Многообразие булевых функций

Рассмотрим функции с неболее чем двумя аргументами

минтермы	функция	обозначение	другое обозначение	название
0000	0	0	-	тождественный ноль
0001	AB	$A \wedge B$	$A \cdot B$, $A\&B$	конъюнкция, И
0010	$A\overline{B}$	$A \nrightarrow B$	A>B, $\neg(A \rightarrow B)$	больше, инверсия прямой импликации
0011	A	A	-	первый операнд
0100	$\overline{A}B$	$A \nleftarrow B$	A<B, $\neg(A \leftarrow B)$	меньше, инверсия обратной импликации
0101	B	B	-	второй операнд
0110	$\overline{A}B + A\overline{B}$	$A \oplus B$	$A \neq B$, $A xor B$	не равно сложение по модулю 2
0111	A + B	$A \vee B$	$A or B$,	дизъюнция
1000	$\overline{AB}$	$A \downarrow B$	A nor B	стрелка Пирса, НЕ-ИЛИ
1001	$\overline{AB} + AB$	A=B	$A \equiv B$, $A \sim B$	равенство, эквивалентность
1010	$\overline{B}$	$\neg B$	B	отрицание второго операнда
1011	$A + \overline{B}$	$A \leftarrow B$	$A \geq B$	обратная импликация
1100	$\overline{A}$	$\neg A$	A	отрицание первого операнда
1101	$\overline{A} + B$	$A \rightarrow B$	$A \leq B$	прямая импликация
1110	$\overline{A} + \overline{B}$	$A \triangledown B$	A|B	штрих Шеффера, НЕ-И
1111	1	1	-	тождественная единица

$f(A,B) = \ldots$

$f(A,B,C) = A \cdot B \cdot C + A \cdot B \cdot C$

$A \downarrow B \downarrow B \downarrow A \ldots = f(A,B)$

Каждую из представленных операций можно использовать в тернарном варианте.

$A \downarrow B \downarrow C$ — функция Вэбба, тернарная стрелка Пирса

$A \oplus B \oplus C$ — тернарное сложение по модулю 2.

Суперпозиция функций

Опр **Суперпозиция функций** — функция, полученная из некоторого множества функций путем **подстановок** одной функции в другую и/или **отождествления** переменных.

Опр **Подстановка функции g в функцию f** — замена i-го аргумента функции f значением функции g.

$f(x_1, x_2, \ldots x_n)$ $\quad g(y_1, \ldots y_m)$ $\quad x_i$ $\quad f, g$ $\quad h$

$$h(x_1, \ldots, y_1, y_2 \ldots, y_m, \ldots x_n) = f(x_1, \ldots g(y_1, \ldots y_m), \ldots x_n);$$

$$h(x_1, \ldots x_i, x_{i+1}, \ldots x_{i+m-1}, \ldots x_{n+m-1}) = f(x_1 \ldots g(x_i, \ldots x_{i+m-1}), \ldots x_{n+m-1})$$

$n+m-1$ аргументов

Пример

$f(a, b, c) = a + bc$ $\qquad g(a, b) = \bar{a} \oplus b$

$g(d, e) = \bar{d} \oplus e$

$$h(a, d, e, c) = f(a, g(d, e), c) = a + (\bar{d} \oplus e)c$$

Опр **Отождествление переменных в функции f** — постановка i-го аргумента функции вместо j-го.

$f(x_1, x_2, \ldots x_i, \ldots x_j, \ldots x_n)$

$$h(x_1, x_2, \ldots x_i, \ldots x_{j-1}, x_{j+1} \ldots x_n) = f(x_1, x_2, \ldots x_i, \ldots x_i, \ldots x_n)$$

Пример

$f(a, b, c) = a + bc$

отождеств a и b

$$h(a, c) = f(a, a, c) = a + ac = a$$

Опр **Ранг суперпозиции** — минимальное число подстановок и отождествлений, за которое суперпозиция может быть получена из исходного множества функций. Суперпозиция K ранга n обозначается как

$h(\ldots)$ $\qquad f \quad g \quad \varphi$

$h(a, b, c) = ab + \bar{a}c$

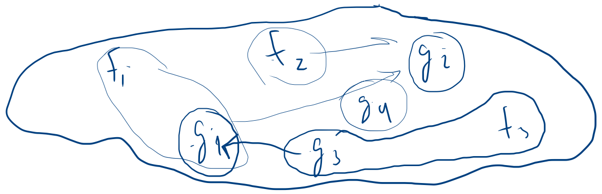
$f(a) = \bar{a}$

$g(a, b) = a + b$

$\varphi(a, b) = a \cdot b$

Понятие замкнутости множества функций

Опр **Замкнутое множество функций** — множество, в котором любая булева функция является суперпозицией некоторого подмножества функций из данного множества.



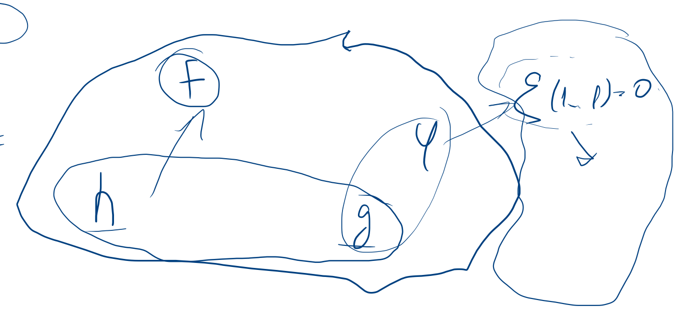
Пример Функции, которые сохраняют единицу (на единичном наборе переменных всегда возвращают единицу)

$f(1,\dots,1) = 1 \qquad g(1,\dots,1) = 1$

$h(1,\dots,1,\dots,1) = f(1,\dots g(1,\dots,1),\dots,1) =$

$= f(1,\dots,1,\dots,1) = 1$

$h(1 \dots 1) = f(1,\dots,1,\dots,1,\dots,1) = 1$

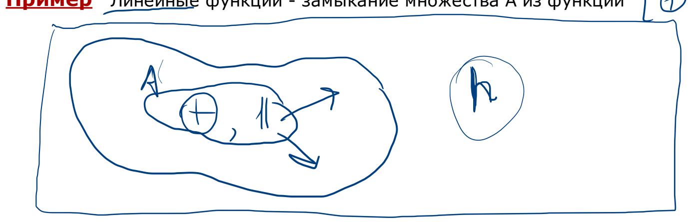


Опр **Замыкание множества функций A** — некоторое подмножество булевых функций, такое что любую из этих функций можно выразить через функции исходного множества A

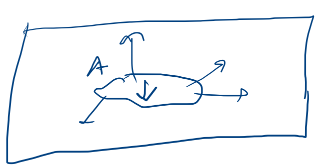
	a		$\bar{a} = 1\oplus a$
	0	1	1
$a\oplus 1$	1	1	0

$h(a,b,c) = a\oplus b\oplus c$

Пример Линейные функции - замыкание множества A из функций $\{\oplus, 1\}$



Опр **Полная система функций** — множество функций, для которого замыкание совпадает с множеством всех булевых функций



Пример

1) $\{\cdot, +, \neg\}$ Булев
2) $\{\oplus, \cdot, 1\}$ Жегалкин
3) $\downarrow$, 4) ∇

Опр **Безызбыточная полная система функций** — полная система функций, которая перестает быть таковой после исключения из неё любой функции

Пример $\overline{A\cdot B} = \overline{A}+\overline{B}$

$\cdot \leftarrow \{+, \neg\}$

$+ \leftarrow \{\cdot, \neg\}$

Булев – избыточен

Жегалкин – безызбыт.

Алгебра Жегалкина

Как в булевом базисе есть возможность представлять функцию в виде ДНФ и КНФ, так и в базисе Жегалкина есть свой вариант представления функций, а именно с помощью так называемого **полинома Жегалкина**

$a \oplus 0 = a$

Базис: $\{\oplus, \cdot, \neg\}$

$\{0, 1\}$

Опр **Полином Жегалкина** — полином с коэффициентами 0 и 1, где произведение представлено операцией конъюнкции, а сложение — сложением по модулю 2 $\oplus$

Общий вид: $P = a_{00\ldots0} \oplus a_{10\ldots0} x_1 \oplus a_{01\ldots0} x_2 \oplus \ldots \oplus a_{00\ldots1} x_n \oplus$

$\oplus a_{11\ldots0} x_1 x_2 \oplus a_{101\ldots0} x_1 x_3 \oplus \ldots a_{00\ldots11} x_{n-1} x_n \oplus a_{111\ldots0} x_1 x_2 x_3 \ldots$

$\ldots \oplus a_{11\ldots1} x_1 x_2 x_3 \ldots x_n$

Свойства операций в алгебре Жегалкина

Коммутативность операции $\oplus$: $A \oplus B = B \oplus A$

Конъюнкция дистрибутивная относительно $\oplus$: $A(B \oplus C) = AB \oplus AC$

Нет дистрибутивности $\oplus$ относительно конъюнкции: $A \oplus BC \neq (A \oplus B)(A \oplus C)$

Связь с булевыми выражениями $\{\oplus, 1, \cdot\}$

1) $A + B = A \oplus B \oplus AB$
2) $\bar{A} = A \oplus 1$
3) $A \oplus A = 0$
4) $A \oplus B = A\bar{B} + \bar{A}B$

A	A	$A \oplus A$
0	0	0
1	1	0

Th Существование и единственность представления булевой функции в виде полинома Жегалкина

Proof 1) 2^{2^n} - всего булев функц

$P = \ldots \oplus \ldots$

2^n - конъюнкций в полиноме

2^{2^n} - полиномов

2) кажд булева функц записывается одним полиномом

от противного

$f: \quad P_1 = P_2: \quad P_1 - P_2 = 0$

$f \oplus f = 0$

$P_1 - P_2 = P_1 \cdot \bar{P_2} = P_1 \cdot (P_2 \oplus 1) =$

пусть есть ненулев коэфф! P

$P = xy \oplus wst \oplus qxst \oplus yt$

$1 \oplus 0 = 1$

$0 \ldots 0\, 1 \ldots 1 \ldots 0$

$P(0, 0, 1, \ldots 1, 0) = 1$

Построение полинома Жегалкина

Существует несколько популярных способов построения полинома Жегалкина для функции (известна её таблица истинности)

f

Способы построения полинома Жегалкина

1) Преобразование ДНФ
2) Преобразование Мёбиуса
3) Метод треугольника
4) Метод Паскаля

Метод треугольника

1) Построить таблицу истинности
2) Построить вспомогательную треугольную таблицу, где первый столбец совпадает со столбцом значений функции
3) Значение для каждой ячейки в следующем столбце вычисляется как xor значений из ячеек предыдущего столбца из той же строки и строкой ниже.
4) Номера столбцов соответвуют конъюнкциям: если данная конъюнкция присутствует в полиноме, то в первой ячейке этого столбца будет единица

$a_{n,0}$

Пример

xyz

№	x	y	z	f	**000**	**001**	010	011	100	101	**110**	111
0	0	0	0	1	1	1	0	0	0	0	1	0
1	0	0	1	0	0	1	0	0	0	1	1	
2	0	1	0	1	1	1	0	0	1	0		
3	0	1	1	0	0	1	0	1	1			
4	1	0	0	1	1	1	1	0				
5	1	0	1	0	0	0	1					
6	1	1	0	0	0	1						
7	1	1	1	1	1							

$f(x,y,z) = 1 \oplus z \oplus yx$

Метод Паскаля

1) Таблица из 2^n столбцов и n+1 строки
2) В первой строке продублированы значения из таблицы истинности
3) Далее каждая строка формируется из блоков предыдущего уровня размером 1 для второй строки, 2 — третьей, 4 — четвертой и т.д. Каждый первый блок переносится в строку ниже без изменения, на место второго ставится результат побитового xor левого и правого блока
4) В последней строке единицами будут указаны конъюнкции, которые должны быть в результирующем полиноме

Пример

xyz

000	**001**	010	011	100	101	**110**	111
1	0	1	0	1	0	0	1
1	1	1	1	1	1	0	1
1	1	0	0	1	1	1	0
1	**1**	0	0	0	0	**1**	0

$f = 1 \oplus z \oplus xy$

$f(A,B,C,D)$

11 11 00   11 01 10

1100 1110 0010

$f \oplus f \oplus f = f$

f: СДНФ или ДНФ

poly

poly

Классы замкнутых функций

Существует достаточно широкое многообразие замкнутых множеств (**классов**) функций.

Наиболее важными из них являются *самодвойственные, линейные, монотонные и сохраняющие ноль или единицу*.

Также эти классы называются **предполными**. !

$f(x_1, \dots x_n) \neq f(\bar{x}_1, \bar{x}_2, \dots \bar{x}_n)$

Опр **Самодвойственная функция** — функция, которая на противоположных наборах дает противоположные значения

S

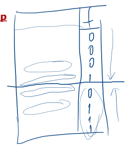
Обозначение: S

Формула: $f(\bar{x}_1, \dots \bar{x}_n) = \overline{f(x_1, \dots x_n)}$

Число самодвойственных функций: различ верх половин $\frac{2^n}{2}$

$2^{2^{n-1}}$

Пример



Опр **Линейная функция** — функция, которая не имеет конъюнкций в своем представлении в виде полинома Жегалкина

Обозначение: L $f = \boxed{x \cdot y}$

Формула: $f(x_1, \dots x_n) = a_{0\dots0} \oplus a_{1\dots0} x_1 \oplus a_{01\dots0} x_2 \oplus \dots a_{0\dots1} x_n$

Число линейных функций: 2^{n+1} т.к. коэффиц $n+1$

Пример

$f(a,b,c) = 1 \oplus b \oplus a \oplus c$

Опр **Монотонная функция** — функция, которая на сравнимых наборах неубывает

$a: (0, 0, 1)$
$b: (0, 1, 0)$

Опр **Сравнимые наборы** — a и b, если $\forall i: a_i \le b_i$

Обозначение: M

Формула: a и b - сравним $a_i \le b_i$
$f(a_1 \dots a_n) \le f(b_1, \dots b_n)$.

a, c - несравнимы
$f(a_1 \dots a_n) > f(c_1 \dots c_n)$

Утв Если наборы не сравнимы, то значения монотонной функции могут на них убывать или оставаться неизменными

Утв Монотонность функции можно определить по её аналитической записи — в ней будут отсутствовать инверсии

Пример

	f
000	0
001	0
010	0
011	1
100	0
101	1
110	1
111	1

Опр **Функция, сохраняющая единицу** — функция, возвращающая единицу на единичном наборе аргументов (11...1)

Обозначение: T_1

Формула: $f(1, \dots 1) = 1$

$2^n - 1$

Утв Если функция, сохраняющая единицу представлена в СДНФ, то в ней обязательно будет присутствовать минтерм с индексом 2^n - 1, где n — число аргументов функции.

m_{2^n-1}

Утв Если функция, сохраняющая единицу представлена в ДНФ, то в неё входит хоть одна конъюнкция без инверсий.

$f(x, \dots z) = + xwt +$
$xwty + xwt\bar{y}$
$xwtyz + xwty\bar{z} + xwt\bar{y} \dots$

Утв Если функция, сохраняющая единицу представлена в КНФ, то во всех её дизъюнкциях должен быть хотя бы один не инверсный аргумент.

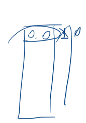
$f(\dots) = (+ + 0 + -)(+ 0 -)(0)$

Опр **Функция, сохраняющая ноль** — функция, возвращающая ноль на нулевом наборе аргументов (00...0)

Обозначение: T_0

Формула: $f(0, \dots 0) = 0$

Утв Если функция, сохраняющая ноль представлена в СДНФ, то в неё не будет входить минтерм m_0.



Утв Если функция, сохраняющая ноль представлена в ДНФ, то в её записи нет ни одной конъюнкции, содержащие только инверсные переменные.

$\bar{A}\bar{B}\bar{W}$

$f(\dots) = \_\_ + \_\_ + \_\_$

Утв Если функция, сохраняющая ноль представлена в КНФ, то есть хотя бы одна дизъюнкция, в которой нет инверсных переменных.

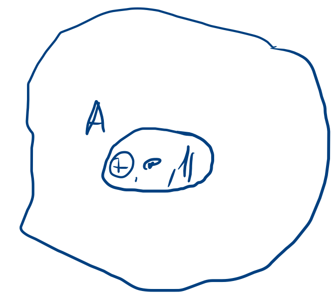
$0 + 0 \dots 0$

$f(\dots) = (\dots)(\quad)(+ +)$

0

Полнота систем функций

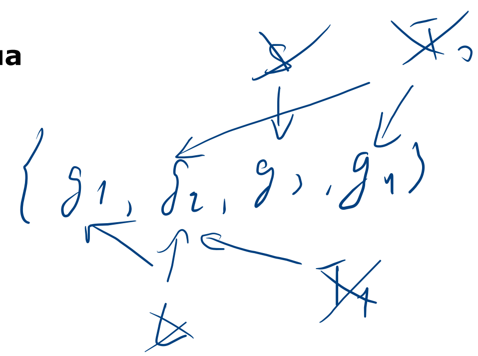
Естественно, что функция может принадлежать или непринадлежать нескольким классам сразу, например:



Рассмотренные классы используются в теореме Поста (критерий Поста), которая определяет **набор функций** как **полный**, если он **не содержится полность ни в одном из предполных классов**

$\{f, g, h\}$

Другими словами среди функций системы есть **хоть одна**



1) Несамодвойственная
2) Нелинейная
3) Немонтонная
4) Не сохраняющая ноль
5) Не сохраняющая единицу

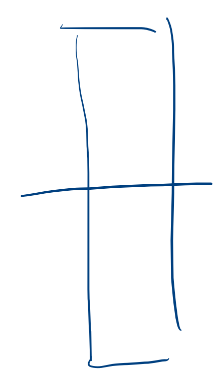
Примеры полных систем:

1) булев базис
2) базис Жегалкина
3) штрих Шеффера
4) стрелка Пирса
5) множество различных, удовлетворяющих теореме Поста

Булев базис + - входит в класс — не входит в класс

·	+	¬	класс
+	+	-	сохраняющая ноль
+	+	-	сохраняющая единицу
-	-	+	самодвойственная
+	+	-	монотонная
-	-	+	линейная

$1 \oplus x$



$f = (x \cdot y$

Базис Жегалкина

Полнота:
Нет строк со всеми +

Избыточность

1	·	⊕	класс
-	+	+	сохраняющая ноль
+	+	-	сохраняющая единицу
-	-	-	самодвойственная
+	+	-	монотонная
+	-	+	линейная

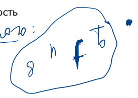
Критерий Поста

Th Набор функций A **полон** тогда и только тогда, когда он **не содержится целиком ни в одном из предполных классов**. То есть в нем есть хотя бы одна несамодвойственная, хотя бы одна нелинейная, хотя бы одна немонотонная, хотя бы одна не сохраняющая ноль и хотя бы одна не сохраняющая единицу функция.

Proof

1) Необходимость

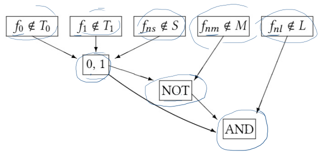
от противного:



2) Достаточность $f_0 \notin T_0,\ f_1 \notin T_1,\ f_2 \notin S,\ f_3 \notin M,\ f_4 \notin L$

$f_0, f_1 \ldots f_4$ могут совпадать

Если из функций полной системы можно выразить все функции, то можно и те, которые образуют булев базис $\{\cdot, \neg\}$



Структура доказательства следующая:

1)С помощью функций несохраняющих ноль, единицу и несамодвойственной можно выразить две константы 0 и 1

2)С помощью констант и немонотонной функции будет показано как выразить отрицание

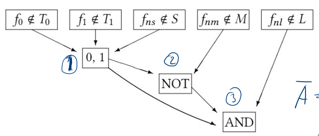
3)С помощью отрицания, констант и нелинейной функции выражается конънкция.сли из функций полной системы можно выразить все функции, то можно и те, которые образуют булев базис

Часть 1

1) $\exists f_0$ - сохр. единицу $f_0 \notin T_0,\ f_1 \notin T_1$

$f_0(0, \ldots 0) = 1$, $f_0(1 \ldots 1) = 1$ | $f_0(x, \ldots x) = 1$

$f_1(0 \ldots 0) = 0$, $f_1(1 \ldots 1) = 0$ | $f_1(x, \ldots x) = 0$



$\overline{A} = f_0(A, \ldots A)$

$f = \overline{A} B$

$\overline{f}$

$f_0(F, \ldots F) = \overline{F}$

2) f_0 - несохр единицу $f_0 \notin T_0,\ f_1 \notin T_1$

$f_0(0 \ldots 0) = 1$, $f_0(1 \ldots 1) = 0$ | $f_0(x, \ldots x) = \overline{x} = NOT(x)$

Выраж. констант

$f_{ns}(\hat{0}, \hat{0}, 1) = f_{ns}(1, 1, 0) = 1$

$f_{ns}(x, x, \overline{x}) = f_{ns}(x, x, NOT(x)) = f_{ns}(x, x, f_0(x, \ldots x)) = \boxed{1}$

$0 = NOT(1) = NOT(f_{ns}(x, x, f_0(x, \ldots x)))$

Часть 2

$f_{nm}(x, y, z)$

$f_{nm}(0, 0, 1) = 1$ $f_{nm}(0, 1, 1) = 0$

$a_i \leq b_i$

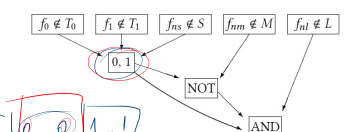
$a_1 = b_1 = 0$

$a_2 < b_2$ $0 < 1$

$a_3 = b_3$ $1 = 1$

$0, \ldots, 0$ | $0, \ldots, 0$ | $1, \ldots 1$

$0, \ldots, 0$ | $1, \ldots, 1$ | $1, \ldots 1$



$\overline{A}$

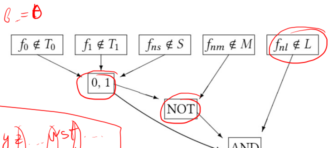
$f_{nm}(0, \ldots 0, x, x \ldots x, 1, \ldots 1) = \overline{x}$

Часть 3

$f_{nl} =$ лин. ч. $\oplus\ xyzwt \oplus yzswt x \ldots$

мин нелин!

$a, b \ldots = 0$



Виды полинома:

$a\ b\ c \ldots\ x\ y\ z \ldots\ w\ s\ t \ldots$

$0\ 0\ 0 \ldots 0\ x\ y\ 1\ 0 \ldots 1\ 0\ 1\ 0 \ldots$

1) $1 \oplus x \oplus y + xy$

2) $1 \oplus x \oplus xy$

3) $1 \oplus y \oplus xy$

4) $1 \oplus xy$

5) $x \oplus y \oplus xy$

6) $x \oplus xy$

7) $y \oplus xy = y(1 \oplus x) = y \cdot \overline{x}$

8) xy

$A \cdot B$

$f_{nl}(0, \ldots 0, A, \ldots 1, \ldots B, \ldots 0) = A \cdot B$

$B \oplus AB$

$f_{nl}(0, \ldots \overline{A}, \ldots 1, \ldots B, \ldots 0) = A \cdot B$

$f_{nl}(p, q, r) = 1 \oplus p \oplus pq \oplus pqr$

$f_{nl}(p, q, 0) = 1 \oplus p \oplus pq = 1 \oplus p(1 \oplus q) = 1 \oplus p\overline{q} = \overline{p\overline{q}}$

$pq = \overline{f_{nl}(p, \overline{q}, 0)}$