Вычислимые Σ - спецификации иерархизированных миров Крипке

В.Н. Глушкова

Донской государственный технический университет, lar@rnd.runnet.ru

Для проверки правильности поведения сложных систем (технических, реагирующих параллельных систем) широко используются различные временные логики: CTL^*,CTL, LTL и др. Практическая значимость этих логик определяется их выразительной силой и вычислительной сложностью основанных на них алгоритмов верификации. В частности, самыми сложными являются верификаторы, основанные на семантике непрерывного времени. Предлагаемый подход базируется на концепции семантического программирования [1], в рамках которого выделен полиномиально реализуемый класс Δ_0 - формул специального вида.

Первый шаг проверки корректности системы состоит в построении ее формальной модели с использованием теории Th квазитождеств с отрицаниями из $\Delta_0 T$-формул вида:

$$(\forall x_1 \dot{\in} t_1) \dots (\forall x_m \dot{\in} t_m)\ (y_1 \prec z_1) \dots (y_p \prec z_p)(\ \varphi(\bar{x}, \bar{t}) \rightarrow \psi(\bar{x}, \bar{t})), \qquad (1)$$

где $\bar{x}$, $\bar{t}$ - последовательности соответствующих переменных; y_j,$z_j \in (\bar{x}, \bar{t})$, $1 \leq j \leq p$. Префикс формул имеет иерархическую структуру дерева с корнем t_1,"согласованную"с $KC-$грамматикой $G = (I, Pr)$, где I,$Pr-$ множества символов и правил [2]. Отношение $\dot{\in}$ - обозначает непосредственное иерархическое подчинение объектов или его транзитивное замыкание, $\prec$ - отношение "левее"для узлов дерева. Формула φ (ψ) - это конъюнкция атомных формул или их отрицаний вида r, $\tau_1 = \tau_2$,$(f = \tau)$. Здесь r, f- предикатный и функциональный символы, τ_1,τ_2- термы многосортной сигнатуры $\sigma =< I \cup \{list\}, C, F, P >$, где $list$ - сорт иерархических списков, структура которых задается грамматикой G; C,F,R - множества констант, функциональных и предикатных символов соответственно. Атомные формулы (их отрицания)из правой части (1)могут содержать одну двуместную модальную связку $\Diamond^2$ некоторого модального типа подобия [3]. Связка $\Box$ - может входить только в левую часть(1).

Для теорий, обладающих свойством нётеровости и конфлюентности, можно построить индуктивно вычислимые модели (миры) из констант сигнатуры σ на основе правила вывода "modus ponens"(MP) и правила обобщения: если φ, то $\Box\varphi$.

Множество миров W составляет фрейм Крипке $\Im =< W, R >$, $R \subseteq W \times W$-частичный порядок на мирах. Интерпретатор начинает работу, исходя из Th_0 - "подтеории"фактов, а именно – формул вида $r(\bar{c})$ $(\neg r(\bar{c}))$, $f(\bar{c}) = c_n$, $\bar{c} \in C^*$, $c_n \in C$. Начальный мир w_1 определяется множеством всех логических следствий теории $Th_1 \cup Th_0$, где теория Th_1 образована аксиомами, не содержащими модальные связки в правой части. Все таблицы значений функций $f(\bar{c}) = c_n$ и предикатов вида $p(\bar{c}), (\neg p(\bar{c}))$, полученные в результате логического вывода, собственно и являются миром w_1. При интерпретации аксиом теории арифметические операции считаются встроенными, а предикатные символы делятся на два класса. Отрицание для предикатов первого класса интерпретируется по принципу "замкнутого мира". Отрицание для других предикатов интерпретируется по принципу "непрерывности", который формулируется следующим образом. Пусть значения одноместного предиката линейно упорядочены отношением $<$. Если установлено $p(c_1)$ и $\neg p(c_2)$ для $c_1 < c_2$ и $\neg\exists c_3 \in [c_1, c_2)\neg p(c_3)$, то $\forall x \in [c_1, c_2)p(x)$. Формально мир w_1 является индуктивно вычислимой моделью теории $Th_1 \cup Th_0$, интерпретируемой на объектах иерархической надстройки $\bigcup\limits_{A \in N} D_G^A(C)$, где $N-$ множество нетерминальных символов грамматики G, $C = \{C_X\}_{X \in I}-$ семейство констант соответствующих сортов.

Остальные миры конструируются при интерпретации аксиом с модальностями в правой части. Если мир w_i построен, то при использовании в посылке правила вывода MP аксиомы с правой частью вида $\diamondsuit^2(p_1(\bar{c}), p_2(\bar{c}))$ интерпретатор порождает два несравнимых мира w_{i1}, w_{i2}, достижимых из w_i, в одном из которых устанавливается истинность $p_1(\bar{c})$, а в другом - $p_2(\bar{c})$ (в частности, это может быть $\neg p_1(\bar{c})$). Т.е. для формул теории Th вида $\varphi(\bar{c}) \to \diamondsuit^2(p_1(\bar{c}), p_2(\bar{c}))$, в случае $(\Im, w_i) \vDash \varphi(\bar{c})$ генерируются два мира w_{i1}, w_{i2}, таких что $w_i R w_{i1}$, $w_i R w_{i2}$, для которых устанавливается: $(\Im, w_{i1}) \vDash p_1(\bar{c})$, $(\Im, w_{i2}) \vDash p_2(\bar{c})$.

Теория Th интерпретируется на иерархических структурах – деревьях, порождаемых КС- грамматикой G. Исходное дерево "достраивается"одновременно с логическим выводом и наследуется мирами в соответствии с отношением R следующим образом. Некоторым аксиомам (1) приписывается последовательность правил из Pr и те константы из $\bar{c}$, для которых выполнено $\varphi(\bar{c})$, используются как для получения следствий $\psi(\bar{c})$, так и в качестве терминальных символов соответствующих правил грамматики. Ограничивая зависимость переменных, входящих в префикс $\Delta_0 T-$ формул, можно выделить класс полиномиально реализуемых формул отно-

сительно количества узлов дерева вывода.

Второй шаг верификации проектируемой системы состоит в спецификации и проверке свойств, которыми она должна обладать. Эта спецификация состоит из произвольных $\Delta_0 T-$ формул, которые проверяются на всех моделях фрейма за полиномиальное время, причем степень полинома зависит от вида грамматики и префикса формулы [4].

Выделенный класс формул можно использовать для спецификации поведения динамических систем, описывая их функционирование относительно непрерывного реального времени, явно заданного. Для примера опишем поведение лифта в упрощенном случае. Грамматика G_l описывает реализуемую иерархию действий лифта. Пусть лифт имеет только один переключатель Sw, значение которого явно зависит от времени t и задается в начальный момент времени t_0 кортежем номеров вызываемых этажей. С изменением t значения из $Sw(t)$ только удаляются. В грамматике в качестве нетерминальных символов используются имена предикатов и функций сигнатуры теории Th_l функционирования лифта. Нетерминальный символ St порождает пары $< m, time >$, определяющие статическое состояние лифта, где целое число m (номер этажа) порождается символом Loc, N- количество этажей. Значение $time$ порождается символом T, которое задается дискретно "мгновенным" значением времени t или "непрерывно"- сегментом $< t_1, t_2 >$. Нетерминальный Act определяет действия лифта: "движение вверх или вниз"(MU, $MD \subseteq St \times St$); процессы "открытия или закрытия двери"(Dop,$Dcl \subseteq St$) и "остановки лифта"($Sp \subseteq St$); символы $BrCd$, $BrOd \subseteq St$ обозначают поломку лифта "двери не закрываются"и "двери не открываются". Правила грамматики G_l имеют вид:

$$
\begin{aligned}
&1. LL \rightarrow \{Act\}^* \\
&2. Act \rightarrow MU(St, St) \mid MD(St, St) \mid Sp(St) \mid Dop(St) \mid Dcl(St) \mid \\
&BrCd(St) \mid BrOd(St) \\
&3. St \rightarrow Loc\, T \\
&4. Loc \rightarrow 1 \mid 2 \mid \ldots \mid N \\
&5. T \rightarrow t \mid (t, t) \mid [t, t) \mid (t, t] \mid [t, t]
\end{aligned}
$$

В зависимости от вида временного сегмента, порождаемого символом T, соответствующий его конец включается или нет в сегмент времени. В теории Th_l также используются предикат "цель": $Goal \subseteq St \times Loc$; функции: $L(st) = st[1]$, определяющая положение лифта в состоянии st ; $T(st) = st[2]$ - временная составляющая

st; $h(< x_1, ..., x_n >) = x_1$, $e(< x_1, ..., x_n >) = x_n$, независимо от того, какого вида сегмент рассматривается.

Основу теории составляют ниже приведенные формулы, в которых все свободные переменные связаны ограниченными кванторами всеобщности. А именно, переменные st сорта "состояние"связаны квантором $\forall st \overset{\star}{\in} Act$, переменные сорта времени t ограничены рассматриваемым промежутком времени; переменные n, m изменяются от 1 до N (количество этажей). В спецификации используются константы: δ- время, необходимое для закрытия и открытия двери лифта; $l-$ расстояние между этажами, $v-$ скорость лифта. Конъюнкция представляется ",". Слева от формул в квадратных скобках приводится последовательность правил грамматики G_l для построения дерева "действий"лифта, где $sp = [3, 4, 5]$. Для начального состояния лифта $st_0 =< n_0, [t_0, t_0 + \delta) >$ выполняеются факты: $Dcl(st_0)$, $\neg Br(st_0)$,; во всех формулах используются обозначения: $n = L(st)$, $t = T(st)$.

1.$Dcl(st), \neg Br(st) \rightarrow Goal(< n, e(t) >, m)$, где m=h(Sw(t))
2.$Goal(st, m), m = L(st) \rightarrow \Diamond(Dop(< m, [t, t + \delta) >), \neg Dop(< m, [t, t + \delta) >)$,
3.$Goal(st, m), m = L(st), \Box Dop(st) \rightarrow Sw(t + \delta) = Sw(t - \delta)/1$
4.$\Box\neg Dop(st) \rightarrow BrOp(st); [2.7, sp]$
5.$\Box Dop(st) \rightarrow \Diamond(Dcl(< n, [t, t + \delta) >), \neg Dcl(< n, [t, t + \delta) >), [2.4, sp]$
6.$\Box\neg Dcl(st) \rightarrow BrCd(st), [2.6, sp]$
7.$Goal(st, m), n < m \rightarrow MU(st, < m, [t + t_1) >)$,
$\Diamond(Dop(m, [t + t_1, t + t_1 + \delta)), \neg Dop(m, [t + t_1, t + t_1 + \delta))$;
где $t_1 = (m - n)l/v); [2.1, sp, sp]$

Иерархизация пространства поведения лифта позволяет в результате интерпретации аксиом теории Th_l сгенерировать дерево "действий", в котором явно отражены все промежутки времени, являющиеся значениями переменных соответствующих предикатов. Если для начального состояния st_0=$< 5, [t_0, t_0 + \delta) >$ выполняются предикаты: $Dcl(st_0)$, $\neg Br(st_0)$, $Sw(t_0) =< 7, 10, 10, 1 >$ и лифт "не ломается"в процессе функционирования, то окончательное дерево будет иметь крону, отражающую действия лифта на всем промежутке времени $[t_0+\delta, t_0+8\delta+14\nu)$, где $\nu = l/v$: $MU\ (< 5, t_0 + \delta >, < 7, t_0 + \delta + 2\nu >)\ Dop(< 7, [t_0 + \delta + 2\nu, t_0 + 2\delta + 2\nu) >)\ Dcl\ (< 7, [t_0 + 2\delta + 2\nu, t_0 + 3\delta + 2\nu) >)\ MU(< 7, t_0 + 3\delta + 2\nu >, < 10, t_0 + 3\delta + 5\nu >) Dop(< 10, [t_0 + 3\delta + 5\nu, t_0 + 4\delta + 5\nu) >)\ Dcl\ (< 10, [t_0 + 4\delta + 5\nu, t_0 + 5\delta + 5\nu) >) Dop\ (< 10, [t_0+5\delta+5\nu), t_0+6\delta+5\nu) >)\ Dcl\ (< 10, [t_0+6\delta+5\nu, t_0+7\delta+5\nu) >)$

$MD(<10, t_0+7\delta+5\nu>, <1, t_0+7\delta+14\nu)>)$ $Dop(<1, [t_0+7\delta+14\nu, t_0+8\delta+14\nu)>)$ $Dcl(<1, [t_0+8\delta+14\nu, t_0+9\delta+14\nu)>)$; $Sw(t_0+8\delta+14\nu) = <>$.

Для фрейма теории Th_l можно формулировать различные ограничения, в частности: $BrCd(st) \to Sp(st)$, $BrOd(st) \to Sp(st)$, означающими, что аварийное состояние лифта ведет к его остановке. В этом случае в Th_l необходимо специфицировать предикат "остановка"лифта $Sp \subseteq St$,например, формулами $MU(st_1, st_2) \to \neg Sp(st_1), Sp(st_2)$; $Dop(st) \to Sp(st)$; $Dcl(st) \to Sp(<n, h(t)>), \neg Sp(<n, e(t)>)$. Формулы второй части спецификации поведения системы можно проверять различными способами, используя специфичные методы сортировки и доступа к соответствующим таблицам, или синтаксически (методом семантических таблиц).

"Дискретную"функцию $Sw(t)-$ можно непрерывно продолжить по времени. Если после построения мира w_i в нем выполняется $Sw(t_0) =< n_1, n_2, ..., n_k >$ и $Sw(t_1) = < n_2, ..., n_k >$, $t_0, t_1 \in C$, $\neg\exists t \in [t_0, t_1)(Sw(t) \neq Sw(t_0))$, то устанавливается, что $\forall t \in [t_0, t_1)(Sw(t) = Sw(t_0))$. Это упрощает задачу спецификации ограничений тем, что при моделировании поведения сложной системы позволяет абстрагироваться от знания конкретных значений, в которых определены функции, но осложняет выделение конструктивных условий нетеровости. Эти условия удается выделить в тех задачах, где естественно считать исходное дерево, на котором интерпретируютя логические формулы, неизменно заданным. Например, при спецификации контекстных условий языка программирования дерево определяется анализируемой программой, а условия нетеровости накладывают ограничения на характер зависимости переменных, входящих в левую и правую часть квазитождества [4]. При логическом моделировании реагирующих систем, которые функционируют неограниченно долго, (даже если удается иерархизировать их пространство действий) не понятно из каких соображений выделить для интерпретации конкретное дерево с заданными значениями терминальных символов. Если же его конструировать в процессе интерпретации логических формул, исходя из некоторого "начального"состояния, то чем руководствоваться при ограничении его роста? Также остается открытым вопрос о классе моделей, соответствующем выделенному классу формул.

Литература

1.Goncharov S.S. and Sviridenko D.I. Theoretical aspects of Σ- programming. Mathematical Methods of Specification and Synthesis of Software Systems' 85. Proceed. of the

Internat. Spring School. Springer-Verlag, April, 1985. pp. 169-179.

2. Глушкова В.Н. Оценка сложности реализации логических спецификаций. Кибернетика и системный анализ. 1996, № 4, с. 51-58.

3. P. Blackburn,M.de Rijke,Y.Venema. Modal Logic.Cambridge Tracts in Theoretical Computer Science, 53, 2004.

4. V. Glushkova. The execution complexity of logical formulas with restricted quantifiers based on CF-grammars. http://www.univ-paris12.fr/lacl/LCCS2001/accepted.html