1 Sets: finite, countable, uncountable. Characterization of finite sets

Определение

Множество A называется **конечным**, тогда и только тогда, когда оно равномощно некоторому натуральному числу n, число n называется его **мощностью**. Множество A называется **счётным**, тогда и только тогда, когда оно равномощно множеству натуральных чисел ω, ω - его мощность. Если множество не является ни конечным, ни счётным, оно называется **несчётным**. Два множества имеют одинаковую мощность, тогда и только тогда, когда они равномощны.

Примеры несчётных множеств

Множество $\mathcal{P}(\omega)$ несчётно по теореме Кантора, и его мощность называется **континуумом**. Множество всех действительных чисел $\mathbb{R}$ также несчётно, и равномощно $\mathcal{P}(\omega)$, следовательно, его мощность также равна континууму.

Теорема

Множество A конечно тогда и только тогда, когда любое из его подмножеств $B \subsetneq A$ не равномощно A: $B \not\approx A$.

Доказательство

Пусть A конечно, без ограничения общности можно предположить, что $A = n \in \omega$ и что существует биекция $f : n \to B$, где $B \subsetneq n$. Рассматривая $|B|$ вместо B можно предположить, что $B = m < n$ также является натуральным числом, и f сохраняет порядок на натуральных числах. Докажем теперь, что это невозможно индукцией по n. Если $n = 1$, то $m = 0$ - пустое множество, но оно должно содержать $f(0)$ - противоречие. Теперь шаг индукции: $n = \{0, 1, \ldots, n-1\} > 1$. Тогда введём ограничение f' для f на множестве $n-1 = \{0, 1, \ldots, n-2\}$. Это биекция $f' : n-1 \to m-1$. По предположению индукции это возможно только если $n-1 = m-1$, следовательно, $n = m$ - противоречие. Теперь возьмем A - множество, которое не равномощно ни одному из своих подмножеств.

Докажем, что существует такое n, что $A \preceq n$. Если такого n не существует, то для любого n, $n \preceq A$, т.е. существует $f_n : n \rightarrowtail A$. Выберем такие отображения, что если $n \leq m$, то $f_n \subseteq f_m$. Действительно, учитывая f_n, построим f_{n+1}, обладающее этим свойством. Отметим, что

$$cod(f_{n+1}) \nsubseteq cod(f_n)$$

потому что иначе $n + 1 \preceq n$, что неверно. Тогда существует некоторое $a \in cod(f_{n+1}) \backslash cod(f_n)$ Следовательно, $f'_{n+1} = f_n \cup \{(n, a)\}$ является инъективным. Рассматривая объединение $\bigcup\{f_n | n \in \omega\}$, получаем инъективное отображение ω в A, тогда существует подмножество $A' \subsetneq A$ такое, что $A' \approx A$

2 The sequential propositional calculus: linear proofs, deduction trees, characterization theorem about proofs

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 $H = \emptyset$.

Определение

Секвенция s называется **выводимой** (или **доказуемой**, **допустимой**) в исчислении высказываний из множества секвенций H, тогда и только тогда, когда существует линейное доказательство $(s_1, \ldots, s_n)$ из множества предпосылок H, такое, что $s = s_n$. Обозначается следующим образом:

$$H \rhd s$$

Если $H = \emptyset$, то можно писать просто $\rhd s$.

Определение

Формула ϕ называется **выводимой** (или **доказуемой**, **допустимой**) в исчислении высказываний, тогда и только тогда, когда секвенция $\vdash \phi$ может быть выведена из пустого множества предпосылок, т.е. $\rhd \vdash \phi$. Обозначается как $\rhd \phi$.

Определение

Теперь по индукции определим **дерево секвенций** T, его высоту $h(T)$, корень $r(T)$ и множество листьев $l(T)$.

- секвенция s является деревом, $h(s) = 0$, $r(T) = s$, $l(T) = \{s\}$
- если $T_1, \ldots, T_n$ - деревья, а s - секвенция, то

  $$T = \frac{T_1 \ \ldots \ T_n}{s}$$

  - является деревом:

  - высоты $h(T) = \max(\{h(T_i) | i \leq n\}) + 1$
  - с корнем $r(T) = s$
  - с листьями $l(T) = \cup \{l(T_i) | i \leq n\}$

переход в дереве секвенций T - 'это поддерево высоты 1, т.е. поддерево в T вида: $\frac{s_1 \ s_2 \ \ldots \ s_n}{s_0}$

Определение

Дерево секвенций T называется **деревом вывода** секвенции s из множества предпосылок H, тогда и только тогда, когда:

1. $r(T) = s$

2. все секвенции из множества листьев $l(T)$ являются аксиомами исчисления высказываний или элементами H, т.е. $l(T) \subseteq H \cup A_{PC}$

3. все переходы $\frac{s_1 \ s_2 \ \dots \ s_n}{s_0}$ из T являются Правилами вывода исчисления высказываний, т.е.

$$\frac{s_1 \ s_2 \ \dots \ s_n}{s_0} \in R_{PC}$$

Теорема

Для любого множества секвенций H и секвенции s,
$H \triangleright s \Leftrightarrow$ для s существует дерево вывода из предпосылок H.

Доказательство

$\Rightarrow$.
Пусть для s существует линейное доказательство $(s_1, \dots, s_n)$ из предпосылок H. Индукцией по n докажем, что для s существует дерево вывода. Основание индукции: если $n = 1$, то $s = s_1 \in H \cup A_{PC}$ - аксиома или предпосылка, тогда $T = s$ - дерево вывода для s. Шаг индукции. Предположим, что утверждение верно для всех $i < n$, т.е. для секвенций $s_1, \dots, s_{n-1}$ существуют деревья вывода $T_1, \dots, T_{n-1}$ с предпосылками H. По индукции линейного доказательства существуют такие $s_{j_1}, \dots s_{j_k}$, что $j_1, \dots, j_k < n$ и $\frac{s_{j_1} \ \dots \ s_{j_k}}{s_n}$ - правило вывода. Тогда

$$\frac{T_{j_1} \ \dots \ T_{j_k}}{s_n}$$

будет деревом вывода для s_n. Обратное включение. $\Leftarrow$.
Пусть существует дерево вывода T для s с предпосылками H. Индукцией по высоте T докажем, что для любого дерева вывода T с предпосылками H его корень линейно доказуем из H. Основание индукции: если $h(T) = 0$, то $T = s$, следовательно, $s \in H \cup A_{PC}$ - аксиома или предпосылка, тогда s очевидно доказуем из H. Шаг индукции. Предположим, что

утверждение верно для всех деревьев высоты $< n$, $T = \frac{T_1 \ \dots \ T_n}{S}$ - дерево вывода высоты n. Тогда $h(T_i) < n$ для всех $1 \leq i \leq n$, следовательно, все корни $r(T_i) = s_i$ линейно доказуемы из H. Пусть P_i - линейное доказательство s_i. Последний переход в дереве T выглядит следующим образом: $\frac{s_1 \ \dots \ s_n}{s}$ и происходит по какому-либо правилу вывода. Тогда секвенция $P = P_1 \,\hat{}\, P_2 \,\hat{}\, \dots \,\hat{}\, P_n \,\hat{}\, s$ будет линейным доказательством s с предпосылками H. $\square$

3 Unifiers, most general unifiers

Определение (унификатор)

Дано множество выражений E и подстановка θ, θ называется **унификатором** E тогда и только тогда, когда для любых $e_1, e_2 \in E$, $\theta(e_1) = \theta(e_2)$.

Унификатор может как существовать, так и нет. Кроме того, в абсолютном смысле он не единственен, потому что, комбинируя унификатор с заменой переменных, можно получить другой унификатор.

Определение

Даны две подстановки θ_1 и θ_2, Подстановка θ_1 называется **более общий** чем θ_2, тогда и только тогда, когда существует такая подстановка δ, что $\theta_2 \subseteq \theta_1 \circ \delta$. Это отношение обозначается как $\theta_1 \geq \theta_2$.

пример: $\{x_1/f(y_1), x_2/y_2\}$ более общая чем $\{x_1/f(g(z_1, z_2)), x_2/h(z_1)\}$, потому что

$$\{x_1/f(g(z_1, z_2)), x_2/h(z_1)\} \subseteq \{x_1/f(y_1), x_2/y_2\} \circ \{y_1/g(z_1, z_2), y_2/h(z_1)\}$$

Определение (наиболее общий унификатор)

Дано множество выражений E и подстановка θ, θ называется **наиболее общим унификатором** тогда и только тогда, когда

- θ является унификатором для E,
- для любого другого унификатора θ' выражения E верно, что $\theta \geq \theta'$, т.е. θ более общий чем θ'.

Отметим, что наиболее общий унификатор не единственен (если он существует), потому что унификатор, полученный в результате комбинации любого наиболее общего унификатора θ с заменой переменных, также является наиболее общим.

Алгоритм унификации

Существует эффективный алгоритм, вычисляющий некоторый наиболее общий унификатор для любого множества выражений E или определяющий, что наиболее общего унификатора для E не существует.