Полином Жегалкина

Полином Жегалкина (англ. *Zhegalkin polynomial*) — полином с коэффициентами вида 0 и 1, где в качестве произведения берётся конъюнкция, а в качестве сложения исключающее или. Полином был предложен в 1927 году И. И. Жегалкиным в качестве средства для представления функций булевой логики. Полином Жегалкина имеет следующий вид:

$$P = a_{000\ldots000} \oplus a_{100\ldots0}x_1 \oplus a_{010\ldots0}x_2 \oplus \ldots \oplus a_{00\ldots01}x_n \oplus a_{110\ldots0}x_1x_2 \oplus \ldots \oplus a_{00\ldots011}x_{n-1}x_n \oplus \ldots \oplus a_{11\ldots1}x_1x_2\ldots x_n$$

Содержание

Полнота

По теореме Поста, чтобы система булевых функций была полной, надо, чтобы в ней существовали

1. Хотя бы одна функция, не сохраняющая 0;
2. Хотя бы одна функция, не сохраняющая 1;
3. Хотя бы одна нелинейная функция;
4. Хотя бы одна немонотонная функция;
5. Хотя бы одна несамодвойственная функция.

Исходя из этого, система функций $\langle \wedge, \oplus, 1 \rangle$ является полной:

x_0	x_1	$\ldots$	x_n	1	$\wedge$	$\oplus$
0	0	$\ldots$	0	1	0	0
1	0	$\ldots$	0	1	0	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
1	1	$\ldots$	1	1	1	0
Сохраняет 0				0	1	1
Сохраняет 1				1	1	0
Самодвойственная				0	0	0
Монотонная				1	1	0
Линейная				1	0	1

На основе этой системы и строятся полиномы Жегалкина.

Существование и единственность представления (теорема Жегалкина)

Теорема (Жегалкина):

> Каждая булева функция единственным образом представляется в виде полинома Жегалкина.

Доказательство:
▷

Заметим, что различных булевых функций от n переменных 2^{2^n} штук. При этом конъюнкций вида $x_{i_1}\ldots x_{i_k}$ существует ровно 2^n, так как из n возможных сомножителей каждый или входит в конъюнкцию, или нет. В полиноме у каждой такой конъюнкции стоит 0 или 1, то есть существует 2^{2^n} различных полиномов Жегалкина от n переменных.

Теперь достаточно лишь доказать, что различные полиномы реализуют различные функции. Предположим противное. Тогда приравняв два различных полинома и перенеся один из них в другую часть равенства, получим полином, тождественно равный нулю и имеющий ненулевые коэффициенты. Тогда рассмотрим слагаемое с единичным коэффициентом наименьшей длины, то есть с наименьшим числом переменных, входящих в него (любой один, если таких несколько). Подставив единицы на места этих переменных, и нули на места остальных, получим, что на этом наборе только одно это слагаемое принимает единичное значение, то есть нулевая функция на одном из наборов принимает значение 1. Противоречие. Значит, каждая булева функция реализуется полиномом Жегалкина единственным образом.

◁

Построение полинома Жегалкина

Существует несколько способов построения полинома Жегалкина.

По таблице истинности

Пусть для функции $f(x_1, x_2, \ldots, x_n)$ задана таблица истинности. Запишем сначала данную функцию в виде полинома Жегалкина с неопределёнными коэффициентами. Затем по очереди подставляем всевозможные наборы в порядке увеличения количества единиц и находим коэффициенты с учётом того, что $a \oplus 1 = \bar{a}$, а $a \oplus 0 = a$. За каждую подстановку находим только один коэффициент.

Пример: Дана функция $f(x_1, x_2, x_3, x_4)$ и её таблица истинности:

x_1	x_2	x_3	x_4	$f(x_1, x_2, x_3, x_4)$
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	1
0	1	1	1	0
1	0	0	0	1
1	0	0	1	0
1	0	1	0	0
1	0	1	1	1
1	1	0	0	1
1	1	0	1	0
1	1	1	0	1
1	1	1	1	0

Построим для неё полином Жегалкина:

$f(x_1, x_2, x_3, x_4) = a_{0000} \oplus a_{1000}x_1 \oplus a_{0100}x_2 \oplus a_{0010}x_3 \oplus a_{0001}x_4 \oplus a_{1100}x_1x_2 \oplus a_{1010}x_1x_3 \oplus a_{1001}x_1x_4 \oplus a_{0110}x_2x_3 \oplus a_{010}$

Так как $f(0, 0, 0, 0) = 0$, то $a_{0000} = 0$. Далее подставляем все остальные наборы в порядке возрастания числа единиц, подставляя вновь полученные значения в следующие формулы:

$f(1, 0, 0, 0) = a_{0000} \oplus a_{1000} = 1$, следовательно $a_{1000} = 1$

$f(0, 1, 0, 0) = a_{0000} \oplus a_{0100} = 0$, следовательно $a_{0100} = 0$

$f(0, 0, 1, 0) = a_{0000} \oplus a_{0010} = 0$, следовательно $a_{0010} = 0$

$f(0, 0, 0, 1) = a_{0000} \oplus a_{0001} = 0$, следовательно $a_{0001} = 0$

$f(1, 1, 0, 0) = a_{0000} \oplus a_{1000} \oplus a_{0100} \oplus a_{1100} = 1$, следовательно $a_{1100} = 0$

$f(1, 0, 1, 0) = a_{0000} \oplus a_{1000} \oplus a_{0010} \oplus a_{1010} = 0$, следовательно $a_{1010} = 1$

$f(1, 0, 0, 1) = a_{0000} \oplus a_{1000} \oplus a_{0001} \oplus a_{1001} = 0$, следовательно $a_{1001} = 1$

$f(0, 1, 1, 0) = a_{0000} \oplus a_{0100} \oplus a_{0010} \oplus a_{0110} = 1$, следовательно $a_{0110} = 1$

$f(0, 1, 0, 1) = a_{0000} \oplus a_{0100} \oplus a_{0001} \oplus a_{0101} = 0$, следовательно $a_{0101} = 0$

$f(0, 0, 1, 1) = a_{0000} \oplus a_{0010} \oplus a_{0001} \oplus a_{0011} = 0$, следовательно $a_{0011} = 0$

$f(1, 1, 1, 0) = a_{0000} \oplus a_{1000} \oplus a_{0100} \oplus a_{0010} \oplus a_{1100} \oplus a_{1010} \oplus a_{0110} \oplus a_{1110} = 1$, следовательно $a_{1110} = 0$

$f(1, 1, 0, 1) = a_{0000} \oplus a_{1000} \oplus a_{0100} \oplus a_{0001} \oplus a_{1100} \oplus a_{1001} \oplus a_{0101} \oplus a_{1101} = 0$, следовательно $a_{1101} = 0$

$f(1, 0, 1, 1) = a_{0000} \oplus a_{1000} \oplus a_{0010} \oplus a_{0001} \oplus a_{1010} \oplus a_{1001} \oplus a_{0011} \oplus a_{1011} = 1$, следовательно $a_{1011} = 0$

$f(0, 1, 1, 1) = a_{0000} \oplus a_{0100} \oplus a_{0010} \oplus a_{0001} \oplus a_{0110} \oplus a_{0101} \oplus a_{0011} \oplus a_{0111} = 0$, следовательно $a_{0111} = 1$

$f(1, 1, 1, 1) = a_{0000} \oplus a_{1000} \oplus a_{0100} \oplus a_{0010} \oplus a_{0001} \oplus a_{1100} \oplus a_{1010} \oplus a_{1001} \oplus a_{0110} \oplus a_{0101} \oplus a_{0011} \oplus a_{1110} \oplus a_{1101} \oplus a_{1011}$ следовательно $a_{1111} = 1$

Таким образом, полином Жегалкина выглядит так:

$f(x_1, x_2, x_3, x_4) = x_1 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_3x_4 \oplus x_1x_2x_3x_4$

Преобразование дизъюнктивной нормальной формы

Этот способ основан на том, что $X \oplus 1 = \bar{X}$. Если функция задана в виде ДНФ, то можно сначала убрать дизъюнкцию, используя правило де Моргана, а все отрицания заменить прибавлением единицы по модулю два, после чего раскрыть скобки по обычным правилам, при этом учитывая, что четное число одинаковых слагаемых равно нулю (так как $X \oplus X = 0$), а нечетное число одинаковых слагаемых равно одному такому слагаемому. Либо же можно заменить дизъюнкцию по следующему правилу: $A \vee B = AB \oplus A \oplus B \ \ (1)$.

Если функция задана в СДНФ, то так как при любых значениях входных переменных в единицу обращается не более одного члена выражения, то достаточно просто заменить все дизъюнкции исключающим ИЛИ.

Пример: Дана функция в ДНФ $f(x_1, x_2, x_3, x_4) = (x_1 \wedge x_2 \wedge \neg x_3 \wedge x_4) \vee (\neg x_1 \wedge \neg x_4) \vee (x_1 \wedge x_2) \vee x_2$, построим полином Жегалкина.

Запишем функцию так:

$f(x_1, x_2, x_3, x_4) = x_1x_2\neg x_3x_4 + \neg x_1\neg x_4 + x_1x_2 + x_2;$

Сгруппируем слагаемые и воспользуемся преобразованием (1):

$f(x_1, x_2, x_3, x_4) = (x_1x_2\neg x_3x_4 \oplus \neg x_1\neg x_4 \oplus x_1x_2\neg x_3x_4\neg x_1\neg x_4) + (x_1x_2 \oplus x_2 \oplus \oplus x_1x_2x_2)$

Воспользуемся свойствами конъюнкции $A \wedge A = A$ и $\neg A \wedge A = 0$, а также тем, что $A \oplus A = 0$, и упростим выражение:

$f(x_1, x_2, x_3, x_4) = (x_1x_2\neg x_3x_4 \oplus \neg x_1\neg x_4) + x_2$

Ещё раз воспользуемся преобразованием (1):

$f(x_1, x_2, x_3, x_4) = x_1x_2\neg x_3x_4 \oplus \neg x_1\neg x_4 \oplus x_2 \oplus (x_1x_2\neg x_3x_4 \oplus \neg x_1\neg x_4)x_2$

Раскроем скобку по алгебраическим правилам:

$f(x_1, x_2, x_3, x_4) = x_1x_2\neg x_3x_4 \oplus \neg x_1\neg x_4 \oplus x_2 \oplus x_1x_2x_2\neg x_3x_4 \oplus \neg x_1x_2\neg x_4$

Снова воспользуемся свойствами конъюнкции и исключающего ИЛИ:

$f(x_1, x_2, x_3, x_4) = \neg x_1\neg x_4 \oplus x_2 \oplus \neg x_1x_2\neg x_4$

Заменим отрицание на прибавление 1:

$f(x_1, x_2, x_3, x_4) = (x_1 \oplus 1)(x_4 \oplus 1) \oplus x_2 \oplus (x_1 \oplus 1)x_2(x_4 \oplus 1)$

Раскроем скобки:

$f(x_1, x_2, x_3, x_4) = x_1x_4 \oplus x_1 \oplus x_4 \oplus 1 \oplus x_2 \oplus x_1x_2x_4 \oplus x_1x_2 \oplus x_2x_4 \oplus x_2$

Выкинем парные слагаемые и получим окончательную формулу:

$f(x_1, x_2, x_3, x_4) = x_1x_2x_4 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_4 \oplus x_1 \oplus x_4 \oplus 1$

Метод треугольника

Метод треугольника позволяет преобразовать таблицу истинности в полином Жегалкина путём построения вспомогательной треугольной таблицы в соответствии со следующими правилами:

1. Строится полная таблица истинности, в которой строки идут в порядке возрастания двоичных кодов от $000\ldots00$ до $111\ldots11$.
2. Строится вспомогательная треугольная таблица, в которой первый столбец совпадает со столбцом значений функции в таблице истинности.
3. Ячейка в каждом последующем столбце получается путём сложения по модулю 2 двух ячеек предыдущего столбца — стоящей в той же строке и строкой ниже.
4. Столбцы вспомогательной таблицы нумеруются двоичными кодами в том же порядке, что и строки таблицы истинности.
5. Каждому двоичному коду ставится в соответствие один из членов полинома Жегалкина в зависимости от позиций кода, в которых стоят единицы. Например, ячейке 111 соответствует член ABC, ячейке 101 — член AC, ячейке 010 — член B, ячейке 000 — член 1 и т.д.
6. Если в верхней строке какого-либо столбца стоит единица, то соответствующий член присутствует в полиноме Жегалкина.

Фактически, этот метод является модификацией метода построения по таблице истинности, описанного выше. По сравнению с ним он удобнее тем, что расчёты занимают мало места и в них сложнее ошибиться, но метод треугольника требует бóльшего количества операций.

Пример преобразования таблицы истинности в полином Жегалкина для функции трёх переменных $P(A, B, C)$ показан на рисунке.

A	B	C	P
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

000	001	010	011	100	101	110	111
1	C	B	BC	A	AC	AB	ABC
①	①	0	0	0	0	①	0
0	1	0	0	0	1	1	
1	1	0	0	1	0		
0	1	0	1	1			
1	1	1	0				
0	0	1					
0	1						
1							

$$P = 1 \oplus C \oplus AB$$

Чтобы получить формулу, по которой рассчитывается какой-либо коэффициент, нужно из клетки, в которой он записан, пройтись всеми возможными путями влево, до столбца $"P"$ таблицы истинности, делая ходы влево и влево-вниз, записать значения в конечных ячейках и сложить их все между собой по модулю 2.

Таким образом, в первом столбце сверху записан коэффициент $a_0 = P(0,0,0)$,

во втором — $a_1 = P(0,0,0) \oplus P(0,0,1)$,

в третьем — $a_2 = P(0,0,0) \oplus P(0,0,1) \oplus P(0,0,1) \oplus P(0,1,0) = P(0,0,0) \oplus P(0,1,0)$,

в четвёртом —

$a_3 = P(0,0,0) \oplus P(0,0,1) \oplus P(0,0,1) \oplus P(0,0,1) \oplus P(0,1,0) \oplus P(0,1,0) \oplus P(0,1,0) \oplus P(0,1,1) = P(0,0,0) \oplus P(0$

и так далее, то есть при построении вспомогательной таблицы коэффициенты полинома просчитываются автоматически.

Преобразование Мёбиуса

Пусть задана булева функция $f : B^n \to B, \quad B = \{0;1\}$. Любая булева функция представима в виде полинома Жегалкина, притом единственным образом.

Пусть $i = (i_1, i_2, \dots i_n), \quad i_k \in \{0;1\}$, и введем обозначение $x^{i_k} \sim \begin{cases} x, & i_k = 1 \\ 1, & i_k = 0 \end{cases}$

Тогда полином Жегалкина можно записать как: $f(x) = \bigoplus\limits_i \alpha_i \cdot x_1^{i_1} \cdot x_2^{i_2} \cdot \ldots \cdot x_n^{i_n}$, где $\alpha_i \in \{0;1\}$.

Множество коэффициентов $\{\alpha_i\}$ можно рассматривать как функцию α, заданной на множестве индексов $i = (i_1, i_2, \dots i_n)$, то есть $\alpha : i \mapsto \alpha_i$.

Очевидно, функцию f можно записать и следующим образом: $f(x) = \bigoplus\limits_i \alpha_i \cdot [x_1, \text{ если } i_1] \cdot [x_2, \text{ если } i_2] \cdot \ldots \cdot [x_n, \text{ если } i_n]$.

Тут запись $[x_k, \text{ если } i_k]$ означает, что элелемент x_k присутствует в соответствующем члене полинома только если $i_k = 1$. Тогда если для какого-то x, $i \succ x*$,то в слагаемом будет существовать хотя бы один множитель, равный нулю, и такое слагаемое на сумму не повлияет. Отсюда ясно, что $f(x) = \bigoplus\limits_{i \preceq x} \alpha_i \quad (2)$ Найдем отображение $f \mapsto \alpha$ (То есть такое, которое по заданной функции вычисляет значения всех коэффициентов).

$* \, i \succ x$ обозначает, что x "меньше" i как последовательность бит

Теорема:

Пусть задана функция f. Тогда функцию α_x можно найти по формуле: $\alpha_x = \bigoplus\limits_{j \preceq x} f(j) \quad (3)$.

Доказательство:
▷

Докажем при помощи индукции по количеству единиц в векторе x (иначе говоря, по сумме $x_1 + x_2 + \ldots + x_n$) и для удобства обозначим это количество единиц(сумму) $wt(x)$.

1) База: если $x = 0$, то, очевидно $f(0) = \alpha_0$

2) Пускай теорема справедлива для всех сумм $wt(x) < k$. Покажем, что в таком случае она верна и для $wt(x) = k$. По (2), а далее по предположению индукции видим: $f(x) = \bigoplus\limits_{i \preceq x} \alpha_i = \left[\bigoplus\limits_{i \prec x} \bigoplus\limits_{j \preceq i} f(j) \right] \oplus \alpha_x$.

Рассмотрим сумму $\left[\bigoplus\limits_{i \prec x}\bigoplus\limits_{j \preceq i} f(j)\right]$. Каждый элемент $f(j)$ содержится в ней, только если $j \prec x$, и для фиксированных j и x элемент $f(j)$ встречается ровно столько раз, сколько существует i , таких, что $j \preceq i \prec x$. Несложно увидеть, что таких i существует ровно $2^{wt(x)-wt(j)} - 1$, то есть нечетное количество раз. Тогда $\left[\bigoplus\limits_{i \prec x}\bigoplus\limits_{j \preceq i} f(j)\right] = \bigoplus\limits_{j \prec x} f(j)$. Но тогда $f(x) = \left[\bigoplus\limits_{j \prec x} f(j)\right] \oplus \alpha_x \Leftrightarrow f(x) \oplus \bigoplus\limits_{j \prec x} f(j) = \alpha_x \Leftrightarrow \alpha_x = \bigoplus\limits_{j \preceq x} f(j)$.

То есть при $wt(x) = k$ формула также выполняется, значит при любых x выполняется $\alpha_x = \bigoplus\limits_{j \preceq x} f(j)$.

$\triangleleft$

Отображение $f \to \alpha$ также называется преобразованием Мёбиуса.

Видно, что (2) и (3) — это одно и тоже преобразование. Значит, если применить преобразование Мёбиуса к функции, а затем вновь применить то же преобразование к получившейся функции, тогда вновь получим исходную функцию f. То есть преобразование Мёбиуса обратно самому себе, иными словами, является инволюцией.

См. также

- Булевы функции
- Полные системы функций, теорема Поста
- ДНФ
- КНФ

Источники информации

- Статистика | Математика НГУ (http://www.stat-mat.com/?p=330)
- Википедия — Полином Жегалкина (http://ru.wikipedia.org/wiki/Полином_Жегалкина)
- Е.Л Рабкин, Ю.Б. Фарфоровская, дискретная математика (http://dvo.sut.ru/libr/himath/w163rabk/index.htm)
- Логачёв О.А, Сальников А.А., Ященко В.В. Булевы фунции в теории кодирования и криптологии — МЦНМО, 2004. - 470с. — ISBN 5-94057-117-4.

- Эта страница последний раз была отредактирована 4 сентября 2022 в 19:36.