Теоретические (“малые”) домашние задания

Математическая логика, ИТМО, M3232-M3239, 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 $\Gamma \vdash \alpha \to \beta$. Например, если было показано существование вывода $A \vdash A$, то тогда теорема гарантирует и существование вывода $\vdash A \to A$.

1. Докажите:
   (a) $\vdash (A \to A \to B) \to (A \to B)$
   (b) $\vdash \neg(A \,\&\, \neg A)$
   (c) $\vdash A \,\&\, B \to B \,\&\, A$
   (d) $\vdash A \vee B \to B \vee A$
   (e) $A \,\&\, \neg A \vdash B$
2. Докажите:
   (a) $\vdash A \to \neg\neg A$
   (b) $\neg A, B \vdash \neg(A \& B)$
   (c) $\neg A, \neg B \vdash \neg(A \vee B)$
   (d) $A, \neg B \vdash \neg(A \to B)$
   (e) $\neg A, B \vdash A \to B$
3. Докажите:
   (a) $\vdash (A \to B) \to (B \to C) \to (C \to A)$
   (b) $\vdash (A \to B) \to (\neg B \to \neg A)$ *(правило контрапозиции)*
   (c) $\vdash A \,\&\, B \to \neg(\neg A \vee \neg B)$
   (d) $\vdash \neg(\neg A \vee \neg B) \to (A \,\&\, B)$
   (e) $\vdash (A \to B) \to (\neg A \vee B)$
   (f) $\vdash A \,\&\, B \to A \vee B$
   (g) $\vdash ((A \to B) \to A) \to A$ *(закон Пирса)*
4. Следует ли какая-нибудь расстановка скобок из другой: $(A \to B) \to C$ и $A \to (B \to C)$? 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», “|”): $A \mid B$ 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» ($\neg\alpha := \alpha \mid \alpha$ 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: $\neg A := A \to \perp$. 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 α и β, причём $\vdash \alpha \to \beta$ и $\nvdash \beta \to \alpha$. Укажите способ построения высказывания γ, такого, что $\vdash \alpha \to \gamma$ и $\vdash \gamma \to \beta$, причём $\nvdash \gamma \to \alpha$ и $\nvdash \beta \to \gamma$.
8. Покажите, что если $\alpha \vdash \beta$ и $\neg\alpha \vdash \beta$, то $\vdash \beta$.

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

1. Покажите, что в классическом исчислении высказываний $\Gamma \models \alpha$ влечёт $\Gamma \vdash \alpha$.
2. Покажите, что следующие высказывания не доказуемы в интуиционистской логике:
   (a) $\neg\neg A \rightarrow A$
   (b) $((A \rightarrow B) \rightarrow A) \rightarrow A$
   (c) $(A \rightarrow B) \vee (B \rightarrow A)$
   (d) $(A \rightarrow B \vee \neg B) \vee (\neg A \rightarrow B \vee \neg B)$
   (e) $\bigvee_{i=0,n-1} A_i \rightarrow A_{(i+1)\%n}$
3. Выполнены ли формулы де Моргана в интуиционистской логике? Докажите или опровергните:
   (a) $\alpha \vee \beta \vdash \neg(\neg\alpha \mathbin{\&} \neg\beta)$ и $\neg(\neg\alpha \mathbin{\&} \neg\beta) \vdash \alpha \vee \beta$
   (b) $\neg\alpha \mathbin{\&} \neg\beta \vdash \neg(\alpha \vee \beta)$ и $\neg(\alpha \vee \beta) \vdash \neg\alpha \mathbin{\&} \neg\beta$
   (c) $\alpha \rightarrow \beta \vdash \neg\alpha \vee \beta$ и $\neg\alpha \vee \beta \vdash \alpha \rightarrow \beta$
4. 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:
   (a) $\star$ — конъюнкция;
   (b) $\star$ — дизъюнкция;
   (c) $\star$ — импликация;
   (d) $\star$ — отрицание.
5. Существует несколько схожих вариантов аксиомы исключённого третьего. Не пользуясь 10 схемой аксиом, покажите следующее:
   (a) $\alpha \vee \neg\alpha, \alpha \rightarrow \neg\alpha \rightarrow \beta \vdash ((\alpha \rightarrow \beta) \rightarrow \alpha) \rightarrow \alpha$
   (b) $((\alpha \rightarrow \beta) \rightarrow \alpha) \rightarrow \alpha, \alpha \rightarrow \neg\alpha \rightarrow \beta \vdash \neg\neg\alpha \rightarrow \alpha$
6. Рассмотрим несколько моделей троичной логики. Логики похожи истинностными значениями ($V = \{-1, 0, 1\}$, истиной считаем 1) и определением большинства операций: $[\![A \mathbin{\&} B]\!] = \min([\![A]\!], [\![B]\!])$, $[\![A \vee B]\!] = \max([\![A]\!], [\![B]\!])$, $[\![\neg A]\!] = -[\![A]\!]$. 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.
   (a) Сильная логика неопределённости Клини: $[\![A \rightarrow B]\!] = [\![\neg A \vee B]\!]$.
   (b) Троичная логика Лукасевича: $[\![A \rightarrow B]\!] = \min(1, 1 - [\![A]\!] + [\![B]\!])$
   (c) Логика Гёделя G_3:
   $$[\![\neg A]\!] = \begin{cases} 1, & [\![A]\!] = -1 \\ -1, & \text{иначе} \end{cases} \qquad [\![A \rightarrow B]\!] = \begin{cases} 1, & [\![A]\!] \leqslant [\![B]\!] \\ [\![B]\!], & \text{иначе} \end{cases}$$
7. 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 — импликации, 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 $B \,\&\, A \to A \,\&\, B$.

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 $Z \to \bot$:

```
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 BHK-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) $A \to B \to A$

(b) $A \,\&\, B \to A \vee B$

(c) $(A \,\&\, (B \vee C)) \to ((A \,\&\, B) \vee (A \,\&\, C))$

(d) $(A \to C) \,\&\, (B \to C) \,\&\, A \vee B \to C$

(e) $(B \vee C \to A) \to (B \to A) \,\&\, (C \to A)$

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

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

(h) $(A \to B) \,\&\, (A \to \neg B) \to \neg A$

(i) Выразимые в интуиционистском исчислении высказываний аналоги правил де Моргана для импликации.

(j) $\bot$

Задание №3. Топология, решётки.

1. Напомним определения: *замкнутое* множество — такое, дополнение которого открыто. *Внутренностью* множества A° назовём наибольшее открытое множество, содержащееся в A. *Замыканием* множества $\overline{A}$ 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 $A^\circ = \{x | x \in A \,\&\, x$ — внутренняя точка$\}$.

   (b) Покажите, что A замкнуто тогда и только когда, когда содержит все свои граничные точки. Также покажите, что $\overline{A} = \{x \mid x$ — внутренняя или граничная точка$\}$. Верно ли, что $\overline{A} = X \setminus ((X \setminus A)^\circ)$?

   (c) Введём топологию на деревьях способом, рассмотренным на лекции. Рассмотрим некоторое множество вершин V. Опишите множества V° и $\overline{V}$. Какие вершины будут являться граничными для V?

   (d) Пусть $A \subseteq B$. Как связаны A° и B°, а также $\overline{A}$ и $\overline{B}$?

   (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 $\overline{\left(\overline{A^\circ}\right)^\circ} = \overline{A^\circ}$.

   (g) *Задача Куратовского.* Будем применять операции взятия внутренности 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.

   (a) Топология Зарисского на $\mathbb{R}$: $\Omega = \{\varnothing\} \cup \{X \subseteq \mathbb{R} \mid \mathbb{R}\backslash X$ конечно$\}$, то есть пустое множество и все множества с конечным дополнением.

   (b) Топология стрелки на $\mathbb{R}$: $\Omega = \{\varnothing, \mathbb{R}\} \cup \{(x, +\infty) | x \in \mathbb{R}\}$, то есть пустое, всё пространство и все открытые лучи.

   (c) Множество всех бесконечных подмножеств $\mathbb{R}$: $\Omega = \{\varnothing\} \cup \{X \subseteq \mathbb{R} \mid X$ бесконечно$\}$

   (d) Множество всевозможных объединений арифметических прогрессий: $A(a) = \{a \cdot x \mid x \in \mathbb{Z}\}$; $X \in \Omega$, если $X = \varnothing$ 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):

   (a) на $\mathbb{N}$ (с дискретной топологией);

   (b) в топологии Зарисского;

   (c) 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.

   (a) Покажите, что линейно связное множество всегда связно;

   (b) 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:

   (a) монотонность: пусть $a \preceq b$ и $c \preceq d$, тогда $a + c \preceq b + d$ и $a \cdot c \preceq b \cdot d$;

   (b) *законы поглощения:* $a \cdot (a + b) = a$; $a + (a \cdot b) = a$;

   (c) $a \preceq b$ выполнено тогда и только тогда, когда $a \to b = 1$;

   (d) из $a \preceq b$ следует $b \to c \preceq a \to c$ и $c \to a \preceq c \to b$;

   (e) из $a \preceq b \to c$ следует $a \cdot b \preceq c$;

   (f) $b \preceq a \to b$ и $a \to (b \to a) = 1$;

   (g) $a \to b \preceq ((a \to (b \to c)) \to (a \to c))$;

   (h) $a \preceq b \to a \cdot b$ и $a \to (b \to (a \cdot b)) = 1$

   (i) $a \to c \preceq (b \to c) \to (a + b \to c)$

   (j) 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 $(\preceq)$ — 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 $[\alpha \to \beta]_{\mathcal{L}}$ — псевдодополнение $[\alpha]_{\mathcal{L}}$ до $[\beta]_{\mathcal{L}}$.

Задание №4. Модели Крипке. Естественный вывод.

1. Опровергните формулы, построив соответствующие модели Крипке:

   (a) $\neg\neg A \to A$

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

   (c) $(A \to B \vee \neg B) \vee (\neg A \to B \vee \neg B)$

   (d) $\bigvee_{i=0,n-1} A_i \to A_{(i+1)\%n}$

2. Покажите, что любая модель Крипке обладает свойством: для любых W_i, W_j, α, если $W_i \le W_j$ и $W_i \Vdash \alpha$, то $W_j \Vdash \alpha$.

3. Несколько задач на упрощение структуры миров моделей Крипке.

   (a) Покажите, что формула опровергается моделью Крипке тогда и только тогда, когда она опровергается древовидной моделью Крипке.

   (b) 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?

   (c) 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?

4. Постройте опровержимую в ИИВ формулу, которая не может быть опровергнута моделью Крипке (ответ требуется доказать):

   (a) глубины 2 и меньше;

   (b) глубины $n \in \mathbb{N}$ и меньше.

5. Покажите аналог теоремы о дедукции для естественного вывода: $\Gamma, \alpha \vdash \beta$ тогда и только тогда, когда $\Gamma \vdash \alpha \to \beta$.

6. Определим отображение между языками вывода (гильбертов и естественный вывод):

$$|\varphi|_е = \begin{cases} |\alpha|_е \star |\beta|_е, & \varphi = \alpha \star \beta \\ |\alpha|_е \to \bot, & \varphi = \neg\alpha \\ X, & \varphi = X \end{cases} \qquad |\varphi|_г = \begin{cases} |\alpha|_г \star |\beta|_г, & \varphi = \alpha \star \beta \\ A \mathbin{\&} \neg A, & \varphi = \bot \\ X, & \varphi = X \end{cases}$$

   (a) Покажите, что $\vdash_е \alpha$ влечёт $\vdash_г |\alpha|_г$;

   (b) Покажите, что $\vdash_г \alpha$ влечёт $\vdash_е |\alpha|_е$.

7. Классическое исчисление высказываний также можно сформулировать в стиле естественного вывода, заменив правило исключения лжи на такое:

$$\frac{\Gamma, \varphi \to \bot \vdash \bot}{\Gamma \vdash \varphi} \ (\text{удал}\neg\neg)$$

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

   (a) Покажите, что если $\vdash_к \varphi$ и $A_1, \dots, A_n$ — все пропозициональные переменные из φ, то $\vdash_е A_1 \vee \neg A_1 \to A_2 \vee \neg A_2 \to \dots \to A_n \vee \neg A_n \to \varphi$.

   (b) Покажите теорему Гливенко: если $\vdash_к \varphi$, то $\vdash_е \neg\neg\varphi$.

Задание №5. Исчисление предикатов

1. Докажите (или опровергните) следующие формулы в исчислении предикатов:

   (a) $(\forall x.\phi) \to (\forall y.\phi[x := y])$, если есть свобода для подстановки y вместо x в ϕ и y не входит свободно в ϕ.

   (b) $(\exists x.\phi) \to (\exists y.\phi[x := y])$, если есть свобода для подстановки y вместо x в ϕ и y не входит свободно в ϕ.

   (c) $(\forall x.\phi) \to (\exists x.\phi)$

(d) $(\forall x.\forall x.\phi) \to (\forall x.\phi)$

(e) $(\forall x.\phi) \to (\neg\exists x.\neg\phi)$

(f) $(\exists x.\neg\phi) \to (\neg\forall x.\phi)$

(g) $(\forall x.\alpha \vee \beta) \to (\neg\exists x.\neg\alpha) \,\&\, (\neg\exists x.\neg\beta)$

(h) $((\forall x.\alpha) \vee (\forall y.\beta)) \to \forall x.\forall y.\alpha \vee \beta$. Какие условия надо наложить на переменные и формулы? Приведите контрпримеры, поясняющие необходимость условий.

(i) $(\alpha \to \beta) \to \forall x.(\alpha \to \beta)$. Возможно, нужно наложить какие-то условия на переменные и формулы? Приведите контрпримеры, поясняющие необходимость условий (если условия требуются).

2. Опровергните формулы $\phi \to \forall x.\phi$ и $(\exists x.\phi) \to (\forall x.\phi)$

3. Докажите или опровергните (каждую формулу в отдельности): $(\forall x.\exists y.\phi) \to (\exists y.\forall x.\phi)$ и $(\exists x.\forall y.\phi) \to (\forall y.\exists x.\phi)$;

4. Докажите или опровергните (каждую формулу в отдельности): $(\forall x.\exists y.\phi) \to (\exists x.\forall y.\phi)$ и $(\exists x.\forall y.\phi) \to (\forall x.\exists y.\phi)$

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:

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

   (b) Покажите, что в интуиционистском исчислении предикатов теорема Гливенко не имеет места (а именно, существует формула α, что $\vdash_{\text{к}} \alpha$, но $\nvdash_{\text{и}} \neg\neg\alpha$).

   (c) Определим операцию $(\cdot)_{\text{Ku}}$:

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

   Тогда *преобразованием Куроды* формулы φ назовём $\neg\neg(\varphi_{\text{Ku}})$. Покажите, что $\vdash_{\text{к}} \alpha$ тогда и только тогда, когда $\vdash_{\text{и}} \neg\neg(\alpha_{\text{Ku}})$.

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 α, что при $|\mathcal{M}| \leqslant n$ выполнено $[\![\alpha]\!]_{\mathcal{M}} = \text{И}$, но $\nvdash \alpha$.

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 α, что $\vdash \alpha \,\&\, \neg\alpha$; (б) существует формула α, 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 φ.

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 φ — некоторая формула и для любой формулы ζ, более короткой, чем φ, 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 ($A_{\text{внешн}} \cap A_{\text{внутр}} = \varnothing$), $\varepsilon \in A_{\text{внешн}}$, $s_{\text{нач}}, s_{\text{доп}} \in A_{\text{внутр}}$, и T — это функция переходов: $T : A_{\text{внутр}} \times A_{\text{внешн}} \to A_{\text{внутр}} \times A_{\text{внешн}} \times \{\leftarrow, \rightarrow, \cdot\}$.

Все неиспользованные клетки ленты заполнены ε, 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:

	ε	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:

$$\underline{0}11 \Rightarrow 1\underline{1}1 \Rightarrow 10\underline{1} \Rightarrow 100\underline{\varepsilon}$$

Заметьте, что на последнем шаге головка сдвинулась вправо, за заполненные клетки — оказавшись на неиспользованной, заполненной символами ε 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:

(a) 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;

(b) в строке в алфавите $\{0, 1, 2\}$ сокращающую все «постоянные» подстроки до одного символа: машина должна превратить 1022220101111 в 1020101;

(c) допускающую правильные скобочные записи (например, (()) должно допускаться, а)()(— отвергаться);

(d) допускающую строки вида $a^n b^n c^n$ в алфавите $\{a, b, c\}$ (например, строка $aabbcc$ должна допускаться, а $abbbc$ — отвергаться);

(e) 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 $0 \leqslant k < 2^n$, 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: $0 \leqslant a$ и $a' \leqslant b'$, если $a \leqslant b$. Докажите, что:

   (a) $x \leqslant x + y$;

   (b) $x \leqslant x \cdot y$ (укажите, когда это так — в остальных случаях приведите контрпримеры);

   (c) Если $a \leqslant b$ и $m \leqslant n$, то $a \cdot m \leqslant b \cdot n$;

   (d) $x \leqslant y$ 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 $0 \leqslant q < b$. 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) $a \dot{-} b \leqslant a + b$;

   (d) $a \dot{-} b = 0$ тогда и только тогда, когда $a \leqslant b$.

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

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

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

   (a) $\vdash \overline{2} \cdot \overline{3} = \overline{6}$;

   (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 ρ со свободными переменными $x_1, \dots, x_k$, что:

   - для всех $\langle a_1, \dots, a_k \rangle \in R$ выполнено $\vdash \rho[x_1 := \overline{a_1}] \dots [x_k := \overline{a_k}]$ (доказуема формула ρ 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 $\vdash \neg\rho[x_1 := \overline{a_1}] \dots [x_k := \overline{a_k}]$.

   Выразите в формальной арифметике (укажите формулу ρ 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:
   $$\textsc{le}(x,y) = \begin{cases} 1, & x \leqslant y \\ 0, & x > y \end{cases}$$

   (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 $n \geqslant 2$ найдётся простое число между n и $2n$);

   (i) частичный логарифм $\textsc{plog}_n(k) = \max\{p \mid k \vdots n^p\}$ (например, $\textsc{plog}_2(96) = 5$);

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

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

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

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

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

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 $\mathrm{SUBST}(p,q)$, заменяющую в формуле с гёделевым номером p все свободные переменные x_1 на формулу q. Тогда покажите, что формулу $\alpha_\varphi := \zeta_\varphi(\overline{\ulcorner\zeta_\varphi\urcorner})$ можно взять в качестве формулы α в лемме об автоссылках: $\vdash \varphi(\overline{\ulcorner\alpha_\varphi\urcorner}) \leftrightarrow \alpha_\varphi$.
4. Какое из условий Гильберта-Бернайса-Лёфа нарушает формула π'?
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 $Th_{\mathcal{S}}$ 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 α. 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` : $(\alpha \rightarrow$ `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) $a \uplus b$ (дизъюнктное 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 ω.
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 ω выполняется аксиоматика Пеано (полная формализация рассуждений не требуется, но из изложения должно быть понятно, как эту формализацию в рамках теории первого порядка получить):
   (a) $\forall x.x \in \omega \rightarrow \neg x' = \varnothing$
   (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 $\phi(\varnothing)$ 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) $\omega \cdot \overline{2} = \overline{2} \cdot \omega$

(b) $\omega \cdot \overline{2} = \omega + \omega$

(c) $(\omega + \overline{1})^{\overline{2}} = \omega^{\overline{2}} + \overline{2} \cdot \omega + \overline{1}$

(d) $\omega^{\omega} = (\omega^{\overline{2}})^{\omega}$

(e) $\omega^{\omega+\overline{1}} = \omega^{\omega} + \overline{1}$

(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 ω^{ω} 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 σ, что существует биекция $f : \mathbb{Q}^+ \to \sigma$, причём для всех $a, b \in \mathbb{Q}^+$ из $a \leqslant b$ следует $f(a) \leqslant f(b)$ (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 $\vdash \{a\} = \{b\} \to a = b$. 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 $a = \varnothing$;

   (b) если $|a| \leqslant |b|$, то $|\mathcal{F}(g, a)| \leqslant |\mathcal{F}(g, b)|$;

   (c) если $|a| \leqslant |b|$ и $\overline{0} < |g|$, то $|\mathcal{F}(a, g)| \leqslant |\mathcal{F}(b, g)|$;

   (d) $|\mathcal{F}(\overline{0}, a)| = \overline{1}$, $|\mathcal{F}(\overline{1}, a)| = \overline{1}$; если $|a| > 0$, то $|\mathcal{F}(a, \overline{0})| = \overline{0}$;

   (e) если $|a| \geqslant \aleph_0$ и $0 < |n| < \aleph_0$, то $|\mathcal{F}(a, n)| = a$.

6. Покажите эквивалентность следующих определений конечного множества (задание (k) предполагает доказательство импликации $(k) \to (k')$; возможно, некоторые из переходов потребуют аксиому выбора):

   (a) a конечно, если каждое непустое семейство подмножеств a имеет максимальный по включению элемент. Например, при $a = \{0, 1, 2\}$ в семействе подмножеств $\{\varnothing, \{0, 1\}, \{1, 2\}\}$ 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 $|a| = \varnothing$ или $|a| \cdot \overline{2} > |a|$.

   (e) a конечно, если $|a| = \varnothing$ или $|a| = \overline{1}$ или $|a|^2 > |a|$.

   (f) a конечно, если $|a| < \aleph_0$.

7. Покажите, что представимая функция $f : a \to b$ 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 $|\{f \mid f : \mathbb{R} \to \mathbb{R}, f \text{ — непрерывна }\}| = \beth_1$ и $|\{f \mid f : \mathbb{R} \to \mathbb{R}\}| = \beth_2$.

11. Покажите, что $|\mathbb{R}| = \beth_1$, также найдите $|\{f \mid f : \mathbb{Q} \to \mathbb{R}, f \text{ — непрерывна }\}|$ и $|\{f \mid f : \mathbb{R} \to \mathbb{Q}, f \text{ — непрерывна }\}|$.

Задание №12. Аксиома выбора

1. Фильтром $\mathcal{F}$ назовём структуру на элементах некоторой решётки $\langle L, (\preceq)\rangle$ со следующими свойствами:

   - $0 \notin \mathcal{F}$;
   - если $a, b \in \mathcal{F}$, то $a \cdot b \in \mathcal{F}$;
   - если $a \in \mathcal{F}$, $a \preceq b$, $b \in L$, то $b \in \mathcal{F}$.

   Фильтр назовём главным для $x \in L$, если $\mathcal{F} = \{a \in L \mid x \preceq a\}$. 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.

   (a) Покажите, что множество дополнений конечных множеств до бесконечного образует фильтр (в качестве отношения порядка рассмотрим отношение включения). Является ли этот фильтр ультрафильтром?

   (b) 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.

   (c) Покажите, что у любого фильтра есть содержащий его ультрафильтр (вам потребуется лемма Цорна для доказательства этого факта).

2. Покажите, что у любых двух множеств A и B их мощности сравнимы ($|A| \leqslant |B|$ или $|B| \leqslant |A|$). 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. Покажите, что если $\vdash_\infty \neg(\alpha \vee \neg\alpha)$, то $\vdash_\infty 1 = 0$.

2. Покажите $\vdash_\infty \forall a.\forall b.a + b = b + a$.

3. Постройте утверждение, доказательство которого не может иметь порядок, меньший ω.

4. 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).