Мат. логика

Автор: Вячеслав Чепелин

Содержание

1. Исчисление высказываний

def: **Предметный язык** — формализация мат. утверждений.

def: **Метаязык** (или язык исследователя) — язык, которым пользуются для формирования математических утвреждений.

def: **Высказывание** — строка, которая либо атомарное высказывание(то есть какая-то переменная), либо составное(составлено с помощью отрицания, дизъюнкции, конъюнкции или импликации из двух высказываний).

def: **Схема высказываний** — высказывание, где мы можем использовать метапеременные (вместо которых можно подставлять что угодно)

def: **Язык исчисления высказываний** — язык, порождаемый грамматикой высказываний.

def: **Оценка высказываний** — множество истинностных значений(множество $V = \{И, Л\}$) и функция оценки переменных. Все оценки составных высказываний рекурсивно задаются

def: α - **тавтология** (общезначима), если $\models \alpha$ или по-другому, что α истинна при всех оценках

def: $\gamma_1, ..., \gamma_n \models \alpha$ - **следствие**, то есть если данные γ выполнены, то α выполнено

def: **Доказательством** назовем конечную последовательность $\delta_1, ..., \delta_n$, где каждое δ_i либо аксиома, либо получаестя по правило Modus Ponens(α, $\alpha \to \beta \Rightarrow \beta$)

В классической логике есть 10 аксиом, которые задаются схемами. Назовем эти аксиомы аксиомами исчисления высказываний.

def: **Доказательство формулы** α — такое доказательство, что $\delta_n \equiv \alpha$. Тогда α называется **доказуемой**.

def: **Вывод формулы из гипотез** $\gamma_1, ..., \gamma_n$ - в доказательстве можем использовать еще и гипотезы. Обозначается $\gamma_1, ..., \gamma_n \vdash \alpha$

def: **Теория корректна**, если любое доказуемое утверждение общезначимо.

def: **Теория полна**, если любое общезначимое утверждение доказуемо.

def: **Теория противоречива**, если существует α , такое что $\vdash \alpha \& \neg\alpha$. Эквивалентно, что любая формула доказуема, или для некоторой α имеет место $\vdash \alpha$ и $\vdash \neg\alpha$

Теорема о дедукции.
$\Gamma, \alpha \vdash \beta \Leftrightarrow \Gamma \vdash \alpha \to \beta$

Доказательство:
Доказательство в левую сторону очевидно. Докажем,что из $\Gamma, \alpha \vdash \beta$ следует $\Gamma \vdash \alpha \to \beta$

Пусть $\Gamma, \alpha \vdash \beta$, т.е. существует вывод $D = (\delta_1, ..., \delta_m)$, где $\delta_m = \beta$.

Построим вывод $\alpha \to \beta$ из Γ **индукцией по длине вывода** D.

База: очевидно

Шаг индукции:

Предположим, для всех выводов длины $\leq m$ утверждение верно. Рассмотрим вывод D длины $m + 1$:

$$\delta_1, ..., \delta_m, \delta_{m+1}(= \beta)$$

По индукционному предположению, уже построены выводы ζ_i из Γ, такие что $\zeta_i = \alpha \to \delta_i$ для $i = 1, ..., m$.

Разберём возможные случаи для δ_{m+1}:

1. δ_{m+1} — **аксиома или** $\delta_{m+1} \in \Gamma$: Тогда $\Gamma \vdash \delta_{m+1}$

   Добавим к построенным $\zeta_1, ..., \zeta_m$ шаги:

   $$\delta_{m+1} \to (\alpha \to \delta_{m+1}) \text{ (акс.1)}$$

   $$\delta_{m+1}$$

   $$\alpha \to \delta_{m+1} \text{ (MP)}$$

2. $\delta_{m+1} \equiv \alpha$, $\alpha \to \alpha$ выводимо всегда

3. δ_{m+1} получен по MP из δ_j и δ_k ($\delta_k \equiv \delta_j \to \delta_{m+1}$), где $j, k < m + 1$:

   По индукционному предположению уже имеем $\Gamma \vdash \alpha \to \delta_j$ и $\Gamma \vdash \alpha \to (\delta_j \to \delta_{m+1})$.

   По акс.2: $(\alpha \to \delta_j) \to (\alpha \to (\delta_j \to \delta_{m+1})) \to (\alpha \to \delta_{m+1})$

   Применив MP дважды, получаем

   $$\Gamma \vdash \alpha \to \delta_{m+1}$$

Таким образом, во всех случаях $\Gamma \vdash \alpha \to \delta_{m+1}$, т.е. $\Gamma \vdash \alpha \to \beta$.

Q.E.D.

2. Теорема о полноте исчисления высказываний

def: Условное отрицание. Зададим некоторую оценку переменных, что $[\![a]\!] = x$. Тогда условным отрицанием формулы α назовем следующую формулу $(\!|a|\!)$:

$$(\!|a|\!) = \begin{cases} \alpha, x = \text{И} \\ \neg\alpha, x = \text{Л} \end{cases}$$

Также, если $\Gamma := \gamma_1, \gamma_2, ..., \gamma_n$, то за $(\!|\Gamma|\!)$ обозначим $(\!|\gamma_1|\!), (\!|\gamma_2|\!), ...(\!|\gamma_n|\!)$.

Теорема о полноте.
Если $\models \alpha$, то $\vdash \alpha$

Доказательство:

1. Построим таблицы истинности для каждой связки $(\star)$ и докажем в них каждую строку:
$$(\!|\varphi|\!), (\!|\psi|\!) \vdash (\!|\varphi \star \psi|\!)$$
2. Построим таблицу истинности для α и докажем в ней каждую строку:
$$(\!|\Xi|\!) \vdash (\!|\alpha|\!)$$
3. Если формула общезначима, то в ней все строки будут иметь вид $(\!|\Xi|\!) \vdash \alpha$, потому от гипотез мы сможем избавиться и получить требуемое $\vdash \alpha$.

Приступим:

Шаг 1. Лемма о связках

Запись $(\!|\varphi|\!), (\!|\psi|\!) \vdash (\!|\varphi \star \psi|\!)$ сводится к 14 утверждениям:

- $\neg\varphi, \neg\psi \vdash \neg(\varphi\&\psi)$ и $\neg\varphi, \neg\psi \vdash (\varphi \to \psi)$
- $\neg\varphi, \psi \vdash \neg(\varphi\&\psi)$ и $\neg\varphi, \psi \vdash (\varphi \to \psi)$
- $\varphi, \neg\psi \vdash \neg(\varphi\&\psi)$ и $\varphi, \neg\psi \vdash \neg(\varphi \to \psi)$
- $\varphi, \psi \vdash (\varphi\&\psi)$ и $\varphi, \psi \vdash (\varphi \to \psi)$
- $\neg\varphi, \neg\psi \vdash \neg(\varphi \vee \psi)$ и $\varphi \vdash \neg\neg\varphi$
- $\neg\varphi, \psi \vdash (\varphi \vee \psi)$ и $\neg\varphi \vdash \neg\varphi$
- $\varphi, \neg\psi \vdash (\varphi \vee \psi)$
- $\varphi, \psi \vdash (\varphi \vee \psi)$

Шаг 2. Обобщение на любую формулу

Лемма. Условное отрицание формул:

Пусть пропозициональные переменные $\Xi := \{X_1, ..., X_n\}$ — все переменные, которые используются в формуле α. И пусть задана некоторая оценка переменных.

Тогда, $(\!|\Xi|\!) \vdash (\!|\alpha|\!)$

Доказательство:

Индукция по длине формулы α.

База:

Формула α — атомарная, т.е. $\alpha \equiv X_i$.

Тогда при любом Ξ выполнено $(\!|\Xi|\!)^{X_i := \text{И}} \vdash X_i$ и $(\!|\Xi|\!)^{X_i := \text{Л}} \vdash \neg X_i$.

Индукционный переход: $\alpha \equiv \varphi \star \psi$, причём $(\!|\Xi|\!) \vdash (\!|\varphi|\!)$ и $(\!|\Xi|\!) \vdash (\!|\psi|\!)$

Тогда построим вывод:

$(1)...(n) - (\!|\varphi|\!)$ (индукционное предположение)

$(n+1)...(k) - (\!|\psi|\!)$ (индукционное предположение)

$(k+1)...(l) - (\!|\varphi \star \psi|\!)$ (лемма о связках: $(\!|\varphi|\!)$ и $(\!|\psi|\!)$ доказаны выше, значит, их можно использовать как гипотезы)

Откуда лемма доказана.

Шаг 3. Избавляемся от гипотез

Лемма (об устранении посылок?):

Пусть при всех оценках переменных $(\!|\Xi|\!) \vdash \alpha$, тогда $\vdash \alpha$.

Доказательство:

Индукция по количеству переменных n.

База: $n = 0$. Тогда $\vdash \alpha$ есть из условия.

Индукционный переход:

Пусть $(\!|X_1, X_2, ...X_{n+1}|\!) \vdash \alpha$. Рассмотрим выводы:

$$(\!|X_1, X_2, ...X_n|\!), X_{n+1} \vdash \alpha \qquad (\!|X_1, X_2, ...X_n|\!), \neg X_{n+1} \vdash \alpha$$

По лемме об исключении допущения тогда $(\!|X_1, X_2, ...X_n|\!) \vdash \alpha$

(Лемма об исключении допущения: $\alpha \vdash \beta$ и $\neg\alpha \vdash \beta$, то $\vdash \beta$. Доказывается очень просто с помощью теоремы о дедукции)

При этом, $(\!|X_1, X_2, ...X_n|\!) \vdash \alpha$ при всех оценках переменных $X_1, ...X_n$. Значит, $\vdash \alpha$ по индукционному предположению.

Q.E.D.

3. Топологические пространства

def: Упорядоченная пара $\langle X, \Omega \rangle$ где X — множество, Omega ⊆ P(X) (называется **топологией**), удовлетворяющая:
1. $\emptyset \in \Omega$, $X \in \Omega$.
2. Конечное пересечение элементов Ω принадлежит Ω.
3. Объединение любого семейства элементов Ω принадлежит Ω.

def: **Открытые множества** - элементы топологии Ω

def: **Замкнутое множество** - множество, дополнение до X которого является открытым.

def: **Внутренность множества** (`A°`) - наибольшее открытое множество, содержащееся в A.

Примеры топологий

- **Топология стрелки**: на $\mathbb{R}$, открытыми являются множества вида [a, +∞) и пустое множество.
- **Топология Зарисского**: на $\mathbb{R}$, открытыми являются $\mathbb{R}$, $\emptyset$ и все множества, дополнения которых конечны.
- **Топология на дереве (лесе)**: Пусть задан лес с множеством вершин V и отношением порядка $\preccurlyeq$ (предок-потомок: a $\preccurlyeq$ b, если b — потомок a). Открытое множество вместе с каждой вершиной содержит всех её потомков.

def: **Непрерывная функция** (между топологическими пространствами) — прообраз любого открытого множества в Y является открытым множеством в X.

def: **Компактное множество** — Множество, из любого его открытого покрытия можно выбрать конечное подпокрытие.

def: **Подпространство топологического пространства** — пространство $\langle X_1, \Omega_1 \rangle$называется подпространством $\langle X, \Omega \rangle$, если $X_1 \subseteq X$ и $\Omega_1 = \{A \cap X_1 \mid A \in \Omega\}$.

def: **Связное пространство** — не существует таких двух непустых открытых множеств $A, B \in \Omega$, что $A \cup B = X$ и $A \cap B = \emptyset$.

def: **Связное множество** — если соответствующее ему подпространство связно.

4. Интуиционистская логика, вывод, интерпретация, решетки

Основные положения интуиционизма:

- Математика не формальна.
- Математика независима от окружающего мира.
- Логика зависит от математики, а не наоборот.

def: Доказательства чистого существования (конструктивный подход): Объект считается существующим, если для него предоставлен эффективный метод построения, а не только доказательство невозможности его отсутствия.

def: BHK-интерпретация (Брауэр, Гейтинг, Колмогоров): Конструктивная интерпретация логических связок, где истинность высказывания означает наличие его построения (доказательства).

- $\alpha \wedge \beta$ построено, если построены α и β.
- $\alpha \vee \beta$ построено, если построено α или β, и известно, какое именно.
- $\alpha \to \beta$ построено, если имеется метод, преобразующий любое построение α в построение β.
- $\bot$ — конструкция, не имеющая построения.
- $\neg\alpha$ построено, если построено $\alpha \to \bot$.

def: Интуиционистское исчисление высказываний (ИИВ) в гильбертовском стиле: Получается из аксиоматики классического исчисления высказываний (КИВ) заменой аксиомы снятия двойного отрицания ($\neg\neg\alpha \to \alpha$) на аксиому ($\alpha \to (\neg\alpha \to \beta)$) (принцип взрыва).

def: Интуиционистское исчисление высказываний (натуральный вывод):
- **Секвенция:** Выражение вида $\Gamma \vdash \alpha$, где Γ — множество гипотез, α — заключение.
- **Аксиома:** $\Gamma, \alpha \vdash \alpha$.
- **Правила введения связок:**
  - Если $\Gamma, \alpha \vdash \beta$, то $\Gamma \vdash \alpha \to \beta$.
  - Если $\Gamma \vdash \alpha$, то $\Gamma \vdash \alpha \vee \beta$. Если $\Gamma \vdash \beta$, то $\Gamma \vdash \alpha \vee \beta$.
  - Если $\Gamma \vdash \alpha$ и $\Gamma \vdash \beta$, то $\Gamma \vdash \alpha \wedge \beta$.
- **Правила удаления связок:**
  - Если $\Gamma \vdash \alpha$ и $\Gamma \vdash \alpha \to \beta$, то $\Gamma \vdash \beta$.
  - Если $\Gamma \vdash \alpha \vee \beta$, $\Gamma \vdash \alpha \to \gamma$ и $\Gamma \vdash \beta \to \gamma$, то $\Gamma \vdash \gamma$.
  - Если $\Gamma \vdash \alpha \wedge \beta$, то $\Gamma \vdash \alpha$. Если $\Gamma \vdash \alpha \wedge \beta$, то $\Gamma \vdash \beta$.
  - Если $\Gamma \vdash \bot$, то $\Gamma \vdash \alpha$ (из лжи следует всё).

Его мы записываем в виде дерева.

def: Закон исключённого третьего ($\alpha \vee \neg\alpha$): В BHK-интерпретации не является общезначимым, так как для нерешённой проблемы у нас нет построения ни для α, ни для $\neg\alpha$.

def: Изоморфизм Карри-Ховарда: Прямая аналогия между логикой и теорией типов в программировании.

- Программа (λ-выражение) $\leftrightarrow$ Доказательство.
- Тип выражения $\leftrightarrow$ Высказывание.
- Тип функции ($A \to B$) $\leftrightarrow$ Импликация ($A \to B$).
- Упорядоченная пара ($A \times B$) $\leftrightarrow$ Конъюнкция ($A \wedge B$).
- Алгебраический тип ($A + B$) $\leftrightarrow$ Дизъюнкция ($A \vee B$).
- Необитаемый тип (void, $\bot$) $\leftrightarrow$ Ложь ($\bot$).

def: Решётка: Упорядоченная пара $\langle X, \preccurlyeq \rangle$, где X — множество, $\preccurlyeq$ — частичный порядок на X, такой что для любых $a, b \in X$ определены:

- **Сумма** (супремум): $a + b = \sup\{a, b\}$ — наименьший элемент c такой, что $a \preccurlyeq c$ и $b \preccurlyeq c$.
- **Произведение** (инфимум): $a \cdot b = \inf\{a, b\}$ — наибольший элемент c такой, что $c \preccurlyeq a$ и $c \preccurlyeq b$.

def: Дистрибутивная решётка: Решётка, в которой для любых a, b, c выполняется: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

def: Псевдодополнение: В решётке псевдодополнением $a \longrightarrow b$ называется наибольший элемент из множества $\{ x \mid a \cdot x \preccurlyeq b \}$.

def: Импликативная решётка: Решётка, в которой для любых двух элементов существует псевдодополнение.

0 и 1 в решётке: 0 — наименьший элемент решётки, 1 — наибольший элемент решётки.

def: Псевдобулева алгебра (алгебра Гейтинга): Импликативная решётка с наименьшим элементом 0. В ней определяется операция отрицания: $\neg a = a \longrightarrow 0$.

def: Булева алгебра: Псевдобулева алгебра, в которой для любого элемента a выполняется закон исключённого третьего в алгебраической форме: $a + \neg a = 1$.

5. Продолжение решеток, алгебра Линдембаума, модели Крипке

def: Пусть L - множество всех высказываний. Тогда **алгебра Линденбаума** $\mathcal{L} = L/_{\simeq}$, где отношения эквивалентности построено, если $a \preceq b, b \preceq a$, где a - предпорядок : $\alpha \preceq \beta := \alpha \vdash \beta$ в иив.

Теорема. $\mathcal{L}$ — псевдобулева алгебра. Доказательство — надо показать, что $\preceq$ отношение порядка на $\mathcal{L}$

def: Пусть некоторое исчисление оценивается значениями из решетки. Оценка **согласованна** с исчисленмем, если «и» это умножение, «или» это сложение и так далее.

Теорема. $[\![\alpha]\!] = [\alpha]_{\mathcal{L}}$

Теорема.
Интуиционисткое исчисление полно в псевдобулевых алгебрах. То есть если $\models \alpha$ во всех псевдобулевых, то $\vdash \alpha$

Доказательство:
Возьмем в качестве модели исчисления алгебру Линдембаума.

Пусть $\models \alpha$, тогда $[\![\alpha]\!] = 1$ во всех псевдобулевых, в том чисое и $[\![\alpha]\!] = 1_{\mathcal{L}}$. То есть $[\alpha]_{\mathcal{L}} = [A \to A]_{\mathcal{L}}$. То есть $A \to A \vdash \alpha$, откуда уже следует искомое.

Идейно мы просто перекидываем все в алгебру Линдембаума и пользуемся ее свойствами

Q.E.D.

def: **Модель Крипке**: Упорядоченная тройка $\langle \mathcal{W}, \preceq, \Vdash \rangle$, где:
- $\mathcal{W}$ — множество миров.
- $\preceq$ — нестрогий частичный порядок на $\mathcal{W}$.
- $\Vdash \subseteq \mathcal{W} \times P$ — отношение вынужденности между мирами и пропозициональными переменными, монотонное относительно порядка: если

$$\mathcal{W}_i \preceq \mathcal{W}_j \text{ и } \mathcal{W}_i \Vdash X, \text{ то } \mathcal{W}_j \Vdash X$$

def: **Вынужденность** (доопределение для формул):

Для любого мира $\mathcal{W} \in \mathcal{W}$:
- $\mathcal{W} \Vdash \alpha \wedge \beta \Leftrightarrow \mathcal{W} \Vdash \alpha$ и $\mathcal{W} \Vdash \beta$
- $\mathcal{W} \Vdash \alpha \vee \beta \Leftrightarrow \mathcal{W} \Vdash \alpha$ или $\mathcal{W} \Vdash \beta$.
- $\mathcal{W} \Vdash \alpha \longrightarrow \beta \Leftrightarrow$ для любого мира $\mathcal{W}_1$ такого, что $\mathcal{W} \preceq \mathcal{W}_1$ и $\mathcal{W}_1 \Vdash \alpha$, выполнено $\mathcal{W}_1 \Vdash \beta$.
- $\mathcal{W} \Vdash \neg\alpha \Leftrightarrow$ ни для какого мира $\mathcal{W}_1$ такого, что $\mathcal{W} \preceq \mathcal{W}_1$, не верно $\mathcal{W}_1 \Vdash \alpha$.

def: **Формула α истинна в модели Крипке**$(\models \alpha)$, если $\mathcal{W} \Vdash \alpha$ для всех миров $\mathcal{W} \in \mathcal{W}$.

def: **Общезначимость в моделях Крипке** $(\underset{\mathcal{K}}{\Vdash} \alpha)$, если она истинна во всех возможных моделях Крипке.

Теорема.
Пусть $\langle \mathcal{W}, \preceq, \Vdash \rangle$ — некоторая модель Крипке. Тогда она есть корректная модель ИИВ.

Доказательство:
Доказательство для древовидного отношения.

Заметим, что $V(\alpha) := \{w \in \mathcal{W} |\ w \Vdash \alpha\}$ открыто в топологии для деревьев. Значит положим $V = \{S \mid \subseteq \mathcal{W} \& S - \text{открыто}\}$ и $[\![\alpha]\!] = V(a)$, получим алгебру Гейтинга

Q.E.D.

def: Система $\langle V, T, f_\wedge, f_\vee, f_\to, f_\neg \rangle$, где:

- V — множество значений.
- $T \in V$ — выделенное значение «истина».
- $f_\wedge, f_\vee, f_\to : V \times V \to V$ — функции для связок.
- $f_\neg : V \to V$ — функция для отрицания.

Оценка называется **табличной**, если значение любой формулы вычисляется рекурсивно через эти функции и оценку переменных $f_P : P \to V$.

def: Если $\vdash \alpha$ влечет $[\![\alpha]\!] = T$ при всех оценках пропозициональных переменных, то $\mathcal{M}$ – **табличная модель**

> **Теорема.**
> Не существует полной конечной табличной модели для ИИВ
>
> просят только формулировку

6. Геделева алгебра, разрешимость ИИВ

def: Гёделевизация алгебры Гейтинга (Γ($\mathcal{A}$)): Для алгебры Гейтинга $\mathcal{A}$ = ⟨A, $\preceq$⟩ операция гёделевизации строит новую алгебру Γ($\mathcal{A}$) = ⟨A ∪ {ω}, $\trianglelefteq$⟩, где:

- ω — новый элемент.
- Отношение порядка $\trianglelefteq$ минимальное, удовлетворяющее:
  - $\mathcal{A} \trianglelefteq$ b, если $\mathcal{A} \preceq$ b в $\mathcal{A}$ и $\mathcal{A}$, b ∉ {ω, 1}.
  - $\mathcal{A} \trianglelefteq$ ω, если $\mathcal{A} \neq 1$ в $\mathcal{A}$.
  - ω $\trianglelefteq$ 1.

Γ($\mathcal{A}$) является гёделевой алгеброй.

def: Отображение $g : \mathcal{A} \to \mathcal{B}$ между алгебрами Гейтинга называется **гомоморфизмом**, если оно сохраняет операции и константы:

$$g(a \wedge b) = g(a) \wedge g(b), g(a \vee b) = g(a) \vee g(b), g(a \to b) = g(a) \to g(b), g(0_{\mathcal{A}}) = 0_{\mathcal{B}}, g(1_{\mathcal{A}}) = 1_{\mathcal{B}}$$

Теорема. Дизъюнктивность ИИВ
Если $\vdash \alpha \vee \beta$, то либо $\vdash \alpha$, либо $\vdash \beta$

Доказательство:
Пусть $\vdash \alpha \vee \beta$. Тогда $[\![\alpha \vee \beta]\!]_{\Gamma(\mathcal{L})} = 1$, так как данная оценка согласованна с ИИВ.

Тогда $[\![\alpha]\!]_{\Gamma(\mathcal{L})} = 1$ или $[\![\beta]\!]_{\Gamma(L)} = 1$, так как $\Gamma(\mathcal{L})$ — геделева

Пусть $[\![\alpha]\!]_{\Gamma(\mathcal{L})} = 1$, тогда из гомоморфизма $[\![\alpha]\!]_{\mathcal{L}} = 1$, откуда из полноты $\mathcal{L}$ получаем, что $\vdash \alpha$

Q.E.D.

def: Решётка $\mathscr{A}'$ = ⟨A', $\preccurlyeq_{„}$⟩ называется **подрешёткой решётки** $\mathscr{A}$ = ⟨A, $\preccurlyeq$⟩, если:

- A' ⊆ A.
- $\preccurlyeq_{„}$ = $\preccurlyeq$ ∩ (A“ × A') (ограничение порядка).
- Для любых a, b ∈ A' их супремум и инфимум в $\mathscr{A}'$ совпадают с супремумом и инфимумом в $\mathscr{A}$.

Лемма.
Существует дистрибутивная подрешетка $\mathcal{L}'$, содержащая $a_1, ..., a_n$ (это какие-то элементы), что $|L'| \leq 2^{2^n}$

Доказательство:

Еще не осмысленно, просто скопировано с теха

Пусть $\mathcal{L}' = \{\varphi(a_1, ..., a_n) \mid \varphi \text{ составлено из } (+) \text{ и } (c\,\cdot)\}, (\preccurlyeq)\}$

Заметим, что если $p, q \in L'$, то $p \star_{\mathcal{L}} q \in L'$ (так как $\varphi_{p((a))} \star \varphi_{q((a))} = \psi((a))$). Также ясно, что если $\sup_{L\{p,q\}} \in L'$ (или $\inf_{L\{p,q\}} \in L'$), то $p \star_{\mathcal{L}} q = p \star_{\{\mathcal{L}'\}} q$. Значит, $\mathcal{L}'$ также дистрибутивна. Построим «ДНФ»:

$$\varphi(a_1, ..., a_n) = \sum_{\text{Кн} \in \text{ДНФ}(\varphi)} \prod_{i \in \text{Кн}} a_i$$

Всего не больше 2^n возможных компонент и 2^{2^n} возможных формул $\varphi((a))$.

Q.E.D.

Теорема.

Если $\nvdash \alpha$ в ИИВ, то существует $\mathcal{G}$, что $\mathcal{G} \nvDash \alpha$, причем $|\mathcal{G}| \leq 2^{2^{|\alpha|+2}}$

Доказательство:
Используем полноту ИИВ относительно алгебр Гейтинга, если α где-то не доказуема, то существует алгебра Гейтинга $\mathcal{H}$, в которой α не истинна.

Рассмотрим подформулы α. Пусть $\varphi_1, ..., \varphi_n$ - все подформулы формулы α(включая саму alpha). Число подформул $n \leq |a|$. Пусть $\mathcal{G}$ - дистрибутивная подрешетка $\mathcal{H}$, построенная по $[\![\varphi_1]\!], ..., [\![\varphi_n]\!], 0$ и 1. Такая существует по лемме. $\mathcal{G}$ алгебра Гейтинга, и можно показать, что $\mathcal{G} \nvDash \alpha$. По лемме $|G| \leq 2^{2^{n+2}} \leq 2^{2^{|\alpha|+2}}$

Q.E.D.

Теорема. ИИВ разрешимо

Доказательство:
Теория разрешима, если существует эффективный алгоритм (программа), который за конечное время может определить, является ли любая заданная формула теоремой этой теории или нет.

Давайте по формуле α построем все возможные алгебры Гейтинга $\mathcal{G}$ размера не больше $2^{2^{|\alpha|+37}}$, если $\mathcal{G} \vDash \alpha$, то α.

Q.E.D.

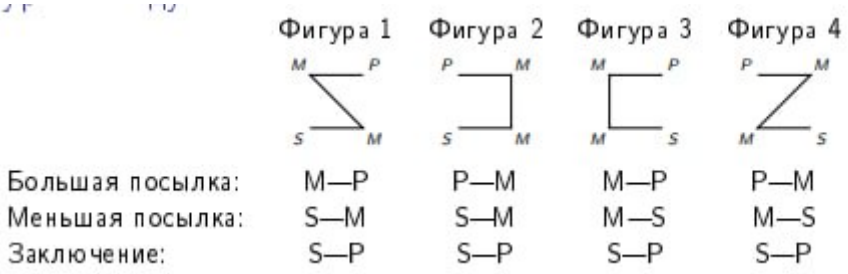
7. Категорические силлогизм и исчиление предикатов.

def: Категорический силлогизм — умозаключение, соединяющее три термина в двух посылках и заключении.

def: Термины:
- **Предикат** (больший термин, P) — термин, являющийся сказуемым в заключении.
- **Субъект** (меньший термин, S) — термин, являющийся подлежащим в заключении.
- **Средний термин** (M) — термин, присутствующий в обеих посылках, но отсутствующий в заключении.

def: Типы высказываний (соотношений):
- A (общеутвердительное): Все S суть P. Обозначение: SaP.
- I (частноутвердительное): Некоторые S суть P. Обозначение: SiP.
- E (общеотрицательное): Ни один S не есть P. Обозначение: SeP.
- O (частноотрицательное): Некоторые S не суть P. Обозначение: SoP.

def: Фигуры категорического силлогизма — расположение терминов в посылках:



def: Модус — комбинация типов высказываний (A, I, E, O) для большой посылки, малой посылки и заключения в определённой фигуре (например, AAA в фигуре 1).

def: Типы модусов:
- **Сильные** (правильные) — модусы, всегда дающие верное заключение при истинных посылках.
- **Слабые** — модусы, выводящие частное заключение, когда возможно общее (например, вывод SiP вместо SaP).
- **Неправильные** — модусы, не гарантирующие истинность заключения при истинных посылках.

def: Ограничения — дополнительные условия корректности для некоторых модусов (например, требование непустоты среднего термина M). Или например существования единорогов.

def: Исчисление предикатов — формальная система для выражения высказываний с учётом предикатов, кванторов, предметных переменных.

def:Язык исчисления предикатов включает:
- Предметные выражения (термы):
  - Предметные переменные (x, y, ...).
  - Функциональные символы (f, g, ...), включая константы (0, 1, ...).
- Логические выражения (формулы):
  - Предикатные символы (P, Q, ...), включая пропозициональные переменные.
  - Логические связки: $\wedge$, $\vee$, $\rightarrow$, $\neg$.
  - Кванторы: $\forall$ (всеобщность), $\exists$ (существование).

def: Метаязык — язык, на котором говорят об объектном языке (исчислении предикатов), использует метапеременные для формул, термов и т.д.

def: Вхождение подформулы в формулу — позиция первого символа этой подформулы в формуле.

def: Свободное вхождение переменной — вхождение переменной x в формулу φ, которое не находится в области действия квантора по x.

def: Множество свободных переменных FV(φ) — множество всех переменных, имеющих свободные вхождения в φ.

def: Подстановка терма θ вместо переменной x в формулу φ (φ[x:=θ]) — замена всех свободных вхождений x в φ на θ.

def: Свобода для подстановки — терм θ свободен для подстановки вместо x в φ, если после подстановки никакая переменная из θ не становится связанной в φ.

def: Аксиоматика исчисления предикатов:
- Схемы аксиом (1)-(10) классического исчисления высказываний.
- (∀x.φ) → φ[x:=θ] (при условии, что θ свободен для подстановки вместо x в φ).
- φ[x:=θ] → ∃x.φ (при том же условии).
- Правила вывода:
  - Modus Ponens (M.P.): Из φ и φ→ψ выводимо ψ.
  - Правило для ∀: Если ⊢ φ→ψ, то ⊢ φ→∀x.ψ (при условии, что x не входит свободно в φ).
  - Правило для ∃: Если ⊢ ψ→φ, то ⊢ ∃x.ψ→φ (при том же условии).

todo: доказательства свойств силлогизмов.

8. Теория моделей и теоремы исчисления предикатов

def: **Оценка**: Упорядоченная четвёрка ⟨D, F, P, E⟩, где:

- D — предметное множество — непустое множество объектов (D $\neq \emptyset$), из которого берутся значения для предметных переменных.
- F — интерпретация функциональных символов. то $F_{f_n} : D^n \to D$.
- P — интерпретация предикатных символов. $P_{T_n} : D^n \to V$, где V = {И, Л}.
- E — оценка предметных переменных. E(x) ∈ D для любой переменной x.

def: Формула φ **общезначима**, если она истинна при любой оценке (при любых D, F, P, E).

def: Формула φ является **логическим следствием множества** формул Г, если φ истинна во всех моделях, в которых истинны все формулы из Г.

Теорема. о дедукции в ИП

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:

$(\Rightarrow)$ — как в КИВ $(\Rightarrow)$ — та же схема, два новых случая.

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

Дополним: обоснуем $\alpha \to \delta_n$, если предыдущие уже обоснованы.

Два новых похожих случая: правила для $\forall$ и $\exists$. Рассмотрим $\forall$.

Доказываем (n) $\alpha \to \psi \to \forall x \varphi$ (правило для $\forall$), значит, доказано

(k) $\alpha \to \psi \to \varphi$.

$(n-0.9)$ $(\alpha \to \psi \to \varphi) \to (\alpha \wedge \psi) \to \varphi$ Т. о полноте КИВ

$(n-0.6)$ $(\alpha \wedge \psi) \to \varphi$ М.Р. $k, n-0.8$

$(n-0.4)$ $(\alpha \wedge \psi) \to \forall x.\varphi$ Правило для $\forall$, $n-0.6$

$(n-0.3)$ $((\alpha \wedge \psi) \to \forall x.\varphi) \to (\alpha \to \psi \to \forall x.\varphi)$ Т. о полноте КИВ

(n) $\alpha \to \psi \to \forall x.\varphi$ М.Р. $n-0.4, n-0.2$

Q.E.D.

Теорема. Корректность подстановки

Если θ свободен для подстановки вместо x в φ, то $[\![\varphi]\!]^{x:=[\![\theta]\!]} = [\![\varphi[x := \theta]]\!]$

Доказательство:

Будем делать индукцией по структуре φ.

База: φ не имеет кванторов - очевидно

Индукционный переход: пусть справедливо для φ. Покажем для $\varphi = \forall y.\psi$

- $x = y$ либо $x \notin FV(\psi)$. Тогда: $[\![\forall y.\psi]\!]^{x:=[\![\theta]\!]} = [\![y.\psi]\!] = [\![(\forall y.\psi)[x := \theta]]\!]$
- $x \neq y$. Тогда

$$[\![\forall y.\psi]\!]^{x=[\![\theta]\!]} = [\![\psi]\!]^{y\in D, x:=[\![\theta]\!]} \overset{1}{=} [\![\psi]\!]^{x:=[\![\theta]\!], y\in D} \overset{2}{=} [\![\psi[x := \theta]]\!]^{y\in D} = [\![(\forall y.\psi)[x := \theta]]\!]$$

Q.E.D.

Теорема. Корректность исчисления предикатов
Если $\Gamma \vdash \alpha$ и в доказательстве не используются кванторы по свободным переменным из $FV(\Gamma)$, то $\Gamma \models \alpha$

Доказательство:
Фиксируем D, F, P. Делаем индукцию по длине доказательства α: при любом E выполнено $\Gamma \models \alpha$ при длине доказательства n, покажем для $n+1$.

Здесь просто аккуратно пользуемся прошлой теоремой.

Q.E.D.

9. Теорема о полноте ИП. Начало

def: Г - **непротиворечивое множество формул**,если $\Gamma \nvdash \alpha \& \neg\alpha$, для любого α

def: Г - **полное непротиворечивое множество замкнутых бесквантворных формул**, если:

- Г содержить только замкнутые бесквантворные формулы
- если α - некоторая замкнутая бесквантворная формула, то либо $\alpha \in \Gamma$, либо $\neg\alpha \in \Gamma$

def: Г - **полное непротиворечивое множество замкнутых формул**, если:

- Г содержить только замкнутые формулы
- если α - некоторая замкнутая формула, то либо $\alpha \in \Gamma$, либо $\neg\alpha \in \Gamma$

Лемма.
Пусть Г непротиворичивое множество замкнутых (бесквантворных) формул. Тогда какова бы не была замкнутая (бесквантворная) формула φ, хотя бы $\Gamma \cup \{\varphi\}$ или $\Gamma \cup \{\neg\varphi\}$ непротиворечиво.

Доказательство:
Из непротиворечивости Г следует, что непротиворечиво хотя бы одно из $\Gamma \cup \{\varphi\}$ или $\Gamma \cup \{\neg\varphi\}$. Если бы оба были противоречивы, то из Г выводилось бы как $\varphi \to (A \wedge \neg A)$, так и $\neg\varphi \to (A \wedge \neg A)$. По законам логики из этого следовало бы, что $\Gamma \vdash A \wedge \neg A$, что противоречит непротиворечивости Г

Q.E.D.

Теорема о пополнении.
Пусть Г — непротиворечивое множество замкнутых (бесквантворных) формул. Тогда найдётся **полное непротиворечивое множество** замкнутых (бесквантворных) формул Δ, такое что $\Gamma \subseteq \Delta$.

Доказательство:

1. Занумеруем все замкнутые (бесквантворные) формулы сигнатуры (их счётное количество): $\varphi_1, \varphi_2, \ldots$
2. Построим последовательность расширяющихся множеств $\{\Gamma_i\}$ индуктивно:
   - $\Gamma_0 = \Gamma$.
   - $\Gamma_{i+1} = \Gamma_i \cup \{\varphi_i\}$, если это множество непротиворечиво. В противном случае $\Gamma_{i+1} = \Gamma_i \cup \{\neg\varphi_i\}$. (это верно из леммы)
3. Положим $\Delta = \cup_i \Gamma_i$.
4. **Докажем, что Δ непротиворечиво.** Предположим противное: $\Delta \vdash \alpha \wedge \neg\alpha$. Доказательство имеет конечную длину и использует конечное число гипотез $\{\delta_1, \ldots, \delta_n\} \subseteq \Delta$. Пусть каждая δ_i принадлежит $\Gamma(d_i)$. *Тогда все они содержатся в* $\Gamma(\mathrm{m})$, где $\mathrm{m} = \max(d_1, \ldots, d_n)$. Следовательно, $\Gamma(m) \vdash \alpha \wedge \neg\alpha$, *что противоречит построению* $\Gamma(\mathrm{m})$ как непротиворечивого множества.

Q.E.D.

def: Моделью для множества формул F назовем такую модель $\mathcal{M}$, что при всяком $\varphi \in F$ выполнено $[\![\varphi]\!]_{\mathcal{M}} = \text{И}$

Теорема.
Любое непротиворечивое множество замкнтуых формул имеет модель.

Доказательство:
Построим. Пусть M - полное непротиворечивое монжество замкнутых бесквантворных формул. Тогда модель $\mathcal{M}$ задается так:

1. D – множество всевозможных предметных выражений без предметных переменных.
2. $[\![f(\theta_1, ..., \theta_n)]\!] = \text{"f("} + [\![\theta_1]\!] + \text{","} + ... + \text{","} + [\![\theta_n]\!] + \text{")"}$
3. $[\![P(\theta_1, ..., \theta_n)]\!] =$ И, если $P(\theta_0, ..., \theta_n) \in M$
4. Так как $D \neq \emptyset$, то найдется $z \in D$. Тогда $[\![x]\!] = z$. Это ничему не помешает, так как формулы замкнуты

Лемма: Покажем, что $\mathcal{M} \vDash \varphi$, тогда и только тогда, когда $\varphi \in M$

Доказательство: Индукция по длине формулы φ:

База: предикат

ИП: Нам надо показать, что если $\mathcal{M} \vDash \alpha \star \beta \Leftrightarrow \alpha \star \beta \in M$. Это делается просто переборои оценок α и β

Концовка

Пусть M — непротиворечивое множество замкнутых бесквантворных формул.

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

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

Q.E.D.

10. Теорема о полноте ИП, продолжение

def: Формула φ имеет **поверхностные кванторы** (находится в предваренной форме), если

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

где τ – формула без кванторов. То есть: $\forall x \exists y \exists z \forall t : \tau$

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

def: Сколемизация: TODO ?????

Теорема. Теорема Геделя о полноте исчисления предикатов
Если M замкнутое непротиворечивое множество формул, то оно имеет модель

Доказательство:
Построи по M множество с поверхностными кванторами. По M' построим непротиворечивое множество замкнутых бескванторных, дополним его до полного, построим для него модель. Тадам

Q.E.D.

Следствие (теорема о полноте).
Исчисление предикатов полно

Доказательство:
Доказательство от противного.

Q.E.D.

11. Машина Тьюринга.

def: Машина Тьюринга — система, задаваемая:

- Внешним алфавитом: конечный набор символов q_1, ..., q_n, включая выделенный символ-заполнитель q_ε.
- Внутренний алфавит (состояний): конечный набор состояний s_1, ..., s_k, включая:
  - s_s — начальное состояние,
  - s_f — допускающее состояние,
  - s_r — отвергающее состояние.
- Таблица переходов: функция, которая для каждой пары (текущее состояние s, текущий символ q) задаёт тройку (новое состояние s', символ для записи q', направление движения головки {←, →, ·}).

def: Язык — произвольное множество конечных слов (строк) над некоторым конечным алфавитом.

def: Разрешимый язык: Язык L называется разрешимым, если существует машина Тьюринга, которая для любого входного слова w:

- Останавливается в допускающем состоянии (s_f), если $w \in L$.
- Останавливается в отвергающем состоянии (s_r), если $w \notin L$.
- Такая машина называется **разрешающей для языка L**.

def: Задача об останове (проблема останова): Задача определения по описанию машины Тьюринга M и входному слову w, остановится ли машина M на входе w.

Теорема о неразрешимости задачи об останове.
Язык останавливающихся машин тьюринга неразрешим

Доказательство:

Схема доказательства (от противного): Предположим, существует разрешающая машина S, которая определяет, остановится ли машина x на входе y. Построим машину W, которая на входе x делает следующее:

1. Запускает S на паре (x, x) (т.е. спрашивает, остановится ли x на своём собственном коде).
2. Если S отвечает «да» (остановится), то W уходит в бесконечный цикл.
3. Если S отвечает «нет» (не остановится), то W останавливается и возвращает 1.

Если теперь подать код W на вход самой W, то получим противоречие: S(W, W) должна быть истинна тогда и только тогда, когда она ложна.

Q.E.D.

Теорема.
Язык всех доказуемых формул исчисления предикатов неразрешим

Доказательство:

Пусть существует машина Тьюринга, разрешающая любую формулу. На ее основе тогда несложно построить некоторую машину Тьюринга, перестраивающую любую машину S (с допускающим состоянием s_f и входом y) в ее ограничения C и разрешаю формулу ИП $C \to \exists w_l . \exists . w . r . F_{S_y}(w_l, w_r, s_f)$. Эта машина разрешит задачу останова, а такого не может быть

Todo:

Q.E.D.

12. Аксиоматика Пеано, Арифметизация

def: Представление чисел через натуральные

- **Целые** $Z = \{\langle x, y\rangle \mid x, y \in \mathrm{N}0\}$ Интуиция: $\langle x, y\rangle = x - y$ $\langle a, b\rangle + \langle c, d\rangle = \langle a + c, b + d\rangle$ $\langle a, b\rangle - \langle c, d\rangle = \langle a + d, b + c\rangle$ Пусть $\langle a, b\rangle \equiv \langle c, d\rangle$, если $a + d = b + c$. Тогда $\mathrm{Z} = Z/\equiv$ $0 = [\langle 0, 0\rangle]$, $1 = [\langle 1, 0\rangle]$, $-7 = [\langle 0, 7\rangle]$
- **Рациональные** $Q = \mathrm{Z} \times \mathrm{N}$ — множество всех простых дробей. $\langle p, q\rangle$ — то же, что p/q $\langle p1, q1\rangle \equiv \langle p2, q2\rangle$, если $p1q2 = p2q1$ $\mathrm{Q} = Q/\equiv$
- **Вещественные** $X = \{A, B\}$, где $A, B \subseteq \mathrm{Q}$ — дедекиндово сечение, если: (a) $A \cup B = \mathrm{Q}$ (b) Если $a \in A$, $x \in \mathrm{Q}$ и $x \leq a$, то $x \in A$ (c) Если $b \in B$, $x \in \mathrm{Q}$ и $b \leq x$, то $x \in B$ (d) A не содержит наибольшего. R — множество всех возможных дедекиндовых сечений. $\sqrt{2} = \{\{x \in \mathrm{Q} \mid x < 0 \vee x\text{^}2 < 2\}, \{x \in \mathrm{Q} \mid x > 0 \;\&\; x\text{^}2 > 2\}\}$

def: Аксиоматика Пеано N (более точно,$\langle N,0,(')\rangle$) соответствует **аксиоматике Пеано**, если следующее определено/выполнено:

- 1. Операция «**штрих**» $(') : N \longrightarrow N$, причём нет $a, b \in N$, что $a' = b$, 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») $P : N \longrightarrow V$, если:(a) $P(0)$(b) При любом $x \in N$ из $P(x)$ следует $P(x')$ то при любом $x \in N$ выполнено $P(x)$.

Как построить? Например, в стиле алгебры Линденбаума:
1. N — язык, порождённый грамматикой $\nu ::= 0 \mid \nu$«'»
2. 0 — это «0», x' — это x + «'»

def: Арифметические операции (возведение в степень) в аксиоматике Пеано.

- **рабы:** $1 = 0'$, $2 = 0''$, $3 = 0'''$
- **сложение:** $a + b = \{a$, если $b = 0 \mid (a + c)'$, если $b = c'$
- **умножение:** $a \cdot b = \{0$, если $b = 0 \mid a \cdot c + a$, если $b = c'$
- **возведение в степень:** **a^b** =

def: Доказательство **коммутативности сложения**.

def: Порядок теории (0, 1, 2).

def: Теорией первого порядка назовём исчисление предикатов с дополнительными («нелогическими» или «математическими»):

• предикатными и функциональными символами;

• аксиомами.

Сущности, взятые из исходного исчисления предикатов, назовём логическими

def: Формальная арифметика — теория первого порядка, со следующими добавленными нелогическими...

• двухместными функциональными символами (+), (·); одноместным функциональным символом (′), нульместным функциональным символом 0;

• двухместным предикатным символом (=);

• восемью нелогическими аксиомами:

(A1) $a = b \longrightarrow a = c \longrightarrow b = c$

(A2) $a = b \longrightarrow a' = b'$

(A3) $a' = b' \longrightarrow a = b$

(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 $\psi[x := 0] \ \& \ (\forall x.\psi \longrightarrow \psi[x := x']) \longrightarrow \psi$ с метапеременными x и ψ.

def: Доказательство **a** = **a**.

Пусть $\top ::= 0 = 0 \longrightarrow 0 = 0 \longrightarrow 0 = 0$, тогда:

(1) $a = b \longrightarrow a = c \longrightarrow b = c$ (Акс. A1)

(2) $(a = b \longrightarrow a = c \longrightarrow b = c) \longrightarrow \top \longrightarrow (a = b \longrightarrow a = c \longrightarrow b = c)$ (Сх. акс. 1)

(3) $\top \longrightarrow (a = b \longrightarrow a = c \longrightarrow b = c)$ (M.P. 1, 2)

(4) $\top \longrightarrow (\forall c.a = b \longrightarrow a = c \longrightarrow b = c)$ (Введ. ∀)

(5) $\top \longrightarrow (\forall b.\forall c.a = b \longrightarrow a = c \longrightarrow b = c)$ (Введ. ∀)

(6) $\top \longrightarrow (\forall a.\forall b.\forall c.a = b \longrightarrow a = c \longrightarrow b = c)$ (Введ. ∀)

(7) $\top$ (Сх. акс 1)

(8) $(\forall a.\forall b.\forall c.a = b \longrightarrow a = c \longrightarrow b = c)$ (M.P. 7, 6)

(9) $(\forall a.\forall b.\forall c.a = b \longrightarrow a = c \longrightarrow b = c) \longrightarrow (\forall b.\forall c.a + 0 = b \longrightarrow a + 0 = c \longrightarrow b = c)$ (Сх. акс. 11)

(10) $\forall b.\forall c.a + 0 = b \longrightarrow a + 0 = c \longrightarrow b = c$ (M.P. 8, 9)

(12) $\forall c.a + 0 = a \longrightarrow a + 0 = c \longrightarrow a = c$ (M.P. 10, 11)

(14) $a + 0 = a \longrightarrow a + 0 = a \longrightarrow a = a$ (M.P. 12, 13)

(15) $a + 0 = a$ (Акс. A5)

(16) $a + 0 = a \longrightarrow a = a$ (M.P. 15, 14)

(17) $a = a$ (M.P. 15, 16)

def: **Арифметизация математики**, формализация категорических силлогизмов, предложенная Лейбницем.

• Любой термин — пара взаимно простых чисел $+a - b$. Например, мудрый — $+70 - 33$,благочестивый — $+10 - 3$.

• Общеутвердительное предложение (каждый $+a - b$ есть $+c - d$): $a : c$ и $b : d$. Всякий мудрый есть благочестивый ($70 = 10 \cdot 7$, $33 = 3 \cdot 11$). • Частноотрицательное предложение — не верно общеутвердительное.

• Общеотрицательное предложение — когда a, d или b, c имеют общий делитель, отличный от 1: Ни один благочестивый (+10−3) не есть несчастный (+5−14), так как $10 = 2{\cdot}5$ и $14 = 2{\cdot}7$.

13. Функции

def: Базовые примитивы (исходные функции):
- Ноль (Z): Z(x) = 0.
- Инкремент (N): N(x) = x+1.
- Проекция (U): $U_n^k(x_1, ..., x_n) = x_k$(возвращает k-й аргумент).
- Подстановка (S): Если g — функция от k аргументов, а f_1, ..., f_k — функции от n аргументов, то

$$S\langle g, f_1, ..., f_k\rangle(x) = g(f_1(x), ..., f_k(x))$$

def: Примитивная рекурсия. Если f — функция от n аргументов, а g — функция от n+2 аргументов, то функция h = R⟨f, g⟩ от n+1 аргумента определяется так:
- h(x, 0) = f(x)
- h(x, y+1) = g(x, y, h(x, y))

def: Примитивно-рекурсивная функция — функция, которую можно получить из базовых примитивов (Z, N, U) с помощью конечного числа применений операций подстановки (S) и примитивной рекурсии (R).

def: Операция минимизации (M): Если f — функция от n+1 аргумента, то $M\langle f\rangle(x) = \min\{y \mid f(x, y) = 0\}$, при условии, что такое y существует. Если для всех y значение $f(x, y) > 0$, то M⟨f⟩(x) не определено.

def: Общерекурсивная функция — Функция, которую можно получить из базовых примитивов с помощью конечного числа применений операций подстановки (S), примитивной рекурсии (R) и минимизации (M).

Лемма.
Функция Аккермана не выражена в примитивно рекурсивных.

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

Доказательство:
Для этого докажем немного другую теорему.

Q.E.D.

Теорема.
Пусть $f(x)$ - примитивно рекурсивная. Тогда найдется k, что $f(x) < A(k, \max(x))$

Доказательство:
Индукция по структуре f.

Q.E.D.

def: Будем говорить, что отношение $R \subseteq \mathbb{N}_0^n$ **выразимо в ФА**, если существует формула ρ, что:
- если $\langle a_1, ..., a_n\rangle \in R$, то $\vdash \rho(a_1, ..., a_n)$
- если $\langle a_1, ..., a_n\rangle \in .\neg R$, то $\vdash \neg\rho(a_1, ..., a_n)$

Теорема.
Отношение «равно» выразимо в Ф.а.: $r = \{\langle x, x\rangle \mid x \in \mathbb{N}_0\}$

def: Будем говорить, что функция $f : \mathbb{N}_0^n \to \mathbb{N}_0$ **представима в ФА**, если существует формула φ, что:
- если $f(a_1, ..., a_n) = u$, то $\vdash \varphi(a_1, ..., a_n, u)$

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

def: Для отношения R его **характеристическая функция** χ_R возвращает 1, если аргумент принадлежит R, и 0 иначе. Отношение выразимо тогда и только тогда, когда представима его характеристическая функция.

14. Представимость примитивов, бета функции

def: Представимость базовых примитивов:

- Функция ноль (Z): Z(x) = 0. Представима формулой ζ(x, y) := (x = x) ∧ (y = 0).
- Функция следования (N): N(x) = x + 1. Представима формулой ν(x, y) := y = x'.
- Функция проекции (U_n^k): $U_n^k(x_1, ..., x_n) = x_k$. Представима формулой $\upsilon(x_1, ..., x_n, y) := y = x_k$
- Операция подстановки: Если функции $g(y_1, ..., y_m)$ и $h_1(x), ..., h_m(x)$ представимы формулами γ и $\eta_1, ..., \eta_m$ соответственно, то функция $f(x) = g(h_1(x), ..., h_m(x))$ представима формулой:

$$\varphi(x, y) := \exists z_1 ... \exists z_m (\gamma(z_1, ..., z_m, y) \wedge \eta_1(x, z_1) \wedge ... \wedge \eta_m(x, z_m))$$

def: β-функция Гёделя: β(b, c, i) = остаток от деления b на (1 + c·(i + 1)).

Теорема Если $a_0, ..., a_n \in N_0$, то найдутся такие $b, c \in N_0$, что $a_i = \beta(b, c, i)$

Теорема. Примитив $R\langle f, g\rangle$ представим в Ф.А. формулой $\rho(x1, \ldots, xn, y, a)$:

$$\exists b. \exists c. (\exists a_0. \beta(b, c, 0, a_0) \phi(x_1, ...x_n, a_0)) \forall k. k < y \to \exists d. \exists e. \beta(b, c, k, d) \beta(b, c, k', e) \gamma(x_1, ..x_n, k, d, e) \beta^{b,c,y,a}$$

Теорема. Пусть функция $f : N_0^{n+1} \to N_0$ представима в Ф.А. формулой $\phi(x_1, ..., x_n, y, r)$. Тогда примитив $M\langle f \rangle$ представим в Ф.А. формулой:

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

Теорема. Если f — рекурсивная функция, то она представима в Ф.А. Индукция по структуре f.

15. Геделева нумерация. Начало пиздеца

def: Рекурсивность представимых в Ф.А. функций

Фиксируем f и $x_1, x_2, ..., x_n$. Обозначим $y = f(x_1, x_2, ..., x_n)$. По представимости нам известна:

ϕ, что $\vdash \phi(x_1, x_2, ..., x_n, y)$.

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 $\vdash \phi(x1, x2, \ldots, xn, y)$.

Теорема.

Следующая функция рекурсивна:

$$\text{proof}(f, x_1, x_2, .., x_n, y, p) = \begin{cases} 1, \text{если p - геделев номер доказательства} \\ 0, \text{иначе} \end{cases}$$

def: Пусть ξ — формула с единственной свободной переменной *x*1. Тогда: $\langle \ulcorner \xi \urcorner, p \rangle \in W_1$, если $\vdash \xi(\ulcorner \xi \urcorner)$и p — номер доказательства

def: Отношение W_1 рекурсивно, поэтому выражено в Ф.А. формулой ω_1 со свободными переменными x_1 и x_2, причём:
1. $\vdash \omega_1(\ulcorner \phi \urcorner, p)$, если p — гёделев номер доказательства самоприменения ϕ;
2. $\vdash \neg\omega_1(\ulcorner \phi \urcorner, p)$ иначе.

Todo: W_2, w_2 - что за ферзь?

16. Теоремы Геделя и пиздец больного ублюдка

def: Теория называется **ω-непротиворечивой**, если для любой формулы $\varphi(x)$ из того, что доказуемы $\varphi(0)$, $\varphi(1)$, $\varphi(2)$, ... (т.е. $\varphi(n)$ для всех натуральных n), следует, что не доказуемо $\exists x.\neg\varphi(x)$.

def: Определим формулу $\sigma(x_1) := \forall p.\neg\omega_1(x_1, p)$.

Первая теорема Гёделя о неполноте арифметики.
- Если формальная арифметика непротиворечива $\nvdash \sigma(\ulcorner\sigma\urcorner)$
- Если формальная арифметика ω-непротиворечива $\nvdash \neg\sigma(\ulcorner\sigma\urcorner)$

Доказательство:
Напомним $\sigma(x_1) := \forall p.\neg w_1(x_1, p)$

1. Пусть $\vdash \sigma(\ulcorner\sigma\urcorner)$. Тогда есть p - номер доказательства, тогда $\vdash w_1(\ulcorner\sigma\urcorner, p)$. Тогда $\vdash \exists p.w_1(\ulcorner\sigma\urcorner, p)$, тогда $\vdash \neg\sigma(\ulcorner\sigma\urcorner)$. Противоречие
2. Пусть $\vdash \sigma(\ulcorner\sigma\urcorner)$. То есть $\exists p.w_1(\ulcorner\sigma\urcorner, p)$
   - Но найдется ли натуральное число p, что $\vdash w_1(\ulcorner\sigma\urcorner, p)$? Пусть нет. Тогда по w-непротиворечивости $\nvdash \exists p.\neg\neg w_1(\ulcorner\sigma\urcorner, p)$. То есть p доказательство самоприменения: $\vdash \omega(\ulcorner\sigma\urcorner)$. Противоречие

   TODO: что что что?

Q.E.D.

def: Теория называется **синтаксически полной**, если для любой замкнутой формулы α этой теории верно либо $\vdash \alpha$, либо $\vdash \neg\alpha$.

def: Теория называется **семантически полной** (относительно своей стандартной модели), если любая формула, истинная в стандартной модели, доказуема в теории.

Теорема.
Формальная арифметика (при условии её непротиворечивости) не является ни синтаксически, ни семантически полной. Существуют формулы, которые неразрешимы (не доказуемы и не опровержимы), и существуют истинные в стандартной модели формулы, которые недоказуемы.

Доказательство:
Рассмотрим Ф.А. с классической моделью. Из теоремы Гёделя имеем $\nvdash \sigma(\ulcorner\sigma\urcorner)$. Рассмотрим $\sigma(\ulcorner\sigma\urcorner) \equiv \forall p.\neg\omega_1(\ulcorner\sigma\urcorner, p)$: нет числа p, что p — номер доказательства $\sigma(\ulcorner\sigma\urcorner)$. То есть, $[\![\forall p.\neg w_1(\ulcorner\sigma\urcorner, p)]\!]$. То есть $\vDash \sigma(\ulcorner\sigma\urcorner)$

Q.E.D.

def: Пусть $\langle\ulcorner\xi\urcorner\rangle \in W_2$, если $\vdash \neg\xi(\ulcorner\xi\urcorner)$ и p номер доказательства. Пусть w_2 выражает W_2 в формальной арифметике.

Первая теорема Геделя в форме Россера.
Рассмотрим $p(x) = \forall p.w_1(x_1, p) \to \exists q.q \le p \& w_2(x_2 q)$. Тогда $\nvdash p(\ulcorner p\urcorner)$ и $\nvdash \neg p(\ulcorner p\urcorner)$. Неформальный смысл: «Меня легче опровергнуть, чем доказать»

def: Теория первого порядка, использующая нелогические функциональные символы 0, $(+)$ и $(c\,\cdot)$, нелогический предикатный символ $(=)$ и следующие нелогические аксиомы, называется **системой Робинсона**.

$$a = a \qquad a = b \to b = a$$
$$a = b \to b = c \to a = c \qquad a = b \to a' = b'$$
$$a' = b' \to a = b \qquad \neg 0 = a'$$
$$a = b \to a + c = b + c \& c + a = c + b \qquad a = b \to a \cdot c = b \cdot c \& c \cdot a = c \cdot b$$
$$\neg a = 0 \to \exists b.a = b' \qquad a + 0 = a$$
$$a + b' = (a + b)' \qquad a \cdot 0 = 0$$
$$a \cdot b' = a \cdot b + a$$

Система Робинсона неполна: аксиомы — в точности утверждения, необходимые для доказательства теорем Гёделя. Система Робинсона не имеет схем аксиом.

def: Теория первого порядка, использующая нелогические функциональные символы 0, 1, $(+)$, нелогический предикатный символ $(=)$ и следующие нелогические аксиомы, называется **арифметикой Пресбургера**.

$$\neg(0 = x + 1)$$
$$x + 1 = y + 1 \to x = y$$
$$x + 0 = x$$
$$x + (y + 1) = (x + y) + 1$$
$$(\varphi(0) \& \forall x.\varphi(x) \to \varphi(x + 1)) \to \forall y.\varphi(y)$$

Теорема. Арифметика Пресбургера разрешима и синтаксически и семантически полна.

17. Продолжение теорем Геделя

def: Обозначим за $\varphi(x, p)$, выражающую в формальной арифметике рекурсивное отношение Proof. Обозначис за $\pi(x) = \exists p.\varphi(x, p)$. (идейно, формула доказуема:?)

def: Consis $\neg\pi(\ulcorner 1 = 0 \urcorner)$

Неформальный смысл: формальная арифметика нерпотиворечива

Вторая теорема Геделя о неполноте арифметики.
Если Consis доказуем, то формальная арифметика противоречива

Доказательство:

Если Consis доказуем, то если мы покажем, что $\vdash \text{Consis} \to \sigma(\ulcorner \sigma \urcorner)$, то из первой теоремы мы проиграем.

Рассмотрим особый Consis':

$$\pi'(x) = \exists p.\varphi(x, p) \& \neg\varphi(\ulcorner 1 = 0 \urcorner, p)$$

$$\text{Consis}' = \neg\pi'(\ulcorner 1 = 0 \urcorner)$$

Если ФА непротиворечива, то $[\![\pi'(x) = \pi(x)]\!]$

TODO:

TODO:

TODO:

TODO:

TODO:

TODO:

Q.E.D.

def: Условия выводимости Гильберта-Бернайса-Лёба

Будем говорить, что формула ψ, выражающая отношение Proof, формула π и формула Consis соответствуют условиям Гильберта-Бернайса-Лёба, если следующие условия выполнены для любой формулы α:
1. $\vdash \alpha$ влечет $\vdash \pi(\ulcorner \alpha \urcorner)$
2. $\vdash \pi(\ulcorner \alpha \urcorner) \longrightarrow \pi(\ulcorner \pi(\ulcorner \alpha \urcorner) \urcorner)$
3. $\vdash \pi(\ulcorner \alpha \longrightarrow \beta \urcorner) \longrightarrow \pi(\ulcorner \alpha \urcorner) \longrightarrow \pi(\ulcorner \beta \urcorner)$

def: Лемма об автоссылках.

Для любой формулы $\varphi(x_1)$ можно построить такую замкнутую формулу α (не использующую неаксиоматических предикатных и функциональных символов), что $\vdash \varphi(\ulcorner \alpha \urcorner) \leftrightarrow \alpha$

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

Доказательство:

Рассмотрим $\Phi(x_1) = \neg\pi(x_1)$. Тогда по Лемме об автоссылках существует γ, что $\vdash \gamma \leftrightarrow \neg\pi(\ulcorner \gamma \urcorner)$

- Предположим, что $\vdash \gamma$. Тогда по вышесказанному $\nvdash \gamma$

- Предположим, что $\vdash \neg\gamma$. Тогда $\vdash \pi(\ulcorner\gamma\urcorner)$, то есть $\vdash \exists p.\psi(\ulcorner\gamma\urcorner, p)$. Тогда по w-непротиворечивости найдется p, что $\vdash \varphi(\ulcorner\gamma\urcorner, p)$, то есть $\vdash \gamma$

Q.E.D.

def: Теория $\mathcal{S}$ - расширение теории $\mathcal{T}$, если из $\underset{\mathcal{T}}{\vdash} \alpha$ следует $\underset{\mathcal{S}}{\vdash} \alpha$

def: Теория $\mathcal{S}$ - рекурсивно-аксиоматизируемая, если найдется $\mathcal{S}'$ с тем же языком, что
- $\underset{S}{\vdash} \alpha$ тогда и только тогда когда $\underset{S'}{\vdash} \alpha$
- Множество аксиом S' рекурсивно (????)

def: $Th_S = \left\{\ulcorner\alpha\urcorner \underset{S}{\vdash} \alpha\right\}$, $Tr_S = \{\ulcorner\alpha\urcorner \mid [\![\alpha]\!]_S = \text{И}\}$, то есть множество доказуемых и общезначимых в теории

тут скипнуто 2 леммы, нужны ли они

Теорема. Теорема о неразрешимость формальной арифметики
Если формальная арифметика непротиворечива, то формальная арифметика неразрешима

Доказательство:
Пусть формальная арифметика разрешима, откуда есть рекурсивная функция $f(x) : f(x) = 1$ тогда и только тогда, когда $x \in Th_{\text{Ф.А}}$. То есть $Th_{\text{Ф.А}}$ выразимо в формальной арифметике.

Q.E.D.

Теорема Тарского о невыразимости истины.
Не существует $\varphi(x)$, что $[\![\varphi(x)]\!] = \text{И}$(в стандартной интерпретации) тогда и только тогда, когда $x \in Tr_{\text{Ф.А}}$

Доказательство:
Пусть теория S - формальная арифметика + аксиомы: все истинные в стандартной интерпритации формулы. Очевидно, что $Th_S = Tr_S = Tr_{\text{Ф.А}}$. То есть $Tr_{\text{Ф.А}}$ невыразимо в S

Пусть φ таково, что $[\![\varphi(x)]\!] = \text{И}$ при $x \in Tr$. Тогда $\vdash \varphi(x)$, если $x \in Tr$ и $\vdash \neg\varphi(x)$, если $x \notin Tr$, тогда Tr выразимо в S противоречие

todo

Q.E.D.

18. Множества.

def: Определения равенства

- Два множества равны, если они содержат одни и те же элементы (аксиома экстенсиональности).
- Формально: $A = B \iff \forall x(x \in A \leftrightarrow x \in B)A = B \iff \forall x(x \in A \leftrightarrow x \in B)$

def: Аксиоматика Цермело–Френкеля (ZF)

- **Равенство «по Лейбницу»**: объекты равны, если неразличимы. Если нечто ходит как утка, выглядит как утка и крякает как утка, то это утка.
- **Принцип объёмности:** объекты равны, если состоят из одинаковых частей.

$$A \subseteq B \equiv \forall x.x \in A \to x \in BA = B \equiv A \subseteq BB \subseteq A$$

- **Аксиома равенства**: равные множества содержатся в одних и тех же множествах.

$$\forall x.\forall y.\forall z.x = yx \in z \to y \in z$$

- **Аксиома пустого**. Существует пустое множество $\emptyset.\exists s.\forall t.\neg t \in s$
- **Аксиома пары**. Существует $\{a, b\}$. Каковы бы ни были два множества a и b, существует множество, состоящее в точности из них.

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

- **Аксиома объединения**: существует $\cup x$. Для любого непустого множества x найдется такое множество, состоящее в точности из тех элементов, из которых состоят элементы x.

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

- **Аксиома степени**: существует $\mathcal{P}(x)$. Каково бы ни было множество x, существует множество, содержащее в точности все возможные подмножества множества x.

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

- **Схема аксиом выделения**: существует $\{t \in x \mid \phi(t)\}$. Для любого множества x и любой формулы от одного аргумента $\phi(y)$ (b не входит свободно в ϕ), найдется b, в которое входят те и только те элементы из множества x, что $\phi(y)$ истинно.

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

def: Упорядоченной парой двух множеств a и b назовём $\{\{a\}, \{a, b\}\}$, или $\langle a, b\rangle$

Теорема.
Упорядоченную пару можно построить для любых множеств.

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

Q.E.D.

def: Типы порядка

- Частичный порядок – рефлексивное, антисимметричное, транзитивное отношение.
- Линейный порядок – частичный порядок, в котором любые два элемента сравнимы.
- Полный (тотальный) порядок – обычно синоним линейного порядка; иногда требует, чтобы каждое подмножество имело наименьший элемент (более сильное условие).

def: Аксиома бесконечности

Инкремент: $x' \equiv x \cup \{x\}$

Аксиома бесконечности. Существует $N: \varnothing \in N \,\&\, \forall x. x \in N \longrightarrow x' \in N$ В N есть всевозможные множества вида $\varnothing$,{$\varnothing$},{$\varnothing$, {$\varnothing$}}, {$\varnothing$, {$\varnothing$}, {$\varnothing$, {$\varnothing$}}}, . . .

def: Ординальные числа

- **Транзитивное множество** X: $\forall x. \forall y. x \in y \,\&\, y \in X \longrightarrow x \in X$.
- **Ординал** (порядковое число) — вполне упорядоченное отношением ($\in$) транзитивное множество

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

- ω — наименьший предельный ординал

Теорема.
ω существует

Доказательство:
Пусть $\omega = \{x \in N \mid x$ конечен$\}$. Тогда:
- меньше ω предельных нет: если θ таков, что $\theta \in \omega$, тогда θ конечен.
- ω предельный: Пусть θ таков, что $\theta' = \omega$. Тогда θ конечен и θ' тоже конечен.

Q.E.D.

ω' — тоже ординал.

def: Порядковый тип множества — некоторое свойство, общее для всех множеств, изоморфных относительно биективных отображений, сохраняющих порядок

Порядковый тип вполне упорядоченного множества $\langle S, (\preceq)\rangle$ — ординал A, для которого есть биективное отображение $f: S \longrightarrow A$, сохраняющее порядок: $a \preceq b$ тогда и только тогда, когда $f(a) \leq f(b)$
Множество Z не имеет порядкового типа (в смысле определения через ординалы): оно не вполне упорядочено.

def: Операции над ординалами
- $a + b$ — порядковый тип $a \uplus b$ (отмеченного объединения), причём $xa < yb$ при любых $x \in a$ и $y \in$ b
- $a \cdot b$ — порядковый тип $a \times b$, произведение упорядочено лексикографически: $\langle x1, y1\rangle < \langle x2, y2\rangle$, если $x1 < x2$ или $x1 = x2$ и $y1 < y2$.

def: upb x — верхняя грань множества ординалов, upb $x = \bigcup_{a \in x} a$.

upb {$\varnothing'$, $\varnothing''$, $\varnothing'''$'} = $\varnothing' \cup \varnothing'' \cup \varnothing'''' = \{\varnothing\} \cup \{\varnothing, \{\varnothing\}\} \cup \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} = \varnothing''''$

def: Ординалы (порядковые числа) и порядок

- Добавить элемент перед бесконечностью: N и N0. $1 + \omega = \omega$.
- Добавить элемент после бесконечности ($+\infty$). $\omega + 1 = \omega$

Упорядоченные пары натуральных чисел имеют порядковый тип $\omega\hat{}2$.

$$\langle 3, 5\rangle < \langle 4, 3\rangle . \omega \cdot 3 + 5 < \omega \cdot 4 + 3$$

Списки натуральных чисел — порядковый тип $\omega\hat{}\omega$.

$$\langle 3, 1, 4, 1, 5, 9\rangle : \omega^5 \cdot 3 + \omega^4 \cdot 1 + \omega^3 \cdot 4 + \omega^2 \cdot 1 + \omega^1 \cdot 5 + 9$$

19. Мощность множеств

def: Аксиома фундирования. В каждом непустом множестве найдется элемент, не пересекающийся с исходным множеством.

$$\forall x.x = \emptyset \vee \exists y.y \in x \& \forall z.z \in x \to z \notin y$$

Иными словами, в каждом множестве есть элемент, минимальный по отношению $(\in)$.

Идея Рассела: каждому множеству припишем тип (тип пустого 0, тип множеств 1, тип множеств множеств 2 и т.п.). Тогда конструкция невозможна: $\{x \mid x \in x\}$. Аксиома фундирования позволяет определить функцию ранга:

$$rk(x) = \text{upb } \{rk(y) \mid y \in x\}$$

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

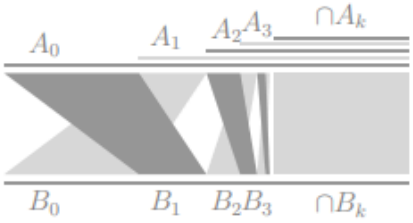
$$\forall s.(\forall x.\forall y_1.\forall y_2.x \in s \& \phi(x, y_1) \& \phi(x, y_2) \to y_1 = y_2) \to (\exists t.\forall y.y \in t \leftrightarrow \exists x.x \in s \& \phi(x, y))$$

def: Множество A **равномощно** B $(|A| = |B|)$, если существует биекция $f : A \to B$.

Теорема Кантора-Бернштейна.
Множество A имеет мощность, не превышающую мощности B $(|A|le|B|)$, если существует инъекция $f : A \to B$.

Доказательство:

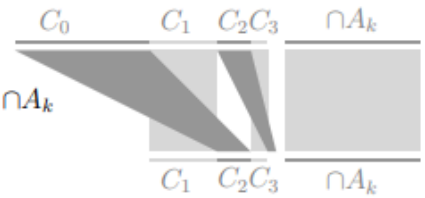
Избавимся от множества B: пусть $A_0 = A$; $A_1 = g(B)$; $A_{k+2} = g(f(A_k))$.



Тогда, если существует $h : A_0 \to A_1$ — биекция, то тогда $g^{-1} \circ h : A \to B$ — требуемая биекция.

Пусть $C_k = A_k \setminus A_{k+1}$. Тогда $g(f(C_k)) = g(f(A_k)) \setminus g(f(A_{k+1})) = A_{k+2} \setminus A_{k+3} = C_{k+2}$.

$$h(x) = \begin{cases} x, & x \in C_{2k+1} \vee x \in \cap A_k \\ g(f(x)), & x \in C_{2k} \end{cases}$$



Тогда определим $h(x)$ следующим образом:

$$h(x) = \begin{cases} x, & x \in C_{2k+1} \vee x \in \cap A_k \\ g(f(x)), & x \in C_{2k} \end{cases}$$

Q.E.D.

def: **Кардинальное число** — наименьший ординал, не равномощный никакому меньшему:

$$\forall x. x \in c \to |x| < |c|$$

Теорема. Конечные ординалы — кардинальные числа.

def: **Мощность множества** ($|S|$) — равномощное ему кардинальное число.

Теорема. **Кантор**
$|\mathcal{P}(S)| > |S|$

Доказательство:
Пусть $S = \{a, b, c, ...\}$

n	$a \in f(n)$	$b \in f(n)$	$c \in f(n)$	...
a	И	Л	И	
b	Л	Л	И	
c	И	И	И	
	Л	И	Л	$y \notin f(y)$

Пусть $f : S \to \mathcal{P}(S)$ — биекция. Тогда $\sigma = \{y \in S \mid y \notin f(y)\}$. Пусть $f(x) = \sigma$.

Но $x \in f(x)$ тогда и только тогда, когда $x \notin \sigma$, то есть $f(x) \neq \sigma$.

Q.E.D.

def: $\aleph_0 := |\omega|; \aleph_{\{k+1\}} := \min\{a \mid a$ -- ординал$\}, \aleph_k < |a|\}$

def: $\beth_0 := |\omega|; \beth_{\{k+1\}} := |\mathcal{P}(\beth_k)|$

Континуум-гипотеза (Г.Кантор, 1877): $\aleph_1 = \beth_1$ (не существует мощности, промежуточной между счётной и континуумом).

Обобщённая континуум-гипотеза: $\aleph_n = \beth_n$ при всех n.

def: Утверждение α противоречит аксиоматике: $\vdash \alpha$ ведёт к противоречию.

def: Утверждение α не зависит от аксиоматики: $\nvdash \alpha$ и $\nvdash \neg\alpha$.

Теорема. Утверждение $\aleph_1 = \beth_1$ не зависит от аксиоматики ZFC.

20. Модели, мощность

def: Пусть задана модель $\langle D, F_n, P_n \rangle$ для некоторой теории первого порядка. Её мощностью будем считать мощность D.

def: Пусть задана формальная теория с аксиомами $\{\alpha_n\}$. Её мощность — мощность множества $\{\alpha_n\}$.

Формальная арифметика, исчисление предикатов, исчисление высказываний — счётно-аксиоматизируемые.

def: $\mathcal{M}' = \langle D', F'_n, P'_n \rangle$ — **элементарная подмодель** $\mathcal{M} = \langle D, F_n, P_n \rangle$, если:

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

Теорема Лёвенгейма-Сколема.
Пусть T — множество всех формул теории первого порядка. Пусть теория имеет некоторую модель $\mathcal{M}$. Тогда найдётся элементарная подмодель $\mathcal{M}'$, причём $|\mathcal{M}'| \leq \max(\aleph_0, |T|)$.

Доказательство:

План:

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

Пусть $\{f_k^0\}$ — все 0-местные функциональные символы теории.

1. $D_0 = \{[\![f_k^0]\!]\}$, если есть хотя бы один f_k^0.
2. Если таких f_k^0 нет, возьмём какое-нибудь одно значение из D.

Очевидно, $|D_0| \geq |T|$.

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

1. φ не имеет свободных переменных — пропустим.
2. φ имеет хотя бы одну свободную переменную y.
   1. $\varphi(y, x_1, ..., x_n)$ при $y, x_i \in D_k$ бывает истинным и ложным — ничего не меняем
   2. $\varphi(y, x_1, ..., x_n)$ при $y \in D$ и $x_i \in D_k$ либо всегда истинен, либо всегда ложен — ничего не меняем
   3. $\varphi(y, x_1, ..., x_n)$ при $y, x_i \in D_k$ тождественно истинен или ложен, но при $y' \in D \setminus D_k$ отличается — добавим y' к $D_{\{k+1\}}$. Вместе добавим всевозможные $[\![\theta(y')]\!]$.

1. Всего добавили не больше $|T| \cdot |T|$ (для каждой формулы φ, возможно, будет добавлен y — и всевозможные выражения $\theta(y)$, допустимые в языке), и $|D_0| \geq |T| \geq |T| \cdot |T|$, отсюда $|D_k| \geq |T| \cdot |T|$.
2. $|D'| = |\cup D_i| \geq |T| \cdot |T| \cdot \aleph_0$.
3. Тогда $|T| \cdot |T| \cdot \aleph_0 = \max(|T|, \aleph_0)$. Разберём случаи:
   1. Если $|T| < \aleph_0$, тогда $(|T| \cdot |T|) \cdot \aleph_0 = \aleph_0$
   2. Если $|T| \leq \aleph_0$, тогда $(|T| \cdot |T|) \cdot \aleph_0 = |T| \cdot \aleph_0 = |T|$.
4. Итого, $|D'| \geq \max(|T|, \aleph_0)$.

Докажем, что $\mathcal{M}'$ — элементарная подмодель

Индукцией по структуре формул $\tau \in T$ покажем, что все формулы можно вычислить, и что $[\![\varphi]\!]_{\mathcal{M}'} = [\![\varphi]\!]_{\mathcal{M}}$.

1. База, 0 связок. $\tau \equiv P\Big(f_1(x_1, ..., x_n), ..., f_{n(x_1,...,x_n)}\Big)$. Если $x_i \in D'$, то значит, добавлены на некоторых шагах (максимальный пусть t). Поэтому в $D_{\{t+1\}}$ можно вычислить формулу, и её значение сохранилось.
2. Переход. Пусть формулы из k связок сохраняют значения. Рассмотрим τ с $k+1$ связкой.
   1. $\tau \equiv \rho \star \sigma$ — очевидно.
   2. $\tau \equiv \forall y.\varphi(y, x_1, ..., x_n)$. Каждый x_i добавлен на каком-то шаге — максимум t. Если $\varphi(y, x_1, ..., x_n)$ бывает истинен и ложен при $y_t, y_f \in D$, то $y_t, y_f \in D_{\{t+1\}}$ (по построению). Поэтому, если $\mathcal{M} \nvDash \forall y.\varphi(y, x_1, ..., x_n)$, то и $\mathcal{M}' \nvDash \forall y.\varphi(y, x_1, ..., x_n)$. Если же $\varphi(y, x_1, ..., x_n)$ не меняется от y, то тем более $[\![\varphi]\!]_{\mathcal{M}'} = [\![\varphi]\!]_{\mathcal{M}}$.
   3. $\tau \equiv \exists y.\varphi(y, x_1, ..., x_n)$ — аналогично.

Q.E.D.

def: «Парадокс» Сколема

Как известно, $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| > |\mathbb{N}| = \aleph_0$. Однако, ZFC — теория со счётным количеством формул. Значит, существует счётная модель ZFC, то есть $|\mathbb{R}| = \aleph_0$. В чём ошибка?

У равенств разный смысл, первое — в предметном языке, второе — в метаязыке.

21. Аксиома выбора

def: Аксиома выбора.Из любого семейства дизъюнктных непустых множеств $\mathcal{A}$ можно выбрать непустую трансверсаль — множество S, что $|S \cup A| = 1$ для каждого $A \in \mathcal{A}$. Иначе, $S \in \times \mathcal{A}\}$.

Теорема: функциональный вариант аксиомы выбора

Теорема. Функциональный вариант аксиомы выбора
Пусть $\mathcal{A}$ — семейство непустых множеств.

Тогда существует $f : \mathcal{A} \to \cup \mathcal{A}$, причём $\forall a. a \in \mathcal{A} \to f(a) \in a$

Доказательство:
Пусть $X(A) = \{\langle A, a\rangle \mid a \in A\}$, по семейству $\mathcal{A}$ рассмотрим $\{X(A) \mid A \in \mathcal{A}\}$
- непустых: если $A \in \mathcal{A}$, $A \neq \emptyset$, то $X(A) \neq \emptyset$;
- дизъюнктное: если $A_0, A_1 \in \mathcal{A}$, $A_0 \neq A_1$, то $X(A_0) \cap X(A_1) = \emptyset$

тогда по аксиоме выбора $\exists f. f \in \times \mathcal{A}$.

Q.E.D.

Теорема. Лемма Цорна.
Если задано $\langle M, (\preceq)\rangle$ и для всякого линейно упорядоченного $S \subseteq M$ выполнено $\mathrm{upb}_M S \neq \emptyset$, то в M существует максимальный элемент.

Теорема Цермело.
На любом множестве можно задать полный порядок.

Теорема.
У любой сюръективной функции существует частичная обратная.

Теорема.
Аксиома выбора $\to$ лемма Цорна: без доказательства.

Назовём (для данного раздела) упорядоченным множеством пару $\langle S, \left(\underset{S}{\prec}\right)\rangle$. Отношение порядка $\left(\underset{S}{\prec}\right)$ может быть как строгим, так и нестрогим.

def: Будем говорить, что $\langle S, \left(\underset{S}{\prec}\right)\rangle$ — **начальный отрезок** $\langle T, \left(\underset{T}{\prec}\right)\rangle$, если:
- $S \subseteq T$;
- если $a, b \in S$, то $a \underset{S}{\prec} b$ тогда и только тогда, когда $a \underset{T}{\prec} b$;
- если $a \in S, b \in T \setminus S$, то $a \underset{T}{\prec} b$.

Будем обозначать это как $\langle S, \left(\underset{S}{\prec}\right)\rangle \sqsubseteq \langle T, \left(\underset{T}{\prec}\right)\rangle$ или как $S \sqsubseteq T$, если порядок на множествах понятен из контекста.

Теорема.
Отношение «быть начальным отрезком» является отношением нестрогого порядка.

Теорема о верхней грани.
Если семейство упорядоченных множеств X линейно упорядочено отношением «быть начальным отрезком», то у него есть верхняя грань.

Доказательство:
Пусть $M = \cup \{T \mid \langle T, (\prec)\rangle \in X\}$ и $(\prec)_M = \cup \{(\prec) \mid \langle T, (\prec)\rangle \in X\}$.

Покажем, что если $\langle A, \left(\underset{A}{\prec}\right)\rangle \in X$, то $A \sqsubseteq M$.

Рассмотрим определение:
- $A \subseteq M$ — выполнено по построению M;
- если $a, b \in A$, то $a \underset{A}{\prec} b$ влечёт $a \underset{M}{\prec} b$ (по построению M). Если же $a \underset{M}{\prec} b$, но $a \not\underset{A}{\prec} b$, то существует A', что $a, b \in A'$ и $a \underset{\{A'\}}{\prec} b$. Тогда $A \not\sqsubseteq A'$ и $A' \not\sqsubseteq A$, что невозможно по линейности порядка;
- если $a \in A$, $b \in M \setminus A$, то найдётся B, что $b \in B$, отчего $a \underset{B}{\prec} b$ (так как $A \sqsubseteq B$) и $a \underset{M}{\prec} b$ (по построению M). Тогда $\langle M, \left(\underset{M}{\prec}\right)\rangle$ — требуемая верхняя грань.

Q.E.D.

Теорема.
Лемма Цорна $\to$ теорема Цермело

Доказательство:
Пусть $S = \{\langle P, (\prec)\rangle \mid P \subseteq X, (\prec)$ --- полный порядок$\}$.

Например, для $X = \{0, 1\}$ множество $S = \{\langle \emptyset, \emptyset\rangle, \langle \{0\}, \emptyset\rangle, \langle \{1\}, \emptyset\rangle, \langle X, 0 \prec 1\rangle, \langle X, 1 \prec 0\rangle\}$

Введём порядок на S как $(\sqsubseteq)$. Заметим, что это — частичный, но не линейный порядок.

Например, $\langle X, 0 \prec 1\rangle$ несравним с $\langle X, 1 \prec 0\rangle$.

По теореме о верхней грани любое линейно упорядоченное подмножество $\langle T, (\sqsubseteq)\rangle$ (где $T \subseteq S$) имеет верхнюю грань.

Например, для $\{\langle \emptyset, \emptyset\rangle, \langle \{0\}, \emptyset\rangle, \langle X, 0 \prec 1\rangle\}$ это $\langle X, 0 \prec 1\rangle$.

По лемме Цорна тогда есть $\langle R, \left(\underset{R}{\sqsubseteq}\right)\rangle = \max S$. Заметим, что $R = X$, потому что иначе пусть $a \in X \setminus R$. Тогда положив $M = \langle R \cup \{a\}, \left(\underset{R}{\sqsubseteq} \cup \{x \prec a \mid x \in R\}\right)\rangle$ получим, что M тоже вполне упорядоченное (и потому $M \in S$), значит, R не максимальное.

Q.E.D.

Теорема.
Теорема Цермело $\to$ у сюръективных функций существует частичная обратная.

Доказательство:

Рассмотрим сюръективную $f : A \to B$. Рассмотрим семейство $R_b = \{a \in A \mid f(a) = b\}$. Построим полный порядок на каждом из R_b. Тогда $f^{\{-1\}}(b) = \min R_b$.

Q.E.D.

Теорема.
Существует частичная обратная у сюръективных функций $\to$ существует трансверсаль у семейства непустых дизъюнктных множеств.

Доказательство:
Пусть дано семейство непустых дизъюнктных множеств $\mathcal{A}$. Рассмотрим $f : \cup \mathcal{A} \to \mathcal{A}$, что $f(a) = \cup \{A \in \mathcal{A} \mid a \in A\}$. Поскольку элементы $\mathcal{A}$ дизъюнктны, $f(a) \in \mathcal{A}$ при всех a. Тогда существует $f^{\{-1\}} : \mathcal{A} \to \cup \mathcal{A}$. Тогда $\left\{f^{\{-1\}}(A) \mid A \in \mathcal{A}\right\} \in \times \mathcal{A}$.

Q.E.D.

22. Применение аксиомы выбора

Теорема Диаконеску.

Если рассмотреть ИИП с ZFC, то для любого P выполнено $\vdash P \vee \neg P$.

Доказательство:

Рассмотрим $\mathcal{B} = \{0, 1\}$, $A_0 = \{x \in \mathcal{B} | x = 0 \vee P\}$ и $A_1 = \{x \in \mathcal{B} | x = 1 \vee P\}$. $\{A_0, A_1\}$ — семейство непустых множеств, и по акс. выбора существует $f : \{A_0, A_1\} \to \cup A_i$, что $f(A_i) \in A_i$. (Если P, то $A_0 = A_1$ и $\{A_0, A_1\} = \{\mathcal{B}\}$).

$\vdash f(A_0) \in A_0 \,\&\, f(A_1) \in A_1$	а.выбора: $f(A_i) \in A_i$
$\vdash f(A_0) \in \mathcal{B} \,\&\, (f(A_0) = 0 \vee P) \,\&\, f(A_1) \in \mathcal{B} \,\&\, (f(A_1) = 1 \vee P)$	а.выделения
$\vdash (f(A_0) = 0 \,\&\, f(A_1) = 1) \vee P$	Удал. (&) + дистр.
$\vdash P \vee f(A_0) \neq f(A_1)$	$0 \neq 1$ и транз.
$\vdash P \to A_0 = A_1$	Определение A_i
$\vdash A_0 = A_1 \to f(A_0) = f(A_1)$	Конгруэнтность
$\vdash f(A_0) \neq f(A_1) \to \neg P$	Контрапозиция
$\vdash P \vee \neg P$	Подставили

Q.E.D.

Теорема конечного выбора.

Если $X_1 \neq \emptyset, .., X_n \neq \emptyset$, $X_i \cap X_j = \emptyset$ при $i \neq j$, то $\times \{X_1, ..., X_n\} \neq \emptyset$.

Доказательство:

Доказательство:

- База: $n = 1$. Тогда $\exists x_1 . x_1 \in X_1$, поэтому $\exists x_1 . \{x_1\} \in \times \{X_1\}$.
- Переход:

$$\exists v . v \in \times \left\{X_{\{1,n\}}\right\} \to \exists x_{\{n+1\}} . x_{\{n+1\}} \in X_{\{n+1\}} \to v \cup \left\{x_{\{n+1\}}\right\} \in \times \left(X_{\{1,n\}} \cup \left\{X_{\{n+1\}}\right\}\right)$$

Q.E.D.

Аксиома счётного выбора.

Для счётного семейства непустых множеств существует функция, каждому из которых сопоставляющая один из своих элементов

Аксиома зависимого выбора.

Если $\forall x \in E . \exists y \in E . xRy$, то существует последовательность $x_n : \forall n . x_n R x_{\{n+1\}}$

def: **Наследственным свойством** множества назовём такое свойство, которым обладает как само множество, так и все его подмножества.

def: **Фундированным множеством** назовём такое, которое не пересекается хотя бы с одним своим элементом.

def: **Универсум фон Неймана** V — все наследственные фундированные множества.

При наличии аксиомы фундирования можно показать, что $V = \cup_a V_a$, где:

$$V_a = \begin{cases} nothing, & a = 0 \\ \mathcal{P}(V_b), & a = b' \\ \bigcup_{b<a}(V_b), & a \text{ --- предельный} \end{cases}$$

def: **Конструктивный универсум** $L = \cup_a L_a$, где:

$$L_a = \begin{cases} nothing, & a = 0 \\ \{\{x \in L_b \mid \varphi(x, t_1, ..., t_k)\} \mid \varphi \text{ --- формула}, t_i \in L_b\}, & a = b' \\ \bigcup_{b<a}(L_b), & a \text{ --- пред.} \end{cases}$$

def: **Аксиома конструктивности:** $V = L$, то есть допустимы только те фундированные множества, которые задаются формулами.

23. Индукция

def: 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 $\varphi(x)$.

def: Принцип полной математической индукции

Какое бы ни было $\psi(x)$, если $\psi(0)$ и при всех x выполнено $(\forall t.t \le x \to \psi(t)) \to \psi(x')$, то при всех x выполнено и само $\psi(x)$.

def: Назовём вполне упорядоченное отношением $(\in)$ множество S **наследственным подмножеством** A, если $\forall x.x \in A \to (\forall t.t \in x \to t \in S) \to x \in S$.

Теорема.
Единственным наследственным подмножеством вполне упорядоченного множества является оно само.

Доказательство:
Пусть $B \subseteq A$ — наследственное и $B \neq A$. Тогда существует $a = \min(A \setminus B)$. Тогда $(\forall t.t \in a \to t \in B) \to a \in B$ по наследственности B, и выполнено $\forall t.t \in a \to t \in B$ (по минимальности a). Значит, $a \in B$.

Q.E.D.

Ограниченная трансфинитная индукция.
Если для $\varphi(x)$ (некоторого утверждения теории множеств) и некоторого ординала ε (ограничения) выполнено $\forall x.x \in \varepsilon \to (\forall t.t \in x \to \varphi(t)) \to \varphi(x)$, то $\forall x.x \in \varepsilon \to \varphi(x)$.

Доказательство:
Рассмотрим $S = \{x \in \varepsilon \mid \varphi(x)\}$. Тогда $x \in S$ равносильно $x \in \varepsilon \& \varphi(x)$. Тогда перепишем: $\forall e.e \in \varepsilon \to (\forall x.x \in e \to x \in S) \to e \in S$. Отсюда по теореме о наследственных множествах $S = \varepsilon$.

Q.E.D.

Неограниченная трансфинитная индукция.
Если для $\varphi(x)$ (некоторого утверждения теории множеств) выполнено $\forall x.\text{ординал}(x) \to (\forall t.t \in x \to \varphi(t)) \to \varphi(x)$, то $\forall x.\text{ординал}(x) \to \varphi(x)$.

ИЛИ

Для ординала ε подмножество $S \in \varepsilon$ — наследственное, если и только если одновременно:
- Если $x \in \varepsilon$ и $x = \emptyset$, то $x \in S$;
- Если $x \in \varepsilon$ и существует y: $y' = x$, то $y \in S \to x \in S$;
- Если $x \in \varepsilon$ и x — предельный, то $(\forall t.t \in x \to t \in S) \to (x \in S)$.

Доказательство:
$(\to)$ очевидно. Докажем $(\le)$: пусть S не наследственное: $E := \{e \in \varepsilon \mid (\forall t.t \in e \to t \in S) \& e \notin S\}$ и $E \neq \emptyset$. Тогда пусть $e = \min E$.

1. $e = \emptyset$ или предельный. Тогда $(\forall t.t \in e \to t \in S) \to (e \in S)$.
2. $e = y'$. Тогда $y \in \varepsilon$ (

ε

— ординал) и

$(\forall t.t \in y \to t \in S) \to (y \in S)$ (так как e минимальный, для которого S не наследственное). По условию, $(y \in S) \to (e \in S)$, отсюда $(\forall t.t \in e \to t \in S) \to (e \in S)$.

Q.E.D.

Теорема.
Если α — кардинальное число, $\alpha \geq \aleph_0$, то $\alpha \cdot \alpha = \alpha$.

Доказательство:
Трансфинитная индукция: $\varphi(x) := x < \omega \vee x \cdot x = x$

1. База: $x = \emptyset$. Тогда

$\varphi(\emptyset) \equiv \emptyset < \omega \vee |\emptyset \times \emptyset| = \emptyset$, что доказуемо.
2. Переход: $\forall y.y < x \to \varphi(y)$, тогда $\varphi(x)$. Три случая:
   1. $x < \omega$. Тогда $\varphi(x)$ истинно (аналогично базе).
   2. $x = \omega$. Счётный случай (рассмотрим отдельно).
   3. $x > \omega$. Общий случай (рассмотрим отдельно).

Счётный случай: $\omega < \omega \vee |\omega \cdot \omega| = \omega$

Тогда $\omega \times \omega$ упорядочим так: $\langle p, q\rangle \prec \langle s, t\rangle$, если:
1. $\max(p, q) < \max(s, t)$
2. $\max(p, q) = \max(s, t)$ и $q < t$
3. $\max(p, q) = \max(s, t)$, $q = t$ и $p < s$

Очевидно, можно построить биекцию между так упорядоченными значениями и ω.

Общий случай: $|\alpha \cdot \alpha| = \alpha$ TODO

Аналогично счётному случаю, $\alpha \times \alpha$ упорядочим так: $\langle p, q\rangle \prec \langle s, t\rangle$, если:
1. $p \cup q < s \cup t$
2. $p \cup q = s \cup t$ и $q < t$
3. $p \cup q = s \cup t$, $q = t$ и $p < s$

- Легко заметить, что это — линейный порядок (показав, что $p \not\prec q$ и $q \not\prec p$ влечёт $p = q$)
- ... и полный порядок. Найти наименьший в $S \neq \emptyset$ возможно, рассмотрев $m_1 := \min\{p \cup q \mid \langle p, q\rangle \in S\}$ и

$M_1 := \{\langle p, q\rangle \mid \langle p, q\rangle \in S, p \cup q = m_1\}$, затем $m_2 := \min\{q \mid \langle p, q\rangle \in M_1\}$, $M_2 := \{\langle p, q\rangle \mid \langle p, q\rangle \in M_1, q = m_2\}$. Тогда требуемым наименьшим в S будет $\min\{p \mid \langle p, q\rangle \in M_2\}$
- Тогда $\langle \alpha \times \alpha, (\prec)\rangle$ соответствует какой-то ординал τ

и сохраняющая порядок биекция $t : \tau \to \alpha \times \alpha$.
- Заметим, что $x < \omega$ тогда и только тогда, когда $\cup\,(\cup\, t(x)) < \omega$

(очевидно из того, что $|\{z \mid \text{ординал}\}(z), z < x\}| = |\{p \mid p \prec t(x)\}|$).
- Покажем, что $|\ \tau\ | = \alpha$.

Докажем $\tau = \alpha$

Очевидно, что $\tau > \alpha$ (так как $|\ \tau\ | = |\alpha \times \alpha| > \alpha$). Но пусть $\tau > \alpha$.

- Тогда $t(\alpha) = \langle \zeta, \eta\rangle$ определено (у α есть образ).
- Пусть $\sigma := \zeta \cup \eta$. Очевидно, $\langle \zeta, \eta\rangle \preceq \langle \sigma, \sigma\rangle$

и $\sigma \in \alpha$.

- Каков образ t на этом начальном отрезке?

$\{t(x) \mid x < \alpha\} \subseteq \{\langle p, q\rangle \mid p, q < \sigma\}$. Поэтому $\alpha < |(\sigma + 1) \times (\sigma + 1)|$.

- С другой стороны, $\sigma < \alpha$. Поскольку α — кардинал (т.е., в частности, предельный ординал),

то $\sigma + 1 < \alpha$ и $|\sigma + 1| < \alpha$.

- По предположению индукции, $|\sigma + 1| < \omega \vee |\sigma + 1| = |\sigma + 1| \cdot |\sigma + 1|$,

по свойствам $(\prec)$ имеем $\sigma > \omega$.

- Отсюда $\alpha < |(\sigma + 1) \times (\sigma + 1)| = |\sigma + 1| < \alpha$, что невозможно.

Q.E.D.

24. Система S_{inf}

def: Введем исчисление S_∞

1. Язык: связки $\neg$, $\vee$, $\forall$, $=$; нелогические символы: $(+)$,$(\cdot)$,$(')$,0; переменные: x.
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:

$$\frac{\zeta \vee \alpha \vee \beta \vee \delta}{\zeta \vee \beta \vee \alpha \vee \delta} \qquad \frac{\alpha \vee \alpha \vee \delta}{\alpha \vee \delta}$$

   Сильные правила

$$\frac{\beta}{\alpha \vee \beta} \quad \frac{\neg\alpha \vee \delta \quad \neg\beta \vee \delta}{\neg(\alpha \vee \beta) \vee \delta} \quad \frac{\alpha \vee \delta}{\neg\neg\alpha \vee \delta} \quad \frac{\neg\alpha[x := \theta] \vee \delta}{(\neg\forall x.\alpha) \vee \delta}$$

   Формулы в правилах, обозначенные буквами ζ и δ, называются боковыми и могут отсутствовать.

4. Бесконечная индукция:

$$\frac{\alpha[x := \overline{0}] \vee \delta \quad \alpha[x := \overline{1}] \vee \delta \quad \alpha[x := \overline{2}] \vee \delta \quad \dots}{(\forall x.\alpha) \vee \delta}$$

5. Сечение:

$$\frac{\zeta \vee \alpha \qquad \neg\alpha \vee \delta}{\zeta \vee \delta}$$

   Здесь α — секущая формула, число связок в $\neg\alpha$ — степень сечения.
   В отличие от других правил, в правиле сечения хотя бы одна из боковых формул ζ или δ должна присутствовать.

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).

$$\frac{\dfrac{(\neg 1 = 0)_1 \quad (\neg 2 = 0)_2 \quad (\neg 3 = 0)_4 \quad (\neg 4 = 0)_8 \dots}{(\forall x.\neg x' = 0)_\omega}}{(\neg\neg\forall x.\neg x' = 0)_{\omega+1}}$$

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

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

Доказательство:
Трансфинитная индукция. Пусть для всех деревьев порядка $t_1 < t$ условие выполнено. Покажем, что оно выполнено для порядка t. Рассмотрим заключительное правило. Это может быть...

1. Не сечение.
2. Сечение, секущая формула — элементарная.

3. Сечение, секущая формула — $\neg\alpha$.
4. Сечение, секущая формула — $\alpha \vee \beta$.
5. Сечение, секущая формула — $\forall x.\alpha$.

Случай 1. Не сечение

$$\frac{(\pi_0)_{t_0}(\pi_1)_{t_1}(\pi_2)_{t_2}\dots}{(\alpha)_t}$$

Заменим доказательства посылок $(\pi_i)_{\{t_i\}}$ на $(\pi_i')_{\{2^{\{t_i\}}\}}$ по индукционному предположению.

1. Поскольку степени посылок $m_i' < m_i$, то $\max m_i' < \max m_i$.
2. Поскольку $t_i \le t$, то $2^{\{t_i\}} \le 2^t$.

Случай 5. Сечение с формулой вида $\forall x.\alpha$

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

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 $\left(m_{1'}, 2^{\{t_1\}}\right)$.
2. По обратимости, можно построить вывод $\zeta \vee \alpha[x := \theta]$ за $\left(m_{1'}, 2^{\{t_1\}}\right)$.
3. В формуле $(\neg\forall x.\alpha) \vee \delta$ формула $\neg\forall x.\alpha$ получена

либо ослаблением, либо квантификацией из $\neg\alpha[x := \theta_k] \vee \delta_k$.

1. Каждое правило квантификации заменим на:

$$\frac{\zeta \vee \alpha[x := \theta_k] \quad (\neg\alpha[x := \theta_k]) \vee \delta_k}{\zeta \vee \delta_k}$$

2. 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 $\neg\forall x.\alpha$.

Q.E.D.

def: Итерационная экспонента

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

Теорема об устранении сечений. Если $\underset{\infty}{\vdash} \sigma$ степени m порядка t, то найдётся доказательство без сечений порядка $(2\uparrow)^{m(t)}$

def: ε_0 — неподвижная точка $\varepsilon_0 = \omega^{\{\varepsilon_0\}}$

Иначе говоря, $\varepsilon_0 = \{\omega, \omega^\omega, \omega^{\omega^\omega}, (\omega\uparrow)^3(\omega), (\omega\uparrow)^4(\omega), \dots\}$

Очевидно, что теорема об устранении сечений может быть доказана трансфинитной индукцией до ординала ε_0 (максимальный порядок дерева вывода, при правильной нумерации вершин).

Лемма. Если $\underset{\infty}{\vdash} \alpha$ и $\underset{\infty}{\vdash} \neg\alpha$, тогда $\underset{\infty}{\vdash} \neg 0 = 0$.

Теорема о непротиворечивости формальной арифметики.
$\underset{\infty}{\nvdash} \neg 0 = 0$

Доказательство:

Пусть $\underset{\infty}{\vdash} \neg 0 = 0$, устраним сечения и рассмотрим 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 ($\alpha \vee \beta$), хотя β обязана присутствовать.
5. Сечение? Исключено по условию.

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

Q.E.D.

25. Метод резолюции

Сколемизация не сохраняет общезначимость

Дана формула α.

1. Упростим формулу — поверхностные кванторы всеобщности, сколемизация. Умеем строить формулу β: $\beta := \forall x_1.\forall x_2.\forall x_k.\delta_1(x_1,...,x_k)\&...\&\delta_n(x_1,...,x_k)$

   α доказуема тогда и только тогда, когда при всех оценках предикатных и функциональных символов найдётся значение сколемовских функций e_k, при которых β всегда истинна (слоёный пирог из кванторов).

2. Упрощаем предметное множество — заменили произвольный D на эрбранов универсум H. Выполнимость формулы эквивалентна выполнимости на эрбрановом универсуме.

3. Осталось избавиться от кванторов всеобщности и организовать правильный перебор (эрбранов универсум может быть бесконечным).

def: **Эрбранов универсум** H_φ — всевозможные комбинации функциональных символов из формулы φ.

Если в формуле нет нульместных функциональных символов, к множеству символов формулы добавляется свежий нульместный функциональный символ a и все комбинации с его участием.

def: Если φ — бескванторная формула, то её **эрбранова оценка** задаётся как $\langle H_\varphi, F, P, E\rangle$, функции F определяются как текстовые подстановки $[\![f(\theta)]\!] = ``f(``+[\![\theta]\!]+`)``$, предикаты P задаются перечислением истинных.

def: Система дизъюнктов $S = \{\delta_1,...,\delta_n\}$ **противоречива**, если для каждой оценки $M = \langle D, P, F, E\rangle$ найдётся δ_t и такой набор $d \in D$, что $[\![\delta_t]\!]^x := \overline{d} = \text{Л}$.

def: Дизъюнкт с подставленными значениями из эрбранового универсума H_β вместо переменных называется **основным примером** формулы β.

def: **Система основных примеров** — все основные примеры, опровергаемые хоть при какой-то эрбрановой оценке $\mathcal{M}$:

$$\mathcal{E}_S = \left\{\delta_t\left[\overline{x} := \overline{d}\right] \mid \text{существует } \ \mathcal{M}\ , \text{ что } \ [\![\delta_t\left[\overline{x} := \overline{d}\right]]\!](M) = \text{Л}; \quad d_i \in H_\beta\right\}$$

Теорема Гёделя о компактности.
Если Γ — некоторое семейство бескванторных формул, то Γ имеет модель тогда и только тогда, когда любое его конечное подмножество имеет модель.

Теорема Эрбрана.
Система дизъюнктов S противоречива тогда и только тогда, когда у $\mathcal{E}_S$ существует конечное противоречивое в эрбрановой интерпретации подмножество.

Доказательство:

$(\Leftarrow)$

Пусть $\{\varepsilon_1,...,\varepsilon_t\} \subseteq \mathcal{E}_S$ противоречиво, $\varepsilon_i = \delta_{\{m_i\}}[x := d_i]$, где d_i — набор значений из H.

То есть, для любой эрбрановой оценки M существует ε_p, что $[\![\varepsilon_p]\!]_M = \text{Л}$. Отсюда, по теореме о выполнимости S тоже противоречива.

$(\Rightarrow)$

Если S противоречива, то $\mathcal{E}_S$ противоречива.

Тогда у неё нет модели. Тогда у неё найдётся конечное противоречивое подмножество (компактность). Возможно убедиться в невыполнимости за конечное время.

Общая схема алгоритма

Цель алгоритма: убедиться, что α доказуемо.

1. По формуле α строим её отрицание $\neg\alpha$.
2. Приводим к виду с поверхностными кванторами, проводим сколемизацию, находим КНФ: $\beta = \forall x_1 ..... \forall x_k . \delta_1 \& ... \& \delta_n$.
3. Убедимся, что при любом D и значениях функциональных и предикатных символов и сколемовских функций e_k найдутся $d_i \in D$, что один из дизъюнктов δ_t при подстановке $x := d$ ложный.
4. Для этого строим универсум Эрбрана H, и систему основных примеров $\mathcal{E}_S$, её противоречивость эквивалентна невыполнимости β.
5. Конечное противоречивое подмножество обязательно находится в каком-то начальном отрезке $\{\varepsilon_1, ..., \varepsilon_t\} \subseteq \mathcal{E}_S$ (если оно есть).

Подмножество $\mathcal{E}$	выполнено в оценке	количество оценок
$\{P(e)\}$	$[\![P(e)]\!] = \text{И}$	2 варианта
$\{P(e), P(e')\}$	$[\![P(e)]\!] = [\![P(e')]\!] = \text{И}$	4 варианта
...		
$\{P(e), \dots, P(e''''), \neg P(e'''')\}$	невыполнимо	32 варианта

Q.E.D.

Правило резолюции (исчисление высказываний).
Пусть даны два дизъюнкта, $\alpha_1 \vee \beta$ и $\alpha_2 \vee \neg\beta$. Тогда следующее правило вывода называется правилом резолюции:

$$\frac{\alpha_1 \vee \beta \qquad \alpha_2 \vee \neg\beta}{\alpha_1 \vee \alpha_2}$$

def: Алгебраический терм $\theta := x \mid (f(\theta_1, ..., \theta_n))$ где x —переменная, $f(\theta_1, ..., \theta_n)$ —применение функции. Напомним, что константы — нульместные функциональные символы, собственно переменные будем обозначать последними буквами латинского алфавита.

def: Система уравнений в алгебраических термах $\begin{cases} \theta_1 = \sigma_1 \\ \vdots \\ \theta_n = \sigma_n \end{cases}$, где θ_i и σ_i — термы

def: $\{x_i\} = X$ **—множество переменных**, $\{\theta_i\} = T$ **—множество термов.**

def: Подстановка—отображение вида: $\pi_0 : X \to T$, тождественное почти везде (за исключением конечного числа переменных). $\pi_0(x)$ может быть либо $\pi_0(x) = \theta_i$, либо $\pi_0(x) = x$.

Доопределим $\pi : T \to T$, где
1. $\pi(x) = \pi_0(x)$
2. $\pi(f(\theta_1, ..., \theta_k)) = f(\pi(\theta_1), ..., \pi(\theta_k))$

Решить уравнение в алгебраических термах—найти такую наиболее общую подстановку π, что $\pi(\theta_1) = \pi(\theta_2)$.

Наиболее общая подстановка — такая, для которой другие подстановки являются её частными случаями.

def: Пусть даны формулы α и β. Тогда решением задачи унификации будет такая наиболее общая подстановка $\pi = \mathcal{U}[\alpha, \beta]$, что $\pi(\alpha) = \pi(\beta)$. Также, π назовём наиболее общим унификатором.

Правило резолюции (исчисление высказываний).
Пусть σ_1 и σ_2 — подстановки, заменяющие переменные в формуле на свежие. Тогда правило резолюции выглядит так:

TODO

26. Информация о курсе

Поток — y2024.

Группы M3232-M3239.

Преподаватель — Штукенберг Дмитрий Григорьевич