Невыразимость доказуемости

$D \subseteq N_0$

$R(x,y)$ — 2 редик.

$\vdash \rho(\bar{x},\bar{y})$ если $(x,y) \in R$

$\vdash \neg\rho(\bar{x},\bar{y})$, если $(x,y) \notin R$

Определение

$Д_S = \{\ulcorner\alpha\urcorner \mid \vdash_S \alpha\}$; $И_S = \{\ulcorner\alpha\urcorner \mid [\![\alpha]\!]_S = И\}$

Лемма

ф-я на гёделевых ном.

Пусть $D(\ulcorner\alpha\urcorner) = \ulcorner\alpha(\overline{\ulcorner\alpha\urcorner})\urcorner$ для любой формулы $\alpha(x)$. Тогда D представима в формальной арифметике.

$\alpha(x) = 2^{a_1} 3^{a_2} p_1^{x} \dots p_2^{x} \dots p_n^{x}$

Теорема

Если расширение Ф.А. $\mathcal{S}$ непротиворечиво и D представима в нём, то $Д_S$ невыразимо в $\mathcal{S}$

Доказательство.

Пусть $\delta(a,p)$ представляет D, и пусть $\sigma(x)$ выражает множество $Д_S$ (рассматриваемое как одноместное отношение).

Пусть $\alpha(x) := \forall p.\delta(x,p) \to \neg\sigma(p)$. Верно ли, что $\ulcorner\alpha\urcorner \in Д_S$? $\square$

Неразрешимость формальной арифметики

Теорема

Если формальная арифметика непротиворечива, то формальная арифметика неразрешима

Доказательство.

Пусть формальная арифметика разрешима. Значит, есть рекурсивная функция $f(x)$: $f(x) = 1$ тогда и только тогда, когда $x \in Д_{Ф.А.}$. То есть, $Д_{Ф.А.}$ выразимо в формальной арифметике.
По теореме о невыразимости доказуемости, $Д_{Ф.А.}$ невыразимо в формальной арифметике. Противоречие. $\square$

Теорема Тарского

Теорема (Тарского о невыразимости истины)

Не существует формулы $\varphi(x)$, что $[\![\varphi(\overline{x})]\!] = И$ (в стандартной интерпретации) тогда и только тогда, когда $x \in И_{ФА}$.

Доказательство.

Пусть теория $\mathcal{S}$ — формальная арифметика + аксиомы: все истинные в стандартной интерпретации формулы. Очевидно, что $Д_{\mathcal{S}} = И_{\mathcal{S}} = И_{ФА}$. То есть $И_{ФА}$ невыразимо в $\mathcal{S}$.

Пусть φ таково, что $[\![\varphi(\overline{x})]\!] = И$ при $x \in И_{ФА}$. Тогда $\vdash \varphi(\overline{x})$, если $x \in И$ и $\vdash \neg\varphi(\overline{x})$, если $x \notin И$.

Тогда $И_{ФА}$ выразимо в $\mathcal{S}$. Противоречие. $\square$

Теорема Тарского

$\exists x. x^2 > 1$

И.П.
Акс. для арифм.
на $\mathbb{R}$

Теорема (Тарского о невыразимости истины)

Не существует формулы $\varphi(x)$, что $[\![\varphi(\overline{x})]\!] = И$ (в стандартной интерпретации) тогда и только тогда, когда $x \in И_{ФА}$.

Доказательство.

(1)

Пусть теория $\mathcal{S}$ — формальная арифметика + аксиомы: все истинные в стандартной интерпретации формулы. Очевидно, что $Д_{\mathcal{S}} = И_{\mathcal{S}} = И_{ФА}$. То есть $И_{ФА}$ невыразимо в $\mathcal{S}$.

(1')

Пусть φ таково, что $[\![\varphi(\overline{x})]\!] = И$ при $x \in И$. Тогда $\vdash \varphi(\overline{x})$, если $x \in И$ и $\vdash \neg\varphi(\overline{x})$, если $x \notin И$.

Тогда И выразимо в $\mathcal{S}$. Противоречие. $\square$

✓ Однако, если взять $D = \mathbb{R}$, истина становится выразима (алгоритм Тарского).

$\neg \exists x. x' = 0.$

Теория множеств

Теория множеств

1. Георг Кантор: 1877 год, «наивная теория множеств». Множество — это «объединение в одно целое объектов, хорошо различаемых нашей интуицией или нашей мыслью».

Теория множеств

1. Георг Кантор: 1877 год, «наивная теория множеств». Множество — это «объединение в одно целое объектов, хорошо различаемых нашей интуицией или нашей мыслью».
2. Неограниченный принцип абстракции $\{x \mid P(x)\}$

$\{x \mid x$ – брадобрей, не бреющий сам$\}$

Теория множеств

1. Георг Кантор: 1877 год, «наивная теория множеств». Множество — это «объединение в одно целое объектов, хорошо различаемых нашей интуицией или нашей мыслью».
2. Неограниченный принцип абстракции $\{x \mid P(x)\}$
3. Парадокс Бурали-Форти (1895, Кантор). Парадокс Рассела: $X := \{x \mid x \notin x\}$; $X \in X$?

Теория множеств

1. Георг Кантор: 1877 год, «наивная теория множеств». Множество — это «объединение в одно целое объектов, хорошо различаемых нашей интуицией или нашей мыслью».
2. Неограниченный принцип абстракции $\{x \mid P(x)\}$
3. Парадокс Бурали-Форти (1895, Кантор). Парадокс Рассела: $X := \{x \mid x \notin x\}$; $X \in X$?
4. Вариант решения парадокса: а, может, запретить все «опасные» ситуации?

Теория множеств

1. Георг Кантор: 1877 год, «наивная теория множеств». Множество — это «объединение в одно целое объектов, хорошо различаемых нашей интуицией или нашей мыслью».
2. Неограниченный принцип абстракции $\{x \mid P(x)\}$
3. Парадокс Бурали-Форти (1895, Кантор). Парадокс Рассела: $X := \{x \mid x \notin x\}$; $X \in X$?
4. Вариант решения парадокса: а, может, запретить все «опасные» ситуации?
5. Аксиоматика Цермело — 1908 год, оставим только то, что используют математики.

Теория множеств

1. Георг Кантор: 1877 год, «наивная теория множеств». Множество — это «объединение в одно целое объектов, хорошо различаемых нашей интуицией или нашей мыслью».
2. Неограниченный принцип абстракции $\{x \mid P(x)\}$
3. Парадокс Бурали-Форти (1895, Кантор). Парадокс Рассела: $X := \{x \mid x \notin x\}$; $X \in X$?
4. Вариант решения парадокса: а, может, запретить все «опасные» ситуации?
5. Аксиоматика Цермело — 1908 год, оставим только то, что используют математики.
6. Что такое множество? Неформально мы понимаем, формально:

Теория множеств

1. Георг Кантор: 1877 год, «наивная теория множеств». Множество — это «объединение в одно целое объектов, хорошо различаемых нашей интуицией или нашей мыслью».
2. Неограниченный принцип абстракции $\{x \mid P(x)\}$
3. Парадокс Бурали-Форти (1895, Кантор). Парадокс Рассела: $X := \{x \mid x \notin x\}$; $X \in X$?
4. Вариант решения парадокса: а, может, запретить все «опасные» ситуации?
5. Аксиоматика Цермело — 1908 год, оставим только то, что используют математики.
6. Что такое множество? Неформально мы понимаем, формально:

Определение

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

Аксиоматика ZF, равенство

Определение

Равенство «по Лейбницу»: объекты равны, если неразличимы.

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

Аксиоматика ZF, равенство

Определение

Равенство «по Лейбницу»: объекты равны, если неразличимы.

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

Определение

Принцип объёмности: объекты равны, если состоят из одинаковых частей

Аксиоматика ZF, равенство

Определение

Равенство «по Лейбницу»: объекты равны, если неразличимы.

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

Определение

Принцип объёмности: объекты равны, если состоят из одинаковых частей

Определение

$A \subseteq B \equiv \overbrace{\forall x.x \in A \to x \in B}$ Ф-ла т.м.

Аксиоматика ZF, равенство

Определение

Равенство «по Лейбницу»: объекты равны, если неразличимы.

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

Определение

Принцип объёмности: объекты равны, если состоят из одинаковых частей

Определение

$A \subseteq B \equiv \forall x.x \in A \rightarrow x \in B$
$A = B \equiv A \subseteq B \,\&\, B \subseteq A$

Аксиоматика ZF, равенство

$a \in B$

Определение

Равенство «по Лейбницу»: объекты равны, если неразличимы.

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

Определение

Принцип объёмности: объекты равны, если состоят из одинаковых частей

Определение

$A \subseteq B \equiv \forall x.x \in A \to x \in B$

$A = B \equiv A \subseteq B \,\&\, B \subseteq A$

$A \equiv$ предикат

$P.$

$P_A(x) = \begin{cases} И, & x \in A \\ Л, & x \notin A \end{cases}$

$A = B$

$A \subseteq P \Leftrightarrow B \subseteq P$

Определение

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

$\forall x.\forall y.\forall z.x = y \,\&\, x \in z \to y \in z.$

Аксиоматика ZF, конструктивные аксиомы

Определение

Аксиома пустого. Существует пустое множество $\varnothing$*.*

$$\exists \overset{\varnothing}{s}.\forall t.\neg t \in s$$

Аксиоматика ZF, конструктивные аксиомы

Определение

Аксиома пустого. Существует пустое множество $\varnothing$.

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

Определение

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

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

Аксиоматика ZF, конструктивные аксиомы 2

$\{1,2,3,4,5\} = \bigcup\{\{1,2\},\{2,3\},\{4,5\}\}$

flatten

Определение

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

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

Аксиоматика ZF, конструктивные аксиомы 2

Определение

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

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

Определение

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

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

Аксиоматика ZF. Схема аксиом выделения (comprehension axiom)

(принцип абстракции)

отличие от неограниченного пр. абс.

Определение

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

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

Немного теорем

Теорема

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

Немного теорем

Теорема

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

Доказательство.

Воспользуемся аксиомой пары: $\{X, X\}$ $\square$

Заметим, что $\{X, X\} = \{X\}$.

$X \in \{X\}$.

$X \in \{X\}$

$\{X, X\} \subseteq \{X\}$

очев. $\{X\} \subseteq \{X, X\}$.

Немного теорем

Теорема

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

Доказательство.

Воспользуемся аксиомой пары: $\{X, X\}$ $\square$

Теорема

Пустое множество единственно.

Немного теорем

Теорема

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

Доказательство.

Воспользуемся аксиомой пары: $\{X, X\}$ $\square$

Теорема

Пустое множество единственно.

Доказательство.

Пусть $\forall p. \neg p \in s$ и $\forall p. \neg p \in t$. Тогда $s \subseteq t$ и $t \subseteq s$. $s = t$ $\square$

Немного теорем

Теорема

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

Доказательство.

Воспользуемся аксиомой пары: $\{X, X\}$ $\square$

Теорема

Пустое множество единственно.

Доказательство.

Пусть $\forall p.\neg p \in s$ и $\forall p.\neg p \in t$. Тогда $s \subseteq t$ и $t \subseteq s$. $\square$

Теорема

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

Немного теорем

Теорема

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

Доказательство.

Воспользуемся аксиомой пары: $\{X, X\}$ $\square$

Теорема

Пустое множество единственно.

Доказательство.

Пусть $\forall p.\neg p \in s$ и $\forall p.\neg p \in t$. Тогда $s \subseteq t$ и $t \subseteq s$. $\square$

Теорема

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

Доказательство. ф-ла.

$s \cap t = \{x \in s \mid x \in t\}$ Сх. аксиом выделения $\square$

Упорядоченная пара

$a, b.$

(1) $\{a, b\}$

(2) $\{a\}$

(3) $\{\{a\}, \{a, b\}\}$

Определение

Упорядоченная пара. 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. □

Теорема

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

Аксиома бесконечности

$a \cup b := \cup \{a, b\}$

Определение

Инкремент: $x' \equiv x \cup \{x\}$

Аксиома бесконечности

$\varnothing \qquad \varnothing' = \varnothing \cup \{\varnothing\} = \{\varnothing\} \qquad \varnothing'' = \{\varnothing\} \cup \{\{\varnothing\}\} =$

$= \{\varnothing, \{\varnothing\}\}.$

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

Определение

Инкремент: $x' \equiv x \cup \{x\}$

Определение

Аксиома бесконечности. Существует $\underline{N} : \varnothing \in N \,\&\, \forall x . x \in N \to x' \in N$

Аксиома бесконечности

Определение

Инкремент: $x' \equiv x \cup \{x\}$

Определение

Аксиома бесконечности. Существует $N : \varnothing \in N \,\&\, \forall x. x \in N \to x' \in N$

В N есть всевозможные множества вида $\varnothing$

Аксиома бесконечности

Определение

Инкремент: $x' \equiv x \cup \{x\}$

Определение

Аксиома бесконечности. Существует $N : \varnothing \in N \,\&\, \forall x. x \in N \to x' \in N$

В N есть всевозможные множества вида $\varnothing$, $\{\varnothing\}$

Аксиома бесконечности

Определение

Инкремент: $x' \equiv x \cup \{x\}$

Определение

Аксиома бесконечности. Существует $N : \varnothing \in N \,\&\, \forall x. x \in N \rightarrow x' \in N$

В N есть всевозможные множества вида $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$,

Аксиома бесконечности

Определение

Инкремент: $x' \equiv x \cup \{x\}$

Определение

Аксиома бесконечности. Существует $N : \varnothing \in N \& \forall x.x \in N \to x' \in N$

В N есть всевозможные множества вида $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$, $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$, ...

Аксиома бесконечности

Определение

Инкремент: $x' \equiv x \cup \{x\}$

Определение

Аксиома бесконечности. Существует $N : \varnothing \in N \,\&\, \forall x.x \in N \rightarrow x' \in N$

В N есть всевозможные множества вида $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$, $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$, ...

(неформально) $\omega = \{\varnothing, \varnothing', \varnothing'', \dots\}$.

Аксиома бесконечности

$\omega = \{\bar{0}, \bar{1}, \bar{2}, \dots\}$ $\qquad$ $N_1 = \{\bar{0}, \bar{1}, \bar{2}, \dots\ \omega, \omega', \omega'', \dots\}$

$\omega \notin \omega.$ $\qquad$ $\omega \in N_1$

Определение

Инкремент: $x' \equiv x \cup \{x\}$

Определение

Аксиома бесконечности. Существует $N : \varnothing \in N \,\&\, \forall x . x \in N \to x' \in N$

В N есть всевозможные множества вида $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$, $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$, ...

— лишнее.

(неформально) $\omega = \{\varnothing, \varnothing', \varnothing'', \dots\}$. Тогда $N_1 = \omega \cup \{\omega, \omega', \omega'', \dots\}$ подходит.

Может д-ть, что ω сущ.

Полный порядок (вполне упорядоченные множества)

1. Частичный: рефлексивность ($a \preceq a$), антисимметричность ($a \preceq b \to b \preceq a \to a = b$), транзитивность ($a \preceq b \to b \preceq c \to a \preceq c$).

Полный порядок (вполне упорядоченные множества)

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

Полный порядок (вполне упорядоченные множества)

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

Полный порядок (вполне упорядоченные множества)

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

Пример

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

Полный порядок (вполне упорядоченные множества)

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

Пример

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

Пример

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

Полный порядок (вполне упорядоченные множества)

нестра

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

Пример

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

Пример

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

Пример

$\mathbb{N}$ *вполне упорядочено.*

Ординалы (порядковые числа)

Определение

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

Ординалы (порядковые числа)

Определение

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

Определение

Ординал (порядковое число) — вполне упорядоченное отношением $(\in)$ *транзитивное множество.*

Ординалы (порядковые числа)

Определение

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

лин.

Определение

Ординал (порядковое число) — вполне упорядоченное отношением $(\in)$ *транзитивное множество.*

$a, b \in X$. Тогда $a \in b$ / $b \in a$ или $a = b$.

!! строгий порядок: $a < b$. то.

впр. вп. уп — $a < b \vee a = b$

для нестрогого.

Пример

Ординалы: $\varnothing$,

нестр.

$a \le b$, $b \le c$ | $S \subseteq A$, $S \ne \varnothing$. то сущ. наим. S.

$s \in S$, $\forall x \in S$ $s \le x$.

стр.

$a < b$
$b < a$
$a = b$.

$S \subseteq A$, $S \ne \varnothing$. сущ. наим.

$s \in S$, $\forall x \in S$ $s < x$ или $s = x$

Ординалы (порядковые числа)

[[ ]]

$\varnothing' = \{\varnothing\}$ — не пусто.

Определение

Транзитивное множество X: $\forall x.\forall y.\underline{x \in y} \;\&\; y \in X \to x \in X$.

1) $\varnothing \subseteq \varnothing'$ — вп. уп.

2) $\varnothing' \subseteq \varnothing'$

Определение

Ординал (порядковое число) — вполне упорядоченное отношением $(\in)$ *транзитивное множество.*

$\varnothing$ — насл-

Пример

Ординалы: $\varnothing$, $\varnothing'$,

Ординалы (порядковые числа)

Определение

Транзитивное множество X: $\forall x.\forall y.x \in y \,\&\, y \in X \rightarrow x \in X$.

Определение

Ординал (порядковое число) — вполне упорядоченное отношением $(\in)$ *транзитивное множество.*

Пример

Ординалы: $\varnothing$, $\varnothing'$, $\varnothing''$, $\ldots$

Ординалы (порядковые числа)

Определение

Транзитивное множество X: $\forall x.\forall y.x \in y \,\&\, y \in X \rightarrow x \in X$.

Определение

Ординал (порядковое число) — вполне упорядоченное отношением $(\in)$ *транзитивное множество.*

Пример

Ординалы: $\varnothing, \varnothing', \varnothing'', \dots$

Определение

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

Ординалы (порядковые числа)

Опр.

одр. $x <_{орд} y$, если $x \in y$.

Определение

Транзитивное множество X: $\forall x.\forall y.x \in y \mathbin{\&} y \in X \to x \in X$.

Определение

Ординал (порядковое число) — вполне упорядоченное отношением $(\in)$ транзитивное множество.

$\omega' = \omega \cup \{\omega\}$.

не кон. преу.

Пример

Ординалы: $\varnothing, \varnothing', \varnothing'', \ldots$

Определение

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

Определение

$a \in \omega \Rightarrow a < \omega$. (опр.)

$b < \omega \Rightarrow b \in \omega$

Ординал x конечный, если он сам не предельный и нет предельного, меньшего его.

ω – пред.

$\omega = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \ldots\}$.

$u \in \omega \Rightarrow u$ – число.

$u' = \omega$?

Ординалы (порядковые числа)

Определение

Транзитивное множество X: $\forall x.\forall y.x \in y \,\&\, y \in X \rightarrow x \in X$.

Определение

Ординал (порядковое число) — вполне упорядоченное отношением $(\in)$ *транзитивное множество.*

Пример

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

Определение

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

Определение

Ординал x *конечный, если он сам не предельный и нет предельного, меньшего его.*

Теорема

Если x, y *— ординалы, то* $x = y$, *или* $x \in y$, *или* $y \in x$. (исп. акс. выб)

Предельные ординалы, ω

Определение

ω — наименьший предельный ординал.

Предельные ординалы, ω

Определение

ω — *наименьший предельный ординал.*

Теорема

ω *существует.*

Предельные ординалы, ω

Конечный ординал — ординал, не сод. предельных

Определение

ω — наименьший предельный ординал.

Можно выразить форм:

Теорема

ω существует.

N: $\varnothing \in N$

Если $x \in N$, то $x' \in N$.

Доказательство.

гарант. акс. беск.

Пусть $\omega = \{x \in N \mid \overset{\dots}{x \text{ конечен}}\}$. Тогда:

- меньше ω предельных нет: если θ таков, что $\theta \in \omega$, тогда θ конечен.

Предельные ординалы, ω

Определение

ω — наименьший предельный ординал.

Теорема

ω существует.

Доказательство.

наим. пред. орд.

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

$\theta < \omega$. θ кон. θ' кон.

$\square$

Пример

ω' — тоже ординал.

Порядковый тип

$\mathbb{N}$. $0, 1, 2, \dots$ ω. ω'

$a < b$ ттт $f(a) < f(b)$ $f : \omega \to \omega'$

сохр. пор.

$\omega > 0$
$\omega > 1$
$\omega > 2$
$\dots$ беск.

Определение (неформальное определение)

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

Определение

Порядковый тип вполне упорядоченного множества $\langle S, (\preceq)\rangle$ — ординал A, для которого есть биективное отображение $f : S \to A$, сохраняющее порядок: $a \preceq b$ тогда и только тогда, когда $f(a) \leq f(b)$

Пример

изоморфн. орд.

Множество $\mathbb{Z}$ не имеет порядкового типа (~~в смысле определения через ординалы~~): оно не вполне упорядочено.

Операции над ординалами

$\mathbb{N} + \mathbb{N} = 0_A\, 1_A \dots\quad 0_B\, 1_B \dots$

A, B $\quad A \uplus B = \{\langle 0, a\rangle \mid a \in A\} \cup \{\langle 1, b\rangle \mid b \in B\}$

$\{x_A \mid x \in A\} \cup \{y_B \mid y \in B\}$

Определение

$a + b$ — порядковый тип $a \uplus b$ (отмеченного объединения), причём $x_a < y_b$ при любых $x \in a$ и $y \in b$

Определение

$a \cdot b$ — порядковый тип $a \times b$, произведение упорядочено лексикографически: $\langle x_1, y_1\rangle < \langle x_2, y_2\rangle$, если $x_1 < x_2$ или $x_1 = x_2$ и $y_1 < y_2$.

$\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}.$

Пример

- ✓ $\overline{3} + \overline{4}$: *порядковый тип множества* $\{0_a, 1_a, 2_a, 0_b, 1_b, 2_b, 3_b\}$, *то есть* $\overline{7}$
- ✓ $\overline{\omega} \cdot \overline{\omega}$: *порядковый тип всех натуральных точек плоскости,* $\{\langle 0, 0\rangle, \dots, \langle 0, 100\rangle, \dots, \langle 100, 0\rangle, \dots\}$

Операции над ординалами — как вычислять

$upb\{0, 1, 7, 14\} = 14$

Определение

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

Операции над ординалами — как вычислять

Определение

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

Пример

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

Операции над ординалами — как вычислять

Определение

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

Пример

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

Операции над ординалами — как вычислять

Определение

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

Пример

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

Теорема

б не пред.

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

$\Leftarrow$ б не пред.

(Ф.А.

| Z.F.

① $\omega + 1 = \omega + 0' = (\omega + 0)' = \omega \cup \{\omega\}$.

Пример

② $\omega + 1 = \omega \cup \{\omega\}$;

Операции над ординалами — как вычислять

Определение

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

Пример

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

Теорема

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

Пример

a a a .

$\omega + 1 = \omega \cup \{\omega\};\ \underline{1 + \omega} = upb\ \{1 + \varnothing, 1 + 1, 1 + 2, \dots\}$

Операции над ординалами — как вычислять

Определение

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

Пример

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

Теорема

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

Пример

$\omega + 1 = \omega \cup \{\omega\}$; $1 + \omega = upb\ \{1 + \varnothing, 1 + 1, 1 + 2, \dots\} = \omega$

Ещё операции над ординалами

Теорема

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

(Ф.А.

Ещё операции над ординалами

Теорема

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

Определение

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

Ещё операции над ординалами

Теорема

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

Определение

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

$\underline{\omega + \omega + \omega + 4}$

$\omega + \omega + \omega$

$\omega + \omega, \ldots$

$\omega + 1, \omega + 2, \omega + 3.$

Пример

$\underline{\omega \cdot \omega} = upb\ \{\omega \cdot 0, \omega \cdot 1, \omega \cdot 2, \omega \cdot 3, \ldots\} = \underline{upb\ \{0, \omega, \omega \cdot 2, \omega \cdot 3, \ldots\}} = \{0, 1, 2 \ldots$

Ординалы (порядковые числа) и порядок

$1+\omega$.

$\Uparrow$ $\mathbb{N}$

$\mathbb{N}_0$

$\boxed{1} + \boxed{\omega}$

$0_A \quad 0_B \, 1_B \, 2_B \ldots$

$0_A < 0_B$

$0_A < 1_B$

$\vdots$

$0_A < k_B$.

Пример

- *Добавить элемент перед бесконечностью:* $\mathbb{N}$ *и* $\mathbb{N}_0$.

Ординалы (порядковые числа) и порядок

$0 \to 1$

$1 \to 2$

$2 \to 3$

$\vdots$

Пример

- *Добавить элемент перед бесконечностью:* $\mathbb{N}$ *и* $\mathbb{N}_0$*.* $1 + \omega = \omega$*.*

Ординалы (порядковые числа) и порядок

Пример

- *Добавить элемент перед бесконечностью:* $\mathbb{N}$ *и* $\mathbb{N}_0$. $1 + \omega = \omega$.
- *Добавить элемент после бесконечности* $(+\infty)$.

Ординалы (порядковые числа) и порядок

type ord1 = Left1 of unit | Right1 of nat

<

ord2 = Left2 of nat | Right2 of unit

ord

Left1 () < Right1 7

Left2 7 < Right2 ()

Пример

- *Добавить элемент перед бесконечностью:* $\mathbb{N}$ *и* $\mathbb{N}_0$. $1 + \omega = \omega$.
- *Добавить элемент после бесконечности* $(+\infty)$. $\omega + 1 \neq \omega$

$\underbrace{0, 1, 2}_{\omega}$ (+) $\underbrace{0}_{1}$

+∞

0, 1, 2 . . . .

0, 1, 2, ...

$0_A < 0_B$

$1_A < 0_B$

0_B не имеет предш.

+∞

Пары и списки

Пример

Упорядоченные пары натуральных чисел имеют порядковый тип ω^2.

Пары и списки

Пример

Упорядоченные пары натуральных чисел имеют порядковый тип ω^2.

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

Пары и списки

Пример

Упорядоченные пары натуральных чисел имеют порядковый тип ω^2*.*

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

Пример

Списки натуральных чисел — порядковый тип ω^ω*.*

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

Дизъюнктные множества

Определение

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

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

Дизъюнктные множества

Определение

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

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

Пример

Дизъюнктное: $\{\{1,2\},\{\rightarrow\},\{\alpha,\beta,\gamma\}\}$

Дизъюнктные множества

Определение

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

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

Пример

Дизъюнктное: $\{\{1,2\},\{\to\},\{\alpha,\beta,\gamma\}\}$
Не дизъюнктное: $\{\{1,2\},\{\to\},\{\alpha,\beta,\gamma,1\}\}$

Прямое произведение множеств

Определение

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

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

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

Прямое произведение множеств

Определение

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

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

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

Пример

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

Аксиома выбора

Определение

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

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

Аксиома выбора

Определение

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

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

Альтернативные варианты: любое множество можно вполне упорядочить,

Аксиома выбора

Определение

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

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

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

Определение

Аксиоматика ZF + аксиома выбора = ZFC

Аксиома выбора

Определение

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

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

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

Определение

Аксиоматика ZF + аксиома выбора = ZFC

Дискуссия вокруг аксиомы выбора

Пример

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

Дискуссия вокруг аксиомы выбора

Пример

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

Теорема

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

Дискуссия вокруг аксиомы выбора

Пример

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

Теорема

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

Теорема

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

Дискуссия вокруг аксиомы выбора

Пример

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

Теорема

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

Теорема

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

Пример

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

Дискуссия вокруг аксиомы выбора

Пример

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

Теорема

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

Теорема

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

Пример

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

Теорема

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

Аксиома фундирования

Определение

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

$$\forall x.x = \varnothing \vee \exists y.y \in x \,\&\, \forall z.z \in x \rightarrow z \notin y$$

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:

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

.

Схема аксиом подстановки

Определение

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* $\phi(x, y)\ \&\ \exists! z.\phi(x, z)$*. Тогда для любого множества S существует множество f(S) — образ множества S при отображении f.*

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

ω-непротиворечивая:

если $\varphi(x)$ при любом:

$\vdash \varphi(\bar{0}) \quad \ldots \quad \vdash \varphi(\bar{k}) \; \vdash \varphi(\overline{k+1})$

влечёт $\nvdash \exists x. \neg \varphi(x)$

$\omega = \{0, 1, 2, \ldots\}$.

KFO

$t: t > \omega$.

$\boxed{\omega' = \{0, 1, 2, \ldots \omega\}.}$

$\omega \to k$

$t \to k'$

$t > \omega$.

$f: \omega' \to \omega$

$f(\omega) = ?$

$f(\omega) = k$.

$f(t) = k'$.

$f^{-1}(k') = ?$