Пълнота на множество от булевите функции. Полиноми на Жегалкин.

Минко Марков
14 януари 2026 г.

Съдържание

1 Пълнота на множества от булеви функции

1.1 Неформална и формална дефиниция

Нека $\mathsf{F} \subseteq \mathcal{F}$. Неформално, множеството F е *пълно*, ако всяка булева функция $\mathsf{f} \in \mathcal{F}$ може да бъде представена чрез функциите от F. Това наистина е неформално, защото какво означава "представяне"?

Формално, нека $[\mathsf{F}]$ означава затварянето на F спрямо унификация на променливи и композиция, като затварянето $[\mathsf{F}]$ може да се дефинира чрез следната индуктивна дефиниция.

Определение 1 (Затваряне на множество от булеви функции)**.** *Нека $\mathsf{F} \subseteq \mathcal{F}$. Тогава $[\mathsf{F}]$ е най-малкото по включване множество, което е подмножество на $\mathcal{F}$, притежаващо следните свойства.*

- $[\mathsf{F}]$ *съдържа всички функции от* F.
- *Нека* f *е функция, която се съдържа в* $[\mathsf{F}]$. *Нека* f *има поне един аргумент. Нека идентифицираме някои от променливите на* f. *Получената функция се съдържа в* $[\mathsf{F}]$.

- *Нека* f *и* g *са произволни функции от* $[F]$. *Нека* f *има* $n \geqslant 1$ *аргумента. Нека* $i \in \{1, \ldots, n\}$. *Тогава композицията на* g *на мястото на* i*-тата променлива на* f *също се съдържа в* $[F]$.

Определение 2 (Пълнота на множество от булеви функции)**.** *В контекста на Определение 1,* F *е пълно множество, ако* $[F] = \mathcal{F}$. □

1.2 Теоремата на Boole: доказателство за пълнота от първи принципи

Теорема 1 (теорема на Boole)**.** *Множеството от трите булеви функции конюнкция, дизюнкция и отрицание е пълно.*

Доказателство: Нека $F = \{\wedge, \vee, \mathtt{neg}\}$. Ще докажем, че всяка $f \in \mathcal{F}$ има формула над F. От това следва веднага, че $[F] = \mathcal{F}$.

Първо да допуснем, че $f \neq 0$. Ще докажем, че съществува СъвДНФ ϕ, такава че f е семантиката на ϕ. Нека f има n аргумента. Тогава f, в каноничното си представяне, е вектор с дължина 2^n. Щом f не е константа нула, този вектор има поне една единица. Нека f има точно k единици, където $1 \leqslant k \leqslant 2^n$. Нека $\mathbf{b}_1$, $\mathbf{b}_2$, …, $\mathbf{b}_k$ са булевите вектори от $\{0,1\}^n$, такива че

$$\begin{aligned} f(\mathbf{b}_1) &= 1 \\ f(\mathbf{b}_2) &= 1 \\ &\cdots \\ f(\mathbf{b}_k) &= 1 \end{aligned}$$

Нека x_1, x_2, …, x_n са булеви променливи, над които ще построим ϕ. Построяваме точно k пълни конюнктивни клаузи λ_1, λ_2, …, λ_k по следните правила. Нека $b_{i,j}$, където $1 \leqslant i \leqslant k$ и $1 \leqslant j \leqslant n$, е j-ият елемент на вектора $\mathbf{b}_i$. За всяко $i \in \{1, \ldots, k\}$ и $j \in \{1, \ldots, n\}$:

- ако $b_{i,j} = 0$, то променливата x_j участва в λ_i с отрицателния си литерал $\overline{x_i}$.
- ако $b_{i,j} = 1$, то променливата x_j участва в λ_i с положителния си литерал x_i.

Тогава $\phi = \lambda_1 \vee \lambda_2 \vee \cdots \vee \lambda_k$.

Ще докажем, че f е семантиката на ϕ.

- Разглеждаме произволен $\mathbf{a} \in \{0,1\}^n$, такъв че $f(\mathbf{a}) = 0$. Тоест, $\mathbf{a}$ не е нито един от векторите $\mathbf{b}_1$, $\mathbf{b}_2$, …, $\mathbf{b}_k$. Мислим за $\mathbf{a}$ като за валюация $\mathbf{t}$ на променливите x_1, x_2, …, x_n. За всяко $i \in \{1, \ldots, k\}$ е вярно, че поне един литерал в клаузата λ_i има стойност 0 под валюацията $\mathbf{t}$. Тогава, по правилата на конюнкцията, клаузата λ_i има стойност 0 под валюацията $\mathbf{t}$. Тогава, по правилата на дизюнкцията, цялата формула ϕ има стойност 0 под валюацията $\mathbf{t}$.
- Разглеждаме произволен $\mathbf{a} \in \{0,1\}^n$, такъв че $f(\mathbf{a}) = 1$. Тоест, $\mathbf{a}$ е един от векторите $\mathbf{b}_1$, $\mathbf{b}_2$, …, $\mathbf{b}_k$. Мислим за $\mathbf{a}$ като за валюация $\mathbf{t}$ на променливите x_1, x_2, …, x_n. За поне едно $i \in \{1, \ldots, k\}$ е вярно, че всеки литерал в клаузата λ_i има стойност 1 под валюацията $\mathbf{t}$. Тогава, по правилата на конюнкцията, клаузата λ_i има стойност 1 под валюацията $\mathbf{t}$. Тогава, по правилата на дизюнкцията, цялата формула ϕ има стойност 1 под валюацията $\mathbf{t}$.

Заключаваме, че f е семантиката на ϕ.

Остава да разгледаме случая, в който $f = 0$. Следната формула

$$x_1 \overline{x_1}$$

реализира функция константа нула. Тази формула не е ДНФ съгласно формалните правила, защото не е конюнктивна клауза, съдържайки два литерала на една и съща променлива. Но е очевидно, че реализира константа нула и че е формула над множеството от булеви функции конюнкция и отрицание. И това е краят на доказателството на теоремата на Boole. □

Ето пример за прилагането на конструкцията на СъвДНФ от теоремата на Boole. Нека $f(x_1, x_2, x_3)$ е отново тази функция:

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

Функцията има стойност 1 върху точно пет вектора. На тези вектори съответстват следните клаузи:

- На вектора 001 съответства $\overline{x_1}\,\overline{x_2}\,x_3$.
- На вектора 010 съответства $\overline{x_1}\,x_2\,\overline{x_3}$.
- На вектора 100 съответства $x_1\,\overline{x_2}\,\overline{x_3}$.
- На вектора 101 съответства $x_1\,\overline{x_2}\,x_3$.
- На вектора 111 съответства $x_1\,x_2\,x_3$.

Конструкцията построява тази СъвДНФ:

$$\overline{x_1}\,\overline{x_2}\,x_3 \vee \overline{x_1}\,x_2\,\overline{x_3} \vee x_1\,\overline{x_2}\,\overline{x_3} \vee x_1\,\overline{x_2}\,x_3 \vee x_1\,x_2\,x_3$$

Нека читателят се убеди сам(а), че семантиката на тази формула е точно f.

И едно предупреждение. Конструкцията на съответна формула-СъвДНФ може да е **много** неефикасна. В току-що разгледания пример може да опростим така:

$$\begin{aligned}
&\overline{x_1}\,\overline{x_2}\,x_3 \vee \overline{x_1}\,x_2\,\overline{x_3} \vee x_1\,\overline{x_2}\,\overline{x_3} \vee x_1\,\overline{x_2}\,x_3 \vee x_1\,x_2\,x_3 = \\
&\overline{x_2}\,x_3\,(\overline{x_1} \vee x_1) \vee \overline{x_1}\,x_2\,\overline{x_3} \vee x_1\,\overline{x_2}\,\overline{x_3} \vee x_1\,x_2\,x_3 = \\
&\overline{x_2}\,x_3 \vee \overline{x_1}\,x_2\,\overline{x_3} \vee x_1\,\overline{x_2}\,\overline{x_3} \vee x_1\,x_2\,x_3
\end{aligned}$$

В екстремния пример, в който $f = 1$, конструкцията генерира СъвДНФ с $n2^n$ литерала; а именно, всички пълни конюнктивни клаузи, конкатенирани чрез "$\vee$". А константа единица може да се получи от формулата $x_1 \vee \overline{x_1}$.

Задачата за генериране на формула с минимална дължина, съответна на дадена функция, в общия случай е практически нерешима. Но въпреки това конструкцията на СъвДНФ е полезна – тя е средство, което ни позволява да конструираме механизъм (СъфДНФ), който реализира някакво поведение (функцията). Известни са алгоритми, чрез които можем значително да намалим дължината на формулата, запазвайки семантиката; въпреки че в общия случай е практически невъзможно да генерираме еквивалентна формула с гарантирано минимална дължина, в много случаи е възможно да съкратим формулата драстично.

1.3 Дуална конструкция чрез СъвКНФ

Всяка булева функция, която е различна от константа единица, има (уникална) СъвКНФ. Тази СъвКНФ се конструира по правила, които са дуални на правилата за конструиране на СъвДНФ в доказателството на Теорема 1. Правилата са тези: разглеждаме само векторите, върху които функцията има стойност 0, за всеки такъв вектор $\mathbf{b}_i$ добавяме точно една пълна дизюнктивна клауза λ_i:

- ако $b_{i,j} = 0$, то променливата x_j участва в λ_i с положителния си литерал x_i.
- ако $b_{i,j} = 1$, то променливата x_j участва в λ_i с отрицателния си литерал $\overline{x_i}$.

Тогава $\phi = (\lambda_1)(\lambda_2)\cdots(\lambda_k)$.

Като пример, нека пак $f(x_1, x_2, x_3)$ е тази функция:

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

Съответната СъвКНФ е $(x_1 \vee x_2 \vee x_3)(x_1 \vee \overline{x_2} \vee \overline{x_3})(\overline{x_1} \vee \overline{x_2} \vee x_3)$.

1.4 Доказателство за пълнота чрез редукция от известно пълно множество

Нека са дадени множества от булеви функции F и G. Нека е известно, че F е пълно. Използвайки този факт, можем да **опитаме** да докажем, че G е пълно, изразявайки всяка от функциите на F чрез подходящи композиции и/или унификации на променливи на функции от G.

Забележете това "да опитаме"! Ако опитът е неуспешен, неуспехът може да се дължи на

- това, че G всъщност не е пълно множество,
- това, че не сме се сетили как да конструираме композициите и/или унификациите, въпреки че G е пълно.

Този вид доказателства много приличат на доказателствата за еквивалентност на съставни съждения p и q чрез еквивалентни преобразувания: ако прозрем как да го направим, успяваме, в противен случай дори не сме сигурни дали всъщност p и q са не-еквивалентни, или са еквивалентни, но ние не сме се сетили за правилна редица от преобразувания.

Ерго, и в двата метода за доказване има асиметрия между успеха на доказателството (твърдението е доказано и толкова) и неуспеха на доказателството (може твърдението да не е вярно, но може да е вярно, а да не сме се сетили как да го докажем). Иначе казано, тези методи не стават за опровергаване.

Теорема 2. *Нека* $\mathsf{F}, \mathsf{G} \subseteq \mathcal{F}$. *Нека* F *е пълно. Нека* $\forall \mathsf{f} \in \mathsf{F} : \mathsf{f} \in [\mathsf{G}]$. *Тогава* G *е пълно.*

Доказателство: Иска се да покажем, че $[\mathsf{G}] = \mathcal{F}$. Това, че $[\mathsf{G}] \subseteq \mathcal{F}$, е очевидно, защото всеки елемент на $[\mathsf{G}]$ е булева функция. Остава да покажем, че $\mathcal{F} \subseteq [\mathsf{G}]$.

Ще покажем, че $\forall \mathsf{h} \in \mathcal{F} : \mathsf{h} \in [\mathsf{G}]$. Нека h е произволна булева функция. По условие, F е пълно множество, така че $\mathsf{h} \in [\mathsf{F}]$. Това означава, че h се получава като композиция на функции от F и може би унификации на променливи. По условие, всяка функция от F се получава като композиция на функции от G и може би унификации на променливи. Тогава очевидно h се получава като композиция на функции от G и може би унификации на променливи. □

В следните примери ще стане ясно защо наричаме този начин за доказателство “редукция”. Да мислим за функционални елементи. Това, че F е пълно, означава, че ако са ни дадени неограничено много функционални елементи за всяка от функциите на F, то за всяка $\mathsf{h} \in \mathcal{F}$ можем да построим каскада C_h от такива функционални елементи, плюс евентуално даване “на късо” на входове, която реализира h. Редукцията е тази: всъщност са ни дадени функционални елементи, реализиращи функциите на G, а не тези на F. За всяка $\mathsf{f} \in \mathsf{F}$:

- първо построяваме каскада C_f от функционални елементи, които са за G, **а не** за F, такава че C_f реализира f,
- и после в C_h, за всеки тип функционален елемент, реализиращ f, заместваме този елемент с C_f.

Да кажем, че така модифицираната схема от функционални елементи се нарича C'_h. Бихейвиорално, C_h и C'_h са неразличими, тоест, те реализират една и съща булева функция. Но C_h и C'_h са конструктивно различни, понеже елементите на C'_h са тези за G, а не тези за F. По отношение на C'_h, функционалните елементи за F са някакви абстракции – ние можем да си мислим за тях, но всеки от тях **всъщност** е съвкупност от елементи за G, свързани по подходящ начин. По отношение на C'_h, ниското ниво, което е истината, се състои изцяло от елементи за G.

Посоката на редукцията е от F към G, понеже елементите на F се реализират (на ниско ниво) чрез елементите на G.

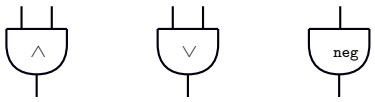
Факт 1. *Множеството от булеви функции* $\{\wedge, \mathtt{neg}\}$ *е пълно.*

Доказателство: Ще използваме Теорема 1 и Теорема 2. От Теорема 1 знаем, че множеството $\mathsf{F} = \{\wedge, \vee, \mathtt{neg}\}$ е пълно. От Теорема 2 знаем, че ако представим всяка от функциите на F чрез функциите на G, имаме доказателство за пълнотата на G. Но $\mathsf{F} \setminus \mathsf{G} = \{\vee\}$, така че

единствено за дизюнкцията трябва да покажем, че тя може да се "получи" от конюнкция и отрицание. Наистина,

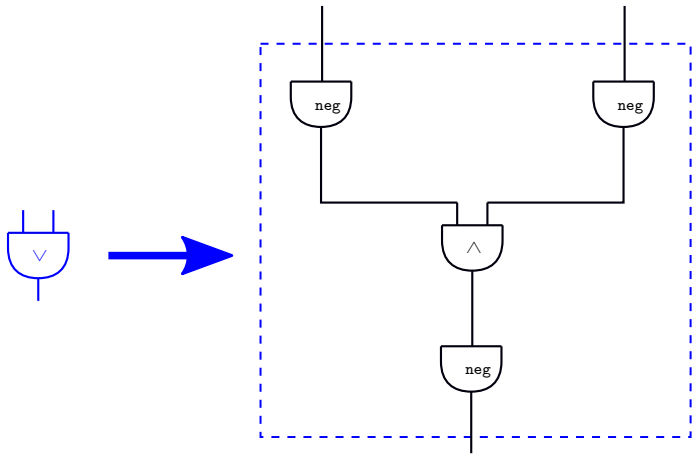
$$\begin{aligned} & x \vee y = && // \text{ двойно отрицание} \\ & \overline{\overline{x \vee y}} = && // \text{ De Morgan} \\ & \overline{\overline{x} \wedge \overline{y}} \end{aligned}$$

Ето практически същото доказателство, но изразено чрез функционални елементи. Елементите за известното пълно множество $\mathsf{F} = \{\wedge, \vee, \mathtt{neg}\}$ са тези:



Елементите за новото множество G, за което искаме да докажем, че е пълно, са тези:

Нека f е произволна булева функция, без значение на колко аргументи. Тя може да се реализира с подходящо свързани в каскада елементи от първия вид. Трябва да покажем, че тя може да се реализира с подходящо свързани в каскада елементи от втория вид. Но първият и вторият вид елементи имат общи елементи. Нещо повече, всеки елемент от вторият вид е и елемент от първия вид, понеже $\mathsf{G} \subset \mathsf{F}$ (това е особеност на настоящата задача, по принцип не е така!). Тогава, за единственият елемент от първия вид, който не е от втория вид, а именно елементът тип дизюнкция, трябва да покажем как да го реализираме чрез другите два вида елементи. Ето как:



Това е краят на доказателството. □

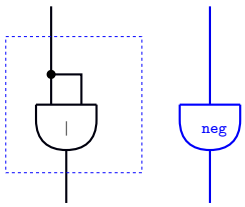
Факт 2. *Множеството от булеви функции* $\{|\}$ *е пълно.*

Доказателство: Ще използваме Теорема 2 и Факт 1: ще изразим и конюкцията, и отрицанието чрез чертата на Sheffer. Наистина,

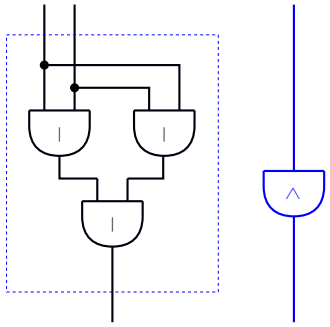
$$\overline{x} = x \mid x \tag{1}$$

$$x \wedge y = \overline{x \mid y} = (x \mid y) \mid (x \mid y) \tag{2}$$

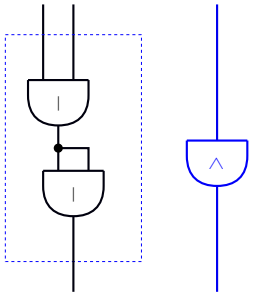
(1), изразено чрез функционален елемент тип черта на Sheffer, изглежда така:



(2), изразено чрез функционален елемент тип черта на Sheffer, изглежда така:



Конюнкция може да се получи чрез функционален елемент тип черта на Sheffer и с по-проста схема:



Забележете, че формулата (2) не може да бъде опростена (съкратена) по аналогичен начин, защото формулите не предоставят механизъм за "пренасяне чрез жица" на вече построена функция, какъвто механизъм е напълно естествен за схемите. Това е илюстрация на факта, че схемите може да са доста по-компактни от съответните формули заради възможността за пренос чрез жица на нещо вече построено (*reusability*). □

Факт 3. *Множеството от булеви функции* $\{xy \oplus z, \overline{x \oplus y} \oplus z\}$ *е пълно.*

Доказателство: Ще използваме Теорема 2 и Факт 1: ще изразим и конюкцията, и отрицанието чрез тези две функции. И двете функции са на три променливи, и двете функции не са симетрични.

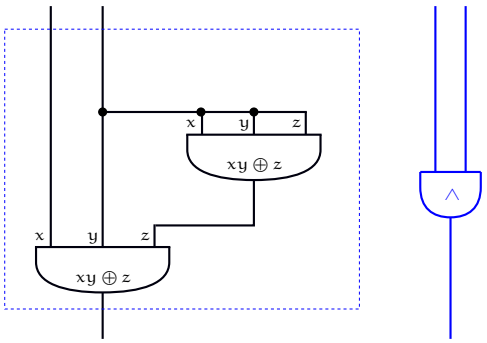
Първо забелязваме, че $xx \oplus x = x \oplus x = 0$. След това забелязваме, че $xy \oplus 0 = xy$. Вече имаме конюнкция.

Да си "направим" отрицание. В сила е $\overline{x \oplus x} \oplus x = \overline{0} \oplus x = 1 \oplus x = \overline{x}$. Имаме и отрицание.

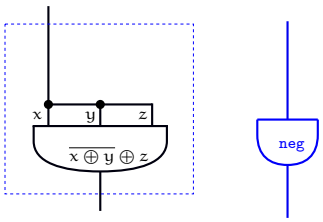
Ето как изглежда това доказателство, написано чрез функционални елементи. Дадени са ни два типа функционални елементи:

Входовете са надписани, понеже съответните функции не са симетрични (така че има значение кое "входно краче" на коя променлива съответства).

Ето как конструираме конюнкция:



Ето как конструираме отрицание:



Факт 4. *Множеството от булеви функции $\{\wedge, \vee\}$ не е пълно.*

Доказателство: Тук се иска да докажем, че множество от булеви функции **не е** пълно. С други думи, да опровергаем пълнота. Не можем да използваме Теорема 2 – с нея можем да докажем пълнота, но не можем да опровергаем пълнота.

Разсъждаваме така. Да допуснем, че $\{\wedge, \vee\}$ е пълно множество. Тогава всяка булева функция може да бъде реализирана като каскада от такива функционални елементи:

Очевидно е, че ако на произволна каскада от такива елементи подадем само нули на входовете, на изхода ще излезе нула. Това следва директно от дефинициите на конюнкция и дизюнкция. Твърдението може да бъде доказано строго със структурна индукция, ако имаме прецизна индуктивна дефиниция на "схема от функционални елементи", но ние засега нямаме такава[†]. За целите на това доказателство го приемаме за очевидно.

Ключовото наблюдение е, че има булеви функции, които имат стойност 1, когато всички аргументи имат стойност 0. Иначе казано, има булеви функции, чието канонично представяне започва с 1[‡]. Веднага забелязваме, че такава булева функция не може да се реализира чрез каскада от елементи тип конюнкция/дизюнкция, защо, ако подадем на всички входове 0, на изхода ще излезе 0.

Дуално, това доказателство може да се направи, подавайки 1 на всички входове, при което на изхода излиза 1, така че не може да се реализира функция, чието канонично представяне завършва на 0. □

2 Полиноми на Жегалкин

2.1 Въведение

Започваме с наблюдението, че множеството от булеви функции $\{0, 1, \wedge, \oplus\}$ е пълно. Това се доказва елементарно чрез Теорема 2 и Факт 1: тъй като $\{0, 1, \wedge, \oplus\}$ съдържа конюнция, достатъчно е да изразим отрицанието чрез фунции от $\{0, 1, \wedge, \oplus\}$. Но отрицанието е сумиране по модул две с единица: $\overline{x} = 1 \oplus x$. Това е и краят на доказателството.

Забелязваме, че 0 е "излишна" по отношение на пълнотата, понеже само $\{1, \wedge, \oplus\}$ е пълно множество. Но държим константа–нула да бъде сред функциите на множеството, защото ще ни трябва за изложението.

Щом $\{0, 1, \wedge, \oplus\}$ е пълно множество, всяка булева функция има формула над него. Формулите, които ще конструираме и ще имаме предвид в тази подсекция, не се изграждат по индуктивната дефиниция на "формули над множество от булеви функции" от предишната лекция. Както вече отбелязахме, онези формули са практически нечетими от хора.

2.2 Първа дефиниция

Започваме с индуктивна дефиниция на "формула над $\{0, 1, \wedge, \oplus\}$", която строи лесни за четене формули. За краткост, ще пишем само "формула". Нека са фиксирани краен брой булеви променливи x_1, x_2, …, x_n. Както при ДНФ и КНФ, и тук въвеждаме понятието "литерал" като буква–име на променлива. И тук различаваме променливата x_i от литерала x_i, въпреки че пишем едно и също. За разлика от ДНФ/КНФ, сега отрицателни литерали **няма**. В контекста на полиномите, използването на $\overline{x_i}$ е **забранено**: такива букви няма!

Определение 3. *Азбуката е* $\Sigma = \{0, 1, x_1, \ldots, x_n, \oplus, (,)\}$.

- *База: всяка буква от* $\{0, 1, x_1, \ldots, x_n\}$ *е формула.*
- *Индуктивна стъпка: нека* $k \geqslant 1$ *и* $t_1, t_2, \ldots, t_k \geqslant 1$. *Нека*

$$\phi_{1,1}, \phi_{1,2}, \ldots, \phi_{1,t_1},\ \phi_{2,1}, \phi_{2,2}, \ldots, \phi_{2,t_2},\ \ \ldots,\ \phi_{k,1}, \phi_{k,2}, \ldots, \phi_{k,t_k}$$

[†]Използваме формално недефинираното, но интуитивно ясно понятие "каскада".

[‡]Забележете, че **половината** булеви функции на n аргумента имат това свойство.

са формули. Тогава

$$(\phi_{1,1}\phi_{1,2}\cdots\phi_{1,t_1} \oplus \phi_{2,1}\phi_{2,2}\cdots\phi_{2,t_2} \oplus \cdots \oplus \phi_{k,1}\phi_{k,2}\cdots\phi_{k,t_k})$$

е формула.

В рамките на тази лекция, когато кажем "формула", имаме предвид формула, конструирана по Дефиниция 3.

Формулите (може да) имат доста чифтове скоби, които изглеждат излишни, но така синтаксисът се дефинира по-просто.

Няма да дефинираме прецизно семантиката на формула. Това трябва да е очевидно, имайки предвид, че семантиката на конкатенация на формули без "$\oplus$" между тях е функцията обобщената конюнкция от функциите–семантики на тези формули. Максималните по включване подстрингове над $\{0, 1, x_1, \ldots, x_n\}$ във формула ще наричаме *произведенията*, което е напълно смислено предвид факта, че конюнкцията е абстрактното умножение.

Въвеждаме съвсем неформално понятието "опростяване на формула". Опростяването на дадена формула е редица от еквивалентни преобразувания, чред която достигаме до формула, която не може да бъде опростена повече. Опростяването, което имаме предвид, е напълно аналогично на опростяването на алгебрични изрази с променливи, константи, скоби, събиране и умножение от училищната математика. В случая събирането е по модул две, а конюнкцията е абстрактното умножение. По отношение на произведенията:

- Ако произведение съдържа поне една буква 0, цялото се заменя с 0.
- В противен случай всички появи на 1 се елиминират, освен ако произведението не се състои само от единици, в който случай се заменя с 1.
- След което многократните появи на един и същи литерал се заменят с една единствена (конюнкцията е идемпотентна), а за прегледност и еднозначност литералите се сортират по индекси. *Степента* на така получено произведение е броят на неговите литерали. Забележете, че произведенията 0 и 1 са от степен нула, понеже 0 и 1 не са литерали.
- Ако има чифтове скоби, ограждащи произведението, те се изтриват.

По отношение на сума от така опростени произведения, ако има еднакви събираеми, те по двойки се заменят с 0 (защото $A \oplus A = 0$), и после всички събираеми 0 се елиминират, освен ако цялата сума не е само от нули, в който случай сумата се заменя с нула. За прегледност и еднозначност, произведенията се сортират по степени, а произведенията от една и съща степен се сортират лексикографски.

Ако има чифтове скоби, ограждащи това, което е останало от сумата, те се елиминират или отварят съгласно асоциативността на сума по модул две или дистрибутивността на конюнкцията спрямо сума по модул две или премахването на всички без един вложени чифтове скоби.

Действаме по този начин, докато повече опростявания не са възможни.

Определение 4. *След извършването на всички възможни гореописани опростявания, ако има чифт скоби, ограждащи получения стринг, те се премахват. Стрингът, който остава, се нарича* полином на Жегалкин.

Степента на полинома е максималната степен на негово произведение. Полиномът е сума (по модул две, естествено) от произведения, точно както очакваме от един полином. Тъй като в произведенията няма повтаряне на букви и сортираме буквите на всяко произведение, а също така в сумата няма повтаряне на събираеми и произведенията на сумата са сортирани, полиномът като синтактичен обект е еднозначно определен от формулата, с която започнахме опростяването. Ерго, за всяка формула ϕ имаме право да говорим за *полином**а**, съответен на* ϕ. Забележете, че събираемо 0 има в един единствен случай: когато цялата формула е 0.

Нека $n = 6$. Ето няколко примера за полиноми:

0 // степен 0
1 // степен 0
x_2 // степен 1
$x_1 \oplus x_1x_3x_4x_6$ // степен 4
$1 \oplus x_1 \oplus x_1x_3x_4x_6$ // степен 4
$1 \oplus x_1 \oplus x_1x_3x_4x_6 \oplus x_1x_2x_3x_4x_5x_6$ // степен 6

2.3 Втора дефиниция

Да разгледаме полиномите по друг начин: чрез *общия вид* и *коефициентите*. Нека n е броят на променливите. Всички възможни събираеми са 2^n: едно събираемо от степен 0, n събираеми от първа степен, $\frac{n(n-1)}{2}$ събираеми от втора степен, и така нататък, едно събираемо от n-та степен. Изобщо, има $\binom{n}{k}$ събираеми от k-та степен. Общият вид на полинома е съгласно Дефиниция 5.

Определение 5. *Нека* $x_1, \ldots, x_n$ *са булеви променливи. Полином на Жегалкин над* $x_1, \ldots, x_n$ *е всеки стринг от вида*

$$a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n \oplus a_{n+1}x_1x_2 \oplus a_{n+2}x_1x_3 \oplus \cdots \oplus a_{\frac{n(n+1)}{2}}x_{n-1}x_n \oplus$$
$$a_{\frac{n(n+1)}{2}+1}x_1x_2x_3 \oplus a_{\frac{n(n+1)}{2}+2}x_1x_2x_4 \oplus \cdots \oplus a_{2^n-1}x_1x_2\cdots x_n \tag{3}$$

където $a_0, a_1, \ldots, a_{2^n-1} \in \{0, 1\}$ *са коефициентите.*

Съгласно Дефиниция 5, полиномът се определя напълно от булевия вектор от коефициентите, който има дължина 2^n:

$$(a_0, a_1, \ldots, a_{2^n-1})$$

Тъй като всяко a_i, за $0 \leqslant i \leqslant 2^n - 1$, има стойност 0 или 1 независимо от другите, има 2^{2^n} такива вектори. Веднага следва, че има 2^{2^n} полинома на Жегалкин на n променливи.

Дефиниция 4 и Дефиниция 5 са същностно еквивалентни, но формално и на практика са много различни. При $n = 4$, полиномът $1 + x_1$ (по Дефиниция 4) се записва в общия си вид (по Дефиниция 5) ето така:

$$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

Представянето на полиномите чрез векторите от коефициентите е много полезно и смислено от абстрактна/теоретична гледна точка, но може да е много разхитително като памет за записване на полинома. По-точно казано, записването на даден полином съгласно Дефиниция 5 може да е експоненциално по-голямо от записването съгласно Дефиниция 4. Ерго,

ако n е от порядъка на няколкостотин, векторът от коефициентите не може да се побере в паметта на никое физическо изчислително устройство.

Видяхме, че за всяко n полиномите над n променливи са точно колкото са булевите функции на n променливи. Това не е случайно! Всяка булева функция си има свой съответен, точно един полином и всеки полином си има своя съответна, точно една булева функция, както предстои да докажем.

Определение 6. *Нека "* $ПЖ^n$ *" означава множеството от полиномите на Жегалкин над* n *променливи.*

Лема 1. *Нека* A *и* B *са произволни крайни непразни равномощни множества. За всяка инекция* $h : A \to B$ *е вярно, че* h *е биекция.*

Доказателство: По индукция по мощността на множествата. Базата е $|A| = |B| = 1$ и твърдението е очевидно вярно.

Нека за произволно $k \geqslant 1$, за всеки две A и B, такива че $|A| = |B| = k$, за всяка $h : A \to B$, ако h е инекция, то h е биекция. Това е индуктивното предположение.

Разглеждаме произволни A и B, такива че $|A| = |B| = k+1$, и произволна инекция $h : A \to B$. Фиксираме произволен елемент $a \in A$ и нека $b = h(a)$. Щом h е инекция, не съществува друг елемент на A, който се изобразява в b от h. От това следва, че релацията $h \setminus \{(a, b)\}$ всъщност е тотална функция от $A \setminus \{a\}$ в $B \setminus \{b\}$. Нещо повече, $h \setminus \{(a, b)\}$ е инекция, понеже премахването на a от A и на b от B не може да доведе до поява на елемент в $B \setminus \{b\}$, върху който се изобразяват повече от един елементи от $A \setminus \{a\}$.

Но $|A \setminus \{a\}| = |B \setminus \{b\}| = k$. Използвайки индуктивното предположение, заключаваме, че $h \setminus \{(a, b)\}$ е биекция. Но тогава h също е биекция, понеже е тотална функция, която е инекция по конструкция и сюрекция, понеже всеки елемент на B се явява образ на елемент на A по отношение на нея. □

Теорема 3. *За всяко естествено* n*, релацията* $M_n \subseteq \mathcal{F}^n \times ПЖ^n$*, дефинирана така*

$$\forall f \in \mathcal{F}^n \, \forall p \in ПЖ^n : (f, p) \in M_n \overset{деф}{\leftrightarrow} f \text{ е семантиката на } p$$

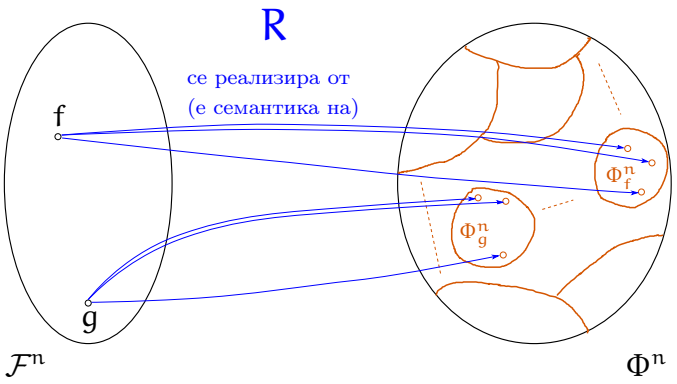
е функция, и то биекция.

Доказателство: На прост български, това, което се твърди, е следното. За всяка булева функция f има точно един полином на Жегалкин p, такъв че f е семантиката на p. За всеки полином на Жегалкин p съществува точно една булева функция f, такава че p реализира f.

Разглеждаме произволно естествено n. Разглеждаме произволна $f \in \mathcal{F}^n$. Щом $\{0, 1, \wedge, \oplus\}$ е пълно множество, f има поне една формула ϕ, изградена съгласно Дефиниция 3, такава че f е семантиката на ϕ, а ϕ реализира f. Нещо повече, f се реализира от безброй много формули, изградени съгласно Дефиниция 3, защото събирането с 0 във формулата не променя семантиката; ерго, щом ϕ реализира f, то $(\phi \oplus 0)$ също реализира f.

Нека Φ^n е (изброимо) безкрайното множество от формули над променливите $x_1, \ldots, x_n$ съгласно Дефиниция 3. За всяка $f \in \mathcal{F}^n$, нека Φ^n_f е (изброимо) безкрайното множество от всички формули, които реализират f. Две формули да реализират една и съща функция е релация на еквивалентност (над $\Phi^n \times \Phi^n$), така че всички Φ^n_f (по всички $f \in \mathcal{F}^n$) именуват нейните класове на еквивалентност, които са 2^{2^n} на брой.

Изображението от крайното множество $\mathcal{F}^n$ в безкрайното Φ^n, което изобразява булева функция във формула, която реализира тази булева функция, е релация. Да наречем тази реалация R (понеже формулите **р**еализират функциите). Визуално, нещата са така:



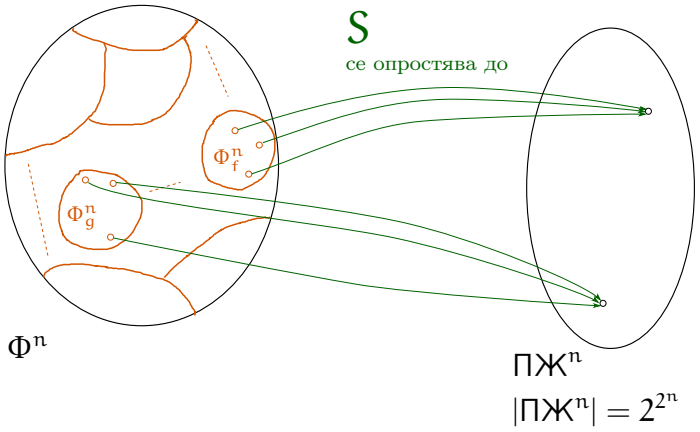
$|\mathcal{F}^n| = 2^{2^n}$

Φ^n е безкрайно, но има 2^{2^n} класове на екв. Класовете са безкрайни.

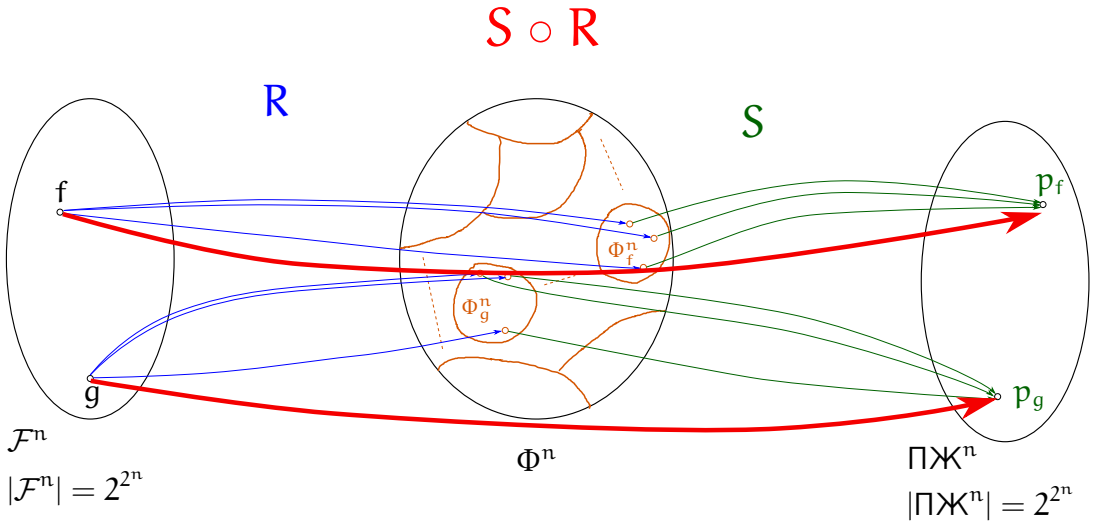
Очевидно е, че за всяка $f \in \mathcal{F}^n$ съществува един единствен израз–полином p, такъв че всяка формула от Φ_f се опростява до p по гореописаните правила за опростяване. Защо? Защото опростяванията са еквивалентни преобразувания, поради което f е семантиката на всяка от междинните формули в процеса на опростяването, а също така и на крайният израз, който е p. Въвеждаме функцията S (от **s**implifies to) $S : \Phi^n \to \text{ПЖ}^n$ така:

$$\forall \phi \in \Phi^n : S(\phi) = p$$

където p е полиномът, който се получава в резултат на опростяването на ϕ. S е такава, че за всяка $f \in \mathcal{F}^n$, всички $\phi \in \Phi^n_f$ се изобразяват върху един и същи полином. Визуално, нещата са така:



Ключовото наблюдение е, че $S \circ R$ е инекция – всеки две **различни** $f, g \in \mathcal{F}$ се изобразяват от $S \circ R$ в **различни** полиноми. S е функция, който изобразява всички формули от Φ^n_f в един полином p_f и всички формули от Φ^n_g в един полином p_g, но p_f и p_g са различни полиноми, понеже опростяването е серия от еквивалентни преобразувания. Визуално, нещата са така:



Знаем, че $|\mathcal{F}^n| = |$ПЖ$^n| = 2^{2^n}$. Щом $\mathcal{F}^n$ са равномощни ПЖ^n и $S \circ R$ е инекция, съгласно Лема 1, $S \circ R$ е биекция. □

Теорема 3 ни дава право да кажем, че p *е полином*$\boldsymbol{m}$*, съответен на* f, като под "съответен" имаме предвид този, който я реализира (иначе казано, на който тя е семантиката). Забележете, че цялото усилие по доказването на биективното съответствие между булеви функции и булеви полиноми е не за каква да е биекция, а именно за тази, която касае семантиката! Ако искахме просто да докажем, че съществува някаква биекция, няма значение каква, от функциите в полиномите, това щеше да следва директно от факта, че $|\mathcal{F}^n| = |$ПЖ$^n|$ и комбинаторния принцип на биекцията[†].

2.4 Конструиране на полиноми на Жегалкин

Дадена е някаква булева функция $f \in \mathcal{F}^n$. Искаме да конструираме нейния полином. Ще разгледаме три начина за това. И за трите начина ще разгледаме пример, като за примерна функция ще ползваме импликацията $x_1 \to x_2$.

2.4.1 Чрез СъвДНФ

Да си припомним каноничния вид на импликацията $x_1 \to x_2$.

x_1	x_2	f
0	0	1
0	1	1
1	0	0
1	1	1

СъвДНФ е $\overline{x_1}\,\overline{x_2} \vee \overline{x_1}x_2 \vee x_1x_2$. Заместваме всеки отрицателен литерал $\overline{x_i}$ с еквивалентния израз $1 \oplus x_i$. Получаваме еквивалентната формула $(1 \oplus x_1)(1 \oplus x_2) \vee (1 \oplus x_1)x_2 \vee x_1x_2$.

Очевидно имаме право да сторим това, понеже ползваме еквивалентно преобразуване. Следващата стъпка може да не е толкова очевидна: заменяме всяка буква "$\vee$" с "$\oplus$". Това вече **не е** еквивалентно преобразуване! Дизюнкцията е различна от сумата по модул две, така че по принцип не може да правим тази замяна и да очакваме да получим еквивалентна формула.

[†]От комбинаториката знаем и броя на всички тези биекции. Той е $(2^{2^n})!$.

Ключовото наблюдение е, че формулата, върху която прилагаме тази замяна, не е каква да е, а е получена от СъвДНФ. Да разгледаме дизюнкцията и сумата по модул две една до друга, с имена на променливите s и t, за да не ги бъркаме с x_1 и x_2.

s	t	$s \vee t$	$s \oplus t$
0	0	0	0
0	1	1	1
1	0	1	1
1	1	1	0

Дизюнкцията и сумата по модул две съвпадат, когато най-много един участник[†] е единица. СъвДНФ е конструирана така, че за всяка валюация на своите литерали, най-много една клауза е единица. Ерго, върху СъвДНФ, замяната на "$\vee$" с "$\oplus$" е еквивалентно преобразуване.

И така, в нашия пример получаваме $(1 \oplus x_1)(1 \oplus x_2) \oplus (1 \oplus x_1)x_2 \oplus x_1x_2$. Остава да отворим скобите и да опростим.

$$
\begin{aligned}
&(1 \oplus x_1)(1 \oplus x_2) \oplus (1 \oplus x_1)x_2 \oplus x_1x_2 = \\
&(11 \oplus 1x_2 \oplus x_1 1 \oplus x_1x_2) \oplus (1x_2 \oplus x_1x_2) \oplus x_1x_2 = \\
&(1 \oplus x_2 \oplus x_1 \oplus x_1x_2) \oplus (x_2 \oplus x_1x_2) \oplus x_1x_2 = \\
&1 \oplus x_2 \oplus x_1 \oplus x_1x_2 \oplus x_2 \oplus x_1x_2 \oplus x_1x_2 = \\
&1 \oplus x_1 \oplus x_1x_2 \oplus x_1x_2 \oplus x_1x_2 = \\
&1 \oplus x_1 \oplus x_1x_2
\end{aligned}
$$

Повече опростявания са невъзможни. Полиномът се оказва $1 \oplus x_1 \oplus x_1x_2$, написан съгласно Дефиниция 4.

Написан съгласно Дефиниция 5, той е (1101). Внимание! Това, че полиномът, написан в общ вид с коефициенти, съвпада с каноничния вид на функцията (импликацията също е 1101), е изключение. Просто за импликацията излиза така. В общия случай, тези два вектора са различни.

2.4.2 Чрез решаване на система от уравнения

Тук ползваме само общия вид на полинома с коефициентите. Щом променливите са x_1 и x_2, полиномът е $a_0 + a_1x_1 + a_2x_2 + a_3x_1x_2$. Нашата задача е да намерим a_0, a_1, a_2 и a_3.

Първо ще намерим коефициента пред свободния член a_0. Знаем, че $x_1 \to x_2$ е 1, ако $(x_1, x_2) = (0, 0)$. Тогава

$$
\begin{aligned}
&a_0 \oplus a_1 0 \oplus a_2 0 \oplus a_3 00 = 1 \ \leftrightarrow \\
&a_0 \oplus 0 \oplus 0 \oplus 0 = 1 \ \leftrightarrow \\
&a_0 = 1
\end{aligned}
$$

Излиза, че $a_0 = 1$.

[†]Пише "участник", понеже s и t може да не са просто булеви променливи, а произволни булеви функции. Щом са такива, всяка от тях има стойност или 0, или 1, за всяка валюация на своите променливи.

Сега ще намерим коефициентите пред произведенията от първа степен. Започваме с намирането на a_1. Знаем, че $x_1 \to x_2$ е 0, ако $(x_1, x_2) = (1, 0)$. Тогава

$$
\begin{aligned}
&a_0 \oplus a_1 1 \oplus a_2 0 \oplus a_3 10 = 0 \ \leftrightarrow \\
&a_0 \oplus a_1 \oplus 0 \oplus 0 = 0 \ \leftrightarrow \\
&a_0 \oplus a_1 = 0
\end{aligned}
$$

Но ние вече знаем, че $a_0 = 1$. Тогава имаме

$$1 \oplus a_1 = 0$$

За да решим това уравнение, добавяме единица към двете страни. По модул две, разбира се. Внимание! Би било груба грешка да приложим механично това, на което сме свикнали от елементарната математика, изваждайки единица от двете страни и заключавайки (погрешно), че $a_1 = -1$. В алгебрата, в която работим в момента, "-1" **няма**. Добавяйки единица, получаваме

$$
\begin{aligned}
&1 \oplus a_1 = 0 \ \leftrightarrow \\
&1 \oplus 1 \oplus a_1 = 1 \oplus 0 \ \leftrightarrow \\
&0 \oplus a_1 = 1 \ \leftrightarrow \\
&a_1 = 1
\end{aligned}
$$

Излиза, че $a_1 = 1$.

Да намерим a_2. Знаем, че $x_1 \to x_2$ е 1, ако $(x_1, x_2) = (0, 1)$. Тогава

$$
\begin{aligned}
&a_0 \oplus a_1 0 \oplus a_2 1 \oplus a_3 01 = 1 \ \leftrightarrow \\
&1 \oplus 0 \oplus a_2 \oplus 0 = 1 \ \leftrightarrow \\
&1 \oplus a_2 = 1 \ \leftrightarrow \\
&1 \oplus 1 \oplus a_2 = 1 \oplus 1 \ \leftrightarrow \\
&0 \oplus a_2 = 0 \ \leftrightarrow \\
&a_2 = 0
\end{aligned}
$$

Излиза, че $a_2 = 0$.

Да намерим a_3. Знаем, че $x_1 \to x_2$ е 1, ако $(x_1, x_2) = (1, 1)$. Тогава

$$
\begin{aligned}
&a_0 \oplus a_1 1 \oplus a_2 1 \oplus a_3 11 = 1 \ \leftrightarrow \\
&1 \oplus 11 \oplus 01 \oplus a_3 = 1 \ \leftrightarrow \\
&1 \oplus 1 \oplus 0 \oplus a_3 = 1 \ \leftrightarrow \\
&0 \oplus 0 \oplus a_3 = 1 \ \leftrightarrow \\
&a_3 = 1
\end{aligned}
$$

Излиза, че $a_3 = 1$.

И така, полиномът е (1101), точно както очаквахме.

2.4.3 Чрез еквивалентни преобразувания

Пак търсим полинома на импликацията $x \to y$. В сила е

$$x \to y = \overline{x} \vee y = \overline{\overline{\overline{x} \vee y}} = \overline{\overline{\overline{x}} \wedge \overline{y}} = \overline{x \wedge \overline{y}} = 1 \oplus x(1 \oplus y) = 1 \oplus x \oplus xy$$

Тогава полиномът е $1 \oplus x \oplus xy$, понеже тази формула **е** полином.

Намирането на полинома с еквивалентни преобразувания може да е много по-лесно в някои случаи. Да кажем, че сега търсим полинома на $f(x, y) = 0010$. Забелязваме, че това е отрицанието на импликацията, тоест, $f(x, y) = \overline{x \to y} = 1 \oplus (x \to y)$. Но вече знаем, че $x \to y = 1 \oplus x \oplus xy$. Тогава $f(x, y) = 1 \oplus 1 \oplus x \oplus xy = x \oplus xy$. Тогава полиномът е $x \oplus xy$, понеже тази формула **е** полином.

За да намерим полинома с еквивалентни преобразувания, трябва да се досетим за подходяща редица от еквивалентни преобразувания. Ерго, този метод е с досещане, а не е алгоритмичен като предните два.

2.5 Линейни булеви функции

Булева функция е *линейна*, ако нейният полином не съдържа произведения от степен, поголяма от едно. Иначе казано, линейна булева функция над променливите $x_1, \ldots, x_n$ е функция, чийто полином е от вида

$$a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n$$

където $a_0, a_1, \ldots, a_n \in \{0, 1\}$ са коефициентите. Казано по трети начин, коефициентите a_{n+1}, a_{n+2}, $\ldots$, a_{2^n-1} в (3) са нули.

Важно свойство на линейните булеви функции, е че множеството от тях е затворено: композиция от линейни функции е линейна функция. Наистина, нека f и g са линейни функции в най-общ вид:

$$f(x_1, x_2, \ldots, x_n) = a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n$$
$$g(y_1, y_2, \ldots, y_m) = b_0 \oplus b_1y_1 \oplus b_2y_2 \oplus \cdots \oplus b_my_m$$

Нека $i \in \{1, 2, \ldots, n\}$. Да разгледаме композицията на g на мястото на x_i в f:

$$f(x_1, x_2, \ldots, x_{i-1}, g(y_1, y_2, \ldots, y_m), x_{i+1}, \ldots, x_n) =$$
$$a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_{i-1}x_{i-1} \oplus a_i(b_0 \oplus b_1y_1 \oplus b_2y_2 \oplus \cdots \oplus b_my_m) \oplus a_{i+1}x_{i+1} \oplus \cdots \oplus a_nx_n$$
$$a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_{i-1}x_{i-1} \oplus a_ib_0 \oplus a_ib_1y_1 \oplus a_ib_2y_2 \oplus \cdots \oplus a_ib_my_m \oplus a_{i+1}x_{i+1} \oplus \cdots \oplus a_nx_n$$

Но това е полином над променливите x_1, x_2, $\ldots$, x_{i-1}, y_1, y_2, $\ldots$, y_m, x_{i+1}, $\ldots$, x_n, понеже a_ib_0, a_ib_1, $\ldots$, a_ib_n са булеви коефициенти. Незначителна техническа подробност е наредбата на произведенията.