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

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

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

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

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

Нижняя оценка $2.5n$ для симметрических функций

Теорема (Stockmeyer, 77)

Для любых $m \geq 3$ и r, $C(MOD^n_{m,r}) \geq 2.5n - c$. Также $C(MOD^n_{4,r}) \leq 2.5n + O(1)$.

Нижняя оценка $2.5n$ для симметрических функций

Теорема (Stockmeyer, 77)

Для любых $m \geq 3$ *и* r, $C(MOD^n_{m,r}) \geq 2.5n - c$. *Также* $C(MOD^n_{4,r}) \leq 2.5n + O(1)$.

Идея доказательства

- В этом доказательстве уже довольно много случаев.

Нижняя оценка $2.5n$ для симметрических функций

Теорема (Stockmeyer, 77)

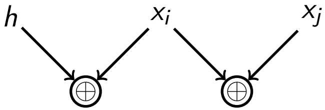
Для любых $m \geq 3$ и r, $C(MOD^n_{m,r}) \geq 2.5n - c$. Также $C(MOD^n_{4,r}) \leq 2.5n + O(1)$.

Идея доказательства

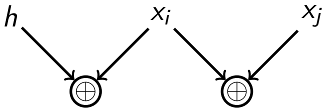
- В этом доказательстве уже довольно много случаев.
- Как обычно, сначала рассматриваются случаи, где довольно легко удалить три гейта одной подстановкой.

Продолжение идеи

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



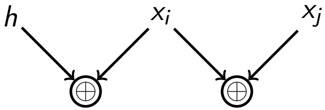
- Не удаётся это сделать в случае, когда в топ-гейт типа $\oplus$ входят две переменные, степень каждой из которых равна 2.



- Ключевой момент: сделаем подстановку $x_i = h$, $x_j = h \oplus 1$.

Продолжение идеи

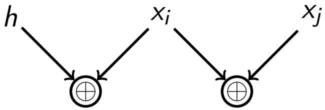
- Не удаётся это сделать в случае, когда в топ-гейт типа $\oplus$ входят две переменные, степень каждой из которых равна 2.



- 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.

Продолжение идеи

- Не удаётся 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.

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

Нижняя оценка $3n$

Теорема (Blum, 84)

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

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

Тогда $C(f) \geq 3n-3$.

Основная идея доказательства

- Как и в случае функции индексации будем подставлять только переменные из x.

Основная идея доказательства

- 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.

Основная идея доказательства

- 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.

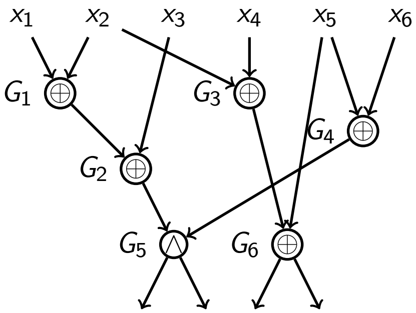
Основная идея доказательства

- 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 $3n-3$ 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

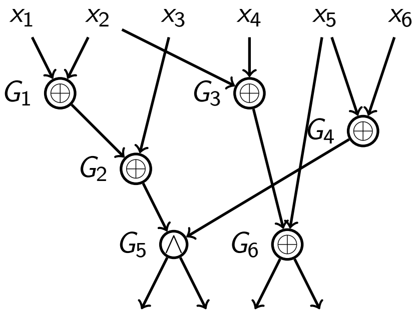
1. Метод элиминации гейтов
2. Примеры свойств функций, использующихся в доказательствах нижних оценок
   - $2.5n$ для симметрических функций
   - $3n$ для обобщённой функции индексации
   - $3n$ для аффинных дисперсеров

Стандартный узкий случай



Стандартный узкий случай

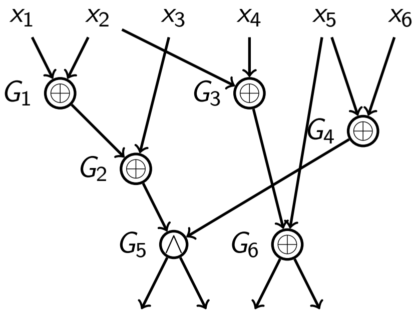
так выглядит стандартный узкий случай



Стандартный узкий случай

так выглядит стандартный узкий случай

подставляя константу вместо переменной мы не можем удалить больше двух гейтов

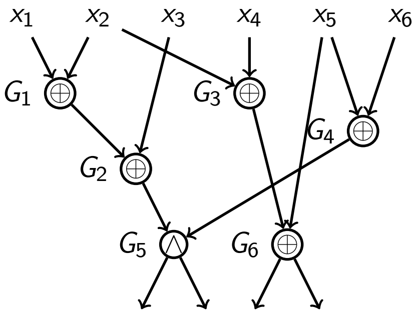


Стандартный узкий случай

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



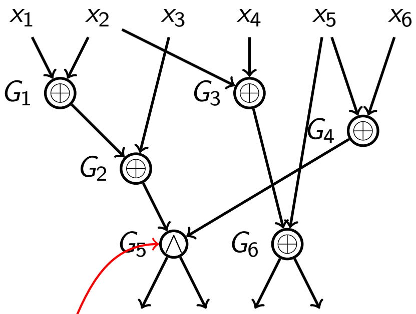
Стандартный узкий случай

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?

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: $x_1 \oplus x_2 = 1, x_3 \oplus x_4 = 1, \dots$.

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: $x_1 \oplus x_2 = 1, x_3 \oplus x_4 = 1, \ldots$.
- Объект, который мы ищем, называется аффинным дисперсером.

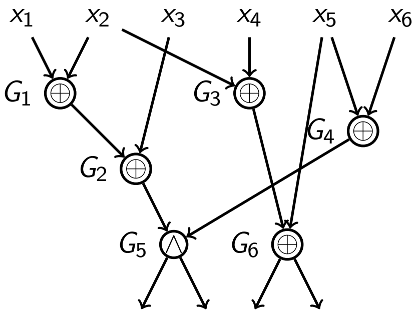
Аффинные дисперсеры

- 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 $f\colon \{0,1\}^n \to \{0,1\}$, которая не константа ни на каком аффинном подпространстве пространства $\{0,1\}^n$ размерности хотя бы d.

Аффинные дисперсеры

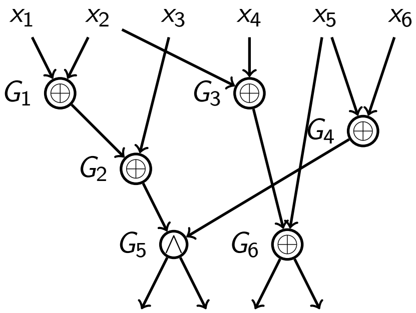
- Итак, линейные подстановки помогают при элиминации гейтов, но где взять функцию, которая выживает относительно таких подстановок?
- Непросто построить функцию, которая не обращается в константу после любых $n - o(n)$ линейных подстановок. Например, любая симметрическая функция становится константой после $n/2$ линейных подстановок: $x_1 \oplus x_2 = 1, x_3 \oplus x_4 = 1, \ldots$.
- Объект, который мы ищем, называется аффинным дисперсером.
- Формально, аффинный дисперсер для размерности d — это функция $f \colon \{0,1\}^n \to \{0,1\}$, 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 Kopparty, 09].

Идея доказательства нижней оценки $3n$

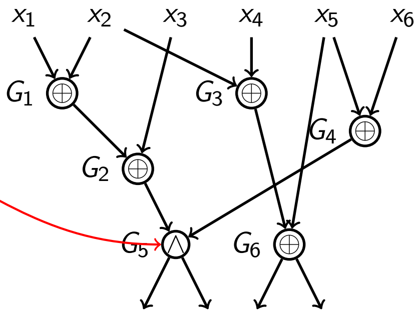


Идея доказательства нижней оценки $3n$

возьмём первый гейт, не являющийся гейтом типа $\oplus$ исходящей степени 1



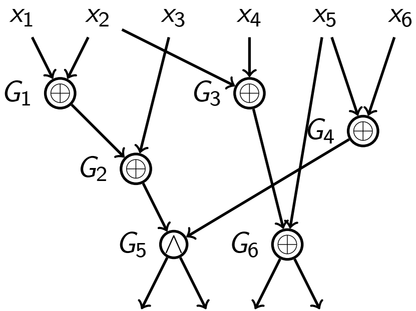
возьмём первый гейт, не являющийся гейтом типа $\oplus$ исходящей степени 1



Идея доказательства нижней оценки $3n$

возьмём первый гейт, не являющийся гейтом типа $\oplus$ исходящей степени 1

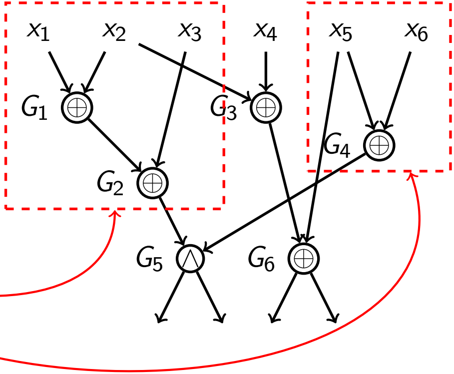
на обоих его входах вычисляются линейные функции



Идея доказательства нижней оценки $3n$

возьмём первый гейт, не являющийся гейтом типа $\oplus$ исходящей степени 1

на обоих его входах вычисляются линейные функции

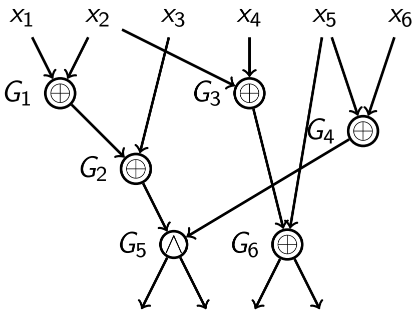


Идея доказательства нижней оценки $3n$

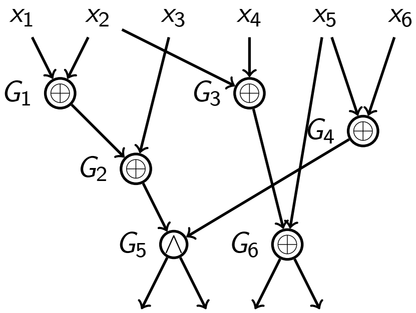
возьмём первый гейт, не являющийся гейтом типа $\oplus$ исходящей степени 1

на обоих его входах вычисляются линейные функции

сделаем подстановку
$x_1 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_6 = 1$



Идея доказательства нижней оценки $3n$



возьмём первый гейт, не являющийся гейтом типа $\oplus$ исходящей степени 1

на обоих его входах вычисляются линейные функции

сделаем подстановку $x_1 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_6 = 1$

это убивает рассматриваемый гейт и его потомков

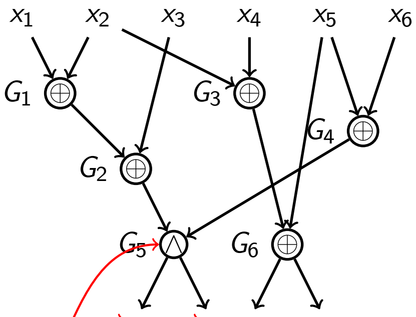
Идея доказательства нижней оценки $3n$

возьмём первый гейт, не являющийся гейтом типа $\oplus$ исходящей степени 1

на обоих его входах вычисляются линейные функции

сделаем подстановку
$x_1 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_6 = 1$

это убивает рассматриваемый гейт и его потомков



Идея доказательства нижней оценки $3n$

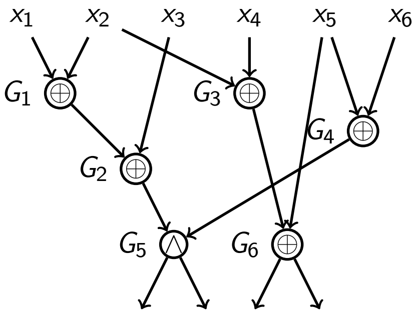
возьмём первый гейт, не являющийся гейтом типа $\oplus$ исходящей степени 1

на обоих его входах вычисляются линейные функции

сделаем подстановку
$x_1 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_6 = 1$

это убивает рассматриваемый гейт и его потомков

более того, его предшественники больше не нужны тоже



Идея доказательства нижней оценки $3n$

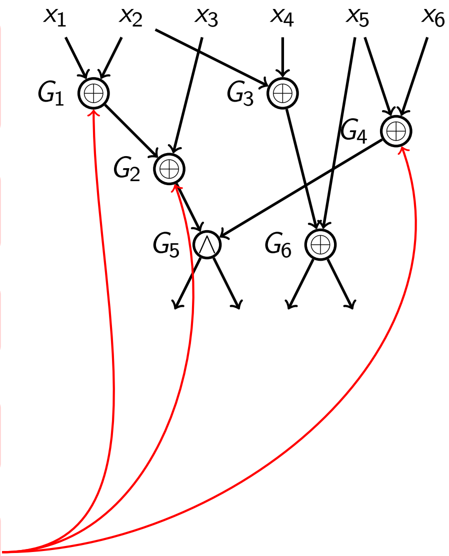
возьмём первый гейт, не являющийся гейтом типа $\oplus$ исходящей степени 1

на обоих его входах вычисляются линейные функции

сделаем подстановку
$x_1 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_6 = 1$

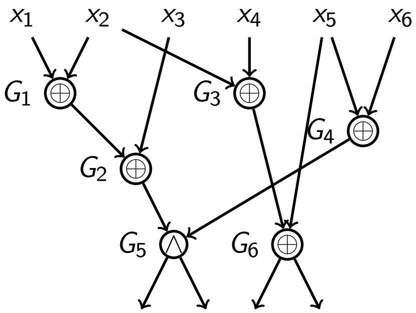
это убивает рассматриваемый гейт и его потомков

более того, его предшественники больше не нужны тоже



Идея доказательства нижней оценки $3n$

небольшим разбором случае можно показать, что так всегда можно удалить 3 гейта; поскольку мы можем сделать $n - o(n)$ таких подстановок, получаем нижнюю оценку $3n - o(n)$



Открытая задача

Открытая задача

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

Спасибо за внимание!