Билеты по матлогике

МФТИ ФПМИ 2022 г

Содержание

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: $\perp$ - 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.

13. ***Аксиомы исчисления высказываний***[7]

(a) $A \to (B \to A)$

(b) $\big(A \to (B \to C)\big) \to \big((A \to B) \to (A \to C)\big)$

(c) $(A \wedge B) \to A$

(d) $(A \wedge B) \to B$

(e) $A \to \big(B \to (A \wedge B)\big)$

(f) $A \to (A \vee B)$

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

[7] Далее просто ИВ

(g) $B \to (A \vee B)$

(h) $(A \to C) \to \Big((B \to C) \to ((A \vee B) \to C)\Big)$

(i) $\neg A \to (A \to B)$

(j) $(A \to B) \to \big((A \to \neg B) \to \neg A\big)$

(k) $A \vee \neg A$

14. ***Modus ponens***[8] - правило вывода формул:

    $\frac{A \quad A \to B}{B}$

15. ***Выводом*** называют конечную последовательность формул, такую что каждая формула в ней или аксиома, или была получена по MP из предыдущих

16. Формула называется ***выводимой***, если она встречается в каком-то выводе

17. ***Резолюции***:

    Если $A \vee x$ и $B \vee \neg x$ одновременно, то $A \vee B$ тоже истинно.

    Данный способ вывода дизъюнктов называется правилом резолюций: $\frac{A \vee x \quad B \vee \neg x}{A \vee B}$, а дизъюнкт $A \vee B$ - резольвентой.

18. ***Ариметичным*** называют предикат выразимый в сигнатуре $\{\mathbb{N}, +, \cdot, =\}$.n-арную функцию же называют ***ариметичной***, если (n + 1)-арный предикат отвечающий данной функции арифметичен.

19. ***Полной*** называют такую теорию Γ, что для любой замкнутой формулы ψ выполнено либо $\Gamma \vdash \psi$, либо $\Gamma \vdash \neg\psi$[9]

20. ***Экзистенциально полной*** в сигнатуре σ называют такую теорию Γ, что для любой формулы ψ, такой что $\Gamma \vdash \exists x\ \psi$, верно также $\Gamma \vdash \psi(t/x)$ - для некоторого замкнутого терма t

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

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

[8] Далее будет использоваться как MP

[9] Отметим, что либо-либо стоит неспроста - одновременно быть такого не должно

[10] Будем обозначать i-ую переменную как p_i

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, 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 $x_i = 1$, 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 $\bigwedge_{j=1}^{n} p_i^{x_i}$ 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[11] $x \geqslant y$ (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:

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

$$g_i \in M \Rightarrow g_i(x) = \neg g_i(\neg x^{12}) \Rightarrow g(x) = \neg g(\neg x)$$

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

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 $\Rightarrow h \in A$

3. Вывод $A \to A$

$$1.\, A \to (A \to A) - Ax.1$$

$$2.\, A \to ((A \to A)) \to A) - Ax.1$$

$$3.\, (A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A)) - Ax.2$$

$$4.\, (A \to (A \to A)) \to (A \to A) - MP\, 2,\, 3$$

$$5.\, (A \to A) - MP\, 2,\, 4$$

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

[12] Покомпонентная инверсия вектора

4. Корректность ИВ

   Если $\vdash \psi$, то ψ - тавтология

   Доказательство

   Любая аксиома тавтология, если же A и $A \to B$ - тавтологии, то B - тавтолия, т.к. если импликация верна и посылка ее истинна, то и заключение истинно, далее же по индукции все тавтологии. **Ч.Т.Д.**

5. Сведение задачи о выполнимости произвольной формулы к задаче о выполнимости 3-КНФ

   Для любой формулы ψ существует формула ψ', такая что:

   а) Множество переменных ψ' включает в себя множество переменных ψ

   б) ψ' является 3-КНФ, т. е. КНФ, в каждом дизъюнкте которой не больше 3 литералов

   в) Длина ψ' в константу раз больше длины ψ

   г) Если ψ невыполнима, то ψ' также невыполнима

   д) Если ψ выполнима, то ψ' также выполнима, более того, ограничение любого выполняющего набора ψ' на общие переменные даст выполняющий набор ψ

   Доказательство

   На каждую подформулу вида $m_i{*}m_j$ или $\neg m_k$ заведем новую переменную m_s, такую что $m_s \iff m_i{*}m_j$ в первом случае и $m_s \iff \neg m_k$ во втором. Потом построим КНФ для $m_s \iff m_i{*}m_j$ или $m_s \iff \neg m_k$ и возьмем конъюнкцию всех их, не забыв добавить в нее дизъюнкт состоящий только из m_m - переменная соответствующая все формуле (формула - подформула самое себя). Покажем что в итоге получим ψ':

   1. Очевидно по построению

   2. Т.к. в $m_s \iff \neg m_k$ и в $m_s \iff m_i * m_j$ не более 3 переменных, то и получится 3-КНФ

   3. Для каждой итерации имеет превосхождение переменных в константу раз, значит, на выходе О большое сохранится

   4. Т.к. вся формула невыполнима, то она ложна на каком-то наборе, а, значит, если все эквивалентности выполнены, то $m_m = 0$, тогда хотя бы один дизъюнкт равен 0, откуда полученная 3-КНФ невыполнима.

   5. Если же выполнима, то из эквивалентностей получим значения дополнительно введенных переменных и $m_m = 1$, тогда ψ' - выполнима то же. И, наоборот, если взять сужение поднабора ψ' на переменные ψ, то получим из эквивалентностей выполняющий набор ψ.

6. Представление задачи о 3-раскраске графа как задачи о выполнимости КНФ

   Можно ли его вершины раскрасить в 3 цвета, так чтобы вершины одного цвета не были соединены ребром?

   Введем две переменные для вершины i: (p_i, q_i). Положим (0, 1), (1, 1), (1, 0) за три различных цвета, для исключения набора (0, 0) добавим формулу $p_i \vee q_i$. Теперь различие цветов пары вершин - это 3-КНФ: $(p_i \vee q_i \vee p_j \vee q_j) \wedge (p_i \vee \neg q_i \vee p_j \vee \neg q_j) \wedge (\neg p_i \vee q_i \vee \neg p_j \vee q_j) \wedge (\neg p_i \vee \neg q_i \vee \neg p_j \vee \neg q_j)$

   Тогда существование расскраски - это выполнимость следующей формулы:

$$\bigwedge_{(i,j)\in E} [(p_i \vee q_i \vee p_j \vee q_j) \wedge (p_i \vee \neg q_i \vee p_j \vee \neg q_j) \wedge (\neg p_i \vee q_i \vee \neg p_j \vee q_j) \wedge (\neg p_i \vee \neg q_i \vee \neg p_j \vee \neg q_j) \wedge (p_i \vee q_i) \wedge (p_j \vee q_j)]$$

7. Представление задачи о расстановке ферзей на шахматной доске как задачи о выполнимости КНФ

   Можно ли расставить 8 ферзей на шахматной доске, так чтобы они не били друг друга?

   Пусть p_{ij} - это переменная обозначающая, что в клетке $(i,\,j)$ стоит ферзь. Первое, что требуем - существование хотя бы одного ферзя на строке, т.е. $\bigvee\limits_{i=1}^{8} p_{ij}$. Теперь по все строкам - ферзей должно быть ровно восемь, $\bigwedge\limits_{j=1}^{8}\bigvee\limits_{i=1}^{8} p_{ij}$. Теперь добавим условия на строки, диагонали и столбцы:

   i-ая строка:

   $$\bigwedge_{k=1}^{8}\ \bigwedge_{m=1,\,k\neq m}^{8} (\neg p_{im} \vee \neg\neg p_{ik})$$

   i-ый столбец:

   $$\bigwedge_{k=1}^{8}\ \bigwedge_{m=1,\,k\neq m}^{8} (\neg p_{mi} \vee \neg\neg p_{ki})$$

   Диагонали для клетки $(i,\,j)$: тут мне уже влом виписывать чудо формулы, поэтому просто конъюнкция всех таких дизъюнктов $(\neg p_{ij} \vee \neg p_{i+k\,j+k})$, $(\neg p_{ij} \vee \neg p_{i-k\,j+k})$, $(\neg p_{ij} \vee \neg p_{i-k\,j-k})$, $(\neg p_{ij} \vee \neg p_{i+k\,j-k})$, где k бегает в нужных пределах

   Далее возьмем конъюнкцию всего и получим нужную формулу.

8. Корректность метода резолюций

   Для выполнимых КНФ $\vdash$ не будет выведен

   Доказательство

   Если формула выполнима, то после добавления любого числа резольвент она сохранит выполнимость. Предположим, что вывелось $\vdash$, тогда при его добавлении к формуле получим, что новая формула невыполнима, следовательно, $\vdash$ не выводится **Ч.Т.Д.**

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[13]

   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:

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

[13] Здесь 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 спроста называется полиномом))[14], 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.**

2. **Лемма о дедукции для исчисления высказываний**

   $\Gamma \vdash A \to B \Leftrightarrow \Gamma \cup \{A\} \vdash B$

   Доказательство

   Если из Γ выводится $A \to B$, то из $\Gamma \cup \{A\}$ тоже выведется $A \to B$, и тогда по MP выведется B.

   Докажем левую часть эквивалентности:

   Пусть $C_1, \dots, C_n$ – вывод из $\Gamma \cup \{A\}$, тогда $\forall i \in \{1, \dots, n\} \hookrightarrow \Gamma \vdash A \to C_i$. Докажем это утверждение по индукции:

   I) C_i – аксиома. Тогда вывод будет выглядеться так:

   (a) C_i Ax.

   (b) $C_i \to (A \to C_i)$ Ax.1

   (c) $A \to C_i$ MP 1, 2

   II) C_i – посылка, те элемент $\Gamma \cup \{A\}$. Если $C_i \in \Gamma$, то вывод аналогичен для п.I, с условием того, что 1-ый пункт выведется не как аксиома, а как посылка.

   Если $C_i = A$, то C_i выводится по лемме 1.

   Если C_i выводится по *modus ponens* из формул C_j и C_k, где $j < i$, $k < i$. Значит $C_k = C_j \to C_i$, иначе *modus ponens* не применить. Тогда вывод будет выглядеть так:

[14] Это все же лучше не говорить на экзамене

(a) $A \to C_j$ По предположению индукции

(b) $A \to C_k = A \to (C_j \to C_i)$ По предположению индукции

(c) $(A \to (C_j \to C_i)) \to ((A \to C_j) \to (A \to C_i))$ Ax. 2

(d) $(A \to C_j) \to (A \to C_i)$ MP 2, 3

(e) $(A \to C_i)$ MP 1, 4

Таким образом, были рассмотрены все случаи, тем самым установлен индукционный переход. А значит, лемма доказана.

3. **Теорема о полноте исчисления высказываний**

Пусть ψ, зависящая от переменных $p_1, \ldots, p_n$ - тавтология, тогда $\vdash \psi$

Сначала докажем две леммы:

Псевдолемма

Справедливы следующие выводы:

(a) $A, B \vdash A \wedge B$

(b) $A, B \vdash A \vee B$

(c) $A, B \vdash A \to B$

(d) $\neg A, B \vdash \neg(A \wedge B)$

(e) $\neg A, B \vdash A \vee B$

(f) $\neg A, B \vdash A \to B$

(g) $A, \neg B \vdash \neg(A \wedge B)$

(h) $A, \vdash A \vee B$

(i) $A, \neg B \vdash \neg(A \to B)$

(j) $\neg A, \neg B \vdash \neg(A \wedge B)$

(k) $\neg A, \vdash A \vee B$

(l) $\neg A, \vdash A \to B$

(m) $A \vdash \neg(\neg A)$

(n) $A \vdash A$

Доказательство ее оставим в качестве упражнения читателю.

Лемма

Пусть A — формула, $x \in \{0, 1\}$. Через A^x обозначим формулу A, если $x = 1$, и формулу $\neg A$, если $x = 0$. Далее, пусть ψ — формула от n переменных, выражающая функцию f. Тогда для всех формул $A_1, \ldots, A_n$ и значений $x_1, \ldots, x_n$ выполнено:

$$A_1^{x_1}, \ldots, A_n^{x_n} \vdash \psi(A_1, \ldots, A_n)^{f(x_1, \ldots, x_n)}$$

Доказательство - по индукции

База индукции: ψ - переменная, f - проектор. Тогда $\psi(A_1, \dots, A_n) = A_i$, а $f(x_1, \dots, x_n) = x_i$ - просто вывели посылку. Переход (Для конъюнкции - для других аналогично)

Пусть уже верно для формул η и ξ, и функций g, h соответственно. Тогда для $\eta \wedge \xi$:

$$A_1^{x_1}, \dots, A_n^{x_n} \vdash \eta(A_1, \dots, A_n)^{g(x_1, \dots, x_n)}$$

$$A_1^{x_1}, \dots, A_n^{x_n} \vdash \xi(A_1, \dots, A_n)^{g(x_1, \dots, x_n)}$$

$$\eta(A_1, \dots, A_n)^{g(x_1, \dots, x_n)}, \xi(A_1, \dots, A_n)^{g(x_1, \dots, x_n)} \vdash (\eta \wedge \xi)(A_1, \dots, A_n)^{(g \wedge h)(x_1, \dots, x_n)}$$

По псевдолемме.

Ч.Т.Д.

Перейдем к доказательству теоремы:

ψ - тавтология, значит она выражает функцию тождественной единицы. По лемме выше получим, что для любого набора $x_1, \dots, x_n$ выполнено: $A_1^{x_1}, \dots, A_n^{x_n} \vdash \psi$. Теперь применим обратную индукцию. Ее база уже упомянута выше, поэтому покажем переход: Пусть для k верно, проверим для $k-1$ По предположению индукции получим:

$$A_1^{x_1}, \dots, A_{k-1}^{x_{k-1}}, A_k \vdash \psi$$

$$A_1^{x_1}, \dots, A_{k-1}^{x_{k-1}}, \neg A_k \vdash \psi$$

По правилу разбора случаев (аксиома 8) получим, что $(A_1^{x_1}, \dots, A_{k-1}^{x_{k-1}}), (\neg A_k \vee A_k) \vdash \psi$, но $(\neg A_k \vee A_k)$ - аксиома, значит, ее можно выкинуть. Откуда получим:

$$A_1^{x_1}, \dots, A_{k-1}^{x_{k-1}} \vdash \psi$$

А, значит, мы так избавимся от всего слева от штопора **Ч.Т.Д.**

4. **Устойчивость выразимых предикатов при автоморфизмах интерпретаций**

Пусть ψ - формула в сигнатуре σ от k параметров. Пусть $\mathcal{I}$ - интерпретация σ, α - ее автоморфизм. Тогда $[\psi](x_1, \dots, x_k)$ эквивалентно $[\psi](\alpha(x_1), \dots, \alpha(x_k))$ **Доказательство** - индукцией по длине формулы.

Сначала для термов:

Пусть t - терм в сигнатуре σ от k параметров. Пусть $\mathcal{I}$ - интерпретация σ, α - ее автоморфизм. Тогда $\alpha([t](x_1, \dots, x_k)) = [t](\alpha(x_1), \dots, \alpha(x_k))$

Если t - переменная, то справа $\alpha(t)$.

Если t - константа, то справа $\alpha(t)$ - тоже константа, но α уважает функциональные символы, значит $t = \alpha(t)$

Если терм составной, т.е. $\alpha([t](t_1, \dots, t_k)) = \alpha([f]([t_1](x_1, \dots, x_k), \dots, [t_m](x_1, \dots, x_k)) = [f](\alpha([t_1](x_1, \dots, x_k), \dots, \alpha$
$[t](\alpha(x_1), \dots, \alpha(x_k))$

Теперь перейдем на формулы:

Атомарная формула:

$\alpha([P](x_1, \ldots, x_k)) = [P](\alpha([t_1](x_1, \ldots, x_k), \ldots, \alpha([t_m](x_1, \ldots, x_k)) = [P](\alpha(x_1), \ldots, \alpha(x_k))$

Булевы операции (для других - аналогично)

Т.к. по предположению индукции $\alpha([\xi](x_1, \ldots, x_k)) = [\xi](\alpha(x_1), \ldots, \alpha(x_k))$ и $\alpha([\eta](x_1, \ldots, x_k)) = [\eta](\alpha(x_1), \ldots, \alpha(x_k))$ то $\alpha([\eta \wedge \xi](x_1, \ldots, x_k)) = [\eta \wedge \xi](\alpha(x_1), \ldots, \alpha(x_k))$ Кванторы (для другого - аналогично):

Из предположения индукции имеем: $\exists x_1\, \varrho(\alpha(x_1), \ldots, \alpha(x_k))$ эквивалентно $\exists x_1\, \varrho(x_1, \ldots, x_k)$, α в свою очередь биекция, поэтому возьмем положим $y = \alpha(x_1)$, а $x_1 = \alpha^{-1}(y)$ и поменяем квантор: $\exists y\, \varrho(y, \ldots, \alpha(x_k))$.

Ч.Т.Д.

d. Вопросы на 4

1. **Теорема о полноте метода резолюций**

   Из невыполнимой КНФ всегда можно вывести $\perp$

   Доказательство - докажем контрапозию к условию теоремы, т.е. если не выведено $\perp$, то формула выполнима

   Итак, построим индуктивно выполняющий набор. Так как $\perp$ не выводится, то выполнимы все дизъюнкты не зависящие от переменных (их просто нет - а для элементов пустого множества все верно). - База индукции

   Теперь пусть уже имеется набор значений $\left\|\begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix}\right\| = \left\|\begin{matrix} a_1 \\ \vdots \\ a_n \end{matrix}\right\|$, который гарантирует выполнимость всех дизъюнктов содержащих только $x_1, \ldots, x_n$. Теперь посмотрим на дизъюнкты, которые содержат x_{n+1}, возможно, какие-то из $x_1, \ldots, x_n$ и при этом не содержащие x_{n+1}...

   Исключим из выбранных дизъюнктов все те, которые уже выполняются на наборе $\left\|\begin{matrix} a_1 \\ \vdots \\ a_n \end{matrix}\right\|$.

   Теперь посмотрим, что осталось: если в сохранившихся дизъюнктах везде есть встречается только x_{n+1}, то расширяем выполняющий набор до $\left\|\begin{matrix} a_1 \\ \vdots \\ a_n \\ 1 \end{matrix}\right\|$, если же только $\neg x_{n+1}$, то $\left\|\begin{matrix} a_1 \\ \vdots \\ a_n \\ 0 \end{matrix}\right\|$

   Рассмотрим случай, когда оба варианта встречаются, т.е. найдутся дизъюнкты $D \vee x_{n+1}$ и $d \vee \neg x_{x+1}$, где D и d - дизъюнкты, зависящие только от $x_1, \ldots, x_n$, тогда по методу резолюций получим резольвенту $D \vee d$ - она выполнима, а так как мы исключили все дизъюнкты, которые уже истинны на заданном наборе, то $D \vee d$ - ложен, но он зависит только от $x_1, \ldots, x_n$, а, значит, должен был быть выполним - противоречие.

   Таким образом, мы получим выполняющий набор. **Ч.Т.Д.**

2. **Теорема Гёделя о полноте исчисления предикатов: расширение любого непротиворечивого**

множества до полного и экзистенциально полного

Лемма 1. О полном пополнении

Любую непротиворечивую теорию Γ *можно расширить до полной непротиворечивой теории* Δ

Доказательство

Индукцией по всем формулам счетной или конечной сигнатуры[15] будем проходить

и строить $\Gamma_i = \begin{cases} \Gamma \cup \psi_i & \text{Если данная теория непротиворечива} \\ \Gamma \cup \neg\psi_i & \text{В противном случае} \end{cases}$

Одновременно два кейса не возможны: из противоречимости выведем какую-то формулу отличную от ψ_i и ее отрицание, далее по лемме о разборе случаев сможем отбросить ψ_i и ее отрицание - получим, что их Γ_i выводится какая-то формула и ее отрицание $\Rightarrow$ данная теория противоречива - противоречие.

Теперь положим $\Delta = \bigcup\limits_{i=1}^{\infty} \Gamma_i$ **Ч.Т.Д.**

Лемма 2. Об экзистенциально полном пополнении

Любую непротиворечивую теорию Γ *в сигнатуре* σ *можно расширить до экзистенциально полной в сигнатуре* τ *непротиворечивой теории* Δ

Доказательство

Для каждой формулы ψ, такой что $\Gamma \vdash \exists x\ \psi$ добавим константу c_ψ в сигнатуру и формулу $\psi(c_\psi/x)$

Покажем, что противоречивость не пропадет:

Пусть $\Gamma, c_\psi \vdash \bot$, тогда $\Gamma \vdash \psi(c_\psi/x) \to \bot$, По Σ-правилу Бернайса получим: $\Gamma \vdash \exists w\ \psi(w/x) \to \bot$. Тогда по MP получим, что $\Gamma \vdash \bot$ - противоречие.**Ч.Т.Д.**

Теперь объединим это все для доказательства теоремы:

Будем чередовать шаги каждый раз - лемму 2, потом лемму 1 и т.д. счетное число, разумеется.[16]

Покажем что получится ровно то, что надо:

1. Непротиворечивость

Если вывелось противоречии, значит, на как-то шаге оно было получено, откуда, на каком-то шаге мы проебались, но леммы говорят, что мы молодцы - посему все заебись.

2. Полнота

Рассмотрим похуй какую замкнутую формулу. В ней лишь конечное число констант. Хуй пойми как, но мы видимо Боги, а потому можем, рассмотрим момент добавления последней константы. На следующем шаге итераций будет выведена либо она сама, либо ее отрицание - заебумба.

3. Экзистенциальное пополнение

Аналогично, магическим образом идем на шаг, где выводится формула $\exists x\ \psi$, на следующем шаге экзистенциального пополнения получим, что добавится формула $\psi(c_\psi/x)$ и константа c_ψ - ахуенно, не так ли

[15] Для больших мощностей можно использовать трансфинитную индукцию и теорему Цермело

[16] У вас сто процентов появился вопрос: а с хуя так то? Ну.. Шень говорит, что формул $\exists x\ \psi$ - не более чем счетное число, к ним хуячим лемму 2, потом полируем лемму 1 - как с водкой: между первой и второй промежуток небольшей. А далее надудониваемся в хлам - ибо это ботать невозможно!

Берем супер-дупер-мега объединение всей хуеты выше - все получилось!

3. **Теорема Гёделя о полноте исчисления предикатов: построение модели из замкнутых термов у любого непротиворечивого, полного и экзистенциально полного множества**

   Итак, ебашим модель:

   Модель - все замкнутые термы

   Интерпретация функциональных символов:[17] Были закнутые термы подали после функц символа в скобках, интерпретируем как функцию для данного функционального символа от всего того, что в скобках

   Предикатных символов

   Интерпретируем $[P]([t_1]\dots[t_k]) = 1)$ тогда и только тогда, когда $\Gamma \vdash P(t_{1k})$, в противном случае - 0.

   Теперь показываем что модель - не хуета, а работает как надо:

   Пусть из Γ вывелось ψ, покажем, что тогда ψ - истина.

   Из полноты[18] докажем, что Γ вывелось ψ, покажем, что тогда ψ - истина, а если не вывелось - то ложно.

   Индукция по глубине фоормулы:

   Если атомарная - то по определению истинна

   Для булевых связок все тривиально выполнено

   Если квантор существования, то по экзитенциальной полноте выведется та же хуйня, но без квантора, она более простая по построению, а значит истинна, тогда и с квантором-хуянтором все истинно.

   Если всеобщности, то херачим закон де Моргана: имеем квантор существования и отрицание - смотрим на два пункта выше и ахуеваем с того какие мы крутые и все сделали.

   Итого, доказали нахуй!

4. **Арифметичность предикатов «n — степень шестёрки» и «$n = 2^k$».**

   Выразим через β-функцию Геделя данные два предиката:

   «n — степень шестёрки»: $\exists x\, \exists a\, \exists b\, (\beta(a,\, b,\, 0) = 1 \wedge \beta(a,\, b,\, x) = n \forall i \in [0,\, x-1]\, \beta(a,\, b,\, i+1) = 6 \cdot \beta(a,\, b,\, i))$

   «$n = 2^k$»: $\exists a\, \exists b\, (\beta(a,\, b,\, 0) = 1 \wedge \beta(a,\, b,\, k) = n \forall i \in [0,\, k-1]\, \beta(a,\, b,\, i+1) = 2 \cdot \beta(a,\, b,\, i))$

   Проверить корректность предлагается проверить читателю самому на экзамене.

е. Вопросы на 5

1. **Представимость конечных последовательностей в арифметике при помощи β-функции Гёделя**

   Лемма 1

[17] Тут Шень спизданул, что ему понятно, только бля вот что-то нихуя не понятно, а потому ловите какашку

[18] Честно вот вообще не ебу, как она тут зачесалась

Для любого k можно найти сколь угодно большое натуральное число b, такое что первые k членов последовательности $b+1,\ 2b+1,\ 3b+1,\ \dots$ были попарно взаимно просты.

Доказательство

Любой НОД данных пар чисел будет делителем их разности, а, значит, и числа μb, где $\mu \in [1,\ k]$. Тогда выберем $b = k!$, откуда все разности будут кратны b, но сами числа последовательности взаимно просты с b **Ч.Т.Д.**

Лемма 2

Для любой последовательности $x_0,\ \dots,\ x_k$ можно найти такие два числа a и b, что x_i есть остаток a от деления на $b(i+1)+1$

Доказательство

По лемме 1 выберем данное b, тогда $b(i+1)+1$ - взаимно простые числа. Тогда воспользуемся КТО и получим, что по модулям $b(i+1)+1$ и числам x_i, можно будет найти, при чем единственный, прообраз по подулю из произведения $b(i+1)+1$ - число a. **Ч.Т.Д.**

Итого, значит любую последовательность можно закодировать тремя числами: a, $b\,k$. Что и делается в β-кодировании Геделя

2. **Вывод коммутативности сложения в арифметике Пеано**

Лемма 1. $\forall x\ 0 + x = x$

(a) $\forall x\ x + 0 = x-$Аксиома нуля

(b) $0 + 0 = 0-$ Подстановка $x = 0$

(c) $\forall x \forall y\ x + Sy = S(x + y)-$Аксиома сложения

(d) $0 + Sx == S(0 + x)-$ Подстановка $x = 0,\ y = x$

(e) $\forall x \forall y\ x = y \to Sx = Sy-$Аксиома равенства

(f) $0 + 0 + x = x \to S(0 + x) = Sx-$ Подстановка $x = 0,\ y = 0 + x$

(g) $0 + x = x \to S(0 + x) = Sx-$ Подстановка b в f

(h) $0 + x = x \to 0 + S(x) = Sx-$Транзитивность

(i) $\forall x\ (0 + x = x \to 0 + S(x) = Sx)-$Правило обобщения

(j) $(0 + 0 = 0 \wedge \forall x\ (0 + x = x \to 0 + S(x) = Sx)) \to \forall x\ 0 + x = x-$Аксиома индукции

(k) $(0+0 = 0) \to (\forall x\ (0+x = x \to 0+S(x) = Sx) \to (0+0 = 0 \wedge \forall x\ (0+x = x \to 0+S(x) = Sx)))-$Ax. 5

(l) $\forall x\ (0 + x = x \to 0 + S(x) = Sx) \to (0 + 0 = 0 \wedge \forall x\ (0 + x = x \to 0 + S(x) = Sx))-$MP b, k

(m) $0 + 0 = 0 \wedge \forall x\ (0 + x = x \to 0 + S(x) = Sx)-$MP i, l

(n) $\forall x\ 0 + x = x-$MP j, m

Лемма 2. $\forall x\ \forall y\ Sx + y = S(x + y)$

(a) $\forall x\ x + 0 = x-$Аксиома нуля

(b) $x + 0 = x -$ Подстановка $x = x$

(c) $Sx + 0 = Sx -$ Подстановка $x = Sx$

(d) $\forall x \forall y\ x = y \to Sx = Sy -$Аксиома равенства

(e) $x + 0 = x \to S(0 + x) = Sx -$ Подстановка $x = x$, $y = 0$

(f) $S(0 + x) = Sx -$MP

(g) $Sx + 0 = S(x + 0) -$Транзитивность

(h) $\forall x \forall y\ x + Sy = S(x + y) -$Аксиома сложения

(i) $Sx + Sy = S(Sx + y) -$ Подстановка $x = Sx$, $y = y$

(j) $S(x + Sy) = S(S(x + y))$Аксиома сложения $+$ равенства

(k) $(Sx + y = S(x + y)) \to (Sx + SSY + S(Sx + y) = S(S(x + y)) = S(x + S(y))$

(l) $\forall x\ ((Sx + y = S(x + y)) \to (Sx + SY = S(Sx + y) = S(S(x + y)) = S(x + S(y)))$ - Правило обобщения

(m) $(Sx + 0 = S(x + 0) \wedge \forall x\ ((Sx + y = S(x + y)) \to (Sx + SY = S(x + Sy)))) \to \forall x\ Sx + y = S(x + y)$ - Аксиома индукции

(n) $\forall x\ Sx + y = S(x + y)$ - MP

(o) $\forall x\ \forall y\ Sx + y = S(x + y)$

Коммутативность сложения

(a) $\forall x\ x + 0 = x -$Аксиома нуля

(b) $\forall x\ 0 + x = x$ - Лемма 1

(c) $x + 0 = x$ - Ax. 12

(d) $0 + x = x$ - Ax. 12

(e) $x + 0 = 0 + x$ - Транзитивность

(f) $\forall x\ \forall y\ Sx + y = S(x + y)$ - Лемма 2

(g) $\forall x \forall y\ x + Sy = S(x + y) -$Аксиома сложения

(h) $Sx + y = S(x + y)$ - Ax. 12

(i) $x + Sy = S(x + y)$ - Ax. 12

(j) $x + y = y + x \to S(x + y) = S(y + x)$ - Аксиома равенства

(k) $x + y = y + x \to Sx + y = x + Sy$ - Транзитивность

(l) $\forall y\ (x + y = y + x \to Sx + y = x + Sy)$ - Правило обобщения

(m) $(x + 0 = 0 + x \wedge \forall y\ (x + y = y + x \to Sx + y = x + Sy)) \to \forall y\ x + y = y + x$ - Аксиома индукции

(n) $\forall y\ x + y = y + x$ - MP

(o) $\forall x\ \forall y\ x + y = y + x$ - Правило обобщения

3. **Множество замкнутых формул, истинных в N, неперечислимо.**

   Доказательство

   Сначала покажем неарифметичность данного множества:

   Пусть $\mathfrak{True}(x)$ - Предикат, показывающий является ли x кодом замкнутой истинной формулы.

   Пусть исходное множество арифметично, тогда для $\mathfrak{True}(x)$ найдется формула, которая БОО будет лежать в классе Σ_k. Пусть ϱ - произвольная формула из класса Σ_{k+1}, тогда данная формула равносильна формуле $\mathfrak{True}(\langle\varrho(x)\rangle)$, которая лежит в Σ_k. Но $\Sigma_k \neq \Sigma_{k+1}$. - Противоречие, значит, данное множество неарфметично.

   Т.к. любое перечислимое множество лежит в Σ_1, то оно арифметично, откуда получаем неперечислимость данного множества. **Ч.Т.Д.**

   Первая теорема Гёделя о неполноте.

   Если формальная арифметика непротиворечива, то в ней есть не доказуемые истинны

   Доказательство

   Обозначим $\mathfrak{Subst}(x, y, z)$ - Предикат, показывающий является ли x кодом замкнутой формулы, полученной подстановкой числа z в формулу с кодом y.

   $\mathfrak{Proof}(p, x)$ - Предикат, показывающий является ли последовательность p доказательством формулы x.
   $\mathfrak{Proovable}(x) = \exists p\, \mathfrak{Proof}(p, x)$

   Пусть $G(y) = \exists x\, (\mathfrak{Subst}(x, y, y) \wedge \neg\mathfrak{Proovable}(x))$ Теперь подставим данную формулу в саму себя: $G(G) = \exists x\, (\mathfrak{Subst}(x, G, G) \wedge \neg\mathfrak{Proovable}(x))$ Тогда получим, что либо данная формула недоказуема - теория не полна, либо доказуема, но ложна - тогда теория неадекватна.

4. **Теорема Тарского**

   Множество истинных арифметических формул неарифметично

   Доказательство

   Обозначим $\mathfrak{Subst}(x, y, z)$ - Предикат, показывающий является ли x кодом замкнутой формулы, полученной подстановкой числа z в формулу с кодом y.

   $\mathfrak{True}(x)$ - Предикат, показывающий является ли x кодом замкнутой истинной формулы.

   Пусть $T(y) = \exists x\, (\mathfrak{Subst}(x, y, y) \wedge \neg\mathfrak{True}(x))$ Теперь подставим данную формулу в саму себя: $T(T) = \exists x\, (\mathfrak{Subst}(x, T, T) \wedge \neg\mathfrak{True}(x))$ Истинность данной формулы равносильна тому, что x - код подстановки формулы T в саму себя, т.е. данной формулы, и данная формула ложна. Т.е. $T(T)$ равносильна собственному отрицанию - противоречие.

f. Доп вопросы на 5

1. **Лемма о скобочном итоге**

   Пусть ψ - пропозициональная формула[19]*, 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

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

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 $(\psi *$[20]$\varphi)$:

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 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 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)

[20]Это один из символов $\to, \wedge, \vee$

- 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 p и отрицания 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	$x_1 \vert x_2$
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:

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

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

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

$$\text{Значит, } g(x_1 \wedge y_1,\ \dots,\ x_n \wedge y_n) = g(x_1,\ \dots,\ x_n) \wedge^{21} g(y_1,\ \dots,\ y_n)$$

$$\text{Тогда, } h(x_1 \wedge y_1,\ \dots,\ x_n \wedge y_n) = f(g(x_1 \wedge y_1,\ \dots,\ x_n \wedge y_n)) = f(g(x_1,\ \dots,\ x_n) \wedge g(y_1,\ \dots,\ y_n)) =$$

$$= f(g(x_1,\ \dots,\ x_n)) \wedge f(g(y_1,\ \dots,\ y_n)) = h(x_1,\ \dots,\ x_n) \wedge h(y_1,\ \dots,\ y_n) \Rightarrow h \in \bigwedge$$

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

2. **Базис монотонных функций**

   $1, 0, \wedge, \vee$ - *базис М.*

   Доказательство

   Так как все эти функции монотонны, то их замыкание лежит в М. 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

[21] Покомпонентная конъюнкция

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[22], называется ***фундированным***.

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

[22]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 $\langle C, \succsim_C \rangle$,

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

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

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

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, $\omega = sup\{1,\, 2,\, 3,\, 4,\, \ldots\}$
    2. $\omega^k,\ k \in \mathbb{N} = \omega^{k-1} \cdot \omega$, причем $\omega^0 = 1$
    3. $\omega^\omega = sup\{\omega^0,\, \omega^1,\, \omega^2,\, \omega^3,\, \ldots\}$
    4. $\varepsilon_0 = sup\{\omega,\, \omega^\omega,\, \omega^{\omega^\omega},\, \omega^{\omega^{\omega^\omega}},\, \ldots\}$

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***[23] 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
$\cup$	$\vee$
$\cap$	$\wedge$
$\triangle$	$\oplus$
$\setminus$	$\nrightarrow$
$-$	$\neg$

[23] 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[24]:

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:

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

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

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

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

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

Доказательства

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

[24] 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[25] $\varphi\, :\, f \mapsto (g_1,\, g_2),\, \varphi\, :\, \begin{cases} g_1(x) = f(x), \text{ если } x \in B \\ g_2(x) = f(x), \text{ если } x \in C \end{cases}$

Данная функция - это биекция[26].

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 $f\, :\, C \to g,\, g\, :\, B \to A$, $h\, :\, (B \times C) \to A,\, \varphi\, :\, h(b,\, c) = (f(c))(b)$[27].

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.

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

[26] 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 B $\Rightarrow g_1$ от них будут различны) - значит инъективна

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

3. Объединение счётных множеств счётно.

   Пусть A и B - счетные множества, $\alpha : \mathbb{N} \to A$, $\beta : \mathbb{N} \to B$ - их биекции из натуральных чисел. Если пересечение A и B 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 A, 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: A счетно, потому есть биекция в четные числа, из B 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)[28], откуда по теореме Кантора-Бернштейна имеем счетность их объединения.

4. Декартово произведение счётных множеств счётно.

   Аналогично A и B - 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 A и j-го элемента B:

	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 $\frac{i(i+1)}{2} + \frac{2i-2+j}{2}(j-1)$.[29] 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, $\varkappa = \lceil k_1 \rceil$[30]. Теперь вычисляем $\Delta = \frac{\varkappa(\varkappa+1)}{2} - n$. Тогда прообразом числа n будет $(\varkappa - \Delta, \Delta + 1)$. Откуда имеем биекцию.[31]

5. В любом бесконечном множестве найдётся счётное подмножество.

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

[29] 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 $\frac{2i-2+j}{2}(j-1)$

[30] Округляем **вверх**

[31] 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[32] $\psi(x) = (p \circ r)(x)$, 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[33] $0,\dots 1(0)$ и $0,\dots 0(9)$, то для однообразности выберем второй вариант. Теперь предположим обратное: чисел на единичном отрезке лишь счетное число.[34] 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. $a \sqsubset$ [35]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[36]:

   1. 11

   2. 101

   3. 1001

   4. 10001

   5. 100001

   6. 1000001

   ...

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

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

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

[34] 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.

[35] Не совпадают конечно же

[36] 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[37]. 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:

[37] 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[38] 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 $\mid \neg$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 $A = \{x \mid f(x) < x\} \neq \varnothing$, 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 структуре вполне упорядоченного множества.**

   Любое вполне упорядоченное множество представимо в виде $\omega \cdot L + F$

[38] Думаю данный случай тривиален и не стоит расписывания

Доказательство

Отметим, что для конечных данное равенство тривиально выполнено ($L = 0$). Далее рассматривает только бесконечные множества.

Сначала высечем F:

Если ВУМ содержит наибольший элемент, то проверим ли является ли он предельным, если да, то внесем его в F', далее аналогично со всеми раньше. Бесконечно данный процесс продолжаться не может - т.к. это ВУМ. Далее "перевернем"F' и F. Теперь наше множество представимо в виде $M + F$, где F - конечно, а M - без наибольшего.

Теперь покажем, что любой ВУМ без наибольшего представим в виде $\omega \cdot L$, где L - множество предельных элементов (кроме, возможно, наибольшего):

По индукции:

Пусть верно для всех таких ВУМов меньше α, тогда выберем какой-то ВУМ меньше α - тут можно сослаться на аксиому выбора. Обозначим его β. По теореме о сравнении ВУМов он изоморфен какому-то начальному отрезку α - $[0, t)$. Тогда рассмотрим ВУМ $\alpha \setminus [0, t)$ - Это тоже ВУМ, который меньше α - тогда для ВУМов β и $\alpha \setminus \beta$ применимы предположения, ибо, очевидно, $\alpha \setminus \beta$ не имеет наибольшего индукции: $\beta = \omega K$, $\alpha \setminus \beta = \omega R$. Теперь магия чисел: $\alpha = \beta + (\alpha \setminus \beta) = \omega K + \omega R = \omega(K + R)$[39], откуда найдем $F = K + M$. **Ч.Т.Д.**

4. **Теорема о трансфинитной рекурсии.**

Сначала немного обозначений:

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

Формулировка теоремы:

Если A - ВУМ, то любое рекурсивное правило F задает функцию f, действующую из A в какое-то непустое множество, 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.**

[39] Тут порядок суммирования очень важен - не проебитесь

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[40] 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:

   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 $\exists a \exists b\,(\neg a\mathcal{R}b \land \neg b\mathcal{R}a)$. Определим порядок $\mathcal{R}'$ как $x\mathcal{R}'y$ если $\left[\begin{array}{c} x\mathcal{R}y \\ x\mathcal{R}a \land b\mathcal{R}y \end{array}\right.$

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

   Рефлексивность, тривиально выполнена.

   Антисимметричность:

[40] Т.е. не равному самому множеству

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.**

3. **Теорема о вычитании ординалов.**

Формальное сложение ординалов (рекурсивное):

1. $\alpha + 0 = \alpha$

2. $\alpha + S(\beta) = S(\alpha + \beta)$

3. $\alpha + sup(\beta) = sup(\alpha + \beta)$ Формулировка теоремы:

Если $\alpha < \beta$, то существует и единственное такое γ, что $\alpha + \gamma = \beta$

Существование: $\gamma \simeq \beta \setminus \alpha$

Единственность: От противного, пусть таких ординала два: γ_1 и γ_2. Тогда по теореме о сравнении ВУМов, БОО $\gamma_1 < \gamma_2$, откуда $\alpha + \gamma_1 < \alpha + \gamma_2$ - Противоречие. **Ч.Т.Д.**

4. **Теорема о делении ординалов.**

Формальное умножение ординалов (рекурсивное):

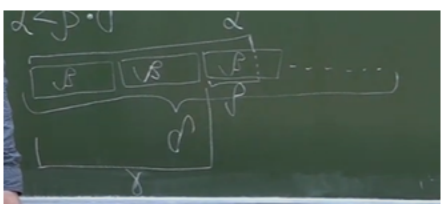
1. $\alpha \cdot 0 = 0$

2. $\alpha \cdot S(\beta) = \alpha \cdot \beta + \alpha$

3. $\alpha \cdot sup(\beta) = sup(\alpha \cdot \beta)$ Формулировка теоремы:

Если $\alpha < \beta$ и $\alpha \neq 0$, то существуют и причем единственные γ и $\delta < \alpha$, такие что $\alpha \cdot \gamma + \delta = \beta$

Существование: Возьмем γ', такое что $\alpha \cdot \gamma'$ заведомо больше β, например, $\gamma' = \beta + 1$. Тогда γ - начальный отрезок $\alpha \cdot \gamma'$, пусть будет $[0, \rho)$. Данный же отрезок будет представим в виде $\alpha \cdot \gamma + \delta$.



Единственность: Единственность остатков получим как следствие из едиственности сложения, если же частны не равны: БОО $\gamma_1 < \gamma_2$, тогда $\gamma_1 + 1 \leqslant \gamma_2$. Откуда получим: $\alpha\gamma_1 + \delta < \alpha\gamma_1 + \alpha = \alpha(\gamma_1 + 1) \leqslant \alpha\gamma_2 \leqslant_2 + \delta$ - Противоречие. **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, $\leqslant_S$)[41], такой что $\forall s \in S\,(s = \varphi([0,\, s)))$[42]

Лемма 1

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

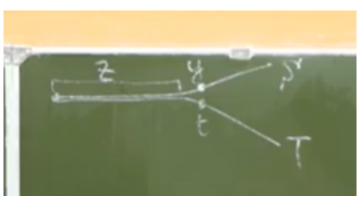
Доказательство

Сначала небольшое пояснение к тому, что тут вообще происходит. S и T - ВУМы, а значит один 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, $S = \bigcup\limits_i S_i$

Рефлексивность:

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

Антисимметричность:

[41] Далее будем просто называть S

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

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![43]

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[44]. 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. $f = min$[45]$\{x \in A \,|\, \forall y \preceq x\, (b > f(y))\}$

   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 $\{f(y) \,|\, y \in [0,\, x)\}$ - цепь, тогда по условию будет ее верхняя грань, а данное множество не имеет - противоречие.

[43] Сам в ахере
[44] Данная хуйня существует по теореме Цермело
[45] В смысле вполне порядка на A

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

Лемма

Если A *- бесконечно, то* $A \times \mathbb{N} \cong A$

Доказательство

По теореме Цермело упорядочим А, тогда по теореме о структуре ВУМов $A \simeq \omega \cdot L + F$. Откуда $A \cong \mathbb{N} \times L \cup F \cong \mathbb{N} \times L$.

$A \times \mathbb{N} \cong \mathbb{N} \times A \cong \mathbb{N} \times \mathbb{N} \times F \cong \mathbb{N} \times F \cong A$ **Ч.Т.Д.**

3. **Объединение двух бесконечных множеств равномощно одному из них.**

   Если A*,* B *- бесконечно,* $A \lessapprox B$ *то* $A \cup B \cong B$ $A \cup B \lessapprox A \times \{0\} \sqcup B \times \{1\} \lessapprox \times \{0, 1\} \lessapprox B \times \mathbb{N} \cong B \lessapprox A \cup B$

   Откуда по теореме Кантора-Бернштейна: $A \cup B \cong B$ **Ч.Т.Д.**

4. **Декартов квадрат бесконечного множества равномощен ему.**

   Рассмотрим множество пар(C, f), таких что $C \subseteq A$, $f : C \to C^2$. Введем на данном множестве порядок: $(C, f) \leqslant (D, g)$, если $C \subseteq D$ и $f = g|_C$.

   Для данного множества выполено условие леммы Цорна: верхней гранью цепи будет объединение как множеств, так и функций - как множеств пар. Покажем это:

   Пусть $\{C_\alpha\}$ - это семейство множеств, $f_\alpha : C_\alpha \to C_\alpha^2$.

   1. f - функция

   $x \in C \Rightarrow x \in C_\alpha \Rightarrow f_\alpha(x) \in C_\alpha^2 \Rightarrow f(x) \in C^2$

   Значение и будет какое-то, то единственное, потому что БОО $C_\alpha \subseteq C_\beta \Rightarrow f_\alpha(x) = f_\beta(x)$

   2. f - инъекция

   $x \in C_\alpha$, $y \in C_\beta$, БОО $C_\alpha \subseteq C_\beta \Rightarrow f_\alpha(x) = f_\beta(x)$. Так как f_β - инъекция, то $f(x) = f_\alpha(x) = f_\beta(x) \neq f_\beta(y) = f(y)$

   2. f - сюръекция

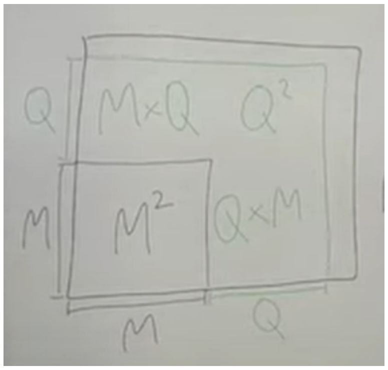
   $(x, y) \in C^2 \Rightarrow x \in C_\alpha$, $y \in C_\beta$, БОО $C_\alpha \subseteq C_\beta \Rightarrow (x, y) \in C_\beta^2$, но f_β - сюръекция, поэтому и найдется прообраз из $C_\beta \subseteq C$.

   Итак, по лемме Цорна получим (M, h) - максимальный элемент.

   Если $M \cong A$, тогда $A \cong M \cong M^2 \cong A^2$

   Если $M \lessapprox A$, тогда $A \setminus M \cong A$, тогда существует $Q \subseteq A \setminus M : Q \cong M$

   Получаем, что $Q \cong M \cong M^2 \cong Q^2 \cong Q^2 \times \{0, 1, 2\} \cong Q \times M \cup Q^2 \cup M \times Q$



А, значит, h можно продолжить на $M \cup Q$. Откуда (M, h) - не максимально - противоречие. **Ч.Т.Д.**

f. Доп вопросы на 5

g. Доп вопросы на 6

h. Доп вопросы на 7

III Вычислимость

a. Определения

b. Определения

1. ***Машиной Тьюринга*** называют кортеж $\langle \Sigma, \Gamma, Q, q_1, q_a, q_r, \delta \rangle$ или $\langle \Sigma, \Gamma, Q, q_1, q_0, \delta \rangle$

   Где:

   Σ - Входной алфавит, символы ленты, которые могут быть поданы на вход машине Тьюринга

   $\Gamma \supsetneq \Sigma$ - Ленточный алфавит, т.е. символы, которые может записывать машина Тьюринга

   Q - множество состояний машины Тьюринга

   q_1 - начальное состояние машины Тьюринга

   q_a - состояние завершения машины Тьюринга, означающее, что МТ вернула значение TRUE

   q_r - состояние завершения машины Тьюринга, означающее, что МТ вернула значение FALSE

   q_0 - состояние завершения машины Тьюринга

   $\delta : Q \times \Gamma \to Q \times \Gamma \times \{\mathcal{L}, \mathcal{N}, \mathcal{R}\}$ - функция перехода

2. ***Конфигурацией*** машины Тьюринга называют тройку $\langle\rangle$

3. ***Вычислимой функцией*** называют такую функцию, что существует алгоритм (машина Тьюринга) ее вычисляющая. Здесь под вычислющим алгоритмом мы понимаем такой алгоритм, что на входе x он останавливается, если f(x) определено и возвращает данное значение, а если f(x) неопределено, то алгоритм не остановится (Данная логика легко переносится на машину Тьюринга - проделайте это сами).

4. ***Разрешимым множеством*** называют такое множество, что существует алгоритм его разрешающий, т.е. которые по каждому элементу скажет, принадлежит ли он данному множеству или нет.

   Эквивалентное определение: Характеристическая функция данного множества вычислима, где под характеристической функцией мы понимаем $\chi(x) = \begin{cases} 0 & x \notin A \\ 1 & x \in A \end{cases}$

5. ***Перечислимым множеством*** называют такое множество, что существует алгоритм его перечисляющий, т.е. при запуске которого выведутся все элементы данного множества[46].

   Эквивалентные определения:

   1. Полухарактеристическая функция данного множества вычислима, где под характеристической функцией мы понимаем $\bar{\chi}(x) = \begin{cases} \text{Не определено} & x \notin A \\ 1 & x \in A \end{cases}$

   2. Данное множество есть область определения некоторой вычислимой функции.

   3. Данное множество является проекцией разрешимого множества пар.

6. ***Универсальной машиной Тьюринга*** называют, такую машину Тьюринга от двух аргументов, что на входе (M, x) она получает код машины Тьюринга M и запускает его на входе x.

[46] Важно отметить, что не уточняется, сколько раз эти элементы будут выведены, главное чтобы все

7. ***Универсальной вычислимой функцией*** называют, такую вычислимую функцию от двух аргументов, что для любой вычислимой функции одного аргумента f найдется такое n, что $\forall x\,(U(n,\,x) = f(x))$

8. ***Главной универсальной вычислимой функцией*** называют, такую универсальную вычислимую функцию, что для любой вычислимой функции двух аргументов V найдется всюду определенная функция s, что $\forall x\,\forall n\,(U(s(n),\,x) = V(n,\,x))$

9. Множетство A ***m-сводимо*** ко множеству B (Обозначение $A \leqslant_m B$, если существует такая вычислимая функция $f\,:\,A \to B$, что $x \in A \Leftrightarrow f(x) \in B$.

c. Простые утверждения

1. **Композиция вычислимых функций вычислима.**

   Пусть первую функцию вычисляет машина Тьюринга M, а вторую - K. Тогда построим машину тьюринга вычисляющую их композицию: Это будет машина Тьюринга Л, которая сначала работает как M, а когда она попадает в завершающее состояние M, то она запускает машину тьюринга K. (Соответственно нумерацию состояний сдвинем на нужное число и получим общую нумерацию для Л).

2. **Существование невычислимых функций, неразрешимых и неперечислимых множеств.**

   Так как всего машин Тьюринга счетное число - это кортежи из конечного числа элементов, то и вычислимых функций тоже счетное число. С другой же стороны всего функций из $\mathbb{N}$ в $\mathbb{N}$ - несчетное число, тогда из соображений мощности найдутся невычислимые функции

   Аналогично и для разрешимых/перечислимых множеств - для них есть машины тьюринга, которые их разрешают/перечисляют, а их не более чем счетное число, в то время как всего подмножеств $\mathbb{N}$ - несчетное.

3. **Разрешимость любого конечного множества.**

   Так как множество лишь конечное, то можно просто проверить подаваемый элемент на равенство каждому элементу.

4. **Перечислимость любого разрешимого множества.**

   Множество разрешимо, следовательно, вычислима его характеристическая функция, тогда построим по ней полухарактеристическую функцию: если характеристическая возвращает 1, то и характеристическая тоже, а если 0 - то зацикливается.

5. **Замкнутость классов разрешимых и перечислимых множеств относительно пересечения и объединения, класса разрешимых относительно дополнения.**

   Разрешимость:

   Пусть χ_A и χ_B - характеристические функции разрешимых множеств A и B. Тогда $\chi_{A\cup B} = \chi_A \vee \chi_B$, $\chi_{A\cap B} = \chi_A \wedge \chi_B$, $\chi_{\bar{A}} = \neg\chi_A$

   Перечислимость:

   Пусть A и B - перечислимы, тогда запустим алгоритм, перечисяющий множество A, на три шага, потом запустим на три шага алгоритм, перечисляющий B, и т.д. Данным образом перечислим все элементы из $A \cup B$

Пусть A и B - перечислимы, тогда запустим как в прошлый раз их перечисляющие алгоритмы. Будем сохранять их вывод - он конечен в каждый момент времени работы, поэтому это возможно (Например, под это можно выделить специальную ленту машины Тьюринга). Тогда если в какой-то момент времени одна из машин Тьюринга выведет число, которое уже вывела вторая - выведем данное число. Так мы перечислим их пересечение.

6. **Существование вычислимой в обе стороны биекции между $\mathbb{N}^2$ и $\mathbb{N}$.**

   Самое время сослаться на тот ужас, что я написал в простых утверждения в тм. "Декартово произведение счётных множеств счётно

7. **Подмножество разрешимого (перечислимого) множества не обязательно разрешимо (перечислимо), и наоборот.**

   Множество натуральных разрешимо и перечислимо, но при этом ранее мы показали, что есть его неперечислимые, а, значит, и неразрешимые подмножества.

   В свою же очередь пустое множество является и разрешимым, и перечислимым. Оно является подмножеством любых множеств, в том числе и неразрешимых/неперечислимых.

8. **Свойства m-сводимости: транзитивность, сводимость дополнений, разрешимость множества, m-сводимого к разрешимому, перечислимость множества, m-сводимого к перечислимому, сводимость разрешимого множества к любому нетривиальному.**

9. **Пример λ-терма, к которому можно применить β-редукцию только после α-конверсии.**

   $(\lambda xy.x)y \to (\lambda xt.x)y \to \lambda t.y$

10. **Пример λ-терма, не имеющего нормальной формы.**

    Это терм $(\lambda a.aa)(\lambda a.aa)$

d. Вопросы на 3

1. **Эквивалентность следующих утверждений: множество перечислимо, полухарактеристическая функция множества вычислима, множество является областью определения вычислимой функции, множество является проекцией разрешимого множества пар.**

   1. Множество перечислимо, т.е. сущесвует алгоритм, перечисляющие все элементы заданного множества
   2. Полухарактеристическая функция множества вычислима
   3. Множество является областью определения вычислимой функции
   4. Множество является проекцией разрешимого множества пар

$1 \to 2$

Берем число на вход полухарактеристической функции, запускаем перечислятор, как только данное число выведется завершаем работу и выводим 1.

$2 \to 3$

Заметим что, областью определения полухарактеристической функции как является наше множество

$3 \to 4$

f - вычислимая функция, Dom которого является нашим перечислимым множеством. Тогда определим множество пар, как $\{(x,\, t) \,|\, f(x)\, \text{останавливается за}\ t\ \text{шагов}\}$

$4 \to 1$

Воспользуемся существованием вычислимой в обе стороны биекции из $\mathbb{N} \to \mathbb{N}^2$ и обойдем все пары $(x,\, y)$, тогда если $(x,\, y)$ во множестве $\{(x\, y)\}$[47], то выведем x - так мы высечем проекцию разрешимого множества - то есть наше перечислимое множество.

2. **Теорема Поста: критерий разрешимости в терминах перечислимости множества и его дополнения.**

   Формулировка:

   A - разрешимо A - перечислимо и коперечислимо

   Доказательство

   $\Rightarrow$

   Еще раз покажем доказательство перечислимости для разрешимого множества:

   Множество разрешимо, следовательно, вычислима его характеристическая функция, тогда построим по ней полухарактеристическую функцию: если характеристическая возвращает 1, то и характеристическая тоже, а если 0 - то зацикливается.

   Так как дополнение разрешимого - разрешимо, вот еще раз доказательство:

   Разрешимость:

   Пусть χ_A и χ_B - характеристические функции разрешимых множеств A и B. Тогда $\chi_{A\cup B} = \chi_A \vee \chi_B$, $\chi_{A\cap B} = \chi_A \wedge \chi_B$, $\chi_{\bar{A}} = \neg\chi_A$

   То аналогичным образом и дополнение A перечислимо - все готово в одну сторону.

   $\Leftarrow$

   Для определения принадлежности множеству элемента, запустим перечисление самого множества на 3 шага, далее перечисление его дополнения - так будем чередовать, пока данный элемент не будет выведен и, в зависимости, от того кем из перечисляторов был выведен данный элемент скажем принадлежит он или нет. **Ч.Т.д.**

3. **Неразрешимость проблем самоприменимости и остановки.**

   Проблема самоприменимости:

   Определить по n, будет ли определена ли $U(n,\, n)$[48] - можно ли применить к машине Тьюринга ее же код

[47] Данный момент вычислимо возможен благодаря разрешимости множества пар

[48] U - некоторая универсальная машина Тьюринга

Для доказательства данных фактов используется так называемый диагональный метод, но увы не Кантора.

Предполагаем обратное - пусть разрешимо. Тогда Построим функцию: $d(x) = \begin{cases} U(n, n) & \text{если определено } U(n, \ ) \\ 0 & \text{иначе} \end{cases}$, далее возьмем функцию $d'(x) = d(x) + 1$ - она вычислима, а значит она где-то занумерована в $U(n, x)$, но она отличается ото всех диагоналей $\Rightarrow$ проблема самоприменимости неразрешима, т.е. неразрешимо множество $\{n \mid U(n, n) \text{ определено}\}$

Проблема остановки:

Определить по n и k, будет ли определена ли $U(n, k)$[49] *- остановится ли машина Тьюринга на заданном входе*

Заметим, что проблема самоприменимости - частный случай проблемы остановки, поэтому из разрешимости второй следовала бы разрешимость первой, а, значит, данная проблема неразрешима.

4. **Теорема Чёрча–Россера (б/д). Единственность нормальной формы.**

   Если $M \twoheadrightarrow N$, $M \twoheadrightarrow P$, то $\exists Q\ (N \twoheadrightarrow Q \wedge P \twoheadrightarrow Q)$, M, N, P, Q - λ-термы

   Единственность нормальной формы

   Пусть $\Lambda \twoheadrightarrow N$, $\Lambda \twoheadrightarrow M$, M, N - нормальные формы Λ, тогда они α-эквивалентны[50]*, т.е. переходят друг в друга α-конверсиями*

   По т. Черча-Россера получим, что найдется такой R, к которому сведутся и M, и N. Но ни к M, и к N применить β-редукцию нельзя, значит R был получен α-конверсиями, а так как они обратимы, то и из N в M можно перейти α-конверсией. **Ч.Т.Д.**

e. Вопросы на 4

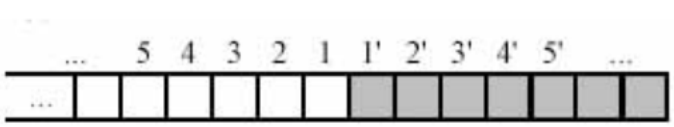
1. **Моделирование машины Тьюринга с несколькими лентами на машине Тьюринга с одной лентой.**

   Приведем общее описание данной машины Тьюринга.

   Лемма

   Для любой машины Тьюринга найдется ей эквивалентная работающая на полубесконечной ленте

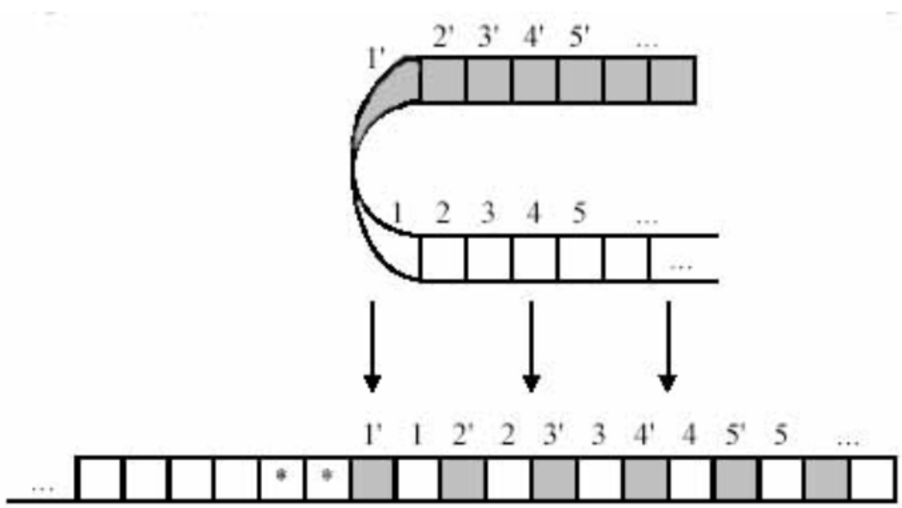
   Выделим специальный символ, который не входит в алфавит машины Тьюринга. БОО пусть это $*$. Выделим какую-то точку отсчета на ленте машины Тьюринга (границу двух клеток), и пустим нумерацию влево и вправо от нее. Положим все клетки что слева на четные номера, а то, что справа - на нечетные.



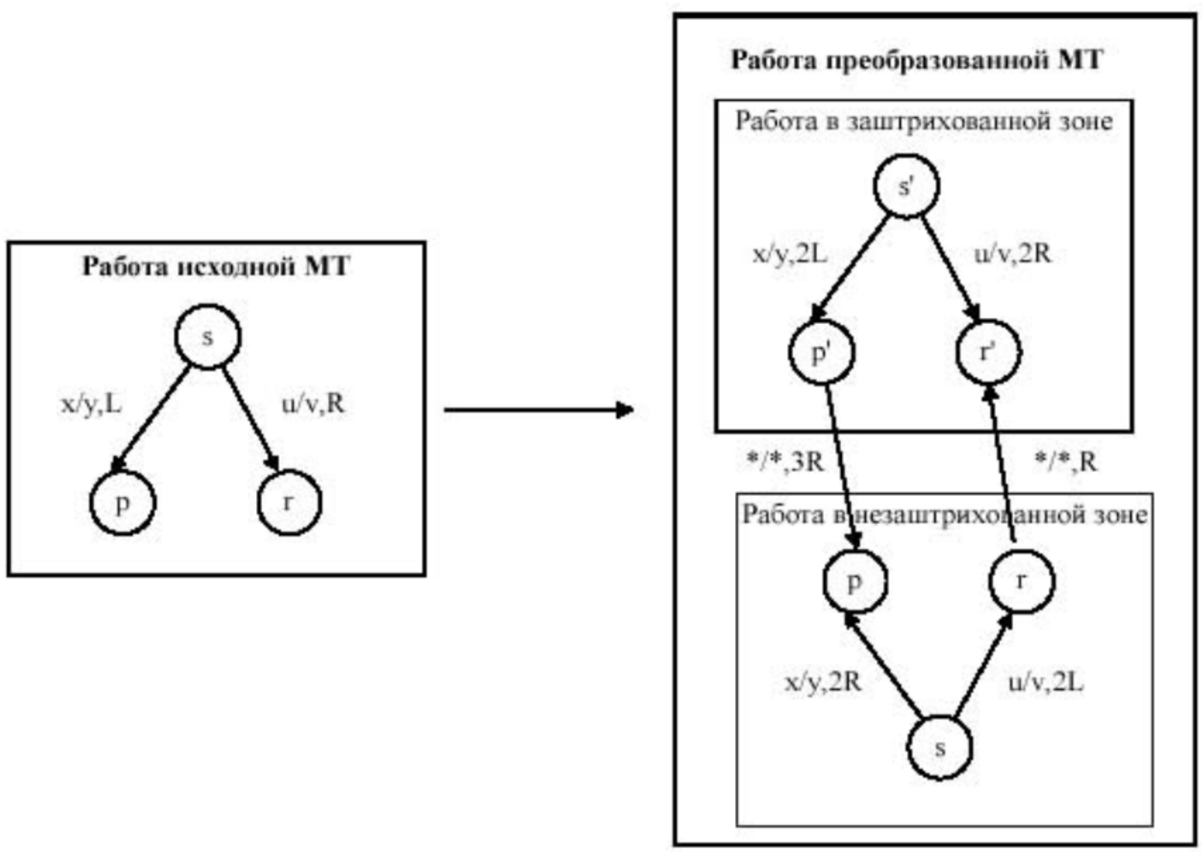
[49] U - некоторая универсальная машина Тьюринга

[50] Умное слово, если не готовы на экзамене доказывать, что α-конверсии задают отношение эквивалентности, то просто скажите пояснение

Теперь отметим на бесконечной ленте два символа $*$ - это теперь наше начало отсчета, и положим все номера, что влево занумерованы на нечетные позиции, а что занумерованы вправо - на четные.



Теперь удвоим количество состояний - для четной и нечетной зоны и сменим работу машины тьюринга так, чтобы она теперь сдвигалась не на одну позицую а на две (например, введением доп состояний перехода).



Далее осталось сказать, что мы добавим еще состояния распознающие $*$ и переключающие четность/нечетность при попадании на них. Так мы получим эквивалентную машину.

Теперь же конструирование машин на несколькоких лентах максимально просто:

Каждую ленту переведем по лемме в полубесконечную. Для определенности занумеруюем их - их будет конечное число - k штук. Теперь же аналогичным методом пользуемся модульной арифметикой: разбиваем подряд ячейки по модулю k. На соответсвующем остатке будет работать своя лента многоленточной машины ТЬюринга (простите за тавтологию). Неформально все готово, формально же осталось сказать как алгоритм переписать. Ну тут все просто: если переход в многоленточной машине Тьюринга - это состояние нескольких, то в одноленточной - просто одной. Поэтому мы каждое состояние многоленточной МТ разбиваем на k состояний одноленточной, которые будут себя последовательно запускать - для определенности по по порядку лент, например. Также выделим для каждого символа ленточного алфавита его помеченную копию - данными символами будем помечать, где машина Тьюринга остановилась сейчас. Теперь добавим еще несколько состояний - напишем "главный процессор"одноленточной. Это будут состояния анализирующие текущее состояние машины тьюринга и запускающие соответствующие рабочие состояния, которые мы уже описали. Если кратко, то они будут выглядеть в виде: состояние анализа ленты 1: дошли до помеченного символа в зависимости от выделенного символа, перешли в соответствующее состояние анализа ленты 2 ... так до ленты k - в ней мы уже точно знаем, что на лентах 1 ... $k-1$ нашли состояние на ленте k - тогда перевели на первую ленту и запустили нужное состояние работы мт (тут ленты - учаски полубесконечной ленты в одноленточной мт). Все готово! Безусловно, мы добавили очень много новых состояний и доп символов, но, очевидно, нигде за конечность не вышли - поэтому все ок.

2. **Несуществование универсальной тотально вычислимой функции.**

   От противного - пусть существует. Снова воспользуемся диагональным методом:

   Определим фунцию $d(x) = T(x, x)$[51], далее возьмем $d'(x) = d(x)+1$, и увы, она с одной стороны должна быть занумерована в T, но она везде отличается на диагонали. Противоречие - **Ч.Т.Д.**

3. **Существование главной универсальной вычислимой функции.**

   Так как найдется вычислимая тернарная функция универсальная для класса всех бинарных функций (Просто занумеруем все бинарные функции (их счетное число), а далее поожим $T(i, x_1, x_2) = B_i(x_1, x_2)$). Теперь по заданному T строим ГУВФ: $\Gamma(\beta(n,k), x) = T(n, k, x)$, где $\beta : \mathbb{N}^2 \to \mathbb{N}$ - вычислимая в обе стороны и тотальная[52] биекция. Тогда по любой бинарной функции $V(k, x)$ найдется тотальная функция $\varrho(k) = \beta(n, k)$, где n - номер V в T, такая что $V(k, x) = \Gamma(\varrho(k), x)$. Т.е. Г - ГУВФ. **Ч.Т.Д.**

4. **Построение комбинаторов логических значений, булевых функций, операций с парами, проверки на ноль для нумералов Чёрча (с доказательством корректности).**

[51] Та самая тотальная функция

[52] Всюду определенная

За логические константы берутся следующие комбинаторы:

$\mathfrak{False} = \lambda y.xy$ - высечение второй координаты

$\mathfrak{True} = \lambda x.xy$ - высечение первой координаты

Теперь я радостно сыпану комбинаторов для кучи булевых функций, а проверять уже их будете вы сами на экзамене - по примеру))

$\wedge$	$\lambda pq.pqp$
$\vee$	$\lambda pq.ppq$
$\neg$	$\lambda p.p\,\mathfrak{False}\,\mathfrak{True}$
$\rightarrow$	$\lambda pq.qq(p\,\mathfrak{False}\,\mathfrak{True})$
$\oplus$	$\lambda pq.(pqp)\,\mathfrak{False}\,(ppq)$
$\leftrightarrow$	$\lambda pq.pq(q\,\mathfrak{False}\,\mathfrak{True})$
$\mid$	$\lambda pq.(pqp)\,\mathfrak{False}\,\mathfrak{True}$
$\downarrow$	$\lambda pq.(ppq)\,\mathfrak{False}\,\mathfrak{True}$

Первые четыре маст хэв, остальные - по желанию.

Теперь проверка:[53]

Для примера возьмем $p \oplus q$:

Пусть $p = 1$, тогда подставляем вместо p - $\mathfrak{True}$:

$(\lambda pq.(pqp)\,\mathfrak{False}\,(ppq))\,\mathfrak{True} \xrightarrow{\beta} \lambda q.(\mathfrak{True}\,q\,\mathfrak{True})\,\mathfrak{False}\,(\mathfrak{True}\,\mathfrak{True}\,q) \xrightarrow{\beta} \lambda q.q\,\mathfrak{False}\,\mathfrak{True}$ - получили отрицание q - все как и надо. Теперь $p = 0$, тогда подставляем вместо p - $\mathfrak{False}$:

$(\lambda pq.(pqp)\,\mathfrak{False}\,(ppq))\,\mathfrak{False} \xrightarrow{\beta} \lambda q.(\mathfrak{False}\,q\,\mathfrak{False})\,\mathfrak{False}\,(\mathfrak{False}\,\mathfrak{False}\,q) \xrightarrow{\beta} \lambda q.q$ - получили q - все как и надо.

Комбинаторы пары:

$\mathfrak{Pair} = \lambda xyp.pxy$ - образование пары

$\mathfrak{Left} = \lambda p.p\,\mathfrak{True}$ - получение левой компоненты

$\mathfrak{Right} = \lambda p.p\,\mathfrak{False}$ - получение правой компоненты Теперь проверка на 0:

$\mathfrak{IsZero} = \lambda k.k(\lambda k.\,\mathfrak{False})\,\mathfrak{True}$

Проверим корректность данной формулы:

$\mathfrak{IsZero}\,\bar{0}$[54] $\xrightarrow{\beta} \bar{0}(\lambda k.\,\mathfrak{False})\,\mathfrak{True} \xrightarrow{\beta} \mathfrak{True}$ - бомбезно

Теперь не ноль, значит имеет вид $\overline{n+1}$:

$$\mathfrak{IsZero}\,\overline{n+1} \xrightarrow{\beta} \overline{n+1}(\lambda k.\,\mathfrak{False})\,\mathfrak{True} \xrightarrow{\beta} \lambda fx.\,\underbrace{f(..f(f}_{n\text{ раз}}\,x)..)(\lambda k.\,\mathfrak{False})\,\mathfrak{True} \xrightarrow{\beta}$$

$$\xrightarrow{\beta} \underbrace{(\lambda k.\,\mathfrak{False})(..(\lambda k.\,\mathfrak{False})((\lambda k.\,\mathfrak{False})}_{n\text{ раз}}\,\mathfrak{True})..) \xrightarrow{\beta} \ldots \xrightarrow{\beta} (\lambda k.\,\mathfrak{False})\mathfrak{True} \xrightarrow{\beta} \mathfrak{False}$$

[53] Возможно к экзамену будет по подробнее - пока так

[54] Мусатов подчеркивал снизу, но в латех заебешься подчеркивать каждый раз снизу - поэтому сверху

f. Вопросы на 5

g. Доп вопросы на 5

h. Доп вопросы на 6

i. Доп вопросы на 7