

XOR a ANF

Nasledujúci text je krátkym zhrnutím vlastností funkcie XOR a náčrtom algoritmu na hľadanie ANF.
Nie je náhradou za prednášku ani za ostatnú odbornú literatúru.

Vlastnosti boolovskej funkcie XOR¹

0. Definícia tabuľkou // „vzorcom“²

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

$$x \oplus y = x.y' + x'.y = (x.y + x'.y')$$

1. $x \oplus y = y \oplus x$

2. $x \oplus 0 = x$, $x \oplus 1 = x'$

3. $x \oplus x = 0$, $x \oplus x' = 1$

4. $x' \oplus y' = x \oplus y$, $x \oplus y' = (x \oplus y)'$

5. $x \oplus (y \oplus z) = (x \oplus y) \oplus z$

6. $x \oplus x.y = x.(x \oplus y) = x.y'$

7. $x.(y \oplus z) = x.y \oplus x.z$

8. $x + y = x \oplus x'.y = x.y' \oplus y$

Tvrdenie

Množina $A = \{1, \oplus, .\}$ je USBF (úplný systém boolovských funkcií).

Dôkaz vychádza z vlastností 2. a 8.

¹ Dôkazy boli uvedené na prednáške. Dá sa však na ne prísť rýchlo a ľahko aj „vlastnou hlavou“.

² Na zápis negácií používame z čisto technických dôvodov znak $(...)'$.

Hľadanie alegebraickej normálnej formy (ANF)

Je daná boolovská funkcia n premenných $f(x_1, x_2, \dots, x_n)$.

Platí: $f(x_1, x_2, \dots, x_n) = x_1' \cdot f(0, x_2, \dots, x_n) \oplus x_1 \cdot f(1, x_2, \dots, x_n)$

Využijeme vlastnosť 2 na „zbavenie sa“ negácie a dostaneme:

$$\begin{aligned} f(x_1, x_2, \dots, x_n) &= (1 \oplus x_1) \cdot f(0, x_2, \dots, x_n) \oplus x_1 \cdot f(1, x_2, \dots, x_n) = \\ &= f(0, x_2, \dots, x_n) \oplus x_1 \cdot (f(0, x_2, \dots, x_n) \oplus f(1, x_2, \dots, x_n)) \end{aligned}$$

Pre použitie znaku $\oplus$ v uvedenom vzťahu je dôležitý fakt, že x a x' nikdy nenadobúdajú naraz hodnotu 1. Uvedený „rozklad podľa premennej“ sa dá urobiť pre ľubovoľnú z premenných x_i .

„Rozklad podľa premennej“ využijeme ako nástroj, pomocou ktorého sa od „tabuľkového zadania“ funkcie dostaneme k jej vyjadreniu v tvare ANF.

Príklad 1a (2 premenné):³

x	y	f
0	0	1
0	1	1
1	0	0
1	1	1

$$\begin{aligned} f(x, y) &= [11 \ 01]_{(x, y)} = [11]_{(y)} \oplus x \cdot ([11] \oplus [01])_{(y)} = [11]_{(y)} \oplus x \cdot ([10])_{(y)} = \\ &= 1 \oplus y \cdot (1 \oplus 1) \oplus x \cdot (1 \oplus y \cdot (1 \oplus 0)) = 1 \oplus x \oplus x \cdot y \end{aligned}$$

XX

Riešme teraz príklad všeobecne zadanej funkcie dvoch premenných:

³ V nasledujúcom postupe z technických príčin píšeme stĺpec funkčných hodnôt f transponovaný na riadok. Na papieri ho možno v záujme názornosti ponechať ako stĺpec.

Hodnoty 0,1 v riadku neoddeľujeme, ale ak je to nutné kvôli prehľadnosti, na oddelenie používame medzery alebo čiarky.

K riadkom funkčných hodnôt spočiatku píšeme aj premenné (porovnajte tento zápis so zapojením multiplexora!), ale neskôr ich už písať nebudeme.

„Rozklad podľa premennej“ sa začína vždy od tej premennej, ktorá má v tabuľke „pokope“ nuly a jednotky. V našom prípade je to zľava od x , ale pri iných konvenciách poradia vstupných hodnôt to môže byť aj inak.

x	y	f
0	0	f_0
0	1	f_1
1	0	f_2
1	1	f_3

Hodnoty f_i sú čísla z množiny $\{0,1\}$.

$$\begin{aligned}
 f(x,y) &= [f_0 f_1 f_2 f_3]_{(x,y)} = [f_0 f_1]_{(y)} \oplus x \cdot [f_0 \oplus f_2, f_1 \oplus f_3]_{(y)} = \\
 &= f_0 \oplus y \cdot (f_0 \oplus f_1) \oplus x \cdot (f_0 \oplus f_2) \oplus xy \cdot (f_0 \oplus f_1 \oplus f_2 \oplus f_3)
 \end{aligned}$$

Zapišeme získané výsledky do tabuľky. Jednotlivé *termy* 1, y, x, xy a im prislúchajúce koeficienty zaradíme do riadkov tak, aby prítomnosť premennej x a y zodpovedala jednotke vo vstupných hodnotách:

x	y	termy	f	koeficienty
0	0	1	f_0	f_0
0	1	y	f_1	$f_0 \oplus f_1$
1	0	x	f_2	$f_0 \oplus f_2$
1	1	xy	f_3	$f_0 \oplus f_1 \oplus f_2 \oplus f_3$

Poradie sčítovaných funkčných hodnôt v koeficientoch sme zmenili tak, aby bolo vidno princíp ich usporiadania:

Budeme postupovať po riadkoch zhora dolu a všimneme si, že funkčná hodnota f_0 sa objavuje v každom ďalšom riadku presne tak, ako sú termy týchto riadkov formálnym „násobkom“ termu 1 z prvého riadku.

Podobne sa v poslednom riadku objavujú hostujúce hodnoty f_1 a f_2 z riadkov s termami y a x, lebo term xy je „násobkom“ termov y a x.

Každý riadok uzatvára príslušná funkčná hodnota f_i – „domáci pán“, ktorý si po usadení hostí nakoniec sám zasadne ku koeficientovému stolu. Za ním už nikto nenasleduje.

Ak si uvedomíme tento organizačný princíp, môžeme konkrétne príklady počítat rýchlejšie ako „rozkladaním podľa premenných“. Ukážeme si to na predošlom príklade.

Príklad 1b:

x	y	termy	f	koeficienty
0	0	1	1	1 = 1
0	1	y	1	$1 \oplus 1 = 0$
1	0	x	0	$1 \oplus 0 = 1$
1	1	xy	1	$1 \oplus 1 \oplus 0 \oplus 1 = 1$

Výsledok: $\text{ANF}(f) = 1.x \oplus 0.y \oplus 1.x \oplus 1.xy = 1 \oplus x \oplus xy$

Príklad 2a (3 premenné):

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

Postup rozkladom podľa premenných:

$$\begin{aligned}
 f(x,y) &= [1101 \ 0100] = [11 \ 01] \oplus x.[10 \ 01] = [11] \oplus y.[10] \oplus x.[10] \oplus xy.[11] = \\
 &= 1 \oplus y \oplus yz \oplus x \oplus xz \oplus xy
 \end{aligned}$$

XX

Všeobecný výpočet pre funkciu 3 premenných:

x	y	z	f
0	0	0	f_0
0	0	1	f_1
0	1	0	f_2
0	1	1	f_3
1	0	0	f_4
1	0	1	f_5
1	1	0	f_6
1	1	1	f_7

$$\begin{aligned}
 f(x,y) &= [f_0 \ f_1 \ f_2 \ f_3] \oplus x.[f_0 \oplus f_4, f_1 \oplus f_5, f_2 \oplus f_6, f_3 \oplus f_7] = \\
 &= [f_0 \ f_1] \oplus y.[f_0 \oplus f_2, f_1 \oplus f_3] \oplus x.[f_0 \oplus f_4, f_1 \oplus f_5] \oplus xy.[f_0 \oplus f_4 \oplus f_2 \oplus f_6, f_1 \oplus f_5 \oplus f_3 \oplus f_7] = \\
 &= f_0 \oplus z.(f_0 \oplus f_1) \oplus y.(f_0 \oplus f_2) \oplus yz.(f_0 \oplus f_2 \oplus f_1 \oplus f_3) \oplus x.(f_0 \oplus f_4) \oplus xz.(f_0 \oplus f_4 \oplus f_1 \oplus f_5) \oplus \\
 &\quad \oplus xy.(f_0 \oplus f_4 \oplus f_2 \oplus f_6) \oplus xyz.(f_0 \oplus f_4 \oplus f_2 \oplus f_6 \oplus f_1 \oplus f_5 \oplus f_3 \oplus f_7)
 \end{aligned}$$

Zhrnutie v tabuľke:

x	y	z	termy	f	koefficienty
0	0	0	1	f_0	f_0
0	0	1	z	f_1	$f_0 \oplus f_1$
0	1	0	y	f_2	$f_0 \oplus f_2$
0	1	1	yz	f_3	$f_0 \oplus f_1 \oplus f_2 \oplus f_3$
1	0	0	x	f_4	$f_0 \oplus f_4$
1	0	1	xz	f_5	$f_0 \oplus f_1 \oplus f_4 \oplus f_5$
1	1	0	xy	f_6	$f_0 \oplus f_2 \oplus f_4 \oplus f_6$
1	1	1	xyz	f_7	$f_0 \oplus f_1 \oplus f_2 \oplus f_3 \oplus f_4 \oplus f_5 \oplus f_6 \oplus f_7$

f_0 ide „na návštevu“ do všetkých riadkov, lebo ich termy sú násobkom 1.
 f_1 ide „na návštevu“ do riadkov s termami yz, xz, xyz, lebo v sebe majú z (sú „násobkami“ z).
 f_2 ide „na návštevu“ do riadkov s termami yz, xy, xyz, lebo v sebe majú y (sú „násobkami“ y).
 f_3 ide „na návštevu“ do riadkov s termom xyz, lebo v sebe má zahrnutý yz.
 f_4 ide „na návštevu“ do riadkov pod ním, lebo v sebe majú zahrnuté x.
 f_5 ide „na návštevu“ do riadku s termom xyz, lebo v sebe zahŕňa xz.
 f_6 ide „na návštevu“ do riadku s termom xyz, lebo v sebe zahŕňa xy.
 Po usadení hostí uzatvára spoločnosť domáci pán.

Príklad 2b:

x	y	z	termy	f	koefficienty
0	0	0	1	1	$1 = 1$
0	0	1	z	1	$1 \oplus 1 = 0$
0	1	0	y	0	$1 \oplus 0 = 1$
0	1	1	yz	1	$1 \oplus 1 \oplus 0 \oplus 1 = 1$
1	0	0	x	0	$1 \oplus 0 = 1$
1	0	1	xz	1	$1 \oplus 1 \oplus 0 \oplus 1 = 1$
1	1	0	xy	0	$1 \oplus 0 \oplus 0 \oplus 0 = 1$
1	1	1	xyz	0	$1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 = 0$

$$f(x,y) = 1 \oplus y \oplus yz \oplus x \oplus xz \oplus xy$$

Úlohy:

1. Zostavte (s podrobným výpočtom) všeobecnú tabuľku termov a koefficientov pre funkcie 4 premenných.
- 2.* Zovšeobecnite získané poznatky a skúsenosti aj na funkciu n premenných (ľubovoľné n).