Червь Беклемишева

Оноприенко Анастасия Александровна

МГУ им. М. В. Ломоносова

НИС "Современные проблемы математической логики",
НИУ ВШЭ, 30.09.2022

Арифметика Пеано PA

Возьмём в качестве σ сигнатуру $\langle =, S \rangle$.

Аксиомы арифметики Пеано (нелогические):

$\forall x \, \neg(0 = S(x))$

$\forall x \forall y (S(x) = S(y) \to x = y)$

$\varphi(0) \wedge \forall x(\varphi(x) \to \varphi(S(x))) \to \forall x \varphi(x)$, где $\varphi(x)$ — любая формула.

Арифметика Пеано PA

Возьмём в качестве σ сигнатуру $\langle =, S \rangle$.

Аксиомы арифметики Пеано (нелогические):

$\forall x \neg(0 = S(x))$

$\forall x \forall y (S(x) = S(y) \to x = y)$

$\varphi(0) \wedge \forall x(\varphi(x) \to \varphi(S(x))) \to \forall x \varphi(x)$, где $\varphi(x)$ — любая формула.

Часто рассматривают арифметику Пеано в более богатой сигнатуре, содержащей $+, \cdot, <$.

Теорема Гёделя о неполноте

Определение

Формальным доказательством называется конечная последовательность формул, каждая из которых является либо аксиомой, либо получена из предыдущих формул данной последовательности по одному из правил вывода.

Теорема Гёделя о неполноте

Существует истинное утверждение про натуральные числа, которое невозможно формально доказать в арифметике Пеано.

Теорема Гёделя о неполноте

Существуют разные пути доказательства теоремы Гёделя о неполноте.

Теорема Гёделя о неполноте

Существуют разные пути доказательства теоремы Гёделя о неполноте.

- Один из путей — предъявить утверждение, содержательно означающее "я недоказуемо".

Теорема Гёделя о неполноте

Существуют разные пути доказательства теоремы Гёделя о неполноте.

- Один из путей — предъявить утверждение, содержательно означающее "я недоказуемо".
- Альтернативный путь: множество доказуемых в PA формул перечислимо. Рассмотрим вычислимый пересчёт $(\varphi_n)_{n\in\mathbb{N}}$ всех вычислимых функций из $\mathbb{N}$ в $\mathbb{N}$, всюду определённость которых доказуема в PA.

Теорема Гёделя о неполноте

Существуют разные пути доказательства теоремы Гёделя о неполноте.

- Один из путей — предъявить утверждение, содержательно означающее “я недоказуемо”.
- Альтернативный путь: множество доказуемых в PA формул перечислимо. Рассмотрим вычислимый пересчёт $(\varphi_n)_{n \in \mathbb{N}}$ всех вычислимых функций из $\mathbb{N}$ в $\mathbb{N}$, всюду определённость которых доказуема в PA.
  Функция $\psi(n) = \max\limits_{i,m \leqslant n} \varphi_i(m) + 1$ всюду определена, вычислима, но не совпадает ни с какой φ_k (так как $\psi(n) > \varphi_k(n)$ для $n \geqslant k$) $\Longrightarrow$ её всюду определённость нельзя доказать в PA.

Системы преобразований термов

Неформально: имеется начальный терм, с которым происходят преобразования по некоторым правилам $t_1 \to t_2 \to t_3 \to \dots$

Системы преобразований термов

Неформально: имеется начальный терм, с которым происходят преобразования по некоторым правилам $t_1 \to t_2 \to t_3 \to \dots$

Определим функцию сложности $C(n)$: максимальное возможное число шагов цепочки преобразований данной системы, начинающейся с терма длины $\leqslant n$.

Системы преобразований термов

Неформально: имеется начальный терм, с которым происходят преобразования по некоторым правилам $t_1 \to t_2 \to t_3 \to \dots$

Определим функцию сложности $C(n)$: максимальное возможное число шагов цепочки преобразований данной системы, начинающейся с терма длины $\leqslant n$.

Система сходится $\iff$ функция C всюду определена.

Системы преобразований термов

Неформально: имеется начальный терм, с которым происходят преобразования по некоторым правилам $t_1 \to t_2 \to t_3 \to \dots$

Определим функцию сложности $C(n)$: максимальное возможное число шагов цепочки преобразований данной системы, начинающейся с терма длины $\leqslant n$.

Система сходится $\iff$ функция C всюду определена.

Существуют *медленно сходящиеся системы*: они сходятся, но число шагов в них нельзя оценить функцией разумного порядка роста от длины начального терма.

Системы преобразований термов

Неформально: имеется начальный терм, с которым происходят преобразования по некоторым правилам $t_1 \to t_2 \to t_3 \to \dots$

Определим функцию сложности $C(n)$: максимальное возможное число шагов цепочки преобразований данной системы, начинающейся с терма длины $\leqslant n$.

Система сходится $\iff$ функция C всюду определена.

Существуют *медленно сходящиеся системы*: они сходятся, но число шагов в них нельзя оценить функцией разумного порядка роста от длины начального терма.

Для таких систем всюду определённость функции C невозможно доказать в PA.

Червь Беклемишева

Червём будем называть конечную последовательность натуральных чисел: $A = n_0 n_1 \dots n_k$ (слово в алфавите $\mathbb{N}$).

Первый элемент n_0 — *голова* червя.

Далее червь эволюционирует: если голова червя равна 0, то на очередном шаге она отмирает; в противном случае голова уменьшается на единицу, но червь регенерируется в соответствии с простым правилом, описанным далее.

Червь Беклемишева

Зададим *функцию червя* $A, m \mapsto A[m]$, где $A = n_0 n_1, \ldots, n_k$, $m \in \mathbb{N}$.

- если $n_0 = 0$, то $A[m] = n_1 \ldots n_k$;
- если $n_0 = n + 1 > 0$, то найдём максимальное начало $n_0 B$ червя A, в котором все элементы больше или равны n_0 (B может быть пустым); если $A = n_0 BC$, то $A[m] = (nB)^{m+1} C$.

Червь Беклемишева

Зададим *функцию червя* $A, m \mapsto A[m]$, где $A = n_0 n_1, \dots, n_k$, $m \in \mathbb{N}$.

- если $n_0 = 0$, то $A[m] = n_1 \dots n_k$;
- если $n_0 = n + 1 > 0$, то найдём максимальное начало $n_0 B$ червя A, в котором все элементы больше или равны n_0 (B может быть пустым); если $A = n_0 BC$, то $A[m] = (nB)^{m+1} C$.

Для любого начального червя A эта функция определяет последовательность $(A_i)_{i \in \mathbb{N}}$, которую мы называем его *эволюцией*:

$$A_0 = A; \quad A_{i+1} = A_i[i+1].$$

Червь Беклемишева

Пример. Рассмотрим эволюцию червя $A = 1302$. На первом шаге мы получаем $B = 3$ и $A_1 = A[1] = 030302$. Далее возникает последовательность

$$
\begin{aligned}
A_0 &= 1302 \\
A_1 &= 030302 \\
A_2 &= 30302 \\
A_3 &= 22220302 \\
A_4 &= 1222122212221222122220302 \\
A_5 &= (022212221222122221222)^6 0302 \\
&\dots
\end{aligned}
$$

.

Червь Беклемишева

Рассмотрим эволюцию червя.

Существует ли червь, который будет жить вечно? Или эволюция любого червя приведёт к пустой последовательности?

Червь Беклемишева

Рассмотрим эволюцию червя.

Существует ли червь, который будет жить вечно? Или эволюция любого червя приведёт к пустой последовательности?

Теорема

(1) Для любого червя A_0 в его эволюции существует такой номер m, что A_m — пустая последовательность.
(2) Утверждение (1) невозможно доказать в арифметике Пеано.

Вполне упорядоченные множества

Множество $(X, \leqslant)$ называется *вполне упорядоченным*, если порядок $\leqslant$ линейный и каждое непустое подмножество X имеет наименьший элемент.

Вполне упорядоченные множества

Множество $(X, \leqslant)$ называется *вполне упорядоченным*, если порядок $\leqslant$ линейный и каждое непустое подмножество X имеет наименьший элемент.

Равносильное определение: не существует бесконечно убывающей цепочки элементов множества X: $x_1 > x_2 > x_3 > \dots$.

Вполне упорядоченные множества

Множество $(X, \leqslant)$ называется *вполне упорядоченным*, если порядок $\leqslant$ линейный и каждое непустое подмножество X имеет наименьший элемент.

Равносильное определение: не существует бесконечно убывающей цепочки элементов множества X: $x_1 > x_2 > x_3 > \dots$.

Очевидно, что натуральные числа $\mathbb{N}$ с естественным порядком являются вполне упорядоченным множеством.

Вполне упорядоченные множества

Множество $(X, \leqslant)$ называется *вполне упорядоченным*, если порядок $\leqslant$ линейный и каждое непустое подмножество X имеет наименьший элемент.

Равносильное определение: не существует бесконечно убывающей цепочки элементов множества X: $x_1 > x_2 > x_3 > \ldots$.

Очевидно, что натуральные числа $\mathbb{N}$ с естественным порядком являются вполне упорядоченным множеством.

Есть ли другие вполне упорядоченные множества?

Ординалы

Натуральные числа $\mathbb{N}$ иначе обозначаются как ω.

Ординалы

Натуральные числа $\mathbb{N}$ иначе обозначаются как ω.

$\omega + 1, \omega + 2, \omega + 3, \omega + 4, \ldots$

Ординалы

Натуральные числа $\mathbb{N}$ иначе обозначаются как ω.

$\omega + 1, \omega + 2, \omega + 3, \omega + 4, \ldots$

$\omega \cdot 2 = \omega + \omega = \sup\{\omega + 1, \omega + 2, \omega + 3, \omega + 4, \ldots\}$

Ординалы

Натуральные числа $\mathbb{N}$ иначе обозначаются как ω.

$\omega + 1, \omega + 2, \omega + 3, \omega + 4, \ldots$

$\omega \cdot 2 = \omega + \omega = \sup\{\omega + 1, \omega + 2, \omega + 3, \omega + 4, \ldots\}$

$\omega, \omega \cdot 2, \omega \cdot 3, \omega \cdot 4, \ldots$

Ординалы

Натуральные числа $\mathbb{N}$ иначе обозначаются как ω.

$\omega + 1, \omega + 2, \omega + 3, \omega + 4, \ldots$

$\omega \cdot 2 = \omega + \omega = \sup\{\omega + 1, \omega + 2, \omega + 3, \omega + 4, \ldots\}$

$\omega, \omega \cdot 2, \omega \cdot 3, \omega \cdot 4, \ldots$

$\omega^2 = \omega \cdot \omega = \sup\{\omega, \omega \cdot 2, \omega \cdot 3, \omega \cdot 4, \ldots\}$

Ординалы

Натуральные числа $\mathbb{N}$ иначе обозначаются как ω.

$\omega+1, \omega+2, \omega+3, \omega+4, \ldots$

$\omega \cdot 2 = \omega + \omega = \sup\{\omega+1, \omega+2, \omega+3, \omega+4, \ldots\}$

$\omega, \omega \cdot 2, \omega \cdot 3, \omega \cdot 4, \ldots$

$\omega^2 = \omega \cdot \omega = \sup\{\omega, \omega \cdot 2, \omega \cdot 3, \omega \cdot 4, \ldots\}$

$\omega, \omega^2, \omega^3, \omega^4, \ldots$

Ординалы

Натуральные числа $\mathbb{N}$ иначе обозначаются как ω.

$\omega + 1, \omega + 2, \omega + 3, \omega + 4, \ldots$

$\omega \cdot 2 = \omega + \omega = \sup\{\omega + 1, \omega + 2, \omega + 3, \omega + 4, \ldots\}$

$\omega, \omega \cdot 2, \omega \cdot 3, \omega \cdot 4, \ldots$

$\omega^2 = \omega \cdot \omega = \sup\{\omega, \omega \cdot 2, \omega \cdot 3, \omega \cdot 4, \ldots\}$

$\omega, \omega^2, \omega^3, \omega^4, \ldots$

$\omega^\omega = \sup\{\omega, \omega^2, \omega^3, \omega^4, \ldots\}$

Ординалы

Натуральные числа $\mathbb{N}$ иначе обозначаются как ω.

$\omega+1, \omega+2, \omega+3, \omega+4, \ldots$

$\omega \cdot 2=\omega+\omega=\sup\{\omega+1, \omega+2, \omega+3, \omega+4, \ldots\}$

$\omega, \omega \cdot 2, \omega \cdot 3, \omega \cdot 4, \ldots$

$\omega^2=\omega \cdot \omega=\sup\{\omega, \omega \cdot 2, \omega \cdot 3, \omega \cdot 4, \ldots\}$

$\omega, \omega^2, \omega^3, \omega^4, \ldots$

$\omega^\omega=\sup\{\omega, \omega^2, \omega^3, \omega^4, \ldots\}$

$\omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \ldots$

Ординалы

Натуральные числа $\mathbb{N}$ иначе обозначаются как ω.

$\omega + 1, \omega + 2, \omega + 3, \omega + 4, \ldots$

$\omega \cdot 2 = \omega + \omega = \sup\{\omega + 1, \omega + 2, \omega + 3, \omega + 4, \ldots\}$

$\omega, \omega \cdot 2, \omega \cdot 3, \omega \cdot 4, \ldots$

$\omega^2 = \omega \cdot \omega = \sup\{\omega, \omega \cdot 2, \omega \cdot 3, \omega \cdot 4, \ldots\}$

$\omega, \omega^2, \omega^3, \omega^4, \ldots$

$\omega^\omega = \sup\{\omega, \omega^2, \omega^3, \omega^4, \ldots\}$

$\omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \ldots$

$\varepsilon_0 = \sup\{\omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \ldots\}$

Канторовская нормальная форма

Любой ординал $\alpha < \varepsilon_0$ однозначно представляется в форме $\alpha = \omega^{\beta_1} + \omega^{\beta_2} + \ldots + \omega^{\beta_k}$, где $\alpha > \beta_1 \geqslant \beta_2 \geqslant \ldots \geqslant \beta_k \geqslant 0$.

Фактически, можно вообще не упоминать ординалы, а говорить о термах вида:

$$<\text{терм}> ::= 0 \mid \omega \mid <\text{терм}> + <\text{терм}> \mid \omega^{<\text{терм}>}$$

Далее нужно научиться сравнивать термы и складывать их (большее слагаемое съедает все меньшие левее него; 0 съедается в том числе нулём). Такие термы с естественным порядком образуют вполне упорядоченное множество (которое можно обозначить как ε_0).

Принцип червя

Обозначим S — множество всех червей (слов в алфавите $\mathbb{N}$);

S_1 — множество всех слов в алфавите $\mathbb{N} \setminus \{0\}$.

Высотой червя назовём его максимальную букву.

Принцип червя

Обозначим S — множество всех червей (слов в алфавите $\mathbb{N}$);
S_1 — множество всех слов в алфавите $\mathbb{N} \setminus \{0\}$.
Высотой червя назовём его максимальную букву.

Теорема (принцип червя)

Для любого червя A_0 в его эволюции существует такой номер m, что $A_m = \Lambda$ (пустая последовательность).

Принцип червя

Обозначим S — множество всех червей (слов в алфавите $\mathbb{N}$);
S_1 — множество всех слов в алфавите $\mathbb{N} \setminus \{0\}$.
Высотой червя назовём его максимальную букву.

Теорема (принцип червя)

Для любого червя A_0 в его эволюции существует такой номер m, что $A_m = \Lambda$ (пустая последовательность).

Идея доказательства: введём функцию $o : S \to \varepsilon_0$ и покажем, что при преобразованиях червя соответствующий ему ординал уменьшается. Поскольку бесконечно уменьшаться таким образом невозможно, любой червь рано или поздно превратится в пустую последовательность.

Принцип червя: доказательство

Обозначим через B^+ результат замены каждой буквы n в слове B на $n + 1$, а через B^- — обратную операцию (определённую для слов $B \in S_1$).

Принцип червя: доказательство

Обозначим через B^+ результат замены каждой буквы n в слове B на $n+1$, а через B^- — обратную операцию (определённую для слов $B \in S_1$).

Значение функции $o(A)$ определяется индукцией по высоте червя A.
Если $A = 0^k$, то $o(A) := k$. Иначе слово A однозначно представляется в виде $A_1 0 A_2 0 \ldots 0 A_n$, где в словах A_i нет нулей и не все они пусты. В этом случае полагаем $o(A) := \omega^{o(A_n^-)} + \ldots + \omega^{o(A_2^-)} + \omega^{o(A_1^-)}$. Каждый из червей A_i^- имеет высоту, меньшую высоты A, поэтому применимо предположение индукции.

Принцип червя: доказательство

Заметим, что:

- $o(\Lambda) = 0$;
- $o(0A) = o(A) + 1$ для любого $A \in S$;
- если $B \neq 0^k$, то $o(B0A) = o(A) + o(B)$;
- если $B \in S_1$ непусто, то $o(B) = \omega^{o(B^-)}$.

Принцип червя: доказательство

Заметим, что:

- $o(\Lambda) = 0$;
- $o(0A) = o(A) + 1$ для любого $A \in S$;
- если $B \neq 0^k$, то $o(B0A) = o(A) + o(B)$;
- если $B \in S_1$ непусто, то $o(B) = \omega^{o(B^-)}$.

Докажем, что $o(A) > o(A[m])$ для любого непустого слова A.

Рассуждаем индукцией по высоте A.

Принцип червя: доказательство

Заметим, что:

- $o(\Lambda) = 0$;
- $o(0A) = o(A) + 1$ для любого $A \in S$;
- если $B \neq 0^k$, то $o(B0A) = o(A) + o(B)$;
- если $B \in S_1$ непусто, то $o(B) = \omega^{o(B^-)}$.

Доказем, что $o(A) > o(A[m])$ для любого непустого слова A. Рассуждаем индукцией по высоте A.

Для слов высоты 0 утверждение очевидно: $o(0^k) = k$, $o(0^k[m]) = o(0^{k-1}) = k - 1$.

Принцип червя: доказательство

Рассмотрим слово $A = A_1 0 A_2 0 ... 0 A_k$, где $A_i \in S_1$ и не все A_i пусты. Обозначим $C := A_2 0 ... 0 A_k$, тогда $A = A_1 0 C$.

Принцип червя: доказательство

Рассмотрим слово $A = A_1 0 A_2 0 ... 0 A_k$, где $A_i \in S_1$ и не все A_i пусты. Обозначим $C := A_2 0 ... 0 A_k$, тогда $A = A_1 0 C$.

Если $A_1 = \Lambda$, то $A = 0C$ и $A[m] = C$, поэтому $o(A) > o(A[m])$.

Принцип червя: доказательство

Рассмотрим слово $A = A_1 0 A_2 0 \ldots 0 A_k$, где $A_i \in S_1$ и не все A_i пусты. Обозначим $C := A_2 0 \ldots 0 A_k$, тогда $A = A_1 0 C$.

Если $A_1 = \Lambda$, то $A = 0C$ и $A[m] = C$, поэтому $o(A) > o(A[m])$.

Пусть $A_1 \neq \Lambda$. Тогда $A[m] = (A_1[m]) 0 C$.

Принцип червя: доказательство

Рассмотрим слово $A = A_1 0 A_2 0 ... 0 A_k$, где $A_i \in S_1$ и не все A_i пусты. Обозначим $C := A_2 0 ... 0 A_k$, тогда $A = A_1 0 C$.

Если $A_1 = \Lambda$, то $A = 0C$ и $A[m] = C$, поэтому $o(A) > o(A[m])$.

Пусть $A_1 \neq \Lambda$. Тогда $A[m] = (A_1[m]) 0 C$.

Если $A_1[m] = 0^k$, то $A_1 = 1$. Тогда
$o(A) = o(10C) = o(C) + \omega > o(C) + k + 1 = o(0^{k+1} C) = o(A[m])$.

Принцип червя: доказательство

Рассмотрим слово $A = A_1 0 A_2 0 ... 0 A_k$, где $A_i \in S_1$ и не все A_i пусты. Обозначим $C := A_2 0 ... 0 A_k$, тогда $A = A_1 0 C$.

Если $A_1 = \Lambda$, то $A = 0C$ и $A[m] = C$, поэтому $o(A) > o(A[m])$.

Пусть $A_1 \neq \Lambda$. Тогда $A[m] = (A_1[m]) 0 C$.

Если $A_1[m] = 0^k$, то $A_1 = 1$. Тогда
$o(A) = o(10C) = o(C) + \omega > o(C) + k + 1 = o(0^{k+1} C) = o(A[m])$.

Если $A_1[m] \neq 0^k$, то
$o(A) = o(C) + o(A_1)$, $o(A[m]) = o(C) + o(A_1[m])$.
То есть достаточно установить, что $o(A_1) > o(A_1[m])$.

Принцип червя: доказательство

Случай 1: $A_1 = 1B, B \in S_1$. Тогда $A_1[m] = (0B)^{m+1}$. Имеем:
$o(A_1) = \omega^{o((1B)^-)} = \omega^{o(B^-)+1} = \omega^{o(B^-)} \cdot \omega$;
$o(A_1[m]) = \omega^{o(B^-)} \cdot (m+1) + 1 < \omega^{o(B^-)} \cdot \omega = o(A_1)$.

Принцип червя: доказательство

Случай 1: $A_1 = 1B, B \in S_1$. Тогда $A_1[m] = (0B)^{m+1}$. Имеем:
$o(A_1) = \omega^{o((1B)^-)} = \omega^{o(B^-)+1} = \omega^{o(B^-)} \cdot \omega$;
$o(A_1[m]) = \omega^{o(B^-)} \cdot (m+1) + 1 < \omega^{o(B^-)} \cdot \omega = o(A_1)$.

Случай 2: $A_1 = (n+1)B$ для некоторого $n > 1$. Тогда по определению функции червя $A_1^-[m] = (A_1[m])^-$. Отсюда по предположению индукции (A_1 имеет меньшую высоту)
$o(A_1) = \omega^{o(A_1^-)} > \omega^{o(A_1^-[m])} = \omega^{o((A_1[m])^-)} = o(A_1[m])$.

Что и требовалось доказать.

Червь Беклемишева

Теорема

(1) Для любого червя A_0 *в его эволюции существует такой номер* m*, что* A_m *— пустая последовательность.*

(2) Утверждение (1) невозможно доказать в арифметике Пеано.

Червь Беклемишева

Теорема

(1) Для любого червя A_0 в его эволюции существует такой номер m, что A_m — пустая последовательность.
(2) Утверждение (1) невозможно доказать в арифметике Пеано.

Обозначим $D(n)$ — максимальное время жизни червей, размер которых не превышает n (размером называем максимум из высоты червя и длины последовательности).

Тогда $D(n)$ растёт настолько быстро, что она больше любой вычислимой функции (начиная с некоторого номера), всюду определённость которой можно доказать в арифметике Пеано.

$D(n)$ всюду определена, вычислима, но её всюду определённость невозможно доказать в арифметике Пеано.

Спасибо за внимание!