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 $\gamma_1, \dots, \gamma_n$ назовём конечную непустую последовательность высказываний $\delta_1, \dots, \delta_t$, 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 $\gamma_1, \dots, \gamma_n$).*

Определение 3. *Будем говорить, что формула α выводится (доказывается) из гипотез $\gamma_1, \dots, \gamma_n$ (и записывать это как $\gamma_1, \dots, \gamma_n \vdash \alpha$), если существует такой вывод из гипотез $\gamma_1, \dots, \gamma_n$, 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. $\gamma_1, \dots, \gamma_n, \alpha \vdash \beta$ *тогда и только тогда, когда* $\gamma_1, \dots, \gamma_n \vdash \alpha \to \beta$.

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 $\nvdash \beta \to \alpha$. Укажите способ построения высказывания γ, такого, что $\vdash \alpha \to \gamma$ и $\vdash \gamma \to \beta$, причём $\nvdash \gamma \to \alpha$ и $\nvdash \beta \to \gamma$.

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 Tex-е, вам потребуется оформить в Tex-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 $a + (b \cdot c) = (a + b) \cdot (a + c)$.