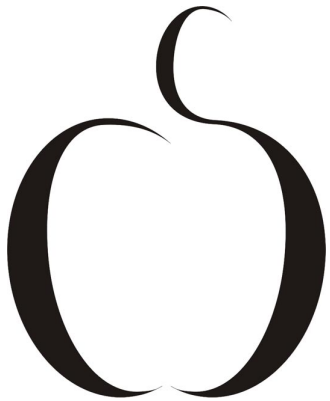
Семинар по сложности булевых функций

Лекция 5: Связь размера и глубины формулы. Нижние оценки на формульную сложность

И. Близнец

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

30.10.2011



План лекции

1. Размер и глубина формулы
2. Квадратичная нижняя оценка для универсальной функции
3. Случайные ограничения, нижняя оценка Субботовской
4. Нижняя оценка Андреева

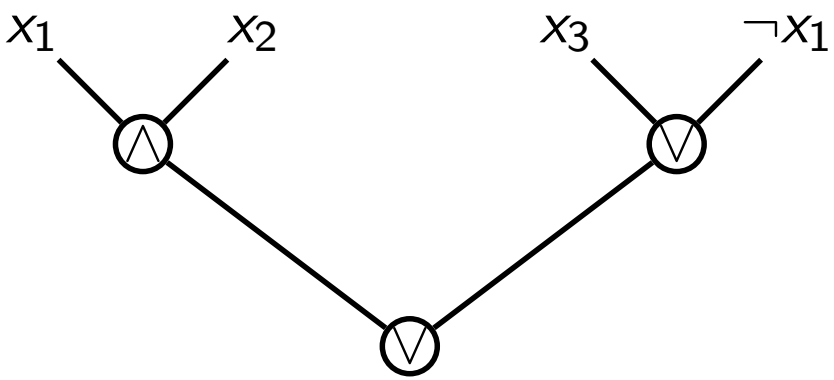
План лекции

1. Размер и глубина формулы
2. Квадратичная нижняя оценка для универсальной функции
3. Случайные ограничения, нижняя оценка Субботовской
4. Нижняя оценка Андреева

Обозначения

Формула

Рассматриваем только формулы де Моргана, то есть формулы, использующие только бинарные $\vee$(ИЛИ), $\wedge$(И) гейты.
Формула — это схема являющаяся деревом.
Входами являются переменные и их литералы.



$$(x_1 \wedge x_2) \vee (x_3 \vee \neg x_1)$$

Размер и глубина формулы

Определение

$f : \{0,1\}^n \to \{0,1\}$.
Размер формулы — это количество листьев в древесном представлении.
$L(f)$ — размер наименьшей (относительно размера) формулы, задающей функцию f.
Глубина формулы — это высота дерева в древесном представлении.
$D(f)$ — глубина наименьшей (относительно глубины) формулы, задающей функцию f.

Размер и глубина формулы

Определение

$f : \{0,1\}^n \to \{0,1\}$.
Размер формулы — это количество листьев в древесном представлении.
$L(f)$ — размер наименьшей (относительно размера) формулы, задающей функцию f.
Глубина формулы — это высота дерева в древесном представлении.
$D(f)$ — глубина наименьшей (относительно глубины) формулы, задающей функцию f.

Утверждение

$$D(f) \geq \log_2 L(f).$$

Размер и глубина формулы

Определение

$f : \{0,1\}^n \to \{0,1\}$.
Размер формулы — это количество листьев в древесном представлении.
$L(f)$ — размер наименьшей (относительно размера) формулы, задающей функцию f.
Глубина формулы — это высота дерева в древесном представлении.
$D(f)$ — глубина наименьшей (относительно глубины) формулы, задающей функцию f.

Утверждение

$$D(f) \geq \log_2 L(f).$$

Утверждение

$$c \cdot \log_2 L(f) > D(f).$$

Теорема о балансировке формулы

Теорема

Для любой булевой функции f верно:

$$D(f) \leq 1.82 \cdot \log_2 L(f).$$

Теорема о балансировке формулы

Теорема

Для любой булевой функции f верно:

$$D(f) \leq 1.82 \cdot \log_2 L(f).$$

Доказательство

Теорема о балансировке формулы

Теорема

Для любой булевой функции f верно:

$$D(f) \leq 1.82 \cdot \log_2 L(f).$$

Доказательство

- Достаточно рассматривать только монотонные формулы, то есть формулы, не содержащие отрицаний.

Теорема о балансировке формулы

Теорема

Для любой булевой функции f верно:

$$D(f) \leq 1.82 \cdot \log_2 L(f).$$

Доказательство

- Достаточно рассматривать только монотонные формулы, то есть формулы, не содержащие отрицаний.
- Заменим $\neg x_i$ на y_i. Вместо $F(x)$ получим $F'(x, y)$

$$F(x) = F'(x, \neg x).$$

Теорема о балансировке формулы (продолжение док-ва)

Теорема

Для любой (монотонной) булевой функции f верно:

$$D(f) \leq 1.82 \cdot \log_2 L(f).$$

Доказательство

Теорема о балансировке формулы (продолжение док-ва)

Теорема

Для любой (монотонной) булевой функции f верно:

$$D(f) \leq 1.82 \cdot \log_2 L(f).$$

Доказательство

- Приведем доказательство для 3, а не для 1.82.

Теорема о балансировке формулы (продолжение док-ва)

Теорема

Для любой (монотонной) булевой функции f верно:

$$D(f) \leq 1.82 \cdot \log_2 L(f).$$

Доказательство

- Приведем доказательство для 3, а не для 1.82.
- Доказательство по индукции, по размеру формулы m.

Теорема о балансировке формулы (продолжение док-ва)

Теорема

Для любой (монотонной) булевой функции f верно:

$$D(f) \leq 1.82 \cdot \log_2 L(f).$$

Доказательство

- Приведем доказательство для 3, а не для 1.82.
- Доказательство по индукции, по размеру формулы m.
- Найдем подформулу Y размера $\geq \frac{m}{2}$.

Теорема о балансировке формулы (продолжение док-ва)

Теорема

Для любой (монотонной) булевой функции f верно:

$$D(f) \leq 1.82 \cdot \log_2 L(f).$$

Доказательство

- Приведем доказательство для 3, а не для 1.82.
- Доказательство по индукции, по размеру формулы m.
- Найдем подформулу Y размера $\geq \frac{m}{2}$.
- Но, так чтобы левая и правая подформулы Y были меньше $\frac{m}{2}$.

Теорема о балансировке формулы (продолжение док-ва)

Теорема

Для любой (монотонной) булевой функции f верно:

$$D(f) \leq 1.82 \cdot \log_2 L(f).$$

Доказательство

- Приведем доказательство для 3, а не для 1.82.
- Доказательство по индукции, по размеру формулы m.
- Найдем подформулу Y размера $\geq \frac{m}{2}$.
- Но, так чтобы левая и правая подформулы Y были меньше $\frac{m}{2}$.
- Пусть F_0, F_1 формулы, получающиеся из F заменой Y на 0 и 1.

Теорема о балансировке формулы (продолжение док-ва)

Теорема

Для любой (монотонной) булевой функции f верно:

$$D(f) \leq 3 \cdot \log_2 L(f).$$

Доказательство

Теорема о балансировке формулы (продолжение док-ва)

Теорема

Для любой (монотонной) булевой функции f верно:

$$D(f) \leq 3 \cdot \log_2 L(f).$$

Доказательство

- Если $F_1(x) = 0$,то $F_0(x) = 0$.

Теорема о балансировке формулы (продолжение док-ва)

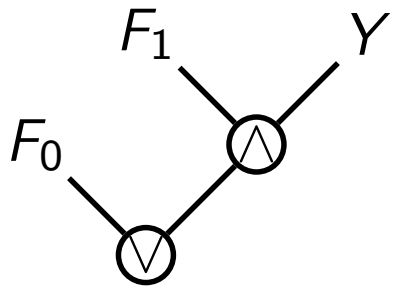
Теорема

Для любой (монотонной) булевой функции f верно:

$$D(f) \leq 3 \cdot \log_2 L(f).$$

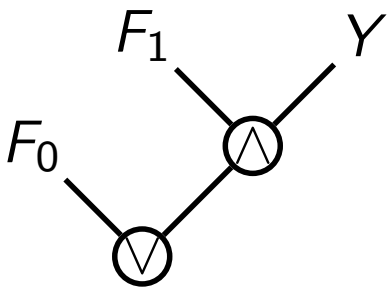
Доказательство

- Если $F_1(x) = 0$,то $F_0(x) = 0$.
- Значит первоначальная формула эквивалентна следующей



Теорема о балансировке формулы (продолжение док-ва)

Доказательство



Формулы F_0, F_1 и левая, правая подформулы Y содержат не более $\frac{m}{2}$ листьев. А значит, для них верно индукционное предположение. То есть, получили требуемое: глубина формулы не более $2 + 1 + 3 \cdot \log_2(\frac{m}{2}) = 3 \cdot \log_2 m$.

План лекции

1. Размер и глубина формулы
2. Квадратичная нижняя оценка для универсальной функции
3. Случайные ограничения, нижняя оценка Субботовской
4. Нижняя оценка Андреева

Универсальная функция (storage access function)

Определение

Универсальная функция (storage access function)

Определение

- Пусть $n = 2^r$. Если $a \in \{0,1\}^r$, обозначим через $bin(a)$ следующее число

$$2^{r-1}a_1 + \cdots + 2a_{r-1} + a_r + 1.$$

Универсальная функция (storage access function)

Определение

- Пусть $n = 2^r$. Если $a \in \{0,1\}^r$, обозначим через $bin(a)$ следующее число

$$2^{r-1}a_1 + \cdots + 2a_{r-1} + a_r + 1.$$

- $U_n \colon \{0,1\}^{n+r} \to \{0,1\}, z \in \{0,1\}^r, y \in \{0,1\}^n$.

Универсальная функция (storage access function)

Определение

- Пусть $n = 2^r$. Если $a \in \{0,1\}^r$, обозначим через $bin(a)$ следующее число
$$2^{r-1}a_1 + \cdots + 2a_{r-1} + a_r + 1.$$
- $U_n \colon \{0,1\}^{n+r} \to \{0,1\}, z \in \{0,1\}^r, y \in \{0,1\}^n$.
- $$U_n(z,y) := y_{bin(z)}.$$

Универсальная функция (storage access function)

Определение

- Пусть $n = 2^r$. Если $a \in \{0,1\}^r$, обозначим через $bin(a)$ следующее число

$$2^{r-1}a_1 + \cdots + 2a_{r-1} + a_r + 1.$$

- $U_n \colon \{0,1\}^{n+r} \to \{0,1\}, z \in \{0,1\}^r, y \in \{0,1\}^n$.
-

$$U_n(z,y) := y_{bin(z)}.$$

Утверждение

Для булевой функции $h(z_1, \ldots z_r)$ существует $b \in \{0,1\}^n$, такое что:

$$U_n(z,b) = h(z).$$

Универсальная функция

Определение

$$x, y \in \{0,1\}^n, n = 2^r, m = \frac{n}{r}.$$

$$x = \begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,m} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{r,1} & x_{r,2} & \cdots & x_{r,m} \end{pmatrix}$$

Универсальная функция

Определение

$$x, y \in \{0,1\}^n, n = 2^r, m = \frac{n}{r}.$$

$$x = \begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,m} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{r,1} & x_{r,2} & \cdots & x_{r,m} \end{pmatrix}$$

Универсальная функция, порожденная функцией ϕ

$$U_n^{\phi}(x, y) := U_n(z_1, \ldots z_r, y), \text{ где } z_i = \phi(x_{i1}, x_{i2}, \ldots x_{im}).$$

Универсальная функция

Определение

$$x, y \in \{0,1\}^n, n = 2^r, m = \frac{n}{r}.$$

$$x = \begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,m} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{r,1} & x_{r,2} & \cdots & x_{r,m} \end{pmatrix}$$

Универсальная функция, порожденная функцией ϕ

$$U_n^{\phi}(x, y) := U_n(z_1, \ldots z_r, y), \text{ где } z_i = \phi(x_{i1}, x_{i2}, \ldots x_{im}).$$

Теорема

Любая бинарная формула, вычисляющая U_n^{OR} содержит не менее $n^{2-o(1)}$ листьев.

$L(U_n^{OR}) \geq n^{2-o(1)}$

Доказательство

$L(U_n^{OR}) \geq n^{2-o(1)}$

Доказательство

- Рассмотрим сложную функцию $h\colon \{0,1\}^r \to \{0,1\}$.

$L(U_n^{OR}) \geq n^{2-o(1)}$

Доказательство

- Рассмотрим сложную функцию $h\colon \{0,1\}^r \to \{0,1\}$.
- Возьмем $b \in \{0,1\}^n$ такое, что: $U_n(z,b) = h(z)$.

$L(U_n^{OR}) \geq n^{2-o(1)}$

Доказательство

- Рассмотрим сложную функцию $h\colon \{0,1\}^r \to \{0,1\}$.
- Возьмем $b \in \{0,1\}^n$ такое, что: $U_n(z,b) = h(z)$.
- $$f(x) := U_n^{OR}(x,b) = h(\bigvee_{j=1}^{m} x_{1j}, \bigvee_{j=1}^{m} x_{2j}, \cdots \bigvee_{j=1}^{m} x_{rj})$$

$L(U_n^{OR}) \geq n^{2-o(1)}$

Доказательство

- Рассмотрим сложную функцию $h\colon \{0,1\}^r \to \{0,1\}$.
- Возьмем $b \in \{0,1\}^n$ такое, что: $U_n(z,b) = h(z)$.
- $$f(x) := U_n^{OR}(x,b) = h(\bigvee_{j=1}^{m} x_{1j}, \bigvee_{j=1}^{m} x_{2j}, \cdots \bigvee_{j=1}^{m} x_{rj})$$
- $$L(U_n^{OR}(x,y)) \geq L(f)$$

$L(U_n^{OR}) \geq n^{2-o(1)}$

Доказательство

- Рассмотрим сложную функцию $h\colon \{0,1\}^r \to \{0,1\}$.
- Возьмем $b \in \{0,1\}^n$ такое, что: $U_n(z,b) = h(z)$.
- $$f(x) := U_n^{OR}(x,b) = h(\bigvee_{j=1}^{m} x_{1j}, \bigvee_{j=1}^{m} x_{2j}, \cdots \bigvee_{j=1}^{m} x_{rj})$$
- $$L(U_n^{OR}(x,y)) \geq L(f)$$
- Докажем, что для любой формулы F вычисляющей f:
$$L(F) \geq n^{2-o(1)}$$

$L(U_n^{OR}) \geq n^{2-o(1)}$

Доказательство

- Рассмотрим сложную функцию $h\colon \{0,1\}^r \to \{0,1\}$.
- Возьмем $b \in \{0,1\}^n$ такое, что: $U_n(z,b) = h(z)$.
- $$f(x) := U_n^{OR}(x,b) = h(\bigvee_{j=1}^{m} x_{1j}, \bigvee_{j=1}^{m} x_{2j}, \cdots \bigvee_{j=1}^{m} x_{rj})$$
- $$L(U_n^{OR}(x,y)) \geq L(f)$$
- Докажем, что для любой формулы F вычисляющей f:
$$L(F) \geq n^{2-o(1)}$$
- В каждой строке матрицы x самую редкую переменную оставим, а все остальные означим нулем.

$L(U_n^{OR}) \geq n^{2-o(1)}$ (продолжение док-ва)

Доказательство

$L(U_n^{OR}) \geq n^{2-o(1)}$ (продолжение док-ва)

Доказательство

- Получим формулу F', причем $L(F) \geq m \cdot L(F')$.

$L(U_n^{OR}) \geq n^{2-o(1)}$ (продолжение док-ва)

Доказательство

- Получим формулу F', причем $L(F) \geq m \cdot L(F')$.
- $$L(F') \geq L(h)$$

$L(U_n^{OR}) \geq n^{2-o(1)}$ (продолжение док-ва)

Доказательство

- Получим формулу F', причем $L(F) \geq m \cdot L(F')$.
- $$L(F') \geq L(h)$$
- $L(U_n^{OR}) \geq L(f) \geq m \cdot L(F') \geq m \cdot L(h) \geq m \cdot O(\frac{n}{\log \log n})$.

$L(U_n^{OR}) \geq n^{2-o(1)}$ (продолжение док-ва)

Доказательство

- Получим формулу F', причем $L(F) \geq m \cdot L(F')$.
- $$L(F') \geq L(h)$$
- $L(U_n^{OR}) \geq L(f) \geq m \cdot L(F') \geq m \cdot L(h) \geq m \cdot O(\frac{n}{\log \log n})$.
- $$L(U_n^{OR}) \geq \frac{n}{\log n} \cdot O\left(\frac{n}{\log \log n}\right) = O\left(\frac{n^2}{\log n \log \log n}\right).$$

□

Замечание

Данное доказательство также показывает, что теорема верна не только для формул де Моргана, но и для любой формулы использующей любые бинарные операции.

План лекции

1. Размер и глубина формулы
2. Квадратичная нижняя оценка для универсальной функции
3. Случайные ограничения, нижняя оценка Субботовской
4. Нижняя оценка Андреева

Вспомогательные замечания и леммы

Лемма

Если F минимальная формула для булевой функции f, тогда для любого листа $z \in \{x_i, \neg x_i\}$ его сосед не содержит переменной x_i.

Доказательство

Вспомогательные замечания и леммы

Лемма

Если F минимальная формула для булевой функции f, тогда для любого листа $z \in \{x_i, \neg x_i\}$ его сосед не содержит переменной x_i.

Доказательство

- Всегда значение переменной внутри соседа можно заменить на константу.

Вспомогательные замечания и леммы

Лемма

Если F минимальная формула для булевой функции f, тогда для любого листа $z \in \{x_i, \neg x_i\}$ его сосед не содержит переменной x_i.

Доказательство

- Всегда значение переменной внутри соседа можно заменить на константу.
- $x \wedge G$, если $x = 0$, то G можно вообще не вычислять.

Вспомогательные замечания и леммы

Лемма

Если F минимальная формула для булевой функции f, тогда для любого листа $z \in \{x_i, \neg x_i\}$ его сосед не содержит переменной x_i.

Доказательство

- Всегда значение переменной внутри соседа можно заменить на константу.
- $x \wedge G$, если $x = 0$, то G можно вообще не вычислять.
- То есть, можно вычилять G, когда вместо x везде стоит 1.

Вспомогательные замечания и леммы

Лемма

Если F минимальная формула для булевой функции f, тогда для любого листа $z \in \{x_i, \neg x_i\}$ его сосед не содержит переменной x_i.

Доказательство

- Всегда значение переменной внутри соседа можно заменить на константу.
- $x \wedge G$, если $x = 0$, то G можно вообще не вычислять.
- То есть, можно вычилять G, когда вместо x везде стоит 1.
- Другие случаи аналогично. □

Лемма Субботовской

Лемма

Для любой булевой функции от n переменных, можно зафиксировать значение одной из них так, что полученная функция f' удовлетворяет:

$$L(f') \leq \left(1 - \frac{1}{n}\right)^{\frac{3}{2}} L(f).$$

Доказательство

Лемма Субботовской

Лемма

Для любой булевой функции от n переменных, можно зафиксировать значение одной из них так, что полученная функция f' удовлетворяет:

$$L(f') \leq \left(1 - \frac{1}{n}\right)^{\frac{3}{2}} L(f).$$

Доказательство

- При одном из означиваний литерала, вычисление значения соседа бессмысленно.

Лемма Субботовской

Лемма

Для любой булевой функции от n переменных, можно зафиксировать значение одной из них так, что полученная функция f' удовлетворяет:

$$L(f') \leq \left(1 - \frac{1}{n}\right)^{\frac{3}{2}} L(f).$$

Доказательство

- При одном из означиваний литерала, вычисление значения соседа бессмысленно.
- $x_j \vee F$ — можно выкинуть F, если $x_j = 1$.

Лемма Субботовской

Лемма

Для любой булевой функции от n переменных, можно зафиксировать значение одной из них так, что полученная функция f' удовлетворяет:

$$L(f') \leq \left(1 - \frac{1}{n}\right)^{\frac{3}{2}} L(f).$$

Доказательство

- При одном из означиваний литерала, вычисление значения соседа бессмысленно.
- $x_j \vee F$ — можно выкинуть F, если $x_j = 1$.
- Выберем переменную x_i, которая чаще всего встречается в формуле минимального размера для функции f.

Лемма Субботовской

Лемма

Для любой булевой функции от n переменных, можно зафиксировать значение одной из них так, что полученная функция f' удовлетворяет:

$$L(f') \leq \left(1 - \frac{1}{n}\right)^{\frac{3}{2}} L(f).$$

Доказательство

- При одном из означиваний литерала, вычисление значения соседа бессмысленно.
- $x_j \vee F$ — можно выкинуть F, если $x_j = 1$.
- Выберем переменную x_i, которая чаще всего встречается в формуле минимального размера для функции f.
- x_i встречается как минимум $\frac{L(f)}{n}$ раз в формуле.

Лемма Субботовской

Лемма

Для любой булевой функции от n переменных, можно зафиксировать значение одной из них так, что полученная функция f' удовлетворяет:

$$L(f') \leq \left(1 - \frac{1}{n}\right)^{\frac{3}{2}} L(f).$$

Доказательство

- При одном из означиваний литерала, вычисление значения соседа бессмысленно.
- $x_j \vee F$ — можно выкинуть F, если $x_j = 1$.
- Выберем переменную x_i, которая чаще всего встречается в формуле минимального размера для функции f.
- x_i встречается как минимум $\frac{L(f)}{n}$ раз в формуле.
- При одном из означиваний x_i пропадает не менее $\frac{L(f)}{2n}$ соседей.

Лемма Субботовской (продолжение док-ва)

Доказательство

Лемма Субботовской (продолжение док-ва)

Доказательство

- Значит, можно означить x_i, так что получится формула размера не больше

$$L(f) - \left(\frac{3}{2}\right)\frac{L(f)}{n} \leq \left(1 - \frac{1}{n}\right)^{\frac{3}{2}} L(f)$$

Лемма Субботовской (продолжение док-ва)

Доказательство

- Значит, можно означить x_i, так что получится формула размера не больше

$$L(f) - \left(\frac{3}{2}\right)\frac{L(f)}{n} \leq \left(1 - \frac{1}{n}\right)^{\frac{3}{2}} L(f)$$

- Неравенство Бернулли

$$(1+x)^r \geq (1+rx), x > -1, r \geq 1$$

Лемма Субботовской (продолжение док-ва)

Доказательство

- Значит, можно означить x_i, так что получится формула размера не больше

$$L(f) - \left(\frac{3}{2}\right)\frac{L(f)}{n} \leq \left(1 - \frac{1}{n}\right)^{\frac{3}{2}} L(f)$$

- Неравенство Бернулли

$$(1+x)^r \geq (1+rx), x > -1, r \geq 1$$

- $$L(f') \leq (1 - \frac{1}{n})^{\frac{3}{2}} L(f).$$

Теорема Субботовской

Теорема

Для любой булевой функции $f : \{0,1\}^n \to \{0,1\}$ *и для любого* k, *можно зафиксировать значение* $n - k$ *переменных, так что полученная функция* f' *удовлетворяет*

$$L(f') \leq \left(\frac{k}{n}\right)^{\frac{3}{2}} L(f).$$

Доказательство

Теорема Субботовской

Теорема

Для любой булевой функции $f : \{0,1\}^n \to \{0,1\}$ *и для любого* k, *можно зафиксировать значение* $n - k$ *переменных, так что полученная функция* f' *удовлетворяет*

$$L(f') \leq \left(\frac{k}{n}\right)^{\frac{3}{2}} L(f).$$

Доказательство

- Применяя лемму Субботовской $n - k$ раз, получаем формулу от k переменных с размером не больше

$$L(f)\left(1-\frac{1}{n}\right)^{\frac{3}{2}}\left(1-\frac{1}{n-1}\right)^{\frac{3}{2}}\cdots\left(1-\frac{1}{k+1}\right)^{\frac{3}{2}} = L(f)\left(\frac{k}{n}\right)^{\frac{3}{2}}.$$

Пример: функция четности

Пример

Пример: функция четности

Пример

- Пусть $f = x_1 \oplus x_2 \oplus \cdots \oplus x_n$.

Пример: функция четности

Пример

- Пусть $f = x_1 \oplus x_2 \oplus \cdots \oplus x_n$.
- Зафиксируем все переменные кроме одной, в виду теоремы Субботовской имеем:

Пример: функция четности

Пример

- Пусть $f = x_1 \oplus x_2 \oplus \cdots \oplus x_n$.
- Зафиксируем все переменные кроме одной, в виду теоремы Субботовской имеем:
- $$1 \leq L(f') \leq \left(\frac{1}{n}\right)^{\frac{3}{2}} L(f).$$

Пример: функция четности

Пример

- Пусть $f = x_1 \oplus x_2 \oplus \cdots \oplus x_n$.
- Зафиксируем все переменные кроме одной, в виду теоремы Субботовской имеем:
- $$1 \leq L(f') \leq \left(\frac{1}{n}\right)^{\frac{3}{2}} L(f).$$
- Получаем нижнюю оценку $L(f) \geq n^{\frac{3}{2}}$.

Случайное ограничение

Определение

Случайное ограничение

Определение

- f — булева функция и $X = \{x_1, x_2, \ldots x_n\}$ — множество переменных.

Случайное ограничение

Определение

- f — булева функция и $X = \{x_1, x_2, \ldots x_n\}$ — множество переменных.
- Частичное ограничение это функция $\rho\colon X \to \{0, 1, *\}$. Звездочка показывает, что переменная не означена.

Случайное ограничение

Определение

- f — булева функция и $X = \{x_1, x_2, \ldots x_n\}$ — множество переменных.
- Частичное ограничение это функция $\rho\colon X \to \{0, 1, *\}$. Звездочка показывает, что переменная не означена.
- Каждое такое ограничение естественно порождает функцию:

$$f_\rho = f(\rho(x_1), \ldots \rho(x_n)).$$

Случайное ограничение

Определение

- f — булева функция и $X = \{x_1, x_2, \ldots x_n\}$ — множество переменных.
- Частичное ограничение это функция $\rho\colon X \to \{0, 1, *\}$. Звездочка показывает, что переменная не означена.
- Каждое такое ограничение естественно порождает функцию:

$$f_\rho = f(\rho(x_1), \ldots \rho(x_n)).$$

Пример

Если $f = (x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee x_2) \wedge (x_1 \vee \neg x_3)$.
И $\rho(x_1) = 1, \rho(x_2) = \rho(x_3) = *$, тогда $f_\rho = x_2$.

Случайное ограничение

Определение

- f — булева функция и $X = \{x_1, x_2, \ldots x_n\}$ — множество переменных.
- Частичное ограничение это функция $\rho\colon X \to \{0, 1, *\}$. Звездочка показывает, что переменная не означена.
- Каждое такое ограничение естественно порождает функцию:

$$f_\rho = f(\rho(x_1), \ldots \rho(x_n)).$$

Пример

Если $f = (x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee x_2) \wedge (x_1 \vee \neg x_3)$.
И $\rho(x_1) = 1, \rho(x_2) = \rho(x_3) = *$, тогда $f_\rho = x_2$.

R_k — множество частичных подстановок, которые оставляют k переменных не зафиксированными.

Вероятностный аналог теоремы Субботовской

Теорема

Пусть $f : \{0,1\}^n \to \{0,1\}$ *и* ρ *— случайное ограничение из* R_k*. Тогда с вероятностью не меньше* $\frac{3}{4}$ *, верно*

$$L(f_\rho) \leq 4 \cdot \left(\frac{k}{n}\right)^{\frac{3}{2}} L(f)$$

Доказательство

Вероятностный аналог теоремы Субботовской

Теорема

Пусть $f : \{0,1\}^n \to \{0,1\}$ *и* ρ *— случайное ограничение из* R_k*. Тогда с вероятностью не меньше* $\frac{3}{4}$ *, верно*

$$L(f_\rho) \leq 4 \cdot \left(\frac{k}{n}\right)^{\frac{3}{2}} L(f)$$

Доказательство

- Мат. ожидание размера новой формулы не более:

$$\left(\frac{k}{n}\right)^{\frac{3}{2}} L(f)$$

Вероятностный аналог теоремы Субботовской

Теорема

Пусть $f : \{0,1\}^n \to \{0,1\}$ *и* ρ *— случайное ограничение из* R_k*. Тогда с вероятностью не меньше* $\frac{3}{4}$ *, верно*

$$L(f_\rho) \leq 4 \cdot \left(\frac{k}{n}\right)^{\frac{3}{2}} L(f)$$

Доказательство

- Мат. ожидание размера новой формулы не более:

$$\left(\tfrac{k}{n}\right)^{\frac{3}{2}} L(f)$$

- Используя неравенство Маркова

$$Pr(|X| \geq a) \leq \frac{M|X|}{a}.$$

Вероятностный аналог теоремы Субботовской

Теорема

Пусть $f : \{0,1\}^n \to \{0,1\}$ *и* ρ *— случайное ограничение из* R_k*. Тогда с вероятностью не меньше* $\frac{3}{4}$ *, верно*

$$L(f_\rho) \leq 4 \cdot \left(\frac{k}{n}\right)^{\frac{3}{2}} L(f)$$

Доказательство

- Мат. ожидание размера новой формулы не более:

$$\left(\tfrac{k}{n}\right)^{\frac{3}{2}} L(f)$$

- Используя неравенство Маркова

$$Pr(|X| \geq a) \leq \frac{M|X|}{a}.$$

- Получаем требуемое. □

План лекции

1. Размер и глубина формулы
2. Квадратичная нижняя оценка для универсальной функции
3. Случайные ограничения, нижняя оценка Субботовской
4. Нижняя оценка Андреева

Универсальная функция

Определение

Рассмотрим универсальную функцию, порожденную функцией четности

$$\oplus(u_1, \ldots u_m) = u_1 \oplus u_2 \oplus \cdots \oplus u_m$$

Универсальная функция

Определение

Рассмотрим универсальную функцию, порожденную функцией четности

$$\oplus(u_1, \ldots u_m) = u_1 \oplus u_2 \oplus \cdots \oplus u_m$$

$$U_n^{\oplus} : \{0,1\}^{2n} \to \{0,1\}, n = 2^r, n = rm$$

Универсальная функция

Определение

Рассмотрим универсальную функцию, порожденную функцией четности

$$\oplus(u_1, \dots u_m) = u_1 \oplus u_2 \oplus \cdots \oplus u_m$$

$$U_n^{\oplus} : \{0,1\}^{2n} \to \{0,1\}, n = 2^r, n = rm$$

$$x = \begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,m} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{r,1} & x_{r,2} & \cdots & x_{r,m} \end{pmatrix}$$

$$U_n^{\oplus}(x, y) = U_n(\bigoplus_{j=1}^{m} x_{1j}, \bigoplus_{j=1}^{m} x_{2j}, \cdots \bigoplus_{j=1}^{m} x_{rj}, y)$$

Оценка Андреева

Теорема

$$L(U_n^{\oplus}) \geq n^{\frac{5}{2}-o(1)}.$$

Доказательство

Оценка Андреева

Теорема

$$L(U_n^{\oplus}) \geq n^{\frac{5}{2}-o(1)}.$$

Доказательство

- Возьмем функцию h со сложностью не меньше

$$\frac{2^{r-1}}{\log r} = \frac{n}{2 \log \log n}$$

Оценка Андреева

Теорема

$$L(U_n^{\oplus}) \geq n^{\frac{5}{2}-o(1)}.$$

Доказательство

- Возьмем функцию h со сложностью не меньше

$$\frac{2^{r-1}}{\log r} = \frac{n}{2 \log \log n}$$

- Существует $b \in \{0,1\}^n$, что

$$f(x) := U_n^{\oplus}(x, b) = h(\bigoplus_{j=1}^{m} x_{1j}, \bigoplus_{j=1}^{m} x_{2j}, \cdots \bigoplus_{j=1}^{m} x_{rj})$$

Оценка Андреева

Теорема

$$L(U_n^{\oplus}) \geq n^{\frac{5}{2}-o(1)}.$$

Доказательство

- Возьмем функцию h со сложностью не меньше

$$\frac{2^{r-1}}{\log r} = \frac{n}{2\log\log n}$$

- Существует $b \in \{0,1\}^n$, что

$$f(x) := U_n^{\oplus}(x,b) = h(\bigoplus_{j=1}^{m} x_{1j}, \bigoplus_{j=1}^{m} x_{2j}, \cdots \bigoplus_{j=1}^{m} x_{rj})$$

- Рассмотрим случайное ограничение $\rho \in R_k$, где $k = \lceil r \ln 4r \rceil$.

Оценка Андреева (продолжение док-ва)

Лемма

Если $\rho \in R_k, k = \lceil r \ln(4r) \rceil$, *то*

$$Pr(\rho \textit{ присваивает } * \textit{ в каждом ряду } x) \geq \frac{3}{4}$$

Доказательство

Оценка Андреева (продолжение док-ва)

Лемма

Если $\rho \in R_k, k = \lceil r \ln(4r) \rceil$, *то*

$$Pr(\rho \textit{ присваивает } * \textit{ в каждом ряду } x) \geq \frac{3}{4}$$

Доказательство

- Каждая переменная означена * с вероятностью $C_{n-1}^{k-1} / C_n^k = \frac{k}{n}$.

Оценка Андреева (продолжение док-ва)

Лемма

Если $\rho \in R_k, k = \lceil r \ln(4r) \rceil$, *то*

$$Pr(\rho \text{ присваивает } * \text{ в каждом ряду } x) \geq \frac{3}{4}$$

Доказательство

- Каждая переменная означена * с вероятностью $C_{n-1}^{k-1} / C_n^k = \frac{k}{n}$.
- Вероятность существования ряда без $*$ не больше:

$$r \cdot \left(1 - \frac{k}{n}\right)^m \leq r \cdot e^{-\frac{km}{n}} \leq re^{-\ln(4r)} = \frac{1}{4} \ .$$

□

Оценка Андреева (продолжение док-ва)

Лемма

Если $\rho \in R_k, k = \lceil r \ln(4r) \rceil$, *то*

$$Pr(\rho \textit{ присваивает } * \textit{ в каждом ряду } x) \geq \frac{3}{4}$$

Доказательство

- Каждая переменная означена * с вероятностью $C_{n-1}^{k-1}/C_n^k = \frac{k}{n}$.
- Вероятность существования ряда без $*$ не больше:

$$r \cdot \left(1 - \frac{k}{n}\right)^m \leq r \cdot e^{-\frac{km}{n}} \leq re^{-\ln(4r)} = \frac{1}{4} \ .$$

□

Учитывая теорему Субботовской, получаем:

$$Pr[L(f_\rho) \leq 4 \left(\frac{k}{n}\right)^{1.5} L(f)] \geq \frac{3}{4}.$$

Оценка Андреева (продолжение док-ва)

Оценка Андреева (продолжение док-ва)

- Имеем

$$Pr(\rho \text{ присваивает } * \text{ в каждом ряду } x) \geq \frac{3}{4}$$

$$Pr[L(f_\rho) \leq 4\left(\frac{k}{n}\right)^{1.5} L(f)] \geq \frac{3}{4}$$

Оценка Андреева (продолжение док-ва)

- Имеем

$$Pr(\rho \text{ присваивает } * \text{ в каждом ряду } x) \geq \frac{3}{4}$$

$$Pr[L(f_\rho) \leq 4\left(\frac{k}{n}\right)^{1.5} L(f)] \geq \frac{3}{4}$$

- Значит существует ограничение ρ, удовлетворяющее двум условиям (внутри скобок).

Оценка Андреева (продолжение док-ва)

- Имеем

$$Pr(\rho \text{ присваивает } * \text{ в каждом ряду } x) \geq \frac{3}{4}$$

$$Pr[L(f_\rho) \leq 4\left(\frac{k}{n}\right)^{1.5} L(f)] \geq \frac{3}{4}$$

- Значит существует ограничение ρ, удовлетворяющее двум условиям (внутри скобок).
-

$$L(f_\rho) \geq L(h).$$

Оценка Андреева (продолжение док-ва)

Напомним $k = \lceil r \ln(4r) \rceil = O(\log n \log\log n)$.
Получаем

$$L(U_n^{\oplus}) \geq L(f) \geq \frac{1}{4}\left(\frac{n}{k}\right)^{1.5} L(f_\rho)$$

$$\geq \frac{1}{4}\left(\frac{n}{k}\right)^{1.5} L(h)$$

$$\geq \frac{1}{4}\left(\frac{n}{k}\right)^{1.5} \frac{n}{2\log\log n}$$

$$\geq n^{5/2-o(1)}$$

Кубическая оценка

Определение

p-случайное ограничение — это когда переменным присваиваем значение $0, 1$ с вероятностью $\frac{1-p}{2}$ и значение $*$ с вероятностью p.

Теорема (Hastad 1998)

Если применить p-случайное ограничение к формуле де Моргана размера L, тогда в среднем размер полученной формулы будет не больше $O(p^2 L)$.

Теорема (Hastad 1998)

$$L(U_n^{\oplus}) \geq n^{3-o(1)}.$$

Спасибо за внимание!