Раздел III

Частично упорядоченные множества. II

Разделы I

Разделы II

Разделы I

Разделы II

Разделы I

Разделы II

Разделы I

Разделы II

Разделы I

Разделы II

Принцип продолжения порядка

Теорема (Шпильрайн-Дашник-Миллер)

1. *Любой частичный порядок может быть продолжен до линейного на том же множестве.*
2. *Каждый порядок есть пересечение всех своих линейных продолжений.*

Доказательство (для конечного случая)

Пусть $\langle P, \sqsubseteq \rangle$ *— ч.у. множество и* P *— не цепь. Построим линейный порядок* $\leqslant$*, содержащий данный частичный.*

В P *найдутся несравнимые элементы* a *и* b*. Произвольно определим порядок на них: для определённости положим, например,* $a \leqslant b$*. Далее для всех* $x \sqsubseteq a$ *и* $b \sqsubseteq y$ *полагаем* $x \leqslant y$*. Если* $\langle P, \leqslant \rangle$ *ещё не цепь, то выберем новую пару несравнимых элементов и поступаем, как указано выше.*

Принцип продолжения порядка...

Доказательство (продолжение)

Через конечное число шагов получаем линейный порядок.

Поскольку возможен различный выбор пар несравнимых элементов a и b и при каждом выборе можно полагать как $a \leqslant b$, так и $b \leqslant a$, то действуя указанным образом можно получить различные возможные продолжения исходного частичного порядка $\sqsubseteq$ до линейного $\leqslant$.

Пересечение всех таких цепей даст исходное ч.у. множество. Действительно, если $x \sqsubseteq y$, то аналогичное следование будет и во всех полученных линейных порядках, а при несравнимых x и y всегда найдётся пара цепей с противоположным их следованием, что в пересечении цепей и даст несравнимость этих элементов.

Принцип продолжения порядка...

- Для счетно-бесконечного упорядоченного множества доказательство проводится методом математической индукции.
- В современной аксиоматической теории множеств принцип продолжения порядка играет роль, сопоставимую с AC.
- Поиск такого продолжения для конечных ч.у. множеств, заданных парами непосредственно следующих друг за другом вершин в теоретическом программировании называют *топологической сортировкой*.
  Термин крайне неудачен: указанная процедура не имеет никакого отношения ни к сортировке, ни к топологии (раздел математики, изучающий понятие непрерывности).
  Алгоритмы, решающие данную задачу за линейное время появились лишь в начале нашего века.

Принцип продолжения порядка: пример

Счётно-бесконечные ч.у. множества такие, что нижние конусы любых элементов конечны, называется *казуальными*.

Примеры: $\langle \mathbb{N}, \leqslant \rangle$, $\langle \mathbb{N}, \mid \rangle$.

Алгоритм последовательного построения $v_1 \lessdot v_2 \lessdot \ldots$ линейного расширения казуального множества P:

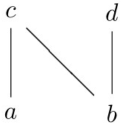
1. в произвольном порядке записываем минимальные элементы M_1 множества P,
2. удаляем из P множество M_1, получая множество P_1;
3. в произвольном порядке записываем минимальные элементы M_2 множества P_1
4. удаляем из P_1 множество M_2, получая множество P_2;
5. и т.д. (среди множеств M_1, M_2, $\ldots$ могут быть бесконечные).

Линейные продолжения ч.у. множеств

Линейный порядок $\leqslant$, включающий в себя данный частичный порядок $\sqsubseteq$ (т.е. $\sqsubseteq \subseteq \leqslant$) на некотором множестве называют *линеаризацией* или *линейным продолжением (расширением)* исходного порядка.

Известны эффективные алгоритмы построения всех линейных расширений конечного ч.у. множества.

Число скачков в некотором линейном расширении L ч.у. множества P, есть минимальное количество пар несравнимых элементов (скачков) P в L.



Например, в линеаризации $[b, d, a, c]$ зигзага N присутствует один скачок: пара (d, a).

Задача нахождения линейного расширения ч.у. множества с минимальным числом скачков NP-трудна.

Двудольные ч.у. множества

Ч.у. множества с диаграммами Хассе, являющимися двудольными графами называют *двудольными ч.у. множествами*. $K_{m,n}$ — обозначение для двудольного ч.у. множества с m максимальными и n минимальными элементам, у которого любой максимальный элемент содержит все минимальные.

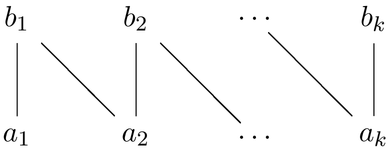
Ранее уже были указаны ч.у. множества, называемые заборами.

Обобщим это понятие: *заборами* или *зигзагами* будем называть двудольные ч.у. множества, состоящие из $n > 2$ элементов $\{v_1, \ldots, v_n\}$ с отношениями включения $v_{2i-1} \lessdot v_{2i}$ и $v_{2i} \gtrdot v_{2i+1}$ (последнее включение при чётном n и $i = n/2$ отсутствует) и двойственные им; символически $\mathbb{Z}_n$.

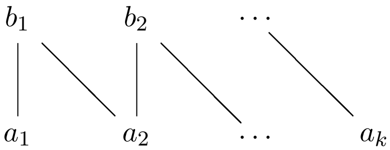
Обычно элементы нижней и верхней долей множества $\mathbb{Z}_n$ обозначают соответственно символами a и b с индексами.

Двудольные ч.у. множества: зигзаги Z_n

Зигзаги с чётным и нечётным числом элементов



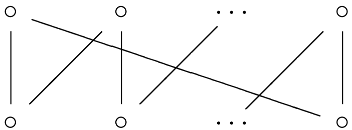
Z_{2k}



Z_{2k-1}

Двудольные ч.у. множества: малая корона s_n

Если в $2n$-элементном заборе при $n \geqslant 3$ добавить условие «последний элемент покрывает первый», то получим ч.у. множество, которое назовём *малой короной* s_n:



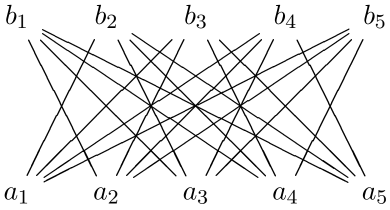
Понятно, что корона $\mathbf{s}_n$ изоморфна упорядоченной по включению совокупности всех
одноэлементных $\{v_1\}, \ldots, \{v_n\}$
и двухэлементных подмножеств вида
$\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_n, v_1\}$
n-элементного множества $\{v_1, \ldots, v_n\}$.

Двудольные ч.у. множеств: полная корона S_n, $n \geqslant 3$

Полная корона S_n — это $2n$-элементное двудольное ч.у. множество, т.е. $S_n = A \cup B$, где $A = \{\, a_1, \ldots, a_n \,\}$ — множество минимальных, а $B = \{\, b_1, \ldots, b_n \,\}$ — множество максимальных элементов.

Порядок $\sqsubseteq$ на S_n задаётся следующим образом: для элементов $a_i \in A$ и $b_i \in B$ полагают $a_i \sqsubseteq b_j$ для всех $i \neq j$, $i, j = 1, \ldots, n$ (и, естественно, $\sqsubseteq$ рефлексивен).

Пример: корона S_5:

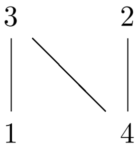


Множество Гёльдера

Пусть дано n-элементное ч.у. множество P.

- произвольным образом занумеруем элементы P первыми n натуральными числами;
- отождествим линейное расширение $\sigma : P \to \mathbf{n}$ ч.у. множества P с перестановкой $\left(\sigma^{-1}(1), \ldots, \sigma^{-1}(n)\right)$ множества $[n]$.

Пример: ч.у. множество и его линейное расширение



$(4, 2, 1, 3)$

Совокупность всех перестановок множества $[n]$, полученных таким образом, называется *множеством Гёльдера* ч.у. множества P.

Число линеаризаций ч.у. множества

Число $e(P) =$ всевозможных линеаризаций конечного ч.у. множества P, очевидно равно мощности множества Гёльдера для P (*проблема Рейни*).

$e(P)$ может интерпретироваться как некоторая оценка сложности P.

Понятно, что $e(n\mathbf{1}) = n!$, $e(C) = 1$ для цепи C и это максимально и минимально возможные значения $e(\cdot)$.

Легко показывается справедливость формул

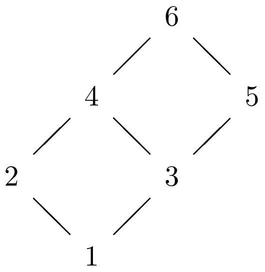
- $e(P \oplus Q) = e(P)\, e(Q)$;
- $e(P + Q) = \binom{n+m}{n}\, e(P)\, e(Q), \quad n = |P|,\ m = |Q|$.

Задача $e(P) = ?$ при $n > 5$ решена лишь для очень немногих типов ч.у. множеств.

Число линеаризаций ч.у. множества...

- $e(\mathbf{2} \times \mathbf{n}) = \dfrac{1}{n+1}\dbinom{2n}{n}$ — числа Каталана.

Пример. Ч.у. множество $\mathbf{2} \times \mathbf{3}$ и его 5-элементное множество Гёльдера ($e(\mathbf{2} \times \mathbf{3}) = \frac{1}{4}\binom{6}{3} = \frac{6\cdot5\cdot4}{4\cdot1\cdot2\cdot3} = 5$):



$$\{\,(1,2,3,4,5,6),\ (1,3,2,4,5,6),\ (1,2,3,5,4,6),\ (1,3,2,5,4,6),\ (1,3,5,2,4,6)\,\}$$

Число линеаризаций ч.у. множества...

- $\displaystyle\sum_{n\geqslant 0} \frac{e(Z_n)\,x^n}{n!} = \operatorname{tg} x + \sec x.$

  Значения $e(Z_n)$ при чётных n называют *числами секанса*, а при нечётных — *числами тангенса*:

$$\operatorname{tg} x = x + \frac{1}{3}x^3 + \frac{2}{15}x^5 + \ldots + \frac{2^{2n}(2^{2n}-1)B_n}{(2n)!}x^{2n-1} + \ldots,$$

$$\sec x = 1 + \frac{x^2}{2} + \frac{5}{24}x^4 + \frac{61}{720}x^6 + \ldots + \frac{E_n}{(2n)!}x^{2n} + \ldots,$$

  где B_n и E_n — числа Бернулли и Эйлера соответственно.
  Например, $e(Z_5) = \frac{2}{15} \cdot 5! = 16$.
  Значение $e(Z_n)$ было впервые установлено как мощность множества *up-down перестановок*: их образуют первые n натуральных чисел, переставленные так, что каждый элемент либо больше, ибо меньше обоих своих соседей.

Число линеаризаций ч.у. множества...

- Легко устанавливается, что $e(S_n) = (n+1)!(n-1)!$. Соотношение для $e(s_n)$ будет приведено далее.
- $$\frac{\log(e(B^n))}{2^n} = \log\binom{n}{\lfloor n/2 \rfloor} - \frac{3}{2}\log e + o(1).$$
- В общем случае: $\lim\limits_{m\to\infty} \frac{|\mathbf{m}^{\mathbf{P}}|}{m^n} = \frac{e(\mathbf{P})}{n!}$.
- Вычисление значения $e(P)$ — #P-полная задача. Один из методов определения $e(P)$ — вероятностный. Для ч.у. множества $\langle \{ v_1, \ldots, v_n \}, \sqsubseteq \rangle$ в n-мерном евклидовом пространстве определим многогранник $\mathcal{P}$: $\mathcal{P} = \{ (x_1, \ldots, x_n) \in \mathbb{R}^n \mid 0 \leqslant x_i \leqslant 1,\ v_i \sqsubseteq v_j \Rightarrow x_i \leqslant x_j \}$ Если $vol(\mathcal{P})$ — объём $\mathcal{P}$, то $e(P) = n! \cdot vol(\mathcal{P})$. Для оценок $vol(\mathcal{P})$ можно применить метод Монте-Карло.

Вероятностное пространство, связанное с ч.у. множеством

Дискретное вероятностное пространство на множестве всех линеаризаций ч.у. множества $\langle P, \sqsubseteq \rangle$: каждой $e(P)$ его линеаризаций приписывают равную вероятность.

В этом пространстве для элементов $x, y, z, \ldots$ данного ч.у. множества рассматривают события E вида $x \sqsubseteq y$, $(x \sqsubseteq y) \,\&\, (x \sqsubseteq z)$ и т.д. Вероятность такого события:

$$\Pr[E] = \frac{\text{\textit{число линеаризаций, в которых имеет место} } E}{e(P)}$$

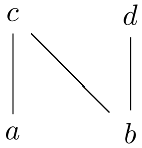
XYZ-теорема

Пусть $\langle P, \sqsubseteq \rangle$ — ч.у. множество и $x, y, z \in P$. Тогда

$$\Pr[x \sqsubseteq y] \cdot \Pr[x \sqsubseteq z] \leqslant \Pr[(x \sqsubseteq y) \,\&\, (x \sqsubseteq z)].$$

XYZ-теорема: пример

Ч.у. множество N



имеет пять линейных расширений:

$$[a, b, c, d],\ [a, b, d, c],\ [b, a, c, d],\ [b, a, d, c],\ [b, d, a, c],$$

откуда

$$\Pr[a \sqsubseteq b] = 2/5,\ \Pr[a \sqsubseteq d] = 4/5 \text{ и } \Pr[(a \sqsubseteq b)\&(a \sqsubseteq d)] = 2/5.$$

По XYZ-теореме: $8/25 \leqslant 2/5$.

Классическая проблема сортировки —

— состоит в определении некоторого линейного порядка L с помощью минимального количества вопросов «*верно ли, что $x < y$ в L?*».

Обобщение этой проблемы — задача восстановлении некоторой зафиксированной, но неизвестной линеаризации L ч.у. множества P с помощью минимального количества таких вопросов.

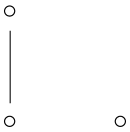
«1/3 – 2/3 предположение» (С.С. Кислицын, 1968)

Любое не являющееся цепью ч.у. множество содержит пару несравнимых элементов x и y, для которых

$$\frac{1}{3} \leqslant \Pr[x \sqsubset y] \leqslant \frac{2}{3}.$$

1/3 – 2/3 предположение...

Пример $\mathbf{2}+\mathbf{1}$ —



показывает, что указанные границы несужаемы.
Данное предположение до сих пор успешно противостоит всем попыткам его доказать и, *представляет собой одну из наиболее интригующих проблем комбинаторной теории ч.у. множеств*.

Наиболее сильный результат на сегодняшний день:

$$0,2764 \approx \frac{5-\sqrt{5}}{10} \leqslant \Pr[x \sqsubset y] \leqslant \frac{5+\sqrt{5}}{10} \approx 0,7236$$

для некоторых несравнимых элементов x и y из произвольного ч.у. множества.

Спектр ч.у. множества

Для ч.у. множества $\langle P, \sqsubseteq \rangle$ совокупность

$$\{ \Pr[a \sqsubseteq b] \mid a, b \in P,\ a \neq b \}$$

всех значений $\Pr[x < y]$ называют *спектром* P.

- Для всех неодноэлементных тривиально упорядоченных множеств спектр есть $\{ \frac{1}{2} \}$.
- $\Pr[a \sqsubseteq b] = 1 - \Pr[b \sqsubseteq a] \Rightarrow$ спектр симметричен относительно $\frac{1}{2}$.
- $\{ 0, \frac{1}{2}, 1 \}$ — единственный трёхэлементный спектр.
- Все четырёхэлементные спектры должны иметь вид $\{ 0, \alpha, 1 - \alpha, 1 \}$, где $0 < \alpha < \frac{1}{2}$.
  Для этого случая высказано недоказанное до сих пор предположение, что всегда $\alpha = \frac{1}{3}$ (E.B. Halvorsen, 2002).

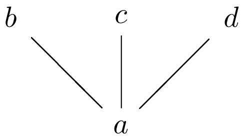
Разделы I

Разделы II

Реализация ч.у. множества

P совпадает с пересечением всех $e(P)$ своих линеаризаций, однако тот же результат можно получить, взяв значительно меньшее число линейных продолжений.

Например, ч.у. множество

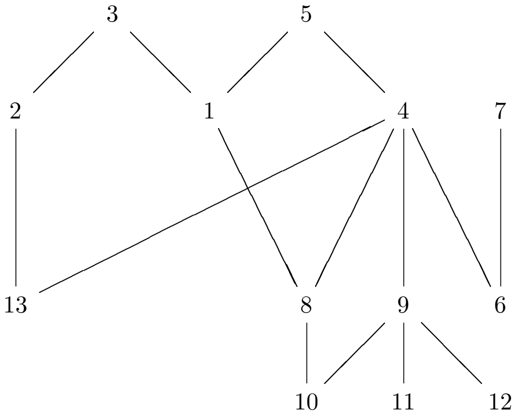


имеющее 6 линеаризаций, может быть представлено в виде пересечения 2 цепей: $[a, b, c, d]$ и $[a, d, c, b]$.

Если P — ч.у. множество и $\mathcal{R} = \{C_1, \ldots, C_k\}$ — совокупность цепей такая, что $P = C_1 \cap \ldots \cap C_k$, то говорят, что $\mathcal{R}$ *реализует* ч.у. множество P.

Реализация ч.у. множества: пример

Набор цепей $\mathcal{R} = \{\,[13, 2, 10, 8, 1, 3, 11, 12, 9, 6, 4, 5, 7],$
$[13, 6, 7, 12, 11, 10, 9, 8, 4, 1, 5, 2, 3],$
$[6, 7, 10, 11, 12, 8, 9, 1, 13, 2, 4, 3, 5]\,\}$ реализует ч.у. множество



Размерность ч.у. множества

Определение

Наименьшее число линейных порядков, дающих в пересечении данное ч.у. множество P называется его *(порядковой) размерностью* последнего и обозначается $\dim(P)$.

Для ч.у. множества P с предыдущего слайда $\dim(P) \leqslant 3$.

Теорема (Оре)

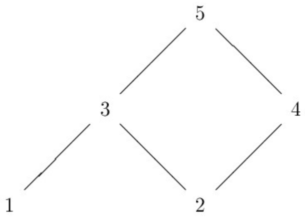
Порядковая и мультипликативная размерности ч.у. множества совпадают.

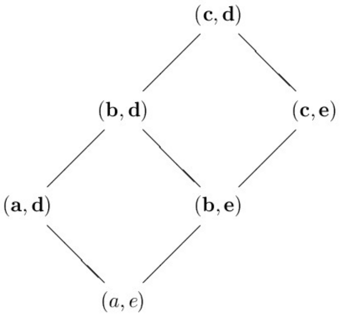
Приведённая теорема позволяет не различать указанные виды размерности и пользоваться единым символом $\dim(\cdot)$.

Размерность 1 имеют только цепи.

Размерность ч.у. множества: пример

Ч.у. множество P выделено жирным —





$$P \hookrightarrow [a, b, c] \times [d, e], \;\; P = [1, 2, 3, 4, 5] \cap [2, 4, 1, 3, 5].$$

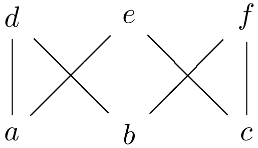
$\dim(\cdot)$ — более тонкая оценка сложности ч.у. множества, чем $e(\cdot)$; в некотором смысле $\dim(\cdot)$ играет ту же роль, что и хроматическое число для графов.

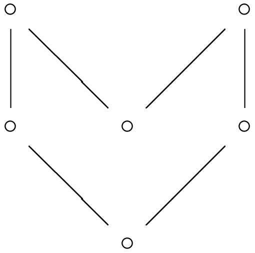
Размерности разных ч.у. множеств

- Размерность 2 имеют:
  - тривиально упорядоченные множества;
  - все отличных от цепей ч.у. множеств, имеющие не более 5 элементов;
  - зигзаги любой длины.

Размерности разных ч.у. множеств

- Размерность 2 имеют:
  - тривиально упорядоченные множества;
  - все отличных от цепей ч.у. множеств, имеющие не более 5 элементов;
  - зигзаги любой длины.
- Размерность 3 имеют 6-элементные ч.у. множества корона s_3, «шеврон» sh и $sh^\sharp$:



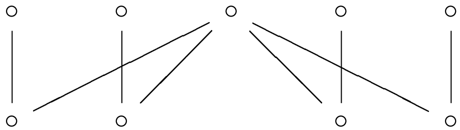


Стандартный пример ч.у. множества размерности n —

— полная корона S_n $(\dim(S_n) = n)$.

Стандартный пример показывает, что существуют ч.у. множества сколь угодно большой размерности.

Пример ч.у. множества размерности 3:



Задача распознавания свойства $\dim(P) \leqslant t$ полиномиальна при $t = 1, 2$ и является NP-полной при $3 \leqslant t$.

Показано существование границ для почти всех n-элементных ч.у. множеств P:

$$\frac{n}{4}\left(1 - \frac{c_1}{\log n}\right) \leqslant \dim(P) \leqslant \frac{n}{4}\left(1 - \frac{c_2}{\log n}\right),$$

где c_1 и c_2 — некоторые константы.

Для ч.у. множеств P и Q справедливо:

- $\varnothing \neq Q \subseteq P \Rightarrow \dim(Q) \leqslant \dim(P)$ и при удалении из ч.у. множества одного элемента его размерность уменьшается не более, чем на 1.
- $\dim(P+Q) = \max\{\dim(P), \dim(Q)\}$, если хотя бы одно из множеств не является цепью и $\dim(P+Q) = 2$, иначе.
- $\dim(P \times Q) \leqslant \dim(P) + \dim(Q)$, причём равенство достигается, например, когда и P, и Q — конечные неодноэлементные множества. В частности:
  - размерность декартова произведения n цепей (мы не считаем одноэлементные множества цепями) есть n; отсюда следует, что размерность n-мерного евклидова пространства $\mathbb{R}^n$, рассмотренного как декартово произведение линейных порядков $\mathbb{R}$ равна n;
  - $\dim(\mathbf{2}^n) = n$;
  - $\dim(S_n \times S_n) = 2n - 2$.

Для ч.у. множеств P и Q справедливо:...

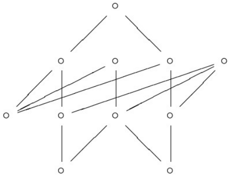
- $\dim(P) \leqslant \dfrac{|P|}{2}$ при $|P| \geqslant 4$ (*теорема Хирагучи*).
- $\dim(P) \leqslant |P - A|$, где A — антицепь в P такая, что $|P - A| \geqslant 2$.
  Таким образом, размерность двудольных ч.у. множеств не превышает мощности наименьшей доли, если обе доли не одноэлементны.
- $\dim(P) \leqslant w(P)$.

Ясно, что наличие у ч.у. множества короны S_n в качестве подмножества означает, что его размерность уже не менее n. Однако ч.у. множество большой размерности может и не содержать стандартного примера в качестве подмножества.
Например, размерность упорядоченной по включению совокупности одно- и двухэлементных подмножеств n-элементного множества неограниченно растёт при $n \to \infty$.

d-несводимые ч.у. множества

Ч.у. множество P называется *d-несводимым* для некоторого $d \geqslant 2$, если $\dim(P) = d$ и $\dim(P') < d$ для любого собственного ч.у. подмножества $P' < P$.

- Единственное 2-несводимое множество есть двухэлементная антицепь $\mathbf{1} + \mathbf{1}$.
- 3-несводимые ч.у. множества: s_3, sh, $sh^\sharp$, $\ldots$.
- Пример 4-несводимого ч.у. множества —
- Единственное $2t$-элементное t-несводимое множество — корона S_t



Общепринятая точка зрения:
3-несводимые множества редки, хорошо изучены и регулярны,
4-несводимые ч.у. множества достаточно часто встречаются и весьма причудливы.

Проблема Ногина —

Каково наибольшее значение $\pi(d, n)$ мощности множества максимальных элементов d-несводимых n-элементных ч.у. множеств при $d \geqslant 4$?

Данная проблема с 1990 г. остаётся открытой.

Утверждение

$$\pi(d, n) \leqslant n - d.$$

Доказательство

Пусть A *— максимальная антицепь в* d*-несводимом* n*-элементном ч.у. множестве* P.
Тогда $|A| = w(P)$ *и* $|P - A| \geqslant 2$.
Поэтому, $d = \dim(P) \leqslant n - w(P)$ *и* $w(P) \leqslant n - \dim(P)$.
Но, очевидно, $\pi(P) \leqslant w(P)$, *откуда* $\pi(P) \leqslant n - \dim(P)$.

Разделы I

Разделы II

Существование экстремальных элементов у бесконечного ч.у. множества

Лемма Куратовского-Цорна: если в ч.у. множестве все цепи имеют верхние грани, то любой его элемент содержится в некотором максимальном (*LKZ, или принцип максимальности*).

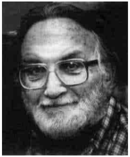
Принцип Хаусдорфа: всякая цепь ч.у. множества может быть вложена в некоторую максимальную цепь.

Оказалось, что приведённые утверждения эквивалентны — любое из них может быть выведено из другого.

Более того, они также эквивалентны приводимым далее фундаментальным теоретико-множественным аксиомам выбора и о полном упорядочении.

К. Куратовский, М. Цорн, Ф. Хаусдорф

Казимир Куратовский (Kazimierz Kuratowski, 1896–1980) — польский математик, тополог



Макс Август Цорн (Max August Zorn, 1906–1993) — американский математик немецкого происхождения, специалист в области теории групп и численного анализа

Феликс Хаусдорф (Felix Hausdorff, 1868–1942) — немецкий математик, один из основоположников современной топологии.

Аксиома выбора. Вполне упорядоченные ч.у. множества

Аксиома выбора (АС): существует отображение, сопоставляющее каждому непустому подмножеству B множества A элемент из B.

АС: для каждого множества $A \neq \varnothing$ найдётся такая функция f_A, что $f_A(B) \in B$ для любого $B \in \mathcal{P}^*(A)$ (= утверждается, что для любого всюду определённого соответствия можно построить вложенное в него функциональное).

Далее потребуются новое понятие.

Определение

Линейно упорядоченное множество называют *вполне упорядоченным* (в.у. множество), если каждое его непустое подмножество содержит наименьший элемент.

Вполне упорядоченные ч.у. множества

- Элементы вполне упорядоченного множества традиционно обозначают строчными греческими булавами $\alpha, \beta, \ldots$.
- Ясно, что вполне упорядоченное множество всегда содержит наименьший элемент.
- Во вполне упорядоченном множестве каждый элемент α,
    - если только он не является наибольшим, имеет единственный непосредственно следующий, обозначаемый $\alpha + 1$,
    - если только он не наименьший, может иметь не более одного непосредственно предшествующего; в этом случае, если α не имеет непосредственно предшествующего элемента, он называется *предельным*.

Вполне упорядоченные множества: примеры

1. Вполне упорядочены все конечные цепи, а так же цепь $\langle \mathbb{N}, \leqslant \rangle$. В этих ч.у. множествах нет предельных элементов.
2. Ч.у. множество $\langle \mathbb{Z}, \leqslant \rangle$ не является вполне упорядоченным, поскольку оно не имеет наименьшего элемента.
3. Множество
$$\left\{ 0, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \ldots, 1, 1+\frac{1}{2}, 1+\frac{2}{3}, \ldots, m, m+\frac{1}{2}, m+\frac{2}{3}, \ldots \right\}$$
с естественным порядком является вполне упорядоченным. Его предельные элементы суть натуральные числа.
4. Линейное расширение казуального множества $\langle \mathbb{N}, | \rangle$ по ранее рассмотренному алгоритму является вполне упорядоченным.

Принцип полного упорядочения

Теорема Цермело (принцип полного упорядочения): любое непустое множество можно вполне упорядочить.

Пример

Множество целых чисел $\mathbb{Z}$ можно вполне упорядочить считая, например, что $0 < 1 < -1 < 2 < -2 < 3 < -3 \ldots$ или

$$1 < 2 < \ldots < 0 < -1 < -2 < \ldots$$

Эрнст Церме́ло
(Ernst Friedrich Ferdinand Zermelo, 1871–1953) — немецкий математик, внёсший значительный вклад в теорию множеств и создание аксиоматических оснований математики

Где же истина?

Как из теоремы Цермело получить аксиому выбора

Пусть множество A непусто и по теореме Цермело его можно считать вполне упорядоченным. Тогда определено отображение, ставящее в соответствие каждому непустому подмножеству $B \subseteq A$ его элемент — наименьший в B.

Утверждения, эквивалентные приведённым: о равномощности множеств X и $X \times X$; о непустоте декартова произведения произвольной совокупности непустых множеств и др.

Таким образом, истинными или ложными все эти утверждения могут быть только одновременно.
Что же имеет место “в действительности”?

Ответ зависит от того, какими свойствами мы наделяем понятие множества в данной аксиоматике.

Об аксиоме выбора

AC (предложена Цермело при разработке *аксиоматической теории множеств*):

- для конечных множеств её справедливость очевидна, но при рассмотрении бесконечных совокупностей бесконечных множеств эта очевидность теряется;
- все попытки свести AC к другим фундаментальным принципам оказались безуспешными;
- AC является независимым от остальных аксиом теории множеств утверждением и добавление к ним как самой этой аксиомы, так и её отрицания порождает две равноправные непротиворечивые аксиоматики теории множеств;
- при практических, не связанных с вопросами оснований математики и теории множеств исследованиях, можно как принять аксиому выбора, так и отказаться от неё.

К чему ведёт принятие/отклонение AC

Отклонение аксиомы выбора — обеднение содержания конкретных математических теорий: не удаётся доказать —

- условия существования максимальных элементов ч.у. множеств;
- наличие базиса у произвольного векторного пространства;
- эквивалентности двух определений непрерывности функции в точке (на языке ε–δ и через пределы последовательностей);
- …

Принятие аксиомы выбора влечёт существование объектов с парадоксальными свойствами:

- неизмеримого по Лебегу множества действительных чисел;
- такого разбиения шара на четыре части, что из них движениями в пространстве оказывается возможным составить два таких же шара;
- …

Реакция на AC в начале XX в.

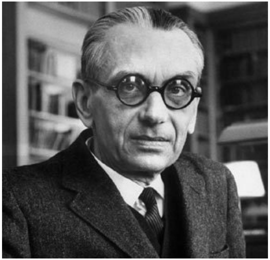
К. Гёдель показал:

- присоединение AC к системе аксиом теории множеств не увеличивает опасности впасть в противоречие (т.е. если в расширенной системе встретилось противоречие, то причина его в исходной системе, а не в AC);
- всякое свойство натуральных чисел, доказываемое с помощью аксиомы выбора, может быть доказано и без неё (т.е. в теории чисел AC можно рассматривать лишь как вспомогательное средство, нужное лишь для упрощения доказательств).

При конкретных математических исследованиях AC, как правило, принимают.

Доказательства, не использующие аксиому выбора (или эквивалентные ей утверждения) называют *эффективными*.

К. Гёдель



Курт Фридрих Гёдель (Kurt Friedrich Godel, 1906–1978) — выдающийся австрийский математик и логик XX века, автор ряда фундаментальных результатов в области математической логики, оснований математики и теории множеств. Сущность его революционных теорем о неполноте логических теорий некоторое время не понималась адекватно даже выдающимися учёными.

Умер он при явных признаках психического расстройства.

Из некролога газеты «Таймс»: *... его плодотворные идеи будут и далее стимулировать новые работы. Мало кто из математиков удостаивается такого рода бессмертия*.

Наивная теория множеств

В нашем курсе мы остаёмся в рамках *наивной теории множеств* с аксиомами (x, y, … — множества)

объёмности: $(x \subseteq y) \& (y \subseteq x) \supset (x = y)$;

свёртки: $y = \{ x \mid \varphi(x) \}$, $\varphi(x)$ — предикат.

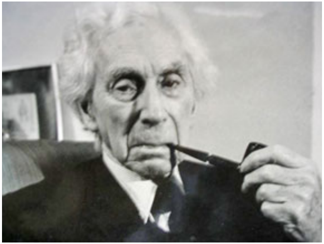
Неограниченное применение аксиомы свёртки может привести к противоречиям (*парадоксам*). Например:

Парадокс Рассела

Множество Рассела — $R = \{ x \mid x \notin x \}$, т.е. $z \in R \Leftrightarrow z \notin z$.
При подстановке $z \mapsto R$ получаем $R \in R \Leftrightarrow R \notin R$ — противоречие.

В современных аксиоматических теориях множеств ни R, ни подобные «экзотические» множества не могут быть построены.

Б. Рассел



Бертран Артур Уильям Рассел (Bertrand Arthur William Russell, 1872–1970) —
— выдающийся английский философ-неопозитивист, логик, социолог и литератор.
Автор (совместно А. Уайтхедом) фундаментальной трехтомной монографии «Principia mathematica» (1910–1913), наиболее полно выражающей концепцию *логицизма* в математике.
В мемориальном сборнике «Бертран Рассел — философ века» (1967) отмечалось, что вклад Рассела в математическую логику является наиболее значительным и фундаментальным со времен Аристотеля.

Лауреат Нобелевской премии по литературе.

Начальный отрезок в.у. множества

Если α — элемент в.у. множества, то интервал $[\,o,\,\alpha\,) \overset{\text{def}}{=} \alpha^{\triangledown} \setminus \{\alpha\}$ называют *начальным отрезком* α.

- Символ $[\,o,\,o\,)$ понимается как пустое множество.
- Предельный элемент α вполне упорядоченного множества $\langle\, C,\, \leqslant \rangle$ определяется условиями $\alpha \neq o$ и отсутствием в $[\,o,\,\alpha\,)$ наибольшего элемента.
- Следующий за предельным α элемент $\alpha + 1$ — наименьший во множестве $\alpha^{\vartriangle} \setminus \{\alpha\}$.

Свойства вполне упорядоченных множеств

Теорема

Пусть $\langle C, \leqslant \rangle$ — вполне упорядоченное множество. Тогда

1. *если и $C^\sharp$ вполне упорядочено, то C — конечная цепь;*
2. *если α — предельный элемент вполне упорядоченного множества, то*
$$[o, \alpha) = \bigcup_{\beta<\alpha} [o, \beta).$$

Доказательство

1. *Поскольку C и $C^\sharp$ вполне упорядочены, то C содержит o и ι, каждый её элемент, отличный от ι имеет последующий, а отличный от o — предшествующий. Следовательно в C отсутствуют предельные элементы, все сечения — скачки, что вместе с наличием o и ι означает конечность C.*

Свойства вполне упорядоченных множеств...

Доказательство (продолжение)

3. *Если* $\gamma \in [\, o,\, \alpha\,)$, *то поскольку между* γ *и* $\gamma + 1$ *элементов нет,* $\gamma + 1 \leqslant \alpha$. *Однако в силу предельности* α, *равенство невозможно.*
   Таким образом
   $$\gamma \in [\, o,\, \gamma + 1\,) \subseteq \bigcup_{\beta<\alpha} [\, o,\, \beta\,), \qquad \text{т.е.}$$
   $$[\, o,\, \alpha\,) \subseteq \bigcup_{\beta<\alpha} [\, o,\, \beta\,).$$
   Обратное включение очевидно.

Сравнение в.у. множеств и кардинальные числа

Теорема (о сравнении вполне упорядоченных множеств)

Пусть A и B — два вполне упорядоченных множества. Тогда имеется лишь одна из следующих возможностей:

1. $A \cong B$;
2. A *изоморфно некоторому начальному отрезку* B;
3. B *изоморфно некоторому начальному отрезку* A.

Факт равномощности множеств A и B обозначают $\overline{\overline{A}} = \overline{\overline{B}}$, а неравномощности — $\overline{\overline{A}} \neq \overline{\overline{B}}$.

Под $\overline{\overline{X}}$ понимается новый объект, связанный с множеством X, называемый *кардинальным числом* X или *кардиналом*.

Закон трихотомии

Теорема (о сравнении множеств — закон трихотомии)

Для любых множеств A и B имеется лишь одна из следующих возможностей:

1. $\overline{\overline{A}} = \overline{\overline{B}}$ (A *эквивалентно* B);
2. $\overline{\overline{A}} = \overline{\overline{B'}}$ *для некоторого* $B' \subseteq B$, *но* $\forall\, A' \subseteq A : \overline{\overline{A'}} \neq \overline{\overline{B}}$;
3. $\overline{\overline{B}} = \overline{\overline{A'}}$ *для некоторого* $A' \subseteq A$, *но* $\forall\, B' \subseteq B : \overline{\overline{B'}} \neq \overline{\overline{A}}$.

Доказательство

По аксиоме о полном упорядочении для A и B справедлива предыдущая теорема (о сравнении в.у.м.).
Тогда либо справедливы утверждения ❷–❸, либо выполняются условия теоремы Кантора-Шрёдера-Бернштейна (если каждое из множеств равномощно подмножеству другого, то множества равномощны), что влечёт выполнение условия ❶.

Закон трихотомии

— лежит в основе учения о мощности множеств, позволяя ввести порядок на множестве кардинальных чисел: считать, что $\overline{\overline{A}} < \overline{\overline{B}}$ и $\overline{\overline{A}} > \overline{\overline{B}}$ соответственно в случаях ❷ и ❸ теоремы.

Теорема (Кантор)

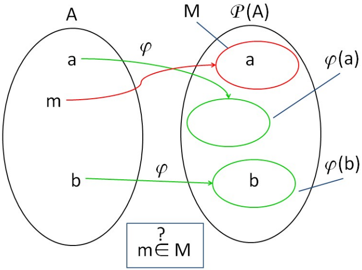
$$\overline{\overline{A}} < \overline{\overline{\mathcal{P}(A)}}.$$

Доказательство

Сопоставив каждому элементу $a \in A$ одноэлементное подмножество $\{a\}$ множества A, получим *вложение* *A в $\mathcal{P}(A)$, и поэтому $\overline{\overline{A}} \leqslant \overline{\overline{\mathcal{P}(A)}}$.*

Допустим теперь, что существует взаимно-однозначное отображение φ множества A в $\mathcal{P}(A)$.

Теорема Кантора...



Доказательство (продолжение)

Во множестве A *определим подмножество* M:

$$M = \{ a \in A \mid a \notin \varphi(a) \} \in \mathcal{P}(A).$$

По определению φ *должен существовать элемент* $m \in A$ *такой, что* $\varphi(m) = M$. *Но тогда получаем противоречие:*

$$m \in M \Rightarrow m \notin \varphi(m) = M \text{ и } m \notin M \Rightarrow m \in \varphi(m) = M.$$

Парадокс Кантора

Из теоремы Кантора сразу следует

Парадокс Кантора

Образуем *множество всех множеств*: $V = \{ x \mid x = x \}$.
Но тогда $\overline{\overline{\mathcal{P}(V)}} \leqslant \overline{\overline{V}}$ — противоречие.

Следовательно, множества всех множеств не существует (причина: не всякое свойство определяет множество, т.е. дело в аксиоме свёртки).

Показывается, что множество кардинальных чисел вполне упорядочено, откуда получают много важных и интересных следствий.

Принцип трансфинитной индукции

Теорема

Пусть C — вполне упорядоченное множество с каждым элементом α которого связано утверждение S_α, которые образуют совокупность S.
Тогда, если из справедливости S_β для всех $\beta \in [o, \alpha)$ следует справедливость S_α, то верны все утверждения из S.

Доказательство

Пусть среди S имеется неверное утверждение и тогда множество E неверных утверждений непусто.
Пусть α — наименьший элемент E, который всегда существует в силу полного порядка на C.
Но тогда, поскольку S_β справедливо для всех $\beta \in [o, \alpha)$, справедливо и S_α — противоречие.

Принцип трансфинитной индукции: применение

Лемма

Пусть $\langle A, \simeq \rangle$ *— пространство толерантности, а* $\langle C, \leqslant \rangle$ *— вполне упорядоченное множество, каждому элементу* α *которого сопоставлен предкласс толерантности* $E_\alpha \subseteq A$ *так, что из* $\alpha_1 < \alpha_2$ *следует* $E_{\alpha_1} \subseteq E_{\alpha_2}$. *Тогда объединение* $\bigcup E_\alpha = E$ *является предклассом толерантности в* A.

Лемма (о классах толерантности)

Для всякого предкласса существует содержащий его класс.

Доказательство

Базис индукции может быть начат с любого класса.

Трансфинитная индукция и LKZ — два альтернативных метода доказательств свойств ч.у. множеств.

Разделы I

Разделы II

8. Некоторые применения теории ч.у. множеств

Применение ч.у. множеств в математике

1. Использование частичных порядков в теории чисел, теории множеств и комбинаторике (теория разбиений и др.) уже были упомянуты.

2. Рассматривают АС, носители которых частично упорядочены.

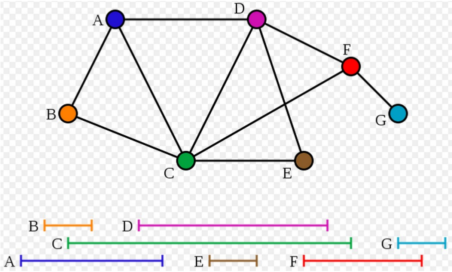
Наиболее исследованы частично упорядоченные группы, кольца и полугруппы (например, системы Туэ).

3. Для представления групп перестановок используют т.н. *PQ-деревья*, являющиеся расширением понятия ч.у. множества. Их применяют поиска перестановок, ограничения на которые становятся известны постепенно, одно за другим (воссоздание ДНК, проверка планарности графа и др.).

Интервальные графы

Планарный граф — граф, который может быть изображён на плоскости без пересечения ребер.

Интервальный граф — граф пересечений мультимножества интервалов на прямой, имеющий по одной вершине для каждого интервала в множестве и по ребру между каждой парой вершин, если соответствующие интервалы пересекаются:

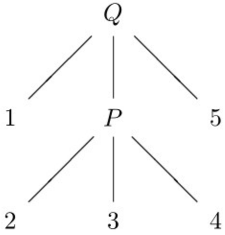


PQ-деревья

PQ-деревья — корневые планарные деревьями, висячие вершины в которых представляют переставляемые элементы, а остальные вершины имеют пометку либо P, либо Q.

Вершины с пометкой Q имеют по крайней мере 3 потомка и их порядок разрешается обращать, а вершины с пометкой P — по крайней мере 2 потомка и их разрешается как угодно переставлять.

Пример: группа перестановок последовательности $(1, 2, 3, 4, 5)$, содержащая, вместе с единичной, перестановку крайних и произвольную перестановку трёх внутренних элементов, описывается PQ-деревом —



Применение параллельно-последовательных ч.у. множеств.

- Параллельно-последовательные ч.у. множества используются в качестве модели событий во временных рядах.
- Параллельно-последовательные ч.у. множества применяют для оптимизации пропускной способности параллельной вычислительной системы при назначении задач для выполнения на том или ином процессоре.

Применение ч.у. множеств в исследовании операций

Важным разделом исследования операций является теория принятия решений при многих критериях.

Согласно принципу Эджворта-Парето наилучшие решения всегда следует выбирать в пределах множества Парето.

Пусть $y(x) = (y_1(x), \ldots, y_n(x)) \in \mathbb{R}^n$, $n \geqslant 2$ — набор критериев эффективности какого-либо решения x из множества допустимых альтернатив X, причём значение каждый из данных критериев желательно максимизировать.

В экономике решение $x^* \in X$ называется *оптимальным по Парето (парето-оптимальным)*, если не существует такого возможного решения $x \in X$, для которого $y_i(x^*) \leqslant y_i(x)$ для всех $i = 1, \ldots, n$.

Все парето-оптимальные решения образуют *множество Парето*, которое мы обозначим здесь Π, $\Pi \subseteq X$.

Применение ч.у. множеств в исследовании операций...

Нахождение множества Парето в простейшем случае, когда множество возможных векторов $Y = \{ y(x) \mid x \in X \}$ состоит из конечного числа N элементов, т.е. имеет вид $\{y^1, \ldots, y^m\}$ (мы опускаем указание на на зависимость y от x), сводится к их попарным сравнениям и исключением из Y и из дальнейшего сравнения векторов, заведомо не входящих в Π — со значениями всех координат, меньших, чем у другого (*доминируемых*).

Задача о выборе наилучшего проектного решения

Для участия в конкурсе представлено пять вариантов строительства предприятий различного типа (например, x^1 — машиностроительный завод, x^2 — текстильная фабрика, x^3 — молочный завод и т.п.) на территории, непосредственно прилегающей к жилому району.

Применение ч.у. множеств в исследовании операций...

Задача о выборе наилучшего проектного решения...

Оценивание качества проекта производится по четырем критериям:

- y_1 — стоимость реализации проекта,
- y_2 — величина прибыли проектируемого предприятия,
- y_3 — величина экологического ущерба от строительства,
- y_4 — заинтересованность жителей района в строительстве данного предприятия.

Пусть в результате экспертизы проектов были получены оценки всех критериев по пятибалльной шкале, которые представленны в нижеследующей таблице.

Применение ч.у. множеств в исследовании операций...

Задача о выборе наилучшего проектного решения...

	y_1	y_2	y_3	y_4
x^1	1	3	1	3
x^2	0	3	2	3
x^3	3	4	3	4
x^4	0	3	3	3
x^5	2	4	2	4

Поскольку 1 и 3-й критерии желательно минимизировать, а не максимизировать как остальные, то заменив в столбцах y_1 и y_3 таблицы значения z на $5-z$, произведём попарное сравнение полученных векторов.
В результате удаления доминируемых элементов, получим множество Парето $\Pi = \{x^1, x^2, x^5\}$, т.е. осуществлять окончательный выбор следует из 1, 2 и 5-го проектов.

Интуиционистское исчисление высказываний ИИВ: формулы

4. Применение ч.у. множеств в математической логике модели Крипке как общего способа установления истинности формул логических исчислений.

Зафиксируем множества

- $Var = \{x, y, \dots\}$ *логических переменных* — символов *атомарных высказываний*;
- $\Phi = \{\neg, \&, \vee, \supset\}$ — *логических связок*.

Определение

Формулой над множеством Φ логических связок называется либо некоторая логическая переменная (*атомарная формула*), либо одно из знакосочетаний вида $(\neg A)$, $(A \& B)$, $(A \vee B)$ или $(A \supset B)$ (*молекулярная формула*), где A и B — формулы.

$\mathcal{A}$ — множество всех логических формул.

ИВВ: экономия скобок и истинностные значения

Для сокращения записи формул принимают соглашения — правила экономии скобок и приоритета связок: внешние скобки у формул опускаются и сила связок убывает в порядке, указанном при их введении выше ($>$ — «сильнее»)

$$\neg > \& > \vee > \supset$$

Каждая логическая переменная может принимать, вообще говоря, счётное множество *истинностных значений* $\{\,\mathbf{0},\, 1,\, \ldots,\,\}$. Первое значение $\mathbf{0}$ назовём *выделенным*.

Неформально выделенное значение символизирует «истину» (**И**), а остальные — различные ситуации отсутствия истинности: неопределённость высказывания, различные формы его «ложности» (**Л**) и т.д. В классической логике множество истинностных значений сужается до двух: $\{$ **И**, **Л** $\}$ и выделенное — **И**.

ИИВ: аксиомы

Следующие формулы назовём *схемами аксиом* ИИВ:

1. $A \supset (B \supset A)$;
2. $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$;
3. $A \& B \supset A$;
4. $A \& B \supset B$;
5. $A \supset (B \supset (A \& B))$;
6. $A \supset A \vee B$;
7. $B \supset A \vee B$;
8. $(A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$;
9. $\neg A \supset (A \supset B)$;
10. $(A \supset B) \supset ((A \supset \neg B) \supset \neg A)$.

Аксиомы ИВВ получаются при подстановке в схемы конкретных формул вместо *метасимволов* A, B и C.

ИИВ: правило вывода и выводимые формулы

В ИИВ имеется единственное правило вывода, обозначаемое *MP* (лат. *modus ponens*, правило отделения), позволяющее из формул A и $A \supset B$ получить формулу B:

$$A,\ A \supset B \vdash B$$

Формула A называется ***выводимой***, если найдётся конечная последовательность формул $A_1, \ldots, A_l$ такая, что $A_l = A$ и каждый элемент последовательности

- либо является аксиомой,
- либо получен по правилу *MP* из каких-то двух предыдущих формул.

Выводимость формулы A записывается как $\vdash A$, в случае отсутствия вывода пишут $\nvdash A$.

ИИВ: пример вывода формулы

В качестве примера вывода покажем $\vdash x \vee y \supset y \vee x$.
Для удобства формулы вывода будем писать друг под другом, нумеруя их и давая краткие комментарии по их получению.

(1) $x \supset y \vee x$ — подстановка в схему 7

(2) $y \supset y \vee x$ — подстановка в аксиому 6

(3) $(x \supset y \vee x) \supset ((y \supset y \vee x) \supset (x \vee y \supset y \vee x))$ — подстановка в аксиому 8: $A \mapsto x$, $B \mapsto y$, $C \mapsto y \vee x$

(4) $(y \supset y \vee x) \supset (x \vee y \supset y \vee x)$ — по MP из (1) и (3)

(5) $x \vee y \supset y \vee x$ — по MP из (2) и (4)

Напоминание:

❻ $A \supset A \vee B$; ❼ $B \supset A \vee B$;

❽ $(A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$.

ИИВ: выводимость из множества формул

Пусть Γ — конечное множество формул.

Формула B называется *выводимой из множества формул* Γ (символически $\Gamma \vdash B$), если найдётся конечная последовательность формул $B_1, \ldots, B_l$ такая, что $B_l = B$ и каждый элемент этой последовательности

- либо является аксиомой,
- либо принадлежит Γ,
- либо получен по правилу MP из каких-то двух предыдущих формул.

Факт выводимости $\Gamma \vdash B$ не изменится, если вместо множества Γ взять одну формулу — конъюнкцию формул из Γ, так что можно рассматривать только одноэлементные множества Γ и опуская фигурные скобки, писать $A \vdash B$.

Знак $\vdash$ является символом отношения предпорядка на множестве $\mathcal{A}$.

Проблема выводимости —

— одна из важнейших проблем любого логического исчисления L: «выводима ли в L данная формула?».

$\vdash A$ — можно либо предъявить соответствующий вывод, либо доказать его существование;

$\nvdash A$ — возможно лишь дать доказательство несуществования вывода A.

Метатеория — теория, изучающая язык, структуру и свойства некоторой другой (*предметной*, или *объектной*) теории:

- корректность,
- непротиворечивость,
- различные виды полноты,
- проблема разрешимости,
- независимость систем аксиом и правил вывода,
- ...

Классическое исчисление высказываний КИВ: определение

Если к схемам аксиом добавить ещё одну:

11. $A \vee \neg A$ — логический закон *TND* (лат. *tertium non datur*, «третьего не дано»),

то получим *классическое исчисление высказываний КИВ*.

Тогда каждой логической переменной можно приписать одно из двух истинностных значений $\mathbf{1}$ или $\mathbf{0}$, понимаемых как «истина» и «ложь» соответственно, и по правилам

$$|\neg A| = \mathbf{1} \;\Leftrightarrow\; |A| = \mathbf{0};$$

$$|A \& B| = \mathbf{1} \;\Leftrightarrow\; |A| = |B| = \mathbf{1};$$

$$|A \vee B| = \mathbf{0} \;\Leftrightarrow\; |A| = |B| = \mathbf{0};$$

$$|A \supset B| = \mathbf{1} \;\Leftrightarrow\; |B| = \mathbf{1} \text{ или } |A| = \mathbf{0}.$$

получить оценку $|F| \in \{\mathbf{1}, \mathbf{0}\}$ любой формулы F.

КИВ: тавтологии

Формулы, истинные при любых *интерпретациях* — возможных вариантах приписываний логическим переменным значений ($\mathbf{1}$ или $\mathbf{0}$) — называются *тавтологиями*.

Примеры: все аксиомы 1–11, $\neg\neg x \supset x$, $\neg(x \vee y) \supset \neg x \& \neg y$, ...

В КИВ выводимыми оказываются все тавтологии и только они $\Rightarrow$ проблема выводимости сводится к проверке формулы на тавтологичность.

В ИИВ задача радикально усложняется: это исчисление не имеет конечнозначной интерпретации, т.е. если в любом конечном наборе $Tr = \{\mathbf{0}, 1, \ldots, k-1\}$ объявив значение $\mathbf{0}$ выделенным и задав правила оценки формул так, чтобы при всех интерпретациях переменным из Var значений из Tr все аксиомы всегда принимали бы только значение $\mathbf{0}$, найдётся такая формула F, что $|F| = \mathbf{0}$, но $\nvdash F$.

ИИВ: проблема разрешимости

- Любая выводимая в ИИВ формула выводима и в КИВ.
- Обратное неверно: например, формулы, получаемые из схемы TND и $\neg\neg x \supset x$, $\neg(x \vee y) \supset \neg x \& \neg y$, ... невыводимы в ИИВ.

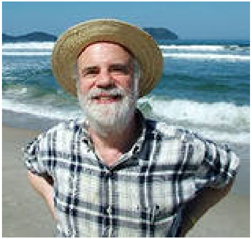
Для разрешения проблемы выводимости в ИИВ применим метод, основанный на построении *шкал Крипке*.

ИИВ: проблема разрешимости

- Любая выводимая в ИИВ формула выводима и в КИВ.
- Обратное неверно: например, формулы, получаемые из схемы TND и $\neg\neg x \supset x$, $\neg(x \vee y) \supset \neg x \& \neg y$, ... невыводимы в ИИВ.

Для разрешения проблемы выводимости в ИИВ применим метод, основанный на построении *шкал Крипке*.

Сол Крипке (Saul Aaron Kripke, 1940) — американский философ и логик, один из десяти выдающихся философов последних 200 лет.
Ещё юношей внёс значительный вклад в математическую логику, философию математики и теорию множеств.



Шкалы Крипке: построение

Чтобы задать такую шкалу нужно:

- указать ч.у. множество $\langle W, \leqslant \rangle$, элементы носителя которого называют *мирами*;
- для каждого мира указать, какие из логических переменных в нём являются истинными (остальные переменные в этом мире ложны).

Факт истинности переменной x в мире w записывают символически $w \Vdash x$, ложности — $w \nVdash x$.
При формировании шкалы Крипке требуется, чтобы

$$u \leqslant v,\, u \Vdash x \;\Rightarrow\; v \Vdash x$$

— т.е. говорят, что *область истинности переменной* ***наследуется вверх*** (*сохраняется в бóльших мирах*) — условие наследования истинности.

Шкалы Крипке: определение, интерпретация порядка

Неформально порядок $u \leqslant v$ между мирами интерпретируется как то, что мир v есть состояние мира u в следующий момент времени, понимая время не в физическом, а в логическом смысле: каждый мир описывается состоянием знаний в данный момент и однажды установленная истинность или доказанный факт остаётся таковым и впоследствии.

Логическое время не обязательно обладает линейным порядком.

Определение

Шкала Крипке есть тройка $\langle W, \leqslant, \Vdash \rangle$, где редукт $\langle W, \leqslant \rangle$ — ч.у. множество, а $\Vdash \subseteq W \times Var$ — соответствие «один ко многим», ставящее каждому миру совокупность истинных в нём логических переменных и удовлетворяющее условию наследования истинности.

Шкалы Крипке: истинность формулы в мирах

Для построенной шкалы Крипке определим истинность данной формулы A в любом мире w:

$w \Vdash A \& B \;\Leftrightarrow\; w \Vdash A$ и $w \Vdash B$;

$w \Vdash A \vee B \;\Leftrightarrow\; w \Vdash A$ или $w \Vdash B$;

$w \Vdash A \supset B \;\Leftrightarrow\; \forall (u \geqslant w)\; u \Vdash B$ или $u \nVdash A$;

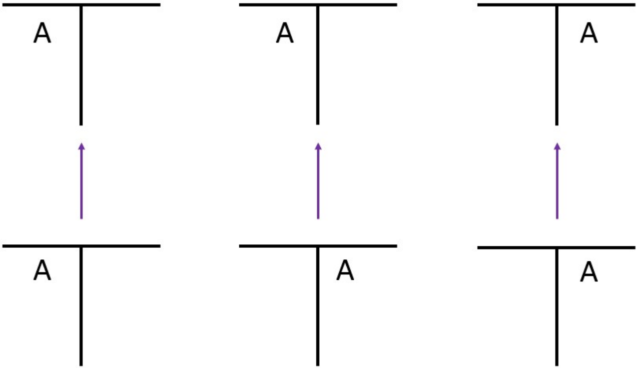
$w \Vdash \neg A \;\Leftrightarrow\; \forall (u \geqslant w)\; u \nVdash A$
(т.е. если $\Vdash \neg A$, то не существует большего мира, в котором бы $\Vdash A$).

Введённые шкалы Крипке задают *семантику* ИИВ, придавая смысл формулам — разделяя их на истинные и ложные в данном мире.

Шкалы Крипке: истинность формулы в мирах...

- Истинная в данном мире формула остаётся истинной и в старших (бóльших) мирах.
- Ложная в данном мире формула была ложной и во всех младших (меньших) мирах.
- Если формула содержит только связки $\&$ и $\vee$, то её истинность в данном мире не зависит от её истинности в других мирах.
- Истинности импликации и отрицания используют порядок на множестве миров.
- Следствием предыдущего является факт независимости импликации от других связок: в ИИВ, например, формулы $A \supset B$ и $\neg A \vee B$ логически не эквивалентны.

Шкалы Крипке: три варианта истинности формулы в шкале из двух связанных миров



Шкалы Крипке: теорема корректности

Теорема (корректности ИИВ относительно шкал Крипке)

Формула, выводимая в ИИВ, истина во всех мирах всех шкал Крипке.

Доказательство

Покажем, что (1) все аксиомы истины во всех мирах и (2) правило MP сохраняет истинность.

Второе очевидно: если и A, и $A \supset B$ истины во всех мирах, то B будет также истина во всех мирах.

Замечание: чтобы в мире w проверить оценку

- *истинность импликации $A \supset B$ надо удостовериться, что $w \Vdash A \Rightarrow w \Vdash B$ ($w \nVdash A$ эта импликация подавно истина);*
- *ложность импликации $A \supset B$ надо удостовериться, что $w \Vdash A \Rightarrow w \nVdash B$.*

Шкалы Крипке: теорема корректности...

Доказательство (Первое — истинность всех аксиом ИИВ)

Проверим 1-ю аксиому $A \supset (B \supset A)$.

Если в некотором мире u *имеет место* $u \Vdash A$, *то во всех мирах* $v \geqslant u$ *(в том числе и в* u*) справедливо* $v \Vdash B \supset A$.

Проверим 2-ю аксиому $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$.

Пусть существует мир u, *где она ложна* $\Rightarrow$ *в нём должны быть истины формулы* $A \supset (B \supset C)$, $A \supset B$ *и* A, *а* C *— ложна.*

Но из $u \Vdash A$ *и* $u \Vdash A \supset B$ *следует* $v \vDash B$ *во всех мирах* $v \geqslant u$.

При $u \vDash A \supset (B \supset C)$ *это означает справедливость* $w \vDash C$ *во всех мирах* $w \geqslant v$.

Отсюда следует справедливость $u \vDash C$ *— противоречие.*

Остальные аксиомы проверяются аналогично и ещё проще.

Шкалы Крипке: теорема корректности — важное ...

Следствие

Для доказательства невыводимости формулы в ИИВ достаточно указать шкалу Крипке, в одном из миров которой она ложна.

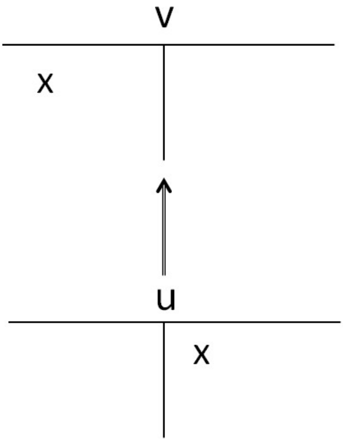
Такая шкала называется *контрмоделью* для данной формулы.

Существует контрмодель, являющаяся корневым деревом, в которой мир с ложной формулой — его корень.

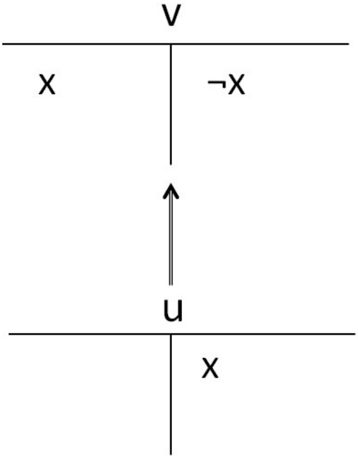
Пример

Постоим шкалу Крипке, содержащую мир, в котором формула $x \vee \neg x$ ложна.
Возьмём два мира u и v такие, что $u \leqslant v$, $u \nVdash x$ и $v \Vdash x$.
Тогда $v \nVdash \neg x$, откуда $u \nVdash \neg x$, что, в свою очередь даёт $u \nVdash x \vee \neg x$ (но $v \Vdash x \vee \neg x$).

Контрмодель для $u \nVdash x \vee \neg x$ (1)

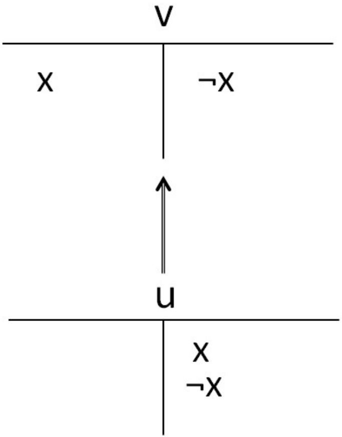


Контрмодель для $u \nVdash x \vee \neg x$ (2)

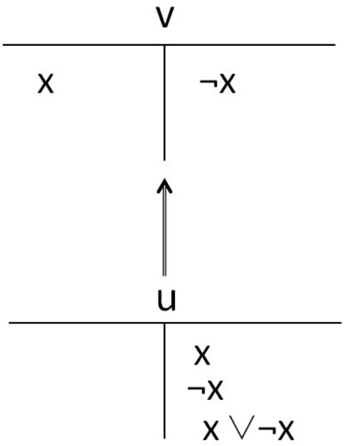


Не может быть $\Vdash \neg x$, т.к. тогда $\nVdash x$ — противоречие.

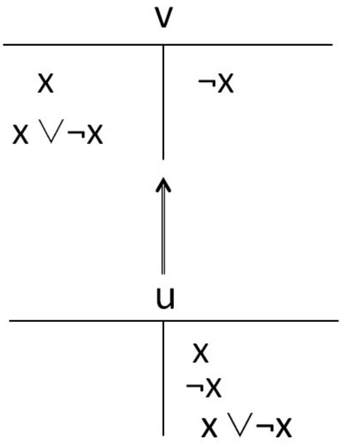
Визуализация контрмодели для $u \not\Vdash x \vee \neg x$ (3)



Контрмодель для $u \nVdash x \vee \neg x$ (4)



Контрмодель для $u \nVdash x \vee \neg x$ (5)



Шкалы Крипке: применение

- Метод автоматической верификации параллельных вычислительных систем (англ. *model checking*), позволяет проверить, удовлетворяет ли заданная модель системы формальным спецификациям. В качестве модели обычно используют шкалы Крипке, а для спецификации аппаратного и программного обеспечения — *темпоральную* (временную) логику.
- *Модальные логики* формализуют *сильные* и *слабые модальные* выражения вида «необходимо/возможно», «всегда/иногда», «здесь/где-то» и т.д. Заменив в определении шкалы Крипке частичный порядок на
  - отношение толерантности — получим семантику для брауэровой логики *B*;
  - аморфное отношение — семантику для логики *S5*;
  - диагональное — модель для модальной логики *M*.