Московский физико-технический институт
Физтех-школа прикладной математики и информатики

МАТЕМАТИЧЕСКАЯ ЛОГИКА

II СЕМЕСТР

Лектор: *Даниил Владимирович Мусатов*

$h\nu$

Автор: *Киселев Николай*
Репозиторий на Github

весна 2025

Содержание

1 Вступление **2**

2 Фундированные множества **2**

2.1 Свойства, эквивалентные фундированности . . . 3
2.2 Непосредственно следующие элементы . . . 4
2.3 Предельные элементы . . . 5
2.4 Сложение и умножение Фундированных множеств и ВУМов . . . 5

3 Ординалы **7**

3.1 Конечные ординалы . . . 8
3.2 Сложение ординалов . . . 8
3.3 Умножение ординалов . . . 9
3.4 Возведение в степень . . . 9
3.4.1 ВУМ, изоморфный α^β . . . 10

4 Лемма Цорна, Теорема Цермело **10**

4.1 Приложения Леммы Цорна и Теоремы Цермело . . . 12

5 Теория вычислимости **13**

5.1 Алгоритм . . . 13
5.2 Однолетночная машина Тьюринга . . . 14
5.3 Свойства, эквивалентные перечислимости . . . 16
5.4 Универсальная машина Тьюринга . . . 17
5.5 Тезис Черча-Тьюринга . . . 17
5.6 Проблема самоприменимости . . . 17
5.7 Проблема остановки . . . 18
5.8 m-сводимость . . . 18
5.8.1 Свойства m-сводимости . . . 19
5.9 Как получать новые неперечислимые множества? . . . 19
5.10 Существует ли универасальная тотально вычислимая функция? . . . 19

6 Связь этого бреда с языками первого порядка **21**

6.1 Арифметическая иерархия . . . 21
6.2 Построение β-функции . . . 23
6.3 Кодирование Смаллиана . . . 23
6.4 Важная Теорема . . . 24
6.5 Доказательства в формальной арифметике . . . 24

6.5.1 Аксиомы . . . 24
6.5.2 Правила вывода . . . 25

7 Теорема Геделя **26**
7.1 Первое доказательство . . . 27
7.2 Второе доказательство . . . 27
7.3 Колмогоровская сложность . . . 27

8 λ-исчисление **28**
8.1 Синтаксис . . . 28
8.1.1 Алфавит . . . 28
8.1.2 λ-термы . . . 28
8.1.3 α-конверсия . . . 28
8.1.4 β-редукция . . . 29
8.1.5 Равенство термов . . . 29
8.2 Семантика . . . 29
8.2.1 Комбинаторы логических значений: . . . 29
8.2.2 Операции с парами . . . 30
8.3 Нумералы Черча . . . 30
8.3.1 Сложение . . . 31
8.3.2 Умножение . . . 31
8.3.3 Возведение в степень . . . 32
8.3.4 Проверка на равенство нулю . . . 32
8.3.5 Трюк Клини . . . 32
8.3.6 Вычитание . . . 33
8.4 Рекурсивное программирование в λ-исчислении . . . 33
8.5 Y-Комбинатор . . . 34
8.6 Комбинатор Клопа . . . 34

9 P vs NP **34**
9.1 Неформально . . . 34
9.2 Задача раскраски . . . 34
9.3 Задача на графах . . . 34
9.4 Задача про простоту . . . 35
9.5 Формально . . . 35

10 Заключение **35**

Короче, как-то будем сдавать какой-то экзамен. Очень сложно, ничего не понятно

1 Вступление

Вот у нас были натуральные числа:

$$\begin{gathered} 0 = \varnothing \\ 1 = \{\varnothing\} \\ 2 = \{\varnothing, \{\varnothing\}\} = \{0, 1\} \\ \vdots \\ n + 1 = \{0, 1, 2, \dots n\} \end{gathered}$$

Вопрос: что будет в бесконечности?

$$\begin{gathered} \omega = \{0, 1, 2, \dots\} \\ \omega + 1 = \{0, 1, 2, \dots, \omega\} \\ \omega + 2 = \{0, 1, 2, \dots, \omega, \omega + 1\} \\ \vdots \\ 2\omega = \dots \\ 2\omega + 1 = \dots \\ \vdots \\ 3\omega = \dots \\ \vdots \\ \omega \cdot \omega = \dots \end{gathered}$$

Таким образом, получаем различные многочлены от ω, если продолжать этот абсурд, то получится ω^ω, потом получится $\underbrace{\omega^{\omega^{\omega^{\dots^\omega}}}}_{\omega}$ и короче всякое такое.

2 Фундированные множества

Определение 2.1. Пусть S — ЧУМ. Тогда S называется Фундированным, если $\forall A \subset S \exists \min A$

Пример (Фундированные)**.**

1. $\mathbb{N}, \leqslant$
2. $\mathbb{N}, |$
3. $\{a, b\}^*, \sqsubset$

Пример (Не фундированные)**.**

1. $\mathbb{Z}, \leqslant$
2. $\mathbb{N}, \geqslant$
3. $[0, 1], \leqslant$
4. $\{a, b\}^*, \leqslant_{lex}$

2.1 Свойства, эквивалентные фундированности

1. (БС) Невозможность бесконечного спуска

$$\nexists a_1 > a_2 > a_3 \dots$$

2. (Ст) Стабилизация

$$\forall a_1 \geqslant a_2 \geqslant a_3 \cdots \Rightarrow \exists k : \forall n > k (a_k = a_n)$$

3. (ТИ) Трансфинитная индукция

$$\forall x (\forall y < x \;\; \varphi(y) \to \varphi(x)) \Rightarrow \forall z \varphi(z)$$

Теорема 2.1. *Свойства Фундированность, БС, Ст, ТИ эквивалентны.*

Доказательство.

1. ¬Ф $\Rightarrow$ ¬БС. Пусть $A \neq \varnothing, \nexists \min A$. Тогда $\forall a_1 \in A \exists a_2 \in A : a_2 < a_1$. Используя аксиому выбора (выбирая по одному элементу из оставшихся), получается бесконечную убывающую последовательность.

2. ¬Ф $\Leftarrow$ ¬БС. Тогда существует $a_1 > a_2 > a_3 \dots$. Рассмотрим это множество, в нем не будет минимального элемента.

3. ¬БС $\Rightarrow$ ¬Ст. Тогда существует $a_1 > a_2 > a_3 \dots$. Заметим, что для это последовательности неверна стабилизация.

4. ¬БС $\Leftarrow$ ¬Ст. Рассмотрим последовательность, которая не стабилизируется. Тогда $\forall n \exists k : a_n > a_k$. Тогда $\exists$ бесконечная убывающая цепочка.

5. ¬Ф $\Rightarrow$ ¬ТИ. $A \neq \varnothing$ — множество без минимального элемента, $\varphi(x) \Leftrightarrow x \notin A \Rightarrow \varphi(x) \not\equiv 1$.

$$\forall y < x \; y \notin A \Rightarrow x \notin A$$

Утверждение вверу верно, т.к. $\forall y < x (y \notin A, x \in A) \Rightarrow x = \min A$.

6. ¬Ф $\Leftarrow$ ¬ТИ. Тогда для некоторго φ верно, что

$$\forall x (\forall y < x \; \varphi(y) \to \varphi(x))$$

Но

$$\neg \forall z \varphi(z) (1)$$

Пусть $A = \{z | \varphi(z) = 0\}$. Причем A непусто, т.к. (1). Тогда рассмотрим минимальный элемент в A и получим противоречие с определением ТИ.

□

Определение 2.2. Вполне упорядоченное множество — Линейная упорядоченность + Фундированность

Пример.

$\mathbb{N}, \leqslant$	ω
$\left\{1 - \frac{1}{n} \middle\| n \in \mathbb{N}_+\right\}$	ω
$\left\{1 - \frac{1}{n} \middle\| n \in \mathbb{N}_+\right\} \cup \left\{2 - \frac{1}{n} \middle\| n \in \mathbb{N}_+\right\}$	$\omega \cdot 2$
$\left\{k - \frac{1}{n} \middle\| k, n \in \mathbb{N}_+\right\}$	ω^2
$\left\{1 - \frac{1}{n} - \frac{1}{m} \middle\| m, n \in \mathbb{N}_+\right\}$	ω^2
$\left\{1 - \frac{1}{n} - \frac{1}{m} - \frac{1}{k} \middle\| m, n, k \in \mathbb{N}_+\right\}$	ω^3
$\left\{1 - \frac{1}{n_1} - \frac{1}{n_2} - \cdots - \frac{1}{n_k} \middle\| k \text{ — произвольное}\right\}$	не фундированное
$\left\{k - \frac{1}{n_1} - \frac{1}{n_2} - \cdots - \frac{1}{n_k} \middle\| k \text{ — произвольное}\right\}$	ω^ω

Определение 2.3. Пусть S — ВУМ. Тогда $K \subset S$ называется начальным отрезком, если $\forall x, y((x \in K \wedge y < x) \to y \in K)$

Эквивалентные свойства:

$$\forall x \in K \forall y \notin K x < y$$

$$\forall x, y((x \notin K \wedge y > x) \to y \notin K)$$

2.2 Непосредственно следующие элементы

Утверждение 2.1. *S — ВУМ, $x \in S, x$ — не наибольший в $S \Rightarrow \exists! y(y > x \wedge \neg\exists z y > z > x)$.*

Доказательство. $\exists$ — из Фундированности, $y = \min\{t \in S | t > x\}$ □

Определение 2.4. y из предыдущего утверждения называется непосредственно следующим элементом после x и обозначается $x + 1$.

Замечание.

$$[0, a] = [0, a + 1)$$

Теорема 2.2. *K — начальный отрезок $S \Rightarrow K = S \vee K = [0, a)$*

Доказательство. Если $K = S$, то победили, иначе рассматриваем $a = \min(S \setminus K)$. Докажем, что $K = [0, a)$.

1. $K \subset [0, a)$: Если $x \in K, x > a$, то $a \in K$, но $a \in S \setminus K$
2. $K \supset [0, a)$: Если $x < a, x \notin K$, то $a \neq \min(S \setminus K)$ — противоречие.

□

Пример.

1. S
2. $[0, \alpha] = \{x | x \leqslant \alpha\}$
3. $[0, \alpha) = \{x | x < \alpha\}$

2.3 Предельные элементы

Определение 2.5. z назывется предельным элементом, если $\nexists y(z = y + 1)$.

или

Определение 2.6. z назывется предельным элементом, если

$$\forall y < z \exists t \in (y, z)$$

Теорема 2.3. *S — ВУМ, $x \in S \Rightarrow \exists l \in S, k \in \mathbb{N} : x = l + k = l + \underbrace{1 + 1 + \cdots + 1}_{k}$*

2.4 Сложение и умножение Фундированных множеств и ВУМов

Сложение и умножение определены так же, как и для ЧУМов.

Теорема 2.4. *1. A, B — фундированные, тогда и $A + B$ — тоже.*

2. A, B — ВУМ, тогда и $A + B$ — тоже.

3. A, B — фундированные, тогда и $A \cdot B$ — тоже.

4. A, B — ВУМ, тогда и $A \cdot B$ — тоже.

Доказательство. $C \subset A \sqcup B$:

1. (a) $C \cap A \neq \varnothing \Rightarrow \min(C \cap A)$ — существует, т.к. A — фундированное
   (b) $C \cap B \neq \varnothing \Rightarrow \min(C \cap B)$ — существует, т.к. B — фундированное
2. Подмножество ЛУМа — ЛУМ, поэтому победили по (1).

□

Замечание. Любое подмножество ВУМ — тоже ВУМ

Замечание. Множество предельных элемнтов ВУМа — ВУМ

Замечание. Между любыми двумя предельными элементами бесконечно много других

Замечание. Элементы между соседними предельными элементами образуют множество, $\approxeq \omega$

Теорема 2.5 (О структуре ВУМ). *S — ВУМ, тогда $\exists L$ — тоже ВУМ, конечное множество K, такие, что $S \cong \omega \cdot L + K$*

Теорема 2.6 (О трансфинитной рекурсии)**.** *Пусть задано рекурсивное правило:*

$$F : f|_{[0,x)} \mapsto f(x) \in R$$

Тогда $\exists! f : S \to R$*, т.ч.* $\forall x f(x) = F(f|_{[0,x)})$

Доказательство.

Единственность. Пусть f, g — 2 подходящие функции.

$$\{x|f(x) \neq g(x)\} \neq \varnothing \Rightarrow \exists m = \min\{x|f(x) \neq g(x)\} \Rightarrow f|_{[0,m)} = g|_{[0,m)}$$

Но тогда $f(m) = F(f|_{[0,m)}) = F(g|_{[0,m)}) = g(m)$, противоречие.

Существование. По трансфинитной индукции докажем сущесвование $f|_{[0,x)}$, соответствующее F.

$$\forall y < x \exists f|_{[0,y)} \Rightarrow \exists f|_{[0,x)}$$

(a) $x = w + 1 \Rightarrow \exists f|_{[0,w)}, f(w) = F(f|_{[0,w)})$

(b) x — предельное

$$y < x \Rightarrow \exists z : y < z < x$$

$$z < x \Rightarrow \exists f : [0, z) \to R$$

Так и доопределяем $f(y)$ (если разные z дают разные значения, то противоречие аналогично с доказательством единственности). То есть $\forall y < x$ задано $f(y) \Rightarrow f$ задано на $[0, x)$.

По трансфинитной индукции получили, что $\forall x \varphi(x)$. Теперь нужно сделать последний переход ко всему множеству (*Прим. от автора:* мы научились делать ее на начальных отрезках $\Rightarrow$ для "самых больших элементов" потенциально могут быть проблемы, т.к. начальные отрезки — полуинтервалы. Их мы и будем чинить последним переходом). Если в множестве есть наибольший элемент, то доопределяем так же, как и в случае а) (Важно: наибольший элемент может быть предельным). Если наибольшего элемента нет, то доопределяем значение, как в пункте б). □

Теорема 2.7 (Обобщенная теорема о трансфинитной рекурсии)**.** *F может быть частично определена, тогда f определена на начальном отрезке.*

Доказательство. Добавим значение $f(x) = \perp$, если функция f не определена в точке x. Тогда по теореме о Трансфинитной рекурсии, $\exists! f : S \to R \cup \{\perp\}$. □

Теорема 2.8 (О сравнимости ВУМов)**.** *Любые два ВУМа либо изоморфны, либо один из них изоморфен начальному отрезку другого.*

Доказательство. Строим $f : S \to T$, заданное правилом $F(f|_{[0,x)}) = \min(T \setminus f([0, x)))$. По обобщенной теореме о трансфинитной рекурсии, $\exists! f$, соответствующая F. Есть два случая:

1. f определена на S. $Im_f = \begin{bmatrix} T \\ [0, t) \end{bmatrix}$. Тогда иначе $\exists t_1 < t_2 : t_1, t_2 \notin Im_f$.
2. f определена на $[0, s) \Rightarrow Im_f = T$, иначе доопределим $f(s)$

□

Утверждение 2.2. *S — ВУМ, $s \in S \Rightarrow s \ncong [0, s)$*

Доказательство. Иначе $\exists$ монотонная $g : S \to [0, s) \Rightarrow$ т.к. $g(s) \geqslant s$ (нетрудно доказать) $\Rightarrow g(s) \notin [0, s)$, противоречие. □

Следствие. Из $S \cong T, S \cong [0, t), T \cong [0, s)$ выполнено ровно 1 утверждение

Теорема 2.9 (Цермело)**.** *У любого множества есть равномощный ему ВУМ*

Из теоремы Цермело и теоремы о сравнимости ВУМов:

Следствие.

$$\forall A, B \quad \left[\begin{array}{l} \exists B' \subset B : A \cong B' \\ \exists A' \subset A : B \cong A' \end{array} \right.$$

3 Ординалы

Определение 3.1. S — транзитивно, если $y \in S, x \in y \Rightarrow x \in S$.

Пример. $\varnothing, \{\varnothing\}$ и все элементы $\mathbb{N}$

Пример. $\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$

Определение 3.2. Ординал — транзитивное множество, любой элемент которого — транзитивен.

Неформально — порядковый тип (отношение эквивалентности на всех множествах)

Утверждение 3.1. *α — ординал, тогда $\beta \subset \alpha$ — тоже.*

Доказательство. β — транзитивно, т.к. β — элемент ординала. $\gamma \in \beta \Rightarrow$ по транизитивности $\alpha \Rightarrow \gamma \in \alpha \Rightarrow \gamma$ — транзитивно. □

Утверждение 3.2. *α — ординал $\Rightarrow \alpha \cup \{\alpha\}$ — ординал.*

Доказательство.

$$\beta \in \alpha \cup \{\alpha\} \Rightarrow \beta \in \alpha \vee \beta = \alpha$$

В обоих случаях, β транзитивно. Теперь рассмотрим $\gamma \in \beta$.

$$\beta \in \alpha \Rightarrow \gamma \in \alpha$$
$$\beta = \alpha \Rightarrow \gamma \in \alpha$$

Т.к. α — транзитивно, то и γ — тоже. □

Утверждение 3.3. *Объединение любого множества ординалов — ординал.*

Доказательство.

$$\alpha = \bigcup_{i \in I} \alpha_i$$
$$\gamma \in \beta, \beta \in \alpha \Rightarrow \gamma \in \beta, \beta \in \alpha_i \Rightarrow \beta, \gamma \in \alpha_i$$

$\Rightarrow \beta, \gamma$ транзитивны □

Утверждение 3.4. *Ординал — ВУМ с отношением $\in$ (как строгого порядка)*

Доказательство.

1. Антирефлексивность: По Аксиоме фундированности, $\neg\exists x_1 \ni x_2 \ni x_3 \cdots \Rightarrow x \notin x$
2. Антисимметричность: $\neg\exists x, y(x \in y \wedge y \in x) \Rightarrow$
3. Транзитивность: по определению
4. Линейность: x — минимальный элемент, не сравнимый с кем-то, а y — минимальный, не сравнимый с x. $z \in x \Rightarrow z$ сравнимо с y.

   Но $z \neq y$, поэтому $y \in z \Rightarrow y \in x$, тогда $z \in y \Rightarrow x \subset y$.

   Теперь, $w \in y \Rightarrow w$ — сравним с $x, w \neq x$. $x \in w \Rightarrow x \in y$. Поэтому $w \in x (\Rightarrow y \subset x)$. Но тогда $x = y$, противоречие.

□

Утверждение 3.5. *α — ординал, $x \in \alpha \Rightarrow x = [0, x)$*

Доказательство. $y \in x \Rightarrow$ по транизитивности $y \in \alpha$. $y \in [0, x)$ (по определению начального отрезка). $y \in [0, x) \Rightarrow y < x \Leftrightarrow y \in x$ □

Теорема 3.1. *Любой ординал — ВУМ, с отношением порядка $\in$, при этом отношение "быть начальным отрезком" — тот же порядок. Подмножества являющиеся ординалами — тоьлко начальные отрезки. То есть $\in, \subset$, "быть начальным отрезком" — один и тот же порядок, называемый ординальным*

Доказательство. очев □

Теорема 3.2 (О сравнимости ординалов)**.** *α, β — ординалы $\Rightarrow \alpha = \beta, \alpha \in \beta, \beta \in \alpha$*

3.1 Конечные ординалы

$$
\begin{aligned}
&0 = \varnothing \\
&1 = \{\varnothing\} \\
&2 = \{\varnothing, \{\varnothing\}\} \\
&\vdots \\
&n + 1 = \{0, 1, 2, \ldots n\}
\end{aligned}
$$

3.2 Сложение ординалов

Неформально: A — ВУМ, $A \cong \alpha$ — ординал; B — ВУМ, $B \cong \beta$ — ординал, тогда $\alpha + \beta$ — ординал, изоморфный $A + B$

Формально:

1. $\alpha + 0 = \alpha$
2. $\alpha + (\beta + 1) = (\alpha + \beta) + 1$
3. $\alpha + \bigcup \gamma_i = \bigcup(\alpha + \gamma_i)$

Замечание.

$$1 + \omega = 1 + \bigcup n = \bigcup (1 + n) = \omega \neq \omega + 1$$

Утверждение 3.6.

$$B \neq \varnothing \Rightarrow A + B \ncong A$$

$$\beta > 0 \Rightarrow \alpha + \beta > \alpha$$

Доказательство. Верно, т.к. α — начальный отрезок $\alpha + \beta$ □

Теорема 3.3 (О вычитании)**.** $\alpha \geqslant \beta \Rightarrow \exists! \gamma : \beta + \gamma = \alpha$

Доказательство. Рассмотрим $A \cong \alpha, B \cong \beta \Rightarrow C = A \setminus B$. Тогда C — ВУМ, γ — ординал, $\cong C$. □

3.3 Умножение ординалов

$\alpha \cdot \beta$ — ординал, изоморфный $A \cdot B$ (обратный лексикографический порядок)

1. $\alpha \cdot 0 = 0$
2. $\alpha \cdot (\beta + 1) = \alpha\beta + \alpha$
3. $\alpha \cdot (\bigcup \gamma_i) = \bigcup (\alpha + \gamma_i)$

Замечание.

$$2 \cdot \omega = \omega, \omega \cdot 2 = \omega + \omega \neq \omega$$

Теорема 3.4 (О делении с остатком)**.** *Пусть* $\alpha \neq 0, \beta$ *— ординалы. Тогда* $\exists! \gamma, \delta : \beta = \alpha \cdot \gamma + \delta, \delta < \alpha$

Доказательство. Пусть μ таково, что $\alpha \cdot \mu > \beta$ □

3.4 Возведение в степень

1. $\alpha^0 = 1$
2. $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$
3. $\alpha^{\bigcup \gamma_i} = \bigcup \alpha^{\gamma_i}$

Замечание.

$$2^\omega = \omega$$

3.4.1 ВУМ, изоморфный α^β

Рассмотрим все функции, которые $\neq 0$ на конечном числе элементов. Тогда: $f > g$, если:

1. $\underbrace{\max\{x|f(x) \neq 0\}}_{m_f} > \underbrace{\max\{x|g(x) \neq 0\}}_{m_g}$
2. $m_f = m_g, f(m_f) > g(m_g)$
3. $m_f = m_g, f(m_f) = g(m_g), \{x < m_f | f(x) \neq 0\} > \max\{x < m_g | g(x) \neq 0\}$

Или: рассмотрим конечное число точек, где $f \neq 0 \vee g \neq 0$, сравниваем обратно лексикографически.

Замечание. 2^ω по этому определению — обратная двоичная запись натуральных чисел

Теорема 3.5 (Об ординарной системе счисления)**.** *Пусть $\gamma < \alpha^\beta$. Тогда $\exists!$ представление $\gamma = \alpha^{\beta_1} \cdot \alpha_1 + \alpha^{\beta_2} \cdot \alpha_2 + \cdots + \alpha^{\beta_n} \cdot \alpha_n$, где $\beta > \beta_1 > \beta_2 > \cdots > \beta_n, \alpha_i < \alpha$*

4 Лемма Цорна, Теорема Цермело

Теорема 4.1. *Если A, B бесконечны, то $A \cup B \cong A \times B \cong \max\{A, B\}$*

Утверждение 4.1 (Аксиома Выбора)**.** *Пусть A — множество. Тогда существует $\varphi : 2^A \setminus \{A\} \to A : \forall S \subsetneq A \;\; \varphi(S) \notin S$*

Определение 4.1. $(S, \leqslant_S)$ — корректный фрагмент множества A, если

1. $S \subset A$
2. $(S, \leqslant_S)$ — ВУМ
3. $\forall x \in S \;\; x = \varphi([0, x)_S)$, где φ — функция из аксиомы выбора

Лемма 4.1. *Если S, T — корректные фрагменты, то тогда S — начальный отрезок T, или T — начальный отрезок S*

Доказательство. По теореме о сравнимости, $T \cong [0, S)$, или $T \cong S$, или $S \cong [0, T)$. Докажем, что изоморфизм тождественнен Б.О.О. $T \cong [0, S)$. Пусть $\mu : [0, S) \to T$ — изоморфизм. Пусть x — минимальный элемент, такой, что $\mu(x) \neq x$. Но тогда, т.к. x — минимальный такой элемент, тогда $[0, x)_S = [0, x)_T \Rightarrow x = \varphi([0, x)_S) = \varphi([0, x)_T) \Rightarrow x \in T$. Но тогда $\Rightarrow \mu(x) <_T x \vee \mu(x) >_T x$. Предположим, что $\mu(x) > x$, тогда $z = \mu^{-1}(x) >_S x \Rightarrow \mu(z) = x <_T \mu(x)$. Если $\mu(x) < x$, тогда $\mu(\mu(x)) < \mu(x) < x$, противоречие с тем, что x — минимальный $\square$

Лемма 4.2. *Объединение $S = \bigcup S_i$ любого множества корректных фрагментов является корректным фрагментом относительно порядка $x \leqslant_S y$, если $\exists i \;\; x \leqslant_{S_i} y$*

Доказательство. Докажем все свойства корректного фрагмента:

1. **Рефлексивность.** $x \leqslant_S x$

$$x \in S \Rightarrow \exists i : x \in S_i \Rightarrow x \leqslant_{S_i} x \Rightarrow x \leqslant_S x$$

2. **Антисимметричность.** $x \leqslant_S y, y \leqslant_S x \Rightarrow x = y$.

$$\exists i, j : x \leqslant_{S_i} y, x \geqslant_{S_j} y$$

При этом, Б.О.О, S_i — начальный отрезок S_j. Тогда $x \leqslant_{S_j} y, x \geqslant_{S_j} y \Rightarrow x = y$

3. **Транзитивность.** $x \leqslant_S y, y \leqslant_S z \Rightarrow x \leqslant_S z$

$$x \leqslant_{S_i} y, y \leqslant_{S_j} z$$

При этом, Б.О.О, S_i — начальный отрезок S_j. Тогда $x \leqslant_{S_j} y, y \geqslant_{S_j} z \Rightarrow x \leqslant_{S_j} z$

4. **Линейность.** Линейность. $x \in S_i, y \in S_j$, при этом, Б.О.О, S_i — начальный отрезок S_j. Тогда x, y сравимы отношением $\leqslant_{S_j}$

5. **Фундированность.** Пусть $x_1 \geqslant_S x_2 \geqslant_S x_3 \ldots$, где $x_k \in S_{i_k}$. Докажем, что $x_k \in S_{i_1}$. Действительно, в проивном случае $S_{i_k} \not\subset S_{i_1}$, но $x_k \leqslant x_1$, и, т.к. S_{i_1} — начальный отрезок S_{i_k} и $x_k \leqslant x_1$, то $x_k \in S_{i_1}$. Но тогда в эта бесконечная последовательность стабилизируется, из чего следует, что наше множесво — ВУМ

6. **Корректность.**

$$x \in S \Rightarrow x = \varphi([0, x)_S)$$

$$x \in S_i, y \leqslant_S x \Leftrightarrow y \leqslant_{S_i} x$$

$$[0, x)_S = [0, x)_{S_i}$$

Но тогда $x = \varphi([0, x)_{S_i}) = \varphi([0, x)_S)$, т.к. S_i — корректный фрагмент.

□

Лемма 4.3. *Объединение всех корректных фрагментов является исходым множеством*

Доказательство. Пусть объединение всех корректных фрагментов дало $B \subseteq A$. Тогда $B \cup \{\varphi(B)\}$ — тоже корректный фрагмент. Проиворечие с тем, что B содержало все корректные фрагменты. □

Теорема 4.2 (Цермело)**.** $\forall A \exists B$ *— ВУМ, такой, что* $B \cong A$

Доказательство. Объединение всех корректных фрагментов будет являться ВУМом и будет равно исходному множеству. □

Следствие. Любые два множества сравнимы по мощности

Определение 4.2. Пусть A — ЧУМ. Цепь в нем — его линейно упорядоченное подмножество

Определение 4.3. Пусть A — ЧУМ, $S \subset A$. Верхняя грань S — такой элемент $b \in A$, что $\forall x \in S x \leqslant b$.

Лемма 4.4 (Цорна)**.** *Пусть у любой цепи есть верхняя грань. Тогда в* A *есть максимальный элемент, более того,* $\forall x \in A \exists$ *максимальный элемент* $m \geqslant x$

Доказательство. Пусь I — ВУМ, мощнее A. Построим функцию $f : I \to A, f(y) =$ элемент, больший всех элементов $f([0, y))$. По теореме о трансфинитной рекурсии, $\exists! f$, удовлетворяющая такому условию. f — инъективно $\Rightarrow$ f определена на начальном отрезке $[0, S)$. Образ $f([0, S))$ — цепь в A. По условию леммы, у $f([0, S))$ есть верхняя грань m. $m \notin f([0, S)) \Rightarrow$ можно доопределить $m = f(S)$. Если m — не максимальный, то можно доопределить $f(s) = w > m$. □

4.1 Приложения Леммы Цорна и Теоремы Цермело

Теорема 4.3. *Любой порядок монжо дополнить до линейного*

Доказательство. Пусть R — порядок на множестве X. Рассмотрим A — множество всех порядков на X, и упорядочим A по вложению. Цепь в A — набор порядков, где следующий продолжает предыдущий.

Утверждение 4.2. *Обьединение порядков цепи — порядок.*

Доказательство. Пусть $\{\leqslant_i\}_{i\in I}$ — цепь. Обозначим $a \leqslant b \Leftrightarrow \exists i : a \leqslant_i b$. Докажем, что $\leqslant$ — порядок

Рефлексивность: $\forall i a \leqslant_i a \Rightarrow a \leqslant a$

Антисимметричность: $a \leqslant_i b, b \leqslant_j a \Rightarrow a \leqslant_{\max(i,j)} b, a \geqslant_{\max(i,j)} b \Rightarrow a = b$

Транзитивность: $a \leqslant_i b, b \leqslant_j c \Rightarrow a \leqslant_{\max(i,j)} b, b \leqslant_{\max(i,j)} c \Rightarrow a \leqslant_{\max(i,j)} c \Rightarrow a \leqslant c$

□

Заметим, что тогда в нашем множестве у любой цепи есть верхняя грань (обьединение всех элементов цепи). Тогда существует максимальный порядок $\leqslant$, такой, что "$\leqslant$" $\geqslant$ "R". Докажем, что $\leqslant$ — линейный. Предположим противное. Тогда существуют несравнимые a, b. Положим $x \leqslant' y \Leftrightarrow \left[\begin{array}{l} x \leqslant y \\ x \leqslant a, b \leqslant y \end{array}\right.$. Докажем, что тогда $\leqslant'$ — порядок.

Рефлексивность: $a \leqslant a$ — выполнено

Антисимметричность: $x \leqslant a, b \leqslant y, y \leqslant a, b \leqslant x \Rightarrow b \leqslant a$ — противоречие.

Транзитивность: $x \leqslant' y, y \leqslant' z$. Несколько случаев разбираются достаточно просто

□

Теорема 4.4. *A — конечно, B бесконечно, тогда $B \cong A \cup B$.*

Теорема 4.5. *A — бесконечно $\Rightarrow A \cong A \times \mathbb{N}$.*

Доказательство. По теореме Цермело, $\exists S$ — ВУМ, такой, что $S \cong A$. Но $S = \omega L + R$ для некоторых L и конечного R. Но тогда S равномощно $\omega L \cong L \times \mathbb{N} \Rightarrow A \cong L \times \mathbb{N} \cong L \times (\mathbb{N} \times \mathbb{N}) \cong A \times \mathbb{N}$. □

Теорема 4.6. *A, B — бесконечны, тогда $A \cup B \cong \max\{A, B\}$*

Доказательство. Б.О.О, $A \geqslant B$. Тогда $A \cup B \lesssim A \times \{0, 1\} \lesssim A \times \mathbb{N} \cong A \lesssim A \cup B$. Тогда по Теореме Кантора-Бернштейна, $A \cong A \cup B$ □

Теорема 4.7. *A — бесконечно $\Rightarrow A \cong A^2$*

Доказательство. Построим ЧУМ из пар (X, f), таких, что f — биекция из $X \to X^2$, $X \subset A$. Определим $(X, f) \leqslant (Y, g) \Leftrightarrow \left\{\begin{array}{l} X \subset Y \\ g|_x \equiv f \end{array}\right.$. Докажем, что выполнено условие Леммы Цорна. Цепь $\{(X_i, f_i)\}_{i\in I}$. Рассмотрим (X, f), где $X = \bigcup_{i\in I} X_i, f(x) = f_i(x) \Leftrightarrow x \in X_i$. Заметим, что $\bigcup_{i\in I} X_i \subset A$, и $x \in X_i \cap X_j \Rightarrow$ Б.О.О. $X_i \subset X_j \Rightarrow f_j|_{X_i} = f_i \Rightarrow f_i(x) = f_j(x)$. Тогда эта пара корректна. Проверим, что f — биекция $X \to X^2$.

Инъективность: Пусть $f(x) = f(y), x \neq y$. При этом, $x \in X_i, y \in X_j$, Б.О.О. $X_i \subset X_j \Rightarrow f_j(x) = f_j(y)$ — не инъективно, противоречие.

Сюрьективность: Пусть $(x, y) \in X^2, x \in X_i, y \in X_j$. Б.О.О. $X_i \subset X_j \Rightarrow (x, y) \in X_j^2 \Rightarrow \exists z : f_j(z) = (x, y) \Rightarrow f(z) = (x, y)$.

Теперь, пусть (M, h) — какой-то максимальный элемент, такой, что M бесконечно.

1. $M \cong A \Rightarrow A \cong M \cong M^2 \cong A$
2. $M \lesssim A \Rightarrow A \setminus M \cong A \Rightarrow M \lesssim A \setminus M \to \exists Q \subset A \setminus M, Q \cong M$. Но тогда $Q \cong Q^2 \cong Q^2 \times \{0, 1, 2\} \cong \mathbb{Q}^2 \cup (Q \times M) \cup (M \times Q)$. Обозначим за b биекцию между множествами $Q, \mathbb{Q}^2 \cup (Q \times M) \cup (M \times Q)$. Положим $f' = \begin{cases} f(x), x \in M \\ b(x), x \in Q \end{cases}$. Заметим, что $f' : (M \cup Q) \to (M \cup Q)^2$ — биекция, противоречие, т.к. (M, f) — не максимальный элемент

□

Определение 4.4. Базис Гамеля в пространстве $\mathbb{R}$ над $\mathbb{Q}$ — такое множество H, что

1. $\alpha_1 h_1 + \cdots + \alpha_n h_n = 0, \alpha_i \in Q, h_i \in H \Rightarrow \alpha_i = 0$
2. $\forall x \in \mathbb{R} \exists n \exists \{h_1, \dots h_n\} \subset H, \exists \{\alpha_1 \dots \alpha_n\} \subset \mathbb{Q}$

Теорема 4.8. *Базис Гамеля существует.*

Доказательство. По Лемме Цорна, рассмотрим линейно независимые над $\mathbb{Q}$ системы с отношением подмножества. Рассмотрим объединение элементов некоторой цепи. Оно тоже будет линейно независимо, т.к. любое конечное подмножество этого множества будет линейно независимо. Тогда в любой цепи есть максимум. Выберем его, он будет базисом Гамеля □

Теорема 4.9. *Существует такая функция $f : \mathbb{R} \to \mathbb{R}$, такая, что верно следующее: $f(x + y) = f(x) + f(y)$, но $\nexists \alpha : \forall x f(x) = \alpha x$.*

Доказательство. Рассмотрим функцию, которая меняет местами две координаты в базисе Гамиля при числах a, b. Заметим, что $f(0) = 0$. При этом $f(a) = b, f(b) = a$. Но тогда $\alpha = \frac{a}{b} = \frac{b}{a}$, противоречие, т.к. $b \neq a$. □

5 Теория вычислимости

5.1 Алгоритм

Неформально: алгоритм — это процедура, преображающая данные, закодированные конечными словами, которая тоже имеет конечное описание и выполняется пошагово

Пример (Не алгоритм)**.** Метод Ньютона нахождения нуля дифференцируемой. Не является алгоритмом, т.к. нельзя сделать предельный переход, однако, если установить точность с которой мы хотим узнать корень, тогда норм.

Пример (Не алгоритм)**.** Метод дележа пирога. Есть пирог, хотим поделить его. Берем нож и несем его над пирогом. Второй человек говорит, когда нам остановиться. Тогда мы и режем пирог. Не является алгоритмом, т.к. время тут не дискретно.

5.2 Однолетночная машина Тьюринга

Однолентоочная машина Тьюринга

$\dots$	m	a	t	l	o	g	$\dots$

Есть бесокнечная в обе стороны лента (см. выше), в которой хранятся некоторые символы некоторого алфавита. Машина тьюринга представляет собой функцию от этой ленты: $qa \mapsto rbD$

1. q — текущее состояние машины
2. a — символ в ячейке, на которую смотрит машина Тьюринга
3. r — новое состояние машины
4. b — новый символ в ячейке
5. D — направление сдвига L, N, R

Итак, формально:

Определение 5.1. Машина Тьюринга — это кортеж $(\Sigma, \Gamma, Q, q_1, q_0, \delta)$, где $Sigma, \Gamma, Q$ — конечные множества

1. Σ — входной алфавит
2. $\Gamma \supset \Sigma$ — ленточный алфавит. $\#$ — пробел, принадлежит $\Gamma \setminus \Sigma$
3. $Q \cap \Gamma = \varnothing$ — множество состояний
4. $q_1, q_0 \in Q$ — начальное и кончное состояния соответственно
5. $\delta : Q \times \Gamma \to Q \times \Gamma \times \{L, N, R\}$

Удобно записывать состояние машины Тьюринга так:

$$AqaB$$

1. a — символ, на который мы сейчас смотрим
2. q — состояние машины в данный момент
3. A, B — лента до и после символа, на который мы смотрим, соответственно

Определение 5.2. Вычисление — последовательность конфигураций, где каждая следующая получается из предыдущей по правилу Машины Тьюринга

Определение 5.3. Функция $f : \Sigma^* \to \Sigma^*$ называется вычислимой, если существует Машина Тьюринга, такая, что

$$\forall x \begin{cases} f(x) \text{ определена } \Rightarrow M(x) = f(x) \\ f(x) \text{ не определена } \Rightarrow M(x) \text{не останавливается} \end{cases}$$

Заметим, что Машин Тьюринга счетное множество, а функций $\Sigma^* \to \Sigma^*$ континуум $\Rightarrow \exists$ невычислимые функции.

Утверждение 5.1. *У f конечная область определения $\Rightarrow$ f вычислима*

Утверждение 5.2. *f, g — вычислимы $\Rightarrow$ $f \circ g$ — тоже*

Определение 5.4. $S \subset \Sigma^*$ разрешимо, если $\exists$ Машина Тьюринга с бинарным ответом, такая, что $M(x) \begin{cases} 1, x \in S \\ 0, x \notin S \end{cases}$ Иначе говоря, S разрешимо, если $\chi_S(x) = \begin{cases} 1, x \in S \\ 0, x \notin S \end{cases}$ вычислима

Утверждение 5.3. *S — конечное $\Rightarrow$ S разрешимо*

Утверждение 5.4. *S, T — разрешимы $\Rightarrow$ $S \cup T, S \cap T, \overline{S}$ — тоже*

Замечание. Подмножество разрешимого множества может быть неразрешимо.

Теорема 5.1 (Критерий Разрешимости)**.** *S разрешимо $\Leftrightarrow$ S можно перечислить по возрастанию*

Доказательство.

$\Rightarrow$
```
for i in 0, 1, 2...
    if i in S:
        print i
```

$\Leftarrow$ Пусть S бесконечно, а на вход подается x. Печатаем элементы, пока они $< x$. Тогда первый элемент, на котором это сломается будет либо равен x, либо будет $> x$. В первом случае выдаем 1, иначе 0. Для конечных оно и так разрешимо.

□

Определение 5.5. Множество называется перечислимым, если существует Машина Тьюринга, которая выводит все его элеметы S и только их

Теорема 5.2 (Поста)**.** *S разрешимо $\Leftrightarrow$ $S, \overline{S}$ перечислимы*

Доказательство.

$\Rightarrow$ пробегаемся по Σ^*, и, если элемент $\in S$, то выводим его. Аналогично для $\overline{S}$

$\Leftarrow$ По очереди перечисляем элементы $S, \overline{S}$. Рано или поздно мы встретим $x \Rightarrow$ выведем, где мы его встретили, в S или $\overline{S}$. □

5.3 Свойства, эквивалентные перечислимости

Далее будем считать, что наш алфавит — $\{0, 1\}$.

1. Можно выводить все элементы, но без повторов
2. Вычислима полухарактеристическая функция $\overline{\chi_A}(x) = \begin{cases} 1, x \in A \\ \text{не определено, } x \notin A \end{cases}$
3. A — область определения некоторой вычислимой функции
4. A — область значений некоторой вычислимой функции
5. $A = \varnothing$ или A — область значений всюду вычислимой функции.
6. A — проекция разрешимого множества пар $A = \{x | \exists y (x, y) \in B\}$, где $B \subset \{0, 1\}^* \times \{0, 1\}^*$

Утверждение 5.5. *A вычислимо $\Rightarrow$ 2)*

Доказательство.

```
chi_A(x) {
    fot i in A {
        if i == x { // если встретим x, то вернем 1
            return 1;
        }
    }
}
```

□

Утверждение 5.6. *2) $\Rightarrow$ 3)*

Доказательство. $A = Dom\ \overline{\chi_A(x)}$ □

Утверждение 5.7. *3) $\Rightarrow$ 4)*

Доказательство. Рассмотрим `f'(x)`:

```
f'(x) {
    f(x);
    return x;
}
```

Тогда $f'(x) = \begin{cases} x, x \in Dom\ f \\ \text{не определено, иначе} \end{cases}$ Заметим, что $Rad\ f' = Dom\ f$. □

Утверждение 5.8. *4) $\Rightarrow$ 5)*

Доказательство. Пусть $A = Ran\ f$. Если $A \neq \varnothing$, то положим a_0 — произвольный элемент в a_0. Положим $f' : \{0,1\}^* \times \mathbb{N} \to \{0,1\}^*$, так, что

$$f'(x,t) = \begin{cases} f(x), \text{ если } f(x) \text{ остановится за } t \text{ шагов} \\ a_0, \text{ иначе} \end{cases}$$

Заметим, что $Ran\ f = Ran\ f'$, а f' — вычислима. □

Утверждение 5.9. *5) ⇒ 6)*

Доказательство. Пусть $A = Ran\ f$. Положим $B = \{(y,(x,t)) : f(x) = y \text{ за } t \text{ шагов}\}$. □

Утверждение 5.10. *6) ⇒ A вычислимо*

Доказательство. Обойдем все пары (x,y), и, если $(x,y) \in B \Rightarrow$ печатаем x. □

5.4 Универсальная машина Тьюринга

Гарвардская архитектура машины — когда есть фиксированная программа и данные, с которыми она работает.

Принстонская архитектура машины — когда есть некоторый процессор, который может запускать различные программы, которые, в свою очередь, будут взаимодействовать с данными

Определение 5.6. Универсальная Машина Тьюринга — такая функция $U(M,x) = M(x)$ — по сути, машина, которая запускает машину M с вводом x.

Определение 5.7. Будем считать, что код Машины Тьюринга записан (как-то) последовательностью $0,1$. Фунуция $U : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ называется универсальной вычислимой функцией, если

1. U вычислима как функция от двух аргументов
2. $\forall f : \{0,1\}^* \to \{0,1\}^*$, где f — вычислима, верно $\exists p \forall x\ U(p,x) = f(x)$

Теорема 5.3. *Универсальная Машина Тьюринга существует.*

5.5 Тезис Черча-Тьюринга

Подробнее...

5.6 Проблема самоприменимости

Пусть нам дана УМТ U. Рассмотрим $S = \{p | U(p,p) \text{ остановится}\}$

Теорема 5.4 (Тьюринга)**.** *S — перечислимо, неразрешимо*

Доказательство.

Перечислимость: S перечислимо, т.к. $S = Dom\ d(p) = U(p,p)$ — область определения вычислимой функции

Нерезрешимость: от противного. Пусть S разрешимо $\Leftrightarrow \chi_S$ вычислимо. Рассмотрим

$$f(x) = \begin{cases} 0, \chi_S(x) = 0 \\ \neq U(x,x), \chi_S(x) = 1 \end{cases}$$

Т.к. $U(p,p)$ — УВФ, то $\exists q \forall x U(q,x) = f(x)$.

(a) $q \in S \Rightarrow U(q,q) = f(q) \neq U(q,q)$

(b) $q \notin S \Rightarrow f(q) = 0$, но $U(q,q)$ не определено

Получили противоречие.

□

5.7 Проблема остановки

$H = \{(p,x) | U(p,x) \text{ остановится}\}$

Теорема 5.5. *H — перечислимо, неразрешимо*

Доказательство.

Перечислимость: H перечислимо, т.к. $S = Dom\ U(p,x)$ — область определения вычислимой функции

Нерезрешимость: от противного. Пусть H разрешимо, но тогда и $S = H \cap D$ тоже разрешимо, где $D = \{(p,p) | p \text{ проивольное}\}$, противоречие, т.к. S неразрешимо.

□

Рассмотрим множества:

1. $C = \{p | \forall x, y (U(p,x), U(p,y) \text{ определены } \Rightarrow U(p,x) = U(p,y))\}$
2. $T = \{p | \forall x (U(p,x) \text{ определено})\}$
3. $FD = \{p | \{x | U(p,x) \text{ определено}\} \text{ конечно}\}$

Определение 5.8. Множество X называется коперечислимым, если $\overline{X}$ перечислимо

Утверждение 5.11. *C — коперечислимо, неразрешимо*

Доказательство. $\overline{C} = \{p | \exists (x,y,t,s)\ \ U(p,x) \text{ ост. за } t \text{ шагов}, U(p,y) \text{ ост. за } s \text{ шагов}, U(p,x) \neq U(p,y)\}$, а оно перечислимо □

Утверждение 5.12. *T, FD — некоперечислимо, некоперечислимо*

5.8 m-сводимость

Определение 5.9. $A \leqslant_m B$, если $\exists$ вычислимая всюду определенная функция $f : \{0,1\}^* \to \{0,1\}^*$, такая, что $\forall x (x \in A \Leftrightarrow f(x) \in B)$.

5.8.1 Свойства m-сводимости

Утверждение 5.13. *$A \leqslant_m B, B$ разрешимо $\Rightarrow A$ — разрешимо*

Доказательство. $\chi_A(x) = \chi_B(f(x))$ □

Утверждение 5.14. $A \leqslant_m B \Leftrightarrow \overline{A} \leqslant_m \overline{B}$

Утверждение 5.15. $A \leqslant_m B, B \leqslant_m C \Leftrightarrow A \leqslant_m C$

Замечание. Т.к. $A \leqslant_m A$, получили, что $\leqslant_m$ — предпорядок

Утверждение 5.16. *$A \leqslant_m B, B$ перечислимо $\Rightarrow A$ — перечислимо*

Следствие. $A \leqslant_m B, A$ неперечислимо $\Rightarrow B$ неперечислимо

5.9 Как получать новые неперечислимые множества?

Докажем, что T неперечислимо и некоперечислимо. Заметим, что $\overline{H}$ — неперечислимое множество. Если мы покажем, что

$$\begin{cases} \overline{H} \leqslant_m T \\ \overline{H} \leqslant_m \overline{T} \end{cases}$$

То мы получим, что T — неперечислимо, некоперечислимо. Однако, удобнее доказывать, что

$$\begin{cases} H \leqslant_m T(1) \\ H \leqslant_m \overline{T}(2) \end{cases}$$

Для этого

1. $(p, x) \mapsto q$, так, что $\forall y U(q, y) = U(p, x)$. Тогда $q \in H \Leftrightarrow q \in T$
2. $(p, x) \mapsto q$, так, что

$$U(q, y) = \begin{cases} 1, \text{ если } U(p, x) \text{ не оставновится за } y \text{ шагов} \\ \text{не определено, иначе} \end{cases}$$

$$(p, x) \in H \Rightarrow \exists t \forall y \geqslant t U(q, y) \text{ не определено } \Rightarrow q \notin T$$

$$(p, x) \notin H \Rightarrow \forall y U(q, y) = 1 \Rightarrow q \in T$$

Получили T, неперечислимое и некоперечислимое.

5.10 Существует ли универасальная тотально вычислимая функция?

Что мы хотим: $U_T : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$, такую, что

1. $\forall p, x \; U_T(p, x)$ определена
2. U_T вычислима
3. $\forall f : \{0,1\}^* \to \{0,1\}^*$, такая, что f — вычислима, всюду определена и $\exists p \forall x f(x) = U_T(p, x)$

Утверждение 5.17. $\nexists U_T$

Доказательство. Иначе рассмотрим $d'(x) = U_T(x,x) + 1$. Тогда $\exists p \forall x\ d'(x) = U_T(p,x) = d'(p) \Rightarrow U_T(p,p) + 1 = U_T(p,p)$ □

Рассмотрим множество $NED = \{p | \exists x U(p,x)$ определено$\}$. Оно перечислимо (можно добавить квантор, указывающий, за какое число шагов).

Утверждение 5.18. *$\overline{NED}$ неперечислимо*

Доказательство. Покажем, что $H \leqslant_m NED \Leftrightarrow \overline{H} \leqslant_m \overline{NED}$. Сопоставим $(p,x) \mapsto q$, так, что

$$U(q,y) = \begin{cases} \text{не определено}, U(p,x) \text{ не остановится за } y \text{ шагов} \\ 1, \text{ иначе} \end{cases}, (p,x) \in H \Leftrightarrow q \in NED$$

Пусть $p_1, p_2, \ldots$ — перечисление $\overline{NED}$. Рассмотрим

$$U'(n,x) = \begin{cases} \text{не определено, если } n = 0 \\ U(p_n, x), n > 0 \end{cases}$$

Заметим, что $NED_{U'} = \{n | \exists x U'(n,x)$ определено$\} = \mathbb{N} \setminus \{0\}$ — разрешимо □

Определение 5.10. $U : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ — главная универсальная вычислимая функция, если

1. U вычислима как функция от двух аргументов
2. $\forall f : \mathbb{N} \to \mathbb{N}$ — вычислимой $\exists p : U(p,x) = f(x)$.
3. $\forall V : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ — вычислимой $\exists$ вычислимая и всюду определенная $s : \mathbb{N} \to \mathbb{N}$, такая, что $\forall p \forall x V(p,x) = U(s(p), x)$.

Теорема 5.6. *Главная Универсальная Вычислимая Функция существует*

Первое доказательство. УМТ задает ГУВФ. V вычислима $\Rightarrow$ V вычисляется некоторой машиной M. Пусть p — программа для V. Тогда если мы положим $s(p)$ — машина M с фиксированным первым аргументом, то получим желаемое □

Второе доказательство. Рассмотрим вычислимую $W : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, универсальную для вычислимых функций от двух аргументов, то есть

$$\forall V : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \exists q \forall p \forall x W(q,p,x) = V(p,x)$$

□

Теорема 5.7 (Райса-Успенского)**.** *$\mathcal{A}$ — множество вычислимых функций, причем $\mathcal{A}, \overline{\mathcal{A}} \neq \varnothing$. Пусть U — ГУВФ, $A = \{p | U(p,\cdot) \in \mathcal{A}\}$. Тогда A неразрешимо*

Доказательство. Рассмотрим $\zeta(x)$ — нигде не определенную функцию. Т.к. $\overline{\mathcal{A}} \neq \varnothing \Rightarrow \exists \xi \in \mathcal{A}$. Рассотрим K — перечислимое, но не разрешимое множество. Положим:

$$V(p,x) = \begin{cases} \xi(x), p \in K \\ \zeta(x), p \notin K \end{cases}$$

$\exists s \forall p \forall x V(p,x) = U(s(p), x)$.

1. $p \in K \Rightarrow U(s(p), x) = \xi(x) \Rightarrow s(p) \notin A$
2. $p \notin K \Rightarrow U(s(p), x) = \zeta(x) \Rightarrow s(p) \in A$

Тогда $p \in K \Leftrightarrow s(p) \notin A \Rightarrow K \leqslant_m \overline{A} \Rightarrow A$ — нерзрешимо □

Теорема 5.8 (Фридберга)**.**

$$\exists V : \forall f \ - \textit{вычислимой } \exists! p : \forall x V(p, x) = f(x)$$

Определение 5.11. Куайн — программа, печатающая свой текст. Например:

```
Напечатать дважды, взяв вторую копию в кавычки:"Напечатать дважды, взяв вторую к
```

Теорема 5.9 (Клини о неподвижной точке)**.** *Пусть U — ГУВФ, $h : \mathbb{N} \times \mathbb{N}$ — вычислимая всюду определенная функция. Тогда $\exists p \forall x U(p, x) = U(h(p), x)$*

Следствие. Существует Куайн.

Доделаю потом

6 Связь этого бреда с языками первого порядка

6.1 Арифметическая иерархия

В прошлом мы рассматривали свойства *Перечислимость*, *Коперечислимость*, а их пересечение давало нам *Разрешимость*. Также мы рассматривали множества:

$$H = \{(p, x) | U(p, x) \text{ определено}\}$$

$$ED \text{ (Empty Domain)} = \{p | \forall x U(p, x) \text{ не определено}\}$$

$$T = \{p | \forall x U(p, x) \text{ определено}\}$$

$$FD \text{ (Finite Domain)} = \{p | \{x | U(p, x) \text{ определено}\} \text{ конечно}\}$$

Заметим, что эти определения этих множеств можно записать так:

$$(p, x) \in H \Leftrightarrow \exists t (U(p, x) \text{ остановится за } \leqslant t \text{ шагов})$$

$$p \in ED \Leftrightarrow \forall (t, x) (U(p, x) \text{ не остановится за } t \text{ шагов})$$

$$p \in T \Leftrightarrow \forall x \exists t (U(p, x) \text{ остановится за } \leqslant t \text{ шагов})$$

$$p \in FD \Leftrightarrow \exists N \forall (t, x) (x > N \to U(p, x) \text{ не остановится за } t \text{ шагов})$$

Определение 6.1. $A \in \Sigma_k$, если существует разрешимый предикат R, такой, что

$$\forall x (x \in A \Leftrightarrow \exists y_1 \forall y_2 \exists y_3 \ldots \overset{\forall}{\exists} y_k R(x, y_1, y_2, \ldots y_k))$$

Определение 6.2. $B \in \Pi_k$, если существует разрешимый предикат R, такой, что

$$\forall x (x \in B \Leftrightarrow \forall y_1 \exists y_2 \forall y_3 \ldots \overset{\forall}{\exists} y_k R(x, y_1, y_2, \ldots y_k))$$

Итак, по определениям выше:

1. Разрешимые множества $= \Sigma_0 = \Pi_0$
2. Перечислимые множества $= \Sigma_1$
3. Коперечислимые множества $= \Pi_1$

Теорема 6.1. $\Sigma_i \subset \Sigma_{i+1}, \Sigma_i \subset \Pi_{i+1}, \Pi_i \subset \Sigma_{i+1}, \Pi_i \subset \Pi_{i+1}$

Доказательство. В предикате R добавим фиктивный аргумент — тогда квантор, соответствующий ему можно поставить в любое место формулы. Если поставить его в начало и в конец, получим желаемое. □

Теорема 6.2 (б/д)**.** $\Sigma_i \subsetneq \Sigma_{i+1}, \Sigma_i \subsetneq \Pi_{i+1}, \Pi_i \subsetneq \Sigma_{i+1}, \Pi_i \subsetneq \Pi_{i+1}$

Утверждение 6.1. $A \in \Sigma_k \Leftrightarrow \overline{A} \in \Pi_k$

Утверждение 6.2. $x \in \overline{A} \Leftrightarrow \neg\exists y_1 \forall y_2 \dots \exists y_k R(x, y_1, \dots y_k) \Leftrightarrow \forall y_1 \exists y_2 \dots \forall y_k \neg R(x, y_1, \dots y_k)$

Утверждение 6.3. $A, B \in \Sigma_k \Rightarrow A \cap B \in \Sigma_k$

Доказательство.

$$x \in A \cap B \Leftrightarrow (x \in A \wedge x \in B) \Leftrightarrow (\exists y_1 \forall y_2 \dots \exists y_k R(x, y_1, \dots y_k) \wedge \exists z_1 \forall z_2 \dots \exists z_k Q(x, z_1, \dots z_k)) \Leftrightarrow$$

$$\Leftrightarrow \exists y_1 \exists z_1 \forall y_2 \forall z_2 \dots \exists y_k \exists z_k (R(x, y_1, \dots y_k) \wedge Q(x, z_1, \dots z_k)) \Leftrightarrow$$

$$\exists (y_1, z_1) \forall (y_2, z_2) \dots \exists (y_k, z_k)(R(x, y_1, \dots y_k) \wedge Q(x, z_1, \dots z_k))$$

□

Рассмотрим следующий язык:

Определение 6.3. Язык арифметики: $\langle 0, S, =, +, \cdot \rangle$

Определение 6.4. Предикат $P : \mathbb{N}^k \to \{0, 1\}$ называется выразимым в арифметики (или арифметичным), если существует формула φ с k параметрами, такая, что $P(x_1, \dots x_k) = 1 \Leftrightarrow \varphi(x_1, \dots x_k)$ истинно

Пример.

1. $x \geqslant y \Leftrightarrow \exists z \; x = y + z$
2. $x \vdots y \Leftrightarrow \exists z \; x = y \cdot z$
3. p — простое $\Leftrightarrow (p > 1 \wedge (\forall q(p \vdots q \to (q = p \vee q = 1))))$
4. $d = \text{НОД}(x, y) \Leftrightarrow (x \vdots d \wedge y \vdots d \wedge \forall t((x \vdots t \wedge y \vdots t) \to d \vdots t))$
5. S — степень 2 $\Leftrightarrow \forall d(s \vdots d \to d = 1 \vee d \vdots 2)$
6. S — степень 4 $\Leftrightarrow \exists q : (q$ степень 2 $\wedge s = q^2)$

7. S — степень 6 $\Leftrightarrow \exists k \exists (s_0, \dots s_k)(s_0 = 1 \wedge s_k = s \wedge \forall i \in [0, k-1] s_{i+1} = 6 \cdot s_i)$, но это не формула первого порядка, проблема

Чтобы понять, как действовать в последнем пункте, надо научиться как-то кодировать такие кортежи произвольной длины. Традиционно сущесвует два способа:

1. β-функция Геделя
2. Кодирование Смаллиана

6.2 Построение β-функции

Лемма 6.1. $\forall k \forall B \exists b > B : b+1, 2b+1, \dots (k+1)b+1$ — *попарно взаимно просты*

Доказательство. Возьмем $b = k! \cdot c$, где у c нет простых делителей $> k$. Положим $d = ((i+1)b+1, (j+1)b+1)$ — делитель $(j-i)b = (j-i)k!c \Rightarrow$ все простые делители $d < k \Rightarrow (i+1)b$ делится на простой делитель d, но и $(i+1)b$ не них делится, противоречие при $d > 1$. □

Лемма 6.2. $\forall (s_0, s_1, \dots s_k) \exists a \exists b \forall i \in [0, k]\ s_i = a \mod ((i+1)b+1)$ — *попарно взаимно просты*

Доказательство. Следует из КТО и предыдущей леммы □

Теорема 6.3 (О β-функции)**.** *Существует $\beta(a, b, i)$, задаваемая арифметической формулой, т.ч.* $\forall (s_0, s_1 \dots s_k) \exists (a, b) : \forall i \in [0, k] s_i = \beta(a, b, i)$

Доказательство. Положим $\beta(a, b, i) = a \mod (i+1)b+1$ □

Утверждение 6.4. *Через β-функцию можно выразить предикат $m = 2^n$*

Доказательство. $\exists (m_0, m_1, \dots m_k) : m_0 = 1 \wedge m_n = m \wedge \forall i\ m_i = 2m_{i-1}$. □

6.3 Кодирование Смаллиана

$n \mapsto \widehat{n} = bin(n+1)$ без ведущей единицы. Тогда $(n, m) \mapsto \widehat{k}$, такое, что $\widehat{k} = \widehat{n} \cdot \widehat{m}$, где $\cdot$ — конкатенация

Второе определение: строим биекцию между строками из 0 и 1 и натуральными числами по возрастанию длины, слова одинаковой длины сравниваем лексигографически

0	1	2	3	4	5	6	7	8	9	...
ε	0	1	00	01	10	11	000	001	010	...

Утверждение 6.5. $\exists$ *арифметическая формула $S(a, b, x)$, такое, что*

1. $\forall a, b \{x | S(a, b, x) = 1\}$ *конечно*
2. S *конечно* $\Leftrightarrow \exists (a, b) \{x | S(a, b, x) = 1\} = S$

Доказательство. Рассмотрим $S(a, b, x) : axa \sqsupset\sqsubset b \wedge |x| < |a|$ (axa является подсловом b)

1. очевидно, т.к. $|x| < |a|$
2. рассмотрим a $= 1\underbrace{0 \dots 0}_{L}1, L > \max\{|x_i|\}, b = ax_1ax_2a_3a \dots ax_ka$

□

6.4 Важная Теорема

Определение 6.5. Ar — множество арифметических предикатов

Определение 6.6. $AH = \bigcup_{k=0}^{\infty} \Sigma_k$ — арифметическая иерархия

Теорема 6.4. *$Ar = AH$ (в том смысле, что прекдикаты из Ar — это те и только те, которые формируют AH)*

Доказательство.

$Ar \subset AH$. φ — выражает $P \Rightarrow$ приведем к предварительной нормальной форме. Получилось нечто следующее:

$$\dots\forall\dots\exists\dots P(\dots)$$

Причем P — предикат, полученный композицией $S, +, \cdot, =$ $\Rightarrow$ вычислим ариметически.

$Ar \supset AH$. Покажем, что любой разрешимый предикат можно превратить в арифметическую формулу. Тогда выражение некоторого элемента арифметической иерархии можно будет представить как какое-то количество кванторов + арифметическая формула $\Rightarrow$ получим желаемое. Пусть M — Машина Тьюринга, вычисляющая R, то есть $R(x, y_1, y_2, \dots y_k) = 1 \Leftrightarrow M$, начав с конфигурации $C_0 = q_1 x \# y_1 \# \dots \# y_k$, сделав некоторое число ходов, приходит в q_a. Более формально, M обходила состояния $(C_0, C_1, \dots C_t)$, так, что $C_i \mapsto C_{i+1}$ в соответствии с программой. Тогда нам нужно выразить предикат

$$\exists(C_0, C_1, \dots C_k)(C_0 = q_1 x \# y_1 \# \dots \# y_k \wedge \forall i(C_i \mapsto C_{i+1} \text{ корректно}) \wedge C_t = q_a)$$

Тут у нас возникает несколько проблем:

(a) Как записать $\exists(C_0, C_1, \dots C_t)$ — решается β-функцией

(b) Как записывать корректные переходы и различные операции со строками, в терминах натуральных чисел — эту проблему решает кодирование Смаллиана

□

6.5 Доказательства в формальной арифметике

6.5.1 Аксиомы

А Аксиомы исчисления высказываний и исчисления предикатов

Б **Аксиомы равенства**

Б1 **Аксиомы отношения эквивалентности**

i. $\forall x \;\; x = x$

ii. $\forall x \forall y (x = y \to y = x)$

iii. $\forall x \forall y \forall z ((x = y \wedge y = z) \to x = z)$

Б2 **Аксиома замены** $\forall x, y, z, t ((x = y \wedge z = t) \to x + z = y + t)$

Замечание. Для произвольной сигнатуры, аксиом замены больше. Допустим, что у нас есть два предикатных символа $P^{(1)}, Q^{(2)}$ и два функциональных символа $f^{(2)}, g^3$. Тогда аксиомы замены для них выглядят следующим образом:

$\forall x \forall y((x = y) \to (P(x) \leftrightarrow P(y)))$
$\forall x \forall y \forall z \forall t((x = y \wedge z = t) \to (Q(x, z) \leftrightarrow Q(y, t)))$
$\forall x_1 \forall y_1 \forall x_2 \forall y_2 \forall x_3 \forall y_3((x_1 = y_1 \wedge x_2 = y_2 \wedge x_3 = y_3) \to (f(x_1, x_2, x_3) = f(y_1, y_2, y_3)))$
$\forall x_1 \forall y_1 \forall x_2 \forall y_2((x_1 = y_1 \wedge x_2 = y_2) \to (g(x_1, x_2) = g(y_1, y_2)))$

Однако, в аксиоматике Пеано, нам достаточно только одной аксиомы замены.

B **Аксиомы арифметики (Аксиомы Пеано)**

B1 **Аксиомы порядка**

i. $\nexists x : S(x) = 0$
ii. $\nexists x, y : (x \neq y \wedge S(x) = S(y))$
iii. **Принцип индукции** $(\varphi(0) \wedge \forall n \varphi(n) \to \varphi(S(n))) \to \forall x \varphi(x)$. Откуда берем φ? Есть несколько вариантов. Принцип первого порядка: φ — произвольная формула с одним параметром. Принцип второго порядка: гласит, что это выполнено $\forall \varphi$

B2 **Аксиомы сложения**

i. $x + 0 = x$
ii. $x + S(y) = S(x + y)$

B2 **Аксиомы умножения**

i. $x \cdot 0 = 0$
ii. $x \cdot S(y) = x \cdot y + x$

6.5.2 Правила вывода

Те же самые, что и в формулах первого порядка
Иногда вместо $S(x)$ пишут просто Sx

Утверждение 6.6.

$$2 + 2 = 4$$

Доказательство. Хотим доказать, что $SS0 + SS0 = SSSS0$.

$$SS0 + SS0 = S(SS0 + S0) = S(S(SS0 + 0)) = SSSS0$$

□

Утверждение 6.7.

$$0 + x = x$$

Доказательство. Почему $0 + x = x$? Рассмотрим $\varphi(x) = (0 + x = x)$ (как булеву формулу)

1. $\varphi(0)$ — по аксиоме B2.i
2. $0 + x = x \Rightarrow 0 + Sx = S(0 + x) = Sx$. Получили, что $\varphi(x) \to \varphi(x + 1)$

Тогда по индукции доказали, что $\forall x \varphi(x)$ □

Следствие. $x + 0 = 0 + x$

Лемма 6.3. $\forall x \forall y (Sx + y = S(x + y))$

Доказательство.
1. $\forall t \ \ t + 0 = t$ — B2.i
2. $Sx + 0 = Sx$ — подставили $t = Sx$
3. $x + 0 = x$ — подстановка $t = x$
4. $x + 0 = x \to S(x + 0) = S(x)$ — Б1.iii
5. $S(x + 0) = Sx$ — m.p. 3, 4
6. $Sx = S(x + 0)$ — Б1.ii
7. $Sx + 0 = S(x + 0)$ — Б1.iii 2, 6
8. $\forall x Sx + 0 = S(x + 0)$ — обобщение. Далее: $\forall y((\forall x Sx + y = S(x + y)) \to (\forall x Sx + Sy = S(x + Sy)))$
9. $Sx + Sy = S(Sx + y)$
10. $x + Sy = S(x + y)$
11. $Sx + y = S(x + y) \to S(Sx + y) = SS(x + y)$
12. $x + Sy = S(x + y) \to S(x + Sy) = SS(x + y)$
13. $S(x + Sy) = SS(x + y)$ Получили, что $Sx + Sy = S(Sx + y) = SS(x + y) = S(x + Sy)$ Тогда по индукции $\forall x \forall y Sx + y = S(x + y)$

□

Утверждение 6.8 (Коммутативность сложения)**.** $\forall x \forall y x + y = y + x$.

Доказательство. Доказываем по индукции, что $\varphi(y) = \forall x x = y = y + x$. $\varphi(0)$ уже есть. Докажем $\forall n \varphi(n) \to \varphi(S(n))$. Следует из того, что $S(x + y) = x + S(y) = S(y) + x = S(y + x)$ □

7 Теорема Геделя

Теорема 7.1. *Множества истинных и доказуемых формул не совпадают*

7.1 Первое доказательство

Определение 7.1. Замкнутая формула φ нащывается доказуемой в формальной арифметике, если $\exists$ вывод, содержащий φ

Утверждение 7.1. *Множество доказуемых формул перечислимо (не только в арифметике, но и в любой теории с разрешимым множеством аксиом)*

Доказательство. Оно является проекцией разрешимного множества пар (φ, доказательство φ). □

Теорема 7.2. *Все Σ_k различны*

Теорема 7.3. *Все $\Sigma_k \cup \Pi_k \subsetneq \Sigma_{k+1} \cup \Pi_{k+1}$ различны*

Теорема 7.4 (Тарского)**.** *Предикат "истинна ли формула в стандартной модели" неарифметичен (т.е. не выражается арифметической формулой, т.е не лежит в арифметической иерархии)*

Доказательство. Пусть $True(\varphi)$ — такой предикат. Он выражается формулой $\Rightarrow$ он лежит на конкретном уровне Σ_n. Пусть $\psi(x) \in \Sigma_{n+1} \setminus \Sigma_n$. Положим $\underline{m} = \underbrace{S \dots S}_{m} 0$. Тогда $\forall m \varphi(m) \leftrightarrow True(\varphi(\underline{m}))$. Получили, что $\varphi(x)$ выразим как $True(\varphi(\underline{m}))$. Можно выбрать такое кодирование, чтобы $\varphi(\underline{m})$ не требовало бы новых кванторов □

Следствие (Теорема Геделя о неполноте)**.** Получили, что истинные формулы неарифметичны. Но тогда истинные $\neq$ доказуемые. Тогда в каждой теории есть либо истинная недоказуемая формула, либо существует ложная доказуемая формула.

7.2 Второе доказательство

Положим $Proof(p, x)$ — предикат проверки, является ли текст с номером p доказательством формулы с номером x. Положим $\Pr(x) = \exists p\ Proof(p, x)$ — предикат доказуемости.

Положим $G(x) \leftrightarrow \exists y(\neg Pr(y) \wedge Subst(y, x, x))$. Положим $Subst(q, r, s)$ — "q является номером формулы, полученной подстановкой числа s в формулу с одним параметром и номером r". Заметим, что $G(G) = \exists y(\neg Pr(y) \wedge Subst(y, G, G)) = \bigvee_y (\neg Pr(y) \wedge Subst(y, G, G)) = \neg P(G(G))$ (подходит единственный $y = G(G)$). Тогда $G(G)$ либо истинна и не доказуема, либо ложна и доказуема.

Тарского. Рассмотрим $T(x) \leftrightarrow \exists y(\neg True(y) \wedge Subst(y, x, x)) =$ аналогично $= \neg True(T(T))$. Получили, что предикат $True$ неарифметичен. □

Теорема 7.5 (Геделя-Россера)**.** *Любая теория либо непротиворечива, либо неполна*

Теорема 7.6 (Вторая теорема Геделя)**.** *Если арифметика непроиворечива, то факт непротиворечивости нельзя доказать (непротиворечивость $= \neg Pr(0 = 1)$)*

7.3 Колмогоровская сложность

Определение 7.2. Колмогоровская сложность слова x — $K(x)$ — длина кратчайшей программы, печатающей x.

Утверждение 7.2. *$K(x)$ невычислима*

Доказательство. Положим $a_n = \min\{x | K(x) > n\}$. Если K вычислимо $\Rightarrow K(a_n) < n + c$ □

Замечание. Среди утверждений вида $K(x) > t$ есть истинные, но не доказуемые

8 λ-исчисление

Исторически это один из первых подходов к теории вычислимости. Раньше все рассматриваемые нами объекты являлись множествами (натуральные числа, машины Тьюринга и т.д.). Сейчас все рассматриваемые нами объекты мы будем определять через функции.

8.1 Синтаксис

8.1.1 Алфавит

Алфавит λ-исчисления состоит из переменных, λ, "." и скобок

8.1.2 λ-термы

Базовое правило: Переменная — терм

Конкатенация: P, Q — термы, тогда (PQ) — тоже

λ-абстракция: x — переменная, P — терм $\Rightarrow (\lambda x.P)$ — тоже

Пример.

$$((\lambda x.(\lambda y.((xy)x)))(\lambda x.x))$$

Соглашения:

1. $PQRS = (((PQ)R)S)$
2. $\lambda xyz.P = \lambda x.(\lambda y.(\lambda z.P))$
3. $\lambda x.PQ = \lambda x.(PQ) \neq ((\lambda x.P)Q)$

8.1.3 α-конверсия

По сути, переименование связной переменной. Формально: $\lambda x.P \mapsto \lambda x.P({}^{x}/_{y})$, т.е. мы заменяем все свободные вхождения x в P на y. При этом,

1. Свободных вхождений y в P не должно
2. области действия квантора λy не должно быть свободных вхождений x.

Пример (Плохая конверсия)**.**

$$\lambda x.xy \not\mapsto \lambda y.yy$$

Нарушается первое правило

Пример (Плохая конверсия)**.**

$$\lambda x.x(\lambda y.xy) \not\mapsto \lambda y.y(\lambda y.yy)$$

Нарушается второе правило

Утверждение 8.1. *α-конверсия обратима*

8.1.4 β-редукция

По сути, подстановка значения переменной. $(\lambda x.P)Q \mapsto P(^{Q}/_{x})$. Причем, переменная из Q не должна попасть под действие квантора из P

Пример (Плохая редукция)**.**

$$(\lambda x.y(\lambda y.xy))y \not\mapsto y(\lambda y.yy)$$

Правильно:

$$(\lambda x.y(\lambda y.xy))y \mapsto_\alpha (\lambda x.y(\lambda z.xz))y \mapsto_\beta y(\lambda z.yz)$$

Замечание. α-конверсию и β-редукцию можно применять как для формул, так и для их корректных подформул

8.1.5 Равенство термов

Введем $=$, которое является симметричным, транзитивным замыканием, для которго выполнено $P \to_\alpha Q \Rightarrow P = Q, P \to_\beta Q \Rightarrow P = Q$

Определение 8.1. $P \to Q$, если существуют $P = P_0, P_1, \dots P_m = Q$, такие, что $P_i \to_\alpha P_{i+1}$ или $P_i \to_\beta P_{i+1}$.

Теорема 8.1 (Черча-Россера о ромбическом свойстве)**.** $P \to Q, P \to R \Rightarrow \exists S : Q \to S, R \to S$

Следствие. $P = Q \Leftrightarrow \exists S : (P \to S, Q \to S)$

Следствие. $P = Q, P, Q$ в нормальной форме $\Rightarrow P \to_\alpha Q$, т.е. нормальная форма единственна с точностью до замены переменных, если она существует.

Определение 8.2. λ-терм P находится в нормальной форме, если нельзя применить β-редукцию после нескольких α-конверсий.

Пример.

$$\Omega = (\lambda x.xx)(\lambda x.xx)$$

Заметим, что $\Omega \to_\beta \Omega \Rightarrow \Omega$ — терм без нормальной формы.

8.2 Семантика

Определение 8.3. Комбинатор — замкнутые терм

8.2.1 Комбинаторы логических значений:

1. $True$**:** $\lambda xy.x$
2. $False$**:** $\lambda xy.y$
3. And**:** $\lambda pq.pqp$ или $\lambda pq.pq\ False$
4. Or**:** $\lambda pq.ppq$ или $\lambda pq.p\ True\ q$
5. Not**:** $\lambda p.p\ False\ True$

8.2.2 Операции с парами

$$Pair = \lambda xyp.pxy \Rightarrow PairXY = \lambda p.pXY$$

1. $Left$: $\lambda p.p\ True$
2. $Right$: $\lambda p.p\ False$

Доказательство. Дейтсвительно:

$$(\lambda p.p\ True)(\lambda p.pXY) = (\lambda p.pXY)True = (\lambda p.pXY)(\lambda xy.x) =$$

$$= (\lambda xy.x)XY = ((\lambda xy.x)X)Y = (\lambda y.X)Y = X$$

Аналогично:

$$(\lambda p.p\ False)(\lambda p.pXY) = (\lambda p.pXY)False = (\lambda p.pXY)(\lambda xy.y) =$$

$$= (\lambda xy.y)XY = ((\lambda xy.y)X)Y = (\lambda y.y)Y = Y$$

□

8.3 Нумералы Черча

Определение 8.4.

$$\begin{array}{ccc} \underline{0} & = & \lambda fx.x \\ \underline{1} & = & \lambda fx.fx \\ \underline{2} & = & \lambda fx.f(fx) \\ \vdots & \vdots & \vdots \\ \underline{n} & = & \lambda fx.\underbrace{f(f(\ldots(f}_{n \text{ раз}}x))) \end{array}$$

Как определить сложение? Для начала определим $Inc\ \underline{n} = \underline{n+1}$.

Определение 8.5.

$$Inc = \lambda nfx.f(nfx)$$

Доказательство. Действительно, заметим, что

$$\underline{n}fx = (\underline{n}f)x = ((\lambda fx.\underbrace{f(f(\ldots(f}_{n \text{ раз}}x)))f)x = (\lambda x.\underbrace{f(f(\ldots(f}_{n \text{ раз}}x))))x = \underbrace{f(f(\ldots(f}_{n \text{ раз}}x)))$$

$$Inc\ \underline{n} = f(\underbrace{f(f(\ldots(f}_{n \text{ раз}}x)))) = \underbrace{f(f(\ldots(f}_{n+1 \text{ раз}}x))) = \underline{n+1}$$

□

8.3.1 Сложение

Далее, хотим, чтобы $Add\ \underline{m}\ \underline{n} = \underline{m+n}$

Определение 8.6 (Первый способ)**.**

$$Add = \lambda mn.m\ Inc\ n$$

Доказательство.

$$Add\ \underline{m}\ \underline{n} = \underbrace{f(f(\dots(f}_{m \text{ раз}}\ x))\ Inc\ n = \lambda fx.\underbrace{Inc(Inc(\dots(Inc}_{m \text{ раз}}\ n))) = \underline{m+n}$$

□

Определение 8.7 (Второй способ)**.**

$$Add = \lambda mnfx.mf(nfx)$$

Доказательство. Воспользуемся двойной β-редукцией: $(\lambda xy.P)QR \to_\beta P({}^{Q}/_{x}, {}^{R}/_{y})$ и получим, что:

$$Add\ \underline{m}\ \underline{m} = \lambda fx.\underline{m}f(\underline{n}fx) = \lambda fx.\underbrace{f(f(\dots(f}_{m \text{ раз}}(\underline{n}fx)))) = \lambda fx.\underbrace{f(f(\dots(f}_{m \text{ раз}}(\underbrace{f(f(\dots(f}_{n \text{ раз}}\ fx)))))))) = \underline{m+n}$$

□

8.3.2 Умножение

Определение 8.8 (Первый способ)**.**

$$Mult = \lambda mn.m\ Add\ n\ \underline{0} = \lambda mn.m\ (\lambda k.Add\ n\ k)\ \underline{0}$$

Доказательство. По сути, мы m раз прибавляем $\underline{n}$ к $\underline{0}$ □

Определение 8.9 (Второй способ)**.**

$$Mult = \lambda mnfx.m(nf)x$$

Доказательство.

$$Mult\ \underline{m}\ \underline{n} = \lambda fx.\underline{m}(f\underline{n})x = \lambda fx.\underbrace{(\underline{n}f)((\underline{n}f)(\dots((\underline{n}f)}_{m \text{ раз}}\ x))) = \lambda fx.\underbrace{f^n(f^n(\dots(f^n}_{n \text{ раз}}(x)))) =$$

$$= \lambda fx.f^{mn}x = \underline{mn}$$

□

8.3.3 Возведение в степень

Определение 8.10 (Первый способ)**.**

$$\lambda mn.n(\lambda k.Mult\ m\ k)\underline{1}$$

Доказательство. По сути, мы m раз умножаем $\underline{n}$ на $\underline{1}$ □

Определение 8.11 (Второй способ)**.**

$$\lambda mnfx.nmfx$$

Доказательство. Набросок доказательства:

$$\underline{nm}fx = ((\underline{nm})f)x = \underbrace{\underline{m}(\underline{m}(\dots(\underline{m}}_{n \text{ раз}}f)))x$$

По сути, n раз умножаем на m □

8.3.4 Проверка на равенство нулю

Реализуем функцию $IsZero$, которая удовлетворяет следующим условиям:

1. $IsZero\ \underline{0} = True$
2. $IsZero\ \underline{n+1} = False$

Определение 8.12.

$$IsZero = \lambda n.n(\lambda x.False)True$$

Доказательство.

1. $IsZero\ \underline{0} = (\lambda fx.x)(\lambda x.False)True = True$
2. $IsZero\ \underline{n+1} = (\lambda fx.f(\dots))(\lambda x.False)True = (\lambda x.False)(\dots) = False$

□

8.3.5 Трюк Клини

Мы хотим реализовать декремент. Строго говоря, он не определен для всех пар натуральных чисел. Поэтому мы реализуем "срезанный декремент":

$$Dec\ \underline{m} = \underline{\max\{m-1, 0\}}$$

Идея состоит в том, что мы рассматриваем следующее преобразование пар:

$$(x, y) \mapsto_g (f(x), x)$$

Чтобы каким-то образом получить число $n-1$, мы сделаем следующее:

$$(x, y) \mapsto (f(x), x) \mapsto (f(f(x)), f(x)) \mapsto \dots \mapsto (f^n(x), f^{n-1}(x))$$

Поэтому для того, чтобы получить f^{n-1}, надо взять функцию f, функцию g, котоаря будет данным образом преобразовывать пару и применить g^n к изначальной паре. Получится $(f^n(x), f^{n-1}(x))$ и теперь достаточно будет взять правую часть этой пары. Формально:

Определение 8.13.

$$DecAux = \lambda fp.Pair(f(Left\ p))(Left\ p)$$

Это аналог g для декремента

Определение 8.14.

$$Dec = \lambda nfx.Right(n(DecAux\ f)(Pair\ x\ x))$$

Доказательство. По сути, мы проделываем описанную выше процедуру. Формально:

1. $Dec\ \underline{0}$

$$= \lambda fx.Right(\underline{0}(DecAux\ f)(Pair\ x\ x)) = \lambda fx.Right(Pair\ x\ x) = \lambda fx.x = \underline{0}$$

2. $Dec\ \underline{n+1}$

$$= \lambda fx.Right(\underline{n+1}(DecAux\ f)(Pair\ x\ x)) =$$

$$= \lambda fx.Right(\underbrace{(DecAux\ f)((DecAux\ f)(\dots((DecAux\ f)}_{n+1\text{ раз}}(Pair\ x\ x)))))$$

Заметим, что

$$DecAux\ f = \lambda p.Pair(f(Left\ p))(Left\ p)$$

$$(DecAux\ f)(Pair\ x\ x) = Pair(f(Left\ (Pair\ x\ x)))(Left\ (Pair\ x\ x)) = Pair(fx)x$$

Поэтому крокодил выше свернется в $\underline{n}$

□

8.3.6 Вычитание

Как и декремент, вычитаение будет "срезанным":

$$m - n = \underline{\max\{m-n, 0\}}$$

Определение 8.15.

$$Sub = \lambda mn.n\ Dec\ m$$

8.4 Рекурсивное программирование в λ-исчислении

Хотим рекурсивно определить деление:

$$\left[\frac{m}{n}\right] = \begin{cases} 0, m < n \\ 1 + \left[\frac{m-n}{n}\right], m \geqslant n \end{cases}$$

Получим уравнение:

$$Div\ \underline{n}\ \underline{m} = (LT\ m\ n)\underline{0}(Inc\ (Div(Sub\ m\ n)n))$$

Div — "Решение уравнения выше" или неподвижная точка преобразования.

Определение 8.16.

$$DivAux = \lambda gmn.(LT\ m\ n)\underline{0}(Inc(g(Sub\ m\ n)n))$$

Хотим, чтобы $Div = DivAux\ Div$

8.5 Y-Комбинатор

Хотим, чтобы $YF = F(YF)$. Тогда, если мы сможем представить Div в виде $Y\ DivAux$, то мы победим.

Определение 8.17.

$$Y = (\lambda xy.y(xxy))(\lambda xy.y(xxy))$$

Доказательство.

$$YF = (\lambda xy.y(xxy))(\lambda xy.y(xxy))F = F((\lambda xy.y(xxy))(\lambda xy.y(xxy))F) = F(YF)$$

□

8.6 Комбинатор Клопа

$$\mathcal{L} = \lambda abcdefghijklmnopqstuvwxyzr.r(thisisafixedpointcombinator)$$

Тогда $Y = \underbrace{\mathcal{L}\mathcal{L}\dots\mathcal{L}}_{26}$

9 P vs NP

9.1 Неформально

Определение 9.1. P — полиномиальное время.

Определение 9.2. NP — недетерминированное полиномиальное время

9.2 Задача раскраски

Задача (2-Раскраска)**.** *Возможно ли раскрасить все вершины графа в два цвета так, что никакие две вершины одного цвета не соединены ребром?*

Решение. Спасибо, Илья Даниилович, за то, что научили такое решать за $O(n+m)$ □

Задача (3-Раскраска)**.** *Возможно ли раскрасить все вершины графа в 3 цвета так, что никакие две вершины одного цвета не соединены ребром?*

Решение. Пока что Илья Даниилович не научил такое решать. Все известные алгоритмы экспоненциальны. Тем не менее, если раскраска дана, то это можно проверить за $O(poly)$ □

9.3 Задача на графах

Задача (Эйлеровость графа)**.** *Является ли данный граф эйлеровым?*

Решение. Существует критерий эйлеровости, который работает за линию □

Задача (Гамильтоновость графа)**.** *Является ли данный граф гамильтоновым?*

Решение. Нет критерия, который бы легко проверялся. Однако, если дан цикл, то можно проверить, что он гамильтонов □

9.4 Задача про простоту

Задача (Проверка на простоту)**.** *Является ли данное число простым*

Решение. Существует алгоритм, работающий за $O(\log^6 n)$ □

Задача (Разложение на множители)**.** *Даны* n, a, b*. Существует ли* $d : d|n \wedge d \in [a, b]$

Решение. Существует алгоритм для квантового компьютера. Для обычных компьютеров пока что такого нет. □

Проще говоря, NP — множество таких задач, которые можно быстро проверить за полиномиальное время.

9.5 Формально

Определение 9.3. $A \subset \{0,1\}^*$. Тогда $A \in P$, если $\exists M$ — Машина Тьюринга, что

1. $\forall x(x \in A \Leftrightarrow M(x) = 1)$
2. $\exists c, d : \forall x M(x)$ останавливается не больше чем за $c|x|^d$ шагов

Определение 9.4. $A \subset \{0,1\}^*$. Тогда $A \in NP$, если $\exists V(x, y)$ — Машина Тьюринга, что

1. $\forall x(x \in A \Leftrightarrow \exists y V(x, y) = 1)$
2. $\exists c, d : \forall x, y V(x, y)$ останавливается не больше чем за $c|x|^d$ шагов

Утверждение 9.1. $NP \subset EXP$*, где* EXP *— множество, разрешимое за* $O(2^{poly(n)})$.

Доказательство. В определении выше, количество бит в y ограничено $c|x|^d$. Тогда можно перебрать все y. □

10 Заключение

Ура! Курс логики закончился. Впереди — сессия! Желаю всем удачи!