

Семинар по сложности булевых функций

Лекция 3: Линейные нижние оценки на схемную сложность и метод элиминации гейтов (продолжение)

А. Куликов

Computer Science клуб при ПОМИ
<http://compsciclub.ru>

02.10.2011



1 / 16

План лекции

- 1 Метод элиминации гейтов
- 2 Примеры свойств функций, использующихся в доказательствах нижних оценок
 - 2.5n для симметрических функций
 - 3n для обобщённой функции индексации
 - 3n для аффинных дисперсеров

2 / 16

План лекции

- 1 Метод элиминации гейтов
- 2 Примеры свойств функций, использующихся в доказательствах нижних оценок
 - 2.5n для симметрических функций
 - 3n для обобщённой функции индексации
 - 3n для аффинных дисперсеров

3 / 16

План лекции

- 1 Метод элиминации гейтов
- 2 Примеры свойств функций, использующихся в доказательствах нижних оценок
 - 2.5n для симметрических функций
 - 3n для обобщённой функции индексации
 - 3n для аффинных дисперсеров

4 / 16

План лекции

- 1 Метод элиминации гейтов
- 2 Примеры свойств функций, использующихся в доказательствах нижних оценок
 - 2.5n для симметрических функций
 - 3n для обобщённой функции индексации
 - 3n для аффинных дисперсеров

5 / 16

Нижняя оценка 2.5n для симметрических функций

Теорема (Stockmeyer, 77)

Для любых $m \geq 3$ и r , $C(MOD_{m,r}^n) \geq 2.5n - c$. Также $C(MOD_{m,r}^n) \leq 2.5n + O(1)$.

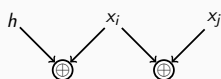
Идея доказательства

- В этом доказательстве уже довольно много случаев.
- Как обычно, сначала рассматриваются случаи, где довольно легко удалить три гейта одной подстановкой.

6 / 16

Продолжение идеи

- Не удастся это сделать в случае, когда в топ-гейт типа \oplus входят две переменные, степень каждой из которых равна 2.



- **Ключевой момент:** сделаем подстановку $x_i = h$, $x_j = h \oplus 1$.
- Вообще говоря, не очень понятно, почему мы можем заменять x_i на функцию h . Позволяет нам это сделать тот факт, что h не зависит от x_i и что x_j мы заменяем на $h \oplus 1$. Такая замена эквивалентна тому, что $x_i + x_j = 1$, то есть мы просто убиваем зависимость симметрической функции от двух переменных.
- Разбором случаев показывается, что при этом можно удалить пять гейтов.

7 / 16

План лекции

- 1 Метод элиминации гейтов
- 2 Примеры свойств функций, использующихся в доказательствах нижних оценок
 - 2.5n для симметрических функций
 - 3n для обобщённой функции индексации
 - 3n для аффинных дисперсеров

8 / 16

Теорема (Blum, 84)

Пусть $f_B: \{0, 1\}^{n+3 \log n+3}$ определяется следующим образом: для $p, q, r \in \{0, 1\}$, $a, b, c \in \{0, 1\}^{\log n}$ и $x \in \{0, 1\}^n$

$$f(a, b, c, p, q, r, x) = q(x_a x_b \vee p x_{|a|} x_{|c|}^r) \vee \bar{q}(x_{|a|} \oplus x_{|b|}).$$

Тогда $C(f) \geq 3l - 3$.

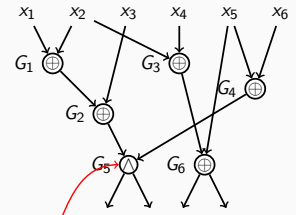
- Как и в случае функции индексации будем подставлять только переменные из x .
- Когда не удаётся подставить константу вместо переменной, попробуем подставить произвольную функцию вместо переменной.
- Если ничего из этого не помогает, то каждая переменная из x входит ровно в один гейт, причём этот гейт типа \oplus и у него ровно один потомок.
- Покажем тогда, что в текущей схеме есть $3l - 3$ гейта. Поможет нам в этом тот факт, что для любых $1 \leq i < j \leq n$ можно так подставить почти все переменные, чтобы функция превратилась как в $x_i x_j$, так и в $x_i \oplus x_j$.

План лекции

- 1 Метод элиминации гейтов
- 2 Примеры свойств функций, использующихся в доказательствах нижних оценок
 - 2.5l для симметрических функций
 - 3l для обобщённой функции индексации
 - 3l для аффинных дисперсеров

Стандартный узкий случай

так выглядит стандартный узкий случай



подставляя константу вместо переменной мы не можем удалить больше двух гейтов

и в то же время не можем исключить, что верх схемы выглядит так

рассмотрим подстановку $x_1 \oplus x_2 \oplus x_3 = 0$: G_5 превращается в константу

Аффинные дисперсеры

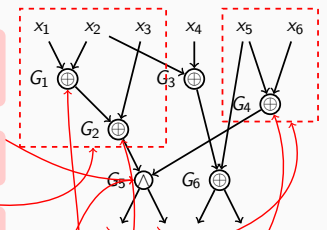
- Итак, линейные подстановки помогают при элиминации гейтов, но где взять функцию, которая выживает относительно таких подстановок?
- Непросто построить функцию, которая не обращается в константу после любых $n - o(n)$ линейных подстановок. Например, любая симметрическая функция становится константой после $n/2$ линейных подстановок: $x_1 \oplus x_2 = 1, x_3 \oplus x_4 = 1, \dots$
- Объект, который мы ищем, называется **аффинным дисперсером**.
- Формально, аффинный дисперсер для размерности d — это функция $f: \{0, 1\}^n \rightarrow \{0, 1\}$, которая не константа ни на каком аффинном подпространстве пространства $\{0, 1\}^n$ размерности хотя бы d .
- Только недавно была представлена явная конструкция аффинных дисперсеров для $d = o(n)$ [Ben-Sasson and Korparty, 09].

Идея доказательства нижней оценки 3л

возьмём первый гейт, не являющийся гейтом типа \oplus исходящего уровня. В разборе случае можно показать, что на обоих его выходах вычисляются линейные функции. Для линейных функций можем сделать $n - o(n)$ подстановку, которую функция не принимает значение 1

это убивает рассматриваемый гейт и его потомков

более того, его предшественники больше не нужны тоже



Открытая задача

Открытая задача

Доказать нижнюю оценку 3.1l на схемную сложность явно заданной булевой функции.

Спасибо за внимание!