Двоични (булеви) функции

Дефиниция 1 *Нека A е крайно множество и $n \in \mathbb{N}$. Всяка функция $f : A^n \to A$ наричаме* n-местна дискретна функция.

Нека $|A| = m$. Колко е броят на n-местните дискретни функции в A?

Да припомним, че от принципа за умножение следва, че броят на функциите $f : X \to Y$ е $|Y|^{|X|}$. Трябва да изберем $|X|$ стойности, като за всяка стойност $f(x)$ имаме $|Y|$ възможности. Също така, отново от принципа за умножение, $|A^n| = m^n$. От това следва, че броят на всички n-местни дискретни функции в A е m^{m^n}.

Дефиниция 2 *При $A = \{0, 1\}$, функциите $f : \{0, 1\}^n \to \{0, 1\}$ наричаме* n-местни двоични (булеви) функции.
Означаваме: $\mathcal{F}_2^n = \{f \mid f : \{0, 1\}^n \to \{0, 1\}\}$, $\mathcal{F}_2 = \bigcup_{n=1}^{\infty} \mathcal{F}_2^n$.

Да напомним, че елементите на $\{0, 1\}^n$ наричаме n-мерни (двоични) булеви вектори.

Често си мислим за една булева функция $f \in \mathcal{F}_2^n$ като функция на n променливи $x_1, x_2, \ldots, x_n$, всяка от които може да приема стойност 0 или 1.

Дефиниция 3 *Нека $f : \{0, 1\}^n \to \{0, 1\}$. Казваме, че x_i е* фиктивна променлива *за f или, че f* не зависи съществено *от x_i, ако за всички стойности $x_j \in \{0, 1\}$ при $j \neq i$ имаме, че*

$$f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) = f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n).$$

Ако x_i не е фиктивна за f, казваме, че f зависи съществено *от x_i.*

Например, ако f се задава с формула, в която не участва x_i, то е ясно, че x_i е фиктивна променлива за f. Обратното в общия случай не е вярно, например $f(x_1) = 0 \cdot x_1$ се задава с формула, в която участва x_1, но f не зависи съществено от x_1.

Ясно е, че ако всички променливи на f са фиктивни, то всяка стойност на f е равна на всяка друга стойност на f, т.е. f е константа. В случая имаме двете константи $\widetilde{0}$ и $\widetilde{1}$ (вълничката поставяме, ако искаме да подчертаем, че разглеждаме самата функция, а не стойността).

Дефиниция 4 *Дефинираме* стандартната линейна (лексикографска) наредба *в множеството $\{0, 1\}^n$ с индукция по $n \geq 1$.*
При $n = 1$ наредбата е: 0, 1.
При $n = 2$ наредбата е: 00, 01, 10, 11.
Нека сме дефинирали наредбата $\alpha_0, \alpha_1, \ldots, \alpha_{2^n-1}$ на $\{0, 1\}^n$.
Тогава наредбата на $\{0, 1\}^{n+1}$ е:

$$0\alpha_0, 0\alpha_1, \ldots, 0\alpha_{2^n-1}, 1\alpha_0, 1\alpha_1, \ldots, 1\alpha_{2^n-1}.$$

Подразбира се, че един n-мерен вектор е в релация с друг n-мерен вектор, ако стои преди него (отляво) в редицата. Наредбата се нарича лексикографска, тъй като е на речников принцип: сравняваме първите компоненти на двата n-мерни вектора, ако те съвпадат преминаваме към вторите компоненти и така нататък.

Друг полезен начин да си мислим за тази наредба е следният: поредният номер на един n-мерен булев вектор α съвпада с естественото число, което има двоично представяне α. Разбира се, номерацията започва от 0 и стига до $2^n - 1$.

При фиксираната стандартна наредба $\alpha_0,\ \alpha_1,\ \ldots,\ \alpha_{2^n-1}$ на $\{0,1\}^n$, всяка функция $f : \{0,1\}^n \to \{0,1\}$ представяме с 2^n-мерния булев вектор $f(\alpha_0)\ f(\alpha_1)\ \ldots\ f(\alpha_{2^n-1})$. От това представяне отново е видно, че броят на булевите функции на n променливи е 2^{2^n}.

Да разгледаме двоичните функции при $n = 1$ (на една променлива x). Те са общо 4 на брой:

x	g_0	g_1	g_2	g_3
0	0	0	1	1
1	0	1	0	1

За функцията g_0 имаме $g_0(0) = g_0(1) = 0$, т.е. g_0 е константата $\widetilde{0}$.

За функцията g_3 имаме $g_3(0) = g_3(1) = 1$, т.е. g_3 е константата $\widetilde{1}$.

Функцията g_1 има свойството $g_1(x) = x$ и можем да я наречем *идентитет*.

За функцията g_2 имаме $g_2(0) = 1$ и $g_2(1) = 0$, нарича се *отрицание*, означаваме $g_2(x) = \overline{x}$. Ако $x = 1$ считаме за стойност истина и $x = 0$ за стойност лъжа, то отрицанието има обичайния логически смисъл. Ако стойността на x се счита като бит информация, отрицанието често се нарича *инвертиране* или *преобръщане* на x.

По-нататък, да разгледаме двоичните функции при $n = 2$ (на две променливи x, y). Те са общо 16 на брой:

x	y	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Ясно е, че f_0 е константата $\widetilde{0}$ и f_{15} е константата $\widetilde{1}$.

Функцията f_1 се нарича *конюнкция* (логическо "и") и още може да се разглежда като умножение по модул 2. Означаваме: $f_1(x, y) = xy = x \wedge y$. Основното свойство на конюнкцията е:

$$xy = 1 \iff x = y = 1.$$

Функцията f_7 се нарича *дизюнкция* (логическо "или"). Означението за нея е: $f_7(x,y) = x \vee y$. Основното свойство е:

$$x \vee y = 0 \iff x = y = 0.$$

Функцията f_6 ще наричаме *сума по модул 2* (изключващо "или", xor) и за нея ще използваме означението $f_6(x,y) = x \oplus y$. В сила е свойството:

$$x \oplus y = 1 \iff (x = 0 \text{ и } y = 1) \text{ или } (x = 1 \text{ и } y = 0).$$

Функцията f_9 ще наричаме *еквиваленция* (логическа еквивалентност) и ще я означаваме с $f_9(x,y) = x \leftrightarrow y$. Основното ѝ свойство е:

$$x \leftrightarrow y = 1 \iff \text{стойностите на } x \text{ и } y \text{ съвпадат.}$$

Лесно се вижда, че $x \leftrightarrow y = \overline{x \oplus y}$.

Функцията f_{13} ще наричаме *импликация* (логическо "ако, то") и ще я означаваме с $f_{13}(x,y) = x \to y$. Нейното основно свойство е:

$$x \to y = 0 \iff x = 1 \text{ и } y = 0.$$

За функцията f_{11} имаме $f_{11}(x,y) = y \to x$ и можем да я наречем *обратна импликация*.

Функцията f_{14} се нарича *черта на Шефер* и се означава с $f_{14}(x,y) = x|y$. Тя представлява отрицание на конюнкцията: $x|y = \overline{xy}$.

Функцията f_8 се нарича *стрелка на Пирс* и се означава с $f_8(x,y) = x \downarrow y$. Тя съвпада с отрицанието на дизюнкцията: $x \downarrow y = \overline{x \vee y}$.

За функциите f_2 и f_4 няма специално наименование. Те могат да се изразят по следния начин: $f_2(x,y) = \overline{x \to y} = x\overline{y}$ и $f_4(x,y) = \overline{y \to x} = \overline{x}y$.

Дотук изброихме всичките 10 функции без фиктивни променливи, т.е. които зависят съществено от x и y.

Освен двете константи, остават още 4 функции, които зависят само от една променлива:

$$f_3(x,y) = x,\ f_5(x,y) = y,\ f_{12}(x,y) = \overline{x},\ f_{10}(x,y) = \overline{y}.$$

Функциите f_3 и f_5 ще означаваме с $f_3 = I_1^2,\ f_5 = I_2^2$.

Твърдение 5 *Основни закони за булевите функции:*

1. *комутативност* $xy = yx,\ x \vee y = y \vee x,\ x \oplus y = y \oplus x,\ x \leftrightarrow y = y \leftrightarrow x$.
2. *асоциативност* $(xy)z = x(yz),\ (x \vee y) \vee z = x \vee (y \vee z)$, $(x \oplus y) \oplus z = x \oplus (y \oplus z)$.
3. *дистрибутивност* $x(y \vee z) = xy \vee xz,\ x \vee yz = (x \vee y)(x \vee z)$, $x(y \oplus z) = xy \oplus xz$.
4. *идемпотентност* $xx = x,\ x \vee x = x$, *но* $x \oplus x = \widetilde{0}$.

5. *константи* $x.\widetilde{0} = \widetilde{0},\ x.\widetilde{1} = x,\ x \vee \widetilde{0} = x,\ x \vee \widetilde{1} = \widetilde{1},$
$x \oplus \widetilde{0} = x,\ x \oplus \widetilde{1} = \overline{x}.$

6. *отрицание* $x\overline{x} = \widetilde{0},\ x \vee \overline{x} = \widetilde{1},\ x \oplus \overline{x} = \widetilde{1},$
$\overline{\overline{x}} = x$ *(двойно отрицание),*
$\overline{xy} = \overline{x} \vee \overline{y},\ \overline{x \vee y} = \overline{x}.\overline{y}$ *(закони на Де Морган).*

Всеки един от тези закони може да се провери чрез изчерпване на всички възможности за стойностите $0, 1$ на променливите x, y, z.

Забележете, че ако в някой от законите заместим всички срещания на x, y или z с произволен булев израз отново получаваме закон. Например, за произволни булеви изрази ϕ, ψ имаме $\overline{\phi\psi} = \overline{\phi} \vee \overline{\psi}$.

Като следствие от асоциативността можем да образуваме многократна конюнкция, дизюнкция и сума по модул 2. За произволни булеви изрази $\phi_1, \phi_2, \ldots, \phi_n$ ще използваме записа

$$\bigvee_{i=1}^{n} \phi_i = \phi_1 \vee \phi_2 \vee \ldots \vee \phi_n$$

и подобно за $\bigwedge_{i=1}^{n} \phi_i$, $\bigoplus_{i=1}^{n} \phi_i$.

Съществува дуалност в част от законите, която по-нататък ще наречем принцип за двойнственост: ако в един закон размените конюнкцията и дизюнкцията, както и $\widetilde{0}$ и $\widetilde{1}$, то отново ще получите валиден закон.

Дефиниция 6 *Нека* $1 \leq k \leq n$. *Функцията* $I_k^n : \{0,1\}^n \to \{0,1\}$, *дефинирана с* $I_k^n(x_1, x_2, \ldots, x_n) = x_k$ *ще наричаме* проектираща функция *или* проекция.

Дефиниция 7 *Нека за* $n, k \geq 1$ *са дадени функциите* $f : \{0,1\}^k \to \{0,1\}$ *и* $g_1, g_2, \ldots, g_k : \{0,1\}^n \to \{0,1\}$. *Функцията* $h : \{0,1\}^n \to \{0,1\}$, *дефинирана с*

$$h(x_1, x_2, \ldots, x_n) = f(g_1(x_1, x_2, \ldots, x_n), g_2(x_1, x_2, \ldots, x_n), \ldots, g_k(x_1, x_2, \ldots, x_n))$$

наричаме суперпозиция *на* f *и* $g_1, g_2, \ldots, g_k$ *и означаваме* $h = f(g_1, g_2, \ldots, g_k)$.

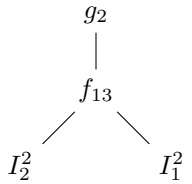
Всъщност, суперпозицията може да се разглежда като композиция на две функции: първо действа функция от тип $\{0,1\}^n \to \{0,1\}^k$, която изпраща $(x_1, x_2, \ldots, x_n)$ в $(g_1(x_1, x_2, \ldots, x_n), g_2(x_1, x_2, \ldots, x_n), \ldots, g_k(x_1, x_2, \ldots, x_n))$, след това действа $f : \{0,1\}^k \to \{0,1\}$.

При дадено множество от булеви функции, ние ще се интересуваме от изразите, които могат да се построят чрез дадените функции, като се започне от проекциите и се прилага неколкократно операцията суперпозиция.

Пример 1. За функцията f_4 по-горе имахме $f_4(x,y) = \overline{y \to x}$. По-подробно, този израз може да се запише по следния начин:

$$f_4(x,y) = g_2(f_{13}(I_2^2(x,y), I_1^2(x,y))),$$

където g_2 е отрицанието и f_{13} е импликацията. Както се вижда, проекциите играят ролята на променливите в израза. Операцията суперпозиция е приложена два пъти, първо с f_{13} и след това с g_2. Друг начин да представим дадения израз е със следното синтактично дърво:



Пример 2. Да разгледаме закона $x(y \vee z) = xy \vee xz$. В него участват конюнкцията f_1, дизюнкцията f_7 и трите проекции I_1^3, I_2^3, I_3^3. Лявата страна се представя с израза

$$f_1(I_1^3(x,y,z), f_7(I_2^3(x,y,z)), I_3^3(x,y,z))),$$

а дясната страна с израза

$$f_7(f_1(I_1^3(x,y,z), I_2^3(x,y,z)), f_1(I_1^3(x,y,z), I_3^3(x,y,z))).$$

Съответните синтактични дървета са:

Обърнете внимание, че двете дървета са различни, но представят една и съща булева функция на трите променливи x, y, z.

Дефиниция 8 (затваряне на множество от булеви функции) *Нека $F \subseteq \mathcal{F}_2$ е множество от булеви функции. Дефинираме редицата $\{F_n\}_{n=0}^{\infty}$ от множества от булеви функции с индукция по n:*

$$\begin{aligned} F_0 &= F \cup \{I_k^n \mid 1 \leq k \leq n\}, \\ F_{n+1} &= F_n \cup \{h \mid \exists\, f, g_1, \ldots, g_k \in F_n : h = f(g_1, \ldots, g_k)\}. \end{aligned}$$

Затварянето *на F е множеството* $[F] = \bigcup_{n=0}^{\infty} F_n$.

С други думи, във F_0 поставяме функциите от F и проекциите. За да образуваме F_{n+1} взимаме полученото до момента F_n и добавяме към него всевъзможните булеви функции, които могат да се получат със суперпозиция на функции във F_n. Накрая, затварянето $[F]$ е обединението на всички образувани множества F_n.

Друга възможна дефиниция на затварянето е следната: $[F]$ е най-малкото (относно $\subseteq$) множество, което съдържа F и проекциите и е затворено относно суперпозиция, т.е.

$$f, g_1, \ldots, g_k \in [F] \implies f(g_1, \ldots, g_k) \in [F]. \qquad (*)$$

Наистина, ако $f \in F_{s_0}$ и $g_i \in F_{s_i}$ за $i = 1, \ldots, k$, то е ясно, че суперпозицията $f(g_1, \ldots, g_k) \in F_s$, където $s = \max(s_0, s_1, \ldots, s_k) + 1$.

Друг начин да опишем по-неформално затварянето: една функция f принадлежи на $[F]$ точно когато тя може да се представи с израз/синтактично дърво, в което всички върхове са надписани с функции от F или с проекции.

Твърдение 9 *В сила са следните основни свойства на затварянето:*

1. $F \subseteq [F]$;
2. $F \subseteq G \implies [F] \subseteq [G]$;
3. $[[F]] = [F]$.

Доказателство. 1) е ясно, тъй като $F \subseteq F_0 \subseteq [F]$.

За 2) да предположим, че $F \subseteq G$. С индукция по n ще покажем, че $F_n \subseteq G_n$. Базата е при $n = 0$: тъй като $F \subseteq G$,

$$F_0 \;=\; F \cup \{I_k^n \mid 1 \le k \le n\} \;\subseteq\; G \cup \{I_k^n \mid 1 \le k \le n\} \;=\; G_0.$$

Стъпка: нека предположим, че е изпълнено $F_n \subseteq G_n$. Да вземем произволна функция $h \in F_{n+1}$. Единият вариант е $h \in F_n$. От индукционното предположение, $h \in G_n$, така че $h \in G_{n+1}$, тъй като $G_n \subseteq G_{n+1}$. Другият вариант е $h = f(g_1, \ldots, g_k)$, където $f, g_1, \ldots, g_k \in F_n$. От индукционното предположение, $f, g_1, \ldots, g_k \in G_n$, така че от дефиницията за затваряне имаме $h \in G_{n+1}$. Така получихме, че $F_{n+1} \subseteq G_{n+1}$. Накрая, $[F] = \bigcup_{n=0}^{\infty} F_n \subseteq \bigcup_{n=0}^{\infty} G_n = [G]$.

За 3) включването $[F] \subseteq [[F]]$ следва от 1). За другото включване ще покажем, че $[F]_n \subseteq [F]$ с индукция по n, подобна на 2).

База: при $n = 0$ имаме $[F]_0 = [F] \cup \{I_k^n \mid 1 \le k \le n\} \subseteq [F]$, тъй като $[F]$ по дефиниция съдържа проекциите.

Стъпка: нека е изпълнено $[F]_n \subseteq [F]$. Да вземем произволна функция $h \in [F]_{n+1}$. Първият вариант е $h \in [F]_n$. От индукционното предположение, $h \in [F]$. Вторият вариант е $h = f(g_1, \ldots, g_k)$, където $f, g_1, \ldots, g_k \in [F]_n$. От индукционното предположение, $f, g_1, \ldots, g_k \in [F]$. Прилагаме (*) и получаваме $h \in [F]$. Така $[F]_{n+1} \subseteq [F]$. Накрая, $[[F]] = \bigcup_{n=0}^{\infty} [F]_n \subseteq [F]$ и доказателството е завършено.