

# Коллоквиум по дискретной математике 2

Ми (@technothecow)

## Содержание

<b>1</b>	<b>Логика и машины Тьюринга</b>	<b>3</b>
1.1	Структуры и сигнатуры. Нормальные структуры. Изоморфизм структур.	3
1.2	Формулы первого порядка данной сигнатуры. Параметры (свободные переменные) формулы. Предложения.	3
1.3	Оценка переменных. Значение терма и формулы в данной структуре при данной оценке. Независимость значения формулы от значений переменных, не являющихся ее параметрами.	3
1.4	Значение терма и формулы на наборе элементов структуры. Выразимые в структуре множества (отношения, функции, элементы). Примеры выразимых множеств.	4
1.5	Значение формулы при изоморфизме структур. Элементарная эквивалентность структур. Изоморфные структуры элементарно эквивалентны.	5
1.6	Значение формулы при изоморфизме структур. Сохранение выразимых множеств автоморфизмами структуры. Примеры невыразимых множеств.	5
1.7	Эквивалентность формул первого порядка. Лемма о фиктивном кванторе. Общезначимые и выполнимые формулы. Квантор всеобщности и общезначимость.	5
1.8	Основные эквивалентности логики первого порядка. Замена подформулы на эквивалентную.	6
1.9	Пропозициональные формулы и задаваемые ими булевы функции. Тавтологии первого порядка.	6
1.10	Лемма о корректной подстановке.	6
1.11	Понятие корректной подстановки («терм свободен для переменной в формуле»). Пример некорректной подстановки. Лемма о корректной подстановке (без доказательства). Переименование связанной переменной. Общезначимость формул вида $\forall x\varphi \rightarrow \varphi(t/x)$ и $\varphi(t/x) \rightarrow \exists x\varphi$ в случае корректной подстановки.	7
1.12	Переименование связанной переменной (без доказательства). Теорема о предваренной нормальной форме.]	7
1.13	Понятие теории первого порядка. Примеры содержательных теорий. Модель теории. Логическое (семантическое) следование (для теорий и предложений).	7
1.14	Исчисление предикатов с равенством (в гильбертовской форме). Теорема о полноте и корректности исчисления предикатов (без доказательства). Теорема о компактности в двух формах: про выполнимость теории и про логическое следование из теории.	8
1.15	Теорема компактности (без доказательства). Любой пример применения.	8
1.16	Одноленточная машина Тьюринга (допустимо неформальное определение с лентой и головкой). Сложение натуральных чисел (при унарном и бинарном кодировании).	9
1.17	Многоленточная машина Тьюринга (допустимо неформальное определение с лентами и головками). Удвоение входного слова за линейное время.	9
1.18	Конфигурации одноленточной и многоленточной машин Тьюринга. Меры сложности «время» и «зона» и их соотношение в обоих случаях.	9
1.19	Сокращение ленточного алфавита и его цена.	9
1.20	Сокращение числа лент и его цена.	9
<b>2</b>	<b>Вычислимость</b>	<b>10</b>
2.1	Вычислимые функции (при интуитивном понимании алгоритма). Разрешимые и перечислимые множества. Связь конечности, разрешимости и перечислимости. Разрешимые множества под действием операций алгебры множеств и декартова произведения.	10
2.2	Перечислимые множества под действием операций алгебры множеств, декартова произведения и проекции. Теорема Поста.	10
2.3	Теорема о графике вычислимой функции. Перечислимость образа и прообраза множества под действием вычислимой функции.	10
2.4	Непустые перечислимые множества суть, в точности, области значений вычислимых тотальных функций.	11
2.5	Полуразрешимость. Перечислимые множества суть, в точности, области определения вычислимых функций.	11

2.6	Перечислимые множества суть, в точности, проекции разрешимых. Теорема о свойствах, равносильных перечислимости (доказательство на основе утверждений предшествующих вопросов). . . . .	11
2.7	Универсальная вычислимая функция (в классе вычислимых функций $\mathbb{N} \xrightarrow{p} \mathbb{N}$ ). Т-Предикаты. Неразрешимость проблем самоприменимости и остановки. . . . .	11
2.8	Неразрешимость проблем самоприменимости и остановки. Примеры перечислимого неразрешимого и неперечислимого множеств. . . . .	12
2.9	Пример вычислимой функции, не имеющей вычислимого тотального продолжения. Область определения вычислимой функции, не имеющей вычислимого тотального продолжения, перечислима, но не разрешима. . . . .	12
2.10	Невозможность универсальной вычислимой тотальной функции. . . . .	12
2.11	Пример непересекающихся перечислимых множеств, не отделимых никаким разрешимым множеством. . . . .	13
2.12	Главная универсальная вычислимая функция. Вычислимое биективное кодирование пар натуральных чисел. Построение главной у.в.ф. с помощью произвольной у.в.ф. . . . .	13
2.13	Теорема Клини о неподвижной точке . . . . .	13
2.14	Бесконечность множества неподвижных точек в смысле теоремы Клини. Теорема о рекурсии как следствие теоремы Клини. Пример применения теоремы о рекурсии. . . . .	14
2.15	Вычислимость индекса композиции вычислимых функций. Совместная рекурсия: решение «систем уравнений» (с тотальными правыми частями). . . . .	14
2.16	Индексные множества. Теорема Райса-Успенского: вывод из теоремы Клини. Пример применения. . . . .	15
2.17	Существование неглавной у. в. ф. . . . .	15
2.18	$m$ -сводимость и её простейшие свойства . . . . .	15
2.19	Индексные множества. Теорема Райса-Успенского: доказательство с помощью сведения. Пример применения. . . . .	16
2.20	Пример неперечислимого множества с неперечислимым дополнением. . . . .	16
2.21	Теорема Райса-Шапиро. Неперечислимость индексов одной функции относительно г. у. в. ф. . . . .	16
2.22	Классы $\Sigma_n$ и $\Pi_n$ арифметической иерархии и их простейшие свойства. . . . .	16
2.23	Классы $\Sigma_n$ и $\Pi_n$ арифметической иерархии. Включение $\Sigma_n$ и $\Pi_n$ ( $\Sigma_{n+1} \cap \Pi_{n+1}$ при $n > 0$ (без доказательства строгости). . . . .	16

# 1 Логика и машины Тьюринга

## 1.1 Структуры и сигнатуры. Нормальные структуры. Изоморфизм структур.

Структура – кортеж множеств  $(M, \mathcal{F}, \mathcal{R}, \mathcal{C})$ , где

1.  $M$  – непустое множество, *носитель структуры*
2.  $\mathcal{F}$  – множество функций вида  $f: M^n \rightarrow M$
3.  $\mathcal{R}$  – множество кортежей из  $M$
4.  $\mathcal{C}$  – подмножество  $M$

Сигнатура – кортеж попарно непересекающихся множеств  $(Fnc, Prd, Cnst)$ , где  $Fnc$  – множество функциональных символов с заданной валентностью,  $Prd$  – непустое множество предикатных символов с заданной валентностью и  $Cnst$  – множество константных символов. (просто набор символов)

\* $\sigma$ -структура (или интерпретация сигнатуры  $\sigma$ ) – это формально кортеж  $\mathcal{M} = (M, \mathcal{F}, \mathcal{R}, \mathcal{C}, \mathcal{I})$ , где  $\mathcal{I}(Fnc) = \mathcal{F}$ ,  $\mathcal{I}(Prd) = \mathcal{R}$  и  $\mathcal{I}(Cnst) = \mathcal{C}$ . Вводим обозначения:  $\mathcal{I}(Fnc) = f^{\mathcal{M}}$ ,  $\mathcal{I}(Prd) = R^{\mathcal{M}}$  и  $\mathcal{I}(Cnst) = c^{\mathcal{M}}$ . Для задания  $\sigma$ -структуры достаточно только  $M$  и  $\mathcal{I}$ . Фактически, мы придаем значение имеющимся значкам из сигнатуры  $\sigma$ : берем носитель и говорим, что делают с ним функции и что делают с ним предикаты.

Нормальная структура – содержащая двувалентный предикатный символ “=” :=  $\{(a, a) \in M^2 \mid a \in M\}$ , где  $M$  – носитель структуры.

Изоморфизм структур: интерпретации  $\mathcal{M}$  и  $\mathcal{N}$  сигнатуры  $\sigma$  с носителями  $M$  и  $N$  соответственно изоморфны если существует биекция  $\eta: M \rightarrow N$  для которой выполняются следующие свойства:

1.  $\eta(f^{\mathcal{M}}(a_1, \dots, a_n)) = f^{\mathcal{N}}(\eta(a_1), \dots, \eta(a_n))$
2.  $(a_1, \dots, a_n) \in R^{\mathcal{M}} \iff (\eta(a_1), \dots, \eta(a_n)) \in R^{\mathcal{N}}$
3.  $\eta(c^{\mathcal{M}}) = c^{\mathcal{N}}$ , где  $c$  – один символ

## 1.2 Формулы первого порядка данной сигнатуры. Параметры (свободные переменные) формулы. Предложения.

Формулы первого порядка – это выражения в логике первого порядка (предикатной логике), построенные по правилам синтаксиса, установленным для данной сигнатуры.

Формулы первого порядка строятся из термов и предикатов, используя логические связки и кванторы. Основные элементы синтаксиса формул первого порядка:

1. Термы: 1) переменные; 2) константы; 3) если  $t_1, \dots, t_n$  – термы, а  $f$  – функция с валентностью  $n$ , то  $f(t_1, \dots, t_n)$  – тоже терм
2. Атомарные формулы: предикаты, примененные к термам.
3. Сложные формулы: атомарные формулы, соединенные логическими операциями ( $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ ) и кванторами ( $\forall, \exists$ ).

Свободные переменные формулы – это переменные, которые не находятся под действием кванторов ( $\forall$  или  $\exists$ ) внутри этой формулы. То есть, они не “связаны” кванторами и могут принимать любые значения из области определения. Множество свободных переменных в формуле  $\varphi$  обозначается как  $FV(\varphi)$ . Множество всех переменных в формуле обозначается как  $V(\varphi)$ .

Предложения в логике первого порядка – это формулы, которые не содержат свободных переменных, то есть все переменные в них связаны кванторами. Такие формулы имеют логическое значение (истинность или ложность) в интерпретации.

## 1.3 Оценка переменных. Значение терма и формулы в данной структуре при данной оценке. Независимость значения формулы от значений переменных, не являющихся ее параметрами.

Оценка переменных – способ присвоения конкретных значений переменным в формуле. По сути это функция  $\mu$ , которая ставит в соответствие *каждой* (в том числе свободной!) переменной какое-то значение.

Значение терма  $t$  и формулы  $\varphi$  в данной структуре  $\mathcal{M}$  при данной оценке  $\mu$ :

1. если  $t$  – переменная, то  $t$  принимает значение  $\mu(t)$

2. если  $t$  – константный символ  $c$ , то  $t$  принимает значение интерпретации  $c$  в  $\mathcal{M}$ :  $c^{\mathcal{M}}$
3. если  $t$  – функция  $f$ , применяемая к термам  $t_1, \dots, t_n$ , то значение  $t$  – это  $f^{\mathcal{M}}(v_1, \dots, v_n)$ , где  $v_1, \dots, v_n$  – это значения термов при данной оценке
4. если  $\varphi$  – атомарная формула  $P(t_1, \dots, t_n)$ , то она истинна, если  $(v_1, \dots, v_n) \in R^{\mathcal{M}}$ , где  $v_1, \dots, v_n$  – это значения термов при данной оценке
5. для сложных формул  $\varphi$  используются стандартные логические правила

Независимость значения формулы от значений переменных, не являющихся ее параметрами: для любых оценок  $\pi_1, \pi_2$ , терма  $t$  и формулы  $\varphi$  выполняется:

1. если для всех  $x \in V(t)$ :  $\pi_1(x) = \pi_2(x)$ , тогда  $[t](\pi_1) = [t](\pi_2)$
2. если для всех  $x \in FV(\varphi)$ :  $\pi_1(x) = \pi_2(x)$ , тогда  $[\varphi](\pi_1) = [\varphi](\pi_2)$

Доказательство:

1. индукция по построению терма  $t$ :
  - (а) если  $t = z$ , тогда  $[t](\pi_1) = \pi_1(z) = \pi_2(z) = [t](\pi_2)$
  - (б) если  $t = f(a_1, \dots, a_n)$ , тогда  $[t](\pi_1) = f([a_1](\pi_1), \dots, [a_n](\pi_1)) = f([a_1](\pi_2), \dots, [a_n](\pi_2)) = [t](\pi_2)$  в силу  $V(a_i) \subseteq V(t)$  по предположению индукции.
2. индукция по построению формулы  $\varphi$ :
  - (а) если  $\varphi = P(a_1, \dots, a_n)$ , то для каждого терма  $a_i$  имеем  $V(a_i) \subseteq FV(\varphi)$ , поэтому  $[\varphi](\pi_1) = P([a_1](\pi_1), \dots, [a_n](\pi_1)) = P([a_1](\pi_2), \dots, [a_n](\pi_2)) = [\varphi](\pi_2)$
  - (б) если  $\varphi = \neg\psi$ , тогда  $[\varphi](\pi_1) = 1 - [\psi](\pi_1) = 1 - [\psi](\pi_2) = [\varphi](\pi_2)$  по предположению индукции в силу  $FV(\varphi) = FV(\psi)$ .
  - (в) если  $\varphi = \psi_1 \wedge \psi_2$ , тогда по предположению индукции в силу  $FV(\psi_i) \subseteq FV(\varphi)$  выполняется  $[\varphi](\pi_1) = \min([\psi_1](\pi_1), [\psi_2](\pi_1)) = \min([\psi_1](\pi_2), [\psi_2](\pi_2)) = [\varphi](\pi_2)$ . Случаи других связок аналогичны.
  - (г) если  $\varphi = \forall z\psi$ , тогда  $[\varphi](\pi_1) = \min_{m \in M} [\psi](\pi_1 + (z \rightarrow m))$ . Так как  $FV(\psi) \subseteq FV(\varphi) \cup \{z\}$ , рассмотрим как работает  $\pi_1 + (z \rightarrow m)$  на  $FV(\varphi) \cup \{z\}$ .
    - i. если  $y \in FV(\varphi)$ , то поскольку  $z \notin FV(\varphi)$ ,  $y \neq z$ , следовательно  $(\pi_1 + (z \rightarrow m))(y) = \pi_1(y) = \pi_2(y) = (\pi_2 + (z \rightarrow m))(y)$ .
    - ii. если  $y = z$ , тогда  $(\pi_1 + (z \rightarrow m))(y) = m = (\pi_2 + (z \rightarrow m))(y)$ .

Таким образом, для любого  $y \in FV(\psi)$  имеем  $(\pi_1 + (z \rightarrow m))(y) = (\pi_2 + (z \rightarrow m))(y)$ . По предположению индукции заключаем  $[\psi](\pi_1 + (z \rightarrow m)) = [\psi](\pi_2 + (z \rightarrow m))$ , из чего следует  $[\varphi](\pi_1) = [\varphi](\pi_2)$ . Случай квантора существования аналогичен.

#### 1.4 Значение терма и формулы на наборе элементов структуры. Выразимые в структуре множества (отношения, функции, элементы). Примеры выразимых множеств.

Значение терма или формулы  $\alpha(x_1, \dots, x_n)$  на наборе элементов  $y = (y_1, \dots, y_n)$  структуры  $\mathcal{M}$  определяется значением функции  $\alpha^{\mathcal{M}}(y) = [\alpha](\pi + (x_1 \rightarrow y_1) + \dots + (x_n \rightarrow y_n))$ , где  $\pi$  – любая оценка.

Выразимые в структуре  $\mathcal{M}$  множества – это множества  $D \subseteq \mathcal{M}$ , которые можно описать с помощью формул логики первого порядка

Примеры:

1. пустое множество:  $\varphi(x) = (x \neq x)$
2. носитель структуры  $\mathcal{M}$ :  $\varphi(y) = (y = y)$
3. четные числа:  $\varphi(z) = \exists a(a \in \mathbb{N} \wedge a + a = z)$

Выразимые в структуре предикаты – это предикаты, для которых существуют эквивалентные формулы логики первого порядка

### 1.5 Значение формулы при изоморфизме структур. Элементарная эквивалентность структур. Изоморфные структуры элементарно эквивалентны.

\*Если  $\sigma$ -предложение  $\varphi$  истинно в  $\mathcal{M}$ , то это обозначается так:  $\mathcal{M} \models \varphi$

\*Теория в языке сигнатуры  $\sigma$  – это какое-то множество  $\sigma$ -предложений.

\*Модель теории  $T$  в языке сигнатуры  $\sigma$  – это такая  $\sigma$ -структура  $\mathcal{M}$ , что все предложения в ней истинны.

\*Модель предложения  $\varphi$  в языке сигнатуры  $\sigma$  – это модель теории  $\{\varphi\}$ .

\*Теория  $\sigma$ -структуры  $\mathcal{M}$  – это все  $\sigma$ -предложения, истинные в  $\mathcal{M}$ . Обозначение:  $Th(\mathcal{M})$ .

Элементарная эквивалентность структур:  $\sigma$ -структуры  $\mathcal{M}$  и  $\mathcal{N}$  эквивалентны если  $Th(\mathcal{M}) = Th(\mathcal{N})$ . Обозначение:  $\mathcal{M} \equiv \mathcal{N}$

Значение формулы  $\varphi$  при изоморфизме  $\eta$  структур  $\mathcal{M}$  и  $\mathcal{N}$ : для любого  $a \in M^n$  и любой формулы  $\varphi$  равносильны  $\mathcal{M} \models \varphi(a)$  и  $\mathcal{N} \models \varphi(\eta(a))$ .

(?) Доказательство: по определению изоморфизма  $\varphi^{\mathcal{N}}(\eta(a)) = \eta(f^{\mathcal{M}}(a))$  и  $\eta(True^{\mathcal{M}}) = True^{\mathcal{N}}$

Элементарная эквивалентность изоморфных структур: изоморфные структуры элементарно эквивалентны.

(?) Доказательство: следует из равносильности  $\mathcal{M} \models \varphi(a)$  и  $\mathcal{N} \models \varphi(\eta(a))$ .

### 1.6 Значение формулы при изоморфизме структур. Сохранение выразимых множеств автоморфизмами структуры. Примеры невыразимых множеств.

Значение формулы при изоморфизме структур: см. билет 1.5

Сохранение выразимых множеств автоморфизмами структуры: семейство выразимых множеств сохраняется между автоморфизмами

(?) Доказательство: пусть  $A \subseteq M$  выразимо в  $\mathcal{M}$ . Это значит, что  $a \in A \iff \mathcal{M} \models \varphi(a)$ . Для автоморфизма  $\eta$ :  $a \in A \iff \mathcal{M} \models \varphi(a) \iff \mathcal{N} \models \varphi(\eta(a)) \iff \eta(a) \in \eta(A)$

Примеры невыразимых множеств: множество всех простых чисел (для этого необходимо проверять все возможные делители); множество натуральных чисел, являющихся степенью двойки (для этого требуется, например, рекурсия, которой нет).

### 1.7 Эквивалентность формул первого порядка. Лемма о фиктивном кванторе. Общезначимые и выполнимые формулы. Квантор всеобщности и общезначимость.

Эквивалентность формул первого порядка: формулы  $\varphi$  и  $\psi$  являются эквивалентными, если их значения совпадают в любой интерпретации при любой оценке. Обозначение  $\varphi \equiv \psi$ .

Лемма о фиктивном кванторе: пусть  $x$  не лежит в множестве свободных переменных формулы  $\varphi$ , тогда  $\varphi \equiv \forall x \varphi$

Доказательство:  $[\forall x \varphi](\pi) = \min_{m \in M} [\varphi](\pi + (x \rightarrow m))$ . Так как  $x \notin FV(\varphi)$ , для всех  $y \in FV(\varphi)$  выполнено  $(\pi + (x \rightarrow m))(y) = \pi(y)$ . По лемме о независимости значения формулы от значений переменных, не являющихся ее параметрами (см. билет 1.3), заключаем  $[\varphi](\pi + (x \rightarrow m)) = [\varphi](\pi)$  для всех  $m \in M$ . Отсюда  $[\forall x \varphi](\pi) = \min_{m \in M} [\varphi](\pi + (x \rightarrow m)) = \min_{m \in M} [\varphi](\pi) = [\varphi](\pi)$

Общезначимая формула – формула, истинная при любой интерпретации и оценке.

Выполнимая формула – формула, для которой существует интерпретация и оценка, в которой она истинна.

Квантор всеобщности и общезначимость: формула  $\varphi$  общезначима  $\iff$  формула  $\forall y \varphi$  общезначима

Доказательство:

- слева направо: формула общезначима, значит для любых оценок равна единице, в частности для оценок вида  $(\pi + (y \rightarrow m))$  для всех  $m \in M$ , поэтому  $[\forall y \varphi](\pi) = 1$
- справа налево:  $\forall y \varphi$  общезначима, значит для любых оценок  $[\varphi](\pi + (y \rightarrow m)) = 1$  для всех  $m \in M$ . Однако для любой оценки  $\pi$  имеем  $\pi = (\pi + (y \rightarrow \pi(y)))$ , поэтому  $[\varphi](\pi) = 1$  для всех оценок  $\pi$ .

## 1.8 Основные эквивалентности логики первого порядка. Замена подформулы на эквивалентную.

Основные эквивалентности логики первого порядка для произвольных  $\varphi$  и  $\psi$ :

1. Пусть  $x$  не является параметром  $\psi$ , тогда  $\forall\{\exists\}x(\varphi \wedge \{\vee\}\psi) \equiv \forall\{\exists\}x\varphi \wedge \{\vee\}\psi$  (итого 4 равенства)
2.  $\forall x(\varphi \wedge \psi) = \forall x\varphi \wedge \forall x\psi$
3.  $\forall x(\varphi \vee \psi) = \forall x\varphi \vee \forall x\psi$
4.  $\neg\forall x\varphi \equiv \exists x\neg\varphi$
5.  $\neg\exists x\varphi \equiv \forall x\neg\varphi$

Доказательство: см. [first-order](#) стр. 7-8

Пусть  $\varphi$  – какая-то формула,  $\varphi \equiv \varphi'$ , тогда замена  $\varphi$  на  $\varphi'$  эквивалентна в случаях использования логического и, или, не, импликации, "тогда и только тогда", квантора всеобщности и существования.

Доказательство: 1-6) тривиально; 7) для любой оценки  $\pi$  и  $m \in M$  имеем  $[\varphi](\pi + (x \rightarrow m)) = [\varphi'](\pi + (x \rightarrow m))$ , отсюда  $[\forall x\varphi](\pi) = \min_{m \in M} [\varphi](\pi + (x \rightarrow m)) = \min_{m \in M} [\varphi'](\pi + (x \rightarrow m)) = [\forall x\varphi'](\pi)$ ; 8) аналогично 7

Замена подформулы на эквивалентную: пусть  $\varphi \equiv \varphi'$  и  $\psi'$  была получена путем замены вхождений  $\varphi$  в  $\psi$  на  $\varphi'$ , тогда  $\psi \equiv \psi'$ .

Доказательство: достаточно рассмотреть случай одного вхождения. Индукция по построению  $\psi$ . Рассмотрим один из случаев: пусть  $\psi = \theta_1 \rightarrow \theta_2$ , тогда подформула либо совпадает с формулой, либо вхождение будет в  $\theta_1$  или  $\theta_2$ . Применим к  $\theta_i$  предположение индукции и получим, например,  $\psi' = \theta'_1 \rightarrow \theta_2$  и  $\theta_1 \equiv \theta'_1$ , далее используем подходящее утверждение из предыдущей леммы (та, что над этой) и заключаем  $\psi = \psi'$ .

## 1.9 Пропозициональные формулы и задаваемые ими булевы функции. Тавтологии первого порядка.

Пропозициональная формула – формула, построенная из пропозициональных переменных (простых букв) с помощью булевых связок.

Каждая пропозициональная формула задаёт булеву функцию, так как для каждого набора значений переменных (истина или ложь) формула принимает одно определённое значение (истина или ложь). То есть, если у вас есть пропозициональная формула  $A$  с переменными  $p$  и  $q$ , можно построить таблицу истинности, которая покажет значение формулы для всех возможных значений  $p$  и  $q$ .

Тавтология – это формула, истинная при любых значениях ее переменных. Любая тавтология общезначима.

## 1.10 Лемма о корректной подстановке.

\*Терм  $t$  свободен для переменной  $x$  в формуле  $\varphi$ , если при подстановке терма  $t$  вместо переменной  $x$  в формуле  $\varphi$  не происходит никаких изменений значений других свободных переменных. Иными словами, терм  $t$  можно подставить на место  $x$  в  $\varphi$  без появления новой привязки переменных, которая может изменить интерпретацию формулы. Обозначение:  $t - x - \varphi$ .

Это определение скорее для понимания, формальное смотреть в конспекте [first-order](#) на страницах 17-18

\*Замена  $y$  на  $x$  в формуле  $\varphi$  обозначается как  $\varphi(y/x)$

Лемма о корректной подстановке: в любой интерпретации при любой оценке  $\pi$  для всех  $\varphi$  - формул,  $t, s$  - термов, и  $x$  - переменной, если  $t - x - \varphi$ , то выполняется:

$$[s(t/x)](\pi) = [s](\pi + (x \rightarrow [t](\pi))) \text{ и } [\varphi(t/x)](\pi) = [\varphi](\pi + (x \rightarrow [t](\pi)))$$

Доказательство: см. лемма 73 в [first-order](#)

### 1.11 Понятие корректной подстановки («терм свободен для переменной в формуле»). Пример некорректной подстановки. Лемма о корректной подстановке (без доказательства). Переименование связанной переменной. Общезначимость формул вида $\forall x\varphi \rightarrow \varphi(t/x)$ и $\varphi(t/x) \rightarrow \exists x\varphi$ в случае корректной подстановки.

см. билет 1.10

Пример некорректной подстановки: возьмем формулу  $\varphi(x, y) = \forall y(P(x, y))$  и терм  $t = y$ . Подставляем:  $\varphi(x/t, y) = \forall y(P(y, y))$ . Смысл формулы изменен т.к. терм не свободен для переменной в формуле.

Переименование связанной переменной:

Лемма 1. Пусть  $y \notin V(\varphi)$  (т.е.  $y$  нет в  $\varphi$ ), тогда  $\forall x\varphi \equiv \forall y\varphi(y/x)$ .

Лемма 2. Для любого терма  $t$  и любой формулы  $\varphi$ , если  $y \notin V(\varphi)$ , то для любой оценки  $\pi$  верно:  $[t(y/x)](\pi) = [t](\pi + (x \rightarrow \pi(y)))$  и  $[\varphi(y/x)](\pi) = [\varphi](\pi + (x \rightarrow \pi(y)))$

1.  $\forall x\varphi \rightarrow \varphi(t/x)$ , если  $t$  свободен для  $x$  в  $\varphi$
2.  $\varphi(t/x) \rightarrow \exists x\varphi(x)$ , если  $t$  свободен для  $x$  в  $\varphi$

TODO: дописать доказательства

### 1.12 Переименование связанной переменной (без доказательства). Теорема о предваренной нормальной форме.]

Переименование связанной переменной:

Лемма 1. Пусть  $y \notin V(\varphi)$  (т.е.  $y$  нет в  $\varphi$ ), тогда  $\forall x\varphi \equiv \forall y\varphi(y/x)$ .

Лемма 2. Для любого терма  $t$  и любой формулы  $\varphi$ , если  $y \notin V(\varphi)$ , то для любой оценки  $\pi$  верно:  $[t(y/x)](\pi) = [t](\pi + (x \rightarrow \pi(y)))$  и  $[\varphi(y/x)](\pi) = [\varphi](\pi + (x \rightarrow \pi(y)))$

\*Предваренная формула – такая, что имеет кванторы только в кванторном префиксе в начале формулы.

Теорема о предваренной нормальной форме: для любой формулы найдется эквивалентная ей предваренная.

Доказательство: индукция по построению. Разберем все случаи:

1. Если формула атомарная, то она уже предваренная.
2. Если формула начинается с квантора, то по предположению индукции заменяем формулу под этим квантором на эквивалентную предваренную.
3. Если формула начинается с отрицания, то по предположению индукции заменяем формулу под отрицанием на эквивалентную предваренную и проносим отрицание вовнутрь, переменяя кванторы.
4. Если в формуле главная связка бинарная, то по предположению индукции заменяем формулы под связкой на эквивалентные предваренные и переименовываем связанные переменные так, чтобы все кванторы можно было вынести наружу и выносим их.

### 1.13 Понятие теории первого порядка. Примеры содержательных теорий. Модель теории. Логическое (семантическое) следование (для теорий и предположений).

Теория первого порядка – логическая система, включающая в себя сигнатуру (набор символов, включающий константы, функции и предикаты), аксиомы (набор утверждений или формул, принимаемых без доказательств) и правила вывода (правила, по которым из аксиом и других утверждений можно выводить новые утверждения)

Примеры содержательных теорий:

1. Теория групп:
  - (а) Сигнатура: бинарная операция  $*$  и константа  $e$

- (b) Аксиомы: ассоциативность, существование нейтрального элемента, существование обратного элемента

## 2. Теория колец:

- (a) Сигнатура: две бинарные операции:  $+$  и  $*$  и константы  $0$  и  $1$ .  
 (b) Аксиомы: дистрибутивность, ассоциативность, коммутативность, существование обратного элемента по сложению

Модель теории – это интерпретация сигнатуры, в которой все аксиомы теории истинны. Например, для теории групп это множество целых чисел с операцией сложения и нулем.

Логическое следование – отношение между формулами и теориями, которое говорит, что если истинны определенные формулы, то и другие формулы истинны.

Для теорий: Теория  $T$  логически следует из множества аксиом  $A$ , если любая модель  $A$  также является моделью  $T$ .

Для предложений: Предложение  $\varphi$  логически следует из теории  $T$  ( $T \models \varphi$ ), если  $\varphi$  истинно в каждой модели  $T$ .

### 1.14 Исчисление предикатов с равенством (в гильбертовской форме). Теорема о полноте и корректности исчисления предикатов (без доказательства). Теорема о компактности в двух формах: про выполнимость теории и про логическое следование из теории.

Исчисление предикатов с равенством – это система логики первого порядка, включающая равенство как основной предикат. В гильбертовской форме исчисления предикатов используются аксиомы и правила вывода.

Аксиомы для равенства:

1. Рефлексивность:  $\forall x(x = x)$
2. Симметричность:  $\forall x \forall y(x = y \rightarrow y = x)$
3. Транзитивность:  $\forall x \forall y \forall z(x = y \wedge y = z \rightarrow x = z)$
4. Замена в формулах: если  $t$  – терм, а  $P$  – предикат, то  $\forall x \forall y(x = y \rightarrow (P(x) \leftrightarrow P(y)))$

Общие аксиомы и правила вывода:

1. Аксиомы логики первого порядка
2. Правило Modus Ponens: из  $\varphi$  и  $\varphi \rightarrow \psi$  следует  $\psi$
3. Правило обобщения: из  $\varphi$  следует  $\forall x \varphi$ , если  $x$  не свободная в  $\varphi$

Теорема о полноте и корректности исчисления предикатов: если  $\varphi$  логически следует из  $A$ , тогда и только тогда  $\varphi$  выводима из  $A$  в исчислении предикатов.

Теорема о компактности: если любая конечная подсистема множества предложений имеет модель, то и все множество имеет модель.

Теорема о компактности в форме про выполнимость теории: если каждое конечное подмножество множества формул  $T$  выполнимо, то и все множество  $T$  выполнимо.

Теорема о компактности в форме про логическое следование из теории: формула  $\varphi$  логически следует из теории  $T$  тогда и только тогда, когда  $\varphi$  логически следует из некоторого конечного подмножества теории  $T$ .

TODO: дополнить доказательствами

### 1.15 Теорема компактности (без доказательства). Любой пример применения.

см. билет 1.14

Пример: хотим показать, что существует бесконечное множество.

Пусть  $T$  – это теория, содержащая набор формул  $F = \{\varphi_n : n \in \mathbb{N}\}$ , где  $\varphi_n$  утверждает, что в нашем множестве существует как минимум  $n$  различных элементов. Любое конечное подмножество  $F$  выполнимо в модели потому что можно найти конечное число элементов, принадлежащих множеству. Применяем теорему компактности: раз каждое подмножество  $F$  имеет модель, то и все множество  $F$  имеет модель, значит существует модель, содержащая бесконечно много элементов.



### 1.16 Одноленточная машина Тьюринга (допустимо неформальное определение с лентой и головкой). Сложение натуральных чисел (при унарном и бинарном кодировании).

Одноленточная машина Тьюринга — это теоретическая модель вычислений, состоящая из следующих частей: лента (бесконечная в обе стороны, разделенная на ячейки, каждая из которых может хранить один символ из конечного алфавита, который обычно содержит спец.символ "пусто": #), головка для чтения/записи (устройство, которое может перемещаться влево или вправо по ленте, считывать символы с ленты и записывать символы на ленту), множество состояний (конечное множество состояний, одно из которых является начальным, а одно или несколько могут быть конечными) и таблица переходов (определяет правила, по которым машина переходит из одного состояния в другое, в зависимости от символа под головкой)

Сложение натуральных чисел в унарном виде: очевидно

Сложение натуральных чисел в бинарном виде: вводим понятие дополнительных переменных в состоянии, типа чтобы хранить  $n$  бит, нам понадобится в  $n$  раз больше состояний. Тогда просто складываем в столбик, поддерживая в данный момент "в уме" (а точнее в дополнении к состоянию) переполнения

### 1.17 Многоленточная машина Тьюринга (допустимо неформальное определение с лентами и головками). Удвоение входного слова за линейное время.

Многоленточная машина Тьюринга — это расширение классической машины Тьюринга, у которой есть несколько лент и несколько головок для чтения/записи. Каждая лента бесконечна в обе стороны и содержит свой собственный алфавит символов.

Удвоение входного слова за линейное время: копируем символы пока не дойдем до решетки. Как дошли до решетки, идем на верхней ленте влево в начало слова и повторяем процедуру.

### 1.18 Конфигурации одноленточной и многоленточной машин Тьюринга. Меры сложности «время» и «зона» и их соотношение в обоих случаях.

Конфигурация машины Тьюринга — это описание текущего состояния машины, которое включает состояние машины, содержимое ленты (лент), позиция головки (головок).

Время выполнения (или временная сложность) алгоритма на машине Тьюринга — это количество шагов, которые машина делает для выполнения задачи. Временная сложность оценивается в зависимости от размера входных данных  $n$ .

Зона выполнения (или пространственная сложность) алгоритма на машине Тьюринга — это количество ячеек ленты, которые машина использует для выполнения задачи.

Существуют [работы](#), которые показывают, что алгоритм, выполненный на МТ из  $k$  лент эмулируется за  $T \log T$  на двуленточной МТ.

Многоленточные машины Тьюринга более эффективны по времени (например, задача удвоения входного слова) по сравнению с одноленточными машинами, так как позволяют параллельно обрабатывать несколько лент и перемещаться быстрее по необходимым данным. Однако, пространственная сложность остаётся асимптотически такой же, как и для одноленточных машин.

### 1.19 Сокращение ленточного алфавита и его цена.

См. страницы 21-24 в ["Введении в сложность вычислений"](#) Крупского

### 1.20 Сокращение числа лент и его цена.

См. страницы 24-27 в ["Введении в сложность вычислений"](#) Крупского

## 2 Вычислимость

### 2.1 Вычислимые функции (при интуитивном понимании алгоритма). Разрешимые и перечислимые множества. Связь конечности, разрешимости и перечислимости. Разрешимые множества под действием операций алгебры множеств и декартова произведения.

Вычислимая функция – это такая частичная функция  $f: \mathbb{N} \rightarrow \mathbb{N}$ , что для нее существует программа (алгоритм), которая на любом входе  $x \in \text{dom } f$  выписывает  $f(x)$ , а иначе закидывается.

Разрешимое множество – такое множество, чья характеристическая функция (функция, которая есть элемент и выдает единицу если элемент в множестве и ноль иначе) вычислима.

Перечислимое множество – такое множество, для которого есть программа, которая последовательно выписывает все элементы множества и только их. Для каждого элемента множества должно существовать  $k \in \mathbb{N}$ , что после  $k$ -ого шага элемент будет выписан.

Связь конечности, разрешимости и перечислимости: 1) конечно, значит разрешимо; 2) разрешимо, значит перечислимо.

Доказательство: 1) конечно, значит можно пронумеровать элементы  $\{a_1, \dots, a_n\}$ . Искомая характеристическая функция равна дизъюнкции (логическому или) булевских значений  $x = a_1 \vee x = a_2 \vee \dots \vee x = a_n$ . Для пустой функции всегда возвращаем ноль, что также вычислимо.

2) перебираем все натуральные числа и выводим текущее если характеристическая функция вернула единицу

Разрешимые множества под действием операций алгебры множеств и декартова произведения:  $A, B$  – разрешимы  $\implies$  разрешимы:  $A \cup B, A \cap B, A \times B, \bar{A}, \bar{B}$

Доказательство: выразим характеристические функции:  $\chi_{A \cup B}(x) = \max(\chi_A(x), \chi_B(x))$ , и т.д.

### 2.2 Перечислимые множества под действием операций алгебры множеств, декартова произведения и проекции. Теорема Поста.

Перечислимые множества под действием операций алгебры множеств, декартова произведения и проекции:  $A, B$  – перечислимы  $\implies$  перечислимы:  $A \cup B, A \cap B, A \times B, \text{pr}^i A, \text{pr}^i B$ .

Доказательство: перечислимость  $A \cup B$ : просто выводим числа по очереди; перечислимость  $A \cap B$ : по очереди выполняем по шагу алгоритмов  $A$  и  $B$  и когда получаем очередной элемент  $a_i$  выводим его только если нам уже попадался равный ему  $b_j$ . Аналогично поступаем с новыми элементами из  $B$ ; перечислимость  $A \times B$ : по очереди выполняем по шагу алгоритмов для  $A$  и  $B$  и когда получаем очередной элемент  $a_i$  выписываем пары со всеми до этого полученными  $b_1, \dots, b_k$ . Аналогично поступаем и для  $B$ ; перечислимость проекции: просто для каждого нового  $a = (a_1, \dots, a_n)$  выводим  $a_i$ .

Теорема Поста: множество разрешимо  $\iff$  его дополнение и оно само перечислимо.

Доказательство: 1) слева направо следует из леммы о связи конечности, разрешимости и перечислимости (билет 2.1)

2) справа налево доказывается с помощью следующего вычислимого алгоритма: будем выполнять по очереди по одному шагу алгоритма для множества и его дополнения. Рано или поздно в первом или втором появится наш проверяемый элемент

### 2.3 Теорема о графике вычислимой функции. Перечислимость образа и прообраза множества под действием вычислимой функции.

Теорема о графике вычислимой функции: функция вычислима  $\iff$  ее график перечислим (то есть множество пар  $(x, f(x))$ )

Доказательство: 1) справа налево: просто ждем пока выдаст нужную пару 2) слева направо: переберем все пары  $(x, k) \in \mathbb{N} \times \mathbb{N}$ .  $x$  – значение,  $k$  – количество шагов, которые проделываются для вычисления  $x$ . Таким образом, если за конечное число шагов значение вычисляется, мы выведем пару.

Перечислимость образа и прообраза множества под действием вычислимой функции: пусть множество  $A$  – перечислимо и  $f$  – вычислимая функция. Тогда  $f(A)$  и  $f^{-1}(A)$  перечислимы.

Доказательство: пусть  $G \subseteq \mathbb{N} \times \mathbb{N}$  – график  $f$ , тогда множества  $M_1 = G \cap (A \times \mathbb{N})$  и  $M_2 = G \cap (\mathbb{N} \times A)$  перечислимы так как являются пересечением двух перечислимых множеств. Заметим, что  $f(A) = \text{pr}^2 M_1$  и  $f^{-1}(A) = \text{pr}^1 M_2$ .

## 2.4 Непустые перечислимые множества суть, в точности, области значений вычислимых тотальных функций.

Лемма: множество  $A$  перечислимо  $\iff A = \emptyset$  или  $\exists f: \mathbb{N} \rightarrow A$ , что  $f$  – тотальная и  $\text{rng } f = A$ .

Доказательство: 1) справа налево: все элементы  $A$  выпишет программа, последовательно вычисляющая  $f(0), f(1), \dots$  (вычисление  $f(n)$  всегда заканчивается за конечное количество шагов ибо  $f$  тотальная и вычислимая).

2) Пусть элементы  $A$  выписывает программа  $p$ . Тогда пусть  $m$  – число шагов в программе  $p$  до вывода первого числа. Определим  $f$  следующим образом:  $f(x)$  = последнему числу после  $m + x$  шагов. Докажем, что любое  $x \in A$  лежит в образе  $f$ . Для  $x$  должно существовать такое  $k \in \mathbb{N}$ , что после  $k$  шагов  $x$  выводится программой  $p$ . Тогда  $f(k - m) = x$ .

Следствие: если  $f$  вычислима, тогда  $\text{dom } f$  и  $\text{rng } f$  перечислимы.

Доказательство: следует из перечислимости образа и прообраза множества под действием вычислимой функции (см. билет 2.3):  $\text{dom } f = f^{-1}(\mathbb{N})$ ,  $\text{rng } f = f(\mathbb{N})$ .

## 2.5 Полуразрешимость. Перечислимые множества суть, в точности, области определения вычислимых функций.

\*Полухарактеристическая функция  $\varphi$  множества  $A$  задается  $\varphi = \begin{cases} 1, & \text{если } x \in A \\ \text{неопр.}, & \text{иначе} \end{cases}$

Полуразрешимое множество – такое, что его полухарактеристическая функция вычислима.

Лемма: множество перечислимо  $\iff$  множество полуразрешимо

Доказательство: 1) слева направо: если перечислимо  $A$ , то перечислимо и  $A \times \{1\} = \Gamma(\varphi)$ . По теореме о графике вычислимой функции (см. билет 2.3),  $\varphi$  вычислима.

2) справа налево: если  $\varphi$  вычислима, то  $A = \text{dom } \varphi$  перечислима по следствию (см. билет 2.4)

## 2.6 Перечислимые множества суть, в точности, проекции разрешимых. Теорема о свойствах, равносильных перечислимости (доказательство на основе утверждений предшествующих вопросов).

Перечислимые множества в точности проекции разрешимых: множество  $A \subseteq \mathbb{N}^n$  перечислимо  $\iff \exists B \subseteq \mathbb{N}^{n+1}$  разрешимое, что  $A = \text{pr}^1(B)$ .

Доказательство: 1) справа налево:  $B$  разрешимо  $\implies B$  перечислимо  $\implies \text{pr}^1(B) = A$  перечислимо

2) слева направо: возьмем перечисляющую элементы  $A$  программу  $p$ . Пусть  $B = \{(x, k) \in \mathbb{N}^{n+1} \mid \text{программа } p \text{ выписывает } x \text{ на шаге } k\}$ . Заметим, что построенное множество отвечает требованиям:  $B$  действительно разрешимо (на входе  $(x, k)$  запустим  $k$  шагов  $p$  и если вывелось  $x$ , то элемент лежит, иначе нет) и  $A = \text{pr}^1(B)$  (т.к. для каждого  $x \in A \exists k \in \mathbb{N}$  – такое, что за  $k$  шагов программы  $p$  выведется  $x$ ).

Пусть  $A \subseteq \mathbb{N}$ , тогда следующее равносильно:

1.  $A$  перечислимо
2.  $\exists f: \mathbb{N} \rightarrow \mathbb{N}$  – вычислимая частичная, что  $A = \text{dom } f$
3.  $\exists f: \mathbb{N} \rightarrow \mathbb{N}$  – вычислимая частичная, что  $A = \text{rng } f$
4.  $A = \emptyset$  или  $\exists f: \mathbb{N} \rightarrow \mathbb{N}$  – вычислимая тотальная, что  $A = \text{rng } f$
5.  $\exists B \subseteq \mathbb{N}^2$  – разрешимое, что  $A = \text{pr}^1(B)$

Доказательство: 1 $\leftrightarrow$ 5) см. лемму выше; 1 $\leftrightarrow$ 4) см. билет 2.4 (лемма); 1 $\rightarrow$ 2) см. билет 2.5 (берем полухарактеристическую функцию); 2 $\rightarrow$ 1) см. билет 2.4 (следствие); 4 $\rightarrow$ 3) очев.; 3 $\rightarrow$ 1) см. билет 2.4 (следствие);

## 2.7 Универсальная вычислимая функция (в классе вычислимых функций $\mathbb{N} \xrightarrow{p} \mathbb{N}$ ). Т-Предикаты. Неразрешимость проблем самоприменимости и остановки.

Универсальная вычислимая функция – такая  $U: \mathbb{N}^2 \rightarrow \mathbb{N}$ , если она вычислима и для любой вычислимой функции  $f$  существует индекс  $i$  такой, что  $U_i = f$ .

**Т-Предикат:** пусть  $U$  - у.в.ф. и  $\mathcal{U}$  - программа, вычисляющая  $U$ , тогда определим множество  $T = \{(n, x, k) \mid \text{алгоритм } \mathcal{U} \text{ останавливается на входе } (n, x) \text{ за } k \text{ шагов}\}$ . Т-Предикатом называется функция  $T(n, x, k) := (n, x, k) \in T$ .

**Неразрешимость проблемы самоприменимости:** невозможно создать алгоритм, определяющий, завершится ли программа на собственном коде.

**Доказательство:** если существует такой алгоритм  $p(x)$ , возвращающий ноль если программа  $x$  закидывается на вводе  $x$  и единицу иначе, то существует программа  $f(x) = \begin{cases} \text{зацикливается,} & \text{если } p(x) = 1 \\ \text{завершается,} & \text{если } p(x) = 0 \end{cases}$ . Рассмотрим случаи: если  $p(x) = 0$ , то по определению  $f$  закидывается, но  $f(f)$  завершается; если  $p(x) = 1$ , то по определению  $f$  завершается, но  $f(f)$  закидывается. Противоречие.

**Неразрешимость проблемы остановки:** нет алгоритма  $g$ , который бы определял, завершится ли программа на данном входе.

**Доказательство:** если бы такой алгоритм существовал, то существовал бы и алгоритм  $p(x) = g(x, x)$ , проверяющий самоприменимость, но такого алгоритма нет.

## 2.8 Неразрешимость проблем самоприменимости и остановки. Примеры пересчитываемого неразрешимого и нересчитываемого множеств.

Неразрешимость проблем самоприменимости и остановки: см. билет 2.7

**Пример пересчитываемого неразрешимого множества:** пусть  $U$  - у.в.ф.,  $d(x) = U(x, x)$  тогда  $K = \{x \in \mathbb{N} \mid d(x) - \text{определено}\}$

**Доказательство:** 1) пересчитываемость следует из того, что  $K = \text{dom } d$  - вычислимой функции 2) предположим, что  $K$  - разрешимо, тогда определим вычислимую функцию  $f(x) = \begin{cases} 0, & x \notin K \\ \text{неопр.}, & x \in K \end{cases}$ . Существует  $n$ , что  $U_n = f$ . Тогда рассмотрим, лежит ли  $n$  в  $K$ : если да, то  $d(n)$  не определено, значит  $n \notin K$ ; если нет, то  $d(n) = 0$  - определено, значит  $n \in K$ . В обоих случаях противоречия, значит предположение ложно.

**Пример нересчитываемого множества:** множество  $\bar{K}$  - если бы оно было пересчитываемым, то по теореме Поста (см. билет 2.2)  $K$  было бы разрешимо, что неправда.

## 2.9 Пример вычислимой функции, не имеющей вычислимого тотального продолжения. Область определения вычислимой функции, не имеющей вычислимого тотального продолжения, пересчитываема, но не разрешима.

**Пример вычислимой функции, не имеющей вычислимого тотального продолжения:** пусть  $U$  - у.в.ф., тогда  $d(x) = U(x, x)$  - искомый пример.

**Доказательство:** 1)  $d$  - вычислима

2) Пусть  $g$  продолжает  $d$ , тогда существует вычислимая тотальная  $h(x) = g(x) + 1$ . Для  $h$  существует  $n$ , что  $U_n = h$ . Разберем случаи: если  $n \notin \text{dom } d$ , тогда не определено  $U(n, n)$ , но  $U(n, n) = U_n(n) = h(n)$  определено, значит  $n \in \text{dom } d$ , тогда  $d(n) = U(n, n) = U_n(n) = h(n) = g(n) + 1 = d(n) + 1$  - противоречие.

Область определения вычислимой функции, не имеющей вычислимого тотального продолжения, пересчитываема, но не разрешима: Пусть вычислимая функция  $f$  не имеет вычислимого тотального продолжения, тогда  $\text{dom } f$  пересчитываемо, но не разрешимо.

**Доказательство:**

1) пересчитываемость из следствия (см. билет 2.4)

2) от противного: пусть  $\text{dom } f$  разрешимо, тогда существует характеристическая функция  $g$ . Определим  $h(x) = \begin{cases} f(x), & \text{если } g(x) = 1 \\ 0, & \text{если } g(x) = 0 \end{cases}$ . Таким образом мы получили вычислимое тотальное продолжение, противоречие.

## 2.10 Невозможность универсальной вычислимой тотальной функции.

**Невозможность универсальной вычислимой тотальной функции:** тотальной у.в.ф. не может быть.

Доказательство: от противного: пусть  $U$  - тотальная у.в.ф., тогда возьмем диагональ  $d(x) = U(x, x)$  и построим  $f(x) = d(x) + 1$  - тотальная вычислимая функция. Значит существует  $n$ , что  $U_n = f$ . Рассмотрим значение  $f(n)$ :  $f(n) = U_n(n) = U(n, n) = d(n)$ , но  $f(n) = d(n) + 1$  по определению, противоречие.

## 2.11 Пример непересекающихся перечислимых множеств, не отделимых никаким разрешимым множеством.

\*Сначала нужно решить упражнение: существует вычислимая функция  $f$ , не имеющая вычислимого тотального продолжения, т. ч.  $\text{rng } f = \{0, 1\}$ .

Доказательство: пусть  $U$  - у.в.ф. и  $d(x) = U(x, x)$ . Определим  $f(x) = \begin{cases} 0, & d(x) = 0 \\ 1, & d(x) \neq 0 \end{cases}$ . Если бы

было вычислимое тотальное продолжение  $f$ , тогда существовало бы и тотальное продолжение  $d(x)$ .

\*Отделимость: множество  $C$  отделяет  $A$  от  $B$ , если  $A \subseteq C$  и  $B \subseteq \overline{C}$

Пример непересекающихся перечислимых множеств, не отделимых никаким разрешимым множеством: рассмотрим  $f$  из упражнения выше и положим  $A = f^{-1}(1)$  и  $B = f^{-1}(0)$ .

Доказательство: 1) непересекаемость очев.

2) перечислимость из теоремы о графике вычислимой функции (см. билет 2.3)

3) неотделимость разрешимой функцией: если разрешимое  $C$  отделяет  $A$  и  $B$ , тогда вычислимая тотальная характеристическая функция  $g$  множества  $C$  продолжает  $f$ , чего не может быть, противоречие.

## 2.12 Главная универсальная вычислимая функция. Вычислимое биективное кодирование пар натуральных чисел. Построение главной у.в.ф. с помощью произвольной у.в.ф.

Главная универсальная вычислимая функция – такая частичная вычислимая  $U: \mathbb{N}^2 \rightarrow \mathbb{N}$ , что для любой частичной вычислимой функции  $F: \mathbb{N}^2 \rightarrow \mathbb{N}$  существует вычислимая тотальная функция  $s: \mathbb{N} \rightarrow \mathbb{N}$ , что  $F_i = U_{s(i)}$

Вычислимое биективное кодирование пар натуральных чисел: пусть  $\langle \cdot, \cdot \rangle: \mathbb{N}^2 \rightarrow \mathbb{N}$  – произвольная тотальная биекция. Определим тотальные функции  $\pi_1$  и  $\pi_2$ , что  $\pi_1(\langle n_1, n_2 \rangle) = n_1$  и  $\pi_2(\langle n_1, n_2 \rangle) = n_2$ . Функции  $\pi_1$  и  $\pi_2$  вычислимы.

Доказательство: опишем алгоритм вычисления  $\pi_1$  (для  $\pi_2$  аналогично). Для заданного  $n \in \mathbb{N}$  перебираем все пары  $(a, b) \in \mathbb{N}^2$  пока не найдем такого, что  $\langle a, b \rangle = n$  и вернем  $a$ . Мы найдем такую пару так как функция - тотальная биекция.

Построение главной у.в.ф. с помощью произвольной у.в.ф.: *редакторское примечание*: построение совсем нетривиальное, просто внимательно следим за руками

Построение: пусть  $U$  - у.в.ф.. Определим нашу г.у.в.ф. так:  $W(n, x) = U(\pi^1(n), \langle \pi^2(n), x \rangle)$ .

Проверим, что она г.у.в.ф.: 1) вычислимость: мы берем вычислимую функцию и подставляем вычислимые аргументы, все ок.

2) Пусть  $V: \mathbb{N}^2 \rightarrow \mathbb{N}$  - какая-то вычислимая функция. Зададим еще одну функцию на основе  $V$ :  $V'(x) = V(\pi^1(x), \pi^2(x))$ , она тоже вычислимая, тогда для нее существует какое-то  $l$ , что  $U_l = V'$ . И последнее: для  $V$  искомая  $s(n) = \langle l, n \rangle$ , она вычислимая тотальная.

Теперь магия:  $W(s(n), x) = W(\langle l, n \rangle, x) = U(\pi^1(\langle l, n \rangle), \langle \pi^2(\langle l, n \rangle), x \rangle) = U(l, \langle n, x \rangle) = U_l(\langle n, x \rangle) = V'(\langle n, x \rangle) = V(\pi^1(\langle n, x \rangle), \pi^2(\langle n, x \rangle)) = V(n, x)$

## 2.13 Теорема Клини о неподвижной точке

Теорема: пусть  $U$  - г.у.в.ф.,  $f: \mathbb{N} \rightarrow \mathbb{N}$  - тотальная вычислимая функция, тогда существует такое  $n$ , что  $U_n = U_{f(n)}$

Доказательство: пусть  $V(k, x) = U(U(k, k), x)$  - вычислимая тотальная. Из главности у.в.ф. найдется тотальная  $s: \mathbb{N} \rightarrow \mathbb{N}$ , что  $U(s(k), x) = V(k, x) = U(U(k, k), x)$ . Композиция  $f$  и  $s$  тоже вычислима, поэтому существует  $t \in \mathbb{N}$ , что  $U_t = f \circ s$ . Имеем  $U(s(t), x) = V(t, x) = U(U(t, t), x) = U(U_t(t), x) = U((f \circ s)(t), x) = U(f(s(t)), x)$ . Искомое  $n = s(t)$ .

## 2.14 Бесконечность множества неподвижных точек в смысле теоремы Клини. Теорема о рекурсии как следствие теоремы Клини. Пример применения теоремы о рекурсии.

Бесконечность множества неподвижных точек в смысле теоремы Клини: пусть  $U$  - г.у.в.ф. и  $f: \mathbb{N} \rightarrow \mathbb{N}$  - тотальная, тогда бесконечно множество  $X$ , состоящее  $n$  таких, что  $U_n = U_{f(n)}$ .

Доказательство: от противного, пусть  $X$  конечно, тогда оно разрешимо и существует вычислимая функция  $g$ , что ни один ее индекс в  $U$  не лежит в  $X$ . Пусть  $m$  - индекс  $g$  в  $U$ . Рассмотрим  $h(x) = \begin{cases} m, & \text{если } x \in X \\ f(x), & \text{если } x \notin X \end{cases}$ . В силу разрешимости  $X$ ,  $h$  тотальная вычислимая. По теореме Клини, существует  $n$ , что  $U_n = U_{h(n)}$ . Разберем случаи: если  $n \in X$ , тогда  $U_n = U_{h(n)} = U_m = g$ , что противоречит определению  $g$ ; если  $n \notin X$ , тогда  $U_n = U_{h(n)} = U_{f(n)}$ , но это значит что  $n \in X$ , противоречие.

Теорема о рекурсии: пусть  $V: \mathbb{N}^2 \rightarrow \mathbb{N}$  - вычислимая частичная функция. Тогда существует  $n$ , что  $U_n = V_n$ .

Доказательство: берем  $s: \mathbb{N} \rightarrow \mathbb{N}$ , что  $V_n = U_{s(n)}$ . По теореме Клини существует  $x$ , что  $U_{s(x)} = U_x$ . Подставляем этот  $x$ :  $U_x = U_{s(x)} = V_x$ .

Пример использования теоремы о рекурсии: существует вычислимая функция  $f(x) = \begin{cases} 1, & x = 0 \\ x \cdot f(x-1), & x > 0 \end{cases}$

Доказательство: построим  $V: \mathbb{N}^2 \rightarrow \mathbb{N}$  следующим образом:  $V_k(x) = \begin{cases} 1, & x = 0 \\ x \cdot V_K(x_1), & x > 0 \end{cases}$ . По теореме о рекурсии находим  $n$ , что для какой-то г.у.в.ф.  $U$  выполняется  $U_n = V_n$ . Индукция по  $x$  показывает что функция  $U_n$  удовлетворяет условиям. (TODO: каким условиям? почему вся задача вообще не очевидная?)

## 2.15 Вычислимость индекса композиции вычислимых функций. Совместная рекурсия: решение «систем уравнений» (с тотальными правыми частями).

Вычислимость индекса композиции вычислимых функций: для г.у.в.ф.  $U$  существует вычислимая тотальная функция  $c: \mathbb{N}^2 \rightarrow \mathbb{N}$ , что для любых  $p, q \in \mathbb{N}$  выполняется  $U_{c(p,q)} = U_p \circ U_q$ .

Доказательство: возьмем вычислимую  $V(n, x) = (U_{\pi^1(n)} \circ U_{\pi^2(n)})(x)$ . Существует тотальная вычислимая  $s: \mathbb{N} \rightarrow \mathbb{N}$ , что  $V_n = U_{s(n)}$ . Положим  $c(x, y) = s(\langle x, y \rangle)$  и имеем:  $U_{c(p,q)} = U_{s(\langle p,q \rangle)} = V_{\langle p,q \rangle} = U_{\pi^1(\langle p,q \rangle)} \circ U_{\pi^2(\langle p,q \rangle)} = U_p \circ U_q$ .

Совместная рекурсия:

Пусть функции  $V_1, V_2: \mathbb{N}^3 \rightarrow \mathbb{N}$  вычислимы. Тогда существуют  $a, b \in \mathbb{N}$ , т.ч. для всех  $x \in \mathbb{N}$  выполнены

$$U(a, x) = V_1(a, b, x) \quad \text{и} \quad U(b, x) = V_2(a, b, x)$$

Доказательство:

По главности  $U$  возьмем  $p_1, p_2$  т.ч

$$U_{p_1} \simeq \pi^1, \quad U_{p_2} \simeq \pi^2.$$

Для вычислимой функции  $V: \mathbb{N}^2 \rightarrow \mathbb{N}$ , т.ч. для всех  $k, x \in \mathbb{N}$

$$V(k, x) = \langle V_1(c(p_1, k), c(p_2, k), x), V_2(c(p_1, k), c(p_2, k), x) \rangle$$

согласно лемме о рекурсии, найдется число  $n \in \mathbb{N}$ , т.ч.  $U_n = V_n$ . Положим  $a = c(p_1, n)$  и  $b = c(p_2, n)$ . Тогда для любого  $x \in \mathbb{N}$

$$U(a, x) \simeq U(c(p_1, n), x) \simeq U_{p_1}(U_n(x)) \simeq \pi^1(V_n(x)) \simeq \pi^1(V(n, x))$$

Здесь остановимся и вспомним, что  $V$  определена как  $\langle V_1(\dots), V_2(\dots) \rangle$ , а  $\pi^1$  "расшифровывает" первую координату. Следовательно для любого  $x \in \mathbb{N}$

$$\pi^1(V(n, x)) \simeq V_1(c(p_1, n), c(p_2, n), x) \simeq V_1(a, b, x)$$

Для  $b$  доказательство аналогичное

## 2.16 Индексные множества. Теорема Райса-Успенского: вывод из теоремы Клини. Пример применения.

\*Множество всех частичных вычислимых функций обозначается  $\mathcal{R}$

\*Индексным множеством семейства (иначе говоря свойства)  $\mathcal{F} \subseteq \mathcal{R}$  относительно у.в.ф.  $U$  называется числовое множество  $F = \{n \in \mathbb{N} \mid U_n \in \mathcal{F}\}$

*Теорема Райса-Успенского.* Пусть  $U$  – г.у.в.ф. и  $\emptyset \neq \mathcal{F} \subsetneq \mathcal{R}$ . Тогда индексное множество  $F = \{n \in \mathbb{N} \mid U_n \in \mathcal{F}\}$  неразрешимо.

Доказательство:

По условию найдутся функции  $f \in \mathcal{F}$  и  $g \in \mathcal{R} \setminus \mathcal{F}$ . Предположим, что множество  $F$  разрешимо. Пусть  $f = U_k, g = U_m$ . Рассмотрим функцию  $h$ , такую что для всех  $n \in \mathbb{N}$

$$h(n) = \begin{cases} m, & \text{если } n \in F \\ k, & \text{если } n \notin F \end{cases}.$$

Заметим, что  $h(n) = m \cdot \chi_F(n) + k \cdot (1 - \chi_F(n))$ , а значит эта тотальная функция вычислима. Согласно теореме Клини, найдется число  $n \in \mathbb{N}$ , т.ч.  $U_{h(n)} = U_n$ .

Если  $n \in F$ , тогда  $U_n \in \mathcal{F}$  и  $U_n = U_{h(n)} = U_m = g \notin \mathcal{F}$ . Противоречие

Значит  $n \notin F$ , тогда  $U_n \notin \mathcal{F}$  и  $U_n = U_{h(n)} = U_k = f \in \mathcal{F}$ . Снова противоречие. Следовательно  $F$  неразрешимо

*Пример применения.* Пусть  $U$  – г.у.в.ф. Рассмотрим множество  $A = \{n \in \mathbb{N} \mid \text{dom } U_n \neq \emptyset\}$ . Это индексное множество множества функций  $\mathcal{A}$ , определенных хотя бы в одной точке. Очевидно, что оно не пусто, и есть функция  $\zeta$  которая закидывается на любом входе. Значит  $\mathcal{A}$  нетривиальна, следовательно по теореме Райса-Успенского  $A$  неразрешимо. Аналогичный факт можно сказать и про  $\bar{A}$  (индексное множество функций, закидывающихся на любом входе).

## 2.17 Существование неглавной у. в. ф.

*Лемма.* Пусть  $U$  – г.у.в.ф и  $\mathcal{F} = \{f\}$  для некоторой  $f \in \mathcal{R}$ . Очевидно,  $\mathcal{F}$  нетривиально. Поэтому по теореме Райса-Успенского неразрешимо множество  $F = \{n \in \mathbb{N} \mid U_n = f\}$ , а значит и не может быть конечным. То есть любая функция имеет бесконечно много индексов и может быть вычислена бесконечным числом программ.

*Существование неглавной у.в.ф.* Пусть  $U$  – произвольная у.в.ф и  $\zeta$  – нигде не определенная функция. Рассмотрим  $A = \{n \in \mathbb{N} \mid \text{dom } U_n \neq \emptyset\}$  – индексное множество  $\mathcal{A}$  для функций, определенных хотя бы в одной точке. Докажем, что  $A$  – перечислимо. Действительно, для всех  $n$

$$n \in A \leftrightarrow \exists x \exists k T(n, x, k)$$

т.е. множество  $A$  является проекцией разрешимого множества  $T$ , а значит, перечислимо.

Вследствие нетривиальности  $\mathcal{A}$ , верно  $A \neq \emptyset$ . Тогда существует вычислимая тотальная функция  $f : \mathbb{N} \rightarrow \mathbb{N}$ , т. ч.  $A = \text{rng } f$ . Теперь положим

$$W(m, x) \simeq \begin{cases} \zeta(x), & \text{если } m = 0 \\ U(f(m-1), x), & \text{если } m > 0 \end{cases}.$$

Понятно, что функция  $W$  вычислима. Также она универсальна для класса вычислимых функций  $g$  одного аргумента: если  $\text{dom } g = \emptyset$ , то  $g = \zeta = W_0$ . Если  $\text{dom } g \neq \emptyset$ , то  $g = U_n \in \mathcal{A}$  влечет  $n \in A$ , откуда  $g = U_{f(k)} = W_{k+1}$  для подходящего  $k$ . Единственным индексом  $\zeta$  относительно  $W$  оказывается 0.

Мы получили, что индексное множество для множества  $\{\zeta\}$  относительно  $W$  конечно, а значит разрешимо. Но для г.у.в.ф. такого быть не может по лемме. Следовательно,  $W$  является неглавной у.в.ф.

## 2.18 $m$ -сводимость и её простейшие свойства

Пусть  $A, B \subset \mathbb{N}$ . Будем говорить, что множество  $A$   $m$ -сводится к  $B$  (обозначается как  $A \leq_m B$ ), если существует вычислимая тотальная функция  $f : \mathbb{N} \rightarrow \mathbb{N}$ :

$$\forall x \in \mathbb{N} (x \in A \leftrightarrow f(x) \in B)$$

*Лемма (основные свойства):* Для любых множеств  $A, B, C \subset \mathbb{N}$  выполнено следующее:

1.  $A \leq_m^{\text{id}_\mathbb{N}} A$ ;
2. если  $A \leq_m^f B$  и  $B \leq_m^g C$ , то  $A \leq_m^{g \circ f} C$ ;
3. если  $A \leq_m^f B$ , то  $\overline{A} \leq_m^f \overline{B}$ ;
4. если  $A \leq_m B$  и  $B$  разрешимо, то  $A$  разрешимо;
5. если  $A \leq_m B$  и  $B$  перечислимо, то  $A$  перечислимо;

*Доказательство:* первые 3 пункта непосредственно следуют из определения. Докажем утверждения 4 и 5: предположим, что  $x \in A \leftrightarrow f(x) \in B$  выполнено для некоторой тотальной функции  $f$  и всех  $x \in \mathbb{N}$ . Но тогда  $\chi_A(x) = \chi_B(f(x))$  и  $\omega_A(x) \equiv \omega_B(f(x))$ , а значит функция  $\chi_A$  будет вычислима, если такова  $\chi_B$ , то же самое верно и для  $\omega_A$  и  $\omega_B$ .

*Упражнение (69)* Пусть множество  $A$  разрешимо и множество  $B$  нетривиально, то есть  $\emptyset \neq B \subsetneq \mathbb{N}$ . Покажем, что  $A \leq_m B$ . Поскольку  $A$  разрешимо, то характеристическая функция множества  $A$ ,  $\chi_A$ , вычислима. Поскольку  $B$  нетривиально, то существуют некоторые  $n, m \in \mathbb{N}$ , что  $n \in B, m \notin B$ . В таком случае модифицируем  $\chi_A$  до функции  $f(x) : f(x) = n$  при  $x \in A$  и  $f(x) = m$  при  $x \notin A$ . Очевидно, что  $f$  сводит  $A$  к  $B$ . Отметим, что нетривиальность  $B$  мы использовали при выборе чисел  $n, m$ , это необходимое и достаточное условие их существования.

*Упражнение (70)* Пусть  $A \leq_m B$  и  $B \leq_m A$ . Верно ли, что в таком случае  $A = B$ . Покажем, что это неверно: пусть  $A$  есть множество четных чисел и  $B$  — множество нечетных чисел. Очевидно, как будет выглядеть сводимость  $A$  к  $B$  и  $B$  к  $A$ , но эти множества даже не пересекаются. Формально в билет не вошли несколько примеров и упражнений (71-75), но рекомендуется с ними также ознакомиться.

- 2.19 Индексные множества. Теорема Райса-Успенского: доказательство с помощью сведения. Пример применения.**
- 2.20 Пример неперечислимого множества с неперечислимым дополнением.**
- 2.21 Теорема Райса-Шапиро. Неперечислимость индексов одной функции относительно г. у. в. ф.**
- 2.22 Классы  $\Sigma_n$  и  $\Pi_n$  арифметической иерархии и их простейшие свойства.**
- 2.23 Классы  $\Sigma_n$  и  $\Pi_n$  арифметической иерархии. Включение  $\Sigma_n$  и  $\Pi_n$  ( $\Sigma_{n+1} \cap \Pi_{n+1}$  при  $n > 0$  (без доказательства строгости)).**