Листок № 1. Множества и соответствия

Буквой «$\boldsymbol{\sigma}$» (греч. $\sigma\eta\mu\alpha\nu\tau\iota\kappa\acute{o}\varsigma$ — важный) отмечены *ключевые* задачи.

1. Существуют ли такие множества A, B и C, что $A \cap B \neq \varnothing$, но $A \cap C = \varnothing$ и $(A \cap B) \setminus C = \varnothing$?

2. Докажите, что если какое-то равенство (содержащее переменные для множеств и операции $\cap$, $\cup$ и $\setminus$) не является истинным для всех множеств, то найдётся контрпример к нему, все множества которого пусты или состоят из одного элемента.

3. Множество U содержит $2n$ элементов. В нём выделено k подмножеств, причём ни одно из них не является подмножеством другого. Каково максимально возможное значение числа k?

Определение. *Упорядоченной парой* множеств x и y назовём множество $\langle x, y\rangle \leftrightharpoons \{\{x\}, \{x, y\}\}$.

4$^{\boldsymbol{\sigma}}$. Докажите, что $\langle x_1, y_2\rangle = \langle x_2, y_2\rangle$ тогда и только тогда, когда $x_1 = x_2$ и $y_1 = y_2$.

Определение. *Декартовым произведением* множеств A и B называется множество $A\times B \leftrightharpoons \{\langle a, b\rangle \mid a \in A, b \in B\}$.

5$^{\boldsymbol{\sigma}}$. Докажите, что **а)** $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$; **б)** $(A \cup B) \times C = (A \times C) \cup (B \times C)$; **в)** $A \subseteq B$ и $C \subseteq D$ тогда и только тогда, когда $A \times C \subseteq B \times D$.

6. Докажите, что $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$. При каких A, B, C и D достигается равенство?

7. Пусть $A, B \neq \varnothing$ и $(A \times B) \cup (B \times A) = C \times D$. Докажите, что $A = B = C = D$.

Определения. *Бинарным соответствием* между множествами A и B называется произвольное подмножество их декартова произведения: $R \subseteq A \times B$. Если $A = B$, то R также называется *бинарным отношением* на A.

Вместо $\langle a, b\rangle \in R$ иногда пишут $a\,R\,b$.

Если $R \subseteq A\times B$ и $S \subseteq B\times C$ — два бинарных соответствия, то их *композицией* называется бинарное соответствие $R \circ T \leftrightharpoons \{\langle a, c\rangle \mid (\exists b \in B)\, \langle a, b\rangle \in R, \langle b, c\rangle \in T\}$.

Через $\mathbf{1}_A$ обозначим *отношение равенства* на A: $\mathbf{1}_A \leftrightharpoons \{\langle a, a\rangle \mid a \in A\}$.

8. Вычислите все возможные композиции отношений $=, \neq, <, >, \leqslant, \geqslant$ на $\mathbf{R}$.

9$^{\boldsymbol{\sigma}}$. Пусть $R \subseteq A \times A$. Докажите, что $R = \mathbf{1}_A$ тогда и только тогда, когда для любого $R_1 \subseteq A \times A$ верно $R \circ R_1 = R_1 \circ R = R_1$.

Определение. *Обратным* к бинарному соответствию $R \subseteq A \times B$ называется соответствие $R^{-1} \leftrightharpoons \{\langle b, a\rangle \mid \langle a, b\rangle \in B\} \subseteq B \times A$.

10$^{\boldsymbol{\sigma}}$. Докажите, что для любых бинарных соответствий R_1, R_2, R_3: **а)** $R_1 \circ (R_2 \circ R_3) = (R_1 \circ R_2) \circ R_3$; **б)** $(R_1 \circ R_2)^{-1} = R_2^{-1} \circ R_1^{-1}$.

11. Образуют ли бинарные отношения на произвольном множестве группу (относительно операций $\circ$ и $^{-1}$)?

Определение. Бинарное соответствие $F \subseteq A \times B$ называется *(частичной) функцией,* если оно обладает *свойством функциональности:* если $\langle x, y_1\rangle \in F$ и $\langle x, y_2\rangle \in F$, то $y_1 = y_2$. Иначе говоря, для каждого x существует не более одного y такого, что $\langle x, y\rangle \in F$. Этот единственный y (если он существует) обозначается $F(x)$. Если для любого $x \in A$ существует $F(x)$, то функция F называется *всюду определённой,* или *тотальной.* Записывается это так: $F\colon A \to B$.

12$^{\boldsymbol{\sigma}}$. Сформулируйте аккуратно определения инъективной, сюръективной и биективной функций.

13$^{\boldsymbol{\sigma}}$. Докажите, что композиция двух функций есть функция; кроме того, операция композиции сохраняет инъективность и сюръективность.

Определение. Пусть $X \subset A$, $R \subseteq A \times B$. Тогда $R(X) \leftrightharpoons \{b \in B \mid (\exists a \in X)\, \langle a, b\rangle \in R\}$.

14. Для любой функции F докажите, что **а)** $F^{-1}(X \cap Y) = F^{-1}(X) \cap F^{-1}(Y)$; **б)** $F^{-1}(X \cup Y) = F^{-1}(X) \cup F^{-1}(Y)$; **в)** $F^{-1}(X \setminus Y) = F^{-1}(X) \setminus F^{-1}(Y)$; **г)** если $X \subseteq Y$, то $F^{-1}(X) \subseteq F^{-1}(Y)$.

15$^{\boldsymbol{\sigma}}$. Пусть $F\colon A \to B$. Докажите, что **а)** F биективна тогда и только тогда F^{-1} — всюду определённая функция; **б)** F инъективна тогда и только тогда, когда F^{-1} — (частичная) функция; **в)** F биективна тогда и только тогда, когда $F \circ F^{-1} = \mathbf{1}_A$ и $F^{-1} \circ F = \mathbf{1}_B$. **г)** Что можно сказать об F, если выполнено только одно из этих условий?

16. Докажите, что всякую $F\colon A \to B$ можно представить в виде композиции $H \circ G$, где G — инъективная функция, а H — сюръективная.

17. Пусть $F\colon A \to B$, $G\colon B \to A$, причём $F \circ G = \mathbf{1}_A$. Докажите, что F инъективна, а G сюръективна.

18. Определим в рамках теории множеств *натуральный ряд:* $0 \leftrightharpoons \varnothing$, $n+1 \leftrightharpoons n \cup \{n\}$. Определите на нём операции сложения и умножения и докажите простейшие правила арифметики. Какое отношение будет отношением порядка на таким образом определённом натуральном ряде?

Листок № 2. Языки первого порядка

1. Докажите *лемму об однозначности синтаксического разбора:* всякая формула либо является атомарной, либо может быть представлена *ровно в одном* из следующих видов: $(A \vee B)$, $(A \wedge B)$, $(A \to B)$, $\neg A$, $\exists x\, A$, $\forall x\, A$, причём A, B и x определяются однозначно.

2. Пусть сигнатура содержит предикат равенства и трёхместный предикат C. Рассмотрим её нормальную интерпретацию на множестве всех точек плоскости, при этом $C(x, y, z)$ означает, что точки x и y равноудалены от точки z. Запишите в этой сигнатуре следующие свойства: **а)** «три различные точки A, B и C лежат на одной прямой»; **б)** «прямые AB и CD параллельны»; **в)** «$\angle ABC = \angle A'B'C'$»; **г)** «$\triangle ABC = \triangle A'B'C'$»; **д)** «из точки M все стороны $\triangle ABC$ видны под углом $120°$»; **е)** «I — центр вписанной окружности $\triangle ABC$»; **ё)** «M — точка пересечения медиан $\triangle ABC$»; **ж)** пятый постулат Евклида.

3. Рассмотрим естественную интерпретацию сигнатуры $\langle =, < \rangle$ на множестве $\mathbb{Z}$. Как выразить отношение $y = x + 1$?

4. Рассмотрим интерпретацию сигнатуры $(=, +, P^2)$ на множестве $\mathbb{R}$: $P(a, b)$ истинно тогда и только тогда, когда $b = a^2$; $=$ и $+$ интерпретируются естественным образом. Выразите формулой трёхместное отношение «$x = yz$».

5. Рассмотрим интерпретацию сигнатуры $(=, f^1)$ на множестве $\mathbb{Z}$: функциональный символ f интерпретируется функцией $x \mapsto (x + 2)$; предикатный символ $=$ интерпретируется естественным образом. Выразимо ли формулой двуместное отношение «$y = x + 1$»?

6. Рассмотрим естественную интерпретацию сигнатуры $(=, +, 0, 1)$ на множестве $\mathbb{R}$. При каких (фиксированных) значениях $\xi \in \mathbb{R}$ предикат «$x = \xi$» выразим формулой?

7. Выразим ли предикат «$x = 2$» в множестве $\mathbb{Z}$ с предикатами равенства и «y кратно z»?

8. Постройте формулу в сигнатуре $(=, <)$, истинную во всех конечных интерпретациях, но не общезначимую.

9. Постройте формулу в языке первого порядка *без равенства,* имеющую 3-элементную модель и не имеющую 2-элементной.

10. Рассмотрим сигнатуру арифметики: $(+, \cdot, =)$ и её естественную интерпретацию на множестве $\mathbb{N}$. Выразимые отношения в этом случае называются *арифметическими.* Докажите, что следующие отношения арифметические: **а)** «$x = 0$»; **б)** «$x = 1$»; **в)** «$x = N$» (N — фиксированное натуральное число); **г)** «$x \leqslant y$»; **д)** «x кратно y»; **е)** «x при делении на y даёт неполное частное q и остаток r»; **ё)** «$z = \text{НОД}(x, y)$»; **ж)** «x есть степень двойки»; **з)** «x — простое число»; **и)** «x — совершенное число».

11. Задайте отношение «$x = N$» формулой длины не большей, чем $C \log_2 N$ для некоторой константы C, не зависящей от N.

12. Зададим соответствие между конечными последовательностями нулей и единиц и натуральными числами следующим образом: припишем к последовательности единицу, рассмотрим полученное выражение как двоичную запись некоторого числа n и сопоставим исходной последовательности число $n - 1$ (у нас натуральные числа начинаются с нуля). Последовательности нулей и единиц будем называть *словами.* Вместо слов мы всегда будем подставлять их коды (соответствующие натуральные числа). Докажите, что следующие отношения арифметичны: **а)** «слово x состоит из одних лишь нулей»; **б)** «слова x и y равной длины»; **в)** «слово z получается приписыванием слова x к слову y»; **г)** «слово x является началом слова y»; **д)** «слово x является подсловом слова y».

13. Докажите, что существует трёхместное арифметическое отношение S со следующими свойствами: (1) для любых a и b множество $S_{ab} = \{x \mid S(x, a, b)\}$ конечно; (2) любое конечное множество натуральных чисел имеет вид S_{ab} для некоторых a и b.

14. Докажите, что следующие отношения арифметичны: **а)** «x есть степень четвёрки»; **б)** «$y = 2^x$»; **в)** «$z = x^y$»; **г)** «x — y-е по порядку простое число».

Листок № 3. Языки первого порядка II

Устранение кванторов

1. Рассмотрим естественную интерпретацию сигнатуры $\langle <^2, =^2 \rangle$ на множестве $\mathbb{Q}$. Постройте бескванторную формулу, эквивалентную (в этой интерпретации) **а)** формуле $\exists x\,(x < y_1 \wedge x = y_2)$; **б)** формуле $\forall x\,(x < y_1 \vee y_2 < x \vee x = y_2)$; **в)** формуле $\forall x\,(x < z_1 \to (\exists y\,(x < y \wedge y < z_2)))$.

2. Докажите, что в условиях предыдущей задачи **а)** любая формула вида $\exists x\,\zeta$, где ζ — конъюнкция атомарных формул и их отрицаний; **б)** любая формула вида $\exists x\,\zeta$, где ζ бескванторная; **в)** произвольная формула эквивалентна некоторой бескванторной формуле.

Теорема Тарского – Зайденберга. Всякая формула в сигнатуре $(=, <, 0, 1, +, \cdot)$ при стандартной интерпретации на множестве $\mathbb{R}$ ($\mathbb{C}$) эквивалентна некоторой бескванторной формуле.

3. Верно ли, что для случая $\mathbb{C}$ всегда можно взять ту же бескванторную формулу, что и для $\mathbb{R}$?

4. **а)** Докажите, что свойство «$x = \alpha$» (α — фиксированное действительное число) выразимо в $(\mathbb{R}; =, <, 0, 1, +, \cdot)$ тогда и только тогда, когда α — алгебраическое число. **б)** Сформулируйте и докажите аналогичное утверждение для $\mathbb{C}$.

5. Задайте бескванторной формулой (в сигнатуре $(=, <, 0, 1, +, \cdot)$) множество таких троек $\langle p, q, r\rangle \in \mathbb{R}^3$, что уравнение $x^3 + px^2 + qx + r = 0$ имеет ровно два положительных корня.

6. Задайте бескванторной формулой (в сигнатуре $(=, <, 0, 1, +, \cdot)$) множество таких четвёрок $\langle p, q, r, s\rangle \in \mathbb{C}^4$, что уравнения $z^2 + pz + q = 0$ и $z^2 + rz + s = 0$ имеют общий корень.

7. Задайте бескванторной формулой (в сигнатуре $(=, <, 0, 1, +, \cdot)$) множество таких троек $\langle p, q, r\rangle \in \mathbb{C}^3$, что многочлен $z^3 + pz^2 + qz + r$ имеет кратный корень.

8. Рассмотрим интерпретацию сигнатуры $(=, S, 0)$ на множестве $\mathbb{Z}$. **а)** Сформулируйте и докажите теорему об устранении кванторов. **б)** Докажите, что отношение «$x < y$» в этой интерпретации невыразимо. **в)** Можно ли это сделать методом автоморфизмов?

Компактность

Моделью теории (множества формул без свободных переменных) называется интерпретация, в которой истинны все формулы данной теории.

Теорема Гёделя – Мальцева о компактности. Теория T имеет модель тогда и только тогда, когда любая её конечная подтеория $T_0 \subset T$ имеет модель.

9. Существует ли теория, имеющая конечные модели сколь угодно большой мощности, но не имеющая бесконечной модели?

10. Рассмотрим сигнатуру, содержащую только двуместный предикатный символ равенства и двуместный предикатный символ R, интерпретации — множества с бинарными отношениями (ориентированные графы). Можно ли выразить формулами 1-го порядка следующие свойства отношения/графа: **а)** симметричность; **б)** рефлексивность; **в)** транзитивность; **г)** существование клики размера 6 (множества из 6 вершин, в котором каждая соединена с каждой стрелками в обе стороны); **д)** конечность множества вершин; **е)** «вершин либо чётное число, либо бесконечно много»; **ё)** ацикличность; **ж)** связность?

11. Рассмотрим сигнатуру, содержащую один двуместный предикат $=$ (равенство), два двуместных функциональных символа: $+$ и $\cdot$ и две константы: 0 и 1. Интерпретации — кольца. Можно ли выразить формулой 1-го порядка следующие свойства колец: **а)** коммутативность; **б)** отсутствие делителей нуля; **в)** «данное кольцо есть поле»; **г)** «данное кольцо есть поле характеристики p» (p — фиксированное простое число); **д)** «данное кольцо есть поле нулевой характеристики»; **е)** «данное кольцо является алгебраически замкнутым полем»?

Элементарная эквивалентность

Две интерпретации называются *элементарно эквивалентными,* если в них истинны одни и те же формулы без свободных переменных.

12. Рассмотрим сигнатуру $(=, <)$. Будут ли элементарно эквивалентны её естественные интерпретации **а)** на $\mathbb{Z}$ и $\mathbb{N}$? **б)** на $\mathbb{Z}$ и $\mathbb{Z} \times \mathbb{Z}$ (во втором случае сначала сравниваются первые компоненты пар, в случае равенства — вторые)?

13. Рассмотрим сигнатуру $(+, =)$. Будут ли элементарно эквивалентны её естественные интерпретации **а)** на $\mathbb{Z}$ и $\mathbb{Q}$? **б)** на $\mathbb{Z}$ и $\mathbb{Z} + \mathbb{Z}$?

14. Рассмотрим сигнатуру $(+, \cdot, S, =)$ и её естественную интерпретацию на множестве $\mathbb{N}$ (функциональный символ S интерпретируется отображением $x \mapsto (x+1)$). Существует ли счётная интерпретация этой сигнатуры, элементарно эквивалентная, но не изоморфная естественной интерпретации на $\mathbb{N}$?

Листок № 4. Языки первого порядка III

Формула 1-го порядка называется *замкнутой,* если она не содержит свободных переменных (все переменные связаны кванторами). *Теорией* называется произвольное множество замкнутых формул. *Моделью* теории (в данной сигнатуре) называется интерпретация (данной сигнатуры), в которой истинны все формулы, входящие в теорию.

1. Пусть B — замкнутая формула в сигнатуре без констант и функциональных символов, имеющая вид $\exists x_1\, \exists x_2\, \ldots \exists x_n\, A$, где A бескванторная. Докажите, что если B выполнима (имеет какую-то модель), то B имеет конечную модель мощности не больше n.

2. Рассмотрим сигнатуру без констант и функциональных символов, все предикатные символы которой одноместны. **а)** Существует ли в этой сигнатуре выполнимая замкнутая формула, не имеющая конечных моделей? **б)** Существует ли алгоритм, проверяющий выполнимость данной замкнутой формулы в этой сигнатуре? Если да, то оцените (хотя бы грубо) время работы этого алгоритма.

3. Назовём *спектром* данной замкнутой формулы A (в сигнатуре с равенством) множество натуральных чисел $\{n \mid$ существует модель формулы A мощности $n\}$. Существует ли формула, спектр которой — **а)** множество $\{2, 6, 100, 2013\}$; **б)** множество $\{1317, 1812, 1945\} \cup \{n \mid n \geqslant 2014\}$; **в)** множество всех чётных чисел; **г)** множество всех степеней двойки; **д)** множество всех простых чисел?

4. Придумайте сигнатуру с тремя предикатными символами (произвольной валентности) и такую её интерпретацию, что в ней каждый из трёх предикатов выражается через два других, но ни один не выражается только через один из двух других.

Исчисление предикатов

Исчисление предикатов задаётся следующими аксиомами и правилами вывода:

Аксиомы:

A1. Формулы, получаемые подстановкой из тавтологий логики высказываний.
A2. Формулы вида $(\forall x\, A) \to A[x := t]$, причём переменные терма t не связаны кванторами внутри A.
A3. Формулы вида $A[x := t] \to (\exists x\, A)$, с тем же условием.

Правила вывода:

$$\textbf{R1.}\ \frac{A \quad A \to B}{B} \qquad \underbrace{\textbf{R2.}\frac{A \to B}{A \to (\forall x\, B)} \qquad \textbf{R3.}\frac{B \to A}{(\exists x\, B) \to A}}_{\text{правила Бернайса}}$$

modus ponens (MP)

В правилах Бернайса требуется, чтобы переменная x не входила свободно в формулу A.

5. Покажите, что ограничения в аксиомах **A2** и **A3** и правилах **R2** и **R3** существенны (без них в исчислении станут выводимыми необщезначимые формулы).

Теорема Гёделя о полноте (в слабой форме). Если замкнутая формула общезначима (т.е. истинна во всех интерпретациях), то она выводима в исчислении предикатов.

Теорема Гёделя о полноте (в сильной форме). Всякая непротиворечивая теория (т.е. теория, из которой средствами исчисления предикатов нельзя одновременно вывести некоторую формулу и её отрицание) имеет модель.

6. **а)** Выведите из теоремы Гёделя о полноте в сильной форме теорему Гёделя о полноте в слабой форме. **б)** Выведите теорему Гёделя о полноте в сильной форме из теоремы Гёделя о полноте в слабой форме и теоремы о компактности (см. предыдущий листок). **в)** Выведите из теоремы Гёделя о полноте (в сильной форме) следующее утверждение: если во всех моделях теории T истинна формула A, то её можно вывести из T средствами исчисления предикатов (коротко это записывают так: $T \vDash A \Rightarrow T \vdash A$). Верна ли обратная импликация?

7. Выводимы ли в исчислении предикатов формулы: **а)** $(\forall x\, (A \to B) \wedge \exists x\, A) \to \exists x\, B$; **б)** $\exists x\, A \to \forall x\, A$; **в)** $\exists x\, \forall y\, A \to \forall y\, \exists x\, A$; **г)** $\forall y\, \exists x\, A \to \exists x\, \forall y\, A$?

8. Докажите, что если $T \vdash (A \to B)$, то $T \vdash (\exists x\, A \to \exists x\, B)$.

9. Назовём непротиворечивую теорию T *полной,* если для любой формулы A либо $T \vdash A$, либо $T \vdash \neg A$. **а)** Докажите, что полная теория обладает *дизъюнктивным свойством:* если $T \vdash B \vee C$, то $T \vdash B$ или $T \vdash C$. **б)** Приведите пример (неполной) теории, не обладающей дизъюнктивным свойством. **в)** Существуют ли неполные теории, обладающие дизъюнктивным свойством?

10. Пусть теории T_1 и T_2 в некоторой сигнатуре таковы, что теория $T_1 \cup T_2$ противоречива. Докажите, что найдётся такая формула A, что $T_1 \vdash A$ и $T_2 \vdash \neg A$.

Листок № 5. Модальная логика

Модальные формулы строятся из счётного числа переменных ($\mathrm{Var} = \{p, q, r, \ldots\}$) при помощи классических связок ($\wedge, \vee, \to, \neg$) и дополнительной одноместной связки $\Box$. Связка $\Diamond$ определяется как сокращённая запись комбинации $\neg\Box\neg$. *Шкала Крипке* есть ориентированный граф $\langle W, R\rangle$, где W — непустое множество (его элементы называются *«мирами»*), а $R \subseteq W \times W$ — произвольное бинарное отношение на W, называемое *отношением достижимости.* Утверждение $\langle x, y\rangle \in R$ мы будем записывать как xRy и иногда произносить как «мир x видит мир y». *Интерпретацией (оценкой)* переменных в данной шкале Крипке называется функция $\theta\colon W \times \mathrm{Var} \to \{0, 1\}$ (в каждом мире истинность переменных определяется независимо). Истинность сложных формул в данном мире определяется индукцией по их построению. Случай классических связок разбирается по таблицам истинности. Формула $\Box A$ истинна в мире u тогда и только тогда, когда во всех видимых из мира u мирах истинна формула v ($u \Vdash \Box A \iff (\forall v)\,(uRv \Rightarrow v \Vdash A)$). Из определений сразу получается, что $u \Vdash \Diamond A \iff (\exists v)\,(uRv$ и $v \Vdash A)$. Формула A называется *общезначимой* в шкале $\langle W, R\rangle$, если она истинна во всех мирах при всех возможных оценках переменных.

1. Рассмотрим шкалу Крипке $\langle \mathbb{Z}, <\rangle$ («миры» — целые числа, мир n «видит» мир m в точности тогда, когда $n < m$). Определим интерпретацию переменных p и q следующим образом: в мире n истинна переменная p тогда и только тогда, когда n чётно; в мире n истинна переменная q тогда и только тогда, когда $n > 0$. В каких точках полученной модели верны формулы: **а)** $\Diamond\Box p$; **б)** $\Diamond\Box q \wedge \Box\Diamond p$; **в)** $\Diamond(q \to \neg p) \wedge \Box\Diamond(p \to q)$?

2. Общезначима ли формула $\Box(\Box p \to p) \to (\Diamond\Box p \to \Box p)$ в шкале Крипке **а)** $\langle \mathbb{N}, <\rangle$; **б)** $\langle \mathbb{Z}, <\rangle$; **в)** $\langle \mathbb{Q}, <\rangle$?

3. Какие из следующих формул общезначимы во всех шкалах Крипке: **а)** $\Box A \to B \to (\Box A \to \Box B)$; **б)** $\Box A \to \Diamond A$; **в)** $\Box(A \to \Box B) \to (\Box A \to \Diamond B)$; **г)** $\Box A \to (\Diamond B \to \Diamond(A \wedge B))$?

4. Для каждой из следующих формул опишите множества шкал Крипке, в которых эта формула общезначима: **а)** $\Box p$; **б)** $\Diamond(p \vee \neg p)$; **в)** $\Diamond\Box p \to \Box\Diamond p$; **г)** $\Diamond\Box p \to p$; **д)** $\Box p \to \Diamond p$; **е)** $\Box(\Box p \to p) \to \Box p$.

* * *

Пусть Γ — некоторое множество модальных формул. Рассмотрим множество W всех максимальных непротиворечивых множеств модальных формул, содержащих Γ (слово «максимальное» здесь означает, что любое дальнейшее расширение этого множества приводит к противоречивому множеству). Определим на W отношение R: для $u, v \in M$ положим uRv, если для любой модальной формулы A утверждение $\Box A \in u$ влечёт $A \in v$.

5. Проверьте, что $\langle W, R\rangle$ является шкалой Крипке.

Шкала $\langle W, R\rangle$ называется *канонической шкалой* для множества Γ. Зададим на шкале $\langle W, R\rangle$ интерпретацию переменных так: переменная p истинна в мире $u \in W$ тогда и только тогда, когда $p \in u$.

6. Проверьте, что это свойство распространяется на произвольные формулы: формула A истинна в мире u (в смысле индуктивного определения истинности) тогда и только тогда, когда $A \in u$.

Построенная модель Крипке называется *канонической моделью* для множества Γ. Множество формул Γ (в частности, отдельную формулу) назовём *каноническим,* если оно общезначимо в своей собственной канонической шкале.

7. Докажите, что формулы $\Box p \to \Box\Box p$, $\Box p \to p$, $\Box\Diamond p \to \Diamond\Box p$, $p \to \Box\Diamond p$, $\Box p \to \Diamond p$ канонические.

8. Докажите, что формула Гёделя – Лёба $\Box(\Box p \to p) \to \Box p$ не является канонической.

9. Пусть Γ — каноническая теория. Докажите, что Γ полна по Крипке, т. е. если некоторая формула общезначима во всех шкалах Крипке, в которых общезначимы все формулы из Γ, то эта формула выводима из Γ. Какими аксиомами и правилами вывода при этом можно пользоваться?

10. Напишите модальную формулу, общезначимую в точности в тех шкалах Крипке, в которых **а)** из каждого мира достижимы не более n миров; **б)** длина максимального пути не больше n.

11. Существует ли *конечная* шкала Крипке, в которой общезначимы в точности все формулы, общезначимые **а)** во всех шкалах Крипке; **б)** в транзитивных шкалах Крипке?

12. Существует ли необщезначимая формула, общезначимая во всех конечных шкалах Крипке?

Листок № 6. Теория алгоритмов

Порождающей грамматикой называется набор $\langle \Sigma, N, \mathcal{P}, S\rangle$, где Σ и N — непересекающиеся алфавиты (алфавит N называется *вспомогательным*), $S \in N$ *(начальный символ)*, а $\mathcal{P}$ — конечное множество правил вида $u \to v$, где u и v — слова в объединённом алфавите $N \cup \Sigma$. Шаг вывода состоит в подстановке: $\eta u \theta \rightsquigarrow \eta v \theta$. Если слово w в алфавите Σ может быть получено из однобуквенного слова S за конечное число таких шагов, то это слово *порождается* данной грамматикой.

1. Постройте грамматику, порождающую **а)** все слова в алфавите $\{a, b\}$, в которых количество букв a равно количеству букв b; **б)** все слова-палиндромы в алфавите $\{a, b, c\}$; **в)** все слова вида uu (для некоторого слова u) в алфавите $\{a, b\}$; **г)** все слова в алфавите $\{a, b\}$, не имеющие вида uu; **д)** все формулы модальной логики с одной переменной p.

2. Какое множество слов порождает грамматика с $\Sigma = \{a\}$, $N = \{S, B, M, E\}$, начальным символом S и правилами $S \to BaE$, $B \to BM$, $Ma \to aaM$, $ME \to E$, $B \to \Lambda$, $E \to \Lambda$? (Λ обозначает пустое слово.)

Вычислимая функция — это функция, вычисляемая некоторым алгоритмом. Заметим, что вычислимая функция может быть определена не всюду: на некоторых входных данных алгоритм может «зависнуть».

Понятие алгоритма можно формализовывать многими различными способами; оказывается, что все они приводят к одному и тому же классу вычислимых функций. Это утверждение (называемое иногда *тезисом Чёрча)* не может быть полностью доказано как математическая теорема (поскольку квантор «для всех разумных формализаций понятия алгоритма» нематематический), однако для двух конкретных формализаций эквивалентность может быть проверена непосредственно.

Разрешимое множество — это множество, характеристическая функция которого вычислима.

Перечислимое множество — это множество значений некоторой вычислимой функции.

Всякое разрешимое множество перечислимо. Обратное неверно, но пример мы построим позже.

3. Докажите, что следующие свойства множества A равносильны:
(1) A перечислимо;
(2) A есть область определения некоторой вычислимой функции;
(3) A либо пусто, либо является множеством значений некоторой всюду определённой вычислимой функции.

4. Докажите, что функция f вычислима тогда и только тогда, когда её *график* (множество $\Gamma_f = \{\langle x, f(x)\rangle \mid x \in D(f)\}$) перечислим.

5. Докажите, что если множества A и B перечислимы, то $A \cup B$ и $A \cap B$ также перечислимы.

6. Докажите *теорему Поста:* множество $A \subseteq \mathbb{N}$ разрешимо тогда и только тогда, когда множества A и $\mathbb{N} - A$ перечислимы.

7. Всюду определённая функция $f\colon \mathbb{N} \to \mathbb{N}$ неубывает (т. е. если $m > n$, то $f(m) \geqslant f(n)$) и вычислима. Докажите, что её множество значений разрешимо. Верно ли, что всякое непустое разрешимое множество $A \subseteq \mathbb{N}$ можно задать таким образом?

8. Разрешимо ли множество **а)** $\{n \in \mathbb{N} \mid (\exists p \geqslant n)\ p \text{ и } p+2 \text{ простые}\}$; **б)** $\{x \in \mathbb{Q} \mid x < e\}$ разрешимо?

9. Множество $F \subseteq \mathbb{N} \times \mathbb{N}$ таково, что для любого $n \in \mathbb{N}$ множества $F_n^{(1)} = \{m \mid \langle n, m\rangle \in F\}$ и $F_n^{(2)} = \{m \mid \langle m, n\rangle \in F\}$ разрешимы. Всегда ли разрешимо само множество F?

10. Докажите, что всякое бесконечное перечислимое множество $A \subseteq \mathbb{N}$ содержит бесконечное разрешимое подмножество.

Пусть T — множество замкнутых формул (теория первого порядка) в некоторой сигнатуре. Положим $[T] = \{\varphi \mid T \vdash \varphi\}$ — множество *теорем* теории T (а само множество T тогда можно назвать *аксиоматизацией* множества $[T]$). Также $[T]$ называется *дедуктивным замыканием* множества T.

Теория T называется *разрешимой (перечислимой)*,, если разрешимо (соответственно, перечислимо) множество $[T]$. Теория T называется *разрешимо (перечислимо) аксиоматизируемой,* если существует разрешимое (соответственно, перечислимое) множество замкнутых формул T', такое, что $[T'] = [T]$.

11. а) Докажите, что всякая перечислимо аксиоматизируемая теория перечислима. **б)** *Трюк Крейга.* Докажите, что всякая перечислимая теория разрешимо аксиоматизируема.

12. Разрешима ли теория **а)** DLO (теория плотных линейных порядков без первого и последнего элементов); **б)** $\mathrm{Th}(\mathbb{R}; +, \cdot, =, <, 0, 1)$ (множество всех формул сигнатуры $\langle +, \cdot, =, <, 0, 1\rangle$, истинных при естественной интерпретации на множестве действительных чисел)?

Листок № 7. Теория алгоритмов II

Пусть все алгоритмы занумерованы натуральными числами и пусть соответствующие им вычислимые функции (из $\mathbb{N}$ в $\mathbb{N}$) суть g_0, g_1, g_2, $\ldots$. *Универсальная вычислимая функция* $F\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ такова, что $F(n,m) = g_n(m)$. При подходящей нумерации алгоритмов сама функция F также вычислима. Кроме того, мы потребуем, чтобы наша универсальная функция была *главной,* т. е. для любой двуместной вычислимой функции G существует всюду определённая одноместная вычислимая функция s, для которой $G(n,m) = F(s(n),m)$.

1. а) Пусть задана главная универсальная вычислимая функция F. Докажите, что существует такая вычислимая функция $c\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$, что для всех m и n верно $g_{c(m,n)} = g_m \circ g_n$ (знак «$\circ$» означает композицию функций). **б)** Верно ли это для неглавной F?

2. Определим функцию

$$f_0(n) = \begin{cases} F(n,n)+1, & \text{если } F(n,n) \text{ определено;}\\ \text{не опр.} & \text{иначе.}\end{cases}$$

Докажите, что f_0 является вычислимой функцией, однако не имеет всюду определённого вычислимого продолжения (т. е. не существует такой всюду определённой вычислимой функции $f\colon \mathbb{N}\to\mathbb{N}$, такой что $f|_{\mathcal{D}(f_0)} = f_0$).

3. Пусть f_0 — вычислимая функция, не имеющая всюду определённого вычислимого продолжения. Докажите, что её область определения является перечислимым, но не разрешимым множеством.

4. а) Докажите, что существуют непересекающиеся перечислимые множества $X, Y \subseteq \mathbb{N}$, которые не отделяются никаким разрешимым множеством (т. е. не существует такого разрешимого $Z \subseteq \mathbb{N}$, что $X \subseteq Z$ и $Y \cap Z = \varnothing$). **б)** Докажите, что существует счётное число непересекающихся перечислимых множеств, никакие два из которых нельзя отделить разрешимым множеством.

5. Докажите *теорему Успенского – Райса:* пусть $\mathcal{K}$ — нетривиальное множество вычислимых функций (т. е. непустое и не совпадающее с множеством всех вычислимых функций). Тогда множество $\{n \mid g_n \in \mathcal{K}\}$ неразрешимо.

6. Разрешимо ли множество $\{\langle n_1, n_2\rangle \mid g_{n_1} \equiv g_{n_2}\}$?

7. Может ли какая-нибудь вычислимая функция встретиться в последовательности g_0, g_1, g_2, $\ldots$ конечное число раз?

8. Напишите на любом языке программирования программу, выводящую на экран свой собственный исходный текст.

9. Некоторое множество S натуральных чисел разрешимо. Разложим все числа из S на простые множители и составим множество D из всех простых чисел, встречающихся в этих разложениях. Можно ли утверждать, что множество D разрешимо?

10. Постройте разрешимо аксиоматизируемую и при этом неразрешимую теорию первого порядка (в некоторой сигнатуре).

Сигнатуру $(S, +, \cdot, 0)$ будем называть *арифметической.* Эта сигнатура допускает естественную интерпретацию на множестве $\mathbb{N}$ (одноместный функциональный символ S интерпретируется функцией $x \mapsto x+1$.

Верна *теорема об определимости перечислимых множеств:* если множество $P \subseteq \mathbb{N}^k$ перечислимо, то существует такая формула $A(x_1,\ldots,x_k)$ в арифметической сигнатуре, что

$$\langle n_1,\ldots,n_k\rangle \in P \iff \mathbb{N} \vDash A(\bar n_1,\ldots,\bar n_k).$$

$(\bar m = \underbrace{S(S\ldots(S}_{m}(0))\ldots).)$

11. а) Докажите, что теория $\mathsf{TA} = \{A \mid \mathbb{N} \vDash A\}$ *(полная арифметика)* неперечислима. **б)** Докажите *1-ю теорему Гёделя о неполноте:* если теория в арифметической сигнатуре корректна относительно интерпретации на $\mathbb{N}$ и разрешимо аксиоматизируема, то эта теория неполна.

Дополнительный листок. Колмогоровская сложность

Будем рассматривать функции над множеством *двоичных слов* (слов из нулей и единиц) $\{0,1\}^*$. Длину слова $x \in \{0,1\}^*$ обозначим $|x|$.

Определение. Пусть фиксирована (частичная) вычислимая функция $D\colon \{0,1\}^* \to \{0,1\}^*$, называемая *способом описания*. *Колмогоровской сложностью* слова $x \in \{0,1\}^*$ относительно способа описания D называется число

$$\mathrm{K}_D(x) = \min\{|y| \mid D(y) = x\}.$$

Если же такого y, что $D(y) = x$, не существует, то $\mathrm{K}_D(x) = +\infty$.

Теорема Соломонова – Колмогорова (об оптимальном способе описания). Существует такой способ описания D, что для любого другого способа описания D' существует константа c, такая что для всех $x \in \{0,1\}^*$

$$\mathrm{K}_D(x) \leqslant \mathrm{K}_{D'}(x) + c.$$

В дальнейшем будем считать, что фиксирован некоторый оптимальный способ описания D, и колмогоровскую сложность будем обозначать просто $\mathrm{K}(x)$ (эта величина определена с точностью до аддитивной константы, зависящей от выбора оптимального способа описания).

1. Докажите, что существует константа c, такая что для любых двух слов x и y верно $\mathrm{K}(xy) \leqslant \mathrm{K}(x) + \mathrm{K}(y) + 2\log_2 \mathrm{K}(x) + c$, где xy — слово, получаемое приписыванием слова y к слову x.

2. Докажите, что для любого n существует «несжимаемое» слово x длины n, такое что $\mathrm{K}(x) \geqslant n$.

3. Чему асимптотически равно среднее арифметическое сложностей всех слов длины n?

4. а) Докажите, что функция $\mathrm{K}\colon x \mapsto \mathrm{K}(x)$ невычислима. **б)** Докажите, что у функции K не существует нетривиальных вычислимых нижних оценок: если функция $k\colon \{0,1\}^* \to \mathrm{N}$ такова, что для всех x из области определения k верно $k(x) \leqslant \mathrm{K}(x)$, то k ограничена сверху константой.

5. *Доказательство Чейтина теоремы Гёделя.* Будем считать, что утверждения о колмогоровской сложности можно записывать в виде формул некоторой корректной арифметической теории T. Докажите, что существует бесконечно много истинных, но не доказуемых в T утверждений вида $\mathrm{K}(x) > n$.