

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, *предположим* 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 $\tilde{\alpha}, \tilde{\beta}$ таких, что $\tilde{\alpha} \leq \tilde{\beta}$, выполнено $f(\tilde{\alpha}) \leq f(\tilde{\beta})$. Набор $\tilde{\alpha}$ называется *нижней единицей* функции f , если $f(\tilde{\alpha}) = 1$ и $f(\tilde{\beta}) = 0$ для всякого набора $\tilde{\beta} \leq \tilde{\alpha}$. Везде далее будем рассматривать всякое множество монотонных ЭК $K_1, \dots, K_l$ как частично упорядоченное, с отношением порядка, порожденным отношением включения на множестве $\{\text{ind}(K_1), \dots, \text{ind}(K_l)\}$. В связи с этим будем говорить о *минимальных* и *максимальных* элементах во множестве $K_1, \dots, K_l$. Докажем вспомогательную лемму.

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

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

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

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 $f(\tilde{0}) = 0$?

Обозначим через $f_{\alpha_1, \dots, \alpha_k}^{i_1, \dots, i_k}(\tilde{x}^n)$ 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 $\tilde{\alpha}$ выполнено $f_{1, \dots, 1}^{i_1, \dots, i_k}(\tilde{x}^n) \equiv 1$, где $\{i_1, \dots, i_k\} = \text{ind}(\tilde{\alpha})$.

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 $P_f = K_1 \oplus \dots \oplus K_l$.

Этап 1. Из леммы 5 следует, что для нахождения всех нижних единиц функции f достаточно найти все минимальные элементы во множестве $\{K_1, \dots, K_l\}$. 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_i 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 $K_{i_1}, \dots, K_{i_m}$. Поскольку $m \leq l$, 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 потребуются $O(l^2)$ элементарных операций алгоритмической модели, описанной в предыдущем параграфе.

Этап 2. Теперь для каждой нижней единицы $\tilde{\alpha}$, выполняем подстановку констант 1 в P_f на места всех переменных с номерами из $\text{ind}(\tilde{\alpha})$. 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. $\square$

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

$$\alpha_{1,1}, \alpha_{1,2}, \dots, \alpha_{1,n}, \alpha_{2,1}, \alpha_{2,2}, \dots, \alpha_{2,n}, \dots, \alpha_{l,1}, \alpha_{l,2}, \dots, \alpha_{l,n},$$

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 называется четной, если $f(x_1, \dots, x_n) = f(\bar{x}_1, \dots, \bar{x}_n)$.

Функция f называется нечетной, если $f(x_1, \dots, x_n) = \bar{f}(\bar{x}_1, \dots, \bar{x}_n)$.

Доказательство трех следующих утверждений предоставляется читателю.

Утверждение 4.2. Функция $f(\tilde{x}^n)$ четна (нечетна) тогда и только тогда, когда функция $\bar{f}(\tilde{x}^n)$ 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 $f(\tilde{x}^n)$ четна тогда и только тогда, когда функция $g(\tilde{x}^n) = f(\tilde{x}^n) \oplus x_i$ нечетна.

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

Доказательство.

$$\begin{aligned} f(\bar{x}_1, \dots, \bar{x}_n) &= \bar{x}_i g(\bar{x}_1, \dots, \bar{x}_{i-1}, \bar{x}_{i+1}, \dots, \bar{x}_n) \oplus h(\bar{x}_1, \dots, \bar{x}_{i-1}, \bar{x}_{i+1}, \dots, \bar{x}_n) = \\ &= x_i g(\bar{x}_1, \dots, \bar{x}_{i-1}, \bar{x}_{i+1}, \dots, \bar{x}_n) \oplus (g(\bar{x}_1, \dots, \bar{x}_{i-1}, \bar{x}_{i+1}, \dots, \bar{x}_n) \oplus h(\bar{x}_1, \dots, \bar{x}_{i-1}, \bar{x}_{i+1}, \dots, \bar{x}_n)) \end{aligned}$$

Из единственности представления функции f полиномом Жегалкина следует, что

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

то есть g — четная функция. $\square$

Лемма 7. Пусть $f(\tilde{x}^n)$ — 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 $\tilde{\alpha}$, на котором значение f равно 1. Следовательно, в P_f найдется слагаемое $K_1 \neq 1$, обращающееся на $\tilde{\alpha}$ в единицу. По определению четной функции, $f(\tilde{\alpha}) = f(\tilde{\alpha})$. Значит в P_f есть слагаемое K_2 , не обращающееся в нуль на наборе $\tilde{\alpha}$. Поэтому

$$\text{ind}(K_2) \subseteq \text{ind}(\tilde{\alpha}) = \{1, 2, \dots, n\} \setminus \text{ind}(\tilde{\alpha}) \subseteq \{1, 2, \dots, n\} \setminus \text{ind}(K_1),$$

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

Лемма 8. Пусть $f(\tilde{x}^n)$ — 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 $f(x_1, \dots, x_n) = x_i g(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \oplus h(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$. 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. $\square$

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

Доказательство. Пусть $f(\tilde{0}) = 0$. Так как $r(P_f) = r$, то в P_f найдется слагаемое K ранга r . У множества K всего 2^r подмножеств $K_1, \dots, K_{2^r}$. 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. $\square$

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

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

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 $f(\tilde{x}^n)$ является четной тогда и только тогда, когда $i(K, P_f) = 0$ для любой монотонной ЭК K над $\{x_1, \dots, x_n\}$.

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

Доказательство. Докажем критерий четности функций. Пусть $P_f = K_1 \oplus \dots \oplus K_l$. Пусть $K_i = x_{i_1} \dots x_{i_{m_i}}$. Полином $P' = P_{f(\bar{x}_1, \dots, \bar{x}_n)}$ получается, если заменить каждое слагаемое K_i в P_f на слагаемое $(x_{i_1} \oplus 1) \dots (x_{i_{m_i}} \oplus 1)$, 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 $f(\tilde{x}^n)$ 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 $\{x_1, \dots, x_n\}$ было выполнено равенство $i(K, P_f) = 0$. Доказательство критерия нечетности функций аналогично, и его мы предоставляем читателю. $\square$

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 $l \geq \sqrt{2^r}$, 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. $\square$

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.