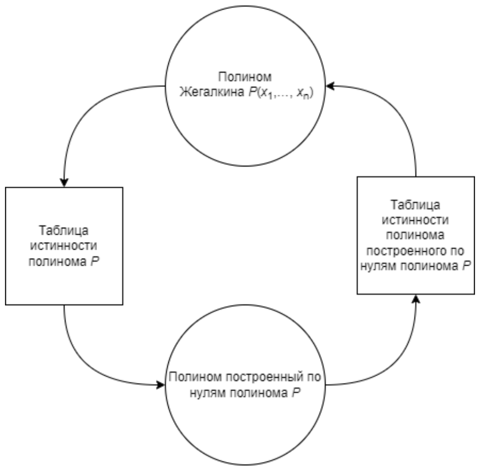
Об одной особенности представления решений бинарных уравнений

Ганцев Сергей Николаевич

October 12, 2022

В данной статье рассмотрим полином построенный по нулям полинома Жегалкина. Покажем что уже по нулям этого нового полинома можно восстановить исходный полином. Схематично это можно представить так:



Символом $+$ обозначаем операцию xor (исключающее "ИЛИ"). Таблица истинности:

a	b	$a+b$
0	0	0
0	1	1
1	0	1
1	1	0

Также мы будем использовать бинарную операцию коньюнкции. В формулах мы не будем ее как-то выделять. Например, под ab мы подразумеваем $a \cdot b$. Таблица истинности:

a	b	ab
0	0	0
0	1	0
1	0	0
1	1	0

В данной статье мы приведем достаточно интересную характеристику решений булевых уравнений. Без потери общности мы считаем левая часть уравнения представляет собой полином Жегалкина.

Общий вид полинома Жегалкина

$$P(x_1, ..., x_n) = a + a_1x_1 + a_2x_2 + \ldots + a_nx_n + a_{12}x_1x_2 + a_{13}x_1x_3 + \ldots + a_{1\ldots n}x_1 \ldots x_n,$$

где $a, a_1, \ldots, a_{1\ldots n} \in \{0, 1\}$.

И более формализованный вид

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

Пример 1. Полином Жегалкина

$$P(x_1, x_2) = x_1x_2 + x_1 + x_2 + 1.$$

В дальнейшем мы будем считать что все полиномы упомянутые в статье это полиномы Жегалкина.

Определение 1 *Построим множество состоящее из ненулевых членов полинома. Т.е. это множество тех членов полинома у которых коэффициенты $a, a_{i_1,\ldots,i_k}$ не равны нулю. Первоначально добавим к этому множеству вектор размерности n с нулевыми значениями $(0, \ldots, 0)$ при условии что коэффициент $a = 1$. Для каждого члена с ненулевым коэфициентом $a_{i_1,\ldots,i_k}$ сопоставим вектор размерности n где на позициях $i_1, \ldots, i_k$ стоят единицы, на остальных позициях нули. Назовем множество таких векторов как* ***множество одночленов*** *полинома.*

Множество одночленов полинома с взаимо однозначно соотвестветствует полиному из которого оно построено. Т.е. по множеству одночленов полинома можно однозначно построить исходный полином и наоборот. Это следует из самой методики построения такого множества.

Пример 2. Множество одночленов. По полиному из **Примера 1** множество одночленов полинома равно $\{(0, 0), (1, 1), (1, 0), (0, 1)\}$. Допустим у нас исходный полином принимает вид $P(x_1, x_2) = x_1x_2 + x_1 + x_2$. Тут нет коэффициента a. Тогда множество одночленов равно $\{(1, 1), (1, 0), (0, 1)\}$.

Определение 2 *Таблицу истинности для полинома обозначим через*

$$T = \{A^i = (a_1^i, \ldots, a_n^i), P(a_1^i, \ldots, a_n^i)\}_{i=1}^{2^n},$$

где $a_k^i \in \{0,1\}, k = 1 \ldots n$. *Она состоит из всевозможных переборов* n *мерного вектора* A^i *и результата вычисления* $P(a_1^i, \ldots, a_n^i)$.

Не ограничивая общности можно считать что $A_1 = (0, \ldots, 0)$. Мы это можем сделать поскольку перебираются всевозможные значения n мерного вектора в таблице T.

Определение 3 *Сопряженным множеством полинома* P *будем считать множество*

$$M^* = \left\{ (0, \ldots, 0) \Big|_{P(0,\ldots,0)=1} \right\} \cup \left\{ A_i \Big|_{P(a_1^i,\ldots,a_n^i)=0} \right\}_{i=2}^{2^n},$$

где $T = \{A^i = (a_1^i, \ldots, a_n^i), P(a_1^i, \ldots, a_n^i)\}_{i=1}^{2^n}$ *- таблица истинности для* P.

Сопряженное множество это набор векторов A_i для случая когда $P(a_1^i, \ldots, a_n^i) = 0, i = 2, \ldots, n$. Плюс туда добавляется нулевой вектор когда $a = 1$ (свободный член P).

Для полинома из **Пример 1** сопряженное множество равно $\{(0,0), (1,1), (1,0), (0,1)\}$.

Определение 4 *Сопряженным полиномом* P^* *будем считать полином построенный по сопряженному множеству* M^*.

Поясню что означает построение полинома. M^* представляет собой набор векторов размерности n. Они заполнены нулями и единицами. Позиция единиц определяют переменные одночлена. Например, вектор $(0,0,1,0,1,0)$ показывает что в полиноме есть одночлен $x_3 x_5$.

Пример 3. Пусть $P(x_1, x_2) = x_1 x_2 + x_2$. Таблица истинности:

a	b	$x_1 x_2 + x_2$
0	0	0
0	1	1
1	0	0
1	1	0

Сопряженное множество $M^* = \{(1,0), (1,1)\}$. Сопряженный полином $P^*(x_1, x_2) = x_1 + x_1 x_2$.

Мы плавно подошли к основному результату статьи.

Теорема 1 *Пусть* P^* *- сопряженный полином к* P. *Тогда сопряженный полином к* P^* *совпадает с* P

Доказательство. Доказательство в следующей версии статьи ...

Пример 4. Пусть $P(x_1, x_2) = x_1x_2x_3 + x_1x_3 + x_3 + 1$. Таблица истинности:

x_1	x_2	x_3	$x_1x_2x_3 + x_1x_3 + x_3 + 1$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

Сопряженное множество $M^* = \{(0,0,0),(0,0,1),(0,1,1),(1,1,1)\}$. Сопряженный полином $P^*(x_1, x_2, x_3) = x_1x_2x_3 + x_2x_3 + x_3 + 1$. Таблица истинности для P^*:

x_1	x_2	x_3	$x_1x_2x_3 + x_2x_3 + x_3 + 1$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

Сопряженное множество к P^* равно $\{(0,0,0),(0,0,1),(1,0,1),(1,1,1)\}$. Сопряженный полином к P^* равен $x_1x_2x_3 + x_1x_3 + x_3 + 1$. Он совпадает с исходным полиномом.

email: gantsevsn@gmail.com