Теоретические домашние задания

Математическая логика, ИТМО, M3232-M3239, осень 2025 года

О нумерации заданий: отдельным заданием считается самый вложенный занумерованный пункт (цифрой или буквой). Пункты без нумерации (если они присутствуют в условии) считаются частью одного задания.

Задание №1. Знакомство с классическим исчислением высказываний.

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) $\vdash (A \to B) \to (B \to C) \to (A \to C)$
   (b) $\vdash (A \to B) \to (\neg B \to \neg A)$ *(правило контрапозиции)*
   (c) $\vdash \neg(\neg A \,\&\, \neg B) \to (A \vee B)$ *(вариант I закона де Моргана)*
   (d) $\vdash A \vee B \to \neg(\neg A \,\&\, \neg B)$
   (e) $\vdash (\neg A \vee \neg B) \to \neg(A \,\&\, B)$ *(II закон де Моргана)*
   (f) $\vdash (A \to B) \to (\neg A \vee B)$
   (g) $\vdash A \,\&\, B \to A \vee B$
   (h) $\vdash ((A \to B) \to A) \to A$ *(закон Пирса)*
   (i) $\vdash A \vee \neg A$
   (j) $\vdash (A \,\&\, B \to C) \to (A \to B \to C)$
   (k) $\vdash A \,\&\, (B \vee C) \to (A \,\&\, B) \vee (A \,\&\, C)$ *(дистрибутивность)*
   (l) $\vdash (A \to B \to C) \to (A \,\&\, B \to C)$
   (m) $\vdash (A \to B) \vee (B \to A)$
   (n) $\vdash (A \to B) \vee (B \to C) \vee (C \to A)$
4. Покажите, что если $\alpha \vdash \beta$ и $\neg\alpha \vdash \beta$, то $\vdash \beta$.
5. Давайте вспомним, что импликация правоассоциативна: $\alpha \to \beta \to \gamma \equiv \alpha \to (\beta \to \gamma)$. Но рассмотрим иную расстановку скобок: $(\alpha \to \beta) \to \gamma$. Возможно ли доказать логическое следствие между этими вариантами расстановки скобок — и каково его направление?
6. Возможно ли, что какая-то из аксиом задаётся двумя разными схемами аксиом? Опишите все возможные коллизии для какой-то одной такой пары схем аксиом. Ответ обоснуйте (да, тут потребуется доказательство по индукции).

7. Заметим, что можно вместо отрицания ввести в исчисление ложь. Рассмотрим *исчисление высказываний с ложью.* В этом языке будет отсутствовать одноместная связка ($\neg$), вместо неё будет присутствовать нульместная связка «ложь» ($\perp$), а 9 и 10 схемы аксиом будут заменены на одну схему:

   ($9_\perp$) $\quad ((\alpha \to \perp) \to \perp) \to \alpha$

   Будем записывать доказуемость в новом исчислении как $\vdash_\perp \alpha$, а доказуемость в исчислении высказываний с отрицанием как $\vdash_\neg \beta$. Также определим операцию трансляции между языками обычного исчисления высказываний и исчисления с ложью как операции рекурсивной замены $\perp := A \,\&\, \neg A$ и $\neg\alpha := \alpha \to \perp$ (и обозначим их как $|\varphi|_\neg$ и $|\psi|_\perp$ соответственно).

   Докажите:

   (a) $\vdash_\perp \alpha$ влечёт $\vdash_\neg |\alpha|_\neg$
   (b) $\vdash_\neg \alpha$ влечёт $\vdash_\perp |\alpha|_\perp$

Задание №2. Теоремы об исчислении высказываний. Знакомство с интуиционистским исчислением высказываний.

1. Покажите, что в классическом исчислении высказываний $\Gamma \models \alpha$ влечёт $\Gamma \vdash \alpha$.

2. *Базой* топологического пространства $\langle X, \Omega\rangle$ назовём множество $\mathcal{B} \subseteq \Omega$, что $\Omega = \{\cup S \mid S \subseteq \mathcal{B}\}$ — любое открытое множество получается объединением некоторого подмножества базы. Например, для дискретной топологии $\mathcal{B} = \{\{x\} \mid x \in X\}$.

   Назовём минимальной базой топологии такую базу, что в ней никакое множество не может быть получено объединением семейства других множеств из базы.

   (a) Покажите, что топологическое пространство на вещественных числах с базой $\mathcal{B} = \{(a, b) \mid a, b \in \mathbb{R}\}$ совпадает с топологическим пространством $\mathbb{R}$ из матанализа (то есть, совпадают множества открытых множеств).
   (b) Существует ли минимальная база для топологии стрелки?
   (c) Существует ли минимальная база для топологии Зарисского (носитель — $\mathbb{R}$, открыты $\varnothing$, $\mathbb{R}$ и все множества с конечным дополнением)?

3. Заметим, что определения стараются давать как можно более узкими: если некоторое свойство вытекает из других, то это уже не свойство из определения, а теорема. Поэтому приведите примеры $\langle X, \Omega\rangle$, нарушающие только первое, только второе и только третье условие на топологию.

4. Напомним, что замкнутое множество — такое, дополнение которого открыто. Заметим, что на $\mathbb{R}$ ровно два множества одновременно открыты и замкнуты — $\varnothing$ и всё пространство. Постройте другую (не евклидову) топологию на $\mathbb{R}$, чтобы в ней было ровно четыре множества, которые одновременно открыты и замкнуты. А возможно ли построить топологическое пространство, в котором было бы ровно три открыто-замкнутых множества?

5. Предложите пример топологического пространства, в котором пересечение произвольного семейства открытых множеств — открыто. Топологическое пространство должно иметь бесконечный носитель (чтобы задача имела содержательный смысл) и не должно иметь дискретную или антидискретную топологию (не должно быть в каком-то смысле вырожденным).

6. Наибольшим (наименьшим) значением в каком-то множестве назовём такое, которое больше (меньше) всех других элементов множества. Несложно заметить, что для отношения включения множеств далеко не всегда такое можно определить: например, на $\mathbb{R}^2$ не существует наибольшего круга с радиусом 1, хотя такой круг существует на $\{z \mid z \in \mathbb{R}^2, |z| \leqslant 1\}$.

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

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

(b) Пусть $A \subseteq B$. Как связаны A° и B°, а также $\overline{A}$ и $\overline{B}$? Верно ли $(A \cap B)^\circ = A^\circ \cap B^\circ$ и $(A \cup B)^\circ = A^\circ \cup B^\circ$?

(c) *Задача Куратовского.* Будем применять операции взятия внутренности и замыкания к некоторому множеству всевозможными способами. Сколько различных множеств может всего получиться? *Указание.* Покажите, что $\overline{\left(\overline{A^\circ}\right)^\circ} = \overline{A^\circ}$.

7. Задача проверки высказываний на истинность в ИИВ сложнее, чем в КИВ. Тем не менее, если формула опровергается, то она опровергается на $\mathbb{R}$ с евклидовой топологией. Если же такого опровержения нет, то формула доказуема (то есть, ИИВ семантически полно на $\mathbb{R}$). Например, формула $A \vee \neg A$ опровергается при $[\![A]\!] = (0, +\infty)$, так как $[\![A \vee \neg A]\!] = \mathbb{R} \backslash \{0\}$.

   Очевидно, что любая интуиционистская тавтология общезначима и в классической логике:

   - формула общезначима в интуиционистской логике;
   - значит, истинна при всех оценках;
   - значит, в частности, при всех оценках на $\mathbb{R}$;
   - то есть, по теореме, упомянутой выше, доказуема в ИИВ;
   - а схема аксиом 10и — частный случай схемы аксиом 10.

   Обратное же неверно. Определите, являются ли следующие формулы тавтологиями в КИВ и ИИВ (предложите опровержение или доказательство общезначимости/выводимости для каждого из исчислений). В качестве доказательств формул приводите их натуральный вывод.

   (a) $((A \to B) \to A) \to A$;
   (b) $\neg\neg A \to A$;
   (c) $(A \to B) \vee (B \to A)$ (из двух утверждений одно непременно следует из другого: например, «я не люблю зиму» и «я не люблю лето»);
   (d) $(A \to B) \vee (B \to C)$;
   (e) $(A \to (B \vee \neg B)) \vee (\neg A \to (B \vee \neg B))$;
   (f) $\alpha \vee \beta \vdash \neg(\neg\alpha \,\&\, \neg\beta)$ и $\neg(\neg\alpha \,\&\, \neg\beta) \vdash \alpha \vee \beta$;
   (g) $\neg\alpha \,\&\, \neg\beta \vdash \neg(\alpha \vee \beta)$ и $\neg(\alpha \vee \beta) \vdash \neg\alpha \,\&\, \neg\beta$;
   (h) $\alpha \to \beta \vdash \neg\alpha \vee \beta$ и $\neg\alpha \vee \beta \vdash \alpha \to \beta$.

8. Известно, что в КИВ все связки могут быть выражены через операцию «и-не» («или-не»). Также, они могут быть выражены друг через друга (достаточно, например, отрицания и конъюнкции). Однако, в ИИВ это не так.

   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 $\vdash A \star B \to \varphi(A, B)$ и $\vdash \varphi(A, B) \to A \star B$. Покажите это для каждой связки в отдельности:

   (a) конъюнкция;
   (b) дизъюнкция;
   (c) импликация;
   (d) отрицание.

Задание №3. Изоморфизм Карри-Ховарда. Дополнительные топологические определения. Решётки.

1. 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);

2. Всегда ли непрерывным образом связного пространства является другое связное (под)пространство? Докажите или опровергните.

3. Как мы помним с лекции, возможно доказывать интуиционистские утверждения, воспользовавшись изоморфизмом Карри-Ховарда, то есть написав соответствующую программу на каком-нибудь статически типизированном языке программирования.

   Например, на C++ так можно доказать $A \to A$:

```
A identity (A x) { return x; }
```

   Докажите следующие утверждения, не пользуясь в коде тем фактом, что обычно языки программирования противоречивы (то есть, не используйте исключений, функций, не возвращающих управления, и других подобных конструкций).

   (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) $(A \to C) \to (B \to C) \to ((A \vee B) \to C)$
   (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.

4. 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.

5. 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: $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

6. Докажите, основываясь на формулах предыдущих заданий, что интуиционистское исчисление высказываний корректно, если в качестве модели выбрать алгебру Гейтинга.

7. Покажите, что на конечном множестве дистрибутивная решётка всегда импликативна.

8. Постройте пример дистрибутивной, но не импликативной решётки.

9. Покажите, что в дистрибутивной решётке всегда $a + (b \cdot c) = (a + b) \cdot (a + c)$.

10. Пусть $R \subseteq A \times A$ — отношение эквивалентности (то есть транзитивное, рефлексивное и симметричное). Тогда фактор-множество $A/_R := \{[x]_R \mid x \in A\}$ — множество *классов эквивалентности*, где $[x]_R = \{t \in A \mid tRx\}$.

    Покажите, что каждый элемент множества A принадлежит в точности одному классу эквивалентности. Два класса эквивалентности либо не пересекаются, либо совпадают.

11. Пусть $R \subseteq A \times A$ — отношение нестрогого предпорядка (транзитивное и рефлексивное). И пусть $a \approx b$, если aRb и bRa. Покажите, что
    (a) Если aRb и $a \approx a'$, $b \approx b'$, то $a'Rb'$.
    (b) $R^{\approx}$ — отношение нестрогого порядка на $A/_{\approx}$ в следующем смысле: $[a]_{\approx} R^{\approx} [b]_{\approx}$ выполнено, если aRb (корректность определения также необходимо показать).

12. Покажите, что $(\preceq)$ из определения алгебры Линденбаума — отношение нестрогого предпорядка, $(\approx)$ — отношение эквивалентности, а $(\preceq)/_{\approx}$ — отношение нестрогого порядка.

13. 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.

14. Покажите, что $[\alpha \to \beta]_{\mathcal{L}}$ — псевдодополнение $[\alpha]_{\mathcal{L}}$ до $[\beta]_{\mathcal{L}}$.

Задание №4. Модели для ИИВ

1. Определение: противоречивая теория — такая, в которой доказуема любая формула. Покажите, что для КИВ (а равно и для ИИВ) определение имеет следующие эквивалентные формулировки:
    - доказуема любая формула исчисления;
    - $\vdash \alpha \,\&\, \neg\alpha$ при некотором α;
    - $\vdash A \,\&\, \neg A$;
    - для некоторой формулы α имеет место $\vdash \alpha$ и $\vdash \neg\alpha$.

    Также покажите, что КИВ непротиворечиво (расшифруйте слово «очевидно», использованное в четвёртой лекции).

2. Опровергните формулы с помощью какой-нибудь модели Крипке:
    (a) $((A \to B) \to A) \to A$;
    (b) $(A \to B) \to \neg A \vee B$;
    (c) $(A \to (B \vee \neg B)) \vee (\neg A \to (B \vee \neg B))$.

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

4. 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 конечной 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?

5. Покажите, что модель Крипке $\mathcal{M}$ из одного узла эквивалентна классической модели. То есть, по каждой такой модели можно найти эквивалентную ей классическую модель $\mathcal{T}$, что $\models_{\mathcal{M}} \alpha$ тогда и только тогда, когда $\models_{\mathcal{T}} \alpha$. Напомним, что для задания классической модели необходимо указать значения всех пропозициональных переменных. Сохранится ли это свойство для модели, заданной на лесе несвязных узлов?

6. Покажите, что формула опровергается моделью Крипке тогда и только тогда, когда она опровергается конечной моделью Крипке.

7. Постройте опровержимую в ИИВ формулу, которая не может быть опровергнута моделью Крипке (ответ требуется доказать):
    (a) (*) глубины 0 или 1;
    (b) (*) глубины $n \in \mathbb{N}$ и меньше.

8. Давайте разберёмся во взаимоотношениях различных формулировок закона исключенного третьего и подобных законов. Для этого определим *минимальное* исчисление высказываний как ИИВ без 10 схемы аксиом. Заметим, что переход от $\vdash \neg\neg\alpha \to \alpha$ при всех α к $\vdash ((\alpha \to \beta) \to \alpha) \to \alpha$ уже был ранее доказан (закон Пирса следует из закона снятия двойного отрицания).

   Давайте продолжим строить кольцо:

$$
\begin{tikzcd}
 & \vdash ((\alpha \to \beta) \to \alpha) \to \alpha \arrow[dr, bend left] & \\
\vdash \neg\neg\alpha \to \alpha \arrow[ur, bend left] & & \vdash \alpha \vee \neg\alpha \arrow[ll, dashed, bend left, "\text{если } \vdash \alpha \to \neg\alpha \to \beta \text{ при всех } \alpha,\ \beta"]
\end{tikzcd}
$$

   для чего покажите, что в минимальном исчислении:

   (a) Если $\vdash ((\alpha \to \beta) \to \alpha) \to \alpha$ при всех α и β, то $\vdash \alpha \vee \neg\alpha$ (закон исключённого третьего следует из закона Пирса).

   (b) Если $\vdash \alpha \to \neg\alpha \to \beta$ («из лжи следует, что угодно», он же ***принцип взрыва***) и $\vdash \alpha \vee \neg\alpha$ при всех α и β, то $\vdash \neg\neg\alpha \to \alpha$.

   (c) (*) Из закона Пирса не следует закон снятия двойного отрицания и из закона исключённого третьего не следует закон Пирса.

   (d) (*) Закон Пирса и принцип взрыва независимы (невозможно доказать один из другого).

Задание №5. Исчисление предикатов

1. (Приводится по учебнику Ивлева Ю.В. «Логика», 2006 год) Определите состав, фигуру, модус силлогизма и проверьте его. Формализуйте утверждение в исчислении предикатов (пусть это будет вывод из посылок вида $\alpha, \beta \vdash \gamma$).

   (a) Некоторые учащиеся являются троечниками. Все студенты — учащиеся. Следовательно, некоторые студенты — троечники.

   (b) Каждый капитан корабля обладает громким голосом. Каждый оперный певец обладает громким голосом. Следовательно, некоторые капитаны кораблей являются оперными певцами.

   (c) Все рыбы дышат жабрами. Некоторые дышащие жабрами живут в море. Следовательно, среди обитателей моря имеются рыбы.

2. (Приводится по учебнику Ивлева Ю.В. «Логика», 2006 год) Осуществите, если это возможно, правильный вывод из следующих посылок по одной из фигур силлогизма. Формализуйте утверждение в исчислении предикатов.

   (a) Все ученые занимаются умственным трудом. Некоторые ученые не являются городскими жителями.

   (b) Некоторые верующие не имеют высшего образования. Все католики — верующие.

3. Формализуйте какой-нибудь силлогизм с «плохим» модусом (требующий условие непустоты среднего термина) в исчислении предикатов. Докажите силлогизм с условием непустоты в исчислении предикатов — и постройте контрпример к силлогизму без условия непустоты среднего термина (постройте надлежащую модель).

4. Постройте по силлогизму из двух разных модусов (сильного и слабого). Формализуйте их и постройте доказательство в исчислении предикатов, что из сильного силлогизма следует слабый (то есть заключение силлогизма сильного модуса влечёт заключение силлогизма слабого модуса при условии, что в силлогизмах совпадают предикат, субъект и средний термин; потребуется подобрать правильную пару силлогизмов). Возможно, вам тут также потребуется условие непустоты — в таком случае приведите контрпример при его отсутствии.

5. 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) $(\forall x.\phi) \to (\exists x.\phi)$ и $(\forall x.\forall x.\phi) \to (\forall x.\phi)$

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

(d) $(\forall x.\alpha \vee \beta) \to (\neg\exists x.\neg\alpha) \mathbin{\&} (\neg\exists x.\neg\beta)$

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

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

(g) $(\alpha \to \forall x.\beta) \to (\forall x.\alpha \to \beta)$ при условии, что x не входит свободно в α.

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

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

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

Задание №6. Теорема о полноте И.П.

1. Докажите теорему Гливенко: в КИВ/ИИВ, если $\vdash_{\text{к}} \varphi$, то $\vdash_{\text{и}} \neg\neg\varphi$. А также покажите *Следствие:* ИИВ противоречиво тогда и только тогда, когда противоречиво КИВ.

2. Докажите, что теорема Гливенко в такой формулировке неверна в интуиционистском исчислении предикатов (её можно переформулировать — но это не входит в данное задание).

   Указание: возможно, вам поможет следующая модель для ИИП. Докажите, что это модель ИИП, если вы пойдёте по этому пути. Пусть $\langle X, \Omega\rangle$ — некоторое топологическое пространство и $V = \Omega$ (как и в исчислении высказываний), пропозициональные связки определим аналогично топологической интерпретации И.И.В., оценки же кванторов сделать такими:

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

3. Пусть заданы какие-то дизъюнктные семейства термов без свободных переменных T_1 и T_2 (то есть $T_1 \cap T_2 = \varnothing$), а также одноместный предикатный символ P. Покажите, что семейство $\Gamma = \{P(\theta) \mid \theta \in T_1\} \bigcup \{\neg P(\theta \mid \theta \in T_2\}$ непротиворечиво.

4. Обозначим за $\sigma \leftrightarrow \zeta$ две импликации: $(\sigma \to \zeta) \mathbin{\&} (\zeta \to \sigma)$. Докажите, что $(\exists x.\varphi) \leftrightarrow ((\exists y.\varphi)[x := y])$. Какие условия надо наложить на φ, чтобы доказательства имели место? Постройте контрпримеры к ситуациям, когда условия не выполнены.

5. Попробуем наметить доказательство теоремы о переносе кванторов, рассмотрев некоторые вспомогательные леммы. Несложно заметить, что используя данные и аналогичные утверждения, возможно доказать всю теорему:

   (a) Какая формула с поверхностными кванторами будет соответствовать формуле $(\forall x.P(x)) \vee \exists y.P(y) \mathbin{\&} Q(y)$? Докажите эквивалентность.

   (b) Эквивалентность предполагает наличие двух импликаций: для внесения кванторов внутрь — или для вынесения их наружу. Для начала вынесем квантор наружу — например, для импликации: $(\forall x.\alpha) \to (\forall y.\beta)$. Как правильно вынести левый квантор, $\forall x.\forall y.\alpha \to \beta$ или $\exists x.\forall y.\alpha \to \beta$? Постройте вывод для правильного варианта, постройте контрпример для неправильного. Какие условия надо наложить на формулы α и β (при наложении условия предложите надлежащий контрпример)?

   (c) И теперь внесём квантор внутрь (например, для дизъюнкции): $(\forall x.\alpha \vee \beta) \to (\forall x.\alpha) \vee (\forall x.\beta)$. Какие условия надо наложить на формулы α и β (при наложении условия предложите обосновывающий его контрпример)?

   (d) Научимся преобразовывать выражение по частям: например, если $\alpha \to \beta$, то $(\beta \to \gamma) \to (\alpha \to \gamma)$ и $(\exists x.\alpha) \to (\exists x.\beta)$ (какие условия надо наложить на формулы α и β?).

Задание №7. Неразрешимость ИП, аксиоматика Пеано, формальная арифметика.

1. Покажите, что исчисление предикатов неполно 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 $\not\vdash \alpha$.

2. Напишите следующие программы для машины Тьюринга и продемонстрируйте их работу с помощью какого-нибудь эмулятора:

   (a) сортирующую строку в алфавите $\{0, 1\}$ (например, из 01110111 программа должна сделать 00111111); в этом и в последующих заданиях в алфавит внешних символов при необходимости можно добавить дополнительные символы;

   (b) вычитающую 1 из числа в двоичной системе (например, из 1011 программа должна сделать 1010);

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

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

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

3. Предложите метод, каким образом возможно закодировать машину Тьюринга с помощью двоичной строки. Символы алфавитов занумеруйте (чтобы не иметь сложностей с разным начертанием букв).

4. На вашем любимом языке программирования напишите программу, печатающую свой текст. Нельзя использовать рефлексию, работу с файлами и другие конструкций языка, дающие доступ к исходному коду. Данная программа (её аналог) используется в доказательстве неразрешимости задачи останова, укажите это место.

5. 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) $(a^b)^c = a^{b \cdot c}$

   (e) $(a + b) + c = a + (b + c)$

6. 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 $b > 0$.

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

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

   Например, $\overline{5} = 0'''''$. Докажите в формальной арифметике (доказательства могут использовать метаязык, но при этом из текста должно быть понятно, как выстроить полное доказательство):

(a) $\vdash \overline{2} \cdot \overline{2} = \overline{4}$;

(b) $\vdash \forall a.a \cdot 0 = 0 \cdot a$;

(c) $\vdash \forall a.a \cdot \overline{2} = a + a$;

(d) $\vdash \forall p.(\exists q.q' = p) \vee p = 0$ (единственность нуля);

8. Покажите, что в аксиоматике Пеано нет делителей нуля (нет положительных p и q, что $pq = 0$), и перенесите это доказательство в формальную арифметику: $\vdash p \cdot q = 0 \rightarrow p = 0 \vee q = 0$.

9. Покажите, что если $a \leqslant b$ (в смысле определения выше), то $\vdash \exists t.\overline{a} + t = \overline{b}$.

Задание №8. Арифметизация логики.

1. Покажите, что какой-нибудь сильный модус (кроме Barbara) в арифметизации Лейбница всегда корректен, а также что какой-нибудь слабый модус корректен, если термины непусты (и предъявите контрпример при пустых терминах).

2. Напомним, 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) «пустое» отношение $R = \varnothing$ (никакие два числа не состоят в отношении);

   (b) отношение $Z = \{\langle x, 0 \rangle \mid x \in \mathbb{N}_0\}$.

3. 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) целочисленное деление и остаток от деления;

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

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

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

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

4. Дадим следующее определение общерекурсивным функциям (отличается от того, что было на лекции): рассмотрим термы языка формальной арифметики (без арифметических операций) и назовём выражение вида $\theta_1 = \theta_1'$ уравнением. Будем говорить, что из системы уравнений E выводится уравнение $\theta_k = \theta_k'$, если оно будет получено путём применения следующих правил:

   - в любом уравнении системы можно заменить все вхождения какой-то одной переменной x на какой-то литерал $\overline{n}$;
   - если в систему входит уравнение вида $f(\overline{n_1}, \dots, \overline{n_k}) = \overline{m}$, то в любом уравнении системы можно заменить его левую часть на правую;
   - в любом уравнении можно поменять левую и правую часть равенства местами.

Функция f называется общерекурсивной, если существует конечная система уравнений E, что при фиксированных $n_1, \dots, n_k$ из неё может быть выведено $f(\overline{n_1}, \dots, \overline{n_k}) = \overline{m}$ для единственного m.

Например,

$$\begin{cases} f(x, 0) = x \\ f(x, y') = f(x, y)' \end{cases}$$

задаёт $f(x, y) = x + y$

Определите следующие функции в общерекурсивных функциях:

(a) умножение, деление;

(b) проверку числа на простоту;

(c) частичный логарифм;

(d) функцию Аккермана.

5. Покажите, что если функция общерекурсивна в смысле прошлого пункта, то она является эффективно вычислимой (предложите любую реализацию, на любом языке, сводящемся к абстрактному алгоритму).

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

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

7. 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.

8. 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 Гёделя о неполноте арифметики. Теория множеств.

1. Покажите, что омега-непротиворечивая теория непротиворечива.

2. Пусть $\zeta_\varphi(x) := \forall z.\sigma(x, x, z) \to \varphi(z)$, 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: $\vdash \varphi(\overline{\ulcorner\alpha_\varphi\urcorner}) \leftrightarrow \alpha_\varphi$.

3. Покажите, что вопрос о принадлежности формулы $\alpha(x) = \forall p.\delta(x, p) \to \neg\sigma(p)$ в доказательстве теоремы о невыразимости доказуемости к множеству $Д_\mathcal{S}$ ведёт к противоречию.

4. Задайте полный порядок на $\mathbb{Z}$ и на $\mathbb{Q}$. Стандартный порядок на вещественных числах не является полным, хотя некоторые его подмножества этим порядком вполне упорядочиваются (натуральные числа). Вполне ли упорядочены вещественные корни квадратных уравнений с натуральными коэффициентами (как подмножество $\mathbb{R}$)?

5. Является ли порядок на алгебре Линденбаума полным? Если нет, то есть ли какие-нибудь вполне упорядоченные бесконечные подмножества алгебры Линденбаума?

6. Пусть заданы списки (в любом языке программирования) $L(\alpha)$, хранящие значения типа α. Для решения задания задайте библиотеку с функциями, являющимися аналогами конструктивных аксиом теории множеств:

   - `empty` : $L(\alpha)$, строит пустой список.
   - `pair` : $(\alpha, \alpha) \to L(\alpha)$, формирует список из двух своих аргументов.
   - `flatten` : $L(L(\alpha)) \to L(\alpha)$, соединяет все списки внутри списка в один.
   - `powerset` : $L(\alpha) \to L(L(\alpha))$, делает из списка список всех возможных подсписков.

- `filter` : $(\alpha \to \texttt{bool}) \to L(\alpha) \to L(\alpha)$, выделяет из списка все элементы, соответствующие условию.

Далее, для каждого из заданий предложите доказательство существования указанных множеств в аксиоматике Цермело-Френкеля и реализацию этого доказательства с использованием библиотеки:

(a) пересечение всех элементов множества ($\bigcap a$);

(b) $a \setminus b$ (разность множеств) и $a \bigtriangleup b$ (симметрическую 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: $\{\langle p, q\rangle \mid p \in a, q \in b\}$);

(e) $\times a$ (прямое произведение дизъюнктного множества a).

7. 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 $b = d$.

8. Восполним пробелы в доказательстве существования ω:

   (a) Определите формулу $\varphi(x)$ для свойства «x — конечный ординал». Укажите замкнутый вид для формулы, задающей ординал ω.

   (b) Покажите, что ω — действительно ординал.

9. Давайте докажем некоторые свойства ординалов.

   (a) Предъявите примеры (i) транзитивного, но не вполне упорядоченного отношением $\in$ множества и (ii) вполне упорядоченного, но не транзитивного множества (задание не делится на пункты). Покажите, что ваши примеры — действительно множества в смысле аксиоматики ZF.

   (b) Покажите, что если x — ординал, то x' — тоже ординал.

   (c) Верно ли, что если x' — ординал, то x — тоже ординал?

   (d) Покажите, что любой непустой ординал содержит пустое множество.

   (e) Покажите, что если $x \in p$ и p — ординал, то либо $x' = p$, либо $x' \in p$.

   (f) Покажите, что если x и y — конечные ординалы, то $x = y$, $x \in y$ или $y \in x$ (не используйте аксиому выбора и следующую из неё аналогичную теорему с лекции).