

# Конспекты по математической логике

Анатолий Коченюк, Георгий Каданцев, Константин Бац

2022 год, семестр 4

## 1 Введение

Логика – довольно старая наука, но наш предмет довольно молодой В какой-то момент логики как дисциплины, которая учит просто правильно рассуждать, стало не хватать. Появилась теория множеств. Общего здравого смысла не хватает, нужен строгий математический язык. Это рубеж 19-20 веков.

У нас теория множеств не будет фокусом, как это могло бы быть на мат. факультете.

Теория множеств, когда она была впервые сформулирована, была противоречива (как матан, сформулированный Ньютоном). Чтобы уверенно и эффективно заниматься матаном, нужно суметь его формализовать.

<Парадокс Рассела / парадокс брадобрея> Мы приписываем элементу-человеку свойство, которое невыполнимо. Объекта, выходит, не существует. Мы смогли очень быстро определить противоречие в этом определении. Но, может быть, мы не смогли его определить в других наших определениях? (конструкциях вещественной прямой, и т.д. и т.д.)

Программа Гильберта.

1. Формализуем математику! Сформулируем теорию на языке (не на русском или английском), который не будет допускать парадоксов,
2. ... и на котором можно будет доказать непротиворечивость.

В 1930 году становится понятно, что сколько-нибудь сильная (= в ней можно построить формальную арифметику) теория не может быть доказана непротиворечивой.

Возможно, сама наша логика неправильная? Эта идея будет нам полезна, и к ней мы ещё вернемся.

Возможно, что это просто свойство мира, и мы хотим невозможного.

Из этих рассуждений выросло большое множество хороших идей, которые оказались полезны в других местах. Матлогика служит широкому кругу нужд.

Мы можем доказывать, что программа работает корректно. Именно доказывать, а не проверять тестами!

Мы можем изучать свойства самих языков. Изоморфизм Карри-Говарда – доказательство это программа, утверждения это тип. Можно изучать языки программирования и можно развернуть изоморфизм: изучать математику как язык программирования.

Функциональные языки: окамль + хаскель. Ознакомление с этими языками представляет собой способ ознакомиться с предметом немного с другой стороны.

## 2 Исчисление высказываний

Мы говорим на двух языках: на предметном языке и метаязыке. Предметный язык – это то, что изучается, а метаязык – это язык, на котором это изучается.

На уроках английского предметным является сам английский, а метаязыком может быть русский. Метаязык – это язык исследователя, а предметный язык – это язык исследуемого. Что такое язык вообще? Хороший вопрос.

Высказывание – это одно из двух:

1. Большая латинская буква начала алфавита, возможно с индексами и штрихами – это пропозициональные переменные.
2. Выражение вида  $(\alpha \wedge \beta)$ ,  $(\alpha \vee \beta)$ ,  $(\alpha \rightarrow \beta)$ ,  $(\neg \alpha)$ .

В определении выше альфа и бета это метапеременные— места, куда можно подставить высказывание.

1.  $\alpha, \beta, \gamma$  — метапеременные для всех высказываний.
2.  $X, Y, Z$  — метапеременные для пропозициональных переменных.

Метапеременные являются частью языка исследователя.

В формализации мы останавливаемся до места, в котором мы можем быть уверены, что сможем написать программу, которая всё проверяет.

Сокращение записи, приоритет операций: сначала  $\neg$ , потом  $\&$ , потом  $\vee$ , потом  $\rightarrow$ . Если скобки опущены, мы восстанавливаем их по приоритетам. Выражение без скобок является частью метаязыка, и становится частью предметного, когда мы восстанавливаем их. Скобки последовательных импликаций расставляются по правилу правой ассоциативности — справа налево.

## 2.1 Теория моделей

У нас есть истинные значения  $\{T, F\}$  в классической логике. И есть оценка высказываний  $\llbracket \alpha \rrbracket$ . Например  $\llbracket A \vee \neg A \rrbracket$  истинно. Всё, что касается истинности высказываний, касается теории моделей.

**Определение 2.1.1.** Оценка — это функция, сопоставляющая высказыванию его истинное (истинностное) значение.

## 2.2 Теория доказательств

**Определение 2.2.1.** Аксиомы — это список высказываний. Схема аксиомы — высказывание вместе с метопеременными; при любой подстановке высказываний вместо метапеременной получим аксиому.

**Определение 2.2.2.** Доказательство (вывод) — последовательность высказываний  $\gamma_1, \gamma_2 \dots$  где  $\gamma_i$  — любая аксиома, либо существуют  $j, k < i$  такие что  $\gamma_j \equiv (\gamma_k \rightarrow \gamma_i)$ . (знак  $\equiv$  здесь сокращение для "имеет вид"). Это правило "перехода по следствию" или Modus ponens.

Определим следующие 10 схем аксиом для того исчисления высказываний, которое мы рассматриваем.

1.  $\alpha \rightarrow \beta \rightarrow \alpha$  — добавляет импликацию
2.  $(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \gamma)$  — удаляет импликацию
3.  $\alpha \wedge \beta \rightarrow \alpha$  — удаление конъюнкции
4.  $\alpha \wedge \beta \rightarrow \beta$  — удаление конъюнкции
5.  $\alpha \rightarrow \beta \rightarrow \alpha \wedge \beta$  — внесение конъюнкции
6.  $\alpha \rightarrow \alpha \vee \beta$  — внесение дизъюнкции
7.  $\beta \rightarrow \alpha \vee \beta$  — внесение дизъюнкции
8.  $(\alpha \rightarrow \gamma) \rightarrow (\beta \rightarrow \gamma) \rightarrow (\alpha \vee \beta \rightarrow \gamma)$
9.  $(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \neg \beta) \rightarrow (\neg \alpha)$
10.  $\neg \neg \alpha \rightarrow \alpha$  — очень спорная штука.

**Пример.** Доказательство  $\vdash A \rightarrow A$ .

1.  $A \rightarrow (A \rightarrow A) \rightarrow A$  (схема 1)
2.  $A \rightarrow A \rightarrow A$  (схема 1)
3.  $(\underbrace{A}_{\alpha} \rightarrow \underbrace{A \rightarrow A}_{\beta}) \rightarrow (\underbrace{A}_{\alpha} \rightarrow \underbrace{(A \rightarrow A) \rightarrow A}_{\beta}) \rightarrow (\underbrace{A}_{\gamma} \rightarrow \underbrace{A}_{\gamma})$  (схема 2)
4.  $(A \rightarrow (A \rightarrow A) \rightarrow A) \rightarrow (A \rightarrow A)$  (m.p 2, 3)
5.  $A \rightarrow A$  (m.p 1, 4)

## 2.3 Теорема о дедукции

**Определение 2.3.1.** (Метаметаопределение). Будем большими греческими буквами  $\Gamma, \Delta, \Sigma \dots$  — списки формул, неупорядоченные.

**Определение 2.3.2.** Вывод из гипотез:  $\Gamma \vdash \alpha$ .

То есть существует  $\delta_1, \dots, \delta_n, \delta_n \equiv \alpha$ , где  $\delta_{i-1}$  или схема аксиом, или m.p. из  $j$  и  $k$  и  $j, k < i$ .

**Теорема 2.3.1.**  $\Gamma, \alpha \vdash \beta$  тогда и только тогда, когда  $\Gamma \vdash \alpha \rightarrow \beta$ .

*Доказательство.*  $\Leftarrow$  Пусть  $\delta_1, \delta_2 \dots \delta_n \equiv \alpha \rightarrow \beta$  выводит  $\alpha \rightarrow \beta$ . Дополним этот вывод двумя доказательствами новыми высказываниями:  $\delta_{n+1} \equiv \alpha$  (дано нам в гипотезе),  $\gamma_{n+2} \equiv \beta$  (MP шагов  $n, n+1$ ) — это и требовалось.

$\Rightarrow$  Пусть  $\Gamma, \alpha \vdash \beta$ . Напишем программу, которая построит  $\Gamma \vdash \alpha \rightarrow \beta$ .

Инвариант, который мы будем поддерживать: всё до  $\alpha \rightarrow \delta_i$  — док-во. Доказательство индукцией по  $n$ .

1. База:  $n = 1$  — без комментариев.
2. Если  $\delta_1, \dots, \gamma_n$  можно перестроить в доказательство  $\alpha \rightarrow \gamma_n$ , то  $\gamma_1 \dots \gamma_{n+1}$  тоже можно перестроить. Разберём случаи:
  - (a)  $\delta_i$  — аксиома или гипотеза из  $\Gamma$ .
    - (i-0.6)  $\delta_i$
    - (i-0.3)  $\delta_i \rightarrow \alpha \rightarrow \delta_i$
    - (i)  $\alpha \rightarrow \delta_i$  (m.p из i-0.6 и i-0.3)
  - (b)  $\delta_i = \alpha$ , то есть надо построить  $\alpha \rightarrow \alpha$ 
    - (i-0.8, i-0.6, i-0.4, i-0.2) (доказательство  $\alpha \rightarrow \alpha$ )
    - (i)  $\alpha \rightarrow \alpha$
  - (c)  $\delta_i$  получено из  $\delta_j$  и  $\delta_k$  ( $\delta_k \equiv \delta_j \rightarrow \delta_i$ ) по индукционному предположению, уже есть строчки вида  $\alpha \rightarrow \delta_j, \alpha \rightarrow \delta_k$ 
    - (j)  $\alpha \rightarrow \delta_j$
    - (k)  $\alpha \rightarrow (\delta_j \rightarrow \delta_i)$
    - (i-0.6)  $(\alpha \rightarrow \delta_j) \rightarrow (\alpha \rightarrow \delta_j \rightarrow \delta_i) \rightarrow (\alpha \rightarrow \delta_i)$  (схема 2)
    - (i-0.3)  $(\alpha \rightarrow \delta_j \rightarrow \delta_i) \rightarrow (\alpha \rightarrow \delta_i)$  (m.p.)
    - (i)  $(\alpha \rightarrow \delta_i)$  (m.p.)

■

## 3 Теория моделей

Мы можем доказывать модели или оценивать их. "Мы можем доказать, что мост не развалится или можем выйти и попрыгать на нём."

**Определение 3.0.1.**  $\mathbb{V}$  — истинностное множество.

$F$  — множество высказываний нашего исчисления высказываний.

$P$  — множество пропозициональных переменных.

$$[\![\cdot]\!] : F \rightarrow \mathbb{V} \text{ — оценка}$$

**Определение 3.0.2.** Для задания оценки необходимо задать оценку пропозициональных переменных.

$$[\![\cdot]\!] : P \rightarrow \mathbb{V} \quad f_P$$

Тогда:

$$[\![x]\!] = f_P(x)$$

**Замечание.** Обозначение: значения пропозициональных переменных будем определять в верхнем индексе:  $[\![\alpha]\!]^{A=T, B=F \dots}$

**Определение 3.0.3.**  $\alpha$  — общезначна (истинна), если  $[\![\alpha]\!] = T$  при любой оценке  $P$ .

$\alpha$  — невыполнима (ложна), если  $[\![\alpha]\!] = F$  при любой оценке  $P$ .

$\alpha$  — выполнима, если  $[\![\alpha]\!] = T$  при некоторой  $f_P$ .

$\alpha$  — опровержима, если  $[\![\alpha]\!] = F$  при некоторой  $f_P$ .

**Определение 3.0.4.** Теория корректна, если доказуемость влечёт общезначимость.

Теория полна, если общезначимость влечёт доказуемость.

**Определение 3.0.5.**  $\Gamma \models \alpha$  означает, что  $\alpha$  следует из  $\Gamma = \{\gamma_1, \dots, \gamma_n\}$ , если  $[\![\alpha]\!] = T$  всегда при  $[\![\gamma_i]\!] = T$  при всех  $i$ .

### 3.1 Корректность исчисления высказываний

**Теорема 3.1.1.** Исчисление высказываний корректно.  $\vdash \alpha$  влечёт  $\models \alpha$ .

*Доказательство.* Индукция по длине доказательства  $\delta_1, \dots, \delta_n$ .

Разбор случаев:

1.  $\delta_i$  аксиома  $\implies$  построить таблицу истинности, проверить, что все верно.

2.  $\delta_i$  — м.п.  $\delta_j, \delta_k \equiv \delta_j \rightarrow \delta_i \implies$  также рассмотрим таблицу истинности.

■

Мы даём доказательство на метаязыке, не пускаясь в отчаянный формализм. Такая строгость нас устраивает.

В матлогике бессмысленно формализовывать русский язык. Она нужна, чтобы дать ответы на сложные вопросы в математике, где здравого смысла недостаточно и нужна формализация.

### 3.2 Полнота исчисления высказываний

**Теорема 3.2.1.** Исчисление высказываний полно.

**Определение 3.2.1.**  $[_\beta]\alpha = \begin{cases} \alpha, & \llbracket \beta \rrbracket = T \\ \neg\alpha, & \llbracket \beta \rrbracket = F \end{cases}$

**Лемма 3.2.1.1.**  $[_\alpha]\alpha,$   
 $[_\beta]\beta \vdash [_{\alpha \star \beta}] \alpha \star \beta,$   
 $[_\alpha]\alpha \vdash [_{\neg\alpha}] \neg\alpha$

**Пример.**  $\llbracket \alpha \rrbracket = T, \llbracket \beta \rrbracket = F \implies \alpha \wedge \neg\beta \vdash \neg(\alpha \wedge \beta).$

**Лемма 3.2.1.2.** Если  $\Gamma \vdash \alpha$ , то  $\Gamma, \Delta \vdash \alpha$ .

**Лемма 3.2.1.3.** Пусть дана  $\alpha, X_1, \dots, X_n$  — её переменные.

$$[_{X_1}]X_1, \dots, [_{X_n}]X_n \vdash [_\alpha] \alpha$$

*Доказательство.* Пусть  $\tilde{X} = [_{X_1}]X_1 \dots [_{X_n}]X_n$ .

Индукция по длине формулы  $\alpha$ .

База:  $\alpha = X_i$ .

Переход: есть  $\alpha, \beta$ . По предположению  $\tilde{X} \vdash [_\alpha] \alpha \quad \tilde{X} \vdash [_\beta] \beta$ .

По леме 1 тогда  $\tilde{X} \vdash [_{\alpha \star \beta}] \alpha \star \beta$ . ■

**Лемма 3.2.1.4.** Если  $\models \alpha$ , то  $\tilde{X} \vdash \alpha$ . То есть при любых подстановках значений  $\alpha$  будет истинна.

**Лемма 3.2.1.5.**

$$\Gamma, Y \vdash \alpha, \quad \Gamma, \neg Y \vdash, \text{ то } \Gamma \vdash \alpha$$

*Доказательство было в дз.* ■

**Лемма 3.2.1.6.** Если  $\tilde{X} \vdash \alpha$  при всех оценках  $X_1, \dots, X_n$ , то  $\vdash \alpha$ .

*Доказательство индукцией по  $n$ .* ■

**Теорема 3.2.2.** Если  $\models \alpha$ , то  $\vdash \alpha$ .

*Доказательство.* По лемме 4 и лемме 6. ■

## 4 Интуиционистская логика

Мы не хотим дурацких коснструкций вроде парадокса брадобрея. Мы не хотим странных, но логически верных утверждений вроде  $A \rightarrow B \vee B \rightarrow A$ . Интуиционистская логика предлагает свою математику, в которой своя интерпретация логических связок. ВНК-интерпретация (Брауер-Гейтинг-Колмогоров).

- $\alpha, \beta, \gamma \dots$  — это конструкции.
- $\alpha \wedge \beta$  если мы умеем строить и  $\alpha$ , и  $\beta$ .
- $\alpha \vee \beta$ , если мы умеем строить  $\alpha, \beta$  и знаем, что именно.
- $\alpha \rightarrow \beta$ , если мы умеем перестроить  $\alpha$  в  $\beta$ .
- $\perp$  — не имеет построения
- $\neg\alpha \equiv \alpha \rightarrow \perp$

”Теория доказательств”. Рассмотрим классическое исчисление высказываний и заменим схему аксиом 10 на следующую

$$\alpha \rightarrow \neg\alpha \rightarrow \beta$$

В этой формализации мы следуем не сути интуиционистской логики, а традиции. В интуиционистской логике формализм это не источник логики.

Примеры моделей.

1. Модели КИВ подходят: корректны, но не полны ( $\llbracket A \vee \neg A \rrbracket = I$ , но  $\not\models_I A \vee \neg A$ ).

2. Пусть  $X$  топологическое пространство.

Пусть истинностные значения — все открытые пространства в классической топологии.

- $\llbracket \alpha \& \beta \rrbracket = \llbracket \alpha \rrbracket \cap \llbracket \beta \rrbracket$ .
- $\llbracket \alpha \vee \beta \rrbracket = \llbracket \alpha \rrbracket \cup \llbracket \beta \rrbracket$ .
- $\llbracket \alpha \rightarrow \beta \rrbracket = (X \setminus \llbracket \alpha \rrbracket \cup \llbracket \beta \rrbracket)^o$ .
- $\llbracket \neg \alpha \rrbracket = (X \setminus \llbracket \alpha \rrbracket)^o$ .

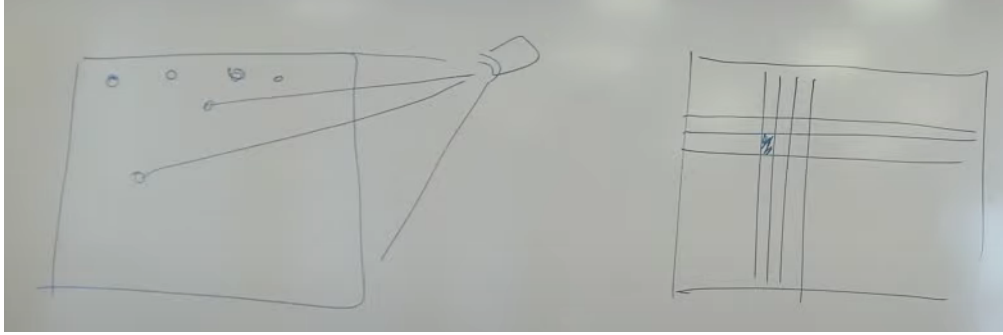
**Теорема 4.0.1.** Топологические модели — корректные модели ИИВ.

**Утверждение 4.0.1.**  $\not\models_I A \vee \neg A$ .

*Доказательство.* Пусть  $A = (0, +\infty)$ ,  $\neg A = (-\infty, 0)$ ,  $A \vee \neg A = \mathbb{R} \setminus \{0\} \neq \mathbb{R}$ . ■

## 4.1 Общая топология

Раньше были телевизоры с *бесконечным* количеством пикселей (это зависит от химических свойств вещества кинескоп).



Возьмем множество  $X$ . Определим на нем топологию как подмножество множества всех подмножеств  $\Omega \subseteq \mathcal{P}(X)$ .  $\Omega$  — топология, если это множество открытых множеств и выполнены следующие условия:

1.  $\emptyset, X \in \Omega$ ;
2.  $\bigcup_i \in \Omega$ , если все  $A_i \in \Omega$ ;
3.  $\bigcap_{i=1}^n A_i \in \Omega$ , если  $A_1, \dots, A_n \in \Omega$ .

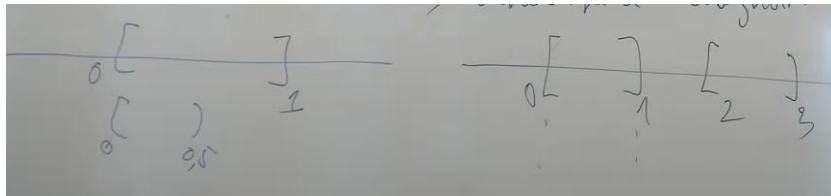
То есть топологическое пространство — пара  $\langle X, \Omega \rangle$  и про  $\Omega$  верны приведенные выше три утверждения.

**Определение 4.1.1** (Замкнутое множество). Множество  $B$  такое, что  $X \setminus B \in \Omega$  называется замкнутым.

**Определение 4.1.2** (Связное топологическое пространство).  $\langle X, \Omega \rangle$  связно, если нет  $A, B \in \Omega$  :  $A \cup B = X$  и  $A \cap B = \emptyset$

**Определение 4.1.3** (Подпространство).  $\langle X_1, \Omega_1 \rangle$  — подпространство  $\langle X, \Omega \rangle$ , если  $X_1 \subseteq X$  и  $\Omega_1 = \{a \cap X_1 \mid a \in \Omega\}$

**Определение 4.1.4** (Связное множество). Множество, являющееся связным подпространством.



## 4.2 Примеры топологических пространств

Возьмем дерево (граф). Множество  $X$  — множество вершин.  $\Omega$  — множество всех вершин, что  $B \in \Omega$ , если  $a \in B$ ,  $x \leq a$  влечет  $x \in B$ . То есть  $\Omega$  — семейство множеств вершин, которые входят вместе с поддеревом.

**Теорема 4.2.1.** Граф без цикла связан тогда и только тогда, когда оно связно как топологическое пространство.

*Доказательство будет в дз.* ■

**Определение 4.2.1** (Решетки).  $X$  — частично упорядоченное множество отношением  $\leq$ .

Множество верхних граней  $a, b$ :  $a \sqcap b$  — множество  $\{x \in X \mid a \leq x, b \leq x\}$ .

Множество нижних граней  $a, b$ :  $a \sqcup b$  — множество  $\{x \in X \mid a \geq x, b \geq x\}$ .

$a$  — наименьший элемент  $A \iff a \in A$  и не существует  $b \in A, b \leq a$ .

$a$  — наибольший элемент  $A \iff a \in A$  и не существует  $b \in A, b \geq a$ .

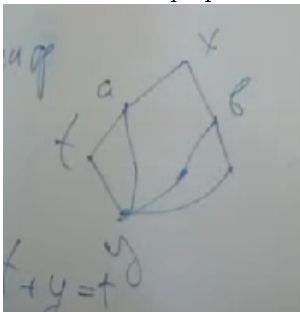
$a + b$  — наименьший элемент множества верхних граней.

$a \cdot b$  — наибольший элемент множества нижних граней.

Решетка — частично упорядоченное множество, где для любых двух элементов существуют  $a + b$  и  $a \cdot b$ .

**Пример.** Дерево — не решетка (в общем случае), так как  $a + b$  есть, а  $a \cdot b$  может не быть.

А вот такой граф является решеткой.



**Теорема 4.2.2.** Пусть  $\langle X, \Omega \rangle$  топологическое пространство,  $A, B \in \Omega$ .  $A \leq B$ , если  $A \subseteq B$ .

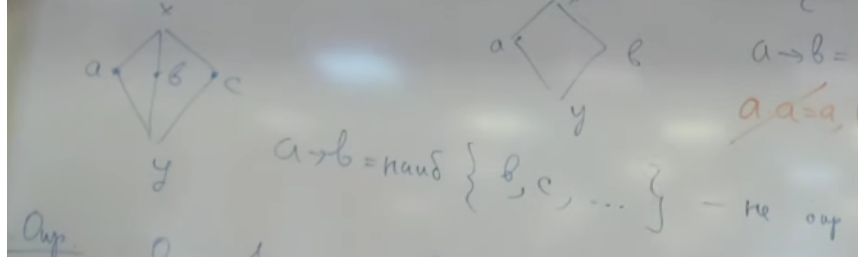
Тогда  $\langle \Omega, \leq \rangle$  — решетка.  $A \cdot B = A \cap B$ ,  $A + B = A \cup B$ .

**Определение 4.2.2.** Дистрибутивная решетка — это такая решетка, что  $a, b, c \in \Omega$ ,  $a + (b \cdot c) = (a + b) \cdot (a + c)$ .

**Лемма 4.2.2.1.** Для дистрибутивной решетки так же верно, что  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ .

**Определение 4.2.3.** Псевдодополнение  $a \rightarrow b = \text{наибольшее}\{c \mid a \cdot c \leq b\}$ .

**Определение 4.2.4.** Бриллиант — такая решетка, что там нет для кого-то псевдодополнения.



**Определение 4.2.5.** Решетка с псевдодополнением для всех элементов называется импликативной.

**Определение 4.2.6.** Определим 0 и 1 следующим образом:

- 0 — элемент, что  $0 \leq x$  при всех  $x$ ;
- 1 — элемент, что  $x \leq 1$  при всех  $x$ .

**Теорема 4.2.3** (В импликативной решетке 1 есть всегда).  $\langle X, \leq \rangle$  — импликативная решетка.

*Доказательство.* Рассмотрим  $a \rightarrow a = \text{наиб}\{c \mid a \cdot c \leq a\} = \text{наиб}\{X\} = 1$ . ■

**Теорема 4.2.4.** Рассмотрим  $\langle X, \Omega \rangle$  — импликативная решетка с 0. Рассмотрим И.И.В.

Определим оценки  $\Vdash = X$ :

- $\Vdash [\alpha \& \beta] = [\alpha] \cdot [\beta]$ .
- $\Vdash [\alpha \vee \beta] = [\alpha] + [\beta]$ .
- $\Vdash [\alpha \rightarrow \beta] = [\alpha] \rightarrow [\beta]$ .
- $\Vdash [\neg \alpha] = [\alpha] \rightarrow 0$ .

$\alpha$  истинно, если  $\Vdash [\alpha] = 1$ .

$\Vdash [\perp] = 0$ .  $\neg \alpha \equiv \alpha \rightarrow \perp$ .

Полученная модель — корректная модель И.И.В.

У нас будет натуральный вывод, интуиция и все такое.



$\overline{\Gamma, \varphi \vdash \varphi}$  (аксиома).

Вывод утверждения в доказательстве  $\Gamma \vdash \varphi$ .

Правила вывода (сверху — посылка, снизу — заключение):

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \rightarrow \psi}, \quad \frac{\Gamma, \varphi \vdash \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi}, \quad \frac{\Gamma, \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \& \psi}, \quad \frac{\Gamma, \vdash \varphi \& \psi}{\Gamma \vdash \varphi}, \quad \frac{\Gamma, \vdash \varphi \& \psi}{\Gamma \vdash \psi},$$
$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}, \quad \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}, \quad \frac{\Gamma, \varphi \vdash \rho \quad \Gamma, \psi \vdash \rho}{\Gamma \vdash \rho}, \quad \frac{\Gamma \vdash \varphi \vee \psi}{\Gamma \vdash \rho}, \quad \frac{\Gamma \vdash \perp}{\Gamma \vdash \varphi}.$$

Вот они, слева направо: введение  $\rightarrow$ , исключение  $\rightarrow$ , введение  $\&$ , два исключения  $\&$ , введения  $\vee$  в двух видах, исключение  $\vee$  и специальное правило для лжи.

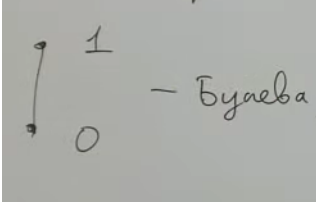
**Теорема 4.2.5.** Если  $\vdash_{\text{И}} \alpha \vee \beta$ , то  $\vdash_{\text{И}} \alpha$  или  $\vdash_{\text{И}} \beta$ .

**Определение 4.2.7.** Алгебра Гейтинга — импликативная решетка с 0.

**Определение 4.2.8.** Введем операцию  $\sim a \equiv a \rightarrow 0$  — дополнение до 0.

**Определение 4.2.9.** Булева алгебра — Алгебра Гейтинга, где  $a + \sim a = 1$ .

**Пример.** Булева Алгебра



- $\cdot$  соответствует  $\&$ ,
- $+$  соответствует  $\vee$ ,
- $\rightarrow$  соответствует  $\rightarrow$ ,
- $\sim$  соответствует  $\neg$ .

Далее  $\alpha, \beta$  — высказывания в ИИВ.

**Определение 4.2.10.**  $\alpha \leq \beta$ , если  $\alpha \vdash \beta$

**Определение 4.2.11.**  $\alpha \approx \beta$ , если  $\alpha \leq \beta$  и  $\beta \leq \alpha$

**Определение 4.2.12.** Пусть  $\xi$  — множество всех высказываний ИИВ.

Тогда  $[\xi]$  — называется алгеброй Линденбаума  $\mathcal{L}$ .

**Теорема 4.2.6.**  $\mathcal{L}$  — Алгебра Гейтинга.

**Лемма 4.2.6.1.**  $1 = [A \rightarrow A]$

*Доказательство.*  $\alpha \vdash A \rightarrow A$ , верно (очевидно), то есть  $[\alpha] \leq [A \rightarrow A]$ , то есть  $[A \rightarrow A] = 1$ . ■

**Теорема 4.2.7.**  $\mathcal{L}$  — корректная модель ИИВ.

**Теорема 4.2.8.**  $\mathcal{L}$  — полная модель ИИВ.

**Теорема 4.2.9.**  $\models \alpha$ , то есть  $[\alpha] = 1$ .

$1 = [A \rightarrow A]$ , то есть  $[\alpha] = 1$ , то есть  $\beta \leq [\alpha]$  при всех  $\beta$ .

Возьмем  $\beta = A \rightarrow A$ ,  $A \rightarrow A \vdash \alpha$ , то есть  $A \rightarrow A, (A \rightarrow A) \rightarrow \alpha$ .

**Теорема 4.2.10.** Алгебра Гейтинга — полная и корректная модель ИИВ.

**Определение 4.2.13.** Исчисление дизъюнктно, если для любых  $\alpha, \beta \vdash \alpha \vee \beta$  влечёт  $\vdash \alpha$  или  $\vdash \beta$ .

**Теорема 4.2.11.** ИИВ дизъюнктно.

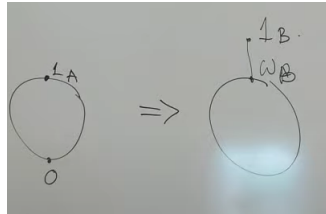
**Определение 4.2.14.** Пусть существует  $f : A \rightarrow B$ ,  $A, B$  — алгебры Гейтинга.

$f$  — гомоморфизм, если  $f(0_A) = 0_B$ ,  $f(1_A) = 1_B$  и  $f(\alpha \star_A \beta) = f(\alpha) \star_B f(\beta)$

**Определение 4.2.15** (Геделева Алгебра). Это такая алгебра, где  $a + b = 1$  влечет  $a = 1$  или  $b = 1$ .

**Определение 4.2.16** ( $\Gamma(A)$ ). Пусть  $A$  — алгебра Гейтинга.

Определим  $\gamma : A \rightarrow \Gamma(A)$  так:  $\gamma(x) = \begin{cases} \omega, & x = 1_A \\ x, & x < 1_A \end{cases}$  и добавим  $1_{\Gamma(A)} : t \leq 1_{\Gamma(A)}$ , если  $t \in \Gamma(A)$ .



**Замечание.**  $\Gamma(A)$  неофициально называется Геделеризацией.

**Теорема 4.2.12.**  $\Gamma(A)$  – Гёделева алгебра.

*Доказательство.* Пусть  $a + b = 1_{\Gamma(A)}$ , посмотрим на картинку. ■

**Утверждение 4.2.1.**  $\Gamma(\mathcal{L})$  – Гёделева алгебра.

*Доказательство.* Определим каноническое отображение  $g(x) : \Gamma(\mathcal{L}) \rightarrow \mathcal{L}$

$$g(x) = \begin{cases} 1 & , x = 1 \text{ или } \omega \\ x & , \text{ иначе} \end{cases}$$

**Утверждение 4.2.2.**  $g(x)$  – гомоморфизм ■

**Теорема 4.2.13.** Рассмотрим ИИВ и алгебры Гейтинга  $\mathcal{L}, \Gamma(\mathcal{L})$

**Утверждение 4.2.3.** Если  $g : A \rightarrow B$  и  $\llbracket \alpha \rrbracket_A = 1_A$ , то  $\llbracket \alpha \rrbracket_B = g(1_A)$ .

*Доказательство теоремы.* Рассмотрим  $\vdash \alpha \vee \beta$ .

$\Gamma(\mathcal{L})$  – Гёделева алгебра, то есть алгебра Гейтинга.

$\llbracket \alpha \vee \beta \rrbracket_{\Gamma(\mathcal{L})} = 1_{\Gamma(\mathcal{L})}$ , т.е. либо  $\llbracket \alpha \rrbracket = 1_{\Gamma(\mathcal{L})}$  либо  $\llbracket \beta \rrbracket_{\Gamma(\mathcal{L})} = 1_{\Gamma(\mathcal{L})}$

Рассмотрим  $g : \Gamma(\mathcal{L}) \rightarrow \mathcal{L}$

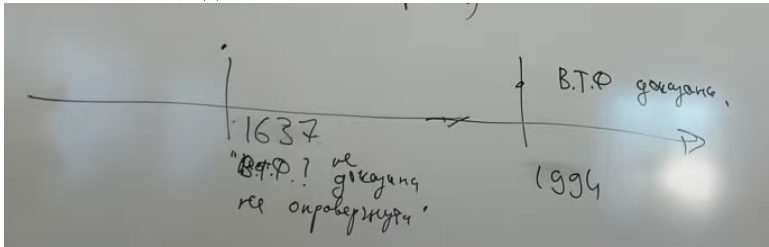
$\llbracket \alpha \rrbracket_{\Gamma(\mathcal{L})} = 1_{\Gamma(\mathcal{L})}$ , тогда  $\llbracket \alpha \rrbracket_{\mathcal{L}} = g(1_{\Gamma(\mathcal{L})}) = 1_{\mathcal{L}}$

т.е.  $\vdash \alpha$ . ■

**Определение 4.2.17.** Модель ИИВ называется табличной, если

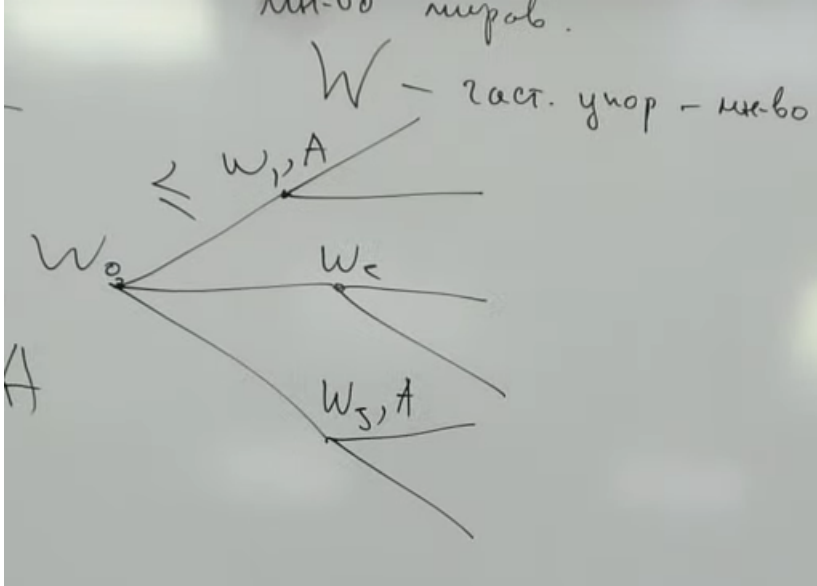
- $\mathbb{V} = \mathcal{S}$ ;
- $\llbracket \alpha \star \beta \rrbracket = f_{\star}(\llbracket \alpha \rrbracket, \llbracket \beta \rrbracket)$ ,
- Существует  $I \in \mathcal{S}$  – выделенная истина  $\llbracket \alpha \rrbracket = I$  тогда и только тогда, когда  $\vdash \alpha$

**Определение 4.2.18** (Модель Крипки). Некоторые факты, появившиеся на оси времени в истинном или ложном виде и больше не меняются



**Замечание.**  $W$  – частично упорядоченное множество миров.

**Определение 4.2.19.**  $\Vdash$



1. Вынужденность переменной  $A$  определяется моделью. При этом, если  $W_x \leq W_y$ ,  $W_x \Vdash A$ , то  $W_y \Vdash A$ .
2. Доопределим  $\Vdash$  на все выражения:
  - (a)  $W \Vdash A \wedge B$ , если  $W \Vdash A$  и  $W \Vdash B$
  - (b)  $W \Vdash A \vee B$ , если  $W \Vdash A$  или  $W \Vdash B$
  - (c)  $W \Vdash \neg A$ , если нет  $W \leq W_x$ , что  $W_x \Vdash A$
  - (d)  $W \Vdash A \rightarrow B$ , если во всех  $W \leq W_x$  из  $W_x \Vdash A$  следует  $W_x \Vdash B$

**Определение 4.2.20.**  $\models \alpha$  если  $W \vdash \alpha$ .

**Теорема 4.2.14.** У ИИВ нет полной конечной табличной модели.

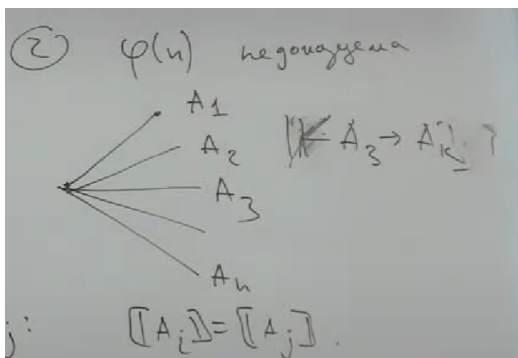
*Доказательство.*  $\varphi(u) = \bigvee_{i=1, j=1, i \neq j}^{n, n} A_i \rightarrow A_j$ .

Пусть  $T$  — модель,  $|\mathbb{V}| = n$ .

Рассмотрим  $\varphi(n+1)$ . По принципу Дирихле. Есть  $A_j$  и  $A_i$ :  $\llbracket A_j \rrbracket = \llbracket A_i \rrbracket$ .

Несложно показать  $\llbracket A_i \rightarrow A_j \rrbracket = \text{И} \implies \llbracket \varphi(n+1) \rrbracket = \text{И}$ .

Рассмотрим модель, где  $\varphi(n)$  не доказуемо ни при каком  $n$ .



$\llbracket A_3 \rightarrow A_k \rrbracket = \mathcal{L}.$

**Теорема 4.2.15.** Модель Крипке — корректная модель ИИВ.

### 4.3 Изоморфизм Кари–Ховарда

**Утверждение 4.3.1.**  $\tau, \sigma$  — типы.

$\tau \rightarrow \sigma$

```
1  f(x :  $\tau$ ):  $\sigma$  {
2      return g(x);
3  }
```

$\tau \& \sigma$

```
1  f(x:  $\tau$ , y:  $\sigma$ )
```

$\tau \vee \sigma$

```
1  f(x: std.variant< $\tau$ ,  $\sigma$ 
```

**Определение 4.3.1** (Изоморфизм Кари–Ховарда). Программа соответствует доказательству. Тип соответствует утверждению. ...  
(всё в интуиционистской логике)

**Замечание.**  $f: \neg\neg\alpha \rightarrow \alpha$  — потом подумаем как это интерпретировать.

## 5 Исчисление предикатов

Нам нужен новый язык. В текущем языке всё хорошо, но он имеет малую выразительную силу. Косвенным свидетельством этого является то, что в нём всё легко разрешается.

В чём была исходная цель Гильберта: формализовать всю математику и доказывать всё, не боясь того, что будет противоречие где-нибудь.

**Пример.**  $\frac{\text{Каждый человек смертен} \quad \text{Сократ человек}}{\text{Сократ смертен}}$   
 $\frac{\text{Каждый объект, если он — человек, то он — смертен} \quad \text{Сократ — человек}}{\text{Сократ — смертен}}$   
 Цель: **кванторы** и **предикаты**.

$$\frac{\forall x. H(x) \rightarrow S(x) \quad H(\text{Сократ})}{S(\text{Сократ})}.$$

Идея: нам нужно построить некоторый язык и затем поверх него построить теорию моделей и теорию доказательств.

**Пример.**  $\forall x. \sin x = 0 \vee (\sin^2 x) + 1 > 1.$

- Предметные (здесь: числовые) выражения

- Предметные переменные  $x$ .
- Одно- и двуместные функциональные символы «синусы», «возведение в квадрат» и «сложение».
- Нульместные функциональные символы «ноль» (0) и «один» (1).
- Логические выражения
  - Предикатные символы «равно» и «больше».

## 5.1 Язык исчисления предикатов

1. Два типа: предметные и логические выражения
2. Предметные выражения: метAPEReменная  $\theta$ 
  - Предметные переменные:  $a, b, c, \dots$ , метAPEReменные  $x, y$ .
  - Функциональные выражения:  $f(\theta_1, \dots, \theta_n)$ , метAPEReменные  $f, g, \dots$
  - Примеры:  $r, q(p(x, s), r)$
3. Логические выражения: метAPEReменные  $\alpha, \beta, \gamma, \dots$ 
  - Предикатные выражения:  $P(\theta_1, \dots, \theta_n)$ , метAPEReменная  $P$ .  
Имена:  $A, B, C, \dots$ ,
  - Связки:  $(\varphi \vee \psi), (\varphi \rightarrow \psi), (\varphi \leftrightarrow \psi), (\neg \varphi)$
  - Кванторы:  $(\forall x. \varphi)$  и  $(\exists x. \varphi)$ .

Сокращенные записи, метаязык

1. МетAPEReменные:
  - $\psi, \phi, \pi, \dots$  — формулы
  - $P, Q, \dots$  — предикатные символы
  - $\theta, \dots$  — термы
  - $f, g, \dots$  — функциональные символы
  - $x, y, \dots$  — предметные переменные
2. Скобки — как в И.В.; квантор — жадный:

$$\underbrace{(\forall a. A \vee B \vee C \rightarrow \exists b. \underbrace{D \& \neg E}_{\exists b. \dots}) \& F}_{\forall a. \dots}$$

3. Дополнительные обозначения при необходимости:

- $(\theta_1 = \theta_2)$  вместо  $E(\theta_1, \theta_2)$ .
- $(\theta_1 + \theta_2)$  вместо  $p(\theta_1, \theta_2)$ .
- 0 вместо  $z$ .

Напомним формулу:

$$\forall x. \sin x = 0 \vee (\sin x)^2 + 1 > 1$$

Без синтаксического сахара:

$$\forall x. E(f(x), z) \vee G(p(q(s(x)), o), o)$$

## 5.2 Два вида значений

### 1. Истинностные (логические) значения:

- (а) предикаты (в том числе пропозициональные переменные = нульместные предикаты);
- (б) логические связки и кванторы.

### 2. Предметные значения:

- (а) предметные переменные;
- (б) функциональные символы (в том числе константы = нульместные функциональные символы)

## 5.3 Оценка исчисления предикатов

**Определение 5.3.1.** Оценка — упорядоченная четвёрка  $\langle D, F, T, E \rangle$ , где:

- 1.  $D$  — предметное множество;
- 2.  $F$  — оценка для функциональных символов. Пусть  $f_n$  —  $n$ -местный функциональный символ:

$$F_{f_n} : D^n \rightarrow D$$

- 3.  $T$  — оценка для предикатных символов. Пусть  $P_n$  —  $n$ -местный предикатный символ:

$$T_{P_n} : D^n \rightarrow V \quad V = \{И, Л\}$$

- 4.  $E$  — оценка для свободных предметных переменных.

$$E(x) \in D$$

Запись и сокращения записи подобны исчислению высказываний:

$$\llbracket \phi \rrbracket \in V, \quad \llbracket E(x, f(x)) \vee R \rrbracket^{x:=1, f(t):=t^2, R:=И} = И$$

- 1. Правила для связок  $\vee, \&, \neg, \rightarrow$  остаются прежние;
- 2.  $\llbracket f_n(\theta_1, \theta_2, \dots, \theta_n) \rrbracket = F_{f_n}(\llbracket \theta_1 \rrbracket, \llbracket \theta_2 \rrbracket, \dots, \llbracket \theta_n \rrbracket)$
- 3.  $\llbracket P_n(\theta_1, \theta_2, \dots, \theta_n) \rrbracket = T_{P_n}(\llbracket \theta_1 \rrbracket, \llbracket \theta_2 \rrbracket, \dots, \llbracket \theta_n \rrbracket)$
- 4.  $\llbracket \forall x. \phi \rrbracket = \begin{cases} И, & \text{если } \llbracket \phi \rrbracket^{x:=t} = И \text{ при всех } t \in D \\ Л, & \text{если найдётся } t \in D, \text{ что } \llbracket \phi \rrbracket^{x:=t} = Л \end{cases}$
- 5.  $\llbracket \exists x. \phi \rrbracket = \begin{cases} И, & \text{если найдётся } t \in D, \text{ что } \llbracket \phi \rrbracket^{x:=t} = И \\ Л, & \text{если } \llbracket \phi \rrbracket^{x:=t} = Л \text{ при всех } t \in D \end{cases}$

**Пример.**  $\llbracket \forall x. \exists y. \neg x + 1 = y \rrbracket$

Зададим оценку:

- $D := \mathbb{N}$ ;
- $F_1 := 1, F_{(+)} — сложение в  $\mathbb{N}$ ;$
- $P_{(=)}$  — равенство в  $\mathbb{N}$ .

Фиксируем  $x \in \mathbb{N}$ . Тогда  $\llbracket x + 1 = y \rrbracket^{y:=x} = Л$  поэтому при любом  $x \in \mathbb{N}$ :

$$\llbracket \exists y. \neg x + 1 = y \rrbracket = И.$$

Итого:  $\llbracket \forall x. \exists y. \neg x + 1 = y \rrbracket = И$

**Пример.** Странная интерпретация  $\llbracket \forall x. \exists y. \neg(x + 1 = y) \rrbracket$ .

Зададим интерпретацию:

- $D := \{\square\}$ ;
- $F_{(1)} := \square$ ,  $F_{(+)}(x, y) := \square$ ;
- $P_{(=)}(x, y) := I$ .

Тогда:  $\llbracket x + 1 = y \rrbracket^{x \in D, y \in D} = I$ .

Итого:  $\llbracket \forall x. \exists y. \neg x + 1 = y \rrbracket = I$ .

Поэтому формулам оценки предикатов верить нельзя. Никакой интуиции за ними может и не стоять.

**Определение 5.3.2.** Формула общезначима, если истинна при любой оценке.

**Утверждение 5.3.1.**  $\llbracket \forall x. Q(f(x)) \vee \neg Q(f(x)) \rrbracket = I$ .

*Доказательство.* Фиксируем  $D, F, P, E$ . Пусть  $x \in D$ . Обозначим  $P_Q(F_f(E_x))$  за  $t$ . Ясно, что  $t \in V$ . Разберём случаи.

- Если  $t = I$ , то  $\llbracket P(f(x)) \rrbracket^{P(f(x)) := t} = I$ , потому  $\llbracket P(f(x)) \vee \neg P(f(x)) \rrbracket^{P(f(x)) := t} = I$ .
- Если  $t = I$ , то  $\llbracket \neg P(f(x)) \rrbracket^{P(f(x)) := t} = I$  потому всё равно  $\llbracket P(f(x)) \vee \neg P(f(x)) \rrbracket^{P(f(x)) := t} = I$ .

■

## 5.4 Подстановки, свобода и связность

**Определение 5.4.1.** Рассмотрим формулу  $\forall x. \psi$  (или  $\exists x. \psi$ ). Здесь переменная  $x$  связана в  $\psi$ . Все вхождения переменной  $x$  в  $\psi$  — **связанные**.

**Определение 5.4.2.** Переменная  $x$  входит свободно в  $\psi$ , если не находится в области действия никакого квантора по  $x$ . Все её вхождения в  $\psi$  — **свободные**.

**Пример.**  $\exists y. (\forall x. P(x)) \vee P(x) \vee Q(y)$ .

Единственное свободное вхождение переменной  $x$  помечено синим цветом.

**Определение 5.4.3.** Подстановка — это ...

$$\psi[x := \theta] := \begin{cases} \psi, & \psi \equiv y, y \neq x \\ \psi, & \psi \equiv \forall x. \pi \text{ или } \psi \equiv \exists x. \pi \\ \pi[x := \theta] \star \rho[x := \theta], & \psi \equiv \pi \star \rho \\ \theta, & \psi \equiv x \\ \forall y. \pi[x := \theta], & \psi \equiv \forall y. \pi \text{ и } y \neq x \\ \exists y. \pi[x := \theta], & \psi \equiv \exists y. \pi \text{ и } y \neq x \end{cases}$$

**Определение 5.4.4.** Терм  $\theta$  свободен для подстановки вместо  $x$  в  $\psi$  ( $\psi[x := \theta]$ ), если ни одно свободное вхождение переменной в  $\theta$  не станет связным после подстановки.

Свобода есть:  $(\forall x. P(y))[y := z]$  или  $(\forall x. \forall y. P(x))[y := z]$ .

Свободы нет:  $(\forall x. P(y))[y := x]$  и  $(\forall y. \forall x. P(t))[t := y]$ .



## 5.5 Теория доказательств

Рассмотрим язык исчисления предикатов. Аксиомы $\ddot{E}$ — все схемы аксиом для классического исчисления высказываний в данном языке.

- |   |  |
|---|--|
| 1. $\alpha \rightarrow \beta \rightarrow \alpha$  | 6. $\alpha \rightarrow \alpha \vee \beta$  |
| 2. $(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \gamma)$ | 7. $\beta \rightarrow \alpha \vee \beta$   |
| 3. $\alpha \wedge \beta \rightarrow \alpha$   | 8. $(\alpha \rightarrow \gamma) \rightarrow (\beta \rightarrow \gamma) \rightarrow (\alpha \vee \beta \rightarrow \gamma)$ |
| 4. $\alpha \wedge \beta \rightarrow \beta$  | 9. $(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \neg \beta) \rightarrow (\neg \alpha)$                      |
| 5. $\alpha \rightarrow \beta \rightarrow \alpha \wedge \beta$   | 10. $\neg \neg \alpha \rightarrow \alpha$  |

Добавим ещё две схемы аксиом (здесь везде  $\theta$  свободен для подстановки вместо  $x$  в  $\varphi$ ):

$$11. (\forall x.\varphi) \rightarrow \varphi[x := \theta]$$

$$12. \varphi[x := \theta] \rightarrow \exists x.\varphi$$

Добавим ещё два правила вывода (здесь везде  $x$  не входит свободно в  $\varphi$ ):

$$1. \text{ Введение } \forall: \frac{\varphi \rightarrow \forall x.\psi}{\varphi \rightarrow \psi},$$

$$2. \text{ Введение } \exists: \frac{(\exists x.\psi) \rightarrow \varphi}{\psi \rightarrow \varphi}.$$

**Утверждение 5.5.1.** Доказуемость, выводимость, полнота, корректность — аналогично исчислению высказываний.

## 5.6 Теорема о дедукции для исчисления предикатов

**Теорема 5.6.1.** Если  $\Gamma \vdash \alpha \rightarrow \beta$ , то  $\Gamma, \alpha \vdash \beta$ . Если  $\Gamma, \alpha \vdash \beta$  и в доказательстве не применяются правила для кванторов по свободным переменным из  $\alpha$ , то  $\Gamma \vdash \alpha \rightarrow \beta$

*Доказательство.*

$\Rightarrow$  также как в К.И.В

$\Leftarrow$  та же схема. У нас появились два новых случая аксиом. Ничего страшного, с ним проблем не возникнет.

Однако таже слоедует обработать два новых правила вывода.

Перестроим:  $\delta_1, \delta_2, \dots, \delta_n \equiv \beta$  в  $\alpha \rightarrow \delta_1, \alpha \rightarrow \delta_2, \dots, \alpha \rightarrow \delta_n$ .

Дополним: обоснуем  $\alpha \rightarrow \delta_n$ , если предыдущие уже обоснованы (по индукции).

Два новых похожих случая: правила для  $\forall$  и  $\exists$ . Рассмотрим  $\forall$ . Для квантора существования аналогично.

Доказываем переход к  $(n)$ .  $\alpha \rightarrow \psi \rightarrow \forall x.\varphi$  (правило для  $\forall$ ), значит, доказано на шаге  $k$ , что  $\alpha \rightarrow \psi \rightarrow \varphi$ .

$$(n - 0.9) \dots (n - 0.8) \quad (\alpha \rightarrow \psi \rightarrow \varphi) \rightarrow (\alpha \& \psi) \rightarrow \varphi$$

$$(n - 0.6) \quad (\alpha \rightarrow \psi) \rightarrow \varphi$$

$$(n - 0.4) \quad (\alpha \rightarrow \psi) \rightarrow \forall x.\varphi$$

$$(n - 0.3) \dots (n - 0.2) \quad ((\alpha \rightarrow \psi) \rightarrow \forall x.\varphi) \rightarrow (\alpha \rightarrow \psi \rightarrow \forall x.\varphi)$$

$$(n) \quad \alpha \rightarrow \psi \rightarrow \forall x.\varphi$$

Т. о полноте КИВ

М.Р.  $k, n - 0.8$

Правило для  $\forall$ ,  $n - 0.6$

Т. о полноте КИВ

М.Р.  $n - 0.4, n - 0.2$

■

## 5.7 Отношение следования

**Определение 5.7.1** (Следование).  $\gamma_1, \gamma_2, \dots, \gamma_n \models \alpha$ , если выполнено два условия:

1.  $\alpha$  выполнено всегда, когда выполнено  $\gamma_1, \gamma_2, \dots, \gamma_n$ ;
2.  $\alpha$  не использует кванторов по переменным, входящим свободно в  $\gamma_1, \gamma_2, \dots, \gamma_n$ .

**Теорема 5.7.1.** Если  $\Gamma \vdash \alpha$  и в доказательстве не используется кванторов по свободным переменным из  $\Gamma$ , то  $\Gamma \models \alpha$ .

Влажность второго условия.

**Пример.** Покажем, что  $\Gamma \models \alpha$  ведёт себя неестественно, если в  $\alpha$  используются кванторы по переменным, входящим свободно в  $\Gamma$ .

Легко показать, что  $P(x) \vdash \forall x.P(x)$ .

- |     |   |                           |
|-----|---|---------------------------|
| (1) | $P(x)$  | Гипотеза                  |
| (2) | $P(x) \rightarrow (A \rightarrow A \rightarrow A) \rightarrow P(x)$ | Сх. акс. 1                |
| (3) | $(A \rightarrow A \rightarrow A) \rightarrow P(x)$                  | М.Р. 1, 2                 |
| (4) | $(A \rightarrow A \rightarrow A) \rightarrow \forall x.P(x)$        | Правило для $\forall$ , 3 |
| (5) | $(A \rightarrow A \rightarrow A)$                                   | Сх. акс. 1                |
| (6) | $\forall x.P(x)$  | М.Р. 5, 4                 |

Пусть  $D = \mathbb{Z}$  и  $P(x) = x > 0$ . Тогда не будет выполнено  $P(x) \models \forall x.P(x)$ .

Зачем нам это потребовалось? Мы будем пользоваться, но не злоупотреблять.

Мы не хотим заранее сильно ограничивать язык. Поэтому мы выбираем такой вариант, чтобы он разрешал некоторые.

## 5.8 Теорема о полноте исчисления предикатов

1. Надо справиться со слишком большим количеством вариантов. Модель задаётся как  $\langle D, F, P, X \rangle$ .
2. Для оценки в модели важно только какие формулы истинны. Модели  $\mathcal{M}_1$  и  $\mathcal{M}_2$  «похожи», если  $\llbracket \varphi \rrbracket_{\mathcal{M}_1} = \llbracket \varphi \rrbracket_{\mathcal{M}_2}$  при всех  $\varphi$ .
3. Поступим так:
  - (а) построим эталонное множество моделей  $\mathfrak{M}$ , каждая модель соответствует списку истинных формул, *но им не является*;
  - (б) докажем полноту  $\mathfrak{M}$ : если каждая  $\mathcal{M} \in \mathfrak{M}$  предполагает  $\mathcal{M} \models \varphi$ , то  $\vdash \varphi$ ;
  - (в) заметим, что если  $\models \varphi$ , то каждая  $\mathcal{M} \in \mathfrak{M}$  предполагает  $\mathcal{M} \models \varphi$ .
4. В ходе доказательства нас ждёт множество технических препятствий.

### 5.8.1 Непротиворечивое множество формул

**Определение 5.8.1.**  $\Gamma$  — *непротиворечивое множество формул*, если  $\Gamma \not\vdash \alpha \& \neg \alpha$  при некотором  $\alpha$ .

**Пример.** Непротиворечиво:

- $\Gamma = \{A \rightarrow B \rightarrow A\}$
- $\Gamma = \{P(x, y) \rightarrow \neg P(x, y), \forall x. \forall y. \neg P(x, y)\}$ ;

Противоречиво:

- $\Gamma = \{P \rightarrow \neg P, \neg P \rightarrow P\}$  так как  $P \rightarrow \neg P, \neg P \rightarrow P \vdash \neg P \& \neg \neg P$ .

Пусть  $D = \mathbb{Z}$  и  $P(x) \equiv (x > 0)$ , аналогом для этой модели будет  $\Gamma = \{P(1), P(2), P(3), \dots\}$ .

На самом деле, нам этого не достаточно. Нам нужно некоторое **полное непротиворечивое множество формул**.

**Определение 5.8.2.**  $\Gamma$  — **полное** непротиворечивое множество замкнутых **бескванторных** формул, если:

1.  $\Gamma$  содержит только замкнутые бескванторные формулы;
2. если  $\alpha$  — некоторая замкнутая бескванторная формула, то  $\alpha \in \Gamma$  или  $\neg\alpha \in \Gamma$ .

**Определение 5.8.3.**  $\Gamma$  — **полное** непротиворечивое множество замкнутых формул, если:

1.  $\Gamma$  содержит только замкнутые формулы;
2. если  $\alpha$  — некоторая замкнутая формула, то  $\alpha \in \Gamma$ , или  $\neg\alpha \in \Gamma$ .

**Теорема 5.8.1** (Пополнение непротиворечивого множества формул). Пусть  $\Gamma$  — непротиворечивое множество замкнутых (бескванторных) формул. Тогда, какова бы ни была замкнутая (бескванторная) формула  $\varphi$ , хотя бы  $\Gamma \cup \{\varphi\}$  или  $\Gamma \cup \{\neg\varphi\}$  — непротиворечиво.

*Доказательство.* Пусть это не так и найдутся такие  $\Gamma$ ,  $\varphi$  и  $\alpha$ , что

$$\begin{aligned} \Gamma, \varphi &\vdash \alpha \& \neg\alpha \\ \Gamma, \neg\varphi &\vdash \alpha \& \neg\alpha. \end{aligned}$$

Тогда по лемме об исключении гипотезы  $\Gamma \vdash \alpha \& \neg\alpha$ .

То есть  $\Gamma$  не является непротиворечивым. Противоречие. ■

**Теорема 5.8.2** (Дополнение непротиворечивого множества формул до полного). Пусть  $\Gamma$  — непротиворечивое множество замкнутых (бескванторных) формул. Тогда найдётся полное непротиворечивое множество замкнутых (бескванторных) формул  $\Delta$ , что  $\Gamma \subseteq \Delta$ .

*Доказательство.* 1. Занумеруем все формулы (их счётное количество):  $\varphi_1, \varphi_2, \dots$

2. Построим семейство множеств  $\{\Gamma_i\}$ :

$$\Gamma_0 = \Gamma \quad \Gamma_{i+1} = \begin{cases} \Gamma_i \cup \{\varphi_i\}, & \text{если } \Gamma_i \cup \{\varphi_i\} \text{ непротиворечиво} \\ \Gamma_i \cup \{\neg\varphi_i\}, & \text{иначе} \end{cases}$$

3. Итоговое множество

$$\Delta = \bigcup_i \Gamma_i$$

4. Непротиворечивость  $\Delta$  не следует из индукции — индукция гарантирует непротиворечивость только  $\Gamma_i$  при натуральном (т.е. *конечном*)  $i$ , потому...

$\Delta$  непротиворечиво:

1. Пусть  $\Delta$  противоречиво, то есть  $\Delta \vdash \alpha \& \neg\alpha$ .
2. Доказательство конечной длины и использует конечное количество гипотез  $\{\delta_1, \delta_2, \dots, \delta_n\} \subset \Delta$ , то есть  $\delta_1, \delta_2, \dots, \delta_n \vdash \alpha \& \neg\alpha$ .
3. Пусть  $\delta_i \in \Gamma_{d_i}$ , тогда  $\Gamma_{d_1} \cup \Gamma_{d_2} \cup \dots \cup \Gamma_{d_n} \vdash \alpha \& \neg\alpha$ .

4. Но  $\Gamma_{d_1} \cup \Gamma_{d_2} \cup \dots \cup \Gamma_{d_n} = \Gamma_{\max(d_1, d_2, \dots, d_n)}$ , которое непротиворечиво, и потому

$$\Gamma_{d_1} \cup \Gamma_{d_2} \cup \dots \cup \Gamma_{d_n} \not\models \alpha \& \neg \alpha.$$

■

### 5.8.2 Модель для множества формул

**Определение 5.8.4** (Модель для множества формул). Моделью для множества формул  $F$  назовём такую модель  $\mathcal{M}$ , что при всяком  $\varphi \in F$  выполнено  $\llbracket \varphi \rrbracket_{\mathcal{M}} = \mathcal{I}$ .

Альтернативное обозначение:  $\mathcal{M} \models \varphi$ .

**Теорема 5.8.3** (О доказательстве непротиворечивости множества формул). Если у множества формул  $M$  есть модель  $\mathcal{M}$ , оно непротиворечиво.

*Доказательство.* Пусть противоречиво:  $M \vdash A \& \neg A$ , в доказательстве использованы гипотезы  $\delta_1, \delta_2, \dots, \delta_n$ .

Тогда  $\vdash \delta_1 \rightarrow \delta_2 \rightarrow \dots \rightarrow \delta_n \rightarrow A \& \neg A$ , то есть  $\llbracket \delta_1 \rightarrow \delta_2 \rightarrow \dots \rightarrow \delta_n \rightarrow A \& \neg A \rrbracket = \mathcal{I}$  (корректность).

Поскольку все  $\llbracket \delta_i \rrbracket_{\mathcal{M}} = \mathcal{I}$ , то и  $\llbracket A \& \neg A \rrbracket_{\mathcal{M}} = \mathcal{I}$  (анализ таблицы истинности импликации).

Однако,  $\llbracket A \& \neg A \rrbracket = \mathcal{L}$ . Противоречие. ■

**Теорема 5.8.4.** Любое непротиворечивое множество замкнутых бескванторных формул имеет модель.

Как построить такую модель?

**Определение 5.8.5.** Пусть  $M$  — полное непротиворечивое множество замкнутых бескванторных формул. Тогда модель  $\mathcal{M}$  задаётся так:

1.  $D$  — множество всевозможных предметных выражений без предметных переменных и дополнительная строка “ошибка!”
2.  $\llbracket f(\theta_1, \dots, \theta_n) \rrbracket = \text{“}f(\text{“} \llbracket \theta_1 \rrbracket + \text{“},\text{”} \# \dots \# \text{“},\text{”} \# \llbracket \theta_n \rrbracket + \text{“})\text{”}$
3.  $\llbracket P(\theta_1, \dots, \theta_n) \rrbracket = \begin{cases} \mathcal{I}, & \text{если “}P(\text{“} \llbracket \theta_1 \rrbracket + \text{“},\text{”} \# \dots \# \text{“},\text{”} \# \llbracket \theta_n \rrbracket + \text{“})\text{”} \in M \\ \mathcal{L}, & \text{иначе} \end{cases}$
4.  $\llbracket x \rrbracket = \text{“ошибка!”}$ , так как формулы замкнуты.

**Лемма 5.8.4.1.** Пусть  $\varphi$  — бескванторная формула, тогда  $\mathcal{M} \models \varphi$  тогда и только тогда, когда  $\varphi \in M$ .

*Доказательство.* Индукция по длине формулы  $\varphi$ .

1. База.  $\varphi$  — предикат. Требуемое очевидно по определению  $\mathcal{M}$ .

2. Переход. Пусть  $\varphi = \alpha \star \beta$  (или  $\varphi = \neg \alpha$ ), причём  $\mathcal{M} \models \alpha$  ( $\mathcal{M} \models \beta$ ) тогда и только тогда, когда  $\alpha \in M$  ( $\beta \in M$ ).

Тогда покажем требуемое для каждой связки в отдельности. А именно, для каждой связки покажем два утверждения:

- (а) если  $\mathcal{M} \models \alpha \star \beta$ , то  $\alpha \star \beta \in M$ .
- (б) если  $\mathcal{M} \not\models \alpha \star \beta$ , то  $\alpha \star \beta \notin M$ .

■

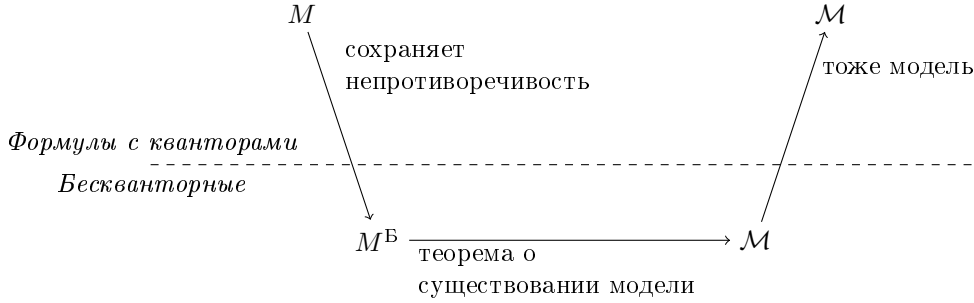
*Доказательство теоремы о существовании модели.* Пусть  $M$  — непротиворечивое множество замкнутых бескванторных формул.

По теореме о пополнении существует  $M'$  — полное непротиворечивое множество замкнутых бескванторных формул, что  $M \subseteq M'$ .

По лемме  $M'$  имеет модель, эта модель подойдёт для  $M$ . ■

**Теорема 5.8.5** (Гёделя о полноте исчисления предикатов). Если  $M$  — непротиворечивое множество замкнутых формул, то оно имеет модель.

*Схема доказательства.* Мы умеем строить только модель без кванторов. Возьмем исходное множество формул, избавимся от кванторов, построим модель (это делать мы уже умеем), а потом покажем, что построенная модель нам подходит.



**Определение 5.8.6.** Формула  $\varphi$  имеет поверхностные кванторы (находится в предварённой форме), если соответствует грамматике

$$\varphi := \forall x.\varphi \mid \exists x.\varphi \mid \tau,$$

где  $\tau$  — формула без кванторов

**Теорема 5.8.6.** Для любой замкнутой формулы  $\psi$  найдётся такая формула  $\varphi$  с поверхностными кванторами, что  $\vdash \psi \rightarrow \varphi$  и  $\vdash \varphi \rightarrow \psi$ .

*Доказательство.* Индукция по структуре, применение теорем о перемещении кванторов (из 5 ДЗ). ■

### 5.8.3 Построение $M^*$

- Пусть  $M$  — полное непротиворечивое множество замкнутых формул с поверхностными кванторами (очевидно, счётное). Построим семейство непротиворечивых множеств замкнутых формул  $M_k$ .
- Пусть  $d_i^k$  — семейство *свежих* констант, в  $M$  не встречающихся.
- Индуктивно построим  $M_k$ :
  - База:  $M_0 = M$
  - Переход: положим  $M_{k+1} = M_k \cup S$ , где множество  $S$  получается перебором всех формул  $\varphi_i \in M_k$ .
    1.  $\varphi_i$  — формула без кванторов, пропустим
    2.  $\varphi_i = \forall x.\psi$  — добавим к  $S$  все формулы вида  $\psi[x := \theta]$ , где  $\theta$  — всевозможные замкнутые термы, использующие символы из  $M_k$ ;
    3.  $\varphi_i = \exists x.\psi$  — добавим к  $S$  формулу  $\psi[x := d_i^{k+1}]$ , где  $d_i^{k+1}$  — некоторая свежая ранее не использовавшаяся в  $M_k$  константа.

**Лемма 5.8.6.1.** Если  $M$  непротиворечиво, то каждое множество из  $M_k$  — непротиворечиво

*Доказательство.* Доказательство по индукции, база очевидна ( $M_0 = M$ ). Переход:

- пусть  $M_k$  непротиворечиво, но  $M_{k+1}$  — противоречиво:  $M_k, M_{k+1} \setminus M_k \vdash A \& \neg A$
- Тогда (т.к. доказательство конечной длины):  $M_k, \gamma_1, \gamma_2, \dots, \gamma_n \vdash A \& \neg A$  где  $\gamma_i \in M_{k+1} \setminus M_k$ .
- По теореме о дедукции:  $M_k \vdash \gamma_1 \rightarrow \gamma_2 \rightarrow \dots \rightarrow \gamma_n \rightarrow A \& \neg A$
- Научимся выкидывать первую посылку:  $M_k \vdash \gamma_2 \rightarrow \dots \rightarrow \gamma_n \rightarrow A \& \neg A$
- И по индукции придём к противоречию:  $M_k \vdash A \& \neg A$ .

■

**Лемма 5.8.6.2.** Если  $M_k \vdash \gamma \rightarrow W$ , и  $\gamma \in M_{k+1} \setminus M_k$ , то  $M_k \vdash W$ .

*Доказательство.* Покажем, как дополнить доказательство до  $M_k \vdash W$ , в зависимости от происхождения  $\gamma$ :

- Случай  $\forall x.\varphi$ :  $\gamma = \varphi[x := \theta]$ .

Допишем в конец доказательства:

|  |               |
|--|---------------|
| $\forall x.\varphi$                                      | (гипотеза)    |
| $(\forall x.\varphi) \rightarrow (\varphi[x := \theta])$ | (сх. акс. 11) |
| $\gamma$   | (М.Р.)        |
| $W$  | (М.Р.)        |

Отдельно случай квантора существования.

- $\gamma = \varphi[x := d_i^{k+1}]$
- Перестроим доказательство  $M_k \vdash \gamma \rightarrow W$ : заменим во всём доказательстве  $d_i^{k+1}$  на  $y$ . Коллизий нет: под квантором  $d_i^{k+1}$  не стоит, переменной не является.
- Получим доказательство  $M_k \vdash \gamma[d_i^{k+1} := y] \rightarrow W$  и дополним его:

|   |  |
|---|--|
| $\varphi[x := y] \rightarrow W$                               | $\varphi[x := d_i^{k+1}][d_i^{k+1} := y]$  |
| $(\exists y.\varphi[x := y]) \rightarrow W$                   | $y$ не входит в $W$  |
| $(\exists x.\varphi) \rightarrow (\exists y.\varphi[x := y])$ | доказуемо (упражнение)   |
| ...   |  |
| $(\exists x.\varphi) \rightarrow W$                           | доказуемо как $(\alpha \rightarrow \beta) \rightarrow (\beta \rightarrow \gamma) \vdash \alpha \rightarrow \gamma$ |
| $\exists x.\varphi$   | гипотеза   |
| $W$   |  |

■

#### 5.8.4 Построение $M^B$

**Определение 5.8.7.**  $M^* = \bigcup_k M_k$

**Теорема 5.8.7.**  $M^*$  непротиворечиво.

*Доказательство.* От противного: доказательство противоречия конечной длины, гипотезы лежат в максимальном  $M_k$ , тогда  $M_k$  противоречив. ■

**Определение 5.8.8.**  $M^B$  — множество всех бескванторных формул из  $M^*$ .

По непротиворечивому множеству  $M$  можем построить  $M^B$  и для него построить модель  $\mathcal{M}$ . Покажем, что эта модель годится для  $M^*$  (и для  $M$ , так как  $M \subset M^*$ ).

### 5.8.5 Построение модели для $M^*$

**Определение 5.8.9.**  $\mathcal{M}$  есть модель для  $M^*$ .

*Доказательство.* Покажем, что при  $\varphi \in M^*$  выполнено  $\mathcal{M} \models \varphi$ . Докажем индукцией по количеству кванторов в  $\varphi$ .

- База:  $\varphi$  без кванторов. Тогда  $\varphi \in M^B$ , откуда  $\mathcal{M} \models \varphi$  по построению  $\mathcal{M}$
- Переход: пусть утверждение выполнено для всех формул с  $n$  кванторами. Покажем, что это выполнено и для  $n + 1$  кванторов.
  - Рассмотрим  $\varphi = \exists x.\psi$ , случай квантор всеобщности — аналогично.
  - Раз  $\exists x.\psi \in M^*$ , то существует  $k$ , что  $\exists x.\psi \in M_k$ .
  - Значит,  $\psi[x := d_i^{k+1}] \in M_{k+1}$ .
  - По индукционному предположению,  $\mathcal{M} \models \psi[x := d_i^{k+1}]$  — в формуле  $n$  кванторов.
  - Но тогда  $\llbracket \psi \rrbracket^{x:=d_i^{k+1}} = I$
  - Отсюда  $\mathcal{M} \models \exists x.\psi$ .

■

**Теорема 5.8.8** (Гёделя о полноте исчисления предикатов). Если  $M$  — замкнутое непротиворечивое множество формул, то оно имеет модель.

- Доказательство.*
- Построим по  $M$  множество формул с поверхностными кванторами  $M'$ .
  - По  $M'$  построим непротиворечивое множество замкнутых бескванторных формул  $M^B$  ( $M^B \subseteq M^*$ , теорема о непротиворечивости  $M^*$ ).
  - Дополним его до полного, построим для него модель  $\mathcal{M}$  (теорема о существовании модели).
  - $\mathcal{M}$  будет моделью и для  $M'$  ( $M' \subseteq M^*$ , лемма о модели для  $M^*$ ), и, очевидно, для  $M$ .

■

**Следствие 5.8.8.1** (из теоремы Гёделя о полноте). Исчисление предикатов полно.

*Доказательство.*

- Пусть это не так, и существует формула  $\varphi$ , что  $\models \varphi$ , но  $\not\vdash \varphi$ .

- Тогда рассмотрим  $M = \{\neg\varphi\}$ .
- $M$  непротиворечиво: если  $\neg\varphi \vdash A \& \neg A$ , то  $\vdash \varphi$  (упражнение).
- Значит, у  $M$  есть модель  $\mathcal{M}$ , и  $\mathcal{M} \models \neg\varphi$ .
- Значит,  $\llbracket \neg\varphi \rrbracket = I$ , поэтому  $\llbracket \varphi \rrbracket = L$ , поэтому  $\not\models \varphi$ . Противоречие.

■

**Теорема 5.8.9.** Если у множества формул  $M$  есть модель  $\mathcal{M}$ , оно непротиворечиво.

*Доказательство.* Пусть противоречиво:  $M \vdash A \& \neg A$ , в доказательстве использованы гипотезы  $\delta_1, \delta_2, \dots, \delta_n$ . Тогда  $\vdash \delta_1 \rightarrow \delta_2 \rightarrow \dots \rightarrow \delta_n \rightarrow A \& \neg A$ , то есть  $\llbracket \delta_1 \rightarrow \delta_2 \rightarrow \dots \rightarrow \delta_n \rightarrow A \& \neg A \rrbracket = I$  (корректность). Поскольку все  $\llbracket \delta_i \rrbracket_{\mathcal{M}} = I$ , то и  $\llbracket A \& \neg A \rrbracket_{\mathcal{M}} = I$  (анализ таблицы истинности импликации). Однако,  $\llbracket A \& \neg A \rrbracket = L$ . Противоречие. ■

**Следствие 5.8.9.1.** Исчисление предикатов непротиворечиво

## 5.9 Машина Тьюринга

**Определение 5.9.1.** Машина Тьюринга — упорядоченная тройка:

1. Внешний алфавит  $q_1, \dots, q_n$
2. Внутренний алфавит (состояний)  $s_1, \dots, s_k$ ;  $s_s$  — начальное,  $s_f$  — конечное.
3. Таблица переходов  $\langle k, s \rangle \Rightarrow \langle k', s', \leftrightarrow \rangle$

**Определение 5.9.2.** Состояние машины Тьюринга — упорядоченная тройка:

1. Бесконечная лента с символом-заполнителем  $q_\varepsilon$ , текст конечной длины.
2. Головка над определённым символом
3. Символ состояния (состояние в узком смысле) — символ внутреннего алфавита.

**Пример** (Машина, меняющая все 0 на 1, а все 1 — на 0). 1. Внешний алфавит  $\varepsilon, 0, 1$

2. Внутренний алфавит  $s_s, s_f$  (начальное и завершающее состояния соответственно).

3. Переходы:

|       | $\varepsilon$                             | 0                                     | 1                                     |
|-------|---|---------------------------------------|---------------------------------------|
| $s_s$ | $\langle s_f, \varepsilon, \cdot \rangle$ | $\langle s_s, 1, \rightarrow \rangle$ | $\langle s_s, 0, \rightarrow \rangle$ |
| $s_f$ | $\langle s_f, \varepsilon, \cdot \rangle$ | $\langle s_f, 0, \cdot \rangle$       | $\langle s_f, 1, \cdot \rangle$       |

Пусть головка — на первом символе 011, состояние  $s_s$ .

$\underline{0}11 \Rightarrow 1\underline{1}1 \Rightarrow 10\underline{1} \Rightarrow 100\underline{\varepsilon}$

Состояние  $s_f$ , завершающее.

### 5.9.1 Разрешимость языка Машины Тьюринга

**Определение 5.9.3.** Язык — множество строк.

**Определение 5.9.4.** Язык  $L$  разрешим, если существует машина Тьюринга, которая для любого слова  $w$  возвращает ответ «да», если  $w \in L$ , и «нет», если  $w \notin L$ .

### 5.9.2 Неразрешимость задачи останова

**Определение 5.9.5.** Рассмотрим все возможные описания машин Тьюринга. Составим упорядоченные пары: описание машины Тьюринга и входная строка. Из них выделим язык останавливающих на данном входе машин Тьюринга.

**Теорема 5.9.1.** Язык всех останавливающих машин Тьюринга неразрешим

*Доказательство.* От противного. Пусть  $S(x, y)$  — машина Тьюринга, определяющая, остановится ли машина  $x$ , примененная к строке  $y$ .

$W(x) = \text{if } (S(x, x)) \{ \text{while } (\text{true}); \text{return } 0; \} \text{ else } \{ \text{return } 1; \}$

Что вернёт  $S(\text{code}(W), \text{code}(W))$ ? ■



## Как закодировать состояние машины?

1. внешний алфавит:  $n$  0-местных функциональных символов  $q_1, \dots, q_n$ ;  $q_\varepsilon$  — символ-заполнитель.
2. список:  $\varepsilon$  и  $c(l, s)$ ; «abc» представим как  $c(q_a, c(q_b, c(q_c, \varepsilon)))$ ;
3. положение головки: «ab.pq» как  $(c(q_b, c(q_a, \varepsilon)), c(q_p, c(q_q, \varepsilon)))$ .
4. внутренний алфавит:  $k$  0-местных функциональных символов  $s_1, \dots, s_k$ . Из них выделенные  $s_s$  — начальное и  $s_f$  — завершающее состояние.

**Достижимые состояния** Предикатный символ  $F_{x,y}(w_l, w_r, s)$ : если у машины  $x$  с начальной строкой  $y$  состояние  $s$  достижимо на строке  $rev(w_l)@w_r$ .

Будем накладывать условия: семейство формул  $C_m$ . Очевидно, начальное состояние достижимо:

$$C_0 = F_{x,y}(\varepsilon, x, s_s).$$

## Кодируем переходы

1. Занумеруем переходы.
2. Закодируем переход  $m$ :  $\langle k, s \rangle \Rightarrow \langle k', s', \rightarrow \rangle$ .

$$C_m = \forall w_l. \forall w_r. F_{x,y}(w_l, c(q_k, w_r), s_s) \rightarrow F_{x,y}(c(q_{k'}, w_l), w_r, s_{s'}).$$

3. Переход посложнее:  $\langle k, s \rangle \Rightarrow \langle k', s', \leftarrow \rangle$ .

$$C_m = \forall w_l. \forall w_r. \forall t. F_{x,y}(c(t, w_l), c(q_k, w_r), s_s) \rightarrow F_{x,y}(w_l, c(t, c(q_{k'}, w_r)), s_{s'}) \& \\ \forall w_l. \forall w_r. F_{x,y}(\varepsilon, c(q_k, w_r), s_s) \rightarrow F_{x,y}(\varepsilon, c(q_{k'}, w_r), s_{s'}).$$

4. и т.п.

Итоговая формула:  $C = C_0 \& C_1 \& \dots \& C_n$  «правильное начальное состояние и правильные переходы между состояниями».

**Теорема 5.9.2.** состояние  $s$  со строкой  $rev(w_l)@w_r$  достижимо тогда и только тогда, когда  $C \vdash F_{x,y}(w_l, w_r, s)$

*Доказательство.* ( $\Leftarrow$ ) Рассмотрим модель: предикат  $F_{x,y}(w_l, w_r, s)$  положим истинным, если состояние достижимо. Это — модель для  $C$  (по построению  $C_m$ ). Значит, доказуемость влечёт истинность (по корректности).

( $\Rightarrow$ ) Индукция по длине лога исполнения. ■

### 5.9.3 Неразрешимость исчисления предикатов: доказательство

**Теорема 5.9.3.** Язык всех доказуемых формул исчисления предикатов неразрешим  
Т.е. нет машины Тьюринга, которая бы по любой формуле  $s$  определяла, доказуема ли она.

*Доказательство.*  $s_f$  — завершающее состояние.

Умение определять истинность формулы  $\exists w_l. \exists w_r. F_{x,y}(w_l, w_r, s_f)$  разрешает задачу останова. ■

## 6 Формальная арифметика и Аксиоматика Пеано

Какие мы знаем числа?

1. Вещественные ( $\mathbb{R}$ ).  $X = \{A, B\}$ , где  $A, B \subseteq \mathbb{Q}$  — дедекиндово сечение, если:

- (a)  $A \cup B = \mathbb{Q}$
- (b) Если  $a \in A$ ,  $x \in \mathbb{Q}$  и  $x \leq a$ , то  $x \in A$
- (c) Если  $b \in B$ ,  $x \in \mathbb{Q}$  и  $b \leq x$ , то  $x \in B$
- (d)  $A$  не содержит наибольшего.

$\mathbb{R}$  — множество всех возможных дедекиндовых сечений.

2. Рациональные ( $\mathbb{Q}$ ).  $Q = \mathbb{Z} \times \mathbb{N}$  — множество всех простых дробей.

$\langle p, q \rangle$  — то же, что  $\frac{p}{q}$

$\langle p_1, q_1 \rangle \equiv \langle p_2, q_2 \rangle$ , если  $p_1 q_2 = p_2 q_1$ .

$\mathbb{Q} = Q / \equiv$

**А что такое целые числа?**

«Бог создал целые числа, всё остальное — дело рук человека.» — Леопольд Кронеккер

$\mathbb{Z} : \dots - 3, -2, -1, 0, 1, 2, 3, \dots$

Определим целые числа так:

•  $Z = \{\langle x, y \rangle \mid x, y \in \mathbb{N}_0\}$

• Интуиция:  $\langle x, y \rangle = x - y$

•

$$\begin{aligned}\langle a, b \rangle + \langle c, d \rangle &= \langle a + c, b + d \rangle \\ \langle a, b \rangle - \langle c, d \rangle &= \langle a + d, b + c \rangle\end{aligned}$$

• Пусть  $\langle a, b \rangle \equiv \langle c, d \rangle$ , если  $a + d = b + c$ . Тогда  $\mathbb{Z} = Z / \equiv$

•  $0 = [\langle 0, 0 \rangle]$ ,  $1 = [\langle 1, 0 \rangle]$ ,  $-7 = [\langle 0, 7 \rangle]$

А что такое натуральные числа?

$\mathbb{N} : 1, 2, \dots$  или  $\mathbb{N}_0 : 0, 1, 2, \dots$

### 6.1 Аксиоматика Пеано

Определим натуральные числа так:

**Определение 6.1.1.**  $N$  (или, более точно,  $\langle N, 0, (') \rangle$ ) соответствует аксиоматике Пеано, если следующее определено/выполнено:

1. Операция «штрих»  $(') : N \rightarrow N$ , причём нет  $a, b \in N$ , что  $a \neq b$ , но  $a' = b'$ .

Если  $x = y'$ , то  $x$  назовём следующим за  $y$ , а  $y$  — предшествующим  $x$ .

2. Константа  $0 \in N$ : нет  $x \in N$ , что  $x' = 0$ .

3. Индукция. Каково бы ни было свойство («предикат»)  $P : N \rightarrow V$ , если:

(a)  $P(0)$

(b) При любом  $x \in N$  из  $P(x)$  следует  $P(x')$

то при любом  $x \in N$  выполнено  $P(x)$ .

Как построить? Например, в стиле алгебры Линденбаума:

1.  $N$  — язык, порождённый грамматикой  $\nu ::= 0 \mid \nu \langle ' \rangle$
2.  $0$  — это  $\langle 0 \rangle$ ,  $x'$  — это  $x \langle + \rangle$

**Пример.** Что не соответствует аксиомам Пеано?

1.  $\mathbb{Z}$ , где  $x' = x^2$ . Функция «штрих» не инъективна:  $-3^2 = 3^2 = 9$ .
2. Кольцо вычетов  $\mathbb{Z}/7\mathbb{Z}$ , где  $x' = x + 1$ .  $6' = 0$ , что нарушает свойства 0.
3.  $\mathbb{R}^+ \cup \{0\}$ , где  $x' = x + 1$ . Пусть  $P(x)$  означает « $x \in \mathbb{Z}$ »:
  - (a)  $P(0)$  выполнено:  $0 \in \mathbb{Z}$ .
  - (b) Если  $P(x)$ , то есть  $x \in \mathbb{Z}$ , то и  $x + 1 \in \mathbb{Z}$  — так что и  $P(x')$  выполнено.
 Однако,  $P(0.5)$  ложно.

Докажем, например, что 0 единственный.

**Теорема 6.1.1.** 0 единственен: если  $t$  таков, что при любом  $y$  выполнено  $y' \neq t$ , то  $t = 0$ .

*Доказательство.* • Определим  $P(x)$  как «либо  $x = 0$ , либо  $x = y'$  для некоторого  $y \in N$ ».

1.  $P(0)$  выполнено, так как  $0 = 0$ .
2. Если  $P(x)$  выполнено, то возьмём  $x$  в качестве  $y$ : тогда для  $P(x')$  будет выполнено  $x' = y'$ .

Значит,  $P(x)$  для любого  $x \in N$ .

- Рассмотрим  $P(t)$ : «либо  $t = 0$ , либо  $t = y'$  для некоторого  $y \in N$ ». Но так как такого  $y$  нет, то неизбежно  $t = 0$ .

■

**Определение 6.1.2.**  $1 = 0'$ ,  $2 = 0''$ ,  $3 = 0'''$ ,  $4 = 0''''$ ,  $5 = 0'''''$ ,  $6 = 0''''''$ ,  $7 = 0'''''''$ ,  $8 = 0''''''''$ ,  $9 = 0'''''''''$

**Определение 6.1.3.**

$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

Например,

$$2 + 2 = 0'' + 0'' = (0'' + 0')' = ((0'' + 0)')' = ((0'')')' = 0''' = 4$$

**Определение 6.1.4.**

$$a \cdot b = \begin{cases} 0, & \text{если } b = 0 \\ a \cdot c + a, & \text{если } b = c' \end{cases}$$

Пример: коммутативность сложения (лемма 1)

**Лемма 6.1.1.1** (1).  $a + 0 = 0 + a$

*Доказательство.* Пусть  $P(x)$  — это  $x + 0 = 0 + x$ .

1. Покажем  $P(0)$ .  $0 + 0 = 0 + 0$
2. Покажем, что если  $P(x)$ , то  $P(x')$ . Покажем  $P(x')$ , то есть  $x' + 0 = \dots$

$$\begin{array}{lll}
\cdots = x' & a = x', b = 0: & x' + 0 \Rightarrow x' \\
\cdots = (x)' & & \\
\cdots = (x + 0)' & a = x, b = 0: & (x + 0) \Leftarrow (x) \\
\cdots = (0 + x)' & P(x): & (x + 0) \Rightarrow (0 + x) \\
\cdots = 0 + x' & a = 0, b = x': & 0 + x' \Leftarrow (0 + x)'
\end{array}$$

Значит,  $P(a)$  выполнено для любого  $a \in N$ . ■

**Лемма 6.1.1.2** (2).  $a + b' = a' + b$

*Доказательство.*  $P(x)$  — это  $a + x' = a' + x$

1.  $a + 0' = (a + 0)' = (a)' = a' = a' + 0$
  2. Покажем, что  $P(x')$  следует из  $P(x)$ :  $a + x'' = (a + x')' = (a' + x)' = a' + x'$
- 

**Теорема 6.1.2.**  $a + b = b + a$

*Доказательство индукцией по b:*  $P(x)$  — это  $a + x = x + a$ . 1.  $a + 0 = 0 + a$  (лемма 1)

2.  $a + x' = (a + x)' = (x + a)' = x + a' = x' + a$
- 

### 6.1.1 Уточнение исчисления предикатов

- Пусть требуется доказывать утверждения про равенство. Введём  $E(p, q)$  — предикат «равенство».
- Однако,  $\not\models E(p, q) \rightarrow E(q, p)$ : если  $D = \{0, 1\}$  и  $E(p, q) ::= (p > q)$ , то  $\models E(p, q) \rightarrow E(q, p)$ .
- Конечно, можем указывать  $\forall p. \forall q. E(p, q) \rightarrow E(q, p) \vdash \varphi$ .
- Но лучше добавим аксиому  $\forall p. \forall q. E(p, q) \rightarrow E(q, p)$ .
- Добавив необходимые аксиомы, получим *теорию первого порядка*.

**Определение 6.1.5.** Теорией первого порядка назовём исчисление предикатов с дополнительными («нелогическими» или «математическими»):

- предикатными и функциональными символами;
- аксиомами.

Сущности, взятые из исходного исчисления предикатов, назовём *логическими*

| Порядок | Кванторы                  | Формализует суждения о...   | Пример |
|---------|---------------------------|---|--------|
| нулевой | запрещены                 | об отдельных значениях  | И.В.   |
| первый  | по предметным переменным  | о множествах<br>$S = \{t \mid \psi[x := t]\}$                           | И.П.   |
| второй  | по предикатным переменным | о множествах множеств<br>$S = \{\{t \mid P(t)\} \mid \varphi[p := P]\}$ |        |
| ...     |                           |   |        |

### 6.1.2 Формальная арифметика

**Определение 6.1.6.** Формальная арифметика — теория первого порядка, со следующими добавленными нелогическими ...

- двуместными функциональными символами  $(+)$ ,  $(\cdot)$ ; одноместным функциональным символом  $(')$ , нульместным функциональным символом  $0$ ;
- двуместным предикатным символом  $(=)$ ;
- восьмью нелогическими *аксиомами*:
 

|  |                                   |
|--|-----------------------------------|
| (A1) $a = b \rightarrow a = c \rightarrow b = c$ | (A5) $a + 0 = a$                  |
| (A2) $a = b \rightarrow a' = b'$                 | (A6) $a + b' = (a + b)'$          |
| (A3) $a' = b' \rightarrow a = b$                 | (A7) $a \cdot 0 = 0$              |
| (A4) $\neg a' = 0$                               | (A8) $a \cdot b' = a \cdot b + a$ |
- нелогической схемой аксиом индукции  $\psi[x := 0] \& (\forall x. \psi \rightarrow \psi[x := x']) \rightarrow \psi$ , с метапеременными  $x$  и  $\psi$ .

**Утверждение 6.1.1.**  $a = a$  в формальной арифметике.

*Доказательство.* Пусть  $\top ::= 0 = 0 \rightarrow 0 = 0 \rightarrow 0 = 0$ , тогда:

- |      |   |                    |
|------|---|--------------------|
| (1)  | $a = b \rightarrow a = c \rightarrow b = c$   | (Акс. А1)          |
| (2)  | $(a = b \rightarrow a = c \rightarrow b = c) \rightarrow \top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$  | (Сх. акс. 1)       |
| (3)  | $\top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$  | (М.Р. 1, 2)        |
| (4)  | $\top \rightarrow (\forall c. a = b \rightarrow a = c \rightarrow b = c)$   | (Введ. $\forall$ ) |
| (5)  | $\top \rightarrow (\forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$  | (Введ. $\forall$ ) |
| (6)  | $\top \rightarrow (\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$   | (Введ. $\forall$ ) |
| (7)  | $\top$  | (Сх. акс 1)        |
| (8)  | $(\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$  | (М.Р. 7, 6)        |
| (9)  | $(\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c) \rightarrow$<br>$\rightarrow (\forall b. \forall c. a + 0 = b \rightarrow a + 0 = c \rightarrow b = c)$ | (Сх. акс. 11)      |
| (10) | $\forall b. \forall c. a + 0 = b \rightarrow a + 0 = c \rightarrow b = c$   | (М.Р. 8, 9)        |
| (12) | $\forall c. a + 0 = a \rightarrow a + 0 = c \rightarrow a = c$  | (М.Р. 10, 11)      |
| (14) | $a + 0 = a \rightarrow a + 0 = a \rightarrow a = a$   | (М.Р. 12, 13)      |
| (15) | $a + 0 = a$   | (Акс. А5)          |
| (16) | $a + 0 = a \rightarrow a = a$   | (М.Р. 15, 14)      |
| (17) | $a = a$   | (М.Р. 15, 16)      |

■

## 6.2 Арифметизация логики

Общие замечания

- Рассматриваем функции  $\mathbb{N}_0^n \rightarrow \mathbb{N}_0$ .
- Обозначим вектор  $\langle x_1, x_2, \dots, x_n \rangle$  как  $\vec{x}$ .

### 6.2.1 Примитивно-рекурсивные функции

**Определение 6.2.1** (Примитивы Z, N, U, S). Примитив «Ноль» (Z)

$$Z : \mathbb{N}_0 \rightarrow \mathbb{N}_0, \quad Z(x_1) = 0.$$

**Определение 6.2.2.** Примитив «Инкремент» (N)

$$N : \mathbb{N}_0 \rightarrow \mathbb{N}_0, \quad N(x_1) = x_1 + 1.$$

**Определение 6.2.3.** Примитив «Проекция» ( $U$ ) — семейство функций; пусть  $k, n \in \mathbb{N}_0, k \leq n$

$$U_n^k : \mathbb{N}_0^n \rightarrow \mathbb{N}_0, \quad U_n^k(\vec{x}) = x_k.$$

**Определение 6.2.4.** Примитив «Подстановка» ( $S$ ) — семейство функций; пусть  $g : \mathbb{N}_0^k \rightarrow \mathbb{N}_0, f_1, \dots, f_k : \mathbb{N}_0^n \rightarrow \mathbb{N}_0$

$$S\langle g, f_1, f_2, \dots, f_k \rangle(\vec{x}) = g(f_1(\vec{x}), \dots, f_k(\vec{x})).$$

**Определение 6.2.5** (примитив «примитивная рекурсия»,  $R$ ). Пусть  $f : \mathbb{N}_0^n \rightarrow \mathbb{N}_0$  и  $g : \mathbb{N}_0^{n+2} \rightarrow \mathbb{N}_0$ . Тогда  $R\langle f, g \rangle : \mathbb{N}_0^{n+1} \rightarrow \mathbb{N}_0$ , причём

$$R\langle f, g \rangle(\vec{x}, y) = \begin{cases} f(\vec{x}), & y = 0 \\ g(\vec{x}, y-1, R\langle f, g \rangle(\vec{x}, y-1)), & y > 0 \end{cases}.$$

```
res := f(x1...xn);
for yi = 0 to y-1 do
  res := g(x1...xn, yi, res);
```

**Пример.**

$$\begin{aligned} R\langle f, g \rangle(\vec{x}, 3) &= g(\vec{x}, 2, R\langle f, g \rangle(\vec{x}, 2)) \\ &= g(\vec{x}, 2, g(\vec{x}, 1, R\langle f, g \rangle(\vec{x}, 1))) \\ &= g(\vec{x}, 2, g(\vec{x}, 1, g(\vec{x}, 0, R\langle f, g \rangle(\vec{x}, 1)))) \\ &= g(\vec{x}, 2, g(\vec{x}, 1, g(\vec{x}, 0, f(\vec{x})))) \end{aligned}$$

## 6.2.2 Примитивно-рекурсивные функции

**Определение 6.2.6.** Функция  $f$  — примитивно-рекурсивна, если может быть выражена как композиция примитивов  $Z, N, U, S$  и  $R$ .

**Теорема 6.2.1.**  $f(x) = x + 2$  примитивно-рекурсивна

*Доказательство.*  $f = S\langle N, N \rangle$

$$N(x) = x + 1$$

$$S\langle g, f \rangle(x) = g(f(x))$$

$$f, g = N \ S\langle N, N \rangle(x) = N(N(x)) = (x + 1) + 1$$

■

**Лемма 6.2.1.1.**  $f(a, b) = a + b$  примитивно-рекурсивна

*Доказательство.*  $f = R\langle U_1^1, S\langle N, U_3^3 \rangle \rangle$ :

$$R\langle f, g \rangle(x, y) = \begin{cases} f(x), & y = 0 \\ g(x, y-1, R\langle f, g \rangle(x, y-1)), & y > 0 \end{cases}$$

- База.  $R\langle U_1^1, S\langle N, U_3^3 \rangle \rangle(x, 0) = U_1^1(x) = x$

- Переход.  $R\langle U_1^1, S\langle N, U_3^3 \rangle \rangle(x, y + 1) =$

$$\dots = S\langle N, U_3^3 \rangle(x, y, R\langle U_1^1, S\langle N, U_3^3 \rangle \rangle(x, y)) =$$

$$\dots = S\langle N, U_3^3 \rangle(x, y, x + y) =$$

$$\dots = N(x + y) = x + y + 1$$

■

## Какие функции примитивно-рекурсивные?

1. Сложение, вычитание
2. Умножение, деление
3. Вычисление простых чисел
4. Неформально: все функции, вычисляемые конечным числом вложенных циклов `for`:

```
for (int i1 = 0; i1 < g1(x1...xn); i1++) {
    for (int i2 = 0; i2 < g2(x1...xn,i1); i2++) {
        ...
        for (int ik = 0; ik < gk(x1...xn,i1,i2...); ik++) {
            // выражение без циклов
        }
        ...
    }
}
```

### 6.2.3 Общерекурсивные функции

**Определение 6.2.7.** Функция — общерекурсивная, если может быть построена при помощи примитивов  $Z$ ,  $N$ ,  $U$ ,  $S$ ,  $R$  и примитива минимизации:

$$M\langle f \rangle(x_1, x_2, \dots, x_n) = \min\{y : f(x_1, x_2, \dots, x_n, y) = 0\}$$

Если  $f(x_1, x_2, \dots, x_n, y) > 0$  при любом  $y$ , результат неопределён.

**Пример.** Пусть  $f(x, y) = x - y^2$ , тогда  $\lceil \sqrt{x} \rceil = M\langle f \rangle(x)$

```
int sqrt(int x) {
    int y = 0;
    while (x-y*y > 0) y++;
    return y;
}
```

Вообще, все почти все функции, о которых мы можем подумать являются примитивно-рекурсивными. Даже, квадратный корень на самом деле можно представить, как примитивно-рекурсивную функцию.

**Определение 6.2.8.** Функция Аккермана:

$$A(m, n) = \begin{cases} n + 1, & m = 0 \\ A(m - 1, 1), & m > 0, n = 0 \\ A(m - 1, A(m, n - 1)), & m > 0, n > 0 \end{cases}.$$

**Теорема 6.2.2.** Функция Аккермана — общерекурсивная, но не примитивно-рекурсивная.

Она вычисляется настолько медленно, что мы не можем заранее сказать сколько итераций потребуется для вычисления.

**Определение 6.2.9.** Тезис Чёрча для общерекурсивных функций: любая эффективно-вычисляемая функция  $\mathbb{N}_0^k \rightarrow \mathbb{N}_0$  является общерекурсивной.

**Определение 6.2.10.** Запись вида  $\psi(\theta_1, \dots, \theta_n)$  означает  $\psi[x_1 := \theta_1, \dots, x_n := \theta_n]$

**Определение 6.2.11** (Литерал числа).

$$\bar{a} = \begin{cases} 0, & \text{если } a = 0 \\ (\bar{b})', & \text{если } a = b + 1 \end{cases}.$$

Пример: пусть  $\psi := x_1 = 0$ . Тогда  $\psi(\bar{3})$  соответствует формуле  $0''' = 0$

**Определение 6.2.12** (Выразимость отношений в Ф.А.). Будем говорить, что отношение  $R \subseteq \mathbb{N}_0^n$  выразимо в ФА, если существует формула  $\rho$ , что:

1. если  $\langle a_1, \dots, a_n \rangle \in R$ , то  $\vdash \rho(\bar{a}_1, \dots, \bar{a}_n)$
2. если  $\langle a_1, \dots, a_n \rangle \notin R$ , то  $\vdash \neg \rho(\bar{a}_1, \dots, \bar{a}_n)$

**Теорема 6.2.3.** отношение «равно» выразимо в Ф.А.:  $R = \{\langle x, x \rangle \mid x \in \mathbb{N}_0\}$

*Доказательство.* Пусть  $\rho := x_1 = x_2$ . Тогда:

- $\vdash p = p$  при  $p := \bar{k}$  при всех  $k \in \mathbb{N}_0$ :  $\vdash 0 = 0$ ,  $\vdash 0' = 0'$ ,  $\vdash 0'' = 0''$ , ...
- $\vdash \neg p = q$  при  $p := \bar{k}$ ,  $q := \bar{s}$  при всех  $k, s \in \mathbb{N}_0$  и  $k \neq s$ .  
 $\vdash \neg 0 = 0'$ ,  $\vdash \neg 0 = 0''$ ,  $\vdash \neg 0''' = 0'$ , ...

■

**Определение 6.2.13** (Представимость функций в Ф.А.). Будем говорить, что функция  $f : \mathbb{N}_0^n \rightarrow \mathbb{N}_0$  представима в ФА, если существует формула  $\varphi$ , что:

1. если  $f(a_1, \dots, a_n) = u$ , то  $\vdash \varphi(\bar{a}_1, \dots, \bar{a}_n, \bar{u})$
2. если  $f(a_1, \dots, a_n) \neq u$ , то  $\vdash \neg \varphi(\bar{a}_1, \dots, \bar{a}_n, \bar{u})$
3. для всех  $a_i \in \mathbb{N}_0$  выполнено  $\vdash (\exists x. \varphi(\bar{a}_1, \dots, \bar{a}_n, x)) \& (\forall p. \forall q. \varphi(\bar{a}_1, \dots, \bar{a}_n, p) \& \varphi(\bar{a}_1, \dots, \bar{a}_n, q) \rightarrow p = q)$

#### 6.2.4 Соответствие рекурсивных и представимых функций

**Теорема 6.2.4.** Любая рекурсивная функция представима в Ф.А.

**Теорема 6.2.5.** Любая представимая в Ф.А. функция рекурсивна.

**Теорема 6.2.6.** Прimitives  $Z$ ,  $N$  и  $U_n^k$  представимы в Ф.А.

*Доказательство.* •  $\zeta(x_1, x_2) := x_2 = 0$ , формальнее:  $\zeta(x_1, x_2) := x_1 = x_1 \& x_2 = 0$



- $\nu(x_1, x_2) := x_2 = x'_1$
  - $\nu(x_1, \dots, x_n, x_{n+1}) := x_k = x_{n+1}$
- формальнее:  $\nu(x_1, \dots, x_n, x_{n+1}) := (\bigwedge_{i \neq k, n+1} x_i = x_i) \& x_k = x_{n+1}$

■

**Примитив S представим в Ф.А.**

$$S\langle f, g_1, \dots, g_k \rangle(x_1, \dots, x_n) = f(g_1(x_1, \dots, x_n), \dots, g_k(x_1, \dots, x_n)).$$

**Теорема 6.2.7.** Пусть функции  $f, g_1, \dots, g_k$  представимы в Ф.А. Тогда  $S\langle f, g_1, \dots, g_k \rangle$  представима в Ф.А.

*Доказательство.* Пусть  $f, g_1, \dots, g_k$  представляются формулами  $\varphi, \gamma_1, \dots, \gamma_k$ .

Тогда  $\langle f, g_1, \dots, g_k \rangle$  будет представлена формулой

$$\exists g_1 \dots \exists g_k. \varphi(g_1, \dots, g_k, x_{n+1}) \& \gamma_1(x_1, \dots, x_n, g_1) \& \dots \& \gamma_k(x_1, \dots, x_n, g_k).$$

■

**$\beta$ -функция Гёделя** Мы хотим закодировать последовательность натуральных чисел произвольной длины.

**Определение 6.2.14.**  $\beta$ -функция Гёделя:  $\beta(b, c, i) := b\%(1 + (i + 1) \cdot c)$   
Здесь (%) — остаток от деления.

**Теорема 6.2.8.**  $\beta$ -функция Гёделя представима в Ф.А. формулой

$$\hat{\beta}(b, c, i, d) := \exists q. (b = q \cdot (1 + c \cdot (i + 1)) + d) \& (d < 1 + c \cdot (i + 1))$$

Деление  $b$  на  $x$  с остатком: найдутся частное ( $q$ ) и остаток ( $d$ ), что  $b = q \cdot x + d$  и  $0 \leq d < x$ .

**Теорема 6.2.9.** Если  $a_0, \dots, a_n \in \mathbb{N}_0$ , то найдутся такие  $b, c \in \mathbb{N}_0$ , что  $a_i = \beta(b, c, i)$ .

*Доказательство.* Китайская теорема об остатках (вариант формулировки): если  $u_0, \dots, u_n$  — попарно взаимно-просты, и  $0 \leq a_i < u_i$ , то существует такой  $b$ , что  $a_i = b\%u_i$ .

Положим  $c = \max(a_0, \dots, a_n, n)! + 1$  и  $u_i = 1 + c \cdot (i + 1)$ .

- НОД( $u_i, u_j$ ) = 1, если  $i \neq j$ . Пусть  $p$  — простое,  $u_i : p$  и  $u_j : p$  ( $i < j$ ). Заметим, что  $u_j - u_i = c \cdot (j - i)$ . Значит,  $c : p$  или  $(j - i) : p$ . Так как  $j - i \leq n$ , то  $c : (j - i)$ , потому если и  $(j - i) : p$ , всё равно  $c : p$ . Но и  $(1 + c \cdot (i + 1)) : p$ , отсюда  $1 : p$  — что невозможно.
- $0 \leq a_i < u_i$ .

Условия китайской теоремы об остатках выполнены и найдётся  $b$ , что  $a_i = b\%(1 + c \cdot (i + 1)) = \beta(b, c, i)$ . ■

**Теорема 6.2.10.** Пусть  $f : \mathbb{N}_0^n \rightarrow \mathbb{N}_0$  и  $g : \mathbb{N}_0^{n+2} \rightarrow \mathbb{N}_0$  представлены формулами  $\varphi$  и  $\gamma$ .

Примитив  $R\langle f, g \rangle$  представим в Ф.А. формулой  $\rho(x_1, \dots, x_n, y, a)$ :

$$\begin{aligned} & \exists b. \exists c. (\exists a_0. \hat{\beta}(b, c, 0, a_0) \& \varphi(x_1, \dots, x_n, a_0)) \\ & \& \forall k. k < y \rightarrow \exists d. \exists e. \hat{\beta}(b, c, k, d) \& \hat{\beta}(b, c, k', e) \& \gamma(x_1, \dots, x_n, k, d, e) \\ & \& \hat{\beta}(b, c, y, a) \end{aligned}$$

*Доказательство.* Зафиксируем  $x_1, \dots, x_n, y \in \mathbb{N}_0$ .

|  |       |  |
|--|-------|--|
| Шаг вычисления   | Об.   | Утверждение в Ф.А.   |
| $R\langle f, g \rangle(x_1, \dots, x_n, 0) = f(x_1, \dots, x_n)$               | $a_0$ | $\vdash \varphi(\overline{x_1}, \dots, \overline{x_n}, \overline{a_0})$                |
| $R\langle f, g \rangle(x_1, \dots, x_n, 1) = g(x_1, \dots, x_n, 0, a_0)$       | $a_1$ | $\vdash \gamma(\overline{x_1}, \dots, \overline{x_n}, 0, \overline{a_1})$              |
| ...  |       |  |
| $R\langle f, g \rangle(x_1, \dots, x_n, y) = g(x_1, \dots, x_n, y-1, a_{y-1})$ | $a_y$ | $\vdash \gamma(\overline{x_1}, \dots, \overline{x_n}, \overline{y-1}, \overline{a_y})$ |

По свойству  $\beta$ -функции, найдутся  $b$  и  $c$ , что  $\beta(b, c, i) = a_i$  для  $0 \leq i \leq y$ . ■

**Теорема 6.2.11.** Пусть функция  $f : \mathbb{N}_0^{n+1} \rightarrow \mathbb{N}_0$  представима в Ф.А. формулой  $\varphi(x_1, \dots, x_n, y, r)$ . Тогда примитив  $M\langle f \rangle$  представим в Ф.А. формулой

$$\mu(x_1, \dots, x_n, y) := \varphi(x_1, \dots, x_n, y, 0) \& \neg \forall u. u < y \rightarrow \varphi(x_1, \dots, x_n, u, 0).$$

**Теорема 6.2.12.** Если  $f$  — рекурсивная функция, то она представима в Ф.А.

*Доказательство.* Индукция по структуре  $f$ . ■

### 6.2.5 Рекурсивность представимых в Ф.А. функций

Фиксируем  $f$  и  $x_1, x_2, \dots, x_n$ . Обозначим  $y = f(x_1, x_2, \dots, x_n)$ . По представимости нам известна  $\varphi$ , что  $\vdash \varphi(\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}, \overline{y})$ . Давайте просто переберём все результаты и доказательства!

1. Закодируем доказательства натуральными числами.
2. Напишем рекурсивную функцию, проверяющую доказательства на корректность.
3. Параллельный перебор значений и доказательств:  $s = 2^y \cdot 3^p$ . Переберём все  $s$ , по  $s$  получим  $y$  и  $p$ . Проверим, что  $p$  — код доказательства  $\vdash \varphi(\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}, \overline{y})$ .

Гёделева нумерация

1. Отдельный символ.

| Номер | Символ        | Номер                        | Символ    | Имя | $k, n$ | Гёделев номер            |
|-------|---------------|------------------------------|-----------|-----|--------|--------------------------|
| 3     | (             | 17                           | &         | 0   | 0, 0   | $27 + 6$                 |
| 5     | )             | 19                           | $\forall$ | (') | 0, 1   | $27 + 6 \cdot 3$         |
| 7     | ,             | 21                           | $\exists$ | (+) | 0, 2   | $27 + 6 \cdot 9$         |
| 9     | .             | 23                           | $\vdash$  | (.) | 1, 2   | $27 + 6 \cdot 2 \cdot 9$ |
| 11    | $\neg$        | $25 + 6 \cdot k$             | $x_k$     | (=) | 0, 2   | $29 + 6 \cdot 9$         |
| 13    | $\rightarrow$ | $27 + 6 \cdot 2^k \cdot 3^n$ | $f_k^n$   |     |        |                          |
| 15    | $\vee$        | $29 + 6 \cdot 2^k \cdot 3^n$ | $P_k^n$   |     |        |                          |

2. Формула.  $\phi \equiv s_0 s_1 \dots s_{n-1}$ . Гёделев номер:  $\ulcorner \phi \urcorner = 2^{\ulcorner s_0 \urcorner} \cdot 3^{\ulcorner s_1 \urcorner} \dots p_{n-1}^{\ulcorner s_{n-1} \urcorner}$ .
3. Доказательство.  $\Pi = \delta_0 \delta_1 \dots \delta_{k-1}$ , его гёделев номер:  $\ulcorner \Pi \urcorner = 2^{\ulcorner \delta_0 \urcorner} \cdot 3^{\ulcorner \delta_1 \urcorner} \dots p_{k-1}^{\ulcorner \delta_{k-1} \urcorner}$ .

**Теорема 6.2.13.** Следующая функция рекурсивна:

$$\text{proof}(f, x_1, x_2, \dots, x_n, y, p) = \begin{cases} 1, & \text{если } \vdash \varphi(\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}, \overline{y}), \\ & p \text{ — гёделев номер вывода, } f = \ulcorner \phi \urcorner \\ 0, & \text{иначе} \end{cases}$$

*Идея доказательства.* 1. Проверка доказательства вычислима.

2. Согласно тезису Чёрча, любая вычислимая функция вычислима с помощью рекурсивных функций.

**Лемма 6.2.13.1.** Следующие функции рекурсивны:

1. Функции  $\text{plog}_k(n) = \max\{p : n \leq k^p\}$ ,  $\text{fst}(x) = \text{plog}_2(x)$  и  $\text{snd}(x) = \text{plog}_3(x)$ .
2. Числовые литералы:  $\bar{k} : \mathbb{N}_0 \rightarrow \mathbb{N}_0$ ,  $\bar{k}(x) = k$ .

**Теорема 6.2.14.** Если  $f : \mathbb{N}_0^n \rightarrow \mathbb{N}_0$ , и  $f$  представима в Ф.А. формулой  $\varphi$ , то  $f$  — рекурсивна.

*Доказательство.* Пусть заданы  $x_1, x_2, \dots, x_n$ . Ищем  $\langle y, p \rangle$ , что  $\text{proof}(\ulcorner \varphi \urcorner, x_1, x_2, \dots, x_n, y, p) = 1$ , напомним:  $y = f(x_1, x_2, \dots, x_n)$ ,  $p = \ulcorner \Pi \urcorner$ ,  $\Pi$  — доказательство  $\varphi(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n, \bar{y})$ .

$$f = S\langle \text{fst}, M\langle S\langle \text{proof}, \ulcorner \varphi \urcorner, U_{n+1}^1, U_{n+1}^2, \dots, U_{n+1}^n, S\langle \text{fst}, U_{n+1}^{n+1} \rangle, S\langle \text{snd}, U_{n+1}^{n+1} \rangle \rangle \rangle \rangle$$

### 6.3 Первая теорема Гёделя о неполноте арифметики

Парадокс лжеца

Предложение, указанное в центре данного слайда — ложное.

Проблема останова

**Теорема 6.3.1.** Невозможно разработать программу (функцию):

`bool p (string source, string arg),`

возвращающую `true`, если программа с исходным кодом `source` имеет один аргумент типа `string` и оканчивает работу, если ей передать на вход значение `arg`.

*Доказательство.* Определим программу

```
bool s (std::string arg) {
    if (p(arg)) {
        while (true);
    }
    return true;
}
```

- Пусть её полный исходный код — в переменной `source`.
- Что вернёт `p (source, source)`?

**Определение 6.3.1.** Определим функцию  $W_1$ :  $W_1(x, p) = 1$ , если  $x = \ulcorner \xi \urcorner$ , где  $\xi$  — формула с единственной свободной переменной  $x_1$ , а  $p$  — доказательство самоприменения  $\xi$ :

$$\vdash \xi(\ulcorner \xi \urcorner)$$

$W_1(x, p) = 0$ , если это не так.

**Замечание.**  $\ulcorner \xi \urcorner$  здесь означает получение гёделева номера  $\xi$  и запись его в виде литерала в Ф.А.

**Теорема 6.3.2.** Существует формула  $\omega_1$  со свободными переменными  $x_1$  и  $x_2$ , такая, что:

1.  $\vdash \omega_1(\overline{\ulcorner \varphi \urcorner}, \overline{p})$ , если  $p$  — гёделев номер доказательства самоприменения  $\varphi$ ;
2.  $\vdash \neg \omega_1(\overline{\ulcorner \varphi \urcorner}, \overline{p})$  иначе.

*Доказательство.* Опираясь на рекурсивность функции proof, легко показать рекурсивность  $W_1$ . Значит, эта функция представима в формальной арифметике некоторой формулой  $\tau_1$ . Возьмём  $\omega_1(x_1, x_2) := \tau_1(x_1, x_2, \overline{1})$ . ■

**Определение 6.3.2.** Определим формулу  $\sigma(x) := \forall p. \neg \omega(x, p)$ .  
Это означает, что самоприменение  $x$  не доказуемо.

**Определение 6.3.3.** Если для любой формулы  $\phi(x)$  из  $\vdash \phi(0), \vdash \phi(\overline{1}), \vdash \phi(\overline{2}), \dots$  выполнено  $\nvdash \exists x. \neg \phi(x)$ , то теория *омега-непротиворечива*.

**Теорема 6.3.3.** Омега-непротиворечивость влечёт непротиворечивость

*Доказательство.* Пусть  $\phi(x) \equiv (x = x) \rightarrow (x = x) \rightarrow (x = x)$ . Тогда  $\vdash \phi(x)$  при всех  $x$ . Тогда  $\nvdash \exists x. \neg \phi(x)$  — то есть существует недоказуемая формула, т.е. теория непротиворечива. ■

## 6.4 Теоремы Гёделя о неполноте арифметики

**Теорема 6.4.1.** Первая теорема Гёделя о неполноте арифметики

Если формальная арифметика непротиворечива, то  $\nvdash \sigma(\overline{\ulcorner \sigma \urcorner})$ .

- Если формальная арифметика  $\omega$ -непротиворечива, то  $\nvdash \neg \sigma(\overline{\ulcorner \sigma \urcorner})$ .

**Замечание.**  $\sigma(x_1) := \forall p. \neg \omega_1(x_1, p)$ .  $W_1(\ulcorner \xi \urcorner, p)$  —  $p$  есть доказательство самоприменения  $\xi$ .

*Доказательство теоремы Гёделя.* .

- Пусть  $\vdash \sigma(\overline{\ulcorner \sigma \urcorner})$ . Значит,  $p$  — номер доказательства. Тогда  $\langle \ulcorner \sigma \urcorner, p \rangle \in W_1$ . Тогда  $\vdash \omega_1(\overline{\ulcorner \sigma \urcorner}, \overline{p})$ . Тогда  $\vdash \exists p. \omega_1(\overline{\ulcorner \sigma \urcorner}, p)$ . То есть  $\vdash \neg \forall p. \neg \omega_1(\overline{\ulcorner \sigma \urcorner}, p)$ . То есть  $\vdash \neg \sigma(\overline{\ulcorner \sigma \urcorner})$ . Противоречие.
- Пусть  $\vdash \neg \sigma(\overline{\ulcorner \sigma \urcorner})$ . То есть  $\vdash \exists p. \omega_1(\overline{\ulcorner \sigma \urcorner}, p)$ .
  - Но найдётся ли натуральное число  $p$ , что  $\vdash \omega_1(\overline{\ulcorner \sigma \urcorner}, \overline{p})$ ?
  - Пусть нет. То есть  $\vdash \neg \omega_1(\overline{\ulcorner \sigma \urcorner}, \overline{0}), \vdash \neg \omega_1(\overline{\ulcorner \sigma \urcorner}, \overline{1}), \dots$
  - По  $\omega$ -непротиворечивости  $\nvdash \exists p. \neg \neg \omega_1(\overline{\ulcorner \sigma \urcorner}, p)$ .

Значит, найдётся натуральное  $p$ , что  $\vdash \omega_1(\overline{\ulcorner \sigma \urcorner}, \overline{p})$ . То есть,  $\langle \ulcorner \sigma \urcorner, p \rangle \in W_1$ . То есть,  $p$  — доказательство самоприменения  $W_1$ :  $\vdash \sigma(\overline{\ulcorner \sigma \urcorner})$ . Противоречие. ■

**Теорема 6.4.2.** Формальная арифметика с классической моделью — неполна.

*Доказательство.* Полная теория — теория, в которой любая общезначимая формула доказуема.

Рассмотрим Ф.А. с классической моделью. Из теоремы Гёделя имеем  $\nvdash \sigma(\overline{\ulcorner \sigma \urcorner})$ .

Рассмотрим  $\sigma(\overline{\ulcorner \sigma \urcorner}) \equiv \forall p. \neg \omega_1(\overline{\ulcorner \sigma \urcorner}, p)$ ,  $p$ : нет числа  $p$ , что  $p$  — номер доказательства  $\sigma(\overline{\ulcorner \sigma \urcorner})$ .

То есть,  $\llbracket \forall p. \neg \omega_1(\overline{\ulcorner \sigma \urcorner}, p) \rrbracket = \text{И}$ . То есть,  $\models \sigma(\overline{\ulcorner \sigma \urcorner})$ . ■

Почему мы должны требовать от нашей теории  $w$ -непротиворечивости? Неужели наша формальная арифметика недостаточно содержательна в том, чтобы сформулировать, какие натуральные числа можно использовать? Этот вопрос занимал математиков и вскоре было предложено решение

### Первая теорема Гёделя о неполноте в форме Россера

**Определение 6.4.1.**  $\theta_1 \leq \theta_2 \equiv \exists p. p + \theta_1 = \theta_2$        $\theta_1 < \theta_2 \equiv \theta_1 \leq \theta_2 \& \neg \theta_1 = \theta_2$ .

**Определение 6.4.2.** Пусть  $\langle \ulcorner \xi \urcorner, p \rangle \in W_2$ , если  $\vdash \neg \xi(\overline{\ulcorner \xi \urcorner})$ . Пусть  $\omega_2$  выражает  $W_2$  в формальной арифметике.

**Теорема 6.4.3.** Рассмотрим  $\rho(x_1) = \forall p. \omega_1(x_1, p) \rightarrow \exists q. q \leq p \& \omega_2(x_1, q)$ .  
Тогда  $\not\vdash \rho(\overline{\ulcorner \rho \urcorner})$  и  $\not\vdash \neg \rho(\overline{\ulcorner \rho \urcorner})$ .

**Замечание.** Смысл  $\rho(\overline{\ulcorner \rho \urcorner})$  примерно такой: «Меня легче опровергнуть, чем доказать».

#### А есть ли более формальное доказательство?

Неполнота варианта теории, изложенной выше, формально доказана на Coq, Russell O'Connor, 2005: “My proof, excluding standard libraries and the library for Pocklington’s criterion, consists of 46 source files, 7 036 lines of specifications, 37 906 lines of proof, and 1 267 747 total characters. The size of the gzipped tarball (gzip -9) of all the source files is 146 008 bytes, which is an estimate of the information content of my proof.”

Утверждение теоремы, записанное на языке Coq.

```
Theorem Incompleteness : forall T : System,
  Included Formula NN T ->
  RepresentsInSelf T ->
  DecidableSet Formula T ->
  exists f : Formula,
  Sentence f /\ (SysPrf T f /\ SysPrf T (notH f) -> Inconsistent LNN T).
```

#### А что мы можем сказать про противоречивать Ф.А.?

**Определение 6.4.3.** Обозначим за  $\psi(x, p)$  формулу, выражающую в формальной арифметике рекурсивное отношение Proof:  $\langle \ulcorner \xi \urcorner, p \rangle \in \text{Proof}$ , если  $p$  — гёделев номер доказательства  $\xi$ .  
Обозначим  $\pi(x) \equiv \exists p. \psi(x, p)$ .

**Определение 6.4.4.** Формулой Consis назовём формулу  $\neg \pi(\overline{\ulcorner 1 = 0 \urcorner})$ .

**Замечание.** Неформальный смысл Consis: «формальная арифметика непротиворечива».

**Теорема 6.4.4** (Вторая теорема Гёделя о неполноте арифметики). Если Consis доказуем, то формальная арифметика противоречива.

*Неформальное доказательство.* Формулировка 1 теоремы Гёделя о неполноте арифметики: «если Ф.А. непротиворечива, то недоказуемо  $\sigma(\overline{\ulcorner \sigma \urcorner})$ ».

То есть,  $\forall p. \neg \omega_1(\overline{\ulcorner \sigma \urcorner}, p)$ .

То есть, если Consis, то  $\sigma(\overline{\ulcorner \sigma \urcorner})$ .

То есть, если Consis, то  $\sigma(\overline{\sigma^1})$ , — и это можно доказать, то есть  $\vdash \text{Consis} \rightarrow \sigma(\overline{\sigma^1})$ .  
Однако, если формальная арифметика непротиворечива, то  $\nvdash \sigma(\overline{\sigma^1})$ . ■

**Определение 6.4.5.** Будем говорить, что формула  $\psi$ , выражающая отношение Proof, формула  $\pi$  и формула Consis соответствуют условиям Гильберта-Бернайса-Лёфа, если следующие условия выполнены для любой формулы  $\alpha$ :

1.  $\vdash \alpha$  влечет  $\vdash \pi(\overline{\alpha^1})$
2.  $\vdash \pi(\overline{\alpha^1}) \rightarrow \pi(\overline{\pi(\overline{\alpha^1})^1})$
3.  $\vdash \pi(\overline{\alpha \rightarrow \beta^1}) \rightarrow \pi(\overline{\alpha^1}) \rightarrow \pi(\overline{\beta^1})$

**Лемма 6.4.4.1.** Лемма об автоссылках. Для любой формулы  $\phi(x_1)$  можно построить такую замкнутую формулу  $\alpha$  (не использующую неаксиоматических предикатных и функциональных символов), что  $\vdash \phi(\overline{\alpha^1}) \leftrightarrow \alpha$ .

**Замечание.**  $\leftrightarrow$  означает, что это можно доказать и слева направо, и справа налево.

**Теорема 6.4.5.** Существует такая замкнутая формула  $\gamma$ , что если Ф.А. непротиворечива, то  $\nvdash \gamma$ , а если Ф.А.  $\omega$ -непротиворечива, то и  $\nvdash \neg\gamma$ .

*Доказательство.* Рассмотрим  $\phi(x_1) \equiv \neg\pi(x_1)$ . Тогда по лемме об автоссылках существует  $\gamma$ , что  $\vdash \gamma \leftrightarrow \neg\pi(\overline{\gamma^1})$ .

- Предположим, что  $\vdash \gamma$ . Тогда  $\vdash \gamma \rightarrow \neg\pi(\overline{\gamma^1})$ , то есть  $\nvdash \gamma$
- Предположим, что  $\vdash \neg\gamma$ . Тогда  $\vdash \pi(\overline{\gamma^1})$ , то есть  $\vdash \exists p.\psi(\overline{\gamma^1}, p)$ . Тогда по  $\omega$ -непротиворечивости найдётся  $p$ , что  $\vdash \psi(\overline{\gamma^1}, \overline{p})$ , то есть  $\vdash \gamma$ .

*Доказательство второй теоремы Гёделя.* 1. Пусть  $\gamma$  таково, что  $\vdash \gamma \leftrightarrow \neg\pi(\overline{\gamma^1})$ .

2. Покажем  $\pi(\overline{\gamma^1}) \vdash \pi(\overline{1 = 0^1})$ .

- (а) По условию 2,  $\vdash \pi(\overline{\gamma^1}) \rightarrow \pi(\overline{\pi(\overline{\gamma^1})^1})$ . По теореме о дедукции  $\pi(\overline{\gamma^1}) \vdash \pi(\overline{\pi(\overline{\gamma^1})^1})$ ;
- (б) Так как  $\vdash \pi(\overline{\gamma^1}) \rightarrow \neg\gamma$ , то по условию 1  $\vdash \pi(\overline{\pi(\overline{\gamma^1}) \rightarrow \neg\gamma^1})$ ;
- (с) По условию 3,  $\pi(\overline{\gamma^1}) \vdash \pi(\overline{\pi(\overline{\gamma^1})^1}) \rightarrow \pi(\overline{\pi(\overline{\gamma^1}) \rightarrow \neg\gamma^1}) \rightarrow \pi(\overline{\neg\gamma^1})$ ;
- (д) Таким образом,  $\pi(\overline{\gamma^1}) \vdash \pi(\overline{\neg\gamma^1})$ ;
- (е) Однако,  $\vdash \gamma \rightarrow \neg\gamma \rightarrow 1 = 0$ . Условие 3 (применить два раза) даст  $\pi(\overline{\gamma^1}) \vdash \pi(\overline{1 = 0^1})$ .

3.  $\neg\pi(\overline{1 = 0^1}) \rightarrow \neg\pi(\overline{\gamma^1})$  (т. о дедукции, контрапозиция).

4.  $\vdash \neg\pi(\overline{1 = 0^1}) \rightarrow \gamma$  (определение  $\gamma$ ). ■

## 7 Теория множеств

Теория множеств была создана, что наконец положить нормальный фундамент в основание математики.

Основной принцип, лежащий в основе теории множеств — *неограниченный принцип абстракции*  $\{x \mid P(x)\}$ .

Тут сразу же возникает парадокс:  $X = \{x \mid x \notin x\}$ . Выполнено ли  $X \in X$ ?

Давайте попробуем решить этот парадокс. Варианты решения:

1. Запретить все «опасные» ситуации
2. Запретить вообще все, кроме некоторого количества разрешенных вещей. Аксиоматика Цермело — 1908 год, оставим только то, что используют математики.

Что такое множество? Не будем отвечать, поступим иначе.

## 7.1 Аксиоматика ZF

*Цермело, Френкель (совсем немного).*

**Определение 7.1.1.** Теория множеств — теория первого порядка, с дополнительным нелогическим двуместным функциональным символом  $\in$ , и следующими дополнительными нелогическими аксиомами и схемами аксиом.

**Определение 7.1.2** (Равенство «по Лейбницу»). Объекты равны, если неразличимы.

Если нечто ходит как утка, выглядит как утка и крякает как утка, то это утка.

**Определение 7.1.3** (Равенство по принципу объёмности). Объекты равны, если состоят из одинаковых частей

Мы бы хотели, чтобы эти определения совпадали. В качестве основного возьмем принцип объёмности, а первый признак докажем.

**Определение 7.1.4.**  $A \subseteq B \equiv \forall x. x \in A \rightarrow x \in B$ .  
 $A = B \equiv A \subseteq B \& B \subseteq A$ .

### 7.1.1 Аксиомы теории множеств

**Определение 7.1.5** (Аксиома равенства). Равные множества содержатся в одних и тех же множествах.

$$\forall x. \forall y. \forall z. x = y \& x \in z \rightarrow y \in z.$$

**Определение 7.1.6** (Аксиома пустого). Существует пустое множество  $\emptyset$ .

$$\exists s. \forall t. \neg t \in s.$$

**Определение 7.1.7** (Аксиома пары). Существует  $\{a, b\}$ . Каковы бы ни были два множества  $a$  и  $b$ , существует множество, состоящее в точности из них.

$$\forall a. \forall b. \exists s. a \in s \& b \in s \& \forall c. c \in s \rightarrow c = a \vee c = b.$$

**Определение 7.1.8** (Аксиома объединения). Существует  $\cup x$ .

Для любого непустого множества  $x$  найдется такое множество, которое состоит в точности из тех элементов, из которых состоят элементы  $x$ .

$$\forall x. (\exists y. y \in x) \rightarrow \exists p. \forall y. y \in p \leftrightarrow \exists s. y \in s \& s \in x.$$

**Замечание.**  $\leftrightarrow$  здесь также, как и раньше, означает импликацию в обе стороны.

**Определение 7.1.9** (Аксиома степени). Существует  $\mathcal{P}(x)$  (булеан).

Каково бы ни было множество  $x$ , существует множество, содержащее в точности все возможные подмножества множества  $x$ .

$$\forall x. \exists p. \forall y. y \in p \leftrightarrow y \subseteq x.$$

**Определение 7.1.10** (Схема аксиом выделения). Существует  $\{t \in x \mid \varphi(t)\}$ .

Для любого множества  $x$  и любой формулы от одного аргумента  $\varphi(y)$  ( $b$  не входит свободно в  $\varphi$ ), найдется  $b$ , в которое входят те и только те элементы из множества  $x$ , что  $\varphi(y)$  истинно.

$$\forall x. \exists b. \forall y. y \in b \leftrightarrow (y \in x \& \varphi(y)).$$

**Теорема 7.1.1.** Для любого множества  $X$  существует множество  $\{X\}$ , содержащее в точности  $X$ .

*Доказательство.* Воспользуемся аксиомой пары:  $\{X, X\}$  ■

**Теорема 7.1.2.** Пустое множество единственно.

*Доказательство.* Пусть  $\forall p. \neg p \in s$  и  $\forall p. \neg p \in t$ . Тогда  $s \subseteq t$  и  $t \subseteq s$ . ■

**Теорема 7.1.3.** Для двух множеств  $s$  и  $t$  существует множество, являющееся их пересечением.

*Доказательство.*  $s \cap t = \{x \in s \mid x \in t\}$  ■

**Определение 7.1.11** (Упорядоченная пара). Упорядоченной парой двух множеств  $a$  и  $b$  назовём  $\{\{a\}, \{a, b\}\}$ , или  $\langle a, b \rangle$ .

**Теорема 7.1.4.** Упорядоченную пару можно построить для любых множеств.

*Доказательство.* Применить аксиому пары, теорему о существовании  $\{X\}$ , аксиому пары. ■

**Теорема 7.1.5.**  $\langle a, b \rangle = \langle c, d \rangle$  тогда и только тогда, когда  $a = c$  и  $b = d$ .

**Определение 7.1.12.** Инкремент:  $x' \equiv x \cup \{x\}$ .

**Определение 7.1.13** (Аксиома бесконечности). Существует  $N : \emptyset \in N \& \forall x. x \in N \rightarrow x' \in N$



В  $N$  есть всевозможные множества вида  $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \dots$  (неформально)  $\omega = \{\emptyset, \emptyset', \emptyset'', \dots\}$ . Тогда  $N_1 = \omega \cup \{\omega, \omega', \omega'', \dots\}$  подходит.

### Полный порядок (вполне упорядоченные множества)

1. Частичный: рефлексивность ( $a \leq a$ ), антисимметричность ( $a \leq b \rightarrow b \leq a \rightarrow a = b$ ), транзитивность ( $a \leq b \rightarrow b \leq c \rightarrow a \leq c$ ).
2. Линейный: частичный +  $\forall a. \forall b. a \leq b \vee b \leq a$ .
3. Полный: линейный + в любом непустом подмножестве есть наименьший элемент.

**Пример.**  $\mathbb{Z}$  не вполне упорядочено: в  $\mathbb{Z}$  нет наименьшего.

**Пример.** Отрезок  $[0, 1]$  не вполне упорядочен:  $(0, 1)$  не имеет наименьшего.

**Пример.**  $\mathbb{N}$  вполне упорядочено.

### 7.1.2 Ординалы

**Определение 7.1.14.** Транзитивное множество  $X$ :  $\forall x. \forall y. x \in y \rightarrow y \subseteq X$ .

**Определение 7.1.15.** Ординал — вполне упорядоченное отношением ( $\in$ ) транзитивное множество.

**Пример.** Ординалы:  $\emptyset, \emptyset', \emptyset'', \dots$

**Определение 7.1.16.** Предельный ординал: такой  $x$ , что  $x \neq \emptyset$  и нет  $y : y' = x$ .

**Определение 7.1.17.** Ординал  $x$  конечный, если он меньше любого предельного.

**Теорема 7.1.6.** Если  $x, y$  — ординалы, то  $x \in y$  или  $y \in x$ .

**Определение 7.1.18.**  $\omega$  — наименьший предельный ординал.

**Теорема 7.1.7.**  $\omega$  существует.

*Доказательство.* Пусть  $\omega = \{x \in N \mid x \text{ конечен}\}$ .

Пусть  $\theta$  таков, что  $\theta \in \omega$ . Тогда  $\theta$  конечен. Пусть  $\theta$  таков, что  $\theta' = \omega$ . Тогда  $\theta \in \omega$ . ■

**Пример.**  $\omega'$  — тоже ординал.

**Определение 7.1.19.**  $\sup x$  — наименьший ординал, содержащий  $x$ :  $x \subseteq \sup x$ .

**Пример.**  $\sup\{\emptyset', \emptyset'', \emptyset'''\} = \{\emptyset, \emptyset', \emptyset'', \emptyset''', \emptyset''''\} = \emptyset''''$

**Определение 7.1.20.** Определим сложение так:

$$a + b \equiv \begin{cases} a, & b \equiv \emptyset \\ (a + c)', & b \equiv c' \\ \sup\{a + c \mid c < b\}, & b \text{ — предельный ординал} \end{cases}.$$

**Пример.**  $\omega + 1 = \omega \cup \{\omega\}$ .

$$1 + \omega = \sup\{1 + \emptyset, 1 + 1, 1 + 2, \dots\} = \omega.$$

**Определение 7.1.21.** Определим умножение так:

$$a \cdot b \equiv \begin{cases} 0, & b \equiv \emptyset \\ (a \cdot c) + a, & b \equiv c' \\ \sup\{a \cdot c \mid c < b\}, & b \text{ — предельный ординал} \end{cases}.$$

**Определение 7.1.22.** Определим возведение в степень так:

$$a^b \equiv \begin{cases} 1, & b \equiv \emptyset \\ (a^c) \cdot a, & b \equiv c' \\ \sup\{a^c \mid c < b\}, & b \text{ — предельный ординал} \end{cases}.$$

**Пример.**  $\omega \cdot \omega = \sup\{\omega, \omega \cdot 2, \omega \cdot 3, \dots\}$ .

**Пример.** Гостиница с  $\omega$  номерами, въезжает постоялец.  $1 + \omega = \omega$ .

Добавить элемент перед бесконечностью.

**Пример.** Ввести особое значение  $+\infty$ .  $\omega + 1 \neq \omega$ .

Добавить элемент после бесконечности.

**Пример.** Упорядочивание алгебраических типов.

Neg of nat | Pos of nat

$\omega + \omega$  — в самом деле, Neg 5 < Pos 5. Neg 5 в данном упорядочении соответствует 5, а Pos 5 соответствует  $\omega + 5$ .

**Определение 7.1.23.** Дизъюнктное (разделённое) множество — множество, элементы которого не пересекаются.

$$Dj(x) \equiv \forall y. \forall z. (y \in x \& z \in x \& \neg y = z) \rightarrow \neg \exists t. t \in y \& t \in z.$$

**Пример.** Д дизъюнктное:  $\{\{1, 2\}, \{\rightarrow\}, \{\alpha, \beta, \gamma\}\}$ .

Не дизъюнктное:  $\{\{1, 2\}, \{\rightarrow\}, \{\alpha, \beta, \gamma, 1\}\}$ .

**Определение 7.1.24.** Прямое произведение дизъюнктного множества  $a$  — множество  $\times a$  всех таких множеств  $b$ , что:

- $b$  пересекается с каждым из элементов множества  $a$  в точности в одном элементе
- $b$  содержит элементы только из  $\cup a$ .

$$\forall b. b \in \times a \leftrightarrow (b \subseteq \cup a \& \forall y. y \in a \rightarrow \exists! x. x \in y \& x \in b).$$

**Пример.**  $\times \{\{\Delta, \square\}, \{1, 2, 3\}\} = \{\{\Delta, 1\}, \{\Delta, 2\}, \{\Delta, 3\}, \{\square, 1\}, \{\square, 2\}, \{\square, 3\}\}$

### 7.1.3 Аксиома выбора

**Определение 7.1.25.** Прямое произведение непустого дизъюнктного множества, не содержащего пустых элементов, непусто.

$$\forall t. Dj(t) \rightarrow (\forall x. x \in t \rightarrow \exists p. p \in x) \rightarrow (\exists p. p \in \times t)$$

Альтернативные варианты: любое множество можно вполне упорядочить, любая сюръективная функция имеет частичную обратную, и т.п.

**Определение 7.1.26.** Аксиоматика  $ZF + \text{аксиома выбора} = ZFC$ .

**Пример.** Парадокс Банаха-Тарского: трёхмерный шар равносоставлен двум своим копиям.

**Теорема 7.1.8.** Теорема (Гёдель, 1938): аксиома выбора не добавляет противоречий в  $ZF$ .

**Теорема 7.1.9.** Теорема (Коэн, 1963): аксиома выбора не следует из других аксиом  $ZF$ .

**Пример.** Односторонние функции: Sha256 и т.п. У Sha256 есть обратная.

**Теорема 7.1.10.** Теорема Диаконеску:  $ZFC$  поверх интуиционистского исчисления предикатов содержит правило исключённого третьего.

**Определение 7.1.27** (Аксиома фундирования). В каждом непустом множестве найдется элемент, не пересекающийся с исходным множеством.

$$\forall x. x = \emptyset \vee \exists y. y \in x \text{ и } y \cap x = \emptyset.$$

Аксиома фундирования исключает множества, которые могут принадлежать сами себе (возможно, через цепочку принадлежностей):  $X \in Y \in Z \in X$ .

**Определение 7.1.28** (Схема аксиом подстановки). Если задана некоторая функция  $f$ , представляемая в исчислении предикатов (то есть задана некоторая формула  $\phi$ , такая, что  $f(x) = y$  тогда и только тогда, когда  $\phi(x, y) \wedge \exists! z \phi(x, z)$ ), то для любого множества  $S$  существует множество  $f(S)$  — образ множества  $S$  при отображении  $f$ .

$$\forall s. (\forall x. \forall y_1. \forall y_2. x \in s \wedge \phi(x, y_1) \wedge \phi(x, y_2) \rightarrow y_1 = y_2) \rightarrow (\exists t. \forall y. y \in t \leftrightarrow \exists x. x \in s \wedge \phi(x, y)).$$

## 7.2 Координальные числа

*Ординальные числа — порядковые, а координальные — количественные.*

**Определение 7.2.1.**  $\langle D$  (обл. определения, domain),  $C$  (обл. значения, codomain),  $G$  (график)  $\rangle$  — это функция.

**Определение 7.2.2.** Биективная функция — сюръективная и инъективная функция.

**Определение 7.2.3.**  $|X| = |Y|$  (множество  $X$  равномощно множеству  $Y$ ), если существует биективная функция  $f : X \rightarrow Y$ .

**Определение 7.2.4.**  $|X| \leq |Y|$  ( $X$  имеет мощность не больше  $Y$ ), если существует инъективная функция  $f : X \rightarrow Y$ .

**Определение 7.2.5.**  $|X| < |Y|$  ( $X$  имеет мощность строго меньше  $Y$ ), если  $|X| \leq |Y|$  и  $|X| \neq |Y|$ .

**Определение 7.2.6.** Координальное число — ординальное число  $a$ , у которого нет меньшего его, равномощного ему, для которого не существует числа  $b$  меньшего, но равномощного ему.  
То есть, нет  $b$ :  $|a| = |b|$ , но  $b \in a$ .

**Пример.** Примеры:  $0, 1, 2, 3, 4, \dots, 178$ .

**Утверждение 7.2.1.**  $\omega$  — это  $0, 1, 2, 3, \dots$ .

*Доказательство.* Действительно, если  $b \in \omega$ , то  $b$  — конечен (по определению  $\omega$ ). Очевидно,  $b$  не равномощен  $\omega$ . ■

**Определение 7.2.7.** На самом деле  $|\omega| = \aleph_0$ .

Что такое  $\aleph_1$ ?

**Определение 7.2.8.**  $\aleph_1$  — такой  $c$ , что  $\aleph_0 < |c|$ .

**Замечание.** Координальные числа так же имеют нумерацию (потому что они ординальные числа и имеют полный порядок).

$$0 < 1 < 2 < \dots < \aleph_0 < \aleph_1.$$

**Определение 7.2.9** (Альтернативное определение). Координальные числа — множество всех равномощных ординальных чисел.

Что такое  $\aleph_1$ ? Какие есть мощности, большие  $\aleph_0$  (больше счетной мощности).

**Пример.** 1.  $|\omega + 1| = \aleph_0$ .

Определим  $f(x) = \begin{cases} \omega, & x = 0 \\ x - 1, & x > 0 \end{cases}$ .  $f$  очевидно биекция, следовательно имеет место быть равномощность.

2.  $|\omega \cdot \omega| = \aleph_0$ .

$\omega \cdot$  — множество упорядоченных пар  $\langle k, l \rangle$ , их можно пересчитать как рациональные числа.

3.  $|\omega^\omega| = \aleph_0$ .

Доказательство в домашнем задании.

### 7.2.1 Теорема Кантора

**Теорема 7.2.1.** Если  $X$  — некоторое множество, то  $|X| < |\mathcal{P}(X)|$ .

**Замечание.**  $\mathcal{P}(X)$  здесь также, как и раньше означает булеан, то есть семейство всех подмножеств  $X$ .

*Доказательство.* Используем диагональный метод.

Пусть не так. Пусть существует  $f : X \rightarrow \mathcal{P}(X)$  и  $f$  — биекция.

Пусть, например  $X = \omega$ .  $f(3) = \{3, 1, 2\}$ ,  $f(2) = \{1, 4\}$ ,  $f(0) = \{\omega\}$ .  $X = \{x_0, x_1, x_2, \dots\}$ .

|       | $x_0$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ |
|-------|-------|-------|-------|-------|-------|
| $x_0$ | ×     | ×     | ×     | ×     | ×     |
| $x_1$ |       |       |       |       |       |
| $x_2$ |       | ×     |       |       | ×     |
| $x_3$ |       | ×     | ×     | ×     |       |

Будем писать табличку.

Биективная ли эта функция? В инъективность мы готовы верить, а вот что с сюръективностью?

Пусть она сюръективна, построим  $T$ , не имеющий прообраз.

Рассмотрим  $f(x_0)$ . Верно ли, что  $x_0 \in f(x_0)$ ? Если да, то  $T \not\ni x_0$ . Если нет, то  $x_0 \in T$ .

То есть  $T = \{x \in \mathcal{P}(X) \mid x \notin f(x)\}$  (просто аксиома выделения).

Каков  $t$ , что  $f(t) = T$ ? Ни  $x_0$ , ни  $x_1$ , ни  $\dots$  не может быть  $t$ .

Значит  $f$  не сюръективна, то есть  $|X| \neq |\mathcal{P}(X)|$ .

Однако,  $|X| \leq |\mathcal{P}(X)|$ . Просто потому что можно рассмотреть функцию  $f(x) = \{x\}$ .  $f$  — инъективна.

Значит  $|X| < |\mathcal{P}(X)|$ . ■

### 7.2.2 Мощности, большие алеф 0, континуум гипотеза

Как тогда получить  $\aleph_1$ ?

Действительно, можно взять  $\mathcal{P}(\omega)$ . Но равно ли  $|\mathcal{P}(\omega)| = \aleph_1$ ?

На самом деле не известно.

**Определение 7.2.10.**  $|\mathcal{P}(\omega)|$  — мощность континуум, то есть мощность вещественных чисел.

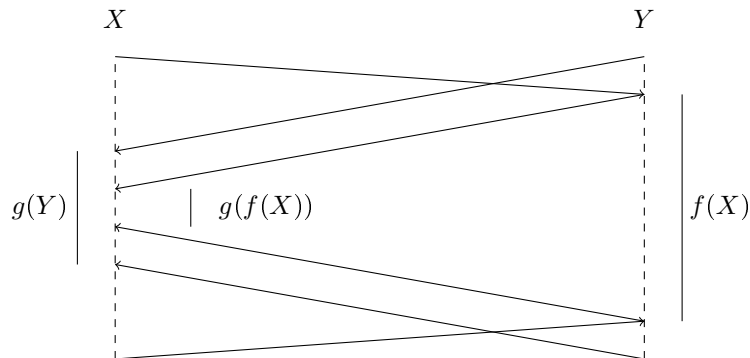
**Утверждение 7.2.2.** Континуум гипотеза: существуют ли промежуточные между  $\aleph_0$  и  $|\mathcal{P}(\omega)|$ ?

**Теорема 7.2.2** (Коэн, 1962–1963). Континуум-гипотеза не зависит от аксиоматики Цермело–Френкеля. Мы можем согласиться с ней, а можем отвергнуть.

### 7.2.3 Теорема Кантора–Бернштейна

**Теорема 7.2.3.** Если  $|X| \leq |Y|$  и  $|Y| \leq |X|$ , то  $|X| = |Y|$ .

*Доказательство.* У нас есть функции  $f : X \rightarrow Y$  и  $g : Y \rightarrow X$ , они обе инъективны.



$|X| = |f(X)|$ ,  $|Y| = |g(Y)|$  (так как функции инъективны), значит  $|g(f(X))| : X \rightarrow X$  — инъективная функция. Хотим показать, что ее образ равномошен исходному образу.

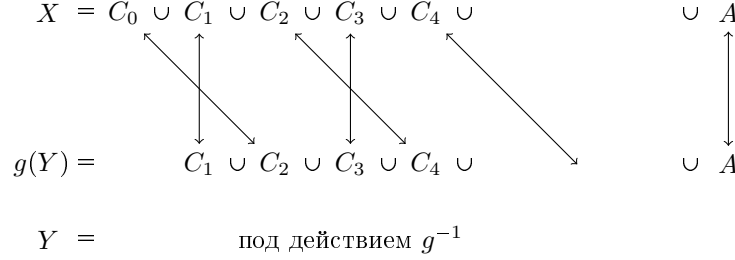
Занумеруем множества.

$$\begin{aligned} X &= A_0 \\ g(Y) &= A_1 \quad A_1 \subseteq A_0, \text{ так как } g : Y \rightarrow X \\ g(f(X)) &= A_2 \quad A_2 \subseteq A_1, \text{ так как } f(X) \subseteq Y \\ g(f(g(Y))) &= A_3 \quad A_3 \subseteq A_2 \\ g(f(g(f(X)))) &= A_4 \quad A_4 \subseteq A_3 \\ \dots &= A_5 \\ \dots \quad A_{n+1} &\subseteq A_n \end{aligned}$$

Давайте пересечем все  $A_i$ :  $A_0 \cap A_1 \cap A_2 \cap \dots = A$ .

Определим  $C_n = A_n \setminus A_{n+1}$ . Тогда  $X = C_0 \cup C_1 \cup C_2 \cup \dots \cup A$ .  $g(f(X)) = C_1 \cup C_2 \cup \dots \cup A$ . Действительно, в  $g(f(X))$  входит все, что входит в  $X$ , кроме  $C_0$ .

Построим биекцию между  $X$  и  $g(Y)$  так:



Обозначим построенное отображение  $p : X \rightarrow g(Y)$  — биекция. Тогда  $q(x) = g^{-1}(p(x)) : X \rightarrow Y$  — биекция. То есть  $|X| = |Y|$ . ■

#### 7.2.4 Мощность вещественных чисел

**Теорема 7.2.4.** Мощность вещественных чисел —  $\mathcal{P}(\omega)$ .

*Доказательство.* Рассмотрим все двоичные дроби:  $10, 101 = 1 \cdot 2^1 + 0 \cdot 2^0 + 1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$ .

- Для каждой двоичной дроби есть вещественное число
- Почти все записи двоичных дробей не равны (тех, которые равны — конечное число).

Все двоичные дроби — это множество всех подмножеств натуральных чисел. ■