

Билеты по матлогике

Содержание

I	Логика и арифметика	5
a.	Определения	5
	Булевы функции	5
	Классы булевых функций	5
	Замыкание класса булевых функций	6
	Композиция булевых функций	6
	Замкнутость	6
	Полнота	6
	Пропозициональные формулы	6
	Скобочный итог	6
	Тавтология	6
	Противоречие	7
	КНФ, ДНФ	7
	Полином Жегалкина	7
b.	Простые утверждения	7
	Т. о существовании КНФ/ДНФ	7
	Т. замкнутости классов Поста	8
c.	Вопросы на 3	9
	Теорема об однозначном представлении булевой функции многочленом Жегалкина	9
d.	Вопросы на 4	10
e.	Вопросы на 5	10
f.	Доп вопросы на 5	10
	Теорема об однозначности синтаксического разбора пропозициональных формул	11
	Критерий Поста	11
g.	Доп вопросы на 6	12
	Базис монотонных функций	12
h.	Доп вопросы на 7	13
II	Теория множеств	14
a.	Определения	14
	Множество	14
	Объединение	14
	Пересечение	14
	Разность	14
	Симметрическая разность	14
	Упорядоченная пара	14
	Декартово произведение	14

Соответствие	14
Отображение	14
Образ	14
Прообраз	14
Инъекция	14
Сюръекция	14
Биекция	14
Композиция	14
Множество в степени множества	14
Равномощность	14
Счетность	14
Континуальность	15
Бинарное отношение	15
Свойства отношений	15
Отношение эквивалентности	15
Отношение порядка	15
Линейный порядок	15
ЧУМ	15
ЛУМ	15
Фундированность	15
ВУМ	15
Минимальный элемент	15
Максимальный элемент	16
Наименьший элемент	16
Наибольший элемент	16
Цепь	16
Верхняя грань	16
Нижняя грань	16
Точная верхняя грань	16
Точная нижняя грань	16
Гомоморфизм ЧУМов	16
Изоморфизм ЧУМов	16
Сложение ЧУМов	16
Произведение ЧУМов	16
Декартово произведение ЧУМов	16
b. Простые утверждения	17
c. Вопросы на 3	17
d. Вопросы на 4	17

e.	Вопросы на 5	17
f.	Доп вопросы на 5	17
g.	Доп вопросы на 6	17
h.	Доп вопросы на 7	17

III	Вычислимость	17
------------	---------------------	-----------

a.	Определения	17
b.	Простые утверждения	17
c.	Вопросы на 3	17
d.	Вопросы на 4	17
e.	Вопросы на 5	17
f.	Доп вопросы на 5	17
g.	Доп вопросы на 6	17
h.	Доп вопросы на 7	17

I Логика и арифметика

а. Определения

1. *n-арной булевой функцией* называется произвольное отображение $\phi : \{0, 1\}^n \rightarrow \{0, 1\}$

Откуда тривиальным образом¹ получаем, что от n аргументов существует ровно $|\{0, 1\}|^{|\{0, 1\}^n|} = 2^{2^n}$

Стартерпак булевых функций:

От нуля переменных будет всего две функции: \perp - тавтологический 0, \top - тавтологическая 1

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

	<table><tr><th>x_1</th><th>x_2</th><th>$x_1 \vee x_2$</th></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table>	x_1	x_2	$x_1 \vee x_2$	0	0	0	0	1	1	1	0	1	1	1	1		<table><tr><th>x_1</th><th>x_2</th><th>$x_1 \rightarrow x_2$</th></tr><tr><td>0</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table>	x_1	x_2	$x_1 \rightarrow x_2$	0	0	1	0	1	1	1	0	0	1	1	1
x_1	x_2	$x_1 \vee x_2$																															
0	0	0																															
0	1	1																															
1	0	1																															
1	1	1																															
x_1	x_2	$x_1 \rightarrow x_2$																															
0	0	1																															
0	1	1																															
1	0	0																															
1	1	1																															
Дизъюнкция:		Импликация:																															

Исключающее или (XOR):	<table><tr><th>x_1</th><th>x_2</th><th>$x_1 \oplus x_2$</th></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>0</td></tr></table>	x_1	x_2	$x_1 \oplus x_2$	0	0	0	0	1	1	1	0	1	1	1	0	Эквиваленция:	<table><tr><th>x_1</th><th>x_2</th><th>$x_1 \leftrightarrow x_2$</th></tr><tr><td>0</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table>	x_1	x_2	$x_1 \leftrightarrow x_2$	0	0	1	0	1	0	1	0	0	1	1	1
	x_1	x_2	$x_1 \oplus x_2$																														
	0	0	0																														
	0	1	1																														
	1	0	1																														
1	1	0																															
x_1	x_2	$x_1 \leftrightarrow x_2$																															
0	0	1																															
0	1	0																															
1	0	0																															
1	1	1																															

	<table><tr><th>x_1</th><th>x_2</th><th>$x_1 x_2$</th></tr><tr><td>0</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>0</td></tr></table>	x_1	x_2	$x_1 x_2$	0	0	1	0	1	1	1	0	1	1	1	0		<table><tr><th>x_1</th><th>x_2</th><th>$x_1 \downarrow x_2$</th></tr><tr><td>0</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>0</td></tr></table>	x_1	x_2	$x_1 \downarrow x_2$	0	0	1	0	1	0	1	0	0	1	1	0
x_1	x_2	$x_1 x_2$																															
0	0	1																															
0	1	1																															
1	0	1																															
1	1	0																															
x_1	x_2	$x_1 \downarrow x_2$																															
0	0	1																															
0	1	0																															
1	0	0																															
1	1	0																															
Штрих Шеффера (NAND):		Стрелка Пирса (NOR):																															

2. Классы функций

P_0 - Сохраняющие 0

Класс² булевых функций (далее бф), таких что на наборе (0 ... 0) они принимают значение 0.

¹def: A^B - множество всех отображений из B в A

²Множество

P_1 - *Сохраняющие 1*

Класс булевых функций (далее бф), таких что на наборе $(1 \dots 1)$ они принимают значение 1.

S - *самодвойственные*

Пусть $f^{(n)}$ ³ - n -арная бф, тогда *двойственной* к ней называется такая n -арная бф $g^{(n)}$, что $f(x_1 \dots x_n) = \neg g(\neg x_1 \dots \neg x_n)$

Тогда S - класс бф, являющихся двойственными по отношению к самим себе

M - *монотонные*

Класс бф, таких что $f(x_1 \dots x_n) \geq f(x'_1 \dots x'_n)$, если $\forall i \in \{1 \dots n\} \hookrightarrow x_i \geq x'_i$

$A(L)$ - *Аффинные (линейные)*

Класс бф, таких что их представление полиномом Жегалкина является линейным. ⁴

3. **Замыканием класса булевых функций** называется класс бф, составленный из композиций исходного любого уровня вложенности, обозначается $[Q]$, где Q - класс булевых функций

4. **Композицией булевых функций** уровня вложенности n называется:

- $n = 0$, Множество всех проекторов
- $n > 0$, Множество всех возможных композиций из $n-1$ уровня и функций из данного класса

5. Класс булевых функций Q называется **замкнутым**, если $[Q] = Q$

6. Класс булевых функций Q называется **полным**, если $[Q]$ - множество всех возможных булевых функций

7. Определение **пропозициональной формулы** (индуктивное):

1. Если p - переменная, то p - пропозициональная формула
2. Если ψ - пропозициональная формула, то $\neg\psi$ - тоже пропозициональная формула
3. Если φ и ψ - пропозициональные формулы, то $(\psi \wedge \varphi)$, $(\psi \vee \varphi)$, $(\psi \rightarrow \varphi)$ - тоже пропозициональные формулы

8. **Скобочным итогом** пропозициональной формулы называют разность между количеством открывающих и закрывающих скобок.

9. **Тавтологией** называется формула, истинная на любом наборе переменных

Примеры: ⁵

- (a) Закон тождества $A \rightarrow A$
- (b) Закон непротиворечия $\neg(A \wedge \neg A)$
- (c) Закон исключенного третьего $\neg A \vee A$
- (d) Закон двойного отрицания $(A \rightarrow \neg\neg A) \wedge (\neg\neg A \rightarrow A)$
- (e) Закон контрапозиции $((A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)) \wedge ((\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B))$

³Будем вверху в скобках показывать аридность функции

⁴Подробнее в пункте про полиномы Жегалкина

⁵Здесь я немного поменял примеры Мусатова - заменил эквиваленцию на конъюнкцию двух импликаций, чтобы подходило под определение пропозициональной формулы

(f) Законы де Моргана $(\neg(A \wedge B) \rightarrow (\neg A \vee \neg B)) \wedge ((\neg A \vee \neg B) \rightarrow \neg(A \wedge B))$ и $(\neg(A \vee B) \rightarrow (\neg A \wedge \neg B)) \wedge ((\neg A \wedge \neg B) \rightarrow \neg(A \vee B))$

(g) Закон силлогизма $((A \rightarrow B) \rightarrow (B \rightarrow C)) \rightarrow (A \rightarrow C)$

10. **Противоречием** называется формула, ложная на любом наборе переменных

11. **Литералом** называется переменная или ее отрицание.

Дизъюнктом называется дизъюнкция литералов

Конъюнктом называется конъюнкция литералов

Конъюнктивной нормальной формой (КНФ) называется конъюнкция дизъюнктов

Дизъюнктивной нормальной формой (ДНФ) называется дизъюнкция конъюнктов

Совершенной конъюнктивной нормальной формой (СКНФ) называется такая КНФ, что в каждом дизъюнкте каждая переменная встречается не более одного раза

Совершенной дизъюнктивной нормальной формой (СДНФ) называется такая ДНФ, что в каждом конъюнкте каждая переменная встречается не более одного раза

12. **Мономом Жегалкина** называется конъюнкция переменных ⁶, при чем принято опускать знак конъюнкции, как в обычных школьных алгебраических мономах.

Полиномом Жегалкина называется сумма мономов Жегалкина, где под суммой понимается исключающее или.

б. Простые утверждения

1. Наличие КНФ или ДНФ для любой бф

КНФ:

Пусть ψ - n-арная булева функция. Тогда по каждому набору (их 2^n), n-мерному вектору x , если функция ложна на нем, построим дизъюнкт по следующему правилу, если $x_i = 0$, то включим i-ую переменную⁷ в дизъюнкт, иначе - ее отрицание. Потом возьмем конъюнкцию всех дизъюнктов. Формально получим:

$$CNF_{\psi} = \bigwedge_{\substack{x \in \{0,1\}^n \\ f(x)=0}} \bigvee_{j=1}^n p_i^{1-x_i}, \quad \text{где } p_i^{x_i} = \begin{cases} p_i & x_i = 1 \\ \neg p_i & x_i = 0 \end{cases}$$

Заметим, что каждый дизъюнкт $\bigvee_{j=1}^n p_i^{1-x_i}$ ложен только на своем наборе x , поэтому конечная формула будет ложна только на тех наборах, где бф принимает 0, значит, построили для нее КНФ. Даже более того, СКНФ. Непокрытым остался лишь случай, когда функция - тавтологическая единица, тогда она

⁶Важно отметить, что конъюнкция переменных (моном) \neq конъюнкт, т.к. второй допускает инверсию переменных, а в мономе никаких инверсий быть не может

⁷Будем обозначать i-ую переменную как p_i

представима в виде $p \vee \neg p$, но это не является СКНФ. Для тавтологий нет СКНФ.

ДНФ:

Пусть ψ - n -арная булева функция. Тогда по каждому набору (их 2^n), n -мерному вектору x , если функция истинна на нем, построим конъюнкт по следующему правилу, если $x_i = 0$, то включим i -ую переменную в конъюнкт, иначе - ее отрицание. Потом возьмем дизъюнкцию всех конъюнктов. Формально получим:

$$DNF_{\psi} = \bigvee_{\substack{x \in \{0,1\}^n \\ f(x)=1}} \bigwedge_{j=1}^n p_i^{x_i}, \quad \text{где } p_i^{x_i} = \begin{cases} p_i & x_i = 1 \\ \neg p_i & x_i = 0 \end{cases}$$

Заметим, что каждый конъюнкт $\bigwedge_{j=1}^n p_i^{x_i}$ истинен только на своем наборе x , поэтому конечная формула будет истинна только на тех наборах, где бф принимает 1, значит, построили для нее ДНФ. Даже более того, СДНФ. Непокрытым остался лишь случай, когда функция - тавтологический ноль, тогда она представима в виде $p \wedge \neg p$, но это не является СДНФ. Для противоречий нет СДНФ.

2. Классы поста (P_0, P_1, S, M, A) замкнуты

P_0 :

$$f^{(n)}, g^{(k)} = \left\| \begin{matrix} g_1^{(k)} \\ \vdots \\ g_n^{(k)} \end{matrix} \right\| \in P_0$$

$$h^{(k)} = f \circ g$$

$$h(0...0) = f(g(0...0))$$

$$g_i \in P_0 \Rightarrow h(0...0) = f(0...0) = 0 \Rightarrow h \in P_0$$

P_1 :

$$f^{(n)}, g^{(k)} = \left\| \begin{matrix} g_1^{(k)} \\ \vdots \\ g_n^{(k)} \end{matrix} \right\| \in P_1$$

$$h(1...1) = f(g(1...1))$$

$$g_i \in P_1 \Rightarrow h(1...1) = f(1...1) = 1 \Rightarrow h \in P_1$$

M :

$$f^{(n)}, g^{(k)} = \left\| \begin{matrix} g_1^{(k)} \\ \vdots \\ g_n^{(k)} \end{matrix} \right\| \in M$$

$$h^{(k)} = f(g)$$

Пусть x, y — n -мерные векторы⁸ $x \geq y$ (покоординатно)

⁸Компоненты векторов - 0 или 1, т.е. это есть не что иное, как наборы значений переменных

$$g_i \in M \Rightarrow g_i(x) \geq g_i(y) \Rightarrow g(x) \geq g(y)$$

$$h(x) = f(g(x)) > f(g(y)) = h(y) \Rightarrow h \in M$$

S:

$$f^{(n)}, g^{(k)} = \left\| \begin{array}{c} g_1^{(k)} \\ \vdots \\ g_n^{(k)} \end{array} \right\| \in S$$

$$g_i \in M \Rightarrow g_i(x) = \neg g_i(\neg x^9) \Rightarrow g(x) = \neg g(\neg x)$$

$$h(x) = f(g(x)) = f(\neg g(\neg x)) = \neg f(g(\neg x)) = \neg h(\neg x) \Rightarrow h \in S$$

A:

$$f^{(n)}, g^{(k)} = \left\| \begin{array}{c} g_1^{(k)} \\ \vdots \\ g_n^{(k)} \end{array} \right\| \in A$$

$$g_m \in A \Rightarrow g_j = \alpha_0^j \oplus \bigoplus_{i=1}^k \alpha_i^j p_i, \text{ где } \alpha_i^j \in \{0, 1\}$$

$$f \in A \Rightarrow f = \beta_0 \oplus \bigoplus_{j=1}^n \beta_j q_j, \text{ где } \beta_j \in \{0, 1\}$$

$$h = f \circ g = \beta_0 \oplus \bigoplus_{j=1}^n \beta_j (\alpha_0^j \oplus \bigoplus_{i=1}^k \alpha_i^j p_i) = \beta_0 \oplus \bigoplus_{j=1}^n \beta_j \alpha_0^j \oplus \bigoplus_{j=1}^n \bigoplus_{i=1}^k \beta_j \alpha_i^j p_i$$

что является линейным полиномом $\Rightarrow h \in A$

с. Вопросы на 3

1. Теорема об однозначном представлении булевой функции многочленом Жегалкина

Для любой бф найдется и при том единственный до перестановки переменных и слагаемых полином Жегалкина¹⁰

Доказательство

Всего функций от n переменных - 2^{2^n} штук. Мономов Жегалкина - 2^n штук (моном по сути - некоторое подмножество переменных, а всего подмножеств - мощность булеана), при чем перед каждым мономом стоит коэффициент 0 или 1. Итого всего 2^{2^n} полиномов Жегалкина от n переменных. Тогда, если мы покажем, что разным полиномам соответствуют разные функции, то мы докажем данное утверждение. Докажем, что разным полиномам сопоставляются разные функции. Предположим противное - пусть существуют два различных полинома, представляющих одну и ту же функцию. Вычтем их друг из друга и получим противоречие

Формально:

$$f = \alpha_0 \oplus \bigoplus_{j=1}^{2^n} \alpha_j m_j, \text{ где } \alpha_j \in \{0, 1\}$$

⁹Покомпонентная инверсия вектора

¹⁰Здесь предполагается, что все повторяющиеся мономы сокращены

Где m_j - это j -ый моном (т.е. занумеруем как-то мономы - их конечное число, поэтому данная операция проста и возможна)

$$f = \beta_0 \oplus \bigoplus_{j=1}^{2^n} \beta_j m_j, \text{ где } \beta_j \in \{0, 1\}$$

$$\exists y \in \{0 \dots 2^n\} : \alpha_y \neq \beta_y$$

Приравняем два равенства:

$$\alpha_0 \oplus \bigoplus_{j=1}^{2^n} \alpha_j m_j = \beta_0 \oplus \bigoplus_{j=1}^{2^n} \beta_j m_j$$

Так как полином Жегалкина не просто называется полиномом)¹¹, то перенесем все вправо и получим (Помним, что хог - это одновременно и сложение и вычитание):

$$\alpha_0 \oplus \bigoplus_{j=1}^{2^n} \alpha_j m_j \oplus \beta_0 \oplus \bigoplus_{j=1}^{2^n} \beta_j m_j = 0$$

$$(\alpha_0 \oplus \beta_0) \oplus \bigoplus_{j=1}^{2^n} (\alpha_j \oplus \beta_j) m_j = 0$$

Откуда: $\forall j \hookrightarrow \alpha_j \oplus \beta_j = 0 \Rightarrow \alpha_j = \beta_j$ - получили противоречие. **Ч.Т.Д.**

d. Вопросы на 4

e. Вопросы на 5

f. Доп вопросы на 5

1. Лемма о скобочном итоге

Пусть ψ - пропозициональная формула¹², s - ее префикс. Тогда скобочный итог s неотрицательный, причем он равен 0 только тогда, когда $s = \psi$ или $s = \{\neg\}^*$

Доказательство индукцией по построению формулы

Для переменной все верно тривиально выполнено

Пусть для ψ условие выполнено. Проверим для $\neg\psi$:

Т.к. \neg на скобочный итог не влияет, то на \neg - выполнено, а далее все как и в ψ - поэтому верно

Пусть для ψ и φ условие выполнено. Проверим для $(\psi * \varphi)$ ¹³:

Любой нетривиальный префикс $(\psi * \varphi)$ - это либо $(\psi'$, где $\psi' \sqsubset \psi$, либо $(\psi * \varphi'$, где $\varphi' \sqsubset \varphi$. В первом случае верность следует из предположения индукции (Для ψ - лемма выполняется - значит скобочный итог ψ' неотрицателен, со скобкой же получим, что больше 0). Во втором же случае скобочный итог формулы есть сумма скобочных итогов ($\psi, *, \varphi'$ - он больше 0, т.к. по предположению индукции для φ'

¹¹Это все же лучше не говорить на экзамене

¹²Здесь полагаем, что все переменные являются односимвольными и все символы различны.

¹³Это один из символов $\rightarrow, \wedge, \vee$

он неотрицателен, для ψ и $*$ - равен 0, скобка же увеличит его на 1 \Rightarrow будет больше 0. А итог всего $(\psi * \varphi)$ равен 0. **Ч.Т.Д.**

2. Лемма о беспрефиксности пропозициональных формул

Никакая пропозициональная формула не может быть префиксом другой.

Доказательство от противного

Пусть нашлись две такие пропозициональные формулы, что одна является префиксом другой. Тогда по лемме о скобочном итоге мы получим, что с одной стороны скобочный итог первой должен быть равен 0 - т.к. это вся формула, с другой же стороны получим, что он больше нуля - т.к. это нетривиальный префикс второй формулы \Rightarrow его скобочный итог больше 0. Имеем противоречие **Ч.Т.Д.**

3. Теорема об однозначности синтаксического разбора пропозициональных формул

По пропозициональной формуле можно однозначно сказать, из каких подформул она была получена и по каким правилам.

Доказательство

Если ψ - переменная, то все тривиально выполнено.

Иначе посмотрим на первый символ ψ - это не переменная. Если это \neg - то построено по правилу 2 из формулы полученной из ψ путем вычеркивания символа отрицания. Иначе первый символ ψ - скобка. Тогда покажем единственность разбора:

Пусть существует два разбора $(\psi_1 * \varphi_1) = (\psi_2 * \varphi_2)$ Если $\psi_1 = \psi_2$, то и $\varphi_1 = \varphi_2$ - разборы совпали. Тогда $\neg(\psi_1 = \psi_2)$. БОО $\psi_1 \sqsubset \psi_2$ - имеем противоречие с леммой о беспрефиксности. **Ч.Т.Д.**

4. Критерий Поста

Класс K является полным тогда и только тогда, когда он полностью не вложен ни в один из классов P_0, P_1, M, S, A .

Доказательство

Если K вложен в какой-то из классов, то его замыкание тоже будет вложено в этот класс. Значит, для полноты класса необходима невложенность не в один из классов выше.

Пусть K не вложен и содержит не сохраняющую 0 функцию f , не сохраняющую 1 функцию g , немонотонную m , несамодвойственную s и неаффиную a . Возможно, некоторые из них совпадут.

Т.к. f не сохраняет 0, то $f(0 \dots 0) = 1$, если тогда еще f не сохраняет 1, то $f(1 \dots 1) = 0$, т.е. $f(p \dots p)$ - отрицание. Иначе $f(1 \dots 1) = 1$, т.е. $f(p \dots p) = \top$. Т.к. g не сохраняет 1, то все то же самое - \perp или \neg . Итого, двумя функциями можно получить или две константы, или константу и отрицание, тогда применив отрицание к константе получим вторую, либо же только отрицание - $f = g$.

m - немонотонна, тогда найдутся такие i и $x_1 \dots x_{i-1}, x_{i+1} \dots x_m$, что $m(x_1 \dots x_{i-1}, 0, x_{i+1} \dots x_m) = 1$ и $m(x_1 \dots x_{i-1}, 1, x_{i+1} \dots x_m) = 0$. Подставим выраженные константы и получим отрицание:

$$m(x_1 \dots x_{i-1}, p, x_{i+1} \dots x_m) = \neg p$$

s - несамодвойственная, тогда найдутся такие $x_1 \dots x_m$, что $s(x_1 \dots x_m) = s(\neg x_1 \dots \neg x_m)$. Имея отрицание подберем вектор из p и отрицания $\neg p$ так, чтобы получить чередования значений ровно как в $x_1 \dots x_m$: т.е. если $x_1 \dots x_m = 1, 0, 0, 0, 1, 1$, то построим вектор $w = (\neg p, p, p, p, \neg p, \neg p)$. Тогда $h(w) = h(\neg w)$ -

значит это константа - при p и $\neg p$ принимает одинаковые значения. Тогда, получив одну константу, применим отрицание к ней и получим вторую.

Итого, точно имеем константы и отрицание.

a - неафинная функция. Тогда пускай БОО он содержит моном, включающий в себя x_1, x_2 , т.е. $a = x_1 x_2 P(x_3 \dots x_n) \oplus x_1 Q(x_3 \dots x_n) \oplus x_2 R(x_3 \dots x_n) \oplus S(x_3 \dots x_n)$. Тогда найдется какие-то $y_3 \dots y_m$, что $P(y_3 \dots y_m) = 1$. Подставим уже выраженные константы вместо $y_3 \dots y_m$ и получим функцию $\hat{a} = x_1 x_2 \oplus q x_1 \oplus r x_2 \oplus s$

Тогда имеем функции:

q	r	s	\hat{a}
0	0	0	$x_1 \wedge x_2$
0	0	1	$x_1 x_2$
0	1	0	$x_1 \nrightarrow x_2$
0	1	1	$x_1 \rightarrow x_2$
1	0	0	$x_1 \leftarrow x_2$
1	0	1	$x_1 \leftarrow x_2$
1	1	0	$x_1 \vee x_2$
1	1	1	$x_1 \downarrow x_2$

В каждом из случаев имеет полную систему - просто выразим через \perp, \top, \neg и одну из функций выше \wedge - получим систему (\neg, \wedge) - полную. **Ч.Т.Д.**

г. Доп вопросы на 6

1. Лемма о дополнительных классах бф

\bigwedge - класс конъюнктивных функций и \bigvee - класс дизъюнктивных функций замкнуты.

Доказательство

\bigwedge - класс таких функций, что $f(x_1 \wedge y_1, \dots, x_n \wedge y_n) = f(x_1, \dots, x_n) \wedge f(y_1, \dots, y_n)$. Покажем его замкнутость:

$$f^{(n)}, g^{(k)} = \left\| \begin{array}{c} g_1^{(k)} \\ \vdots \\ g_n^{(k)} \end{array} \right\| \in \bigwedge$$

$$h^{(k)} = f \circ g$$

$$g_i \in \bigwedge \Rightarrow g_i(x_1 \wedge y_1, \dots, x_n \wedge y_n) = g_i(x_1, \dots, x_n) \wedge g_i(y_1, \dots, y_n)$$

$$\text{Значит, } g(x_1 \wedge y_1, \dots, x_n \wedge y_n) = g(x_1, \dots, x_n) \wedge^{14} g(y_1, \dots, y_n)$$

$$\begin{aligned} \text{Тогда, } h(x_1 \wedge y_1, \dots, x_n \wedge y_n) &= f(g(x_1 \wedge y_1, \dots, x_n \wedge y_n)) = f(g(x_1, \dots, x_n) \wedge g(y_1, \dots, y_n)) = \\ &= f(g(x_1, \dots, x_n)) \wedge f(g(y_1, \dots, y_n)) = h(x_1, \dots, x_n) \wedge h(y_1, \dots, y_n) \Rightarrow h \in \bigwedge \end{aligned}$$

Аналогично показывается замкнутость класса \bigvee - класс таких функций, что $f(x_1 \vee y_1, \dots, x_n \vee y_n) = f(x_1, \dots, x_n) \vee f(y_1, \dots, y_n)$.

¹⁴Покомпонентная конъюнкция

2. Базис монотонных функций

$1, 0, \wedge, \vee$ - базис M .

Доказательство

Так как все эти функции монотонны, то их замыкание лежит в M . Также, ни одна из них не может быть выражена через другие (без 0 (1) - все сохраняют 1 (0), без \wedge - все вложены в класс конъюнктивных функций, без \vee - в класс дизъюнктивных функций)

Покажем, что любую монотонную можно выразить через данные 4 функции:

Если функция - константа, то тривиально выполнено, иначе - не константа, тогда на $(0 \dots 0)$ она принимает значение 0 , а на $(1 \dots 1)$ - 1 . Назовем набор значений минимальным, если смена любой единицы на ноль приведет к уменьшению значения функции. Тогда по каждому минимальному набору построим конъюнкцию переменных: если значение соответствующей переменной равно 1 , то включим ее в конъюнкцию. Потом возьмем дизъюнкцию все полученных конъюнкций.

Полученная формула - есть представление функции. Т.к. если f приняла значение 1 на каком-то наборе, то найдется такая конъюнкция, что содержит часть переменных, что равны 1 на данном наборе. (Найдет предшествующий данному набору минимальный - при "подъеме" вверх по таблице истинности "триггерные" переменные не поменяют значение и будут равны 1 , дойдем до минимального - для него есть конъюнкция по построению дающая 1 , "спустившись" обратно вниз снова "триггеры" не поменяют значение) **Ч.Т.Д.**

h. Доп вопросы на 7

II Теория множеств

а. Определения

1. *Множество* - неопределяемое понятие

2. *Объединение множеств*:

$$A \cup B := \{x \mid x \in A \vee x \in B\}$$

3. *Пересечение множеств*:

$$A \cap B := \{x \mid x \in A \wedge x \in B\}$$

4. *Разность множеств*:

$$A \setminus B := \{x \mid x \in A \wedge \neg(x \in B)\}$$

5. *Симметрическая разность множеств*:

$$A \Delta B := \{x \mid x \in A \oplus x \in B\}$$

6. *Упорядоченная пара*

$$\text{По Куратовскому: } (a, b) := \{a, \{a, b\}\}$$

7. *Декартово произведение*

$$A \times B := \{(a, b) \mid a \in A, b \in B\}$$

8. *Соответствием* называют производное подмножество декартова произведения множеств.

9. *Отображением* называют такое соответствие, что у каждого элемента ровно один образ.

10. *Образом* множества S называют множество $f(S) := \bigcup_{x \in S} f(x)$.

11. *Прообразом* множества S называют множество $f^{-1}(S) := \{x \mid f(x) \in S\}$.

12. *Инъекцией* называют такое отображение $f : A \rightarrow B$, что $\forall a_1 \neq a_2 \in A \hookrightarrow f(a_1) \neq f(a_2)$.

13. *Сюръекцией* называют такое отображение $f : A \rightarrow B$, что $\forall b \in B \exists a \in A \hookrightarrow f(a) = b$.

14. *Биекцией* называют отображение, являющееся и инъекцией, и сюръекцией.

15. Пусть $f : A \rightarrow B$ и $g : B \rightarrow C$ - отображения. Тогда *композицией* отображений f и g называют отображение $h : A \rightarrow C$, обозначаемое $h = g \circ f$, которое определяется как $\{(a, c) \in A \times C \mid \exists b \in B : (a, b) \in f \wedge (b, c) \in g\}$

16. Пусть A и B - произвольные множества, тогда A^B - множество всех отображений из B в A

17. Пусть A и B - произвольные множества, тогда они называются *равномощными*, если существует биекция из A в B . Обозначение: $A \cong B$

18. Множество называется **счетным**, если оно равномощно \mathbb{N} .
19. Множество называется **континуальным**, если оно равномощно \mathbb{R} .
20. **Бинарным отношением** на множестве называют любое подмножество его декартова квадрата.
21. **Свойства отношений**. Пусть \mathcal{R} - отношение на A :

(a) Рефлексивность

$$\forall a \in A \hookrightarrow a\mathcal{R}a$$

(b) Иррефлексивность

$$\forall a \in A \hookrightarrow \neg(a\mathcal{R}a)$$

(c) Симметричность

$$\forall a \in A \forall b \in A \hookrightarrow a\mathcal{R}b \Rightarrow b\mathcal{R}a$$

(d) Антисимметричность

$$\forall a \in A \forall b \in A \hookrightarrow a\mathcal{R}b \wedge b\mathcal{R}a \Rightarrow a = b$$

(e) Транзитивность

$$\forall a \in A \forall b \in A \forall c \in A \hookrightarrow a\mathcal{R}b \wedge b\mathcal{R}c \Rightarrow a\mathcal{R}c$$

(f) Полнота

$$\forall a \in A \forall b \in A \hookrightarrow a\mathcal{R}b \vee b\mathcal{R}a$$

22. Рефлексивное, симметричное и транзитивное отношение называется **отношением эквивалентности**.
23. Рефлексивное, антисимметричное и транзитивное отношение называется **отношением порядка**.
24. Порядок \preceq на A будет называться **линейным**, если:

$$\forall a \in A \forall b \in A \hookrightarrow a \preceq b \vee b \preceq a$$

25. Множество с введенными на нем порядком называется **(Частично) Упорядоченным Множеством - ЧУМ/УМ**
26. Множество с введенными на нем линейным порядком называется **Линейно Упорядоченным Множеством - ЛУМ**
27. Множество, в каждом подмножестве которого существует минимальный элемент¹⁵, называется **фундированным**.
28. Фундированное множество с линейным порядком называется **Вполне Упорядоченным Множеством - ВУМ**

¹⁵т.е. такой, меньше которого нет, - не путать с наименьшим - меньше всех

29. **Минимальным** называют элемент, меньше которого нет.
30. **Максимальным** называют элемент, больше которого нет.
31. **Наименьшим** называют элемент в множестве, который не больше всех элементов в данном множестве.
32. **Наибольшим** называют элемент в множестве, который не меньше всех элементов в данном множестве.
33. **Цепью** в упорядоченном множестве $\langle M, \lesssim \rangle$ называют последовательность элементов $a_1 \dots a_n$, такую что $a_1 \lesssim a_2 \lesssim \dots \lesssim a_n$
34. **Верхней гранью** множества $S \subseteq M : \langle M, \lesssim \rangle$ называется $m \in M$, такое что $\forall s \in S \hookrightarrow m \gtrsim s$
35. **Нижней гранью** множества $S \subseteq M : \langle M, \lesssim \rangle$ называется $m \in M$, такое что $\forall s \in S \hookrightarrow s \gtrsim m$
36. **Точной верхней гранью** множества $S \subseteq M : \langle M, \lesssim \rangle$ или *супремумом* называют такую верхнюю грань, что она принадлежит S и является наименьшей среди всех остальных верхних граней.
37. **Точной нижней гранью** множества $S \subseteq M : \langle M, \lesssim \rangle$ или *инфимумом* называют такую нижнюю грань, что она принадлежит S и является наибольшей среди всех остальных нижних граней.
38. **Гомоморфизмом** ЧУМов называют отображение, уважающее порядок. Формально: $\langle A, \lesssim_A \rangle$ и $\langle B, \lesssim_B \rangle$ - ЧУМы, $\varphi : A \rightarrow B$ - гомоморфизм, если $\forall x, y \in A \hookrightarrow x \lesssim_A y \Rightarrow \varphi(x) \lesssim_B \varphi(y)$
39. **Изоморфизмом** ЧУМов называют гомоморфизм ЧУМов, являющийся биекцией.
40. **Суммой** ЧУМов $\langle A, \lesssim_A \rangle$ и $\langle B, \lesssim_B \rangle$ называют такой ЧУМ $\langle C, \lesssim_C \rangle$,
что $C = A \cup B, x \lesssim_C y$, если $\begin{cases} 1. x \in B \wedge y \in A \\ 2. x, y \in A \wedge x \lesssim_A y \\ 3. x, y \in B \wedge x \lesssim_B y \end{cases}$
41. **Прозведением** ЧУМов $\langle A, \lesssim_A \rangle$ и $\langle B, \lesssim_B \rangle$ называют такой ЧУМ $\langle C, \lesssim_C \rangle$,
что $C = A \times B, (p, q) \lesssim_C (s, t)$, если $\begin{cases} 1. q \succ_B t \\ 2. q =_B t \wedge p \lesssim_A s \end{cases}$
42. **Декартово проведением** ЧУМов $\langle A, \lesssim_A \rangle$ и $\langle B, \lesssim_B \rangle$ называют такой ЧУМ $\langle C, \lesssim_C \rangle$,
что $C = A \times B, (p, q) \lesssim_C (s, t)$, если $q \lesssim_B t \wedge p \lesssim_A s$

- b. Простые утверждения
- c. Вопросы на 3
- d. Вопросы на 4
- e. Вопросы на 5
- f. Доп вопросы на 5
- g. Доп вопросы на 6
- h. Доп вопросы на 7

III ВЫЧИСЛИМОСТЬ

- a. Определения
- b. Простые утверждения
- c. Вопросы на 3
- d. Вопросы на 4
- e. Вопросы на 5
- f. Доп вопросы на 5
- g. Доп вопросы на 6
- h. Доп вопросы на 7