Нахождение эффективных булевых схем при помощи SAT-солверов

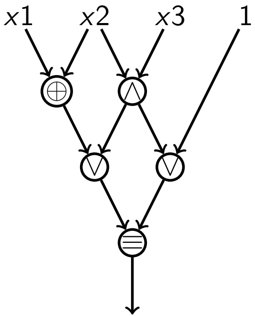
Григорий Ярославцев

Санкт-Петербургский академический университет
научно-образовательный центр нанотехнологий РАН
http://logic.pdmi.ras.ru/~grigory

1 июня, 2010 г.

Булевы схемы

- входы: пропозициональные переменные $x_1, x_2, \ldots, x_n$ и константы 0, 1
- гейты: бинарные функции
- исходящая степень гейта не ограничена



Симметрические функции

Определение

Булева функция называется симметрической, если ее значение зависит только от суммы входов.

Пример: $MAJ(x_1, \ldots, x_n) = 1 \iff x_1 + \ldots + x_n \geq n/2$

Симметрические функции

Определение

Булева функция называется симметрической, если ее значение зависит только от суммы входов.

Пример: $MAJ(x_1, \ldots, x_n) = 1 \iff x_1 + \ldots + x_n \geq n/2$

Модулярные функции

Пусть $\mathrm{MOD}^n_{m,r}(x_1, \ldots, x_n) = 1 \iff \sum_{i=1}^n x_i \equiv r \pmod{m}$.

Пример: $\mathrm{MOD}^n_{4,0}(x_1, \ldots, x_n = 1) \iff \sum_{i=1}^n x_i \equiv \{0, 4, 8, \ldots\}$

Применение практики к теории

“Для многих интересных функций имеется большой зазор между известными нижними и верхними оценками на схемную сложность. В связи с этим нахождение оптимальных схем даже для небольшого количества входов может быть полезным. Знание оптимальных схем может помочь нам лучше понять структуру оптимальных схем с произвольным количеством входов.”

Р. Вильямс (2008)

Применение практики к теории

> *“Для многих интересных функций имеется большой зазор между известными нижними и верхними оценками на схемную сложность. В связи с этим нахождение оптимальных схем даже для небольшого количества входов может быть полезным. Знание оптимальных схем может помочь нам лучше понять структуру оптимальных схем с произвольным количеством входов.”*
>
> *Р. Вильямс (2008)*

Более того, используя блоки небольшого размера можно получать верхние оценки на схемную сложность.

Основная идея

Полный перебор

- Количество $F(n, t)$ схем размера $\leq t$ с n входами не превышает

$$\left(16(t+n+2)^2\right)^t .$$

Каждому из t гейтов мы можем присвоить 16 различных булевых функций, которые зависят от предыдущих вершин схемы, и каждая из предыдущих вершин может быть либо гейтом ($\leq t$ вариантов), либо входом или константой ($\leq n+2$ вариантов).

Основная идея

Полный перебор

- Количество $F(n, t)$ схем размера $\leq t$ с n входами не превышает

$$\left(16(t+n+2)^2\right)^t .$$

  Каждому из t гейтов мы можем присвоить 16 различных булевых функций, которые зависят от предыдущих вершин схемы, и каждая из предыдущих вершин может быть либо гейтом ($\leq t$ вариантов), либо входом или константой ($\leq n+2$ вариантов).
- Для нахождения схемы из 10 гейтов от 5 переменных полному перебору потребуется изучить порядка $\sim 4.4 * 10^{36}$ схем.

Основная идея

Пусть дана функция $f : \{0,1\}^n \to \{0,1\}^m$ (n, m это константы), мы преобразуем утверждение "существует схема размера m, вычисляющая функцию f" в пропозициональную КНФ-формулу и используем SAT-солверы для проверки ее выполнимости.

Основная идея

Пусть дана функция $f : \{0,1\}^n \to \{0,1\}^m$ (n, m это константы), мы преобразуем утверждение “существует схема размера m, вычисляющая функцию f” в пропозициональную КНФ-формулу и используем SAT-солверы для проверки ее выполнимости.

Кодировка

- Все возможные графы
- Все возможные функции, вычисляемые в гейтах
- Какие гейты являются выходами
- Функция, вычисляемая схемой

Результаты

Результаты

- Новая верхняя оценка для $\mathrm{MOD}_{3,*}^n$: $3n + c$ в полном бинарном базисе B_2 (ранее известна оценка $5n + o(n)$), использующая блок с 5 входами и 9 гейтами.

Результаты

Результаты

- Новая верхняя оценка для $\mathrm{MOD}_{3,*}^n$: $3n + c$ в полном бинарном базисе B_2 (ранее известна оценка $5n + o(n)$), использующая блок с 5 входами и 9 гейтами.
- Новая верхняя оценка для $\mathrm{MOD}_{3,*}^n$: $5.5n + c$ в базисе $U_2 = B_2 \setminus \{\oplus, \equiv\}$ (ранее $7n + o(n)$), использующая блок с 4 входами и 11 гейтами.

Результаты

Результаты

- Новая верхняя оценка для $\mathrm{MOD}^n_{3,*}$: $3n + c$ в полном бинарном базисе B_2 (ранее известна оценка $5n + o(n)$), использующая блок с 5 входами и 9 гейтами.
- Новая верхняя оценка для $\mathrm{MOD}^n_{3,*}$: $5.5n + c$ в базисе $U_2 = B_2 \setminus \{\oplus, \equiv\}$ (ранее $7n + o(n)$), использующая блок с 4 входами и 11 гейтами.

- При поиске данных блоков использовался автоматический подбор кодировки остатка.
- Использовался тот факт, что часть входов является симметричной.
- Также использовались различные эвристики.

Результаты

Определение

Функцией Шеннона $C(f)$ некоторого класса функций называется максимальная схемная сложность функции данного класса.

Эквивалентными можно считать функции, которые совпадают при перестановке выходов или выходов и некоторой расстановке отрицаний перед ними.

Результаты

- Оптимальные схемы для предикатов от четырех переменных (402 функции, $C(f) = 7$).
- Оптимальные схемы для биективных функций от трех переменных (118 функций, $C(f) = 7$).
- Верхние и нижние оценки для симметрических функций от пяти переменных (20 функций, $C(f) \geq 9$).

Спасибо за внимание!