

**ТЕОРЕТИЧЕСКИЕ ДОМАШНИЕ ЗАДАНИЯ**  
*Математическая логика, ИТМО, М3232-М3239, осень 2024 года*

## Общие замечания

1. Одно задание оценивается в 3.5 балла. При использовании TeX или Turst 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  $\gamma_1, \dots, \gamma_n \vdash \alpha \rightarrow \beta$ .

Пример использования: пусть необходимо доказать  $\vdash A \rightarrow A$  — то есть доказать существование вывода формулы  $A \rightarrow A$  (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  $\vdash A \rightarrow A$  (то есть, существование вывода формулы  $A \rightarrow A$ , не использующего гипотезы).

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

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)  $\vdash (A \rightarrow B) \rightarrow (B \rightarrow C) \rightarrow (A \rightarrow C)$
- (b)  $\vdash (A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$  (правило контрапозиции)
- (c)  $\vdash \neg(\neg A \& \neg B) \rightarrow (A \vee B)$  (вариант I закона де Моргана)
- (d)  $\vdash A \vee B \rightarrow \neg(\neg A \& \neg B)$
- (e)  $\vdash (\neg A \vee \neg B) \rightarrow \neg(A \& B)$  (II закон де Моргана)
- (f)  $\vdash (A \rightarrow B) \rightarrow (\neg A \vee B)$
- (g)  $\vdash A \& B \rightarrow A \vee B$
- (h)  $\vdash ((A \rightarrow B) \rightarrow A) \rightarrow A$  (закон Пирса)
- (i)  $\vdash A \vee \neg A$
- (j)  $\vdash (A \& B \rightarrow C) \rightarrow (A \rightarrow B \rightarrow C)$

- (k)  $\vdash A \& (B \vee C) \rightarrow (A \& B) \vee (A \& C)$  (дистрибутивность)  
 (l)  $\vdash (A \rightarrow B \rightarrow C) \rightarrow (A \& B \rightarrow C)$   
 (m)  $\vdash (A \rightarrow B) \vee (B \rightarrow A)$   
 (n)  $\vdash (A \rightarrow B) \vee (B \rightarrow C) \vee (C \rightarrow A)$

4. Даны высказывания  $\alpha$  и  $\beta$ , причём  $\vdash \alpha \rightarrow \beta$  и  $\nvdash \beta \rightarrow \alpha$ . Укажите способ построения высказывания  $\gamma$ , такого, что  $\vdash \alpha \rightarrow \gamma$  и  $\vdash \gamma \rightarrow \beta$ , причём  $\nvdash \gamma \rightarrow \alpha$  и  $\nvdash \beta \rightarrow \gamma$ .
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:

$$\frac{\varphi \rightarrow \psi \quad \neg\psi}{\neg\varphi}$$

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  $\delta_j \equiv \varphi \rightarrow \psi$  (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:  $\alpha \rightarrow \beta \rightarrow \gamma \equiv \alpha \rightarrow (\beta \rightarrow \gamma)$ . Но рассмотрим иную расстановку скобок:  $(\alpha \rightarrow \beta) \rightarrow \gamma$ . 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:

$$(9_{\perp}) \quad ((\alpha \rightarrow \perp) \rightarrow \perp) \rightarrow \alpha$$

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  $\neg\alpha := \alpha \rightarrow \perp$  (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  $\emptyset$  и  $X$ ), топология стрелки, топология Зарисского (носитель —  $\mathbb{R}$ , открыты  $\emptyset$ ,  $\mathbb{R}$  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 —  $\emptyset$  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.
- Постройте минимальную базу для дискретной топологии.
  - Существует ли минимальная база для топологии стрелки?
  - Существует ли минимальная база для топологии Зарисского (носитель —  $\mathbb{R}$ , открыты  $\emptyset$ ,  $\mathbb{R}$  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  $\{z \mid z \in \mathbb{R}^2, |z| \leq 1\}$ .
- Внутренностью* множества  $A^\circ$  назовём наибольшее открытое множество, содержащееся в  $A$ . Покажите, что внутренность множества всегда определена.
13. Напомним определения: *замкнутое* множество — такое, дополнение которого открыто. *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.
- Покажите, что  $A$  открыто тогда и только тогда, когда все точки  $A$  — внутренние. Также покажите, что  $A^\circ = \{x \mid x \in A \text{ \& } x \text{ — внутренняя точка}\}$ ;
    - Покажите, что  $A$  замкнуто тогда и только тогда, когда содержит все свои граничные точки. Также покажите, что  $\bar{A} = \{x \mid x \text{ — внутренняя или граничная точка}\}$ .
    - Верно ли, что  $\bar{A} = X \setminus ((X \setminus A)^\circ)$ ?
  - Пусть  $A \subseteq B$ . Как связаны  $A^\circ$  и  $B^\circ$ , а также  $\bar{A}$  и  $\bar{B}$ ? Верно ли  $(A \cap B)^\circ = A^\circ \cap B^\circ$  и  $(A \cup B)^\circ = A^\circ \cup B^\circ$ ?
  - Задача Куратовского.* Будем применять операции взятия внутренней и замыкания к некоторому множеству всевозможными способами. Сколько различных множеств может всего получиться? *Указание.* Покажите, что  $(\bar{A}^\circ)^\circ = \bar{A}^\circ$ .
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  $\llbracket A \rrbracket = (0, +\infty)$ , так как  $\llbracket A \vee \neg A \rrbracket = \mathbb{R} \setminus \{0\}$ .

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)  $((A \rightarrow B) \rightarrow A) \rightarrow A$ ;
  - (b)  $\neg\neg A \rightarrow A$ ;
  - (c)  $(A \rightarrow B) \vee (B \rightarrow A)$  (из двух утверждений одно непременно следует из другого: например, «я не люблю зиму» и «я не люблю лето»);
  - (d)  $(A \rightarrow B) \vee (B \rightarrow C)$ ;
  - (e)  $(A \rightarrow (B \vee \neg B)) \vee (\neg A \rightarrow (B \vee \neg B))$ ;
  - (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)  $\alpha \rightarrow \beta \vdash \neg\alpha \vee \beta$  и  $\neg\alpha \vee \beta \vdash \alpha \rightarrow \beta$ .
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  $\vdash A \star B \rightarrow \varphi(A, B)$  и  $\vdash \varphi(A, B) \rightarrow A \star B$ . Покажите это для каждой связки в отдельности:
- (a) конъюнкция;
  - (b) дизъюнкция;
  - (c) импликация;
  - (d) отрицание.

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

- 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);
- Докажите, что функция  $f : \mathbb{R} \rightarrow \mathbb{R}$  непрерывна тогда и только тогда, когда  $\lim_{x \rightarrow x_0} f(x) = f(x_0)$  для всех  $x_0 \in \mathbb{R}$ .
- 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.
- Всегда ли непрерывным образом связного пространства является другое связное (под)пространство? Докажите или опровергните.
- 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  $A \rightarrow A$ :

```
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)  $A \rightarrow B \rightarrow A$
  - (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.
6. Рассмотрим подмножество частично упорядоченного множества, и рассмотрим следующие свойства:
- (a) 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  $a \leq b$  и  $c \leq d$ , тогда  $a + c \leq b + d$  и  $a \cdot c \leq b \cdot d$ ;
  - (b) законы поглощения:  $a \cdot (a + b) = a$ ;  $a + (a \cdot b) = a$ ;
  - (c)  $a \leq b$  выполнено тогда и только тогда, когда  $a \rightarrow b = 1$ ;
  - (d) из  $a \leq b$  следует  $b \rightarrow c \leq a \rightarrow c$  и  $c \rightarrow a \leq c \rightarrow b$ ;
  - (e) из  $a \leq b \rightarrow c$  следует  $a \cdot b \leq c$ ;
  - (f)  $b \leq a \rightarrow b$  и  $a \rightarrow (b \rightarrow a) = 1$ ;
  - (g)  $a \rightarrow b \leq ((a \rightarrow (b \rightarrow c)) \rightarrow (a \rightarrow c))$ ;
  - (h)  $a \leq b \rightarrow a \cdot b$  и  $a \rightarrow (b \rightarrow (a \cdot b)) = 1$
  - (i)  $a \rightarrow c \leq (b \rightarrow c) \rightarrow (a + b \rightarrow c)$
  - (j) импликативная решётка дистрибутивна:  $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$
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  $(\leq)$  из определения алгебры Линденбаума — отношение нестрогого предпорядка,  $(\approx)$  — отношение эквивалентности, а  $(\leq)/\approx$  — 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  $[\alpha \rightarrow \beta]_{\mathcal{L}}$  — 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  $\alpha$ ;
- $\vdash A \ \& \ \neg A$ ;
- для некоторой формулы  $\alpha$  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)  $((A \rightarrow B) \rightarrow A) \rightarrow A$ ;
- (b)  $(A \rightarrow B) \rightarrow \neg A \vee B$ ;
- (c)  $(A \rightarrow (B \vee \neg B)) \vee (\neg A \rightarrow (B \vee \neg B))$ .

3. Покажите, что любая модель Крипке обладает свойством: для любых  $W_i, W_j, \alpha$ , если  $W_i \leq W_j$  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 исключённого третьего и подобных законов. Для этого определим *минимальное* исчисление высказываний как ИИВ без 10 схемы аксиом. Заметим, что переход от  $\vdash \neg\neg\alpha \rightarrow \alpha$  при всех  $\alpha$  к  $((\alpha \rightarrow \beta) \rightarrow \alpha) \rightarrow \alpha$  уже был ранее доказан (закон Пирса следует из закона снятия двойного отрицания).

Давайте продолжим строить кольцо:



для чего покажите, что в минимальном исчислении:

- (a) Если  $\vdash ((\alpha \rightarrow \beta) \rightarrow \alpha) \rightarrow \alpha$  при всех  $\alpha$  и  $\beta$ , то  $\vdash \alpha \vee \neg \alpha$  (закон исключённого третьего следует из закона Пирса).
- (b) Если  $\vdash \alpha \rightarrow \neg \alpha \rightarrow \beta$  («из лжи следует, что угодно», он же *принцип взрыва*) и  $\vdash \alpha \vee \neg \alpha$  при всех  $\alpha$  и  $\beta$ , то  $\vdash \neg \neg \alpha \rightarrow \alpha$ .
- (c) (\*) Из закона Пирса не следует закон снятия двойного отрицания и из закона исключённого третьего не следует закон Пирса.
- (d) (\*) Закон Пирса и принцип взрыва независимы (невозможно доказать один из другого).

## Задание №5. Исчисление предикатов

1. (Приводится по учебнику Ивлева Ю.В. «Логика», 2006 год) Определите состав, фигуру, модус силлогизма и проверьте его. Формализуйте утверждение в исчислении предикатов (пусть это будет вывод из посылок вида  $\alpha, \beta \vdash \gamma$ ).
  - (a) Некоторые учащиеся являются троечниками. Все студенты — учащиеся. Следовательно, некоторые студенты — троечники.
  - (b) Каждый капитан корабля обладает громким голосом. Каждый оперный певец обладает громким голосом. Следовательно, некоторые капитаны кораблей являются оперными певцами.
  - (c) Все рыбы дышат жабрами. Некоторые дышащие жабрами живут в море. Следовательно, среди обитателей моря имеются рыбы.
2. (Приводится по учебнику Ивлева Ю.В. «Логика», 2006 год) Осуществите, если это возможно, правильный вывод из следующих посылок по одной из фигур силлогизма. Формализуйте утверждение в исчислении предикатов.
  - (a) Все ученые занимаются умственным трудом. Некоторые ученые не являются городскими жителями.
  - (b) Некоторые верующие не имеют высшего образования. Все католики — верующие.
3. Формализуйте какой-нибудь силлогизм с «плохим» модусом (требующий условие непустоты среднего термина) в исчислении предикатов. Докажите силлогизм с условием непустоты в исчислении предикатов — и постройте контрпример к силлогизму без условия непустоты среднего термина (постройте надлежащую модель).
4. Постройте по силлогизму из двух разных модусов (сильного и слабого). Формализуйте их и постройте доказательство в исчислении предикатов, что из сильного силлогизма следует слабый (то есть заключение силлогизма сильного модуса влечёт заключение силлогизма слабого модуса при условии, что в силлогизмах совпадают предикат, субъект и средний термин; потребуется подобрать правильную пару силлогизмов). Возможно, вам тут также потребуется условие непустоты — в таком случае приведите контрпример при его отсутствии.
5. Докажите (или опровергните) следующие формулы в исчислении предикатов:
  - (a)  $(\forall x.\phi) \rightarrow (\forall y.\phi[x := y])$ , если есть свобода для подстановки  $y$  вместо  $x$  в  $\phi$  и  $y$  не входит свободно в  $\phi$ .
  - (b)  $(\forall x.\phi) \rightarrow (\exists x.\phi)$  и  $(\forall x.\forall x.\phi) \rightarrow (\forall x.\phi)$
  - (c)  $(\forall x.\phi) \rightarrow (\neg \exists x.\neg \phi)$  и  $(\exists x.\neg \phi) \rightarrow (\neg \forall x.\phi)$
  - (d)  $(\forall x.\alpha \vee \beta) \rightarrow (\neg \exists x.\neg \alpha) \ \& \ (\neg \exists x.\neg \beta)$
  - (e)  $((\forall x.\alpha) \vee (\forall y.\beta)) \rightarrow \forall x.\forall y.\alpha \vee \beta$ . Какие условия надо наложить на переменные и формулы? Приведите контрпримеры, поясняющие необходимость условий.
  - (f)  $(\alpha \rightarrow \beta) \rightarrow \forall x.(\alpha \rightarrow \beta)$ . Возможно, нужно наложить какие-то условия на переменные и формулы? Приведите контрпримеры, поясняющие необходимость условий (если условия требуются).
  - (g)  $(\alpha \rightarrow \forall x.\beta) \rightarrow (\forall x.\alpha \rightarrow \beta)$  при условии, что  $x$  не входит свободно в  $\alpha$ .
6. Опровергните формулы  $\phi \rightarrow \forall x.\phi$  и  $(\exists x.\phi) \rightarrow (\forall x.\phi)$
7. Докажите или опровергните (каждую формулу в отдельности):  $(\forall x.\exists y.\phi) \rightarrow (\exists y.\forall x.\phi)$  и  $(\exists x.\forall y.\phi) \rightarrow (\forall y.\exists x.\phi)$ ;
8. Докажите или опровергните (каждую формулу в отдельности):  $(\forall x.\exists y.\phi) \rightarrow (\exists x.\forall y.\phi)$  и  $(\exists x.\forall y.\phi) \rightarrow (\forall x.\exists y.\phi)$

## Задание №6. Теорема о полноте И.П.

1. Докажите теорему Гливенко: в КИВ/ИИВ, если  $\vdash_K \varphi$ , то  $\vdash_{\text{И}} \neg\neg\varphi$ . А также покажите *Следствие*: ИИВ противоречиво тогда и только тогда, когда противоречиво КИВ.
2. Докажите, что теорема Гливенко неверна в интуиционистском исчислении предикатов.

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

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

3. Для построения аналога теоремы Гливенко определим операцию  $(\cdot)_{\text{Ку}}$ :

$$(\varphi \star \psi)_{\text{Ку}} = \varphi_{\text{Ку}} \star \psi_{\text{Ку}}, \quad (\forall x. \varphi)_{\text{Ку}} = \forall x. \neg\neg\varphi_{\text{Ку}}, \quad (\exists x. \varphi)_{\text{Ку}} = \exists x. \varphi_{\text{Ку}}$$

Тогда *преобразованием Куроды* формулы  $\varphi$  назовём  $\neg\neg(\varphi_{\text{Ку}})$ . Покажите, что  $\vdash_K \alpha$  тогда и только тогда, когда  $\vdash_{\text{И}} \neg\neg(\alpha_{\text{Ку}})$ .

4. Пусть задано какое-то семейство термов без свободных переменных  $T$  и одноместный предикатный символ  $P$ . Покажите, что семейство  $\Gamma = \{P(\theta) \mid \theta \in T\}$  непротиворечиво (семейство всех формул подобного вида). Скажем, пример с лекции непротиворечив:  $\Gamma = \{P(1), P(2), P(3), \dots\}$
5. Пусть  $M$  — полное 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  $\varphi$  — некоторая формула и для любой формулы  $\zeta$ , более короткой, чем  $\varphi$ , выполнено  $\mathcal{M} \models \zeta$  тогда и только тогда, когда  $\zeta \in M$ , тогда покажите:
  - (а) 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  $\alpha \vee \beta \notin M$ ;
  - (б) если  $\varphi \equiv \neg\alpha$ ,  $\mathcal{M} \models \neg\alpha$ , то  $\neg\alpha \in M$ ; и если  $\mathcal{M} \not\models \neg\alpha$ , то  $\neg\alpha \notin M$ .
6. Обозначим за  $\sigma \leftrightarrow \zeta$  две импликации:  $(\sigma \rightarrow \zeta) \& (\zeta \rightarrow \sigma)$ . Докажите, что  $(\exists x. \varphi) \leftrightarrow ((\exists y. \varphi)[x := y])$ . Какие условия надо наложить на  $\varphi$ , чтобы доказательства имели место? Постройте контрпримеры к ситуациям, когда условия не выполнены.
7. Попробуем наметить доказательство теоремы о переносе кванторов:

- (а) Например, внесём квантор внутрь для конъюнкции:  $(\forall x. \alpha \& \beta) \rightarrow (\forall x. \alpha) \& (\forall x. \beta)$ . Какие условия надо наложить на формулы  $\alpha$  и  $\beta$  (при наложении условия предложите надлежащий контрпример)?
- (б) И теперь вынесем квантор наружу — например, для импликации:  $(\forall x. \alpha) \rightarrow (\forall y. \beta)$ . Как правильно вынести левый квантор,  $\forall x. \forall y. \alpha \rightarrow \beta$  или  $\exists x. \forall y. \alpha \rightarrow \beta$ ? Постройте вывод для правильного варианта, постройте контрпример для неправильного. Какие условия надо наложить на формулы  $\alpha$  и  $\beta$  (при наложении условия предложите надлежащий контрпример)?
- (с) Научимся преобразовывать выражение по частям: например, если  $\alpha \rightarrow \beta$ , то  $(\beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \gamma)$  и  $(\forall x. \alpha) \rightarrow (\forall x. \beta)$  (какие условия надо наложить на формулы  $\alpha$  и  $\beta$ ?).
- (д) Докажите, что для любого выражения  $\varphi$  найдётся эквивалентное ему выражение с поверхностными кванторами  $\psi$ . В доказательстве можно ссылаться на предыдущие пункты и на другие аналогичные утверждения (например, для других связок). В полном доказательстве  $\vdash \varphi \rightarrow \psi$ , известном автору, используется 38 подобных вспомогательных утверждений.

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

1. Покажите, что исчисление предикатов неполно в моделях ограниченной конечной мощности. А именно, пусть дана модель  $\mathcal{M} = \langle D, F, T, E \rangle$ . Назовём мощностью модели мощность её предметного множества:  $|\mathcal{M}| = |D|$ . Покажите, что для любой конечной мощности модели  $n \in \mathbb{N}$  найдётся такая формула  $\alpha$ , что при  $|\mathcal{M}| \leq n$  выполнено  $\llbracket \alpha \rrbracket_{\mathcal{M}} = \text{И}$ , но  $\not\models \alpha$ .



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

- (а) сортирующую строку в алфавите  $\{0, 1\}$  (например, из 01110111 программа должна сделать 00111111); в этом и в последующих заданиях в алфавит внешних символов при необходимости можно добавлять дополнительные символы;
- (б) прибавляющую 1 к числу в двоичной системе (например, из 1011 программа должна сделать 1100);
- (с) в строке в алфавите  $\{0, 1, 2\}$  сокращающую все «постоянные» подстроки до одного символа: машина должна превратить 1022220101111 в 1020101;
- (д) допускающую правильные скобочные записи (например,  $(( ))$  должно допускаться, а  $)() ($  — отвергаться);
- (е) допускающую строки вида  $a^n b^n c^n$  в алфавите  $\{a, b, c\}$  (например, строка  $aabbcc$  должна допускаться, а  $abbbcc$  — отвергаться);
- (ф) 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  $0 \leq k < 2^n$ , 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).

4. Рассмотрим аксиоматику Пеано. Пусть

$$a^b = \begin{cases} 1, & b = 0 \\ a^c \cdot a, & b = c' \end{cases}$$

Докажите, что:

- (а)  $a \cdot b = b \cdot a$
- (б)  $(a + b) \cdot c = a \cdot c + b \cdot c$
- (с)  $a^{b+c} = a^b \cdot a^c$
- (д)  $(a^b)^c = a^{b \cdot c}$
- (е)  $(a + b) + c = a + (b + c)$

5. Определим отношение «меньше или равно» так:  $0 \leq a$  и  $a' \leq b'$ , если  $a \leq b$ . Докажите, что:

- (а)  $x \leq x + y$ ;
- (б)  $x \leq x \cdot y$  (укажите, когда это так — в остальных случаях приведите контрпримеры);
- (с) Если  $a \leq b$  и  $m \leq n$ , то  $a \cdot m \leq b \cdot n$ ;
- (д)  $x \leq y$  тогда и только тогда, когда существует  $n$ , что  $x + n = y$ ;
- (е) 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  $b > 0$ .

6. 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:

- (а)  $a + b \dot{-} b = a$ ;
- (б)  $(a \dot{-} b) \cdot c = a \cdot c \dot{-} b \cdot c$ ;
- (с)  $a \dot{-} b \leq a + b$ ;
- (д)  $a \dot{-} b = 0$  тогда и только тогда, когда  $a \leq b$ .

7. 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)  $\vdash \forall a. \forall b. a = b \rightarrow b = a$ ;
- (c)  $\vdash \forall a. a \cdot 0 = 0 \cdot a$ ;
- (d)  $\vdash \forall a. a \cdot \bar{2} = a + a$ ;
- (e)  $\vdash \forall p. (\exists q. q' = p) \vee p = 0$  (единственность нуля);
- (f)  $\vdash p \cdot q = 0 \rightarrow p = 0 \vee q = 0$  (отсутствие делителей нуля);

## Задание №8. Арифметизация логики.

1. Покажите, что модус Darapti выполнен в формализации категорических силлогизмов Лейбница.
2. Покажите, что модус Cesaro выполнен в формализации категорических силлогизмов Лейбница.
3. Будем говорить, что  $k$ -местное отношение  $R$  выразимо в формальной арифметике, если существует формула формальной арифметики  $\rho$  со свободными переменными  $x_1, \dots, x_k$ , что:

- для всех  $\langle a_1, \dots, a_k \rangle \in R$  выполнено  $\vdash \rho[x_1 := \bar{a}_1] \dots [x_k := \bar{a}_k]$  (доказуема формула  $\rho$  с подставленными значениями  $a_1, \dots, a_k$  вместо свободных переменных  $x_1, \dots, x_k$ );
- для всех  $\langle a_1, \dots, a_k \rangle \notin R$  выполнено  $\vdash \neg \rho[x_1 := \bar{a}_1] \dots [x_k := \bar{a}_k]$ .

Выразите в формальной арифметике (укажите формулу  $\rho$  и докажите требуемые свойства про неё):

- (a) «пустое» отношение  $R = \emptyset$  (никакие два числа не состоят в отношении);
  - (b) двуместное отношение «хотя бы один из аргументов равен 0».
  - (c) одноместное отношение «аргумент меньше 3».
4. С использованием эмулятора рекурсивных функций (применённый на лекции синтаксис подсказывает использование библиотеки на C++, но вы можете выбрать любой другой способ эмуляции), покажите, что следующие функции примитивно-рекурсивны. Ваше решение должно быть продемонстрировано в работе на простых примерах. Возможно, при реализации сложных функций вам потребуется для ускорения работы заменить базовые функции на «нативные» (например, умножение, реализованное через примитивы, заменить на встроенную операцию) — это можно делать при условии, что для них у вас есть эквивалентная примитивно-рекурсивная реализация.
    - (a) умножение и ограниченное вычитание;
    - (b) целочисленное деление и остаток от деления;
    - (c) вычисление  $n$ -го простого числа (напомним теорему Бертрана-Чебышёва: для любого натурального  $n \geq 2$  найдётся простое число между  $n$  и  $2n$ );
    - (d) частичный логарифм  $\text{PLOG}_n(k) = \max\{p \mid k \leq n^p\}$  (например,  $\text{PLOG}_2(96) = 5$ );
    - (e) вычисление длины списка в гёделевой нумерации (например,  $\text{LEN}(3796875000) = \text{LEN}(2^3 \cdot 3^5 \cdot 5^9) = 3$ );
    - (f) выделение подсписка из списка (например,  $\text{SUBLIST}(2^2 \cdot 3^3 \cdot 5^4 \cdot 7^5, 2, 2) = 2^4 \cdot 3^5$ );
    - (g) склейка двух списков в гёделевой нумерации (например,  $\text{APPEND}(2^3 \cdot 3^5, 2^7 \cdot 3^6) = 2^3 \cdot 3^5 \cdot 5^7 \cdot 7^6$ ).
  5. Дадим следующее определение общерекурсивным функциям (отличается от того, что было на лекции): рассмотрим термы языка формальной арифметики (без арифметических операций) и назовём выражение вида  $\theta_1 = \theta'_1$  уравнением. Будем говорить, что из системы уравнений  $E$  выводится уравнение  $\theta_k = \theta'_k$ , если оно будет получено путём применения следующих правил:
    - в любом уравнении системы можно заменить все вхождения какой-то одной переменной  $x$  на какой-то литерал  $\bar{n}$ ;

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

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

Например,

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

задаёт  $f(x, y) = x + y$

Определите следующие функции в общерекурсивных функциях:

- умножение, деление;
  - проверку числа на простоту;
  - функцию Аккермана.
- Покажите, что если функция общерекурсивна в смысле прошлого пункта, то она является эффективно вычислимой (предложите любую реализацию, на любом языке, сводящемся к абстрактному алгоритму).
  - Пусть  $n$ -местное отношение  $R$  выразимо в формальной арифметике. Покажите, что тогда его характеристическая функция  $C_R$  представима в формальной арифметике:

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

- Покажите, что в определении представимости пункт  $\vdash \neg\varphi(\overline{x_1}, \dots, \overline{x_n}, \overline{y})$  при  $f(x_1, \dots, x_n) \neq y$  не является обязательным и может быть доказан из остальных пунктов определения представимой функции.
- Покажите, что функция  $f(x) = x + 2$  представима в формальной арифметике (в ответе также требуется привести все пропущенные на лекции выводы в формальной арифметике).

## Задание №9. Теоремы о неполноте арифметики.

- Покажите, что омега-непротиворечивая теория непротиворечива.
- Пусть  $\zeta_\varphi(x) := \forall z. \sigma(x, x, z) \rightarrow \varphi(z)$ , где формула  $\sigma(p, q, r)$  представляет функцию  $\text{SUBST}(p, q)$ , заменяющую в формуле с гёделевым номером  $p$  все свободные переменные  $x_1$  на формулу  $q$ . Тогда покажите, что формулу  $\alpha_\varphi := \zeta_\varphi(\ulcorner \zeta_\varphi \urcorner)$  можно взять в качестве формулы  $\alpha$  в лемме об автоссылках:  $\vdash \varphi(\ulcorner \alpha_\varphi \urcorner) \leftrightarrow \alpha_\varphi$ .
- Покажите, что если в некоторой корректной теории  $\mathcal{S}$ , имеющей модель  $M$ , ввести дополнительную аксиому  $\alpha$ , причём  $\llbracket \alpha \rrbracket_M = \text{И}$ , то тогда получившаяся теория не станет противоречивой и будет иметь ту же модель  $M$  и те же оценки для формул, что и исходная.
- Покажите, что вопрос о принадлежности формулы  $\alpha(x) = \forall p. \delta(x, p) \rightarrow \neg\sigma(p)$  в доказательстве теоремы о невыразимости доказуемости к множеству  $\text{Th}_{\mathcal{S}}$  ведёт к противоречию.
- Покажите, что формула  $D(x)$  из доказательства теоремы о невыразимости доказуемости является представимой в формальной арифметике.
- Рассмотрим определение предела последовательности:

$$\forall \varepsilon > 0. \exists N \in \mathbb{N}. \forall n \in \mathbb{N}. n > N \rightarrow |a_n - l| < \varepsilon$$

Раскройте все нелогические предикатные и функциональные символы, переведите эту формулу на язык исчисления предикатов, постройте эквивалентную формулу с поверхностными кванторами, проведите её сколемизацию и постройте эквивалентную систему дизъюнктов.

- Рассмотрим формулы  $\forall n. P(n) \rightarrow Q(n)$  и  $\forall n. P(n) \rightarrow P(f(n)) \vee P(g(n))$ , здесь  $P$  и  $Q$  — некоторые предикатные символы. Постройте для каждой из них эрбранов универсум и система основных примеров.

8. Принципом Дирихле («pigeonhole principle») называется утверждение о том, что нельзя разместить  $n$  кроликов в  $m$  ящиках (при  $m < n$ ) так, чтобы каждый кролик находился бы в ящике один.

Пусть пропозициональные переменные  $P_{i,j}$ , где  $i \in \overline{1, n}$  и  $j \in \overline{1, m}$  соответствуют утверждениям вида «кролик  $i$  находится в ящике  $j$ ». Формализуйте в исчислении высказываний условие «каждый кролик находится в отдельном ящике в одиночестве», понимаемое как условие на переменные  $P_{i,j}$ , постройте соответствующее выражение в КНФ.

Какова будет его система основных примеров? Покажите, что система основных примеров формулы противоречива при  $m < n$ .

## Задание №10. Метод резолюций.

- На выбранном вами языке (кроме C, C++, Pascal) напишите программу, печатающую свой текст. Программа не должна использовать внешний мир (на чтение): например, использовать специальные команды печати своего текста, рефлексии, работу с файлами и т.п.
- На лекции мы приводили способ проверки доказуемости  $\gamma_1, \dots, \gamma_n \vdash \alpha$ , а именно, строили систему дизъюнктов  $\{SNF(\gamma_1), \dots, SNF(\gamma_n), SNF(\neg\alpha)\}$  и проверяли её противоречивость (здесь  $SNF(\varphi)$  — сколемизация формулы  $\varphi$  и приведение её к КНФ). Обоснуйте данный способ.
- Мы доказывали теорему Эрбрана, проводя следующее схематическое рассуждение:

- дано — система основных примеров  $\mathcal{E}_S$ , построенная по системе дизъюнктов  $S$ , противоречива;
- значит, эта система не имеет модели;
- значит, по теореме Гёделя о компактности, у  $\mathcal{E}_S$  есть конечное противоречивое подмножество.

Заметим, что теорема Гёделя о компактности (равно как и её контрапозиция) не может быть здесь непосредственно применена. Укажите отличия и восполните пробелы в схематическом рассуждении.

- Постройте универсум Эрбрана для аксиомы индукции при  $\varphi := \exists y.P(x, y)$ :

$$(\exists y.P(0, y)) \ \& \ (\forall x.(\exists y.P(x, y)) \rightarrow \exists y.P(x', y)) \rightarrow \exists y.P(x, y)$$

Напомним, что универсум Эрбрана строится для формулы в КНФ после сколемизации.

- Рассмотрим множество дизъюнктов исчисления высказываний  $S$ . Обозначим шаг применения правила резолюции всеми возможными способами к дизъюнктам множества  $S$  как операцию  $\mathcal{R}(S)$ . Положим  $S_0 = S$ ,  $S_{n+1} = S_n \cup \mathcal{R}(S_n)$  и  $S' = \cup S_i$ .
  - Покажите, что  $S'$  противоречиво (то есть для любой интерпретации  $M$  найдутся значения для свободных переменных  $d_1, \dots, d_k$  и дизъюнкт  $\delta \in S'$ , что  $M \models \delta[x_1 := d_1, \dots, x_k := d_k]$ ) тогда и только тогда, когда  $S$  противоречиво.
  - Покажите, что для формул исчисления высказываний  $S'$  конечно при конечном  $S$ .
  - Покажите, что если  $S$  противоречиво, то в  $S'$  обязательно найдутся дизъюнкты с явным противоречием ( $\beta$  и  $\neg\beta$ ).
- Покажите, что если  $J = \{\delta_1, \neg\delta_2\}$  и  $\delta_1$  явно противоречит  $\neg\delta_2$  при некоторой подстановке свободных переменных (то есть,  $\sigma(\delta_1) = \sigma(\delta_2)$ ), то  $J$  также противоречива.
- В данном задании будет необходимо проверить выводимость утверждений в исчислении предикатов с помощью метода резолюций. Продемонстрируем метод на простом примере. Докажем  $(\forall x.P(x)) \rightarrow P(0)$ .

- Возьмём отрицание:  $\neg((\forall x.P(x)) \vee P(0))$ , то есть  $\neg\forall x.P(x) \vee P(0)$ , то есть  $\forall x.P(x) \ \& \ \neg P(0)$
- Проведём сколемизацию и переведём в КНФ:  $\{P(x), \neg P(0)\}$  при свободной переменной  $x$  (по которой имеется неявный квантор всеобщности).
- Применяем правило резолюции:

$$\frac{P(x) \quad \neg P(0)}{\square} \pi = \mathcal{U}[P(x'), P(0)]$$

- Получили пустой дизъюнкт (то есть явное противоречие), формула доказана.

Убедитесь с помощью метода резолюций, что:

- (a)  $(\exists x.P(x)) \rightarrow (\exists y.P(y))$
- (b)  $(\exists x.\forall y.P(x, y)) \rightarrow (\forall y.\exists x.P(x, y))$
- (c)  $(\forall x.P(x') \rightarrow P(x)) \& P(0''') \rightarrow P(0)$
- (d)  $(\forall x.P(x, y) \rightarrow P(f(x), y)) \& (\forall y.P(x, y) \rightarrow P(x, g(y))) \& P(a, b) \rightarrow P(f(f(f(a))), g(g(b)))$

8. Формализуйте следующие утверждения и покажите с помощью метода резолюций:

- (a) Категорический силлогизм «Barbara»
- (b) Категорический силлогизм «Camenes»
- (c) Слабый силлогизм, без дополнительного условия непустоты (такой вывод получится некорректным). Как поведёт себя метод резолюции для такого силлогизма? Также добавьте условие непустоты и примените метод резолюции.

9. Примените метод резолюции к доказательству принципа Дирихле для  $n = 4$  и  $m = 3$  (см. предыдущее домашнее задание).

10. В правиле резолюции к ответу применяются унифицирующая подстановка  $\pi$  и подстановки  $\sigma_1$  и  $\sigma_2$ , заменяющие переменные в дизъюнктах на свежие. Покажите, что эти подстановки важны. А именно, предложите непротиворечивый набор дизъюнктов, из которого можно вывести противоречие методом резолюции, если в правиле резолюции не применять  $\pi$  к результату. Правило, иллюстрирующее проблему:

$$\frac{\varphi \vee \beta_1 \quad \neg\beta_2 \vee \psi}{\varphi \vee \psi} \pi = \mathcal{U}[\beta_1, \beta_2]$$

11. Покажите, что семейство  $S$  непротиворечиво тогда и только тогда, когда  $S$  с добавленным применением правила резолюции для исчисления предикатов также непротиворечиво.

12. Можно ли проверить аксиому индукции с помощью метода резолюций? То есть, закончится ли процесс применения правила резолюций к отрицанию аксиомы получением противоречия?

## Задание №11. Лямбда-исчисление

Для проверки и демонстрации заданий используйте какой-нибудь эмулятор лямбда-исчисления, например LCI: <https://www.chatzi.org/lci/>

1. Определите следующие функции в лямбда-исчислении. В качестве подсказки заметим, что у задач на чёрчевские нумералы есть отдалённое сходство с задачами на примитивно-рекурсивные функции: все функции, предложенные в упражнениях, могут быть реализованы с помощью фиксированного количества циклов **for** (то есть, при помощи указания надлежащих функций **f** в аргументах чёрчевских нумералов). Также напоминаем, что в лямбда-исчислении несложно выражаются упорядоченные пары и значения алгебраических типов.

- (a) «Исключающее ИЛИ» на 3 аргумента, а также «Мажоритарный элемент», проверяющий, что большинство входных аргументов — истина:  $M(a_1, a_2, a_3) = \text{И}$ , если  $|\{i \mid i = \overline{1 \dots 3}, a_i = \text{И}\}| \geq 2$ .
- (b) **IsZero**, возвращающую истину, если аргумент равен 0, **IsEven**: возвращает истину, если аргумент чётен.
- (c) **Div3**: делит нумерал на 3 с округлением вверх, **Fib**: вычисляет соответствующее число Фибоначчи.
- (d) Вычисление квадратного корня числа (округление вниз).
- (e) Ограниченное вычитание и сравнение двух нумералов.
- (f) Деление с остатком для чёрчевских нумералов (возвращает упорядоченную пару).

2. Найдите нормальную форму для следующих выражений (а также докажите, почему она именно такова):

- (a)  $\bar{2} \bar{2}$  и  $\bar{2} \bar{2} \bar{2}$
- (b)  $\bar{m} \bar{n}$

3. На лекции был приведён комбинатор неподвижной точки  $Y := \lambda f.(\lambda x.f (x x)) (\lambda x.f (x x))$ , обладающий свойством  $Y P =_{\beta} P (Y P)$  для любого терма  $P$ . С его помощью оказывается возможным реализовывать рекурсию.

Например, зададим функцию, возводящую 2 в соответствующую степень:

$$P := \lambda f.\lambda x.(IsZero x) 1 ((f (Dec x)) \cdot 2)$$

Сравните это с кодом на Си:

```
unsigned f (unsigned x) { return x == 0 ? 1 : f (x-1) * 2; }
```

Тогда, вызванная как  $Y P x$ , эта функция вычислит  $2^x$ . Например,  $Y P 1 =_{\beta}$

$$\begin{aligned} &=_{\beta} P (Y P) 1 = (\lambda f.\lambda x.(IsZero x) 1 ((f (Dec x)) \cdot 2)) (Y P) 1 \\ &=_{\beta} (IsZero 1) 1 ((Y P (Dec 1)) \cdot 2)) =_{\beta} (Y P 0) \cdot 2 \\ &=_{\beta} (P (Y P) 0) \cdot 2 \\ &=_{\beta} (IsZero 0) 1 ((Y P (Dec 0)) \cdot 2)) \cdot 2 \\ &=_{\beta} 1 \cdot 2 =_{\beta} 2 \end{aligned}$$

С помощью  $Y$ -комбинатора реализуйте:

- (a) Вычисление  $k$ -го простого числа.
  - (b) Частичный логарифм.
  - (c) Предложите три других комбинатора неподвижной точки (других — то есть, не бета-эквивалентных  $Y$  и между собой).
4. Напомним, что список может быть задан с помощью алгебраического типа с двумя конструкторами, `Nil` и `Cons` (см. доказательство неразрешимости исчисления предикатов). С учётом этого знания, и с учётом представления алгебраических типов, приведённого на лекции, реализуйте следующие конструкции:
- (a) Функцию, вычисляющую длину списка.
  - (b) Функцию высшего порядка `map2` — последовательно применяет функцию к головам двух списков, возвращая список результатов: `map2 (*) [1;3] [2;4]` вернёт `[2;12]`.
  - (c) Функцию `rev`, возвращающую перевёрнутый список. Например, `rev[1, 3, 5] = [5, 3, 1]`.
5. Напомним определение:

$$\begin{aligned} S &:= \lambda x.\lambda y.\lambda z.x z (y z) \\ K &:= \lambda x.\lambda y.x \\ I &:= \lambda x.x \end{aligned}$$

Известна теорема о том, что для любого комбинатора  $X$  можно найти выражение  $P$  (состоящее только из скобок, пробелов и комбинаторов  $S$  и  $K$ ), что  $X =_{\beta} P$ . Будем говорить, что комбинатор  $P$  *выражает* комбинатор  $X$  в базисе  $SK$ .

Выразите в базисе  $SK$ :

- (a)  $\lambda x.x x, \Omega$
  - (b)  $F, \bar{I}$
  - (c)  $\lambda x.\lambda y.\lambda z.y$
6. По аналогии с импликативным фрагментом ИИВ, мы можем рассмотреть полное просто типизированное лямбда-исчисление, в котором добавить конструкции для упорядоченной пары (конъюнкции), алгебраического типа (дизъюнкции) и необитаемого типа (лжи).

Правила для конъюнкции:

$$\begin{aligned} &\frac{\Gamma \vdash A : \alpha \quad \Gamma \vdash B : \beta}{\Gamma \vdash \langle A, B \rangle : \alpha \& \beta} \text{ Конструктор пары} \\ &\frac{\Gamma \vdash P : \alpha \& \beta}{\Gamma \vdash \pi_L P : \alpha} \text{ Левая проекция} \quad \frac{\Gamma \vdash P : \alpha \& \beta}{\Gamma \vdash \pi_R P : \beta} \text{ Правая проекция} \end{aligned}$$

Правила для дизъюнкции:

$$\begin{array}{c}
\frac{\Gamma \vdash A : \alpha}{\Gamma \vdash \text{In}_L A : \alpha \vee \beta} \text{ Левая инъекция} \quad \frac{\Gamma \vdash B : \beta}{\Gamma \vdash \text{In}_R B : \alpha \vee \beta} \text{ Правая инъекция} \\
\frac{\Gamma \vdash L : \alpha \rightarrow \gamma \quad \Gamma \vdash R : \beta \rightarrow \gamma \quad \Gamma \vdash D : \alpha \vee \beta}{\Gamma \vdash \text{Case } L R D : \gamma} \text{ Сопоставление с образцом}
\end{array}$$

Правило для лжи:

$$\frac{\Gamma \vdash E : \perp}{\Gamma \vdash \text{absurd } E : \alpha}$$

Постройте натуральный вывод для следующих утверждений, а также постройте соответствующее в смысле изоморфизма Карри-Ховарда лямбда-выражение (и докажите его тип):

- (a) Карринг:  $(\alpha \& \beta \rightarrow \gamma) \leftrightarrow (\alpha \rightarrow \beta \rightarrow \gamma)$
- (b)  $(\alpha \vee \beta \rightarrow \gamma) \leftrightarrow (\alpha \rightarrow \gamma) \& (\beta \rightarrow \gamma)$
- (c)  $((\alpha \rightarrow \perp) \vee \beta) \rightarrow (\alpha \rightarrow \beta)$

7. Покажите, что в отличие от бета-редуцируемости, для бета-редукции не выполнена теорема Чёрча-Россера (рефлексивность и транзитивность отношения для теоремы существенна). А именно, существует такое лямбда-выражение  $T$ , что  $T \rightarrow_\beta A$ ,  $T \rightarrow_\beta B$ ,  $A \neq B$ , но нет  $S$ , что  $A \rightarrow_\beta S$  и  $B \rightarrow_\beta S$ .

8. Рассмотрим комбинаторы  $Y$  и  $\Omega := (\lambda x.x x) (\lambda x.x x)$ .

- (a) Покажите, что если  $\vdash A : \alpha$ , то любое подвыражение  $A$  также имеет тип.
- (b) Покажите, что  $Y$  и  $\Omega$  не имеют типа в просто-типизированном лямбда-исчислении.
- (c) Выразите их в языке Хаскель (Окамль). Каковы их типы?

9. Пусть фиксирован тип чёрчевского нумерала, это  $(\alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha)$ . Найдите выражения и их тип в просто-типизированном лямбда-исчислении (и докажите наличие этого типа) для следующих выражений.

Возможно, вам в этом поможет язык Хаскель: определим на языке Хаскель следующую функцию: `show_church n = show (n (+1) 0)`. Легко заметить, что `show_church (\f -> \x -> f (f x))` вернёт 2. Как вы думаете, какой у выражения `(\f -> \x -> f (f x))` тип?

- (a) Инкремент чёрчевского нумерала — то есть, докажите, что  $\vdash \lambda n.\lambda f.\lambda x.n f (f x) : \eta \rightarrow \eta$ , где  $\eta = (\alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha)$ .
- (b) Сложение двух чёрчевских нумералов;
- (c) Умножение двух чёрчевских нумералов (не каждая реализация умножения подойдёт).

10. Напомним, что в одном выражении может быть более одного бета-редекса. Назовём порядок редукции *нормальным*, если всегда вычисляется тот бета-редекс, первый символ которого стоит левее всего в строке. *Аппликативным* порядком назовём такой, при котором вычисляется самый левый из наиболее вложенных редексов. Например, в выражении

$$(\lambda x.x) ((\lambda n.\lambda f.\lambda x.n f (f x)) \lambda f.\lambda x.x)$$

точками подчёркнут редекс для нормального порядка, а прерывистой линией — для аппликативного.

Интуитивно в нормальном порядке сперва вычисляется тело функции, а параметры вычисляются потом, по мере надобности. Аппликативный же порядок предполагает обязательное вычисление параметров перед вычислением самой функции.

Известна теорема о том, что если у выражения в принципе существует нормальная форма, то она может быть получена путём применения нормального порядка редукции.

Обычно в языках программирования применяется аппликативный порядок редукции, однако, в (практически) любом языке конструкция `if` вычисляется с помощью нормального порядка, поскольку условный оператор вычисляет только одну из веток (`then` или `else`).

Предложите лямбда-выражение, количество редукций которого до нормальной формы различается более чем в  $n$  раз при применении нормального и аппликативного порядков (по заданному заранее  $n$ ).

## Задание №12. Теория множеств.

1. Задайте полный порядок на  $\mathbb{Z}$  и на  $\mathbb{Q}$ . Стандартный порядок на вещественных числах не является полным, хотя некоторые его подмножества этим порядком вполне упорядочиваются (натуральные числа). Вполне ли упорядочены вещественные корни квадратных уравнений с натуральными коэффициентами (как подмножество  $\mathbb{R}$ )?
2. Является ли порядок на алгебре Линденбаума полным? Если нет, то какие подмножества алгебры Линденбаума являются вполне упорядоченными?
3. Пусть заданы списки (в любом языке программирования)  $L(\alpha)$ , хранящие значения типа  $\alpha$ . Для решения задания задайте библиотеку с функциями, являющимися аналогами конструктивных аксиом теории множеств:
  - `empty` :  $L(\alpha)$ , строит пустой список.
  - `pair` :  $(\alpha, \alpha) \rightarrow L(\alpha)$ , формирует список из двух своих аргументов.
  - `flatten` :  $L(L(\alpha)) \rightarrow L(\alpha)$ , соединяет все списки внутри списка в один.
  - `powerset` :  $L(\alpha) \rightarrow L(L(\alpha))$ , делает из списка список всех возможных подсписков.
  - `filter` :  $(\alpha \rightarrow \text{bool}) \rightarrow L(\alpha) \rightarrow L(\alpha)$ , выделяет из списка все элементы, соответствующие условию.

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

- (a) пересечение всех элементов множества  $(\bigcap a)$ ;
  - (b)  $a \setminus b$  (разность множеств) и  $a \triangle b$  (симметрическую разность множеств);
  - (c)  $a \oplus b$  (дизъюнктивное объединение множеств:  $\{\langle x, 0 \rangle \mid x \in a\} \cup \{\langle x, 1 \rangle \mid x \in b\}$ );
  - (d)  $a \times b$  (декартово произведение множеств:  $\{\langle p, q \rangle \mid p \in a, q \in b\}$ );
  - (e)  $\times a$  (прямое произведение дизъюнктивного множества  $a$ ).
4. Определим упорядоченную пару  $\langle a, b \rangle := \{\{a\}, \{a, b\}\}$ . Покажите, что  $\langle a, b \rangle = \langle c, d \rangle$  тогда и только тогда, когда  $a = c$  и  $b = d$ .
  5. Восполним пробелы в доказательстве существования  $\omega$ :
    - (a) Определите формулу  $\varphi(x)$  для свойства « $x$  — конечный ординал». Укажите замкнутый вид для формулы, задающей ординал  $\omega$ .
    - (b) Покажите, что  $\omega$  — действительно ординал.
  6. Давайте докажем некоторые свойства ординалов.
    - (a) Предъявите примеры (i) транзитивного, но не вполне упорядоченного отношением  $\in$  множества и (ii) вполне упорядоченного, но не транзитивного множества (задание не делится на пункты). Покажите, что ваши примеры — действительно множества в смысле аксиоматики ZF.
    - (b) Покажите, что если  $x$  — ординал, то  $x'$  — тоже ординал.
    - (c) Верно ли, что если  $x'$  — ординал, то  $x$  — тоже ординал?
    - (d) Покажите, что любой непустой ординал содержит пустое множество.
    - (e) Покажите, что если  $x \in p$  и  $p$  — ординал, то либо  $x' = p$ , либо  $x' \in p$ .
    - (f) Покажите, что если  $x$  и  $y$  — конечные ординалы, то  $x = y$ ,  $x \in y$  или  $y \in x$  (не используйте аксиому выбора и следующую из неё аналогичную теорему с лекции).
  7. Покажите, что аксиома фундирования запрещает существование такого множества  $x$ , что  $x \in x$ .
  8. Покажите, что на множестве  $\omega$  выполняется аксиоматика Пеано (полная формализация рассуждений не требуется, но из изложения должно быть понятно, как эту формализацию в рамках теории первого порядка получить):
    - (a)  $\forall x. x \in \omega \rightarrow \neg x' = \emptyset$
    - (b)  $\forall x. \forall y. x \in \omega \ \& \ y \in \omega \rightarrow x' = y' \rightarrow x = y$
    - (c) (указание к следующему пункту) покажите, что если  $\vdash \forall x. \neg \phi(x) \rightarrow A \ \& \ \neg A$ , то  $\vdash \forall x. \phi(x)$ .



- (d) Если  $\phi(\emptyset)$  и  $\forall x.x \in \omega \rightarrow \phi(x) \rightarrow \phi(x')$ , то  $\forall x.x \in \omega \rightarrow \phi(x)$ .
9. Проверьте следующие равенства (докажите или опровергните):
- (a)  $\omega \cdot \bar{2} = \bar{2} \cdot \omega$
  - (b)  $\omega \cdot \bar{2} = \omega + \omega$
  - (c)  $(\omega + \bar{1})^{\bar{2}} = \omega^{\bar{2}} + \bar{2} \cdot \omega + \bar{1}$
  - (d)  $\omega^\omega = (\omega^{\bar{2}})^\omega$
  - (e)  $\omega^{\omega + \bar{1}} = \omega^\omega + \bar{1}$
  - (f) Имеет ли место ассоциативность сложения и/или умножения?
10. Верно ли, что  $1^\omega = \omega$  и/или  $\omega^1 = \omega$ ?
11. Рассмотрим все конечные двоичные деревья без значений в вершинах и узлах, и зададим лексикографический порядок на них: листья друг другу равны, лист всегда меньше узла, узлы упорядочены лексикографически своими потомками (сравниваем левых сыновей, если равны — то правых). Является ли это полным порядком, если да, то какое порядковое число соответствует этому упорядочению?
12. Зачёт за пункт ставится, если одновременно решены два подпункта: (i) Покажите, что множество  $\omega^\omega$  имеет счётную мощность (здесь: имеется биекция на  $\omega$ , возможно, не сохраняющая порядок). (ii) Определим  $\uparrow k$  (башню из омег) так:

$$\uparrow k = \begin{cases} \omega, & k = 1 \\ \omega^{\uparrow n}, & k = n' \end{cases}$$

Скажем,  $\uparrow 3 = \omega^{(\omega^\omega)}$ . Будет ли счётным ординал  $\text{crb} \{\uparrow k \mid k \in \omega\}$ ?

13. На лекции было приведено два различных определения для сложения и умножения ординалов. Покажите, что эти определения эквивалентны.
- (a) Покажите, что  $\text{crb } X = \bigcup X$  — ординал, если каждый элемент  $X$  — ординал. Не забывайте, что рассуждение по индукции по числу элементов в  $X$  не подойдёт.
  - (b) Пусть  $a$  и  $b$  — ординалы. Покажите, что порядковое число для  $a \uplus b$  эквивалентно  $a + b$ .
  - (c) Пусть  $a$  и  $b$  — ординалы. Покажите, что порядковое число для  $a \times b$  эквивалентно  $a \cdot b$ .

## Задание №13. Мощность множеств.

1. Рассмотрим следующую теорию первого порядка и её модель  $\mathcal{M}$  при  $D = \mathbb{R}$ . В ней мы зададим один нелогический двуместный предикатный символ  $B$  и константу 0. Никаких нелогических аксиом мы не задаём. Модель  $\mathcal{M}$  имеет  $D = \mathbb{R}$ . Название  $B$  — от выражения «Because I can!», поскольку в  $\mathcal{M}$  только  $B(\pi, e)$  истинно, а при других параметрах предикат ложен. Значение 0 задано естественно:  $\llbracket 0 \rrbracket_{\mathcal{M}} = 0$ . Заметим, что  $\models_{\mathcal{M}} \exists p. \exists q. B(p, q)$ . Примените к этой теории теорему Лёвенгейма-Сколема, опишите, какие множества  $D_n$  будут построены, и покажите, какая счётная модель получится.
2. Покажите следующее (обозначим за  $\mathcal{F}(p, q)$  множество функций из  $p$  в  $q$ ):
- (a)  $|a| = 0$  тогда и только тогда, когда  $a = \emptyset$ ;
  - (b) если  $|a| \leq |b|$ , то  $|\mathcal{F}(g, a)| \leq |\mathcal{F}(g, b)|$ ;
  - (c) если  $|a| \leq |b|$  и  $\bar{0} < |g|$ , то  $|\mathcal{F}(a, g)| \leq |\mathcal{F}(b, g)|$ ;
  - (d)  $|\mathcal{F}(\bar{0}, a)| = \bar{1}$ ,  $|\mathcal{F}(a, \bar{1})| = \bar{1}$ ; если  $|a| > 0$ , то  $|\mathcal{F}(a, \bar{0})| = \bar{0}$ ;
  - (e) если  $|a| \geq \aleph_0$  и  $0 < |n| < \aleph_0$ , то  $|\mathcal{F}(n, a)| = a$ .
3. Покажите эквивалентность следующих определений конечного множества (задание  $(k)$  предполагает доказательство импликации  $(k) \rightarrow (k')$ ; возможно, некоторые из переходов потребуют аксиомы выбора):
- (a)  $a$  конечно, если каждое непустое семейство подмножеств  $a$  имеет максимальный по включению элемент. Например, при  $a = \{0, 1, 2\}$  в семействе подмножеств  $\{\emptyset, \{0, 1\}, \{1, 2\}\}$  элементы  $\{0, 1\}$  и  $\{1, 2\}$  — максимальны.

- (b)  $a$  конечно, если  $\mathcal{P}(a)$  не равномощно своему собственному подмножеству (собственное подмножество — подмножество, не совпадающее с множеством).
- (c)  $a$  конечно, если оно не равномощно своему собственному подмножеству.
- (d)  $a$  конечно, если  $|a| = \emptyset$  или  $|a| \cdot 2 > |a|$ .
- (e)  $a$  конечно, если  $|a| = \emptyset$  или  $|a| = \bar{1}$  или  $|a|^2 > |a|$ .
- (f)  $a$  конечно, если  $|a| < \aleph_0$ .
4. Покажите, что представимая функция  $f : a \rightarrow b$  биективна (т.е. инъективна и сюръективна) тогда и только тогда, когда  $\forall y. \exists! x. \phi(x, y)$ . Здесь за  $\phi(x, y)$  мы обозначаем формулу, представляющую функцию  $f$  в теории множеств, по аналогии с формальной арифметикой.
5. Покажите в ZFC, что если  $a$  и  $b$  — непустые множества, то существует функция из  $a$  в  $b$  (однако функция не обязана быть инъективной или сюръективной).
6. Фильтром  $\mathcal{F}$  назовём структуру на элементах некоторой решётки  $\langle L, (\leq) \rangle$  со следующими свойствами:
- $0 \notin \mathcal{F}$ ;
  - если  $a, b \in \mathcal{F}$ , то  $a \cdot b \in \mathcal{F}$ ;
  - если  $a \in \mathcal{F}$ ,  $a \leq b$ ,  $b \in L$ , то  $b \in \mathcal{F}$ .
- Фильтр назовём главным для  $x \in L$ , если  $\mathcal{F} = \{a \in L \mid x \leq a\}$ . Фильтр  $\mathcal{F}'$  назовём собственным подфильтром  $\mathcal{F}$ , если  $\mathcal{F}' \subset \mathcal{F}$ . Фильтр назовём ультрафильтром, если он не является собственным подфильтром никакого фильтра на  $L$ .
- (a) Покажите, что главный фильтр для  $x \in L$  является ультрафильтром.
- (b) Покажите, что множество дополнений конечных множеств до бесконечного образует фильтр (в качестве отношения порядка рассмотрим отношение включения). Является ли этот фильтр ультрафильтром?
- (c) Покажите, что для ультрафильтра  $F$  на булевой алгебре  $L$  и  $x \in L$  выполнено  $x \in F$  или  $\sim x \in F$ . Также покажите, что полное непротиворечивое множество формул образует ультрафильтр.
- (d) Покажите, что у любого фильтра есть содержащий его ультрафильтр (вам потребуется лемма Цорна для доказательства этого факта).
7. Покажите, что у любых двух множеств  $A$  и  $B$  их мощности сравнимы ( $|A| \leq |B|$  или  $|B| \leq |A|$ ). Для доказательства вам потребуется один из вариантов аксиомы выбора.
8. Покажите, что мощность множества всех непрерывных функций  $\mathbb{R} \rightarrow \mathbb{R}$  —  $\beth_1$ .
9. Покажите, что мощность множества всех функций  $\mathbb{N} \rightarrow \mathbb{N}$  — также  $\beth_1$ .
10. Пусть  $a \in \mathbb{R}$ , причём  $0 < a < 1$ . Пусть  $r(a)$  — множество его десятичных записей (бесконечная последовательность цифр от 0 до 9). Например,  $(5, 0, 0, \dots) \in r(0.5)$  и  $(4, 9, 9, \dots) \in r(0.5)$ . Покажите, что:
- для любой последовательности цифр  $x_n$  найдётся число  $a$ , что  $(x_0, x_1, x_2, \dots) \in r(a)$ .
  - какое бы ни было число  $a$ , если  $(x_0, x_1, x_2, \dots) \in r(a)$  и  $(y_0, y_1, y_2, \dots) \in r(a)$ , то  $x_i = y_i$ , либо  $x_i, y_i \in \{0, 9\}$ .
11. Покажите, что если  $|T| \geq \aleph_0$ , то  $||T| \times |T|| = |T \times T| = |T|$  (ссылка вперёд: предполагает трансфинитную индукцию, 16 лекция).

## Задание №14. Аксиома выбора.

- На лекции была рассмотрена теорема: если семейство упорядоченных множеств  $X$  линейно упорядочено отношением «быть начальным отрезком», то у него есть верхняя грань. Покажите, что отношение  $(<_M) = \cup \{ (<) \mid \text{из предлагаемой теоремой верхней грани действительно является отношением порядка} \}$ .
- Покажите, что если функциональный вариант аксиомы выбора принять за аксиому, то тогда утверждение аксиомы выбора станет доказуемо.

3. Лемма Цорна утверждает, что если любое линейно-упорядоченное подмножество имеет верхнюю грань, то множество имеет максимальный элемент. А верно ли, что этот элемент также всегда будет наибольшим (как это было в случае с теоремой Цермело)?
4. Покажите, что у любого векторного пространства есть базис. *Указание:* вам потребуется лемма Цорна для этого, или какой-то ещё вариант аксиомы выбора; также надо предложить упорядочивание множества базисов по какому-то критерию и показать, что максимальный базис подходит.