Лекция 7

Неразрешимость исчисления предикатов
Аксиоматика Пеано и формальная арифметика

Общие результаты об исчислениях

	К.И.В.	И.И.В.	К.И.П.
корректность	да (лекция 1)	да (ДЗ 3.8)	да (лекция 5)
непротиворечивость	да (очев.)	да (из непр. КИВ)	да (лекция 6)
полнота	да (лекция 2)	да (лекция 3)	да (лекция 6)
разрешимость	да (лекция 2)	да (лекция 4)	

Общие результаты об исчислениях

	К.И.В.	И.И.В.	К.И.П.
корректность	да (лекция 1)	да (ДЗ 3.8)	да (лекция 5)
непротиворечивость	да (очев.)	да (из непр. КИВ)	да (лекция 6)
полнота	да (лекция 2)	да (лекция 3)	да (лекция 6)
разрешимость	да (лекция 2)	да (лекция 4)	Нет (сейчас)

Машина Тьюринга

Определение

Машина Тьюринга:

1. *Внешний алфавит* $q_1, \ldots, q_n$, *выделенный символ-заполнитель* q_ε
2. *Внутренний алфавит (состояний)* $s_1, \ldots, s_k$; s_s *— начальное,* s_f *— допускающее,* s_r *— отвергающее.*
3. *Таблица переходов* $\langle k, s \rangle \Rightarrow \langle k', s', \leftrightarrow \rangle$

Определение

Состояние машины Тьюринга:

1. *Бесконечная лента с символом-заполнителем* q_ε*, текст конечной длины.*
2. *Головка над определённым символом.*
3. *Символ состояния (состояние в узком смысле) — символ внутреннего алфавита.*

Машина, меняющая все 0 на 1, а все 1 — на 0

1. Внешний алфавит $\varepsilon, 0, 1$.
2. Внутренний алфавит s_s, s_f (начальное и допускающее состояния соответственно).
3. Переходы:

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

Машина, меняющая все 0 на 1, а все 1 — на 0

1. Внешний алфавит $\varepsilon, 0, 1$.
2. Внутренний алфавит s_s, s_f (начальное и допускающее состояния соответственно).
3. Переходы:

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

Пример

Головка — на первом символе 011, *состояние* s_s.

Машина, меняющая все 0 на 1, а все 1 — на 0

1. Внешний алфавит $\varepsilon, 0, 1$.
2. Внутренний алфавит s_s, s_f (начальное и допускающее состояния соответственно).
3. Переходы:

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

Пример

Головка — на первом символе 011, *состояние* s_s.

$\underline{0}11$

Машина, меняющая все 0 на 1, а все 1 — на 0

1. Внешний алфавит $\varepsilon, 0, 1$.
2. Внутренний алфавит s_s, s_f (начальное и допускающее состояния соответственно).
3. Переходы:

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

Пример

Головка — на первом символе 011*, состояние* s_s*.*

$\underline{0}11 \Rightarrow 1\underline{1}1$

Машина, меняющая все 0 на 1, а все 1 — на 0

1. Внешний алфавит $\varepsilon, 0, 1$.
2. Внутренний алфавит s_s, s_f (начальное и допускающее состояния соответственно).
3. Переходы:

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

Пример

Головка — на первом символе 011, *состояние* s_s.

$\underline{0}11 \Rightarrow 1\underline{1}1 \Rightarrow 10\underline{1}$

Машина, меняющая все 0 на 1, а все 1 — на 0

1. Внешний алфавит $\varepsilon, 0, 1$.
2. Внутренний алфавит s_s, s_f (начальное и допускающее состояния соответственно).
3. Переходы:

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

Пример

Головка — на первом символе 011*, состояние* s_s*.*

$\underline{0}11 \Rightarrow 1\underline{1}1 \Rightarrow 10\underline{1} \Rightarrow 100\underline{\varepsilon}$

Машина, меняющая все 0 на 1, а все 1 — на 0

1. Внешний алфавит $\varepsilon, 0, 1$.
2. Внутренний алфавит s_s, s_f (начальное и допускающее состояния соответственно).
3. Переходы:

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

Пример

Головка — на первом символе 011, *состояние* s_s.

$\underline{0}11 \Rightarrow 1\underline{1}1 \Rightarrow 10\underline{1} \Rightarrow 100\underline{\varepsilon}$

Состояние s_f, *допускающее.*

Разрешимость

Определение

Язык — множество строк

Определение

Язык L разрешим, если существует машина Тьюринга, которая для любого слова w переходит в допускающее состояние, если $w \in L$, и в отвергающее, если $w \notin L$.

Неразрешимость задачи останова

Определение

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

Теорема

Язык всех останавливающихся машин Тьюринга неразрешим

Доказательство.

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

Неразрешимость задачи останова

Определение

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

Теорема

Язык всех останавливающихся машин Тьюринга неразрешим

Доказательство.

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

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

Неразрешимость задачи останова

Определение

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

Теорема

Язык всех останавливающихся машин Тьюринга неразрешим

Доказательство.

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

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

Что вернёт $S(code(W), code(W))$? $\square$

Кодируем состояние

1. внешний алфавит: n 0-местных функциональных символов $q_1, \ldots, q_n$; q_ε — символ-заполнитель.
2. список: ε и $c(l, s)$; «abc» представим как $c(q_a, c(q_b, c(q_c, \varepsilon)))$.
3. положение головки: «$ab\underline{p}q$» как $(c(q_b, c(q_a, \varepsilon)), c(q_p, c(q_q, \varepsilon)))$.
4. внутренний алфавит: k 0-местных функциональных символов $s_1, \ldots, s_k$. Из них выделенные s_s — начальное и s_f — допускающее состояние.

Достижимые состояния

Предикатный символ $F_{x,y}(w_l, w_r, s)$: если у машины x с начальной строкой y состояние s достижимо на строке $rev(w_l)@w_r$.

Достижимые состояния

Предикатный символ $F_{x,y}(w_l, w_r, s)$: если у машины x с начальной строкой y состояние s достижимо на строке $rev(w_l)@w_r$. Будем накладывать условия: семейство формул C_m.

Достижимые состояния

Предикатный символ $F_{x,y}(w_l, w_r, s)$: если у машины x с начальной строкой y состояние s достижимо на строке $rev(w_l)@w_r$. Будем накладывать условия: семейство формул C_m. Очевидно, начальное состояние достижимо:

$$C_0 := F_{x,y}(\varepsilon, y, s_s)$$

Кодируем переходы

1. Занумеруем переходы.

Кодируем переходы

1. Занумеруем переходы.
2. Закодируем переход m:

$$\langle k, s\rangle \Rightarrow \langle k', s', \rightarrow\rangle, \text{ в случае } q_k \neq q_\varepsilon$$

$C_m = \forall w_l.\forall w_r.F_{x,y}(w_l, c(q_k, w_r), s_s) \rightarrow F_{x,y}(c(q_{k'}, w_l), w_r, s_{s'})$
(здесь требуется, чтобы под головкой находился непустой символ q_k, потому мы обязательно требуем, чтобы лента была непуста)

Кодируем переходы

1. Занумеруем переходы.
2. Закодируем переход m:

$$\langle k, s\rangle \Rightarrow \langle k', s', \rightarrow\rangle, \text{ в случае } q_k \neq q_\varepsilon$$

   $C_m = \forall w_l.\forall w_r.F_{x,y}(w_l, c(q_k, w_r), s_s) \rightarrow F_{x,y}(c(q_{k'}, w_l), w_r, s_{s'})$
   (здесь требуется, чтобы под головкой находился непустой символ q_k, потому мы обязательно требуем, чтобы лента была непуста)
3. Переход посложнее:

$$\langle k, s\rangle \Rightarrow \langle k', s', \leftarrow\rangle, \text{ в случае } q_k \neq q_\varepsilon$$

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

Кодируем переходы

1. Занумеруем переходы.
2. Закодируем переход m:

$$\langle k, s\rangle \Rightarrow \langle k', s', \rightarrow\rangle, \text{ в случае } q_k \neq q_\varepsilon$$

   $C_m = \forall w_l.\forall w_r.F_{x,y}(w_l, c(q_k, w_r), s_s) \rightarrow F_{x,y}(c(q_{k'}, w_l), w_r, s_{s'})$
   (здесь требуется, чтобы под головкой находился непустой символ q_k, потому мы обязательно требуем, чтобы лента была непуста)
3. Переход посложнее:

$$\langle k, s\rangle \Rightarrow \langle k', s', \leftarrow\rangle, \text{ в случае } q_k \neq q_\varepsilon$$

   $C_m = \forall w_l.\forall w_r.\forall t.F_{x,y}(c(t, w_l), c(q_k, w_r), s_s) \rightarrow F_{x,y}(w_l, c(t, c(q_{k'}, w_r)), s_{s'})\ \&$
   $\forall w_l.\forall w_r.F_{x,y}(\varepsilon, c(q_k, w_r), s_s) \rightarrow F_{x,y}(\varepsilon, c(q_\varepsilon, c(q_{k'}, w_r)), s_{s'})$
4. и т.п.

Итоговая формула

$$C = C_0 \mathbin{\&} C_1 \mathbin{\&} \cdots \mathbin{\&} C_n$$

«правильное начальное состояние и правильные переходы между состояниями»

Итоговая формула

$$C = C_0 \mathbin{\&} C_1 \mathbin{\&} \cdots \mathbin{\&} C_n$$

«правильное начальное состояние и правильные переходы между состояниями»

Теорема

Состояние s со строкой $rev(w_l)@w_r$ достижимо тогда и только тогда, когда $C \vdash F_{x,y}(w_l, w_r, s)$

Итоговая формула

$$C = C_0 \mathbin{\&} C_1 \mathbin{\&} \cdots \mathbin{\&} C_n$$

«правильное начальное состояние и правильные переходы между состояниями»

Теорема

Состояние s со строкой $rev(w_l)@w_r$ достижимо тогда и только тогда, когда $C \vdash F_{x,y}(w_l, w_r, s)$

Доказательство.

($\Leftarrow$) Рассмотрим модель: предикат $F_{x,y}(w_l, w_r, s)$ положим истинным, если состояние достижимо.

Итоговая формула

$$C = C_0 \ \& \ C_1 \ \& \cdots \& \ C_n$$

«правильное начальное состояние и правильные переходы между состояниями»

Теорема

Состояние s со строкой $rev(w_l)@w_r$ достижимо тогда и только тогда, когда $C \vdash F_{x,y}(w_l, w_r, s)$

Доказательство.

($\Leftarrow$) Рассмотрим модель: предикат $F_{x,y}(w_l, w_r, s)$ положим истинным, если состояние достижимо. Это — модель для C (по построению C_m).

Итоговая формула

$$C = C_0 \mathbin{\&} C_1 \mathbin{\&} \cdots \mathbin{\&} C_n$$

«правильное начальное состояние и правильные переходы между состояниями»

Теорема

Состояние s со строкой $rev(w_l)@w_r$ достижимо тогда и только тогда, когда $C \vdash F_{x,y}(w_l, w_r, s)$

Доказательство.

($\Leftarrow$) Рассмотрим модель: предикат $F_{x,y}(w_l, w_r, s)$ положим истинным, если состояние достижимо. Это — модель для C (по построению C_m). Значит, доказуемость влечёт истинность (по корректности).

Итоговая формула

$$C = C_0 \mathbin{\&} C_1 \mathbin{\&} \cdots \mathbin{\&} C_n$$

«правильное начальное состояние и правильные переходы между состояниями»

Теорема

Состояние s со строкой $rev(w_l)@w_r$ достижимо тогда и только тогда, когда $C \vdash F_{x,y}(w_l, w_r, s)$

Доказательство.

($\Leftarrow$) Рассмотрим модель: предикат $F_{x,y}(w_l, w_r, s)$ положим истинным, если состояние достижимо. Это — модель для C (по построению C_m). Значит, доказуемость влечёт истинность (по корректности).

($\Rightarrow$) Индукция по длине лога исполнения. $\square$

Неразрешимость исчисления предикатов: доказательство

Теорема

Язык всех доказуемых формул исчисления предикатов неразрешим

Т.е. нет машины Тьюринга, которая бы по любой формуле α определяла, доказуема ли она.

Неразрешимость исчисления предикатов: доказательство

Теорема

Язык всех доказуемых формул исчисления предикатов неразрешим

Т.е. нет машины Тьюринга, которая бы по любой формуле α определяла, доказуема ли она.

Доказательство.

Пусть существует машина Тьюринга, разрешающая любую формулу.

Неразрешимость исчисления предикатов: доказательство

Теорема

Язык всех доказуемых формул исчисления предикатов неразрешим

Т.е. нет машины Тьюринга, которая бы по любой формуле α определяла, доказуема ли она.

Доказательство.

Пусть существует машина Тьюринга, разрешающая любую формулу. На её основе тогда несложно построить некоторую машину Тьюринга, перестраивающую любую машину S (с допускающим состоянием s_f и входом y) в её ограничения C и разрешающую формулу ИП $C \rightarrow \exists w_l.\exists w_r.F_{S,y}(w_l, w_r, s_f)$. Эта машина разрешит задачу останова. $\square$

Аксиоматика Пеано и формальная арифметика

Формализуем дальше: числа

«Бог создал целые числа, всё остальное — дело рук человека.»
Леопольд Кронекер, 1886 г.

Формализуем дальше: числа

«Бог создал целые числа, всё остальное — дело рук человека.»
Леопольд Кронекер, 1886 г.

1. Рациональные ($\mathbb{Q}$).

Формализуем дальше: числа

«Бог создал целые числа, всё остальное — дело рук человека.»
Леопольд Кронекер, 1886 г.

1. Рациональные ($\mathbb{Q}$).
   $Q = \mathbb{Z} \times \mathbb{N}$ — множество всех простых дробей.

Формализуем дальше: числа

«Бог создал целые числа, всё остальное — дело рук человека.»
Леопольд Кронекер, 1886 г.

1. Рациональные ($\mathbb{Q}$).
   $Q = \mathbb{Z} \times \mathbb{N}$ — множество всех простых дробей.
   $\langle p, q \rangle$ — то же, что $\frac{p}{q}$

Формализуем дальше: числа

«Бог создал целые числа, всё остальное — дело рук человека.»
Леопольд Кронекер, 1886 г.

1. Рациональные ($\mathbb{Q}$).
   $Q = \mathbb{Z} \times \mathbb{N}$ — множество всех простых дробей.
   $\langle p, q \rangle$ — то же, что $\frac{p}{q}$
   $\langle p_1, q_1 \rangle \equiv \langle p_2, q_2 \rangle$, если $p_1 q_2 = p_2 q_1$

Формализуем дальше: числа

«Бог создал целые числа, всё остальное — дело рук человека.»
Леопольд Кронекер, 1886 г.

1. Рационалыные ($\mathbb{Q}$).
   $Q = \mathbb{Z} \times \mathbb{N}$ — множество всех простых дробей.
   $\langle p, q \rangle$ — то же, что $\frac{p}{q}$
   $\langle p_1, q_1 \rangle \equiv \langle p_2, q_2 \rangle$, если $p_1 q_2 = p_2 q_1$
   $\mathbb{Q} = Q/_{\equiv}$
2. Вещественные ($\mathbb{R}$).

Формализуем дальше: числа

«Бог создал целые числа, всё остальное — дело рук человека.»
Леопольд Кронекер, 1886 г.

1. Рациональные ($\mathbb{Q}$).
   $Q = \mathbb{Z} \times \mathbb{N}$ — множество всех простых дробей.
   $\langle p, q \rangle$ — то же, что $\frac{p}{q}$
   $\langle p_1, q_1 \rangle \equiv \langle p_2, q_2 \rangle$, если $p_1 q_2 = p_2 q_1$
   $\mathbb{Q} = Q/_{\equiv}$
2. Вещественные ($\mathbb{R}$). $X = \{A, B\}$, где $A, B \subseteq \mathbb{Q}$ — дедекиндово сечение, если:

Формализуем дальше: числа

«Бог создал целые числа, всё остальное — дело рук человека.»
Леопольд Кронекер, 1886 г.

1. Рациональные ($\mathbb{Q}$).
   $Q = \mathbb{Z} \times \mathbb{N}$ — множество всех простых дробей.
   $\langle p, q \rangle$ — то же, что $\frac{p}{q}$
   $\langle p_1, q_1 \rangle \equiv \langle p_2, q_2 \rangle$, если $p_1 q_2 = p_2 q_1$
   $\mathbb{Q} = Q/_{\equiv}$
2. Вещественные ($\mathbb{R}$). $X = \{A, B\}$, где $A, B \subseteq \mathbb{Q}$ — дедекиндово сечение, если:
   2.1 $A \cup B = \mathbb{Q}$

Формализуем дальше: числа

«Бог создал целые числа, всё остальное — дело рук человека.»
Леопольд Кронекер, 1886 г.

1. Рациональные ($\mathbb{Q}$).
   $Q = \mathbb{Z} \times \mathbb{N}$ — множество всех простых дробей.
   $\langle p, q \rangle$ — то же, что $\frac{p}{q}$
   $\langle p_1, q_1 \rangle \equiv \langle p_2, q_2 \rangle$, если $p_1 q_2 = p_2 q_1$
   $\mathbb{Q} = Q/_{\equiv}$
2. Вещественные ($\mathbb{R}$). $X = \{A, B\}$, где $A, B \subseteq \mathbb{Q}$ — дедекиндово сечение, если:
   2.1 $A \cup B = \mathbb{Q}$
   2.2 Если $a \in A$, $x \in \mathbb{Q}$ и $x \leq a$, то $x \in A$

Формализуем дальше: числа

«Бог создал целые числа, всё остальное — дело рук человека.»
Леопольд Кронекер, 1886 г.

1. Рациональные ($\mathbb{Q}$).
   $Q = \mathbb{Z} \times \mathbb{N}$ — множество всех простых дробей.
   $\langle p, q \rangle$ — то же, что $\frac{p}{q}$
   $\langle p_1, q_1 \rangle \equiv \langle p_2, q_2 \rangle$, если $p_1 q_2 = p_2 q_1$
   $\mathbb{Q} = Q/_{\equiv}$
2. Вещественные ($\mathbb{R}$). $X = \{A, B\}$, где $A, B \subseteq \mathbb{Q}$ — дедекиндово сечение, если:
   2.1 $A \cup B = \mathbb{Q}$
   2.2 Если $a \in A$, $x \in \mathbb{Q}$ и $x \leq a$, то $x \in A$
   2.3 Если $b \in B$, $x \in \mathbb{Q}$ и $b \leq x$, то $x \in B$

Формализуем дальше: числа

«Бог создал целые числа, всё остальное — дело рук человека.»
Леопольд Кронекер, 1886 г.

1. Рациональные ($\mathbb{Q}$).
   $Q = \mathbb{Z} \times \mathbb{N}$ — множество всех простых дробей.
   $\langle p, q \rangle$ — то же, что $\frac{p}{q}$
   $\langle p_1, q_1 \rangle \equiv \langle p_2, q_2 \rangle$, если $p_1 q_2 = p_2 q_1$
   $\mathbb{Q} = Q/_{\equiv}$
2. Вещественные ($\mathbb{R}$). $X = \{A, B\}$, где $A, B \subseteq \mathbb{Q}$ — дедекиндово сечение, если:
   2.1 $A \cup B = \mathbb{Q}$
   2.2 Если $a \in A$, $x \in \mathbb{Q}$ и $x \leq a$, то $x \in A$
   2.3 Если $b \in B$, $x \in \mathbb{Q}$ и $b \leq x$, то $x \in B$
   2.4 A не содержит наибольшего.

Формализуем дальше: числа

«Бог создал целые числа, всё остальное — дело рук человека.»
Леопольд Кронекер, 1886 г.

1. Рациональные ($\mathbb{Q}$).
   $Q = \mathbb{Z} \times \mathbb{N}$ — множество всех простых дробей.
   $\langle p, q \rangle$ — то же, что $\frac{p}{q}$
   $\langle p_1, q_1 \rangle \equiv \langle p_2, q_2 \rangle$, если $p_1 q_2 = p_2 q_1$
   $\mathbb{Q} = Q/_{\equiv}$
2. Вещественные ($\mathbb{R}$). $X = \{A, B\}$, где $A, B \subseteq \mathbb{Q}$ — дедекиндово сечение, если:
   2.1 $A \cup B = \mathbb{Q}$
   2.2 Если $a \in A$, $x \in \mathbb{Q}$ и $x \leq a$, то $x \in A$
   2.3 Если $b \in B$, $x \in \mathbb{Q}$ и $b \leq x$, то $x \in B$
   2.4 A не содержит наибольшего.

   $\mathbb{R}$ — множество всех возможных дедекиндовых сечений.

Формализуем дальше: числа

«Бог создал целые числа, всё остальное — дело рук человека.»
Леопольд Кронекер, 1886 г.

1. Рациональные ($\mathbb{Q}$).
   $Q = \mathbb{Z} \times \mathbb{N}$ — множество всех простых дробей.
   $\langle p, q \rangle$ — то же, что $\frac{p}{q}$
   $\langle p_1, q_1 \rangle \equiv \langle p_2, q_2 \rangle$, если $p_1 q_2 = p_2 q_1$
   $\mathbb{Q} = Q/_{\equiv}$
2. Вещественные ($\mathbb{R}$). $X = \{A, B\}$, где $A, B \subseteq \mathbb{Q}$ — дедекиндово сечение, если:
   2.1 $A \cup B = \mathbb{Q}$
   2.2 Если $a \in A$, $x \in \mathbb{Q}$ и $x \le a$, то $x \in A$
   2.3 Если $b \in B$, $x \in \mathbb{Q}$ и $b \le x$, то $x \in B$
   2.4 A не содержит наибольшего.

   $\mathbb{R}$ — множество всех возможных дедекиндовых сечений.
   $\sqrt{2} = \{\{x \in \mathbb{Q} \mid x < 0 \vee x^2 < 2\}, \{x \in \mathbb{Q} \mid x > 0 \ \& \ x^2 > 2\}\}$

Целые числа тоже попробуем определить

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

Целые числа тоже попробуем определить

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

- $Z = \{\langle x, y \rangle \mid x, y \in \mathbb{N}_0\}$

Целые числа тоже попробуем определить

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

- $Z = \{\langle x, y\rangle \mid x, y \in \mathbb{N}_0\}$
- Интуиция: $\langle x, y\rangle = x - y$

Целые числа тоже попробуем определить

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

- $Z = \{\langle x, y \rangle \mid x, y \in \mathbb{N}_0\}$
- Интуиция: $\langle x, y \rangle = x - y$
- $$\langle a, b \rangle + \langle c, d \rangle \quad = \quad \langle a + c, b + d \rangle$$

Целые числа тоже попробуем определить

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

- $Z = \{\langle x, y\rangle \mid x, y \in \mathbb{N}_0\}$
- Интуиция: $\langle x, y\rangle = x - y$
- $$\begin{aligned} \langle a, b\rangle + \langle c, d\rangle &= \langle a + c, b + d\rangle \\ \langle a, b\rangle - \langle c, d\rangle &= \langle a + d, b + c\rangle \end{aligned}$$

Целые числа тоже попробуем определить

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

- $Z = \{\langle x, y \rangle \mid x, y \in \mathbb{N}_0\}$
- Интуиция: $\langle x, y \rangle = x - y$
- $$\begin{aligned} \langle a, b \rangle + \langle c, d \rangle &= \langle a + c, b + d \rangle \\ \langle a, b \rangle - \langle c, d \rangle &= \langle a + d, b + c \rangle \end{aligned}$$
- Пусть $\langle a, b \rangle \equiv \langle c, d \rangle$, если $a + d = b + c$. Тогда $\mathbb{Z} = Z/_{\equiv}$

Целые числа тоже попробуем определить

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

- $Z = \{\langle x, y\rangle \mid x, y \in \mathbb{N}_0\}$
- Интуиция: $\langle x, y\rangle = x - y$
- $$\begin{aligned} \langle a, b\rangle + \langle c, d\rangle &= \langle a + c, b + d\rangle \\ \langle a, b\rangle - \langle c, d\rangle &= \langle a + d, b + c\rangle \end{aligned}$$
- Пусть $\langle a, b\rangle \equiv \langle c, d\rangle$, если $a + d = b + c$. Тогда $\mathbb{Z} = Z/_{\equiv}$
- $0 = [\langle 0, 0\rangle]$, $1 = [\langle 1, 0\rangle]$, $-7 = [\langle 0, 7\rangle]$

Натуральные числа: аксиоматика Пеано, 1889

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

Натуральные числа: аксиоматика Пеано, 1889

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

Определение

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

Натуральные числа: аксиоматика Пеано, 1889

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

Определение

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

1. *Операция «штрих» $(')$: $N \to N$, причём нет $a, b \in N$, что $a \neq b$, но $a' = b'$.*

Натуральные числа: аксиоматика Пеано, 1889

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

Определение

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

1. *Операция «штрих» $(') : N \to N$, причём нет $a, b \in N$, что $a \neq b$, но $a' = b'$. Если $x = y'$, то x назовём следующим за y, а y — предшествующим x.*

Натуральные числа: аксиоматика Пеано, 1889

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

Определение

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

1. *Операция «штрих» $(') : N \to N$, причём нет $a, b \in N$, что $a \neq b$, но $a' = b'$. Если $x = y'$, то x назовём следующим за y, а y — предшествующим x.*
2. *Константа $0 \in N$: нет $x \in N$, что $x' = 0$.*

Натуральные числа: аксиоматика Пеано, 1889

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

Определение

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

1. *Операция «штрих» $(') : N \to N$, причём нет $a, b \in N$, что $a \neq b$, но $a' = b'$. Если $x = y'$, то x назовём следующим за y, а y — предшествующим x.*
2. *Константа $0 \in N$: нет $x \in N$, что $x' = 0$.*
3. *Индукция. Каково бы ни было свойство («предикат») $P : N \to V$, если:*
   3.1 $P(0)$
   3.2 *При любом $x \in N$ из $P(x)$ следует $P(x')$*

   то при любом $x \in N$ выполнено $P(x)$.

Натуральные числа: аксиоматика Пеано, 1889

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

Определение

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

1. *Операция «штрих» $(') : N \to N$, причём нет $a, b \in N$, что $a \neq b$, но $a' = b'$. Если $x = y'$, то x назовём следующим за y, а y — предшествующим x.*
2. *Константа $0 \in N$: нет $x \in N$, что $x' = 0$.*
3. *Индукция. Каково бы ни было свойство («предикат») $P : N \to V$, если:*
   - 3.1 $P(0)$
   - 3.2 *При любом $x \in N$ из $P(x)$ следует $P(x')$*

   то при любом $x \in N$ выполнено $P(x)$.

Как построить? Например, в стиле алгебры Линденбаума:

Натуральные числа: аксиоматика Пеано, 1889

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

Определение

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

1. *Операция «штрих» $(') : N \to N$, причём нет $a, b \in N$, что $a \neq b$, но $a' = b'$. Если $x = y'$, то x назовём следующим за y, а y — предшествующим x.*
2. *Константа $0 \in N$: нет $x \in N$, что $x' = 0$.*
3. *Индукция. Каково бы ни было свойство («предикат») $P : N \to V$, если:*
   3.1 $P(0)$
   3.2 *При любом $x \in N$ из $P(x)$ следует $P(x')$*

   то при любом $x \in N$ выполнено $P(x)$.

Как построить? Например, в стиле алгебры Линденбаума:

1. N — язык, порождённый грамматикой $\nu ::= 0 \mid \nu$«'»

Натуральные числа: аксиоматика Пеано, 1889

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

Определение

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

1. *Операция «штрих» $(') : N \to N$, причём нет $a, b \in N$, что $a \neq b$, но $a' = b'$. Если $x = y'$, то x назовём следующим за y, а y — предшествующим x.*
2. *Константа $0 \in N$: нет $x \in N$, что $x' = 0$.*
3. *Индукция. Каково бы ни было свойство («предикат») $P : N \to V$, если:*
   3.1 $P(0)$
   3.2 *При любом $x \in N$ из $P(x)$ следует $P(x')$*

   то при любом $x \in N$ выполнено $P(x)$.

Как построить? Например, в стиле алгебры Линденбаума:

1. N — язык, порождённый грамматикой $\nu ::= 0 \mid \nu$«’»
2. 0 — это «0», x' — это x ++ «’»

Примеры: что не соответствует аксиомам Пеано

1. $\mathbb{Z}$, где $x' = x^2$

Примеры: что не соответствует аксиомам Пеано

1. $\mathbb{Z}$, где $x' = x^2$
   Функция «штрих» не инъективна: $-3^2 = 3^2 = 9$

Примеры: что не соответствует аксиомам Пеано

1. $\mathbb{Z}$, где $x' = x^2$
   Функция «штрих» не инъективна: $-3^2 = 3^2 = 9$
2. Кольцо вычетов $\mathbb{Z}/7\mathbb{Z}$, где $x' = x + 1$

Примеры: что не соответствует аксиомам Пеано

1. $\mathbb{Z}$, где $x' = x^2$
   Функция «штрих» не инъективна: $-3^2 = 3^2 = 9$
2. Кольцо вычетов $\mathbb{Z}/7\mathbb{Z}$, где $x' = x + 1$
   $6' = 0$, что нарушает свойства 0

Примеры: что не соответствует аксиомам Пеано

1. $\mathbb{Z}$, где $x' = x^2$
   Функция «штрих» не инъективна: $-3^2 = 3^2 = 9$
2. Кольцо вычетов $\mathbb{Z}/7\mathbb{Z}$, где $x' = x + 1$
   $6' = 0$, что нарушает свойства 0
3. $\mathbb{R}^+ \cup \{0\}$, где $x' = x + 1$

Примеры: что не соответствует аксиомам Пеано

1. $\mathbb{Z}$, где $x' = x^2$
   Функция «штрих» не инъективна: $-3^2 = 3^2 = 9$
2. Кольцо вычетов $\mathbb{Z}/7\mathbb{Z}$, где $x' = x + 1$
   $6' = 0$, что нарушает свойства 0
3. $\mathbb{R}^+ \cup \{0\}$, где $x' = x + 1$
   Пусть $P(x)$ означает «$x \in \mathbb{Z}$»:

Примеры: что не соответствует аксиомам Пеано

1. $\mathbb{Z}$, где $x' = x^2$
   Функция «штрих» не инъективна: $-3^2 = 3^2 = 9$
2. Кольцо вычетов $\mathbb{Z}/7\mathbb{Z}$, где $x' = x + 1$
   $6' = 0$, что нарушает свойства 0
3. $\mathbb{R}^+ \cup \{0\}$, где $x' = x + 1$
   Пусть $P(x)$ означает «$x \in \mathbb{Z}$»:
   3.1 $P(0)$ выполнено: $0 \in \mathbb{Z}$.

Примеры: что не соответствует аксиомам Пеано

1. $\mathbb{Z}$, где $x' = x^2$
   Функция «штрих» не инъективна: $-3^2 = 3^2 = 9$
2. Кольцо вычетов $\mathbb{Z}/7\mathbb{Z}$, где $x' = x + 1$
   $6' = 0$, что нарушает свойства 0
3. $\mathbb{R}^+ \cup \{0\}$, где $x' = x + 1$
   Пусть $P(x)$ означает «$x \in \mathbb{Z}$»:
   3.1 $P(0)$ выполнено: $0 \in \mathbb{Z}$.
   3.2 Если $P(x)$, то есть $x \in \mathbb{Z}$, то и $x + 1 \in \mathbb{Z}$ — так что и $P(x')$ выполнено.

Примеры: что не соответствует аксиомам Пеано

1. $\mathbb{Z}$, где $x' = x^2$
   Функция «штрих» не инъективна: $-3^2 = 3^2 = 9$
2. Кольцо вычетов $\mathbb{Z}/7\mathbb{Z}$, где $x' = x + 1$
   $6' = 0$, что нарушает свойства 0
3. $\mathbb{R}^+ \cup \{0\}$, где $x' = x + 1$
   Пусть $P(x)$ означает «$x \in \mathbb{Z}$»:
   3.1 $P(0)$ выполнено: $0 \in \mathbb{Z}$.
   3.2 Если $P(x)$, то есть $x \in \mathbb{Z}$, то и $x + 1 \in \mathbb{Z}$ — так что и $P(x')$ выполнено.

   Однако $P(0.5)$ ложно.

Пример доказательства

Теорема

0 единственен: если t таков, что при любом y выполнено $y' \neq t$, то $t = 0$.

Пример доказательства

Теорема

0 единственен: если t таков, что при любом y выполнено $y' \neq t$, то $t = 0$.

Доказательство.

- Определим $P(x)$ как «либо $x = 0$, либо $x = y'$ для некоторого $y \in N$».

Пример доказательства

Теорема

0 единственен: если t таков, что при любом y выполнено $y' \neq t$, то $t = 0$.

Доказательство.

- Определим $P(x)$ как «либо $x = 0$, либо $x = y'$ для некоторого $y \in N$».
  1. $P(0)$ выполнено, так как $0 = 0$.

Пример доказательства

Теорема

0 единственен: если t таков, что при любом y выполнено $y' \neq t$, то $t = 0$.

Доказательство.

- Определим $P(x)$ как «либо $x = 0$, либо $x = y'$ для некоторого $y \in N$».
  1. $P(0)$ выполнено, так как $0 = 0$.
  2. Если $P(x)$ выполнено, то возьмём x в качестве y: тогда для $P(x')$ будет выполнено $x' = y'$.

Пример доказательства

Теорема

0 единственен: если t таков, что при любом y выполнено $y' \neq t$, то $t = 0$.

Доказательство.

- Определим $P(x)$ как «либо $x = 0$, либо $x = y'$ для некоторого $y \in N$».
  1. $P(0)$ выполнено, так как $0 = 0$.
  2. Если $P(x)$ выполнено, то возьмём x в качестве y: тогда для $P(x')$ будет выполнено $x' = y'$.

  Значит, $P(x)$ для любого $x \in N$.

Пример доказательства

Теорема

0 единственен: если t таков, что при любом y выполнено $y' \neq t$, то $t = 0$.

Доказательство.

- Определим $P(x)$ как «либо $x = 0$, либо $x = y'$ для некоторого $y \in N$».
  1. $P(0)$ выполнено, так как $0 = 0$.
  2. Если $P(x)$ выполнено, то возьмём x в качестве y: тогда для $P(x')$ будет выполнено $x' = y'$.

  Значит, $P(x)$ для любого $x \in N$.
- Рассмотрим $P(t)$: «либо $t = 0$, либо $t = y'$ для некоторого $y \in N$». Но так как такого y нет, то неизбежно $t = 0$.

$\square$

Обозначения и определения

Определение

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

Обозначения и определения

Определение

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

Определение

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

Обозначения и определения

Определение

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

Определение

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

Например,

$$2 + 2 = 0'' + 0'' =$$

Обозначения и определения

Определение

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

Определение

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

Например,

$$2 + 2 = 0'' + 0'' = (0'' + 0')' =$$

Обозначения и определения

Определение

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

Определение

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

Например,

$$2 + 2 = 0'' + 0'' = (0'' + 0')' = ((0'' + 0)')' =$$

Обозначения и определения

Определение

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

Определение

$$a + b = \begin{cases} a, & \textit{если } b = 0 \\ (a + c)', & \textit{если } b = c' \end{cases}$$

Например,

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

Обозначения и определения

Определение

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

Определение

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

Например,

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

Определение

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

Пример: коммутативность сложения (лемма 1)

Лемма (1)

$a + 0 = 0 + a$

Пример: коммутативность сложения (лемма 1)

Лемма (1)

$a + 0 = 0 + a$

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

Пример: коммутативность сложения (лемма 1)

Лемма (1)

$a + 0 = 0 + a$

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

Доказательство.

Пусть $P(x)$ — это $x + 0 = 0 + x$.

Пример: коммутативность сложения (лемма 1)

Лемма (1)

$a + 0 = 0 + a$

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

Доказательство.

Пусть $P(x)$ — это $x + 0 = 0 + x$.

1. Покажем $P(0)$. $0 + 0 = 0 + 0$

Пример: коммутативность сложения (лемма 1)

Лемма (1)

$a + 0 = 0 + a$

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

Доказательство.

Пусть $P(x)$ — это $x + 0 = 0 + x$.

1. Покажем $P(0)$. $0 + 0 = 0 + 0$
2. Покажем, что если $P(x)$, то $P(x')$. Покажем $P(x')$, то есть $x' + 0 = \ldots$

Пример: коммутативность сложения (лемма 1)

Лемма (1)

$a + 0 = 0 + a$

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

Доказательство.

Пусть $P(x)$ — это $x + 0 = 0 + x$.

1. Покажем $P(0)$. $0 + 0 = 0 + 0$
2. Покажем, что если $P(x)$, то $P(x')$. Покажем $P(x')$, то есть $x' + 0 = \dots$

$$\dots = x' \qquad a = x', b = 0: \quad x' + 0 \Rightarrow x'$$

Пример: коммутативность сложения (лемма 1)

Лемма (1)

$a + 0 = 0 + a$

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

Доказательство.

Пусть $P(x)$ — это $x + 0 = 0 + x$.

1. Покажем $P(0)$. $0 + 0 = 0 + 0$
2. Покажем, что если $P(x)$, то $P(x')$. Покажем $P(x')$, то есть $x' + 0 = \dots$

$$\dots = x' \qquad a = x', b = 0: \quad x' + 0 \Rightarrow x'$$

$$\dots = (x)'$$

Пример: коммутативность сложения (лемма 1)

Лемма (1)

$a + 0 = 0 + a$

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

Доказательство.

Пусть $P(x)$ — это $x + 0 = 0 + x$.

1. Покажем $P(0)$. $0 + 0 = 0 + 0$
2. Покажем, что если $P(x)$, то $P(x')$. Покажем $P(x')$, то есть $x' + 0 = \dots$

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

Пример: коммутативность сложения (лемма 1)

Лемма (1)

$a + 0 = 0 + a$

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

Доказательство.

Пусть $P(x)$ — это $x + 0 = 0 + x$.

1. Покажем $P(0)$. $0 + 0 = 0 + 0$
2. Покажем, что если $P(x)$, то $P(x')$. Покажем $P(x')$, то есть $x' + 0 = \dots$

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

Пример: коммутативность сложения (лемма 1)

Лемма (1)

$a + 0 = 0 + a$

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

Доказательство.

Пусть $P(x)$ — это $x + 0 = 0 + x$.

1. Покажем $P(0)$. $0 + 0 = 0 + 0$
2. Покажем, что если $P(x)$, то $P(x')$. Покажем $P(x')$, то есть $x' + 0 = \dots$

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

Пример: коммутативность сложения (лемма 1)

Лемма (1)

$a + 0 = 0 + a$

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

Доказательство.

Пусть $P(x)$ — это $x + 0 = 0 + x$.

1. Покажем $P(0)$. $0 + 0 = 0 + 0$
2. Покажем, что если $P(x)$, то $P(x')$. Покажем $P(x')$, то есть $x' + 0 = \dots$

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

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

Пример: коммутативность сложения (завершение)

Лемма (2)

$a + b' = a' + b$

Пример: коммутативность сложения (завершение)

Лемма (2)

$a + b' = a' + b$

Доказательство.

$P(x)$ — это $a + x' = a' + x$

Пример: коммутативность сложения (завершение)

Лемма (2)

$a + b' = a' + b$

Доказательство.

$P(x)$ — это $a + x' = a' + x$

1. $a + 0' = (a + 0)' = (a)' = a' = a' + 0$

Пример: коммутативность сложения (завершение)

Лемма (2)

$a + b' = a' + b$

Доказательство.

$P(x)$ — это $a + x' = a' + x$

1. $a + 0' = (a + 0)' = (a)' = a' = a' + 0$
2. Покажем, что $P(x')$ следует из $P(x)$: $a + x'' = (a + x')' = (a' + x)' = a' + x'$

$\square$

Пример: коммутативность сложения (завершение)

Лемма (2)

$a + b' = a' + b$

Доказательство.

$P(x)$ — это $a + x' = a' + x$

1. $a + 0' = (a + 0)' = (a)' = a' = a' + 0$
2. Покажем, что $P(x')$ следует из $P(x)$: $a + x'' = (a + x')' = (a' + x)' = a' + x'$

$\square$

Теорема

$a + b = b + a$

Пример: коммутативность сложения (завершение)

Лемма (2)

$a + b' = a' + b$

Доказательство.

$P(x)$ — это $a + x' = a' + x$

1. $a + 0' = (a + 0)' = (a)' = a' = a' + 0$
2. Покажем, что $P(x')$ следует из $P(x)$: $a + x'' = (a + x')' = (a' + x)' = a' + x'$

$\square$

Теорема

$a + b = b + a$

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

1. $a + 0 = 0 + a$ (лемма 1)

Пример: коммутативность сложения (завершение)

Лемма (2)

$a + b' = a' + b$

Доказательство.

$P(x)$ — это $a + x' = a' + x$

1. $a + 0' = (a + 0)' = (a)' = a' = a' + 0$
2. Покажем, что $P(x')$ следует из $P(x)$: $a + x'' = (a + x')' = (a' + x)' = a' + x'$

$\square$

Теорема

$a + b = b + a$

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

1. $a + 0 = 0 + a$ (лемма 1)
2. $a + x' = (a + x)' = (x + a)' = x + a' = x' + a$

$\square$

Уточнение исчисления предикатов

- Пусть требуется доказывать утверждения про равенство. Введём $E(p, q)$ — предикат «равенство».

Уточнение исчисления предикатов

- Пусть требуется доказывать утверждения про равенство. Введём $E(p, q)$ — предикат «равенство».
- Однако $\nvdash E(p, q) \rightarrow E(q, p)$: если $D = \{0, 1\}$ и $E(p, q) ::= (p > q)$, то $\not\models E(p, q) \rightarrow E(q, p)$.

Уточнение исчисления предикатов

- Пусть требуется доказывать утверждения про равенство. Введём $E(p, q)$ — предикат «равенство».
- Однако $\nvdash E(p, q) \rightarrow E(q, p)$: если $D = \{0, 1\}$ и $E(p, q) ::= (p > q)$, то $\not\models E(p, q) \rightarrow E(q, p)$.
- Конечно, можем указывать $\forall p.\forall q.E(p, q) \rightarrow E(q, p) \vdash \varphi$.

Уточнение исчисления предикатов

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

Уточнение исчисления предикатов

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

Теория первого порядка

Определение

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

- *предикатными и функциональными символами;*
- *аксиомами.*

Сущности, взятые из исходного исчисления предикатов, назовём логическими

Порядок логики/теории

Порядок	Кванторы	Формализует суждения...	Пример
нулевой	запрещены	об отдельных значениях	И.В.
первый	по предметным переменным	о множествах	И.П.
	$\{2,3,5,7,\dots\} = \{t \mid \forall p.\forall q.(p \neq 1 \,\&\, q \neq 1) \rightarrow (t \neq p \cdot q)\}$		
второй	по предикатным переменным	о множествах множеств	Типы
	$S = \{\{t \mid P(t)\} \mid \varphi[p := P]\}$		
	...		

Порядок логики/теории

Порядок	Кванторы	Формализует суждения...	Пример
нулевой	запрещены	об отдельных значениях	И.В.
первый	по предметным переменным	о множествах	И.П.
	$\{2,3,5,7,\dots\} = \{t \mid \forall p.\forall q.(p \neq 1 \,\&\, q \neq 1) \to (t \neq p \cdot q)\}$		
второй	по предикатным переменным	о множествах множеств	Типы
	$S = \{\{t \mid P(t)\} \mid \varphi[p := P]\}$		
	...		

Пример (логики 2 порядка)

$\alpha \to \beta \to \alpha$ (сх. акс. 1) $\quad \forall a.\forall b.a \to b \to a$

```
let rec map f l = match l with
| [] -> []
| l1::ls -> f l1 :: map f l1
```

$map : \forall a.\forall b.(a \to b) \to a\ \texttt{list} \to b\ \texttt{list}$

```
map ((+) 1) [1;2;3] = [2;3;4]
```

Формальная арифметика

Определение

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

- *двухместными функциональными символами* $(+)$, $(\cdot)$; *одноместным функциональным символом* $(')$, *нульместным функциональным символом* 0;

Формальная арифметика

Определение

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

- *двухместными функциональными символами* $(+)$, $(\cdot)$; *одноместным функциональным символом* $(')$, *нульместным функциональным символом* 0;
- *двухместным предикатным символом* $(=)$;

Формальная арифметика

Определение

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

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

(A1) $a = b \rightarrow a = c \rightarrow b = c$	(A5) $a + 0 = a$
(A2) $a = b \rightarrow a' = b'$	(A6) $a + b' = (a + b)'$
(A3) $a' = b' \rightarrow a = b$	(A7) $a \cdot 0 = 0$
(A4) $\neg a' = 0$	(A8) $a \cdot b' = a \cdot b + a$

Формальная арифметика

Определение

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

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

(A1) $a = b \to a = c \to b = c$	(A5) $a + 0 = a$
(A2) $a = b \to a' = b'$	(A6) $a + b' = (a + b)'$
(A3) $a' = b' \to a = b$	(A7) $a \cdot 0 = 0$
(A4) $\neg a' = 0$	(A8) $a \cdot b' = a \cdot b + a$

- *нелогической схемой аксиом индукции* $\psi[x := 0] \,\&\, (\forall x.\psi \to \psi[x := x']) \to \psi$ *с метапеременными* x *и* ψ.

Докажем, что $a = a$

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

Докажем, что $a = a$

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

(1)	$a = b \to a = c \to b = c$	(Акс. A1)
(2)	$(a = b \to a = c \to b = c) \to \top \to (a = b \to a = c \to b = c)$	(Сх. акс. 1)
(3)	$\top \to (a = b \to a = c \to b = c)$	(M.P. 1, 2)
(4)	$\top \to (\forall c.a = b \to a = c \to b = c)$	(Введ. $\forall$)

Докажем, что $a = a$

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

(1)	$a = b \rightarrow a = c \rightarrow b = c$	(Акс. A1)
(2)	$(a = b \rightarrow a = c \rightarrow b = c) \rightarrow \top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$	(Сх. акс. 1)
(3)	$\top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$	(M.P. 1, 2)
(4)	$\top \rightarrow (\forall c.a = b \rightarrow a = c \rightarrow b = c)$	(Введ. $\forall$)
(5)	$\top \rightarrow (\forall b.\forall c.a = b \rightarrow a = c \rightarrow b = c)$	(Введ. $\forall$)
(6)	$\top \rightarrow (\forall a.\forall b.\forall c.a = b \rightarrow a = c \rightarrow b = c)$	(Введ. $\forall$)

Докажем, что $a = a$

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

(1)	$a = b \rightarrow a = c \rightarrow b = c$	(Акс. A1)
(2)	$(a = b \rightarrow a = c \rightarrow b = c) \rightarrow \top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$	(Сх. акс. 1)
(3)	$\top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$	(M.P. 1, 2)
(4)	$\top \rightarrow (\forall c.a = b \rightarrow a = c \rightarrow b = c)$	(Введ. $\forall$)
(5)	$\top \rightarrow (\forall b.\forall c.a = b \rightarrow a = c \rightarrow b = c)$	(Введ. $\forall$)
(6)	$\top \rightarrow (\forall a.\forall b.\forall c.a = b \rightarrow a = c \rightarrow b = c)$	(Введ. $\forall$)
(7)	$\top$	(Сх. акс 1)
(8)	$(\forall a.\forall b.\forall c.a = b \rightarrow a = c \rightarrow b = c)$	(M.P. 7, 6)

Докажем, что $a = a$

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

(1)	$a = b \rightarrow a = c \rightarrow b = c$	(Акс. A1)
(2)	$(a = b \rightarrow a = c \rightarrow b = c) \rightarrow \top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$	(Сх. акс. 1)
(3)	$\top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$	(M.P. 1, 2)
(4)	$\top \rightarrow (\forall c.a = b \rightarrow a = c \rightarrow b = c)$	(Введ. $\forall$)
(5)	$\top \rightarrow (\forall b.\forall c.a = b \rightarrow a = c \rightarrow b = c)$	(Введ. $\forall$)
(6)	$\top \rightarrow (\forall a.\forall b.\forall c.a = b \rightarrow a = c \rightarrow b = c)$	(Введ. $\forall$)
(7)	$\top$	(Сх. акс 1)
(8)	$(\forall a.\forall b.\forall c.a = b \rightarrow a = c \rightarrow b = c)$	(M.P. 7, 6)
(9)	$(\forall a.\forall b.\forall c.a = b \rightarrow a = c \rightarrow b = c) \rightarrow$	
	$\rightarrow (\forall b.\forall c.a + 0 = b \rightarrow a + 0 = c \rightarrow b = c)$	(Сх. акс. 11)

Докажем, что $a = a$

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

(1)	$a = b \to a = c \to b = c$	(Акс. A1)
(2)	$(a = b \to a = c \to b = c) \to \top \to (a = b \to a = c \to b = c)$	(Сх. акс. 1)
(3)	$\top \to (a = b \to a = c \to b = c)$	(M.P. 1, 2)
(4)	$\top \to (\forall c.a = b \to a = c \to b = c)$	(Введ. $\forall$)
(5)	$\top \to (\forall b.\forall c.a = b \to a = c \to b = c)$	(Введ. $\forall$)
(6)	$\top \to (\forall a.\forall b.\forall c.a = b \to a = c \to b = c)$	(Введ. $\forall$)
(7)	$\top$	(Сх. акс 1)
(8)	$(\forall a.\forall b.\forall c.a = b \to a = c \to b = c)$	(M.P. 7, 6)
(9)	$(\forall a.\forall b.\forall c.a = b \to a = c \to b = c) \to$	
	$\to (\forall b.\forall c.a + 0 = b \to a + 0 = c \to b = c)$	(Сх. акс. 11)
(10)	$\forall b.\forall c.a + 0 = b \to a + 0 = c \to b = c$	(M.P. 8, 9)

Докажем, что $a = a$

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

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

Докажем, что $a = a$

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

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

Докажем, что $a = a$

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

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