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

1.4 Эквивалентные формулы. Основные эквивалентности теории булевых функций

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

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

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

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

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

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

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

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

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

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 $\Phi(x_1, \ldots, x_n)$ 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 $a_1, \ldots, a_n \in \{0, 1\}$ и подставим в формулы:

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

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

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

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

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

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 $x_1, \ldots, x_n$ - это конъюнкт вида $x_1^{a_1} \wedge \cdots \wedge x_n^{a_n}$, где $(a_1, \ldots, a_n) \in \{0, 1\}^n$.

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

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 $x_1, \ldots, x_n$ - это дизъюнкция совершенных конъюнктов от $x_1, \ldots, x_n$, в которой нет попарно эквивалентных слагаемых

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

Теорема 1.3 (о существовании и единственности СДНФ)**.** *Любая булева функция $f(x_1, \ldots, x_n) \neq 0$ 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 $f(x_1, \ldots, x_n) \neq 0$

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

2. Единственность. Пусть, у функции $f(x_1, \ldots, x_n) \neq 0$ 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 $x_1^{a_1} \ldots x_n^{a_n}$. По лемме о совершенных конъюнктах это слагаемое истинно при $(x_1, \ldots, x_n) = (a_1, \ldots, a_n)$. Тогда и вся дизъюнкция $\Phi(a_1, \ldots, a_n) = 1$, а в силу эквивалентности формул и $\Psi(a_1, \ldots, a_n) = 1$

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

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

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

2. Два совершенных конъюнкта от перменных $x_1, \ldots, x_n$ 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: $\Phi(x_1, \ldots, x_n) \equiv \Phi(y \vee \overline{y}) \equiv \Phi \wedge y \vee \Phi \wedge \overline{y}$

   СКНФ: $\Phi(x_1, \ldots, x_n) \equiv \Phi \vee y \wedge \overline{y} \equiv (\Phi \vee y) \wedge (\Phi \vee \overline{y})$
4. Вычеркиваем повторяющиеся слагаемые(множители).

1.8 Минимизация нормальных форм (карты Карно)

Определение. ДНФ Φ булевой функции называется минимальной, если в любой ДНФ этой функции количество литер не меньше, чем в Φ

Определение. Карта Карно функции $f(x_1, \ldots, x_n)$ - это двумерная таблица построенная следующим образом.

1. Разделим набор переменных $x_1, \ldots, x_n$ На две части: $x_1, \ldots, x_k$ и $x_{k+1}, \ldots, x_n$
2. Строкам таблицы соответсвуют всевозможные наборы нзачений переменных $x_1, \ldots, x_k$, колонкам - $x_{k+1}, \ldots, x_n$. При этом наборы в двух соседних строках/колонках должны отличаться не более, чем одним значением. Крайние строки/колонки считаются соседними
3. В ячейки заносятся значения функции $f(x_1, \ldots, x_n)$ на соответсвующих наборах.

Замечание. Алгоритм построения минимальной ДНФ с помощью карт Карно

1. Строим карту Карно функции f
2. В карте находим покрытие всех ячеек со значением 1 прямоугольникам со свойствами:
   (a) Длины сторон прямоугольника - $2^k, k \geq 0$
   (b) каждый прямоугольник содержит только 1
   (c) каждая ячейка с 1 покарыта прямоугольником максимальной площади
   (d) количество прямоугольников минимально
3. По кааждому прямоугольнику выписываем конъюнкт. Конъюнкт образуют литеры, значения которых в прямоугольнике не меняются

1.9 Полином Жегалкина, его существование и единственность. Алгоритм построения

Определение. Моном от перменных $x_1, \ldots, x_n$ - это либо 1, либо конъюнкт вида $x_{i_1} \cdot \cdots \cdot x_{i_k}$, где x_{i_k} - переменная из списка $x_1, \ldots, x_n$, без повторяющихся множителей

Определение. Полином Жегалкина от переменных $x_1, \ldots, x_n$ - это либо 0, либо сумма мономов от переменных $x_1, \ldots, x_n$ без эквивалентных слагаемых

Теорема 1.4 (о существовании и единственности полинома Жегалкина)**.** *Любая булева функция может быть определена полиномом Жегалкина. Полином Жегалкина буленвой функции единственный с точностью до перестановок слагаемых и множителей*

Доказательство. • (Существование) Т.к. для любой булевой функции можно определить ДНФ, доказывает, что любую булеву функцию можно выразить через $\wedge, \vee, '$. Выразим $\wedge, +, 1$ через $\wedge, \vee, '$.

$$\overline{x} = x + 1$$

$$x \vee y = \overline{\overline{x \vee y}} = \overline{\overline{x}\overline{y}} = (x+1)(y+1) + 1 = xy + x + 1 + 1 = xy + x + y.$$

• (Единственность)

Количество булевых функций от n переменных 2^{2^n}

Найдем количество полиномов Жегалкина от $x_1, \ldots, x_n$

Сопоставим моному упорядоченный набор чисел $(a_1, .., a_n) a_i \in \{0, 1\}$, по принципу: $a_i = 1 \leftrightarrow$ переменная x_i в моному есть. Это соответствие является биекцией. Таким образом, мономов от n переменных столько же, сколько наборов вида $(a_1, \ldots, a_n), a_i \in \{0, 1\}$, а их 2^n штук.

Произвольный полином Жегалкина от n переменных можно представить в виде: $p(x_1, \ldots, x_n) = b_1 M_1 + \cdots + b_k M_k, k = 2^n$, где $b_j \in \{0, 1\}$, а $M_1, \ldots, M_k$ - все мономы от $x_1, \ldots, x_n$.

Сопоставим полиному p набор коэффициентов $(b_1, \ldots, b_k), b_j \in \{0, 1\}$.

Это снова биекция, поэтому полиномов столько же сколько таких наборов, а их $2^k = 2^{2^n}$

Получили, что количество полиномов Жегалкина от n переменных равно количеству булевых функций от n переменных.

Допустим теперь, что у какой-то булевой функции f два разных полинома. Тогда для какой-то другой функции g полинома не хватит. Но это противоречит тому, что каждую булеву функцию можно представить полиномом Жегалкина. ▶

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 K), если ее замыкание равно классу всех булевых функций(классу K)

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

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 $g(x_1, \ldots, x_n)$ называется двойственной к БФ $f(x_1, \ldots, x_n)$ (обозначается g = f*), если $g(x_1, \ldots, x_n) = f'(x_1', \ldots, x_n')$.

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

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

1.14 Класс монотонных функций

Определение. Назовем два набора из 0 и 1 $a = (a_1, \ldots a_n), b = (b_1, \ldots b_n)$ **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 $f(x_1, \ldots x_n)$ 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. $g, g_1, \ldots g_k \in M, F(x_1, \ldots, x_n) = g(g_1, \ldots g_k)$ и рассмотрим два произвольных набора $a \prec b$. Пусть $c_1 = g_1(a), d_1 = g_1(b), \ldots\ c_k = g_k(a), \ldots d_k = g_k(b)$

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

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

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

$$c \prec e_1 \prec \cdots \prec e_l \prec d$$

(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. $f(x_1, \ldots, x_n) = a0 \oplus a_1(f_1(x_1, \ldots, x_n) \cdots \oplus a_m f_m(x_1, \ldots, x_n) = a_0 \oplus a1(b_0^1 \oplus b_1^1 x_1 \cdots \oplus b_n^1 x_n) \ldots \cdots \oplus a_m(b_0^m \oplus b_1^m x_1 \cdots \oplus b_n^m x_n) = (a_0 \oplus a_1 b_0^1 \cdots \oplus a_m b_0^m) \oplus (a_1 b_1^1 \oplus \cdots \oplus a_m b_1^m) x_1 \oplus \cdots \oplus (a_1 b_n^1 \oplus \cdots \oplus a_m b_n^m) x_n$. ▶

1.16 Леммы о несамодвойственной, немонотонной, нелинейной функциях

Лемма 1.2 (о несамодвойственной функции). *Если БФ $f(x_1, \ldots, x_n)$ 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 $a_1, \ldots, a_n$ значений аргументов такой, что $f(a_1, \ldots, a_n) \neq \neg f(\neg a_1, \ldots, \neg a_n)$
Так как БФ принимают только значения 0 и 1, то $f(a_1, \ldots, a_n) = f(\neg a_1, \ldots, \neg a_n)$
Составим функцию $g(x) = f(x^{a_1}, \ldots, x^{a_n})$, 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.
$g(0) = f(0^{a_1}, \ldots, 0^{a_n}) = f(\neg a_1, \ldots, \neg a_n)$, $g(1) = f(1^{a_1}, \ldots, 1^{a_n}) = f(a_1, \ldots, a_n)$,
$g(0) = g(1)$ - g - константа, g и $\neg g$ принимают значения 0 и 1 чтд. ▶

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

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

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

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

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

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

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

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

▶

1.17 Теорема Поста о полноте системы булевых функций

Теорема 1.5 (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 $f_1 \ldots f_k$ 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

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

Все БФ из замыкания этих функций $G \in [f_1, \ldots, f_k]$ (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 $g(x) = f(x, \ldots, x) \notin T_0$. 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 $g(x) = f(x, \ldots, x) \notin T_1$. 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 $f(x_1, \ldots, x_n) \notin S$. $x' \in S$, 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, $f(x_1, \ldots, x_n) \notin M$. 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, $f(x_1, \ldots, x_n) \notin L$. 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)

Определение. Реле это некоторое устройство, которое может находиться в одном из двух возможных состояний: включенном и выключенном.

Пример. Примеры реле: различные выключатели, термодатчики, датчики движения и т.п.

Реле используются в построении различных электрических схем. Включение или выключение реле приводит к появлению или исчезновению тока на определённых участках электрической схемы.

Пусть S некоторая электрическая схема, содержащая реле $x_1, \dots, x_n$. Со схемой S можно связать функцию проводимости f_S, которая равна 1, если схема проводит ток при заданном состоянии реле (и f_S равна 0 в противном случае). Возникает вопрос: а какие аргументы имеет функция f_S? Для определения аргументов f_S мы будем рассматривать каждое реле x_i как переменную, принимающую значения из множества $\{0, 1\}$ с очевидной интерпретацией: $x_i = 0$, если реле выключено, и $x_i = 1$, если реле включено.

Таким образом функция проводимости $f_S(x_1, \dots, x_n)$ становится булевой функцией, зависящей от текущего состояния своих реле.

1. цепь замкнута - $f_S = 1$
2. цепь не замкнута $f_S = 0$
3. последовательное соединение $f_S(x, y) = xy$
4. параллельное соединение $f_S(x, y) = x \vee y$

Задачи, связанные с релейно-контактными схемами можно подразделить на две большие группы:

1. дана схема, нужно построить более простую схему с такой же функцией проводимости
2. нужно построить схему по описанию её функции проводимости.

2 Логика высказываний

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

Утверждение (Рассел)**.** Множество M будем называть нормальным, если оно не принадлежит самому себе как элемент. Например, множество кошек нормально, поскольку множество кошек не является кошкой. А вот каталог каталогов по-прежнему останется каталогом, поэтому множество каталогов, не является нормальным. Рассмотрим теперь множество B, составленное из всевозможных нормальных множеств. Формально множество B определяется так:

$x \in B \Leftrightarrow x \notin x$ (2)

Возникает вопрос: будет ли B принадлежать самому себе как элемент? И тут возникает парадокс: дело в том, что если вместо x из формулы (2) подставить B, то возникнет явное противоречие $B \in B \Leftrightarrow B \notin B$.

Утверждение (Кантор?)**.** Предположим, что множество всех множеств $V = \{x \mid x = x\}$ существует. В этом случае справедливо $\forall x \forall T (x \in T \to x \in V)$, то есть всякое множество Tявляется подмножеством V. Но из этого следует $\forall T \ |T| \leqslant |V|$ — мощность любого множества не превосходит мощности V.

Но в силу аксиомы множества всех подмножеств, для V, как и любого множества, существует множество всех подмножеств$\mathcal{P}(V)$, и по теореме Кантора $|\mathcal{P}(V)| = 2^{|V|} > |V|$, что противоречит предыдущему утверждению. Следовательно, V не может существовать, что вступает в противоречие с «наивной» гипотезой о том, что любое синтаксически корректное логическое условие определяет множество, то есть что $\exists y \forall z (z \in y \leftrightarrow A)$ для любой формулы A, не содержащей y свободно.

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

Определение. Интерпретация переменных - это отображение вида $\alpha : \{x, x_1, \dots, x_n\} \to \{0, 1\}$. Задать интерпретацию - приписать j-той переменной значение 0, 1

Если Φ - формула, а α - интерпретация, то Φ^α - значение формулы, когда вместо x_i подставили $\alpha(x_i)$

Первый способ определить математическое понятие доказательства - логическое следование.

Определение. Γ - множество формул, Φ - формула логики высказываний. Формула Φ логически следует из Γ ($\Gamma \models \Phi$), если для любой интерпретации α_k верно - если истинны все формулы из Γ при этой интерпретации, то истинна и Φ.

$\forall\alpha(\forall\psi \in \Gamma\ \psi^\alpha = 1) \implies \Phi^\alpha = 1$

Свойства логического следования

1. $\Phi \models \Psi, \Psi \models \Theta \implies \Phi \models \Theta$
2. Γ, Δ - множество формул, Φ - формула. Если $\forall\psi \in \Delta\ \Gamma \models \psi$ $[\Gamma \models \Delta]$ $\&\Delta \models \Phi$, то $\Gamma \models \Phi$
3. Если $\Gamma \models \Phi, \Gamma \subseteq \Delta, \implies \Delta \models \Phi$
4. $\models \Phi \implies \Phi \equiv 1$
5. $\Phi_1, \dots, \Phi_n \models \Phi_1, \& \dots, \&\Phi_n$ &
   $\Phi_1, \& \dots, \&\Phi_n \models \Phi_1 \dots \Phi_n$
6. $\Gamma, \Phi \models \Psi \Leftrightarrow \Gamma \models \Phi \to \Psi$
7. Если $\Gamma = \{\Phi_1, \dots, \Phi_n\}$ - конечное, то $\Gamma \models \Phi \Leftrightarrow \Phi_1, \& \dots, \&\Phi_n \to \Phi \equiv 1$

Доказательство. 1. Следует из 2 $[\Delta = \{\Psi\}, \Gamma = \{\Phi\}]$

2. $\Gamma \models \Delta : \forall\alpha$ - интерпретация $\forall\Psi \in \Delta[(\forall\theta \in \Gamma \quad \theta^\alpha = 1) \implies \Psi^\alpha = 1]$
   $\Delta \models \Phi : \forall\alpha$ - интерпретация $[(\forall\Psi \in \Delta \quad \Psi^\alpha = 1) \implies \Phi^\alpha = 1]$
   $(\forall\theta \in \Gamma \quad \theta^\alpha = 1) \implies \forall\Psi \in \Delta \quad \Psi^\alpha = 1 \implies \Phi^\alpha = 1$
   $\implies \Gamma \models \Phi$
   [тупо пишем условие]
3. $\Gamma \models \Phi \implies \Phi : \forall\alpha[(\forall\Psi \in \Gamma \quad \Psi^\alpha = 1) \implies \Phi^\alpha = 1]$
   $\Gamma \subseteq \Delta : \forall\Psi \in \Delta \quad \Psi^\alpha = 1 \implies \forall\Psi \in \Gamma \quad \Psi^\alpha = 1 \implies \Phi^\alpha = 1$
4. $\models \Phi \Leftrightarrow \forall\alpha(\forall\Psi \in \varnothing \quad \Psi^\alpha = 1) \to \Phi^\alpha = 1 \implies \forall\alpha \quad \Phi^\alpha = 1 \implies \Phi \equiv 1$
5. α - инт., тогда $(\forall\Psi \in \{\Phi_1, \dots, \Phi_n\}\Psi^\alpha = 1) \Leftrightarrow (\Phi_1, \dots, \Phi_n)^\alpha = 1 \implies \Phi_1, \dots, \Phi_n \models \Phi_1, \& \dots, \&\Phi_n$. Обратное аналогично.
6. $\Rightarrow$
   $$\forall\alpha\text{- инт.}[(\forall\theta \in \Gamma \quad \theta^\alpha = 1 \quad \& \quad \Phi^\alpha = 1) \implies \Psi^\alpha = 1] \tag{*}$$
   пусть $\alpha : (\forall\theta \in \Gamma \quad \theta^\alpha = 1)$
   (a) $\Phi^\alpha = 1$, тогда из (*) $\Psi^\alpha = 1(\Phi \to \Psi)^\alpha = 1$
   (b) $\Phi^\alpha = 0 \implies (\Phi \to \Psi) = 1 \implies$
   $(\Phi \to \Psi)^\alpha = 1$

   $\Leftarrow$ $\Gamma \models \Phi \to \Psi$:
   $\alpha : (\forall\theta \in \Gamma \quad \theta^\alpha = 1) \implies (\Phi \to \Psi)^\alpha = 1$
   Из истинности всех формул из Γ следует истинность импликации, а если добавить еще и истинность Φ при той же интерпретации, то из этого будет следовать истинность посылки, то есть Ψ.
7. Следует из п.4-п.6

►

Проверять логическое следование можно при помощи таблиц истинности и эквивалентных преобразований, пользуясь 7 свойством (проверить, является ли импликация тождественно истинной функцией или нет).

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

Многие математические теоремы имеют структуру, выражаемую формулой $X \to Y$. Утверждение X называется условием теоремы, а утверждение Y — ее заключением. Далее, если некоторая теорема имеет форму $X \to Y$, утверждение $Y \to X$ называется **обратным** для данной теоремы. Это утверждение может быть справедливым, и тогда оно называется теоремой, **обратной** для теоремы $X \to Y$, которая, в свою очередь, называется **прямой** теоремой.

Для теоремы, сформулированной в виде импликации $X \to Y$, кроме обратного утверждения $Y \to X$ можно сформулировать противоположное утверждение. Им называется утверждение вида $\neg X \to \neg Y$. Утверждение, противоположное данной теореме, может быть также теоремой, т. е. быть истинным высказыванием, но может таковым и не быть.

Теорема, обратная противоположной: $\neg X \to \neg Y$ (контрапозиция).

Утверждение. $A \to B \models B' \to A'$
$A \to B, B \to A \models B' \to A', A' \to B'$

1. Из прямого следует противоположное обратному
2. Из прямого утверждения в общем случае не следует обратное и противоположное
3. Если одновременно истинно и прямое, и обратное, то истинны все четыре

Пример. Если формула - ДНФ, то это дизъюнкция. Прямое и контрапозиция верны, а противоположное и обратное нет.

2.4 Понятия необходимых и достаточных условий

Если некоторая математическая теорема имеет структуру, выражаемую формулой $X \to Y$, то высказывание Y называется **необходимым** условием для высказывания X (другими словами, если X истинно, то Y с необходимостью должно быть также истинным), а высказывание X называется **достаточным** условием для высказывания Y (другими словами, для того чтобы Y было истинным, достаточно, чтобы истинным было высказывание X).

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. $\Gamma \vdash \phi : \exists \phi_1, \dots, \phi_n = \phi$. Так как вывод конечный, то можно найти конечное множество гипотез, оно и будет Γ_0
2. Есть вывод $\Gamma \vdash \phi : \phi_1, \dots, \phi_n = \phi$
   Гипотезы $\Gamma \subseteq$ гипотезы из $\Delta \implies \Delta \vdash \phi$
3. $\Gamma \vdash \Delta, \Delta \vdash \psi$
   $\psi_{i1}, \dots, \psi_{ik} = \psi_i$ - вывод ψ_i из Γ $[\Delta = \bigcup_i \psi_i]$
   $\theta_1, \dots, \theta_m = \phi$ - вывод $\Delta \vdash \psi$
   Построим единую последовательность $\psi_{i1}, \dots, \psi_{ik}, \theta_1, \dots, \theta_m = \phi$ (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 $\to$ (A $\to$ B) (аксиома A1)
   (c) A $\to$ B (1,2, MP)

3. Если B = A, то A $\to$ B = A $\to$ A. Но $\vdash$ A $\to$ 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 $\vdash$ B и утверждение ($\Rightarrow$) верно для всех более коротких выводов, т.е. для всех C, если Γ, A $\vdash$ C и вывод C из Γ, A короче, чем вывод B, то Γ $\vdash$ A $\to$ C.

Докажем, что Γ $\vdash$ A $\to$ B.

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

(*) Γ $\vdash$ 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 A2)
4. (A $\to$ C) $\to$ (A $\to$ B) (2,3, MP)
5. A $\to$ B (1,4, MP)

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

▶

2.8 Теорема о полноте и непротиворечивости ИВ

Теорема 2.2 (Теорема о полноте ИВ). $\vdash A$ *тогда и только тогда, когда* A *- тавтология*

Доказательство. => Если формула A выводится из аксиом($\vdash$), то A является тавтологией <= Пусть A - тавтология. Тогда $\bar{A}$ - тождественно ложная. Докажем что множество $\Gamma = \{\bar{A}\}$ является противоречивым. Если оно непротиворечиво , то по лемме 7.6 существует полное непротиворечивое множество $^{-}\supset$. По лемме 7.7 для множества$^{-}$существует набор значений переменных $\bar{a}$, на котором все формулы из$^{-}$(в том числе и $\neg A$) принимают значение 1. Мы приходим к противоречию, поскольку формула $\neg A$ тождественно ложна. В соответсвии с теоремой ИВ Гильберта из множества Γ выводится абсолютно любая формула в том числе и формула A.

$\neq A \vdash A$. По теорема дедукции это означает, что формула $\neg A \to A$ выводится из аксиом ИВ Гильберта, то есть $\vdash \neg A \to A$. Напишем такой вывод.

1. $(\neg A \to A) \to ((\neg\neg A \to A) \to A)$
2. $\neg A \to A$
3. $(\neg\neg A \to A) \to A$ MP(1, 2)
4. $\neg\neg A \to A$
5. A MP(3, 4)

Построенный вывод показывает, что формула A является теоремой ИВ Гильберта, то есть $\vdash A$. ▶

Замечание. Лемма 7.6 Для каждого непротиворечивого мноэества формул Γ существует полное непротиворечивое множество $' \supset$

Замечание. Лемма 7.7 Для любого непротиворечивого полного множества формул Γ сущесвует набор переменных, на которых все формулы множества Γ истинны.

2.9 ИВ Генцена, его полнота

1. Алфавит: $\{x_1, \dots, x_n, \&, \vee, \to, ', (,), \vdash, "\}$
2. Используем слова двух видов:
   (a) Формулы - формулы логики высказываний
   (b) Секвенции - слова вида $\Gamma \vdash \Delta$, где Γ, Δ - множества формул

   Из всех формул Γ вместе следует хотя бы одна формула из Δ ($\&\Gamma \to \vee\Delta$)
3. Аксиомы: секвенции

   $\Gamma, \phi \vdash \Delta, \phi$
4. Правила вывода:

   $\vdash \ \&$ $\frac{\Gamma\vdash\phi,\Delta \quad \Gamma\vdash\psi,\Delta}{\Gamma\vdash\phi\&\psi,\Delta}$

   $\vdash \ \vee$ $\frac{\Gamma\vdash\phi,\psi,\Delta}{\Gamma\vdash\phi\vee\psi,\Delta}$

   $\vdash \to$ $\frac{\Gamma,\phi\vdash\Delta \quad \Gamma\vdash\psi,\Delta}{\Gamma\vdash\phi\to\psi,\Delta}$

   $\vdash \ '$ $\frac{\Gamma,\phi\vdash\Delta}{\Gamma\vdash\phi',\Delta}$

   $\& \ \vdash$ $\frac{\Gamma,\phi,\psi\vdash\Delta}{\Gamma,\phi\&\psi\vdash\Delta}$

   $\vee \ \vdash$ $\frac{\Gamma,\phi\vdash\Delta \quad \Gamma,\psi\vdash\Delta}{\Gamma,\phi\vee\psi\vdash\Delta}$

   $\to \vdash$ $\frac{\Gamma\vdash\phi,\Delta \quad \Gamma,\psi\vdash\Delta}{\Gamma,\phi\to\psi\vdash\Delta}$

   $' \ \vdash$ $\frac{\Gamma\vdash\phi,\Delta}{\Gamma,\phi'\vdash\Delta}$

Определение. Секвенция $\Gamma \vdash \Delta$ доказуема, если существует конечная последовательность секвенций $\Gamma_1 \vdash \Delta_1, \dots, \Gamma_n \vdash \Delta_n \vdash \Gamma \vdash \Delta$, в которой каждая секвенция:

- либо аксиома;
- либо получена из предыдущих по одному из правил вывода.

Замечание (Алгоритм поиска контрпримера к секвенции).

1. Взять исходную секвенцию $\Gamma \vdash \Delta$ и разместить её в корне дерева.
2. С помощью правил вывода ИВ Генцена добавлять в дерево новые вершины. Правила вывода нужно применять верх ногами, то есть по имеющейся секвенции выписать секвенции, которые находятся в верхней строке правил вывода ИВ Генцена.
3. Процесс построения дерева завершается, когда во всех его листьях строят секвенции без логических операций.
4. Если во всех листьях дерева строят аксиомы ИВ Генцена, то исходная секвенция $\Gamma \vdash \Delta$ не имеет контрпримера. Иначе, у секвенции $\Gamma \vdash \Delta$ существует контрпример.

Пример. $x \to y \vdash x' \vee y$
Строим вывод:

$\to \vdash$ $\frac{x\vdash x,y \quad y,x\vdash y}{x\to y,x\vdash y}$

$\vdash \ '$ $\frac{x\to y,x\vdash y}{x\to y\vdash x',y}$

$\vdash \ \vee$ $\frac{x\to y\vdash x',y}{x\to y\vdash x'\vee y}$

Определение. $\Gamma = \{\phi_1, \dots, \phi_n\}, \Delta = \{\psi_1, \dots, \psi_m\}$. Секвенция $\Gamma \vdash \Delta$ тождественно истинна, если тождественно истинна формула $(\phi_1, \& \dots, \&\phi_n) \to (\psi_1 \vee \dots \vee \psi_m)$

Теорема 2.3. *Секвенция* $\Gamma \vdash \Delta$ *доказуема* $\Leftrightarrow$ $\Gamma \vdash \Delta$ *тождественно истинна*

- $\Rightarrow$ (Корректность ИВ Генцена) $\Gamma \vdash \Delta$ доказуема $\Leftrightarrow$ есть вывод $\Gamma_1 \vdash \Delta_1, \dots, \Gamma_n \vdash \Delta_n \vdash \Gamma \vdash \Delta$ Индукция по номеру секвенции: докажем, что все секвенции в выводе тождественно истинны:

  Основание: k = 1.

  $\Gamma_1 \vdash \Delta_1$ аксиома, т.е имеет вид $\Gamma, \Psi \vdash \widetilde{\Delta}, \Psi$ - она тожд. истинная => $\&\Gamma_1 \to \vee\Delta_1 \sim \phi\&\&\Gamma_1 \to (\phi \vee \vee\Delta_1)$

  Шаг индукции. Докажем для $\Gamma_k \vdash \Delta_k$, считая, что для всех предыдущих секвенций все доказано

  1. $\Gamma_k \vdash \Delta_k$ аксиома - все аксиомы тожд. истинны (как и раньше)
  2. Если секвенция получена по правилу вывода из секвенций $\Gamma_i \vdash \Delta_i, \Gamma_j \vdash \Delta_j, i, j < k$

  По инд. допущению, они тожд. истинны.

  Осталось доказать, что любое правило вывода из тождественно истинных секвенций даст тождественно истинную секвенцию. Это делается перебором правил: $[\vdash\ \&]\ \frac{\Gamma\vdash\phi,\Delta \quad \Gamma\vdash\psi,\Delta}{\Gamma\vdash\phi\&\psi,\Delta}$

  $\Gamma \vdash \phi, \Delta$ тождественно истинны <=> $\&\Gamma \to (\phi \vee \vee\Delta) \sim 1$

  $\Gamma \vdash \psi, \Delta$ тождественно истинны <=> $\&\Gamma \to (\psi \vee \vee\Delta) \sim 1$

  1. $\&\Gamma \to \vee\Delta \sim 1$ => $\&\Gamma \to (\psi\&\phi \vee \vee\Delta) \sim 1$
  2. $\&\Gamma \to \vee\Delta$не ~ 1
     $\&\Gamma \to \phi \sim 1$ и $\&\Gamma \to \psi \sim 1$ => $\&\Gamma \to (\psi\&\phi) \sim 1$ и поэтому $\&\Gamma \to (\psi\&\phi \vee \vee\Delta) \sim 1$

  Остальные правила вывода аналогично.

- $\Leftarrow$ (Полнота ИВ Генцена) $\Gamma \vdash \Delta$ - тождественно истинна.

  Заметим, что во всех правилах верхняя секвенция содержит на одну связку меньше, чем нижняя.

  Пусть в Δ есть формула со связкой, например, $\Phi \vee \Psi$. По правилу получим:

  $\frac{\Gamma,\phi,\psi\vdash\widetilde{\Delta}}{\Gamma\vdash\phi\vee\psi,\widetilde{\Delta}}, \phi \vee \psi, \widetilde{\Delta} = \Delta$

  Действуя аналогично, уберем в формулах из Δ все логические связки, уберем и в Γ

  Получим набор секвенций $\Gamma \vdash \Delta$ в которых Γ и Δ состоят только из переменных.

  1. Пусть есть переменная $x \in \Gamma \cap \Delta$ => это аксиома
  2. нет $x \in \Gamma \cap \Delta = \varnothing$, пусть $\Gamma = \{y_1, \dots, y_k\}, \Delta = \{z_1, \dots, z_n\}$
     положим $y_1 = \dots = y_k = 1, z_1, = \dots = z_n = 0$, при этой интерпретации $\&\Gamma \to \vee\Delta^\alpha = 0$

  Перебирая правила, докажем, что при любой интепретации α, если одна из секвенций $\Gamma_1 \vdash \Delta_1$ $\Gamma_2 \vdash \Delta_2$ ложна, то и результат тоже ложь

  $[\vdash\ \&]\ \frac{\Gamma\vdash\phi,\Delta \quad \Gamma\vdash\psi,\Delta}{\Gamma\vdash\phi\&\psi,\Delta}$

  α - интерпретация $(\&\Gamma \to (\phi \vee \vee\Delta))^\alpha = 0 \Leftrightarrow (\&\Gamma)^\alpha = 1$

  $(\phi \vee \vee\Delta)^\alpha = 0\phi^\alpha = 0$ и $(\&\Delta)^\alpha = 0$, тогда

  $(\&\Gamma \to (\phi\&\psi \vee \vee\Delta))^\alpha = 0[\&\Gamma = 1, \phi\&\psi = 0, \bigvee \Delta = 0]$

  Спускаясь вниз к исходной секвенции, получаем что она ложна => противоречие.

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 A - это отображение вида $P : A^n \to \{0, 1\}$

Определение. n-местная операция на множестве A - 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 A - это отображение, которое

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

Определение. Алгебраическая система - набор, состоящий из множества A, сигнатуры σ и интерпретации σ на A. Множество A 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

Определение. Множество истинности формулы ϕ в алгебраической системе $\mathfrak{a}$ - это $A_\phi = \{(a_1, \dots, a_n) | a_i \in A, \mathfrak{a} \models \phi(a_1, \dots, a_n)\}$

Определение. Множество $B \subseteq A^n$ выразимо в алгебраической системе $\mathfrak{a}$, если $\exists$ формула ϕ такая , что $A_\phi = B$
ИЛИ ПО ШЕВЛЯКОВУ

Предикат $Q(x1, \dots, x_n)$ называется выразимым на АС $\mathfrak{A} =< A, \sigma >$ сигнатуры σ, если существует формула $\phi(x1, \dots, xn)$ сигнатуры σ со свободными переменными $x1, \dots, x_n$ такая, что $\mathfrak{A} \models \phi(a_1, \dots, a_n) \Leftrightarrow Q(a_1, \dots, a_n)$.

Определение. Функция $f : A^n \to A$ выразима, если выразимо множество $\Gamma_f = \{(a_1, \dots, a_n, b) | a_i, b \in A, b = f(a_1, \dots, a_n)\}$

Определение. Предикат $P : A^n \to \{0, 1\}$ выразим, если выразимо его множество истинности. !!!

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

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

Определение.

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

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

Определение. АС $\mathfrak{a} =< A, \sigma >, \mathfrak{b} =< B, \sigma >$ сигнатуры σ изоморфны, если существует отображение $F : A \to B$ со свойствами: 1. F - биекция между основными множествами А и В; 2. $F(c_A) = c_B$, где c_A, c_B интерпретации константного символа $c \in \sigma$ в АС $\mathfrak{a}$ и $\mathfrak{b}$ соответственно (биекция F должна переводить константы одной АС в константы другой АС); 3. $F(f_A(x_1, \dots, x_n)) = f_B(F(x_1), \dots F(x_n))$, где f_A, f_B интерпретации функционального символа $f \in \sigma$ в АС $\mathfrak{a}$ и $\mathfrak{b}$ соответственно (говорят, что биекция F сохраняет значение функции f); 4. $P_A(x1, \dots, xn) = 1 \Leftrightarrow P_B(F(x1), \dots, F(xn)) = 1$, где P_A, P_B интерпретации предикатного символа $P \in \sigma$ в АС $\mathfrak{a}$ и $\mathfrak{b}$ соответственно (то есть биекция F отображает отображает область истинности предиката P_A на область истинности предиката P_B).

Определение. Алгебраические системы А и В изоморфны (обозначение: А $\cong$ В), если существует изоморфизм А на В.

Утверждение. Отношение изоморфизма есть отношение эквивалентности.

Определение. Автоморфизм - изоморфизм алгебраической системы самой на себя.

Теорема 3.1 (Теорема о сохранении значений термов и формул в изоморфных системах). $\alpha(x)$ - *изоморфизм,* $\mathfrak{a} =< A, \sigma >$*, на* $\mathfrak{b} =< B, \sigma >$

Тогда:

1. *Для любого терма* $t(x_1, \dots, x_n)$ *сигнатуры* σ
   $\forall a_1, \dots, a_n \in A : \alpha(t_\mathfrak{a}(a_1, \dots, a_n)) = t_\mathfrak{b}(\alpha(a_1), \dots, \alpha(a_n))$
2. *Для любой формулы* $\phi(x_1, \dots, x_n)$ *сигнатуры* σ
   $\forall a_1, \dots, a_n \in A : \mathfrak{a} \models \phi(a_1, \dots, a_n) \Leftrightarrow \mathfrak{b} \models \phi(\alpha(a_1), \dots, \alpha(a_n))$

Доказательство. Индукция по построению термов. Основание: const/переменная

1. $t(x_1,\dots,x_n) = x_i \implies \alpha(t_A(a_1,\dots,a_n)) = \alpha(a_i) = t_B(\alpha(a_1),\dots,\alpha(a_n))$
2. $t(x_1,\dots,x_n) = c \implies \alpha(t_A(a_1,\dots,a_n)) = [t_A(a_1,\dots,a_n) = c_A] = c_B = t_B(\alpha(a_1),\dots,\alpha(a_n))$

Шаг индукции
Пусть утверждение теоремы доказано для термов $t_1(x_1,\dots,x_n),\dots,t_k(x_1,\dots,x_n)$ ▶

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

Определение. Пусть $\mathfrak{A}$ АС сигнатуры σ. Множество всех замкнутых формул сигнатуры σ, истинных на A называется теорией АС $\mathfrak{A}$ и обозначается $\mathrm{Th}(\mathfrak{A})$. Более формально, $Th(\mathfrak{a}) = \{\phi | \mathfrak{a} \models \phi\}$

Определение. АС $\mathfrak{a} =< A, \sigma >, \mathfrak{b} =< B, \sigma >$ элементарно эквивалентны, если $Th(\mathfrak{a}) = Th(\mathfrak{b})$. Обозначается $\mathfrak{a} \equiv \mathfrak{b}$

Теорема 3.2. *Если две алгебраические системы изоморфны, то они элементарно эквивалентны*

$A \cong B => A \equiv B$. $\mathfrak{a}, \mathfrak{b}$ изоморфны, берем произвольную замкнутую формулу, по теореме о сохранении изоморфизмом значений термов и формул
$(\mathfrak{a} \models \phi \Leftrightarrow \mathfrak{b} \models \phi) \Leftrightarrow \mathfrak{a} \equiv \mathfrak{b}$ ▶

Замечание. Обратное не верно в общем случае.
$\sigma = \{P^{(2)}\}, \mathfrak{A} =< \mathbb{Q}, \sigma >, \mathfrak{B} =< \mathbb{R}, \sigma >$ $P_A(x,y) = P_B(x,y) = \{x < y\}$
Их элементарные теории совпадают, однако они не изоморфны ($|\mathbb{Q}| \neq |\mathbb{R}|$)
Однако для конечных множеств выполняется следующее:

Теорема 3.3. *Конечные АС изоморфны $\Leftrightarrow$ элементарно эквивалентны.*

$A \cong B <= A \equiv B$. Построим формулу, которая кодирует операции, предикаты и константы на $\mathfrak{A} : \phi_{\mathfrak{A}}$
$\sigma = P \cup f \cup c, |a| = n, x_1,\dots,x_n-$ пронумерованные элементы A
$\phi_A = \exists x_1,\dots,\exists x_n(\neg(x_1 = x_2)\&\neg(x_1 = x_3)\dots\&\neg(x_n = x_{n-1}))\&$ [равенство / неравенство элементов A]
$P_1(x_i),\dots P_1(x_j)\&$ [множество истинности всех предикатов]
$(f(x_l) = x_r)\dots\&$ [значения для операций]
$(c = x_v)\dots\&$ [значения для констант]
$\forall x[(x = x_1) \vee \dots \vee (x = x_n)])$ [$\forall x$ зависит от кванторов существования]
Так как $\mathfrak{A} \models \phi_A$, то из элементарной эквивалентности следует что и $\mathfrak{B} \models \phi_A$
Это означает, что B состоит из того же кол-ва элементов, функции, предикаты, константы устроены точно так же, как и на A, поэтому они изоморфны. ▶

Замечание. Это док-во показывает, почему для бесконечных АС теорема не верна. Дело в том, чтобы описать бесконечное множество необходимо бесконечное количество переменных, а формула - конечное выражение.

Чтобы определить, что АС элементарно не эквивалентны, необходимо сформулировать свойство, которое верно для одной АС, и ложно в другой, и записать свойство в виде замкнутой формулы сигнатуры.

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

3.9 Эквивалентность формул логики предикатов

Определение. Формулы $\phi(x_1,\dots,x_n)$ и $\psi(x_1,\dots,x_n)$ сигнатуры σ эквивалентны в алгебраической системе $\mathfrak{a} =< A, \sigma >$ $(\phi \sim_{\mathfrak{a}} \psi)$, если

$$\forall a_1,\dots,a_n \in A \quad \mathfrak{a} \models \psi(a_1,\dots,a_n)$$

Определение. Формулы $\phi(x_1,\dots,x_n)$ и $\psi(x_1,\dots,x_n)$ сигнатуры σ эквивалентны $(\phi \sim \psi)$, если

$$\forall \mathfrak{a} =< A, \sigma > (\phi \sim_{\mathfrak{a}} \psi)$$

3.10 Тождественно истинные (ложные) и выполнимые формулы

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

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

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.

3.11 Пренексный вид формулы

Определение. Формула ϕ находится в пренексном виде, если она

- либо не содержит кванторов (бескванторная)
- либо имеет вид $Q_1 x_1 \dots Q_n x_n \psi$, где Q_i - кванторы, а формула ψ бескванторная.

Теорема 3.4 (о приведении формулы логики предикатов в пренексный вид)**.** *Любая формула логики предикатов может быть преобразована в эквивалентную формулу в пренексном виде.*

Доказательство. На основании предложения о эквивалентностях логики высказываний выразим все связки через $\&, \vee, \neg$. Получим эквивалентную формулу Ψ.

Индукция по построению формулы Ψ.

Основание - ψ - бескванторная, то есть уже в ПНФ.

Предположение индукции: допустим, теорема доказана для формул с $\leq k$ логическими знаками и кванторами. Шаг индукции: докажем теорему для формул с k + 1 логическими знаками и кванторами. Рассмотрим последний логический знак или квантор, входящий в формулу:

1. $A = \neg A_1$,
2. $A = A_1 \vee A_2$,
3. $A = A_1 \& A_2$,
4. $A = A_1 \to A_2$,
5. $A = \exists x A_1(x)$,
6. $A = \forall x A_1(x)$,

причем формулы A_1, A_2 содержат $\leq k$ логических знака и квантора и для них теорема доказана. Значит, для них существуют эквивалентные формулы, находящиеся в пренексной нормальной форме. Обозначим их через B_1, B_2 : $A_1 \sim B_1$ и $A_2 \sim B_2$. Можно считать, что связанные переменные, входящие в формулу B_1 , не совпадают со связанными переменными, входящими в формулу B_2 (иначе их можно переименовать).

Пусть B_1, B_2 имеют вид:

$B_1 = Q_1 y_1 Q_2 y_2 \dots Q_n y_n C_1(y_1, y_2, \dots, y_n, u_1, u2, \dots, u_{l_1})$,

$B_2 = R_1 z_1 R_2 z_2 \dots R_m z_m C_2(z_1, z_2, \dots, z_m, v_1, v_2, \dots, v_{l_2})$,

где $C_1(y_1, y_2, \dots, y_n, u_1, u_2, \dots, u_{l_1}), C_2(z_1, z_2, \dots, z_m, v_1, v_2, \dots, v_{l_2})$

- формулы, не содержащие кванторов. Чтобы не загромождать запись, будем писать просто C_1, C_2 , не указывая переменные.

В каждом из 6 случаев построим формулу, эквивалентную A и находящуюся в пренексной нормальной форме, используя эквивалентности логики предикатов. Последняя формула в цепочке эквивалентностей находится в пренексной нормальной форме.

1. $A = \neg A_1 \sim \neg B_1 \sim Q'_1 y 1 Q'_2 y_2 \dots Q'_n y_n \neg C_1$, где

$$Q'_i = \begin{cases} \exists, \text{если} Q_i = \forall, \\ \forall, \text{если} Q_i = \exists \end{cases}$$

2. $A = A_1 \vee A_2 \sim B_1 \vee B_2 = Q_1y_1Q_2y_2, \dots, Q_ny_nC_1 \vee R_1z_1R_2z_2 \dots R_mz_mC_2$
   $\sim Q_1y_1Q_2y_2, \dots, Q_ny_nR_1z_1R_2z_2 \dots R_mz_m(C_1 \vee C_2)$
3. $A = A_1 \& A_2 \sim B_1 \& B_2 = Q_1y_1Q_2y_2, \dots, Q_ny_nC_1 \& R_1z_1R_2z_2 \dots R_mz_mC_2$
   $\sim Q_1y_1Q_2y_2, \dots, Q_ny_nR_1z_1R_2z_2 \dots R_mz_m(C_1 \& C_2)$
4. $A = A_1 \to A_2 \sim B_1 \to B_2 = Q_1y_1Q_2y_2, \dots, Q_ny_nC_1 \to R_1z_1R_2z_2 \dots R_mz_mC_2$
   $\sim Q_1y_1Q_2y_2, \dots, Q_ny_nR_1z_1R_2z_2 \dots R_mz_m(C_1 \to C_2)$
5. $A = \exists x A_1(x) \sim \exists x B_1(x) \sim \exists x Q_1y_1Q_2y_2, \dots, Q_ny_nC_1$
6. $A = \forall x A_1(x) \sim \forall x B_1(x) \sim \forall x Q_1y_1Q_2y_2, \dots, Q_ny_nC_1$

▶

Алгоритм приведения ф. ЛП в ПНФ:

1. Выразить все связки через $\&, \vee, '$
2. Переименовать все связанные переменные так, чтобы они отличались друг от друга и от связанных переменных
3. Действуя от внутренних подформул к внешним, выносим кванторы влево.

(нельзя переименовывать свободную формулу)

3.12 Основные эквивалентности логики предикатов

Утверждение (Об эквивалентностях ЛВ). Пусть $\phi(x_1, \dots, x_n), \psi(x_1, \dots, x_n)$ от булевых переменных, $\phi_1, \dots, \phi_n$ - формулы ЛП

Тогда если $\phi \sim \psi$ В ЛВ, то результат подстановки эквивалентен в ЛП

Доказательство. $\mathfrak{a}$ - произвольная алг. система сигнатуры σ, $a_1, \dots, a_n \in A$, тогда $b_i = \phi_i(a_1, \dots, a_k) \in \{0,1\}$ $\phi \sim \psi$ в ЛВ $\Leftrightarrow \forall b_1, \dots, b_n \in \{0,1\} \phi(b_1, \dots, b_n) = \psi(b_1, \dots, b_n)$ ▶

Теорема 3.5 (Основные эквивалентности ЛП). *След. пары формул эквивалентны [свободные переменные остаются свободными]:*

1. *(Перестановка одноименных кванторов)*
$$\forall y \forall x P(x) \sim \forall x \forall y P(x) \qquad \exists y \exists x P(x) \sim \exists x \exists y P(x)$$
2. *(Переименование связанных переменных) нельзя брать свободные переменные*
$$\forall x \psi(x) \sim \forall y \psi(y) \qquad \exists x \psi(x) \sim \exists y \psi(y)$$
3. *(Отрицание и кванторы)*
$$\neg(\forall x \psi(x)) \sim \exists x \neg\psi(x) \qquad \neg(\exists x \psi(x)) \sim \forall x \neg\psi(x)$$
4. $$(\forall x \phi(x)) \& (\forall x \psi(x)) \sim \forall x \phi(x) \& \psi(x) \qquad (\exists x \phi(x)) \vee (\exists x \psi(x)) \sim \exists x \phi(x) \vee \psi(x)$$
5. $$(\forall x \phi(x)) \vee (\forall y \psi(y)) \sim \forall x \forall y (\phi(x) \vee \psi(y)) \qquad (\exists x \phi(x)) \& (\exists y \psi(y)) \sim \exists x \exists y (\phi(x) \& \psi(y))$$
6. $$(\forall x \phi(x)) \& / \vee (\exists y \psi(y)) \sim \forall x \exists y (\phi(x) \& / \vee \psi(y)) \sim \exists y \forall x (\phi(x) \& / \vee \psi(y))$$
7. *переменная x не входит свободно в ψ*
$$(\forall x \phi(x)) \& / \vee \psi \sim \forall x (\phi(x) \& / \vee \psi) \qquad (\exists x \phi(x)) \& / \vee \psi \sim \exists x (\phi(x) \& / \vee \psi)$$

Доказательство. Для доказательства эквивалентности необходимо показать, что на любой модели, сигнатура которой содержит сигнатуру формул, при любых значениях свободных переменных обе формулы либо истинны, либо ложны одновременно.

1. Очевидно
2. Очевидно
3. Пусть $\neg\forall x A(x)$ истинна при заданной фиксации свободных переменных, тогда $\forall x A(x)$ - ложь. То есть формула $A(x)$ ложна при некотором значении x. Тогда при этом значении x формула $\neg A(x)$ истинна. Значит, истинна и формула $\exists x \neg A(x)$.

   Пусть теперь истинна формула $\exists x \neg A(x)$ при заданной фиксации свободных переменных. Тогда формула $\neg A(x)$ истинна при некотором значении x. Значит, формула $A(x)$ ложна при этом значении x. По смыслу квантора всеобщности, ложна формула $\forall x A(x)$. Следовательно, формула $\neg\forall x A(x)$ истинна.
4. Пусть M - модель, сигнатура которой содержит предикаты A(x) и B(x). Если предикаты содержат другие свободные переменные, кроме переменной x, то фиксируем произвольные значения для них.

   Пусть $\exists x A(x) \vee \exists x B(x)$ - ложна при заданных значениях свободных переменных. Тогда ложна как формула $\exists x A(x)$, так и формула $\exists x B(x)$. По смыслу квантора существования, A(x) и B(x) ложны при любом значении x. Значит, при любом x ложна формула $A(x) \vee B(x)$. По смыслу квантора существования, формула $\exists x(A(x) \vee B(x))$ также ложна.

   Пусть $\exists x(A(x) \vee B(x))$ ложна при заданных значениях свободных переменных. Тогда $A(x) \vee B(x)$ ложна при любом значении x. Значит, A(x) и B(x) ложны при любом значении x. Отсюда следует, что ложны формулы $\exists x A(x)$ и $\exists x B(x)$ и ложна их дизъюнкция $\exists x A(x) \vee \exists x B(x)$

►

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

Вид кванторного префикса в ПНФ - показатель сложности формулы

Определение. Класс Σ_n (n > 0) состоит из всех формул в пренексном виде, у которых кванторный префикс начинается с квантора существования и содержит (n-1) перемену кванторов.

Определение. Класс Π_n (n > 0) состоит из всех формул в пренексном виде, у которых кванторный префикс начинается с квантора всеобщности и содержит (n-1) перемену кванторов.

Определение. Класс Δ_n (n > 0) состоит из всех формул, которые можно привести как к виду Π_n, так и к виду Σ_n.

При n = 0 классы $\Sigma_0 = \Pi_0 = \Delta_0$ — все бескванторные формулы.

Теорема 3.6 (соотношения между классами формул). *$i, j > 0$,формулы из Π_i и Σ_i можно преобразовать в Δ_{i+1}, а формулы из Δ_i можно преобразовать в формулы из Π_{i+1} и Σ_{i+1}*

Доказательство. Поскольку каждая формула первого порядка имеет ПНФ, каждой формуле присваивается по крайней мере одна классификация. Поскольку избыточные кванторы могут быть добавлены к любой формуле, как только формуле присваивается классификация Σ_n или Π_n ему будут присвоены классификации Σ_r и Π_r для каждого $r > n$. Таким образом, единственной релевантной классификацией, присвоенной формуле, является классификация с наименьшим числом n; все остальные классификации могут быть определены на ее основе.

Из Δ_n Π_n и Σ_n выводятся по определению класса дельта. ►

3.14 Нормальная форма Сколема, ее построение (на примерах)

3.15 Проверка существования вывода методом резолюций (алгоритм)

3.16 Логическое следование в логике предикатов

Определение. Пусть Γ — множество формул логики предикатов сигнатуры $\sigma, \phi(x_1, \ldots, x_n)$ – формула сигнатуры σ. Тогда формула ϕ **логически следует** из множества $\Gamma(\Gamma \models \phi)$, если для любой алгебраической системы $\mathfrak{a} =< A, \sigma >$ и любых элементов $a_1, \ldots, a_n \in A$, если на этих элементах в системе $\mathfrak{a}$ истинны все формулы из Γ, то истинна и $\phi(a_1, \ldots, a_n)$.

3.17 Исчисление предикатов (ИП) Гильберта. Свойства выводов

3.18 Теория. Модель теории

Определение. Теория сигнатуры σ - это произвольное множество замкнутых формул сигнатуры σ.

Определение. Модель теории T — это алгебраическая система A, в которой истинны одновременно все формулы теории T.

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

Определение. Теория T противоречивая, если существует формула ϕ такая, что одновременно $T \models \phi$ и $T \models \neg\phi$. В противном случае теория T непротиворечивая.

3.20 Теорема о существовании модели (без доказательства)

Теорема 3.7 (Теорема о существовании модели). *Каждая непротиворечивая теория имеет модель.*

3.21 Теорема о связи выводимости и противоречивости

3.22 Теоремы о корректности и полноте ИП

3.23 Теорема компактности

Теорема 3.8 (Теорема компактности). *Теория имеет модель $\Leftrightarrow$ каждая ее конечная подтеория имеет модель.*

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)