A1. Algebraická normálna forma

Definícia A.1. Binárnu operáciu $\oplus$ na booleovskej algebre $\mathbb{B}$ definovanú B-výrazom

$$x \oplus y = x\bar{y} + \bar{x}y$$

budeme nazývať *XOR (exclusive OR, vylučujúca disjunkcia).*

Veta A.1. Operácia $\oplus$ je komutatívna, asociatívna, súčin . je vzhľadom k nej distributívny a systém $\{., \oplus\}$ tvorí USBF.

Dôkaz. Vyjadríme operácia $\bar{}$ a $+$ pomocou . a $\oplus$.

$$x + y = x \oplus y \oplus xy$$

$$\bar{x} = 1 \oplus x$$

Komutatívnosť, asociatívnosť a distributívnosť operácií . a $\oplus$ sa dá dokázať priamo z definície.
■

Definícia A.2. *Algebraickou normálnou formou (ANF)* B-funkcie $f(x_1, x_2, ..., x_n)$ budeme nazývať B-výraz

$$\sum_{i=0}^{2^n-1} q_i x_1^{i1} x_2^{i2} \ldots x_n^{in},$$

kde $i = i_1 2^0 \oplus i_2 2^1 \oplus \ldots \oplus i_n 2^{n-1}$, $q_i \in \mathbb{B}$, $x_k^{ik} = x_k$, ak $i_k = 1$, $x_k^{ik} = 1$, ak $i_k = 0$.

Lema. Pre každú B-funkciu $f(x_1, x_2, ..., x_n, x_{n+1})$ a pre každé $(x_1, x_2, ..., x_n, x_{n+1}) \in \mathbb{B}^{n+1}$,

$f(x_1, x_2, ..., x_m, x_{m+1}) = f(x_1, x_2, ..., x_m, 0) \oplus x_{m+1}(f(x_1, x_2, ..., x_m, 0) \oplus f(x_1, x_2, ..., x_m, 1))$

Dôkaz.
Pre $x_{m+1} = 0$

$f(x_1, x_2, ..., x_m, x_{m+1}) = f(x_1, x_2, ..., x_m, 0) \oplus 0.(f(x_1, x_2, ..., x_m, 0) \oplus f(x_1, x_2, ..., x_m, 1)) = f(x_1, x_2, ..., x_m, 0)$

a pre $x_{m+1} = 1$

$f(x_1, x_2, ..., x_m, x_{m+1}) = f(x_1, x_2, ..., x_m, 0) \oplus 1.(f(x_1, x_2, ..., x_m, 0) \oplus f(x_1, x_2, ..., x_m, 1)) = f(x_1, x_2, ..., x_m, 1)$
■

Veta A.2. Každá B-funkcia m premenných f sa dá jednoznačne vyjadriť v tvare ANF, t.j.

$$f(x_1, x_2, ..., x_n) = \sum_{i=0}^{2^n-1} q_i x_1^{i1} x_2^{i2} ... x_n^{in},$$

kde $i = i_1 2^0 \oplus i_2 2^1 \oplus ... \oplus i_n 2^{n-1}$, $x_k^{ik} = x_k$, ak $i_k = 1$, $x_k^{ik} = 1$, ak $i_k = 0$, pričom

$$q_i = \sum_{j \in M(i)} f(j)$$

kde $M(i) = M(i_1 i_2 ... i_n) = \{j = (j_1 j_2 ... j_n); j_k = 1 \Rightarrow i_k = 1 \text{ pre } k = 1, 2, ..., n\}$.

Dôkaz. Indukciou vzhľadom k n:

Pre $n = 1$ $M(0) = \{0\}$, $M(1) = \{0, 1\}$, $q_0 = f(0)$, $q_1 = f(0) \oplus f(1)$,

$f(x_1) = f(0).1 \oplus (f(0) \oplus f(1))x_1$

platí pre všetky štyri možné B-funkcie jednej premennej: 00, 01, 10, 11.

Predpokladáme, že tvrdenie vety platí pre B-funkciu n premenných a ukážeme, že potom platí aj pre B-funkciu $n + 1$ premenných.

Keďže $f(x_1, x_2, ..., x_n, 0)$ a $f(x_1, x_2, ..., x_n, 1)$ sú B-funkcie n premenných, platí pre ne indukčný predpoklad a podľa Lemy dostávame:

$$f(x_1, x_2, ..., x_n, x_{n+1}) = f(x_1, x_2, ..., x_n, 0) \oplus x_{n+1}(f(x_1, x_2, ..., x_n, 0) \oplus f(x_1, x_2,$$

$$..., x_n, 1)) = \sum_{i=0}^{2^n - 1} q_i' x_1^{i1} x_2^{i2} ... x_n^{in} \oplus x_{n+1}(\sum_{i=0}^{2^n - 1} q_i' x_1^{i1} x_2^{i2} ... x_n^{in} \oplus$$

$$\sum_{i=0}^{2^n - 1} q_i'' x_1^{i1} x_2^{i2} ... x_n^{in}) = \sum_{i=0}^{2^n - 1} q_i' x_1^{i1} x_2^{i2} ... x_n^{in} \oplus (\sum_{i=0}^{2^n - 1} q_i' x_1^{i1} x_2^{i2} ... x_n^{in} x_{n+1} \oplus$$

$$\sum_{i=0}^{2^n - 1} q_i'' x_1^{i1} x_2^{i2} ... x_n^{in} x_{n+1}) = \sum_{i=0}^{2^n - 1} q_i' x_1^{i1} x_2^{i2} ... x_n^{in} \oplus$$

$$\sum_{i=0}^{2^n - 1} (q_i' \oplus q_i'') x_1^{i1} x_2^{i2} ... x_n^{in} x_{n+1}$$

kde q_i' resp. q_i'' sú koeficienty ANF funkcií $f(x_1, x_2, ..., x_n, 0)$, resp. $f(x_1, x_2, ..., x_n, 1)$, t.j.

$$q_i' = \sum_{j \in M(i)} f(j) \qquad q_i'' = \sum_{j \in M(i)} f(j + 2^n)$$

Na dokončenie dôkazu stačí pre koeficienty súčinových členov, ktoré neobsahujú x_{n+1}, t.j. pre $i < 2^n$ položiť $q_i = q_i'$ a pre $2^n \le i < 2^{n+1}$ si uvedomiť, že

$$M(i) = M(i - 2^n) \cup (M(i) - M(i - 2^n)),$$

a

$$\sum_{j \in M(i-2^n)} f(j + 2^n) = \sum_{j \in M(i) - M(i-2^n)} f(j),$$

odkiaľ pre koeficienty súčinových členov, ktoré obsahujú x_{n+1} dostaneme

$$q_i = q_i' + q_i'' = \sum_{j \in M(i-2^n)} f(j) + \sum_{j \in M(i) - M(i-2^n)} f(j) = \sum_{j \in M(i)} f(j)$$

■

Príklad. B-funkcia f(x, y, z) je daná tabuľkou. Nájdite M(i), q_i, a ANF danej funkcie podľa definície. Potom riešte úlohu pomocou algoritmu založeného na Leme.

i	x	y	z	f(x, y, z)	M(i)	q_i
0	0	0	0	1	{0}	f(0) = 1
1	1	0	0	0	{0, 1}	f(0) ⊕ f(1) = 1
2	0	1	0	1	{0, 2}	f(0) ⊕ f(2) = 0
3	1	1	0	1	{0, 1, 2, 3}	f(0) ⊕ f(1) ⊕ f(2) ⊕ f(3) = 1
4	0	0	1	0	{0, 4}	f(0) ⊕ f(4) = 1
5	1	0	1	1	{0, 1, 4, 5}	f(0) ⊕ f(1) ⊕ f(4) ⊕ f(5) = 0
6	0	1	1	0	{0, 2, 4, 6}	f(0) ⊕ f(2) ⊕ f(4) ⊕ f(6) = 0
7	1	1	1	1	{0, 1, 2, 3, 4, 5, 6, 7}	f(0) ⊕ f(1) ⊕ f(2) ⊕ f(3) ⊕ f(4) ⊕ f(5) ⊕ f(6) ⊕ f(7) = 1

f(x, y, z) = 1⊕ x ⊕ xy ⊕ z ⊕ xyz

Algoritmus:
10110101 = 1011 ⊕ z(1011 ⊕ 0101) = 1011 ⊕ z(1110) =
= 10 ⊕ y(10 ⊕ 11) ⊕ z(11 ⊕ y(11 ⊕ 10)) =
= 10 ⊕ y(01) ⊕ z(11 ⊕ y(01)) =
= 1 ⊕ x(1 ⊕ 0) ⊕ y(0 ⊕ x(0 ⊕ 1)) ⊕ z(1 ⊕ x(1 ⊕ 1)) ⊕ y(0 ⊕ x(0 ⊕ 1)) =
= 1 ⊕ x ⊕ xy ⊕ z ⊕ xyz

Literatúra.
Karla Čipková, Ladislav Satko, Základy kódovania, STU Bratislava, 2009