Полиноми на Жегалкин

Това е ф-ла над м-вото функции $\{\tilde{0}, \tilde{1}, \&, \oplus\}$.

Th | 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 $\alpha = \langle a_0, a_1, \dots, a_{2^n-1} \rangle \in J_2^{2^n}$.

Т.е. дали една конюнкция ще участва в дизюнкцията от изключващи "или"-та се определя от съответния коеф. $a_i \in \{0, 1\}$.

Знаем, че $|J_2^{2^n}| = |\{\langle a_0, \dots, a_{2^n-1} \rangle \mid a_i \in \{0,1\}\}| =$
$= 2^{2^n} = |\mathcal{F}_2^n|$.

Дължина на ПЖ - броят ненулеви 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 преобразования на ф-ли.
Т.к. $\{\tilde{1}, \tilde{0}, \&, \oplus\}$ е пълно, то можем всяка булева ф-я да я изразим чрез тях.
b) От съвърш. ДНФ
Нека $f(\tilde{x}^3) = \langle 01101000 \rangle$.
$$\begin{array}{cccccccc} 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{array}$$
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 $\&$, $\oplus$
- Асоциативност на $\&$, $\oplus$
- $x \& x = x$; $\qquad x \oplus \tilde{0} = x$;

  $x \oplus x = \tilde{0}$; $\qquad x \& \tilde{0} = \tilde{0}$;

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

  $x \& \tilde{x} = \tilde{0}$; $\qquad x \oplus \tilde{1} = \bar{x}$

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

Така $f(\tilde{x}^3) \models (\tilde{1} \oplus x) \& (\tilde{1} \oplus y) \& z \oplus$
$(\tilde{1} \oplus x) \& y \& (\tilde{1} \oplus z) \oplus$
$x \& (\tilde{1} \oplus y) \& (\tilde{1} \oplus z) \models$

$(\tilde{1} \oplus x \oplus y \oplus x \& y) \& z \oplus$
$(\tilde{1} \oplus x \oplus z \oplus x \& z) \& y \oplus$ нека $\&$ слепено да пишем
$(\tilde{1} \oplus y \oplus z \oplus y \& z) \& x \models$

$z \oplus \cancel{xz} \oplus \cancel{yz} \oplus \cancel{xyz} \oplus y \oplus \cancel{xy} \oplus$
$\cancel{zy} \oplus \cancel{xyz} \oplus x \oplus \cancel{xy} \oplus \cancel{zx} \oplus xyz \models$

$\boxed{x \oplus y \oplus z \oplus xyz}$.

c) Чрез метод на неопределените кое ф.

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

НПФ $\underset{\underset{f(x_1,\dots,x_n)}{\parallel}}{P_f}(x_1,\dots,x_n) = a_0 \oplus a_1 x_n \oplus \dots \oplus a_{2^n-1} x_1 \dots x_n$.

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

$$\begin{cases} P_f(0,0,\dots,0) = f(0,0,\dots,0) \\ P_f(0,0,\dots,0,1) = f(0,0,\dots,0,1) \\ \dots \\ P_f(1,1,\dots,1,1) = f(1,1,\dots,1,1) \end{cases}$$

Нека $f(\tilde{x}^3) = \langle 10110100 \rangle$.

Тогава

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

$$\begin{cases} P_f(0,0,0) = f(0,0,0) \rightarrow \boxed{a_0 = 1} \\ P_f(0,0,1) = f(0,0,1) \rightarrow 1 \oplus a_3 = 0 \rightarrow \boxed{a_3 = 1} \\ P_f(0,1,0) = f(0,1,0) \rightarrow 1 \oplus a_2 = 1 \rightarrow \boxed{a_2 = 0} \\ P_f(0,1,1) = f(0,1,1) \rightarrow 1 \oplus 1 \oplus a_6 = 1 \rightarrow \boxed{a_6 = 1} \\ P_f(1,0,0) = f(1,0,0) \rightarrow 1 \oplus a_1 = 0 \rightarrow \boxed{a_1 = 1} \\ P_f(1,0,1) = f(1,0,1) \rightarrow 1 \oplus 1 \oplus 1 \oplus a_5 = 1 \rightarrow \boxed{a_5 = 0} \end{cases}$$

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

$P_f(1,1,1) = f(1,1,1) \rightarrow 1 \oplus 1 \oplus 1 \oplus 1 \oplus a_7 = 0 \Rightarrow \boxed{a_7 = 0}$

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

Зад. Да се намери полинома на Жегалкин на функцията.

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

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

(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 $\underline{\underline{1}}$.

---

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

Т.е. трябва едната част да е 0, а другата 1 (Те са конюнкции).
По-лесно е да преброим тези вектори нарушаващи условието. Нека $k \in \{1, \dots, n-1\}$

$\mathcal{U} \leftrightharpoons J_2^n$, $|\mathcal{U}| = 2^n$

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

$B \leftrightharpoons \{\alpha \mid \alpha \in J_2^n \ \& \ P(\alpha) \neq 1\} =$
$\{\alpha \mid \alpha \in J_2^n \ \& \ P(\alpha) = 0\}$.

$A \cap B = \emptyset$, $A \cup B = J_2^n$.

Кога $P(\alpha) = 0$? Когато или двете страни на $\oplus$ са 1, или и двете са едновременно 0. Само един вектор ги прави едновременно 1 и това е $\alpha = \langle 1, 1, \dots, 1 \rangle$. Сега броим за 0.
И двете конюнкции са 0, т.е.

има поне по една променлива
x_i за $i \le k$ т.е. в α на i-та поз. има 0
и поне една променлива x_j за $k < j \le n$
т.е. в α на j-та поз. имаме 0.

$$|B| = |\{\langle 1, \dots, 1\rangle\}| + |\{\beta \mid \beta \in J_2^k \ \& \ w(\beta) < k\}| \cdot |\{\beta \mid \beta \in J_2^{n-k} \ \& \ w(\beta) < n-k\}|$$

Т.е. броим всички вектори с дълж. k D
и поне една 0 и ги умножаваме
по всички вектори с дълж. $(n-k)$ и
пак с поне една 0, за за получения
вектор, който ние искаме.

$|C| = 2^k - 1$ единици вектор

$|D| = 2^{n-k} - 1$.

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

Минимизация на двоични ф-ции
(Минимално покритие)

<u>def</u>/ Една елем. конюнкция k е <u>импликанта</u> за ф-я f, ако
$\mathbb{T}(k) \subseteq \mathbb{T}(f)$
Единиците на k са единици и на f.

<u>def</u>/ 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 $\mathbb{T}(k) \subseteq \mathbb{T}(k') \subseteq \mathbb{T}(f)$),
т.е., ако махнем буква от k, то тя престава да бъде импликанта

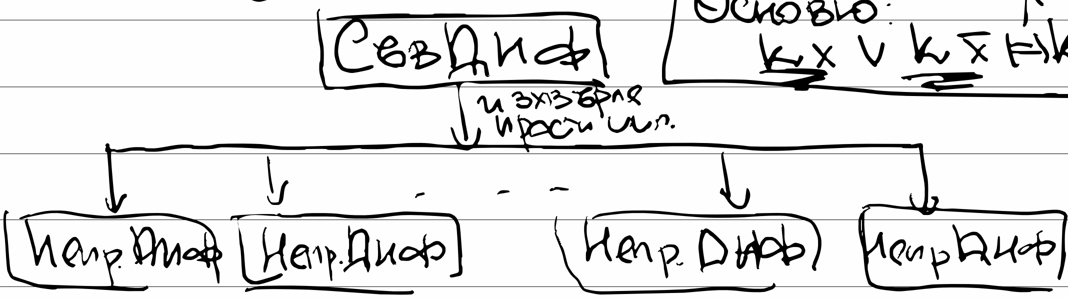
<u>def</u>/ • Сложност на ДНФ - брой букви, които я формират
• Всяка <u>минимална ДНФ</u> се състои от прости импликанти (подбрани да покриват единиците на f)
• <u>Съкратена ДНФ</u> - всички прости импликанти
• <u>Неприводима ДНФ</u> - ако махнем кой да е проста импликанта, то тя

престава да представя ф-ята.
Една ф-я Булева 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 Куйн-Маккласки

Основно: $kx \vee k\bar{x} \equiv k$

$(x \vee \bar{x}) \equiv 1$



Всеки от неприводимите, чийто брой
букви е минимален, се нарича
минимална ДНФ.

Идеята е да започнете от всички импликанти и да ги сведете до прости.
① 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 може да получите различни (или единствени) варианти за неприводими ДНФ. От тях избираме минималните които искаме да са с възможно най-малка дължина (колкото се може по-малко букви в записа (изкл. &, v, ¬)).

(302) $f \in F_2^3$. По метода 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
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	$\boxed{1}$

Редно импликантите се определя с броя на изтритите елемове

импл. от ред 1

имп. от ред 2

импл. от ред 0	→ 0	1	2
1	0 0 1	(a) 0 – 1	—
3	0 1 1	(b) – 1 1	—
7	1 1 1		

това ще са прости импликанти

Сега да видим коя какво покрива.

	1	3	7
(а)	●	○	
(б)		○	●

1 и 7 колоните се покриват само от (а) и (б). Такива импликанти се наричат ядрени/атомарни и те автоматично се включват в мин. ДНФ.

Отг: $f = \bar{x}z \vee yz$

Дължина: 4 (броя на буквите в f).

b) $f = \langle 10000010 \rangle$

	x	y	z	f
0	0	0	0	1
6	1	1	0	1

импликанти от 0-лев ред които не могат да се съкратят. В този случай <u>мин. ДНФ съвпада със Съв. ДНФ</u>.

Отг: $f = \bar{x}\bar{y}\bar{z} \vee xy\bar{z}$.

c) $f = \langle \overset{0}{0}\overset{1}{1}\overset{2}{1}\overset{3}{1}\overset{4}{0}\overset{5}{1}\overset{6}{0}\overset{7}{1} \rangle$

	x	y	z
1	0	0	1
2	0	1	0
3	0	1	1
5	1	0	1
7	1	1	1

гр 0

	x	y	z
1&3	0	–	1
1&5	–	0	1
2&3	0	1	–
3&7	–	1	1
5&7	1	–	1

гр 1

вече проста

	x	y	z
1&3&5&7	–	–	1
1&5&3&7	–	–	1

гр 2

прости имп.

Коя какво покрива?

	1	2	3	5	7
– – 1	●		○	●	●
0 1 –		●	○		

И взете са зелени: Отг: $f = xy \vee z$

зелн. З.

---

* Може да има прости импликанти от различни гр!

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 с минимален брой импликанти.

d) $f = \langle 11111111 \rangle = \tilde{1}$.

Импликанти от ред 3: – – – прости.

Значи минДНФ $f = \tilde{1}$.

e) $f = \langle 11100111 \rangle$

	x y z		x y z	
0	0 0 0	0&1	0 0 –	t_1
1	0 0 1	0&2	0 – 0	t_2
2	0 1 0	1&5	– 0 1	t_3
5	1 0 1	2&6	– 1 0	t_4
6	1 1 0	5&7	1 – 1	t_5
7	1 1 1	6&7	1 1 –	t_6

всички имп. от ред 1 са прости!

СъкрДНФ: $f = \bar{x}\bar{y} \vee \bar{x}\bar{z} \vee \bar{y}z \vee y\bar{z} \vee xz \vee xy$.

Сега неприводимите ДНФ. Ще имаме повече от една минимална тук.

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

се $\Leftrightarrow (t_1 \vee t_2).(t_1 \vee t_3)(t_2 \vee t_4).(t_3 \vee t_5)$
$(t_4 \vee t_6).(t_5 \vee t_6)$

Се описва кои неща са покрития в КНФ-е. Сега за да видим кои неща са дали покрития минаваме в ДНФ.

се $\Leftrightarrow (t_1 \vee t_2.t_3)(t_4 \vee t_2.t_6)(t_5 \vee t_3 t_6) \Leftrightarrow$

$\Leftrightarrow (t_1 t_4 \vee t_1 t_2 t_6 \vee t_2 t_3 t_4 \vee t_2 t_3 t_6).$
$(t_5 \vee t_3 t_6) \Leftrightarrow$

$\Leftrightarrow t_1 t_4 t_5 \vee t_1 t_2 t_5 t_6 \vee t_2 t_3 t_4 t_5 \vee \cancel{t_2 t_3 t_5 t_6} \vee$
$t_1 t_3 t_4 t_6 \vee \cancel{t_1 t_2 t_3 t_6} \vee \cancel{t_2 t_3 t_4 t_6} \vee t_2 t_3 t_6$

Те са покрития. Още може да се опрости. Ако имаме елементи, т.е. един е подмн-во на друг, то по-големия го махаме.

$\Leftrightarrow t_1 t_4 t_5 \vee t_1 t_2 t_5 t_6 \vee t_2 t_3 t_4 t_5 \vee$
$t_1 t_3 t_4 t_6 \vee t_2 t_3 t_6$

Тези са неприводими покрития в смисъл, че ако махнем импликанта, то спираме да имаме покритие на единиците на f.

За мин ДНФ казахме, че издираме неприводими ДНФ с възможно най-малко букви.

Така

$f(\tilde{x}^3) \models \bar{x}\bar{y} \vee y\bar{z} \vee xz$ (опция 1

$\models \bar{x}\bar{z} \vee \bar{y}z \vee xy$ (опция 2

за мин ДНФ.

Зад Намерете всички мин ДНФ на

а) $f = \langle 1101001110101010 \rangle$

b) $f = \langle 0110101111010001 \rangle$

Критерий за пълнота на м-во от булеви функции

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

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

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

самодвойнствени ф-ции. ← вектори от дин. 1-ци за f.

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

монотонни ф-ции

частична наредба предшествие (хиперкуб върховете)

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

линейни функции

Th | Пост-Яблонски

Нека $F \subseteq \mathcal{F}_2$.

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

Следствие |

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

За $f \in \mathcal{F}_2$:

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

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

Нека $n \in \mathbb{N}_{>0}$.

$$\mathcal{U} \leftrightharpoons \{ f \mid f \in \mathcal{F}_2^n \ \& \ \underbrace{[\{f\}] = \mathcal{F}_2}_{f \notin T_0 \cup T_1 \cup S} \} =$$

$$= \{ f \mid f \in \mathcal{F}_2^n \ \& \ f(\tilde{0}) = 1 \ \& \ f(\tilde{1}) = 0 \ \& \ (\nexists \alpha \in J_2^n)[f(\alpha) \neq \overline{f(\bar{\alpha})}] \} =$$

$$= \overbrace{\{ f \mid f \in \mathcal{F}_2^n \ \& \ f(\tilde{0}) = 1 \ \& \ f(\tilde{1}) = 0 \}}^{A} \setminus \underbrace{\{ f \mid f \in \mathcal{F}_2^n \ \& \ f(\tilde{0}) = 1 \ \& \ f(\tilde{1}) = 0 \ \& \ (\forall \alpha \in J_2^n)[f(\alpha) = \overline{f(\bar{\alpha})}] \}}_{B}$$

$|A| = 2^{2^n - 2}$ → фиксирани за $\tilde{0}$ и $\tilde{1}$

$|B| = 2^{\frac{2^n - 2}{2}} = 2^{2^{n-1} - 1}$ → таблицата е предопределена

↑ огледалните

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

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