Секция «Математика и механика»

Новый метод верификации дискретных процессов

Миронов Андрей Михайлович

Кандидат наук

Московский государственный университет имени М.В. Ломоносова, Механико-математический факультет, Москва, Россия

E-mail: amironov66@gmail.com

В докладе излагается метод верификации процессов, основанный на доказательстве наблюдаемой эквивалентности верификцируемого процесса и его спецификации. Сформулировано достаточное условие наблюдаемой эквивалентности процессов. Проблема формального представления и верификации дискретных процессов является одной из наиболее важных проблем в теоретической информатике. Существует несколько подходов к этой проблеме, наиболее важными из них являются: исчисление взаимодействующих систем Р.Милнера (CCS) и π-исчисление [1], [2], теория взаимодействующих процессов Ч.Хоара (CSP) и её обобщения [3], темпоральная логика и model checking [4], сети Петри [5], процессные алгебры [6], теория взаимодействующих машин с конечным числом состояний [7]. Дискретные процессы представляются в нашей модели в виде графов, рёбра которых помечены операторами. Эти операторы состоят из внутренних действий и действий ввода-вывода. Доказательства корректности процессов представляются множествами формул, связанных с парами состояний анализируемых процессов. Наш метод доказательства наблюдаемой эквивалентности двух процессов основан на нижеследующей теореме. Для формулировки и доказательства этой теоремы мы введём вспомогательные понятия и обозначения.

1. Пусть задан процесс P и пара состояний $s, s' \in S_P$. **Составной переход (СП)** из s в s' – это последовательность T переходов процесса P вида

$$s = s_0 \xrightarrow{O_1} s_1, \quad s_1 \xrightarrow{O_2} s_2, \quad \ldots \quad s_{n-1} \xrightarrow{O_n} s_n = s' \tag{1}$$

такая, что среди $O_1, \ldots, O_n$ – не более одного оператора ввода или вывода, и определены все конкатенации в выражении

$$(\ldots(O_1 \cdot O_2) \cdot \ldots) \cdot O_n \tag{2}$$

Последовательность (1) м.б. пустой, в этом случае $s = s'$. Если СП T непуст и имеет вид (1), то запись O_T обозначает значение выражения (2), а если T пуст, то $O_T \stackrel{\text{def}}{=} [\,]$. Мы будем использовать для СП те же понятия и обозначения, что и для обычных переходов ($start(T)$, $end(T)$, N_T и т.п.). Мы будем называть СП T вводом выводом или внутренним, если O_T – оператор ввода, вывода или внутренний соответственно. Как и для обычных переходов, для СП можно ввести понятие реализации, которое будет обладать следующими свойствами:

   (a) если СП T – внутренний или вывод, то для каждого $\xi \in X_P^\bullet$, такого, что $\langle T\rangle^\xi = 1$, существуют единственные $\xi' \in X_P^\bullet$ и $a \in \mathcal{A}$, такие, что (ξ, a, ξ') – реализация T, мы будем обозначать такое ξ' записью $\xi \cdot T$, и

   (b) если СП T – ввод, то для каждого $\xi \in X_P^\bullet$, такого, что $\langle T\rangle^\xi = 1$, и каждого $d \in \mathcal{D}$ существует единственное $\xi' \in X_P^\bullet$, такое, что $(\xi, N_T?d, \xi')$ – реализация T, мы будем обозначать такое ξ' записью $\xi \cdot T^d$.

2. Если b и b' – формулы, то запись $b \leq b'$ является сокращённой записью утверждения о том, что формула $b \to b'$ истинна.

3. Если O_1, O_2 – операторы и $b \in \mathcal{B}$, то запись $(O_1, O_2) \cdot b$ обозначает формулу, определяемую излагаемым ниже рекурсивным определением. Пусть $[O_1] = o_1, \ldots, o_n$ и $[O_2] = o'_1, \ldots, o'_m$, тогда формула

$$(O_1, O_2) \cdot b \tag{3}$$

   определяется следующим образом

   (a) $\langle O_1\rangle \wedge \langle O_2\rangle \wedge b$, если $n = m = 0$

   (b) $(O_1 \setminus o_n, O_2) \cdot o_n(b)$, если o_n – присваивание

   (c) $(O_1, O_2 \setminus o'_m) \cdot o'_m(b)$, если o'_m – присваивание

   (d) $((O_1 \setminus o_n), (O_2 \setminus o'_m)) \cdot b(z/x, z/y)$, если $o_n = \alpha?x,\ o'_m = \alpha?y$, и $b(z/x, z/y)$ – формула, получаемая из b заменой всех вхождений x и y на новую переменную z (не входящую в O_1, O_2 и b)

   (e) $((O_1 \setminus o_n), (O_2 \setminus o'_m)) \cdot ((e_1 = e_2) \wedge b)$, если $o_n = \alpha!e_1$ и $o'_m = \alpha!e_2$

   (f) $\perp$, в остальных случаях.

Теорема. Пусть $P_i = (S_{P_i}, s^0_{P_i}, T_{P_i}, \langle P_i\rangle)$ $(i = 1, 2)$ – процессы, причём $S_{P_1} \cap S_{P_2} = \emptyset$ и $X_{P_1} \cap X_{P_2} = \emptyset$. P_1 и P_2 наблюдаемо эквивалентны, если существует совокупность $\{b_{s_1 s_2} \mid s_i \in S_{P_i}\ (i = 1, 2)\}$ формул с переменными из $(X_{P_1} \cup X_{P_2}) \setminus \{at_{P_1}, at_{P_2}\}$, обладающих следующими свойствами.

1. $\langle P_1\rangle \wedge \langle P_2\rangle \leq b_{s^0_{P_1} s^0_{P_2}}$

2. Для каждого перехода $s_1 \xrightarrow{O} s'_1$ процесса P_1 и каждого состояния $s_2 \in S_{P_2}$ существует совокупность СП процесса P_2, имеющая вид $\{s_2 \xrightarrow{T_i} s^i_2 \mid i \in \Im\}$ и такая, что

$$b_{s_1 s_2} \wedge\ \langle O\rangle \leq \bigvee_{i \in \Im} (O, O_{T_i}) \cdot b_{s'_1 s^i_2}$$

3. Свойство, симметричное предыдущему свойству: для каждого перехода $s_2 \xrightarrow{O} s'_2$ процесса P_2 и каждого состояния $s_1 \in S_{P_1}$ существует совокупность СП процесса P_1, имеющая вид $\{s_1 \xrightarrow{T_i} s^i_1 \mid i \in \Im\}$ и такая, что

$$b_{s_1 s_2} \wedge\ \langle O\rangle \leq \bigvee_{i \in \Im} (O_{T_i}, O) \cdot b_{s^i_1 s'_2}$$

Список литературы

[1] R. Milner: A Calculus of Communicating Systems. Number 92 in Lecture Notes in Computer Science. Springer Verlag (1980)

[2] R. Milner: Communicating and Mobile Systems: the π-calculus. Cambridge University Press (1999)

[3] C.A.R. Hoare: Communicating Sequential Processes. Prentice Hall (1985)

[4] Clarke, E.M., Grumberg, O., and Peled, D.: Model Checking, MIT Press (1999)

[5] C.A. Petri: Introduction to general net theory. In W. Brauer, editor, Proc. Advanced Course on General Net Theory, Processes and Systems, number 84 in LNCS, Springer Verlag (1980)

[6] J.A. Bergstra, A. Ponse, and S.A. Smolka, editors: Handbook of Process Algebra. North-Holland, Amsterdam (2001)

[7] D. Brand, P. Zafiropulo: On Communicating Finite-State Machines. Journal of the ACM, Volume 30 Issue 2, April 1983, pp. 323-342. ACM New York, NY, USA (1983)