Символьная верификация программ

Лекция N 4 курса “Современные задачи теоретической информатики”

Юрий Лифшиц
yura@logic.pdmi.ras.ru

ИТМО

Осень’2005

Часто, в минуты наших торжественных сомнений, мы хорошо про себя знаем, где находится неподвижная точка, несокрушимая вершина долга; но нам кажется, что между долгом настоящей минуты и этой слишком одинокой и слишком сверкающей вершиной расстояние таково, что было бы неблагоразумно пройти его сразу.

Морис Метерлинк, “Мудрость и судьба”

Общие идеи лекции

- Мы строим новый алгоритм верификации CTL
- Для неявного описания моделей Крипке будем использовать **двоичные разрешающие диаграммы**
- Для каждой подформулы в неявном виде хранить множество выполняющих состояний
- Переход от подформул к формуле будем делать с помощью **алгоритма нахождения неподвижной точки**

План лекции

План лекции

1. **Двоичные разрешающие диаграммы**
   - Определения и свойства
   - Операции над диаграммами
   - Диаграммы и модель Крипке
2. Вычисление неподвижной точки
3. Символьный алгоритм верификации CTL

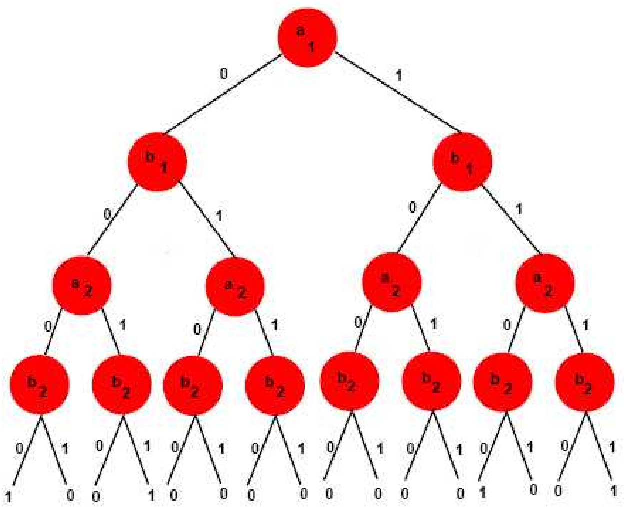
Двоичное разрешающее дерево

Рассматриваем булевы функции вида:

$$F : \{0,1\}^k \to \{0,1\}$$

Двоичное разрешающее дерево — способ задания булевых функций.

- Ориентированное корневое дерево
- Исходящие степени внутренних вершин (нетерминалов) равны двум
- Каждая вершина помечена какой-то переменной
- Одно исходящее ребро помечено 1, другое 0
- На листьях (терминалах) написаны значения функции

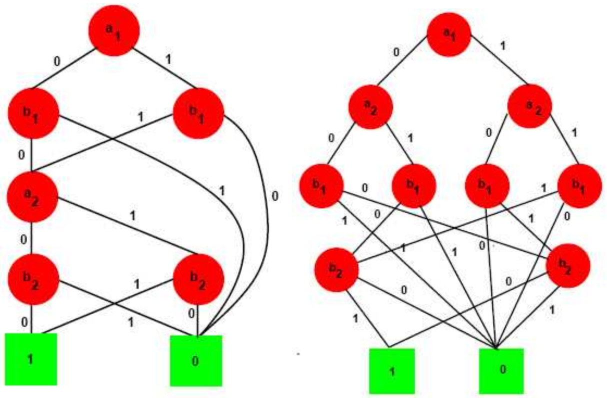


Какая функция представлена этим деревом?

Двоичная разрешающая диаграмма

Двоичная разрешающая диаграмма:
Вместо дерева — ациклический граф

Упорядоченная двоичная разрешающая диаграмма (OBDD):
Переменные упорядочены
На каждом пути переменные встречаются именно в этом порядке



Порядок переменных

Некоторые факты

- Для каждого порядка есть единственная минимальная OBDD
- Для функции $(a_1 \oplus b_1) \& \ldots \& (a_n \oplus b_n)$ при разных порядках размер меняется от $3n+2$ до $3 \cdot 2^n - 1$
- Есть функции, при любом порядке дающие OBDD экспоненциального размера

Оптимальный порядок

- Найти оптимальный порядок — **NP**-трудная задача
- Есть эвристические алгоритмы подбирающие порядок

Операции над OBDD

Пусть есть OBDD-представление функций f и f'

Хотим построить OBDD для:

- $\neg f$
- $f \vee f'$
- $f \wedge f'$
- Любой бинарной булевой функции от f и f'

Кстати, сколько всего бинарных булевых функций?

Алгоритм Бриана

Пусть даны OBDD-представление функций f и f', а также бинарная операция $*$.

Для любой вершины a в OBDD для f, можем рассмотреть OBDD "висящую" на этой вершине, соответствующую функцию обозначим f_a

Идея алгоритма:

Построить для всех пар a — вершина f-OBDD, a' — вершина $f' - OBDD$ диаграмму для $f_a * f'_a$

Формулы разложения Шеннона

$$f * f' = (x \wedge (f|_{x\to 1} * f')) \vee (\neg x \wedge (f|_{x\to 0} * f'))$$

$$f * f' = (x \wedge (f|_{x\to 1} * f'|_{x\to 1})) \vee (\neg x \wedge (f|_{x\to 0} * f'|_{x\to 0}))$$

Алгоритм Бриана II

1. **База:** вычислить OBDD для пар терминал из f-OBDD, терминал из f'-OBDD
2. **Переход, случай 1:** a и a', помечены одинаковой переменной. Пусть их дети - a_0, a_1, a'_0, a'_1. Рисуем вершину, слева OBDD для $f_{a_0} * f'_{a'_0}$, справа — OBDD для $f_{a_1} * f'_{a'_1}$
3. **Случай 2:**Если разные переменные, то слева — $f_{a_0} * f'_{a'}$, справа — $f_{a_1} * f'_{a'}$
4. На каждом шаге делаем упрощение OBDD

Трудоемкость: $O(|f - OBDD| \cdot |f' - OBDD|)$

Вспоминаем модель Крипке

Что такое модель Крипке?

AP — множество атомарных высказываний. Модель Крипке над AP — четверка $M = (S, S_0, R, L)$, в которой:

1. S - конечное множество состояний
2. $S_0 \subseteq S$ — множество начальных состояний
3. $R \subseteq S \times S$ отношение переходов
4. $L : S \to 2^{AP}$ — функция истинности

Модель Крипке и OBDD

Пусть $|AP| = n$. Будем считать, что $S \subseteq \{0, 1\}^n$

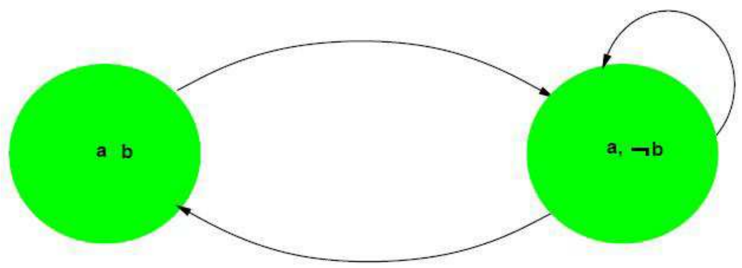
Для описания модели Крипке зададим:

Характеристическую функцию f_S для множества S

Характеристическую функцию f_R для отношения

$$R(x_1, \dots, x_n, x'_1, \dots, x'_n)$$

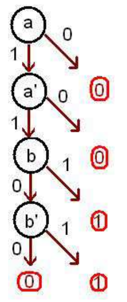
Пример модели Крипке и OBDD



$R = (a \wedge b \wedge a' \wedge \neg b') \vee (a \wedge \neg b \wedge a' \wedge b') \vee (a \wedge \neg b \wedge a' \wedge \neg b')$

Пример модели Крипке и OBDD

Диаграмма для f_R:



Как выглядит диаграмма для f_S?

План лекции

Понятие неподвижной точки

Пусть $\tau : 2^U \to 2^U$
Множество $S \subseteq U$ называется **неподвижной точкой** относительно τ, если $\tau(S) = S$

Множество S — минимальная неподвижная точка, если
1) S — неподвижная точка
2) Любая неподвижная точка содержит S

Аналогично определяется максимальная неподвижная точка

Обозначения: $\mu S\,.\,\tau(S)$ и $\nu S\,.\,\tau(S)$

Существование неподвижной точки

Пусть U конечно.

Отображение τ **монотонно**, если:
$X \subset Y \Rightarrow \tau(X) \subset \tau(Y)$

Тарский: Если отображение τ монотонно, то существуют минимальная и максимальная неподвижные точки

Алгоритм для неподвижной точки

Лемма о неподвижной точке

$\mu S \,.\, \tau(S) = \cup_{i=1}^{\infty} \tau^i(\varnothing)$
$\nu S \,.\, \tau(S) = \cap_{i=1}^{\infty} \tau^i(U)$

Доказательство.

1. Для каждого i верно $\tau^i(\varnothing) \subseteq \tau^{i+1}(\varnothing)$
2. Пусть $S = \cup_{i=1}^{\infty} \tau^i(\varnothing)$
3. $S \subseteq \tau(S)$
4. $\tau(S) \subseteq S$
5. Множество S содержится в любой неподвижной точке

□

План лекции

Задача верификации CTL

Логика CTL строится из конструкций вида:

- $\neg f$, $f \vee g$
- **EX**f
- **EG**f
- **E**$[f$**U**$g]$

Задача верификации *CTL*
Данные: модель Крипке $M = (S, R, L)$,
формула CTL-логики f
Найти: множество $\{s \in S \quad | \quad M, s \models f\}$

Идеи алгоритма

Соображения

- Модель получаем в виде OBDD для f_S и f_R
- Для каждой подформулы будем строить OBDD состояний, ее выполняющих
- Для атомарных высказываний делаем подстановку в f_S
- Для операций $\vee$ и $\neg$ используем алгоритм Бриана

Оператор EX

Множество состояний, выполняющих $\mathbf{EX}f$ характеризуется формулой:

$$\exists \bar{v}'[f(v') \wedge R(v, v')]$$

Факт: есть несложный алгоритм, который по OBDD для f и R строит OBDD для выполняющего набора для $\mathbf{EX}f$.

Оператор EG

Оператор $\tau(Z) = (f \wedge \mathbf{EX})(Z)$ действует на подмножествах S следующим образом: по множеству состояний Z он возвращает состояния, где

1. выполнена формула f
2. есть исходящее ребро в множество Z

Оператор EG II

$$\tau(Z) = f \wedge \mathbf{EX}Z$$

Лемма 1: Отображение τ монотонно.

Лемма 2: Для любого состояния $\cap_{i=1}^{\infty}\tau^i(S)$ выполнена формула $\mathbf{EG}f$.

Лемма 3: Все состояния, для которых выполнено $\mathbf{EG}f$ попали в $\cap_{i=1}^{\infty}\tau^i(S)$

Вывод: Выполняющее множество $\mathbf{EG}f$ является наибольшей неподвижной точкой $\tau(Z) = f \wedge \mathbf{EX}Z$.

Алгоритм для EG

1. Начинаем с OBDD для f_S
2. Последовательно вычисляем OBDD для $(f \wedge \mathbf{EX})^i(S)$
3. Останавливаемся, когда стпень $i+1$ равна i-ой

Задачи на дом

Придумайте какую-нибудь несложную булеву функцию, у которой экспоненциальная OBDD относительно любого порядка переменных

Неподвижную точку какого вспомогательного оператора надо вычислять для $\mathbf{E}[f\mathbf{U}g]$?

Последний слайд

Если не запомните ничего другого:

- Упорядоченные двоичные разрешающие диаграммы используются для неявного хранения модели Крипке и выполняющих множеств
- Для применения операторов **EG** и $\mathbf{E}[f\mathbf{U}g]$? используется алгоритм нахождения неподвижной точки для вспомогательного оператора
- Не забудьте порешать задачи!

Вопросы?