Булеви функции

"There are 10 types of people - those who understand binary and those who don't" $_{
m HOHM}$ 2025

Преди задачите е представена малко теоретична основа за различни теми в булевата алгебра и булевите функции, а също са разгледани основни похвати за решаването на някои типове задачи. Забележка. Възможно е настоящето на места да се отклонява от строгата формалност за булеви функции.

1 Булеви функции

Дефиниция. Дефинираме множеството от булевите функции на n аргумента като $\mathfrak{F}_n := \{f \mid f : \{0,1\}^n \to \{0,1\}\}$ и множестовто от всички булеви функции $\mathfrak{F} := \bigcup_{n \in \mathbb{N}} \mathfrak{F}_n$.

Homauus. Макар съответствието с логическите съюзи да е голямо, има известни различия в записа/названията на някои функции:

- Вместо $x \wedge y$ понякога се ползва x & y, както и xy;
- $x \oplus y$ тук е cyма по модул 2, ползва и записът x+y
- \overline{x} е съответно отрицанието на x;
- $x \downarrow y$ (NOR), Стрелка на Пърс;
- $x \mid y$ (NAND), Черта на Шефър;

Свойство 1. Свойствата на булевите функции на един и два аргумента са аналогични на тези на логическите операции. Да обърнем обаче внимание на: $x \oplus y = \overline{x}y \lor x\overline{y}, \ x | y = \overline{x}\overline{y}, \ x \downarrow y = \overline{x} \lor \overline{y}.$

2 Нормални форми

2.1 ДHФ

Дефиниция (*литерал*). Литерал е синтактичен обект, име на променлива (потенциално с черта отгоре).

Дефиниция (*конюнктивна клауза*). Непразна формула, съставена от конкатенация на литерали така, че всяко име на променлива се появява не повече от веднъж (с или без черта).

Дефиниция (*пълна конюнктивна клауза*). Конюнктивна клауза, в която всяко име на променлива участва.

//TO DO

2.2 KH Φ

Трансформация на Цейтин*

2.3 Полином на Жегалкин (АНФ)

По-надолу ще покажем, че множеството от булевите функции $\{\land, \oplus, \mathbf{1}\}$ (което също записваме и като $\{., +, \mathbf{1}\}$) е пълно, т.е. всяка булева функция може да бъде "представена" чрез тези три. Именно такова представяне е и полиномът на Жегалкин (наричан още *алгебрична нормална форма*, $AH\Phi$). Всъщност всеки полином на Жегалкин на n променливи x_1, \cdots, x_n има общ вид

$$\bigoplus_{1 \le i_1 < \dots < i_k \le n} c_j x_{i_1} \dots x_{j_k} = c_1 x_1 \dots x_n + \dots + c_{2^n - 1} x_n + c_{2^n},$$

където коефициентите $c_j \in \{0,1\}$. Така например полиномите на Жегалкин на 3 променливи имат общ вид $c_1x_1x_2x_3+c_2x_1x_2+c_3x_1x_3+c_4x_2x_3+c_5x_1+c_6x_2+c_7x_3+c_8$. Забележете, че в мономите (конюнктивните клаузи на полинома) всяка променлива участва на степен *не повече от 1*, т.е. изрази като $x_1x_2^4x_3$ *не* са мономи от полином на Жегалкин. Причината е, че в контекста на булевото "умножение" (конюнкцията) полза от степени няма, понеже $x^m=x.x.\cdots x=x \land x \land \cdots x=x$. Така $x_1x_2^4x_3=x_1x_2x_3$. Ще разгледаме два възможни начина за получаване на такова представяне. С цел по-добро разбиране на материята, може би тук е добре да се отбележи, че $(\mathbb{Z}_2,+,.)=(\mathbb{Z}_2,\oplus,\wedge)$ е комутативен пръстен с единица, откъдето полиномите R[x] и изобщо $R[x_1,\cdots,x_n]$ са също комутативни пръстени с единица.

1 н.) Ползвайки СДНФ,

Алгоритъм:

- 1. Намираме СДНФ за дадената функция
- 2. Замяна: В СДНФ формулата заменяме:
 - всеки *отрицателен литерал* \overline{x} с x+1 (просто защото $\overline{x}=x\oplus 1$);
 - всеки символ \lor за дизюнкция с такъв за *сума по модул* 2, +;
- 3. Опростяване: В получения израз разкриваме скобите по познатия от алгебрата начин. В контекста на булевата алгебра $x^k := \underbrace{x.x.\cdots x}_k = \underbrace{x \wedge x \wedge \cdots x}_k = x$, тоест всякакви степени са излишни и могат да бъдат премахнати от крайния вид на полинома. Знаем също, че $x+x=x\oplus x=0$ с други думи еднаквите изрази се "унищожават" (било то и по-сложни като например xyz+xyz) и също могат да бъдат премахнати.

Пример: Търсим полиномът на Жегалкин за булевата формула $x\overline{y} \lor zy$. Ще използваме наготово, че СДН Φ за дадената е $f(x,y,z) = \overline{x}yz \lor x\overline{y}z \lor x\overline{y}z \lor xyz$.

Замяна: Преобразуваме $\overline{x}yz \lor x\overline{yz} \lor x\overline{y}z \lor xyz \Rightarrow (x+1)yz + x(y+1)(z+1) + x(y+1)z + xyz$

Опростяване:
$$(x+1)yz + x(y+1)(z+1) + x(y+1)z + xyz = xyz + yz + [x(y+1)(z+1) + x(y+1)z] + xyz = yz + [x(y+1)(z+1+z)] = yz + x(y+1)1 = yz + x(y+1) = yz + x(y+1)$$

Трикче: Понякога конюнктивните клаузи в СДНФ могат да станат значително много. Например ако функцията дава стойност 1 върху повечето входове. Тогава опростяването става досадно. В такъв случай би било по-лесно да се намери полином на Жегалкин за *противоположната функция* и полученото да се събере (в смисъл на \oplus) с 1 (от $x \oplus 1 = \overline{x}$).

Например разгледайте $f(x_1,x_2,x_3,x_4)=\overline{x_1x_2x_3x_4}.\overline{x_1}\overline{x_2}\overline{x_3}\overline{x_4}$, която дава 0 само при входове 0000 и 1111, а 1 във всички останали случаи. СДНФ за нея би имала 16-2=14 клаузи, дълго... Малко по-лесно е да намерим СДНФ за $\overline{f(x)}$, а именно $\overline{x_1}\overline{x_2}\overline{x_3}\overline{x_4}\vee x_1x_2x_3x_4$, което задава полином на Жегалкин $(x_1+1)(x_2+1)(x_3+1)(x_4+1)+x_1x_2x_3x_4$. Тогава $f(x)=(x_1+1)(x_2+1)(x_3+1)(x_4+1)+x_1x_2x_3x_4+1=\dots$

Друг вариант, спестяващ излишно удължаване в подобни случаи, е свеждането в СДНФ (или директно до полином на Жегалкин) да се намери не с таблица, а с еквивалентни преобразувания.

Коректност:

Възниква въпросът защо това работи. За намирането на СДНФ, опростяването и замяната на \overline{x} с (x+1) е ясно, че не променят семантиката на формулата, т.е. те са един вид еквивалентни преобразувания. Интересно е обаче защо втората замяна (на \vee с +) в СДНФ е коректна и дава еквивалентна

формула. В контекста на дадения пример, чудим се защо $\overline{x}yz \lor x\overline{y}z \lor x\overline{y}z \lor xyz = \overline{x}yz + x\overline{y}z + x\overline{y}z + xyz$ (с напомнянето, че + е \oplus). Това можем да изведем в следната теорема:

1: Коректност на алгоритъма за построяване на полинома на Жегалкин

Нека f е булева формула в СДНФ, а ϕ е формула, получена от f при замяна на символа "\" с "+". Тогава f и ϕ имат еднаква семантика.

Доказателство. Ясно е, че при тази конструкция семантиката на конюнктивните клаузи на двете формули е еднаква (защото те са и синтактично еднакви). Това показва, че ако някоя от конюнктивните клаузи на ϕ има стойност 1, то същата клауза ще има стойност 1 във f, откъдето f ще приеме стойност 1. Това автоматично отхвърля случай, в който за дадена валюация f има стойност 0, а ϕ стойност 1. Остава въпросът дали е възможно обратното - да съществува остойностяване на променливите на функциите, за което f има стойност 1, а ϕ съответно 0. Да допуснем, че такова има. Понеже f има стойност 1, то поне една от конюнктивните клаузи има (семантика, съответстваща на) стойност 1. Но ϕ има стойност 0, което означава, че има четен брой конюнктивни клаузи със семантика 1, т.е. поне 2. Не е трудно да се види, че последното е невъзможно. Причината е, че в СДН Φ клаузите са nълни и всеки две имат поне един различен литерал на една и съща променлива (едната клауза съдържа x, а другата - \overline{x}), тоест няма как едновременно да имат стойност 1. Противоречие. Значи за всяка валюация двете формули имат еднаква стойност, тоест тяхната семантика е еднаква, еквиваленти са.

 $\it Забележка.$ Ако конюнктивните клаузи на f не бяха пълни, тази еквивалентност нямаше да е в сила!

2 н.) Със заместване:

Както отбелязахме, полиномът на Жегалкин за n променливи има общ вид $\sum_{1 \leq i_1 < \dots < i_k \leq n} c_j x_{i_1} \cdots x_{i_k}$, където $c_j \in \{0,1\}$ и събирането е no модул 2 (т.е. \oplus). Можем да намерим коефициентите $c_j \in \{0,1\}$ с последователно разглеждане на функцията в различни точки. Така в случая на 3 променливи $f(000) = c_1000 + c_200 + c_300 + c_400 + c_50 + c_60 + c_70 + c_8 = c_8, f(001) = c_7 + c_8, f(010) = c_6 + c_8, f(100) = c_5 + c_8, f(011) = c_4 + c_6 + c_7 + c_8, \dots$, което ни дава лесно решима система, от която коефициентите могат да се намерят.

Забележска: Когато е възможно, все пак ще се придържаме към използване на първия метод за намиране на полином на Жегалкин.

Единственост: Възниква въпрос дали представянето на дадена функция в АНФ е единствено. Оказва се, че е.

2: Единственост на полинома на Жегалкин

Съществува единствен полином на Жегалкин с n променливи, който задава дадена функция.

 \mathcal{A} а напомним, че твърдението изключва от разглеждането полиноми, съдържащи мономи с повисоки степени като $x_1^4x_2 \ (=x_1x_2)$.

Комбинаторно доказателство. Вече знаем, че всяка функция $f:\{0,1\}^n \to \{0,1\}$ има (поне един) полином на Жегалкин, който ѝ съответства. Алгоритъмът, който показахме горе, намира един такъв. Същевременно две различни функции не могат да имат един и същи съответен полином на Жегалкин, защото това би означавало, че те са равни. Всичко това показва, че отношението функция-полином е "инективно" (кавичките се, защото формално не можем да говорим за инективност в контекста на релация, за която още не сме доказали, че е функция).

Полиномите на Жегалкин на n променливи имат общ вид $\sum_{1 \leq i_1 < ... < i_k \leq n} c_j x_{i_1} ... x_{i_k}$, като $c_j \in \{0,1\} \ \forall j \leq 2^n$. Различните мономи са 2^n на брой и всеки от тях може, както да участва, така и да не участва в полинома. Тогава има точно 2^{2^n} такива полинома, колкото са и функциите $f: \{0,1\}^n \to \{0,1\}$. Това означава, че "инектвиното" отношение в частност е и биективно, така на всяка функция съответства точно един полином. Казано по-просто - щом всяка функция си има поне един съответен полином, различните функции имат различни полиноми и броят полиноми е

равен на броя функции, то явно, че не може функция да има повече от един съответен полином.

(опит за) Алгебрично доказателство /по идея на Кристиян Гърчев/. Ще докажем исканото по индукция по броя променливи n. За да не става объркване, с $f(x) \equiv g(x)$ ще означаваме равенство в смисъл на еквивалентност (двата полинома са равни като функции - за един и същи вход, дават една и съща стойност), а с f(x) = g(x) ще означаваме равенство на полиноми (тоест коефициентите пред равните степени са равни). Да отбележим, че второто равенство влече първото (еквивалентността), ние обаче искаме да докажем обратното.

Да допуснем, че за дадена булева функция съществуват два полинома на Жегалкин $f(x_1,...,x_n)$, $g(x_1,...,x_n)$, които я реализират, т.е. $f \equiv g$. Ще докажем, че f = g.

База: Нека n=1, тогава $f(x)=c_0x+c_1$ и $g(x)=d_0x+d_1$, като $c_0,c_1,d_0,d_1\in\{0,1\}$. Понеже f(0)=g(0),f(1)=g(1), то $c_0=f(0)=g(0)=d_0,c_0+c_1=f(1)=g(1)=d_0+d_1\Rightarrow c_1=d_1$ и $f(x)=c_0x+c_1=d_0x+d_1=g(x)$. \checkmark

ИП: За всеки два полинома на Жегалкин $f_0(x_1,...,x_{n-1}), g_0(x_1,...,x_{n-1})$ на n-1 променливи, ако $f_0 \equiv g_0$, то $f_0 = g_0$.

ИС: Понеже f,g са полиноми на няколко променливи, можем да ги запишем като полиноми на коя да е тяхна променлива, в частност на x_n . Понеже f,g са и полиноми на Жегалкин, то последните ще са линейни. Така $f(x_1,...,x_n)=f_1(x_1,...,x_{n-1}).x_n+f_2(x_1,...,x_{n-1})$ и $g(x_1,...,x_n)=g_1(x_1,...,x_{n-1}).x_n+g_2(x_1,...,x_{n-1})$, където f_1,f_2,g_1,g_2 също са полиноми на Жегалкин, но на n-1 променливи. При заместване на $x_n=0$ получаваме $f_2(x_1,...,x_{n-1})=f_1(x_1,...,x_{n-1}).0+f_2(x_1,...,x_{n-1})=f(x_1,...,x_{n-1},0)\equiv g(x_1,...,x_{n-1},0)=g_1(x_1,...,x_{n-1}).0+g_2(x_1,...,x_{n-1})=g_2(x_1,...,x_{n-1})$, т.е $f_2\equiv g_2$, откъдето по ИП следва $f_2=g_2$.

Сега ако в $f_1.x_n+f_2=f\equiv g=g_1.x_n+g_2$ прибавим $f_2=g_2$ към двете страни, получаваме $f_1.x_n\equiv f_1.x_n+f_2+f_2=f+f_2\equiv g+g_2=g_1.x_n+g_2+g_2\equiv g_1.x_n$ (унищожават се, защото събирането е \oplus , а и изобщо в поле с 2 елемента събирането и изваждането са еквивалентни). При заместване на $x_n=1$ излиза $f_1\equiv g_2$, откъдето по ИП те са равни и като полиноми, $f_1=g_1$. Но тогава $f(x_1,...,x_n)=f_1.x_n+f_2=g_1.x_n+g_2=g(x_1,...,x_n)$, което и искаме.

За упражнение върху полином на Жегалкин разгледайте задачи 12, 13, 14.

2.4 Blake canonical form*

3 Пълнота на множества булеви функции

Дефиниция. (затваряне на множество от булеви функции) Затваряне на множество от булеви функции $F \subseteq \mathcal{F}$ наричаме най-малкото множество, което: съдържа F, съдържа всички проекции $\pi_n^i(x_1,\cdots,x_n)=x_i$ и е затворено относно суперпозиция, т.е. композиция и идентифициране (ползване на една и съща променлива на различни места).

Казано неформално, [F] е множеството от всички, функции, които могат да се построят от тези в F.

Дефиниция. (пълно множество булеви функции) Множество $F \subseteq \mathcal{F}$ е пълно, ако $[F] = \mathcal{F}$.

повече информация тук

3: Теорема на Boole

Множеството от трите булеви фунцкии негация, конюнкция, дизюнкция е пълно.

4: Условие за пълнота

Ако $G, F \subseteq \mathcal{F}$ (множеството от всички булеви функции). Тогава, ако F е пълно и $\forall f \in F$: $f \in [G]$, то и G е пълно.

В задачи понякога се налага да определим дали дадено множество от булеви функции G е пълно. Ако е, достатъчно е да покажем как чрез функциите от G могат да бъдат изразени функциите на някое пълно множество F (обикновено това е $\{\lor, \neg\}$ или $\{\land, \neg\}$). В този случай решението следва резултата от втората теорема (условието за пълнота).

Как обаче се доказва обратното - че множество G от булеви функции не е пълно? - Най-общият отговор на това е " $c\bar{c}c$ структурна индукция по построение на булевите формули", но това след малко. Тук ще покажем три подхода, които могат да се ползват за доказване на непълнота, а в sada 4 10 ще ги видим и приложени на практика.

Обща схема за доказване: Преди да се спрем върху конкретните подходи, да дадем някаква интуиция. Общата идея за доказателството е проста - показваме, че всички функции, които можем да получим като композиция на тези от G, се държат еднакво, т.е. изпълняват някакво свойство (предикат P), $\forall g \in [G]: P(g)$. Същевременно показваме, че съществува булева функция, която не изпълнява това свойство ($\exists f \in \mathcal{F}: \neg P(g)$). Е, тогава е ясно, че $[G] \neq \mathcal{F}$, значи G не е пълно. Обикновено предикатот P е принадлежност към някой клас функции - монотонни, линейни, запазващи 0/1, самодвойствени и ∂p .

1. Доказателство с остойностяване: Това е частен случай на горния подход. С него може да се докаже непълнота на функции, запазващи 1 (респективно 0), т.е. такива, за които $f(1,1,\cdots,1)=1$. Идеята е, че ако при фиксиране на някои входни стойности (т.е. подаване на конкретни константи като аргументи - обикновено само 1-ци/само 0-ли) всички функции от даденото множество се държат еднакво (връщат една и съща стойност), то множеството не е пълно. Това е така, защото не всички функции във \mathcal{F} дават еднаква стойност при конкретен вход. При този тип доказателство предикатът по-горе обикновено има горе-долу следния вид: P(g) := при вход само 1-ци g връща 1. $\Pi pumep$: нека $G = \{\land, \lor\}$, не е трудно да се види, че всички функции от [G] при вход $\overrightarrow{x} = (1, \cdots, 1)$ имат стойност 1. Ясно е обаче, че ne всички функции в \mathcal{F} изпълняват това, например едноаргументната функция neq: neq(1) = 0 го нарушава, така че $[G] \neq \mathcal{F}$. \checkmark

Ако искаме да сме по-педантични, частта с "не е трудно да се види, че всички ϕ -ии от [G]..." трябва да се докаже по индукция (структурна).

2. Показване, че отрицанието neg не е част от множеството: Тук ще опитаме да докажем отсъствието на някоя функция от [G] (в частност отрицанието) малко по-прецизно, по индукция. За целта ще разгледаме конкретен пример: искаме да докажем, че $G = \{\land, \lor\}$ не е пълно. Функцията neg е едноаргументна, така че можем да считаме, че съществува булева формула/израз e, в която участва само една променлива x и чиято семантика е именно neg(x). Ограничаваме се до азбуката $\Sigma = \{\lor, \land, x, (,)\}$. Ще правим структурна индукция по построение на булевите формули, така че е добре да имаме предвид тяхната индуктивната дефиниция. Нека E е множеството (езикът) от коректните булеви изрази, конструирани само с горните. Базата е $x \in E$. Ако $e_1, e_2 \in E$, то $(e_1 \lor e_2), (e_1 \land e_2) \in E$ (стъпка).

Тези формули/изрази обаче са само синтактични обекти, а нашата цел е да докажем, че тяхната семантика е различна от тази на neg(x). Следва същинското доказателство по индукция:

База: Булевият израз x има семантика стойността на променливата x.

ИП: Нека $e_1, e_2 \in E$ са два булеви израза, получени чрез суперпозиция (композиция) от променливата x и \vee , \wedge и имат семантика x.

ИС: Тогава изразите $(e_1 \lor e_2), (e_1 \land e_2)$ имат семантика съответно $x \lor x = x, x \land x = x$. Това показва, че всички едноаргументни функции от [G] имат семантика x, но не и \overline{x} , множеството не е пълно. \checkmark

3. Доказателство с монотонност:

Дефиниция. (монотонна функция) Булева функция $f:\{0,1\}^n \to \{0,1\}$ е монотонна, ако $\forall i \leq n \ \forall x_i, y_i \in \{0,1\}, x_i \leq y_i: f(x_1, \cdots, x_n) \leq f(y_1, \cdots, y_n)$, или по-просто $\forall x, y \in \{0,1\}^n, x \leq y: f(x) \leq f(y)$, като сравнението на булеви вектори е почленно.

Пример: Функциите \land, \lor са монотонни, а \neg, \to не са.

Важно за нас е следното свойство:

5: Лема

Композиция на монотонни функции е монотонна функция.

Доказателство. Нека $f:\{0,1\}^n \to \{0,1\}, g_i:\{0,1\}^m \to \{0,1\}$ за $i\leq n$ са монотонни функции. Разглеждаме композицията $h(x_1,\cdots x_m)=f(g_1(x_1,\cdots ,x_m),\cdots ,g_n(x_1,...,x_m)).$ Нека $x',x''\in\{0,1\}^m,x'\leq x''.$ От монотонността на $g_i:\forall i\leq n:g_i(x')\leq g_i(x''),$ откъдето пък $h(x')=f(g_1(x'),\cdots ,g_n(x'))\leq f(g_1(x''),\cdots ,g_n(x''))=h(x''),$ като вземем предвид и монотонността на f. Следва, че h(x) също е монотонна.

Забележска. Тук ползвахме общо приетата форма на композиция $h(x) := f(g_1(x), \dots, g_n(x)), x \in \{0,1\}^m$. Визуално това може да има различия с композирането в лекционните записки, но имат еднаква изразителна мощ (функциите, които генерират са еднакви).

Самата идея за подхода с монотонност не е сложна. - Показваме, че функциите от [G] са монотонни (например ползвайки свойството, че композицията запазва монотонност, като може това да се придружи с индукция). Не всички функции във $\mathcal F$ обаче са монотонни, както стана ясно от примера. Тогава G не е пълно. \checkmark

Още малко за пълнота: Горните подходи на пръв поглед разглеждат частни случаи и са "ad hoc". Донякъде да, но оказва се, че те са в основата на следващото необходимо и достатъчно условие за пълнота на множество функции. Преди това обаче една дефиниция.

Дефиниция (Post function classes). Следните 5 множества наричаме класове на Пост:

- множеството от функции, запазващи 0: $T_0 := \{ f \in \mathcal{F} | f(0, \dots, 0) = 0 \};$
- множеството от функции, запазващи 1: $T_1 := \{ f \in \mathcal{F} | f(1, \dots, 1) = 1 \};$
- множеството от монотонните функции: $M := \{ f \in \mathcal{F} | f \text{ е монотонна } \};$
- множеството от самодвойствените функции: $S := \{ f \in \mathcal{F} | f(\overline{x}) = \overline{f(x)}, x \in \{0,1\}^n \};$
- множеството от линейните функции: $L := \{ f \in \mathcal{F} | f \text{ е иразима само чрез} + (XOR)$ и константи $\}$, например x + y + z;

6: Post's Functional Completeness Theorem

Множество G не е пълно тстк е подмножество на поне един от петте класа T_0, T_1, M, S, L .

За упражнение върху (не)пълнота разгледайте задача 10.

Схеми от функционални елементи

Logic synthesis, SAT solvers*

Binary Decision Diagrams (BDD)*

Булеви производни*

Poretsky's law of forms*

Huffman coding*

Задачи

Задача 1. Еквивалентни ли са следните двойки булеви изрази:

- \bullet \overline{x} и x|x
- $A \wedge B$ и (A|B)|(A|B)
- A(B+C) и AB+AC
- A(A+B) и A+AB
- $\overline{x}(y \oplus z)$ и $\overline{x \vee ((y \to z)(z \to y))}$

Решение.

- $x|x = \overline{x} = \overline{x}$
- $(A|B)|(A|B) = \overline{AB} \mid \overline{AB} = \overline{\overline{AB} \wedge \overline{AB}} = AB \vee AB = AB = A \wedge B$
- $A(B+C) = A(B\overline{C} \vee C\overline{B}) = AB\overline{C} \vee AC\overline{B}$ и $AB+AC = AB.\overline{AC} \vee \overline{AB}.AC = AB(\overline{A} \vee C) \vee AC(\overline{A} \vee \overline{B}) = AB\overline{C} \vee AC\overline{B}$
- $A(A+B)=A(\overline{A}B\vee A\overline{B})=A\overline{A}B\vee AA\overline{B}=0\vee A\overline{B}=A\overline{B},$ също и $A+AB=\overline{A}AB\vee A\overline{AB}=A\overline{A}B=A(\overline{A}\vee \overline{B})=A\overline{B}$
- $\overline{x}(y \oplus z) = \overline{x}.\overline{y \leftrightarrow z} = \overline{x \lor (y \leftrightarrow z)} = \overline{x \lor ((y \to z) \land (z \to y))}$

Задача 2. Колко са всички тотални булеви функции над n променливи?

Решение. Тоталните булеви функции са от вида $f:\{1,0\}^n \to \{1,0\}$. Домейнът е 2^n -елементен, а кодомейнът е двуелементен, значи търсеният брой е 2^{2^n} (на всяка стойност от домейна могат да съпоставени две стойности).

Задача 3. Намерете |F|, ако:

- $F := \{ f \in \mathcal{F}^n | \forall \mathbf{x} \in \{0, 1\}^n : f(\mathbf{x}) = \overline{f(\overline{\mathbf{x}})} \}$
- $F := \{ f \in \mathcal{F}^n | \forall \mathbf{x} \in \{0, 1\}^n : f(\mathbf{x}) = f(\overline{\mathbf{x}}) \}$

Дефиниция (cиметрична функция). Функция на n променливи е симетрична тстк стойността ѝ е една и съща за всяка пермутация на променливите ѝ.

Задача 4. Да се намери броят на симетричните булеви функции на n променливи.

Решение. Да започнем с пример за онагледяване, нека f(x,y,x) е симетрична, тогава f(0,0,1)=f(0,1,0)=f(1,0,0). Аналогично f(0,1,1)=f(1,0,1)=f(1,1,0). Забелязваме, че необходимо и достатъчно условие, за да бъде дадена функция с n аргумента симетрична, е $\forall 0 \leq k \leq n$: за всеки вход с точно k единици, функцията да дава една и съща стойност. Имаме n+1 различни k-та, за всяко можем имаме свобода в определяне каква стойност да дава функцията при вход с точно k единици, "изборите" са независими, тоест общо 2^{n+1} .

Задача 5. Да се намери броят на булеви функции на $n \ge 2$ променливи, които запазват стойността си при размяна на променливите x_1 и x_2 .

Решение. Търсим броя булеви функции, за които $f(x_1,x_2,x_3\cdots,x_n)=f(x_2,x_1,x_3,\cdots,x_n)$. В частност това е еквивалентно на $f(1,1,x_3,\cdots)=f(1,1,x_3,\cdots)$ (винаги изпълнено), $f(0,1,x_3,\cdots)=f(1,0,x_3,\cdots)$, $f(0,0,x_3,\cdots)=f(0,0,x_3,\cdots)$ (също винаги изпълнено). Тоест се интересуваме единствено от функциите, за които $f(1,0,x_3,...,x_n)=f(0,1,x_3,...,x_n)$. За стойността на функцията върху останалите входове няма ограничения. Това означава, че стойностите $f(x), x \in \{0,1\}^n$ на функцията върху входове от вида $x=00x_3...x_n,01x_3...x_n$, $x_n=11x_3...x_n$ я определят еднозначно. Това са $x_n=11x_3...x_n$ в определят еднозначно.

Задача 6. Да се намери броят на булеви функции на n променливи, които приемат стойност 1 върху поне една двойка противоположни входни вектори.

Решение. Да отбележим, че всеки вектор има единствен противоположен, различен от самия него. Така броят двойки противоположни вектори е $\frac{2^n}{2} = 2^{n-1}$. По-лесно е да преброим колко функции не изпълняват исканото по условие. За да бъде то нарушено, трябва върху всяка двойка противоположни вектори функцията да дава поне една стойност 0 (тоест възможните резултати върху два противоположни вектора са 0 и 0,0 и 1,1 и 0 - 3 на брой). Така общият брой функции е $3^{2^{n-1}}$ (за всяка двойка вектори избираме един от три варианта). В крайна сметка търсените функции, изпълняващи условието, са $2^{2^n} - 3^{2^{n-1}}$. ■

Дефиниция. (фиктивна променлива) Променлива x_i е фиктивна за функция $f \in \mathcal{F}^n$, ако $\forall x_1, \cdots, x_{i-1}, x_{i+1}, \cdots, x_n \in \{0, 1\} : f(x_1, \cdots, x_{i-1}, 0, x_{i+1}, \cdots, x_n) = f(x_1, \cdots, x_{i-1}, 1, x_{i+1}, \cdots, x_n).$

Дефиниция. (*съществена променлива*) *Съществени* наричаме всички променливи, които не са фиктивни.

Задача 7. Да се намери броят на булеви функции на n променливи, които нямат фиктивни променливи.

Задача 8. Дадени са булевите функции f=1010, g=1100, да се намери каноничното представяне на функцията $h(x_5,x_3,x_1)=f(x_3,g(x_1,x_5))$

Решение. Можем да преименуваме променливите $y_1 = x_5, y_2 = x_3, y_3 = x_1 \Rightarrow h(y_1, y_2, y_3) = f(y_2, g(y_3, y_1))$. Така например откриваме h(0, 0, 1) = f(0, g(1, 0)) = f(0, 1) = 0, останалите стойности се намират аналогично.

Задача 9. Дадени са булевите функции f(x,y) = 1010, g(x,y) = 1101, да се намери каноничното представяне на функцията h(x,y) = f(g(x,y),g(y,x)).

Pешение. Можем директно да направим таблицата на h:

\boldsymbol{x}	y	g(x,y)	g(y,x)	f(g(x,y),g(y,x)) = h(x,y)
0	0	1	1	0
0	1	1	0	1
1	0	0	1	0
1	1	1	1	0

 $\Rightarrow h = 0100.$

Задача 10. (*) Докажете или опровергайте, че следните множества от булеви функции са пълни:

- $\{\land, neg\}$
- $\{\land, \oplus, \mathbf{1}\}$
- {↓}
- {|}
- $\{f,g\}$, ako f(x,y) = 0110, g(x,y) = 1101
- $\{\rightarrow, \mathbf{0}\}$
- ullet $\{ \rightarrow, 1 \}$
- $\{\land, \oplus\}$
- $\{\land,\lor\}$
- $\{\land,\lor,\to\}$

Решение. Ще използваме Теорема 3:

- Пълно е. Следва от факта, че $F = \{ \land, \lor, neg \}$ е пълно и всеки от трите му елемента може да бъде изразен посредством функциите в $G = \{ \land, neg \}$, по-конкретно $x \lor y = \overline{x} \land \overline{y}$.
- Отново е пълно, $x \oplus 1 = \overline{x}$, с което сведохме до горното множество, което е пълно. \blacksquare
- Пълно е: $x \downarrow x = \overline{x \lor x} = \overline{x}$, а също $x \lor y = \overline{x \downarrow y} = (x \downarrow y) \downarrow (x \downarrow y)$, с което изведохме функциите негация и дизюнкция, които са пълно множество.
- Пълно е: $x|x = \overline{x \wedge x} = \overline{x}$, а също $x \wedge y = \overline{x|y} = (x|y)|(x|y)$, с което изведохме функциите негация и конюнкция, които са пълно множество.
- Макар че можем да се справим и без това, тук наблюдение, че f е \oplus , а g е \rightarrow , би улеснило нещата. Ще докажем, че $\{\oplus, \rightarrow\}$ е пълно: $x \to x = 1 \Rightarrow \overline{x} = 1 \oplus x = (x \to x) \oplus x$, а $x \lor y = (x \to y) \to y$.
- Множеството е пълно: $x \to \mathbf{0} = \overline{x}, \ (x \to y) \to y = x \lor y,$ като така сведохме до пълното множество $\{\neg, \lor\}$.
- Оказва се, че $\{\to, \mathbf{1}\}$ не е пълно. Лесно се вижда, че произволна булева функция, построена само с помощта на горните има стойност 1 при вход 1-ци. С други думи, функциите от $[\{\to, \mathbf{1}\}]$ запазват 1, тоест това не са всички функции.
- Множеството $\{\land, \oplus\}$ не е пълно. Причината е, че $[\{\land, \oplus\}] \subseteq T_0$ (класа на Пост с функции, запазващи 0 /0-preserving functions/), тоест при вход само 0-ли, функциите от затварянето връщат винаги 0.
- Множеството $\{\land,\lor\}$ също не е пълно. Тук можем да ползваме, че функциите \land,\lor са монотонни, както са и всички техни производни, образувани при композиции. Следователно $[\{\land,\lor\}]\subseteq M$ съдържа само монотонни функции, но разбира се, не всички във $\mathcal F$ са такива.
- Ще докажем, че негацията не може да се представи само чрез горните. Подобно доказателство вече сме правили става чрез индукция по построение на булевите изрази. База: Променливата x има стойност x.

ИП: Разглеждаме булеви изрази e_1, e_2 , построени само с една променлива x и трите операции \land, \lor, \rightarrow , които имат семантика стойността на x или 1.

ИС: Разглеждаме произволен сложен булев израз, записан само чрез горните. Нека операцията с най-нисък приоритет е $op \in \{\land, \lor, \to\}$ (на върха на дървото на израз), тя е измежду трите операции по-горе, така че е двуместна. Тоест имаме нещо от сорта на e_1 op e_2 . По ИП e_1 и e_2 имат семантика стойността на x или **1**. Вижда се, че при прилагане на op стойността остава това остава в сила (на практика разглеждаме $x \lor x$, $x \lor 1$, $1 \lor 1$, $x \land x$, $x \land 1$, $1 \land 1$, $x \to x$, $x \to 1$, $x \to x$, $x \to$

Задача 11. Да се намери булева формула, ползваща само негация, конюнкция, дизюнцкия за следните:

- за f = 0000 (константа 0);
- за f = 1111 (константа 1);
- за f = 00110101;
- за f = 10010110;

Задача 12. Да се намерят СДНФ, СКНФ и полиномът на Жегалкин за следните булеви функции:

- $f(x, y, z) = x \lor y \to z$
- f = 11011101;
- $f(x, y, z) = (\overline{x} \lor z) \land (x \oplus y)$
- $f = x \oplus (\overline{y} \wedge x)$
- h(x,y) = f(g(x,y), g(y,x)), ako f(x,y) = 0110, g(x,y) = 1101

Решение. Ще направим таблицата единствено за първия пример.

• Таблицата изглежда така:

x	y	z	$x \vee y$	f(x,y,z)
0	0	0	0	1
0	0	1	0	1
0	1	0	1	0
0	1	1	1	1
1	0	0	1	0
1	0	1	1	1
1	1	0	1	0
1	1	1	1	1

От нея се вижда, че каноничната форма на функцията е f=11010101.

За намиране СДН Φ гледаме редовете, в които функцията има стойност 1 (затъмнените). СДН Φ е: $\overline{x}\,\overline{y}\,\overline{z} \lor \overline{x}\,\overline{y}\,z \lor \overline{x}yz \lor xyz \lor xyz$.

Тогава полиномът на Жегалкин (АНФ) за функцията ще е: (x+1)(y+1)(z+1)+(x+1)(y+1)z+(x+1)yz+x(y+1)z+xyz=1+x+y+xy+xz+yx+xyz.

СКНФ намираме отново от таблицата, този път гледайки немаркираните редове. СКНФ за функцията е: $(x \lor \overline{y} \lor z)(\overline{x} \lor y \lor z)(\overline{x} \lor \overline{y} \lor z)$.

• СДНФ: $\overline{x} \overline{y} \overline{z} \lor \overline{x} \overline{y}z \lor \overline{x}yz \lor x \overline{y} \overline{z} \lor x \overline{y}z \lor xyz$,

CKH Φ : $(x \vee \overline{y} \vee z)(\overline{x} \vee \overline{y} \vee z)$,

AHΦ: 1 + y + yz;

• f = 00110100,

СДНФ: $\overline{x}y\overline{z} \vee \overline{x}yz \vee x\overline{y}z$,

CKH Φ : $(x \lor y \lor z)(x \lor y \lor \overline{z})(\overline{x} \lor y \lor z)(\overline{x} \lor \overline{y} \lor z)(\overline{x} \lor \overline{y} \lor \overline{z}),$

AHΦ: y + xy + xz + xyz;

• СДНФ: xy,

CKH Φ : $(x \vee y)(x \vee \overline{y})(\overline{x} \vee y)$,

 $AH\Phi$: xy;

• h = 0110,

СДНФ: $\overline{x}y \vee x\overline{y}$,

CKH Φ : $(\overline{x} \vee y)(x \vee \overline{y})$,

AHΦ: x + y;

Задача 13 (*). Да се намери полиномът на Жегалкин за булевите функции:

• $f(x_1, x_2, x_3, x_4, x_5) = (x_2 \vee \overline{x}_3 \vee \overline{x}_4 \vee \overline{x}_5) \wedge (\overline{x}_1 \vee x_2 \vee x_3 \vee \overline{x}_4)$

```
• f(x) = ((x_1 \land x_2) \to x_3) \oplus ((x_4 \land x_5) \to x_6) \oplus ((x_7 \land x_8) \to x_9)
```

•
$$f(x) = ((x_1 \lor x_2) \to x_3) \oplus (x_4 \land (x_5 \lor x_6)) \oplus (x_7 \to x_8 \land x_9)$$

Решение. Целта на тази задача е да покаже някои примери, в които директно прилагане на алгоритъма би довело до дълги и сложни преобразувания.

- Намиране на СДНФ по познатия начин би изисквало попълване на таблица с 32 реда. Да направим някои наблюдения за дадената функция по-точно кога тя може да даде стойност 0. Достатъчно е една от клаузите да дава стойност 0. Така $x_2 \vee \overline{x}_3 \vee \overline{x}_4 \vee \overline{x}_5 = 0$ единствено върху входове 00111, 10111, а пък $\overline{x}_1 \vee x_2 \vee x_3 \vee \overline{x}_4 = 0$ за 10010, 10011. С оглед на това лесно можем да намерим СДНФ за противоположната функция: $\overline{f(x)} = \overline{x_1x_2}x_3x_4x_5 \vee x_1\overline{x_2}x_3x_4x_5 \vee x_1\overline{x_2}x_3x_4x_5$, в което има само 4 (а не 28 клаузи), което определя полинома $(1+x_2)x_3x_4x_5 + x_1(1+x_2)(1+x_3)x_4 = x_2x_3x_4x_5 + x_1x_2x_3x_4 + x_3x_4x_5 + x_1x_2x_4 + x_1x_3x_4 + x_1x_4$, откъдето $f(x) = \overline{f(x)} + 1 = x_2x_3x_4x_5 + x_1x_2x_3x_4 + x_3x_4x_5 + x_1x_2x_4 + x_1x_3x_4 + x_1x_4 + 1$.
- Ясно е, че директно използване на алгоритъма за намиране на полинома на Жегалкин изисква намиране на СДН Φ за функцията съответно и попълване на таблица с $2^9=512$ реда, отпада...

Можем обаче да се възползваме от факта, че между отделните клаузи в горната формула стои именно \oplus , което и целим като краен вид. Това позволява за всяка клауза независимо да бъде намерен съответен полином на Жегалкин и получените да бъдат директно заместени във формулата (тук се ползва асоциативността на \oplus).

Фокусираме се върху първата клауза, $(x_1 \wedge x_2) \to x_3$. Можем да съобразим, че тя дава стойност 1 при всички входове освен 110, така че намиране на полином Жегалкин за противоположната функция ще е лесно: $x_1x_2\overline{x_3} = x_1x_2x_3 + x_1x_2$, откъдето $(x_1 \wedge x_2) \to x_3 = x_1x_2x_3 + x_1x_2 + 1$. Аналогично това важи за останалите две клаузи от формулата, които са синтактично идентични на тази. Тогава $f(x) = (x_1x_2x_3 + x_1x_2 + 1) + (x_4x_5x_6 + x_4x_5 + 1) + (x_7x_8x_9 + x_7x_8 + 1) = x_1x_2x_3 + x_1x_2 + x_4x_5x_6 + x_4x_5 + x_7x_8x_9 + x_7x_8 + 1$.

Намирането на полинома за $\underline{(x_1 \wedge x_2)} \to x_3$ може да стане и с преобразувания: $(x_1 \wedge x_2) \to x_3 = \overline{x_1 \wedge x_2} \vee x_3 = \overline{x_1 x_2} \overline{x_3} = \overline{x_1 x_2} (x_3 + 1) = x_1 x_2 (x_3 + 1) + 1 = x_1 x_2 x_3 + x_1 x_2 + 1$. \checkmark

- Идеята отново е да намерим АНФ (полином на Жегалкин) за трите клаузи поотделно. За разнообразие тук ще използваме споменатите различни начини за постигане на това:
 - Полиномът на Жегалкин за $x_1 \vee x_2 \to x_3$ има общ вид $f(x_1, x_2, x_3) = c_1x_1x_2x_3 + c_2x_1x_2 + c_3x_1x_3 + c_4x_2x_3 + c_5x_1 + c_6x_2 + c_7x_3 + c_8$. Тогава $\underline{c_8} = g(000) = 0 \vee 0 \to 0 = \underline{1}, \ c_7 + c_8 = g(001) = 0 \vee 0 \to 1 = 1 \Rightarrow \underline{c_7} = \underline{0}, c_6 + c_8 = g(010) = 0 \vee 1 \to 0 = 0 \Rightarrow \underline{c_6} = \underline{1}, \ c_5 + c_8 = g(100) = 1 \vee 0 \to 0 = 0 \Rightarrow \underline{c_5} = \underline{1}, \ c_4 + c_6 + c_7 + c_8 = g(011) = 0 \vee 1 \to 1 = 1 \Rightarrow \underline{c_4} = \underline{1}, \ c_3 + c_5 + c_7 + c_8 = g(101) = 1 \vee 0 \to 1 = 1 \Rightarrow \underline{c_3} = \underline{1}, \ c_2 + c_5 + c_6 + c_8 = g(110) = 1 \vee 1 \to 0 = 0 \Rightarrow \underline{c_2} = \underline{1}, \ c_1 + c_2 + \dots + c_8 = g(111) = 1 \vee 1 \to 1 = 1 \Rightarrow \underline{c_1} = \underline{1}.$ Така полиномът е $x_1x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2 + 1$. \checkmark
 - Нека полинома на Жегалкин за втората клауза намерим с преобразувания: $x_4 \wedge (x_5 \vee x_6) = x_4 \cdot \overline{x_5} \cdot \overline{x_6} = x_4 \cdot ((x_5 + 1)(x_6 + 1) + 1) = x_4 \cdot (x_5 + x_6 + x_5 x_6) = x_4 \cdot x_5 + x_4 \cdot x_6 + x_4 \cdot x_5 \cdot x_6$. \checkmark
 - Полинома на Жегалкин за последната клауза $h(x_7, x_8, x_9) = x_7 \to x_8 \land x_9$ ще намерим по алгоритъма (от СДНФ). Тук отново ще е по-лесно да се гледа противоположната функция $\overline{h(x)}$, която има стойност 1 само върху входове 100, 101, 110 \Rightarrow СДНФ за $\overline{h(x)}$ е: $x_7\overline{x}_8\overline{x}_9 \lor x_7\overline{x}_8x_9 \lor x_7x_8\overline{x}_9 \Rightarrow$ полиномът на Жегалкин за нея е: $x_7(x_8+1)(x_9+1)+x_7(x_8+1)x_9+x_7x_8(x_9+1)=x_7(x_8+1)(x_9+1+x_9)+x_7x_8(x_9+1)=x_7x_8x_9+x_7\Rightarrow$ полиномът за оргиналната функция h(x) е: $x_7x_8x_9+x_7+1$. \checkmark

Така полиномът за $f(x_1, \dots, x_9) = (x_1x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2 + 1) + (x_4x_5 + x_4x_6 + x_4x_5x_6) + (x_7x_8x_9 + x_7 + 1) = x_1x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2 + 1 + x_4x_5 + x_4x_6 + x_4x_5x_6 + x_7x_8x_9 + x_7.$

Задача 14 (*). Верни ли са равенствата по-долу? Дайте кратка аргументация защо.

• $w\overline{x}yz \lor w\overline{x}y\overline{z} \lor \overline{w}x\overline{y}z \lor \overline{w}xy\overline{z} \lor wxyz = w\overline{x}yz + w\overline{x}y\overline{z} + \overline{w}x\overline{y}z + \overline{w}xy\overline{z} + wxyz?$

• $w\overline{x}y \lor w\overline{xyz} \lor \overline{w}x\overline{y}z \lor \overline{w}xy\overline{z} \lor wyz = w\overline{x}y + w\overline{xyz} + \overline{w}x\overline{y}z + \overline{w}xy\overline{z} + wyz$

Решение. Еквивалентни преобразувания и разглеждане на таблици на истинност не биха били удачни решения на тази задача, защото удължават решението чрезмерно. Освен това към примерите могат да бъдат добавени още променливи и клаузи, които да не променят идеята, но пък биха затормозили допълнително горните подходи.

- Да, равенството е вярно. Аргументацията е същата като тази, която ползвахме в доказателството на коректността на алгоритъма за образуване на полином Жегалкин от СДНФ. Важното тук е, че конюнктивните клаузи са пълни.
- Не всички конюнктивни клаузи са пълни. Това ни навежда на мисълта, че няма равенство. Наистина, при w=y=z=1, x=0 LHS има стойност 1, а RHS има стойност 0, така че двете формули не са еквивалентни.

Дефиниция. Дефинираме релацията $\leq \leq \{0,1\}^n \times \{0,1\}^n$. Два булеви вектора $a,b \in \{0,1\}^n$ са в релация $a \leq b$ точно когато $\forall i \leq n : a_i \leq b_i$ (всеки бит на първия вектор е не по-голям от съответния му бит във втория вектор).

Задача 15 (*). Дадена е функция $f \in \mathcal{F}_n$, за която съществуват k двоични вектора $a_1, \dots, a_k \in \{0,1\}^n$ такива, че $a_1 \leq a_2 \leq \dots \leq a_k$ и $f(a_i) \neq f(a_{i+1}) \ \forall i < n$. Да се докаже, че функцията има поне k-1 съществени променливи.

Peшение. //TO DO

Дефиниция (симетрична функция). Функция на n променливи е симетрична тстк стойността ѝ е една и съща за всяка пермутация на променливите ѝ. Формално $f(x_1, \cdots, x_n) = f(x_{\tau(1)}, \cdots, x_{\tau(n)})$ за всяка биекция $\tau: \{1, ..., n\} \to \{1, ..., n\}$ (пермутаци-

Задача 16 (*). Докажете, че всяка симетрична булева функция, различна от константа, има само съществени променливи.

Задача 17 (*). Нека $f,g \in \mathcal{F}_n$ са такива, че $f(x) \oplus g(x) = 1$ за точно нечетен брой вектори $x \in \{0,1\}^n$. Да се докаже, че всяка променлива е съществена за поне едната от функциите f и g.

Благодарности

Благодаря на Крис Гърчев за дадената идея за алгебричното доказателство на единствеността на полинома на Жегалкин.