Теоретические домашние задания

Математическая логика, ИТМО, M3232-M3239, осень 2024 года

Общие замечания

1. Одно задание оценивается в 3.5 балла. При использовании TeX или Typst для оформления задание оценивается в 4 балла. При крайне плохом оформлении оценка может быть понижена до 3 баллов.
2. Заданием (по умолчанию) считается один пункт, занумерованный цифрой или буквой. Пункты без нумерации считаются частями одного задания.
3. Курс можно условно разделить на три части (исчисления высказываний и предикатов, формальная арифметика, теория множеств). В каждой из частей можно ответить не более четырёх заданий.

Задание №1. Знакомство с классическим исчислением высказываний.

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, существование вывода формулы $A \to A$, не использующего гипотезы).

Теорема будет доказана конструктивно: будет предъявлен алгоритм, перестраивающий вывод $\gamma_1, \dots, \gamma_n, \alpha \vdash \beta$ в вывод $\gamma_1, \dots, \gamma_n \vdash \alpha \to \beta$

1. Докажите:
   (a) $\vdash (A \to A \to B) \to (A \to B)$
   (b) $\vdash \neg(A \mathbin{\&} \neg A)$
   (c) $\vdash A \mathbin{\&} B \to B \mathbin{\&} A$
   (d) $\vdash A \vee B \to B \vee A$
   (e) $A \mathbin{\&} \neg A \vdash B$
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) $\vdash \neg(\neg A \mathbin{\&} \neg B) \to (A \vee B)$ *(вариант I закона де Моргана)*
   (d) $\vdash A \vee B \to \neg(\neg A \mathbin{\&} \neg B)$
   (e) $\vdash (\neg A \vee \neg B) \to \neg(A \mathbin{\&} B)$ *(II закон де Моргана)*
   (f) $\vdash (A \to B) \to (\neg A \vee B)$
   (g) $\vdash A \mathbin{\&} B \to A \vee B$
   (h) $\vdash ((A \to B) \to A) \to A$ *(закон Пирса)*
   (i) $\vdash A \vee \neg A$
   (j) $\vdash (A \mathbin{\&} B \to C) \to (A \to B \to C)$

(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. 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 $\vdash \beta$.

6. Покажите, что классическое исчисление высказываний допускает правило Modus Tollens:

$$\frac{\varphi \to \psi \qquad \neg\psi}{\neg\varphi}$$

А именно, пусть дан некоторый вывод, в котором каждая формула — либо аксиома, либо получена по правилу Modus Ponens, либо имеет вид $\delta_n \equiv \neg\varphi$, причём ранее в доказательстве встречается $\delta_i \equiv \neg\psi$ и $\delta_j \equiv \varphi \to \psi$ (при этом $\max(i, j) < n$). Тогда такой вывод можно перестроить в корректное доказательство в классическом исчислении высказываний.

В данном задании от вас требуется аккуратное изложение доказательства, видимо, использующее математическую индукцию. То есть, чётко сформулированное индукционное предположение и полные доказательства базы и перехода.

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

1. 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? Зависит ли это от варианта исчисления (классическое/интуиционистское)?

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

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

4. 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).

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

6. 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).

7. Покажите, что дискретная топология, антидискретная топология (открыты только $\varnothing$ и X), топология стрелки, топология Зарисского (носитель — $\mathbb{R}$, открыты $\varnothing$, $\mathbb{R}$ и все множества с конечным дополнением) являются топологиями.

8. 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.

9. 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?

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

    (a) Постройте минимальную базу для дискретной топологии.

    (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)?

11. 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).

12. 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. Покажите, что внутренность множества всегда определена.

13. Напомним определения: *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 $\overline{A} = \{x \mid x \text{ — внутренняя или граничная точка}\}$.
    - 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 $\overline{\left(\overline{A^\circ}\right)^\circ} = \overline{A^\circ}$.

14. Задача проверки высказываний на истинность в ИИВ сложнее, чем в КИВ — не существует конечного набора значений, на которых можно проверить формулу, чтобы определить её истинность (мы эту теорему докажем). 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):

(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 $\neg\alpha \vee \beta \vdash \alpha \to \beta$.

15. 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. Докажите, что функция $f : \mathbb{R} \to \mathbb{R}$ непрерывна тогда и только тогда, когда $\lim_{x \to x_0} f(x) = f(x_0)$ для всех $x_0 \in \mathbb{R}$.

3. Связным множеством в топологическом пространстве назовём такое, которое связно как подпространство. Линейно связным множеством назовём такое, в котором две произвольные точки могут быть соединены путём, образ которого целиком лежит в множестве.

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

    (b) Покажите, что связное не обязательно линейно связное.

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

5. 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) $(A \to C) \& (B \to C) \& (A \vee B) \to C$
(e) $(B \vee C \to A) \to (B \to A) \& (C \to A)$
(f) $(A \to B) \to (\neg B \to \neg A)$
(g) $((A \to B) \to C) \to (A \to (B \to C))$
(h) $(A \to B) \& (A \to \neg B) \to \neg A$
(i) Выразимые в интуиционистском исчислении высказываний аналоги правил де Моргана для импликации.

6. 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.

7. Покажите следующие утверждения для импликативных решёток:

   (a) монотонность: пусть $a \le b$ и $c \le d$, тогда $a + c \le b + d$ и $a \cdot c \le b \cdot d$;
   (b) *законы поглощения:* $a \cdot (a + b) = a$; $a + (a \cdot b) = a$;
   (c) $a \le b$ выполнено тогда и только тогда, когда $a \to b = 1$;
   (d) из $a \le b$ следует $b \to c \le a \to c$ и $c \to a \le c \to b$;
   (e) из $a \le b \to c$ следует $a \cdot b \le c$;
   (f) $b \le a \to b$ и $a \to (b \to a) = 1$;
   (g) $a \to b \le ((a \to (b \to c)) \to (a \to c))$;
   (h) $a \le b \to a \cdot b$ и $a \to (b \to (a \cdot b)) = 1$
   (i) $a \to c \le (b \to c) \to (a + b \to c)$
   (j) импликативная решётка дистрибутивна: $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

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

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

10. Постройте пример дистрибутивной, но не импликативной решётки.

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

12. 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.

13. 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).

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

15. 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.

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

Задание №4. Модели для ИИВ

В этих задачах вводится ранжирование задач по сложности. Простые задачи будут оцениваться в 3.5 балла, как раньше, а сложные задачи в 5.5 баллов. Сложные задачи отмечены звёздочкой.

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» с первого слайда 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 $W_i \le W_j$ 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:

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

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).