1) Математическая логика (МЛ). Ее предмет и задачи.

Логика - это анализ методов рассуждение.
Осн. задача: найти корректные способы рассуждение.

Формальная логика (Кант) - раздел философии который изучает и анализирует высказывание, опираясь на истину или ложь (рассм. форму).

МЛ - яв-ся формальной, это более узкий раздел, она не рассматривает ничего, что не определено четко и однозначно. Отн-ся только к математике.

Причины развития МЛ:
- изменение роли математики в науке
- стал понятен хар-р нетривиальной связи между теорией и экспериментом
- зависимость научных рез-тов от структуры и состава языка науки.

Задачи МЛ:
- изучение и формализация языка науки.
- развитие основ математики
- разработка принципов и методов построение теорий и их совершенствование

② Антиномии и их влияние на развитие МЛ

На рубеже 19-20 вв были обнаружены антиномии, связанные с основными понятиями теории множеств. Анализ антиномий привел к различным планам по их устранению.

Антиномии – ситуации, в которых противоречащие друг другу высказывание об одном и том же объекте имеют логически равноправное обоснование, т.к. нельзя четко обосновать их истинность или ложность.

Антиномии делятся на ~~лог~~ семантические и логические.

Логические (П) Парадокс Рассела:

~~Я~~- Мн-во всех мн-в, кот-е не содержат себя в качестве собственного эл-та. $x \in X \Leftrightarrow x \notin X$

Какой бы подход к исследованию парадоксов не выбрать, нужно сперва исследовать язык логики и математики, чтобы разобраться, какие символы могут быть использованы, как из них составляются ~~[illegible]~~, ~~[illegible]~~, термы, формулы, утв-е и док-ва, ~~[illegible]~~ что может и не может быть доказано, если исходить из тех или иных аксиом и правил вывода. В этом состоит одна из задач МЛ. Глубокие исследования различных математиков привели к завоеванию для МЛ положения независимой ветви математики.

3. Семиотика (осн. понятия и опр-е, равносильность форм).

Наука семиотика занимается изучением языка как такового.

Основные понятия:

Высказывание — нек-е фраза или предложение естественного языка, о котором разумно говорить, истинно оно или ложно.

Буква — некоторый символ, который воспринимается только как нечто целое.

Алфавит — конечная совокупность букв.

Слово — любая совокупность букв данного алфавита, записанных одна за одной в строку.

Выражение — любая совокупность букв фиксированного алфавита, записанная в разумном порядке.

Переменная — нек-е буква, которая может принимать мн-во разных значений (именные и высказывательные). Переменная может иметь 2 варианта вхождения в форму: свободное и связанное. $\mathfrak{A}(x, y, z \dots)$ $\mathfrak{P}(x, y, z, w, v)$

Если из контекста понятно, от каких перем-х зависит форма, то исп-ют обознач-е $*\mathfrak{A}(\cdot)$.

Форма — выражение, которое содержит хотя бы одну переменную. (именная и высказыват-я)

$!\mathfrak{A}(a, b, c)$ — означает, что от этих значений форма становится осмысленным выражением.

Форма наз-ся формулой, если для наборов своих переменных она принимает значение высказывания.

Равносильность (эквивалентность) форм.

Две формы наз-ся равносильными, если для каждого набора значений своих переменных они либо не определены, либо обе определены и принимают одно и то же значение.

Равносильность обозн-ся как „$\simeq$"

для высказ. „$\equiv$" для имен. „$=$"

Смысловые аспекты исп-я „$=$":

1) Два имени одного и того же
2) Задание выск-х форм
3) Для записи ур-ий с числовыми формами.
4) Равносильность именных форм.

[5)] Для определений ($\leftrightharpoons$, $\triangleq$, $\overline{\overline{Df}}$)

Для исп-я символа как имени объекта, его необходимо заключать в кавычки.

4. Конструктивное определение множества.

Формальное определение понятия:

1) $\varnothing$ – пустое множество.

2) Пусть M – нек-й объект, тогда $\{M\}$ – мн-во.

3) Пусть M_1 и M_2 мн-ва, тогда $M_1 \cap M_2$, $M_1 \cup M_2$, $M_1 \setminus M_2$ – мн-ва.

4) Совокупность бесконечных мн-в N, R, Z, C

5) Пусть M – мн-во, тогда $\exists$ мн-во всех его подмножеств $\mathfrak{M}$.

6) Пусть M – нек-е мн-во, $\mathcal{O}(x)$, $x \in M \to$
$\to M_1 = \{x \in M \mid \mathcal{O}(x)\}$ – мн-во.

7) Других мн-в не существует.

5. Кортеж (определение, прямое произв-е, проекция)

Кортеж – n-ка $<a_1, a_2, \dots, a_n>$ нек-е выр-е, ~~~~ начинающееся с <, содержащее набор нек-х имен, набор „," , „>"

Число компонент кортежа называют его длиной.

Вектор – частный случай кортежа (компоненты – коорд-ы)

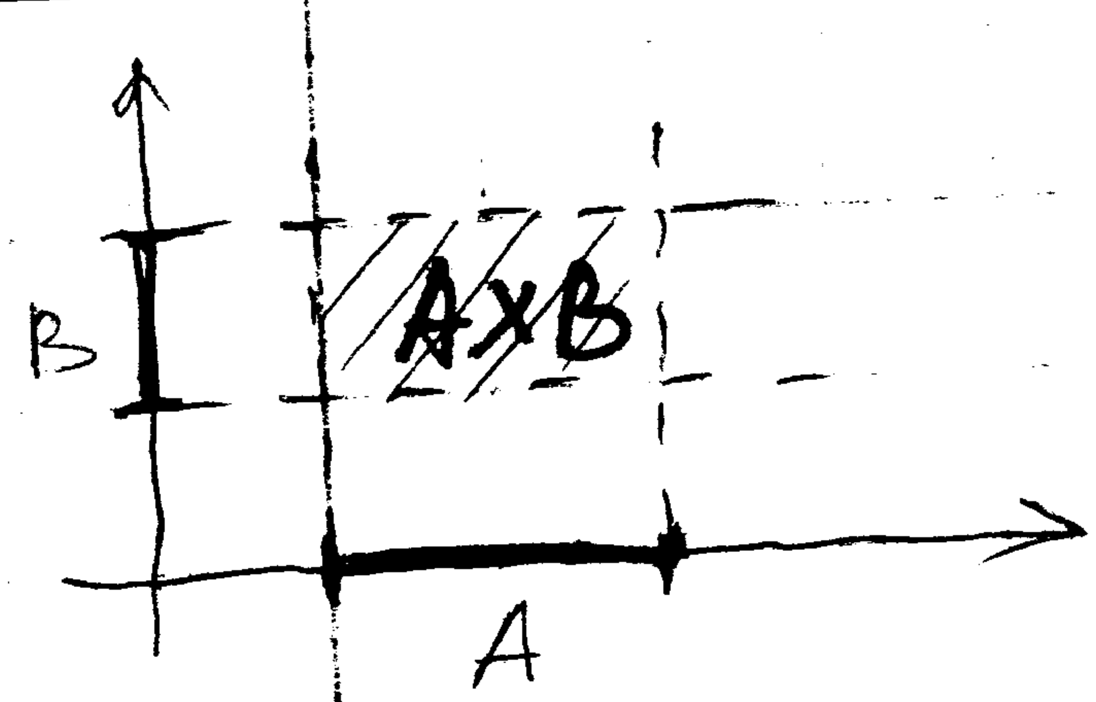
Кортеж, у которого нет ни одной компоненты, наз-ся пустым и обозн-ся Λ или $<>$.

Кортеж длины 2 наз-ся парой, 3 – тройкой и т.д.

Кортежи считаются равными, когда они одинаковой длины и соотв-щие ~~~~ компоненты равны.

$\alpha \leftrightharpoons <a, b>$, тогда $\alpha^{-1} = <b, a>$ (инверсия)

Прямое произведение мн-в $M_1 \times M_2$ – мн-во тех и только тех пар, первая компонента которых из M_1, а вторая из M_2.



<u>Проекция:</u>

$Пр_i\, \alpha$

Пусть α - нек-й кортеж $\langle a_1, a_2, \dots, a_n \rangle$

$Пр_i\, \alpha = a_i$

$Пр_{i,j,\dots k}\, \alpha = \langle a_i, a_j, \dots, a_k \rangle$, $i < j < \dots < k$

Проекция мн-ва - операция проекций применимо только к мн-вам кортежей одинаковой длины или к $\varnothing$.

$Пр_i\, M = \{\dots\}$ - проекц. i-ых эл-тов кортежей.

$Пр\, \varnothing = \varnothing$

$Пр_\varnothing\, M = \{\lambda\}$, если $M \neq \varnothing$

(6.) <u>График.</u>

График G - нек-е мн-во пар. $G \subseteq A \times B$

$пр_1 G$ - обл. опр-я графика.

$пр_2 G$ - обл значений графика.

Инверсия графика (G^{-1}) - мн-во инверсий его пар. График наз-ся симметричным, если вместе с любой парой он содержит ее инверсию. $\varnothing$ - симметр. гр-к.

Композиция графиков:

$G \circ F \rightleftharpoons \{\langle a, y \rangle \mid \exists z\ \langle a, z \rangle \in G, \langle z, y \rangle \in F\}$

Гр-к наз-ся функциональным, если не содержит пар с одинаковыми первыми и различными вторыми координатами.

Гр-к наз-ся инъективным, если не содержит пар с различными первыми и одинаковыми вторыми координатами.

Композиция сохраняет ф-ность и инъек-ть.

Док-во (для инъект.) G и F - инъективн. графики.
Докажем, что $G \circ F$ - инъективен.

Допустим противное $\Rightarrow \langle a, y\rangle, \langle b, y\rangle \in G \circ F, a \neq b$

$\langle a, z\rangle \in G \quad \langle z, y\rangle \in F$

$\langle b, x\rangle \in G \quad \langle x, y\rangle \in F$

Если $z \neq x \Rightarrow F$ не инъективен

Если $z = x \Rightarrow G$ не инъективен.

Противореч. доказывает св-во.

Док-во (для ф-ти): Докажем, что $G \circ F$ - ф-ный гр-к, если G и F - ф-ные гр-ки.

Предположим противное, тогда:

$\langle x, a\rangle, \langle x, b\rangle \in G \circ F, \quad a \neq b$

$\langle x, c\rangle \in G, \quad \langle c, a\rangle \in F$

$\langle x, d\rangle \in G \quad \langle d, b\rangle \in F$

Если $c = d \Rightarrow F$ не ф-лен.

Если $c \neq d \Rightarrow G$ не ф-лен.

Противоречие доказывает св-во.

Инверсия меняет ф-ность на инъективность и инъективность на ф-ность.

(7) Соответствие

Соответствием наз-ае тройка мн-в $<G, X, Y>$,
где X - обл. отправл.
Y - обл. прибытия
G - график, $G \subseteq X \times Y$.
$пр_1 G \subseteq X$, $пр_2 G \subseteq Y$
$\Gamma \leftrightharpoons <G, X, Y>$

- $\Gamma^{-1} \leftrightharpoons <G^{-1}, Y, X>$ инверсия.

$\Theta = <T, Z, W>$

- $\Gamma \circ \Theta = <G \circ T, X, W>$ композиция
- $\Gamma_A \leftrightharpoons <G \cap A \times пр_2 G, X, Y>$ сужение Γ на мн-во A.

<u>Сечение</u> $B \subseteq Y$, $B = \Gamma(\{a\})$ - те эл-ты из Y, кот-е
$a \in пр_1 G$ поставлены в соотв.-е a.
<u>Образ</u> мн-ва A. $\Gamma(A)$ при соотв. Γ.
$\Gamma(A) \subseteq пр_2 G$, $A \subseteq пр_1 G$
<u>Прообраз</u>. $\Gamma^{-1}(A) \subseteq пр_1 G$
$A \cap пр_2 G$

Св-ва:
1) $A \subseteq B \Rightarrow \Gamma(A) \subseteq \Gamma(B)$
2) $\Gamma \circ \Theta(A) = \Theta(\Gamma(A))$
3) $\Theta \circ \Gamma(A) = \Theta(\Gamma(A))$
4) Соотв-е ф-но, если его гр-к ф-лен.
5) Соотв-е инъективно, если его гр-к инъективен
6) Соотв-е всюду определено, если $пр_1 G = X$
7) Соотв-е сюръективно, если $пр_2 G = Y$
8) Соотв-е биективно, если обл-ет св-вами 4, 5, 6, 7.

(8.) Функция

Функция - это функциональное соответствие.

$f = \langle F, X, Y \rangle$, F - ф-ный график

$пр_1 F$ - обл. отправ-е

$пр_2 F$ - обл. прибытия

$f: X \to Y$

$!f(a)$ - ф-ия определена

$$\left.\begin{matrix} f(a) = b \\ f(\{a\}) = \{b\} \end{matrix}\right\} \langle a, b \rangle \in F$$

Частные случаи ф-ий:

1) $F = \varnothing$ ф-ия нигде не опр-на

2) $I_m \leftrightharpoons \langle \Delta m, M, M \rangle$ тождественная ф-ия

3) $A \subseteq пр_1 F$ ф-ия опр-на на ...

4) Отображение $X \to Y$ - ф-ия задана на X и отобр.-на в Y...

Если ф-ия инъективна, то ее инверсия функцион-на

$f^{-1} \circ f = пр_2 F$

$f \circ f^{-1} = пр_1 F$

Для любой ф-ии f сущ-ет такая ф-ия g, что:

$\forall f \ \exists g: g \circ f = I\, пр_2 F$

Док-во: $b \in пр_2 F$

$\langle x, b \rangle \in F$ $i = \overline{1, n}$

$\langle b, x \rangle \in G$ $// \langle x, b \rangle \in F$.

Обратная ф-ия:

Для f обратной наз-ся ф-ия g такая, что:

1) $g \circ f = I\, пр_2 F$

2) g - инъекция

3) $\left[\begin{matrix} пр_1 G = пр_2 F \\ пр_2 G \subseteq пр_1 F \end{matrix}\right]$ $G \subseteq F^{-1}$

9. <u>Отношение</u>.

1) Отношение – мн-ва n-ок (n-местное отн-е)
$\langle a_1, a_2, \dots a_n \rangle \in \Phi$

2) Бинарное отношение.
а) График (мн-во пар, ориент. граф, таблица)
б) Соответствие $\varphi \triangleq \langle \Phi, M \rangle : \Phi \subseteq M^2$
в) Высказывательная форма $x \varphi y = \mathfrak{A}(x, y)$

частные случаи отношений:
- $\Theta_m \triangleq \langle \varnothing, M \rangle$ отн-е с пустым гр-ком
- $\Theta_m \triangleq \langle M^2, M \rangle$ отн-е с прямым произв-ем.
- $E_m \triangleq \langle \Delta_m, M \rangle$ отн-е равенства
- $O_\varnothing \triangleq \langle \varnothing, \varnothing \rangle$
- $\Theta_m \setminus E_m$ отн-е неравенства

<u>Операции</u> над отношениями:
1) $\varphi \vee \psi \Leftrightarrow \Phi \cup \Psi$
2) $\cap$ $\cap$
3) $\setminus$ $\setminus$
4) $\overline{\varphi} \overset{=}{_{df}} \Theta_m \setminus \varphi$ $\varphi \langle \Phi, M \rangle$ $M^2 \setminus \Phi$ дополнение
5) $\varphi^{-1} \triangleq \langle \Phi^{-1}, M \rangle$
6) $\varphi \circ \psi \triangleq \langle \Phi \circ \Psi, M \rangle$
7) $\varphi_A \triangleq \langle \Phi \cap A^2, A \rangle$, $A \subseteq M$ сужение.
8) $x \varphi y$ $\triangleq$ $\varphi \in \{ \neg, \&, \vee \}$
9) $\varphi \to \psi \leftrightarrow \Phi \subseteq \Psi$ – импплицирование (отн-е между двумя соотв-ями). φ импплицирует ψ, если Φ включен в гр-к Ψ

Св-во отношений:
1) Рефлексивность: $\forall x \in M \quad x \varphi x$, $\Delta_m \subseteq \Phi$. %: O_ϕ, Θ_m, E_m
2) Антирефлексивность: $\neg(x\varphi x) \ \forall x \in M$, $\Delta_m \cap \Phi = \varnothing$. %: O_m, O_ϕ
3) Симметричность $\forall x,y \in M \quad x\varphi y \leftrightarrow y \varphi x$, $\Phi = \Phi^{-1}$ %: $O_\phi, O_m, \Theta_m, E_m$
4) Антисимметричность $\forall x,y \in M \ x\varphi y \rightarrow \neg(y\varphi x)$, $\Phi \cap \Phi^{-1} \subseteq \Delta_m$ %: O_ϕ, O_m, E_m
5) Транзитивность $\forall x,y,z \in M \ x\varphi y \,\&\, y\varphi z \rightarrow x \varphi z$, $\Phi \circ \Phi = \Phi$. %: $O_\phi, O_m, \Theta_m, E_m$
6) Связанность $\forall x \neq y \in M \ x\varphi y \vee y \varphi x$, $M^2 | \Delta_m \subseteq \Phi \cup \Phi^{-1}$ %: O_ϕ, O_m, Θ_m

Теорема: Если отношение обладает каким-либо св-вом, то оно сохраняется при инверсии.

Док-во (для транзит., ост. аналог.) Пусть φ - транзитивно.
$\varphi^{-1} \quad x\varphi^{-1} y \,\&\, y \varphi^{-1} z \leftrightarrow y\varphi x \,\&\, z \varphi y \xrightarrow{\text{транз.}} z \varphi x \leftrightarrow x \varphi^{-1} z$

Теорема: Операция ~~композиции~~ сужение сохраняет все отношение.

Док-во: (для симметр., ост. аналог.). Пусть φ, ψ - симметр.
$x \varphi \circ \psi y \leftrightarrow \exists_z \in M \ x \varphi z \,\&\, z \psi y \leftrightarrow z \varphi x \,\&\, y \psi z \leftrightarrow y \varphi \circ \psi x$

$\tilde{\varphi}$ - отн-е эквивалентности.
1) $\tilde{\varphi}$ - рефлекс-ть, симметр-ть, транз-ть, $\sim$ эквив-ть
$M\,K_a$, где $a \in M$, $K_a \subseteq M$, $b \in M$ & $\langle a,b\rangle \in \tilde{\Phi} \rightarrow b \in K_a$
2) Нестрогий порядок - рефлекс, антисимметр., транзитив.,
$A \subseteq B$

3) Нестрогий совершенный порядок - нестрогий + связанность. $a \leq b$

4) Строгий порядок - антирефлекс. и антисимметр. $A \subset B$
5) Строгий совершенный порядок - строгий + связанность

Терм - обобщение понятий const, переменная и ф-ия от их значений.

(10) Разбиение, сопряженное с отношением.

Разбиение - система мн-в со следующими св-вами: $\mathfrak{M}$ - разбиение

1) $\forall A \in \mathfrak{M} \rightarrow A \subseteq M,\ A = \emptyset$
2) $\forall A, B \in \mathfrak{M} \rightarrow A \cap B = \emptyset$
3) $\bigcup_{A \in \mathfrak{M}} A = M \quad // \quad \bigcup A \supseteq M$

Примитивные разбиение: M-исх. мн-во.

1) Полное разбиение $\mathfrak{M} = \{M\}$
2) Поэлементное разбиение $\forall a \in M \rightarrow \{a\} \in \mathfrak{M}$

$\emptyset$ - полное $\Rightarrow \{\emptyset\}$ $\qquad \{\{a\}\} \Leftarrow \{a\}$

~~$\{a\}$~~ поэлементное $\Rightarrow \emptyset$ $\qquad \{\{a\}\} \Leftarrow$

~~Отнош~~ Разбиение, сопряженное с отношением.

$\varphi = \langle \Phi, M \rangle \qquad \mathfrak{M} = \bigcup A$

φ сопряжено с $\mathfrak{M}$ т.т.т.к. $a, b \in A \leftrightarrow a \varphi b$.

<u>Теорема 1</u> Пусть $\mathfrak{M}_1$ и $\mathfrak{M}$ - два разбиение мн-ва M и они сопряжены с одним и тем же отношением φ на этом мн-ве. Тогда $\mathfrak{M}_1 = \mathfrak{M}$

<u>Док-во:</u> Допустим, что $\mathfrak{M}_1 \neq \mathfrak{M} \Rightarrow$

$\Rightarrow \exists a, b \in M : a, b \in K_1 \in \mathfrak{M}_1 \Rightarrow a \varphi b$

$\underbrace{a \in K_2 \in \mathfrak{M}_1,\ b \in K_3 \in \mathfrak{M},\ K_2 \neq K_3}_{\neg(a \varphi b)}$

Получили противоречие, которое доказывает теорему.

Теорема 2. Если отношение φ на мн-ве M сопряжено с разбиением $\mathfrak{M}$, то это отношение $\tilde{\varphi}$

Док-во: $\forall a \in M$ $a \in K_i \to a \varphi a$ – рефлексивность

$a \varphi b \Rightarrow a, b \in K_i \to b, a \in K_i \to b \varphi a$ – симметричность

Пусть $a \varphi b$ и $b \varphi c \to a, b \in K_2$, $b, c \in K_2 \to a, c \in K_2 \to$

$\to a \varphi c$ – транзитивность

Теорема 3. Если некоторое отношение яв-ся отношением эквивалентности, то сущ-ет сопряженное с ним разбиение.

Док-во: возьмем $a \in M$, $a \tilde{\varphi} b$

K_a (яв-ся сечением a, все эл-ты из M, которые нах-ся в отношений $\tilde{\varphi}$ с a)

$K_a \subseteq M$, $M \setminus K_a \neq \varnothing \to \alpha$ K_α

Продолжаем до полного исчерпания M.

Мы построили разбиение

$\{K_a, K_\alpha, \dots, K_z\} = \mathfrak{M}$ – разбиение, сопряженное с нашим отн-ем эквивалентности

(11) Формальные (аксиоматические) теории. Разрешимость

Формальная (аксиоматическая) теория считается заданной, если:

1) Определен алфавит — набор символов, которыми оперирует система.

2) Все выражения, полученные с помощью символов пункта 1, делятся на 2 класса: формулы и не формулы.

Правильно построенная формула (ППФ):

а) Любой пропозициональный символ есть ППФ

б) Если A и B ППФ, то $\neg A$, $A \& B$, $A \vee B$, $A \to B$, $A \leftrightarrow B$ — тоже ППФ.

в) Других ППФ нет.

3) Из формул выделяют нек-е мн-во, из формул которого составляются аксиомы.

4) Мн-во $R_1, R_2 \dots R_n$, заданное на мн-во формул. Произв. отн-ю R_i ставится в соответствии одна формула $\mathfrak{N}_i$ (правило вывода)

Если сущ-ет любой (универсальный) алгоритм определения, является ли данная формула аксиомой или нет, то теория называется эффективно аксиоматизированной или аксиоматической.

Выводом наз-ся посл-ть формул $\mathfrak{N}_1, \mathfrak{N}_2, \dots \mathfrak{N}_n = \mathfrak{N}$, тогда последняя формула яв-ся:

$\Gamma \vdash \mathfrak{N}$ (выводима из Г)

$\mathfrak{N}_j$ — либо аксиома, либо выведена из предыдущих формул по одному из правил вывода.

Modus ponendo ponens	Если A влечет B и A, то B.
Modus tollendo tollens	Если A влечет B и не B, то не A
Modus tollendo ponens	Если A либо B и не A, то B
Modus ponendo tollens	Если неверно, что A и B, то не B.

Если для формальной теории сущ-ет общий способ определения, яв-ся ли оно теоремой или нет, то теория наз-ся разрешимой.

Примеры ~~ФТ~~ ФТ:

1) $\bullet$, $\rightarrow$, f, $a \div z$
2) Частный случай ППФ
3) $$\left.\begin{array}{l} - \; p \to (q \to p) \; - \text{ ЗУК} \\ - \; (s \to (p \to q)) \to ((s \to p) \to (s \to q)) \; - \text{ ЗСИ} \\ - \; ((p \to f) \to f) \to p \end{array}\right\} \text{схемы аксиом.}$$
4) – MP $\dfrac{p \to q,\ p}{q}$

(12) Натуральное исчисление.

1) (,), $\neg$, &, $\vee$, $\rightarrow$, $\leftrightarrow$, $A_i \div Z_j$ — набор символов
2) ППФ: $x_1 \rightarrow (x_2 \rightarrow (x_3 \rightarrow \ldots x_n \rightarrow y) \ldots))$
3) $\varnothing$ — нет аксиом
4) МР $\dfrac{x \rightarrow y,\ x}{y}$; УК $\dfrac{x \& y}{x}$, $\dfrac{x \& y}{y}$; ВК $\dfrac{x,\ y}{x \& y}$;

УД $\dfrac{x \rightarrow z,\ y \rightarrow z,\ x \vee y}{z}$; ВД $\dfrac{x}{x \vee y}$, $\dfrac{y}{x \vee y}$.

x_i — посылки n-кратной импликации.

Док-ва: — квазипрямой метод.
— косвенный метод.

Квазипрямой метод:
1) Гипотеза (x_i)
2) Ранее доказанная формула (РДФ)
3) лог. следствие по одному из 5 правил вывода.
~~4) Отрицание заключения.~~

Если получим y, то теорема доказана.

Косвенный метод: можем записать отрицание заключения $\neg y$. Если получится α и $\neg\alpha$ — противоречие, то оно доказывает, что $\neg y$ — неверное предположение.

СИЛ $\dfrac{(x \rightarrow y)(y \rightarrow z)}{x \rightarrow z}$ — закон условного силлогизма.

УЭ $\dfrac{x \leftrightarrow y}{x \rightarrow y}$, $\dfrac{x \leftrightarrow y}{y \rightarrow x}$ — удаление эквивалентности.

$MP_Э$ $\dfrac{x \leftrightarrow y,\ x}{y}$; $\dfrac{x \leftrightarrow y,\ y}{x}$

Док-во частями:

$$X_1 \to (X_2 \to \ldots \to (X_n \to y_1 \& y_2))\ldots)$$

<u>Ч1</u>. $X_1 \to (X_2 \to \ldots \to (X_n \to y_1))\ldots)$ <u>Ч2</u> $X_1 \to (X_2 \to \ldots \to (X_n \to y_2)\ldots)$

Разбор случаев:

$$X_1 \to (X_2 \to \ldots \to (y \vee z \to v)\ldots)$$

<u>C1</u>. $X_1 \to (X_2 \to \ldots \to (y \to v)\ldots)$ <u>C2</u>. $X_1 \to (X_2 \to \ldots \to (z \to v)\ldots)$

УО $\dfrac{\neg\neg X}{X}$, ВО $\dfrac{X \to \cancel{X},\ X \to \neg X}{\neg X}$; УОК $\dfrac{\neg(X \& y), X}{\neg y}$, $\dfrac{\neg(X \& y), y}{\neg X}$,

ВОК $\dfrac{\neg(X \vee y)}{\neg X}$, $\dfrac{\neg(X \vee y)}{\neg y}$; $M_{[t]}T$ $\dfrac{X \to y, \neg y}{\neg X}$

MTD $\dfrac{X \vee y, \neg X}{y}$, $\dfrac{X \vee y, \neg X}{X}$

Дилеммы:

ДИЛ1 $\dfrac{X \to y,\ X \to z,\ y \vee z}{X}$ — простая конструктивная дилемма

ДИЛ2 $\dfrac{X \to z,\ y \to w,\ z \vee w}{X \vee y}$ — сложная конструктивная дилемма

ДИЛ3 $\dfrac{X \to y,\ X \to z,\ \neg y \vee \neg z}{\neg X}$ — простая деструктивная дилемма

ДИЛ4 $\dfrac{X \to z,\ y \to w,\ \neg z \vee \neg w}{\neg X \vee \neg y}$ — сложная деструктивная дилемма.

(13) Непротиворечивость исчисления высказываний.

1) Теория наз-ся непротиворечивой отн-но преобр-я $A \to \bar{A}$, если A или $\bar{A}$ не яв-ся теоремой ФТ.

2) Если не всякая формула может быть теоремой, то теория абсолютно непротиворечива

3) Непротиворечивость в смысле Поста: Если пропозициональная перем-я не яв-ся теоремой ФТ, то ФТ непротиворечива в смысле Поста.

Теорема 5 ~~вс~~ Всякая теорема исчисления P_1 является тавтологией.

Док-во: возьмем исх. аксиомы. Т.к. они яв-ся тавтологиями, а правило вывода НР сохраняет тавтологию, то в рез-те мы получим новую тавтологию.

Теорема 6 Всякая тавтология яв-ся теоремой P_1 (т.е. существует и выводима)

Док-во: пусть дана $\mathfrak{A}$ $\mathfrak{A}' \leftrightharpoons (\mathfrak{A} \to f)$

а) Если $\mathfrak{A}$ - тавтология, то $\mathfrak{A}$ - противореч. >- но в P_1 такие ~~тавто~~ теоремы недоказуемы.

~~б)~~ Значит P_1 непротиворечива отн-но этого преобр-я!

б) f - не тавтология, значит P_1 - абсолютно непротивор.

в) A - не тавтология

(И) | Никакая пропозиц. ~~то~~ переменная не

(Л) | яв-ся теоремой — непротиворечива в смысле Поста.

(14) Полнота исчисления высказываний.

Пусть имеется ф-ла $\mathfrak{A}$:

- либо она доказана
- либо присоединяется в кач-ве аксиомы — тогда теория становится противоречивой.

1) Теория наз-ся полной отн-но преобразования ф-лы ($\mathfrak{A} \to \mathfrak{A}'$, если: а) $\vdash \mathfrak{A}$ ($\mathfrak{A}$ - есть теорема)
б) Присоед. этой ф-лы в кач-ве аксиомы превращает ФТ в противореч.

2) Теория наз-ся полной в абсолютном смысле, если: а) $\mathfrak{A}$ есть теорема
б) Присоед. этой ф-лы в кач-ве аксиомы превращает ФТ в противоречие в абсолютном смысле.

3) Теория полна в смысле Поста, если:
а) $\mathfrak{A}$ есть теорема.
б) Присоед. этой ф-лы в кач-ве аксиомы превращает ФТ в противоречие в смысле Поста.

Докажем, что P_1 полна во всех смыслах

P_1 $\mathfrak{A} \to \mathfrak{A} \to f$

Согласно Т5, всякая теорема - тавтология, а по Т6 всякая тавтология доказуема.

$\mathfrak{A}$ — не тавтолог. (т.к. нет док-ва)

$\mathfrak{A}$ - константа, $\mathfrak{A} = 1 \Rightarrow$

$\vdash \underbrace{\mathfrak{A} \to f, \mathfrak{A}}_{MP} \Rightarrow f$ - тавтология. Противореч. отн-но преобразование.

$f \to \mathfrak{A}$ - тавтология

по MP $\mathfrak{A}$ - теорема, что противоречит 2б.

$\neg\mathfrak{A} = f$ - тоже теорема (противореч. 3б) в смысле Поста

...ры.

...вная форма, которая после $\forall x P(x)$, $\exists x P(X)$ замены переменных становится ист. или лож.

...) - сущ. единств.

...сущ. бескон. много

..., $\exists x \exists y \mathfrak{A}(x,y) \Leftrightarrow \exists y \exists x \mathfrak{A}(x,y)$

...y) (обратное неверно)

...x, y).

— $\neg\exists x \mathfrak{A}(X) \equiv \forall x \neg\mathfrak{A}(X)$

(16) Область истинности предиката.

$\widehat{\mathfrak{A}}$ – область истинности $\mathfrak{A}$ ($\mathfrak{A}$ – выск. форма), множество всех тех наборов значений его переменных, для которых этот предикат превращается в истинное высказывание.

$\forall$	$\exists$
&	$\vee$

$\neg$	&	$\vee$	$\exists$
$-$	$\cap$	$\cup$	пр$_i$

$\widehat{\mathfrak{A} \,\&\, \mathfrak{B}} = \widehat{\mathfrak{A}} \cap \widehat{\mathfrak{B}}$; $\widehat{\mathfrak{A} \vee \mathfrak{B}} = \widehat{\mathfrak{A}} \cup \widehat{\mathfrak{B}}$

$\widehat{\exists x\, \mathfrak{A}(x,y)} = пр_2 \widehat{\mathfrak{A}}$

$\mathfrak{A}(x,y) \equiv 1 \iff \langle x, y \rangle \in \widehat{\mathfrak{A}}$

$\exists x\, \mathfrak{A}(x,y)$ $\quad \forall x\ \langle x, b \rangle \in \widehat{\mathfrak{A}}$

Терм: 1) любая предметная константа
2) любая пропозиц-ная или объектная перем-я
3) любой ф-ный символ от любого кол-ва перем-х

Формулы ЛП.

Ф-ла – нек-е осмысленное выражение. Она превращается в предикат после опред-я всех его предикатных, ф-ных и других символов.

Символы ИП:
1) (/) / , / $\neg$ / & / $\vee$ / $\rightarrow$ / $\leftrightarrow$ / $\forall$ / $\exists$.
2) x_i – переменные, a_i – константы
3) P_j^i – предикатные символы
4) f_j^i – ф-ные символы.

Предикат тесно связан с областью, на которой он задан. Говорят, что предикат задан на мн-ве М.

3 типа предиката:

- тождественно истинный (для всех наборов своих значений принимает знач-е истина $\overline{\mathfrak{A}} = M$)
- тождественно ложный $\overline{\mathfrak{A}} = \varnothing$
- выполнимый $\overline{\mathfrak{A}} \neq \varnothing \ \& \ \overline{\mathfrak{A}} \subset M$.

Две формулы $\mathfrak{A}$ и $\mathfrak{B}$ равносильны на М, если:

1) все их ~~ф~~ предикаты - ии-е отн-е на М;
2) эти ф-лы для всех значений из М становятся равносильными ~~при~~ после превращения в предикаты.

20. Приведенная форма ф-лы ЛП - равносильная ей ф-ла, но не содержащая операций →, и ¬ применено к простым ф-лам.

Теорема. Для любой ф-лы ~~ф~~ ЛП сущ-ет равносильная ей ф-ла в приведенной форме.

Предваренная нормальная форма - формула вида:

$\forall x_1, \forall x_2, \ldots \forall x_n \, \mathfrak{A}(\cdot)$, причем $\mathfrak{A}$ не содержит кванторов и находится в приведенной форме.

Теорема. $\forall$ ф-лы ЛП $\exists$ равносильная ей ф-ла в предваренной нормальной форме.

(17) Интерпретация.

~~Интерпретация~~ Способ замены одного отношения другим, при котором тождество 1-го варианта остается истинным для 2-го тождества наз-ся док-вом с пом-ю интерпретации.

Интерпретацией наз-ся пара <D, Г>, где D – мн-во „область интерпретации", Г – соответствие, которое:

1) каждой константе теории ставит в соотв-е эл-т из D.

2) каждому предикатному символу ставит в соотв-вие конкретное отн-е на мн-ве D P_j^i.

3) каждому ф-ному символу f_k^i ставит в соотв-е ф-ию $\Gamma: D^k \to D$

Формула наз-ся:

– выполнимой, если сущ-ет интерпретация, ~~в~~ хотя бы на одной посл-ти кот-й данная ф-ла выполнима

– логически общезначимой, если она истинна в любой инт-ии.

– противоречием ИП, если она ложна в любой инт-ии.

Св-ва выполнимости и истинности:

1) $\mathfrak{A}$ истинна т.т.т.к. $\neg\mathfrak{A}$ – ложно в данной инт-ии.

2) Никакая ф-ла не может быть И. вместе со своим отр-ем.

3) $\mathfrak{A} \to \mathfrak{B}$ – И, $\mathfrak{A}$ – И $\Rightarrow \mathfrak{B} \to$ И.

4) $\mathfrak{A} \to \mathfrak{B}$ – ложно т.т.т.к. $\mathfrak{A}$ – И

5) $\mathfrak{A}$ & $\mathfrak{B}$ – И, если $\mathfrak{A}$ – И и $\mathfrak{B}$ – И

$\mathfrak{A} \vee \mathfrak{B}$ –

$\mathfrak{A} \leftrightarrow \mathfrak{B}$, когда $\mathfrak{A}$ и $\mathfrak{B}$ одновр. или И, или Л.

$\exists x_i\, \mathfrak{A}(x_i)$ если найд. нек-я посл-ть, для кот. вып-ся ~~*~~, то вып-ся и это.

6) Пусть S и S' – 2 послед. одинаковые компоненты $b_i, b_{i+1} \dots b_r$, тогда $\mathcal{O}(x_i, x_{i+1} \dots x_r)$ выполнено на S т.т.т.к. она выполнена на S'

7) $\mathcal{O}(x)$ истинно в данной инт-ии т.т.т.к $\exists(\forall)\mathcal{O}(x)$ – И.

8) Частный случай тавтологии И в любой инт-ии.

9) Замкнутая ф-ла либо И, либо Л. в любой инт-ии.

18. Модель.

Пусть имеется некоторое мн-во формул Δ. Если каждая ф-ла истинна в данной интерпретации, тогда данная интерпретация наз-ся моделью.

(19.) Теорема Чёрча

Не сущ-ет конечного общего алгоритма, определяющего для любой предикатной ф-лы, является ли она логически общезначимой. Т.е. теория исчисления предикатов 1-го порядка неразрешима. (без док-ва)

(20.) Приведенная и предваренная нормальная форма. Теорема о них. (в предыдущей тетради)

(21.) Теории 1-го порядка.

1) Знач-ями перем. не могут быть предиката (только объектные значения)

2) Кванторы не могут навешиваться по предик-м.

1° Символы теории.

										const	перем	ф. симв	пред. симв.
,	(	)	$\neg$	&	$\vee$	$\rightarrow$	$\leftrightarrow$	$\exists$	$\forall$	a_i	x_i	f_i^k	P_j^r

2° Формулами теории 1-го порядка яв-ся формулы ЛП.

3° а) Логические аксиомы, принад. любой т. 1-го пор-ка.

A1. ЗУК $\mathfrak{A}(\cdot) \rightarrow (\mathfrak{B}(\cdot) \rightarrow \mathfrak{A}(\cdot))$

A2. ЗСД $(\mathfrak{A}(\cdot) \rightarrow (\mathfrak{B}(\cdot) \rightarrow \mathfrak{C}(\cdot))) \rightarrow ((\mathfrak{A} \rightarrow \mathfrak{B}) \rightarrow (\mathfrak{A} \rightarrow \mathfrak{C}))$

A3. $(\neg\mathfrak{A}(\cdot) \rightarrow \neg\mathfrak{B}(\cdot)) \rightarrow ((\neg\mathfrak{A} \rightarrow \mathfrak{B}) \rightarrow \mathfrak{A})$

A4. $\forall x\, \mathfrak{A}(x) \rightarrow \mathfrak{A}(t)$ t - своб. для всех x в $\mathfrak{A}$

A5. $\forall x(\mathfrak{A} \rightarrow \mathfrak{B}(x)) \rightarrow (\mathfrak{A} \rightarrow \forall x\, \mathfrak{B}(x))$

Терм t своб. для нек-х перем-х в нек-й ф-ле, если никакие своб. вхожд-я перем-х в этой ф-ле не нах-ся в области действия никакого квантора, навешенного по перем. из t

б) Собственные аксиомы.

4° Правило вывода. MP пр-ло обобщения Gen $\dfrac{\mathfrak{A}(x)}{\forall x\, \mathfrak{A}(x)}$

Если теория 1-го порядка м. имеет собств. аксиом, то она наз-ся ИП 1-го порядка.

Св-во теорий 1-го порядка:

<u>Теорема</u> Пусть $\mathfrak{A}$ - формула, являющаяся частным случаем. Тогда сущ-ет вывод в ИП этой формулы, причем только с исп-ем аксиом 1, 2, 3 и правила MP.

<u>Док-во</u>: пусть в тавтологии были произведены замены пропозициональных символов на какие-то ф-лы, но при этом возможно существование пропозициональные символы ω_i, кот-е не представлены в ф-ле $\mathfrak{A}$, а представлены в выводе.

U_i - присутствуют в $\mathfrak{A}$

u_i - не присутствуют в $\mathfrak{A}$

каждое ω_i можем заменить любой формулой.

(22) Теоремы редукции.

Теорема редукции ИВ.

Пусть ф-ла $\mathfrak{M}$ выводима из совокупности Γ и $\{\mathfrak{A}\}$. Тогда сущ-ет вывод из Γ ф-лы $\mathfrak{A} \to \mathfrak{M}$. ($\Gamma$ - мн-во нек-х РДФ)

$\Gamma \cup \{\mathfrak{A}\} \vdash \mathfrak{M} \to \Gamma \vdash \mathfrak{A} \to \mathfrak{M}$

Док-во: $\exists\ \mathfrak{M}_1, \mathfrak{M}_2, \dots, \mathfrak{M}_n \equiv \mathfrak{M}$ - вывод из Γ и $\{\mathfrak{A}\}$. $1 \le i \le n$

Пусть $i = 1$. Возможны 3 случая.

1) $\mathfrak{M}_1$ - аксиома. Тогда рассм. вывод:
1. $\mathfrak{M}_1$
2. $\mathfrak{M}_1 \to (\mathfrak{A} \to \mathfrak{M}_1)$
3. $\mathfrak{A} \to \mathfrak{M}_1$ МР 2,1.

2) Пусть $\mathfrak{M}_1 \in \Gamma$, тогда док-во аналогично п. 1.

3) Пусть $\mathfrak{M}_1 \in \mathfrak{A}$. Тогда $\vdash_y \mathfrak{M}_1 \to \mathfrak{M}_1 \Rightarrow \vdash_y \mathfrak{A} \to \mathfrak{M}_1$.

Т.о., $\Gamma \vdash \mathfrak{A} \to \mathfrak{M}_1$.

Пусть $i < k$. Рассмотрим вывод $\mathfrak{M}_k$. Возможны 4 случая.

1) $\mathfrak{M}_k$ - аксиома
2) $\mathfrak{M}_k \in \Gamma$
3) $\mathfrak{M}_k \in \mathfrak{A}$
4) $\mathfrak{M}_k$ получено из $\mathfrak{M}_i$ и $\mathfrak{M}_j$ по МР, причем $i, j < k$, и $\mathfrak{M}_i = \mathfrak{M}_j \to \mathfrak{M}_k$

Для п. 1,2,3 док-во аналогично док-ву при $i = 1$.

Для пункта 4:

1) $\Gamma \vdash \mathfrak{A} \to \mathfrak{M}_i$ $\quad \mathfrak{M}_j$
2) $\Gamma \vdash \mathfrak{A} \to (\mathfrak{M}_i \to \mathfrak{M}_k)$
3) $(\mathfrak{A} \to (\mathfrak{M}_i \to \mathfrak{M}_k)) \to ((\mathfrak{A} \to \mathfrak{M}_i) \to (\mathfrak{A} \to \mathfrak{M}_k))$
4) $(\mathfrak{A} \to \mathfrak{M}_i) \to (\mathfrak{A} \to \mathfrak{M}_k)$ по МР 3,2.
5) $\mathfrak{A} \to \mathfrak{M}_k$ по МР 4,1

Т.о., для любого k, в т.ч. для $k = n$ $\Gamma \vdash \mathfrak{A} \to \mathfrak{M}_k$.

#

Теорема редукции ИП.

Пусть $\Gamma \cup \{\mathfrak{A}\} \vdash \mathfrak{M}$. Тогда, если правило обобщения не применялось ни к одной формуле, зависящей от $\mathfrak{A}$ по своб. переменной в ф-ле $\mathfrak{A}$, тогда $\Gamma \vdash \mathfrak{A} \to \mathfrak{M}$.

Док-во: $\mathfrak{M}_1, \mathfrak{M}_2 \dots \mathfrak{M}_n = \mathfrak{M}$ - базис, вывод из Γ
$1 \le i \le n$. Пусть $i = 1$, тогда для $\mathfrak{M}_1$ возм. 3 случая:

$$\left.\begin{array}{l} 1)\ \mathfrak{M}_1 \in \Gamma \\ 2)\ \mathfrak{M}_1 \text{ аксиома} \\ 3)\ \mathfrak{M}_1 \in \mathfrak{A} \end{array}\right\} \text{док-во аналогично док-ву для } \mathfrak{M}_1 \text{ из Т.Д.ИВ.}$$

Для $\mathfrak{M}_k$ возможна 5 случаев:

1) $\mathfrak{M}_k \in \Gamma$; 2) $\mathfrak{M}_k$ - аксиома; 3) $\mathfrak{M}_k \in \mathfrak{A}$ } док-во аналог.
4) $\mathfrak{M}_k$ получена из $\mathfrak{M}_i$ и $\mathfrak{M}_j$ с пом. MP (аналог. 4п. ТДИВ)
5) $\mathfrak{M}_k$ получена из $\mathfrak{M}_i$ и $\mathfrak{M}_j$ с пом-ю Gen

Если правило обобщения применяется по какой-то ф-ле $\mathfrak{M}_i$.

а) $\mathfrak{M}_i$ не зависит от $\mathfrak{A}$

$\Gamma, \mathfrak{A} \vdash \mathfrak{M}_i \Rightarrow \Gamma \vdash \mathfrak{M}_i$ (•)

(Gen) $\forall x\, \mathfrak{M}_i(x)$ $\quad \forall x\, \mathfrak{M}_i(x) \to (\mathfrak{A} \to \forall x\, \mathfrak{M}_i(x))$

$\Gamma \vdash (\mathfrak{A} \to \forall x\, \mathfrak{M}_i(x))$

б) $\mathfrak{M}_i$ зависит от $\mathfrak{A}$.

$\vdash \mathfrak{A} \to \mathfrak{M}_i$, $\underset{\text{Gen}}{\forall y\, (\mathfrak{A} \to \mathfrak{M}_i)}$ ($\mathfrak{A}$ не зависит от y)

$\forall y\, (\mathfrak{A} \to \mathfrak{M}_i(y)) \to (\mathfrak{A} \to \forall y\, \mathfrak{M}_i(y))$ А5.

$\mathfrak{A} \to \mathfrak{M}_i$ MP

(23) Теорема Гёделя о полноте.

Лемма 1 ИП. Пусть K – теория 1-го порядка, кот-я не позволяет вывести для нек-ой замкнутой формулы $\mathfrak{A}$ отрицание. Тогда теория K_1, полученная из K путем добавления к ней $\mathfrak{A}$, будет непротиворечива отн-но преобр-я формул $\mathfrak{A} \to \neg\mathfrak{A}$.

Док-во: от противного. Пусть K_1 противоречива, и в ней выводимы как $\mathfrak{B}$, так и $\neg\mathfrak{B}$.

Частный случай тавтологии:

$\vdash_{K_1} \mathfrak{B} \to (\neg\mathfrak{B} \to \neg\mathfrak{A})$

$\Gamma, \mathfrak{A} \vdash_{K_1} \neg\mathfrak{A} \overset{TD}{\Longrightarrow} \Gamma \vdash_{K_1} \mathfrak{A} \to \neg\mathfrak{A}$

$\vdash (\mathfrak{A} \to \neg\mathfrak{A}) \to \neg\mathfrak{A} \Rightarrow \vdash_K \neg\mathfrak{A}$ – противоречие с усл. леммы #

Лемма 2 ИП. Все логические аксиомы ИП яв-ся логически общезначимыми.

Док-во: $A1, A2, A3$ – тавтологии.

$A4: \forall x \mathfrak{A}(x) \to \mathfrak{A}(t)$ t-терм, ~~сво~~ свободен для x в ф-ле $\mathfrak{A}$

Истинна для любой интерпретации.

$A5: \underbrace{\forall x(\mathfrak{A} \to \mathfrak{B}(x))} \to (\mathfrak{A} \to \forall x \mathfrak{B}(x))$ – нет своб. вхождений.

$\mathfrak{B} \to$ а) лог. общезн – все ф-ла лог. общезн.

б) не лог. общезн.

Лемма 3 ИП. Правила MP и Gen сохраняют логическую общезначимость.

Док-во: 1) MP : $\dfrac{\mathfrak{A} \to \mathfrak{B}, \mathfrak{A}}{\mathfrak{B}}$

2) Gen : $\mathfrak{A}(x)$ – логич. общезн. ф-ла в любой инт-ии $\Rightarrow \forall x \mathfrak{A}(x)$ – истина

Из лемм 2 и 3 следует:

Теорема 13. Всякая теорема ИП лог. общезначима

Теорема 14. Всякая логически общезначимая ф-ла яв-ся теоремой.

(24) Формальная арифметика.

ФА - теория 1-го порядка со следующими собственными аксиомами и алфавитом:

1) В алфавите одна константа: 0.

одни предикатный символ: P_1^2 ~ "=" $P(x,y) \rightsquigarrow x=y$

три функцион-х символа: $f_1^1(x) \rightsquigarrow$ ' (след. по пор-ку)

$f_1^2(x,y) \rightsquigarrow x+y$

$f_2^2(x,y) \rightsquigarrow x \cdot y$

2) Формулы ЛП те же.

3) а) логические аксиомы (те же, что и в теор. 1-го пор-ка)

б) Собственные аксиомы.

S1. $x_1 = x_2 \to (x_1 = x_3 \to x_2 = x_3)$

S2. $x_1 = x_2 \to x_1' = x_2'$

S3. $0 \neq x$

S4. $x_1' = x_2' \to x_1 = x_2$

S5. $x + 0 = x$

S6. $x + y' = (x+y)'$

$\}$ рекурсивное задание сложения.

S7. $x \cdot 0 = 0$

S8. $x \cdot y' = x \cdot y + x$

$\}$ задание умножения

S9. $\mathfrak{A}(0) \to (\forall x(\mathfrak{A}(x) \to \mathfrak{A}(x')) \to \forall x\, \mathfrak{A}(x))$

Теорема 15.

$\forall t, r, s$ теоремами яв-ся след. формулы:

а) $t = t$ // рефлексивность

б) $t = r \to r = t$ // симметричность

в) $t = r \to (r = s \to t = s)$ // транзитивность.

Док-во:

а) 1. $t+0 = t \to (t+0 = t \to t = t)$ S_1^1

2. $t+0 = t$ $S5^1$

3. $t+0 = t \to t = t$ MP 1,2

4. $t = t$ MP 3,2

б) 1. $t=r \to (t=t \to r=t)$ S_1^1

2. $\vdash (A \to (B \to C)) \to (B \to (A \to C))$ тавтология

3. $(t=r \to (t=t \to r=t)) \to (t=t \to ((t=r) \to (r=t)))$ подстан. в 2.

4. $t=t \to ((t=r) \to (r=t))$ MP 3,1.

5. $t=t$ согласно а)

6. $t=r \to r=t$ MP 4,5.

в) 1. $r=t \to (r=s \to t=s)$ S_1^1

2. $\vdash t=r \to r=t$ согласно б)

3. $\vdash (D \to A) \to ((A \to (B \to C)) \to (D \to (B \to C)))$ тавтология

4. $(t=r \to r=t) \to ((r=t \to (r=s \to t=s)) \to (t=r \to (r=s \to t=s)))$ подстан. в 3.

5. $(r=t \to (r=s \to t=s)) \to (t=r \to (r=s \to t=s))$ MP 4,2.

6. $t=r \to (r=s \to t=s)$ MP 5,1.

(25) Нестандартная модель арифметики.

Моделью наз-ся интерпретация, в которой истинны все аксиомы теории.

Изоморфизм интерпретаций:

~~Интерпретации ~~наз-ся~~ M и M' наз-ся изоморфными, если сущ-ет такое отображение D из инт-ии M на D' из инт-ии M', $g: D \to D'$ такое, что~~

Пусть даны 2 инт-ии $\langle D', P' \rangle$, $\langle D^*, P^* \rangle$. говорят, что они изоморфны, если сущ-ет биекция

$g: D' \to D^*$ такая, что

$a_i^* = g(a_i')$

$(P_e^k)'(b_1 \dots b_k) \equiv (P_e^k)^*(g(b_1) \dots g(b_k))$

$g((f_e^n)'(b_1 \dots b_n)) = (f_e^n)^*(g(b_1) \dots g(b_n))$

Стандартная модель арифметики – инт-я в которой симв. „0" проинт-н как число 0,

$x' \rightsquigarrow N(x)$ // next, $x+y \rightsquigarrow$ сложение x и y

$x \cdot y \rightsquigarrow$ умножение x и y

$= \rightsquigarrow I_D$ тождества

Нормальная модель ФА, неизоморфная стандартной, наз-ся нестандартной моделью.

26) Примитивно-рекурсивные функции и предикаты

Есть 3 исходных функции:

$Z(x) = 0$

$N(x) = x' = x + 1.$

$U_i^n (x_1 \dots x_n)$

Есть два способа получения новых функций

1) Подстановка

$h(x_1 \dots x_n) = \rho(f_1(x_1 \dots x_n), \dots, f_k(x_1 \dots x_n))$

2) рекурсия

$f(0) = k$

$f(y+1) = h(y, f(y))$

$f(x_1 \dots x_n, 0) = \rho(x_1 \dots x_n)$

$f(x_1, \dots x_n, y+1) = h(x_1, \dots x_n, f(x_1 \dots x_n, y))$

Если некоторая ф-ия получена из исходных путем конечного числа операций подстановки и рекурсии, то она называется примитивно-рекурсивной.

Есть еще один способ получения новых ф-ий.

3) μ-оператор

$$\mu y_{y<z} R(\bullet) = \begin{cases} \mu y R(\bullet), & \exists y < z \; R(x_1 \dots x_n, y) \equiv И \\ z \end{cases}$$

$\mu y R(x_1 \dots x_n, y)$ – это выражение обозначает, что ~~...~~ y равно такому значению, что данный предикат истинный, и это значение y наименьшее из тех, при которых он истинен.

Всякая ф-ия, полученная из исходных путем конечного числа операций подстановки, рекурсии и μ-оператора, наз-ся рекурсивной.

Предикат наз-ся примитивно-рекурсивным (рекурсивным), если его характер-кая ф-ия представима как прим.-рек. (рек.)

(27) Общие свойства алгоритмов.

Алгоритм – предписание, которое однозначно определяет протекание или выполнение некоторого конструктивного процесса, приводящего к какому-либо результату, который заранее неизвестен.

Общие свойства алгоритмов.

1) Детерминированность (однозначность)
2) Массовость
3) Направленность (результативность)
4) Область применимости.

(28) Вербальные переменные, предикаты и алгоритмы

Вербальная переменная – перем-я, значениями которой яв-ся различные слова в нек-м алфавите. Алфавит – нек-е слово, подразумевающее мн-во символов алфавита. Любой символ алфавита наз-ся литерой.

Если алфавит состоит из единственного символа „|", то все вербальные перем-е наз-ся натуральными.

В отличие от теорий I-го порядка, в НАМ допустимы предикатные переменные, но ими могут объявляться только свободные переменные, а сами предикаты, которые образовываются вербальными.

Вербальный алгоритм (алгорифм) – алгоритм, работающий со словами.

(29) Взаимно простые слова.

P и Q наз-се взаимнопростыми словами относительно начала, если за исключением пустого слова у них нет общих начал.

Теорема:

$\forall P \forall Q \exists S \exists R \exists T : [P \stackrel{\circ}{=} RS \,\&\, Q \stackrel{\circ}{=} RT \,\&\, [S$ и T - взаимно-простые$]]$

(30) Схема.

$\int$ - система, члены которой только ф-лы подстановок, наз-се схемой и эл-т этой схемы действует на нек-е слово, если ядро действует на это слово.

Активный эл-т - тот, который действует на слово и ему не предшествует эл-т, действующий на это слово. Тогда рез-том действие схемы на слово наз-се рез-т действие на слово ее активного эл-та.

Схема Σ переводит слово P в слово Q ($\Sigma : P \vdash Q$), если Q есть рез-тат действие схемы Σ на слово P.

$\Sigma : P \vdash Q$ просто переводит

$\Sigma : P \vdash \cdot$ заключительно переводит

$\Sigma : P \urcorner$ не действует на P.

(31) Переводная система.

Это $\int$-система вида:

$\int P \int \ldots \int Q \int$, где P и $Q \in A$ (A-алфавит)

Эта система соединяет слово P со словом Q.

Пусть $Z: P \models Q$ (преобразует) за n шагов, если сущ-ет переводная система схемы Z, соединяющая слово P и Q и имеющая объем $n+1$ ($[X^\circ \overset{\circ}{=} N1]$)

Будем говорить, что $Z: P \models Q$? (естественно преобразует) слово P в Q за N шагов, и Z такая, что схема не действует на слово Q

? $Z: P \models \cdot Q$ (заключительно преобразует) P в Q за n шагов, если сущ-ет единственное слово R, такое, что R: $Z: P \models R$ & $R \vdash \cdot Q$?

$(Z:P)$ - число шагов, за которые схема Z перерабатывает слово P.

(32) Тезис Черча и принцип нормализации.

Алгорифмы $\mathfrak{A}$ и $\mathfrak{N}$ эквивалентны отн-но алфавита $Б$, если выполнено:

$\mathfrak{A}(P) \overset{\circ}{=} Q \leftrightarrow \mathfrak{N}(P) \overset{\circ}{=} Q$, где P и Q - слово из $Б$.

$\mathfrak{A}$ и $\mathfrak{N}$ наз-ся вполне эквивалентными, если ~~выполнено~~ они эквивалентны отн-но $Б$ и выполнено:

$\forall Q \in \mathfrak{A}$ и $\forall Q \in \mathfrak{N}$ $\mathfrak{A}(P) \overset{\circ}{=} Q \leftrightarrow \mathfrak{N}(P) \overset{\circ}{=} Q$

<u>Принцип нормализации</u>: любой НА может быть заменен вполне эквивалентным ему НА. Говорят, что алгорифм нормализуем.

<u>Тезис Черча</u>: всякая эффективно-вычислимая ф-ия эквивалентна нек-ой Я-определимой ф-ии.

33. Нормальные алгорифмы, применимость, замкнутость, композиция.

Нормальный алгорифм определяется:

1) Алфавитом, в котором он работает (A)

2) 3-мя спец. символами: $\alpha \sim \rightarrow$

которые не принадлежат $\beta \sim \rightarrow \cdot$

алфавиту. $\gamma \sim$ CR (возврат каретки и перевод строки)

3) Схемой, которая работает над словами. (Z) -

$\delta A \delta \alpha \beta \gamma \delta Z \delta \sim \mathfrak{A}$

Будем говорить, что алгорифм применим к слову P, если за конечное число шагов он перерабатывает слово P в слово Q и останавливается. Q - рез-т работы алгорифма $\mathfrak{A}$.

Любой сокращающий ~~норм~~ НА применим к любому слову и перерабатывает его за кол-во шагов, не превышающее длину этого слова.

НА не применим ни ~~ко~~ к какому слову, если в словах нету символов, принадлежащих алфавиту алгоритма.

НА наз-ся замкнутым, если в схеме имеется подстановка с пустой левой частью. Такой НА действует на любое слово. Естественного завершения у такого НА быть не может.

Композиция НАМ. $\mathfrak{A}(P) \circ \mathfrak{B}(Q) = \mathfrak{B}(\mathfrak{A}(P))$

Для любых нормальных алгорифмов $\mathfrak{A}$ и $\mathfrak{B}$ сущ-ет такой алгорифм $\mathfrak{C}$ над объед. алфавитами $\mathfrak{A}$ и $\mathfrak{B}$, что $\mathfrak{C}(P) \simeq \mathfrak{B}(\mathfrak{A}(P))$, где P - слово в объед. алфавите.

34. Естественная сложность НА, число шагов.

Естественная сложность НА – число формул подстановки. $|A| = n$ (длина схемы)

$(\mathfrak{Z} : P)$ – число шагов, за которое схема $\mathfrak{Z}$ перерабатывает слово P.

35. Арифметические алгоритмы

Это частный случай вербального алгоритма – алгоритм над алфавитом, содержащим единственный символ „1"

Число шагов – $\min(x, y)$

Пример Алгоритм Евклида (поиск НОД)

$$\begin{cases} 1*1 \to \alpha * \\ 1\alpha \to \alpha 1 \\ 1* \to *\beta \\ \beta \to 1 \\ \alpha \to \gamma \\ \gamma \to 1 \\ *1 \to \cdot 1 \end{cases}$$

36 Понятие о массовой алгоритмической проблеме.

Нормальная массовая проблема — построить НА над алфавитом, содержащим все возможные символы входных наборов единичных задач, применимых к любому входному набору, и перерабатывающий его в пустое слово т.т.т.к эта единичная задача разрешима в положительном смысле.

Теорема (о неразрешимости задачи применимости НА)

НА $\mathfrak{M}$ может быть построен в алфавите $\{a, b\}$, такой, что $\nexists$ НА (над тем же алфавитом), перерабатывающего любое слово в этом алфавите в пустое слово т.т.т.к $\mathfrak{M}$ применим к этому слову.

37. Классы задач.

Функция $f(n)$ не превосходит по порядку ф-ию $g(n)$, если сущ-ет такая const C, что для любых натур. чисел $f(n) \le C \cdot g(n)$

Класс P — массовые задачи эффективно-разрешимы, с алгоритмы имеют полиномиальную оценку сложности. $O(n^c)$

увеличение сложности

- $O(n)$ - линейная сложность (проще всего)
- $O(n \log_2 n)$
- $O(n\sqrt{n})$
- $O(n^2)$
- $O(n^3)$

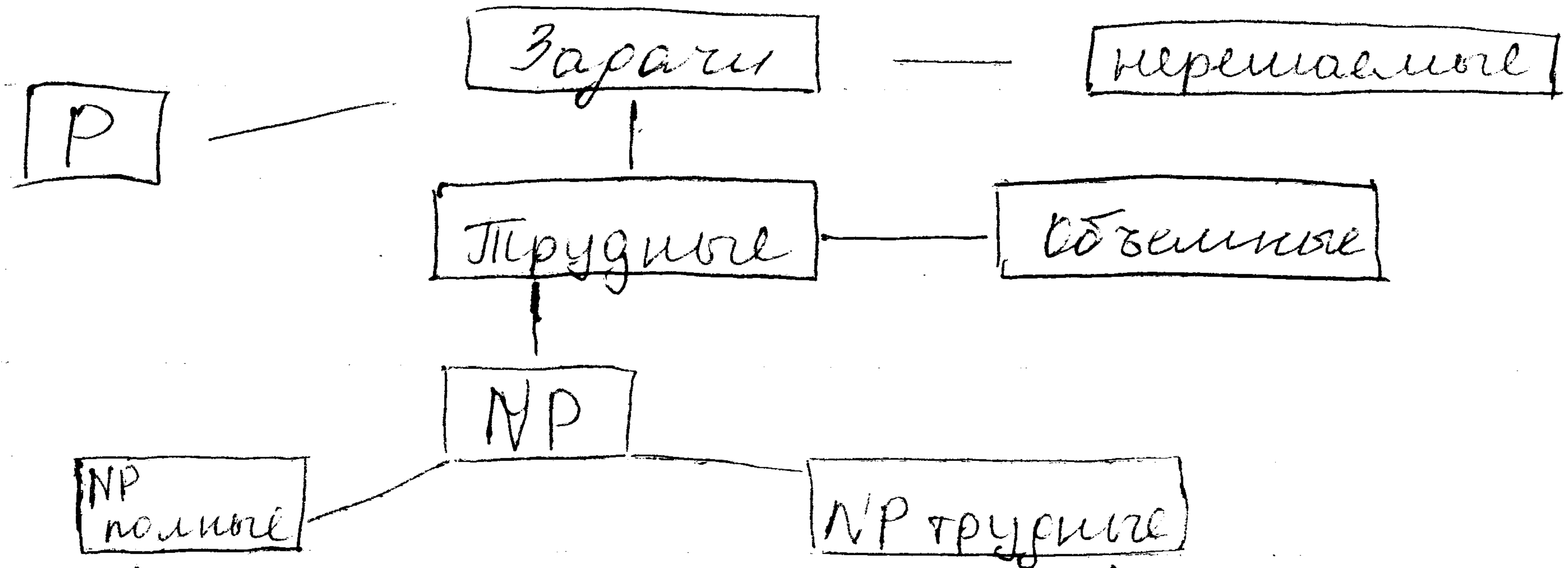
Задачи распознавания NP. Недетерминированный алгоритм.

$\{A_1, A_2 \dots A_m\}$ - набор алгоритмов.

$a = \underbrace{\langle q_1, q_2 \dots q_k \rangle}_{\text{„Оракул"}}$ - ключ, где $a \in \{e_1, e_2\}^k$

A_a - детермин. + полиномиальный.

Если нет „Оракула", то алгоритм недетерминированный экспоненциальный.



класс задач, кот-е друг к другу сводятся

можно найти NP-полную, кот-я сводится к NP-трудной.