Полиноми на Жегалкин

Това е ф-ла над я-вото функции $\{\bar{0}, \tilde{1}, \&(\wedge), \oplus\}$.

<u>Th</u> | Всяка булева ф-я има единствен полином на Жегалкин.

За $f \in \mathcal{F}_2^n$

$$f(x_1, \dots, x_n) = a_0 \oplus a_1 \& x_1 \oplus \dots \oplus a_n \& x_n \oplus$$
$$a_{n+1} \& x_1 \& x_2 \oplus \dots \oplus a_{n+\binom{n}{2}} \& x_{n-1} \& x_n \oplus \dots$$
$$\dots \oplus a_{2^n-1} \& x_1 \& x_2 \& \dots \& x_n$$

с $\alpha = \langle a_0, a_1, \dots, a_{2^n-1} \rangle \in \mathcal{J}_2^{2^n}$.

$\forall f$ $\qquad a_i \in \{0,1\}$

Т.е. всяка една конюнкция i ще участва в дизюнкцията от изброените или не, и това се определя от съответния коеф. $a_i \in \{0,1\}$.

Значи, че $|\mathcal{Y}_2^{2^n}| = |\{\langle a_0, \ldots, a_{2^n-1}\rangle \mid a_i \in \{0,1\}\}| = 2^{2^n} = |F_2^n|$.

Дължина на ПЖ - броят ненулевите елементи в сумата.

Степен на ПЖ: Максималният ранг на елементарна конюнкция в полинома.

Ранг на елем. кон.: брой на различните букви в нея.

Построяване на полином на Жегалкин

a) Чрез еквивалентни преобразувания на ф-ли.

Т.к. $\boxed{\{\tilde{1}, \tilde{0}, \&, \oplus\} \text{ е пълно}}$, то можем всяка булева ф-я да я изразим чрез тях.

$$x^{\sigma} = \begin{cases} x, & \sigma = 1 \\ \bar{x}, & \sigma = 0 \end{cases}$$

b) От съвърш. ДНФ

Нека $f(\tilde{x}^3) = \langle 0\,1\,1\,0\,1\,0\,0\,0 \rangle$.

$$\begin{array}{cccccccc} 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{array}$$

$$f(\tilde{x}^3) = \bigvee_{\substack{\alpha \in J_2^3 \\ f(\alpha) = 1 \\ \alpha = \langle \sigma_1, \sigma_2, \sigma_3 \rangle}} x_1^{\sigma_1} . x_2^{\sigma_2} . x_3^{\sigma_3}$$

Тогава СъвДНФ

$$f(\tilde{x}^3) \equiv \bar{x}_1.\bar{x}_2.x_3 \vee \bar{x}_1.x_2.\bar{x}_3 \vee x_1.\bar{x}_2.\bar{x}_3$$

Сега използваме, че

- заменяме $\vee$ с $\oplus$, защото винаги точно една конюнкция е вярна
- използваме дистрибутивен закон

$$x \& (y \oplus z) \equiv (x \& y) \oplus (x \& z)$$

• Комутативност на & ⊕

• Асоциативност на & ⊕

• $x \,\&\, x = x$; $\quad x \oplus \tilde{0} = x$;

$\boxed{x \oplus x = \tilde{0}}$; $\quad x \,\&\, \tilde{0} = \tilde{0}$;

$x \oplus \bar{x} = \tilde{1}$; $\quad x \,\&\, \tilde{1} = x$

$x \,\&\, \bar{x} = \tilde{0}$; $\quad \boxed{x \oplus \tilde{1} = \bar{x}}$

$\tilde{1} \oplus \tilde{1} = \tilde{0}$; $\quad \tilde{0} \oplus \tilde{0} = \tilde{0}$

$\{\tilde{0}, \tilde{1}, \wedge, \oplus\}$

Така $f(\tilde{x}^3) \dashv\vdash \bar{x}_1.\bar{x}_2.x_3 \vee \bar{x}_1.x_2.\bar{x}_3 \vee x_1.\bar{x}_2.\bar{x}_3 \dashv\vdash$

$\bar{x}_1.\bar{x}_2.x_3 \oplus \bar{x}_1.x_2.\bar{x}_3 \oplus x_1.\bar{x}_2.\bar{x}_3 \dashv\vdash$

$(x_1 \oplus \tilde{1}).(x_2 \oplus \tilde{1}).x_3 \oplus (x_1 \oplus \tilde{1}).x_2.(x_3 \oplus \tilde{1}) \oplus x_1.(x_2 \oplus \tilde{1}).(x_3 \oplus \tilde{1})$

$\dashv\vdash (x_1.x_2 \oplus x_1 \oplus x_2 + \tilde{1}).x_3 \oplus (x_1.x_3 \oplus x_1 \oplus x_3 \oplus \tilde{1}).x_2 \oplus$

$(x_2.x_3 \oplus x_2 \oplus x_3 + \tilde{1}).x_1 \dashv\vdash$

$\cancel{x_1.x_2.x_3} \oplus \cancel{x_1.x_3} \oplus \cancel{x_2.x_3} \oplus x_3 \oplus \cancel{x_1.x_2.x_3} \oplus \cancel{x_1.x_2} \oplus \cancel{x_3.x_2} \oplus$

$x_2 \oplus x_1.x_2.x_3 \oplus \cancel{x_1.x_2} \oplus \cancel{x_1.x_3} \oplus x_1 \dashv\vdash$

$x_1.x_2.x_3 \oplus x_1 \oplus x_2 \oplus x_3 \dashv\vdash x_1 \oplus x_2 \oplus x_3 \oplus x_1.x_2.x_3$

c) Чрез метод на неопределените коеф.

Нека $f \in F_2^n \rightsquigarrow f(x_1, \dots, x_n) = f(\tilde{x}^n)$.

или $\underbrace{P_f(x_1, \dots, x_n)}_{= f(x_1, \dots, x_n)} = a_0 \oplus a_1 x_n \oplus \dots \oplus a_{2^n - 1} x_1 \dots x_n$.

Съставяме и решаваме следната система от уравнения, за да определим неизвестните $\boxed{a_0, \dots, a_{2^n-1}}$

$$\left|\begin{array}{l} P_f(0, 0, \dots, 0) = f(0, 0, \dots, 0) \\ P_f(0, 0, \dots, 0, 1) = f(0, 0, \dots, 0, 1) \\ \dots \\ P_f(1, 1, \dots, 1, 1) = f(1, 1, \dots, 1, 1) \end{array}\right.$$

Нека $f(\tilde{x}^3) = \langle 10110100 \rangle$ $\quad x\,y\,z$

Тогава

$P_f(x,y,z) = a_0 \oplus a_1.x \oplus a_2 y \oplus a_3 z \oplus a_4 xy \oplus a_5 xz \oplus a_6 yz \oplus a_7 xyz$

$P_f(0,0,0) = f(0,0,0) \to \boxed{a_0 = 1}$

$P_f(0,0,1) = f(0,0,1) \to 1 \oplus a_3 = 0 \to \boxed{a_3 = 1}$

$P_f(0,1,0) = f(0,1,0) \to 1 \oplus a_2 = 1 \to \boxed{a_2 = 0}$

$P_f(0,1,1) = f(0,1,1) \to \underbrace{1 \oplus 1}_{0} \oplus a_6 = 1 \to \boxed{a_6 = 1}$

$P_f(1,0,0) = f(1,0,0) \to 1 \oplus a_1 = 0 \to \boxed{a_1 = 1}$

$P_f(1,0,1) = f(1,0,1) \to 1 \oplus 1 \oplus 1 \oplus a_5 = 1 \to \boxed{a_5 = 0}$

$P_f(1,1,0) = f(1,1,0) \to 1 \oplus 1 \oplus a_4 = 0 \to \boxed{a_4 = 0}$

$P_f(1,1,1) = f(1,1,1) \to 1 \oplus 1 \oplus 1 \oplus 1 \oplus a_7 = 0 \quad \boxed{a_7 = 0}$

Тоест

$f(\tilde{x}^3) = 1 \oplus x \oplus z \oplus y.z$

Зад. Да се намери полинома на Жегалкин на функцията.

a) $f(x,y) \rightleftharpoons x \vee y$

b) $f(x,y) \rightleftharpoons \langle 1001 \rangle$

c) $f(x,y,z) \rightleftharpoons \langle 01101000 \rangle$

d) $f(x,y,z) \rightleftharpoons \langle 11111000 \rangle$

e) $f(x,y,z) \rightleftharpoons (x \mid y) \downarrow z$ Nand Nor

f) $f(x,y,z) \rightleftharpoons (x \to y) \,\&\, (y \downarrow z)$

g) $f(x,y,z) \rightleftharpoons ((x \to y) \vee z) \mid x.$

$(x \mid y) \downarrow z \Leftrightarrow \overline{(x \wedge y)} \downarrow z \Leftrightarrow \overline{\overline{(x \wedge y)} \vee z} \Leftrightarrow$

$xy.\bar{z} \Leftrightarrow x.y(1 \oplus z) \Leftrightarrow x.y \oplus xyz$

$\Leftrightarrow (\bar{x} \vee y).\overline{(y \vee z)} \Leftrightarrow \overline{x.\bar{y}}.\bar{y}.\bar{z} \Leftrightarrow (x.(1 \oplus y) \oplus 1)(1 \oplus y)(1 \oplus z).$

$$\dashv\vdash \left(x.(\tilde{1} \oplus y) \oplus \tilde{1} \right)(\tilde{1} \oplus y) \quad \dashv\vdash (x \oplus x.y \oplus \tilde{1}).(\tilde{1} \oplus z \oplus y \oplus yz)$$

$(\tilde{1} \oplus z)$

$$\dashv\vdash x \oplus x.y \oplus \tilde{1} \oplus x.z \oplus \cancel{x.y} \oplus \cancel{z} \oplus \cancel{x.y} \oplus \cancel{x.y} \oplus \cancel{xy}z \oplus \cancel{\tilde{1}} \oplus \cancel{z} \oplus y \oplus yz \dashv\vdash x \oplus y \oplus x.y \oplus y.z$$

g) $f(x,y,z) \equiv ((x \to y) \vee z) \mid x.$

$$\overline{(\bar{x} \vee y \vee z).x} \dashv\vdash \overline{(x.\bar{y}.\bar{z}).x} \dashv\vdash \overline{(x.(1 \oplus y).(1 \oplus z)).x}$$

$$\dashv\vdash (x \oplus x.y \oplus x.z \oplus x.y.z \oplus 1).x \oplus 1 \dashv\vdash$$

$$\cancel{x} \oplus xy \oplus x.z \oplus x.y.z \oplus \cancel{x} \oplus 1 \dashv\vdash 1 \oplus x.y \oplus x.z \oplus x.y.z$$

(300) Да се намери броят на булевите вектори с дължина n, за които полиномът

$P(x_1, \dots, x_n) = x_1 \dots x_k \oplus x_{k+1} \dots x_n$ приема

ст-т 1.

Сметане на 0-ите.

$\to 1 \oplus 1 \to \langle 1, \dots 1 \rangle \to 1$ вектор.

$\to 0 \oplus 0$

$|\{\alpha \mid \alpha \in J_2^k \ \& \ \omega(\alpha) < k\}| = 2^k - 1$

$|\{\alpha \mid \alpha \in J_2^{n-k} \ \& \ \omega(\alpha) < n-k\}| = 2^{n-k} - 1$

Търсени случаи: $2^n - ((2^k - 1) \cdot (2^{n-k} - 1) + 1) =$

$= 2^n - 1 - (2^n - 2^k - 2^{n-k} + 1) =$

$= \cancel{2^n} - 1 - \cancel{2^n} + 2^k + 2^{n-k} - 1 = 2^k + 2^{n-k} + 2$

Минимизация на двоични ф-ции

(Минимални покрития)

def | Една елем. конюнкция k е <u>импликанта за ф-я f</u>, ако

$\underline{\mathbb{1}(k)} \subseteq \underline{\mathbb{1}(f)}$

Единиците ѝ са единици на f.

def | Проста импликанта.

k е <u>проста имп.</u> за f, ако

(i) k е имп. за f.

(ii) $\neg \exists k'$ (k' имп. за f и $\mathbb{1}(k) \subseteq \mathbb{1}(k') \subseteq \mathbb{1}(f)$)

Т.е., ако махнем буква от k, то

тя престава да бъде <u>импликанта</u>.

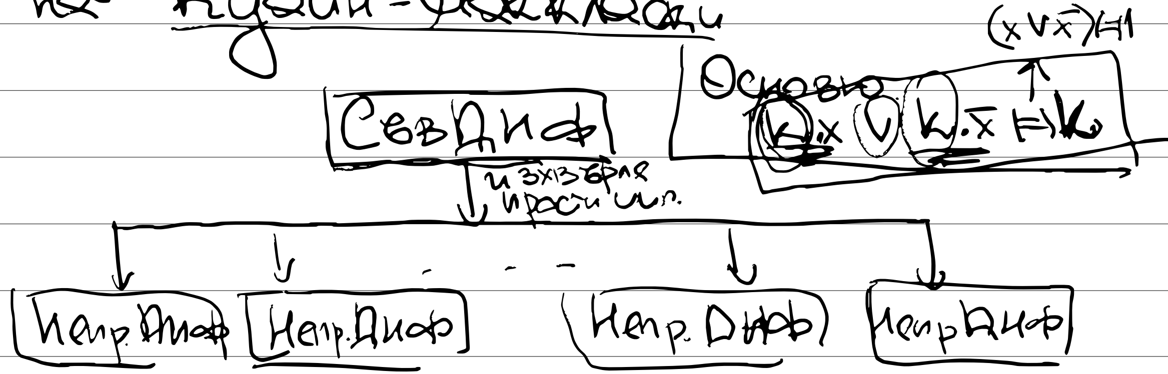
def | • Сложност на ДНФ - броят букви които я формират

• Всяка минимална ДНФ се състои от прости импликанти (подбрани да покриват единиците на f)

• Съкратена ДНФ - всички прости импликанти

• Неприводима ДНФ - ако махнем кой да е прост импликант, то тя престава да представя ф-ята. Една ф-я може да има повече от една неприводима ДНФ. Минималните ДНФ се определят от неприводимите.

Т.к. не ефективно с пълно изчерп. за търсене минимални покрития ще се запознаем с алгоритъма на Куайн-Маккласки



Всеки от неприводимите, чийто брой букви е минимален, се наричат минимални ДНФ.

Идеята е да започнете от всички импликанти и да ги сведете до прости.
Ако сформирате дизюнкция от простите импликанти ще получите Съкратена ДНФ.
Оттам нататък, за да получите неприводими ДНФ, от които ще подберете минималните, то трябва да вземете простите импликанти и да видите кои единици покриват f.

Оттам нататък можете да получите различни (или единствени) варианти за неприводими ДНФ. От тях избираме минималните които искаме да са с възможно най-малка дължина (колкото може по-малко букви в записа (знаци &, v, ¬)).

зад $f \in F_2^3$. По метод на Куайн-Маккласки генерирайте мин. ДНФ на f

a) $f = \langle 01010001 \rangle$

b) $f = \langle 10000010 \rangle$

c) $f = \langle 01110101 \rangle$

d) $f = \langle 11111111 \rangle$

e) $f = \langle 11100111 \rangle$

* може да има прости импликанти от различен ред!

Съкратено ДНФ ≡ всички прости импликанти съдържа, а мин. ДНФ = след избор на някои от простите имп., т.е. всички 1-ци да са покрити и да е минимален броя на импликантите

Зад. Намерете всички минДНФ на

a) $f = \langle 1101001110101010 \rangle$

b) $f = \langle 0110101111010001 \rangle$

Критерий за пълнотата на мн-во от булеви функции

Затворени подмн-во на $\mathcal{F}_2$, максимални подмн-во на $\mathcal{F}_2$, които не са пълни:

- $T_0 \leftrightharpoons \{ f \mid f \in \mathcal{F}_2 \ \& \ f(\tilde{0}) = 0 \}$

запазващи нулата ф-ции

- $T_1 \leftrightharpoons \{ f \mid f \in \mathcal{F}_2 \ \& \ f(\tilde{1}) = 1 \}$

запазващи единицата ф-ции

- $S \leftrightharpoons \{ f \mid f \in \mathcal{F}_2 \ \& \ f(\alpha) = f(\bar{\alpha}) \}$

самодвойнствени ф-ции.

вектори от 0-ци и 1-ци за f.

- $M \leftrightharpoons \{ f \mid f \in \mathcal{F}_2 \ \& \ [\alpha \preceq \beta \Rightarrow f(\alpha) \le f(\beta)] \}$

монотонни ф-ции

$\preceq$ – частична наредба предшествие (хиперкуб върховете)

• $L = \{ f \mid f \in \mathcal{F}_2 \ \& \ f = a_0 \oplus a_1 x_1 \oplus \dots \oplus a_n x_n$ за $a_i \in \{0,1\} \}$

линейни функции

<u>Th | Пост-Яблонски</u>

Нека $F \subseteq \mathcal{F}_2$.

F е пълно $\iff F \not\subseteq T_0, F \not\subseteq T_1, F \not\subseteq L,$
$F \not\subseteq M, F \not\subseteq S.$

<u>Следствие |</u>

една ф-я f е Шеферова, ако $[\{f\}] = \mathcal{F}_2$.

за $f \in \mathcal{F}_2$:

$\{f\}$ е пълно $\iff f \notin T_0 \cup T_1 \cup S$

(зад) Да се намери броят на шеферовите ф-ции на n променливи.

302 Да се провери пълно ли е м-вото от булеви ф-ции:

a) $\{x \to y,\ x \to y \& z\}$

b) $\{x \& y,\ \bar{x} \leftrightarrow y \& z\}$

c) $\{\langle 01101001\rangle,\ \langle 10001101\rangle,\ \langle 00011100\rangle\}$