30 ноября 2012

Инсерционное моделирование 1

Лекция 13

Проблема выполнимости

Выполнимость пропозициональных функций

SAT проблема
DPLL: Davis-Putnam-Logemann-Loveland
алгоритм

$$f(x_1, x_2, \ldots) = x_1 \wedge f(1, x_2, \ldots) \vee \overline{x_1} \wedge f(0, x_2, \ldots)$$

Продолжение развертки – разложение Шеннона.
BDD (binary decision diagram)
Стратегии выбора переменной
для разложения – современные алгоритмы решения
SAT проблемы

SAT проблема для кнф

Две простейшие эвристики:

дизъюнкт *x*

переменная *x* входит только позитивно или только с отрицанием

Выбор переменной

Пример критерия (Padderborn 93, SAT competition):

Рассматриваются cnf. Для каждой переменной строится $(H_1(x), H_2(x), \ldots)$ и выбирается лексикографический максимум.

$H_i(x)=\max\{h_i(x), h_i(\neg x)\}+\mathbf{2}\min\{h_i(x),h_i(\neg x)\}$

$h_i(x)$: число вхождений литерала x в дизъюнкты длины i

Model checking

BDD, темпоральная логика (LTL,...)

Модель определяется базовыми протоколами с булевскими атрибутами

Символьная модель: состояния системы – булевские формулы

SMT

Бескванторные формулы

Формулы с кванторами

Логические теории, используемые в VRS

Линейные неравенства для вещественных атрибутов
Линейные неравенства для целочисленных атрибутов
Теория свободных термов (символьные данные)
Перечислимые типы (в том числе Boolean)
Смешанная теория

    int<real<symb
    Bool, enum{a,b,…}<symb

Теория с функциональными атрибутами

    (неинтерпретированные функциональные символы)

Списки (очереди)
Алгебра поведений

Теория вещественных линейных неравенств

Алгоритм Фурье-Моцкина

Дано: замкнутая формула с линейными неравенствами

Определить: будет ли формула истинной

Метод: элиминация кванторов

Элиминация кванторов позволяет **решать системы неравенств.**

$$\exists x P(x, y_1, y_2, \ldots)$$

$$\exists x (P \vee Q) \Leftrightarrow \exists x P \vee \exists x Q$$

$$\forall x P(x) \Leftrightarrow \neg \exists x \neg P(x)$$

$$s \le t \Leftrightarrow s < t \vee s = t$$

$$s > t \Leftrightarrow t < s$$

$$\exists x ((x = f(y)) \wedge P(x, y)) \Leftrightarrow P(f(y), y)$$

$$\exists x ((s_1, s_2, \ldots) < x \wedge x < (t_1, t_2, \ldots)) \Leftrightarrow (s_1, s_2, \ldots) < (t_1, t_2, \ldots)$$

$$(s_1, s_2, \ldots) < (t_1, t_2, \ldots) \Leftrightarrow$$
$$s_1 < t_1 \wedge s_2 < t_2 \wedge \ldots \wedge$$
$$s_2 < t_1 \wedge s_2 < t_2 \wedge \ldots \wedge$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Сложность – суперэкспонента

Теория линейных целочисленных неравенств разрешима:

Алгоритм Прессбургера

Теория нелинейных вещественных неравенств разрешима:

Алгоритм Тарского

Теория нелинейных целочисленных неравенств **неразрешима**:

Результат Матиасевича (10-я проблема Гильберта)

Теория свободных термов разрешима:

Алгоритм унификации (метод резолюций Робинсона)

Выполнимость бескванторных формул в теории свободных термов

Сводится к решению системы равенств и отрицаний равенств.

Равенства:

$$\omega(t_1, t_2, \ldots) = \omega'(s_1, s_2, \ldots) \Leftrightarrow (\omega = \omega') \wedge (t_1 = s_1) \wedge (t_2 = s_2) \wedge \ldots$$

Решение (если существует):

$$x_1 = f_1(y_1, y_2, \ldots) \wedge x_2 = f_2(y_1, y_2, \ldots) \wedge \ldots$$

$$R \subseteq Y^2, Y = \{y_1, y_2, \ldots\}$$

R есть эквивалентность на множестве неизвестных, $f_i(y_1, y_2, \ldots) \notin Y$

Система равенств: решаем равенство, подставляем x, затем, выбрав по одному представителю, y. Метод исключения (Гаусса).

Отрицания равенств:

Конъюнкция отрицаний выполнима, если не содержит отрицания тождественно равных термов (предположение о бесконечности символьных константных термов).

$$\omega(t_1, t_2, \ldots) \neq \omega'(s_1, s_2, \ldots) \Leftrightarrow (\omega \neq \omega') \vee (t_1 \neq s_1) \vee (t_2 \neq s_2) \vee \ldots$$

Решить уравнения

1. $((a,b,y),(b,(v,a),(x,z),a),(a,b)) = ((a,u),(b,((a,y,z),a),(x,y,z),z),x)$

2. $((a,y,u),(v,z,(x,z),(a,u))) = (z,(u,(a,(a,x,x),v),((a,v),z),x))$

Элиминация кванторов в теории свободных термов

$\exists x(y=(a,x))$ не элиминируется, но, если добавить операции …

$\mathrm{type}(y)=((),()) \wedge \mathrm{arg}(y,1)=a$

Разрешимость полной теории А.И.Мальцев, 1961
Сложность не является элементарной.

В теории свободных термов,
расширенной операциями $\mathrm{arg}(x,i)$,
предикатами $\mathrm{type}(x)=f((),\ldots,())$ и константой $()$
возможна элиминация кванторов.

$$(\mathrm{type}(g(t_1,t_2,\ldots)) = f((),\ldots,())) \Leftrightarrow g = f$$

$$(\mathrm{arg}(g(t_1,t_2,\ldots,t_n),i) = t_i, 1 \le i \le n$$

$$(\mathrm{arg}(g(t_1,t_2,\ldots,t_n),i) = (), i > n$$

$$n \ge 0, i \ge 1$$

$$\mathrm{arg}(x,(i,j,\ldots)) = \mathrm{arg}(\ldots\mathrm{arg}(\mathrm{arg}(x,i),j),\ldots)$$

Перечислимые типы

$$\exists x P(x) \Leftrightarrow P(a_1) \vee P(a_2) \vee \ldots$$

$$\forall x P(x) \Leftrightarrow P(a_1) \wedge P(a_2) \wedge \ldots$$

$$\forall x (x = a_1 \vee x = a_2 \vee \ldots \vee x = a_n) = 1$$

Смешанная теория, выполнимость бескванторных формул

Числовые + символьные + перечислимые

Нужно доказать выполнимость конъюнкции литералов вида:

равенства

отрицание равенств

числовые неравенства

Сначала решаем равенства

$$x_1 = f_1(y_1, y_2, \ldots) \wedge x_2 = f_2(y_1, y_2, \ldots) \wedge \ldots$$

Для целочисленных

$$ax = f(y_1, y_2, \ldots)$$

Затем подставляем в отрицания и неравенства (для целочисленных умножаем на константу).

Символьные отрицания элиминируем

Остаются числовые.

Проверяем выполнимость с помощью Фурье и Пресбургера.

Выполнимость формул VRS

Главное отличие от рассмотренных случаев – функциональные атрибуты, неинтерпретированные функциональные символы

Простые атрибуты: навешивание кванторов существования

Функциональные атрибуты:

Метод Аккермана-Шостака

Элиминация суперпозиций:

$$P(f(g(x),...)) \Leftrightarrow \exists y(y = g(x) \wedge P(f(y,...)))$$

замена $f(x_i)$ на y_i

с добавлением формул $(x_i = x_j) \to (y_i = y_j)$

и ограничений для индексов массивов

$$P(f(x_1), f(x_2),...) \Leftrightarrow$$

$$\exists(y_1, y_2,...)((\bigwedge((x_i = x_j) \to (y_i = y_j)) \wedge Q(x) \wedge P(y_1, y_2,...))$$

x_i вектора, $Q(x)$ – ограничения на индексы

Списки

Список (двусторонняя очередь)

L=(t1,t2,…)

Get_from_head(L)
Get_from_tail(L)

Редукция

add_to_head(L,t)
add_to_tail(L,t)
remove_from_head(L)
remove_from_tail(L)

Неполные списки

$$L = (a_1,\ldots,a_n, \mathrm{Nil}), n > 0$$ *Непустой полный список*

$$L = (a_1,\ldots,a_n, \mathrm{Nil}; b_1,\ldots,b_m, \mathrm{Nil}), m, n > 0$$ *Список с непустыми головой и хвостом*

$$L = (\mathrm{Nil}; b_1,\ldots,b_m, \mathrm{Nil})$$ *Список с непустым хвостом*

$$L = (a_1,\ldots,a_n, \mathrm{Nil}; \mathrm{Nil})$$ *Список с непустой головой ☺*

$$L = (\mathrm{Nil}; \mathrm{Nil})$$ *Произвольный список*

$$L = \mathrm{Nil}$$ *Пустой список*

L **– атрибутное выражение типа список**

L=u **– высказывание о возможных значениях этого выражения**

Редукция требует введения кванторов по спискам:

$$L = (a_1,\ldots,a_n, Nil; b_1,\ldots,b_m, Nil) \Leftrightarrow \exists S(L = (a_1,\ldots,a_n, Nil) * S * (b_1,\ldots,b_m, Nil))$$