

2.2 Сложность булевых функций в классе поляризованных полиномов

Начнем с определений. Будем через $l(P)$ обозначать длину, т.е. число слагаемых, полинома P . Пусть $f(\tilde{x}^n) \in \mathbb{P}_2$. Введем функционал

$$l_{\text{п.п.}}(f) = \min_{\tilde{\delta} \in E_2^n} P_f^{\tilde{\delta}},$$

обозначающий минимальную длину поляризованного полинома для функции f . Значение $l_{\text{п.п.}}(f)$ называется *сложностью функции f в классе поляризованных полиномов*. Также рассмотрим функцию

$$L_{\text{п.п.}}(n) = \max_{f \in \mathbb{P}_2(n)} l_{\text{п.п.}}(f),$$

характеризующую сложность "самой сложной функции" от n переменных в классе поляризованных полиномов. Функция $L_{\text{п.п.}}(n)$ называется *функцией Шеннона сложности в классе поляризованных полиномов*.

В 1995 году Н.А.Перязев установил точное значение функции $L_{\text{п.п.}}(n)$. Оказывается, класс поляризованных полиномов "в полтора раза лучше" для представления булевых функций, чем класс полиномов Жегалкина.

Теорема 2.3 ([5]).

$$L_{\text{п.п.}}(n) = \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor. \quad (2.1)$$

Доказательство. Сначала докажем, что для любой функции $f \in \mathbb{P}_2(n)$ выполнено неравенство

$$L_{\text{п.п.}}(f) \leq \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor. \quad (2.2)$$

Проведем доказательство индукцией по n .

Если $n = 1$, то $L(f) = 1 \leq \left\lfloor \frac{2}{3} \cdot 2^1 \right\rfloor$.

Пусть $n \geq 1$, и $L_{\text{п.п.}}(n) \leq \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor$. Пусть $f(\tilde{x}^{n+1})$ — произвольная булева функция. Для $\sigma \in E_2$ обозначим $f_\sigma(x_2, \dots, x_{n+1}) = f(\sigma, x_2, \dots, x_{n+1})$. Запишем очевидные равенства:

$$\begin{aligned} f(x_1, \dots, x_{n+1}) &= \bar{x}_1 \cdot f_0 \oplus x_1 \cdot f_1 = \\ &= \bar{x}_1(f_0 \oplus f_1) \oplus f_1 = \\ &= x_1(f_0 \oplus f_1) \oplus f_0. \end{aligned} \quad (2.3)$$

Положим $f' = f_0 \oplus f_1$. По предположению индукции, найдется вектор $\tilde{\delta}'$ такой, что

$$l(P_{f'}^{\tilde{\delta}'}) \leq \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor \leq \frac{2}{3} \cdot 2^n.$$

Для $\sigma \in E_2$ положим $P'_\sigma = P_{f'_\sigma}^{\tilde{\delta}'}$. Имеем

$$f = \bar{x}_1 \cdot P'_0 \oplus x_1 \cdot P'_1. \quad (2.4)$$

Пусть найдется ЭК, встречающаяся в обоих полиномах P'_0 и P'_1 — вынесем ее в качестве отдельного слагаемого в правой части равенства (2.4). Например, пусть $P'_0 = K \oplus P''_0$ и $P'_1 = K \oplus P''_1$. Тогда

$$\begin{aligned} f &= \bar{x}_1 \cdot (K \oplus P''_0) \oplus x_1 \cdot (K \oplus P''_1) = \\ &= \bar{x}_1 \cdot P''_0 \oplus x_1 \cdot P''_1 \oplus \bar{x}_1 \cdot K \oplus x_1 \cdot K = \\ &= \bar{x}_1 \cdot P''_0 \oplus x_1 \cdot P''_1 \oplus K. \end{aligned}$$

Если в полиномах P_0'' и P_1'' найдутся одинаковые ЭК, снова вынесем их отдельно. Так будем действовать до тех пор, пока не получим для f представление

$$f = \bar{x}_1 \cdot P_0 \oplus x_1 \cdot P_1 \oplus P_2,$$

где в полиномах P_0 , P_1 и P_2 уже не будет одинаковых слагаемых. Теперь заметим, что

$$f' = P_0' \oplus P_1' = P_0 \oplus P_1, \quad (2.5)$$

то есть $P_0 \oplus P_1$ — это $\tilde{\delta}'$ -поляризованный полином для f' . Вектор $\tilde{\delta}'$ выбирался так, что $l(P_0 \oplus P_1) \leq \frac{2}{3} \cdot 2^n$. Хотя бы один из полиномов P_0 , P_1 имеет длину, не превосходящую

$$\frac{1}{2} \cdot l(P_0 \oplus P_1) = \frac{2^n}{3}.$$

Предположим для определенности, что $l(P_0) \leq \frac{2^n}{3}$. Возьмем $\tilde{\delta} = (0, \tilde{\delta}')$. Из (2.3), (2.5), а также из равенства $P_0' = P_0 \oplus P_2$, получаем:

$$f = x_1 \cdot (f_0 \oplus f_1) \oplus f_0 = x_1 \cdot (P_0 \oplus P_1) \oplus P_0 \oplus P_2.$$

Поскольку полиномы P_0 , P_1 и P_2 содержат различные слагаемые, их суммарная длина не превосходит 2^n . Кроме того, $l(P_0) = \frac{2^n}{3}$. Поэтому длина полинома, получающегося при раскрытии скобок в выражении

$$x_1 \cdot (P_0 \oplus P_1) \oplus P_0 \oplus P_2,$$

не превосходит $\frac{1}{3} \cdot 2^n + 2^n = \frac{2}{3} \cdot 2^{n+1}$. Нетрудно видеть, что этот полином является $\tilde{\delta}$ -поляризованным полиномом, реализующим функцию f . Таким образом, индуктивный переход завершен и неравенство $L_{\text{п.п.}}(n) \leq \lfloor \frac{2}{3} \cdot 2^n \rfloor$ доказано.

Осталось доказать неравенство

$$L_{\text{п.п.}}(n) \geq \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor. \quad (2.6)$$

Рассмотрим функции f_n , g_n и h_n , задаваемые рекурсивно следующим образом: Если $n = 1$, то $f_1 = 1$, $g_1 = \bar{x}_1$, $h_1 = x_1$. Если $n \geq 1$, то

$$\begin{aligned} f_{n+1} &= \bar{x}_{n+1} \cdot f_n \oplus x_{n+1} \cdot g_n, \\ g_{n+1} &= \bar{x}_{n+1} \cdot g_n \oplus x_{n+1} \cdot h_n, \\ h_{n+1} &= \bar{x}_{n+1} \cdot h_n \oplus x_{n+1} \cdot f_n. \end{aligned} \quad (2.7)$$

Покажем, что для любого фиксированного вектора $\tilde{\delta}$ из чисел $l(P_{f_n}^{\tilde{\delta}})$, $l(P_{g_n}^{\tilde{\delta}})$, $l(P_{h_n}^{\tilde{\delta}})$

два равны $\frac{2^{n+1}-1}{3}$, и одно равно $\frac{2^{n+1}+2}{3}$, когда n нечетно,

два равны $\frac{2^{n+1}+1}{3}$, и одно равно $\frac{2^{n+1}-2}{3}$, если n четно (из этого сразу следует (2.6)).

В случае, когда $n = 1$ и $n = 2$ это свойство проверяется, например, перебором. Пусть $n \geq 2$, и пусть $\tilde{\delta} = (\delta', \delta_{n+1}) \in E_2^{n+1}$. По индукции легко доказать (и это предлагается проделать в качестве упражнения), что $f_n \oplus g_n \oplus h_n = 0$, откуда $f_n \oplus g_n = h_n$. Запишем цепочку равенств

$$\begin{aligned} f_{n+1} &= \bar{x}_{n+1} \cdot f_n \oplus x_{n+1} \cdot g_n = \\ &= x_{n+1} \cdot f_n \oplus f_n \oplus x_{n+1} \cdot g_n = \\ &= x_{n+1} \cdot (f_n \oplus g_n) \oplus f_n = \\ &= x_{n+1} \cdot h_n \oplus f_n. \end{aligned}$$

Аналогично можно доказать равенство $f_{n+1} = \bar{x}_{n+1} \cdot h_n \oplus g_n$. Для функций g_{n+1} и h_{n+1} тем же способом получают аналогичные представления. Окончательно имеем:

$$\begin{aligned} f_{n+1} &= x_{n+1} \cdot h_n \oplus f_n = \bar{x}_{n+1} \cdot h_n \oplus g_n, \\ g_{n+1} &= x_{n+1} \cdot f_n \oplus g_n = \bar{x}_{n+1} \cdot f_n \oplus h_n, \\ h_{n+1} &= x_{n+1} \cdot g_n \oplus h_n = \bar{x}_{n+1} \cdot g_n \oplus f_n. \end{aligned}$$

Отсюда видно, что если $\delta_{n+1} = 0$, то

$$\begin{aligned} l(P_{f_{n+1}}^{\tilde{\delta}}) &= l(P_{h_n}^{\tilde{\delta}'}) + l(P_{f_n}^{\tilde{\delta}'}), \\ l(P_{g_{n+1}}^{\tilde{\delta}}) &= l(P_{f_n}^{\tilde{\delta}'}) + l(P_{g_n}^{\tilde{\delta}'}), \\ l(P_{h_{n+1}}^{\tilde{\delta}}) &= l(P_{g_n}^{\tilde{\delta}'}) + l(P_{h_n}^{\tilde{\delta}'}). \end{aligned}$$

Если же $\delta_{n+1} = 1$, то

$$\begin{aligned} l(P_{f_{n+1}}^{\tilde{\delta}}) &= l(P_{h_n}^{\tilde{\delta}'}) + l(P_{g_n}^{\tilde{\delta}'}), \\ l(P_{g_{n+1}}^{\tilde{\delta}}) &= l(P_{f_n}^{\tilde{\delta}'}) + l(P_{h_n}^{\tilde{\delta}'}), \\ l(P_{h_{n+1}}^{\tilde{\delta}}) &= l(P_{g_n}^{\tilde{\delta}'}) + l(P_{f_n}^{\tilde{\delta}'}). \end{aligned}$$

Эти равенства завершают (проверьте!) индуктивный переход, а значит и доказательство неравенства (2.6).

Из (2.2) и (2.6) следует (2.1). Теорема доказана. $\square$

Примечание. Функции f_n, g_n, h_n , определяемые из (2.7), являются единственными функциями, сложность которых в точности равняется $\lfloor \frac{2}{3} \cdot 2^n \rfloor$. Подумайте, как это можно доказать.

Упражнение 6. Для функции $h_3(\tilde{x}^3)$, определяемой по формуле (2.7), запишите поляризованный полином длины 5.

Глава 3

Реализация булевых функций обобщенными полиномами

3.1 Сложность булевых функций в классе обобщенных полиномов

Обозначим через $\mathcal{P}(n)$ множество всех обобщенных полиномов от переменных из $\{x_1, \dots, x_n\}$. Как и в предыдущем параграфе, введем функции сложности:

$$l(f) = \min_{P_f} l(P_f)$$

$$L_{\text{о.п.}}(n) = \max_{f \in \mathbb{P}_2(n)} l(f) \text{ — функция Шеннона сложности в классе обобщенных полиномов.}$$

В данном параграфе приводятся лучшие известные на сегодняшний день (ноябрь 2006 г.) оценки для функции $L_{\text{о.п.}}(n)$, причем верхняя оценка получена совсем недавно, а нижняя — почти 40 лет назад. С доказательства нижней оценки мы и начнем этот параграф.

Теорема 3.1 ([11]).

$$L_{\text{о.п.}}(n) \geq \frac{2^n}{n \log_2 3}. \quad (3.1)$$

Доказательство. Пусть $L_{\text{о.п.}}(n) = L$. Всего существует 3^n ЭК от n переменных. Поэтому число полиномов длины не больше L от n переменных не превосходит $(3^n)^L$. Число булевых функций от n переменных равно 2^{2^n} . Очевидно, число полиномов не должно быть меньше числа функций, иначе найдется функция, которую реализовать полиномом длины $\leq L$ не получится — вопреки определению $L_{\text{о.п.}}(n)$.

Получаем $3^{nL} \geq 2^{2^n}$, откуда сразу следует утверждение теоремы. $\square$

Упражнение 7. Покажите, что с помощью идеи из доказательства теоремы 3.1 порядок оценки (3.1) нельзя улучшить, даже оценивая число полиномов длины не больше L точно, как сумму

$$\sum_{i=0}^L \binom{3^n}{i}.$$

Теперь получим существенно менее тривиальную верхнюю оценку для $L_{\text{о.п.}}(n)$. Для этого нам потребуется сначала дать несколько новых определений.

Для всякого набора $\tilde{\alpha} \in E_2^n$ определим его *тень*

$$s(\tilde{\alpha}) = \{\tilde{\beta} \mid \tilde{\beta} \leq \tilde{\alpha}, |\tilde{\beta}| = |\tilde{\alpha}| - 1\}.$$

Для множества наборов T тень определяется следующим образом:

$$s(T) = \bigcup_{\tilde{\alpha} \in T} s(\tilde{\alpha}).$$

Множество $T \subseteq E_2^n$ назовем *затеняющим*, если $s(T) = E_2^n \setminus \{\tilde{1}\}$.

Будем говорить, что монотонная элементарная конъюнкция K *соответствует* набору $\tilde{\alpha}$, если $\text{ind}(K) = \text{ind}(\tilde{\alpha})$.

Набор $\tilde{\alpha}$ *затеняет* набор $\tilde{\beta}$, если $\tilde{\beta} \in s(\tilde{\alpha})$.

Пример 3.1. Множество $T = \{(111), (011), (110), (001)\}$ является затеняющим в E_2^3 . Наборам этого множества соответствуют ЭК $x_1x_2x_3$, x_2x_3 , x_1x_2 , и x_3 .

Упражнение 8. Найдите в E_2^4 затеняющее множество мощности 7.

Теорема 3.2 ([3]). Если в E_2^n найдется затеняющее множество мощности l , то для любой функции от n переменных существует реализующий ее обобщенный полином длины не большей, чем $(l+1)$.

Доказательство. Пусть $T = \{\tilde{\alpha}^{(1)}, \tilde{\alpha}^{(2)}, \dots, \tilde{\alpha}^{(l)}\} \subseteq E_2^n$ — затеняющее множество. Будем считать, что наборы в T упорядочены по невозрастанию, то есть $\tilde{\alpha}^{(1)} = \tilde{1}$, и при $i < j$ наборы $\tilde{\alpha}^{(i)}$ и $\tilde{\alpha}^{(j)}$ либо несравнимы, либо $\tilde{\alpha}^{(i)} > \tilde{\alpha}^{(j)}$. Через $K^{(m)}$ будем обозначать ЭК, соответствующую набору $\tilde{\alpha}^{(m)}$.

Пусть $f(\tilde{x}^n) \in \mathbb{P}_2(n)$ — произвольная функция. Пусть P_0 — полином Жегалкина для функции $f(\tilde{x}^n) \oplus K^{(1)} \oplus K^{(2)} \oplus \dots \oplus K^{(l)}$. Приведем явный алгоритм преобразования полинома P_0 в обобщенный полином длины не больше $(l+1)$ для f . Алгоритм состоит из l шагов. Опишем шаг с номером $m \geq 1$:

Пусть $\text{ind}(K^{(m)}) = \{i_1, \dots, i_{r_m}\}$. Построим конъюнкцию $\hat{K}^{(m)} = x_{i_1}^{\sigma_1} \cdot \dots \cdot x_{i_{r_m}}^{\sigma_{r_m}}$, где

$$\sigma_s = \begin{cases} 0, & \text{если в } P_{m-1} \text{ найдется ЭК } K \text{ такая, что } K^{(m)} = K \cdot x_{r_s} \\ 1, & \text{иначе.} \end{cases}$$

Пусть $P(\hat{K}^{(m)})$ — полином Жегалкина для $\hat{K}^{(m)}$. Результатом шага с номером m является полином

$$P_m = P_{m-1} \oplus \hat{K}^{(m)} \oplus K^{(m)} \oplus P(\hat{K}^{(m)}).$$

После l шагов алгоритма мы получаем полином P_l . Он, очевидно, реализует функцию f , поскольку на каждом шаге m мы прибавляем к полиному P_{m-1} некоторый полином, реализующий функцию $K^{(m)}$. Начали мы с полинома P_0 , реализующего $f(\tilde{x}^n) \oplus K^{(1)} \oplus K^{(2)} \oplus \dots \oplus K^{(l)}$, значит в результате получим полином, реализующий f .

Осталось показать, что длина P_l не превосходит $(l+1)$. Основная идея состоит в том, что на шаге с номером m мы удаляем из полинома P_{m-1} все монотонные ЭК ранга $(r(K^{(m)}) - 1)$ такие, что соответствующие им наборы затеняются набором $\tilde{\alpha}^{(m)}$. Правда, приходится платить за это добавлением ЭК $\hat{K}^{(m)}$ и некоторого числа слагаемых ранга не больше $(r(K^{(m)}) - 2)$. Из определения затеняющего множества следует, что для всякого $k < n$ на каком-то шаге m_k мы удалим все монотонные ЭК ранга k , а все слагаемые ранга $\geq k$ будут исчерпываться конъюнкциями $\hat{K}^{(1)}, \dots, \hat{K}^{(m_k)}$, и, возможно, конъюнкцией $x_1x_2 \cdot \dots \cdot x_n$ ранга n (поскольку, если она была в полиноме P_0 , избавиться от нее мы не сможем). На шаге l мы придем, таким образом, либо к полиному

$$P_l = \hat{K}^{(1)} \oplus \dots \oplus \hat{K}^{(l)},$$

либо к полиному

$$P_l = x_1 \cdot \dots \cdot x_n \oplus \hat{K}^{(1)} \oplus \dots \oplus \hat{K}^{(l)}.$$

В любом случае, в P_l будет не более $(l+1)$ слагаемых. Теорема доказана. $\square$

Пример 3.2. Приведем пример работы описанного в теореме 3.2 алгоритма.

Пусть $f(x_1, x_2, x_3) = x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1 \oplus x_3 \oplus 1$. Будем использовать затеняющее множество из примера 3.1. Имеем

$$P_0 = x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1 \oplus x_3 \oplus 1 \oplus x_1x_2x_3 \oplus x_2x_3 \oplus x_1x_2 \oplus x_3 = x_1x_3 \oplus x_2x_3 \oplus x_1 \oplus 1$$

Шаг 1.

$$\tilde{\alpha}^{(1)} = (111)$$

$$K^{(1)} = x_1x_2x_3$$

$$\hat{K}^{(1)} = \bar{x}_1\bar{x}_2x_3$$

$$P(\hat{K}^{(1)}) = x_1x_2x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3$$

$$P_1 = x_1x_3 \oplus x_2x_3 \oplus x_1 \oplus 1 \oplus \bar{x}_1\bar{x}_2x_3 \oplus x_1x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3 = \bar{x}_1\bar{x}_2x_3 \oplus x_1 \oplus x_3 \oplus 1$$

Шаг 2.

$$\tilde{\alpha}^{(2)} = (011)$$

$$K^{(2)} = x_2x_3$$

$$\hat{K}^{(2)} = \bar{x}_2x_3$$

$$P(\hat{K}^{(2)}) = x_2x_3 \oplus x_3$$

$$P_2 = \bar{x}_1\bar{x}_2x_3 \oplus x_1 \oplus x_3 \oplus 1 \oplus \bar{x}_2x_3 \oplus x_2x_3 \oplus x_2x_3 \oplus x_3 = \bar{x}_1\bar{x}_2x_3 \oplus \bar{x}_2x_3 \oplus x_1 \oplus 1$$

Шаг 3.

$$\tilde{\alpha}^{(3)} = (110)$$

$$K^{(3)} = x_1x_2$$

$$\hat{K}^{(3)} = x_1\bar{x}_2$$

$$P(\hat{K}^{(3)}) = x_1x_2 \oplus x_1$$

$$P_3 = \bar{x}_1\bar{x}_2x_3 \oplus \bar{x}_2x_3 \oplus x_1 \oplus 1 \oplus x_1\bar{x}_2 \oplus x_1x_2 \oplus x_1x_2 \oplus x_1 = \bar{x}_1\bar{x}_2x_3 \oplus \bar{x}_2x_3 \oplus x_1\bar{x}_2 \oplus 1$$

Шаг 4.

$$\tilde{\alpha}^{(4)} = (001)$$

$$K^{(4)} = x_3$$

$$\hat{K}^{(4)} = \bar{x}_3$$

$$P(\hat{K}^{(4)}) = x_3 \oplus 1$$

$$P_4 = \bar{x}_1\bar{x}_2x_3 \oplus \bar{x}_2x_3 \oplus x_1\bar{x}_2 \oplus 1 \oplus \bar{x}_3 \oplus x_3 \oplus x_3 \oplus 1 = \bar{x}_1\bar{x}_2x_3 \oplus \bar{x}_2x_3 \oplus x_1\bar{x}_2 \oplus \bar{x}_3$$

Итак, $f = \bar{x}_1\bar{x}_2x_3 \oplus \bar{x}_2x_3 \oplus x_1\bar{x}_2 \oplus \bar{x}_3$. Заметим, что на самом деле $l(f) = 2$, поскольку можно указать, например, такой полином длины 2 для $f: x_1\bar{x}_2\bar{x}_3 \oplus \bar{x}_3$ (а полиномом длины ≤ 1 функцию f реализовать невозможно).

Теорема 3.2 позволяет получать оценки для функции $L_{\text{о.п.}}(n)$ путем построения в E_2^n затеняющих множеств “небольшой мощности”.

Любое затеняющее множество $T \subseteq E_2^n$ можно разбить на “слои” $T_1, \dots, T_n$. Слой T_i содержит все наборы ранга i из T , и затеняет все наборы ранга $(i-1)$ из E_2^n . Решать задачу поиска T можно, очевидно, по шагам, строя множества T_i последовательно. При этом выбор множества T_i никак не зависит от выбора других множеств T_j , $j \neq i$. Поэтому для решения задачи о нахождении множества T нам достаточно уметь решать подзадачи такого вида: найти множество T_i наборов ранга i , затеняющее все наборы ранга $i-1$. Воспользуемся для решения подзадач *градиентным алгоритмом*:

Шаг 1. Полагаем $T_i^{(1)} = \{\tilde{\alpha}\}$, где $\tilde{\alpha}$ — произвольный набор ранга i .

Шаг k . Пусть результатом предыдущего шага является $T_i^{(k-1)}$. Если в E_2^n нет набора, который не затеняется множеством $T_i^{(k-1)}$, то полагаем $T_i = T_i^{(k-1)}$ и алгоритм завершается. В противном случае, полагаем $T_i^{(k)} = T_i^{(k-1)} \cup \{\tilde{\alpha}\}$, где $\tilde{\alpha}$ — произвольный набор, затеняющий наибольшее число наборов из множества $E_2^n \setminus s(T_i^{(k-1)})$.

Описанный алгоритм, очевидно, строит множество T_i с нужными свойствами, и число шагов алгоритма не превосходит мощность множества наборов ранга $(i-1)$. Оценим мощность полученного множества T_i . Введем обозначения:

$t = \binom{n}{i}$ — мощность множества R_i всех наборов ранга i .

$m = \binom{n}{i-1}$ — мощность множества R_{i-1} всех наборов ранга $(i-1)$.

$p = n - i + 1$ — число наборов ранга i , затеняющих фиксированный набор ранга $(i-1)$.

Теорема 3.3. *Если множество T_i построено градиентным алгоритмом, то*

$$|T_i| \leq 1 + \frac{t}{p} \ln\left(\frac{emp}{t}\right), \quad (3.2)$$

где $e = 2,71828\dots$

Доказательство. Пусть δ_k — доля наборов из R_{i-1} , остающихся незатененными после k -го шага алгоритма. Будем считать по определению, что $\delta_0 = 1$. Положим $\gamma = \frac{p}{t}$. Среднее число наборов из $R_{i-1} \setminus s(T_i^k)$, затеняемых $(t-k)$ наборами из T_i^k , оценивается снизу как

$$\delta_k \frac{mp}{t-k}.$$

Градиентный алгоритм на $(k+1)$ -ом шаге выбирает набор, затеняющий *максимальное*, а значит, не меньшее, чем $\delta_k \frac{mp}{t-k}$ число наборов из $R_{i-1} \setminus s(T_i^k)$. Поэтому

$$m\delta_k - m\delta_{k+1} \geq \delta_k \frac{mp}{t-k}.$$

Отсюда

$$\delta_{k+1} \leq \delta_k \left(1 - \frac{p}{t-k}\right) \leq \delta_k (1 - \gamma). \quad (3.3)$$

Из (3.3) по индукции получаем, что $\delta_k \leq (1 - \gamma)^k$. Поскольку на каждом шаге алгоритма в множество, полученное на предыдущем шаге, добавляется ровно один набор, то общее число шагов не превосходит величины $(k + m\delta_k)$, причем это верно для любого k . В результате получаем, что

$$|T_i| \leq k + m\delta_k \leq k + m(1 - \gamma)^k \leq k + me^{-\gamma k}. \quad (3.4)$$

В неравенстве в (3.4) мы воспользовались тем, что $1 - x \leq e^{-x}$ для любого действительного x .

Полагая в (3.4) число k равным $\left\lceil \frac{1}{\gamma} \ln(\gamma m) \right\rceil$, получаем (3.2). $\square$

Следствие 3.1. *При любом $n \geq 1$ в E_2^n существует затеняющее множество T мощности не больше*

$$2 \cdot \frac{2^n}{n} (1 + \ln n) - 1.$$

Доказательство. Пусть $n \geq 5$. Построим множество T как объединение n множеств T_i , каждое из которых получено градиентным алгоритмом. Имеем

$$\begin{aligned} |T| &= \sum_{i=1}^n |T_i| \leq \sum_{i=1}^n \left(1 + \frac{\binom{n}{i}}{n-i+1} \ln\left(\frac{e \binom{n-1}{i-1} (n-i+1)}{\binom{n}{i}}\right)\right) = \\ &= \sum_{i=0}^{n-1} \left(1 + \frac{\binom{n}{i+1}}{i+1} \ln\left(\frac{e \binom{n}{i+1} (i+1)}{\binom{n}{i+1}}\right)\right) = \\ &= \sum_{i=0}^{n-1} \left(1 + \frac{\binom{n}{i+1}}{i+1} \ln(e(n-i))\right) = \\ &= \sum_{i=1}^n \left(1 + \frac{\binom{n+1}{i}}{n+1} (1 + \ln(n-i+1))\right) \leq \\ &\leq n + \frac{2^{n+1}}{n+1} (1 + \ln n) \leq \\ &\leq \frac{2^{n+1}}{n} (1 + \ln n) - 1. \end{aligned}$$

Ограничение $n \geq 5$ нам понадобилось только для обеспечения последнего неравенства в приведенной выше цепочке.

Если $n \leq 4$, то достаточно воспользоваться результатами примера 3.1 и упражнения 8. $\square$

Из теоремы 3.2 и следствия 3.1 мгновенно вытекает следующее утверждение, дающее лучшую по порядку известную на сегодняшний день (декабрь 2006) верхнюю оценку для $L_{o.n.}(n)$.

Теорема 3.4.

$$L_{o.n.}(n) \leq 2 \cdot \frac{2^n}{n} (1 + \ln n).$$

3.2 Приближенная реализация булевых функций

В этом параграфе мы займемся получением оценок для длины и ранга полиномов Жегалкина, *приближенно* реализующих булевы функции. Уточним сначала, что мы будем понимать под приближенной реализацией. Везде далее разделе рассматриваются только полиномы Жегалкина.

Расстоянием между функциями $f(\tilde{x}^n)$ и $g(\tilde{x}^n)$ (обозначается $d(f, g)$) называется расстояние Хемминга $d(\tilde{f}, \tilde{g})$ между векторами-столбцами значений этих функций. Иными словами, $d(f, g)$ — это число наборов, на которых значения функций f и g отличаются.

Пусть $\delta \in [0, 1]$ — действительная константа. Будем говорить, что функция $g(\tilde{x}^n)$ является δ -приближением функции $f(\tilde{x}^n)$, если

$$\frac{d(f, g)}{2^n} \leq \delta,$$

иначе говоря, доля наборов, на которых f и g совпадают, должна быть не меньше $1 - \delta$.

Если полином P реализует какое-то δ -приближение функции f , то будем говорить, что P реализует f с точностью δ .

Заметим, что, вообще говоря, один и тот же полином может приближенно реализовывать несколько функций, и для одной функции может быть несколько δ -приближений. Любая функция является 1-приближением любой другой функции. 0-приближением всякой функции является только она сама.

Введем функции сложности

$$\begin{aligned} r_\delta(f) &= \min_{g - \delta\text{-пр. } f} r(P_g) \\ l_\delta(f) &= \min_{g - \delta\text{-пр. } f} l(P_g) \\ r_\delta(n) &= \max_{f \in \mathbb{P}_2(n)} r_\delta(f) \\ l_\delta(n) &= \max_{f \in \mathbb{P}_2(n)} l_\delta(f) \end{aligned}$$

В данном параграфе мы установим асимптотику функции $r_\delta(n)$ и получим оценку сверху для $l_\delta(n)$. Вначале нам потребуется доказать некоторые оценки для биномиальных коэффициентов и их сумм.

Лемма 1. *При любых r и n таких, что $2r < n$, выполнено неравенство*

$$\binom{n}{r} \leq \frac{2^n}{n - 2r}. \quad (3.5)$$

Доказательство. При $2r < n$ имеем

$$\begin{aligned} & \sum_{i=0}^{\lfloor (n-1)/2 \rfloor} \binom{n}{i} \geq \sum_{i=r}^{\lfloor (n-1)/2 \rfloor} \binom{n}{i} \geq \\ & \geq \sum_{i=r}^{\lfloor (n-1)/2 \rfloor} \binom{n}{r} = \binom{n}{r} \cdot \left(\left\lfloor \frac{n-1}{2} \right\rfloor - r + 1 \right) \geq \\ & \geq \binom{n}{r} \cdot \left(\frac{n}{2} - r \right). \end{aligned} \quad (3.6)$$