Теоретические домашние задания

Математическая логика, ИТМО, M3232-M3239, осень 2023 года

Задание №1. Знакомство с исчислением высказываний.

Справочное изложение теории, частично разобранной на лекции.

Определение 1. *Аксиомой является любая формула исчисления высказываний, которая может быть получена из следующих схем аксиом:*

(1)	$\alpha \to \beta \to \alpha$
(2)	$(\alpha \to \beta) \to (\alpha \to \beta \to \gamma) \to (\alpha \to \gamma)$
(3)	$\alpha \to \beta \to \alpha \& \beta$
(4)	$\alpha \& \beta \to \alpha$
(5)	$\alpha \& \beta \to \beta$
(6)	$\alpha \to \alpha \vee \beta$
(7)	$\beta \to \alpha \vee \beta$
(8)	$(\alpha \to \gamma) \to (\beta \to \gamma) \to (\alpha \vee \beta \to \gamma)$
(9)	$(\alpha \to \beta) \to (\alpha \to \neg\beta) \to \neg\alpha$
(10)	$\neg\neg\alpha \to \alpha$

Определение 2. *Выводом из гипотез $\gamma_1, \ldots, \gamma_n$ назовём конечную непустую последовательность высказываний $\delta_1, \ldots, \delta_t$, для каждого из которых выполнено хотя бы что-то из списка:*

1. *высказывание является аксиомой;*
2. *высказывание получается из предыдущих по правилу Modus Ponens (то есть, для высказывания δ_i найдутся такие δ_j и δ_k, что $j, k < i$ и $\delta_k \equiv \delta_j \to \delta_i$);*
3. *высказывание является гипотезой (то есть, является одной из формул $\gamma_1, \ldots, \gamma_n$).*

Определение 3. *Будем говорить, что формула α выводится (доказывается) из гипотез $\gamma_1, \ldots, \gamma_n$ (и записывать это как $\gamma_1, \ldots, \gamma_n \vdash \alpha$), если существует такой вывод из гипотез $\gamma_1, \ldots, \gamma_n$, что последней формулой которого является формула α.*

Заметим, что доказательство формулы α — это вывод формулы α из пустого множества гипотез.

При решении заданий вам может потребоваться теорема о дедукции (будет доказана на второй лекции):

Теорема 1. $\gamma_1, \ldots, \gamma_n, \alpha \vdash \beta$ *тогда и только тогда, когда* $\gamma_1, \ldots, \gamma_n \vdash \alpha \to \beta$.

Пример использования: пусть необходимо доказать $\vdash A \to A$ — то есть доказать существование вывода формулы $A \to A$ (заметьте, так поставленное условие не требует этот вывод предъявлять, только доказать его существование). Тогда заметим, что последовательность из одной формулы A доказывает $A \vdash A$. Далее, по теореме о дедукции, отсюда следует и $\vdash A \to A$ (то есть, вывода формулы $A \to A$, не использующего гипотезы).

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) $\vdash (\neg A \vee \neg B) \to \neg(A \,\&\, B)$ *(II закон де Моргана)*

(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)*

(h) $\vdash A \vee \neg A$

(i) $\vdash (A \,\&\, B \to C) \to (A \to B \to C)$

(j) $\vdash (A \to B \to C) \to (A \,\&\, B \to C)$

(k) $\vdash (A \to B) \vee (B \to A)$

(l) $\vdash (A \to B) \vee (B \to C) \vee (C \to A)$

4. Даны высказывания α и β, причём $\vdash \alpha \to \beta$ и $\not\vdash \beta \to \alpha$. Укажите способ построения высказывания γ, такого, что $\vdash \alpha \to \gamma$ и $\vdash \gamma \to \beta$, причём $\not\vdash \gamma \to \alpha$ и $\not\vdash \beta \to \gamma$.

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

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

1. (только для очной практики) На память приведите греческий алфавит — запишите на доске в алфавитном порядке все большие и маленькие греческие буквы и назовите их.

2. 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?

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

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

5. Возможно ли, что какая-то из аксиом задаётся двумя разными схемами аксиом? Опишите все возможные коллизии, если они есть. Ответ обоснуйте (да, тут потребуется доказательство по индукции).

6. 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 $\vdash_\perp |\alpha|_\perp$

7. Изоморфизм Карри-Ховарда — соответствие между логическими исчислениями (например, 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.). Атомарным высказываниям мы сопоставим элементарные типы. Понятие же доказуемости превращается в *обитаемость* типа. Например, доказать обитаемость типа `int` возможно, предъявив значение этого типа: `5`.

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

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

доказывает $B \& A \to A \& B$. В самом деле, данные функции являются элементами соответствующих типов, поэтому их можно понимать как доказательства соответствующих типам логических выражений.

Ложь — это необитаемый тип; тип, не имеющий значений. В некоторых языках такие типы можно выписать явно. Например, в Хаскеле можно построить алгебраический тип без конструкторов:

```
data False
main = do print "Hi"
```

В других (например, в C++) эти значения можно сымитировать. Например, в одних случаях сделать параметром темплейта. Тогда, если мы никаких ограничений на этот параметр не делаем, кто-то мог бы подставить и необитаемый тип вместо этого параметра:

```
template <class Bot>
Bot (*contraposition (A a)) (A a, B b, Bot (*neg_b) (B));
```

В самом деле, $(A \to B) \to ((B \to \perp) \to (A \to \perp))$ есть частный случай высказывания $(A \to B) \to ((B \to \alpha) \to (A \to \alpha))$, которое тоже можно доказать при всех α.

В некоторых случаях можно воспользоваться конструкцией, не возвращающей управления, которая *понятна компилятору*. Например, можно так задать правило удаления лжи ($\perp \to A$):

```
template <class Bot>
A remove_bot(Bot x) { throw x; }

int a = remove_bot<int> (...);
char* b = remove_bot<char*> (...);
char(*c)() = remove_bot<char(*)()> (...);
```

В завершение теоретической части заметим, что

- логика, которая получится, если мы будем играть в эту игру честно — это уже будет не классическая логика; для неё не будут справедливы все схемы аксиом, 10 схема будет нарушаться;
- большинство языков программирования противоречивы в смысле логической теории; в частности, там можно доказать ложь. Но для того, чтобы это получилось, вам обычно требуется использовать либо инструменты обхода ограничений типовой системы (например, явные приведения типов), либо конструкции, не возвращающие управления: бесконечная рекурсия, исключения и т.п.

Докажите следующие утверждения, написав соответствующую программу на выбранном вами языке программирования, не используя противоречивости его типовой системы (кроме последнего задания). В случае C++ можно также использовать правило удаления лжи, указанное выше; для других языков при необходимости можно выделить какое-то похожее правило:

(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) $(A \to B \to C) \to ((A \& B) \to C)$
(j) $\neg(A \vee B) \to (\neg A \& \neg B)$ и $(\neg A \& \neg B) \to \neg(A \vee B)$
(k) Одно из двух утверждений: $(A \to B) \to \neg A \vee B$ или $\neg A \vee B \to (A \to B)$. Сразу заметим, что оставшееся утверждение доказать без использования противоречивости языка не получится.
(l) $\perp$ (любым доступным в языке способом)

Для зачёта по пункту условия требуется написать код программы и продемонстрировать его работу на компьютере. Если вы желаете получить дополнительные 0.5 балла за оформление в Тех-е, вам потребуется оформить в Тех-е исходный код программы (подсказка: для языков программирования могут существовать специальные пакеты для красивого оформления кода).

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) (i) Покажите, что A открыто тогда и только тогда, когда все точки A — внутренние. Также покажите, что $A^\circ = \{x | x \in A \;\&\; x \text{ — внутренняя точка}\}$; (ii) Покажите, что A замкнуто тогда и только когда, когда содержит все свои граничные точки. Также покажите, что $\overline{A} = \{x \mid x \text{ — внутренняя или граничная точка}\}$. (iii) 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 $\overline{\left(\overline{A^\circ}\right)^\circ} = \overline{A^\circ}$.

2. Напомним, что евклидовой топологией называется топология на $\mathbb{R}$ с базой $\mathcal{B} = \{(a, b) \mid a, b \in \mathbb{R}\}$. Связны ли $\mathbb{Q}$ и $\mathbb{R} \backslash \mathbb{Q}$ как топологические подпространства $\mathbb{R}$?

3. Примеры топологий. Для каждого из примеров ниже проверьте, задано ли в нём топологическое пространство, и ответьте на следующие вопросы, если это так: (а) каковы окрестности точек в данной топологии; (б) каковы замкнутые множества в данной топологии; (в) связно ли данное пространство.

   Единица оценивания в этой задаче — ответ на все вопросы, приведённые выше, для одной из топологий:

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

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

   (c) Множество всевозможных объединений арифметических прогрессий: $A(a, b) = \{a \cdot x + b \mid x \in \mathbb{Z}\}$ при $a > 0, b \in \mathbb{R}$; $X \in \Omega$, если $X = \varnothing$ или $X = \bigcup_i A(a_i, b_i)$.

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): (i) на $\mathbb{N}$ (с дискретной топологией); (ii) в топологии Зарисского.

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. Покажите, что линейно связное множество всегда связно, но связное не обязательно линейно связное.

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

7. Пусть дано компактное топологическое пространство. Пусть в нём непустое семейство замкнутых множеств S_i такое, что любое его конечное подмножество имеет непустое пересечение. Покажите, что тогда всё семейство имеет непустое пересечение. Указание: открытое множество — это такое, дополнение которого замкнуто.

8. 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.

9. Покажите следующие свойства импликативных решёток:

   (a) (i) *монотонность:* пусть $a \le b$ и $c \le d$, тогда $a + c \le b + d$ и $a \cdot c \le b \cdot d$; (ii) *законы поглощения:* $a \cdot (a + b) = a$; $a + (a \cdot b) = a$; (iii) $a \le b$ выполнено тогда и только тогда, когда $a \to b = 1$;

(b) (i) из $a \le b$ следует $b \to c \le a \to c$ и $c \to a \le c \to b$; (ii) из $a \le b \to c$ следует $a \cdot b \le c$;

(c) (i) $b \le a \to b$ и $a \to (b \to a) = 1$; (ii) $a \to b \le ((a \to (b \to c)) \to (a \to c))$;

(d) (i) $a \le b \to a \cdot b$ и $a \to (b \to (a \cdot b)) = 1$; (ii) $a \to c \le (b \to c) \to (a + b \to c)$

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

11. *Подрешёткой* назовём замкнутое относительно операций $(+)$ и $(\cdot)$ подмножество элементов исходной решётки (отношение порядка на подрешётке — сужение исходного отношения подрядка). Покажите, что решётка дистрибутивна тогда и только тогда, когда у неё нет подрешётки, являющейся пентагоном или диамантом.

12. Покажите, что на конечном множестве дистрибутивная решётка всегда импликативна. Постройте пример дистрибутивной, но не импликативной решётки.

13. Покажите, что импликативная решётка всегда дистрибутивна, и что в дистрибутивной решётке всегда $a + (b \cdot c) = (a + b) \cdot (a + c)$.

Задание №4. Модели для ИИВ

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

   Также покажите, что КИВ непротиворечиво (расшифруйте слово «очевидно» с первого слайда лекции).

2. Напомним, что ИИВ полно относительно алгебр Гейтинга. То есть, если формула не доказуема в ИИВ, то найдётся алгебра Гейтинга и оценка переменных, при которой оценка формулы не равна 1. Более того, возможно доказать, что ИИВ полно в $\mathbb{R}$. Например, формула $A \vee \neg A$:

$$[\![A \vee \neg A]\!]^{A:=(-\infty,0)} = (-\infty, 0) \cup (0, \infty) \neq \mathbb{R}$$

   Покажите, что следующие доказуемые в КИВ высказывания не доказуемы в ИИВ: (i) обосновав их в КИВ, (ii) построив некоторое топологическое пространство X и дав значения переменным, при которых оценка высказывания не равна 1_X, и (iii) построив опровергающую высказывания модель Крипке:

   (a) $\neg\neg A \to A$ *(Закон снятия двойного отрицания)*

   (b) $((A \to B) \to A) \to A$ *(Закон Пирса)*

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

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

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

3. Существуют ли формулы, доказуемые в КИВ, но не в ИИВ, которые бы опровергались:

   (a) в топологии стрелки;

   (b) в топологии Зарисского?

4. Выполнены ли формулы де Моргана в интуиционистской логике? Докажите или опровергните:

   (a) $\alpha \vee \beta \vdash \neg(\neg\alpha \,\&\, \neg\beta)$ и $\neg(\neg\alpha \,\&\, \neg\beta) \vdash \alpha \vee \beta$

   (b) $\neg\alpha \,\&\, \neg\beta \vdash \neg(\alpha \vee \beta)$ и $\neg(\alpha \vee \beta) \vdash \neg\alpha \,\&\, \neg\beta$

   (c) $\alpha \to \beta \vdash \neg\alpha \vee \beta$ и $\neg\alpha \vee \beta \vdash \alpha \to \beta$

5. 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.

6. 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 $W_j \Vdash \alpha$.

7. 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?

8. 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.

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

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

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

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

6. 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 $\vdash_{\text{и}} \neg\neg(\alpha_{\text{Ku}})$.

7. 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 №6-7. Теоремы об исчислении предикатов, аксиоматика Пеано, формальная арифметика.

1. 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 $\varphi \equiv \alpha \vee \beta$, $\mathcal{M} \models \alpha \vee \beta$, то $\alpha \vee \beta \in M$; и если $\mathcal{M} \not\models \alpha \vee \beta$, то $\alpha \vee \beta \notin M$;

   (b) если $\varphi \equiv \neg\alpha$, $\mathcal{M} \models \neg\alpha$, то $\neg\alpha \in M$; и если $\mathcal{M} \not\models \neg\alpha$, то $\neg\alpha \notin M$.

2. 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: $T : A_{\text{внутр}} \times A_{\text{внешн}} \to A_{\text{внутр}} \times A_{\text{внешн}} \times \{\leftarrow, \to, \cdot\}$.

   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) складывающую два числа на ленте, записанные в двоичной системе счисления через разделитель (знак плюса);

(f) 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).

3. 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).

4. 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.

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. 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 $a \leqslant b$.