

13

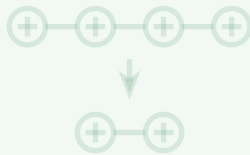
Лекция

1–2 декабря

Минимизация и полином Жегалкина

Константин Чухарев

Дискретная математика — Осень 2026



Минимизация и полином Жегалкина

Преждевременная оптимизация — корень всех зол.

— Дональд Кнут

Зачем минимизировать?

Каждый литерал формулы в железе — провод и вход вентиля.

Цена избыточности прямая: больше вентиляей, длиннее задержка, выше энергопотребление.

Совершенная форма — отправная точка, а не результат.

Цель минимизации — равносильная формула с наименьшим числом литералов.

Пример: функция большинства

Пример

$f(x, y, z) = 1$ при двух и более единицах на входах — СДНФ из четырёх минтермов по три литерала:

$$f = \bar{x}yz \vee x\bar{y}z \vee xy\bar{z} \vee xyz.$$

Склейки сжимают её до трёх термов:

$$f = xy \vee xz \vee yz.$$

Двенадцать литералов — против шести.

Склейка минтермов

Минтермы, отличающиеся ровно в одной переменной, склеиваются:

$$xyz \vee xy\bar{z} = xy(z \vee \bar{z}) = xy.$$

Определение 1 (Простая импликанта)

Конъюнкция литералов называется **простой импликантой** (*prime implicant*) функции f , если она истинна только при истинной f и перестаёт быть такой при вычёркивании любого литерала.

Минимальная ДНФ — покрытие всех единиц таблицы простыми импликантами.

Карта Карно

Определение 2 (Карта Карно)

Таблица истинности, у которой строки и столбцы идут в коде Грея, называется **картой Карно** (*Karnaugh map*).

Соседние клетки отличаются ровно в одной переменной.

Прямоугольная группа из 2^k соседних единиц — конъюнкция из $n - k$ литералов.

Карта замкнута в тор: крайние строки и столбцы тоже соседние.

Группа может переходить через край.

Группа из четырёх клеток

Пример

Функция $f(x, y, z) = x$ равна 1 ровно на четырёх наборах.

Её четыре минтерма — $x\bar{y}\bar{z}$, $x\bar{y}z$, $xy\bar{z}$, xyz — образуют на карте прямоугольник 2^2 .

По правилу $n - k$ литералов остаётся один: сам x .

Карта Карно: пример

	$\bar{x}$	x
yz		
00		
01		1
11	1	1
10		1

Пример

Три пары единиц — три простые импликанты: xy , xz , yz .

Каждая существенна: покрываемая ею единица больше никем не покрывается.

Минимальная ДНФ — $xy \vee xz \vee yz$.

Минимизация по карте Карно

1. Выделить максимальные группы из 2^k соседних единиц.
2. Взять существенные импликанты — их «свои» единицы никто больше не покрывает.
3. Покрыть оставшиеся единицы минимальным числом групп.
4. Неопределённые значения ($\times$) присоединять к группам, если это укрупняет их.

Ручной метод жив при $n \leq 4$.

Дальше карты перестают помещаться на листе — нужны алгоритмы.

Квайн—МакКласки: склеивание

Фаза склеивания.

1. Выписать минтермы в двоичном виде.
2. Склеивать пары, отличающиеся ровно в одном бите: различающий бит заменяется прочерком.
3. Повторять, пока склеивания возможны.
4. Несклеенные термы — простые импликанты.

Пример

Минтермы 010 и 011 дают терм $01 \times$: бит z вычеркнут.

Квайн—МакКласки: покрытие

Фаза покрытия.

1. Составить таблицу: строки — простые импликанты, столбцы — исходные минтермы.
2. Выбрать минимальное число строк, покрывающее все столбцы.

Склейка та же, что на карте Карно, — но систематическая и программная.

Фаза покрытия в общем случае NP-трудна, на практике её решают эвристики.

Полином Жегалкина

Определение 3 (Полином Жегалкина)

Запись функции в виде

$$f(x_1, \dots, x_n) = \bigoplus_{S \subseteq \{1, \dots, n\}} a_S \cdot \prod_{i \in S} x_i,$$

где $a_S \in \{0, 1\}$, а сложение — $\oplus$, называется **полиномом Жегалкина** (алгебраической нормальной формой, АНФ).

Мономы — произведения подмножеств переменных, без отрицаний.

Пример

$$\bar{x} = x \oplus 1, \text{quad } x \vee y = x \oplus y \oplus xy.$$

Единственность АНФ

Теорема 1 (Единственность)

Всякая булева функция имеет ровно один полином Жегалкина.

Доказательство

Докажем подсчётом.

Мономов 2^n — по одному на подмножество переменных, и каждый либо входит в полином, либо нет.

Значит, полиномов 2^{2^n} — столько же, сколько булевых функций.

Методы построения ниже предъявляют полином для любой функции, поэтому лишних полиномов нет.

Почему XOR?

СДНФ канонична среди ДНФ, АНФ — единственная без оговорок.

Причина — выбор сложения: $x \oplus x = 0$, повтор сам себя убирает.

Дизъюнкция идемпотентна: $x \vee x = x$.

Повтор слагаемого ничего не меняет, поэтому равносильных ДНФ много.

Единственность АНФ — свойство поля $\text{GF}(2)$, а не самой формы.

Тождества перехода

Теорема 2 (NOT и OR через XOR)

$$\bar{x} = x \oplus 1, \quad x \vee y = x \oplus y \oplus xy.$$

Эти два тождества переводят любую формулу в АНФ: отрицание — добавлением константы, дизъюнкция — тремя слагаемыми.

Конъюнкция и $\oplus$ остаются как есть.

АНФ импликации

Пример

$$\begin{aligned}x \rightarrow y &= \bar{x} \vee y \\&= (x \oplus 1) \oplus y \oplus (x \oplus 1)y \\&= x \oplus 1 \oplus y \oplus xy \oplus y \\&= 1 \oplus x \oplus xy.\end{aligned}$$

Проверка на наборе $(1, 0)$: $1 \oplus 1 \oplus 0 = 0$ — импликация ложна, как и положено.

Полином читается напрямую: $1 \oplus x$ — отрицание x , моном xy — поправка, включающаяся при $x = 1, y = 1$.

Треугольник Паскаля

Построение АНФ по таблице.

1. Выписать значения f по всем наборам — от $(0, \dots, 0)$ до $(1, \dots, 1)$.
2. Каждая следующая строка — попарный $\oplus$ соседей предыдущей.
3. Повторять, пока не останется один элемент.
4. Первые элементы строк — коэффициенты полинома.

Метод не требует ни решения систем, ни алгебраических преобразований — ничего, кроме столбца значений.

Треугольник: пример

Пример

Значения $x \rightarrow y$ по наборам $(0, 0), (0, 1), (1, 0), (1, 1)$: 1, 1, 0, 1.

1	1	0	1
0	1	1	
	1	0	
		1	

Коэффициенты при $1, y, x, xy$: $(1, 0, 1, 1)$.

Итог $x \rightarrow y = 1 \oplus x \oplus xy$ — совпал с методом тождеств.

АНФ в криптоанализе

Степень полинома Жегалкина измеряет нелинейность функции.

- Симметричные шифры собирают из линейных операций ($\oplus$, сдвиги) и нелинейных S-блоков.
- Если АНФ S-блока имеет низкую степень, шифр сводится к системе уравнений над $GF(2)$ — алгебраическая атака.

S-блоки проектируют с высокой степенью АНФ: у координат S-блока AES степень 7 из 8 переменных.

Полином Жегалкина — инструмент проектирования, а не только форма записи.

Лекция 13: что мы поняли?

- Избыточность СДНФ стоит денег: каждый лишний литерал становится вентилем.
- Карта Карно — код Грея на клетках: группа из 2^k соседних единиц снимает k переменных.
- Квайн—МакКласки — та же склейка, но алгоритмом, с таблицей покрытия простых импликант.
- Полином Жегалкина — единственная каноническая запись через $\oplus$ и $\wedge$.
- Два пути к АНФ: тождества $\bar{x} = x \oplus 1$ и $x \vee y = x \oplus y \oplus xy$ — или треугольник Паскаля.

Вопросы для самопроверки

1. Минимизируйте по карте Карно $f = \overline{x}yz \vee \overline{x}yz \vee xy\overline{z} \vee x\overline{y}z$.
2. Что даёт склейка минтермов xyz и $x\overline{y}z$? Какая переменная исчезает?
3. Постройте полином Жегалкина для $x \rightarrow y$ двумя способами: тождествами и треугольником.
4. Почему АНФ единственна, а минимальная ДНФ — нет?
5. Какое наибольшее число мономов может входить в АНФ функции от n переменных? Приведите функцию, у которой мономов именно столько.
6. Функция трёх переменных равна 1 при чётном числе единиц на входе. Найдите её АНФ и ответьте, линейна ли она.

Чтение к следующей паре

- m10 — «Минимизация» (карты Карно, Квайн—МакКласки), «Полином Жегалкина».
- m11 — «Логические вентили и схемы», «Сумматоры», «Код Грея».
- Флеш-опросник — в начале лекции 14.
- Контрольная 4 (булева алгебра и, возможно, простой номер на коды) — на следующей неделе, на отдельной паре.