ПОСТРОЕНИЕ СОКРАЩЕННОГО ГРАФА ДОСТИЖИМЫХ СОСТОЯНИЙ ПАРАЛЛЕЛЬНОГО АЛГОРИТМА

Черемисинова Л. Д., Черемисинов Д. И.
Объединённый институт проблем информатики Национальной академии наук Беларуси
Минск, Республика Беларусь
E-mail: cldr@newman.bas-net.by, cher@newman.bas-net.by

Рассматривается задача верификации систем управления с параллелизмом поведения на основе графа достижимых состояний. Показано, как можно существенно сократить сложность такого графа для систем рассматриваемого класса, и предложен метод построения сокращенного графа достижимых состояний.

Введение

Рост сложности современных микроэлектронных систем, повышение требований к надежности их проектирования и реализации обусловили тот факт, что неотъемлемой частью процесса проектирования стало тестирование, в частности проверка соответствия поведения системы требованиям, предъявляемым спецификацией на ее проектирование. Одной из широко используемых технологий для решения этой проблемы является тестирование на основе моделей [1], которое предполагает моделирование реальной системы на тестовой последовательности, генерируемой на основе модели (спецификации), описывающей желаемое поведение системы.

В настоящее время наиболее разработанным направлением в области тестирования является верификация на основе моделей, представляемых конечными автоматами. Проблема тестирования систем, которым присущ параллелизм происходящих в них процессов, менее изучена. Обычно рассматриваются системы, состоящие из параллельно работающих компонентов, которые моделируются сетью конечных автоматов. Известны также подходы к тестированию систем с использованием моделей «истинного параллелизма», таких как сети Петри, основанные на использовании графов достижимости.

В настоящей работе рассматриваются системы управления с параллелизмом поведения, спецификация на проектирование которых задается на языке параллельных автоматов [2] (подкласс раскрашенных сетей Петри). Основным инструментом, лежащим в основе методов анализа поведенческих свойств систем рассматриваемого типа, является граф достижимых состояний параллельного автомата, в процессе обхода которого генерируется тестовая последовательность. Основным недостатком такого подхода является то, что размер графа достижимости растет экспоненциально с ростом числа состояний и переходов параллельных автоматов.

В работе показано, как можно существенно сократить сложность такого графа и предложен метод построения сокращенного графа достижимых состояний.

I. Параллельный автомат и граф достижимых состояний

В отличие от классического конечного автомата в параллельном автомате рассматриваются так называемые частичные состояния. В любой момент времени параллельный автомат может одновременно находиться в нескольких таких состояниях. Параллельный автомат можно рассматривать как динамическую дискретную систему, которая допускает параллельные процессы, соответствующие взаимно параллельным частичным состояниям. Множество таких состояний в момент времени определяет полное (глобальное) состояние S_t, которое можно интерпретировать как маркировку сети Петри.

Алгоритм поведения систем управления на языке параллельных автоматов представляется совокупностью переходов вида: $\tau_i = (\gamma_i^1, k_i^1) \rightarrow (\gamma_i^2, k_i^2)$, где γ_i^1 и γ_i^2 – подмножества частичных состояний, в которых автомат находится перед и после срабатывания i-го перехода; k_i^1 и k_i^2 – конъюнкции входных и выходных булевых переменных, трактуемые как условие перехода и выходные сигналы, сопровождающие переход. Переход срабатывает, когда текущее полное состояние S_t включает все состояния из γ_i^1, а переменные автомата принимают значения, обращающие k_i^1 в единицу. После срабатывания перехода переменным из k_i^2 присваиваются значения, обращающие k_i^2 в единицу, а состояние S_t заменяется на $S_{t+1} = (S_t \setminus \gamma_i^1) \cup \gamma_i^2$.

Таким образом, динамика параллельных автоматов описывается в пространстве достижимых полных состояний и значений логических сигналов. Чтобы вычислить следующее полное состояние S_{t+1} автомата, необходимо определить множество T переходов τ_i, которые запускаются в состоянии S_t и состояние K_{t+1} на множестве переменных автомата. Следующие состояния задаются таким образом:

1) $S_{t+1} = (S_t \setminus \gamma^1) \cup \gamma^2$, где $\gamma^1 = \cup_i \gamma_i^1$ и $\gamma^2 = \cup_i \gamma_i^2$ – объединения множеств частичных

состояний всех параллельно выполняемых переходов τ_i из T;

2) состояниеK_{t+1} на множестве переменных получается из K_t таким изменением значений переменных, входящих в конъюнкции k_i^2 всех переходов τ_i, чтобы все $k_i^2 = 1$.

Основной подход к тестированию системы управления состоит в исследовании пространства всех возможных состояний его модели и всех переходов, которые система может совершать между этими состояниями. Граф достижимых состояний задает динамику системы управления при всевозможных изменениях сигналов на его входных полюсах.

Граф достижимости является ориентированным мультиграфом, вершинам которого соответствуют все возможные полные состояния S_t автомата, а дугам – переходы. Дуга графа помечается символом перехода τ_i и связывает вершины S_t и S_p графа, если результат срабатывания τ_i меняет состояние S_t автомата на S_p. Граф достижимости легко получается путем вычисления всех полных состояний S_t, начиная с начальной.

II. Сокращение числа вершин в графе достижимости

Граф достижимости содержит все достижимые состояния параллельного автомата, получаемые путем всевозможных частичных упорядочений параллельных переходов. Его размер растет экспоненциально с увеличением числа частичных состояний и степени параллелизма переходов. Большое пространство состояний негативно влияет на время тестирования. Иногда система слишком велика, чтобы построить график достижимости и получить даже какую-нибудь тестовую последовательность путем обхода его вершин.

Эффективным подходом к сокращению графа достижимости является доопределение частичного порядка на множестве параллельных переходов, в основу которого положена коммутативность асинхронно протекающих процессов. Различные методы доопределения частичного порядка используются [3] при формальной верификации сетей Петри. Эти методы, однако, не учитывают информационное взаимодействие переходов, что недопустимо при решении задачи генерации тестовых наборов.

Доопределение частичного порядка на множестве параллельных переходов основано на том факте, что некоторые параллельно выполняемые переходы не зависят друг от друга, в том смысле, что порядок выполнения одних переходов не влияет на условия срабатывания других. Соответственно, можно рассматривать не все возможные порядки выполнения таких переходов, а упорядочить их произвольным образом, в том числе и совместив их выполнение. Получаемый в результате граф достижимых состояний эквивалентен исходному по степени соответствия спецификации системы, но содержит значительно меньше вершин и дуг.

III. Подход к сокращению графа достижимости

Переход $\tau_i = (\gamma_i^1, k_i^1) \rightarrow (\gamma_i^2, k_i^2)$ срабатывает в состоянии S_t параллельного автомата, если $\gamma_i^1 \subseteq S_t$ и $k_i^1 \wedge K_t \neq 0$.

Пара переходов $\tau_i = (\gamma_i^1, k_i^1) \rightarrow (\gamma_i^2, k_i^2)$ и $\tau_j = (\gamma_j^1, k_j^1) \rightarrow (\gamma_j^2, k_j^2)$, срабатывающих в состоянии S_t параллельного автомата, являются совместимыми (коммутативными) в том смысле, что они могут быть выполнены в любом порядке, приводя к одному и тому же полному состоянию, если при любых значениях входных сигналов автомата выполняются следующие условия:

1) условия срабатывания переходов совместимы, т.е. $k_i^1 \wedge k_j^1 \neq 0$;

2) изменение значений переменных в результате срабатывания одного перехода не приводит к нарушению условия срабатывания другого, т.е. $k_j^1 \wedge k_i^2 \neq 0$ и $k_i^1 \wedge k_j^2 \neq 0$;

3) изменения значений выходных сигналов, вызываемые переходами, совместимы, т.е. $k_i^2 \wedge k_j^2 \neq 0$.

При любом порядке выполнения совместимых переходов полное состояние автомата заменяется на состояние $(S_t \setminus (\gamma_i^1) \cup \gamma_j^1)) \cup (\gamma_i^2) \cup \gamma_j^2)$. Определение совместимости переходов может быть обобщено и на случай более двух переходов: переходы, возможные в некотором состоянии, могут быть выполнены одновременно, если они попарно совместимы.

Предлагаемый метод сокращения графа достижимости основан на просмотре его вершин (начиная с начальной) со степенью исхода, большей 1. Среди переходов из такой вершины выделяются подмножества попарно совместимых, соответствующие переходам дуги, а также достижимые из них вершины графа, объединяются.

IV. Заключение

Предлагаемый подход к сокращению графа достижимости лег в основу метода построения сокращенного графа достижимости непосредственно по описанию алгоритма на языке параллельных автоматов.

V. Список литературы

1. Tretmans, J. Model based testing with labelled transition systems / J. Tretmans // Formal Methods and Testing: Lecture Notes in Computer Science. – 2008. – Vol. 4949. – P. 1–38.
2. Закревский, А.Д. Параллельные алгоритмы логического управления / А.Д. Закревский // Минск: Ин-т техн.кибернетики НАН Беларуси, 1999. – 202 с.
3. Lluch-Lafuente, A. Partial Order Reduction in Directed Model Checking / A. Lluch-Lafuente // Proc. of the 9th Intern. SPIN Workshop on Model Checking of Software, Heidelberg, April 11–13, 2002. – P. 112–127.