Алгоритмы нахождения полинома Жегалкина

Н.А. Перязев

Санкт-Петербургский государственный электротехнический университет
«ЛЭТИ» им. В. И. Ульянова (Ленина)

2021

Полином Жегалкина и его вектор

- Общий вид полинома Жегалкина:

$$a_{0\ldots0} \oplus a_{0\ldots01}x_n \oplus \ \ldots \oplus a_{1\ldots10}x_1\ldots x_{n-1} \oplus a_{1\ldots1}x_1\ldots x_n$$

где коэффициенты $a_{i_1\ldots i_n} \in \{0, 1\}$.

- Любая булева операция единственным образом представима полиномом Жегалкина.

$$f(x_1, \ldots, x_n) = a_{0\ldots0} \oplus a_{0\ldots01}x_n \oplus \ \ldots \oplus a_{1\ldots10}x_1\ldots x_{n-1} \oplus a_{1\ldots1}x_1\ldots x_n$$

Вектор $P(f) = (a_{0\ldots0}, a_{0\ldots01}, \ \ldots, a_{1\ldots10}, a_{1\ldots1})$ называем вектором полинома Жегалкина для операции f.

Матричный метод

$$S_0 = (1),\ S_i = \begin{pmatrix} S_{i-1} & 0 \\ S_{i-1} & S_{i-1} \end{pmatrix},\ P(f) = S_n \times f.$$

Сложность: $L(n) = 2^n(2^n + (2^n - 1)) = 2^{2n+1} - 2^n$.

Пример для $f = (00101001)$

$$P(f) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

$f = x_2 \oplus x_2x_3 \oplus x_1 \oplus x_1x_3 \oplus x_1x_2x_3;\ L(3) = 120.$

Метод треугольника (Супрун В.П., 1987г.)

Рассмотрим на примере. Пусть $f = (00101001)$

x_1	x_2	x_3	f							
0	0	0	0							
0	0	1	0	0						
0	1	0	1	1	1					
0	1	1	0	1	0	1				
1	0	0	1	1	0	0	1			
1	0	1	0	1	0	0	0	1		
1	1	0	0	0	1	1	1	1	0	
1	1	1	1	1	1	0	1	0	1	1

Сложность: $L(n) = (2^n - 1) + ... + 2 + 1 = 2^{2n-1} - 2^{n-1}$.

$P(f) = (00111101)$

$f = x_2 \oplus x_2x_3 \oplus x_1 \oplus x_1x_3 \oplus x_1x_2x_3$; $L(3) = 28$.

Метод четности остаточных операций

Остаточная нулевая и единичная операции от f по x_i определяются так:

$$f^0_{x_i}(x_1, ..., x_{i-1}, x_{i+1}, ..., x_n) = f(x_1, ..., x_{i-1}, 0, x_{i+1}, ..., x_n);$$

$$f^1_{x_i}(x_1, ..., x_{i-1}, x_{i+1}, ..., x_n) = f(x_1, ..., x_{i-1}, 1, x_{i+1}, ..., x_n).$$

Четность операции $Zf = f(0, ..., 0) \oplus ... \oplus f(1, ..., 1)$.

Тогда $a_{i_1 ... i_n} = Zf^{0 ... 0}_{x_{j_1} ... x_{j_s}}$, где $\{j_1, ..., j_s\} = \{i_k | i_k = 0\}$.
Сложность:
$L(n) = (2^1 - 1)C^1_n + (2^2 - 1)C^2_n + ... + (2^n - 1)C^n_n = 3^n - 2^n$.
Пример для $f = (0010\ 1001)$

$$a_{000} = Zf^{000}_{x_1x_2x_3} = Z(0) = 0; \quad a_{100} = Zf^{00}_{x_2x_3} = Z(01) = 1;$$
$$a_{001} = Zf^{00}_{x_1x_2} = Z(00) = 0; \quad a_{101} = Zf^{0}_{x_2} = Z(0010) = 1;$$
$$a_{010} = Zf^{00}_{x_1x_3} = Z(01) = 1; \quad a_{110} = Zf^{0}_{x_3} = Z(0110) = 0;$$
$$a_{011} = Zf^{0}_{x_1} = Z(0010) = 1; \quad a_{111} = Zf = Z(00101001) = 1.$$

$f = x_2 \oplus x_2x_3 \oplus x_1 \oplus x_1x_3 \oplus x_1x_2x_3$; $L(3) = 19$.

Метод деления вектора пополам

Пусть $f'_{x_i} = f^0_{x_i} \oplus f^1_{x_i}$ – производная f по x_i.
Рекуррентно строим последовательность: $f_0, f_1, ..., f_n$:
$f_0 = f, \quad f_i = \bar{x}_i (f_{i-1})^0_{x_i} \oplus x_i (f_{i-1})'_{x_i}$ где $i = 1, ..., n$.
Тогда $P(f) = f_n$.
Сложность: $L(n) = n2^{n-1}$.

Пример для $f = (0010\ 1001)$
$f_0 = (0010\ 1001)$
$f_1 = (0010\ 1011)$
$f_2 = (0010\ 1001)$
$f_3 = (0011\ 1101)$

$P(f) = (0011\ 1101)$
$f = x_2 \oplus x_2x_3 \oplus x_1 \oplus x_1x_3 \oplus x_1x_2x_3$; $L(3) = 12$.