Построяване на полином на Жегалкин

a) Чрез еквивалентни преобразования на ф-ли.

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

b) От Съвърш. ДНФ

Нека $f(\tilde{x}^3) = \langle \overset{000}{0}\overset{001}{1}\overset{010}{1}\overset{011}{1}\overset{100}{0}\overset{101}{1}\overset{110}{0}\overset{111}{0} \rangle$.

Тогава СъвДНФ.

$f(\tilde{x}^3) = \bar{x} \& \bar{y} \& z \vee \bar{x} \& y \& \bar{z} \vee x \& \bar{y} \& \bar{z}$

Сега използваме, че

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

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

- Комутативност на &, ⊕
- Асоциативност на &, ⊕
- $x \& x = x$; $x \oplus \tilde{0} = x$;
$x \oplus x = \tilde{0}$; $x \& \tilde{0} = \tilde{0}$;
$x \oplus \bar{x} = \tilde{1}$; $x \& \tilde{1} = x$
$x \& \bar{x} = \tilde{0}$; $x \oplus \tilde{1} = \bar{x}$
$\tilde{1} \oplus \tilde{1} = \tilde{0}$; $\tilde{0} \oplus \tilde{0} = \tilde{0}$

$f(\tilde{x}^3) \models \bar{x} \& \bar{y} \& z \vee \bar{x} \& y \& \bar{z} \vee x \& \bar{y} \& \bar{z} \models$
$(1 \oplus x).(1 \oplus y).z \oplus (1 \oplus x).y.(1 \oplus z) \oplus x.(1 \oplus y).(1 \oplus z) \models$
$(1 \oplus x \oplus y \oplus x.y).z \oplus (1 \oplus x \oplus z \oplus x.z).y \oplus (1 \oplus y \oplus z \oplus yz).x \models$
$z \oplus \cancel{xz} \oplus \cancel{yz} \oplus \cancel{xyz} \oplus y \oplus \cancel{xy} \oplus \cancel{yz} \oplus \cancel{xyz} \oplus x \oplus \cancel{xy} \oplus$
$\cancel{xz} \oplus xyz \models x \oplus y \oplus z \oplus xyz$

c) Чрез метод на неопределените коеф.

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

Има $P_f(x_1, .., x_n) = a_0 \oplus a_1 x_n \oplus ... \oplus a_{2^n-1} x_1 ... x_n$.

$\overset{f(x_1,..,x_n)}{\models}$

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

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

Εστω $f(\bar{x}^3) = \langle \underbrace{1}_{000}\, \underbrace{0}_{001}\, \underbrace{1}_{010}\, \underbrace{1}_{011}\, \underbrace{0}_{100}\, \underbrace{1}_{101}\, \underbrace{0}_{110}\, \underbrace{0}_{111} \rangle$.

Τοτε

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

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

$$P_f(0,0,1) = f(0,0,1) \to a_0 \oplus a_3 = 0 \Leftrightarrow \boxed{a_3 = 1.}$$

$$P_f(0,1,0) = f(0,1,0) \to a_0 \oplus a_2 = 1 \Leftrightarrow \boxed{a_2 = 0}$$

$$P_f(1,0,0) = f(1,0,0) \to a_0 \oplus a_1 = 0 \Leftrightarrow \boxed{a_1 = 1}$$

$$P_f(0,1,1) = f(0,1,1) \to \underbrace{a_0}_{1} \oplus \underbrace{a_2}_{0} \oplus \underbrace{a_3}_{1} \oplus a_6 = 1 \Leftrightarrow \boxed{a_6 = 1}$$

$$P_f(1,0,1) = f(1,0,1) \to \underbrace{a_0}_{1} \oplus \underbrace{a_3}_{1} \oplus \underbrace{a_1}_{1} \oplus a_5 = 1 \Leftrightarrow \boxed{a_5 = 0}$$

$$P_f(1,1,0) = f(1,1,0) \to \underbrace{a_0}_{1} \oplus \underbrace{a_1}_{1} \oplus \underbrace{a_2}_{0} \oplus a_4 = 0 \Leftrightarrow \boxed{a_4 = 0}$$

$$P_f(1,1,1) = f(1,1,1) \to \underbrace{a_0}_{1} \oplus \underbrace{a_1}_{1} \oplus \underbrace{a_2}_{0} \oplus \underbrace{a_3}_{1} \oplus \underbrace{a_4}_{0} \oplus \underbrace{a_5}_{0} \oplus \underbrace{a_6}_{1} \oplus a_7 = 0$$

$$\boxed{a_7 = 0}$$

$f(x, y, z) = 1 \oplus x \oplus z \oplus yz.$

Зад) Да се намери полинома на Жегалкин на функциите.

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

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

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

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

e) $f(x,y,z) \leftrightharpoons (x \mid y) \downarrow z$

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

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

a) $x \vee y \dashv\vDash \overline{(\bar{x} \& \bar{y})} \dashv\vDash (1 \oplus ((1 \oplus x) \& (1 \oplus y))) \dashv\vDash$

$\dashv\vDash (\underbrace{1 \oplus (1}_{0} \oplus x \oplus y \oplus x.y)) \dashv\vDash x \oplus y \oplus x.y$

f) $f(x,y,z) \Leftrightarrow (x \rightarrow y) \& (y \downarrow z)$

f) $(\bar{x} \vee y) \& (\neg (y \vee z)) \models \overline{(\bar{\bar{x}} \& \bar{y})} \& (\bar{y} \& \bar{z}) \models$

$\models (1 \oplus (x \,.\, (1 \oplus y))) \,.\, (1 \oplus y) \,.\, (1 \oplus z) \models$

$\models (1 \oplus x \oplus xy) \,.\, (1 \oplus y \oplus z \oplus yz) \models 1 \oplus y \oplus z \oplus yz \oplus$

$\oplus x \oplus xy \oplus xz \oplus xyz \oplus \cancel{xy} \oplus \cancel{xy} \oplus \cancel{xyz} \oplus \cancel{xyz} \models$

$\models 1 \oplus x \oplus y \oplus z \oplus xy \oplus xz \oplus yz \oplus xyz.$

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

$P(x_1, \ldots, x_n) = \underbrace{\overbrace{x_1 \ldots x_k}}_{\text{ст-т } 1} \oplus \overbrace{\underline{x_{k+1} \ldots x_n}}$ приема

$U \leq J_2^n$,

$A \leq \{\alpha \mid \alpha \in J_2^n \;\&\; P(\alpha) = 1\}$

$B \leq \{\alpha \mid \alpha \in J_2^n \;\&\; P(\alpha) \neq 1\} = \underline{\{\alpha \mid \alpha \in J_2^n \;\&\; P(\alpha) = 0\}}$

$A \cap B = \emptyset$, $A \cup B = U$.

$|A| = |U| - |B|$. Нека $k \in \{0, \ldots, n-1\}$.

$\langle 1, 1, \ldots, 1 \rangle \in B$

$|B| = |\{\langle 1, 1, \ldots, 1 \rangle\}| + \overbrace{|\{\beta \mid \beta \in J_2^k \;\&\; \omega(\beta) < k\}|}^{C} \cdot \underbrace{|\{\beta \mid \beta \in J_2^{(n-k)} \;\&\; \omega(\beta) < n-k\}|}_{D}$.

$|C| = 2^k - 1$

$|D| = 2^{(n-k)} - 1$, $|B| = 1 + (2^k - 1) \cdot (2^{(n-k)} - 1)$

$|A| = 2^n - 1 - (2^k - 1) \cdot (2^{n-k} - 1) =$

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

Минимизация на двоични ф-ции
(Минимално покритие)

def/ Елем. конюнкция k е **импликанта** за ф-я f, ако
$\mathbb{I}(k) \subseteq \mathbb{I}(f)$
Единиците на k са единици и на f.

def/ Проста импликанта.

$x_{i_1}^{\sigma_{i_1}} x_{i_2}^{\sigma_{i_2}} \dots x_{i_k}^{\sigma_{i_k}}$

$\{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$

k е проста имп. за f, ако
(i) k е имп. за f.
(ii) $\neg \exists k'$ (k' имп. за f и $\mathbb{I}(k) \subseteq \mathbb{I}(k') \subseteq \mathbb{I}(f)$)
т.е., ако махнем буква от k, то тя престава да бъде импликанта

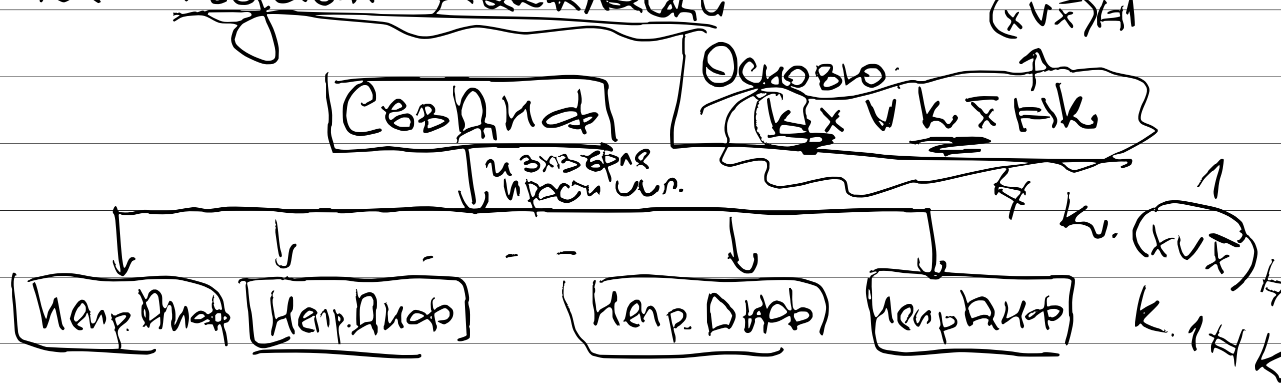
def/ • Сложност на ДНФ – броят букви, които я формират $xyz \vee \bar{x}y$ -> сложност 5

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

• Съкратена ДНФ – всички прости импликанти

• Неприводима ДНФ – ако някоя от дадена е проста импликанта, 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.
да търсим минимални покрития
ще се запознаем с алгоритъма
на Куайн-Маккласки



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

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) $f = \langle 11100111 \rangle$

a)

	x y z	f(x,y,z)
0	0 0 0	0
1	0 0 1	$\boxed{1}$
2	0 1 0	0
3	0 1 1	$\boxed{1}$
4	1 0 0	0
5	1 0 1	0
6	1 1 0	0
7	1 1 1	$\boxed{1}$

$f(x,y,z) = \bar{x}.\bar{y}.z \vee \bar{x}.y.z \vee x.y.z$

	мин. от ред 0	мин. от ред 1	
1	0 0 1	0 – 1 t_1	—
3	0 1 1	– 1 1 t_2	—
7	1 1 1		

	1	3	7
t_1	●	○	
t_2		○	●

ядрени импликанти

$$f(x,y,z) = \bar{x}z \vee yz.$$

b) $f = <\overset{000}{1}0000\,\overset{110}{0}10>$

	имп. отред0	
0	0 0 0 ∨	
6	1 1 0 ∨	

$$f = \bar{x}\bar{y}\bar{z} \vee xy\bar{z} \Leftrightarrow (\bar{x}\&\bar{y} \vee x\&y).\bar{z} \Leftrightarrow (x \Leftrightarrow y).\bar{z} \Leftrightarrow \neg(x \oplus y).\bar{z}$$

0 1 2 3 4 5 6 7

c) $f = \langle 0\ 1\ 1\ 1\ 0\ 1\ 0\ 1 \rangle$

	grup 0	grup 1		grup 2		
1	0 0 1	(1 3)	0 – 1	(1 3 5 7)	– – 1	✓ t_1
2	0 1 0	(1 5)	– 0 1	(1 5 3 7)	– – 1	
3	0 1 1	(2 3)	0 1 – ✓ t_2			
5	1 0 1	(3 7)	– 1 1			
7	1 1 1	(5 7)	1 – 1			

	1	2	3	5	7
t_1	●		o	o	o
t_2		●	o		

$f = \bar{x} \cdot y \vee z$

d) $f = \langle 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1 \rangle$

$\underbrace{- - -}_{\text{nr. of grup} = 3} \rightarrow f = 1$

e) $f = \langle 11100111 \rangle$

	x y z	f(x,y,z)
0	0 0 0	1
1	0 0 1	1
2	0 1 0	1
3	0 1 1	0
4	1 0 0	0
5	1 0 1	1
6	1 1 0	1
7	1 1 1	1

	peg 0	peg 1	
0	000	0&1 00-	t_1
1	001	0&2 0-0	t_2
2	010	1&5 -01	t_3
5	101	2&6 -10	t_4
6	110	5&7 1-1	t_5
7	111	6&7 11-	t_6

СокДНФ $f = t_1 \vee t_2 \vee t_3 \vee t_4 \vee t_5 \vee t_6$

	0	1	2	5	6	7
$t_1 : \bar{x}\bar{y}$	0	0				
$t_2 : \bar{x}\bar{z}$	0		0			
$t_3 : \bar{y}z$		0		0		
$t_4 : y\bar{z}$			0		0	
$t_5 : xz$				0		0
$t_6 : xy$					0	0

$\varphi = (t_1 \vee t_2) \cdot (t_1 \vee t_3) \cdot (t_2 \vee t_4) \cdot (t_3 \vee t_5) \cdot (t_4 \vee t_6) \cdot (t_5 \vee t_6)$

[illegible]

ДНФ

$\varphi \equiv (t_1 \vee t_2).(t_1 \vee t_3).(t_2 \vee t_4).$
$.(t_3 \vee t_5).(t_4 \vee t_6).(t_5 \vee t_6) \models\!\!\dashv$

$(t_1 \vee t_2.t_3).(t_4 \vee t_2.t_6).(t_5 \vee t_3.t_6) \models\!\!\dashv$

$(t_1.t_4 \vee t_1.t_2.t_6 \vee t_2.t_3.t_4 \vee t_2.t_3.t_6).(t_5 \vee t_3.t_6) \models\!\!\dashv$

$t_1.t_4.t_5 \vee t_1.t_4.t_3.t_6 \vee t_1.t_2.t_5.t_6 \vee \cancel{t_1.t_2.t_3.t_6} \vee$
$t_2.t_3.t_4.t_5 \vee \cancel{t_2.t_3.t_4.t_6} \vee \cancel{t_2.t_3.t_5.t_6} \vee t_2.t_3.t_6 \models\!\!\dashv$

$\underbrace{t_1.t_4.t_5}_{6} \vee \underbrace{t_2.t_3.t_6}_{8} \vee \overbrace{t_1.t_3.t_4.t_6}^{\text{слож } 8} \vee \overbrace{t_1.t_2.t_5.t_6}^{8} \vee$
$\underbrace{t_2.t_3.t_4.t_5}_{8}.$

$\to \underline{t_1 \vee t_4 \vee t_5}$ неприводимо ДНФ.

Т.е. само две мин. ДНФ.

$f(x,y,z) \models\!\!\dashv \underbrace{\bar{x}.\bar{y} \vee y\bar{z} \vee xz}_{} \models\!\!\dashv \underbrace{\bar{x}\bar{z} \vee \bar{y}z \vee xy}_{}$

Критерий за пълнотата на м-во от булеви функции

Затворени подм-во на F_2, максимални подм-ва на F_2, които не са пълни:

- $T_0 \leftrightharpoons \{f \mid f \in F_2 \ \&\ f(\tilde{0}) = 0\}$
  запазващи нулата ф-ции
- $T_1 \leftrightharpoons \{f \mid f \in F_2 \ \&\ f(\tilde{1}) = 1\}$
  запазващи единицата ф-ции

$\alpha \in J_2^n$, $\bar{\alpha} = \langle \bar{a}_0, \dots, \bar{a}_{n-1} \rangle$

- $S \leftrightharpoons \{f \mid f \in F_2 \ \&\ f(\alpha) = \overline{f(\bar{\alpha})}\}$
  самодвойствени ф-ции.

вектори от 0-ци и 1-ци за f.

- $M \leftrightharpoons \{f \mid f \in F_2 \ \&\ [\alpha \preceq \beta \Rightarrow f(\alpha) \leq f(\beta)]\}$
  монотонни ф-ции

частична наредба предшествие (хиперкуб върховете)

- $L = \{f \mid f \in F_2 \;\&\; f = a_0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n$ за $a_i \in \{0,1\}\}$

линейни функции

<u>Th | Пост-Яблонски</u>

Нека $F \subseteq F_2$.

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

$F \not\subseteq T_0 \cup T_1 \cup L \cup M \cup S$

<u>Следствие</u> |

една ф-я f е Шеферова, ако $[f] = F_2$.

$f \in F_2$:

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

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

Нека $n \in \mathbb{N}_{>0}$.

следствие

$$\mathcal{U} \leftrightharpoons \{f \mid f \in \mathcal{F}_2^n \ \&\ [\{f\}] = \mathcal{F}_2\} =$$

$$= \{f \mid f \in \mathcal{F}_2^n \ \&\ f \notin T_0 \cup T_1 \cup S\} =$$

$$= \{f \mid f \in \mathcal{F}_2^n \ \&\ \overset{=1}{f(\tilde{0}) \neq 0} \ \&\ \overset{=0}{f(\tilde{1}) \neq 1} \ \&\ (\nexists \alpha \in \mathcal{J}_2^n)[f(\alpha) \neq \overline{f(\overline{\alpha})}]\} =$$

$$= \underbrace{\{f \mid f \in \mathcal{F}_2^n \ \&\ f(\tilde{0}) = 1 \ \&\ f(\tilde{1}) = 0\}}_{A} \setminus$$

$$\underbrace{\{f \mid f \in \mathcal{F}_2^n \ \&\ f(\tilde{0}) = 1 \ \&\ f(\tilde{1}) = 0 \ \&\ (\forall \alpha \in \mathcal{J}_2^n)[f(\alpha) = \overline{f(\overline{\alpha})}]\}}_{B}.$$

$$|A| = 2^{2^n - 2}$$

$$|B| = 2^{2^{n-1} - 1} =$$

половината → 2^{n-1}

-1 → защото

$$= 2^{\frac{2^n - 2}{2}}$$

$$|\mathcal{U}| = 2^{(2^n - 2)} - 2^{(2^{n-1} - 1)}$$

$\langle 0, \ldots, 0\rangle$	σ_1
$\vdots$	$\vdots$
$\langle 0, 1, \ldots, 1\rangle$	$\sigma_{2^{n-1}-1}$
$\langle 1, 0, \ldots, 0\rangle$	$\overline{\sigma}_{2^{n-1}-1}$
$\vdots$	$\vdots$
$\langle 1, \ldots, 1\rangle$	$\overline{\sigma}_1$

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

a) $\overbrace{\{\underbrace{x \to y}_{f_1},\ \underbrace{x \to \bar{y} \& z}_{f_2}\}}^{F} \not\subseteq T_0 \cup T_1 \cup S \cup L \cup M$

- $f_1(0,0) = 1 \rightsquigarrow f_1 \notin T_0 \to F \not\subseteq T_0$

- $f_2(1,1,1) = 0 \rightsquigarrow f_2 \notin T_1 \to F \not\subseteq T_1$

  $f_2(0,1,0) = 1 \rightsquigarrow f_2 \notin M \to F \not\subseteq M$

- $\to f_1 \notin S \rightsquigarrow F \not\subseteq S$

00	1
01	1
10	0
11	1

- $\bar{x} \vee y = \overline{(x \& \bar{y})} = 1 \oplus (x.(1 \oplus y)) = 1 \oplus x \oplus x.y \rightsquigarrow f_1 \notin L \to F \not\subseteq L$

b) $\{\overbrace{x \,\&\, y}^{f_1}, \overbrace{\bar{x} \leftrightarrow y \,\&\, z\, y}^{f_2}\}\ F$

c) $\{\underbrace{\langle 0110\,1001 \rangle}_{f_1}, \underbrace{\langle 1\,0001101 \rangle}_{f_2}, \underbrace{\langle 00011100 \rangle}_{f_3}\}$

b) $f_2(0,0,0) = 1 \Leftrightarrow 0 = 0$

$\{f_1, f_2\} = F \subseteq T_0$ т.е. F не пълно.

c) $f_2(\tilde{0}) = 1 \rightsquigarrow f_2 \notin T_0$

$f_3(\tilde{1}) = 0 \rightsquigarrow f_3 \notin T_1 \to f_3(1,0,1) = 1 \not\leq 0 = f(1,1,1) \to f_3 \notin M.$

$f_2 \notin S$

$f_3 = \bar{x} y z \vee x \bar{y} \bar{z} \vee x \bar{y} z \Leftrightarrow (1 \oplus x).y.z \oplus x.(1 \oplus y).(1 \oplus z) \oplus x.z(1 \oplus y) \Leftrightarrow$

$\Leftrightarrow y.z \oplus \cancel{x.y.z} \oplus x \oplus y.x \oplus \cancel{z.x} \oplus \underline{x.y.z} \oplus \cancel{x.z} \oplus \cancel{x.z.y}$

$f_3 \notin L$

F е пълно м-во.