Конспекты по математической логике

Анатолий Коченюк, Георгий Каданцев, Константин Бац

2022 год, семестр 4

Лектор: Дмитрий Григорьевич Штукенберг.
Запись лекций: `https://youtube.com/playlist?list=PLd7QXkfmSY7Yk0X2WLQIY_nQDvh8FleTX`.
Конспект основан на слайдах с лекций: `https://github.com/shd/logic2022`.

1 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 вообще такое язык? Это отдельный 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. Они являются частью языка исследователя.

1. α, β, γ — метапеременные для всех высказываний.

2. X, Y, Z — метапеременные для пропозициональных переменных.

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.

1.1 Теория моделей

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

Определение 1.1.1. Оценка — это функция, сопоставляющая высказыванию его истинное (истинностное) значение.

1.2 Теория доказательств

Определение 1.2.1. Аксиомы — это список высказываний. Схема аксиомы — высказывание вместе с метапеременными; при любой подстановке высказываний вместо метапеременной получим аксиому.

Определение 1.2.2. Доказательство (вывод) — последовательность высказываний $\gamma_1, \gamma_2 \dots$ где γ_i— любая аксиома, либо существуют $j, k < i$ такие что γ_j имеет вид $(\gamma_k \to \gamma_i)$. Это правило "перехода по следствию" или Modus ponens.

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

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

Пример. Доказательство $\vdash A \to A$.

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

1.3 Теорема о дедукции

Определение 1.3.1. (Метаметаопределение). Будем большими греческими буквами $\Gamma, \Delta, \Sigma \dots$ — списки формул, неупорядоченные.

Определение 1.3.2. Вывод из гипотез: $\Gamma \vdash \alpha$.
То есть существует $\delta_1, \dots, \delta_n$, $\delta_n \equiv \alpha$, где δ_i или аксиома, гипотеза или m.p. из j и k и $j, k < i$.

Теорема 1.3.1. $\Gamma, \alpha \vdash \beta$ тогда и только тогда, когда $\Gamma \vdash \alpha \to \beta$.

Доказательство. $\Leftarrow$ Пусть $\delta_1, \delta_2 \dots \delta_n \equiv \alpha \to \beta$ выводит $\alpha \to \beta$. Дополним этот вывод до доказательства двумя 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 $\Gamma \vdash \alpha \to \beta$.

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

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

■

1.4 Теория моделей

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

Определение 1.4.1. $\mathbb{V}$ — истинностное множество.
F — множество высказываний нашего исчисления высказываний.
P — множество пропозициональных переменных.

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

Определение 1.4.2. Для задания оценки необходимо задать оценку пропозициональных переменных.

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

Тогда:

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

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

Определение 1.4.3. α — общезначимая (истинна), если $[\![\alpha]\!] = \text{И}$ при любой оценке P.
α — невыполнима (ложна), если $[\![\alpha]\!] = \text{Л}$ при любой оценке P.
α — выполнима, если $[\![\alpha]\!] = \text{И}$ при некоторой f_P.
α — опровержима, если $[\![\alpha]\!] = \text{Л}$ при некоторой f_P.

Определение 1.4.4. Теория корректна, если доказуемость влечёт общезначимость.
Теория полна, если общезначимость влечёт доказуемость.

Определение 1.4.5. $\Gamma \models \alpha$ означает, что α следует из $\Gamma = \{\gamma_1, \dots, \gamma_n\}$, если $[\![\alpha]\!] = И$ всегда при $[\![\gamma_i]\!] = И$ при всех i.

1.5 Корректность исчисления высказываний

Теорема 1.5.1. Исчисление высказываний корректно. $\vdash \alpha$ влечёт $\models \alpha$.

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

Разбор случаев:

1. δ_i аксиома $\implies$ построить таблицу истинности, проверить, что все верно.
2. δ_i — м.п. δ_j, $\delta_k \equiv \delta_j \to \delta_i \implies$ 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.

1.6 Полнота исчисления высказываний

Теорема 1.6.1. Исчисление высказываний полно.

Определение 1.6.1. ${}_{[\beta]}\alpha = \begin{cases} \alpha, & [\![\beta]\!] = И \\ \neg\alpha, & [\![\beta]\!] = Л \end{cases}$

Лемма 1.6.1.1. ${}_{[\alpha]}\alpha$, ${}_{[\beta]}\beta \vdash_{[\alpha\star\beta]} \alpha \star \beta$,
${}_{[\alpha]}\alpha \vdash_{[\neg\alpha]} \neg\alpha$

Доказательство было в дз. ■

Пример. $[\![\alpha]\!] = И, [\![\beta]\!] = Л \implies \alpha \wedge \neg\beta \vdash \neg(\alpha \wedge \beta)$.

Лемма 1.6.1.2. Если $\Gamma \vdash \alpha$, то $\Gamma, \Delta \vdash \alpha$.

Лемма 1.6.1.3. Пусть дана α, $X_1, \dots, X_n$ — её переменные.

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

Доказательство. Пусть $\widetilde{X} =_{[X_1]} X_i \dots {}_{[X_n]} X_n$.

Индукция по длине формулы α.

База: $\alpha = X_i$.

Переход: есть α, β. По предположению $\widetilde{X} \vdash_{[\alpha]} \alpha \quad \widetilde{X} \vdash_{[\beta]} \beta$.

По лемме 1 тогда $\widetilde{X} \vdash_{[\alpha\star\beta]} \alpha \star \beta$. ■

Лемма 1.6.1.4. Если $\models \alpha$, то при любой оценке $\widetilde{X} \vdash \alpha$. То есть при любых подстановках значений α будет истинна.

Лемма 1.6.1.5.

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

Доказательство было в дз. ■

Лемма 1.6.1.6. Если $\tilde{X} \vdash \alpha$ при всех оценках $X_1, \dots, X_n$, то $\vdash \alpha$.

Доказательство индукцией по n. ■

Теорема 1.6.1. Исчисление высказываний полно. Если $\models \alpha$, то $\vdash \alpha$.

Доказательство. По лемме 4 и лемме 6. ■

2 Интуиционистская логика

Мы не хотим дурацких конструкций вроде парадокса брадобрея. Мы не хотим странных, но логически верных утверждений вроде $A \to B \vee B \to A$. 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 α, и β.
- $\alpha \vee \beta$, если мы умеем строить α, β и знаем, что именно.
- $\alpha \to \beta$, если мы умеем перестроить α в β.
- $\perp$ — не имеет построения
- $\neg\alpha \equiv \alpha \to \perp$

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

$$\alpha \to \neg\alpha \to \beta$$

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 ($[\![A \vee \neg A]\!] = И$, но $\not\vdash_{\text{И}} A \vee \neg A$).

2. Пусть X топологическое пространство.

   Пусть истинностные значения — все открытые пространства в классической топологии.

   - $[\![\alpha \& \beta]\!] = [\![\alpha]\!] \cap [\![\beta]\!]$.
   - $[\![\alpha \vee \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$.
   - $[\![\alpha \to \beta]\!] = (X \backslash [\![\alpha]\!] \cup [\![\beta]\!])^o$.
   - $[\![\neg\alpha]\!] = (X \backslash [\![\alpha]\!])^o$.

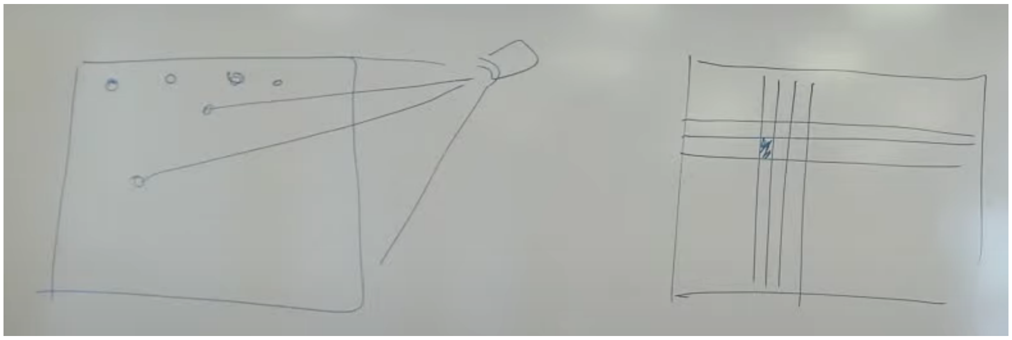
Теорема 2.0.1. Топологические модели — корректные модели ИИВ.

Утверждение 2.0.1. $\not\vdash_{\text{И}} A \vee \neg A$.

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

2.1 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 $\Omega \subseteq \mathcal{P}(X)$. Ω — топология, если это множество открытых множеств и выполнены следующие условия:

1. $\varnothing, X \in \Omega$;
2. $\bigcup\limits_i A_i \in \Omega$, если все $A_i \in \Omega$;
3. $\bigcap\limits_{i=1}^{n} A_i \in \Omega$, если $A_1, \ldots, A_n \in \Omega$.

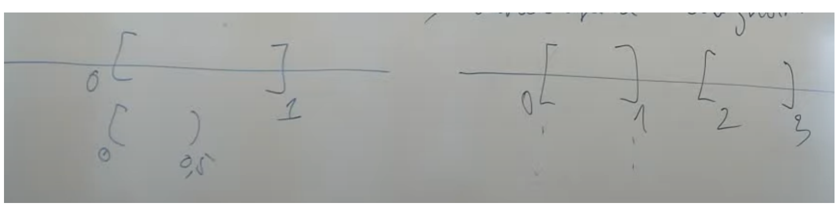
То есть топологическое пространство — пара $\langle X, \Omega \rangle$ и про Ω верны приведенные выше три утверждения.

Определение 2.1.1 (Замкнутое множество)**.** Множество B такое, что $X \backslash B \in \Omega$ называется замкнутым.

Определение 2.1.2 (Связное топологическое пространство)**.** $\langle X, \Omega \rangle$ связно, если нет $A, B \in \Omega\ :\ A \cup B = X$ и $A \cap B = \varnothing$

Определение 2.1.3 (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 2.1.4 (Связное множество)**.** Множество, являющееся связным подпространством.



2.2 Примеры топологических пространств

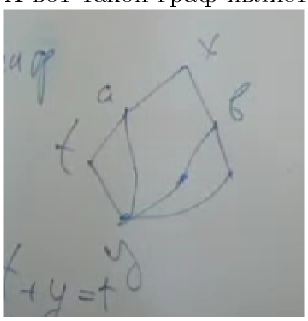
Возьмем дерево (граф). Множество X — множество вершин. Ω — множество всех вершин, что $B \in \Omega$, если $a \in B$, $x \leqslant a$ влечет $x \in B$. То есть Ω — семейство множеств вершин, которые входят вместе с поддеревом.

Теорема 2.2.1. Граф без цикла связен тогда и только тогда, когда оно связно как топологическое пространство.

Доказательство будет в дз. ■

Определение 2.2.1 (Решетки). X — частично упорядоченное множество отношением $\leqslant$.
Множество верхних граней a, b $a \sqcap b$ — множество $\{x \in X \mid a \leqslant x, b \leqslant x\}$.
Множество нижних граней a, b: $a \sqcup b$ — множество $\{x \in X \mid a \geqslant x, b \geqslant x\}$.
a — наименьший элемент $A \iff a \in A$ и любой $b \in A$, $b \geqslant a$.
a — наибольший элемент $A \iff a \in A$ и любой $b \in A$, $b \leqslant a$.
$a + b$ = наименьший элемент множества верхних граней.
$a \cdot b$ = наибольший элемент множества нижних граней.
Решетка — частично упорядоченное множество, где для каждых двух элементов существуют $a + b$ и $a \cdot b$.

Пример. Дерево — не решетка (в общем случае), так как $a + b$ есть, а $a * b$ может не быть.
А вот такой граф является решеткой.



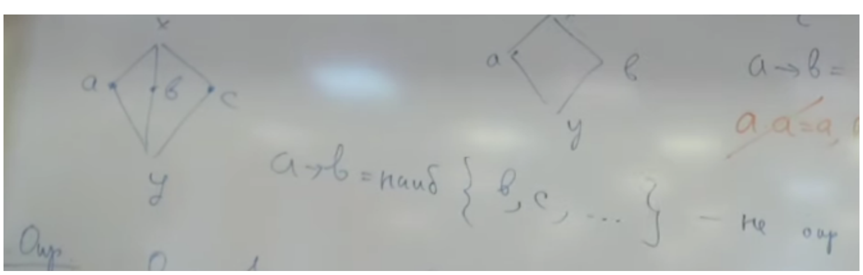
Теорема 2.2.2. Пусть $\langle X, \Omega \rangle$ топологическое пространство, $A, B \in \Omega$. $A \leqslant B$, если $A \subseteq B$.
Тогда $\langle \Omega, \leqslant \rangle$ — решетка. $A \cdot B = A \cap B$, $A + B = A \cup B$.

Определение 2.2.2. Дистрибутивная решетка — это такая решетка, что $a, b, c \in \Omega$, $a + (b \cdot c) = (a + b) \cdot (a + c)$.

Лемма 2.2.2.1. Для дистрибутивной решетки так же верно, что $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Определение 2.2.3. Псевдодополнение $a \to b$ = наибольшее$\{c \mid a \cdot c \leqslant b\}$.

Определение 2.2.4. Диамант — такая решетка, что там нет для кого-то псевдодополнения.



Определение 2.2.5. Решетка с псевдодополнением для всех элементов называется импликативной.

Определение 2.2.6. Определим 0 и 1 следующим образом:

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

Теорема 2.2.3 (В импликативной решетке 1 есть всегда)**.** $\langle X, \leqslant\rangle$ — импликативная решетка.

Доказательство. Рассмотрим $a \to a = \text{наиб}\{c \mid a \cdot c \leqslant a\} = \text{наиб}\{X\} = 1$. ∎

Теорема 2.2.4. Рассмотрим $\langle X, \Omega\rangle$ — импликативная решетка с 0. Рассмотрим И.И.В.

Определим оценки $\mathbb{V} = X$:

- $[\![\alpha \& \beta]\!] = [\![\alpha]\!] \cdot [\![\beta]\!]$.
- $[\![\alpha \vee \beta]\!] = [\![\alpha]\!] + [\![\beta]\!]$.
- $[\![\alpha \to \beta]\!] = [\![\alpha]\!] \to [\![\beta]\!]$.
- $[\![\neg\alpha]\!] = [\![\alpha]\!] \to 0$.

α истинно, если $[\![\alpha]\!] = 1$.
$[\![\bot]\!] = 0$. $\neg\alpha \equiv \alpha \to \bot$.
Полученная модель — корректная модель И.И.В.

Определение 2.2.7. Натуральный вывод — построение доказательства в виде дерева, где полученное утверждение в самом низу.

$\overline{\Gamma, \varphi \vdash \varphi}$ (аксиома).
Вывод утверждения в доказательстве $\Gamma \vdash \varphi$.
Правила вывода (сверху — посылка, снизу — заключение):

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}, \quad \frac{\Gamma, \varphi \vdash \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi}, \quad \frac{\Gamma \vdash \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \& \psi}, \quad \frac{\Gamma \vdash \varphi \& \psi}{\Gamma \vdash \varphi}, \quad \frac{\Gamma \vdash \varphi \& \psi}{\Gamma \vdash \psi},$$

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}, \quad \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}, \quad \frac{\Gamma, \varphi \vdash \rho \quad \Gamma, \psi \vdash \rho \quad \Gamma \vdash \varphi \vee \psi}{\Gamma \vdash \rho}, \quad \frac{\Gamma \vdash \bot}{\Gamma \vdash \varphi}.$$

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

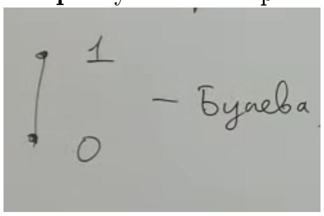
Теорема 2.2.5. Если $\vdash_{\text{И}} \alpha \vee \beta$, то $\vdash_{\text{И}} \alpha$ или $\vdash_{\text{И}} \beta$.

Определение 2.2.8. Алгебра Гейтинга (псевдобулева алгебра) — импликативная решетка с 0.

Определение 2.2.9. Введем операцию $\sim a \equiv a \to 0$ — дополнение до 0.

Определение 2.2.10. Булева алгебра — Алгебра Гейтинга, где $a + \sim a = 1$.

Пример. Булева Алгебра



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

Далее α, β — высказывания в ИИВ.

Определение 2.2.11. $\alpha \leqslant \beta$, если $\alpha \vdash \beta$

Определение 2.2.12 (Равносильность высказываний)**.** $\alpha \approx \beta$, если $\alpha \leqslant \beta$ и $\beta \leqslant \alpha$

Определение 2.2.13 (Алгебра Линденбаума)**.** Пусть ξ — множество всех высказываний ИИВ.

$[\xi]$ (множество классов эквивалентности высказываний по отношению $\approx$) называется алгеброй Линденбаума $\mathcal{L}$.

Теорема 2.2.6. $\mathcal{L}$ (алгебра Линденбаума) — Алгебра Гейтинга.

Введем оценку высказывания в алгебре Линденбаума. Отобразим $[\![\alpha]\!] = [\alpha]$ (то есть оценка α есть ее класс эквивалентности).

Лемма 2.2.6.1. $\mathbb{1} = [A \to A]$

Доказательство. $\alpha \vdash A \to A$, верно (очевидно), то есть $[\alpha] \leqslant [A \to A]$, то есть $[A \to A] = \mathbb{1}$. ∎

Теорема 2.2.7. $\mathcal{L}$ — корректная модель ИИВ.

Доказательство. Действительно, каждая формула имеет оценку, оценки представляются в виде решетки по отношению доказуемости. Если $[\alpha] = [A \to A]$, то и $[\![\alpha]\!] = [A \to A] = \mathbb{1}$. ∎

Теорема 2.2.8. $\mathcal{L}$ — полная модель ИИВ.

Доказательство. $\vDash \alpha$, то есть $[\alpha] = \mathbb{1}$.

$[\![\alpha]\!] = \mathbb{1}$, значит $[\![\alpha]\!] = [A \to A]$, это есть что α эффективна $\mathbb{1}$, то есть $\beta \leqslant [\alpha]$ при всех β.

Возьмем $\beta = A \to A$. Докажем, что $\vdash \alpha$.

1-5) $A \to A$

6) $A \to A \to \alpha$ (теорема о дедукции)

7) α

■

Теорема 2.2.9. Алгебра Гейтинга (все возможные ее модели) — полная и корректная модель ИИВ.

Определение 2.2.14. Исчисление дизъюнктно, если для любых $\alpha, \beta \quad \vdash \alpha \vee \beta$ влечёт $\vdash \alpha$ или $\vdash \beta$.

Теорема 2.2.10. ИИВ дизъюнктно.

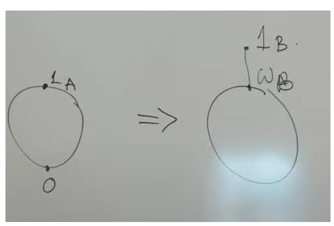
Определение 2.2.15. Пусть существует $f : A \to B, \quad A, B$ – алгебры Гейтинга.

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

Определение 2.2.16 (Геделева Алгебра)**.** Это такая алгебра, где $a + b = 1$ влечет $a = 1$ или $b = 1$.

Определение 2.2.17 ($\Gamma(A)$)**.** Пусть A — алгебра Гейтинга.

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



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

Теорема 2.2.11. $\Gamma(A)$ – Гёделева алгебра.

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

Определение 2.2.18. Каноническое отображение $g(x) : \Gamma(\mathcal{L}) \to \mathcal{L}$
$g(x) = \begin{cases} 1, & x = 1 \text{ или } \omega \\ x, & \text{иначе} \end{cases}$.

Утверждение 2.2.1. $g(x)$ – гомоморфизм

Утверждение 2.2.2. $\Gamma(\mathcal{L})$ — Гёделева алгебра.

Теорема 2.2.12. Рассмотрим ИИВ и алгебры Гейтинга $\mathcal{L}, \Gamma(\mathcal{L})$

Утверждение 2.2.3. Если $g : A \to B$ и $[\![\alpha]\!]_A = 1_A$, то $[\![\alpha]\!]_B = g(1_A)$.

Доказательство теоремы. Рассмотрим $\vdash \alpha \vee \beta$.
$\Gamma(\mathcal{L})$ — Гёделева алгебра, то есть алгебра Гейтинга.
$[\![\alpha \vee \beta]\!]_{\Gamma(\mathcal{L})} = 1_{\Gamma(\mathcal{L})}$, т.е. либо $[\![\alpha]\!] = 1_\gamma \mathcal{L}$ либо $[\![\beta]\!]_{\Gamma(\mathcal{L})} = 1_{\Gamma(\mathcal{L})}$
Рассмотрим $g : \Gamma(\mathcal{L}) \to \mathcal{L}$
$[\![\alpha]\!]_{\Gamma(\mathcal{L})} = 1_{\Gamma(\mathcal{L})}$, тогда $[\![\alpha]\!]_{\mathcal{L}} = g(1_{\Gamma(\mathcal{L})}) = 1_{\mathcal{L}}$
т.е. $\vdash \alpha$. ∎

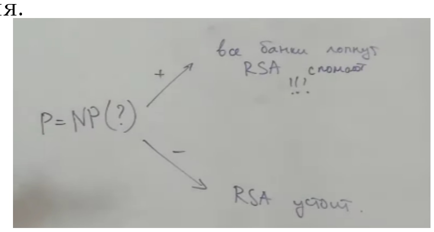
Определение 2.2.19. Модель ИИВ называется табличной, если

- $\mathbb{V}$ — множество истинностных значений;
- $[\![\alpha \star \beta]\!] = f_\star([\![\alpha]\!], [\![\alpha, \beta]\!])$,
- Существует $И \in \mathcal{S}$ – выделенная истина $[\![\alpha]\!] = И$ тогда и только тогда, когда $\models \alpha$.

Определение 2.2.20. Конечная табличная модель — модель, где $\mathbb{V}$ — конечная.

Замечание. Оценка работает так: $[\![P_i]\!] = f_\rho(P_i)$, $[\![\alpha \star \beta]\!] = f_\star([\![\alpha,]\!], [\![\beta]\!])$, $[\![\neg\alpha]\!] = f_\neg([\![\alpha,]\!])$. Если $\vdash \alpha$, то $[\![\alpha]\!] = И$ при любой оценке.

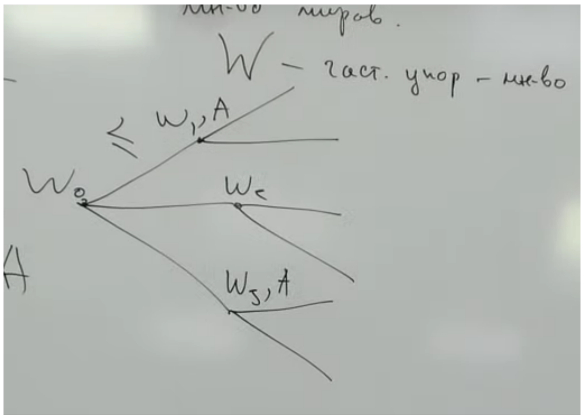
Представим не один мир, а много миров, в которых высказывания могут принимать разные значения.



Определение 2.2.21 (Модель Крипки)**.** Рассмотрим W_i множество миров, имеющие частичный порядок ($\leqslant$).
Зададим отношение вынужденности $W_i \Vdash P_i$ ($\Vdash \subseteq W_i \times P_i$).
При этом если $W_j \Vdash P_i$ и $W_j \leqslant W_k$, то $W_k \Vdash P_i$.

Определение 2.2.22. Доопределим связки $\Vdash$ на все выражения:

1. $W_i \Vdash \alpha \& \beta$, если $W_i \Vdash \alpha$ и $W_i \Vdash \beta$
2. $W_i \Vdash \alpha \vee \beta$, если $W_i \Vdash v$ или $W_i \Vdash \beta$
3. $W_i \Vdash \neg\alpha$, если нет $W_j \geqslant W_i$, что $W_j \Vdash \alpha$
4. Пусть во всех $W_j \geqslant W_i$ всегда, когда $W_j \Vdash \alpha$, имеет место $W_j \Vdash \beta$, тогда в мире W_i вынуждена импликация.



Определение 2.2.23. Если $W_i \Vdash \alpha$ при всех $W_i \in W$, то $\vDash \alpha$ (α общезначима).

Теорема 2.2.13. Модель Крипке — корректная модель ИИВ.

Доказательство. Пусть $\langle W, \Omega \rangle$ — топология, $\Omega = \{\widetilde{W} \subseteq W \mid \text{если } W_i \in \widetilde{W}, W_i \leqslant W_j, \text{ то } W_j \in \widetilde{W}\}$ (множество всех подлесов, где каждый узел присутствует вместе со своим поддеревом).
Пусть $\{W_k \mid W_k \Vdash P_j\}$ — открытое множество.
Примем $[\![P_j]\!] = \{W_k \mid W_k \Vdash P_j\}$, тогда $[\![\alpha]\!] = \{W_k \mid W_k \Vdash \alpha\}$.

Поскольку любая топологическая модель — корректная модель ИИВ, то и модель Крипке — корректная. ■

Определение 2.2.24. $\vDash \alpha$ если $W \vdash \alpha$.

Теорема 2.2.14. У ИИВ нет полной конечной табличной модели.

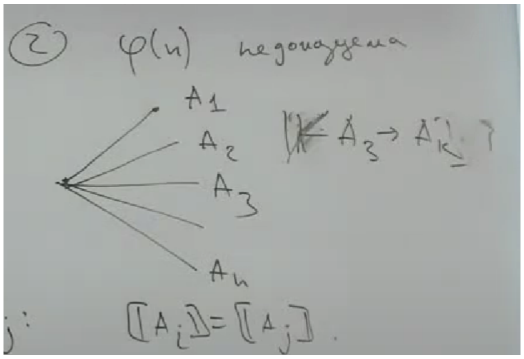
Доказательство. $\varphi(n) = \bigvee\limits_{i=1, j=1, i \neq j}^{n,n} A_i \to A_j$.

Пусть T — модель, $|\mathbb{V}| = n$.

Рассмотрим $\varphi(n+1)$. По принципу Дирихле. Есть A_j и A_i: $[\![A_j]\!] = [\![A_i]\!]$.

Несложно показать $[\![A_i \to A_j]\!] = \text{И} \implies [\![\varphi(n+1)]\!] = \text{И}$.

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



$[\![A_3 \to A_k]\!] = Л$. ∎

2.3 Изоморфизм Кари–Ховарда

Утверждение 2.3.1. τ, σ – типы.

$\tau \to \sigma$

```
f(x : τ): σ {
    return g(x);
}
```

$\tau \& \sigma$

```
f(x: τ, y: σ)
```

$\tau \vee \sigma$

```
f(x: std:variant<τ, σ>)
```

> **Определение 2.3.1** (Изоморфизм Кари–Ховарда)**.** Программа соответствует доказательству. Тип соответствует утверждению. ... (всё в интуиционистской логике)

Замечание. $f : \neg\neg\alpha \to \alpha$ – потом подумаем как это интерпретировать.

3 Исчисление предикатов

Нам нужен новый язык. В текущем языке всё хорошо, но он имеет малую выразитеьную 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. $\dfrac{\text{Каждый человек смертен} \quad \text{Сократ человк}}{\text{Сократ смертен}}$

$\dfrac{\text{Каждый объект, если он – человек, то он – смертен} \quad \text{Сократ – человк}}{\text{Сократ – смертен}}$

Цель: кванторы и предикаты.

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

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).

- Логическе выражения

    – Предикатные символы «равно» и «больше».

3.1 Язык исчисления предикатов

1. Два типа: предметные и логические выражения

2. Предметные выражения: метапеременная θ

    - Предметные переменные: a, b, c, ..., метапеременные x, y.
    - Функциональные выражения: $f(\theta_1, \ldots, \theta_n)$, метапеременные f, g, $\ldots$
    - Примеры: r, $q(p(x, s), r)$

3. Логические выражения: метапеременные α, β, γ, $\ldots$

    - Предикатные выражения: $P(\theta_1, \ldots, \theta_n)$, метапеременная P.
      Имена: A, B, C, $\ldots$,
    - Связки: $(\varphi \vee \psi)$, $(\varphi \to \psi)$, $(\varphi \to \psi)$, $(\neg\varphi)$
    - Кванторы: $(\forall x.\varphi)$ и $(\exists x.\varphi)$.

Сокращенные записи, метаязык

1. Метепаременные:

    - ψ, ϕ, π, ... — формулы
    - P, Q, ... — предикатные символы
    - θ, ... — термы
    - f, g, ... — функциональные символы
    - x, y, ... — предметные переменные

2. Скобки — как в И.В.; квантор — жадный:

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

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:

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

3.2 Два вида значений

1. Истинностные (логические) значения:
   (a) предикаты (в том числе пропозициональные переменные = нульместные предикаты);
   (b) логические связки и кванторы.
2. Предметные значения:
   (a) предметные переменные;
   (b) функциональные символы (в том числе константы = нульместные функциональные символы)

3.3 Оценка исчисления предикатов

Определение 3.3.1. 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:
$$F_{f_n} : D^n \to D$$
3. T — оценка для предикатных символов. Пусть P_n — n-местный предикатный символ:
$$T_{P_n} : D^n \to V \qquad V = \{\text{И}, \text{Л}\}$$
4. E — оценка для свободных предметных переменных.
$$E(x) \in D$$

Запись и сокращения записи подобны исчислению высказываний:
$$[\![\phi]\!] \in V, \quad [\![E(x, f(x)) \vee R]\!]^{x:=1, f(t):=t^2, R:=\text{И}} = \text{И}$$

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

Пример. $[\![\forall x.\exists y.\neg x + 1 = y]\!]$
Зададим оценку:

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

Фиксируем $x \in \mathbb{N}$. Тогда $[\![x + 1 = y]\!]^{y:=x} = \text{Л}$ поэтому при любом $x \in \mathbb{N}$:
$$[\![\exists y.\neg x + 1 = y]\!] = \text{И}.$$

Итого: $[\![\forall x.\exists y.\neg x + 1 = y]\!] = \text{И}$

Пример. Странная интерпретация $[\![\forall x.\exists y.\neg(x+1=y)]\!]$.

Зададим интерпретацию:

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

Тогда: $[\![x+1=y]\!]^{x\in D, y\in D} = \text{И}$.
Итого: $[\![\forall x.\exists y.\neg x+1=y]\!] = \text{Л}$.
Поэтому формулам оценки предикатов верить нельзя. Никакой интуиции за ними может и не стоять.

Определение 3.3.2. Формула общезначима, если истинна при любой оценке.

Утверждение 3.3.1. $[\![\forall x.Q(f(x)) \vee \neg Q(f(x))]\!] = \text{И}$.

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 $t = \text{И}$, то $[\![P(f(x))]\!]^{P(f(x)):=t} = \text{И}$, потому $[\![P(f(x)) \vee \neg P(f(x))]\!]^{P(f(x)):=t} = \text{И}$.
- Если $t = \text{Л}$, то $\neg P(f(x))]\!]^{P(f(x)):=t} = \text{И}$ потому всё равно $[\![P(f(x)) \vee \neg P(f(x))]\!]^{P(f(x)):=t} = \text{И}$.

■

3.4 Подстановки, свобода и связность

Определение 3.4.1. Рассмотрим формулу $\forall x.\psi$ (или $\exists x.\psi$). Здесь переменная x связзана в ψ. Все вхождения переменой x в ψ – **связанные**.

Определение 3.4.2. Переменная x входит свободно в ψ, если не находится в области действия никакого квантора по x. Все её вхождения в ψ — **свободные**.

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

Единственное свободное вхождение прееменной x помеченно синим цветом.

Определение 3.4.3. Подстановка — это ...

$$\psi[x := \theta] := \begin{cases} \psi, & \psi \equiv y, y \not\equiv x \\ \psi, & \psi \equiv \forall x.\pi \text{ или } \psi \equiv \exists x.\pi \\ \pi[x := \theta] \star \rho[x := \theta], & \psi \equiv \pi \star \rho \\ \theta, & \psi \equiv x \\ \forall y.\pi[x := \theta], & \psi \equiv \forall y.\pi \text{ и } y \not\equiv x \\ \exists y.\pi[x := \theta], & \psi \equiv \exists y.\pi \text{ и } y \not\equiv x \end{cases}$$

Определение 3.4.4. Терм θ свободен для подстановки вместо x в ψ ($\psi[x := \Theta]$), если ни одно свободное вхождение переменной в Θ 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 $(\forall y.\forall x.P(t))[t := y]$.

3.5 Теория доказательств

Рассмотрим язык исчисления предикатов. Аксиомы — все схемы аксиом для классического исчисления высказываний в данном языке.

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

Добавим ещё две схемы аксиом (здесь везде θ свободен для подстановки вместо x в φ):

11. $(\forall x.\varphi) \to \varphi[x := \theta]$
12. $\varphi[x := \theta] \to \exists x.\varphi$

Добавим ещё два правила вывода (до этого был только Modus Ponens):

1. Введение $\forall$: $\dfrac{\varphi \to \psi}{\varphi \to \forall x.\psi}$,
2. Введение $\exists$: $\dfrac{\psi \to \varphi}{(\exists x.\psi) \to \varphi}$.

В обоих правилах x не входит свободно в φ.

Пример. $\dfrac{x = 5 \to x^2 = 25}{x = 5 \to \forall x.x^2 = 25}$. Между x и x^2 была связь, которую мы нарушили ограничение.

Утверждение 3.5.1. Доказыуемость, выводимость, полнота, корректность — аналогично исчислению высказываний.

3.6 Теорема о дедукции для исчисления предикатов

Теорема 3.6.1. Если $\Gamma \vdash \alpha \to \beta$, то $\Gamma, \alpha \vdash \beta$. Если $\Gamma, \alpha \vdash \beta$ и в доказательстве не применяются правила для кванторов по свободным переменным из α, то $\Gamma \vdash \alpha \to \beta$

Доказательство.

$\Longrightarrow$ также как в К.И.В

$\Longleftarrow$ 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 $\alpha \to \delta_1, \alpha \to \delta_2, \dots, \alpha \to \delta_n$.

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

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

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

$(n-0.9)-(n-0.8)$	$(\alpha \to \psi \to \varphi) \to (\alpha \& \psi) \to \varphi$	Т. о полноте КИВ (формула общезначима)
$(n-0.6)$	$(\alpha \& \psi) \to \varphi$	М.Р. k,$n-0.8$
$(n-0.4)$	$(\alpha \& \psi) \to \forall x.\varphi$	Правило для $\forall$, $n-0.6$
$(n-0.3)-(n-0.2)$	$((\alpha \& \psi) \to \forall x.\varphi) \to$ $(\alpha \to \psi \to \forall x.\varphi)$	Т. о полноте КИВ $(((\alpha \& \psi) \to \beta) \to (\alpha \to \psi \to \beta))$
(n)	$\alpha \to \psi \to \forall x.\varphi$	М.Р. $n-0.4$, $n-0.2$

■

3.7 Отношение следования

Определение 3.7.1 (Следование)**.** $\gamma_1, \gamma_2, \dots, \gamma_n \models \alpha$, если выполнено два условия:

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

Теорема 3.7.1 (Корректность исчисления предикатов)**.** Если $\Gamma \vdash \alpha$ и в доказательстве не используется кванторов по свободным переменным из Γ, то $\Gamma \models \alpha$.

Следующий пример обращает внимание на важность второго условия.

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

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

(1)	$P(x)$	Гипотеза
(2)	$P(x) \to (A \to A \to A) \to P(x)$	Сх. акс. 1
(3)	$(A \to A \to A) \to P(x)$	M.P. 1, 2
(4)	$(A \to A \to A) \to \forall x.P(x)$	Правило для $\forall$, 3
(5)	$(A \to A \to A)$	Сх. акс. 1
(6)	$\forall x.P(x)$	M.P. 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.

3.8 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 $[\![\varphi]\!]_{\mathcal{M}_1} = [\![\varphi]\!]_{\mathcal{M}_2}$ при всех φ.
3. Поступим так:
   (a) построим эталонное множество моделей $\mathfrak{M}$, каждая модель соответствует списку истинных формул, *но им не является*;
   (b) докажем полноту $\mathfrak{M}$: если каждая $\mathcal{M} \in \mathfrak{M}$ предполагает $\mathcal{M} \models \varphi$, то $\vdash \varphi$;
   (c) 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.

3.8.1 Непротиворечивое множество формул

Определение 3.8.1. У множества есть модель, если любая его формула истинна в данной модели.

Определение 3.8.2. Γ — *непротиворечивое множество формул*, если $\Gamma \not\vdash \alpha \& \neg\alpha$ для любого α.

Пример. Непротиворечиво:

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

Противоречиво:

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

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 3.8.3. Γ — **полное** непротиворечивое множество замкнутых **бескванторных** формул, если:

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

Замечание. Замкнутая формула — формула, не содержащая свободных переменных вовсе или имеющая только такие их вхождения, которые нельзя связывать кванторами, не выходя за рамки данного исчисления.

Определение 3.8.4. Γ — **полное** непротиворечивое множество замкнутых формул, если:

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

Теорема 3.8.1 (Пополнение непротиворечивого множества формул)**.** Пусть Γ — непротиворечивое множество замкнутых (бескванторных) формул. Тогда, какова бы ни была замкнутая (бескванторная) формула φ, хотя бы $\Gamma \cup \{\varphi\}$ или $\Gamma \cup \{\neg\varphi\}$ — непротиворечиво.

Доказательство. Пусть это не так и найдутся такие Γ, φ и α, 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 Γ не является непротиворечивым. Противоречие. ■

Теорема 3.8.2 (Дополнение непротиворечивого множества формул до полного)**.** Пусть Γ — непротиворечивое множество замкнутых (бескванторных) формул. Тогда найдётся полное непротиворечивое множество замкнутых (бескванторных) формул Δ, что $\Gamma \subseteq \Delta$.

Доказательство.

1. Занумеруем все формулы (их счётное количество): $\varphi_1, \varphi_2, \dots$.
2. Построим семейство множеств $\{\Gamma_i\}$:
$$\Gamma_0 = \Gamma \qquad \Gamma_{i+1} = \begin{cases} \Gamma_i \cup \{\varphi_i\}, & \text{если } \Gamma_i \cup \{\varphi_i\} \text{ непротиворечиво} \\ \Gamma_i \cup \{\neg\varphi_i\}, & \text{иначе} \end{cases}$$
3. Итоговое множество
$$\Delta = \bigcup_i \Gamma_i$$
4. Непротиворечивость Δ не следует из индукции — индукция гарантирует непротиворечивость только Γ_i при натуральном (т.е. *конечном*) i, потому...

Δ непротиворечиво:

1. Пусть Δ 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
$$\Gamma_{d_1} \cup \Gamma_{d_2} \cup \dots \cup \Gamma_{d_n} \not\vdash \alpha \& \neg\alpha.$$

■

3.8.2 Модель для множества формул

Определение 3.8.5 (Модель для множества формул)**.** Моделью для множества формул F назовём такую модель $\mathcal{M}$, что при всяком $\varphi \in F$ выполнено $[\![\varphi]\!]_{\mathcal{M}} = И$.

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

Теорема 3.8.3 (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 $\vdash \delta_1 \to \delta_2 \to \dots \to \delta_n \to A \& \neg A$, то есть $[\![\delta_1 \to \delta_2 \to \dots \to \delta_n \to A \& \neg A]\!] = И$ (корректность).
Поскольку все $[\![\delta_i]\!]_{\mathcal{M}} = И$, то и $[\![A \& \neg A]\!]_{\mathcal{M}} = И$ (анализ таблицы истинности импликации).
Однако, $[\![A \& \neg A]\!] = Л$. Противоречие. ■

Теорема 3.8.4. Любое непротиворечивое множество замкнутых бескванторных формул имеет модель.

Как строить такую модель?

Определение 3.8.6. 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. $[\![f(\theta_1, \dots, \theta_n)]\!] =$ “f(” $+\!\!+\ [\![\theta_1]\!]\ +\!\!+$ “,” $+\!\!+ \dots +\!\!+$ “,” $+\!\!+\ [\![\theta_n]\!]\ +\!\!+$ “)”

3. $[\![P(\theta_1, \dots, \theta_n)]\!] = \begin{cases} \text{И}, & \text{если “P(”} +\!\!+ [\![\theta_1]\!] +\!\!+ \text{“,”} +\!\!+ \dots +\!\!+ \text{“,”} +\!\!+ [\![\theta_n]\!] +\!\!+ \text{“)”} \in M \\ \text{Л}, & \text{иначе} \end{cases}$

4. $[\![x]\!] =$ “ошибка!”, так как формулы замкнуты.

Лемма 3.8.4.1. Пусть φ — бескванторная формула, тогда $\mathcal{M} \models \varphi$ тогда и только тогда, когда $\varphi \in M$.

Доказательство. Индукция по длине формулы φ.

1. База. φ — 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:

   (a) если $\mathcal{M} \models \alpha \star \beta$, то $\alpha \star \beta \in M$.

   (b) если $\mathcal{M} \not\models \alpha \star \beta$, то $\alpha \star \beta \notin M$.

Пример доказательсвта для импликации.

Если $\varphi = \alpha \to \beta$ и для любой формулы ζ, более короткой, чем φ, выполнено $\mathcal{M} \models \zeta$ тогда и только тогда, когда $\zeta \in M$, тогда:

1. если $\mathcal{M} \models \alpha \to \beta$, то $\alpha \to \beta \in M$;

2. если $\mathcal{M} \not\models \alpha \to \beta$, то $\alpha \to \beta \notin M$.

Доказательство (разбором случаев).

1. $\mathcal{M} \models \alpha \to \beta$: $[\![\alpha]\!] =$ Л. Тогда по предположению $\alpha \notin M$, потому по полноте $\neg\alpha \in M$. И, поскольку в ИВ $\neg\alpha \vdash \alpha \to \beta$, то $M \vdash \alpha \to \beta$. Значит, $\alpha \to \beta \in M$, иначе по полноте $\neg(\alpha \to \beta) \in M$, что делает M противоречивым.

2. $\mathcal{M} \models \alpha \to \beta$: $[\![\alpha]\!] =$ И и $[\![\beta]\!] =$ И. Рассуждая аналогично, используя $\alpha, \beta \vdash \alpha \to \beta$, приходим к $\alpha \to \beta \in M$.

3. $\mathcal{M} \not\models \alpha \to \beta$. Тогда $[\![\alpha]\!] =$ И, $[\![\beta]\!] =$ Л, то есть $\alpha \in M$ и $\neg\beta \in M$. Также, $\alpha, \neg\beta \vdash \neg(\alpha \to \beta)$, отсюда $M \vdash \neg(\alpha \to \beta)$. Предположим, что $\alpha \to \beta \in M$, то $M \vdash \alpha \to \beta$ — отсюда $\alpha \to \beta \notin M$.

■

Теорема 3.8.4. Любое непротиворечивое множество замкнутых бескванторных формул имеет модель.

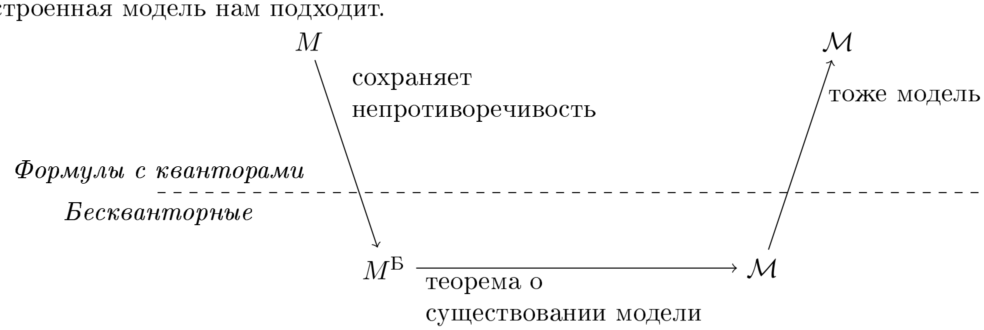
Доказательство теоремы о существовании модели. Пусть M — непротиворечивое множество замкнутых бескванторных формул.

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

Схема доказательства. Мы умеем стооить 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 3.8.7. Формула φ имеет поверхностные кванторы (находится в предварённой форме), если соответствует грамматике

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

где τ — формула без кванторов

Теорема 3.8.6. Для любой замкнутой формулы ψ найдётся такая формула φ с поверхностными кванторами, что $\vdash \psi \to \varphi$ и $\vdash \varphi \to \psi$.

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

3.8.3 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. φ_i — формула без кванторов, пропустим
    2. $\varphi_i = \forall x.\psi$ — добавим к S все формулы вида $\psi[x := \theta]$, где θ — 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 3.8.6.1. 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: $M_k, M_{k+1} \backslash M_k \vdash A \& \neg A$
- Тогда (т.к. доказательство конечной длины): $M_k, \gamma_1, \gamma_2, \dots, \gamma_n \vdash A \& \neg A$ где $\gamma_i \in M_{k+1} \backslash M_k$.
- По теореме о дедукции: $M_k \vdash \gamma_1 \to \gamma_2 \to \dots \to \gamma_n \to A \& \neg A$
- Научимся выкидывать первую посылку: $M_k \vdash \gamma_2 \to \dots \to \gamma_n \to A \& \neg A$
- И по индукции придём к противоречию: $M_k \vdash A \& \neg A$.

■

Лемма 3.8.6.2. (Устранение посылки) Если $M_k \vdash \gamma \to W$, и $\gamma \in M_{k+1} \backslash M_k$, то $M_k \vdash W$.

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

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

  Допишем в конец доказательства:

$\forall x.\varphi$	(гипотеза)
$(\forall x.\varphi) \to (\varphi[x := \theta])$	(сх. акс. 11)
γ	(M.P.)
W	(M.P.)

- Случай квантора существования.

  - $\gamma = \varphi[x := d_i^{k+1}]$
  - Перестроим доказательство $M_k \vdash \gamma \to W$: 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 $M_k \vdash \gamma[d_i^{k+1} := y] \to W$ и дополним его:

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

■

3.8.4 Построение M Б

Определение 3.8.8. $M^* = \bigcup_k M_k$

Теорема 3.8.7. M^* непротиворечиво.

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

Определение 3.8.9. $M^{\text{Б}}$ — множество всех бескванторных формул из M^*.

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

3.8.5 Постоение модели для M*

Определение 3.8.10. $\mathcal{M}$ есть модель для M^*.

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

- База: φ без кванторов. Тогда $\varphi \in M^{\text{Б}}$, отсюда $\mathcal{M} \models \varphi$ 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 $[\![\psi]\!]^{x := [\![d_i^{k+1}]\!]} = \text{И}$
  - Отсюда $\mathcal{M} \models \exists x.\psi$.

■

Теорема 3.8.8 (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 $M^{Б}$ ($M^{Б} \subseteq M^*$, 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 3.8.8.1 (из теоремы Гёделя о полноте)**.** Исчисление предикатов полно.

Доказательство.
- Пусть это не так, и существует формула φ, что $\models \varphi$, но $\nvdash \varphi$.
- 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, $[\![\neg\varphi]\!] = \textit{И}$, поэтому $[\![\varphi]\!] = \textit{Л}$, поэтому $\not\models \varphi$. Противоречие.

■

Теорема 3.8.9. 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 $\vdash \delta_1 \to \delta_2 \to \dots \to \delta_n \to A\&\neg A$, то есть $[\![\delta_1 \to \delta_2 \to \dots \to \delta_n \to A\&\neg A]\!] = \textit{И}$ (корректность). Поскольку все $[\![\delta_i]\!]_{\mathcal{M}} = \textit{И}$, то и $[\![A\&\neg A]\!]_{\mathcal{M}} = \textit{И}$ (анализ таблицы истинности импликации). Однако, $[\![A\&\neg A]\!] = \textit{Л}$. Противоречие. ■

Следствие 3.8.9.1. Исчисление предикатов непротиворечиво

3.9 Машина Тьюринга

Определение 3.9.1. 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 3.9.2. Состояние машины Тьюринга — упорядоченная тройка:

1. Бесконечная лента с символом-заполнителем q_ε, 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:

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

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.

3.9.1 Разрешимость языка Машины Тьюринга

Определение 3.9.3. Язык — множество строк.

Определение 3.9.4. Язык L разрешим, если существует машина Тьюринга, которая для любого слова w возвращает ответ «да», если $w \in L$, и «нет», если $w \notin L$.

3.9.2 Неразрешимость задачи останова

Определение 3.9.5. Рассмотрим все возможные описания машин Тьюринга. Составим упорядоченные пары: описание машины Тьюринга и входная строка. Из них выделим язык останавливающихся на данном входе машин Тьюринга.

Теорема 3.9.1. Язык всех останавливающихся машин Тьюринга неразрешим

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

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

Что вернёт $S(code(W), code(W))$? ∎

Как закодировать состояние машины?

1. внешний алфавит: n 0-местных функциональных символов $q_1, \ldots, q_n$; q_ε — символ-заполнитель.
2. список: ε 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 $s_1, \ldots, s_k$. 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: $\langle k, s\rangle \Rightarrow \langle k', s', \leftarrow\rangle$.

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

4. и т.п.

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

Теорема 3.9.2. 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. ■

3.9.3 Неразрешимость исчисления предикатов: доказательство

Теорема 3.9.3. 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. ■

4 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 $x \leqslant a$, то $x \in A$
   (c) Если $b \in B$, $x \in \mathbb{Q}$ и $b \leqslant x$, 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

   $$\mathbb{Z} : \cdots - 3, -2, -1, 0, 1, 2, 3, \ldots.$$

   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?

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

4.1 Акиоматика Пеано

Определим натуральные числа так:

Определение 4.1.1. N (или, более точно, $\langle N, 0, (')\rangle$) *соответствует* аксиоматике Пеано, если следующее определено/выполнено:

1. Операция «штрих» $(') : N \to N$, 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») $P : N \to V$, 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 $\nu ::= \mathtt{0} \mid \nu$«`'`»
2. 0 — это «`0`», x' — это x ++ «`'`»

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 4.1.1. 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 4.1.2. $1 = 0'$, $2 = 0''$, $3 = 0'''$, $4 = 0''''$, $5 = 0'''''$, $6 = 0''''''$, $7 = 0'''''''$, $8 = 0''''''''$, $9 = 0'''''''''$

Определение 4.1.3.
$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a+c)', & \text{если } b = c' \end{cases}$$

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

Определение 4.1.4.
$$a \cdot b = \begin{cases} 0, & \text{если } b = 0 \\ a \cdot c + a, & \text{если } b = c' \end{cases}$$

Пример: коммутативность сложения (лемма 1)

Лемма 4.1.1.1 (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 $x' + 0 = \dots$

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

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

Лемма 4.1.1.2 (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 4.1.2. $a + b = b + a$

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

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

■

4.1.1 Уточнение исчисления предикатов

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

Определение 4.1.5. 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 $S = \{t \mid \psi[x := t]\}$	И.П.
второй	по предикатным переменным	о множествах множеств $S = \{\{t \mid P(t)\} \mid \varphi[p := P]\}$	
	...		

4.1.2 Формальная арифметика

Определение 4.1.6. Формальная арифметика — теория первого порядка, со следующими добавленными нелогическими ...

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

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

Утверждение 4.1.1. $a = a$ в формальной арифметике.

Доказательство. Пусть $\top ::= 0 = 0 \to 0 = 0 \to 0 = 0$, тогда:

(1)	$a = b \to a = c \to b = c$	(Акс. A1)
(2)	$(a = b \to a = c \to b = c) \to \top \to (a = b \to a = c \to b = c)$	(Сх. акс. 1)
(3)	$\top \to (a = b \to a = c \to b = c)$	(М.Р. 1, 2)
(4)	$\top \to (\forall c.a = b \to a = c \to b = c)$	(Введ. $\forall$)
(5)	$\top \to (\forall b.\forall c.a = b \to a = c \to b = c)$	(Введ. $\forall$)
(6)	$\top \to (\forall a.\forall b.\forall c.a = b \to a = c \to b = c)$	(Введ. $\forall$)
(7)	$\top$	(Сх. акс 1)
(8)	$(\forall a.\forall b.\forall c.a = b \to a = c \to b = c)$	(М.Р. 7, 6)
(9)	$(\forall a.\forall b.\forall c.a = b \to a = c \to b = c) \to$ $\to (\forall b.\forall c.a + 0 = b \to a + 0 = c \to b = c)$	(Сх. акс. 11)
(10)	$\forall b.\forall c.a + 0 = b \to a + 0 = c \to b = c$	(М.Р. 8, 9)
(11)	$(\forall b.\forall c.a + 0 = b \to a + 0 = c \to b = c) \to$ $\to (\forall c.a + 0 = a \to a + 0 = c \to a = c)$	(Сх. акс. 11)
(12)	$\forall c.a + 0 = a \to a + 0 = c \to a = c$	(М.Р. 10, 11)
(13)	$(\forall c.a + 0 = a \to a + 0 = c \to a = c) \to$ $\to (a + 0 = a \to a + 0 = a \to a = a)$	(Сх. акс. 11)
(14)	$a + 0 = a \to a + 0 = a \to a = a$	(М.Р. 12, 13)
(15)	$a + 0 = a$	(Акс. A5)
(16)	$a + 0 = a \to a = a$	(М.Р. 15, 14)
(17)	$a = a$	(М.Р. 15, 16)

■

4.2 Арифметизация логики

Общие замечания

- Рассматриваем функции $\mathbb{N}_0^n \to \mathbb{N}_0$.
- Обозначим вектор $\langle x_1, x_2, \ldots, x_n \rangle$ как $\overrightarrow{x}$.

4.2.1 Примитивно-рекурсивные функции

Определение 4.2.1. Примитив «Ноль» (Z)

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

Определение 4.2.2. Примитив «Инкремент» (N)

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

Определение 4.2.3. Примитив «Проекция» (U) — семейство функций; пусть $k, n \in \mathbb{N}_0, k \leqslant n$

$$U_n^k : \mathbb{N}_0^n \to \mathbb{N}_0, \qquad U_n^k(\overrightarrow{x}) = x_k.$$

Определение 4.2.4. Примитив «Подстановка» (S) — семейство функций;
пусть $g : \mathbb{N}_0^k \to \mathbb{N}_0, \quad f_1, \ldots, f_k : \mathbb{N}_0^n \to \mathbb{N}_0$

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

Определение 4.2.5 (примитив «примитивная рекурсия», R)**.** Пусть $f : \mathbb{N}_0^n \to \mathbb{N}_0$ и $g : \mathbb{N}_0^{n+2} \to \mathbb{N}_0$. Тогда $R\langle f, g\rangle : \mathbb{N}_0^{n+1} \to \mathbb{N}_0$, причём

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

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

Пример.

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

4.2.2 Примитивно-рекурсивные функции

Определение 4.2.6. Функция f — примитивно-рекурсивна, если может быть выражена как композиция примитивов Z, N, U, S и R.

Теорема 4.2.1. $f(x) = x + 2$ 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 4.2.1.1. $f(a,b) = a + b$ 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. $R\langle U_1^1, S\langle N, U_3^3\rangle\rangle(x, y+1) =$
  $... = S\langle N, U_3^3\rangle(x, y, R\langle U_1^1(x), S\langle N, U_3^3\rangle\rangle(x,y)) =$
  $... = S\langle N, U_3^3\rangle(x, y, x+y) =$
  $... = N(x+y) = x + y + 1$

■

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; i_1 < g1(x1...xn); i1++) {
        for (int i2 = 0; i_2 < g2(x1...xn,i1); i2++) {
            ...
               for (int ik = 0; ik < gk(x1...xn,i1,i2...); ik++) {
                   // выражение без циклов
               }
            ...
        }
    }
```

4.2.3 Общерекурсивные функции

Определение 4.2.7. 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 4.2.8. 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 4.2.2. Функция Аккермана — общерекурсивная, но не примитивно-рекурсивная.

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

Определение 4.2.9. Тезис Чёрча для общерекурсивных функций: любая эффективно–вычислимая функция $\mathbb{N}_0^k \to \mathbb{N}_0$ является общерекурсивной.

Замечание. Эффективно–вычислимая функция — такая функция, для вычисления которой можно написать программу, например на машине Тьюринга, но можно и в конце–концов на `C`.

Определение 4.2.10. Запись вида $\psi(\theta_1, \dots, \theta_n)$ означает $\psi[x_1 := \theta_1, \dots, x_n := \theta_n]$

Определение 4.2.11 (Литерал числа)**.**

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

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

Определение 4.2.12 (Выразимость отношений в Ф.А.)**.** Будем говорить, что отношение $R \subseteq \mathbb{N}_0^n$ выразимо в ФА, если существует формула ρ, что:

1. если $\langle a_1, \ldots, a_n\rangle \in R$, то $\vdash \rho(\overline{a_1}, \ldots, \overline{a_n})$
2. если $\langle a_1, \ldots, a_n\rangle \notin R$, то $\vdash \neg\rho(\overline{a_1}, \ldots, \overline{a_n})$

Теорема 4.2.3. 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 $p := \overline{k}$ при всех $k \in \mathbb{N}_0$: $\vdash 0 = 0$, $\vdash 0' = 0'$, $\vdash 0'' = 0''$, ...
- $\vdash \neg p = q$ при $p := \overline{k}$, $q := \overline{s}$ 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 4.2.13 (Представимость функций в Ф.А.)**.** Будем говорить, что функция $f : \mathbb{N}_0^n \to \mathbb{N}_0$ представима в ФА, если существует формула φ, что:

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

4.2.4 Соответствие рекурсивных и представимых функций

Теорема 4.2.4. Любая рекурсивная функция представима в Ф.А.

Доказательство проведем в несколько этапов.

Теорема 4.2.5. Примитивы Z, N и U_n^k представимы в Ф.А.

Доказательство.

- $\zeta(x_1, x_2) := x_2 = 0$, формальнее: $\zeta(x_1, x_2) := x_1 = x_1\&x_2 = 0$
- $\nu(x_1, x_2) := x_2 = x_1'$
- $\upsilon(x_1, \ldots, x_n, x_{n+1}) := x_k = x_{n+1}$
  формальнее: $\upsilon(x_1, \ldots, x_n, x_{n+1}) := (\underset{i \neq k, n+1}{\&} x_i = x_i)\&x_k = x_{n+1}$

■

Примитив S представим в Ф.А.

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

Теорема 4.2.6. Пусть функции $f, g_1, \ldots, g_k$ представимы в Ф.А. Тогда $S\langle f, g_1, \ldots, g_k\rangle$ представима в Ф.А.

Доказательство. Пусть f, g_1, ..., g_k представляются формулами φ, γ_1, ..., γ_k.

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

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

■

β-функция Гёделя Мы хотим закодировать последовательность натуральных чисел произвольной длины.

Определение 4.2.14. β-функция Гёделя: $\beta(b, c, i) := b\%(1 + (i + 1) \cdot c)$
Здесь (%) — остаток от деления.

Теорема 4.2.7. β-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 $0 \leqslant d < x$.

Теорема 4.2.8. Если $a_0, \ldots, a_n \in \mathbb{N}_0$, то найдутся такие $b, c \in \mathbb{N}_0$, что $a_i = \beta(b, c, i)$.

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

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

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

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

Теорема 4.2.9. Пусть $f : \mathbb{N}_0^n \to \mathbb{N}_0$ и $g : \mathbb{N}_0^{n+2} \to \mathbb{N}_0$ представлены формулами φ и γ.

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

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

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

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

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

Теорема 4.2.10. Пусть функция $f:\mathbb{N}_0^{n+1}\to\mathbb{N}_0$ представима в Ф.А. формулой $\varphi(x_1,\ldots,x_n,y,r)$.
Тогда примитив $M\langle f\rangle$ представим в Ф.А. формулой

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

Теорема 4.2.11. Если f — рекурсивная функция, то она представима в Ф.А.

Доказательство. Индукция по структуре f. ■

4.2.5 Рекурсивность представимых в Ф.А. функций

Теорема 4.2.12. Любая представимая в Ф.А. функция рекурсивна.

Фиксируем f и $x_1,x_2,\ldots,x_n$. Обозначим $y=f(x_1,x_2,\ldots,x_n)$. По представимости нам известна φ, что $\vdash\varphi(\overline{x_1},\overline{x_2},\ldots,\overline{x_n},\overline{y})$. 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 $\vdash\varphi(\overline{x_1},\overline{x_2},\ldots,\overline{x_n},\overline{y})$.

Гёделева нумерация

Введем функцию, которая по формуле возвращает ее гёделев номер: $\ulcorner\varphi\urcorner$.

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	$\vdash$	$(\cdot)$	$1,2$	$27+6\cdot 2\cdot 9$
11	$\neg$	$25+6\cdot k$	x_k	$(=)$	$0,2$	$29+6\cdot 9$
13	$\to$	$27+6\cdot 2^k\cdot 3^n$	f_k^n			
15	$\vee$	$29+6\cdot 2^k\cdot 3^n$	P_k^n			

2. Формула. $\phi\equiv s_0s_1\ldots s_{n-1}$. Гёделев номер: $\ulcorner\phi\urcorner=2^{\ulcorner s_0\urcorner}\cdot 3^{\ulcorner s_1\urcorner}\cdot\ldots\cdot p_{n-1}^{\ulcorner s_{n-1}\urcorner}$.
3. Доказательство. $\Pi=\delta_0\delta_1\ldots\delta_{k-1}$, его гёделев номер: $\ulcorner\Pi\urcorner=2^{\ulcorner\delta_0\urcorner}\cdot 3^{\ulcorner\delta_1\urcorner}\cdot\ldots\cdot p_{k-1}^{\ulcorner\delta_{k-1}\urcorner}$

Теорема 4.2.13. Следующая функция рекурсивна:

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

Идея доказательства. 1. Проверка доказательства вычислима.

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

∎

Лемма 4.2.13.1. Следующие функции рекурсивны:

1. Функции $\mathrm{plog}_k(n) = \max\{p : n \vdots k^p\}$, $\mathrm{fst}(x) = \mathrm{plog}_2(x)$ и $\mathrm{snd}(x) = \mathrm{plog}_3(x)$.
2. Числовые литералы: $\overline{k} : \mathbb{N}_0 \to \mathbb{N}_0$, $\overline{k}(x) = k$.

Теорема 4.2.14. Если $f : \mathbb{N}_0^n \to \mathbb{N}_0$, и f представима в Ф.А. формулой φ, то f — рекурсивна.

Доказательство. Пусть заданы $x_1, x_2, \dots, x_n$. Ищем $\langle y, p\rangle$, что $\mathrm{proof}(\ulcorner\varphi\urcorner, x_1, x_2, \dots, x_n, y, p) = 1$, напомним: $y = f(x_1, x_2, \dots, x_n)$, $p = \ulcorner\Pi\urcorner$, Π — доказательство $\varphi(\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}, \overline{y})$.

$$f = S\langle \mathrm{fst}, M\langle S\langle \mathrm{proof}, \overline{\ulcorner\varphi\urcorner}, U^1_{n+1}, U^2_{n+1}, \dots, U^n_{n+1}, S\langle \mathrm{fst}, U^{n+1}_{n+1}\rangle, S\langle \mathrm{snd}, U^{n+1}_{n+1}\rangle\rangle\rangle\rangle$$

∎

4.3 Первая теорема Гёделя о неполноте арифметики

Парадокс лжеца

Предложение, указанное в центре данного слайда — ложное.

Проблема останова

Теорема 4.3.1. 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 4.3.1. Определим функцию W_1: $W_1(x, p) = 1$, если $x = \ulcorner\xi\urcorner$, где ξ — формула с единственной свободной переменной x_1, а p — доказательство самоприменения ξ:

$$\vdash \xi(\overline{\ulcorner\xi\urcorner})$$

$W_1(x, p) = 0$, если это не так.

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

Теорема 4.3.2. Существует формула ω_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 φ;
2. $\vdash \neg\omega_1(\overline{\ulcorner\varphi\urcorner}, \overline{p})$ иначе.

Доказательство. Опираясь на рекурсивность функции proof, легко показать рекусривность W_1. Значит, эта функция представима в формальной арифметике некоторой формулой τ_1. Возьмём $\omega_1(x_1, x_2) := \tau_1(x_1, x_2, \overline{1})$. ■

Определение 4.3.2. Определим формулу $\sigma(x) := \forall p.\neg\omega(x, p)$.
Это означает, что самоприменение x не доказуемо.

Определение 4.3.3. Если для любой формулы $\phi(x)$ из $\vdash \phi(0)$, $\vdash \phi(\overline{1})$, $\vdash \phi(\overline{2})$, ... выполнено $\nvdash \exists x.\neg\phi(x)$, то теория *омега-непротиворечива.*

Теорема 4.3.3. Омега-непротиворечивость влечёт непротиворечивость

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

4.4 Теоремы Гёделя о неполноте арифметики

Теорема 4.4.1. Первая теорема Гёделя о неполноте арифметики
Если формальная арифметика непротиворечива, то $\nvdash \sigma(\overline{\ulcorner\sigma\urcorner})$.

- Если формальная арифметика ω-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 ξ.

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 $\vdash \neg\omega_1(\overline{\ulcorner\sigma\urcorner}, \overline{0})$, $\vdash \neg\omega_1(\overline{\ulcorner\sigma\urcorner}, \overline{1})$, ...
  - По ω-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 4.4.2. 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 $\sigma(\overline{\ulcorner\sigma\urcorner}) \equiv \forall p.\neg\omega_1(\overline{\ulcorner\sigma\urcorner}), p$: нет числа p, что p — номер доказательства $\sigma(\overline{\ulcorner\sigma\urcorner})$.
То есть, $[\![\forall p.\neg\omega_1(\overline{\ulcorner\sigma\urcorner}), p)]\!] = $ И. То есть, $\models \sigma(\overline{\ulcorner\sigma\urcorner})$. ■

Почему мы должны требовать от нашей теории w–непротиворечивости? Неужели наша формальная ариметика 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 4.4.1. $\theta_1 \leqslant \theta_2 \equiv \exists p.p + \theta_1 = \theta_2 \qquad \theta_1 < \theta_2 \equiv \theta_1 \leqslant \theta_2 \& \neg \theta_1 = \theta_2$.

Определение 4.4.2. Пусть $\langle \ulcorner\xi\urcorner, p\rangle \in W_2$, если $\vdash \neg\xi(\overline{\ulcorner\xi\urcorner})$. Пусть ω_2 выражает W_2 в формальной арифметике.

Теорема 4.4.3. Рассмотрим $\rho(x_1) = \forall p.\omega_1(x_1, p) \rightarrow \exists q.q \leqslant p \& \omega_2(x_1, q)$.
Тогда $\nvdash \rho(\overline{\ulcorner\rho\urcorner})$ и $\nvdash \neg\rho(\overline{\ulcorner\rho\urcorner})$.

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."

Утрмерждение 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 4.4.3. 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 ξ.
Обозначим $\pi(x) \equiv \exists p.\psi(x, p)$.

Определение 4.4.4. Формулой Consis назовём формулу $\neg\pi(\overline{\ulcorner 1 = 0\urcorner})$.

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

Теорема 4.4.4 (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 $\sigma(\overline{\ulcorner\sigma\urcorner})$, — и это можно доказать, то есть $\vdash$ Consis $\to \sigma(\overline{\ulcorner\sigma\urcorner})$.

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

Определение 4.4.5. Будем говорить, что формула ψ, выражающая отношение Proof, формула π и формула Consis соответствуют условиям Гильберта-Бернайса-Лёфа, если следующие условия выполнены для любой формулы α:

1. $\vdash \alpha$ влечет $\vdash \pi(\overline{\ulcorner\alpha\urcorner})$
2. $\vdash \pi(\overline{\ulcorner\alpha\urcorner}) \to \pi(\overline{\ulcorner\pi(\overline{\ulcorner\alpha\urcorner})\urcorner})$
3. $\vdash \pi(\overline{\ulcorner\alpha \to \beta\urcorner}) \to \pi(\overline{\ulcorner\alpha\urcorner}) \to \pi(\overline{\ulcorner\beta\urcorner})$

Лемма 4.4.4.1. Лемма об автоссылках. Для любой формулы $\phi(x_1)$ можно построить такую замкнутую формулу α (не использующую неаксиоматических предикатных и функциональных символов), что $\vdash \phi(\overline{\ulcorner\alpha\urcorner}) \leftrightarrow \alpha$.

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

Теорема 4.4.5. Существует такая замкнутая формула γ, что если Ф.А. непротиворечива, то $\nvdash \gamma$, а если Ф.А. ω-непротиворечива, то и $\nvdash \neg\gamma$.

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

- Предположим, что $\vdash \gamma$. Тогда $\vdash \gamma \to \neg\pi(\overline{\ulcorner\gamma\urcorner})$, то есть $\nvdash \gamma$
- Предположим, что $\vdash \neg\gamma$. Тогда $\vdash \pi(\overline{\ulcorner\gamma\urcorner})$, то есть $\vdash \exists p.\psi(\overline{\ulcorner\gamma\urcorner}, p)$. Тогда по ω-непротиворечивости найдётся p, что $\vdash \psi(\overline{\ulcorner\gamma\urcorner}, \overline{p})$, то есть $\vdash \gamma$.

■

Доказательство второй теоремы Гёделя.

1. Пусть γ таково, что $\vdash \gamma \leftrightarrow \neg\pi(\overline{\ulcorner\gamma\urcorner})$.
2. Покажем $\pi(\overline{\ulcorner\gamma\urcorner}) \vdash \pi(\overline{\ulcorner 1 = 0\urcorner})$.
   (a) По условию 2, $\vdash \pi(\overline{\ulcorner\gamma\urcorner}) \to \pi(\overline{\ulcorner\pi(\overline{\ulcorner\gamma\urcorner})\urcorner})$. По теореме о дедукции $\pi(\overline{\ulcorner\gamma\urcorner}) \vdash \pi(\overline{\ulcorner\pi(\overline{\ulcorner\gamma\urcorner})\urcorner})$;
   (b) Так как $\vdash \pi(\overline{\ulcorner\gamma\urcorner}) \to \neg\gamma$, то по условию 1 $\vdash \pi(\overline{\ulcorner\pi(\overline{\ulcorner\gamma\urcorner}) \to \neg\gamma\urcorner})$;
   (c) По условию 3, $\pi(\overline{\ulcorner\gamma\urcorner}) \vdash \pi(\overline{\ulcorner\pi(\overline{\ulcorner\gamma\urcorner})\urcorner}) \to \pi(\overline{\ulcorner\pi(\overline{\ulcorner\gamma\urcorner}) \to \neg\gamma\urcorner}) \to \pi(\overline{\ulcorner\neg\gamma\urcorner})$;
   (d) Таким образом, $\pi(\overline{\ulcorner\gamma\urcorner}) \vdash \pi(\overline{\ulcorner\neg\gamma\urcorner})$;
   (e) Однако, $\vdash \gamma \to \neg\gamma \to 1 = 0$. Условие 3 (применить два раза) даст $\pi(\overline{\ulcorner\gamma\urcorner}) \vdash \pi(\overline{\ulcorner 1 = 0\urcorner})$.
3. $\neg\pi(\overline{\ulcorner 1 = 0\urcorner}) \to \neg\pi(\overline{\ulcorner\gamma\urcorner})$ (т. о дедукции, контрапозиция).
4. $\vdash \neg\pi(\overline{\ulcorner 1 = 0\urcorner}) \to \gamma$ (определение γ).

■

5 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 пародокс: $X = \{x \mid x \notin x\}$. 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.

5.1 Аксиоматика ZF

Цермело, Френкель (совсем немного).

Определение 5.1.1. Теория множеств — теория первого порядка, с дополнительным нелогическим двуместным функциональным символом $\in$, и следующими дополнительными нелогическими аксиомами и схемами аксиом.

Определение 5.1.2 (Равенство «по Лейбницу»)**.** Объекты равны, если неразличимы.

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

Определение 5.1.3 (Равенство по принципу объёмности)**.** Объекты равны, если состоят из одинаковых частей

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

Определение 5.1.4. $A \subseteq B \equiv \forall x.x \in A \to x \in B$.
$A = B \equiv A \subseteq B \& B \subseteq A$.

5.1.1 Аксиомы теории множеств

Определение 5.1.5 (Аксиома равенства)**.** Равные множества содержатся в одних и тех же множествах.
$\forall x.\forall y.\forall z.x = y \& x \in z \to y \in z$.

Определение 5.1.6 (Аксиома пустого)**.** Существует пустое множество $\varnothing$.

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

Определение 5.1.7 (Аксиома пары)**.** Существует $\{a, b\}$. Каковы бы ни были два множества a и b, существует множество, состоящее в точности из них.

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

Определение 5.1.8 (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.

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

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

Определение 5.1.9 (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 5.1.10 (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 φ), найдется b, в которое входят те и только те элементы из множества x, что $\phi(y)$ истинно.

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

Теорема 5.1.1. Для любого множества X существует множество $\{X\}$, содержащее в точности X.

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

Теорема 5.1.2. 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 5.1.3. Для двух множеств s и t существует множество, являющееся их пересечением.

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

Определение 5.1.11 (Упорядоченная пара)**.** Упорядоченной парой двух множеств a и b назовём $\{\{a\}, \{a, b\}\}$, или $\langle a, b\rangle$.

Теорема 5.1.4. Упорядоченную пару можно построить для любых множеств.

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

Теорема 5.1.5. $\langle a, b\rangle = \langle c, d\rangle$ тогда и только тогда, когда $a = c$ и $b = d$.

Определение 5.1.12. Инкремент: $x' \equiv x \cup \{x\}$.

Определение 5.1.13 (Аксиома бесконечности)**.** Существует $N : \varnothing \in N \& \forall x.x \in N \to x' \in N$

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

Полный порядок (вполне упорядоченные множества)

1. Частичный: рефлексивность ($a \preceq a$), антисимметричность ($a \preceq b \to b \preceq a \to a = b$), транзитивность ($a \preceq b \to b \preceq c \to a \preceq c$).
2. Линейный: частичный $+$ $\forall a.\forall b.a \preceq b \vee b \preceq a$.
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.

5.1.2 Ординалы

Определение 5.1.14. Транзитивное множество X: $\forall x.\forall y.x \in y \& y \in X \to x \in X$.

Определение 5.1.15. Ординал — вполне упорядоченное отношением $(\in)$ транзитивное множество.

Пример. Ординалы: $\varnothing$, $\varnothing'$, $\varnothing''$, ...

Определение 5.1.16. Предельный ординал: такой x, что $x \neq \varnothing$ и нет $y : y' = x$.

Определение 5.1.17. Ординал x конечный, если он меньше любого предельного.

Теорема 5.1.6. Если x, y — ординалы, то $x \in y$ или $y \in x$.

Определение 5.1.18. ω — наименьший предельный ординал.

Теорема 5.1.7. ω существует.

Доказательство. Пусть $\omega = \{x \in N \mid x \text{ конечен}\}$.
Пусть θ таков, что $\theta \in \omega$. Тогда θ конечен. Пусть θ таков, что $\theta' = \omega$. Тогда $\theta \in \omega$. ∎

Пример. ω' — тоже ординал.

Определение 5.1.19. $\sup x$ — наименьший ординал, содержащий x: $x \subseteq \sup x$.

Пример. $\sup\{\varnothing', \varnothing'', \varnothing''''\} = \{\varnothing, \varnothing', \varnothing'', \varnothing''', \varnothing''''\} = \varnothing'''''$

Определение 5.1.20. Определим сложение так:

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

Пример. $\omega + 1 = \omega \cup \{\omega\}$.
$1 + \omega = \sup\{1 + \varnothing, 1 + 1, 1 + 2, \dots\} = \omega$.

Определение 5.1.21. Определим умножение так:

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

Определение 5.1.22. Определим возведение в степень так:

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

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

Пример. Гостиница с ω 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` $\prec$ `Pos 5`. `Neg 5` в данном упорядочении соответствует 5, а `Pos 5` соответствует $\omega + 5$.

Определение 5.1.23. Дизъюнктное (разделённое) множество — множество, элементы которого не пересекаются.

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

Пример. Д изъюнктное: $\{\{1, 2\}, \{\to\}, \{\alpha, \beta, \gamma\}\}$.
Не дизъюнктное: $\{\{1, 2\}, \{\to\}, \{\alpha, \beta, \gamma, 1\}\}$.

Определение 5.1.24. 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 $\cup a$.

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

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

5.1.3 Аксиома выбора

Определение 5.1.25. Прямое произведение непустого дизъюнктного множества, не содержащего пустых элементов, непусто.

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

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

Определение 5.1.26. Аксиоматика ZF + аксиома выбора = ZFC.

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

Теорема 5.1.8. Теорема (Гёдель, 1938): аксиома выбора не добавляет противоречий в ZF.

Теорема 5.1.9. Теорема (Коэн, 1963): аксиома выбора не следует из других аксиом ZF.

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

Теорема 5.1.10. Теорема Диаконеску: ZFC поверх интуиционистского исчисления предикатов содержит правило исключённого третьего.

Определение 5.1.27 (Аксиома фундирования)**.** В каждом непустом множестве найдется элемент, не пересекающийся с исходным множеством.

$$\forall x.x = \varnothing \vee \exists y.y \in x \& y \cap x = \varnothing.$$

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

Определение 5.1.28 (Схема аксиом подстановки)**.** Если задана некоторая функция f, представимая в исчислении предикатов (то есть задана некоторая формула ϕ, такая, что $f(x) = y$ тогда и только тогда, когда $\phi(x, y) \& \exists! z \phi(x, z)$), то для любого множества S существует множество f(S) — образ множества S при отображении f.

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

5.2 Координальные числа

Ординальные числа — порядковые, а координальные — количественные.

Определение 5.2.1. $\langle D$ (обл. определения, domain)$, C$ (обл. значения, codomain)$, G$ (график)$\rangle$ — это функция.

Определение 5.2.2. Биективная функция — сюрективная и инъективная функция.

Определение 5.2.3. $|X| = |Y|$ (множество X равномощно множеству Y), если существует биективная функция $f : X \to Y$.

Определение 5.2.4. $|X| \leqslant |Y|$ (X имеет мощность не больше Y), если существует инъектиная функция $f : X \to Y$.

Определение 5.2.5. $|X| < |Y|$ (X имеет мощность строго меньше Y), если $|X| \leqslant |Y|$ и $|X| \neq |Y|$.

Определение 5.2.6. 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 5.2.1. ω — это $0, 1, 2, 3, \dots$.

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

Определение 5.2.7. На самом деле $|\omega| = \aleph_0$.

Что такое $\aleph_1$?

Определение 5.2.8. $\aleph_1$ — 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 5.2.9 (Альтернативное определение)**.** Координальные числа — множество всех равномощных ориднальных 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.

5.2.1 Теорема Кантора

Теорема 5.2.1. 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 $f : X \to \mathcal{P}(X)$ и f — биекиця.

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

Будем писать табличку.

	x_0	x_1	x_2	x_3	x_4
x_0	×	×	×	×	×
x_1					
x_2		×			×
x_3		×	×	×	

Биективная ли эта функция? В инъективность мы готовы поверить, а вот что с сюрьективностью?

Пусть она сюрьективна, 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 сюрьективна, то есть $|X| \neq |\mathcal{P}(X)|$.

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

Значит $|X| < |\mathcal{P}(X)|$. ■

5.2.2 Можности, большие алеф 0, континум 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 5.2.10. $|\mathcal{P}(\omega)|$ — мощность континум, то есть мощность вещественных чисел.

Утверждение 5.2.2. Континум гипотеза: существуют ли промежуточные между $\aleph_0$ И $|\mathcal{P}(\omega)|$?

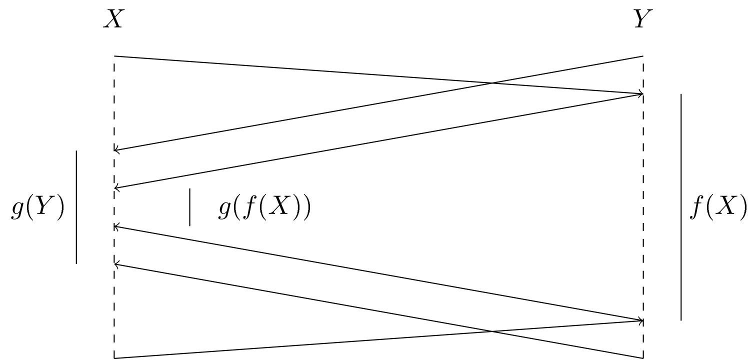
Теорема 5.2.2 (Коэн, 1962–1963)**.** Континум–гипотеза не зависит от аксиоматики Цермело–Френкеля.

Мы можем согласиться с ней, а можем отвергнуть.

5.2.3 Теорема Кантора–Бернштейна

Теорема 5.2.3. Если $|X| \leqslant |Y|$ и $|Y| \leqslant |X|$, то $|X| = |Y|$.

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



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

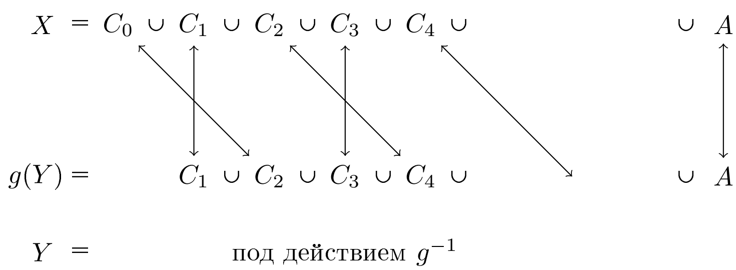
Занумеруем множества.

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

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

Опреедлим $C_n = A_n \backslash A_{n+1}$. 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 $p : X \to g(Y)$ — биекиця. Тогда $q(x) = g^{-1}(p(X)) : X \to Y$ — биекция. То есть $|X| = |Y|$. ■

5.2.4 Мощность вещественных чисел

Теорема 5.2.4. 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. ■

5.3 Теорема Лёвенгейма–Сколема

Как пересчитать вещественные числа (неформально)?

1. Пусть номер вещественного числа — первое упоминание в литературе, т.е. $\langle j, y, n, p, r, c \rangle$:
   - j — гёделев номер названия журнала,

- y — год издания,
- n — номер,
- p — страница,
- r — строка,
- c — позиция.

2. Попробуйте предъявить x, не имеющий номер? Это рассуждение сразу же даст номер.

Определение 5.3.1. Пусть задана модель $\langle D, F_n, P_n\rangle$ для некоторой теории первого порядка. Ее мощностью будем считать мощность D.

Определение 5.3.2. Пусть задана формальная теория с аксиомами α_n. Ее мощность — мощность множества $\{\alpha_n\}$.

Пример. Формальная Арифметика, исчисление предикатов, исчисление высказываний — счетно–аксиоматизируемые.

Определение 5.3.3. $\mathcal{M}' = \langle D', F'_n, P'_n\rangle$ — элементарная подмодель $\mathcal{M} = \langle D, F_n, P_n\rangle$, если

1. $D' \subseteq D$, F'_n, P'_n — сужение F_n, P_n (замкнутое на D').
2. $\mathcal{M}' \models \varphi(x_1, \dots, x_n)$ тогда и только тогда, когда $\mathcal{M} \models \varphi(x_1, \dots, x_n)$ при $x_i \in D'$.

Пример. Когда сущение $\mathcal{M}$ не является элементарной подмоделью?

$\forall x.\exists y.x \neq y$. Истинно в $\mathbb{N}$.

Но пусть $D' = \{\square\}$, тогда наше сужение не является элементарной подмоделью (нарушается второе свойство).

5.3.1 Теорема Лёвенгейма–Сколема

Теорема 5.3.1. Пусть T — множество всех формул теории первого порядка. Пусть теория имеет некоторую модель $\mathcal{M}$. Тогда найдется элементарная подмодель $\mathcal{M}'$, причем $|\mathcal{M}'| = \max(\aleph_0, |T|)$.

Следствие 5.3.1.1 (Более слабая версия теоремы)**.** Пусть теория счетно–аксиоматизируема, тогда найдется элементарная подмодель счетной мощности.

Доказательство. План доказательства:

1. Построим D_0 — множество всех значений, которые упомянуты в языке теории.
2. Будем последовательно пополнять D_i: $D_0 \subseteq D_1 \subseteq D_2 \dots$, следя за мощностью $D' = \bigcup D_i$.
3. Покажем, что $\langle D', F_n, P_n\rangle$ – требуемая подмодель.

Начальный D

Пусть $\{f_k^0\}$ — все 0–местные функцииональные символы теории.

1. $D_0 = \{[\![f_k^0]\!]\}$, если есть хотя бы один f_k^0.

   Например, для формальной арифметики множеством D_0 будет $\{0\}$. А для теории множест $D_0 = \{\varnothing, N\}$ (N — то бесконечное множество, существование которого гарантируется).

2. Если таких f_k^0 нет, возьмем какое-нибудь значение из D.

Очевидно, $|D_0| \leqslant |T|$.

Пополнение D

Фиксируем некоторый D_k. Напомним, T — множество всех формул теории. Рассмотрим $\varphi \in T$.

1. Если φ не имеет свободных переменных — пропустим.
2. Если φ имеет хотя бы одну свободную переменную y.
   (a) $\varphi(y, x_1, \ldots, x_n)$ при $y, x_i \in D_k$ бывает истинным и ложным — ничего не меняем.
   (b) $\varphi(y, x_1, \ldots, x_n)$ при $y \in D, x_i \in D_k$ всегда истинный или ложный — ничего не меняем.
   (c) $\varphi(y, x_1, \ldots, x_n)$ при $y \in D, x_i \in D_k$ всегда истинный или ложный, но при $y' \in D \backslash D_k$ отличается — добавим y' к D_{k+1}.
   Добавляя y', добавим все возможные $[\![\theta\,(y')]\!]$ (формулы, которые используют y').

Заметим, что мы добавили не больше $|T| \cdot |D_k|$ формул.

Заметим, что $|\bigcup D_i| \leqslant |T| \cdot |D_k| \cdot \aleph_0 = \max\,(|T|, \aleph_0)$.

Почему то, что мы построили элементарная подмодель? Пройдемся индукцией по структуре формул $\tau \in T$ и покажем, что все формулы можно вычислить, и что $[\![\varphi]\!]_{\mathcal{M}'} = [\![\varphi]\!]_{\mathcal{M}}$.

1. База, 0 связок. $\tau \equiv P(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$.
2. Переход. Пусть формула из k связок сохраняют значения. Рассмотрим τ с $k+1$ связкой.
   (a) $\tau \equiv \rho \star \sigma$ — очевидно.
   (b) $\tau \equiv \forall y.\varphi(y, x_1, \ldots, x_n)$. Каждый из x_i добавен на каком-то шаге — максимум t.
   Если $\varphi(y, x_1, \ldots, x_n)$ бывает истинен и ложен при $y_t, y_f \in D$, то $y_t, y_f \in D_{t+1}$ (по построению). Поэтому если $\mathcal{M} \not\models \forall y.\varphi(y, x_1, \ldots, x_n)$, то и $\mathcal{M}' \not\models \forall y.\varphi(y, x_1, \ldots, x_n)$.
   Если же $\varphi(y, x_1, dots, x_n)$ не меняется от y, то тем более $[\![\varphi]\!]_{\mathcal{M}'} = [\![\varphi]\!]_{\mathcal{M}}$.
   (c) $\tau \equiv \exists y.\varphi(y, x_1, dots, x_n)$ — аналогично.

■

5.3.2 «Парадокс» Сколема

Как известно, $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| > |\mathbb{N}| = \aleph_0$. Однако, ZFC — счетно–аксиоматизируемая теория. Значит, существует счтеная модель ZFC, то есть $|\mathbb{R}| = \aleph_0$. В чем ошибка?

На самом деле, у равенств выше разный смысл. Первое равенство — в предметном языке, а второе — в метаязыке. То есть, второе равенство не возможно формализовать в ZFC, значит и парадокса здесь нет.

6 Теорема о корректности формальной арифметики

6.1 Трансфинитная индукция

Эквивалентность слабой ($n \to n+1$) и сильной ($1 \ldots n \to n+1$) индукции.

Определение 6.1.1 (Принцип математической индукции)**.** Какое бы ни было $\varphi(x)$, если $\varphi(0)$ и при всех x выполнено $\varphi(x) \to \varphi(x')$, то при всех x выполнено и само $\varphi(x)$.

Определение 6.1.2 (Принцип полной математической индукции)**.** Какое бы ни было $\psi(x)$, если $\psi(0)$ и при всех x выполнено $(\forall t.x < t \to \psi(x)) \to \psi(x')$, то при всех x выполнено и само $\psi(x)$.

Теорема 6.1.1. Принципы математической индукции эквивалентны

Доказательство. ($\Rightarrow$) взяв $\varphi := \psi$, имеем выполненность $\varphi(x) \to \varphi(x')$, значит, $\forall x.\psi(x)$.

($\Leftarrow$) возьмём $\psi(x) := \forall t.t \leqslant x \to \varphi(t)$ ∎

Теорема 6.1.2 (Принцип трансфинитной индукции)**.** Если для $\varphi(x)$ — некоторого утверждения теории множеств — выполнено:

1. $\varphi(\varnothing)$
2. Если $\forall u.u \in v \to \varphi(u)$, то $\varphi(v)$ (где v - это ординал)

то $\forall u.\varphi(u)$.

Лемма 6.1.2.1. Свойство индукции выполнено для натуральных чисел: если $\varphi(0)$ и $\forall x \in \mathbb{N}_0.f(x) \to f(x')$, то $\forall x \in \mathbb{N}_0.f(x)$.

Доказательство. Пусть $\varphi(\varnothing)$ и $\forall u.(u \in \omega) \to \varphi(u) \to \varphi(u')$. Рассмотрим $\tau(n) = \forall u.u \in n \to \varphi(u)$. Очевидно, что если $m \in n$, то $\tau(n) \to \tau(m)$. Значит, выполнены условия принципа трансфинитной индукции для ω, отсюда $\tau(\omega)$, отсюда $\forall u.(u \in \omega) \to \varphi(u)$. ∎

6.2 Исчисление S_∞

1. Язык: связки $\neg$, $\vee$, $\forall$; нелогические символы: $(+)$,$(\cdot)$,$(')$,0,$(=)$.
2. Аксиомы: все истинные формулы вида $\theta_1 = \theta_2$; все истинные отрицания формул вида $\neg\theta_1 = \theta_2$ (θ_i — термы без переменных).
3. Структурные (слабые) правила:
$$\frac{\zeta \vee \alpha \vee \beta \vee \delta}{\zeta \vee \beta \vee \alpha \vee \delta}, \qquad \frac{\alpha \vee \alpha \vee \delta}{\alpha \vee \delta}.$$
4. Сильные правила
$$\frac{\delta}{\alpha \vee \delta} \qquad \frac{\neg\alpha \vee \delta \quad \neg\beta \vee \delta}{\neg(\alpha \vee \beta) \vee \delta} \qquad \frac{\alpha \vee \delta}{\neg\neg\alpha \vee \delta} \qquad \frac{\neg\alpha[x := \theta] \vee \delta}{(\neg\forall x.\alpha) \vee \delta}.$$
5. Бесконечная индукция
$$\frac{\alpha[x := \overline{0}] \vee \delta \quad \alpha[x := \overline{1}] \vee \delta \quad \alpha[x := \overline{2}] \vee \delta \quad \dots}{(\forall x.\alpha) \vee \delta}.$$
6. Сечение
$$\frac{\zeta \vee \alpha \qquad \neg\alpha \vee \delta}{\zeta \vee \delta}.$$
Здесь:
α — секущая формула
Число связок в $\neg\alpha$ — степень сечения.

Дерево доказательства

1. Доказательства образуют деревья.
2. Каждой формуле в дереве сопоставим порядковое число (ординал).

3. Порядковое число заключения любого неструктурного правила строго больше порядкового числа его посылок (больше или равно в случае структурного правила).

$$\dfrac{\dfrac{}{0=0} \quad \dfrac{\dfrac{\dfrac{}{0=0}}{\dots}}{0'=0'} \quad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{0=0}}{\dots}}{0'=0'}}{\dots}}{0''=0''} \quad \dots}{(\forall a.a=a)_\omega} \qquad \dfrac{\dfrac{}{0=0} \quad \dfrac{}{0'=0'} \quad \dfrac{}{0''=0''} \quad \dots}{(\forall a.a=a)_1}.$$

4. Существует конечная максимальная степень сечения в дереве (назовём её степенью вывода).

Теорема 6.2.1. Если $\vdash_{\text{фа}} \alpha$, то $\vdash_\infty |\alpha|_\infty$.

Теорема 6.2.2. Если Ф.А. противоречива, то противоречива и S_∞.

Пример. Обратное неверно:

$$\dfrac{\neg\omega(\overline{0}, \overline{\ulcorner\sigma\urcorner}) \qquad \neg\omega(\overline{1}, \overline{\ulcorner\sigma\urcorner}) \qquad \neg\omega(\overline{2}, \overline{\ulcorner\sigma\urcorner}) \qquad \dots}{\forall x.\neg\omega(x, \overline{\ulcorner\sigma\urcorner})}.$$

Теорема 6.2.3. Если формула α доказана и имеет вид, похожий на заключение правил де Моргана, отрицания и бесконечной индукции — то посылки соответствующих правил могут быть получены из самой формулы α доказательством, причём доказательством с не большей степенью и не большим порядком.

Доказательство. Например, формула вида $\neg\neg\alpha \vee \delta$.

Проследим историю α; она получена:

1. ослаблением — заменим $\neg\neg\alpha$ на α в этом узле и последующих.

2. отрицанием — выбросим правило, заменим $\neg\neg\alpha$ на α в последующих.

Изменённый вывод — доказательство требуемого. ■

Теорема 6.2.4. Если α имеет вывод степени $m > 0$ порядка t, то можно найти вывод степени строго меньшей m с порядком 2^t.

Доказательство. Трансфинитная индукция по порядку t.

1. База. Если $t = 0$, то неструктурных правил нет, отсюда $m = 0$.

2. Переход. Рассмотрим заключительное правило.

   (a) Не сечение.

   (b) Сечение, секущая формула — элементарная.

   (c) Сечение, секущая формула — $\neg\alpha$.

   (d) Сечение, секущая формула — $\alpha \vee \beta$.

   (e) Сечение, секущая формула — $\forall x.\alpha$.

Случай 1. Не сечение

$$\frac{\pi_{t_0} \quad \pi_{t_1} \quad \pi_{t_2} \quad \dots}{\alpha}.$$

Заменим доказательства посылок π_i по индукционному предположению.

1. Если $m_i' < m_i$, то $\max m_i' < \max m_i$
2. Если $t_i \leqslant t$, то $2^{t_i} \leqslant 2^t$.

Случай 2.4. Сечение с формулой вида $\forall x.\alpha$

$$\frac{\zeta \vee \forall x.\alpha \qquad \neg(\forall x.\alpha) \vee \delta}{\zeta \vee \delta}.$$

Причём степень и порядок выводов компонент, соответственно, (m_1, t_1) и (m_2, t_2).

1. По индукции, вывод $\zeta \vee \forall x.\alpha$ можно упростить до $(m_1', 2^{t_1})$.
2. По обратимости, для постоянного θ можно построить вывод $\zeta \vee \alpha[x := \theta]$ за $(m_1', 2^{t_1})$.
3. В формуле $(\neg\forall x.\alpha) \vee \delta$ формула $\neg\forall x.\alpha$ получена либо ослаблением, либо квантификацией из $\neg\alpha[x := \theta_k] \vee \delta_k$.
   (a) Каждое правило квантификации заменим на:
   $$\frac{\zeta \vee \alpha[x := \theta_k] \qquad (\neg\alpha[x := \theta_k]) \vee \delta_k}{\zeta \vee \delta_k}.$$
   (b) Остальные вхождения $\neg\forall x.\alpha$ заменим на ζ (в правилах ослабления).
4. В получившемся дереве меньше степень — так как в $\neg\alpha[x := \theta]$ меньше связок, чем в $\neg\forall x.\alpha$.
5. Нумерацию можно также перестроить.

■

6.2.1 Теорема об устранении сечений

Определение 6.2.1. Итерационная экспонента

$$(a\uparrow)^m(t) = \begin{cases} t, & m = 0 \\ a^{(a\uparrow)^{m-1}(t)}, & m > 0 \end{cases}.$$

Теорема 6.2.5. Если $\vdash_\infty \sigma$ степени m порядка t, то найдётся доказательство без сечений порядка $(2\uparrow)^m(t)$

Доказательство. В силу конечности m воспользуемся индукцией по m и теоремой об уменьшении степени. ■

6.3 Непротиворечивость формальной арифметики

Теорема 6.3.1. Система S_∞ непротиворечива

Доказательство. Рассмотрим формулу $\neg 0 = 0$. Если эта формула выводима в S_∞, то она выводима и в S_∞ без сечений. Тогда какое заключительное правило?

1. Правило Де-Моргана? Нет отрицаний дизъюнкции $(\neg(\alpha \vee \beta) \vee \delta)$.

2. Отрицание? Нет двойного отрицания ($\neg\neg\alpha \vee \delta$).

3. Бесконечная индукция или квантификация? Нет квантора.

4. Ослабление? Нет дизъюнкции ($\alpha \vee \delta$).

То есть, неизбежно, $\neg 0 = 0$ — аксиома, что также неверно. $\blacksquare$