Семинар по сложности булевых функций

Лекция 2: Линейные нижние оценки на схемную сложность и метод элиминации гейтов

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
   - $2n$ для функций, имеющих хотя бы три различные подфункции относительно любых двух переменных
   - $2n$ для функции индексации
   - $7n/3$ для функций высокой степени

План лекции

1. Метод элиминации гейтов
2. Примеры свойств функций, использующихся в доказательствах нижних оценок
   - $2n$ для функций, имеющих хотя бы три различные подфункции относительно любых двух переменных
   - $2n$ для функции индексации
   - $7n/3$ для функций высокой степени

Лучшие известные нижние оценки

Базис всех бинарных булевых функций B_2

$2n - c$	[Клосс и Малышев, 65]
$2n - c$	[Schnorr, 74]
$2.n - o(n)$	[Paul, 77]
$2.5n - o(n)$	[Paul, 77]
$2.5n - c$	[Stockmeyer, 77]
$3n - o(n)$	[Blum, 84]
$2.33n - c$	[Кожевников и Куликов, 09]
$3n - o(n)$	[Деменков и Куликов, 10]

Базис $U_2 = B_2 \setminus \{\oplus, \equiv\}$

$4n - c$	[Zwick, 91]
$4.5n - o(n)$	[Lachish and Raz, 01]
$5n - o(n)$	[Iwama and Morizumi, 02]

Метод элиминации гейтов

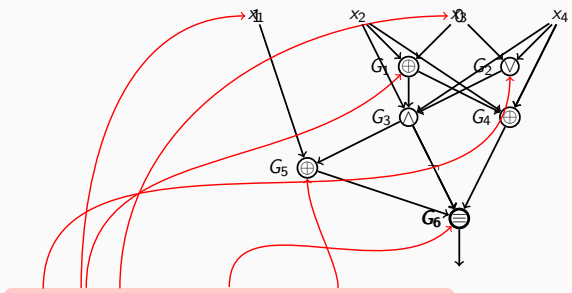
Основная идея метода

- Возьмём оптимальную схему для рассматриваемой функции.
- Подставив значения одной или нескольким переменным, удалим несколько гейтов и получим функцию того же типа (чтобы действовать по индукции).
- Гейт удаляется, если он не зависит от одного из своих входов.
- По индукции получаем, что в исходной схеме было много гейтов.

Замечание

Вряд ли данный метод позволит доказать нелинейную нижнюю оценку. Для нелинейных оценок нужен принципиально новый метод.

Пример



$G_2 = x_4$ равен x_2 $x_3 = 0$ ункцию, присвоенную G_6

План лекции

1. Метод элиминации гейтов
2. Примеры свойств функций, использующихся в доказательствах нижних оценок
   - $2n$ для функций, имеющих хотя бы три различные подфункции относительно любых двух переменных
   - $2n$ для функции индексации
   - $7n/3$ для функций высокой степени

План лекции

1. Метод элиминации гейтов
2. Примеры свойств функций, использующихся в доказательствах нижних оценок
   - $2n$ для функций, имеющих хотя бы три различные подфункции относительно любых двух переменных
   - $2n$ для функции индексации
   - $7n/3$ для функций высокой степени

Класс функций $Q^n_{2,3}$

Определение

Функция $f\colon \{0,1\}^n \to \{0,1\}$ принадлежит классу $Q^n_{2,3}$, если

1. для любых различных $i, j \in \{1,\dots,n\}$, среди четырёх функций, получаемых их f подстановкой констант вместо x_i и x_j, хотя бы три различны;
2. для всех $i \in \{1,\dots,n\}$, после подстановки x_i константы получается функция из $Q^{n-1}_{2,3}$ (при $n \geq 4$).

Пример: функция остатка по модулю

- Пусть $\mathrm{MOD}^n_{m,r}(x_1,\dots,x_n) = 1 \Leftrightarrow \sum_{i=1}^n x_i \equiv r \pmod m$.
- Тогда $\mathrm{MOD}^n_{3,r}, \mathrm{MOD}^n_{4,r} \in Q^n_{2,3}$, но $\mathrm{MOD}^n_{2,r} \notin Q^n_{2,3}$.

Нижняя оценка $2n$ [Schnorr, 74]

Теорема

Для $f \in Q^n_{2,3}$, $C(f) \geq 2n - 8$.

Доказательство

- Индукция по n. Если $n \leq 4$, тогда утверждение очевидно.
- Рассмотрим оптимальную схему и её топ-гейт Q, то есть такой гейт, в который входят две переменные x_i и x_j (они различны, поскольку схема оптимальна).
- Заметим, что $Q = Q(x_i, x_j)$ может принимать всего два значения при подстановке x_i и x_j, а именно, значения 0 и 1.
- Значит, хотя бы одна из x_i и x_j должна входить в какой-то другой гейт P.
- Подставляя константу вместо этой переменной, мы удаляем хотя бы два гейта (P и Q) и получаем подфункцию из $Q^{n-1}_{2,3}$. □

План лекции

1. Метод элиминации гейтов
2. Примеры свойств функций, использующихся в доказательствах нижних оценок
   - $2n$ для функций, имеющих хотя бы три различные подфункции относительно любых двух переменных
   - $2n$ для функции индексации
   - $7n/3$ для функций высокой степени

Функция индексации

Определение

Функция индексации (storage access function) — это функция $\mathrm{SA}\colon \{0,1\}^{\log n + n} \to \{0,1\}$, такая что $\mathrm{SA}(a,x) = x_{|a|}$, где $a \in \{0,1\}^{\log n}$, $x \in \{0,1\}^n$, а $|a|$ — число, бинарным представлением которого является a.

Теорема (Paul, 77; Klein and Paterson, 80)

$$2n - 2 \leq C(SA) \leq 2n + o(n)\,.$$

План лекции

1. Метод элиминации гейтов
2. Примеры свойств функций, использующихся в доказательствах нижних оценок
   - $2n$ для функций, имеющих хотя бы три различные подфункции относительно любых двух переменных
   - $2n$ для функции индексации
   - $7n/3$ для функций высокой степени

Гейты типа $\wedge$ против гейтов типа $\oplus$

Бинарные булевы функции

Множество B_2 всех бинарных булевых функций содержит 16 функций $f(x,y)$:

1. 2 константы: 0, 1
2. 4 вырожденные функции: x, $\bar{x}$, y, $\bar{y}$.
3. 2 функции типа $\oplus$: $x \oplus y \oplus a$, где $a \in \{0,1\}$.
4. 8 функции типа $\wedge$: $(x \oplus a)(y \oplus b) \oplus c$, где $a, b, c \in \{0,1\}$.

Замечание

Оптимальные схемы содержат только гейты типа $\wedge$ и $\oplus$, так как константные и вырожденные гейты могут быть удалены их схемы без увеличения размера.

Разница между двумя типами гейтов

- С гейтами типа $\wedge$ бороться проще, чем с гейтами типа $\oplus$.
- Пусть $Q(x_i, x_j) = (x_i \oplus a)(x_j \oplus b) \oplus c$ — гейт типа $\wedge$. Тогда подставляя $x_i = a$ или $x_j = b$, мы делаем данный гейт константным. Значит, мы удаляем не только этот гейт, но и всех его потомков!
- В то время как подставляя x_i, мы превращаем $Q(x_i, x_j) = x_i \oplus x_j \oplus c$ в x_j или $\bar{x}_j$.
- В частности, по этой причине оценки для базиса B_2 ниже оценок для базиса $U_2 = B_2 \setminus \{\oplus, \equiv\}$.
- Как правило, самым сложным случаем в доказательстве является схема, в которой много гейтов типа $\oplus$ сверху.

Многочлены над GF(2)

Многочлены над GF(2)

- Обозначим через $\tau(f)$ единственный многочлен над GF(2), представляющий f.
- Например, $\tau(\mathrm{MOD}^3_{3,0}) = x_1x_2x_3 + (1-x_1)(1-x_2)(1-x_3)$.
- Напомним, что $\tau(f)$ линеен по каждой переменной.
- Нетрудно показать, что для любого r, $\deg(\tau(\mathrm{MOD}^n_{4,r})) \leq 3$, в то время как $\deg(\tau(\mathrm{MOD}^n_{3,r})) \geq n - 1$.

Лемма (Degree lower bound)

В любой схеме для f есть не менее $deg(\tau(f)) - 1$ гейтов типа $\wedge$.

Комбинированная мера сложности

Идея

Итак, в самом трудном случае у нас обычно одни гейты типа $\oplus$, но несколько гейтов типа $\wedge$ нам даны заранее. Давайте попробуем увеличить вес гейтов типа $\oplus$.

Определение

Для схемы C через $A(C)$ и $X(C)$ обозначим, соответственно, количество гейтов типа $\wedge$ и $\oplus$. Пусть также $\mu(C) = 3X(C) + 2A(C)$.

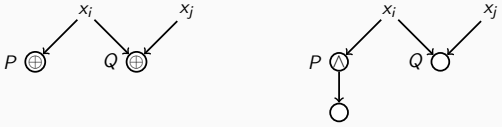
Улучшенная нижняя оценка

Лемма

Для любой схемы C, вычисляющей функцию $f \in Q^n_{2,3}$, верно неравенство $\mu(C) = 3X(C) + 2A(C) \geq 6n - 24$.

Доказательство

- Как и в прошлый раз, мы берём топ-гейт $Q(x_i, x_j)$ и НУО считаем, что x_i также входит в другой гейт P.
- Есть два случая:



- В обоих случаях, подставляя x_i (правильную) константу, мы уменьшаем μ хотя бы на 6. □

Нижняя оценка $7n/3$

Теорема

Для $f \in Q^n_{2,3}$, такой что $deg(\tau(f)) \geq n - c$, верно неравенство $C(f) \geq 7n/3 - c'$.

Доказательство

Пусть C — оптимальная схема, вычисляющая f.

$$\frac{\begin{array}{r} 3X(C)+2A(C) \geq 6n - 24 \\ A(C) \geq n - c - 1 \end{array}}{3C(f) = 3X(C)+3A(C) \geq 7n - 25 - c}$$

□

□

Спасибо за внимание!