

# ТЕОРЕТИЧЕСКИЕ (“МАЛЫЕ”) ДОМАШНИЕ ЗАДАНИЯ

Математическая логика, ИТМО, М3232-М3239, весна 2023 года

## Задание №1. Знакомство с исчислением высказываний.

При решении заданий вам может потребоваться теорема о дедукции (будет доказана на второй лекции):  $\Gamma, \alpha \vdash \beta$  тогда и только тогда, когда  $\Gamma \vdash \alpha \rightarrow \beta$ . Например, если было показано существование вывода  $A \vdash A$ , то тогда теорема гарантирует и существование вывода  $\vdash A \rightarrow A$ .

1. Докажите:

- (a)  $\vdash (A \rightarrow A \rightarrow B) \rightarrow (A \rightarrow B)$
- (b)  $\vdash \neg(A \& \neg A)$
- (c)  $\vdash A \& B \rightarrow B \& A$
- (d)  $\vdash A \vee B \rightarrow B \vee A$
- (e)  $A \& \neg A \vdash B$

2. Докажите:

- (a)  $\vdash A \rightarrow \neg\neg A$
- (b)  $\neg A, B \vdash \neg(A \& B)$
- (c)  $\neg A, \neg B \vdash \neg(A \vee B)$
- (d)  $A, \neg B \vdash \neg(A \rightarrow B)$
- (e)  $\neg A, B \vdash A \rightarrow B$

3. Докажите:

- (a)  $\vdash (A \rightarrow B) \rightarrow (B \rightarrow C) \rightarrow (C \rightarrow A)$
- (b)  $\vdash (A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$  (правило контрапозиции)
- (c)  $\vdash A \& B \rightarrow \neg(\neg A \vee \neg B)$
- (d)  $\vdash \neg(\neg A \vee \neg B) \rightarrow (A \& B)$
- (e)  $\vdash (A \rightarrow B) \rightarrow (\neg A \vee B)$
- (f)  $\vdash A \& B \rightarrow A \vee B$
- (g)  $\vdash ((A \rightarrow B) \rightarrow A) \rightarrow A$  (закон Пирса)

4. Следует ли какая-нибудь расстановка скобок из другой:  $(A \rightarrow B) \rightarrow C$  и  $A \rightarrow (B \rightarrow C)$ ? Предложите вывод в исчислении высказываний или докажите, что его не существует (например, воспользовавшись теоремой о корректности, предложив соответствующую оценку).

5. Предложите схемы аксиом, позволяющие добавить следующие новые связки к исчислению.

- (a) Связка «и-не» («штрих Шеффера», “ $|$ ”):  $A | B$  истинно, когда один из аргументов ложен. Новые схемы аксиом должны давать возможность исключить конъюнкцию и отрицание из исчисления. Поясним, что мы понимаем под словами «исключить связку». Как вы знаете, конъюнкция и отрицание выражаются через «и-не» ( $\neg\alpha := \alpha | \alpha$  и т.п.). При такой замене все схемы аксиом для конъюнкции и отрицания должны стать теоремами. При этом исчисление должно остаться корректным относительно классической модели исчисления высказываний.
- (b) Связка «или-не» («стрелка Пирса», “ $\downarrow$ ”):  $A \downarrow B$  истинно, когда оба аргумента ложны. Новые схемы аксиом должны давать возможность исключить дизъюнкцию и отрицание из исчисления.
- (c) Нуль-местная связка «ложь» (“ $\perp$ ”). Мы ожидаем вот такую замену:  $\neg A := A \rightarrow \perp$ . Аналогично, аксиомы для отрицания в новом исчислении должны превратиться в теоремы.

6. Достаточно ли лжи и «исключённого или» ( $A \oplus B$  истинно, когда  $A \neq B$ ) для выражения всех остальных связок?

7. Даны высказывания  $\alpha$  и  $\beta$ , причём  $\vdash \alpha \rightarrow \beta$  и  $\nvdash \beta \rightarrow \alpha$ . Укажите способ построения высказывания  $\gamma$ , такого, что  $\vdash \alpha \rightarrow \gamma$  и  $\vdash \gamma \rightarrow \beta$ , причём  $\nvdash \gamma \rightarrow \alpha$  и  $\nvdash \beta \rightarrow \gamma$ .

8. Покажите, что если  $\alpha \vdash \beta$  и  $\neg\alpha \vdash \beta$ , то  $\vdash \beta$ .

## Задание №2. Теоремы об исчислении высказываний. Интуиционистская логика.

- Покажите, что в классическом исчислении высказываний  $\Gamma \models \alpha$  влечёт  $\Gamma \vdash \alpha$ .
- Покажите, что следующие высказывания не доказуемы в интуиционистской логике:
  - $\neg\neg A \rightarrow A$
  - $((A \rightarrow B) \rightarrow A) \rightarrow A$
  - $(A \rightarrow B) \vee (B \rightarrow A)$
  - $(A \rightarrow B \vee \neg B) \vee (\neg A \rightarrow B \vee \neg B)$
  - $\bigvee_{i=0, n-1} A_i \rightarrow A_{(i+1)\%n}$
- Выполнены ли формулы де Моргана в интуиционистской логике? Докажите или опровергните:
  - $\alpha \vee \beta \vdash \neg(\neg\alpha \& \neg\beta)$  и  $\neg(\neg\alpha \& \neg\beta) \vdash \alpha \vee \beta$
  - $\neg\alpha \& \neg\beta \vdash \neg(\alpha \vee \beta)$  и  $\neg(\alpha \vee \beta) \vdash \neg\alpha \& \neg\beta$
  - $\alpha \rightarrow \beta \vdash \neg\alpha \vee \beta$  и  $\neg\alpha \vee \beta \vdash \alpha \rightarrow \beta$
- Покажите, что никакие связки не выражаются друг через друга: то есть, нет такой формулы  $\varphi(A, B)$  из языка интуиционистской логики, не использующей связку  $\star$ , что  $\vdash A \star B \rightarrow \varphi(A, B)$  и  $\vdash \varphi(A, B) \rightarrow A \star B$ . Покажите это для каждой связки в отдельности:
  - $\star$  — конъюнкция;
  - $\star$  — дизъюнкция;
  - $\star$  — импликация;
  - $\star$  — отрицание.
- Существует несколько схожих вариантов аксиомы исключённого третьего. Не пользуясь 10 схемой аксиом, покажите следующее:
  - $\alpha \vee \neg\alpha, \alpha \rightarrow \neg\alpha \rightarrow \beta \vdash ((\alpha \rightarrow \beta) \rightarrow \alpha) \rightarrow \alpha$
  - $((\alpha \rightarrow \beta) \rightarrow \alpha) \rightarrow \alpha, \alpha \rightarrow \neg\alpha \rightarrow \beta \vdash \neg\neg\alpha \rightarrow \alpha$
- Рассмотрим несколько моделей троичной логики. Логика похожа истинностными значениями ( $V = \{-1, 0, 1\}$ , истиной считаем 1) и определением большинства операций:  $\llbracket A \& B \rrbracket = \min(\llbracket A \rrbracket, \llbracket B \rrbracket)$ ,  $\llbracket A \vee B \rrbracket = \max(\llbracket A \rrbracket, \llbracket B \rrbracket)$ ,  $\llbracket \neg A \rrbracket = -\llbracket A \rrbracket$ . Отличаются логики определением импликации (ниже), и в одном случае — определением отрицания. Про каждую из них ответьте на четыре вопроса: являются ли они корректными и/или полными моделями классического и/или интуиционистского исчисления высказываний.
  - Сильная логика неопределённости Клини:  $\llbracket A \rightarrow B \rrbracket = \llbracket \neg A \vee B \rrbracket$ .
  - Троичная логика Лукасевича:  $\llbracket A \rightarrow B \rrbracket = \min(1, 1 - \llbracket A \rrbracket + \llbracket B \rrbracket)$
  - Логика Гёделя  $G_3$ :

$$\llbracket \neg A \rrbracket = \begin{cases} 1, & \llbracket A \rrbracket = -1 \\ -1, & \text{иначе} \end{cases} \quad \llbracket A \rightarrow B \rrbracket = \begin{cases} 1, & \llbracket A \rrbracket \leq \llbracket B \rrbracket \\ \llbracket B \rrbracket, & \text{иначе} \end{cases}$$

- Изоморфизм Карри-Ховарда — соответствие между интуиционистским исчислением высказываний, с одной стороны, и языками программирования, с другой. А именно, можно заметить, что программа соответствует доказательству, тип программы — логическому высказыванию. Связки (как составные части логического высказывания) соответствуют определённым типовым конструкциям: функция — импликация, конъюнкция — упорядоченной паре, дизъюнкция — алгебраическому типу (`std::variant` и т.п.).

Например, функция `A id(A x) { return x; }` доказывает  $A \rightarrow A$ , а функция

```
std::pair<A,B> swap(std::pair<B,A> x) { return std::pair(x.second, x.first); }
```

доказывает  $B \& A \rightarrow A \& B$ .

Ложь выражается менее очевидно. Давайте за ложь мы возьмём выражение, имеющее тип несвязанного типового параметра (идея в том, чтобы данное выражение легко приводилось бы к любому типу: из лжи следует всё что угодно). Данный код доказывает  $\neg Z$ , то есть  $Z \rightarrow \perp$ :

```
template <class A>
A negate(Z x) { throw ("Value of type Z is impossible"); }
```

Конечно, в смысле изоморфизма Карри-Ховарда большинство языков программирования противоречивы.

В завершение теоретической части заметим, что в свете ВНК-интерпретации в изоморфизме Карри-Ховарда нет ничего странного: если под конструкцией мы понимаем тип, то любое значение типа — это метод построения конструкции (типы, значения которых можно построить, мы будем называть *обитаемыми*), а функция — это способ перестроения одного значения в другое.

Докажите следующие утверждения, написав соответствующую программу:

- (a)  $A \rightarrow B \rightarrow A$
- (b)  $A \& B \rightarrow A \vee B$
- (c)  $(A \& (B \vee C)) \rightarrow ((A \& B) \vee (A \& C))$
- (d)  $(A \rightarrow C) \& (B \rightarrow C) \& A \vee B \rightarrow C$
- (e)  $(B \vee C \rightarrow A) \rightarrow (B \rightarrow A) \& (C \rightarrow A)$
- (f)  $(A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$
- (g)  $((A \rightarrow B) \rightarrow C) \rightarrow (A \rightarrow (B \rightarrow C))$
- (h)  $(A \rightarrow B) \& (A \rightarrow \neg B) \rightarrow \neg A$
- (i) Выразимые в интуиционистском исчислении высказываний аналоги правил де Моргана для импликации.
- (j)  $\perp$

### Задание №3. Топология, решётки.

1. Напомним определения: *замкнутое* множество — такое, дополнение которого открыто. *Внутренностью* множества  $A^\circ$  назовём наибольшее открытое множество, содержащееся в  $A$ . *Замыканием* множества  $\bar{A}$  назовём наименьшее замкнутое множество, содержащее  $A$ . Назовём *окрестностью* точки  $x$  такое открытое множество  $V$ , что  $x \in V$ . Будем говорить, что точка  $x \in A$  *внутренняя*, если существует окрестность  $V$ , что  $V \subseteq A$ . Точка  $x$  — *граничная*, если любая её окрестность  $V$  пересекается как с  $A$ , так и с его дополнением.

- (a) Покажите, что  $A$  открыто тогда и только тогда, когда все точки  $A$  — внутренние. Также покажите, что  $A^\circ = \{x | x \in A \text{ \& } x \text{ — внутренняя точка}\}$ .
  - (b) Покажите, что  $A$  замкнуто тогда и только тогда, когда содержит все свои граничные точки. Также покажите, что  $\bar{A} = \{x | x \text{ — внутренняя или граничная точка}\}$ . Верно ли, что  $\bar{A} = X \setminus ((X \setminus A)^\circ)$ ?
  - (c) Введём топологию на деревьях способом, рассмотренным на лекции. Рассмотрим некоторое множество вершин  $V$ . Опишите множества  $V^\circ$  и  $\bar{V}$ . Какие вершины будут являться граничными для  $V$ ?
  - (d) Пусть  $A \subseteq B$ . Как связаны  $A^\circ$  и  $B^\circ$ , а также  $\bar{A}$  и  $\bar{B}$ ?
  - (e) Верно ли  $(A \cap B)^\circ = A^\circ \cap B^\circ$  и  $(A \cup B)^\circ = A^\circ \cup B^\circ$ ?
  - (f) Покажите, что  $\overline{(A^\circ)^\circ} = \bar{A}^\circ$ .
  - (g) *Задача Куратовского.* Будем применять операции взятия внутреннейности и замыкания к некоторому множеству всевозможными способами. Сколько различных множеств может всего получиться?
2. Напомним, что евклидовой топологией называется топология на  $\mathbb{R}$  с базой  $\mathcal{B} = \{(a, b) \mid a, b \in \mathbb{R}\}$ .
- (a) Связны ли  $\mathbb{Q}$  и  $\mathbb{R} \setminus \mathbb{Q}$  как топологические подпространства  $\mathbb{R}$ ?
  - (b) Связен ли интервал  $(0, 1)$ ?

3. Примеры топологий. Для каждого из примеров ниже проверьте, задано ли в нём топологическое пространство, и ответьте на следующие вопросы, если это так: каковы окрестности точек в данной топологии; каковы замкнутые множества в данной топологии; связно ли данное пространство.
  - (а) Топология Зарисского на  $\mathbb{R}$ :  $\Omega = \{\emptyset\} \cup \{X \subseteq \mathbb{R} \mid \mathbb{R} \setminus X \text{ конечно}\}$ , то есть пустое множество и все множества с конечным дополнением.
  - (б) Топология стрелки на  $\mathbb{R}$ :  $\Omega = \{\emptyset, \mathbb{R}\} \cup \{(x, +\infty) \mid x \in \mathbb{R}\}$ , то есть пустое, всё пространство и все открытые лучи.
  - (с) Множество всех бесконечных подмножеств  $\mathbb{R}$ :  $\Omega = \{\emptyset\} \cup \{X \subseteq \mathbb{R} \mid X \text{ бесконечно}\}$
  - (д) Множество всевозможных объединений арифметических прогрессий:  $A(a) = \{a \cdot x \mid x \in \mathbb{Z}\}$ ;  $X \in \Omega$ , если  $X = \emptyset$  или  $X = \bigcup_i A(a_i)$  (все  $a_i > 0$ ).
4. Непрерывной функцией называется такая, для которой прообраз открытого множества всегда открыт. Путём на топологическом пространстве  $X$  назовём непрерывное отображение вещественного отрезка  $[0, 1]$  в  $X$ . Опишите пути (то есть, опишите, какие функции могли бы являться путями):
  - (а) на  $\mathbb{N}$  (с дискретной топологией);
  - (б) в топологии Зарисского;
  - (с) на дереве (с топологией с лекции);
5. Связным множеством в топологическом пространстве назовём такое, которое связно как подпространство. Линейно связным множеством назовём такое, в котором две произвольные точки могут быть соединены путём, образ которого целиком лежит в множестве.
  - (а) Покажите, что линейно связное множество всегда связно;
  - (б) Покажите, что связное не обязательно линейно связное.
6. Всегда ли непрерывным образом связного пространства является другое связное (под)пространство? Докажите или опровергните.
7. Рассмотрим подмножество частично упорядоченного множества, и рассмотрим следующие свойства:
  - (а) наличие наибольшего элемента; (б) наличие супремума; (в) наличие единственного максимального элемента. Всего можно рассмотреть шесть утверждений ((а) влечёт (б), (а) влечёт (в), и т.п.) — про каждое определите, выполнено ли оно в общем случае, и приведите либо доказательство, либо контрпример. Задача состоит из одного пункта, для получения баллов все шесть утверждений должны быть разобраны.
8. Покажите следующие утверждения для импликативных решёток:
  - (а) монотонность: пусть  $a \leq b$  и  $c \leq d$ , тогда  $a + c \leq b + d$  и  $a \cdot c \leq b \cdot d$ ;
  - (б) законы поглощения:  $a \cdot (a + b) = a$ ;  $a + (a \cdot b) = a$ ;
  - (с)  $a \leq b$  выполнено тогда и только тогда, когда  $a \rightarrow b = 1$ ;
  - (д) из  $a \leq b$  следует  $b \rightarrow c \leq a \rightarrow c$  и  $c \rightarrow a \leq c \rightarrow b$ ;
  - (е) из  $a \leq b \rightarrow c$  следует  $a \cdot b \leq c$ ;
  - (ф)  $b \leq a \rightarrow b$  и  $a \rightarrow (b \rightarrow a) = 1$ ;
  - (г)  $a \rightarrow b \leq ((a \rightarrow (b \rightarrow c)) \rightarrow (a \rightarrow c))$ ;
  - (д)  $a \leq b \rightarrow a \cdot b$  и  $a \rightarrow (b \rightarrow (a \cdot b)) = 1$ ;
  - (и)  $a \rightarrow c \leq (b \rightarrow c) \rightarrow (a + b \rightarrow c)$ ;
  - (ж) импликативная решётка дистрибутивна:  $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$
9. Докажите, основываясь на формулах предыдущих заданий, что интуиционистское исчисление высказываний корректно, если в качестве модели выбрать алгебру Гейтинга.
10. Покажите, что на конечном множестве дистрибутивная решётка всегда импликативна.
11. Постройте пример дистрибутивной, но не импликативной решётки.
12. Покажите, что в дистрибутивной решётке всегда  $a + (b \cdot c) = (a + b) \cdot (a + c)$ .
13. Покажите, что  $(\leq)$  — отношение предпорядка, а  $(\approx)$  — отношение эквивалентности.
14. Покажите, что  $[\alpha]_{\mathcal{L}} + [\beta]_{\mathcal{L}} = [\alpha \vee \beta]_{\mathcal{L}}$ . Зависит ли результат от выбора представителей классов эквивалентности  $[\alpha]$  и  $[\beta]$ ? Ответ также докажите.
15. Покажите, что  $[\alpha \rightarrow \beta]_{\mathcal{L}}$  — псевдодополнение  $[\alpha]_{\mathcal{L}}$  до  $[\beta]_{\mathcal{L}}$ .

## Задание №4. Модели Крипке. Естественный вывод.

- Опровергните формулы, построив соответствующие модели Крипке:
  - $\neg\neg A \rightarrow A$
  - $((A \rightarrow B) \rightarrow A) \rightarrow A$
  - $(A \rightarrow B \vee \neg B) \vee (\neg A \rightarrow B \vee \neg B)$
  - $\bigvee_{i=0, n-1} A_i \rightarrow A_{(i+1)\%n}$
- Покажите, что любая модель Крипке обладает свойством: для любых  $W_i, W_j, \alpha$ , если  $W_i \leq W_j$  и  $W_i \Vdash \alpha$ , то  $W_j \Vdash \alpha$ .
- Несколько задач на упрощение структуры миров моделей Крипке.
  - Покажите, что формула опровергается моделью Крипке тогда и только тогда, когда она опровергается древовидной моделью Крипке.
  - Верно ли, что если формула опровергается некоторой древовидной моделью Крипке (причём у каждой вершины не больше двух сыновей), то эту древовидную модель можно достроить до полного бинарного дерева, с сохранением свойства опровержимости?
  - Верно ли, что если некоторая модель Крипке опровергает некоторую формулу, то добавление любого мира к модели в качестве потомка к любому из узлов оставит опровержение в силе?
- Постройте опровержимую в ИИВ формулу, которая не может быть опровергнута моделью Крипке (ответ требуется доказать):
  - глубины 2 и меньше;
  - глубины  $n \in \mathbb{N}$  и меньше.
- Покажите аналог теоремы о дедукции для естественного вывода:  $\Gamma, \alpha \vdash \beta$  тогда и только тогда, когда  $\Gamma \vdash \alpha \rightarrow \beta$ .
- Определим отображение между языками вывода (гильбертов и естественный вывод):
 
$$|\varphi|_e = \begin{cases} |\alpha|_e \star |\beta|_e, & \varphi = \alpha \star \beta \\ |\alpha|_e \rightarrow \perp, & \varphi = \neg\alpha \\ X, & \varphi = X \end{cases} \quad |\varphi|_r = \begin{cases} |\alpha|_r \star |\beta|_r, & \varphi = \alpha \star \beta \\ A \& \neg A, & \varphi = \perp \\ X, & \varphi = X \end{cases}$$
  - Покажите, что  $\vdash_e \alpha$  влечёт  $\vdash_r |\alpha|_r$ ;
  - Покажите, что  $\vdash_r \alpha$  влечёт  $\vdash_e |\alpha|_e$ .
- Классическое исчисление высказываний также можно сформулировать в стиле естественного вывода, заменив правило исключения лжи на такое:

$$\frac{\Gamma, \varphi \rightarrow \perp \vdash \perp}{\Gamma \vdash \varphi} \text{ (удал}\neg\rightarrow\text{)}$$

В этом задании будем обозначать через  $\Gamma \vdash_K \varphi$  тот факт, что формула  $\varphi$  выводится из контекста  $\Gamma$  в классическом И.В. в варианте естественного вывода.

- Покажите, что если  $\vdash_K \varphi$  и  $A_1, \dots, A_n$  — все пропозициональные переменные из  $\varphi$ , то  $\vdash_e A_1 \vee \neg A_1 \rightarrow A_2 \vee \neg A_2 \rightarrow \dots \rightarrow A_n \vee \neg A_n \rightarrow \varphi$ .
- Покажите теорему Гливенко: если  $\vdash_K \varphi$ , то  $\vdash_e \neg\neg\varphi$ .

## Задание №5. Исчисление предикатов

- Докажите (или опровергните) следующие формулы в исчислении предикатов:
  - $(\forall x.\phi) \rightarrow (\forall y.\phi[x := y])$ , если есть свобода для подстановки  $y$  вместо  $x$  в  $\phi$  и  $y$  не входит свободно в  $\phi$ .
  - $(\exists x.\phi) \rightarrow (\exists y.\phi[x := y])$ , если есть свобода для подстановки  $y$  вместо  $x$  в  $\phi$  и  $y$  не входит свободно в  $\phi$ .
  - $(\forall x.\phi) \rightarrow (\exists x.\phi)$

- (d)  $(\forall x.\forall x.\phi) \rightarrow (\forall x.\phi)$   
 (e)  $(\forall x.\phi) \rightarrow (\neg\exists x.\neg\phi)$   
 (f)  $(\exists x.\neg\phi) \rightarrow (\neg\forall x.\phi)$   
 (g)  $(\forall x.\alpha \vee \beta) \rightarrow (\neg\exists x.\neg\alpha) \& (\neg\exists x.\neg\beta)$   
 (h)  $((\forall x.\alpha) \vee (\forall y.\beta)) \rightarrow \forall x.\forall y.\alpha \vee \beta$ . Какие условия надо наложить на переменные и формулы? Приведите контрпримеры, поясняющие необходимость условий.  
 (i)  $(\alpha \rightarrow \beta) \rightarrow \forall x.(\alpha \rightarrow \beta)$ . Возможно, нужно наложить какие-то условия на переменные и формулы? Приведите контрпримеры, поясняющие необходимость условий (если условия требуются).
2. Опровергните формулы  $\phi \rightarrow \forall x.\phi$  и  $(\exists x.\phi) \rightarrow (\forall x.\phi)$
3. Докажите или опровергните (каждую формулу в отдельности):  $(\forall x.\exists y.\phi) \rightarrow (\exists y.\forall x.\phi)$  и  $(\exists x.\forall y.\phi) \rightarrow (\forall y.\exists x.\phi)$ ;
4. Докажите или опровергните (каждую формулу в отдельности):  $(\forall x.\exists y.\phi) \rightarrow (\exists x.\forall y.\phi)$  и  $(\exists x.\forall y.\phi) \rightarrow (\forall x.\exists y.\phi)$
5. Рассмотрим интуиционистское исчисление предикатов (добавим схемы аксиом и правила вывода с кванторами поверх интуиционистского исчисления высказываний).
- (a) Определим модель для исчисления предикатов. Пусть  $\langle X, \Omega \rangle$  — некоторое топологическое пространство. Возможно ли рассмотреть  $V = \Omega$  (как и в исчислении высказываний), пропозициональные связки определить аналогично топологической интерпретации И.И.В., оценки же кванторов сделать такими:

$$\llbracket \forall x.\varphi \rrbracket = \left( \bigcap_{v \in D} \llbracket \varphi \rrbracket^{x:=v} \right)^\circ, \quad \llbracket \exists x.\varphi \rrbracket = \bigcup_{v \in D} \llbracket \varphi \rrbracket^{x:=v}$$

- (b) Покажите, что в интуиционистском исчислении предикатов теорема Гливенко не имеет места (а именно, существует формула  $\alpha$ , что  $\vdash_K \alpha$ , но  $\not\vdash_I \neg\neg\alpha$ ).
- (c) Определим операцию  $(\cdot)_{Ku}$ :

$$(\varphi \star \psi)_{Ku} = \varphi_{Ku} \star \psi_{Ku}, \quad (\forall x.\varphi)_{Ku} = \forall x.\neg\neg\varphi_{Ku}, \quad (\exists x.\varphi)_{Ku} = \exists x.\varphi_{Ku}$$

Тогда *преобразование Куроды* формулы  $\varphi$  назовём  $\neg\neg(\varphi_{Ku})$ . Покажите, что  $\vdash_K \alpha$  тогда и только тогда, когда  $\vdash_I \neg\neg(\alpha_{Ku})$ .

6. Покажите, что исчисление предикатов не полно в моделях ограниченной конечной мощности. А именно, пусть дана модель  $\mathcal{M} = \langle D, F, T, E \rangle$ . Назовём мощностью модели мощность её предметного множества:  $|\mathcal{M}| = |D|$ . Покажите, что для любой конечной мощности модели  $n \in \mathbb{N}$  найдётся такая формула  $\alpha$ , что при  $|\mathcal{M}| \leq n$  выполнено  $\llbracket \alpha \rrbracket_{\mathcal{M}} = I$ , но  $\not\vdash \alpha$ .

## Задание №6. Теорема о полноте исчисления предикатов

1. Покажите, что следующие определения противоречивой теории эквивалентны (ваше рассуждение должно подходить для всех исчислений, которые мы проходили до этого момента — КИВ, ИИВ, КИП; задача состоит из одного пункта, для получения баллов все четыре утверждения должны быть разобраны): (а) существует формула  $\alpha$ , что  $\vdash \alpha \& \neg\alpha$ ; (б) существует формула  $\alpha$ , что  $\vdash \alpha$  и  $\vdash \neg\alpha$ ; (в)  $\vdash A \& \neg A$ ; (г) любая формула доказуема.
2. Покажите, что если классическое исчисление высказываний противоречиво, то также противоречиво и интуиционистское исчисление высказываний.
3. Покажите, что если  $\neg\varphi \vdash \varphi$ , то  $\vdash \varphi$ . Аналогично, покажите, что из  $\neg\varphi \vdash \alpha \& \neg\alpha$  следует  $\vdash \varphi$ . Покажите требуемые утверждения конструктивно, перестроив данные в условии доказательства в доказательство  $\varphi$ .
4. Пусть  $M$  — непротиворечивое множество формул и  $\mathcal{M}$  — построенная в соответствии с теоремой о полноте исчисления предикатов оценка для  $M$ . Мы ожидаем, что  $\mathcal{M}$  будет моделью для  $M$ , для чего было необходимо доказать несколько утверждений. Восполните некоторые пробелы в том доказательстве. А именно, если  $\varphi$  — некоторая формула и для любой формулы  $\zeta$ , более короткой, чем  $\varphi$ , выполнено  $\mathcal{M} \models \zeta$  тогда и только тогда, когда  $\zeta \in M$ , тогда покажите:

- (a) если  $\varphi = \alpha \& \beta$ ,  $\mathcal{M} \models \alpha \& \beta$ , то  $\alpha \& \beta \in M$ ; и если  $\mathcal{M} \not\models \alpha \& \beta$ , то  $\alpha \& \beta \notin M$ ;  
 (b) если  $\varphi = \neg\alpha$ ,  $\mathcal{M} \models \neg\alpha$ , то  $\neg\alpha \in M$ ; и если  $\mathcal{M} \not\models \neg\alpha$ , то  $\neg\alpha \notin M$ .

5. Напомним, что *машиной Тьюринга* называется упорядоченная шестёрка

$$\langle A_{\text{внешн}}, A_{\text{внутр}}, T, \varepsilon, s_{\text{нач}}, s_{\text{доп}} \rangle$$

где внешний и внутренний алфавиты конечны и не пересекаются ( $A_{\text{внешн}} \cap A_{\text{внутр}} = \emptyset$ ),  $\varepsilon \in A_{\text{внешн}}$ ,  $s_{\text{нач}}, s_{\text{доп}} \in A_{\text{внутр}}$ , и  $T$  — это функция переходов:  $T: A_{\text{внутр}} \times A_{\text{внешн}} \rightarrow A_{\text{внутр}} \times A_{\text{внешн}} \times \{\leftarrow, \rightarrow, \cdot\}$ .

Все неиспользованные клетки ленты заполнены  $\varepsilon$ , головка перед запуском стоит на самой левой заполненной клетке. При работе машина последовательно выполняет переходы и двигает ленту (в соответствии с  $T$ ), пока не окажется в допускающем состоянии  $s_{\text{доп}}$  (успешное завершение). Также можно выделить отвергающее состояние  $s_{\text{отв}}$ , оказавшись в котором, машина оканчивает работу с ошибкой (неуспешное завершение).

Например, пусть  $A_{\text{внешн}} = \{0, 1, \varepsilon\}$ ,  $A_{\text{внутр}} = \{s_s, s_f\}$ ,  $s_{\text{нач}} = s_s$ ,  $s_{\text{доп}} = s_f$ , отвергающего состояния не задано, и функция переходов указана в таблице ниже:

	$\varepsilon$	0	1
$s_s$	$\langle s_f, \varepsilon, \cdot \rangle$	$\langle s_s, 1, \rightarrow \rangle$	$\langle s_s, 0, \rightarrow \rangle$
$s_f$	$\langle s_f, \varepsilon, \cdot \rangle$	$\langle s_f, 0, \cdot \rangle$	$\langle s_f, 1, \cdot \rangle$

Такая машина Тьюринга меняет на ленте все 0 на 1, а все 1 — на 0. Например, для строки 011:

$$\underline{011} \Rightarrow \underline{111} \Rightarrow \underline{101} \Rightarrow \underline{100\varepsilon}$$

Заметьте, что на последнем шаге головка сдвинулась вправо, за заполненные клетки — оказавшись на неиспользованной, заполненной символами  $\varepsilon$  части ленты — и остановилась благодаря тому, что  $T(s_s, \varepsilon) = \langle s_f, \dots \rangle$ .

Напишите следующие программы для машины Тьюринга и продемонстрируйте их работу на каком-нибудь эмуляторе:

- разворачивающую строку в алфавите  $\{0, 1\}$  в обратном порядке (например, из 01110111 программа должна сделать 11101110); в этом и в последующих заданиях в алфавит внешних символов при необходимости можно добавить дополнительные символы;
  - в строке в алфавите  $\{0, 1, 2\}$  сокращающую все «постоянные» подстроки до одного символа: машина должна превратить 1022220101111 в 1020101;
  - допускающую правильные скобочные записи (например,  $(( ))$  должно допускаться, а  $)() ($  — отвергаться);
  - допускающую строки вида  $a^n b^n c^n$  в алфавите  $\{a, b, c\}$  (например, строка  $aabbcc$  должна допускаться, а  $abbbc$  — отвергаться);
  - допускающую только строки, состоящие из констант и импликаций (алфавит  $\{0, 1, \rightarrow, (, )\}$ ), содержащие истинные логические выражения; например, выражение  $(( (0 \rightarrow 1) \rightarrow 0) \rightarrow 0)$  машина должна допустить, а выражение  $((1 \rightarrow 1) \rightarrow 0)$  — отвергнуть. Можно считать, что выражение написано в корректном синтаксисе (все скобки корректно расставлены, никаких скобок не пропущено).
6. Пусть дано число  $k \in \mathbb{N}$ . Известно, что если  $0 \leq k < 2^n$ , то возможно закодировать  $k$  с помощью  $n$  цифр 0 и 1. А как закодировать число, если мы не знаем верхней границы  $n$ ? Какую лучшую асимптотику длины кодировки относительно  $\log_2 k$  вы можете предложить? Кодировка должна использовать только символы 0 и 1, также код должен быть префиксным (ни один код не является префиксом другого).
7. Как известно, машина Тьюринга может быть проинтерпретирована другой машиной Тьюринга. Предложите способ закодировать машину Тьюринга в виде текста в алфавите  $\{0, 1\}$ . Естественно, символы алфавитов при кодировке меняются на их номера, и эти номера надо будет как-то записывать в виде последовательностей цифр 0 и 1.

## Задание №7. Аксиоматика Пеано, формальная арифметика.

1. Рассмотрим аксиоматику Пеано. Пусть

$$a^b = \begin{cases} 1, & b = 0 \\ a^c \cdot a, & b = c' \end{cases}$$

Докажите, что:

- (a)  $a \cdot b = b \cdot a$
- (b)  $(a + b) \cdot c = a \cdot c + b \cdot c$
- (c)  $a^{b+c} = a^b \cdot a^c$
- (d)  $(a^b)^c = a^{b \cdot c}$

2. Определим отношение «меньше или равно» так:  $0 \leq a$  и  $a' \leq b'$ , если  $a \leq b$ . Докажите, что:

- (a)  $x \leq x + y$ ;
- (b)  $x \leq x \cdot y$  (укажите, когда это так — в остальных случаях приведите контрпримеры);
- (c) Если  $a \leq b$  и  $m \leq n$ , то  $a \cdot m \leq b \cdot n$ ;
- (d)  $x \leq y$  тогда и только тогда, когда существует  $n$ , что  $x + n = y$ ;
- (e) Будем говорить, что  $a$  делится на  $b$  с остатком, если существуют такие  $p$  и  $q$ , что  $a = b \cdot p + q$  и  $0 \leq q < b$ . Покажите, что  $p$  и  $q$  всегда существуют и единственны, если  $b > 0$ .

3. Определим «ограниченное вычитание»:

$$a \dot{-} b = \begin{cases} 0, & a = 0 \\ a, & b = 0 \\ p \dot{-} q, & a = p', b = q' \end{cases}$$

Докажите, что:

- (a)  $a + b \dot{-} b = a$ ;
- (b)  $(a \dot{-} b) \cdot c = a \cdot c \dot{-} b \cdot c$ ;
- (c)  $a \dot{-} b \leq a + b$ ;
- (d)  $a \dot{-} b = 0$  тогда и только тогда, когда  $a \leq b$ .

4. Обозначим за  $\bar{n}$  представление числа  $n$  в формальной арифметике:

$$\bar{n} = \begin{cases} 0, & n = 0 \\ (\bar{k})', & n = k + 1 \end{cases}$$

Например,  $\bar{5} = 0''''$ . Докажите в формальной арифметике:

- (a)  $\vdash \bar{2} \cdot \bar{3} = \bar{6}$ ;
- (b)  $\vdash \forall p. (\exists q. q' = p) \vee p = 0$  (единственность нуля);
- (c)  $\vdash p \cdot q = 0 \rightarrow p = 0 \vee q = 0$  (отсутствие делителей нуля);

5. Будем говорить, что  $k$ -местное отношение  $R$  выразимо в формальной арифметике, если существует формула формальной арифметики  $\rho$  со свободными переменными  $x_1, \dots, x_k$ , что:

- для всех  $\langle a_1, \dots, a_k \rangle \in R$  выполнено  $\vdash \rho[x_1 := \bar{a}_1] \dots [x_k := \bar{a}_k]$  (доказуема формула  $\rho$  с подставленными значениями  $a_1, \dots, a_k$  вместо свободных переменных  $x_1, \dots, x_k$ );
- для всех  $\langle a_1, \dots, a_k \rangle \notin R$  выполнено  $\vdash \neg \rho[x_1 := \bar{a}_1] \dots [x_k := \bar{a}_k]$ .

Выразите в формальной арифметике (укажите формулу  $\rho$  и докажите требуемые свойства про неё):

- (a) «полное» отношение  $R = \mathbb{N}^2$  (любые два числа состоят в отношении);
- (b) отношение  $(=)$ ;
- (c) двуместное отношение «хотя бы один из аргументов равен 0».



## Задание №8. Рекурсивные функции. Выразимость и представимость.

1. С использованием эмулятора рекурсивных функций (применённый на лекции синтаксис подсказывает использование библиотеки на C++, но вы можете выбрать любой другой способ эмуляции), покажите, что следующие функции примитивно-рекурсивны. Ваше решение должно быть продемонстрировано в работе на простых примерах. Возможно, при реализации сложных функций вам потребуется для ускорения работы заменить базовые функции на «нативные» (например, умножение, реализованное через примитивы, заменить на встроенную операцию) — это можно делать при условии, что для них у вас есть эквивалентная примитивно-рекурсивная реализация.

(a) умножение и ограниченное вычитание;

(b) сравнение:

$$\text{LE}(x, y) = \begin{cases} 1, & x \leq y \\ 0, & x > y \end{cases}$$

(c) факториал;

(d) целочисленное деление и остаток от деления;

(e) извлечение квадратного корня (на лекции речь шла только о рекурсивности квадратного корня);

(f) функции построения упорядоченной пары и взятия её проекций; в решении используйте представление пары натуральных чисел  $\langle a, b \rangle$  через диагональную нумерацию:

a \ b	0	1	2	3	...
0	0	2	5	9	
1	1	4	8	13	
2	3	7	12	18	
3	6	11	17	24	
...					

(g) сложение и вычитание целых чисел (в стиле определения целых чисел через упорядоченную пару), также добавьте функцию нормализации (назовём целое число  $\langle p, q \rangle$  записанным в нормальном виде, если  $p \cdot q = 0$ );

(h) вычисление  $n$ -го простого числа (напомним теорему Бертрана-Чебышёва: для любого натурального  $n \geq 2$  найдётся простое число между  $n$  и  $2n$ );

(i) частичный логарифм  $\text{PLOG}_n(k) = \max\{p \mid k \leq n^p\}$  (например,  $\text{PLOG}_2(96) = 5$ );

(j) вычисление длины списка в гёделевой нумерации (например,  $\text{LEN}(3796875000) = \text{LEN}(2^3 \cdot 3^5 \cdot 5^9) = 3$ );

(k) выделение подсписка из списка (например,  $\text{SUBLIST}(2^2 \cdot 3^3 \cdot 5^4 \cdot 7^5, 2, 2) = 2^4 \cdot 3^5$ );

(l) склейка двух списков в гёделевой нумерации (например,  $\text{APPEND}(2^3 \cdot 3^5, 2^7 \cdot 3^6) = 2^3 \cdot 3^5 \cdot 5^7 \cdot 7^6$ ).

(m) проверка парности скобок: дана строка из скобок в гёделевой нумерацией, верните 1, если скобки парные и 0 иначе (например,  $\text{ISPAIRED}(2^{(C} \cdot 3^{(C} \cdot 5^{)}) = 0$ , но  $\text{ISPAIRED}(1944) = 1$ )

2. С использованием эмулятора рекурсивных функций покажите, что функция Аккермана — рекурсивная.

3. Пусть  $n$ -местное отношение  $R$  выразимо в формальной арифметике. Покажите, что тогда его характеристическая функция  $C_R$  представима в формальной арифметике:

$$C_R(\vec{x}) = \begin{cases} 1, & \vec{x} \in R \\ 0, & \text{иначе} \end{cases}$$

4. Покажите, что в определении представимости пункт  $\vdash \neg \varphi(\overline{x_1}, \dots, \overline{x_n}, \overline{y})$  при  $f(x_1, \dots, x_n) \neq y$  не является обязательным и может быть доказан из остальных пунктов определения представимой функции.

5. Покажите, что функция  $f(x) = x + 2$  представима в формальной арифметике (в ответе также требуется привести все пропущенные на лекции выводы в формальной арифметике).

## Задание №9. Теоремы о неполноте арифметики.

1. Покажите, что омега-непротиворечивая теория непротиворечива.
2. Предложите пример омега-противоречивой теории, являющейся расширением формальной арифметики.
3. Пусть  $\zeta_\varphi(x) := \forall z. \sigma(x, x, z) \rightarrow \varphi(z)$ , где формула  $\sigma(p, q, r)$  представляет функцию  $\text{SUBST}(p, q)$ , заменяющую в формуле с гёделевым номером  $p$  все свободные переменные  $x_1$  на формулу  $q$ . Тогда покажите, что формулу  $\alpha_\varphi := \zeta_\varphi(\ulcorner \zeta_\varphi \urcorner)$  можно взять в качестве формулы  $\alpha$  в лемме об автоссылках:  $\vdash \varphi(\ulcorner \alpha_\varphi \urcorner) \leftrightarrow \alpha_\varphi$ .
4. Какое из условий Гильберта-Бернайса-Лёфа нарушает формула  $\pi'$ ?
5. Покажите, что вопрос о принадлежности формулы  $\alpha(x) = \forall p. \delta(x, p) \rightarrow \neg \sigma(p)$  в доказательстве теоремы о невыразимости доказуемости к множеству  $Th_S$  ведёт к противоречию.
6. Покажите, что формула  $D(x)$  из доказательства теоремы о невыразимости доказуемости является представимой в формальной арифметике.

## Задание №10. Теория множеств.

1. Пусть заданы списки (в любом языке программирования)  $L(\alpha)$ , хранящие значения типа  $\alpha$ . Реализуйте следующие функции, являющиеся аналогами конструктивных аксиом теории множеств:
  - **empty** :  $L(\alpha)$ , строит пустой список.
  - **pair** :  $(\alpha, \alpha) \rightarrow L(\alpha)$ , формирует список из двух своих аргументов.
  - **flatten** :  $L(L(\alpha)) \rightarrow L(\alpha)$ , соединяет все списки внутри списка в один.
  - **powerset** :  $L(\alpha) \rightarrow L(L(\alpha))$ , делает из списка список всех возможных подсписков.
  - **filter** :  $(\alpha \rightarrow \text{bool}) \rightarrow L(\alpha) \rightarrow L(\alpha)$ , выделяет из списка все элементы, соответствующие условию.

Данное задание не разбивается на пункты.

2. Определим упорядоченную пару  $\langle a, b \rangle := \{\{a\}, \{a, b\}\}$ . Покажите, что  $\langle a, b \rangle = \langle c, d \rangle$  тогда и только тогда, когда  $a = c$  и  $b = d$ .
3. Докажите, что следующие конструкции являются множествами, также предложите их реализацию в смысле п.1:
  - (a) пересечение всех элементов множества  $(\bigcap a)$ ;
  - (b)  $a \setminus b$  (разность множеств);
  - (c)  $a \uplus b$  (дизъюнктивное объединение множеств:  $\{\langle x, 0 \rangle \mid x \in a\} \cup \{\langle x, 1 \rangle \mid x \in b\}$ );
  - (d)  $a \times b$  (декартово произведение множеств:  $\{\langle p, q \rangle \mid p \in a, q \in b\}$ ).
4. Определите формулу  $\varphi(x)$  для свойства « $x$  — конечный ординал». Укажите замкнутый вид для формулы, задающей ординал  $\omega$ .
5. Покажите, что если  $x$  — ординал, то  $x'$  — тоже ординал.
6. Верно ли, что если  $x'$  — ординал, то  $x$  — тоже ординал?
7. Покажите, что на множестве  $\omega$  выполняется аксиоматика Пеано (полная формализация рассуждений не требуется, но из изложения должно быть понятно, как эту формализацию в рамках теории первого порядка получить):
  - (a)  $\forall x. x \in \omega \rightarrow \neg x' = \emptyset$
  - (b)  $\forall x. \forall y. x \in \omega \ \& \ y \in \omega \rightarrow x' = y' \rightarrow x = y$
  - (c) (указание к следующему пункту) покажите, что если  $\vdash \forall x. \neg \phi(x) \rightarrow A \ \& \ \neg A$ , то  $\vdash \forall x. \phi(x)$ .
  - (d) Если  $\phi(\emptyset)$  и  $\forall x. x \in \omega \rightarrow \phi(x) \rightarrow \phi(x')$ , то  $\forall x. x \in \omega \rightarrow \phi(x)$ .
8. Проверьте следующие равенства (докажите или опровергните):

- (a)  $\omega \cdot \bar{2} = \bar{2} \cdot \omega$
  - (b)  $\omega \cdot \bar{2} = \omega + \omega$
  - (c)  $(\omega + \bar{1})^{\bar{2}} = \omega^{\bar{2}} + \bar{2} \cdot \omega + \bar{1}$
  - (d)  $\omega^\omega = (\omega^{\bar{2}})^\omega$
  - (e)  $\omega^{\omega + \bar{1}} = \omega^\omega + \bar{1}$
  - (f) Имеет ли место ассоциативность сложения и/или умножения?
9. Верно ли, что  $1^\omega = \omega$  и/или  $\omega^1 = \omega$ ?
10. Зачёт за пункт ставится, если одновременно решены два подпункта: (i) Покажите, что множество  $\omega^\omega$  имеет счётную мощность. (ii) Определим  $\uparrow k$  (башню из омег) так:

$$\uparrow k = \begin{cases} \omega, & k = 1 \\ \omega^{\uparrow n}, & k = n' \end{cases}$$

Скажем,  $\uparrow 3 = \omega^{(\omega^\omega)}$ . Будет ли счётным ординал  $\sup\{\uparrow k \mid k \in \omega\}$ ?

11. Существует ли ординал, которому соответствует множество неотрицательных рациональных чисел и упорядоченность на нём? То есть, существует ли ординал  $\sigma$ , что существует биекция  $f: \mathbb{Q}^+ \rightarrow \sigma$ , причём для всех  $a, b \in \mathbb{Q}^+$  из  $a \leq b$  следует  $f(a) \leq f(b)$  (и обратно).

## Задание №11. Порядок и мощность.

1. Покажем, что оба условия в определении ординала существенны: предъявите примеры вполне упорядоченного отношением  $(\in)$  и не транзитивного множества, а также транзитивного и не вполне упорядоченного отношением  $(\in)$  множества.
2. Покажите, что аксиома фундированности запрещает существование множества  $x$ , что  $x \in x$ . Указание: рассмотрите множество  $\{x\}$ .
3. Покажите  $\vdash \{a\} = \{b\} \rightarrow a = b$ . Доказательство может использовать метаязык, но должно показывать существование вывода в предметном языке.
4. Верно ли, что для любого отношения полного порядка на счётном множестве существует соответствующий ему ординал, имеющий тот же порядок?
5. Покажите следующее (обозначим за  $\mathcal{F}(p, q)$  множество функций из  $p$  в  $q$ ):
  - (a)  $|a| = 0$  тогда и только тогда, когда  $a = \emptyset$ ;
  - (b) если  $|a| \leq |b|$ , то  $|\mathcal{F}(g, a)| \leq |\mathcal{F}(g, b)|$ ;
  - (c) если  $|a| \leq |b|$  и  $\bar{0} < |g|$ , то  $|\mathcal{F}(a, g)| \leq |\mathcal{F}(b, g)|$ ;
  - (d)  $|\mathcal{F}(\bar{0}, a)| = \bar{1}$ ,  $|\mathcal{F}(\bar{1}, a)| = \bar{1}$ ; если  $|a| > 0$ , то  $|\mathcal{F}(a, \bar{0})| = \bar{0}$ ;
  - (e) если  $|a| \geq \aleph_0$  и  $0 < |n| < \aleph_0$ , то  $|\mathcal{F}(a, n)| = a$ .
6. Покажите эквивалентность следующих определений конечного множества (задание  $(k)$  предполагает доказательство импликации  $(k) \rightarrow (k')$ ; возможно, некоторые из переходов потребуют аксиомы выбора):
  - (a)  $a$  конечно, если каждое непустое семейство подмножеств  $a$  имеет максимальный по включению элемент. Например, при  $a = \{0, 1, 2\}$  в семействе подмножеств  $\{\emptyset, \{0, 1\}, \{1, 2\}\}$  элементы  $\{0, 1\}$  и  $\{1, 2\}$  — максимальны.
  - (b)  $a$  конечно, если  $\mathcal{P}(a)$  не равномощно своему собственному подмножеству (собственное подмножество — подмножество, не совпадающее с множеством).
  - (c)  $a$  конечно, если оно не равномощно своему собственному подмножеству.
  - (d)  $a$  конечно, если  $|a| = \emptyset$  или  $|a| \cdot \bar{2} > |a|$ .
  - (e)  $a$  конечно, если  $|a| = \emptyset$  или  $|a| = \bar{1}$  или  $|a|^2 > |a|$ .
  - (f)  $a$  конечно, если  $|a| < \aleph_0$ .

7. Покажите, что представимая функция  $f : a \rightarrow b$  биективна (т.е. инъективна и сюръективна) тогда и только тогда, когда  $\forall y. \exists! x. \phi(x, y)$ . Здесь за  $\phi(x, y)$  мы обозначаем формулу, представляющую функцию  $f$  в теории множеств, по аналогии с формальной арифметикой.
8. Покажите, что если  $a$  и  $b$  — непустые множества, то существует функция из  $a$  в  $b$  (однако функция не обязана быть инъективной или сюръективной).
9. Пусть множество  $a$  вполне упорядоченное. Назовём множество  $\{x \in a \mid x < y\}$ , где  $y \in a$ , начальным отрезком  $a$ . Рассмотрим произвольную пару вполне упорядоченных множеств  $a$  и  $b$ . Покажите, что либо между  $a$  и  $b$  есть биекция, сохраняющая порядок (такая, что  $x < y$  влечёт  $f(x) < f(y)$ ), либо есть инъективное отображение из одного множества в начальный отрезок другого, также сохраняющее порядок.
10. Покажите, что  $|\{f \mid f : \mathbb{R} \rightarrow \mathbb{R}, f \text{ — непрерывна}\}| = \beth_1$  и  $|\{f \mid f : \mathbb{R} \rightarrow \mathbb{R}\}| = \beth_2$ .
11. Покажите, что  $|\mathbb{R}| = \beth_1$ , также найдите  $|\{f \mid f : \mathbb{Q} \rightarrow \mathbb{R}, f \text{ — непрерывна}\}|$  и  $|\{f \mid f : \mathbb{R} \rightarrow \mathbb{Q}, f \text{ — непрерывна}\}|$ .

## Задание №12. Аксиома выбора

1. Фильтром  $\mathcal{F}$  назовём структуру на элементах некоторой решётки  $\langle L, (\leq) \rangle$  со следующими свойствами:
  - $0 \notin \mathcal{F}$ ;
  - если  $a, b \in \mathcal{F}$ , то  $a \cdot b \in \mathcal{F}$ ;
  - если  $a \in \mathcal{F}$ ,  $a \leq b$ ,  $b \in L$ , то  $b \in \mathcal{F}$ .

Фильтр назовём главным для  $x \in L$ , если  $\mathcal{F} = \{a \in L \mid x \leq a\}$ . Фильтр  $\mathcal{F}'$  назовём собственным подфильтром  $\mathcal{F}$ , если  $\mathcal{F}' \subset \mathcal{F}$ . Фильтр назовём ультрафильтром, если он не является собственным подфильтром никакого фильтра на  $L$ .

  - (а) Покажите, что множество дополнений конечных множеств до бесконечного образует фильтр (в качестве отношения порядка рассмотрим отношение включения). Является ли этот фильтр ультрафильтром?
  - (б) Покажите, что для ультрафильтра  $F$  на булевой алгебре  $L$  и  $x \in L$  выполнено  $x \in F$  или  $\sim x \in F$ . Также покажите, что полное непротиворечивое множество формул образует ультрафильтр.
  - (в) Покажите, что у любого фильтра есть содержащий его ультрафильтр (вам потребуются лемма Цорна для доказательства этого факта).
2. Покажите, что у любых двух множеств  $A$  и  $B$  их мощности сравнимы ( $|A| \leq |B|$  или  $|B| \leq |A|$ ). Для доказательства вам потребуется один из вариантов аксиомы выбора.
3. Покажите, что ординалы  $\beth_1$  и  $\beth_2$  существуют (Неужели мы не доказывали этого факта раньше? Видимо нет, надо доказать).

## Задание №13. Теорема о непротиворечивости формальной арифметики

1. Приведите пример наследственного подмножества  $\mathbb{R}$ , не совпадающего со всем  $\mathbb{R}$  (это возможно в силу отсутствия полного порядка на  $\mathbb{R}$ ).
2. Покажите, что если  $\vdash_\infty \neg(\alpha \vee \neg\alpha)$ , то  $\vdash_\infty 1 = 0$ .
3. Покажите  $\vdash_\infty \forall a. \forall b. a + b = b + a$ .
4. Постройте утверждение, доказательство которого не может иметь порядок, меньший  $\omega$ .
5. Покажите, что если  $\vdash_\infty \alpha$  и  $\vdash_\infty \neg\alpha \vee \beta$ , то  $\vdash_\infty \beta$  (правило Modus Ponens — источник появления сечений в перенесённых доказательствах из формальной арифметики).

## Задание №14. Лямбда-исчисление

Для проверки и демонстрации заданий используйте какой-нибудь эмулятор лямбда-исчисления, например LCI: <https://www.chatzi.org/lci/>

1. Определите следующие функции в лямбда-исчислении. В качестве подсказки заметим, что у задач на чётрчевские нумералы есть отдалённое сходство с задачами на примитивно-рекурсивные функции: все функции, предложенные в упражнениях, могут быть реализованы с помощью фиксированного количества циклов *for* (то есть, при помощи указания надлежащих функций *f* в аргументах чётрчевских нумералов). Также напоминаем, что в лямбда-исчислении несложно выражаются упорядоченные пары и значения алгебраических типов.
  - (a) Стрелка пирса и штрих шеффера.
  - (b) **If**: если первый аргумент — истина, возвращает второй аргумент, иначе — третий. Также **IsZero** — возвращает истину, если аргумент равен 0.
  - (c) **IsEven**: возвращает истину, если аргумент чётен, и **Div3**: делит нумерал на 3 с округлением вниз.
  - (d) **Fib**: вычисляет соответствующее число Фибоначчи.
  - (e) **Fact**: вычисляет факториал числа.
2. Определим на языке Хаскель следующую функцию: `show_church n = show (n (+1) 0)` Убедитесь, что `show_church (\f -> \x -> f (f x))` вернёт 2. Пользуясь данным определением и его идеей, реализуйте следующие функции:
  - (a) `int_to_church` — возвращает чётрчевский нумерал (т.е. функцию от двух аргументов) по натуральному числу. Каков точный тип результата этой функции?
  - (b) сложение двух чётрчевских нумералов.
  - (c) умножение двух чётрчевских нумералов.
3. Найдите нормальную форму для следующих выражений:
  - (a)  $\bar{2} \bar{2}$
  - (b)  $\bar{2} \bar{2} \bar{2}$
  - (c)  $\bar{2} \bar{2} \bar{2} \bar{2} \bar{2} \bar{2} \bar{2}$
4. Напишите лямбда-выражения для вычисления следующих функций:
  - (a) Возведение в степень для чётрчевских нумералов.
  - (b) Ограниченное вычитание и сравнение двух нумералов.
  - (c) Деление (округление вниз) для чётрчевских нумералов.
  - (d) Функция Аккермана.
5. Напомним определение:

$$\begin{aligned} S &:= \lambda x. \lambda y. \lambda z. x \ z \ (y \ z) \\ K &:= \lambda x. \lambda y. x \\ I &:= \lambda x. x \end{aligned}$$

Известна теорема о том, что для любого комбинатора  $X$  можно найти выражение  $P$  (состоящее только из скобок, пробелов и комбинаторов  $S$  и  $K$ ), что  $X =_{\beta} P$ . Будем говорить, что комбинатор  $P$  *выражает* комбинатор  $X$  в базисе  $SK$ .

Выразите в базисе  $SK$ :

- (a)  $F = \lambda x. \lambda y. y$
- (b)  $\bar{1}$
- (c)  $\lambda x. x \ x$  (а также  $\Omega$ )
- (d)  $Not$
- (e)  $Xor$
- (f)  $InL$

6. Покажите, что в отличие от бета-редуцируемости, для бета-редукции не выполнена теорема Чёрча-Россера (рефлексивность и транзитивность отношения для теоремы существенна). А именно, существует такое лямбда-выражение  $T$ , что  $T \rightarrow_\beta A$ ,  $T \rightarrow_\beta B$ ,  $A \neq B$ , но нет  $S$ , что  $A \rightarrow_\beta S$  и  $B \rightarrow_\beta S$ .
7. Пусть фиксирован тип чёрчевского нумерала, это  $(\alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha)$ . Найдите выражения и их тип в просто-типизированном лямбда-исчислении (и докажите наличие этого типа) для следующих выражений.
  - (a) Инкремент чёрчевского нумерала — то есть, докажите, что  $\vdash \lambda n. \lambda f. \lambda x. n \ f \ (f \ x) : \eta \rightarrow \eta$ , где  $\eta = (\alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha)$ .
  - (b) Сложение двух чёрчевских нумералов;
  - (c) Умножение двух чёрчевских нумералов (не каждая реализация умножения подойдёт).
8. Покажите, что если  $\vdash A : \alpha$ , то любое подвыражение  $A$  также имеет тип.
9. Найдите необитаемый тип в просто-типизированном лямбда-исчислении: такой  $\tau$ , что  $\not\vdash A : \tau$  ни для какого  $A$ . Напомним, что в базовом варианте исчисления тип — это либо константа, либо функция из типа в тип; другие связки, в частности ложь, конъюнкция, дизъюнкция, в базовый набор типов просто-типизированного исчисления не входят.
10. Напомним, что в одном выражении может быть более одного бета-редекса. Назовём порядок редукции *нормальным*, если всегда вычисляется тот бета-редекс, первый символ которого стоит левее всего в строке. *Аппликативным* порядком назовём такой, при котором вычисляется самый левый из наиболее вложенных редексов. Например, в выражении

$$\begin{array}{c}
 (\lambda x.x) \ ((\lambda n. \lambda f. \lambda x. n \ f \ (f \ x)) \ \lambda f. \lambda x.x) \\
 \hline
 \dots\dots\dots
 \end{array}$$

точками подчёркнут редекс для нормального порядка, а прерывистой линией — для аппликативного.

Интуитивно в нормальном порядке сперва вычисляется тело функции, а параметры вычисляются потом, по мере надобности. Аппликативный же порядок предполагает обязательное вычисление параметров перед вычислением самой функции.

Известна теорема о том, что если у выражения в принципе существует нормальная форма, то она может быть получена путём применения нормального порядка редукции.

Обычно в языках программирования применяется аппликативный порядок редукции, однако, в (практически) любом языке конструкция `if` вычисляется с помощью нормального порядка, поскольку условный оператор вычисляет только одну из веток (`then` или `else`).

Предложите лямбда-выражение, количество редукций которого до нормальной формы различается более чем в  $n$  раз при применении нормального и аппликативного порядков (по заданному заранее  $n$ ).

## Задание №15. Метод резолюции

1. Известно, что в метрических пространствах компактность подмножества эквивалентна его замкнутости и ограниченности. Но в произвольной топологии компакты могут быть причудливы. Постройте топологию на  $\mathbb{R}$ , что в ней будет существовать пример нетривиального  $X \notin \{\emptyset, \mathbb{R}\}$  и неограниченного в метрическом смысле, но компактного множества. Также покажите, что замкнутое подпространство компактного пространства компактно.
2. Пусть дано компактное топологическое пространство. Пусть в нём непустое семейство замкнутых множеств  $S_i$  такое, что любое его конечное подмножество имеет непустое пересечение. Покажите, что тогда всё семейство имеет непустое пересечение. Указание: открытое множество — это такое, дополнение которого замкнуто.
3. Докажите счётный вариант теоремы Гёделя о компактности. Пусть  $T$  — счётное полное множество замкнутых формул исчисления предикатов. Если каждое его конечное подмножество имеет модель, то и у всего  $T$  есть модель. Указание: проанализируйте теорему Гёделя о полноте исчисления предикатов.
4. Постройте универсум Эрбрана для формулы  $\forall x. \exists y. P(x, y)$  (помните, универсум Эрбрана строится для формулы в ДНФ после сколемизации).

5. Рассмотрим множество дизъюнктов исчисления высказываний  $S$ . Обозначим шаг применения правила резолюции всеми возможными способами к дизъюнктам множества  $S$  как операцию  $\mathcal{R}(S)$ . Положим  $S_0 = S$ ,  $S_{n+1} = S_n \cup \mathcal{R}(S_n)$  и  $S' = \cup S_i$ .

- (a) Покажите, что  $S'$  противоречиво (то есть для любой интерпретации  $M$  найдутся значения для свободных переменных  $d_1, \dots, d_k$  и дизъюнкт  $\delta \in S'$ , что  $M \models \delta[x_1 := d_1, \dots, x_k := d_k]$ ) тогда и только тогда, когда  $S$  противоречиво.
- (b) Покажите, что для формул исчисления высказываний  $S'$  конечно при конечном  $S$ .
- (c) Покажите, что если  $S$  противоречиво, то в  $S'$  обязательно найдутся дизъюнкты с явным противоречием ( $\beta$  и  $\neg\beta$ ).

6. Покажите, что если  $J = \{\delta_1, \neg\delta_2\}$  и  $\delta_1$  явно противоречит  $\neg\delta_2$  при некоторой подстановке свободных переменных (то есть,  $S(\delta_1) = S(\delta_2)$ ), то  $J$  также противоречива.

7. В данном задании будет необходимо проверить выводимость утверждений в исчислении предикатов с помощью метода резолюций. Продемонстрируем метод на простом примере. Докажем  $(\forall x.P(x)) \rightarrow P(0)$ .

- Возьмём отрицание:  $\neg((\forall x.P(x)) \rightarrow P(0))$ , то есть  $\neg\forall x.P(x) \vee P(0)$ , то есть  $\exists x.P(x) \& \neg P(0)$
- Проведём сколемизацию и переведём в ДНФ:  $\{P(x), \neg P(0)\}$  при свободной переменной  $x$  (по которой имеется неявный квантор всеобщности).
- Применяем правило резолюции:

$$\frac{P(x) \quad \neg P(0)}{\square} \pi = \mathcal{U}[(P(x'), P(0))]$$

- Получили пустой дизъюнкт (то есть явное противоречие), формула доказана.

Убедитесь с помощью метода резолюций, что:

- (a)  $(\forall x.P(x)) \rightarrow (\exists x.P(x))$
- (b)  $(\forall x.E(x, f(x))) \rightarrow (\forall x.\exists y.E(x, y))$
- (c)  $(\forall x.P(x) \rightarrow P(f(x))) \& P(0) \rightarrow P(f(f(f(0))))$

8. В правиле резолюции к ответу применяются унифицирующая подстановка  $\pi$  и подстановки  $\sigma_1$  и  $\sigma_2$ , заменяющие переменные в дизъюнктах на свежие. Покажите, что эти подстановки важны. А именно:

- (a) Предложите непротиворечивый набор дизъюнктов, из которого можно вывести противоречие методом резолюции, если в правиле резолюции не применять  $\pi$  к результату. Правило, иллюстрирующее проблему:

$$\frac{\varphi \vee \beta_1 \quad \neg\beta_2 \vee \psi}{\varphi \vee \psi} \pi = \mathcal{U}[\beta_1, \beta_2]$$

- (b) Предложите противоречивый набор дизъюнктов, из которого не получится вывести противоречие, если в правиле резолюции не применять  $\sigma_1/\sigma_2$  к результату. Правило, иллюстрирующее проблему:

$$\frac{\varphi \vee \beta_1 \quad \neg\beta_2 \vee \psi}{\pi(\varphi \vee \psi)} \pi = \mathcal{U}[\beta_1, \beta_2]$$

9. Покажите, что семейство  $S$  непротиворечиво тогда и только тогда, когда  $S$  с добавленным применением правила резолюции для исчисления предикатов также непротиворечиво.

10. Продемонстрируйте, как будет вести себя метод резолюций на следующем примере:  $\forall x.P(x) \rightarrow P(f(x))$