# 1 Отношение эквивалентности

### Определение

Бинарное отношение $r \subseteq A^2$ называется **отношением эквивалентности**, тогда и только тогда, когда оно рефлексивно, симметрично и транзитивно. Другими словами, выполняются следующие свойства:

1. **рефлексивность** $\forall a \in A\ (a, a) \in r$
2. **симметричность** $\forall a, b \in A\ (a, b) \in r \Rightarrow (b, a) \in r$
3. **транзитивность** $\forall a, b, c \in A\ (a, b) \in r,\ (b, c) \in r \Rightarrow (a, c) \in r$

Для обозначения отношений эквивалентности используются символы вида $\sim$, $\equiv$. Если использовать символ $\sim$ (или $\equiv$) для отношения эквивалентности $r$, то вместо $(a, b) \in \sim$ можно писать $a \sim b$ и называть $\sim$ просто эквивалентностью.

## Примеры отношений эквивалентности

### Пример 1

Определим эквивалентность $\sim_{\mathbb{Q}}$ на множестве $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$:

$$(n_1, n_2) \sim_{\mathbb{Q}} (m_1, m_2) \Leftrightarrow n_1 \cdot m_2 = n_2 \cdot m_1$$

Понятно, что $(n_1, n_2) \sim_{\mathbb{Q}} (m_1, m_2)$ означает, что $\frac{n_1}{n_2} = \frac{m_1}{m_2}$

Пусть $n, k \in \mathbb{N}$ - натуральные числа. Введем следующие обозначения:

- $\lfloor n/k \rfloor$ - целая часть от деления $n$ на $k$, т.е. $\lfloor n/k \rfloor \cdot k \leq n < (\lfloor n/k \rfloor + 1) \cdot k$
- $rest(n, k) \rightleftharpoons n - \lfloor n/k \rfloor \cdot k$ - остаток от деления $n$ на $k$

### Пример 2

Мы можем определить отношение эквивалентности $\equiv_k$ на множестве $\mathbb{Z}$:

$$n_1 \equiv_k n_2 \Leftrightarrow rest(n_1, k) = rest(n_2, k)$$

# 2 Отношение частичного порядка

### Определение

Бинарное отношение $r \subseteq A^2$ называется отношением **частичного порядка**, или просто **частичным порядком**, если оно рефлексивно, антисимметрично и транзитивно. Другими словами, оно должно удовлетворять следующим свойствам:

1. **рефлексивность**: $\forall a \in A \ (a, a) \in r$
2. **антисимметричность**: $\forall a, b \in A \ (a, b) \in r, (b, a) \in r \Rightarrow a = b$
3. **транзитивность**: $\forall a, b, c \in A \ (a, b) \in r, \ (b, c) \in r \Rightarrow (a, c) \in r$

Для обозначения отношения частичного порядка обычно используются следующие символы: $\leq, \subseteq, \preceq, \sqsubseteq, \ldots$. Если такой символ используется в качестве $r$, то вместо $(a, b) \in \leq$ можно использовать более общие обозначения $a \leq b$ и называть $\leq$ просто частичным порядком.

Важный частный случай частичного порядка, также называемый линейным порядком..

### Определение

Частичный порядок $\leq$ на множестве $A$ называется **линейным порядком**, если выполняется следующее свойство:

$$\forall a, b \in A \ (a, b) \in r \text{ или } (b, a) \in r$$

## Примеры частичных порядков

### Пример 1

Обычное отношение $\leq$ на действительных числах $\mathbb{R}$ является линейным порядком.

### Пример 2

Пусть $A$ - множество. Тогда бинарное отношение $\subseteq_A$ на множестве $\mathcal{P}(A)$ будет частичным порядком, но не линейным в общем случае.

**Пример 3**

Определим отношение делимости $|$ на множестве натуральных чисел $\mathbb{N} = \{1, 2, 3, \ldots\}$ как:

$$n|m \Leftrightarrow n \text{ делит } m$$

Тогда $|$ является частичным порядком на $\mathbb{N}$.

# 3 Равномощность множеств

**Определение**

Два множества $A$ и $B$ **равномощны**, тогда и только тогда, когда существует биекция из $A$ в $B$. Это отношение обозначается как $A \approx B$. В множестве $A$ содержится **не более** элементов, чем в $B$, тогда и только тогда, когда существует всюду определенная инъекция из $A$ в $B$. Это отношение обозначается как $A \preceq B$.

# 4 $\lambda$-term

**Определение**

$\lambda$-терм, составленный из переменных $X$ и констант $C$ - это слово в алфавите $\mathcal{A}_\lambda \cup X \cup C$, определяемое по индукции:

- любая переменная $x \in X$ и любая константа $c \in C$ являются $\lambda$-термом.
- для любых $\lambda$-термов $p$ и $q$ запись

  $$(p\ q)$$

  является $\lambda$-термом и называется **аппликацией** $p$ к $q$.
- для любой переменной $x \in X$ и $\lambda$-терма $f$, запись

  $$(\lambda x.f)$$

  является $\lambda$-термом и называется **абстракцией** $f$ от $x$.

# 5 $\beta$-редукция

**$\beta$-редукция** правило переписывания:

$$(\lambda x.t)s \Rightarrow_\beta t[x = s]$$

может применяться когда подстановка $t[x = s]$ не создаёт конфликта имен переменных в $t$, т.е. когда $s$ свободно относительно $x$ в $t$.

$\beta$-редукция - это элементарный шаг вычисления, при котором все вхождения переменной $x$ просто заменяются на $s$ внутри $t$, как только выражение $(\lambda x.t)s$ встречается в переписываемом терме. Терм вида $(\lambda x.t)s$ называется **$\beta$-редексом**, а результат редукции $t[x = s]$ называется **$\beta$-сокращением**.

# 6 Нормальная форма $\lambda$-терма

### Определение

$\lambda$-терм $t$ находится в **нормальной форме**, если он не содержит подтерма $s$, такого, что существует некоторый $\alpha$-эквивалентный к $s$ терм $s'$, образующий $\beta$ или $\eta$ редекс в $t$.

Дальнейшая редукция терма в нормальной форме невозможна, поскольку он не имеет редексов.

### Примеры нормальных форм

- $I = \lambda x.x$ находится в нормальной форме
- $(f(tsr))$ находится в нормальной форме
- $(f((\lambda x.(gxh))sr))$ не находится в нормальной форме, потому что он имеет редекс $(\lambda x.(gxh))s$

# 7 Формулы логики высказываний

### Определение

Алфавит логики высказываний: $\mathcal{A}_{prop} = \{(,), \wedge, \vee, \rightarrow, \neg, \top, \bot\} \cup V$ где $V = \{v_i | i \in \omega\}$ - бесконечное множество **пропозициональных переменных**.

**Определение**

**формула** логики высказываний - это слово алфавита $\mathcal{A}_{prop}$, определяемое по индукции:

1. $\top, \bot$ и $v_i$ для всех $i \in \omega$ являются **атомарными** формулами
2. если $\phi, \psi$ являются формулами, то следующие слова также являются формулами:
   - $(\phi \wedge \psi)$
   - $(\phi \vee \psi)$
   - $(\phi \to \psi)$
   - $\neg\phi$

# 8 Истинность формул логики высказываний

**Определение**

Если $\gamma(\phi) = 1$, то будем говорить, что эта формула **истинна** при означивании $\gamma$, если $\gamma(\phi) = 0$ будем говорить, что формула **ложна** при означивании $\gamma$.

# 9 Линейное доказательство в логике высказываний

**Определение**

**Линейное доказательство** (или **линейный вывод**) из множества секвенций $H$ в исчислении высказываний - это последовательность секвенций $(s_1, s_2, \ldots, s_n)$ такая, что каждая секвенция $s_i$:

- аксиома исчисления высказываний, т.е. $s_i \in A_{PC}$
- или $s_i \in H$
- или получена из некоторых секвенций $s_{j_1}, s_{j_2}, \ldots, s_{j_k}$, где $j_1, j_2, \ldots, j_k < i$, по одному из правил вывода, т.е.

$$\frac{s_{j_1}, s_{j_2}, \ldots, s_{j_k}}{s_i} \in R_{PC}$$

Множество $H$ называется множеством **предпосылок** или **предположений**, и если не указано, то будем считать, что $H = \emptyset$.

# 10 Формулы логики предикатов

**Определение**

Пусть $\sigma = (P, F, \mu)$ - некоторая сигнатура. Тогда **алфавит** логики предикатов (или логики первого порядка) сигнатуры $\sigma$ - это множество:

$$\mathcal{A}_{FOL}(\sigma) \rightleftharpoons \{\wedge, \vee, \rightarrow, \neg, (,)\top, \bot, \forall, \exists, =\} \cup P \cup F \cup \{x_i | i \in \omega\} \cup \{,\}$$

Здесь $V = \{x_i | i \in \omega\}$ - бесконечное множество **предметных** переменных.

**Определение**

Пусть $\sigma = (P, F)$ - сигнатура. Тогда **язык формул** $F(\sigma)$ сигнатуры $\sigma$ можно определить как множество слов алфавита $\mathcal{A}_{FOL}(\sigma)$ по индукции:

1. если $t_1, t_2 \in T(\sigma)$ - два терма, то $(t_1 = t_2) \in F(\sigma)$
2. если $p^n \in P$ - предикатный символ, $t_1, \ldots, t_n \in T(\sigma)$ - термы, то $p(t_1, \ldots, t_n) \in F(\sigma)$
3. если $\phi \in F(\sigma)$, то $\neg\phi \in F(\sigma)$
4. если $\phi, \psi \in F(\sigma)$, то $(\phi \bullet \psi) \in F(\sigma)$ для любого $\bullet \in \{\wedge, \vee, \rightarrow\}$
5. если $\phi \in F(\sigma)$, $x \in V$ - предметная переменная, то $Qx\phi \in F(\sigma)$, где $Q \in \{\forall, \exists\}$ - кванторы.

Слова из множества $F(\sigma)$ называются **формулами** сигнатуры $\sigma$.

Формулы, полученные по 1 и 2 называются **атомарными**.

# 11 Истинность формул логики предикатов

**Определение**

Пусть $\mathcal{M} = (M, \sigma)$ - структура сигнатуры $\sigma$, $\phi(\bar{x})$ - некоторая формула сигнатуры $\sigma$, $\gamma$ - означивание переменных $\bar{x}$ в структуре $\mathcal{M}$. Определим отношение **истинности** $\models$ формулы $\phi$ в структуре $\mathcal{M}$ при означивании $\gamma$:

- $\mathcal{M} \models (t_1 = t_2)[\gamma] \overset{def}{\Leftrightarrow} t_1^{\mathcal{M}}[\gamma] = t_2^{\mathcal{M}}[\gamma]$
- $\mathcal{M} \models p(t_1, \ldots, t_n)[\gamma] \overset{def}{\Leftrightarrow} (t_1^{\mathcal{M}}[\gamma], \ldots, t_n^{\mathcal{M}}[\gamma]) \in p^{\mathcal{M}}$
- $\mathcal{M} \models (\phi \wedge \psi)[\gamma] \overset{def}{\Leftrightarrow} (\mathcal{M} \models \phi[\gamma]) \wedge (\mathcal{M} \models \psi[\gamma])$
- $\mathcal{M} \models (\phi \vee \psi)[\gamma] \overset{def}{\Leftrightarrow} (\mathcal{M} \models \phi[\gamma]) \vee (\mathcal{M} \models \psi[\gamma])$
- $\mathcal{M} \models \neg\phi[\gamma] \overset{def}{\Leftrightarrow} \mathcal{M} \not\models \phi[\gamma] \Leftrightarrow \neg(\mathcal{M} \models \phi[\gamma])$
- $\mathcal{M} \models (\phi \to \psi)[\gamma] \overset{def}{\Leftrightarrow} (\mathcal{M} \models \phi[\gamma]) \to (\mathcal{M} \models \psi[\gamma])$
- $\mathcal{M} \models \forall x \phi[\gamma] \overset{def}{\Leftrightarrow} \forall a \in M \ (\mathcal{M} \models \phi[\gamma_a^x])$
- $\mathcal{M} \models \exists x \phi[\gamma] \overset{def}{\Leftrightarrow} \exists a \in M \ (\mathcal{M} \models \phi[\gamma_a^x])$

# 12 Линейное доказательство в логике предикатов

### Определение

**Линейное доказательство** (или **линейный вывод**) из множества секвенций $H$ в $\mathrm{PredC}_\sigma$ - это последовательность секвенций $(s_1, s_2, \ldots, s_n)$ такая, что каждая секвенция $s_i$:

- аксиома, т.е. $s_i \in A_{PredC}(\sigma)$
- предпосылка, т.е. $s_i \in H$
- получена из секвенций $s_{j_1}, s_{j_2}, \ldots, s_{j_k}$, где $j_1, j_2, \ldots, j_k < i$, по одному из правил вывода $\mathrm{PredC}_\sigma$, т.е.

$$\frac{s_{j_1}, s_{j_2}, \ldots, s_{j_k}}{s_i} \in R_{PredC}(\sigma)$$

Множество $H$ называется множеством **предпосылок** или **предположений**, и если не указано, то будем считать, что $H = \emptyset$.

# 13 Условие частичной корректности

### Проблема: формальная корректность

Дана программа $\pi$, и некоторое множество входных данных, соответствующее формуле $\phi$ (**предусловие**), будут ли выходные данные соответствовать формуле $\psi$ (**постусловие**)?

Отметим, что здесь мы *формализовали* технические требования к программе, используя *формулы* логики предикатов. В сокращённых обозначениях проблема корректности записывается как:

$$\{\phi\}\pi\{\psi\}$$

и называется **тройка Хоара** или **условие частичной корректности**.