $[\sigma^* \cdot V]$, где S_j — тот класс разбиения Σ , которому принадлежит s , равен 1.

Утверждение в предыдущем абзаце равносильно следующему: найдётся $n \geq 0$, такое что элемент S_j столбца $\sigma^n \cdot V$ больше 0, или

$$\text{найдётся } n \geq 0, \text{ такое что } I_{S_j} \cdot \sigma^n \cdot V > 0. \quad (36)$$

Поскольку $I_{S_j} = I_s \cdot \pi$, то (36) равносильно (34), что и требовалось доказать. Таким образом, теорема 1 полностью доказана. $\square$

5.4. Редукция вероятностных систем переходов

5.4.1. Задача редукции ВСП

Пусть задана ВСП $D = (S, s^0, P, L)$. Задача редукции ВСП D заключается в построении ВСП D' , которая эквивалентна D и число состояний которой меньше, чем число состояний ВСП D .

Излагаемый в настоящем разделе алгоритм редукции ВСП является вероятностным обобщением алгоритма редукции детерминированных автоматов. Идея данного алгоритма основана на отождествлении неразличимых состояний ВСП:

- алгоритм вычисляет классы эквивалентности $S_1, \dots, S_k$ множества S , соответствующие разбиению $\rho(PCTL)$,
- ВСП D преобразуется путём удаления состояний в классах эквивалентности $S_1, \dots, S_k$ (и соответствующего переопределения функции перехода) до тех пор, пока не останется по одному состоянию в каждом из этих классов.

В результате этих удалений получается искомая ВСП D' .

5.4.2. Построение разбиения множества состояний редуцируемой ВСП

Разбиение множества S состояний ВСП $D = (S, s^0, P, L)$, соответствующее отношению эквивалентности $\rho(PCTL)$, вычисляется следующим образом.

1. Находится разбиение Σ^0 , соответствующее отношению эквивалентности $\rho(AP)$. Нетрудно убедиться, что

$$\rho(AP) = \{(s_1, s_2) \in S \times S \mid L(s_1) = L(s_2)\}.$$

2. Затем работает цикл, состоящий из следующих шагов.

Пусть для некоторого $i \geq 0$ определены отношение эквивалентности ρ^i , которое имеет вид $\rho(Fm)$ для некоторого множества Fm формул логики PCTL, причём $AP \subseteq Fm$, и соответствующее ему разбиение Σ^i , которое состоит из классов $S_1^i, \dots, S_k^i$. Обозначим через $\Sigma_1^i, \dots, \Sigma_k^i$ строки матрицы π^i , соответствующей детерминированной СФ $\pi^i: S \rightarrow \Sigma^i$, и через $\varphi_1^{\Sigma^i}, \dots, \varphi_k^{\Sigma^i}$ список формул, таких что

$$S(\varphi_j^{\Sigma^i}) = \Sigma_j^i \text{ для каждого } j = 1, \dots, k$$

(существование таких формул следует из леммы 3).

Определим отношение эквивалентности ρ^{i+1} на S :

$$\rho^{i+1} \stackrel{\text{def}}{=} \rho^i \cap \rho(\mathbf{X}\varphi_1^{\Sigma^i}, \dots, \mathbf{X}\varphi_k^{\Sigma^i}). \quad (37)$$

Нетрудно убедиться, что если $\rho^i = \rho(Fm)$ для некоторого множества Fm формул логики PCTL, то

$$\rho^{i+1} = \rho(Fm \cup \{\mathbf{X}\varphi_1^{\Sigma^i}, \dots, \mathbf{X}\varphi_k^{\Sigma^i}\}).$$

Разбиение Σ^{i+1} , соответствующее отношению ρ^{i+1} , можно построить следующим образом:

- вычисляются вектор-столбцы

$$S(\mathbf{X}\varphi_j^{\Sigma^i}) = P \cdot \Sigma_j^i \quad (38)$$

(каждый из которых, как легко заметить, является суммой некоторых столбцов матрицы P : для каждого $j = 1, \dots, k$ вектор-столбец (38) является суммой таких столбцов s матрицы P , для которых $s \in S_j$)

- классы разбиения Σ^{i+1} получаются путём измельчения классов разбиения Σ^i : в один и тот же класс разбиения Σ^{i+1} попадают такие состояния, для которых соответствующие им компоненты векторов (38) совпадают для каждого $j = 1, \dots, k$.

Возможны два случая.

1. $\Sigma^{i+1} = \Sigma^i$. В этом случае искомое разбиение $\rho(\text{PCTL})$ найдено: оно совпадает с Σ^i . Действительно, из равенства $\rho^{i+1} = \rho^i$ и из определения (37) следует включение

$$\rho^i \subseteq \rho(\mathbf{X}\varphi_1^{\Sigma^i}, \dots, \mathbf{X}\varphi_k^{\Sigma^i}). \quad (39)$$

Лемма 6. *Определённое выше разбиение Σ^i совместимо с функцией перехода P .*

Доказательство. Согласно лемме 4 для доказательства леммы достаточно доказать, что для каждого $j = 1, \dots, k$ вектор $P \cdot \Sigma_j^i$ является линейной комбинацией векторов $\Sigma_1^i, \dots, \Sigma_k^i$.

Из (39) следует, что для каждого $j = 1, \dots, k$ верно включение

$$\rho^i \subseteq \rho(\mathbf{X}\varphi_j^{\Sigma^i}),$$

которое можно интерпретировать следующим образом: классы $S_1^i, \dots, S_k^i$ разбиения Σ^i содержатся в классах разбиения, соответствующего вектору

$$S(\mathbf{X}\varphi_j^{\Sigma^i}) = P \cdot S(\varphi_j^{\Sigma^i}) = P \cdot \Sigma_j^i,$$

т. е. компоненты вектора $P \cdot \Sigma_j^i$, соответствующие элементам из одного и того же класса разбиения Σ^i , одинаковы. Это равносильно тому, что вектор $P \cdot \Sigma_j^i$ является линейной комбинацией векторов $\Sigma_1^i, \dots, \Sigma_k^i$. $\square$

Поскольку $\rho^i = \rho(\text{Fm})$ для некоторого множества Fm формул логики PCTL, причём $\text{AP} \subseteq \text{Fm}$, то на основании леммы 6 и теоремы 1 отсюда следует желаемое равенство

$$\rho^i = \rho(\text{PCTL}).$$

2. $\Sigma^i \neq \Sigma^{i+1}$. В этом случае мы увеличиваем i на 1 и возвращаемся в начало цикла (т. е. выполняем шаг 2 с увеличенным значением i).

Нетрудно убедиться, что таких возвращений может быть не больше количества элементов множества S (так как разбиение Σ^{i+1} является измельчением разбиения Σ^i).

5.4.3. Удаление эквивалентных состояний из вероятностных систем переходов

Пусть ВСП $D = (S, s^0, P, L)$ содержит пару эквивалентных состояний s_1, s_2 , где $s_1 \neq s^0$. Определим ВСП

$$D_1 \stackrel{\text{def}}{=} (S_1, s^0, P_1, L_1), \quad (40)$$

где

$$\begin{aligned} S_1 &\stackrel{\text{def}}{=} S \setminus \{s_1\}, \\ P_1(s, s') &\stackrel{\text{def}}{=} \begin{cases} P(s, s') + P(s, s_1), & \text{если } s' = s_2, \\ P(s, s'), & \text{если } s' \neq s_2 \end{cases} \quad \text{для любых } s, s' \in S_1, \\ L_1(s) &\stackrel{\text{def}}{=} L(s) \quad \text{для каждого } s \in S_1. \end{aligned}$$

Таким образом, матрица P_1 получается из матрицы P прибавлением к столбцу s_2 столбца s_1 и удалением строки s_1 и столбца s_1 , а матрица L_1 получается из матрицы L удалением строки s_1 .

Ниже мы будем использовать следующие обозначения. Пусть A — матрица, соответствующая СФ вида $S \xrightarrow{r} S$. Для каждого $s \in S$ мы будем обозначать через $A \setminus \vec{s}$ матрицу, получаемую из A удалением строки s , и через $A \setminus s^\downarrow$ матрицу, получаемую из A удалением столбца s .

Нетрудно убедиться, что матрицы P_1 и L_1 связаны с матрицами P и L следующим образом:

$$\begin{aligned} P_1 &= (\text{id}_S \setminus \vec{s}_1) \cdot P \cdot \text{id}_S(s_1, s_2, 1) \cdot (\text{id}_S \setminus s_1^\downarrow), \\ L_1 &= (\text{id}_S \setminus \vec{s}_1) \cdot L, \end{aligned} \tag{41}$$

где $\text{id}_S(s_1, s_2, 1)$ — матрица, получаемая из матрицы id_S заменой в ней элемента в строке s_1 и столбце s_2 на 1.

Мы будем говорить что ВСП (40) получается из ВСП D путём *удаления состояния s_1 , эквивалентного состоянию s_2* . Согласно определению ВСП (40) каждое её состояние является также и состоянием ВСП D .

Для каждого $s \in S_1$ и каждой формулы f логики PCTL мы будем обозначать через $s_D(f)$ и $s_{D_1}(f)$ значения формулы f в состоянии s в ВСП D и D_1 соответственно и через $S_D(f)$ и $S_{D_1}(f)$ — вектор-столбцы значений формулы f в состояниях ВСП D и D_1 соответственно.

Теорема 2. Пусть ВСП (40) получается из ВСП D путём удаления состояния s_1 , эквивалентного состоянию s_2 . Тогда

$$s_{D_1}(f) = s_D(f) \quad \text{для каждого } s \in S_1. \tag{42}$$

Доказательство. Отметим, что утверждение (42) эквивалентно равенству

$$S_{D_1}(f) = S_D(f) \setminus \vec{s}_1. \tag{43}$$

Доказательство того, что для произвольной формулы f логики PCTL верно (42) или (43), мы будем вести индукцией по структуре формулы f .

Пусть $f = p \in \text{AP}$. Поскольку $L_1(s) = L(s)$ для каждого $s \in S_1$, то

$$s_{D_1}(p) = 1 \iff p \in L_1(s) \iff p \in L(s) \iff s_D(p) = 1,$$

т. е. в данном случае (42) верно.

Предположим, что для каждой подформулы f' формулы f верно равенство (42) или (43), в котором f заменено на f' . Докажем, что в этом случае будет верно (42) или (43).

1. Пусть f является булевой комбинацией. Рассмотрим, например, случай $f = \neg f'$. Для каждого $s \in S_1$

$$s_{D_1}(f) = s_{D_1}(\neg f') = 1 - s_{D_1}(f') = 1 - s_D(f') = s_D(\neg f') = s_D(f).$$

Другие случаи возможного вида f , когда f является булевой комбинацией, рассматриваются аналогично.

2. Пусть $f = \mathcal{P}_{\Delta a} \alpha$. Тогда

$$s_{D_1}(f) = \Delta(s_{D_1}(\alpha), a) = \Delta(s_D(\alpha), a) = s_D(f).$$

3. Пусть $f = \mathbf{X}f'$. Докажем, что верно равенство (43). Согласно определению матрицы $\text{id}_S \setminus \vec{s}_1$ данное равенство равносильно равенству

$$S_{D_1}(f) = (\text{id}_S \setminus \vec{s}_1) \cdot S_D(f). \quad (44)$$

Мы предполагаем, что (44) будет верно, если f заменить на f' , т. е. справедливо

$$S_{D_1}(f') = (\text{id}_S \setminus \vec{s}_1) \cdot S_D(f'). \quad (45)$$

Согласно определению значений формулы $\mathbf{X}f'$, верны равенства

$$S_{D_1}(f) = S_{D_1}(\mathbf{X}f') = P_1 \cdot S_{D_1}(f'), \quad S_D(f) = S_D(\mathbf{X}f') = P \cdot S_D(f').$$

Учитывая (41) и индуктивное предположение (45), можно переписать доказываемое равенство (44) следующим образом:

$$\begin{aligned} (\text{id}_S \setminus \vec{s}_1) \cdot P \cdot \text{id}_S(s_1, s_2, 1) \cdot (\text{id}_S \setminus s_1^\perp) \cdot (\text{id}_S \setminus \vec{s}_1) \cdot S_D(f') = \\ = (\text{id}_S \setminus \vec{s}_1) \cdot P \cdot S_D(f'). \end{aligned} \quad (46)$$

Нетрудно проверить, что

- произведение матриц $(\text{id}_S \setminus s_1^\perp) \cdot (\text{id}_S \setminus \vec{s}_1)$ совпадает с матрицей $\text{id}_S(s_1, s_1, 0)$, получаемой из id_S заменой элемента в строке s_1 и столбце s_1 на 0;
- произведение $\text{id}_S(s_1, s_2, 1) \cdot \text{id}_S(s_1, s_1, 0)$ совпадает с матрицей

$$\text{id}_S \begin{pmatrix} s_1, s_2, 1 \\ s_1, s_1, 0 \end{pmatrix},$$

получаемой из id_S заменой элемента в строке s_1 и столбце s_2 на 1 и элемента в строке s_1 и столбце s_1 на 0;

- произведение

$$\text{id}_S \begin{pmatrix} s_1, s_2, 1 \\ s_1, s_1, 0 \end{pmatrix} \cdot S_D(f') \quad (47)$$

совпадает с вектор-столбцом, получаемым из $S_D(f')$ заменой элемента в строке s_1 на элемент $s_2(f')$.

Поскольку состояния s_1 и s_2 по предположению эквивалентны, то по определению понятия эквивалентности состояний верно равенство $s_1(f') = s_2(f')$. Следовательно, (47) совпадает с $S_D(f')$.

Из приведённых утверждений следует, что левая часть доказываемого равенства (46) совпадает с его правой частью, что и требовалось доказать.

4. Пусть $f = \varphi_1 \mathbf{U}^{\leq n} \varphi_2$. Обозначим эту формулу через α_n . Докажем индукцией по n , что

$$S_{D_1}(\alpha_n) = S_D(\alpha_n) \setminus \vec{s}_1.$$

Если $n = 0$, то по определению

$$S(\alpha_n) = S(\varphi_2)$$

и доказываемое утверждение верно потому, что φ_2 — подформула формулы f .

Если $n > 0$, то по определению

$$S(\alpha_n) = \max(S(\varphi_2), S(\varphi_1) \circ S(\mathbf{X}\alpha_{n-1}))$$

и истинность доказываемого утверждения следует из его истинности для φ_1 , φ_2 , α_{n-1} и $\mathbf{X}\alpha_{n-1}$, а также из определения операций $\max$ и $\circ$ на вектор-столбцах.

5. Пусть $f = \varphi_1 \mathbf{U} \varphi_2$. Согласно определению вектор-столбцы $S_D(f)$ и $S_{D_1}(f)$ удовлетворяют соотношениям

$$S_D(f) = \max\left(S_D(\varphi_2), [P^* \cdot S_D(\varphi_2)] \circ S_D(\varphi_1) \circ (P \cdot S_D(f))\right), \quad (48)$$

$$S_{D_1}(f) = \max\left(S_{D_1}(\varphi_2), [(P_1)^* \cdot S_{D_1}(\varphi_2)] \circ S_{D_1}(\varphi_1) \circ (P_1 \cdot S_{D_1}(f))\right). \quad (49)$$

Для доказательства равенства (43) мы докажем следующее утверждение: замена в соотношении (49) компонентов вектора $S_{D_1}(f)$ на соответствующие компоненты вектора $S_D(f) \setminus \vec{s}_1$ не нарушает истинности этого соотношения. Это утверждение следует из (48), определения операций $\max$ и $\circ$ на вектор-столбцах и из следующих соотношений:

— равенств

$$\begin{aligned} S_{D_1}(\varphi_1) &= S_D(\varphi_1) \setminus \vec{s}_1, \\ S_{D_1}(\varphi_2) &= S_D(\varphi_2) \setminus \vec{s}_1, \end{aligned} \quad (50)$$

которые верны по индуктивному предположению;

— равенств

$$[P^* \cdot S_D(\varphi_2)] \setminus \vec{s}_1 = [(P_1)^* \cdot S_{D_1}(\varphi_2)], \quad (51)$$

$$(P \cdot S_D(f)) \setminus \vec{s}_1 = P_1 \cdot (S_{D_1}(f) \setminus \vec{s}_1). \quad (52)$$

Из второго равенства в (50) следует, что (51) можно заменить на равенство

$$[P^* \cdot S_D(\varphi_2)] \setminus \vec{s}_1 = [(P_1)^* \cdot (S_D(\varphi_2) \setminus \vec{s}_1)]. \quad (53)$$

Истинность равенства (52) доказывается рассуждениями, аналогичными тем, которые были приведены в пункте 3 настоящего доказательства.

Докажем (53). Для каждого $n \geq 0$ верно равенство

$$(P^n \cdot S_D(\varphi_2)) \setminus \vec{s}_1 = P_1^n \cdot (S_D(\varphi_2) \setminus \vec{s}_1), \quad (54)$$

которое нетрудно доказать индукцией по n .

Для каждого $s \in S_1$ элемент s столбца $[P^* \cdot S_D(\varphi_2)] \setminus \vec{s}_1$ равен 1 тогда и только тогда, когда найдётся такое $n \geq 0$, что элемент s столбца $(P^n \cdot S_D(\varphi_2)) \setminus \vec{s}_1$ отличен от 0. Согласно (54) это эквивалентно тому, что найдётся такое $n \geq 0$, что элемент s столбца $P_1^n \cdot (S_D(\varphi_2) \setminus \vec{s}_1)$ отличен от 0, а это эквивалентно тому, что элемент s столбца $[P_1^* \cdot (S_D(\varphi_2) \setminus \vec{s}_1)]$ равен 1. Это доказывает равенство (53).

Таким образом, теорема 2 полностью доказана. $\square$

5.4.4. Описание алгоритма редукции ВСП

Теорема 2 является обоснованием излагаемого ниже алгоритма редукции ВСП $D = (S, s^0, P, L)$. Этот алгоритм имеет следующий вид.

1. Вычисляется разбиение множества состояний ВСП D , соответствующее отношению эквивалентности $R \stackrel{\text{def}}{=} \rho(\text{PCTL})$ (для этого выполняются действия, изложенные в пункте 5.4.2).
2. Искомая ВСП D' строится путём удаления состояний из ВСП D и перепределения функции перехода и отношения R следующим образом.
 - 1) Если отношение R содержит пару (s_1, s_2) , такую что $s_1 \neq s_2$ и $s_2 \neq s^0$, то выберем произвольную такую пару (s_1, s_2) , и преобразуем компоненты ВСП D описываемым ниже образом. Мы будем излагать данное преобразование в терминах графа, соответствующего ВСП D (данный граф мы будем обозначать тем же символом D).
 - а) Если граф D содержит ребро с началом в некоторой вершине s и с концом в s_2 , то данное ребро удаляется, а к метке ребра с началом в s и с концом в s_1 прибавляется число, равное метке удалённого ребра. Данная операция выполняется до тех пор, пока имеются рёбра с концом в s_2 .
 - б) Вершина s_2 удаляется, и, кроме того, удаляются все рёбра, входящие из этой вершины.
 - в) Из R удаляются все пары, содержащие s_2 .
 - г) После этого мы переходим на шаг 1).
 - 2) Если каждая пара, входящая в R , имеет вид (s, s) , то алгоритм завершает работу.

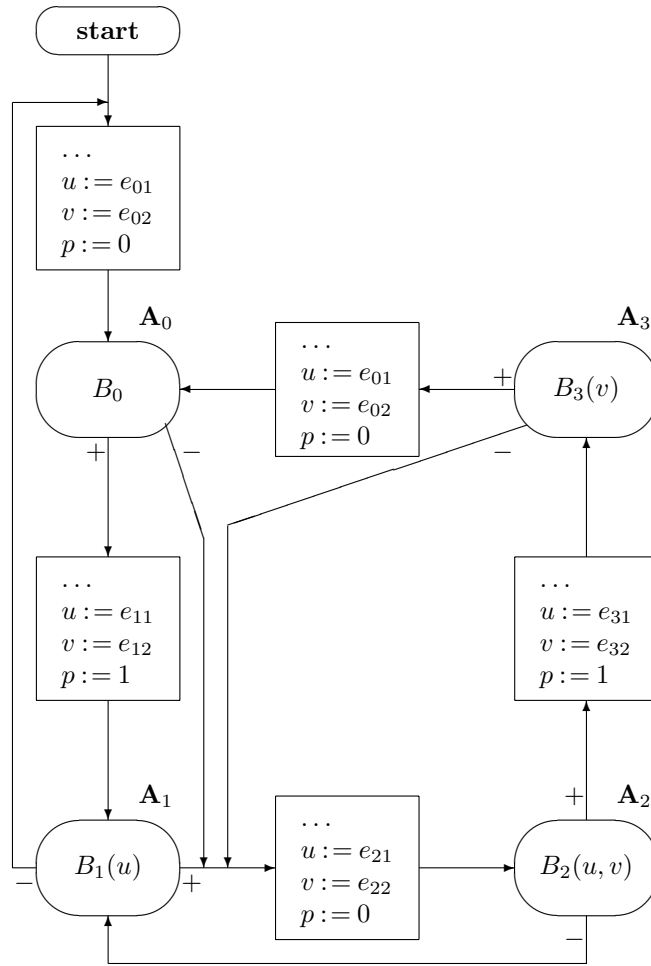
Нетрудно доказать, что временную сложность данного алгоритма можно оценить сверху функцией $O(2^p \cdot n + n^3)$, где p — число элементов множества АР и n — число состояний ВСП.

6. Пример редукции вероятностной системы переходов

В этом разделе мы рассмотрим пример использования предложенного в настоящей работе алгоритма редукции ВСП.

6.1. Описание редуцируемой ВСП

ВСП, рассматриваемая в этом примере, является вероятностной абстракцией последовательной незавершающейся программы, представляемой блок-схемой



(55)

где символы $\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$ рядом с условными операторами можно рассматривать как имена данных операторов.

Программа содержит булевы переменные p, u, v (которые мы будем рассматривать как существенные переменные данной блок-схемы) и некоторые другие переменные, не указанные на данной блок-схеме (их мы будем рассматривать как несущественные переменные данной блок-схемы). В условных операторах данной блок-схемы используются булевозначные выражения B_0 и т. д., в каждом из которых в скобках указаны лишь существенные переменные, от которых зависит данное булевозначное выражение.

Значения переменных p, u и v изменяются операторами присваивания, в правой части которых стоит терм, зависящий от u, v и других переменных блок-схемы. Операторы присваивания, которые изменяют значения переменных, отличных от p, u и v , не принимаются во внимание и изображены многоточием.

Предположим, что анализируется какое-либо частное свойство данной блок-схемы, связанное со статистическими закономерностями изменения значения переменной p . Для анализа свойства данного типа мы построим ВСП, являющуюся вероятностной абстракцией данной блок-схемы.

Процесс функционирования данной блок-схемы можно интерпретировать как процесс перехода от одного условного оператора $\mathbf{A}_i$ к другому оператору $\mathbf{A}_j$ с выполнением операторов присваивания, которые встречаются на пути от $\mathbf{A}_i$ к $\mathbf{A}_j$, т. е.

- при переходе от $\mathbf{A}_0$ к $\mathbf{A}_1$ выполняются операторы присваивания $\dots, u := e_{11}, v := e_{12}, p := 1$,
- при переходе от $\mathbf{A}_0$ к $\mathbf{A}_2$ выполняются операторы присваивания $\dots, u := e_{21}, v := e_{22}, p := 0$
- и т. д.

Напомним (см. [3]), что полная диаграмма состояний, соответствующая блок-схеме, представляет собой граф, вершины которого отвечают состояниям блок-схемы, где под состоянием понимается набор значений, поставленных в соответствие переменным блок-схемы, а также управляющей переменной, которая не входит в число переменных блок-схемы и значениями которой являются операторы блок-схемы.

Построим упрощённую диаграмму состояний данной блок-схемы, соответствующую такому уровню абстракции, при котором из переменных блок-схемы мы будем учитывать лишь переменные p, u и v и множество значений управляющей переменной будем считать равным $\{\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3\}$ (принимая во внимание высказанное выше замечание о том, что каждый шаг функционирования блок-схемы можно интерпретировать как переход от оператора вида $\mathbf{A}_i$ к оператору вида $\mathbf{A}_j$ с выполнением присваиваний, находящихся на пути от $\mathbf{A}_i$ к $\mathbf{A}_j$).

Таким образом, при выбранном уровне абстракции диаграмма состояний должна содержать $2 \cdot 2 \cdot 2 \cdot 4$ состояний. Однако из визуального анализа блок-схемы мы можем заключить, что значение переменной p однозначно определяется значением управляющей переменной (в операторах $\mathbf{A}_0$ и $\mathbf{A}_2$ значение p равно 0,

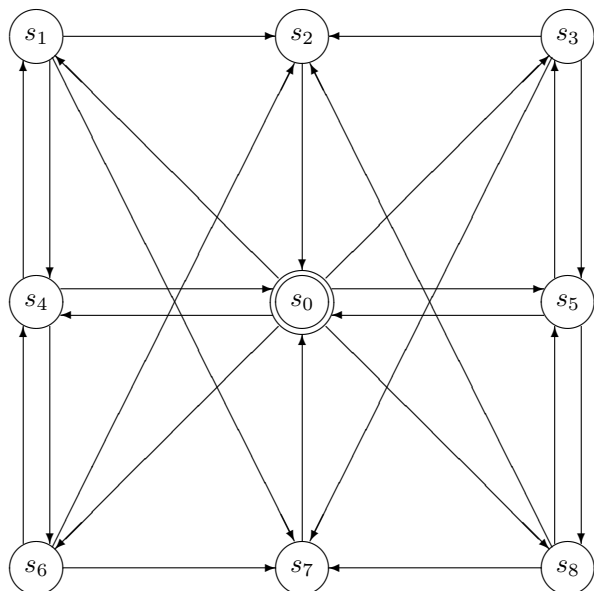
а в операторах $\mathbf{A}_1$ и $\mathbf{A}_3$ значение p равно 1), и следовательно, количество состояний может быть сокращено до $2 \cdot 2 \cdot 4$. Мы будем обозначать эти состояния записями вида $\mathbf{A}_i(j, k)$, где j и k — значения переменных u и v в состоянии $\mathbf{A}_i(j, k)$.

Из визуального анализа блок-схемы видно, что

- функционирование блок-схемы в тот момент, когда значение её управляющей переменной равно $\mathbf{A}_0$, не зависит от значений переменных u и v , поэтому все состояния вида $\mathbf{A}_0(j, k)$ можно рассматривать как одинаковые, мы будем обозначать все такие состояния через $\mathbf{A}_0$,
- функционирование блок-схемы в тот момент, когда значение её управляющей переменной равно $\mathbf{A}_1$, зависит только от значения переменной u , поэтому состояния вида $\mathbf{A}_1(j, k)$ с одинаковыми первыми компонентами в скобках можно рассматривать как одинаковые, мы будем обозначать их $\mathbf{A}_1(0)$ и $\mathbf{A}_1(1)$,
- функционирование блок-схемы в тот момент, когда значение её управляющей переменной равно $\mathbf{A}_3$, зависит только от значения переменной v , поэтому состояния вида $\mathbf{A}_3(j, k)$ с одинаковыми вторыми компонентами в скобках можно рассматривать как одинаковые, мы будем обозначать эти состояния $\mathbf{A}_3(0)$ и $\mathbf{A}_3(1)$.

Таким образом, после всех вышеперечисленных отождествлений осталось девять состояний: $\mathbf{A}_0$, $\mathbf{A}_1(0)$, $\mathbf{A}_1(1)$, $\mathbf{A}_2(0, 0)$, $\mathbf{A}_2(0, 1)$, $\mathbf{A}_2(1, 0)$, $\mathbf{A}_2(1, 1)$, $\mathbf{A}_3(0)$, $\mathbf{A}_3(1)$. Мы будем обозначать их более коротко s_0 , s_4 , s_5 , s_1 , s_6 , s_3 , s_8 , s_7 , s_2 .

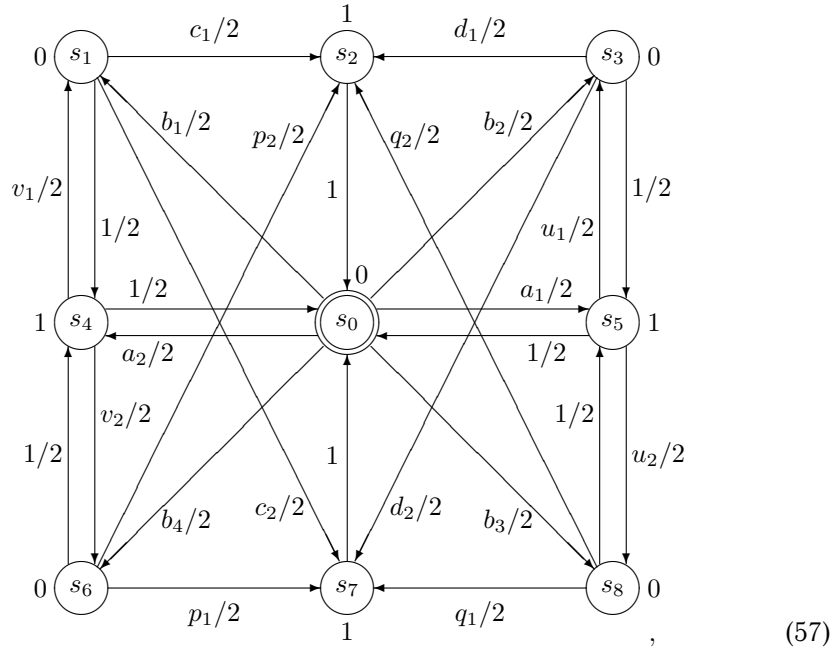
Путём дополнительного анализа данной блок-схемы можно установить, что граф переходов, соответствующий данному множеству состояний, имеет вид



(56)

Путём проведения тестовых испытаний с блок-схемой мы определяем статистические закономерности: для каждого перехода $s_i \rightarrow s_j$ в данной диаграмме мы определяем вероятность того, что если в текущий момент времени блок-схема находится в состоянии s_i , то в следующий момент времени она будет находиться в состоянии s_j . Искомая ВСП представляет собой граф (56), с каждым ребром которого связана соответствующая вероятность (полученная экспериментальным образом).

Предположим, что в результате проведения таких испытаний была получена следующая ВСП:



где в обозначениях вероятностей переходов мы используем буквенные обозначения, которые имеют следующий смысл: символы $a_1, a_2, \dots$ обозначают неотрицательные действительные числа, удовлетворяющие следующим ограничениям:

$$\begin{aligned}
 a_1 + a_2 &= 1, \\
 b_1 + b_2 + b_3 + b_4 &= 1, \\
 c_1 + c_2 &= 1, \\
 d_1 + d_2 &= 1, \\
 p_1 + p_2 &= 1, \\
 q_1 + q_2 &= 1, \\
 u_1 + u_2 &= 1, \\
 v_1 + v_2 &= 1.
 \end{aligned}
 \tag{58}$$

В этой ВСП множество АР атомарных утверждений состоит из одного утверждения p , т. е. множество 2^{AP} состоит из двух элементов: $\emptyset$ и $\{p\}$. Мы будем обозначать эти элементы символами 0 и 1 соответственно.

Начальным состоянием данной ВСП является состояние s_0 , оно обозначено двойным кружком. Рядом с каждым состоянием s приписана метка, которая равна значению $L(s)$.

Матрицу P , соответствующую данной ВСП, мы представим в виде следующей таблицы:

	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
s_0	0	$b_1/2$	0	$b_2/2$	$a_2/2$	$a_1/2$	$b_4/2$	0	$b_3/2$
s_1	0	0	$c_1/2$	0	$1/2$	0	0	$c_2/2$	0
s_2	1	0	0	0	0	0	0	0	0
s_3	0	0	$d_1/2$	0	0	$1/2$	0	$d_2/2$	0
s_4	$1/2$	$v_1/2$	0	0	0	0	$v_2/2$	0	0
s_5	$1/2$	0	0	$u_1/2$	0	0	0	0	$u_2/2$
s_6	0	0	$p_2/2$	0	$1/2$	0	0	$p_1/2$	0
s_7	1	0	0	0	0	0	0	0	0
s_8	0	0	$q_2/2$	0	0	$1/2$	0	$q_1/2$	0

Левый столбец и верхняя строка в этой таблице не являются элементами матрицы P , они предназначены для интерпретации коэффициентов в этой таблице: для каждой пары состояний $(s_i, s_j) \in S \times S$ значение $P(s_i, s_j)$ располагается в пересечении строки, содержащей s_i , и столбца, содержащего s_j .

6.2. Вычисление эквивалентности $\rho(PCTL)$ для редуцируемой ВСП

Вычисление эквивалентности $\rho(PCTL)$ для ВСП (56) происходит следующим образом.

1. Вычисляется отношение эквивалентности ρ^0 , которое состоит из всех пар $(s_1, s_2) \in S \times S$, удовлетворяющих равенству $L(s_1) = L(s_2)$.

Нетрудно убедиться, что Σ^0 состоит из двух классов

$$\{s_0, s_1, s_3, s_6, s_8\}, \quad \{s_2, s_4, s_5, s_7\}. \quad (59)$$

2. Матрица π^0 , соответствующая детерминированной СФ $\pi^0: S \rightarrow \Sigma^0$, имеет вид

s_0	1	0
s_1	1	0
s_2	0	1
s_3	1	0
s_4	0	1
s_5	0	1
s_6	1	0
s_7	0	1
s_8	1	0

Затем вычисляется матрица $P \cdot \pi^0$. Она будет иметь вид

0	$b_1/2 + b_2/2 + b_4/2 + b_3/2$	$a_2/2 + a_1/2$
1	0	$c_1/2 + 1/2 + c_2/2$
2	1	0
3	0	$d_1/2 + 1/2 + d_2/2$
4	$1/2 + v_1/2 + v_2/2$	0
5	$1/2 + u_1/2 + u_2/2$	0
6	0	$p_2/2 + 1/2 + p_1/2$
7	1	0
8	0	$q_2/2 + 1/2 + q_1/2$

Принимая во внимание ограничения (58), данную матрицу можно упростить до

0	1/2	1/2
1	0	1
2	1	0
3	0	1
4	1	0
5	1	0
6	0	1
7	1	0
8	0	1

(60)

По матрице (60) нетрудно вычислить отношение ρ^1 и соответствующее ему разбиение Σ^1 . Из определения отношения ρ^1 непосредственно следует, что состояния s_1 и s_2 находятся в одном и том же классе разбиения Σ^1 тогда и только тогда, когда они оба находятся в одном и том же классе из списка (59), и, кроме того, строки матрицы (60), соответствующие состояниям s_1 и s_2 , совпадают.

Разбиение Σ^1 будет состоять из трёх классов (измельчится первый класс в (59), а второй класс останется тем же), эти классы имеют следующий вид:

$$\{s_0\}, \quad \{s_1, s_3, s_6, s_8\}, \quad \{s_2, s_4, s_5, s_7\}. \quad (61)$$

3. Затем вычисляется матрица π^1 , соответствующая детерминированной СФ $\pi^1: S \xrightarrow{r} \Sigma^1$. Она будет иметь следующий вид:

0	1	0	0
1	0	1	0
2	0	0	1
3	0	1	0
4	0	0	1
5	0	0	1
6	0	1	0
7	0	0	1
8	0	1	0

Произведение $P \cdot \pi_1$ имеет следующий вид:

0	0	$b_1/2 + b_2/2 + b_4/2 + b_3/2$	$a_2/2 + a_1/2$
1	0	0	$c_1/2 + 1/2 + c_2/2$
2	1	0	0
3	0	0	$d_1/2 + 1/2 + d_2/2$
4	1/2	$v_1/2 + v_2/2$	0
5	1/2	$u_1/2 + u_2/2$	0
6	0	0	$p_2/2 + 1/2 + p_1/2$
7	1	0	0
8	0	0	$q_2/2 + 1/2 + q_1/2$

Принимая во внимание ограничения (58), данную матрицу можно упростить до

0	0	1/2	1/2
1	0	0	1
2	1	0	0
3	0	0	1
4	1/2	1/2	0
5	1/2	1/2	0
6	0	0	1
7	1	0	0
8	0	0	1

После этого, действуя аналогично предыдущему пункту, вычисляем классы разбиения Σ^2 , соответствующего эквивалентности ρ^2 . Таких классов будет четыре (измельчится третий класс в (61), а первый и второй классы останутся теми же), эти классы имеют следующий вид:

$$\{s_0\}, \quad \{s_1, s_3, s_6, s_8\}, \quad \{s_2, s_7\}, \quad \{s_4, s_5\}. \quad (62)$$

4. Затем вычисляется матрица π^2 , соответствующая детерминированной СФ $\pi^2: S \xrightarrow{r} \Sigma^2$. Данная матрица будет иметь следующий вид:

0	1	0	0	0
1	0	1	0	0
2	0	0	1	0
3	0	1	0	0
4	0	0	0	1
5	0	0	0	1
6	0	1	0	0
7	0	0	1	0
8	0	1	0	0

Произведение $P \cdot \pi_2$ имеет следующий вид:

0	0	$b_1/2 + b_2/2 + b_4/2 + b_3/2$	0	$a_2/2 + a_1/2$
1	0	0	$c_1/2 + c_2/2$	1/2
2	1	0	0	0
3	0	0	$d_1/2 + d_2/2$	1/2
4	1/2	$v_1/2 + v_2/2$	0	0
5	1/2	$u_1/2 + u_2/2$	0	0
6	0	0	$p_2/2 + p_1/2$	1/2
7	1	0	0	0
8	0	0	$q_2/2 + q_1/2$	1/2

Принимая во внимание ограничения (58), данную матрицу можно упростить до

0	0	1/2	0	1/2
1	0	0	1/2	1/2
2	1	0	0	0
3	0	0	1/2	1/2
4	1/2	1/2	0	0
5	1/2	1/2	0	0
6	0	0	1/2	1/2
7	1	0	0	0
8	0	0	1/2	1/2

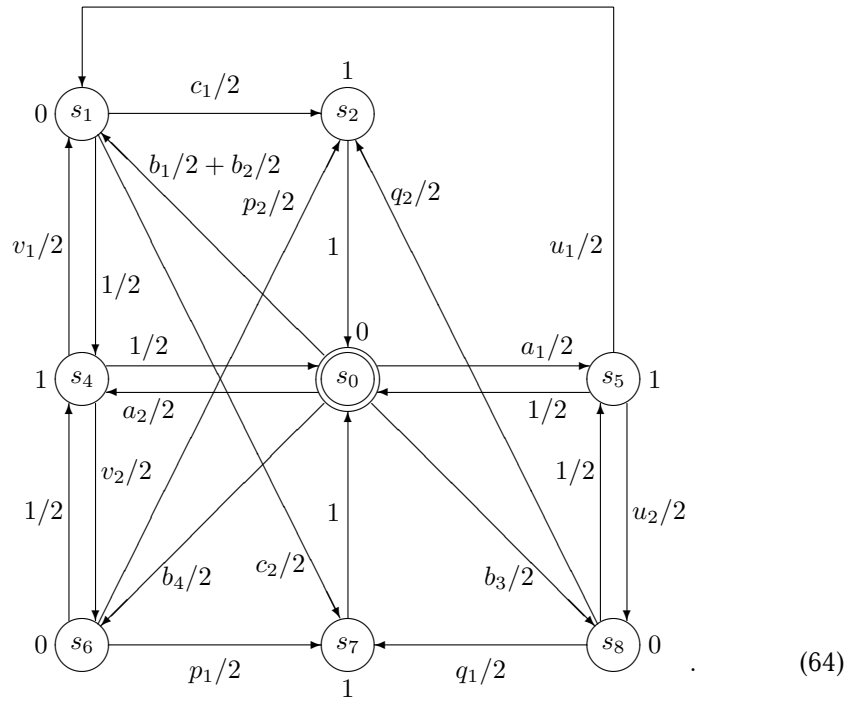
(63)

После этого, действуя аналогично предыдущему пункту, вычисляем классы разбиения Σ^3 , соответствующего эквивалентности ρ^3 . Нетрудно проверить, что классы разбиения Σ^3 будут иметь точно такой же вид, что и классы эквивалентности разбиения Σ^2 . Это означает, что искомое разбиение множества S на классы эквивалентных состояний построено, оно имеет вид (62).

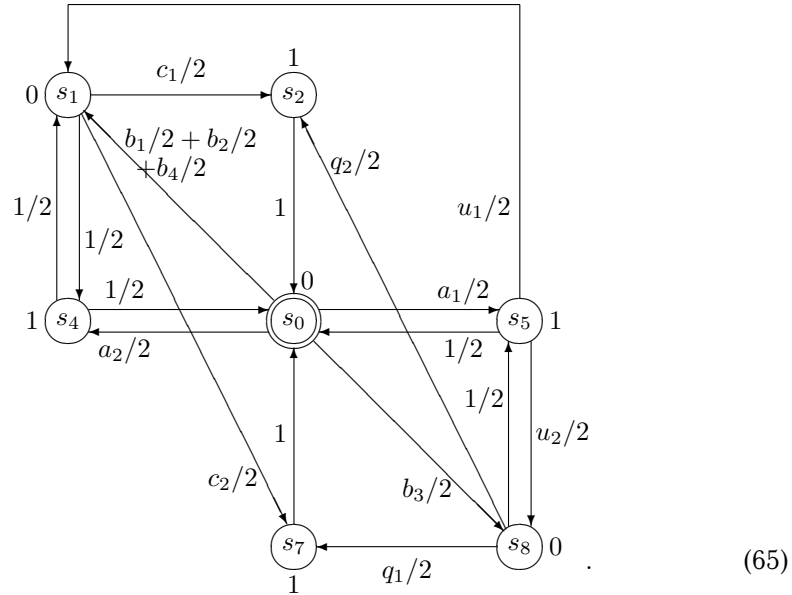
6.3. Удаление избыточных состояний

Теперь можно приступить к удалению избыточных состояний (чтобы среди оставшихся состояний было ровно по одному состоянию из каждого класса эквивалентности (62)). Нетрудно убедиться, что можно удалить состояния s_3 , s_6 , s_8 , s_7 , s_5 .

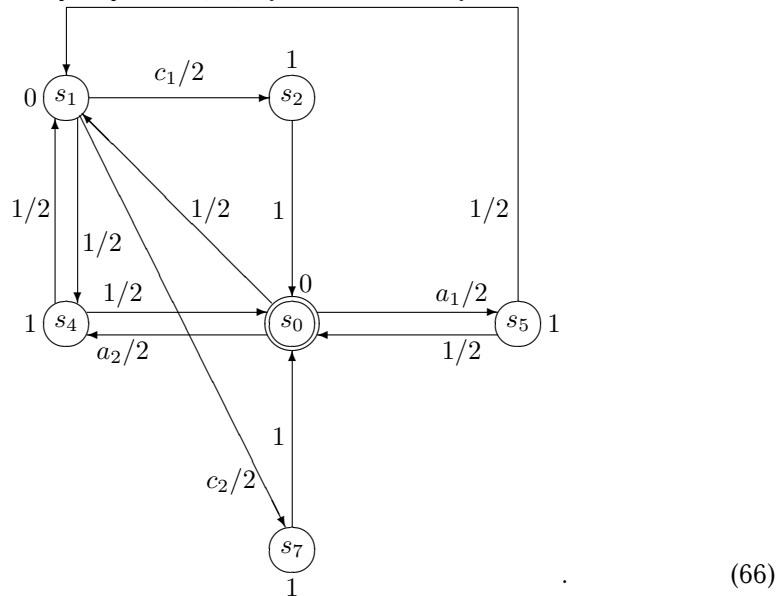
1. Удаление состояния s_3 . Совокупность всех рёбер ВСП (57) с концом s_3 и ненулевыми метками имеет следующий вид: ребро из s_0 в s_3 с меткой $b_2/2$ и ребро из s_5 в s_3 с меткой $u_1/2$. В соответствии с алгоритмом к меткам рёбер из s_0 в s_1 и из s_5 в s_1 мы прибавляем $b_2/2$ и $u_1/2$ соответственно и удаляем состояние s_3 и все связанные с ним рёбра. После удаления состояния s_3 и связанных с ним рёбер ВСП (57) примет следующий вид:



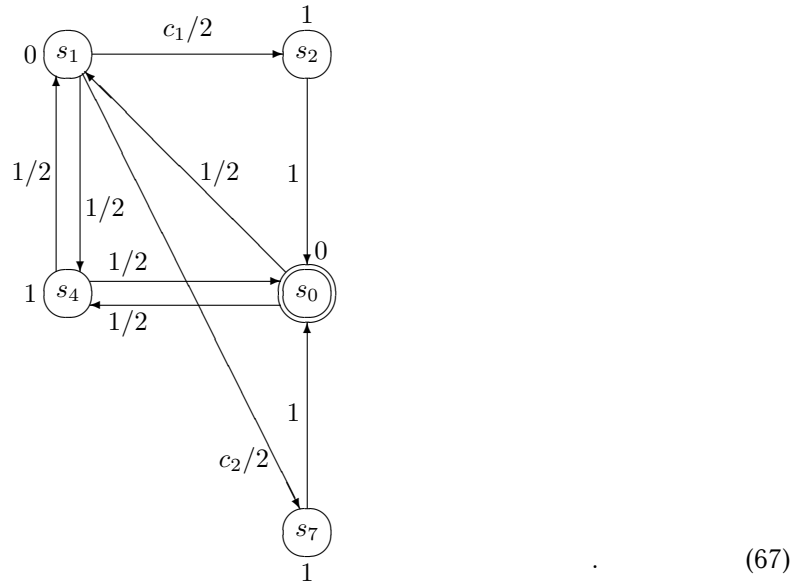
2. Удаление состояния s_6 . Совокупность всех рёбер ВСП (64) с концом s_6 и ненулевыми метками имеет следующий вид: ребро из s_0 в s_6 с меткой $b_4/2$ и ребро из s_4 в s_6 с меткой $v_2/2$. В соответствии с алгоритмом к меткам рёбер из s_0 в s_1 и из s_4 в s_1 мы прибавляем $b_4/2$ и $v_2/2$ соответственно и удаляем состояние s_6 и все связанные с ним рёбра. Принимая во внимание соотношение $v_1 + v_2 = 1$, получаем, что после удаления состояния s_6 и связанных с ним рёбер ВСП (64) будет иметь следующий вид:



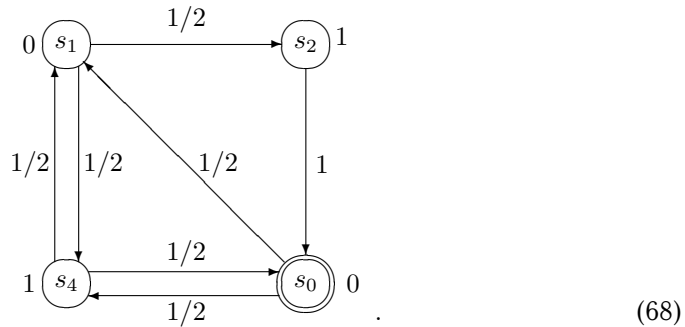
3. Удаление состояния s_8 . Совокупность всех рёбер ВСП (65) с концом s_8 и ненулевыми метками имеет следующий вид: ребро из s_0 в s_8 с меткой $b_3/2$ и ребро из s_5 в s_8 с меткой $u_2/2$. В соответствии с алгоритмом к меткам рёбер из s_0 в s_1 и из s_5 в s_1 мы прибавляем $b_3/2$ и $u_2/2$ соответственно и удаляем состояние s_8 и все связанные с ним рёбра. Принимая во внимание соотношения $u_1 + u_2 = 1$ и $b_1 + b_2 + b_3 + b_4 = 1$, получаем, что после удаления состояния s_8 и связанных с ним рёбер ВСП (65) будет иметь следующий вид:



4. Удаление состояния s_5 . Совокупность всех рёбер ВСП (66) с концом s_5 и ненулевыми метками состоит из одного ребра из s_0 в s_5 с меткой $a_1/2$. В соответствии с алгоритмом к метке ребра из s_0 в s_4 мы прибавляем $a_1/2$ и удаляем состояние s_5 и все связанные с ним рёбра. Принимая во внимание соотношение $a_1 + a_2 = 1$, получаем, что после удаления состояния s_5 и связанных с ним рёбер ВСП (66) будет иметь следующий вид:



5. Удаление состояния s_7 . Совокупность всех рёбер ВСП (67) с концом s_7 и ненулевыми метками состоит из одного ребра из s_1 в s_7 с меткой $c_2/2$. В соответствии с алгоритмом к метке ребра из s_1 в s_2 мы прибавляем $c_2/2$ и удаляем состояние s_7 и все связанные с ним рёбра. Принимая во внимание соотношение $c_1 + c_2 = 1$, получаем, что после удаления состояния s_7 и связанных с ним рёбер ВСП (67) будет иметь следующий вид:



ВСП (68) далее не редуцируется: нетрудно убедиться, что все её состояния неэквивалентны.

Таким образом, в результате редукции исходная ВСП (57) с девятью состояниями упростится до эквивалентной ей ВСП (68) с четырьмя состояниями.

7. Пример вычисления значений формулы логики PCTL в состояниях вероятностных систем переходов

Рассмотрим в качестве примера следующую формулу логики PCTL:

$$\mathcal{P}_{=1} \mathbf{F}^{\leq 2} p. \quad (69)$$

Мы будем интерпретировать эту формулу следующим образом. Значение переменной p в каком-либо состоянии мы будем понимать как наличие некоторой неисправности в этом состоянии: если $s(p) = 1$, то мы будем считать, что в состоянии s моделируемой системы имеется неисправность, если $s(p) = 0$, то мы считаем, что в состоянии s неисправность отсутствует. При такой интерпретации формулу (69) можно интерпретировать как следующее утверждение: с вероятностью 1 из любого состояния будет достижимо за не более чем два шага состояние, в котором будет присутствовать неисправность.

Вычислим значения этой формулы в состояниях ВСП (57). Для этого мы должны вычислить значения всех подформул формулы (69) в состояниях ВСП (57). Нетрудно убедиться, что список подформул формулы (69) имеет следующий вид:

$$p, \mathbf{F}^{\leq 2} p, \mathcal{P}_{=1} \mathbf{F}^{\leq 2} p. \quad (70)$$

Значения подформулы p в состояниях ВСП (57) имеют следующий вид:

	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
p	0	0	1	0	1	1	0	1	0

Для вычисления значений подформулы $\mathbf{F}^{\leq 2} p$ в состояниях ВСП (57) мы будем использовать следующий алгоритм вычисления значений формул вида $\mathbf{F}^{\leq n} \varphi$ (непосредственно вытекающий из определения значений формул вида $\varphi_1 \mathbf{U}^{\leq n} \varphi_2$): значения

$$a_{sn} \stackrel{\text{def}}{=} s(\mathbf{F}^{\leq n} \varphi)$$

вычисляем следующим образом:

- для каждого $i = 0, \dots, n$ и каждого $s \in S$

$$a_{si} := s(\varphi);$$

- для каждого $i = 1, \dots, n$ и каждого $s \in S$ если $a_{si} = 0$, то

$$a_{si} := \sum_{s' \in S} P(s, s') \cdot a_{s', i-1}.$$

Согласно этому алгоритму, значения a_{si} , соответствующие формуле $\mathbf{F}^{\leq 2}p$ и состояниям ВСП (57), имеют следующий вид:

	$i = 0$	$i = 1$	$i = 2$
s_0	0	$b_1/2 \cdot 0 + b_2/2 \cdot 0 + b_3/2 \cdot 0 +$ $+ b_4/2 \cdot 0 + a_1/2 \cdot 1 +$ $+ a_2/2 \cdot 1 = 1/2$	$b_1/2 \cdot 1 + b_2/2 \cdot 1 + b_3/2 \cdot 1 +$ $+ b_4/2 \cdot 1 + a_1/2 \cdot 1 +$ $+ a_2/2 \cdot 1 = 1$
s_1	0	$c_1/2 \cdot 1 + c_2/2 \cdot 1 + 1/2 \cdot 1 = 1$	$c_1/2 \cdot 1 + c_2/2 \cdot 1 + 1/2 \cdot 1 = 1$
s_2	1	1	1
s_3	0	$d_1/2 \cdot 1 + d_2/2 \cdot 1 + 1/2 \cdot 1 = 1$	$d_1/2 \cdot 1 + d_2/2 \cdot 1 + 1/2 \cdot 1 = 1$
s_4	1	1	1
s_5	1	1	1
s_6	0	$p_1/2 \cdot 1 + p_2/2 \cdot 1 + 1/2 \cdot 1 = 1$	$p_1/2 \cdot 1 + p_2/2 \cdot 1 + 1/2 \cdot 1 = 1$
s_7	1	1	1
s_8	0	$q_1/2 \cdot 1 + q_2/2 \cdot 1 + 1/2 \cdot 1 = 1$	$q_1/2 \cdot 1 + q_2/2 \cdot 1 + 1/2 \cdot 1 = 1$

Таким образом, значение подформулы $\mathbf{F}^{\leq 2}p$ во всех состояниях ВСП (57) равно 1, откуда следует, что значение формулы (69) во всех состояниях ВСП (57) равно 1.

Теперь рассмотрим задачу вычисления значений той же самой формулы (69) в состояниях редуцированной ВСП (68). Так же, как и в предыдущем случае, мы вычисляем значения всех подформул формулы (69) в состояниях ВСП (68).

Значения подформулы p в состояниях ВСП (68) имеют следующий вид:

	s_0	s_1	s_2	s_4
p	0	0	1	1

Значения a_{si} , соответствующие формуле $\mathbf{F}^{\leq 2}p$ и состояниям ВСП (68), вычисляются по описанному выше алгоритму и имеют следующий вид:

	$i = 0$	$i = 1$	$i = 2$
s_0	0	$1/2 \cdot 0 + 1/2 \cdot 1 = 1/2$	$1/2 \cdot 1 + 1/2 \cdot 1 = 1$
s_1	0	$1/2 \cdot 1 + 1/2 \cdot 1 = 1$	$1/2 \cdot 1 + 1/2 \cdot 1 = 1$
s_2	1	1	1
s_4	1	1	1

Таким образом, как и в предыдущем случае, значение подформулы $\mathbf{F}^{\leq 2}p$ во всех состояниях ВСП (68) равно 1, откуда следует, что значение формулы (69) во всех состояниях ВСП (68) равно 1.

Отметим, что процедура вычисления значений формулы (69) в состояниях редуцированной ВСП (68) имеет существенно меньшую сложность, чем процедура вычисления значений этой формулы в состояниях исходной ВСП (57). Это

свидетельствует о пользе предложенного в настоящей работе подхода редукции анализируемой ВСП перед вычислением значений формул логики PCTL в её состояниях.

8. Заключение

В настоящей работе изложен алгоритм редукции вероятностных систем переходов, идея которого заключается в удалении избыточных состояний. Отметим, что в результате такой редукции может получиться ВСП, которая, хотя и не содержит различных эквивалентных состояний, может не являться минимальной по числу состояний среди всех ВСП, эквивалентных исходной ВСП. В связи с этим встаёт вопрос об алгоритме нахождения минимальной по числу состояний ВСП, эквивалентной заданной ВСП, и исследовании единственности такой минимальной ВСП (с точностью до подходящим образом сформулированного понятия изоморфизма). Также представляет интерес исследование проблем минимизации других классов моделей, связанных с вероятностной верификацией, в частности минимизации марковских решающих процессов.

Кроме этих задач, для вероятностной верификации актуальны все задачи, связанные с классической теорией Model Checking, в частности

- разработка методов верификации ВСП «на лету» (см. [3]), т. е. методов, связанных с построением тех фрагментов ВСП, которых достаточно для проверки анализируемого свойства;
- построение символьных методов вероятностной верификации (в том числе нахождение аналогов понятия бинарных разрешающих диаграмм [3] для ВСП).

Литература

- [1] Бухараев Р. Г. Основы теории вероятностных автоматов. — М.: Наука, 1985.
- [2] Кемени Дж., Снелл Дж. Конечные цепи Маркова. — М.: Наука, 1970.
- [3] Кларк Э. М., Грамберг О., Пелед Д. Верификация моделей программ. Model Checking. — М.: МЦНМО, 2002.
- [4] De Alfaro L., Kwiatkowska M., Norman G., Parker D., Segala R. Symbolic model checking of probabilistic processes using MTBDDs and the Kronecker representation // Proc. 6th Int. Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'00) / S. Graf, M. Schwartzbach, eds. — Berlin: Springer, 2000. — (Lect. Notes Comput. Sci.; Vol. 1785). — P. 395—410.
- [5] D'Argenio P., Niebert P. Partial order reduction on concurrent probabilistic programs // Proc. 1st Int. Conf. on Quantitative Evaluation of Systems (QEST'04). — IEEE Comput. Sci. Press, 2004. — P. 240—249.
- [6] Baier C., Clarke E., Hartonas-Garmhausen V., Kwiatkowska M., Ryan M. Symbolic model checking for probabilistic processes // Proc. 24th Int. Colloq. on Automata,

- Languages and Programming (ICALP'97) / P. Degano, R. Gorrieri, A. Marchetti-Spaccamela, eds. — Berlin: Springer, 1997. — (Lect. Notes Comput. Sci.; Vol. 1256). — P. 430—440.
- [7] Baier C., Grösser M., Ciesinski F. Partial order reduction for probabilistic systems // Proc. 1st Int. Conf. on Quantitative Evaluation of Systems (QEST'04). — IEEE Comput. Sci. Press, 2004. — P. 230—239.
 - [8] Baier C., Haverkort B., Hermanns H., Katoen J.-P. Model-checking algorithms for continuous-time Markov chains // IEEE Trans. Software Engineering. — 2003. — Vol. 29, no. 6. — P. 524—541.
 - [9] Bianco A., de Alfaro L. Model checking of probabilistic and nondeterministic systems // Proc. 15th Conf. on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'95) / P. Thiagarajan, ed. — Berlin: Springer, 1995. — (Lect. Notes Comput. Sci.; Vol. 1026). — P. 499—513.
 - [10] Courcoubetis C., Yannakakis M. Verifying temporal properties of finite state probabilistic programs // Proc. 29th Annual Symp. on Foundations of Computer Science (FOCS'88). — IEEE Comput. Soc. Press, 1988. — P. 338—345.
 - [11] Donaldson A., Miller A. Symmetry reduction for probabilistic model checking using generic representatives // Proc. 4th Int. Symp. Automated Technology for Verification and Analysis (ATVA'06) / S. Graf, W. Zhang, eds. — Berlin: Springer, 2006. — (Lect. Notes Comput. Sci.; Vol. 4218). — P. 9—23.
 - [12] Hansson H. Time and Probability in Formal Design of Distributed Systems. — Amsterdam: Elsevier, 1994.
 - [13] Hansson H., Jonsson B. A logic for reasoning about time and reliability // Formal Aspects Computing. — 1994. — Vol. 6, no. 5. — P. 512—535.
 - [14] Hart S., Sharir M., Pnueli A. Termination of probabilistic concurrent programs // ACM Trans. Programming Languages Systems. — 1983. — Vol. 5, no. 3. — P. 356—380.
 - [15] Hermanns H., Katoen J.-P., Meyer-Kayser J., Siegle M. A Markov chain model checker // Proc. 6th Int. Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'00) / S. Graf, M. Schwartzbach, eds. — Berlin: Springer, 2000. — (Lect. Notes Comput. Sci.; Vol. 1785). — P. 347—362.
 - [16] Kwiatkowska M., Norman G., Parker D. Probabilistic model checking in practice: Case studies with PRISM // ACM SIGMETRICS Performance Evaluation Review. — 2005. — Vol. 32, no. 4. — P. 16—21.
 - [17] Kwiatkowska M., Norman G., Parker D. Symmetry reduction for probabilistic model checking // Proc. 18th Int. Conf. on Computer Aided Verification (CAV'06) / T. Ball, R. Jones, eds. — Berlin: Springer, 2006. — (Lect. Notes Comput. Sci.; Vol. 4114). — P. 234—248.
 - [18] Kwiatkowska M., Norman G., Parker D. PRISM 4.0: Verification of probabilistic real-time systems // Proc. 23rd Int. Conf. on Computer Aided Verification (CAV'11) / G. Gopalakrishnan, S. Qadeer, eds. — Berlin: Springer, 2011. — (Lect. Notes Comput. Sci.; Vol. 6806). — P. 585—591.
 - [19] Kwiatkowska M., Parker D. Advances in Probabilistic Model Checking. — <http://qav.comlab.ox.ac.uk/papers/marktoberdorf11.pdf>.
 - [20] <http://www.prismmodelchecker.org/>.
 - [21] <http://qav.comlab.ox.ac.uk/>.

- [22] Vardi M. Automatic verification of probabilistic concurrent finite state programs // Proc. 26th Annual Symp. on Foundations of Computer Science (FOCS'85). — IEEE Comput. Soc. Press, 1985. — P. 327—338.

