Круговорот полиномов Жегалкина в природе

Ганцев Сергей Николаевич

January 22, 2023

Добрый день дорогие читатели. Хочу поделится одним моим случайным открытием. Не будем тянуть кота за хвост, поехали. Возьмем произвольный полином Жегалкина. Пусть это будет $P(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3 + x_2 + 1$. Тут знак сложения это операция исключающего "ИЛИ" (операция xor). Найдем для этого полинома таблицу истинности

x_1	x_2	x_3	$x_1x_2 + x_1x_3 + x_2x_3 + x_2 + 1$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	1

Запомним те значения x_1, x_2, x_3 при которых последняя колонка принимает нулевое значение. Плюс туда же добавим нулевой вектор $(0, 0, 0)$, он отвечает за свободный член полинома, в нашем случае он не нулевой. Получаем множество

$$\{(0, 0, 0), (0, 1, 0), (1, 0, 1)\}.$$

По этому множеству построим полином, где каждый вектор соответствует одночлену полинома и элемент вектора соотвествует переменной. Если элемент вектора равен единице, то переменная есть в одночлене. Нулевой вектор, как я и писал ранее, соотвествует свободному члену. И так, получаем $P^*(x_1, x_2, x_3) = x_1x_3 + x_2 + 1$. Ну и последний штрих, по этому полиному строим таблицу истинности.

x_1	x_2	x_3	$x_1x_3 + x_2 + 1$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Как и ранее, построим по нулям и нулевому вектору полином. И вот чудо, он совпадает с нашим исходным полиномом $P(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3 + x_2 + 1$.

В чем прелесть этой найденной закономерности? По сути это один из самых простых методов восстановления полинома из таблицы истинности. Нам нужно просто найти нули полинома построенного по заданной таблице истинности. Даже первоклашка справится.

Еще одно немало важное свойство найденной закономерности - это связь между одночленами полинома и его нулями. На основании нулей полинома P мы постороили полином P^*. При этом по нулям P^* однозначно строится полином P. Вот вам и круговорот полиномов Жегалкина.

Далее перейдем к формализации. Язык алгебры несколько сух, его могут разбавить только примеры либо геометрическая интерпритация. По возможности, я буду этим пользоваться.

Общий вид полинома Жегалкина.

$$P(x_1, ..., x_n) = a + \sum_{1 \le i_1 < ... < i_k \le n,\ 1 \le k \le n} a_{i_1,...,i_k} x_{i_1} \cdot \ldots \cdot x_{i_k}, \qquad a, a_{i_1,...,i_k} \in \{0, 1\}, \quad (1)$$

где знак "+" означает исключающее "или" (операция xor), а умножение - операция конъюнкции.

В дальнейшем, без ограничения общности, везде где мы упоминаем полином мы подразумеваем полином Жегалкина.

Обозначим через $E_2^n = \{0, 1\}^n$, т.е. это множество наборов n мерных наборов векторов элементы которых могут принимать значения 0 либо 1.

Под операцией конъюнкции $\wedge$ над двумя векторами будем понимать операцию побитовой конъюнкции (умножения) элементов с равными индексами.

Пример 1. $(1, 1, 1, 0, 0) \wedge (0, 1, 1, 1, 1) = (0, 1, 1, 0, 0)$.

В начале статьи приведен пример в котором по набору векторов строится полином и обратно по полиному строится набор векторов. Опишем процедуру построения полинома по заданному множеству векторов.

Возьмем произвольный набор вектров $\{V_i = (v_1^i, \ldots, v_n^i) \in E_2^n\}_{i=1}^m$. Нулевой вектор в наборе соотвествует свободному члену полинома (коэффициент a, см. формулу

(1)), если он присутствует в наборе то свободный член равнен единице. Если нулевого вектора нет то свободный член равен нулю. Каждый вектор набора соответствует определенному одночлену полинома. Если элемент v_l^i равен единице, то это значит что в i- м одночлене присутствует переменная x_l, где $l \in 1 \dots n$. Множество $\{V_i\}_{i=1}^m$ назовем *множеством одночленов полинома*.

Пусть Q - множество всех нулей произвольного полинома. *Сопряженным нулевым множеством полинома* будем называть объединение Q с нулевым ветором $(0, \dots, 0)$ если свободный член полинома равен единице. Если свободный член равен нулю, то берется просто множество Q.

Теорема 1 *Пусть P - произвольный полином, P^* - полином построенный по сопряженному нулевому множеству полинома P. Тогда сопряженное нулевое множество P^* совпадает с множеством одночленов полинома P.*

Пусть $\{V_i = (v_1^i, \dots, v_n^i) \in E_2^n\}_{i=1}^{m_v}$ - множество одночленов P. $\{Q_j = (q_1^j, \dots, q_n^j) \in E_2^n\}_{j=1}^{m_q}$ - сопряженное нулевое множество P.

Упростим формулы с индексами. В дальнейшем, если указывается индекс i то подразумевается что он может принимать значения от 1 до m_v и относится к множеству одночленов P. Аналогично, $j \in 1 \dots m_q$ и относится к сопряженному нулевому множеству полинома P.

Для доказательства теоремы достаточно показать что для любого i справедливо равенство

$$P^*(V_i) = 0. \tag{2}$$

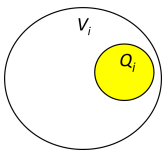
Нам достаточно рассмотреть только те Q_j для которых справедливо равенство $Q_j \wedge V_i = Q_j$. В случае если у нас $Q_j \wedge V_i \neq Q_j$ тогда значение одночлена P_j^* соответствующее вектору Q_j в точке V_i равно нулю. Для доказательства теоремы достаточно показать что количество одночленов m_q (количество одночленов полинома P^*) четное при нулевом свободном члене P и нечетное количество при свободном члене равном единице.

Одночлен соответствующий Q_j в точке V_i можно представить в виде:

$$P_j^*(v_1^i, \dots, v_n^i) = \left(v_1^i\right)^{q_1^j} \cdot \dots \cdot \left(v_n^i\right)^{q_n^j}. \tag{3}$$

Неравенство $Q_j \wedge V_i \neq Q_j$ означает, что существует k при котором $q_k^j = 1$ и $v_k^i = 0$, $1 \leq k \leq n$. Соотвественно, $\left(v_k^i\right)^{q_k^j} = 0$ и в месте с этим наш одночлен также равен нулю.

Геометрически $Q_j \wedge V_i = Q_j$ выглядит следующим образом



Пример 2. Пусть $Q_1 = (0,0,1,1)$ и $V_i = (1,1,1,0)$. Согласно формуле (3)

$$P_1^*(1,1,1,0) = 1^0 \cdot 1^0 \cdot 1^1 \cdot 0^1 = 0.$$

Заметим, что в этом примере $P_1^*(x_1,x_2,x_3,x_4) = x_3x_4$. Получаем аналогичный результат

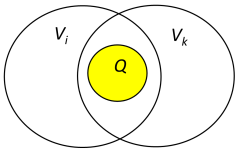
$$P_1^*(1,1,1,0) = 1 \cdot 0 = 0.$$

Пусть теперь $Q_1 = (0,0,1,1)$ и $V_i = (1,1,1,1)$. В этом случае $P_1^*(1,1,1,1) = 1$.

Подсчитаем максимальное количество возможных одночленов P_j^* равных единице в точке V_i. Допустим у вектора V_i количество ненулевых элементов равно N_i. Количество всевозможных векторов $V \in E_2^n$ таких что $V \wedge V_i = V$ равно $2^{N_i} - 1$. Это нетрудно посчитать, нужно убрать все нулевые элементы в векторе V_i, останется вектор размерности N_i. Количество векторов побитово меньших (кроме нулевого) этого вектора и есть искомое количество.

И так, нам нужно показать справедливость равенства (2) для любого V_i при условии $Q_j \wedge V_i = Q_j$.

Пусть для некоторого $k \in 1 \dots n$ справедливо неравенство $V_k \wedge V_i \neq V_k$. Если говорить простыми словами, существует индекс $l \in 1 \dots n$ такой что $v_l^k = 1$ и $v_l^i = 0$. Для таких векторов $P_k(Q) = 0$ при условии $Q \wedge V_i = Q$, где $Q = (q_1, \dots, q_n) \in E_2^n$. Покажем это. У нас существует l при котором $v_l^i = 0$, элементы вектора Q могут принимать значение единицы только там где элементы V_i равны единице, следовательно $q_l^i = 0$. Соответственно, $V_k \wedge Q \neq V_k$ и как следствие $P_k(Q) = 0$. Наглядно это видно на рисунке:

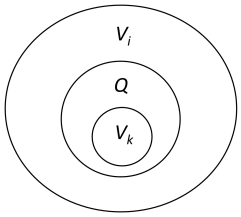


Можно сделать вывод что одночлены P_k не влияют на нули P поскольку всегда равны нулю при условии $Q_j \wedge V_i = Q_j$. Поэтому мы можем их убрать из полинома P.

Далее мы постепенно будет строить полином P начиная с одночлена P_i добавляя все оставшиеся полиномы. P_i равен единице для всех $Q \in E_2^n$ при условии $V_i \wedge Q = V_i$. И с учетом того что $Q \wedge V_i = Q$ получаем что P_i принимает значение единицы только в точке V_i. На текущем этапе построения P количество нулей равно четному числу $2^{N_i} - 2$, где N_i - количество единиц в векторе V_i.

Осталось добавить оставшиеся полиномы для которых $V_k \wedge V_i = V_k$. Пусть $Q \in E_2^n$ и $Q \wedge V_i = Q$. У вектора Q единичные элементы возможны только на тех позициях что и у V_i только с меньшим либо равным количеством. Далее одночлен $P_k(Q)$ равен единице только при условии $V_k \wedge Q = V_k$. Тут у вектора V_k единичные элементы возможны только на тех позициях что и у Q только с меньшим либо

равным количеством. Поэтому количество таких Q будет равно $2^{N_i - N_k}$, где N_i, N_k - количество единиц у векторов V_i и V_k. Наглядно это можно представить так:



Соберем все детали нашего конструктора. Мы рассматриваем только те нули полинома P которые удовлетворяют равенству $Q_j \wedge V_i = Q_j$. Нужно показать что их четное количество, только в этих одночленах $P_j^*(V_i)$ равны единице.

У P_i количество нулей $2^{N_i} - 2$. V_k для которых $V_k \wedge V_i \neq V_k$ мы не учитываем. У каждого V_k для которого $V_k \wedge V_i = V_k$ количество единиц равно $2^{N_i - N_k}$. Полином $P_i + P_k$ будет содержать четное количество нулей, поскольку количество единиц которое влияют на область значений P_i при прибавлении P_k четное. Ничто нам не мешает прибавить все оставшиеся V_k для которых $V_k \wedge V_i = V_k$. Получившийся полином совпадает с P в точках $Q \wedge V_i = Q$ и содержит четное количество элементов. Теорема доказана.

Стойте, последний штрих. Я тут почти забыл про ненулевой свободный член полинома P. Давайте разберемся. У P_i количество нулей $2^{N_i} - 2$. У $P_i + 1$ один только ноль в точке V_i. Каждое V_k для которого $V_k \wedge V_i = V_k$ прибавляет к области значений четное количество единиц. Следовательно, количество нулей при ненулевом свободном члене P равно нечетному количество. Ух, теперь точно все. Отдыхаем!

gantsevsn@gmail.com