Пълни множества от булеви функции

Дефиниция 1 *Казваме, че $F \subseteq \mathcal{F}_2$ е* пълно, *ако $[F] = \mathcal{F}_2$.*

С други думи, F е пълно, ако всяка булева функция може да се изрази с формула, в която участват само проекции (променливи) и функции от F. Например, $\mathcal{F}_2$ е пълно (всяка функция се изразява чрез себе си), но ще видим и доста по-съдържателни примери.

Дефиниция 2 *Нека $a \in \{0,1\}$. Въвеждаме означението:*

$$x^a = \begin{cases} \overline{x}, & \text{ако } a = 0, \\ x, & \text{ако } a = 1. \end{cases}$$

По този начин, x^a приема стойност 1 при $a = 0,\ x = 0$ и при $a = 1,\ x = 1$. Разбира се, това означава, че x^a съвпада с $x \leftrightarrow a$, но записът със степени е по-удобен (един символ по-малко).

Изразите от вида $x_1^{a_1} x_2^{a_2} \dots x_k^{a_k}$ наричаме *елементарни конюнкции.*

Можем да считаме, че $x_i \neq x_j$ при $i \neq j$, тъй като $x^a x^a = x^a$ и също ако една променлива x участва заедно с отрицанието си $\overline{x}$, то елементарната конюнкция съвпада с константата $\widetilde{0}$.

Лема 3 *Равенството $b_1^{a_1} b_2^{a_2} \dots b_k^{a_k} = 1$ е в сила тогава и само тогава, когато $b_1 = a_1,\ b_2 = a_2,\ \dots,\ b_k = a_k$.*

Доказателство. От свойството на конюнкцията, $b_1^{a_1} b_2^{a_2} \dots b_k^{a_k} = 1$ е еквивалентно на $b_1^{a_1} = 1,\ b_2^{a_2} = 1,\ \dots,\ b_k^{a_k} = 1$, което от горните разглеждания е същото като $b_1 = a_1,\ b_2 = a_2,\ \dots,\ b_k = a_k$.

Твърдение 4 (разлагане на булева функция по i променливи) *Нека $f : \{0,1\}^n \to \{0,1\}$ е булева функция на променливите $x_1, x_2, \dots, x_n$ и $1 \leq i \leq n$. Тогава е в сила равенството:*

$$f(x_1, x_2, \dots, x_n) \quad = \bigvee_{a_1,\dots,a_i \in \{0,1\}} x_1^{a_1} \dots\ x_i^{a_i} . f(a_1, \dots, a_i, x_{i+1}, \dots, x_n).$$

Доказателство. Да означим дясната страна с $g(x_1, \dots, x_n)$. За произволно $(b_1, \dots, b_n) \in \{0,1\}^n$ имаме:

$$\begin{aligned} g(b_1, \dots, b_n) = 1 \iff & \text{ съществуват } a_1, \dots, a_i \in \{0,1\}, \text{ такива че} \\ & b_1^{a_1} \dots b_i^{a_i} . f(a_1, \dots, a_i, b_{i+1}, \dots, b_n) = 1 \\ \iff & \text{ съществуват } a_1, \dots, a_i \in \{0,1\}, \text{ такива че} \\ & b_1 = a_1,\ \dots,\ b_i = a_i,\ f(a_1, \dots, a_i, b_{i+1}, \dots, b_n) = 1 \\ \iff & f(b_1, \dots, b_n) = 1. \end{aligned}$$

За първата еквивалентност използвахме свойството на дизюнкцията. За втората еквивалентност приложихме горната лема. Третата еквивалентност

е логически тривиална, тъй като няма свобода за стойностите на $a_1, \ldots, a_i$, пред които стои кванторът за съществуване.

Разбира се, тъй като f и g са булеви функции на n променливи, това е достатъчно за да заключим, че $f = g$.

Теорема 5 (Бул) *Множеството* $\{\overline{x},\ xy,\ x \vee y\}$ *е пълно.*

Доказателство. Нека $f \in \mathcal{F}_2^n$ е произволна булева функция на n променливи. Ако $f = \widetilde{0}$, то е ясно, че $f(x_1, x_2, \ldots, x_n) = x_1.\overline{x_1}$ и следователно $f \in [\{\overline{x},\ xy,\ x \vee y\}]$ (дори без използване на дизюнкцията).

Нека $f \neq \widetilde{0}$. Прилагаме горното твърдение при $i = n$ и получаваме равенството:

$$f(x_1, x_2, \ldots, x_n) \quad = \bigvee_{a_1,\ldots,a_n \in \{0,1\}} x_1^{a_1} \ldots\ x_n^{a_n}.f(a_1, a_2, \ldots, a_n).$$

Ако $f(a_1, a_2, \ldots, a_n) = 0$, то съответният член има стойност 0 и не допринася към дизюнкцията ($x \vee 0 = x$). Затова можем да се ограничим до онези членове с $f(a_1, a_2, \ldots, a_n) = 1$ и така имаме представянето:

$$f(x_1, x_2, \ldots, x_n) \quad = \bigvee_{\substack{a_1,\ldots,a_n \in \{0,1\} \\ f(a_1,a_2,\ldots,a_n)=1}} x_1^{a_1} \ldots\ x_n^{a_n}.$$

Тъй като $x_i^{a_i} \in \{x_i, \overline{x_i}\}$, в дясната страна участват само дизюнкция, конюнкция и отрицание. Така и в този случай $f \in [\{\overline{x},\ xy,\ x \vee y\}]$.

Израз за булева функция f, който представлява дизюнкция на елементарни конюнкции се нарича *дизюнктивна нормална форма* на f.

Получената формула за f в доказателството на теоремата на Бул се нарича *съвършена* дизюнктивна нормална форма на f, тъй като във всяка елементарна конюнкция участват *всички* променливи $x_1, x_2, \ldots, x_n$.

По този начин, всяка функция $f \neq \widetilde{0}$ притежава единствена съвършена дизюнктивна нормална форма, но може да има и други дизюнктивни нормални форми.

Например, дизюнкцията $x \vee y$ има 3 единични стойности, при аргументи $x = 0,\ y = 1$; $x = 1,\ y = 0$; $x = y = 1$. Следователно, нейната съвършена дизюнктивна нормална форма е:

$$x \vee y \quad = \quad \overline{x}y \ \vee \ x\overline{y} \ \vee \ xy.$$

Освен това, тя притежава още 3 дизюнктивни нормални форми:

$$x \vee y \quad = \quad x \vee y \ = \ x \vee \overline{x}y \ = \ x\overline{y} \vee y.$$

Последните две могат да се получат с така наречената *слепване*:

$$\psi\phi \ \vee \ \overline{\psi}\phi \ = \ \phi$$

за произволни булеви изрази ϕ, ψ.

Следващото твърдение позволява да построим и други пълни множества, като следствие от теоремата на Бул.

Твърдение 6 *Нека $F \subseteq \mathcal{F}_2$ е пълно и $G \subseteq \mathcal{F}_2$ е такова, че $F \subseteq [G]$. Тогава G също е пълно.*

Доказателство. Използваме свойствата на затварянето. По условие имаме $F \subseteq [G]$, така че $[F] \subseteq [[G]] = [G]$. Тъй като $[F] = \mathcal{F}_2$, това влече $[G] = \mathcal{F}_2$.

Твърдението показва, че ако F е пълно и можем да изразим всяка функция от F чрез проекциите и функции от G, то G също е пълно.

Следствие 7 *$\{\overline{x},\ xy\}$ е пълно.*

Доказателство. Очевидно имаме, че $\overline{x},\ xy \in [\{\overline{x},\ xy\}]$. Освен това от законите на Де Морган, $x \vee y\ =\ \overline{\overline{x}.\overline{y}}$, което показва, че $x \vee y \in [\{\overline{x},\ xy\}]$. Получихме, че $\{\overline{x},\ xy,\ x \vee y\} \subseteq [\{\overline{x},\ xy\}]$. От теоремата на Бул в комбинация с твърдението, $\{\overline{x},\ xy\}$ е пълно.

Следствие 8 *$\{\overline{x},\ x \vee y\}$ е пълно.*

Доказателство. Аналогично на предходното следствие, като използваме другия закон на Де Морган $xy\ =\ \overline{\overline{x} \vee \overline{y}}$.

Следствие 9 *$\{\widetilde{0},\ \widetilde{1},\ xy,\ x \oplus y\}$ е пълно.*

Доказателство. Достатъчно е да отбележим, че $\overline{x} = x \oplus \widetilde{1}$ и да използваме първото следствие.

Разбира се, константата $\widetilde{0}$ не е необходима, тъй като $\widetilde{0} = \widetilde{1} \oplus \widetilde{1}$, но я включваме за удобство.

Дефиниция 10 *Израз от вида*

$$a_\emptyset \bigoplus_{1\le i\le n} a_i x_i \bigoplus_{1\le i<j\le n} a_{ij} x_i x_j \bigoplus_{1\le i<j<k\le n} a_{ijk} x_i x_j x_k \bigoplus \ldots \bigoplus a_{12\ldots n} x_1 x_2 \ldots x_n,$$

където $a_I \in \{0,1\}$ за $I \subseteq \{1,2,\ldots,n\}$ се нарича полином на Жегалкин *на променливите $x_1, x_2, \ldots, x_n$.*

Забележете, че в сумата $\bigoplus_{1\le i_1<i_2<\ldots i_k<n} a_{i_1 i_2 \ldots i_k} x_{i_1} x_{i_2} \ldots x_{i_k}$ има $\binom{n}{k}$ събираеми. Общият брой събираеми е $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ (и толкова е броят на коефициентите a_I в полинома).

Теорема 11 *Всяка булева функция $f \in \mathcal{F}_2^n$ се представя по единствен начин чрез полином на Жегалкин.*

Доказателство. Първо да съобразим, че такова представяне за $f \in \mathcal{F}_2^n$ съществува. От последното следствие получаваме, че f се представя с израз, в който участват само функциите $\widetilde{0},\ \widetilde{1},\ xy,\ x \oplus y$ и променливите $x_1, x_2, \ldots, x_n$. В този израз разкриваме скобите, като използваме дистрибутивния закон $x(y \oplus z) = xy \oplus xz$. След това имаме $xx = x,\ x\widetilde{1} = x,\ x\widetilde{0} = \widetilde{0}$, така че всяко от получените неконстантни събираеми може да се представи като конюнкция (произведение) на различни променливи (без степени). Ако някое от тези събираеми участва повече от веднъж, съкращаваме го със $s \oplus s = \widetilde{0}$. Така получаваме полином на Жегалкин за f.

Остава да съобразим, че представянето е единствено. Да разгледаме съответствието, което съпоставя на всеки полином на Жегалкин P на n променливи, функцията $f \in \mathcal{F}_2^n$, която се представя с P. Ясно е, че това е добре определено съответствие, което е сюрективно (от първата част на доказателството). От друга страна, в общия вид на полинома на Жегалкин има 2^n коефициента, така че броят на различните полиноми е 2^{2^n}. Точно толкова са и функциите $f \in \mathcal{F}_2^n$. Сюрективно изображение между две крайни множества с еднакъв брой елементи е задължително и инективно (това следва от принципа на Дирихле). Така получаваме по един единствен полином на Жегалкин за всяка функция. По-неформално можем да разсъждаваме така: ако някоя функция f се представя с два различни полинома P_1 и P_2, то останалите $2^{2^n} - 2$ полинома няма да стигнат за останалите $2^{2^n} - 1$ функции (от първата част ние знаем, че не е възможно функция да остане без съответен полином).

Възниква въпросът как практически да намерим полинома на Жегалкин на дадена булева функция.

Първи начин(метод на неопределените коефициенти). Ще го илюстрираме върху функция на две променливи x, y.

Общият вид на полинома е $f(x, y) = a_0 \oplus a_1 x \oplus a_2 y \oplus a_{12} xy$.

Предполагаме, че $f(0,0) = f_0,\ f(1,0) = f_1,\ f(0,1) = f_2,\ f(1,1) = f_3$, където f_0, f_1, f_2, f_3 са известни булеви стойности (обърнете внимание, че тук разменяме местата на f_1 и f_2, т.е. векторът на функцията е $f_0 f_2 f_1 f_3$). За всяко от тези равенства получаваме по едно уравнение относно неизвестните коефициенти:

$$\begin{aligned} a_0 &= f_0, \\ a_0 \oplus a_1 &= f_1, \\ a_0 \oplus a_2 &= f_2, \\ a_0 \oplus a_1 \oplus a_2 \oplus a_{12} &= f_3. \end{aligned}$$

Получената система е в триъгълен вид, така че тя лесно може да се разреши отгоре надолу.

Като пример да разгледаме импликацията $f(x, y) = x \to y$.

Нейните стойности са $f_0 = f_2 = f_3 = 1$ и $f_1 = 0$. Системата има вида:

$$\begin{aligned} a_0 &= 1, \\ a_0 \oplus a_1 &= 0, \\ a_0 \oplus a_2 &= 1, \\ a_0 \oplus a_1 \oplus a_2 \oplus a_{12} &= 1. \end{aligned}$$

Получаваме последователно: $a_0 = 1,\ a_1 = 1,\ a_2 = 0,\ a_{12} = 1$. Окончателно:

$$f(x, y) \ = \ x \to y \ = \ 1 \oplus x \oplus xy.$$

Втори начин(от съвършена дизюнктивна нормална форма). Ще го илюстрираме за дизюнкцията $f(x, y) \ = \ x \vee y$.

Започваме със съвършената дизюнктивна нормална форма на f:

$$f(x, y) \ = \ \overline{x}y \vee x\overline{y} \vee xy.$$

В нея заместваме всяко участие на $\vee$ с $\oplus$. Разбира се, това са различни функции, но в случая такова заместване е позволено, тъй като при произволни стойности на променливите x, y *най-много един* от членовете на съвършената дизюнктивна нормална форма има стойност 1, а всички останали нейни членове имат стойност 0. Дизюнкция на най-много една 1 и още няколко на брой 0 съвпада със сумата по модул 2 на тази 1 и съответния брой 0.

Получаваме:

$$f(x, y) \ = \ \overline{x}y \oplus x\overline{y} \oplus xy.$$

Остава да заместим отрицанието с добавяне на 1 по модул 2 и да разкрием скобите:

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

Забележете, че в общия случай този метод не е валиден за произволна дизюнктивна нормална форма на f. Например, $f(x, y) \ = \ x \vee y$ е дизюнктивна нормална форма, но в нея не можем да заместим $\vee$ с $\oplus$.

Затворени множества от булеви функции

Дефиниция 12 *Казваме, че $F \subseteq \mathcal{F}_2$ е* затворено, *ако $[F] = F$.*

Забележете, че F е затворено и пълно само при $F = \mathcal{F}_2$. Така затворените множества, различни от $\mathcal{F}_2$ никога не са пълни и по-общо не съдържат пълни подмножества.

Следващото твърдение дава начин да проверяваме затвореност на различни множества от булеви функции.

Твърдение 13 (критерий за затвореност) *Нека е дадено $F \subseteq \mathcal{F}_2$, за което са изпълнени условията:*

1. $I_k^n \in F$ за произволни n, k с $1 \leq k \leq n$.

2. $f, g_1, \ldots, g_k \in F \ \Rightarrow \ f(g_1, \ldots, g_k) \in F$.

Тогава F е затворено множество.

Доказателство. С индукция по n ще проверим, че $F_n \subseteq F$, където множествата F_n са от дефиницията за затваряне.

База: при $n = 0$ имаме $F_0 = F \cup \{I_k^n \mid 1 \leq k \leq n\}$. От условие 1. получаваме, че $F_0 \subseteq F$.

Стъпка: нека е изпълнено $F_n \subseteq F$ и да вземем $h \in F_{n+1}$. Първият вариант е $h \in F_n$ и 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 $f, g_1, \ldots, g_k \in F$ и от условие 2. $h \in F$. С това проверихме, че $F_{n+1} \subseteq F$ и индукцията е завършена. Накрая, $[F] = \bigcup_{n=0}^{\infty} F_n \subseteq F$ и също $F \subseteq [F]$, така че $[F] = F$.

Дефиниция 14 (булеви функции запазващи константите) *Казваме, че $f \in \mathcal{F}_2^n$* запазва нулата*, ако $f(0, 0, \ldots, 0) = 0$. Казваме, че $f \in \mathcal{F}_2^n$* запазва единицата*, ако $f(1, 1, \ldots, 1) = 1$. Означаваме:*

$T_0^n = \{f \in \mathcal{F}_2^n \mid f$ *запазва нулата*$\}$, $T_0 = \bigcup_{n=1}^{\infty} T_0^n$,
$T_1^n = \{f \in \mathcal{F}_2^n \mid f$ *запазва единицата*$\}$, $T_1 = \bigcup_{n=1}^{\infty} T_1^n$.

Примери. $xy \in T_0 \cap T_1$, $x \vee y \in T_0 \cap T_1$, $\widetilde{0} \in T_0 \setminus T_1$, $\widetilde{1} \in T_1 \setminus T_0$,
$\overline{x} \notin T_0 \cup T_1$, $x|y \notin T_0 \cup T_1$, $x \downarrow y \notin T_0 \cup T_1$.

Забележете, че $|T_0^n| = |T_1^n| = 2^{2^n - 1} = \frac{1}{2}|\mathcal{F}_2^n|$, тъй като всяка n-местна булева функция, запазваща някоя от константите се дефинира свободно върху всички n-мерни двоични вектори, с изключение на един. По-точно можем да кажем, че в зависимост от стойностите си в нулевия и в единичния вектор $\mathcal{F}_2^n$ се разбива на 4 непресичащи се множества с еднакъв брой елементи: $T_0^n \setminus T_1^n$, $T_1^n \setminus T_0^n$, $T_0^n \cap T_1^n$, $\mathcal{F}_2^n \setminus (T_0^n \cup T_1^n)$. Обединението на първото и третото множество дава T_0^n, а обединението на второто и третото множество дава T_1^n.

Твърдение 15 *Множествата T_0 и T_1 са затворени.*

Доказателство. Нека $c \in \{0, 1\}$. Проверяваме двете условия:

1. $I_k^n(c, c, \ldots, c) = c$ за $1 \leq k \leq n$, така че $I_k^n \in T_c$.
2. Нека $f, g_1, \ldots, g_k \in T_c$ и $h = f(g_1, \ldots, g_k)$.

Тогава $h(c, c, \ldots, c) = f(g_1(c, c, \ldots, c), \ldots, g_k(c, c, \ldots, c)) = f(c, \ldots, c) = c$, така че $h \in T_c$.

От критерия за затвореност, T_0 и T_1 са затворени.

Двойнствени булеви функции

Дефиниция 16 *Нека $f \in \mathcal{F}_2^n$ е булева функция на n променливи.*

Дефинираме функцията $f^\star \in \mathcal{F}_2^n$, която се нарича двойнствена *на f с равенството:*

$$f^\star(x_1, x_2, \ldots, x_n) = \overline{f(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n})}.$$

Векторите $\alpha \in \{0, 1\}^n$, $\alpha = a_1 a_2 \ldots a_n$ и $\overline{\alpha} = \overline{a_1}\ \overline{a_2} \ldots \overline{a_n}$ ще наричаме *противоположни*. Можем да кажем, че f и $f^\star$ приемат противоположни стойности върху противоположни вектори.

Да съобразим, че α и $\overline{\alpha}$ са винаги симетрично разположени спрямо средата в стандартната линейна наредба на n-мерните двоични вектори.

Нека α има позиция x, т.е. x е числото с двоично представяне α. Тогава е ясно, че $\overline{\alpha}$ има позиция $2^n - 1 - x$. С други думи, преди α в стандартната наредба има x на брой вектори, а след $\overline{\alpha}$ има също x на брой вектори. Щом α и $\overline{\alpha}$ са на еднакво разстояние от двата края на наредбата, то те са на еднакво разстояние и от средата | на наредбата:

$$\underbrace{0^n \ldots\ldots}_{x \text{ вектора}} \ \alpha \ \ldots | \ldots \ \overline{\alpha} \ \underbrace{\ldots\ldots 1^n}_{x \text{ вектора}}.$$

Получаваме следния *алгоритъм за намиране на* $f^\star$*:*

Даден е вектор $\alpha_0\alpha_1 \ldots \alpha_{2^n-1}$, представящ функцията $f \in \mathcal{F}_2^n$.

1. Намираме вектора на функцията $f(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n})$, т.е. обръщаме реда на стойностите в дадения вектор: $\alpha_{2^n-1}\alpha_{2^n-2} \ldots \alpha_0$.

2. Взимаме противоположни стойности на вектора от 1. и окончателно получаваме вектора на $f^\star$: $\overline{\alpha_{2^n-1}}\ \overline{\alpha_{2^n-2}}\ \ldots\ \overline{\alpha_0}$.

Забележете, че двете стъпки комутират, т.е. могат да се извършат и в обратен ред. Също така, всяка от двете стъпки, приложена двукратно към един вектор дава същия вектор. От това следва, че $(f^\star)^\star = f$, т.е. двойнствената на $f^\star$ съвпада с f.

Пример 1. Да намерим двойнствената на xy. Това може да стане директно с дефиницията: $(xy)^\star = \overline{\overline{x}.\overline{y}} = \overline{\overline{x} \vee \overline{y}} = x \vee y$. Или с алгоритъма: векторът на xy е 0001, стъпка 1. дава 1000 и стъпка 2. дава 0111, което е векторът на $x \vee y$. Разбира се, това показва също, че $(x \vee y)^\star = xy$.

Пример 2. $x^\star = \overline{\overline{x}} = x$. С алгоритъма: $01 \to 10 \to 01$.

Пример 3. $(\overline{x})^\star = \overline{\overline{\overline{x}}} = \overline{x}$. С алгоритъма: $10 \to 01 \to 10$.

Пример 4. $(\widetilde{0})^\star = \widetilde{1}$, $(\widetilde{1})^\star = \widetilde{0}$. Забележете, че стъпка 1. не променя вектора на двете константи.

Твърдение 17 (принцип за двойнственост) *Нека* $h = f(g_1, \ldots, g_k)$. *Тогава* $h^\star = f^\star(g_1^\star, \ldots, g_k^\star)$.

Доказателство. За произволни стойности на $x_1, \ldots, x_n$:

$$\begin{aligned} h^\star(x_1, \ldots, x_n) &= \overline{h(\overline{x_1}, \ldots, \overline{x_n})} \\ &= \overline{f(g_1(\overline{x_1}, \ldots, \overline{x_n}), \ldots, g_k(\overline{x_1}, \ldots, \overline{x_n}))} \\ &= \overline{f(\overline{g_1^\star(x_1, \ldots, x_n)}, \ldots, \overline{g_k^\star(x_1, \ldots, x_n)})} \\ &= f^\star(g_1^\star(x_1, \ldots, x_n), \ldots, g_k^\star(x_1, \ldots, x_n)). \end{aligned}$$

Принципът за двойнственост по-общо показва, че ако в един израз, представящ функцията f, заместим всяко участие на функция с нейната двойнствена, то получаваме израз, представящ функцията $f^\star$.

Пример 1. Знаем, че е в сила дистрибутивният закон $x(y \vee z) = xy \vee xz$. Прилагаме принципа за двойнственост към това равенство, т.е. разменяме конюнкциите с дизюнкциите. Отново получаваме валиден закон (това всъщност е другият дистрибутивен закон): $x \vee yz = (x \vee y)(x \vee z)$.

Пример 2. Да вземем един от законите на Де Морган: $\overline{xy} = \overline{x} \vee \overline{y}$.

Прилагаме принципа за двойнственост (отрицанията не се променят). Получаваме другия закон на Де Морган: $\overline{x \vee y} = \overline{x}.\overline{y}$.