

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 α и β , причём $\vdash \alpha \rightarrow \beta$ и $\nvdash \beta \rightarrow \alpha$. Укажите способ построения высказывания γ , 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. Логики похожи 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° 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° и \bar{V} . Какие вершины будут являться граничными для V ?
 - (d) Пусть $A \subseteq B$. Как связаны A° и B° , 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 $\mathcal{B} = \{(a, b) | a, b \in \mathbb{R}\}$.
- (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) $a \rightarrow b \leq ((a \rightarrow (b \rightarrow c)) \rightarrow (a \rightarrow c))$;
 - (х) $a \leq b \rightarrow a \cdot b$ и $a \rightarrow (b \rightarrow (a \cdot b)) = 1$;
 - (и) $a \rightarrow c \leq (b \rightarrow c) \rightarrow (a + b \rightarrow c)$;
 - (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 (\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, α , 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:

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

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

- Покажите, что если $\vdash_{\text{к}} \varphi$ и A_1, \dots, A_n — все пропозициональные переменные из φ , 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 $\vdash_{\text{к}} \varphi$, 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 ϕ и y не входит свободно в ϕ .
 - $(\exists x.\phi) \rightarrow (\exists y.\phi[x := y])$, если есть свобода для подстановки y вместо x в ϕ и y не входит свободно в ϕ .
 - $(\forall x.\phi) \rightarrow (\exists x.\phi)$

- (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 α , 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 φ 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 α , 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 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 ($A_{\text{внешн}} \cap A_{\text{внутр}} = \emptyset$), $\varepsilon \in A_{\text{внешн}}$, $s_{\text{нач}}, s_{\text{доп}} \in A_{\text{внутр}}$, 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 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:

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

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

- 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 ρ со свободными переменными x_1, \dots, x_k , что:

- (a) 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 ρ с подставленными значениями a_1, \dots, a_k вместо свободных переменных x_1, \dots, x_k);
- (b) 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 ρ и докажите требуемые свойства про неё):

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