Московский Государственный Университет
имени М. В. Ломоносова

Факультет Вычислительной Математики и Кибернетики

Булевы функции и полиномы

Лектор — к.ф.-м.н. С. Н. Селезнева
Составители — А. Б. Дайняк, М. С. Шуплецов

Москва, 2006

Глава 1

Введение

1.1 Основные определения

Будем обозначать через E_k множество $\{0, 1, 2, \ldots, k-1\}$ первых k целых неотрицательных чисел. Наборы (векторы) длины n, компонентами которых являются элементы из E_k, будем, как правило, обозначать греческими буквами $\widetilde{\alpha}^n$, $\widetilde{\beta}^n$, ... Набор длины n, состоящий из одних нулей, будем обозначать $\widetilde{0}^n$, единичный набор аналогичным образом обозначим $\widetilde{1}^n$. Иногда верхний индекс n будем опускать, если из контекста ясно, какую длину имеет рассматриваемый набор. Компоненты наборов будем обозначать соответствующими греческими буквами с нижними индексами: например, α_i — это i-ая компонента набора $\widetilde{\alpha}$.

На множестве E_k можно ввести стандартный линейный порядок: $0 < 1 < \ldots < k-1$. На множестве E_k^n вводится стандартный частичный порядок:

$$\forall \widetilde{\alpha}^n \, \forall \widetilde{\beta}^n (\widetilde{\alpha} \leqslant \widetilde{\beta} \Leftrightarrow \forall i \in [1, n] (\alpha_i \leqslant \beta_i)).$$

На множестве E_2^n вводится *метрика (расстояние) Хемминга* d:

$$d(\widetilde{\alpha}, \widetilde{\beta}) = |\{i \in [1, n] \mid \alpha_i \neq \beta_i\}|.$$

Для набора $\widetilde{\alpha}$ через $|\widetilde{\alpha}|$ будем обозначать число единичных компонент в $\widetilde{\alpha}$. Число $|\widetilde{\alpha}|$ будем называть рангом набора $\widetilde{\alpha}$. Очевидно, $|\widetilde{\alpha}| = d(\widetilde{\alpha}, \widetilde{0})$.

Индексной характеристикой набора $\widetilde{\alpha}$ называется множество $\mathrm{ind}(\widetilde{\alpha}) = \{i \mid \widetilde{\alpha}_i = 1\}$. При этом $\mathrm{ind}(1) = \emptyset$.

Булевой функцией (или *функцией алгебры логики*) называется отображение $f \colon E_2^n \to E_2$. Множество всех булевых функций от n переменных обозначается $\mathbb{P}_2(n)$. Множество всех булевых функций обозначается через $\mathbb{P}_2$. Не ограничивая общности, будем полагать, что всякая функция из $\mathbb{P}_2(n)$ зависит от переменных из множества $\{x_1, \ldots, x_n\}$.

Элементарная конъюнкция (ЭК) ранга r — это выражение вида $x_{i_1}^{\sigma_1} \ldots x_{i_r}^{\sigma_r}$, где все x_{i_j} — различные булевы переменные. Будем считать тождественными ЭК, в которые входят одни и те же литералы (возможно, в разном порядке).

Монотонной ЭК называется ЭК, в которую все переменные входят без отрицаний. Будем считать, что 1 — это монотонная ЭК ранга 0. Ранг ЭК K будем обозначать $r(K)$. *Индексной характеристикой* монотонной ЭК K называется множество $\mathrm{ind}(K) = \{i \mid x_i \text{ входит в } K\}$.

Пусть $K_1, \ldots, K_l$ — элементарные конъюнкции. Выражение вида $K_1 \oplus \ldots \oplus K_l$ называется *(обобщенной) полиномиальной формой*, или просто *(обобщенным) полиномом*.

Полином, в который входят только монотонные ЭК, называется *полиномом Жегалкина*.

Полином, в который каждая переменная входит либо только с отрицанием, либо только без отрицания, называется *поляризованным полиномом*.

Мы будем отождествлять полиномы, в которые входят одни и те же ЭК (возможно, в разном порядке). Кроме того, будем считать, что пустой полином реализует функцию, тождественно равную нулю.

Под обозначением P_f будем понимать полином (Жегалкина, поляризованный, обобщенный), реализующий функцию f.

Глава 2

Полиномы Жегалкина и поляризованные полиномы

2.1 Простейшие факты

Теорема 2.1 ([9]). *Для каждой функции из $\mathbb{P}_2$ существует единственный реализующий её полином Жегалкина.*

Доказательство. 1. Существование. Пусть $f \in \mathbb{P}_2(n)$. Функцию f можно представить в виде

$$\begin{aligned} f(x_1, \ldots, x_n) &= x_1 \cdot f(1, x_2, \ldots, x_n) \oplus \overline{x}_1 \cdot f(0, x_2, \ldots, x_n) = \\ &= x_1 \cdot f(1, x_2, \ldots, x_n) \oplus x_1 \cdot f(0, x_2, \ldots, x_n) \oplus f(0, x_2, \ldots, x_n). \end{aligned}$$

Функции $f(0, x_2, \ldots, x_n)$ и $f(1, x_2, \ldots, x_n)$ можно, в свою очередь, разложить по переменной x_2, и т.д. Наконец, мы придем к выражению, представляющему собой сумму конъюнкций переменных x_i и констант. Упростив его, используя тождества $0 \oplus K = 1 \cdot K = K$, $0 \cdot K = 0$ и $K \oplus K = 0$, получим полином Жегалкина, реализующий f.

2. Единственность. Пусть P_1 и P_2 — различные полиномы Жегалкина, реализующие одну и ту же функцию. Тогда полином $P = P_1 \oplus P_2$ является непустым полиномом Жегалкина, реализующим тождественный нуль. Пусть $K = x_{i_1} \cdot \ldots \cdot x_{i_r}$ — ЭК минимального ненулевого ранга r в полиноме P. Присвоим значение 0 всем переменным, не входящим в K, и значение 1 — всем переменным из K, кроме x_{i_1}. Получим функцию от единственной переменной x_{i_1}, которая будет *существенно* зависеть от x_{i_1}, что противоречит предположению о том, что полином P реализует константу 0. □

Следствие 2.1. *Для каждой функции из $f \in \mathbb{P}_2(n)$ и каждого вектора поляризации $\widetilde{\delta}^n$ существует единственный реализующий ее поляризованный по вектору $\widetilde{\delta}^n$ полином.*

В соответствии с теоремой 2.1 и следствием к ней полиномы P_f и $P_f^{\widetilde{\delta}}$ для произвольного вектора поляризации $\widetilde{\delta}$ однозначно определены ($f \in \mathbb{P}_2(n)$).

Упражнение 1. *Дайте другое доказательство единственности в теореме 2.1. Для этого установите равенство числа различных функций и числа различных полиномов Жегалкина от n переменных.*

Упражнение 2. *Докажите следствие к теореме 2.1.*

Упражнение 3. *Постройте по схеме п. 1 доказательства теоремы 2.1 полином Жегалкина для функции $f(\widetilde{x}^3)$, заданной столбцом значений:* (01001011).

Итак, для каждой функции можно найти единственный полином Жегалкина. Сразу же возникает вопрос: каким способом можно его построить? Хотя доказательство теоремы 2.1 фактически дает способ нахождения полинома Жегалкина для произвольной функции, его нельзя считать удовлетворительным из-за его громоздкости. Тем же недостатком обладает и метод неопределенных коэффициентов. Оказывается, однако, существует простой, быстрый способ преобразования столбца значений функции в вектор коэффициентов ее полинома Жегалкина.

Каждую монотонную ЭК от переменных $x_1, \ldots, x_n$ можно закодировать двоичным вектором $\widetilde{\kappa} = (\kappa_1, \ldots, \kappa_n)$, где $\kappa_i = 1$ тогда и только тогда, когда переменная x_i входит в K. Число, двоичная запись которого определяется ветором $\widetilde{\kappa}$, назовем номером конъюнкции K. Всякий полином Жегалкина от переменных $x_1, \ldots, x_n$ можно закодировать ветором $\widetilde{c}$ длины 2^n, в котором $c_i = 1$ тогда и только тогда, когда ЭК с номером i входит в этот полином. Через $\widetilde{c}_f$ будем обозначать вектор коэффициентов полинома Жегалкина функции f, а через $\widetilde{f}$ — вектор-столбец значений этой функции.

Пусть $n \geqslant 1$. Определим по рекурсии преобразование $\Pi_n \colon E_2^{2^n} \to E_2^{2^n}$:

Если $n = 1$, то $\Pi_n(\alpha_0, \alpha_1) = (\alpha_0, \alpha_0 \oplus \alpha_1)$.

Если $n \geqslant 1$ и $\widetilde{\alpha} = (\widetilde{\beta}, \widetilde{\gamma})$, где $\widetilde{\beta}$ и $\widetilde{\gamma}$ — векторы длины 2^n, то $\Pi_{n+1}(\widetilde{\alpha}) = (\Pi_n(\widetilde{\beta}), \Pi_n(\widetilde{\beta}) \oplus \Pi_n(\widetilde{\gamma}))$, где суммирование векторов ведется покоординатно.

Теорема 2.2 ([1]). *Пусть $f \in \mathbb{P}_2(n)$. Тогда $\Pi_n(\widetilde{f}) = \widetilde{c}_f$.*

Доказательство. Доказательство проводится индукцией по числу n переменных функции f. □

Аналогично преобразованию Π_n можно построить преобразование $\Pi_n^{\widetilde{\delta}}$, которое преобразует столбец значений функции в вектор коэффициентов ее $\widetilde{\delta}$–поляризованного полинома.

Если $n = 1$ и $\widetilde{\delta} = (\delta_0)$, то

$$\Pi_n^{\widetilde{\delta}}(\alpha_0, \alpha_1) = \begin{cases} (\alpha_0, \alpha_0 \oplus \alpha_1), & \text{если } \delta_0 = 0, \\ (\alpha_1, \alpha_0 \oplus \alpha_1), & \text{если } \delta_0 = 1. \end{cases}$$

Пусть $n \geqslant 1$. Если $\widetilde{\delta} = (\delta_0, \widetilde{\delta}')$ — вектор длины $(n+1)$, и $\widetilde{\alpha} = (\widetilde{\beta}, \widetilde{\gamma})$, то

$$\Pi_{n+1}^{\widetilde{\delta}}(\widetilde{\beta}, \widetilde{\gamma}) = \begin{cases} (\Pi_n^{\widetilde{\delta}'}(\widetilde{\beta}), \Pi_n^{\widetilde{\delta}'}(\widetilde{\beta}) \oplus \Pi_n^{\widetilde{\delta}'}(\widetilde{\gamma})), & \text{если } \delta_0 = 0, \\ (\Pi_n^{\widetilde{\delta}'}(\widetilde{\gamma}), \Pi_n^{\widetilde{\delta}'}(\widetilde{\beta}) \oplus \Pi_n^{\widetilde{\delta}'}(\widetilde{\gamma})), & \text{если } \delta_0 = 1. \end{cases}$$

Доказательство "правильности функционирования" преобразования $\Pi_n^{\widetilde{\delta}}$ может быть легко проведено по индукции.

Упражнение 4. *Для функции из упражнения 3 постройте в соответствии с преобразованием $\Pi_3^{(010)}$ поляризованный по вектору (010) полином.*

Итак, мы видим, что поляризованные полиномы и полиномы Жегалкина во многом схожи. В чем же тогда мы выигрываем при использовании поляризованных полиномов для задания булевых функций? Преимущество состоит в свободе выбора вектора поляризации. Очевидно, что для всякого фиксированного вектора поляризации можно подобрать функцию $f \in \mathbb{P}_2(n)$ такую, что длина (число слагаемых) полинома $P_f^{\widetilde{\delta}}$ будет равна 2^n — то есть будет максимально возможной. Но если нам задана функция f, то мы можем подобрать вектор $\widetilde{\delta}$ так, чтобы максимально сократить размер полинома $P_f^{\widetilde{\delta}}$. Подробно этот вопрос рассматривается в следующем параграфе.

Упражнение 5. *Для какой функции от n переменных полином Жегалкина имеет максимальную длину (2^n)? Как по заданному вектору поляризации $\widetilde{\delta}$ найти столбец значений функции, для которой длина $\widetilde{\delta}$–поляризованного полинома максимальна?*

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 $f(\widetilde{x}^n) \in \mathbb{P}_2$. Введем функционал

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

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 "са́мой 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])**.**

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

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

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

Проведем доказательство индукцией по n.

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

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

$$\begin{array}{rcll} f(x_1, \ldots, x_{n+1}) = & \overline{x}_1 \cdot f_0 \oplus x_1 \cdot f_1 & = \\ = & \overline{x}_1 (f_0 \oplus f_1) \oplus f_1 & = \\ = & x_1 (f_0 \oplus f_1) \oplus f_0. \end{array} \tag{2.3}$$

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

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

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

$$f = \overline{x}_1 \cdot P'_0 \oplus x_1 \cdot P'_1. \tag{2.4}$$

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

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

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

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

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

$$f' = P_0' \oplus P_1' = P_0 \oplus P_1, \tag{2.5}$$

то есть $P_0 \oplus P_1$ — это $\widetilde{\delta}'$–поляризованный полином для f'. Вектор $\widetilde{\delta}'$ выбирался так, что $l(P_0 \oplus P_1) \leqslant \frac{2}{3} \cdot 2^n$. 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 $l(P_0) \leqslant \frac{2^n}{3}$. Возьмем $\widetilde{\delta} = (0, \widetilde{\delta}')$. 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 $\widetilde{\delta}$–поляризованным полиномом, реализующим функцию f. Таким образом, индуктивный переход завершен и неравенство $L_{\text{п.п.}}(n) \leqslant \left\lfloor \frac{2}{3} \cdot 2^n \right\rfloor$ доказано.

Осталось доказать неравенство

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

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

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

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

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 $n \geqslant 2$, и пусть $\widetilde{\delta} = (\widetilde{\delta}', \delta_{n+1}) \in E_2^{n+1}$. 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

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

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

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

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

$$l(P^{\tilde{\delta}}_{f_{n+1}}) = l(P^{\tilde{\delta}'}_{h_n}) + l(P^{\tilde{\delta}'}_{f_n}),$$
$$l(P^{\tilde{\delta}}_{g_{n+1}}) = l(P^{\tilde{\delta}'}_{f_n}) + l(P^{\tilde{\delta}'}_{g_n}),$$
$$l(P^{\tilde{\delta}}_{h_{n+1}}) = l(P^{\tilde{\delta}'}_{g_n}) + l(P^{\tilde{\delta}'}_{h_n}).$$

Если же $\delta_{n+1} = 1$, то

$$l(P^{\tilde{\delta}}_{f_{n+1}}) = l(P^{\tilde{\delta}'}_{h_n}) + l(P^{\tilde{\delta}'}_{g_n}),$$
$$l(P^{\tilde{\delta}}_{g_{n+1}}) = l(P^{\tilde{\delta}'}_{f_n}) + l(P^{\tilde{\delta}'}_{h_n}),$$
$$l(P^{\tilde{\delta}}_{h_{n+1}}) = l(P^{\tilde{\delta}'}_{g_n}) + l(P^{\tilde{\delta}'}_{f_n}).$$

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

Из (2.2) и (2.6) следует (2.1). Теорема доказана. □

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

Упражнение 6. *Для функции $h_3(\widetilde{x}^3)$, 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 $\{x_1, \ldots, x_n\}$. Как и в предыдущем параграфе, введем функции сложности:

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

$L_{\text{о.п.}}(n) = \max_{f \in \mathbb{P}_2(n)} l(f)$ — 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])**.**

$$L_{o.n.}(n) \geqslant \frac{2^n}{n \log_2 3}. \tag{3.1}$$

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 $\leqslant L$ не получится — вопреки определению $L_{\text{о.п.}}(n)$.

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

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 $\widetilde{\alpha} \in E_2^n$ определим его *тень*

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

Для множества наборов T тень определяется следующим образом:

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

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

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

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

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

Пусть $f(\widetilde{x}^n) \in \mathbb{P}_2(n)$ — произвольная функция. Пусть P_0 — полином Жегалкина для функции $f(\widetilde{x}^n) \oplus K^{(1)} \oplus K^{(2)} \oplus \ldots \oplus K^{(l)}$. 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 $m \geqslant 1$:

Пусть $\mathrm{ind}(K^{(m)}) = \{i_1, \ldots, i_{r_m}\}$. Построим конъюнкцию $\widehat{K}^{(m)} = x_{i_1}^{\sigma_1} \cdot \ldots \cdot x_{i_{r_m}}^{\sigma_{r_m}}$, 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 $P(\widehat{K}^{(m)})$ — полином Жегалкина для $\widehat{K}^{(m)}$. Результатом шага с номером m является полином

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

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 $f(\widetilde{x}^n) \oplus K^{(1)} \oplus K^{(2)} \oplus \ldots \oplus K^{(l)}$, 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 $\widetilde{\alpha}^{(m)}$. Правда, приходится платить за это добавлением ЭК $\widehat{K}^{(m)}$ 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 $\geqslant k$ будут исчерпываться конъюнкциями $\widehat{K}^{(1)}, \ldots, \widehat{K}^{(m_k)}$, и, возможно, конъюнкцией $x_1x_2 \cdot \ldots \cdot x_n$ 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

$$P_l = \widehat{K}^{(1)} \oplus \ldots \oplus \widehat{K}^{(l)},$$

либо к полиному

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

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

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.

$$\widetilde{\alpha}^{(1)} = (111)$$
$$K^{(1)} = x_1x_2x_3$$
$$\widehat{K}^{(1)} = \overline{x}_1\overline{x}_2x_3$$
$$P(\widehat{K}^{(1)}) = x_1x_2x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3$$
$$P_1 = x_1x_3 \oplus x_2x_3 \oplus x_1 \oplus 1 \oplus \overline{x}_1\overline{x}_2x_3 \oplus x_1x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3 = \overline{x}_1\overline{x}_2x_3 \oplus x_1 \oplus x_3 \oplus 1$$

Шаг 2.

$$\widetilde{\alpha}^{(2)} = (011)$$
$$K^{(2)} = x_2x_3$$
$$\widehat{K}^{(2)} = \overline{x}_2x_3$$
$$P(\widehat{K}^{(2)}) = x_2x_3 \oplus x_3$$
$$P_2 = \overline{x}_1\overline{x}_2x_3 \oplus x_1 \oplus x_3 \oplus 1 \oplus \overline{x}_2x_3 \oplus x_2x_3 \oplus x_2x_3 \oplus x_3 = \overline{x}_1\overline{x}_2x_3 \oplus \overline{x}_2x_3 \oplus x_1 \oplus 1$$

Шаг 3.

$$\widetilde{\alpha}^{(3)} = (110)$$
$$K^{(3)} = x_1x_2$$
$$\widehat{K}^{(3)} = x_1\overline{x}_2$$
$$P(\widehat{K}^{(3)}) = x_1x_2 \oplus x_1$$
$$P_3 = \overline{x}_1\overline{x}_2x_3 \oplus \overline{x}_2x_3 \oplus x_1 \oplus 1 \oplus x_1\overline{x}_2 \oplus x_1x_2 \oplus x_1x_2 \oplus x_1 = \overline{x}_1\overline{x}_2x_3 \oplus \overline{x}_2x_3 \oplus x_1\overline{x}_2 \oplus 1$$

Шаг 4.

$$\widetilde{\alpha}^{(4)} = (001)$$
$$K^{(4)} = x_3$$
$$\widehat{K}^{(4)} = \overline{x}_3$$
$$P(\widehat{K}^{(4)}) = x_3 \oplus 1$$
$$P_4 = \overline{x}_1\overline{x}_2x_3 \oplus \overline{x}_2x_3 \oplus x_1\overline{x}_2 \oplus 1 \oplus \overline{x}_3 \oplus x_3 \oplus x_3 \oplus 1 = \overline{x}_1\overline{x}_2x_3 \oplus \overline{x}_2x_3 \oplus x_1\overline{x}_2 \oplus \overline{x}_3$$

Итак, $f = \overline{x}_1\overline{x}_2x_3 \oplus \overline{x}_2x_3 \oplus x_1\overline{x}_2 \oplus \overline{x}_3$. Заметим, что на самом деле $l(f) = 2$, поскольку можно указать, например, такой полином длины 2 для f: $x_1\overline{x}_2\overline{x}_3 \oplus \overline{x}_3$ (а полиномом длины $\leqslant 1$ 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" $T_1, \ldots, T_n$. 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 $T_i^{(1)} = \{\widetilde{\alpha}\}$, где $\widetilde{\alpha}$ — 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 $T_i^{(k)} = T_i^{(k-1)} \cup \{\widetilde{\alpha}\}$, где $\widetilde{\alpha}$ — 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*

$$|T_i| \leqslant 1 + \frac{t}{p}\ln(\frac{emp}{t}), \tag{3.2}$$

где $e = 2,71828\ldots$

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

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

Отсюда

$$\delta_{k+1} \leqslant \delta_k(1 - \frac{p}{t-k}) \leqslant \delta_k(1-\gamma). \tag{3.3}$$

Из (3.3) по индукции получаем, что $\delta_k \leqslant (1-\gamma)^k$. 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

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

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

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

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

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

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

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

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

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

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

Теорема 3.4.

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

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 $f(\widetilde{x}^n)$ и $g(\widetilde{x}^n)$ (обозначается $d(f,g)$) называется расстояние Хемминга $d(\widetilde{f},\widetilde{g})$ 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 $g(\widetilde{x}^n)$ является δ–приближением функции $f(\widetilde{x}^n)$, если

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

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*

$$\binom{n}{r} \leqslant \frac{2^n}{n-2r}. \tag{3.5}$$

Доказательство. При $2r < n$ имеем

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

С другой стороны, из равенств $\binom{n}{i} = \binom{n}{n-i}$ и

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n$$

следует, что

$$\sum_{i=0}^{\lfloor (n-1)/2 \rfloor} \binom{n}{i} \leqslant 2^{n-1}. \tag{3.7}$$

Из (3.6) и (3.7) следует (3.5). □

Лемма 2. *Пусть* $0 \leqslant r < \frac{n}{2}$. *Тогда*

$$\sum_{i=0}^{r} \binom{n}{i} \leqslant \frac{n-r}{(n-2r)^2} \cdot 2^n. \tag{3.8}$$

Доказательство. Пусть $r > 0$. Заметим, что для любого $i < r$

$$\binom{n}{i} = \binom{n}{r} \cdot \frac{r(r-1)\cdot \ldots \cdot (i+1)}{(n-r+1)(n-r+2)\cdot \ldots \cdot (n-i)} \leqslant \binom{n}{r} \cdot \frac{r^{r-i}}{(n-r+1)^{r-i}}.$$

Отсюда

$$\begin{aligned} \sum_{i=0}^{r} \binom{n}{i} &\leqslant \tbinom{n}{r} \cdot \sum_{i=0}^{r} \frac{r^{r-i}}{(n-r+1)^{r-i}} = \binom{n}{r} \cdot \sum_{i=0}^{r} \frac{r^i}{(n-r+1)^i} \leqslant \\ &\leqslant \tbinom{n}{r} \cdot \sum_{i=0}^{\infty} \left(\frac{r}{n-r}\right)^i = \binom{n}{r} \cdot \frac{1}{1-\frac{r}{n-r}} = \\ &= \tbinom{n}{r} \cdot \tfrac{n-r}{n-2r}. \end{aligned}$$

Итак,

$$\sum_{i=0}^{r} \binom{n}{i} \leqslant \binom{n}{r} \cdot \frac{n-r}{n-2r}. \tag{3.9}$$

Осталось воспользоваться неравенством (3.5).

Мы действовали в предположении, что $r > 0$. Но если $r = 0$, то неравенство (3.8) также, очевидно, выполнено. □

Следствие 3.2. *Учитывая то, что* $\binom{n}{i} = \binom{n}{n-i}$, *из леммы 2 следует, что при* $\frac{n}{2} < r \leqslant n$ *выполнено неравенство*

$$\sum_{i=r}^{n} \binom{n}{i} \leqslant \frac{r}{(2r-n)^2} \cdot 2^n.$$

Лемма 3. *Пусть* $\delta \in (0, \frac{1}{2})$ *— фиксированная константа. Тогда существует такая константа* $\epsilon < 1$, *что при всех достаточно больших* n *и всех* $r \leqslant \delta n$ *выполнено неравенство*

$$\sum_{i=0}^{r} \binom{n}{i} \leqslant 2^{\epsilon n}.$$

Доказательство. Случай $r = 0$ тривиален. Пусть $r > 0$. Положим $t = \frac{r}{n-r}$. Учитывая то, что $t < 1$, имеем

$$t^{-r}(1+t)^n = t^{-r} \sum_{i=0}^{n} \binom{n}{i} t^i \geqslant \sum_{i=0}^{r} \binom{n}{i} t^{i-r} \geqslant \sum_{i=0}^{r} \binom{n}{i}.$$

Учитывая, что $t^{-r}(1+t)^n = \frac{n^n}{r^r(n-r)^{n-r}}$, получаем:

$$\sum_{i=0}^{r}\binom{n}{i} \leqslant \frac{n^n}{r^r(n-r)^{n-r}} = 2^{n\cdot H(\frac{r}{n})},$$

где функция H — *функция двоичной энтропии*, задаваемая при $x \in [0,1]$ равенством[1]

$$H(x) = -x\log_2 x - (1-x)\log_2(1-x).$$

В качестве несложного упражнения, предоставляем читателю показать, что функция $H(x)$ возрастает на интервале $(0, \frac{1}{2})$, и что $H(x) < 1$ при $x \in (0, \frac{1}{2})$. Из этого непосредственно будет следовать доказываемое утверждение — в качестве искомого ϵ достаточно будет взять любое число из интервала $[H(\delta), 1)$. □

Теперь у нас есть все необходимые технические средства для доказательства следующей теоремы.

Теорема 3.5 ([2, 6]). *$r_\delta(n) = 0$ при $\delta \geqslant \frac{1}{2}$.*
$r_\delta(n) = n$ при $\delta = 0$.
$r_\delta(n) \sim \frac{1}{2}n$ при $\delta \in (0, \frac{1}{2})$.

Доказательство. Доказательство в случае $\delta = 0$ и $\delta \geqslant \frac{1}{2}$ предоставляется читателю.

Пусть $\delta \in (0, \frac{1}{2})$. Получим сначала асимптотическое неравенство $r_\delta(n) \lesssim \frac{n}{2}$. Пусть $f(\widetilde{x}^n)$ — произвольная функция. Пусть $r \in [1, n]$ — некоторое натуральное число. Пусть P — полином, получающийся из полинома Жегалкина для f отбрасыванием всех слагаемых, ранг которых больше r. Подберем r так, чтобы полином P реализовывал f с точностью δ. Заметим, что полином P реализует функцию, совпадающую с f на всех наборах ранга, не превосходящего r. Поэтому достаточно взять такое r, для которого число наборов ранга больше r составляет от числа всех наборов долю, не большую δ. Этому условию удовлетворяют такие значения r, при которых

$$\sum_{i=r}^{n}\binom{n}{i} \leqslant \delta\cdot 2^n.$$

Для выполнения этого неравенства, в силу следствия 3.2, достаточно, чтобы r удовлетворяло неравенствам $r > \frac{n}{2}$ и

$$\frac{r}{(2r-n)^2} \leqslant \delta. \tag{3.10}$$

При $r > \frac{n}{2}$ неравенство (3.10) эквивалентно неравенству

$$n - r \leqslant \delta(n-2r)^2.$$

Этому квадратичному неравенству удовлетворяет, например,

$$r = \left\lceil \frac{n}{2} + \frac{1+\sqrt{8\delta n+1}}{8\delta} \right\rceil \lesssim \frac{n}{2}.$$

Отсюда $r_\delta(n) \lesssim \frac{n}{2}$.

Нижнюю оценку для $r_\delta(n)$ получим мощностным методом. Число всех полиномов Жегалкина ранга не больше r равно

$$2^{\sum_{i=0}^{r}\binom{n}{i}}.$$

Число функций, приближаемых с точность δ одним полиномом, равно

$$\sum_{i=0}^{\lfloor\delta\cdot 2^n\rfloor}\binom{2^n}{i}.$$

[1] При этом полагают $0\cdot\log_2 0 = 0$.

Число булевых функций от n переменных равно 2^{2^n}, поэтому должно быть выполнено неравенство

$$2^{\sum_{i=0}^{r_\delta(n)}\binom{n}{i}} \cdot \sum_{i=0}^{\lfloor\delta\cdot 2^n\rfloor}\binom{2^n}{i} \geqslant 2^{2^n}. \tag{3.11}$$

По лемме 3, при достаточно больших n

$$\sum_{i=0}^{\lfloor\delta\cdot 2^n\rfloor}\binom{2^n}{i} \leqslant 2^{\epsilon\cdot 2^n},$$

где $\epsilon < 1$. Поэтому при больши́х n для выполнения (3.11) необходимо, чтобы $r_\delta(n)$ удовлетворяло неравенству

$$\sum_{i=0}^{r_\delta(n)}\binom{n}{i} > (1-\epsilon)\cdot 2^n.$$

Это неравенство, в свою очередь, в силу леммы 2, влечет

$$\frac{n - r_\delta(n)}{(n-2r_\delta(n))^2} \geqslant 1-\epsilon.$$

Решая это неравенство, получаем

$$r_\delta(n) \geqslant \frac{n}{2} - \frac{1+\sqrt{8(1-\epsilon)n+1}}{8(1-\epsilon)} \gtrsim \frac{n}{2}.$$

Объединяя верхнюю и нижнюю оценки, получаем $r_\delta(n) \sim \frac{1}{2}n$. Теорема доказана. □

Лемма 4. *Для любого непустого множества $S \subseteq E_2^n$ и любой функции $f \in \mathbb{P}_2(n)$ найдется полином Жегалкина P, обладающий свойствами*

1. *P совпадает с f на множестве S.*
2. *Для любой ЭК K из P найдется набор $\widetilde{\alpha} \in S$ такой, что $\mathrm{ind}(K) = \mathrm{ind}(\widetilde{\alpha})$.*

Доказательство. Доказательство проведем индукцией по мощности множества S. Если $S = \{\widetilde{\alpha}\}$, и $\mathrm{ind}(\widetilde{\alpha}) = \{i_1, \ldots, i_r\}$, то полагаем

$$P = \begin{cases} 0, & \text{если } f(\widetilde{\alpha}) = 0, \\ x_{i_1}\cdot\ldots\cdot x_{i_r}, & \text{если } f(\widetilde{\alpha}) = 1. \end{cases}$$

Пусть $|S| = l+1$ и утверждение леммы верно для всех множеств мощности $1 \ldots, l$. Пусть $\widetilde{\alpha}$ — такой набор из S, что не существует $\widetilde{\beta} \in S$, для которого $\mathrm{ind}(\widetilde{\alpha}) \subset \mathrm{ind}(\widetilde{\beta})$. По предположению существует полином P', совпадающий с f на множестве $S \setminus \{\widetilde{\alpha}\}$. Пусть $\mathrm{ind}(\widetilde{\alpha}) = \{i_1, \ldots, i_r\}$. Нетрудно видеть, что полином

$$P = \begin{cases} P', & \text{если } f(\widetilde{\alpha}) \oplus P'(\widetilde{\alpha}) = 0, \\ x_{i_1}\cdot\ldots\cdot x_{i_r} \oplus P', & \text{если } f(\widetilde{\alpha}) \oplus P'(\widetilde{\alpha}) = 1. \end{cases}$$

удовлетворяет всем свойствам из утверждения леммы. □

Следствие 3.3. *При $\delta \in [0,1]$ справедлива оценка $l_\delta(n) \leqslant (1-\delta)\cdot 2^n + 1$.*

Доказательство. Пусть $f \in \mathbb{P}_2(n)$ — произвольная функция. Выберем произвольное множество $S \subseteq E_2^n$ мощности $\lceil(1-\delta)\cdot 2^n\rceil$. По лемме 4, существует полином P, совпадающий с f на S. Нетрудно видеть, что P имеет длину не больше $\lceil(1-\delta)\cdot 2^n\rceil \leqslant (1-\delta)\cdot 2^n + 1$. Кроме того, P реализует f с точностью δ, поскольку совпадает с f по крайней мере на $\lceil(1-\delta)\cdot 2^n\rceil$ наборах. □

Оценку, которую дает это следствие, можно, оказывается, улучшить вдвое, о чем утверждает следующая теорема.

Теорема 3.6 ([6]). $l_\delta(n) = 1$ *при* $\delta \geqslant \frac{1}{2}$.
$l_\delta(n) = 2^n$ *при* $\delta = 0$.
$l_\delta(n) \leqslant \frac{1}{2}(1-\delta)\cdot 2^n + 1$ *при* $\delta \in (0, \frac{1}{2})$.

Доказательство. Разбор случаев $\delta \geqslant \frac{1}{2}$ и $\delta = 0$ предоставляется читателю.

Пусть $\delta \in (0, \frac{1}{2})$, и $f \in \mathbb{P}_2(n)$ — произвольная функция. Пусть $l_0 = \lceil (1-\delta)\cdot 2^n + 1 \rceil$. Построим множество S по правилу: сначала в S добавим набор $\widetilde{0}$, затем все набора ранга 1, все наборы ранга 2, и т.д., пока не наберем l_0 наборов. При этом если r — максимальный ранг наборов, то S необязательно содержит все наборы ранга r. Множество S обладает тем свойством, что для всякого набора из S все наборы меньшего ранга также принадлежат S. По лемме 4, существует полином P, совпадающий с f на S, длина которого не превосходит l_0. Возможны два случая:

$l(P) \leqslant \frac{1}{2}l_0$. Нетрудно видеть, что по выбору l_0, полином P реализует f с точностью δ.

$l(P) > \frac{1}{2}l_0$. Рассмотрим функцию $h(\widetilde{x}^n) = \overline{x}_1 \cdot \ldots \cdot \overline{x}_n$. Полином Жегалкина P_h для этой функции содержит все монотонные ЭК от переменных $x_1, \ldots, x_n$. Пусть P'_h — полином, полученный из P_h отбрасыванием всех ЭК, соответствующих наборам из $E_2^n \setminus S$. Очевидно, что в силу структуры множества S, полином P'_h реализует функцию, совпадающую с h на S. Но функция h принимает значение 1 только на нулевом наборе. Следовательно, и значение P'_h отличается на S от нуля только на наборе $\widetilde{0}$. Рассмотрим полином $P' = P \oplus P'_h$. Этот полином имеет длину $\leqslant \frac{1}{2}l_0$ и реализует функцию, совпадающую с f на множестве $S \setminus \{\widetilde{0}\}$ мощности $(l_0 - 1)$.

Итак, в любом случае, можно построить полином длины не больше $\frac{1}{2}\lceil (1-\delta)\cdot 2^n + 1 \rceil \leqslant \frac{1}{2}(1-\delta)\cdot 2^n + 1$, реализующий функцию, совпадающую с f на множестве мощности не меньше $\lceil (1-\delta)\cdot 2^n \rceil$. Этот полином будет, очевидно, реализовывать f с точностью δ. □

Глава 4

Распознавание свойств функций, заданных полиномами

4.1 Постановка задачи

Рассмотрим задачу следующего вида. Пусть нам дана функция $f \in \mathbb{P}_2(n)$ и некоторое *свойство* $\mathcal{P}$. Требуется ответить на вопрос: обладает ли f свойством $\mathcal{P}$. Данная глава посвящена оценке сложности алгоритмов, позволяющих решать описанную задачу для фиксированного $\mathcal{P}$. Наиболее естественными свойствами функций является их принадлежность замкнутым классам в $\mathbb{P}_2$, и, прежде всего, *предполным* замкнутым классам.

Проблема получения оценок сложности алгоритмов определения принадлежности функций предполным классам хорошо изучена для случая, когда функции заданы своими векторами значений. Мы же будем рассматривать алгоритмы, на вход которых подается в некоторой кодировке *полином Жегалкина* функции, свойства которой нужно определить. Обозначим через $\mathcal{A}_{\mathcal{P}}(n, l)$ алгоритм, который принимает на вход полином Жегалкина длины l некоторой функции $f \in \mathbb{P}_2(n)$, и на выходе дает ответ «да» или «нет» в зависимости от того, обладает ли f свойством $\mathcal{P}$.

Как и ранее, для функции f через P_f будем обозначать полином Жегалкина, реализующий f. Через $l(P)$ будем обозначать длину полинома P. Введем функции сложности:

$L_{\mathcal{A}}(f)$ — число элементарных операций, которое нужно произвести в соответствии с алгоритмом $\mathcal{A} = \mathcal{A}_{\mathcal{P}}(n, l)$ для распознавания свойства $\mathcal{P}$ функции $f \in \mathbb{P}_2(n)$, задаваемой полиномом длины l.

$L_{\mathcal{A}}(l) = \max_{l(P_f)=l} l_{\mathcal{A}}(f)$ — максимальное число элементарных операций, достаточное для распознавания алгоритмом $\mathcal{A}$ свойства $\mathcal{P}$ функции, заданной полиномом длины l.

В связи с тем, что мы рассматриваем только полиномы Жегалкина, и, соответственно, только монотонные ЭК, мы будем отождествлять ЭК со множествами входящих в них переменных (то есть с индексами этих ЭК). При получении оценок для функции $L_{\mathcal{A}}(l)$ будем рассматривать формальную алгоритмическую модель, содержащую следующие элементарные операции:

- операции присваивания
- подстановка констант в заданную ЭК вместо некоторых переменных
- оператор условного присваивания
- операции над ЭК как над множествами переменных, т.е. операции вида $K := K_1 \cup K_2$, $K := K_1 \cap K_2$, $K := K_1 \setminus K_2$
- операции сравнения ЭК как множеств переменных: $K_1 \subset K_2?$, $K_1 \subseteq K_2?$, $K_1 = K_2?$ и т.д.

Сложность алгоритма равна суммарному числу элементарных операций, выполняемых алгоритмом до получения ответа в худшем случае.

Описанная алгоритмическая модель может показаться искусственной, однако нетрудно видеть, что *полиномиальные* верхние оценки сложности алгоритмов в данной модели приводят к *полиномиальным* верхним оценкам в известных стандартных моделях, например, в классе схем из функциональных элементов (СФЭ), или в классе машин Тьюринга. Вполне естественно исследовать, прежде всего, свойства функций, определяющих их принадлежность предполным классам Поста. Очевидно, распознать линейность функции, а также свойства сохранения нуля и единицы, по полиному Жегалкина можно за линейное время. Нетривиальным остается только распознавание монотонности и самодвойственности функций по их полиномиальным представлениям. Этому и посвящены следующие два параграфа.

4.2 Распознавание монотонности

Цель этого параграфа — построить алгоритм распознавания монотонности функций, задаваемых полиномами фиксированной длины. Напомним, что функция f называется *монотонной*, если для любых наборов $\widetilde{\alpha}$, $\widetilde{\beta}$ таких, что $\widetilde{\alpha} \leqslant \widetilde{\beta}$, выполнено $f(\widetilde{\alpha}) \leqslant f(\widetilde{\beta})$. Набор $\widetilde{\alpha}$ называется *нижней единицей* функции f, если $f(\widetilde{\alpha}) = 1$ и $f(\widetilde{\beta}) = 0$ для всякого набора $\widetilde{\beta} \leqslant \widetilde{\alpha}$. Везде далее будем рассматривать всякое множество монотонных ЭК $K_1, \ldots, K_l$ как частично упорядоченное, с отношением порядка, порожденным отношением включения на множестве $\{\mathrm{ind}(K_1), \ldots, \mathrm{ind}(K_l)\}$. В связи с этим будем говорить о *минимальных* и *максимальных* элементах во множестве $K_1, \ldots, K_l$. Докажем вспомогательную лемму.

Лемма 5. *Пусть $f \in \mathbb{P}_2(n)$ задана полиномом Жегалкина $P_f = K_1 \oplus \ldots \oplus K_l$. Пусть $K_{i_1}, \ldots, K_{i_m}$ — все минимальные элементы во множестве $\{K_1, \ldots, K_l\}$. Тогда между множеством $\{K_{i_1}, \ldots, K_{i_m}\}$ и множеством всех нижних единиц функции f можно установить взаимно однозначное соответствие. При этом ЭК K_{i_j} соответствует нижняя единица $\widetilde{\alpha}_j$ такая, что $\mathrm{ind}(\widetilde{\alpha}_j) = \mathrm{ind}(K_{i_j})$.*

Доказательство. Пусть $K_{i_j} \in \{K_{i_1}, \ldots, K_{i_m}\}$. Тогда на наборе $\widetilde{\alpha}_j$ таком, что $\mathrm{ind}(\widetilde{\alpha}_j) = \mathrm{ind}(K_{i_j})$ слагаемое K_{i_j} в P_f обращается в единицу, а все остальные слагаемые равны нулю. Таким образом, $f(\widetilde{\alpha}_j) = 1$. При этом для всякого набора $\widetilde{\beta}$, меньшего $\widetilde{\alpha}_j$, слагаемое K_{i_j} обнуляется, и все остальные слагаемые по-прежнему равны нулю, значит $f(\widetilde{\beta}) = 0$. Таким образом, $\widetilde{\alpha}_j$ является, по определению, нижней единицей f.

Пусть теперь $\widetilde{\alpha}$ — какая-то нижняя единица функции f. Из определения следует, что она не сравнима со всеми другими нижними единицами f. Поскольку на наборе $\widetilde{\alpha}$ хотя бы одно слагаемое в P_f в нуль не обращается, то на $\widetilde{\alpha}$ не обращается в нуль и какое-то из слагаемых $K_{i_1}, \ldots, K_{i_m}$. Отсюда $\widetilde{\alpha}$ совпадает с одной из нижних единиц $\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_m$. Лемма доказана. □

Упражнение 9. *Найдите все нижние единицы функции $f(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_2x_3 \oplus x_3$.*

Какое максимальное и минимальное число нижних единиц может быть у функции из $\mathbb{P}_2(n)$, заданной полиномом длины l?

Останется ли верным утверждение леммы 5, если отбросить ограничение $f(\widetilde{0}) = 0$?

Обозначим через $f^{i_1, \ldots, i_k}_{\alpha_1, \ldots, \alpha_k}(\widetilde{x}^n)$ функцию, получающуюся из функции f подстановкой констант α_j на места соответствующих переменных x_{i_j}. Непосредственно из определений вытекает следующее утверждение.

Утверждение 4.1. *Функция f монотонна тогда и только тогда, когда для каждой ее нижней единицы $\widetilde{\alpha}$ выполнено $f^{i_1, \ldots, i_k}_{1, \ldots, 1}(\widetilde{x}^n) \equiv 1$, где $\{i_1, \ldots, i_k\} = \mathrm{ind}(\widetilde{\alpha})$.*

Теорема 4.1 ([7])**.** *Существует детерминированный алгоритм, распознающий монотонность функции f по ее полиному Жегалкина P_f за $O(l^3)$ операций, где l — длина полинома P_f.*

Доказательство. Если в P_f есть слагаемое 1, то функция f является монотонной в том и только том случае, если $P_f = 1$. Разбор этого тривиального случая требует выполнения $O(l)$ операций. Пусть теперь $P_f = K_1 \oplus \ldots \oplus K_l$.

Этап 1. Из леммы 5 следует, что для нахождения всех нижних единиц функции f достаточно найти все минимальные элементы во множестве $\{K_1, \ldots, K_l\}$. Укажем схему, по которой это можно сделать. Положим $P := P_f$. Построим множество S_1 следующим образом. Положим вначале $S_1 := \{K_1\}$. Вычеркнем из P слагаемое K_1. Теперь будем просматривать последовательно все слагаемые в P в некотором фиксированном порядке. Пусть просматривается слагаемое K_i, и пусть в этот момент $S_1 = \{K_j\}$.

- Если $K_j < K_i$, то вычеркиваем слагаемое K_i из P и продолжаем просмотр дальше.
- Если $K_j > K_i$, то полагаем $S_1 := \{K_i\}$ и вычеркиваем K_j из P.
- Если же K_j и K_s несравнимы, то продолжаем просмотр дальше.

После окончания просмотра множество S_1 содержит некоторый минимальный элемент K_{i_1}, а в полиноме P нет слагаемых, сравнимых с K_{i_1}. Если полином P пуст, то других минимальных элементов нет. В противном случае, аналогичным образом находим множество $S_2 = \{K_{i_2}\}$, где K_{i_2} — минимальный элемент, и так далее.

В итоге мы найдем все минимальные элементы $K_{i_1}, \ldots, K_{i_m}$. Поскольку $m \leqslant l$, и при поиске очередного минимального элемента нам требуется просмотреть каждое слагаемое в P всего один раз (а слагаемых в P не более l). Отсюда на поиск всех минимальных элементов потребуется $O(l^2)$ элементарных операций алгоритмической модели, описанной в предыдущем параграфе.

Этап 2. Теперь для каждой нижней единицы $\widetilde{\alpha}$, выполняем подстановку констант 1 в P_f на места всех переменных с номерами из $\mathrm{ind}(\widetilde{\alpha})$. Затем упрощаем P_f, используя тождество $K \oplus K = 0$. Если в результате получается полином, тождественно равный 1, то переходим к следующей нижней единице, в противном случае выдаем ответ «нет» (f не монотонна). В случае, если проверены все нижние единицы, выдаем ответ «да» (f монотонна). Корректность ответа обеспечивается утверждением 4.1. Число всех нижних единиц функции f не превосходит l, и для каждой нижней единицы на упрощение полинома требуется не более $O(l^2)$ операций. Отсюда на втором этапе всего необходимо выполнить $O(l^3)$ операций.

Нетрудно видеть, что второй этап является самым трудоемким в алгоритме. Итак, за $O(l^3)$ операций мы нашли ответ на вопрос о монотонности функции f, что и завершает доказательство теоремы. □

Упражнение 10. *Постройте по описанному алгоритму распознавания монотонности набросок схемы из функциональных элементов в базисе* $\{\vee, \wedge, \neg\}$*, сложность которой ограничена полиномом от размера входа. Вход схемы задается вектором длины* $n \cdot l$ *вида*

$$\alpha_{1,1}, \alpha_{1,2}, \ldots, \alpha_{1,n}, \alpha_{2,1}, \alpha_{2,2}, \ldots, \alpha_{2,n}, \ldots, \alpha_{l,1}, \alpha_{l_2}, \ldots, \alpha_{l,n},$$

где $\alpha_{i,j} = 1 \Leftrightarrow x_j \in K_i$*. Схема выдает на выходе* 1 *если и только если функция, задаваемая входным полиномом, монотонна.*

Упражнение 11. *Двойственным к понятию нижней единицы является понятие* верхнего нуля*. Можно ли по функции, заданной полиномом длины* l*, найти все ее нижние нули за полиномиальное по* l *число операций?*

4.3 Распознавание самодвойственности

Перейдем к вопросу о распознавании самодвойственности функций. Распознавание самодвойственности с алгоритмической точки зрения оказывается более сложной задачей, чем распознавание монотонности, и нам придется вначале заняться исследованием свойств четных и нечетных булевых функций.

Функция f назывется четной, если $f(x_1, \ldots, x_n) = f(\overline{x}_1, \ldots, \overline{x}_n)$.

Функция f назывется нечетной, если $f(x_1, \ldots, x_n) = \overline{f}(\overline{x}_1, \ldots, \overline{x}_n)$.

Доказательство трех следующих утверждений предоставляется читателю.

Утверждение 4.2. *Функция $f(\widetilde{x}^n)$ четна (нечетна) тогда и только тогда, когда функция $\overline{f}(\widetilde{x}^n)$ четна (соответственно, нечетна).*

Утверждение 4.3. *Сумма двух четных, или двух нечетных функций является четной функцией. Сумма четной и нечетной функции есть нечетная функция.*

Утверждение 4.4. *Функция $f(\widetilde{x}^n)$ четна тогда и только тогда, когда функция $g(\widetilde{x}^n) = f(\widetilde{x}^n) \oplus x_i$ нечетна.*

Лемма 6. *Пусть $f(x_1, \ldots, x_n) = x_i g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \oplus h(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$. Тогда, если функция f четна, то g тоже четна.*

Доказательство.

$$f(\overline{x}_1, \ldots, \overline{x}_n) = \overline{x}_i g(\overline{x}_1, \ldots, \overline{x}_{i-1}, \overline{x}_{i+1}, \ldots, \overline{x}_n) \oplus h(\overline{x}_1, \ldots, \overline{x}_{i-1}, \overline{x}_{i+1}, \ldots, \overline{x}_n) =$$
$$= x_i g(\overline{x}_1, \ldots, \overline{x}_{i-1}, \overline{x}_{i+1}, \ldots, \overline{x}_n) \oplus (g(\overline{x}_1, \ldots, \overline{x}_{i-1}, \overline{x}_{i+1}, \ldots, \overline{x}_n) \oplus h(\overline{x}_1, \ldots, \overline{x}_{i-1}, \overline{x}_{i+1}, \ldots, \overline{x}_n))$$

Из единственности представления функции f полиномом Жегалкина следует, что

$$g(\overline{x}_1, \ldots, \overline{x}_{i-1}, \overline{x}_{i+1}, \ldots, \overline{x}_n) = g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n),$$

то есть g — четная функция. □

Лемма 7. *Пусть $f(\widetilde{x}^n)$ — четная, не равная тождественно нулю функция. Тогда в P_f найдутся слагаемые K_1 и K_2 (не обязательно различные), для которых $K_1 \cap K_2 = \emptyset$.*

Доказательство. 1. Если $f(\tilde{0}^n) = 1$, то полином P_f содержит слагаемое 1. Выберем $K_1 = K_2 = 1$.

2. Пусть $f(\tilde{0}^n) = 0$, тогда полином P_f не содержит слагаемое 1. Так как $f(\tilde{x}^n)$ не тождественно равная нулю функция, найдется набор $\widetilde{\alpha}$, на котором значение f равно 1. Следовательно, в P_f найдется слагаемое $K_1 \neq 1$, обращающееся на $\widetilde{\alpha}$ в единицу. По определению четной функции, $f(\overline{\widetilde{\alpha}}) = f(\widetilde{\alpha})$. Значит в P_f есть слагаемое K_2, не обращающееся в нуль на наборе $\overline{\widetilde{\alpha}}$. Поэтому

$$\mathrm{ind}(K_2) \subseteq \mathrm{ind}(\overline{\widetilde{\alpha}}) = \{1, 2, \ldots n\} \setminus \mathrm{ind}(\widetilde{\alpha}) \subseteq \{1, 2, \ldots n\} \setminus \mathrm{ind}(K_1),$$

откуда следует, что $\mathrm{ind}(K_1) \cap \mathrm{ind}(K_2) = \emptyset$. □

Лемма 8. *Пусть $f(\widetilde{x}^n)$ — четная, не равная тождественно нулю функция. Пусть K — произвольная монотонная ЭК. Тогда, если в P_f найдется слагаемое L такое, что $K \subseteq L$, то в P_f найдутся слагаемые L_1 и L_2 (не обязательно различные) такие, что $L_1 \cap L_2 = K$.*

Доказательство. Проведем доказательство индукцией по рангу конъюнкции K. Если $r(K) = 0$ (т.е. $K = 1$), то достаточно воспользоваться леммой 7. Предположим теперь, что утверждение леммы верно для всех ЭК ранга, не превосходящего r. Пусть $K' = x_i \cdot K$, где $r(K) = r$. Пусть в P_f есть слагаемое L' такое, что $K' \subseteq L'$. Значит x_i — существенная переменная функции f. Представим f в виде $f(x_1, \ldots, x_n) = x_i g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \oplus h(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$. По лемме 6, функция g — четная. По предположению индукции, в P_g найдутся слагаемые L_1, L_2 такие, что $L_1 \cap L_2 = K$. Но тогда в P_f входят слагаемые $L'_1 = x_i \cdot L_1$ и $L'_2 = x_i \cdot L_2$. Очевидно, $L'_1 \cap L'_2 = K'$, а это и требовалось. □

Теорема 4.2. *Пусть $f(\widetilde{x}^n)$ — четная функция. Тогда тогда длина l и ранг r полинома P_f удовлетворяют неравенству $l \geqslant \sqrt{2^r}$.*

Доказательство. Пусть $f(\widetilde{0}) = 0$. Так как $r(P_f) = r$, то в P_f найдется слагаемое K ранга r. У множества K всего 2^r подмножеств $K_1, \ldots, K_{2^r}$. По лемме 8, для каждого K_i в P_f найдется пара слагаемых L'_i и L''_i, дающих в пересечении это подмножество. Очевидно, при $i \neq j$ пары (L'_i, L''_i) и (L'_j, L''_j) различны. Но всего в P_f можно выбрать не более l^2 различных пар слагаемых. Отсюда и следует утверждение теоремы. □

Следствие 4.1. *Пусть функция f нечетна. Тогда для ранга r и длины l полинома P_f выполнено неравенство $l \geqslant \sqrt{2^r} - 1$.*

Доказательство. По утверждению 4.4, функция $f \oplus x_1$ четна. Применим к этой функции теорему 4.2. □

Пусть K — произвольная монотонная ЭК, P — полином Жегалкина. Обозначим через $i(K, P)$ остаток от деления на 2 мощности множества $\{K' \in P \mid K \subset K'\}$. Справедливо следующее утверждение.

Лемма 9. *1. Функция $f(\widetilde{x}^n)$ является четной тогда и только тогда, когда $i(K, P_f) = 0$ для любой монотонной ЭК K над $\{x_1, \ldots, x_n\}$.*

2. Функция $f(\widetilde{x}^n)$ является нечетной тогда и только тогда, когда $i(K, P_f) = 0$ для любой монотонной ЭК K над $\{x_1, \ldots, x_n\}$, не равной 1, и при этом $i(1, P_f) = 1$.

Доказательство. Докажем критерий четности функций. Пусть $P_f = K_1 \oplus \ldots \oplus K_l$. Пусть $K_i = x_{i_1} \cdot \ldots \cdot x_{i_m}$. Полином $P' = P_{f(\overline{x}_1, \ldots, \overline{x}_n)}$ получается, если заменить каждое слагаемое K_i в P_f на слагаемое $(x_{i_1} \oplus 1) \cdot \ldots \cdot (x_{i_m} \oplus 1)$, и затем раскрыть скобки. Таким образом, каждое слагаемое K_i из P_f дает вклад в P' в виде всех ЭК, содержащихся в K_i. Отсюда видно, что после упрощения в P' останутся те и только те ЭК, которые содержались в нечетном числе слагаемых полинома P_f (а этому условию удовлетворяют, во-первых, те K_i, для которых $i(K, P_f) = 0$, и во-вторых не содержащиеся в P_f ЭК, для которых $i(K, P_f) = 1$). Но для того, чтобы функция $f(\widetilde{x}^n)$ была четной, необходимо и достаточно, чтобы P' совпадал с P_f. То есть описанному условию должны удовлетворять все слагаемые P_f и только они. Это и равносильно тому, что для любой ЭК K над $\{x_1, \ldots, x_n\}$ было выполнено равенство $i(K, P_f) = 0$. Доказательство критерия нечетности функций аналогично, и его мы предоставляем читателю. □

Докажем, наконец, основную теорему этого параграфа.

Теорема 4.3 ([7])**.** *Существует детерминированный алгоритм, распознающий самодвойственность функции f по ее полиному Жегалкина P_f за $O(l^4)$ операций, где l — длина полинома P_f.*

Доказательство. Рассмотрим алгоритм, состоящий из двух этапов:

1. Находим l, и ранг r полинома P_f. Если $l < \sqrt{2^r}$, то, по следствию 4.1, функция f не является самодвойственной, и алгоритм завершается. Если $l \geqslant \sqrt{2^r}$, то переходим ко второму этапу.

2. На данном этапе мы рассматриваем все ЭК K, содержащиеся в слагаемых полинома f, и проверяем выполнение условий $i(K, P_f) = 0$, $i(1, P_f) = 1$. По лемме 9, данной проверки нам достаточно для определения самодвойственности функции f.

На первом этапе мы затрачиваем $O(l)$ операций. На втором этапе для каждого из l слагаемых K_i необходимо просмотреть не более 2^r ЭК, содержащихся в K_i, и для каждой из этих ЭК подсчитать, в каком числе слагаемых P_f эта конъюнкция содержится. На это мы затрачиваем всего $O(l \cdot 2^r \cdot l) = O(l^4)$ операций. Здесь мы существенно пользуемся неравенством из следствия 4.1. □

На втором этапе алгоритма теоремы мы фактически организуем полный перебор. Полиномиальность алгоритма обеспечивается только «мизерным» рангом слагаемых, по сравнению с длиной полинома. Можно ли построить алгоритм распознавания самодвойственности, не использующий оценку из следствия 4.1? Ответ на этот вопрос пока не найден.

Глава 5

Представление булевых функций полиномами над $\mathbb{Z}$

Ранее мы уже рассматривали рекурсивную процедуру нахождения коэффициентов полинома Жегалкина булевой функции через столбец значений. Пусть f — произвольная функция. Обозначим через $c(\widetilde{\gamma})$ коэффициент в полиноме Жегалкина функции f при слагаемом $K_{\widetilde{\gamma}}$, соответствующем набору $\widetilde{\gamma}$. При этом $c(\widetilde{\gamma})$ можно рассматривать как функцию от того же числа переменных, что и f. Например, Для функции $f(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_2x_3$ имеем $c(1,1,0) = c(0,1,1) = c(1,1,1) = 1$, а на всех остальных наборах значение функции c равно нулю.

Упражнение 12. *Покажите, что имеет место равенство*

$$f(\widetilde{\alpha}) = \bigoplus_{\substack{\widetilde{\gamma}\in E_2^n \\ \widetilde{\gamma}\leqslant\widetilde{\alpha}}} c(\widetilde{\gamma}). \tag{5.1}$$

Следующая теорема показывает, что функции f и c оказываются в некотором смысле взаимно обратными[1].

Теорема 5.1. *Пусть* $f(\widetilde{x}^n) = \bigoplus\limits_{\widetilde{\gamma}\in E_2^n} c(\widetilde{\gamma})K_{\widetilde{\gamma}}$. *Тогда*

$$c(\widetilde{\alpha}) = \bigoplus_{\substack{\widetilde{\gamma}\in E_2^n \\ \widetilde{\gamma}\leqslant\widetilde{\alpha}}} f(\widetilde{\gamma}). \tag{5.2}$$

Доказательство. Проведем индукцию по рангу набора $|\widetilde{\alpha}|$. Если $|\widetilde{\alpha}| = 0$, т.е. $\widetilde{\alpha} = \widetilde{0}$, то утверждение теоремы верно, поскольку $c(\widetilde{0}) = f(\widetilde{0})$. Пусть теперь (5.2) выполнено для всех наборов ранга не больше r. Пусть $|\widetilde{\alpha}| = r + 1$. Тогда из (5.1) следует, что

$$f(\widetilde{\alpha}) = \bigoplus_{\substack{\widetilde{\gamma}\in E_2^n \\ \widetilde{\gamma}\leqslant\widetilde{\alpha}}} c(\widetilde{\gamma}) = c(\widetilde{\alpha}) \oplus \bigoplus_{\substack{\widetilde{\gamma}\in E_2^n \\ \widetilde{\gamma}<\widetilde{\alpha}}} c(\widetilde{\gamma}).$$

Для завершения индуктивного перехода осталось показать, что

$$\bigoplus_{\substack{\widetilde{\gamma}\in E_2^n \\ \widetilde{\gamma}<\widetilde{\alpha}}} c(\widetilde{\gamma}) = \bigoplus_{\substack{\widetilde{\gamma}\in E_2^n \\ \widetilde{\gamma}<\widetilde{\alpha}}} f(\widetilde{\gamma}). \tag{5.3}$$

[1] Теорема 5.1, также, как и следующая ниже теорема 5.2, является частным примером т.н. *обращения Мёбиуса*. Подробнее об этом можно узнать из [12]

Пользуясь индуктивным предположением, получаем

$$\bigoplus_{\substack{\widetilde{\gamma}\in E_2^n\\ \widetilde{\gamma}<\widetilde{\alpha}}} c(\widetilde{\gamma}) = \bigoplus_{\substack{\widetilde{\gamma}\in E_2^n\\ \widetilde{\gamma}<\widetilde{\alpha}}}\ \bigoplus_{\substack{\widetilde{\beta}\in E_2^n\\ \widetilde{\beta}\leqslant\widetilde{\gamma}}} f(\widetilde{\beta}) = \bigoplus_{\substack{\widetilde{\beta}\in E_2^n\\ \widetilde{\beta}<\widetilde{\alpha}}}\ \bigoplus_{\substack{\widetilde{\gamma}\in E_2^n\\ \widetilde{\beta}\leqslant\widetilde{\gamma}<\widetilde{\alpha}}} f(\widetilde{\beta}).$$

Каждая сумма $\bigoplus\limits_{\substack{\widetilde{\gamma}\in E_2^n\\ \widetilde{\beta}\leqslant\widetilde{\gamma}<\widetilde{\alpha}}} f(\widetilde{\beta})$ представляет собой сумму из $(2^{|\widetilde{\alpha}|-|\widetilde{\beta}|}-1)$ одинаковых слагаемых, поэтому

$$\bigoplus_{\substack{\widetilde{\gamma}\in E_2^n\\ \widetilde{\beta}\leqslant\widetilde{\gamma}<\widetilde{\alpha}}} f(\widetilde{\beta}) = f(\widetilde{\beta}).$$

Отсюда непосредственно следует (5.3). □

Весом функции $f\in\mathbb{P}_2(n)$ называется суммарное число наборов, на которых значение f равно 1. Вес функции f обозначается через $\mathrm{wt}(f)$. Из теоремы 5.1 следует, что четность веса функции из $\mathbb{P}_2(n)$ совпадает с четностью коэффициента при ЭК $x_1\cdot\ldots\cdot x_n$ в ее полиноме Жегалкина. Таким образом, существует полиномиальный алгоритм, который определяет четность веса функции по ее полиному Жегалкина.

Обозначим через $\mathbb{Z}[\widetilde{x}^n]$ кольцо полиномов с целыми коэффициентами от переменных $x_1,\ \ldots,\ x_n$. Через $\mathbb{Z}^b[\widetilde{x}^n]$ обозначим множество полиномов из $\mathbb{Z}[\widetilde{x}^n]$, у которых каждый моном имеет вид $\widehat{c}\cdot\widehat{K}$, где $\widehat{c}\in\mathbb{Z}$, а $\widehat{K}$ — произведение вида $x_{i_1}\cdot\ldots\cdot x_{i_m}$, где $i_j\neq i_k$ при $j\neq k$.

Например, $3x_1^2+x_1x_2^5x_4^3-18x_3x_4\in\mathbb{Z}[\widetilde{x}^4]$, $3x_1+x_1x_2x_4-18x_3x_4\in\mathbb{Z}^b[\widetilde{x}^4]$.

Аналогично тому, как это делалось для полиномов Жегалкина, можно определить произведение $\widehat{K}_{\widetilde{\alpha}}$, соответствующее набору $\widetilde{\alpha}\in E_2^n$. В это произведение будут входить те и только те x_i, для которых $\alpha_i=1$. Для фиксированного полинома $\widehat{P}\in\mathbb{Z}^b[\widetilde{x}^n]$ через $\widehat{c}(\widetilde{\alpha})$ будем обозначать коэффициент при $\widehat{K}_{\widetilde{\alpha}}$ в этом полиноме.

Всякую булеву функцию можно рассматривать как функцию над $\mathbb{Z}$, определенную лишь для наборов значений переменных из E_2^n. Будем говорить, что полином $\widehat{P}_f\in\mathbb{Z}[\widetilde{x}^n]$ реализует булеву функцию f, если функция $\widehat{P}_f$ совпадает с f на E_2^n.

Утверждение 5.1. *Для любой функции из $\mathbb{P}_2(n)$ найдется реализующий ее полином из $\mathbb{Z}^b[\widetilde{x}^n]$.*

Доказательство. Булевы функции 1, $x\wedge y$ и $x\oplus y$ реализуются соответственно полиномами 1, xy и $x+y-2xy$. Суперпозиция полиномов суть полиномом, поэтому по любой формуле от $\widetilde{x}^n$ в базисе $\{1,\oplus,\wedge\}$ (в т.ч. по полиному Жегалкина) можно построить полином $\widehat{P}'\in\mathbb{Z}[\widetilde{x}^n]$, реализующий ту же булеву функцию. Очевидно, если в $\widehat{P}'$ заменить все ненулевые показатели степеней x_i на единицу, то полученный полином $\widehat{P}\in\mathbb{Z}^b[\widetilde{x}^n]$ по-прежнему будет реализовывать ту же булеву функцию. □

Теорема 5.2. *Пусть* $f(\widetilde{x}^n)=\sum\limits_{\widetilde{\alpha}\in E_2^n}\widehat{c}(\widetilde{\alpha})\widehat{K}_{\widetilde{\alpha}}$. *Тогда*

$$\widehat{c}(\widetilde{\alpha})=\sum_{\substack{\widetilde{\gamma}\in E_2^n\\ \widetilde{\gamma}\leqslant\widetilde{\alpha}}}(-1)^{|\widetilde{\alpha}|-|\widetilde{\gamma}|}f(\widetilde{\gamma}). \tag{5.4}$$

Доказательство. Рассуждение аналогично доказательству теоремы 5.1. Будем вести индукцию по рангу набора $\widetilde{\alpha}$. Если $|\widetilde{\alpha}|=0$, т.е. $\widetilde{\alpha}=\widetilde{0}$, то утверждение теоремы верно, поскольку $\widehat{c}(\widetilde{0})=f(\widetilde{0})$. Пусть теперь (5.4) выполнено для всех наборов ранга не больше r. Пусть $|\widetilde{\alpha}|=r+1$. Имеем

$$f(\widetilde{\alpha})=\sum_{\substack{\widetilde{\gamma}\in E_2^n\\ \widetilde{\gamma}\leqslant\widetilde{\alpha}}}\widehat{c}(\widetilde{\gamma})=\widehat{c}(\widetilde{\alpha})+\sum_{\substack{\widetilde{\gamma}\in E_2^n\\ \widetilde{\gamma}<\widetilde{\alpha}}}\widehat{c}(\widetilde{\gamma}).$$

Таким образом,

$$\widehat{c}(\widetilde{\alpha}) = f(\widetilde{\alpha}) - \sum_{\substack{\widetilde{\gamma}\in E_2^n \\ \widetilde{\gamma}<\widetilde{\alpha}}} \widehat{c}(\widetilde{\gamma}).$$

Для завершения индуктивного перехода осталось показать, что

$$\sum_{\substack{\widetilde{\gamma}\in E_2^n \\ \widetilde{\gamma}<\widetilde{\alpha}}} \widehat{c}(\widetilde{\gamma}) = \sum_{\substack{\widetilde{\gamma}\in E_2^n \\ \widetilde{\gamma}<\widetilde{\alpha}}} (-1)^{|\widetilde{\alpha}|-|\widetilde{\gamma}|+1} f(\widetilde{\gamma}). \tag{5.5}$$

Пользуясь индуктивным предположением, получаем

$$\begin{aligned}\sum_{\substack{\widetilde{\gamma}\in E_2^n \\ \widetilde{\gamma}<\widetilde{\alpha}}} \widehat{c}(\widetilde{\gamma}) &= \sum_{\substack{\widetilde{\gamma}\in E_2^n \\ \widetilde{\gamma}<\widetilde{\alpha}}} \sum_{\substack{\widetilde{\beta}\in E_2^n \\ \widetilde{\beta}\leqslant\widetilde{\gamma}}} (-1)^{|\widetilde{\beta}|-|\widetilde{\gamma}|} f(\widetilde{\beta}) = \sum_{\substack{\widetilde{\beta}\in E_2^n \\ \widetilde{\beta}<\widetilde{\alpha}}} \sum_{\substack{\widetilde{\gamma}\in E_2^n \\ \widetilde{\beta}\leqslant\widetilde{\gamma}<\widetilde{\alpha}}} (-1)^{|\widetilde{\beta}|-|\widetilde{\gamma}|} f(\widetilde{\beta}) = \\ &= \sum_{\substack{\widetilde{\beta}\in E_2^n \\ \widetilde{\beta}<\widetilde{\alpha}}} \left(f(\widetilde{\beta}) \cdot \sum_{\substack{\widetilde{\gamma}\in E_2^n \\ \widetilde{\beta}\leqslant\widetilde{\gamma}<\widetilde{\alpha}}} (-1)^{|\widetilde{\beta}|-|\widetilde{\gamma}|} \right).\end{aligned} \tag{5.6}$$

Обозначив $t = |\widetilde{\beta}| - |\widetilde{\gamma}|$, имеем

$$\sum_{\substack{\widetilde{\gamma}\in E_2^n \\ \widetilde{\beta}\leqslant\widetilde{\gamma}<\widetilde{\alpha}}} (-1)^{|\widetilde{\beta}|-|\widetilde{\gamma}|} = \sum_{k=0}^{t-1} \binom{t}{k} (-1)^k = \sum_{k=0}^{t} \binom{t}{k} (-1)^k - (-1)^t = (-1)^{t+1}. \tag{5.7}$$

Из (5.6) и (5.7) следует (5.5). □

Из теоремы 5.2 и утверждения 5.1 вытекает следующее утверждение.

Следствие 5.1. *Для любой булевой функции $f \in \mathbb{P}_2(n)$ во множестве $\mathbb{Z}^b[\widetilde{x}^n]$ существует единственный реализующий ее полином $\widehat{P}_f$.*

Теорема 5.2 позволяет получить выражение для веса булевой функции f через коэффициенты полинома $\widehat{P}_f$.

Лемма 10. *Пусть* $f(\widetilde{x}^n) = \sum_{\widetilde{\alpha}\in E_2^n} \widehat{c}(\widetilde{\alpha}) \widehat{K}_{\widetilde{\alpha}}$. *Тогда* $\mathrm{wt}(f) = \sum_{\widetilde{\alpha}\in E_2^n} 2^{n-|\widetilde{\alpha}|} \widehat{c}(\widetilde{\alpha})$.

Доказательство.

$$\mathrm{wt}(f) = \sum_{\widetilde{\alpha}\in E_2^n} f(\widetilde{\alpha}) = \sum_{\widetilde{\alpha}\in E_2^n} \sum_{\substack{\widetilde{\gamma}\in E_2^n \\ \widetilde{\gamma}\leqslant\widetilde{\alpha}}} \widehat{c}(\widetilde{\gamma}) = \sum_{\widetilde{\gamma}\in E_2^n} \left(\widehat{c}(\widetilde{\gamma}) \sum_{\substack{\widetilde{\alpha}\in E_2^n \\ \widetilde{\alpha}\geqslant\widetilde{\gamma}}} 1 \right) = \sum_{\widetilde{\gamma}\in E_2^n} \widehat{c}(\widetilde{\gamma}) \cdot 2^{n-|\widetilde{\gamma}|}.$$

□

Пример 5.1. Построим полином из $\mathbb{Z}^b[\widetilde{x}^3]$, реализующий функцию $f(\widetilde{x}^3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3$:

$$\widehat{P}_f = x_1x_2 + x_2x_3 + x_1x_3 - 2x_1x_2x_2x_3 - 2x_1x_2x_1x_3 - 2x_2x_3x_1x_3 + 4x_1x_2x_2x_3x_1x_3 = x_1x_2 + x_2x_3 + x_1x_3 - 2x_1x_2x_3.$$

Вес этой функции равен $2^{3-2} \cdot 3 + 2^{3-3} \cdot (-2) = 4$.

Упражнение 13. *1. Покажите, что функция $x_1 \oplus \ldots \oplus x_n$ реализуется полиномом*

$$\sum_{s=1}^{n} \sum_{1 \leqslant i_1 < \ldots < i_s \leqslant n} (-2)^{s-1} x_{i_1} \cdot \ldots \cdot x_{i_s}.$$

2. Покажите, что функция $x_1 \vee \ldots \vee x_n$ реализуется полиномом

$$\sum_{s=1}^{n} \sum_{1 \leqslant i_1 < \ldots < i_s \leqslant n} (-1)^{s-1} x_{i_1} \cdot \ldots \cdot x_{i_s}.$$

3. Пусть $K_1 \oplus \ldots \oplus K_l$ — полином Жегалкина функции f. Для каждого $i, 1 \leqslant i \leqslant l$, пусть $\widehat{K}_i$ — произведение, соответствующее тому же набору, что и ЭК K_i. Покажите, что f реализуется полиномом

$$\sum_{s=1}^{l} \sum_{1 \leqslant i_1 < \ldots < i_s \leqslant l} (-2)^{s-1} \widehat{K}_{i_1} \cdot \ldots \cdot \widehat{K}_{i_s}.$$

Пусть $K_{i_1}, \ldots, K_{i_s}$ — монотонные ЭК над переменными $x_1, \ldots, x_n$. Через $r(K_{i_1} \cdot \ldots \cdot K_{i_s})$ будем обозначать ранг набора, которому соответствует ЭК, полученная в результате упрощения выражения $K_{i_1} \cdot \ldots \cdot K_{i_s}$ с применением законов коммутативности, ассоциативности, и тождеств $x_i \cdot x_i = x_i$. Например, $r(x_1 x_2 \cdot x_1 x_3) = 3$.

Лемма 11. *Пусть $f(\widetilde{x}^n) = K_1 \oplus \ldots \oplus K_l$. Тогда*

$$\mathrm{wt}(f) = \sum_{s=1}^{l} \sum_{1 \leqslant i_1 < \ldots < i_s \leqslant l} (-2)^{s-1} \cdot 2^{n - r(K_{i_1} \cdot \ldots \cdot K_{i_s})}. \tag{5.8}$$

Доказательство. Пусть $f(\widetilde{x}^n) = K_1 \oplus \ldots \oplus K_l$. Согласно пункту 3 упражнения 13, полином из $\mathbb{Z}^b[\widetilde{x}^n]$, реализующий функцию f, будет иметь вид:

$$f(\widetilde{x}^n) = \sum_{s=1}^{l} \sum_{1 \leqslant i_1 < \ldots < i_s \leqslant l} (-2)^{s-1} \widehat{K}_{i_1} \cdot \ldots \cdot \widehat{K}_{i_s}. \tag{5.9}$$

В дальнейшем, запись $\mathrm{ind}(\widehat{K}_{i_1} \cdot \ldots \cdot \widehat{K}_{i_s}) = \mathrm{ind}(\widetilde{\alpha})$ будем понимать так: “в произведение $\widehat{K}_{i_1} \cdot \ldots \cdot \widehat{K}_{i_s}$ входят переменные x_i с теми и только теми индексами i, для которых $\alpha_i = 1$”. Это аналогично введенному ранее понятию индексной характеристики монотонной ЭК.

Группируя слагаемые в правой части (5.9), получаем:

$$f(\widetilde{x}^n) = \sum_{\widetilde{\alpha} \in E_2^n} \sum_{s=1}^{l} \sum_{\substack{1 \leqslant i_1 < \ldots < i_s \leqslant l \\ \mathrm{ind}(\widehat{K}_{i_1} \cdot \ldots \cdot \widehat{K}_{i_s}) = \mathrm{ind}(\widetilde{\alpha})}} (-2)^{s-1} \widehat{K}_{i_1} \cdot \ldots \cdot \widehat{K}_{i_s}. \tag{5.10}$$

По лемме 10,

$$\mathrm{wt}(f) = \sum_{\widetilde{\alpha} \in E_2^n} 2^{n - |\widetilde{\alpha}|} \widehat{c}(\widetilde{\alpha}). \tag{5.11}$$

Из (5.10) и (5.11) вытекает, что

$$\mathrm{wt}(f) = \sum_{\widetilde{\alpha} \in E_2^n} 2^{n-|\widetilde{\alpha}|} \sum_{s=1}^{l} \sum_{\substack{1 \leqslant i_1 < \ldots < i_s \leqslant l \\ \mathrm{ind}(\widehat{K}_{i_1} \cdot \ldots \cdot \widehat{K}_{i_s}) = \mathrm{ind}(\widetilde{\alpha})}} (-2)^{s-1} = \sum_{s=1}^{l} \sum_{1 \leqslant i_1 < \ldots < i_s \leqslant l} (-2)^{s-1} \cdot 2^{n - r(K_{i_1} \cdot \ldots \cdot K_{i_s})}.$$

□

Теорема 5.3 ([8]). *Пусть k — фиксированное число. Существует детерминированный алгоритм, который по полиному Жегалкина булевой функции $f(\widetilde{x}^n)$ находит остаток от деления $\mathrm{wt}(f)$ на 2^k со сложностью $O(l^k)$, где l — длина полинома.*

Доказательство. Пусть функция f задана полиномом Жегалкина $P_f = K_1 \oplus \ldots \oplus K_l$. Непосредственно из леммы 11 следует, что

$$\mathrm{wt}(f) \equiv \sum_{s=1}^{k} \sum_{1 \leqslant i_1 < \ldots < i_s \leqslant l} (-2)^{s-1} \cdot 2^{n - r(K_{i_1} \cdot \ldots \cdot K_{i_s})} \pmod{2^k}.$$

Таким образом, для нахождения остатка от деления $\mathrm{wt}(f)$ на 2^k необходимо выполнить следующие действия. Перебрать всевозможные конъюнкции вида $K_{i_1} \cdot \ldots \cdot K_{i_s}$ не более чем k слагаемых полинома P_f (число таких конъюнкций равно $\sum_{s=1}^{k} \binom{l}{s}$):

a) для каждой из них определить $r(K_{i_1} \cdot \ldots \cdot K_{i_s})$;

b) выполнить $O(1)$ арифметических операций для вычисления $(-2)^{s-1} \cdot 2^{n - r(K_{i_1} \cdot \ldots \cdot K_{i_s})}$ и добавить это число к общей сумме по модулю 2^k.

Очевидно, сложность приведенного вычисления равна $O(\sum_{s=1}^{k} \binom{l}{s}) = O(l^k)$. Теорема доказана. □

Описанный выше алгоритм позволяет при фиксированном k за полиномиальное время проверять, делится ли вес некоторой функции $f \in \mathbb{P}_2(n)$ на 2^k. Вопрос о том, существует ли решение аналогичной задачи за полиномиальное время в случае, когда k является параметром, зависящим от n, пока остается открытым. Например, представлял бы интерес полиномиальный алгоритм, отвечающий на вопрос «$\mathrm{wt}(f) = 2^{n-1}$?» (или доказательство того, что такого алгоритма не существует).

Пример 5.2. Пусть $f(\widetilde{x}^3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3$. Найдем остаток от деления $\mathrm{wt}(f)$ на 2^k при $k = 2$ с помощью описанного в теореме 5.3 алгоритма. Промежуточное значение остатка будем хранить в переменной w. Вначале полагаем $w := 0$.

1. Полином P_f состоит из трех ЭК ранга 2. Полагаем

$$w := w + (-2)^0 2^{3-2} + (-2)^0 2^{3-2} + (-2)^0 2^{3-2} = 6 \equiv 2 \pmod{2^2}.$$

2. Рассматриваем всевозможные произведения пар ЭК из P_f. Получаем три одинаковые конъюнкции $x_1x_2x_3$ ранга 3. Полагаем

$$w := w + (-2)^1 2^{3-3} + (-2)^1 2^{3-3} + (-2)^1 2^{3-3} = -4 \equiv 0 \pmod{2^2}.$$

Получаем, что $\mathrm{wt}(f)$ без остатка делится на 2^2.

Литература

[1] Гаврилов Г. П., Сапоженко А. А. *Задачи и упражнения по дискретной математике.* М., Физматлит, 2004. (Гл. 1, п. 3, с. 52-58)

[2] Джавадов Р. М. *О сложности приближенного задания функций алгебры логики.* ДАН, т. 265, вып. 1, 1982, с. 24-27.

[3] Кириченко К. Д. *Верхняя оценка сложности полиномиальных нормальных форм булевых функций.* Дискретная математика, т. 17, вып. 3, 2005, с. 80-88.

[4] Логачев О. А., Сальников А. А., Ященко В. В. *Булевы функции в теории кодирования и криптологии.* М., МЦНМО, 2004. (Гл. 2, п. 2.1-2.2, с. 65-90)

[5] Перязев Н. А. *Сложность булевых функций в классе полиномиальных поляризованных форм.* Алгебра и логика, 34, вып. 3, 1995, с. 323-326.

[6] Селезнева С. Н. *О приближении с заданной точностью функций многозначных логик полиномами.* В печати.

[7] Селезнева С. Н. *О сложности распознавания полноты множеств булевых функций, реализованных полиномами Жегалкина.* Дискретная математика, т. 9, вып. 4, 1997, с. 24-31.

[8] Селезнева С. Н. *Об алгоритмической сложности нахождения остатка от деления на степень двойки веса булевой функции, заданной полиномом.* Вестник МГУ. Серия 15 - Вычислительная математика и кибернетика, т. 17, вып. 1, 2007, с. 32-36.

[9] Яблонский С. В. *Введение в дискретную математику.* М., Высшая школа, 2001. (Гл. 1, с. 9-42)

[10] Carlet C., Guillot Ph. *A new representation of Boolean function.* Technical report, INRIA Project CODES, 1999, p. 1-14.

[11] Even S., Kohavi I., Paz A. *On minimal modulo 2 sums of products for switching functions.* IEEE Trans. Elect. Comput., 1967, p. 671-674.

Дополнительная литература

[12] Айгнер М. *Комбинаторная теория.* М., Мир, 1982. (Гл. 4)

Оглавление