Содержание

1 Теория булевых функций

1.1 Определение булевой функции (БФ). Количество БФ от n переменных. Таблица истинности БФ

Определение. Булева функция от n переменных - это отображение $\{0,1\}^n \to \{0,1\}$

Замечание. Количество БФ от n переменных - 2^{2^n}

Доказательство. Каждая булева функция определяется своим столбцом значений. Столбец является булевым вектором длины $m = 2n$, где n – число аргументов функции. Число различных векторов длины m (а значит и число булевых функций, зависящих от n переменных) равно $2^m = 2^{2^n}$ ▶

1.2 Булевы функции одной и двух переменных (их таблицы, названия)

Булевы функции одной переменной:

x	f_1	f_2	f_3	f_4
0	0	0	1	1
1	0	1	0	1

f_1 - тождественный 0, f_2 - тождественная функция, f_3 - отрицание ($\neg$), f_4 - тождественная 1

Булевы функции двух переменных

x	y	0	$\wedge$	$\to'$	x	$\leftarrow'$	y	$+$	$\vee$	$\downarrow$	$\leftrightarrow$	y'	$\leftarrow$	x'	$\to$	$\mid$	1
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

1. $\wedge$ - конъюнкция
2. $\leftarrow$ - антиимпликация
3. $\to$ - импликация
4. $\vee$ - дизъюнкция
5. $|$ - штрих Шеффера
6. $\downarrow$ - стрелка Пирса
7. $+$ - взаимоисключающее или, сложение по модулю 2 (XOR)

1.3 Формулы логики высказываний. Представление БФ формулами

Определение. Формула логики высказываний - слово алфавита логики высказываний, построенное по следующим правилам:

1. символ переменной - формула
2. символы 0 и 1 - формулы
3. если Φ_1 и Φ_2 - формулы, то слова $(\Phi_1 \& \Phi_2)$, $(\Phi_1 \leftrightarrow \Phi_2)$, $(\Phi_1 \to \Phi_2)$, $(\Phi_1 | \Phi_2)$, ... , Φ_1' тоже формулы

Очевидно, что каждой формуле логики высказываний можно поставить в соответствие булеву функцию, причем если формуле F_1 соответствует функция f_2, а формуле F_2 функция f_2 и $F_1 \equiv F_2$, то $f_1 \equiv f_2$.

Каждая формула $\Phi(x_1, \ldots, x_n)$ логики высказываний однозначно определяет некоторую булеву функцию $f(x_1, \ldots, x_n)$ Это булева функция, определенная таблицей истинности формулы Φ.

1.4 Эквивалентные формулы. Основные эквивалентности теории булевых функций

Определение. Формулы логики высказываний $\Phi(x_1,\ x_2,\ ...,\ x_n)$ и $\Psi(x_1,\ x_2,\ ...,\ x_n)$ эквивалетные, если для всех наборов значений $a_1,\ ...,\ a_n \in \{0,\ 1\}$ $\Phi(a_1,\ ...,\ a_n) = 1 \Leftrightarrow \Psi(a_1,\ ...,\ a_n) = 1$

Теорема 1.1 (Об эквивалентных формулах). *1. Если $\Phi(x_1, ..., x_n) \equiv \Psi(x_1, ..., x_n)$ и $\theta_i(x_1, ..., x_k)$, $i = 1,\ ...,\ n$, - формулы логики высказываний, то $\Phi(\theta_1, ..., \theta_n) \equiv \Psi(\theta_1, ..., \theta_n)$*

2. Если в формуле Φ заменить подформулу Ψ на эквивалетную формулу Θ, то результат замены эквивалентен Φ.

Доказательство. 1. После подстановки в $\Phi(x_1, ..., x_n)$ формул $\theta_i(x_1, ..., x_k)$ получим формулу от k переменных:

$$\Phi(\theta_1, ..., \theta_n)(x_1, ..., x_k) = \Phi(\theta_i(x_1, ..., x_k), ..., \theta_n(x_1, ..., x_k))$$

и аналогично для Ψ. Выберем произвольный набор элементов $a_1, ..., a_k \in \{0, 1\}$ и подставим:

$$\Phi(\theta_1(a_1, ..., a_k), ..., \theta_n(a_1, ..., a_k)) = \Phi(b_1, ..., b_n), b_i = \theta_i(a_1, ..., a_k),$$

$$\Psi(\theta_1(a_1, ..., a_k), ..., \theta_n(a_1, ..., a_k), ..., \theta_n(a_1, ..., a_k)) = \Psi(b_1, ..., b_n).$$

Т.к. $\Phi \equiv \Psi, \Phi(b_1, ..., b_n) = 1 \leftrightarrow \Psi(b_1, ..., b_n) = 1$, значит и $\Phi(\theta_1, ..., \theta_n)(a_1, ..., a_k) = 1 \leftrightarrow \Psi(\theta_1, ..., \theta_n)(a_1, ..., a_k)$, т.е. $\Phi(\theta_1, ..., \theta_n) \equiv \Psi(\theta_1, ..., \theta_n)$.

2. По условию $\Psi \equiv \Theta$. Обозначим результат замены в формуле Φ подформулы Ψ на Θ через $\Phi[\Psi/\Theta]$.

Индукцию по числу логических связанок в формуле Φ. Пусть k - число связок в подфомруле Ψ.

Заметим, что, если формула Φ содержит менее k связок, то в ней нет подформулы Ψ. А если формула Φ имеет ровно k связок, то единственный случай, когда она содержит подформулу Ψ - это $\Phi = \Psi$

База индукции.

(a) Формула Φ содержит не более k связок и при этом $\Phi \neq \Psi$. Тогда Φ не содержит подформулы Ψ, поэтому при данной операции не меняется: $\Phi[\Psi/\Theta] = \Phi$, отсюда $\Phi[\Psi/\Theta] \equiv \Phi$

(b) Формула Φ содержит k связок и $\Phi = \Psi$. Тогда $\Phi[\Psi/\Theta] = \Theta$ результат замены эквивалентен исходной формуле $\Phi = \Psi$

Шаг индукции.

Рассмотрим формулу $\Phi(x_1, ..., x_n)$ содержающую m + 1 связки, считая, что для формул из не более, чем m связок, утверждение доказано. Тогда Φ имеет вид $\Phi_1 \wedge \Phi_2, \Phi_1 \vee \Phi_2$ и т.д.

Рассмотрим случай конъюнкции(остальные аналогично). Выберем набор элементов $a_1, ..., a_n \in \{0, 1\}$ и подставим в формулы:

$$\Phi(a_1, ..., a_n) = \Phi_1(a_1, ..., a_n) \wedge \Phi_2(a_1, ..., a_n),$$

$$\Phi[\Psi/\Theta](a_1, ..., a_n) = \Phi_1[\Psi/\Theta](a_1, ..., a_n) \wedge \Phi_2[\Psi/\Theta](a_1, ..., a_n).$$

По индукционному допущению формулы $\Phi_1 \equiv \Phi_1[\Psi/\Theta]$ аналогично для Φ_2 Поэтому

$$\Phi(a_1, ..., a_n) = \Phi_1(a_1, ..., a_n) \wedge \Phi_2(a_1, ..., a_n),$$

$$\Phi[\Psi/\Theta](a_1, ..., a_n) = \Phi_1[\Psi/\Theta](a_1, ..., a_n) \wedge \Phi_2[\Psi/\Theta](a_1, ..., a_n),$$

т.е. $\Phi \equiv \Phi[\Psi/\Theta]$

▶

Теорема 1.2. *Справедливы следующие эквивалетности*

1. $a \vee b \equiv b \vee a$ ***симметричность***
2. $a \wedge b \equiv b \wedge a$
3. $a \vee (b \vee c) \equiv (a \vee b) \vee c$ ***ассоциативность***
4. $a \wedge (b \wedge c) \equiv (a \wedge b) \wedge c$
5. $a \wedge (b \vee c) \equiv a \wedge b \vee a \wedge c$ ***дистрибутивность***
6. $a \vee b \wedge c \equiv (a \vee b) \wedge (a \vee c)$
7. $a \vee a \equiv a$ ***идемпотентность***
8. $a \wedge a \equiv a$
9. $\overline{(a \vee b)} \equiv \overline{a} \wedge \overline{b}$ ***законы де Моргана***
10. $\overline{(a \wedge b)} \equiv \overline{a} \vee \overline{b}$

11. $\overline{\overline{a}} \equiv a$ ***двойное отрицание***

12. $a \vee a \wedge b \equiv a$ ***поглощение***

13. $a \wedge (a \vee b) \equiv a$

14. $a \vee \overline{a} \wedge b \equiv a \vee b$ ***слабое поглощение***

15. $a \wedge (\overline{a} \vee b) \equiv ab$

16. $a \vee 0 \equiv a$

17. $a \wedge 0 \equiv 0$

18. $a \vee 1 \equiv 1$

19. $a \wedge 1 \equiv a$

20. $a \vee \overline{a} \equiv 1$

21. $a\overline{a} \equiv 0$

22. $a \to b \equiv \overline{a} \vee b$

23. $a \leftrightarrow b \equiv \overline{a} \wedge \overline{b} \vee a \wedge b \equiv (a \to b) \wedge (b \to a)$

24. $a + b \equiv \overline{a \leftrightarrow b} \equiv \overline{a} \wedge b \vee a \wedge \overline{b}$

25. $a|b \equiv \overline{a \wedge b}$

26. $a \downarrow b \equiv \overline{a \vee b}$

Доказательство. Доказательство сводится к построению таблиц истинности для левой и правой частей каждой эквивалентности ►

1.5 Тождественно истинные (ложные) и выполнимые БФ

Определение. Формула $\Phi(x_1, \ldots, x_n)$ называется тождественно истинной (ложной), если для любого набора значений $\Phi(x_1, \ldots, x_n) = 1(0)$

Определение. Формула $\Phi(x_1, \ldots, x_n)$ называется выполнимой, если существует набор значений, для которого $\Phi(x_1, \ldots, x_n) = 1$

1.6 ДНФ и КНФ, алгоритмы приведения

Определение. Литера - это переменная или отрицание переменной

Определение. Конъюнкт(элементарная конъюнкция) - это либо литера, либо конъюнкция литер

Определение. Дизъюнктивная нормальная форма(ДНФ) - это либо конъюнкт, либо дизъюнкия конъюнктов

Определение. Дизъюнкт(элементарная дизъюнкция) - это либо литера, либо дизъюнкция литер

Определение. Конъюнктивная нормальная форма (КНФ) - это либо дизъюнкт, либо конъюнкция дизъюнктов

Замечание. Алгоритм построения ДНФ(КНФ) по заданной ТИ

1. Выбрать в таблице все строки со значением функции f = 1 (f = 0)
2. Для каждой такой строки (x, y, z) = (a_1, a_2, a_3) выписать конъюнкт(дизъюнкт) по принципу: пишем переменную с отрицанием, если ее значение 0(1), иначе пишем переменную без переменную без отрицания.
3. берем дизъюнкцию(конъюнкцию) построенных конъюнктов(дизъюнктов)

Замечание. Алгоритм приведения формулы к ДНФ/КНФ методом эквивалентностей

1. Выразить все связки в формуле через конъюнкцию, дизъюнкцию и отрицание.
2. Внести все отрицания внутрь скобок
3. Устранить двойные отрицания
4. Применять свойство дистрибутивности, пока это возможно

1.7 СДНФ и СКНФ, теоремы существования и единственности, алгоритмы приведения

Определение. Совершенный конъюнкт от переменных $x_1, ..., x_n$ - это конъюнкт вида $x_1^{a_1} \wedge ... \wedge x_n^{a_n}$, где $(a_1, ..., a_n) \in \{0, 1\}^n$.

Определение. Совершенный дизъюнкт от переменных $x_1, ..., x_n$ - это конъюнкт вида $x_1^{a_1} \vee ... \vee x_n^{a_n}$, где $(a_1, ..., a_n) \in \{0, 1\}^n$.

Замечание.

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

Определение (СДНФ)**.** Совершенная дизъюнктивная нормальная форма(СДНФ) от переменных $x_1, ..., x_n$ - это дизъюнкция совершенных конъюнктов от $x_1, ..., x_n$, в которой нет попарно эквивалентных слагаемых

Определение (СКНФ)**.** Совершенная конъюктивная нормальная форма(СКНФ) от переменных $x_1, ..., x_n$ - это конъюнкция совершенных дизъюнктов от $x_1, ..., x_n$, в которой нет попарно эквивалентных слагаемых.

Теорема 1.3 (о существовании и единственности СДНФ)**.** *Любая булева функция $f(x_1, ..., x_n) \neq 0$ определяется формулой, находящейся в СЛНФ, причем эта СДНФ единственная с точностью до перестановок слагаемых и множителей в слагаемых*

Доказательство. 1. Существование. По следствию к теореме о разложении получаем для $f(x_1, ..., x_n) \neq 0$

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

2. Единственность. Пусть, у функции $f(x_1, ..., x_n) \neq 0$ две СДНФ, обозначим их Φ и Ψ. Так как они определяют одну и ту же функцию, то $\Phi \equiv \Psi$

   Выберем в Φ произвольное слагаемое $x_1^{a_1}...x_n^{a_n}$. По лемме о совершенных конъюнктах это слагаемое истинно при $(x_1, ..., x_n) = (a_1, ..., a_n)$. Тогда и вся дизъюнкция $\Phi(a_1, ..., a_n) = 1$, а в силу эквивалентности формул и $\Psi(a_1, ..., a_n) = 1$

   Но тогда в Ψ есть слагаемое $x_1^{b_1}...x_n^{b_n}$, истинное на наборе $(a_1, ..., a_n)$. Снова по лемме это возможно только при $(a_1, ..., a_n) = (b_1, ..., b_n)$.

   Получаем, что все слагаемые СДНФ Φ есть в Ψ. Рассуждая симметрично, получаем, что и Ψ содержится в Φ, т.е. они равны

►

Замечание (Лемма о совершенных конъюнктах). 1. Пусть $\Phi(x_1, ..., x_n) = x_1^{a_1}...x_n^{a_n}$ - совершенный конъюнкт. Тогда для любого набора значений $(b_1, ..., b_n) \in \{0, 1\}^n$

$$\Phi(b_1, ..., b_n) = 1 \leftrightarrow (b_1, ..., b_n) = (a_1, ..., a_n).$$

2. Два совершенных конъюнкта от перменных $x_1, ..., x_n$ эквивалентны тогда и только тогда, когда они равны с точностью до перестановки литер.

Замечание. Рассуждая двойственным образом, можно получить теорему о СКНФ

Замечание. Алгоритм приведения формулы к СДНФ(СКНФ)

1. Строим ДНФ(КНФ) формулы.
2. Вычеркиваем тождественно ложные(истинные) слагаемые(множители).
3. В каждое слагаемое(множитель) добавляем переменны по правилам:
   СДНФ: $\Phi(x_1, ..., x_n) \equiv \Phi(y \vee \overline{y}) \equiv \Phi \wedge y \vee \Phi \wedge \overline{y}$
   СКНФ: $\Phi(x_1, ..., x_n) \equiv \Phi \vee y \wedge \overline{y} \equiv (\Phi \vee y) \wedge (\Phi \vee \overline{y})$
4. Вычеркиваем повторяющиеся слагаемые(множители).

1.8 Минимизация нормальных форм (карты Карно)

1.9 Полином Жегалкина, его существование и единственность. Алгоритм построения

1.10 Суперпозиция булевых функций. Замкнутые классы булевых функций

Определение. Суперпозиция булевых функций $f(x_1, \ldots, x_n)$ и $f_i(x_1, \ldots, x_k), i = 1, \ldots, n,$ — это функция $F(x_1, \ldots, x_k) = f(f_1, \ldots, f_n)$.

Определение. Подстановка переменной y вместо x_i в булеву функцию $f(x_1, \ldots, x_n)$ — это суперпозиция вида $f(x_1, \ldots, x_{i-1}, y, x_{i+1}, \ldots, x_n)$.

Определение. Замыкание класса K булевых функций (обозначение: [K]) — это наименьший класс, содержащий все функции класса K, всевозможные их суперпозиции и результаты подстановок переменных, суперпозиции полученных функций и т.д.

Определение. Замкнутый класс булевых функций — это класс, равный своему замыканию.

Пример. $M = \{x', x \oplus y\}$.

1. $0 \in [M]$, так как $0 = x \oplus x$
2. $1 \in [M]$, так как $1 = (x \oplus x)'$
3. $x \oplus y \oplus z \in [M]$

1.11 Полные системы булевых функций, базисы

Определение. Система булевых функций является полной(в классе К), если ее замыкание равно классу всех булевых функций(классу К)

Пример (Примеры полных систем).

1. $M = \{\neg x, xy, x \vee y\}$ **каждая БФ может быть записана в виде ДНФ**
2. $M = \{\neg x, x \vee y\}$ **выражаем** xy **через отрицание и дизъюнкцию по закону де Моргана**
3. $M = \{\neg x, xy\}$
4. $M = \{\oplus, *, 1\}$ **полином Жегалкина**
5. $\{\leftrightarrow, \vee, 0\}$ **навесить отрицание на функции из предыдущей системы**
6. $M = \{x|y\}$, $\neg x \equiv x|x, xy \equiv \neg(x|y) \equiv (x|y)|(x|y)$ **аналогично стрелка Пирса**

Определение. Полная (в классе К) система функций называется базисом (класса К), если никакая ее подсистема не будет полной (в классе К).

Пример (Примеры базисов).

1. $M = \{x|y\}$, $\neg x \equiv x|x, xy \equiv \neg(x|y) \equiv (x|y)|(x|y)$ **аналогично стрелка Пирса**
2. $M = \{\&, '\}$, аналогично $\{\vee, '\}$ Мы не могли вычеркнуть отрицание, так как xy и $x \vee y \in T_0 \implies [xy, x \vee y] \subseteq T_0$ и $1 \notin T_0 \implies \neg x \in [xy, x \vee y] \implies \{\vee, \&\}$ не полна
3. $M = \{\oplus, *, 1\}$ **полином Жегалкина**

Замечание. Никакой базис не может содержать более 4 функций.

Доказательство. Из доказательства теоремы Поста $g_0(x)$ (не сохраняющая 0 функция $f(x_1, \ldots, x_n)$, в которую подставлили одну и ту же переменную x) либо несамодвойственна, либо немонотонна, $\implies$ полной будет система из 4 функций. Этим доказано, что всякая полная система содержит полную подсистему не более чем из четырёх функций. В базисе нет собственных полных подсистем, поэтому в нём не более четырёх функций.

Оценку нельзя уменьшить, так как существует система $\{0, 1, xy, x \oplus y \oplus z\}$. Построим таблицу с классами Поста, видим, что система полна и никакая ее собственная подсистема не полна. ▶

1.12 Классы T_0, T_1 (функции, сохраняющие 0 и 1)

Определение. Класс $T_0 = \{f(x_1, \ldots, x_n) \mid f(0, \ldots, 0) = 0\}$

Определение. Класс $T_1 = \{f(x_1, \ldots, x_n) \mid f(1, \ldots, 1) = 1\}$

	T_0	T_1	S	M	L
0	+	-	-	+	+
1	-	+	-	+	+
x	+	+	-	+	+
$\neg x$	-	-	+	-	+
xy	+	+	-	+	-
$x \vee y$	+	+	-	+	-
$x \oplus y$	+	-	-	-	+
$x \leftrightarrow y$	-	+	-	-	+
$x \to y$	-	+	-	-	-
$x\|y$	-	-	-	-	-
$x \downarrow y$	-	-	-	-	-

Замечание. Классы T_0, T_1 являются замкнутыми.

Доказательство. Докажем для T_0. Достаточно взять булевы функции $g, g_1, \ldots, g_n \in T_0$ и доказать, что их суперпозиция из класса T_0.

$g(g_1(0, \ldots, 0), \ldots, g_n(0, \ldots, 0)) = g(0, \ldots, 0) = 0$ ▶

1.13 Класс S самодвойственных функций, определение двойственной БФ

Определение. Булева функция $g(x_1, \dots, x_n)$ называется двойственной к БФ $f(x_1, \dots, x_n)$ (обозначается g = f*), если $g(x_1, \dots, x_n) = f'(x_1', \dots, x_n')$.

Из закона двойного отрицания следует, что $(f^*)^* = f$

Определение. Булева функция f называется самодвойственной, если $f = f^*$.

Определение. Класс самодвойственных функций = $\{f \mid f = f^*\}$

Замечание. Класс S является замкнутым.

Доказательство. Возьмем БФ $g, g_1, \dots g_k \in S$ и докажем, что их суперпозиция будет также из класса S.
Если $F(x_1, \dots, x_n) = g(g_1(x_1, \dots, x_n), \dots, g_k(x_1, \dots, x_n))$,
то $F^*(x_1, \dots, x_n) = \neg F(\neg x_1, \dots, \neg x_n) = \neg g(g_1(\neg x_1, \dots, \neg x_n), \dots, g_k(\neg x_1, \dots, \neg x_n))$.

Так как $g_i \in S$, то $g_i(x_1, \dots, x_n) = \neg g_i(\neg x_1, \dots, \neg x_n)$, что эквивалентно $\neg g_i(x_1, \dots, x_n) = g_i(\neg x_1, \dots, \neg x_n)$. Следовательно, $F^*(x_1, \dots, x_n) = \neg g(\neg g_1(x_1, \dots, x_n), \dots, \neg g_k(x_1, \dots, x_n))$.
Так как $g \in S$, то $\neg g(\neg g_1(x_1, \dots, x_n), \dots, \neg g_k(x_1, \dots, x_n)) = (g_1(x_1, \dots, x_n), \dots, g_k(x_1, \dots, x_n)) \implies f^*(x_1, \dots, x_n) = F(x_1, \dots, x_n)$ ▸

1.14 Класс монотонных функций

Определение. Назовем два набора из 0 и 1 $a = (a_1, \dots a_n), b = (b_1, \dots b_n)$ **соседними**, если все их координаты (кроме одной) совпадают.

Определение. Пусть k - номер единственной координаты, по которой отличаются соседние наборы a, b. Если $a_k = 0$, $b_k = 1$, то мы будем говорить, что набор a **меньше** набора b $(a \prec b)$

Определение (Монотонная функция)**.** БФ $f(x_1, \dots x_n)$ называется монотонной, если $\forall$ соседних наборов a, b таких, что $a \prec b \implies f(a) \leq f(b)$

Замечание. Класс M является замкнутым.

Доказательство. $g, g_1, \dots g_k \in M, F(x_1, \dots, x_n) = g(g_1, \dots g_k)$ и рассмотрим два произвольных набора $a \prec b$. Пусть $c_1 = g_1(a), d_1 = g_1(b), \dots\ c_k = g_k(a), \dots d_k = g_k(b)$

$g_i \in M \implies c_i \leq d_i$

Если наборы $c = (c_1, \dots, c_k)$ и $d = (d_1, \dots, d_k)$ - соседние, то и $F(c) \leq F(d)$

В противном случае легко показать, что $\exists$ цепочка

$$c \prec e_1 \prec \dots \prec e_l \prec d$$

(то есть наши наборы сравнимы по определению Ашаева)

и $g(c) \leq g(d) \implies F(c) \leq F(d) \implies F \in M$ ▸

1.15 Класс линейных функций

Определение. БФ называется линейной, если ее полином Жегалкина линеен, т.е не содержит конъюнкции т.е его степень не выше 1.

Лемма 1.1. *Класс L является замкнутым.*

Доказательство. При подстановке линейных функций в линейную функцию не может появиться конъюнкции. $f(x_1, \dots, x_n) = a0 \oplus a_1(f_1(x_1, \dots, x_n) \dots \oplus a_m f_m(x_1, \dots, x_n) = a_0 \oplus a1(b_0^1 \oplus b_1^1 x_1 \dots \oplus b_n^1 x_n) \dots \dots \oplus a_m(b_0^m \oplus b_1^m x_1 \dots \oplus b_n^m x_n) = (a_0 \oplus a_1 b_0^1 \dots \oplus a_m b_0^m) \oplus (a_1 b_1^1 \oplus \dots \oplus a_m b_1^m) x_1 \oplus \dots \oplus (a_1 b_n^1 \oplus \dots \oplus a_m b_n^m) x_n$. ▸

1.16 Леммы о несамодвойственной, немонотонной, нелинейной функциях

Лемма 1.2 (о несамодвойственной функции)**.** *Если БФ $f(x_1, \dots, x_n)$ несамодвойственна, то замыкание класса $[f, \neg x]$ содержит тождественно ложную БФ 0 и тождественно истинную БФ 1.*

Доказательство. Так как f несамодвойственна, то существует набор $a_1, \dots, a_n$ значений аргументов такой, что $f(a_1, \dots, a_n) \neq \neg f(\neg a_1, \dots, \neg a_n)$
Так как БФ принимают только значения 0 и 1, то $f(a_1, \dots, a_n) = f(\neg a_1, \dots, \neg a_n)$
Составим функцию $g(x) = f(x^{a_1}, \dots, x^{a_n})$, где

$$x^a = \begin{cases} x & \text{если } a = 1 \\ \neg x & \text{если } a = 0 \end{cases}$$

Очевидно, что $g \in [f, \neg x]$, так как является их суперпозицией.
$g(0) = f(0^{a_1}, \dots, 0^{a_n}) = f(\neg a_1, \dots, \neg a_n)$, $g(1) = f(1^{a_1}, \dots, 1^{a_n}) = f(a_1, \dots, a_n)$,
$g(0) = g(1)$ - g - константа, g и $\neg g$ принимают значения 0 и 1 чтд. ▶

Лемма 1.3 (О немонотонной функции)**.** *Если $f(x_1, \dots, x_n)$ немонотонна, то $x' \in [f, 0, 1]$*

Доказательство. Из немонотонности f следует существование двух соседних наборов $a = (a_1, \dots, a_n) \prec (b_1, \dots, b_n) = b$ такие, что $f(a) > f(b)$. Б.О.О считаем, что они отличаются только в первой координате

$$a_1 = 0$$
$$b_1 = 1$$
$$a_i = b_i$$

$\lhd g(x, a_2, \dots, a_n) \in [f, 0, 1]$
$g(0) = f(a) = 1 \quad , g(1) = f(b) = 0 \implies g \equiv x'$ ▶

Лемма 1.4 (О нелинейной функции)**.** $f(x_1, \dots, x_n) \notin L \implies xy \in [f, 0, 1, x']$

Доказательство. $f(x_1, \dots, x_n) \notin L \implies$ полином Жегалкина функции f содержит конъюнкцию двух переменных x_1 и x_2
$\implies f(x_1, \dots, x_n) = x_1 x_2 h_{12}(x_3, \dots x_n) + x_1 h_1(x_3, \dots x_n) + h_0(x_3, \dots x_n)$
$f \notin L \implies h_{12} \neq 0 \implies \exists (a_3, \dots a_n) h_{12}(a_3, \dots a_n) = 1$
Подставим этот набор в ПЖ f:
$g(x_1, x_2) = f(x_1, x_2, a_3 \dots a_n) = x_1 x_2 h_{12}(a_3, \dots a_n) + x_1 h_1(a_3, \dots a_n) + h_0(a_3, \dots a_n)$
$h_i \in \{0, 1\} \implies \exists 8$ вариантов того, как выглядит полином Жегалкина

1. Система функций $[g, \neg, 0, 1]$ полна и содержит конъюнкцию
2. g - конъюнкция
3. $xy = g(x, y') \lor xy = g(x', y) \implies xy \in$замыкание

Т.к g выражается через $f(x_1, \dots x_n), 0, 1$, то конъюнкция также лежит в замыкании $[f, \neg, 0, 1]$

▶

1.17 Теорема Поста о полноте системы булевых функций

Теорема 1.4 (Теорема Поста)**.** *Система БФ является полной тогда и только тогда, когда она не лежит целиком ни в одном из классов Поста.*

Доказательство.

- $\Rightarrow$ Пусть все функции из 1 класса, б.о.о. они из T_0. Так как он замкнут, то замыкание этих функций не совпадает с $\mathcal{B} \implies$ набор не полон.

- $\Leftarrow$ Если набор $f_1 \dots f_k$ не содержится полностью ни в одном из классов Поста, то существуют БФ $f_0 \notin T_0, f_1 \notin T_1, f_S \notin S, f_M \notin M, f_L \notin L$

  Заменим все переменные этих функций на x и получим функцию одного аргумента

  $g_0(x) = f_0(x, x, \dots, x), g_1(x) = f_1(x, x, \dots, x), g_S(x) = f_S(x, x, \dots, x), g_M(x) = f_M(x, x, \dots, x), g_L(x) = f_L(x, x, \dots, x).$

Все БФ из замыкания этих функций $G \in [f_1, \dots, f_k]$ (переименовали переменные). Докажем полноту набора $[G]$ через полноту $[\neg x, xy]$:

Для $g_0, g_1 : g_0(0) = 1, g_1(1) = 0$

$g_0(1)$	$g_1(0)$	
0	0	$g_0 \equiv \neg x, g_1 \equiv 0$
0	1	$g_0 \equiv \neg x, g_1 \equiv \neg x$
1	0	$g_0 \equiv 1, g_1 \equiv 0$
1	1	$g_0 \equiv 1, g_1 \equiv \neg x$

1. $[G] \ni \neg x, 0, 1$ по лемме о нелинейной функции содержит xy
2. $[G] \ni \neg x \implies$ по лемме о несамодвойственной функции содержит 0 и 1 $\implies$ по лемме о нелинейной функции содержит xy
3. $[G] \ni 0, 1 \implies$ по лемме о немонотонной функции содержит $\neg x \implies$ по лемме о нелинейной функции содержит xy
4. $[G] \ni \neg x, 0, 1$ по лемме о нелинейной функции содержит xy

▶

Предполные классы

Определение. Предполным классом K называется неполный класс, при добавлении любой функции, которая не принадлежит ему, получается класс полный.

Утверждение. Предполный класс является замкнутым.

Доказательство. Пусть класс A не замкнут. Значит, найдется функция $f \in [A] \setminus A$. Получаем: $[A \cup f] = [A]$.

$A \neq \mathcal{B}$, но при добавлении f получаем полную систему (по определению) $\implies$ противоречие. Значит, A — замкнутый класс. ▶

Утверждение (Максимальные замкнутые классы)**.** Классы Поста являются максимальными замкнутыми классами (предполными) и других нет.

Доказательство.

- Докажем максимальность T_0. Пусть он не максимален, т.е существует замкнутый класс A такой, что $T_0 \subset A \subset \mathcal{B}$, тогда $[T_0] \subseteq A$

  Пусть $f_0 \in A \setminus T_0$, тогда $g(x) = f(x, \dots, x) \notin T_0$. Если $g(1) = 0, g \equiv \neg(x)$, иначе $g \equiv 1$. Так как $T_0 \ni 0, xy$, немонотонные и несамодвойственные функции, $[T_0, f] = \mathcal{B}$, а это противоречит $[T_0, f] \subseteq A$.

- Докажем максимальность T_1. Пусть он не максимален, т.е существует замкнутый класс A такой, что $T_1 \subset A \subset \mathcal{B}$, тогда $[T_1] \subseteq A$

  Пусть $f_1 \in A \setminus T_1$, тогда $g(x) = f(x, \dots, x) \notin T_1$. Если $g(0) = 1, g \equiv \neg(x)$, иначе $g \equiv 0$. Так как $T_1 \ni 1, xy$, немонотонные и несамодвойственные функции, $[T_1, f] = \mathcal{B}$, а это противоречит $[T_1, f] \subseteq A$.

- K = S. Пусть $f(x_1, \dots, x_n) \notin S$. $x' \in S$, по лемме о несамодвойственной функции $0, 1 \in [f, x'] \subseteq [S, f]$

  Выберем в S нелинейную функцию, например, $g = xy + yz + xz$. По лемме о нелинейной функции $xy \in [g, 0, 1, x'] \subseteq [S, f] \implies \{xy, x'\} \in [S, f]$

  $\mathcal{B} = [xy, x'] \subseteq [S, f] = B$

- K = M, $f(x_1, \dots, x_n) \notin M$. По лемме о немонотонной функции $0, 1 \in M$; $x' \in [f, 0, 1] \subseteq [M, f]$

  $\{xy, x'\} \in [M, f] \implies \mathcal{B} = [xy, x'] \subseteq [M, f] = B$

- K = L, $f(x_1, \dots, x_n) \notin L$. По лемме о нелинейной функции $x', 0, 1 \in L$; $xy \in [0, 1, x', f] \subseteq [L, f]$

  $\{xy, x'\} \in [L, f] \implies \mathcal{B} = [xy, x'] \subseteq [Lf] = B$

▶

1.18 Релейно-контактные схемы: определение, примеры, функция проводимости. Анализ и синтез РКС (умение решать задачи)

2 Логика высказываний

2.1 Парадоксы в математике. Парадоксы Г. Кантора и Б. Рассела

2.2 Логическое следование в логике высказываний. Проверка логического следования с помощью таблиц истинности и эквивалентных преобразований.

2.3 Понятия прямой теоремы, а также противоположной, обратной и обратной к противоположной теорем

2.4 Понятия необходимых и достаточных условий

2.5 Формальные системы. Выводы в формальных системах. Свойства выводов

Определение. Формальная система состоит из четырех элементов:

1. алфавит (некоторое множество)
2. набор формул (множество слов, отобранных с помощью некоторых правил)
3. набор аксиом (множество формул, отобранных по некоторым правилам)
4. набор правил вывода вида $\frac{\phi_1,\ldots,\phi_n}{\Psi}$ (из формул $\phi_1, \ldots, \phi_n$ следует формула Ψ)

Определение. Вывод формулы ϕ из множества формул Γ в формальной системе — это конечная последовательность формул $\phi_1, \ldots, \phi_n = \phi$, в которой каждая ϕ_i

- либо аксиома формальной системы
- либо принадлежит множеству Γ (является гипотезой)
- либо получена из предыдущих формул по одному из правил вывода.

Определение. Формула ϕ выводится из множества формул Γ (обозначение:$\Gamma \vdash \phi$), если существует вывод ϕ из Γ.

Утверждение (Свойства выводов).

1. Если $\Gamma \vdash \phi$, то существует конечное подмножество $\Gamma_0 \subseteq \Gamma$ такое, что $\Gamma_0 \vdash \phi$.
2. Если $\Gamma \vdash \phi$ и $\Gamma \subseteq \Delta$, то $\psi \vdash \Delta$.
3. (транзитивность выводимости) Если $\Gamma \vdash \Delta$ (т.е. все формулы из Δ выводятся из Γ) и $\Delta \vdash \phi$, то и $\Gamma \vdash \phi$.

Доказательство.

1. $\Gamma \vdash \phi : \exists \phi_1, \ldots, \phi_n = \phi$. Так как вывод конечный, то можно найти конечное множество гипотез, оно и будет Γ_0
2. Есть вывод $\Gamma \vdash \phi : \phi_1, \ldots, \phi_n = \phi$
   Гипотезы $\Gamma \subseteq$ гипотезы из $\Delta \implies \Delta \vdash \phi$
3. $\Gamma \vdash \Delta, \Delta \vdash \psi$
   $\psi_{i1}, \ldots, \psi_{ik} = \psi_i$ - вывод ψ_i из Γ $[\Delta = \bigcup_i \psi_i]$
   $\theta_1, \ldots, \theta_m = \phi$ - вывод $\Delta \vdash \psi$
   Построим единую последовательность $\psi_{i1}, \ldots, \psi_{ik}, \theta_1, \ldots, \theta_m = \phi$ (проходим по всевозможным ψ_i)

▶

2.6 Исчисление высказываний (ИВ) Гильберта. Примеры выводов

Определение. Исчисление высказываний - конкретная формальная система на базе логики высказываний.

1. алфавит = символы переменных, отрицание, импликация, скобки
2. формулы ИВ - формулы языка ЛВ, использующие только отрицание и импликацию
3. (схемы аксиом) аксиомы ИВ:

   A_1 $A \to (B \to A)$
   A_2 $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
   A_3 $(B' \to A') \to ((B' \to A) \to B)$
4. силлогизм: $\frac{A, A \to B}{B}$ **modus ponens**

Пример. $A, A \to B, \vdash B$

1. A
2. $A \to B$
3. B (MP 1, 2)

Пример. $A \vdash B \to A$

1. (A_1) $A \to (B \to A)$
2. A
3. $B \to A$ (MP 1, 2)

Замечание. Если $\Gamma = \varnothing$, то пишем $\vdash \phi(\phi$ доказуема)

2.7 Теорема о дедукции для ИВ

Теорема 2.1. Γ - *множество формул, A, B - формулы ИВ. Тогда* $\Gamma, A \vdash B \Leftrightarrow \Gamma, \vdash A \to B$

Доказательство. $\Leftarrow$ $\Gamma \vdash A \to B$, строим $\Gamma, A \vdash B$

$\Gamma, A \vdash A, A \to B$ и $A, A \to B \vdash B(MP)$, По транзитивности получаем требуемое.

$\Rightarrow$ доказывается индукцией по длине вывода B из Γ, A.

1. Если этот вывод — длины 1, то B — аксиома или гипотеза. Если B — аксиома, то имеем вывод A → B (из ∅):
   (a) B (аксиома)
   (b) B → (A → B) (аксиома A1)
   (c) A → B (1,2, MP)
2. Если B ∈ Γ, то имеем такой же вывод A → B из Γ:
   (a) B (гипотеза)
   (b) B → (A → B) (аксиома A1)
   (c) A → B (1,2, MP)
3. Если B = A, то A → B = A → A. Но ⊢ A → A:
   (a) (A_2) $(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$
   (b) (A_1) $A \to ((A \to A) \to A)$
   (c) (MP 1, 2) $(A \to (A \to A)) \to (A \to A)$
   (d) (A_1) $A \to (A \to A)$
   (e) (MP 3, 4)$A \to A$
4. Предположим теперь, что Γ, A ⊢ B и утверждение (⇒) верно для всех более коротких выводов, т.е. для всех C, если Γ, A ⊢ C и вывод C из Γ, A короче, чем вывод B, то Γ ⊢ A → C.

Докажем, что $\Gamma \vdash A \to B$.

Рассмотрим вывод из Г, А, который заканчивается формулой В. При этом В может оказаться аксиомой или гипотезой (тогда все предыдущие формулы для доказательства В не нужны). Но в этом случае $\Gamma \vdash A \to B$ по (1)–(3). Остается случай, когда В получается по МР из формул С, $C \to B$, причем $\Gamma, A \vdash C$ и $\Gamma, A \vdash C \to B$ с более короткими доказательствами. По предположению индукции имеем

(*) $\Gamma \vdash A \to C, A \to (C \to B)$. С другой стороны, (**) $A \to C, A \to (C \to B) \vdash A \to B$:

1. $A \to C$ (гипотеза)
2. $A \to (C \to B)$ (гипотеза)
3. $(A \to (C \to B)) \to ((A \to C) \to (A \to B))$ (аксиома А2)
4. $(A \to C) \to (A \to B)$ (2,3, МР)
5. $A \to B$ (1,4, МР)

Из (*), (**) по транзитивности получаем $\Gamma \vdash A \to B$.

►

2.8 Теорема о полноте и непротиворечивости ИВ

2.9 ИВ Генцена, его полнота

2.10 Метод резолюций для логики высказываний (без обоснования корректности)

3 Логика предикатов

3.1 Понятие предиката и операции, их представления, примеры

Определение. n-местный предикат на множестве А - это отображение вида $P : A^n \to \{0, 1\}$

Определение. n-местная операция на множестве А - это отображение вида $f : A^n \to A$

Предикат можно задать как множество тех аргументов, на которых он является истинным

Пример. $P = \{1, 3\} : P = 1 \Leftrightarrow x = 1 \vee x = 3$

Пример. $Q = \{(1, 2), (3, 4), (5, 6)\}$

Способы задания:

1. описательный
2. множество (отношения)
3. таблица (истинности)
4. графы

   для предиката $P(x, y)$ ребро (x, y) обозначает $P(x, y) = 1$

   для операции $f(x)$ дуга (x, y) обозначает $y = f(x)$

3.2 Сигнатура, интерпретация сигнатуры на множестве, алгебраические системы

Определение. Сигнатура - набор предикатных, функциональных и константных символов с указанием местностей

Пример. $\sigma = \{P^{(1)}, Q^{(2)}, f^{(1)}, g^{(2)}, c\}$

Определение. Две сигнатуры считаем *равными*, если в них одинаковое кол-во символов каждого сорта и местности соответствующих символов равны

Определение. Интерпретация сигнатуры σ на множестве А - это отображение, которое

1. каждому n-местному предикатному символу $P^{(n)} \in \sigma$ сопоставляет n-местный предикат на А
2. каждому n-местному функциональному символу $f^{(n)} \in \sigma$ сопоставляет n-местную операцию на А
3. каждому константному символу сопоставляет элемент множества А

Определение. Алгебраическая система - набор, состоящий из множества А, сигнатуры σ и интерпретации σ на А. Множество А называют основным множеством системы ($\mathfrak{a} =< A, \sigma >$)

3.3 Язык логики предикатов, термы, формулы логики предикатов

Зафиксируем сигнатуру σ. Алфавит логики предикатов сигнатуры σ — это множество
$\sigma_{АЛП} = \sigma \cup \{x_1, x_2 \ldots, \&, \vee, \rightarrow, \leftrightarrow, \neg, \forall, \exists, (,), =, ,\}$

Определение. Терм - слово алфавита логики предикатов, построенное по правилам:

1. символ переменной - терм
2. константный символ - терм
3. если $t_1, \ldots t_n$ - термы, $f^{(n)} \in \sigma$, то и $f(t_1, \ldots, t_n)$ - терм

Определение. Атомарная формула сигнатуры σ - это слово одного из двух видов:

1. $t_1 = t_2$, где t_1, t_2 - термы
2. предикат $P(t_1, \ldots, t_n), P^{(n)} \in \sigma, t_1, \ldots t_n$ - термы

Определение. Формула ЛП сигнатуры σ - слово, построенное по правилам:

1. атомарная формула - формула
2. если ϕ_1 и ϕ_2 - формулы, то слова $(\phi_1 \& \phi_2)$, $(\phi_1 \vee \phi_2), (\phi_1 \leftrightarrow \phi_2), (\phi_1 \rightarrow \phi_2), \neg\phi_1$ тоже формулы
3. если ϕ - формула, то слова $(\forall x \phi)$ и $(\exists x \phi)$ тоже формулы

3.4 Свободные и связанные переменные. Замкнутые формулы

Определение. Вхождение переменной x в формулу ϕ **связанное**, если x попадает в область действия квантора $\exists x / \forall x$, в противном случае вхождение x **свободное**

Определение. Переменная x **свободна** в формуле ϕ, если есть хотя бы одно свободное вхождение x в ϕ, в противном случае она **связанная**

Определение. Формула замкнутая, если она не содержит свободных переменных.

3.5 Истинность формул на алгебраической системе

Каждый терм $t(x_1, \ldots, x_n)$ определяет в системе $\mathfrak{a}$ функцию $t_{\mathfrak{a}} : A^n \rightarrow A$ следующим образом: в терме все функциональные и константные символы заменяются на их интерпретации в системе A, после чего вычисляется полученная суперпозиция от входных аргументов.

Пусть также $\phi(x_1 \ldots, x_n)$ — формула со свободными переменными $x_1, \ldots, x_n$. Определим понятие истинности формулы ϕ на наборе элементов $a_1, \ldots a_n \in \mathfrak{a}$ в алгебраической системе $\mathfrak{a}$ (обозначение: $\mathfrak{a} \models \phi(a_1, \ldots a_n)$) следующим образом.

Определение.

1. Пусть ϕ имеет вид $t_1 = t_2$. Тогда $A \models \phi(a_1, \ldots a_n) \Leftrightarrow t_{1A}(a_1, \ldots a_n) = t_{2A}(a_1, \ldots a_n)$ (здесь t_{iA} — функция, определяемая термом t_i в системе A).
2. Пусть ϕ имеет вид $P(t_1, \ldots, t_k)$. Тогда $A \models \phi(a_1, \ldots a_n) \Leftrightarrow P_A(t_{1A}(a_1, \ldots a_n), \ldots, t_{kA}(a_1, \ldots a_n)) = 1$, где P_A — интерпретация предикатного символа P в системе A.
3. Пусть ϕ имеет вид $(\phi_1 \& \phi_2), (\phi_1 \vee \phi_2), (\phi_1 \rightarrow \phi_2), (\phi_1 \leftrightarrow \phi_2), \neg\phi_1$. Тогда истинность формулы ϕ определяется по значениям $\phi_1(a_1, \ldots a_n)$ и $\phi_2(a_1, \ldots a_n)$ по таблицам истинности логических связок.
4. Пусть $\phi(x_1 \ldots, x_n)$ имеет вид $(\forall x \phi(x, x_1, \ldots x_n))$. Тогда $A \models \phi(a_1, \ldots a_n) \Leftrightarrow$ для всех элементов $b \in A$ выполнено $A \models \phi(b, a_1, \ldots a_n)$.
5. Пусть $\phi(x_1 \ldots, x_n)$ имеет вид $(\exists x \phi(x, x_1, \ldots x_n))$. Тогда $A \models \phi(a_1, \ldots a_n) \Leftrightarrow$ для некоторого элемента $b \in A$ выполнено $A \models \phi(b, a_1, \ldots a_n)$.

Определение. Формула $\phi(x_1, \ldots, x_n)$ сигнатуры σ тождественно истинная (ложна) в алгебраической системе $A =< A, \sigma >$, если для всех наборов элементов $a_1 \ldots a_n \in A$ выполнено $A \models \phi(a_1 \ldots a_n) (A \not\models \phi(a_1 \ldots a_n))$.

Определение. Формула $\phi(x_1, \ldots, x_n)$ выполнима в алгебраической системе $A =< A, \sigma >$, если для хотя бы одного набора элементов $a_1 \ldots a_n \in A$ выполнено $A \models \phi(a_1 \ldots a_n)$.

Определение. Формула ϕ сигнатуры σ тождественно истинная (ложна), если ϕ тождественно истинна (ложна) во всех алгебраических системах сигнатуры σ.

Определение. Формула ϕ сигнатуры σ выполнима, если ϕ выполнима хотя бы в одной алгебраической системе сигнатуры σ.

3.6 **Изоморфизм систем. Теорема о сохранении значений термов и формул в изоморфных системах. Автоморфизм**

3.7 **Элементарная теория алгебраической системы. Элементарная эквивалентность систем. Связь понятий изоморфизма и элементарной эквивалентности**

3.8 **Выразимость свойств в логике предикатов. Умение записать формулой различные свойства систем и элементов систем**

3.9 **Эквивалентность формул логики предикатов**

3.10 **Тождественно истинные (ложные) и выполнимые формулы**

3.11 **Пренексный вид формулы**

3.12 **Основные эквивалентности логики предикатов**

3.13 **Классы формул $\Sigma_n, \Pi_n, \Delta_n$. Соотношения между классами**

3.14 **Нормальная форма Сколема, ее построение (на примерах)**

3.15 **Проверка существования вывода методом резолюций (алгоритм)**

3.16 **Логическое следование в логике предикатов**

3.17 **Исчисление предикатов (ИП) Гильберта. Свойства выводов**

3.18 **Теория. Модель теории**

3.19 **Непротиворечивая теория. Полная теория. Свойства непротиворечивых и полных теорий**

3.20 **Теорема о существовании модели (без доказательства)**

3.21 **Теорема о связи выводимости и противоречивости**

3.22 **Теоремы о корректности и полноте ИП**

3.23 **Теорема компактности**

3.24 **Аксиоматизируемые и конечно аксиоматизируемые классы. Конечно аксиоматизируемые теории**

3.25 **Обоснование нестандартного анализа (построение алгебраической системы, элементарно эквивалентной полю вещественных чисел, содержащей бесконечно малые элементы)**

3.26 **Метод резолюций для логики предикатов (без доказательства корректности)**