Билеты по матлогике

МФТИ ФПМИ 2022 г

Содержание

I Логика и арифметика **7**

a. Определения . . . 7

Булевы функции . . . 7

Классы булевых функций . . . 7

Замыкание класса булевых функций . . . 8

Композиция булевых функций . . . 8

Замкнутость . . . 8

Полнота . . . 8

Пропозициональные формулы . . . 8

Скобочный итог . . . 8

Тавтология . . . 8

Противоречие . . . 9

КНФ, ДНФ, СКНФ, СДНФ . . . 9

Полином Жегалкина . . . 9

b. Простые утверждения . . . 9

Т. о существовании КНФ/ДНФ . . . 9

Т. замкнутости классов Поста . . . 10

c. Вопросы на 3 . . . 11

Теорема об однозначном представлении булевой функции многочленом Жегалкина . . . 11

d. Вопросы на 4 . . . 12

e. Вопросы на 5 . . . 12

f. Доп вопросы на 5 . . . 12

Теорема об однозначности синтаксического разбора пропозициональных формул . . . 13

Критерий Поста . . . 13

g. Доп вопросы на 6 . . . 14

Базис монотонных функций . . . 15

h. Доп вопросы на 7 . . . 15

II Теория множеств **16**

a. Определения . . . 16

Множество . . . 16

Объединение . . . 16

Пересечение . . . 16

Разность . . . 16

Симметрическая разность . . . 16

Упорядоченная пара . . . 16

Декартово произведение . . . 16

Соответствие . . . 16
Отображение . . . 16
Образ . . . 16
Проообраз . . . 16
Инъекция . . . 16
Сюръекция . . . 16
Биекция . . . 16
Композиция . . . 16
Множество в степени множества . . . 16
Равномощность . . . 16
Счетность . . . 16
Континуальность . . . 17
Бинарное отношение . . . 17
Свойства отношений . . . 17
Отношение эквивалентности . . . 17
Отношение порядка . . . 17
Линейный порядок . . . 17
ЧУМ . . . 17
ЛУМ . . . 17
Фундированность . . . 17
ВУМ . . . 17
Минимальный элемент . . . 17
Максимальный элемент . . . 18
Наименьший элемент . . . 18
Наибольший элемент . . . 18
Цепь . . . 18
Верхняя грань . . . 18
Нижняя грань . . . 18
Точная верхняя грань . . . 18
Точная нижняя грань . . . 18
Гомоморфизм ЧУМов . . . 18
Изоморфизм ЧУМов . . . 18
Сложение ЧУМов . . . 18
Произведение ЧУМов . . . 18
Декартово произведение ЧУМов . . . 18
Начальный отрезок . . . 18
Предельный элемент . . . 18
Транзитивные множества . . . 18

Порядковые типы и ординалы . . . 18
Аксиома выбора . . . 19
Базис Гамеля . . . 19
b. Простые утверждения . . . 19
Основные тождества тм . . . 19
Равномощность . . . 21
Объединение и декартово произведение счетных множеств . . . 21
В любом бесконечном множестве найдётся счётное подмножество . . . 22
Несчётность множества точек на отрезке . . . 23
Нефундированность прямого лексикографического порядка на конечных словах . . . 23
Любой начальный отрезок вполне упорядоченного множества, отличный от всего множества, представляется в виде $[0, a)$ . . . 23
Вполне упорядоченное множество неизоморфно своему начальному отрезку вида $[0, a)$ . . . 24
Сумма и произведение фундированных множеств фундированы, вполне упорядоченных - вполне упорядочены . . . 24
Свойства сложения и умножения вполне упорядоченных множеств . . . 24
Сравнимость любых двух множеств по мощности . . . 25
c. Вопросы на 3 . . . 25
Эквивалентность фундированности, отсутствия бесконечно убывающей последовательности элементов и принципа трансфинитной индукции . . . 25
Лемма о монотонной функции из вполне упорядоченного множества в себя . . . 26
Теорема о трансфинитной рекурсии . . . 26
d. Вопросы на 4 . . . 27
Сравнимость любых двух вполне упорядоченных множеств . . . 27
Любой частичный порядок можно дополнить до линейного . . . 27
e. Вопросы на 5 . . . 28
Теорема Цермело . . . 28
Лемма Цорна . . . 30
f. Доп вопросы на 5 . . . 30
g. Доп вопросы на 6 . . . 30
h. Доп вопросы на 7 . . . 30

III Вычислимость **31**
a. Определения . . . 31
b. Простые утверждения . . . 31
c. Вопросы на 3 . . . 31
d. Вопросы на 4 . . . 31
e. Вопросы на 5 . . . 31

f. Доп вопросы на 5 31
g. Доп вопросы на 6 31
h. Доп вопросы на 7 31

Предисловие

Данные билеты были написаны Калининым Иваном, поэтому по всем вопросам обращаться ко мне в лс. Также буду признателен за сообщения об обсерах в индексах, как это часто бывает, и об ошибках в определениях/доказательствах - надеюсь, их все же нет.
Экзамен по матлогике предполагает выбор лишь 3-х вопросов по каждой теме из доп вопросов, поэтому здесь написаны лишь по 3 билета на каждый балл доп вопроса на выбор автора теха.

P.S. Данные решения не являются единственно верными, и существует большое множество других вариантов доказательств. Поэтому не надо воспринимать данный тех как сборник единственно верных решений.

I Логика и арифметика

a. Определения

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

   Откуда тривиальным образом[1] 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: $\bot$ - тавтологический 0, $\top$ - тавтологическая 1

Инверсия (отрицание):

x	$\neg x$
0	1
1	0

Конъюнкция:

x_1	x_2	$x_1 \wedge x_2$
0	0	0
0	1	0
1	0	0
1	1	1

Дизъюнкция:

x_1	x_2	$x_1 \vee x_2$
0	0	0
0	1	1
1	0	1
1	1	1

Импликация:

x_1	x_2	$x_1 \to x_2$
0	0	1
0	1	1
1	0	0
1	1	1

Исключающее или (XOR):

x_1	x_2	$x_1 \oplus x_2$
0	0	0
0	1	1
1	0	1
1	1	0

Эквиваленция:

x_1	x_2	$x_1 \leftrightarrow x_2$
0	0	1
0	1	0
1	0	0
1	1	1

Штрих Шеффера (NAND):

x_1	x_2	$x_1 \vert x_2$
0	0	1
0	1	1
1	0	1
1	1	0

Стрелка Пирса (NOR):

x_1	x_2	$x_1 \downarrow x_2$
0	0	1
0	1	0
1	0	0
1	1	0

2. **Классы функций**

   P_0 - Сохраняюшие 0

   Класс[2] булевых функций (далее бф), таких что на наборе (0 ... 0) они принимают значение 0.

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

[2] Множество

P_1 - Сохраняюшие 1

Класс булевых функций (далее бф), таких что на наборе (1 ... 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 $f(x_1 \dots x_n) \geqslant f(x'_1 \dots x'_n)$, если $\forall i \in \{1 \dots n\} \hookrightarrow x_i \geqslant x'_i$

A (L) - Аффиные (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 $(\psi \wedge \varphi)$, $(\psi \vee \varphi)$, $(\psi \to \varphi)$ - 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 $A \to A$

   (b) Закон непротиворечия $\neg(A \wedge \neg A)$

   (c) Закон исключенного третьего $\neg A \vee A$

   (d) Закон двойного отрицания $(A \to \neg\neg A) \wedge (\neg\neg A \to A)$

   (e) Закон контрапозиции $((A \to B) \to (\neg B \to \neg A)) \wedge ((\neg B \to \neg A) \to (A \to B))$

---

[3] Будем вверху в скобках показывать арность функции

[4] Подробнее в пункте про полиномы Жегалкина

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

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

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

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 ровно один раз (или если побольше демагогий, то

    1. каждая переменная не повторяется внутри дизъюнкта

    2. в каждом дизъюнкте присутствуют все переменные от которых зависит функция

    3. нет одинаковых дизъюнктов)

    Совершенной дизъюнктивной нормальной формой (СДНФ) называется такая ДНФ, что в каждом дизъюнкте каждая переменная встречается ровно один раз (или если побольше демагогий, то

    1. каждая переменная не повторяется внутри конъюнкта

    2. в каждом конъюнкте присутствуют все переменные от которых зависит функция

    3. нет одинаковых конъюнктов)

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.

b. 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 переменную[7] в дизъюнкт, иначе - ее отрицание. Потом возьмем конъюнкцию всех дизъюнктов. Формально получим:

$$CNF_\psi = \bigwedge_{\substack{x \in \{0,1\}^n \\ f(x)=0}} \bigvee_{j=1}^{n} p_i^{1-x_i}, \quad \text{где } p_i^{x_i} = \begin{cases} p_i & x_1 = 1 \\ \neg p_i & x_i = 0 \end{cases}$$

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

[7] Будем обозначать i-ую переменную как p_i

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

$$DNF_\psi = \bigvee_{\substack{x \in \{0,1\}^n \\ f(x)=1}} \bigwedge_{j=1}^{n} p_i^{x_i}, \quad \text{где } p_i^{x_i} = \begin{cases} p_i & x_1 = 1 \\ \neg p_i & x_i = 0 \end{cases}$$

Заметим, что каждый конъюнкт $\bigwedge\limits_{j=1}^{n} p_i^{x_i}$ истенен только на своем наборе x, поэтому конечная формула будет истинна только на тех наборах, где бф принимает 1, значит, постоили 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:

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

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

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

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

P_1:

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

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

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

M:

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

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

Пусть $x, y - n$-мерные векторы[8] $x \geqslant y$ (покоординатно)

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

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

S:

$$f^{(n)},\, g^{(k)} = \begin{Vmatrix} g_1^{(k)} \\ \vdots \\ g_n^{(k)} \end{Vmatrix} \in S$$

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

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

A:

$$f^{(n)},\, g^{(k)} = \begin{Vmatrix} g_1^{(k)} \\ \vdots \\ g_n^{(k)} \end{Vmatrix} \in A$$

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

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

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

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

c. 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 Жегалкина[10]

   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

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

[9] Покомпонентная инверсия вектора

[10] Здесь предполагается, что все повторяющиеся мономы сокращены

существуют два различных полинома, представляющих одну и ту же функцию. Вычтем их друг из друга и получим противоречие

Формально:

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

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

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

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

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 спроста называется полиномом))[11], то перенесем все вправо и получим (Помним, что xor - 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 формула[12]*, 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 итоге не влияет, то на $\neg$ - выполнено, а далее все как и в ψ - поэтому верно

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

[11] Это все же лучше не говорить на экзамене

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

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

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 итоге формулы есть сумма скобочных итогов (, ψ, $*$, φ' - он больше 0, т.к. по предположени индукции для φ' 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 беспрефиксноти 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 одназначно 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 беспрефиксносте. **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, дляя 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 ... 0) = 1, если тогда еще f не сохраняет 1, то f(1 ... 1) = 0, т.е. f(p ... p) - отрицание. Иначе f(1 ... 1) = 1, т.е f(p ... p) - $\top$. Т.к. g не сохраняет 1, то все то же самое - $\bot$ 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 р и отрицания р 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.

а - неафинная функция. Тогда пускай БОО он содержит моном, включающий в себя x_1, x_2, т.е. $a = x_1x_2P(x_3 \dots x_n) \oplus x_1Q(x_3 \dots x_n) \oplus x_2R(x_3 \dots x_n) \oplus S(x_3 \dots x_n)$. 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 $\hat{a} = x_1x_2 \oplus qx_1 \oplus rx_2 \oplus s$

Тогда имеем функции:

q	r	s	$\hat{a}$
0	0	0	$x_1 \wedge x_2$
0	0	1	$x_1 \vert x_2$
0	1	0	$x_1 \nrightarrow x_2$
0	1	1	$x_1 \rightarrow x_2$
1	0	0	$x_1 \nleftarrow x_2$
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 $\bot, \top, \neg$ и одну из функций выше $\wedge$ - получим систему $(\neg, \wedge)$ - полную. **Ч.Т.Д.**

g. 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:

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

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

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

Значит, $g(x_1 \wedge y_1, \dots, x_n \wedge y_n) = g(x_1, \dots, x_n) \wedge$[14]$g(y_1, \dots, y_n)$

[14] Покомпонентная конъюнкция

$$\text{Тогда, } h(x_1 \wedge y_1, \ldots, x_n \wedge y_n) = f(g(x_1 \wedge y_1, \ldots, x_n \wedge y_n)) = f(g(x_1, \ldots, x_n) \wedge g(y_1, \ldots, y_n)) =$$
$$= f(g(x_1, \ldots, x_n)) \wedge f(g(y_1, \ldots, y_n)) = h(x_1, \ldots, x_n) \wedge h(y_1, \ldots, y_n) \Rightarrow h \in \bigwedge$$

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

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 выполенено, иначе - не константа, тогда на (0 ... 0) она принимает значение 0, а на (1 .. 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

a. Определения

1. ***Множество*** - неопределяемое понятие

2. ***Объединение множеств***:
$$A \cup B := \{x \,|\, x \in A \vee x \in B\}$$

3. ***Пересечение множеств***:
$$A \cap B := \{x \,|\, x \in A \wedge x \in B\}$$

4. ***Разность множеств***:
$$A \setminus B := \{x \,|\, x \in A \wedge \neg(x \in B)\}$$

5. ***Симметрическая разность множеств***:
$$A \triangle B := \{x \,|\, x \in A \oplus x \in B\}$$

6. ***Упорядоченная пара***
$$\text{По Куратовскому:} \quad (a, b) := \{a, \{a,\, b\}\}$$

7. ***Декартово произведение***
$$A \times B := \{(a,\, b) \,|\, a \in A,\, b \in B\}$$

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

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

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

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

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

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

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

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

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 $\precsim$ на A будет называться ***линейным***, если:
    $$\forall a \in A\, \forall b \in A \hookrightarrow a \precsim b \vee b \precsim a$$

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 элемент[15], называется ***фундированным***.

28. Фундированное множество с линейным порядком называется ***Вполне Упорядоченным Множеством - ВУМ***

[15] т.е. такой, меньше которого нет, - не путать с наимешьшим - 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 $\langle M, \precsim\rangle$ называют последовательность элементов $a_1 \dots a_n$, такую что $a_1 \precsim a_2 \precsim \dots \precsim a_n$

34. ***Верхей гранью*** множества $S \subseteq M : \langle M, \succsim\rangle$ называется $m \in M$, такое что $\forall s \in S\,(m \succsim s)$

35. ***Нижней гранью*** множества $S \subseteq M : \langle M, \succsim\rangle$ называется $m \in M$, такое что $\forall s \in S\,(s \succsim m)$

36. ***Точной верхей гранью*** множества $S \subseteq M : \langle M, \succsim\rangle$ или *супремумом* называют такую верхнюю грань, что она принадлежит S и является наимешьшей среди всех остальных верхних граней.

37. ***Точной нижней гранью*** множества $S \subseteq M : \langle M, \succsim\rangle$ 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: $\langle A, \succsim_A\rangle$ и $\langle B, \succsim_B\rangle$ - ЧУМы, $\varphi : A \to B$ - гомоморфизм, если $\forall x,\, y \in A\,(x \succsim_A y \Leftrightarrow \varphi(x) \succsim_B \varphi(y))$

39. ***Изоморфизмом*** ЧУМов называют гомоморфизм ЧУМов, являющийся биекцией.

40. ***Суммой*** ЧУМов $\langle A, \succsim_A\rangle$ и $\langle B, \succsim_B\rangle$ называют такой ЧУМ $\langle C, \succsim_C\rangle$,

    что $C = A \cup B,\, x \succsim_C y, \quad$ если $\begin{cases} 1.\ x \in B \wedge y \in A \\ 2.\ x,\, y \in A \wedge x \succsim_A y \\ 3.\ x,\, y \in B \wedge x \succsim_B y \end{cases}$

41. ***Прозведением*** ЧУМов $\langle A, \succsim_A\rangle$ и $\langle B, \succsim_B\rangle$ называют такой ЧУМ $\langle C, \succsim_C\rangle$,

    что $C = A \times B,\, (p,\, q) \succsim_C (s,\, t), \quad$ если $\begin{cases} 1.\ q \succ_B t \\ 2.\ q =_B t \wedge p \succsim_A s \end{cases}$

42. ***Декартово прозведением*** ЧУМов $\langle A, \succsim_A\rangle$ и $\langle B, \succsim_B\rangle$ называют такой ЧУМ $\langle C, \succsim_C\rangle$, что $C = A \times B,\, (p,\, q) \succsim_C (s,\, t), \quad$ если $q \succsim_B t \wedge p \succsim_A s$

43. Пусть ВУМ Ψ разбит на две непересекающиеся части $M \sqcup \Lambda = \Psi$, такие что $\forall \mu \in M\, \forall \lambda \in \Lambda\,(\mu < \lambda)$. Тогда множество M называется ***начальным отрезком*** ВУМа Ψ.

44. ***Предельным элементом*** в ВУМе называют такой элемент, у которого нет предыдущего. Формально:

    $$\langle A, \leqslant_A\rangle \text{ - ВУМ, тогда } a \text{ - предельный, если } \nexists y : y \leqslant a$$

45. Множество M называется ***транзитивным***, если $\forall A \in M\, \forall x \in A\,(x \in M)$

46. ***Порядковым типом*** или ***ординалом*** называют такое транзитивное множество, что любой его элемент тоже транзитивен.

    Примеры:

    1. ω - наименьший счетный ординал, $\omega = sup\{1, 2, 3, 4, \dots\}$
    2. ω^k, $k \in \mathbb{N} = \omega^{k-1} \cdot \omega$, причем $\omega^0 = 1$
    3. $\omega^\omega = sup\{\omega^0, \omega^1, \omega^2, \omega^3, \dots\}$
    4. $\varepsilon_0 = sup\{\omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \dots\}$

47. ***Аксиома выбора***

    Формулировки (эквивалентны):

    1. $\forall M\, \exists \varphi \,:\, 2^M \setminus M \to M$ такая что $\forall M' \subsetneq M (\varphi(M') \notin M')$
    2. $\forall M\, \exists \varphi \,:\, 2^M \setminus \varnothing \to M$ такая что $\forall M' \subsetneq M (\varphi(M') \in M')$

48. ***Базисом Гамеля***[16] называется линейно независимый набор векторов, такой что любой вектор пространства является их линейной комбинацией.

b. Простые утверждения

1. Основные тождества теоретико-множественных операций, декартово произведение и возведение множества в степени множества.

   Данные тождества слишком тривиальны, чтобы приводить их доказательства. Опишу лишь способы доказательства:

   - Круги Эйлера

   Просто нарисовали три кружочка и красим области

   - По определению

   Расписываем, что значит, что x принадлежит левой части равенства, выводим из этого правую. (Показали вложенность левого множества в правом) Аналогично проделываем справа налево. В итоге правое в левом, а левое в правом, следовательно, они равны.

   - Булевы функции

   Данный метод эквивалентен предыдущему. Сопоставляем каждому множеству в равенстве его характеристическую функцию (1 - если лежит, 0 - в противном случае) и переходим на булевы функции и фокусы покусы там. Вот список переходов из операций тм в операции бф:

ТМ	БФ
$\cup$	$\vee$
$\cap$	$\wedge$
$\triangle$	$\oplus$
$\setminus$	$\not\to$
$-$	$\neg$

[16] Или если говорить для простых смертных *просто базисом*

Теперь сами тождества:

Ассоциативность

$(A \cup B) \cup C = A \cup (B \cup C)$

$(A \cap B) \cap C = A \cap (B \cap C)$

$(A \triangle B) \triangle C = A \triangle (B \triangle C)$

Коммутативность

$A \cup B = B \cup A$

$A \cap B = B \cap A$

$A \triangle B = B \triangle A$

Инволютивность

$\overline{\overline{A}} = A$

Идемпотентность

$A \cup A = A$

$A \cap A = A$

Аннигиляция

$A \setminus A = \varnothing$

$A \triangle A = \varnothing$

де Моргана

$\overline{A \cup B} = \bar{A} \cap \bar{B}$

$\overline{A \cap B} = \bar{A} \cup \bar{B}$

Дистрибутивность

$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$

$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

$(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$

Правила отождествления кортежей[17]:

1. $((a,\, b),\, c) \sim (a,\, (b,\, c))$

2. $(a,\, \varnothing) \sim (a)$

3. Правила 1 и 2 можно применять к составным частям кортежа. Свойства декартового умножения:

$(A \times B) \times C \sim A \times (B \times C)$

$A^n \sim \underbrace{A \times A \times \dots \times A}_{\text{n раз}}$

$A^m \times A^k \sim A^{m+k}$

$A \times \{\varnothing\} \sim A$

$(A^n)^m \sim A^{nm}$

Доказательства

1. Вытекает из того, что мы отождествляем $((a,\, b),\, c)$ и $(a,\, (b,\, c))$

[17]Здесь надо напомнить, что под кортежем длины 0 мы понимаем пустое множество, а под кортежем длины $n > 0$ мы понимаем упорядоченную пару из первого элемента данного кортежа и другого кортежа длины $n-1$, построенного из оставшихся элементов

2. Вытекает из того, что мы отождествляем $((\dots((a_0,\, a_1), a_2)\dots),\, a_n)$ и $(a_0,\, a_1\, \dots,\, a_n)$

3. Аналогично отождествляем $(x,\, \varnothing)$ и x

4. Данное отождествление выполняется, если сраведливо отождествление $((a_1,\, \dots,\, a_k),\, (a_{k+1},\, \dots,\, a_n)) \sim (a_1,\, \dots,\, a_n)$. Покажем это:

$((a_1,\, \dots,\, a_k),\, (a_{k+1},\, \dots,\, a_n)) \sim ((a_1,\, \dots,\, a_k),\, (a_{k+1},\, (a_{k+2},\, \dots,\, a_n))) \sim (((a_1,\, \dots,\, a_k),\, a_{k+1}),\, (a_{k+2},\, \dots,\, a_n))) \sim ((a_1,\, \dots,\, a_k,\, a_{k+1}),\, (a_{k+2},\, \dots,\, a_n))) \sim \dots \sim ((a_1,\, \dots,\, a_n),\, \varnothing) \sim (a_1,\, \dots,\, a_n)$

5. Абсолютно также показывается, что $((a_{1,\,1},\, \dots,\, a_{n,\,1}),\, \dots,\, (a_{1,\,m},\, \dots,\, a_{n,\,m})) \sim (a_1,\, \dots,\, a_n m)$

Свойста возведения множеств в степень множества:

1. $A^B \times A^C \cong A^{B\sqcup C}$

2. $A^C \times B^C \cong (A \times B)^C$

3. $(A^B)^C \cong A^{B\times C}$

Доказательства

1. Элемент $A^{B\sqcup C}$ - это функция $f\,:\,(B\sqcup C)\to A$, элемент $A^B\times A^C$ - это пара функций $(g_1,\, g_2)$, таких что $g_1\,:\,B\to A,\; g_2\,:\,C\to A$. Рассмотрим функцию[18] $\varphi\,:\,f\mapsto(g_1,\, g_2),\, \varphi\,:\,\begin{cases} g_1(x)=f(x), \text{ если } x\in B \\ g_2(x)=f(x), \text{ если } x\in C\end{cases}$

Данная функция - это биекция[19].

2. Аналогичными соображениями с п.1 получаем биекцию $\varphi\,:\,f\mapsto(g_1,\, g_2),\, \varphi\,:\,\begin{cases} g_1 = pr_1\circ f \\ g_2 = pr_2\circ f\end{cases}$, где pr_i - функция возвращающая i-ую компоненту кортежа (по сути проектор).

3. Аналогичными соображениями с п.1 получаем биекцию $\varphi\,:\,f\mapsto h$, где $f\,:\,C\to g,\; g\,:\,B\to A$, $h\,:\,(B\times C)\to A,\, \varphi\,:\,h(b,\, c)=(f(c))(b)$[20].

2. Равномощность - отношение эквивалентности.

Доказательство

1. Рефлексивность

$A\cong A$, т.к. существует биекция из A в A: $id_A\,:\,A\to A$ - тождественное отображение.

2. Симметричность

Пусть $A\cong B$, тогда есть биекция $\psi\,:\,A\to B$. Но $\psi^{-1}\,:\,B\to A$ - обратное отображение к ψ - тоже биекция. Откуда получаем, что $B\cong A$

3. Транзитивность

Пусть $A\cong B$ и $B\cong C$, тогда найдутся две биекции $\varpi\,:A\to B$ и $\vartheta\,:\,B\to C$. Возьмем их композицию: $\varphi=\vartheta\circ\varpi,\, \varphi\,:\,A\to C$, т.к. композиция двух биекций - биекция, то получим, что $A\cong C$.

Выполнены три аксиомы отношения эквивалентности $\Rightarrow$ равномощность - отношение эквивалентности.

Ч.Т.Д.

[18]Это такая интересна херня, которая по одной функции строит две

[19]Биективность ее очевидна: по любым двум можно построить прообраз просто объединив их - имеем сюръективность, по различным двум функциям получатся две различные пары (отличаются значения на каком-то х, БОО он в В $\Rightarrow g_1$ от них будут различны) - значит инъективна

[20]Напоминаем, что $f(c)$ - это какая-то функция из B в A

3. Объединение счётных множеств счётно.

   Пусть А и В - счетные множества, $\alpha : \mathbb{N} \to A$, $\beta : \mathbb{N} \to B$ - их биекции из натуральных чисел. Если пересечение А и В пусто, то построим биекцию $\gamma : \mathbb{N} \to (A \sqcup B)$ по следующему правилу: если x - четно, то $\gamma(x) = \alpha(x)$, иначе $\gamma(x) = \beta(x)$. Если же их пересечение непусто, то их объединение содержит А, следовательно, не менее чем счетно. Но с другой стороны $A \cup B = A \sqcup (B \setminus (A \cap B))$, $(B \setminus (A \cap B)) \subseteq B$, а потому не более чем счетно, значит, их их дизъюктное объединение не более чем счетно (Здесь формально делается так: А счетно, потому есть биекция в четные числа, из В аналогично в нечетные, тогда если $(B \setminus (A \cap B)) \subseteq B$, то есть биекция из $(B \setminus (A \cap B))$ в некоторое подмножество нечетных. Тогда их дизъюнктное объединение - биекция в некоторое подмножество натуральных чисел (четные и нечетные - непересекаются, потому все ок), а, значит, не более чем счетно)[21], откуда по теореме Кантора-Бернштейна имеем счетность их объединения.

4. Декартово произведение счётных множеств счётно.

   Аналогично А и В - счетные множества. Тогда построим табличку $\mathbb{N} \times \mathbb{N}$, в которой под элементом на пересечении i-ой строки и j-го столбца будем понимать пару из i-го элемента А и j-го элемента В:

	1	2	3	4	5	...
1	1	2	4	7	11	...
2	3	5	8	12	17	...
3	6	9	13	18	24	...
4	10	14	19	25	32	...
5	15	20	26	33	41	...
...	...	...	...	...	...	...

   Для данной нумерации можно привести конкретную функцию:

   Элементу (i, j) сопоставляется число $\frac{i(i+1)}{2} + \frac{2i-2+j}{2}(j-1)$.[22] Инъективность данной формулы очевидна, сюръективность же.. Расскажем как искать прообраз числа:

   Сначала зажимаем натуральное число между двумя треугольными: по сути решаем уравнение $\frac{k(k+1)}{2} = n$ или $k^2 + k - 2n = 0$ Используем всемогущий дискриминант $k_1 = \frac{\sqrt{1+8n}-1}{2}$, $k_2 = \frac{-\sqrt{1+8n}-1}{2}$. Так как работаем с натуральными числами, то, очевидно, что нам нужен k_1, или, если быть точнее, $\varkappa = \lceil k_1 \rceil$[23]. Теперь вычисляем $\Delta = \frac{\varkappa(\varkappa+1)}{2} - n$. Тогда прообразом числа n будет $(\varkappa - \Delta, \Delta + 1)$. Откуда имеем биекцию.[24]

5. В любом бесконечном множестве найдётся счётное подмножество.

[21] Данный метод необходим в силу того, что первый способ применим только для дизъюнктного объединения

[22] Для тех кому интересно откуда такая чудо формула: Заметим что, по первому столбцу расположены треугольные числа для них формула $\frac{i(i+1)}{2}$, далее числа в i-ой строке получаются прибавлением i, $i+1$, ... к первому числу в строке - арифметическая прогрессия, формула $\frac{2i-2+j}{2}(j-1)$

[23] Округляем **вверх**

[24] Очень вероятно, что вас кокнет это говно, поэтому объясню зачем: далее в блоке вычислимость будет нужно говорить про вычислимую в обе стороны биекцию, здесь же она и приведена. Да еще и показана как все вычисляется в обе стороны.

Пусть $\mathcal{M}$ - бесконечное множество. Выделим из него счетное подмножество $\mathcal{L}$ следующим образом: согласно аксиоме выбора, т.к. $\mathcal{M} \neq \varnothing$ можно выбрать какой-то элемент $\alpha_0 \in \mathcal{M}$, положим его в $\mathcal{L}$. Далее т.к. $\mathcal{M} \setminus \{\alpha_0\} \neq \varnothing$ (иначе $\mathcal{M}$ было бы конечно), то выделим из него α_1 и снова положим в $\mathcal{L}$. Аналогичным образом будем продолжать для любого α_i - таким образом выделим счетное подмножество $\mathcal{L} = \{\alpha_0, \alpha_1, \alpha_2, \dots\}$

6. Несчётность множества точек на отрезке.

   Т.к. любой отрезок $[\alpha; \beta]$ может быть получен из $[0; 1]$ путем применения к элементам $[0; 1]$ следующей функции[25] $\psi(x) = (p \circ r)(x)$, где $p(x) = x + \alpha$, а $r(x) = \beta x$, то достаточно показать несчетность точек на $[0; 1]$. Для этого воспользуемся приемом, называемым **диагональным методом Кантора**

   Сопоставим каждому числу из $[0; 1]$ его разложение в виде бесконечной десятичной дроби, у которой целая часть равна 0. (Для 1 – это 0,91)) Оговорим, что если есть два представления, а именно БОО[26] $0,\dots 1(0)$ и $0,\dots 0(9)$, то для однообразности выберем второй вариант. Теперь предположим обратное: чисел на единичном отрезке лишь счетное число.[27] Тогда построим число γ следующим образом:

   1. $\gamma = 0,$

   2. Берем i-ое число и его i-ую цифру в дробной части. Если она равна 9, то i-ую цифру в дробной части числа γ положим за 0, иначе за 9.

   Очевидно, $\gamma \in [0; 1]$, но оно отличается от всех занумерованных чисел. Получили противоречие, значит их несчетно. **Ч.Т.Д.**

7. Нефундированность прямого лексикографического порядка на конечных словах.

   Сначала напомним, что есть прямой лексикографический порядок. Пусть задан порядок на символах алфавита. Тогда $a \prec b$, если:

   1. $a \sqsubset$ [28]b

   2. $a = \sigma_0\sigma_1 \dots \sigma_n\tau \dots, \;\; b = \sigma_0\sigma_1 \dots \sigma_n\pi \dots \;$ и $\tau \prec \pi$

   Теперь покажем бесконечно убывающую цепочку, что равносильно нефундированности[29]:

   1. 11

   2. 101

   3. 1001

   4. 10001

   5. 100001

   6. 1000001

   ...

8. Любой начальный отрезок вполне упорядоченного множества, отличный от всего множества, представ-

[25] Это биекция как композиция биекций, потому они все равномощны. Биективность же p и r остается в качестве несложного упражнения читателю))

[26] Возможно не 1 и 0, а 2 и 1, 3 и 2 ...

[27] Формально обратным будет утверждение, что их не более чем счетное, но их бесконечность весь очевидна, а кому нет - тогда вот вам числа: $\{\frac{1}{n}\}$ их бесконечно много, значит и на $[0; 1]$ тоже бесконечно много.

[28] Не совпадают конечно же

[29] Здесь приведен пример для $\{0, 1\}^*$ как стандартного алфавита для машин Тьюринга

ляется в виде $[0,\, a)$.

Назовем исходное множество , а отрезок . Тогда из того, что $O \neq M$ имеем $M \setminus O \neq \varnothing$, а значит из фундированности M имеем $\exists a\, (a = min(M \setminus O))$ из линейности порядка получим, что а - наименьший. 1. $O \subseteq [0,\, a)$: От противного, пусть есть х принадлежащий $[0,\, a)$, но не O, тогда а - не минимальный. 2. $[0,\, a) \subseteq O$: Возьмем произольный элемент M который не лежит в O, тогда он лежит в $M \setminus O$. Значит, он больше или равен а (а - наименьший), следовательно, он не лежит в $[0,\, a)$. По контрапозиции получим, если элемент лежит в $[0,\, a)$, то он также лежит и в O.

Тогда имеем, что $O = [0;\, a)$ **Ч.Т.Д.**

9. Вполне упорядоченное множество неизоморфно своему начальному отрезку вида $[0,\, a)$.

   Доказательство: (от противного)

   Пусть $\psi : M \to [0,\, a)$ - изоморфизм. Он сохраняет порядок, а потому монотонная функция. $\psi(a) \in [0,\, a) \Rightarrow \psi(a) < a$. Тогда по лемме о монотонной функции $\psi(a) \geqslant a$ - имеем противоречие. **Ч.Т.Д.**

10. Сумма и произведение фундированных множеств фундированы, вполне упорядоченных - вполне упорядочены.

    Сумма:

    Пусть $\Lambda \subseteq A + B$. Если $\Lambda \subseteq A$ или $\Lambda \subseteq B$, то в нем есть минимальный элемент, как подмножества фундированных множеств, если же Λ содержит элементы и из А и из В, то рассмотрим $\Lambda' = \Lambda|_A$, т.е. все такие х из Λ, что лежат в А, Λ' имеет минимальный, как подмножество фундированного, но его минимальный также является минимальным для Λ, ибо все элементы из В больше чем элементы из А в данной сумме[30]. Тогда любое подмножество А + В имеет минимальный, откуда, сумма фундированна.

    Произведение:

    Пусть $\Lambda = A \cdot B$. Рассмотрим произвольную убывающую цепочку Λ. В - фундированно, значит любая убывающая цепочка должна стабилизироваться, т.е. вторая координата рано или поздно стабилизируется, тогда из определения порядка на произведении, если бы существовала бесконечно убывающая цепочка, то должна была бы бесконечно убывать первая координата, но первая координата - это элементы А, которое в свою очередь также фундированно, значит любая цепочка в произведении стабилизируется. Откуда получаем ее фундированность.

    Осталось добавить, что сумма и произведение ЛУМов - ЛУМ. (Если любые два элемента А и В сравнимы, то любые элементы сравнимы либо если оба из А/В, либо если один из А, а второй из В - то по определению порядка на сумме. На произведении получим же, что все первые/вторые координаты сравнимы между собой, тогда по определению порядка любые две пары из произведения сравнимы). Тогда получим фундированность + ЛУМ = ВУМ **Ч.Т.Д.**

11. Свойства сложения и умножения вполне упорядоченных множеств.

    Сумма:

[30] Если бы взяли В + А, то все было бы наоборот.

Ассоциативность

(A + B) + C = A + (B + C) - Следует напрямую из ассоциативности объединения множеств

Отсутствие коммутативность

$\{a\} + \mathbb{N} \not\simeq \mathbb{N} + \{a\}$, т.к. первое не имеет наибольшего элемента, а второе имеет.

Нейтральный элемент

$\forall A\,(\varnothing + A = A + \varnothing = A)$, т.к. $\varnothing \cup A = A \cup \varnothing = A$

Произведение:

Ассоциативность

(A · B) · C = A · (B · C) - Следует напрямую из ассоциативности объединения множеств

Отсутствие коммутативность

$\{1, 2\} \cdot \mathbb{N} \not\simeq \mathbb{N} \cdot \{1, 2\}$, т.к. первое изоморфно $\mathbb{N}$ - изоморфно покраске четных чисел в 2, а нечетных в 1, второе же изоморфно $\mathbb{N} + \mathbb{N}$ - в нем есть 2 предельных элемента (0 из первой копии и 0 из второй), в первом же нет.

Нулевой элемент

$\forall A\,(\varnothing \cdot A = A \cdot \varnothing = \varnothing)$, т.к. $\varnothing \times A = A \times \varnothing = \varnothing$

Левая дистрибутивность и отсутствие правой

$A \cdot (B + C) = (A \cdot B) + (A \cdot C)$ Это вытекает из дистрибутивности декартого произведения множеств и объединения + справа все элементы из B меньше C, тогда при сравнении по второй координате пары (a, b) < (a, c), что равносильно сложить все пары (a, b) и (a, c) способом слева.

Но $(\{1\} + \{2\}) \cdot \mathbb{N} \not\simeq (\{1\} \cdot \mathbb{N}) + (\{2\} \cdot \mathbb{N})$ первое в свою очередь изоморфно $\mathbb{N}$, а второе $\mathbb{N} + \mathbb{N}$, что, как было отмечено выше, не изоморфно.

12. Сравнимость любых двух множеств по мощности.

    По теореме Цермело вполне упорядочим данные два множества. Далее к ним можно применить теорему о сравнении ВУМов, получим, что одно изоморфно начальному отрезку другого, а, значит, есть биекция в некоторое подножество, откуда получим, что одно множество не более мощно, чем другое. (Возможно, и из второго есть изоморфизм в начальный отрезок первого - тогда по теореме Кантора-Бернштейна получим равномощность, но это только возможно)

c. Вопросы на 3

1. **Эквивалентность фундированности, отсутствия бесконечно убывающей последовательности элементов и принципа трансфинитной индукции.**

   Данные три определения эквивалентны:

   1. Множество фундированно, т.е. в любом его непустом множестве есть минимальный элемент

   2. Во множестве нет бесконечно убывающей цепочки

   3. Ко множеству применим принцип индукции:

$$\forall x\,(\forall y\,((y < x) \to A(y)) \to A(x)) \to \forall x A(x)$$

Доказательство:

$\neg 1 \to \neg 2$

Если M не пусто[31] и не фундированно, то существует M' $\subseteq$ M, не имеющее минимального элемента, т.е. $\forall x \in M' \, \exists y \in M' \, (y < x)$. Возьмем произвольный $x_0 \in M'$, для него есть $x_1 < x_0$, для которого найдется $x_2 < x_1 < x_0$ и т.д. - имеем бесконечно убывающую цепочку.

$\neg 2 \to \neg 1$

Если есть бесконечно убывающая цепочка во множестве, то возьмем его подмножество, порожденное данной цепочкой, в нем не найдется минимального элемента.

$3 \to 1$ - от противного

Пусть M не фундированно, тогда B - его непустое подмножество без минимального элемента. Положим A(x) - x $\in \bar{M}$. Если для всех y $<$ x это верно, то и для x тоже, иначе x - минимальный элемент, а такого в B нет. Значит, по индукции получим, что для всех элементов B справедливо, что они лежат в его дополнении, т.е. B - пусто. Противоречие

$1 \to 3$ - от противного

Пусть M - фундированно, тогда пусть верно предположение для A(x), но она - верная не везде функция. Значит, множество {x | $\neg$A(x)} не пусто, откуда по фундированности найдется его минимальный элемент - x_0, тогда для любого $y < x_0$ A(y) верно, откуда по предположению индукции A(x_0) истинно, что противоречит выбору x_0, тогда A(x) истинна на всех x.

2. **Лемма о монотонной функции из вполне упорядоченного множества в себя.**

   Пусть f - строго монотонная функция действующая из ВУМа в самого себя, тогда образ любого элемента ВУМА больше или равен емму самому. Формально:

$$\forall x \forall y ((x < y) \to (f(x) < f(y))) \quad \text{Тогда } \forall x (f(x) \geqslant x)$$

   Через фундированность:

   Пусть $A = \{x \,|\, f(x) < x\} \neq \varnothing$, тогда найдется x_0 - его минимальный элемент, тогда $f(x_o) < x_0$. По монотонности $f(f(x_o)) < f(x_o)$, значит $f(x_o) \in A$ - имеем противоречие с минимальностью x_0.

   Через бесконечный спуск:

   Опять же от противного пусть существует x, такой что f(x) $<$ x, тогда по монотонности f(f(x)) $<$ f(x) $<$ x, и так далее - получим бесконечную цепочку - получим противоречение с тем, что исходное множество ВУМ.

   Через индукцию:

   Пусть $\forall y < x (f(y) \geqslant y)$, но $f(x) < x$, тогда по монотонности: $f(f(x)) < f(x)$, но по предположению индукции $f(f(x)) \geqslant f(x)$ - противоречие, следовательно, $f(x) \geqslant x$. Откуда по принципу индукции имеем: $\forall x (f(x) \geqslant x)$

3. **Теорема о трансфинитной рекурсии.**

   Сначала немного обозначений:

[31] Думаю данный случай тривиален и не стоит расписывания

$f(x) = F(f(y)|_{y<x})$ - Рекуррентно заданная функция f рекурсивным правилом F.

Формулировка теоремы:

Если A - ВУМ, то любое рекурсивное правило F задает функцию f, причем единственным образом.

Доказательство

1. Существование

Зададим свойство $A(x)$ - существует $f|_{[0,\,x)}$, заданное правилом F.

Пусть найдется такое t, что $x = t + 1$. Тогда по предположению индукции верно $A(t)$, т.е. существует $f|_{[0,\,t)}$, тогда определим $f(t) = F(f|_{[0,\,t)})$. Откуда определено $f|_{[0,\,t+1)}$ или же $f|_{[0,\,x)}$

Теперь пусть x - предельный элемент. Тогда по предположению индукции $f|_{[0,\,t)}$ определено для всех $t < x$. Значит, положим $f|_{[0,\,x)}$ как объединение всех $f|_{[0,\,t)}$ - по единственности все будет корректно (см. далее)

2. Единственность

От противного: пусть по одному и то му же рекурсивному правилу заданы две различные функции: $f(x) = F(f(y)|_{y<x})$ и $g(x) = F(g(y)|_{y<x})$. Тогда $\exists x\,(g(x) \neq f(x))$ Из того, что A - ВУМ, среди данных иксов будет минимальный - x_0. Значит $\forall y < x_0\,(f(y) = g(y)) \Rightarrow f|_{[0,\,x_o)} = g|_{[0,\,x_o)} \Rightarrow f(x_0) = F(f(y)|_{y<x_0}) = F(g(y)|_{y<x_0}) = g(x_0)$ - Противоречие. **Ч.Т.Д.**

d. Вопросы на 4

1. **Сравнимость любых двух вполне упорядоченных множеств.**

   Сначала введем отношение порядка на всех ВУМах: скажем, что $A < B$, если A изоморфно некоторому собственному[32] начальному отрезку B.

   Теперь перейдем к доказательству самой теоремы. Пусть A и B - ВУМы. Введем функцию $f(a) = min\{b \in B \,|\, b \neq f(t)\,\text{для}\,t < a\}$ Пусть это не сюръекция, тогда найдутся такое b, что $f^{-1}(b)$ неопределено. Выберем из них минимальное - b_0, так как B - ВУМ. Для всех $k < b_0$ $f^{-1}(k)$ определена. Возьмем минимум из всех $m > f^{-1}(k)\forall k$. Тогда для него по построению должен был использоваться b_0 - противоречие. Итого сюръекция. Покажем сохранение порядка: Если $k < t$, то если $f(t) < f(k)$, получим, что когда определяли $f(k)$, $f(t)$ было не занято, а потому мы не могли выбрать $f(k)$, равенство же не достигается из того, что в определении есть $b \neq f(t)$ - это показывает инъективность фунцкии. Итого получили, что данная функция действительно изоморфизм.

   Возможно, f будет неопределено, если множество внутри min - пустое. Тогда по обощенной теореме о трансфинитной рекурсии f определено либо на начальном отрезке, либо на всем A. В первом случаем получим что $A < B$, во втором же если образ A - все B, то они изморфны, иначе образ - не все,

2. **Любой частичный порядок можно дополнить до линейного.**

   Пусть $\mathcal{O}$ - частичный порядок. Рассмотрим семейство частичных порядков $\mathcal{PO}$ с введенным на нем отношением вложенности порядков. Тогда покажем выполнимость условия леммы Цорна для этого множества:

[32] Т.е. не равному самому множеству

Пусть $\mathcal{R} = \{\mathcal{R}_\alpha\}$ - это какая-то цепь из порядков. Она определенно имеет верхнюю грань - объединение всех порядков как множеств пар. Покажем, что данное объединение тоже порядок:

Рефлексивность:

$x \in \mathcal{R} \Rightarrow x \in \mathcal{R}_\alpha \Rightarrow x\mathcal{R}_\alpha x \Rightarrow x\mathcal{R}x$

Антисимметричность:

Если обе пары лежат в одном и том же множестве - все вытекает из порядка соответствующего множества, если же нет, то: $x\mathcal{R}_\alpha y$, $y\mathcal{R}_\beta x$ БОО $\mathcal{R}_\alpha \subset \mathcal{R}_\beta$. Тогда $x\mathcal{R}_\alpha y \Rightarrow x\mathcal{R}_\beta y$ По антисимметричности $\mathcal{R}_\beta$ имеем равенство.

Аналогично транзитивность.

Покажем, что $\mathcal{R}$ - линейный порядок. Пусть не так, тогда $\exists a \exists b\, (\neg a\mathcal{R}b \wedge \neg b\mathcal{R}a)$. Определим порядок $\mathcal{R}'$ как $x\mathcal{R}'y$ если $\left[\begin{array}{c} x\mathcal{R}y \\ \\ x\mathcal{R}a \wedge b\mathcal{R}y \end{array}\right.$

Очевидно, $\mathcal{R} \subsetneq \mathcal{R}'$. Покажем, что $\mathcal{R}'$ - тоже порядок, тогда получим противоречие, а, значит, докажем теорему.

Рефлексивность, тривиально выполнена.

Антисимметричность:

1. $x\mathcal{R}y \wedge y\mathcal{R}x$ - все супер по антисимметричности $\mathcal{R}$.

2. $x\mathcal{R}y \wedge y\mathcal{R}a \wedge b\mathcal{R}x$ - по транзитивности $\mathcal{R}$ получим, что $b\mathcal{R}a$ - противоречие. Симместричный случай аналогично.

3. $x\mathcal{R}a \wedge b\mathcal{R}y \wedge y\mathcal{R}a \wedge b\mathcal{R}x$. По транзитивности $\mathcal{R}$ получим, что $b\mathcal{R}a$ - имеем противоречие.

Транзитивность абсолютно аналогично. **Ч.Т.Д.**

e. Вопросы на 5

1. **Теорема Цермело.**

Формулировки:

1. Любое множество можно вполне упорядочить.

2. Для любого множества найдется равномощное ему вполне упорядоченное.

Возьмем из аксиомы выбора функцию $\varphi : 2^M \setminus M \to M$ такая что $\forall M' \subsetneq M (\varphi(M') \notin M')$

Введем объект:

Корректным отрезком называется ВУМ (S, $\leqslant_S$)[33], такой что $\forall s \in S\, (s = \varphi([0,\, s)))$[34]

Лемма 1

Для любых двух корректных отрезков S и T справедливо, что один из них является начальным отрезком другого.

Доказательство

Сначала небольшое пояснение к тому, что тут вообще происходит. S и T - ВУМы, а значит один

[33] Далее будем просто называть S

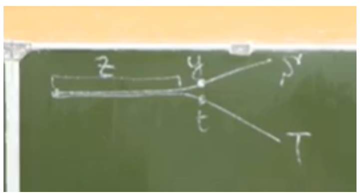
[34] Эта штука кажется весь неправдоподобной, поэтому ловите примеры: $\{\varphi(\varnothing)\}$, $\{\varphi(\varnothing), \varphi(\{\varphi(\varnothing)\})\}$ и т.д.

из них изоморфен начальному отрезку другого. Но и S и T - это подмножества нашего множества, которого мы хотим упорядочить. Поэтому мы докажем, что имеет не просто изоморфизм, а равенство.

Пусть S $\simeq$ какому-то начальному отрезку T, p(x) - изоморфизм.

Если для любого x p(x) = x, то все супер и равенство очевидно, но если p(x) - не тождественный изоморфизм, то найдется такие x, что p(x) $\neq$ x. В силу вполне упорядоченности среди них найдется миниматьный - y. Положим p(y) = t.

Тогда φ([0, y)) = y, а φ([0, t)) = t - из корректности отрезков. Но т.к. все точки из отрезка [0, y) меньше чем y, то тогда для них p - тождественный изоморфизм, а значит [0, y) = [0, t) = z - на картинке, откуда следует равенство y = t, т.е. y = p(y). А, значит, так S и тот отрезок, которому оно изорфно "как молния"получатся одинковыми:



Лемма 2

Объединение любого числа корректных отрезков - корректный отрезок.

Доказательство

1. Получится порядок:

Снова небольшое пояснение: так как на каждом корректном отрезке свой порядок, а объединяем мы их следующим образом: отдельно объединили множества, а отдельно порядки, как пары элементов. То на самом деле вообще нихрена не понятно, что за динозавр получается в итоге.

Итак, $S = \bigcup_i S_i$

Рефлексивность:

$x \in S \Rightarrow x \in S_i \Rightarrow x \leqslant_{S_i} x \Rightarrow x \leqslant_S$

Антисимметричность:

Если обе пары лежат в одном и том же множестве - все вытекает из порядка соответствующего множества, если же нет, то: $x \leqslant_{S_i} y$, $y \leqslant S_j x$ По лемме 1 один из данных корректных отрезков - нач отрезок другого. БОО S_i - нач отрезок S_j. Тогда $x \leqslant_{S_i} y \Rightarrow x \leqslant_{S_j} y$ По антисимметричности $\leqslant_{S_j}$ имеем равенство.

Аналогично транзитивность.

Итого порядок!! Теперь линейность:

Если x и y из одного множества, то они сравнимы из-за линейности соответствующего порядка. Иначе $x \in S_i$, $y \in S_j$ БОО S_i - нач отрезок S_j. Тогда $x \in S_j$, следовательно, x и y сравнимы по порядку $\leqslant_{S_j}$, а, значит, и по агрегированному.

Фундированность:

Пусть есть бесконечно убывающая цепочка $x_1 > x_2 > x_3 > \ldots$. Пусть $x_i \in S_\alpha$, тогда и все последующии в S_α. Пусть не так, тогда какой-то лежит в S_β, начальным отрезком которого будет S_α, тогда по порядку $\leqslant_{S_\beta}$ последующий будет больше x_i, чего быть не может. Но S_α - ВУМ, значит данная цепочка будет стабилизироваться - имеем фундированность.

Корректность:

$x \in S \Rightarrow x \in S_i \Rightarrow x = \varphi([0,\, x)_{S_i}) \Rightarrow x = \varphi([0,\, x)_S)$ - получили корректность.

О чудо! Доказали эту дичь![35]

Теперь непосредственно доказательство теоремы Цермело:

Покажем, что объединение все таких корректных отрезков - это исходное множество: Пусть не так. Тогда рассмотрим множество $S \cup \{\varphi(S)\}$. Это корректный отрезок, причем он больше чем S - но S - объединение всех корректных отрезков - получили противоречие. Значит объединение всей этой бурды и есть наше множество. **Ч.Т.Д.**

2. **Лемма Цорна.**

   Формулировка: *Пусть любая цепь ЧУМа имеет верхнюю грань, тогда все множество имеет максимальный элемент. Более того,* $\forall a \exists m > a\, (m - \text{максимум})$

   Доказательство

   Пусть $(A,\, \leqslant)$ - искомый ЧУМ. Тогда положим $I = (2^A,\, \preceq)$ - ВУМ[36]. По теореме же Цермело можно ввести вполне порядок на A. Теперь построим функцию $f : I \to A$ по следующему правилу:

   $f(0) = a$ - тот самый элемент для которого мы ищем максимальный. $f = min$[37]$\{x \in A \mid \forall y \preceq x\, (b > f(y))\}$

   Теперь по теореме о трансфинитной рекурсии получим, что f определена либо на всем I, либо на каком-то его начальном отрезке, первое же невозможно т.к. I по теореме Кантора более мощно, чем A и f по построению инъекция. Тогда f определена на каком-то начальном отрезке I.

   Пусть она определена на $[0;\, x]$, тогда $f(x)$ - максимум. Если же на $[0;\, x)$ то тогда $\{f(y) \mid y \in [0,\, x)\}$ - цепь, тогда по условию будет ее верхняя грань, а данное множество не имеет - противоречие.

   Итого получили, что найдется максимум. **Ч.Т.Д.**

f. Доп вопросы на 5

g. Доп вопросы на 6

h. Доп вопросы на 7

[35] Сам в ахере

[36] Данная хуйня существует по теореме Цермело

[37] В смысле вполне порядка на A

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