

A1. Algebraická normálna forma

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

$$x \oplus y = \overline{xy} + \overline{\overline{x}\overline{y}}$$

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

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

Dôkaz. Vyjadríme operácia $\cdot$ a $+$ pomocou $\cdot$ a $\oplus$.

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

–

$$x = 1 \oplus x$$

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

■

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

$$2^n - 1$$

$$\bigoplus_{i=0}^{2^n-1} q_i x_1^{i_1} x_2^{i_2} \dots x_n^{i_n},$$

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

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

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

Dôkaz.

Pre $x_{m+1} = 0$

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

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

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

■

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

$$f(x_1, x_2, \dots, x_n) = \bigoplus_{i=0}^{2^n-1} q_i x_1^{i_1} x_2^{i_2} \dots x_n^{i_n},$$

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

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

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

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

$$\begin{aligned}
 f(x_1, x_2, \dots, x_n, x_{n+1}) &= f(x_1, x_2, \dots, x_n, 0) \oplus x_{n+1}(f(x_1, x_2, \dots, x_n, 0) \oplus f(x_1, x_2, \\
 &\quad \dots, x_n, 1)) = \bigoplus_{i=0}^{2^n-1} q_i' x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \oplus x_{n+1} \left(\bigoplus_{i=0}^{2^n-1} q_i' x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \oplus \right. \\
 &\quad \left. \bigoplus_{i=0}^{2^n-1} q_i'' x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \right) = \bigoplus_{i=0}^{2^n-1} q_i' x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \oplus \left(\bigoplus_{i=0}^{2^n-1} q_i' x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} x_{n+1} \oplus \right. \\
 &\quad \left. \bigoplus_{i=0}^{2^n-1} q_i'' x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} x_{n+1} \right) = \bigoplus_{i=0}^{2^n-1} q_i' x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \oplus \\
 &\quad \bigoplus_{i=0}^{2^n-1} (q_i' \oplus q_i'') x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} x_{n+1}
 \end{aligned}$$

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

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

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 $2^n \leq i < 2^{n+1}$ si uviesť, že

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

a

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

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

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

■

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}	$f(0) \oplus f(1) = 1$
2	0	1	0	1	{0, 2}	$f(0) \oplus f(2) = 0$
3	1	1	0	1	{0, 1, 2, 3}	$f(0) \oplus f(1) \oplus f(2) \oplus f(3) = 1$
4	0	0	1	0	{0, 4}	$f(0) \oplus f(4) = 1$
5	1	0	1	1	{0, 1, 4, 5}	$f(0) \oplus f(1) \oplus f(4) \oplus f(5) = 0$
6	0	1	1	0	{0, 2, 4, 6}	$f(0) \oplus f(2) \oplus f(4) \oplus f(6) = 0$
7	1	1	1	1	{0, 1, 2, 3, 4, 5, 6, 7}	$f(0) \oplus f(1) \oplus f(2) \oplus f(3) \oplus f(4) \oplus f(5) \oplus f(6) \oplus f(7) = 1$

$$f(x, y, z) = 1 \oplus x \oplus xy \oplus z \oplus xyz$$

Algoritmus:

$$\begin{aligned}
 10110101 &= 1011 \oplus z(1011 \oplus 0101) = 1011 \oplus z(1110) = \\
 &= 10 \oplus y(10 \oplus 11) \oplus z(11 \oplus y(11 \oplus 10)) = \\
 &= 10 \oplus y(01) \oplus z(11 \oplus y(01)) = \\
 &= 1 \oplus x(1 \oplus 0) \oplus y(0 \oplus x(0 \oplus 1)) \oplus z(1 \oplus x(1 \oplus 1)) \oplus y(0 \oplus x(0 \oplus 1)) = \\
 &= 1 \oplus x \oplus xy \oplus z \oplus xyz
 \end{aligned}$$

Literatúra.

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