Часть IV

Частично упорядоченные множества

Разделы

Частично упорядоченные множества: определение и примеры

Определение

Пару $\mathbf{P} = \langle P, \leqslant \rangle$, где P — непустое множество, а $\leqslant$ — рефлексивное, антисимметричное и транзитивное бинарное отношение на нём, называют *частично упорядоченным множеством* (сокращённо *ч.у. множеством*, англ. *poset*).

Рефлексивность (R): $x \leqslant x$;
Антисимметричность (AS): $(x \leqslant y) \,\&\, (y \leqslant x) \;\Rightarrow\; x = y$;
Транзитивность (T): $(x \leqslant y) \,\&\, (y \leqslant z) \;\Rightarrow\; x \leqslant z$.

Примеры

- $\langle \mathcal{P}(M), \subseteq \rangle$ — классический пример ч.у. множества (упорядочивание множеств *по включению*, $M \neq \varnothing$);
- $\langle \mathbb{N}, \leqslant \rangle$ и $\langle \mathbb{N}, \mid \rangle$ — два упорядочивания одного множества.

Предпорядки

Вопрос

Пусть M — множество людей, $h(x)$ — рост, а $w(x)$ — вес человека x.
Определим на отношение ρ на M:

$$x\rho y \Rightarrow (h(x) \leqslant h(y)) \mathbin{\&} (w(x) \leqslant w(y)).$$

Является ли ρ отношением частичного порядка на M?

Ответ. Нет. ρ — рефлексивно и транзитивно, но не является антисимметричным отношением: $x\rho y \mathbin{\&} y\rho x \not\Rightarrow x = y$ (могут найтись два человека с одинаковыми ростом и весом).

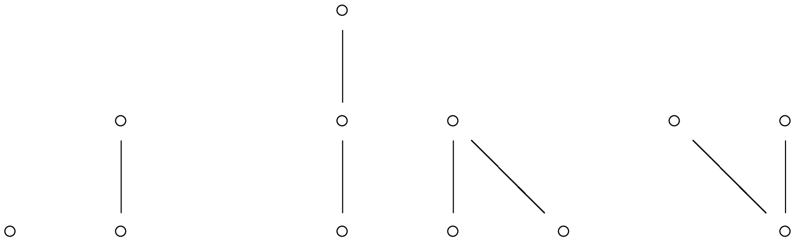
Отношения со свойствами (R) и (T) называют *предпорядками*.

Понятное обозначение: $a < b \stackrel{\text{def}}{=} (a \leqslant b)\&(a \neq b)$

Ч.у. множество $\mathbf{P} = \langle P, \leqslant \rangle$ — основные понятия:

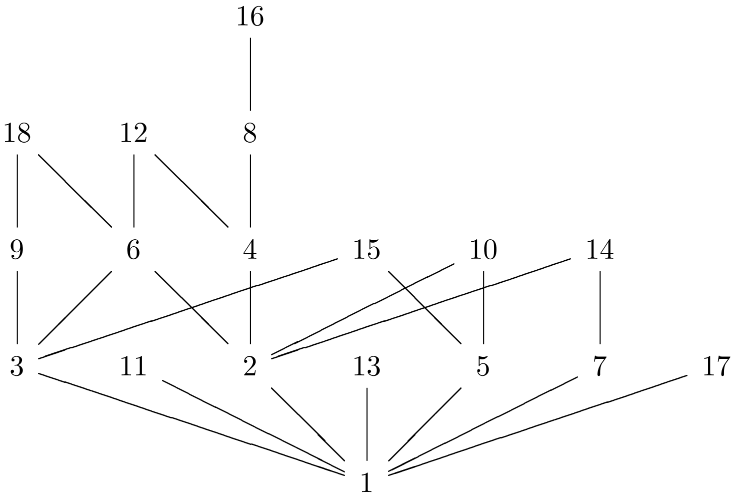
- если $(x \leqslant y) \vee (y \leqslant x)$, то x и y *сравнимы* $(x \sim y)$, иначе они *несравнимы* $(x \nsim y)$;
- *полный (линейный) порядок*, если $\forall\, x, y : x \sim y$;
- если в $\mathbf{P}$ нет ни одной пары различных сравнимых элементов, то это тривиально упорядоченное множество;
- x *непосредственно предшествует* y (y *непосредственно следует за* x), $x \lessdot y$, если $x \leqslant z \leqslant y \Rightarrow (z = x) \vee (z = y)$;
- $\{\, x \in P \mid a \leqslant x \leqslant b \,\}$ — *интервал* $[\, a, b \,]$;
- $v_1 < \ldots < v_n \stackrel{\text{def}}{=} [v_1, \ldots, v_n]$ — *цепь* $\mathbf{n}$, а совокупность попарно несравнимых элементов — *антицепь* в $\mathbf{P}$;
- цепь *максимальная* (*насыщенная*), если при добавлении к ней любого элемента она перестаёт быть цепью;
- $\geqslant$ — двойственный к $\leqslant$ порядок: $\leqslant^d \stackrel{\text{def}}{=} \geqslant$.

Диаграммы Хассе



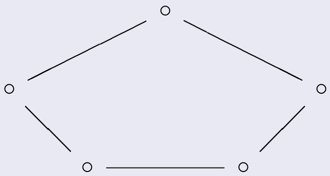
Диаграммы Хассе четырёх нетривиальных непомеченных трёхэлементных ч.у. множеств.

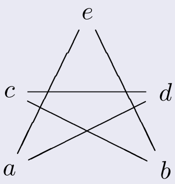
Диаграмма Хассе ч.у. множества $\langle \{1, \ldots, 18\}, | \rangle$



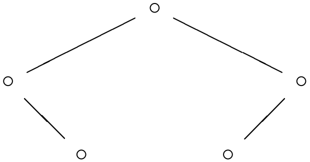
Диаграммы Хассе: да или нет

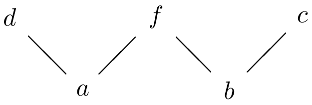
Вопрос: это диаграммы Хассе?





Ответ. Нет! Правильно:





Диаграммы всех 4-элементных ч.у. множеств

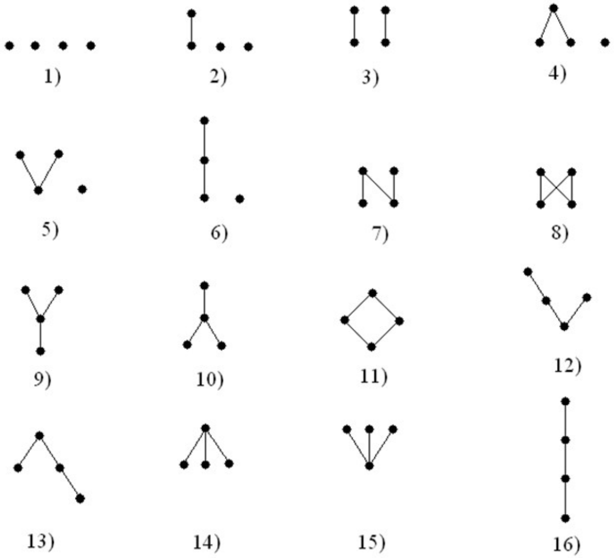
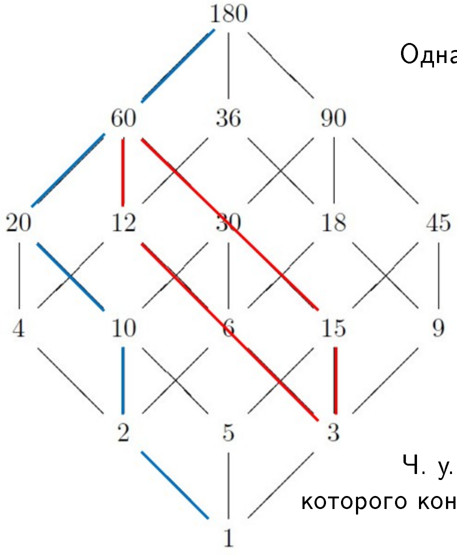


Диаграмма $D(180)$ всех делителей числа $180 = 2^2 3^2 5$



Одна из максимальных цепей и интервал $[3,\, 60]$.

Ч. у. множество, все интервалы которого конечны — *локально конечное*

Задача

Построить диаграмму Хассе всех подполей поля $GF\left(2^{18}\right)$, упорядоченных по включению.

Решение. $\mathbb{F}_p^n \subseteq \mathbb{F}_p^k \Leftrightarrow k \mid n$. Все делители числа $18 = 2 \cdot 3^2$: $D(18) = \{1, 2, 3, 6, 9, 18\}$.

$$
\begin{tikzcd}[arrows=dash]
 & & GF\left(2^{18}\right) \arrow[dl] \arrow[dr] & \\
 & GF\left(2^{6}\right) \arrow[dl] \arrow[dr] & & GF\left(2^{9}\right) \arrow[dl] \\
GF\left(2^{2}\right) \arrow[dr] & & GF\left(2^{3}\right) \arrow[dl] & \\
 & GF(2) & &
\end{tikzcd}
$$

Ч.у. множества: особые элементы

Определение

Элемент $u \in P$ ч.у. множества $\langle P, \leqslant \rangle$ называют:

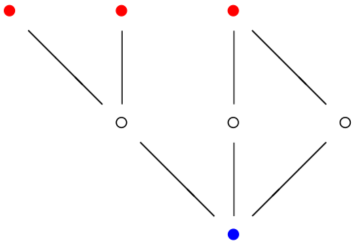
- *максимальным*, если $u \leqslant x \Rightarrow u = x$,
- *минимальным*, если $u \geqslant x \Rightarrow u = x$,
- *наибольшим*, если $x \leqslant u$,
- *наименьшим*, если $x \geqslant u$

для любых $x \in P$.

Элемент

- наибольший, если все другие элементы содержатся в нём;
- максимальный, если нет элементов, содержащих его (аналогично для наименьшего и минимального элементов).

Особые элементы ч.у. множества: пример

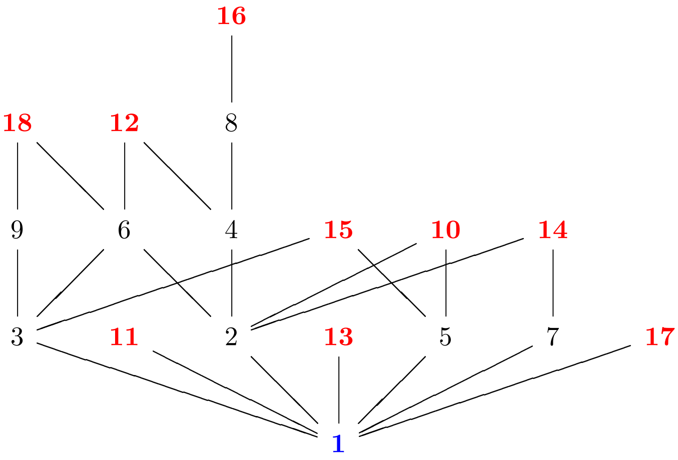


- ● — максимальные элементы;
- ● — минимальный и наименьший элемент;

Наибольший (1) и наименьший (0) — *граничные элементы*.

В конечном ч.у. множестве имеется как минимум по одному максимальному и минимальному элементу.

Ч.у. множество $\langle \{1, \ldots, 18\}, | \rangle$



1 — наименьший элемент, ● — максимальные.

Ранжированные ч.у. множества

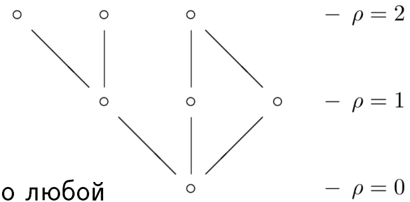
Цепное условие Жордана-Дедекинда

Все максимальные цепи между любыми двумя сравнимыми элементами элементами локально конечного ч.у. множества имеют одинаковую длину.

Если ч.у. множество удовлетворяет условию Жордана-Дедекинда и имеет наименьший элемент 0, то оно *ранжируемо*, т.е. на нём можно определить *функцию ранга* ρ:

1. $\rho(0) = 0$;
2. $a \lessdot b \Rightarrow \rho(b) = \rho(a) + 1$

и такое множество имеет *слои*.



Если множество ранжируемо, то любой его слой (но не только!) является антицепью.

Порядковые гомоморфизмы

Определение

Отображение $\varphi\colon P \to P'$ носителей ч.у. множеств называется соответственно

- *изотонным* (*монотонным*, *порядковым гомоморфизмом*), если $x \leqslant y \;\Rightarrow\; \varphi(x) \leqslant \varphi(y)$;
- *обратно изотонным*, если $\varphi(x) \leqslant \varphi(y) \;\Rightarrow\; x \leqslant y$;
- *антиизотонным*, если $x \leqslant y \;\Rightarrow\; \varphi(x) \geqslant \varphi(y)$.

Если φ изотонно, обратно изотонно и инъективно, то это *вложение* или *(порядковый) мономорфизм* ($P \overset{\varphi}{\hookrightarrow} P'$).
Сюръективный мономорфизм — *(порядковый) изоморфизм* ($P \cong P'$ или $P \overset{\varphi}{\cong} P'$).
Изоморфизм ч.у. множества в себя — *(порядковый) автоморфизм*.

Идеалы и фильтры ч.у. множеств

Определение

Подмножество J элементов ч.у. множества $\langle P, \leqslant \rangle$ называется его *(порядковым) идеалом*, если

$$(x \in J) \,\&\, (y \leqslant x) \;\Rightarrow\; y \in J.$$

Подмножество F элементов P называется его *(порядковым) фильтром*, если

$$(x \in F) \,\&\, (x \leqslant y) \;\Rightarrow\; y \in F.$$

$\varnothing$ и всё ч.у. множество P — *несобственные* порядковые идеалы.

Важное свойство: объединение и пересечение порядковых идеалов есть порядковый идеал.

Обозначение: $J(P)$ — множество всех порядковых идеалов ч.у. множества P.

Конусы

Определение

Пусть $\langle P, \leqslant \rangle$ — ч.у. множество и $A \subseteq P$. Множества $A^{\vartriangle}$ и $A^{\triangledown}$

$A^{\vartriangle} = \{x \in P \mid \underset{A}{\forall a}\,(a \leqslant x)\}$ и $A^{\triangledown} = \{x \in P \mid \underset{A}{\forall a}\,(x \leqslant a)\}$

называются верхним и нижним *конусами* множества A, а их элементы — верхними и нижними *гранями* множества A соответственно.

Для одноэлементного множества $A = \{a\}$ — $a^{\vartriangle}$ и $a^{\triangledown}$.

Понятно, что если $a \leqslant b$, то $a^{\vartriangle} \cap b^{\triangledown} = [a, b]$.

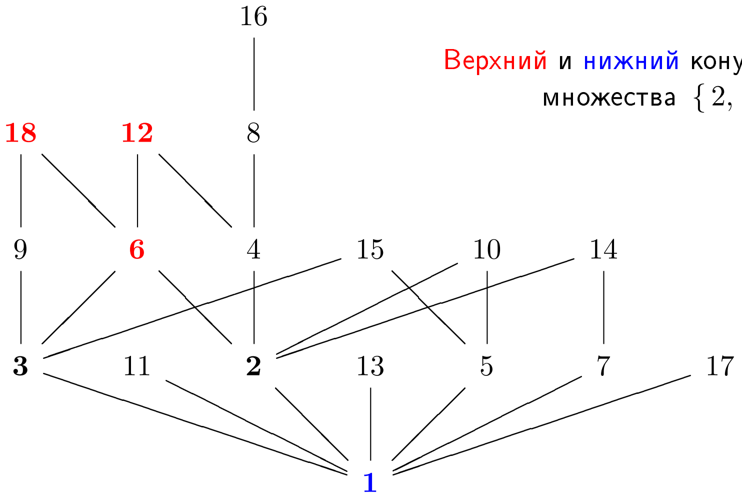
$x^{\triangledown} = \langle x \rangle = J(x)$ — идеал, а $x^{\vartriangle}$ — фильтр P;

такие идеалы и фильтры называют *главными*.

Конечнопорождённый идеал:

$$\langle a_1, \ldots, a_k \rangle \overset{\text{def}}{=} \bigcup_{i=1}^{k} {a_i}^{\triangledown},\ a_i \nsim a_j,\ i \neq j.$$

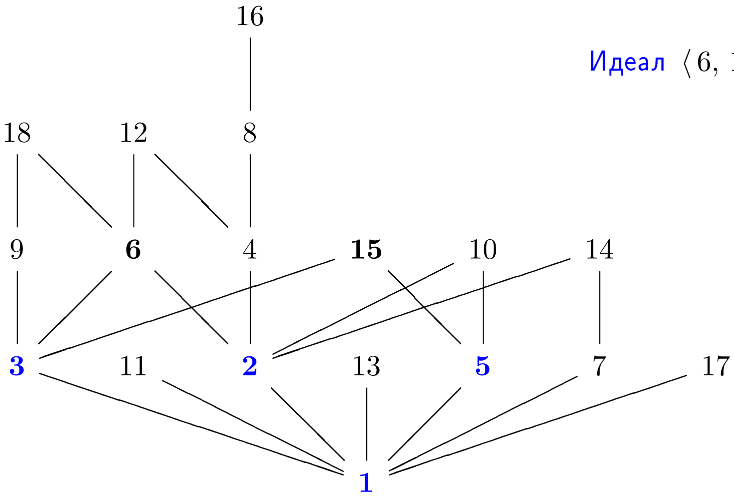
Конусы: пример



Верхний и нижний конусы множества $\{2, 3\}$

Идеалы: пример

Идеал $\langle 6, 15 \rangle$



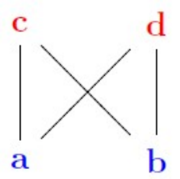
Точные грани

Определение

Пусть $\langle P, \leqslant \rangle$ — ч.у. множество и $A \subseteq P$.

- Наименьший элемент в $A^{\triangle}$ называется *точной верхней гранью множества* A (символически $\sup A$).
- Наибольший элемент в $A^{\triangledown}$ называется *точной нижней гранью множества* A (символически $\inf A$).

Пример ($\sup A$ и/или $\inf A$ могут и не существовать)

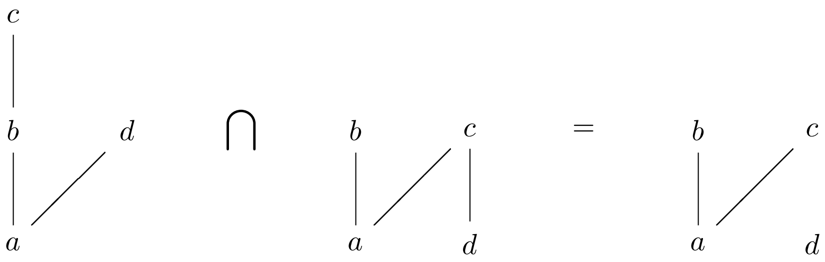


$\{a, b\}^{\triangle} = \{c, d\}$, но множество $\{c, d\}$ не имеет инфимума $\Rightarrow$ $\sup\{a, b\}$ отсутствует. Аналогично, отсутствует $\inf\{c, d\}$.

Разделы

Пересечение

$$\underline{\langle\, P,\, \leqslant_1 \rangle \cap \langle\, P,\, \leqslant_2 \rangle \;=\; \langle\, P,\, \leqslant_1 \cap \leqslant_2 \rangle}.$$



Свойства ч.у. множеств могут не сохраняются при пересечении. Например, «быть цепью»: если P — цепь, тогда P^d — также цепь, а $P \cap P^d$ — тривиально упорядоченное множество.

Прямая сумма

$\mathbf{P} = \langle\, P,\, \leqslant_P \,\rangle$ и $\mathbf{Q} = \langle\, Q,\, \leqslant_Q \,\rangle$ — два ч.у. множества, причём $P \cap Q = \varnothing$.

$$\underline{\mathbf{P} + \mathbf{Q} \;=\; \langle\, P \cup Q,\, \leqslant_P \vee \leqslant_Q \,\rangle.}$$

Справедливы соотношения

$$P + Q \;\cong\; P + R \;\Rightarrow\; Q \;\cong\; R \quad \text{и} \quad (P + Q)^d \;\cong\; P^d + R^d\,.$$

$n\mathbf{P}$ — прямая сумма n экземпляров $\mathbf{P}$,
$n\mathbf{1}$ — n-элементная антицепь.

Диаграмма прямой суммы состоит из двух диаграмм соответствующих ч.у. множеств, рассматриваемых как единая диаграмма.
Ч.у. множество, не являющееся прямой суммой некоторых двух других ч.у. множеств, называется *связным*.

Прямое произведение: определение

Прямым или *декартовым произведением* ч.у. множеств $\mathbf{P} = \langle P, \leqslant_P \rangle$ и $\mathbf{Q} = \langle Q, \leqslant_Q \rangle$ называется множество

$$\mathbf{P} \times \mathbf{Q} = \langle P \times Q, \leqslant \rangle,$$

где $(p, q) \leqslant (p', q') \Leftrightarrow (p \leqslant_P p')\&(q \leqslant_Q q')$.

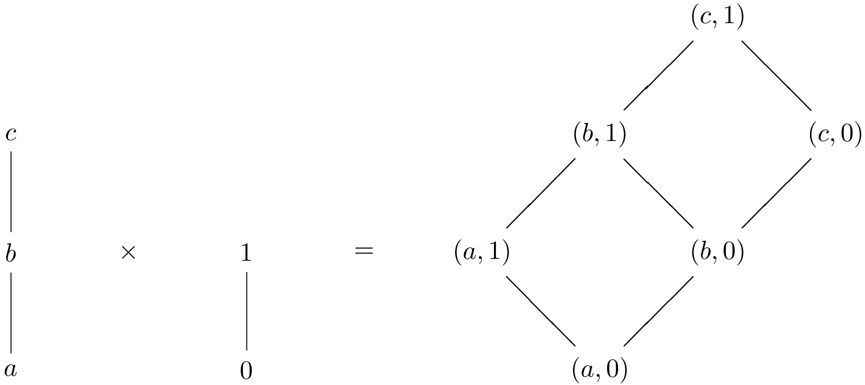
$\mathbf{P}^n$ — прямое произведение n экземпляров $\mathbf{P}$: $B^n = \mathbf{2}^n$.

Если P, Q ранжированы и их ранговые функции суть ρ_P и ρ_Q, то $P \times Q$ также ранжировано и $\rho(x_1, x_2) = \rho_P(x_1) + \rho_Q(x_2)$;

Справедливы соотношения $P \times Q \cong Q \times P$

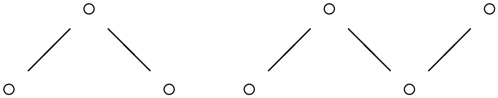
$$P \times R \cong Q \times R \Rightarrow P \cong Q, \quad P^n \cong Q^n \Rightarrow P \cong Q.$$

Прямое произведение: пример 1

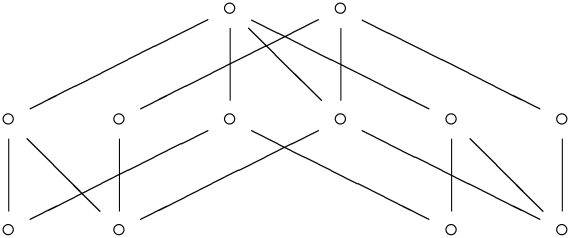


Прямое произведение цепей **3** и **2**

Прямое произведение: пример 2



Зигзаги (или заборы) $\mathbf{Z}_3$ и $\mathbf{Z}_4$



Прямое произведение $\mathbf{Z}_3 \times \mathbf{Z}_4$

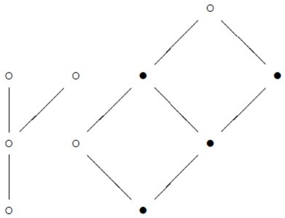
Теорема Оре

Теорема

Каждый частичный порядок изоморфен некоторому подмножеству декартова произведения цепей.

Определение

Мультипликативной размерностью ч.у. множества $\mathbf{P}$ называется наименьшее число k линейных порядков $\mathbf{L}_i$ таких, существует вложение $\mathbf{P} \hookrightarrow \mathbf{L}_1 \times \ldots \times \mathbf{L}_k$.



Разделы

Принцип продолжения порядка

Теорема (Шпильрайна)

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

$$\mathbf{P} \to \mathbf{L}, \qquad \mathbf{P} = \mathbf{L}_1 \cap \ldots \cap \mathbf{L}_{e(\mathbf{P})},$$

где $e(\mathbf{P})$ — число всех линеаризаций ч.у. множества $\mathbf{P}$.

Доказательство (для конечного случая, $|P| = n$)

1. *Если $\mathbf{P}$ — не цепь, то в P найдутся несравнимые элементы; произвольно определим порядок на них и продолжим его по транзитивности. Если получившиеся ч.у. множество ещё не цепь, то выберем новую пару несравнимых элементов и поступаем, как указано выше.*

   Через конечное число шагов получаем линейный порядок.

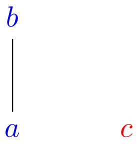
Принцип продолжения порядка...

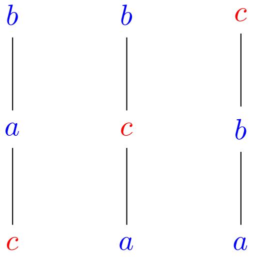
Доказательство (продолжение)

1. *Т.к. возможен различный выбор пар несравнимых элементов и при каждом выборе можно полагать любой их порядок, то можно получить все возможные линейные продолжения исходного частичного порядка.*
2. *Пересечение всех таких цепей даст исходное ч.у. множество: если $x \leqslant y$, то аналогичное следование будет и во всех полученных линейных порядках, а при $x \nsim y$ всегда найдётся пара цепей с противоположным их следованием, что в пересечении цепей и даст несравнимость этих элементов.*

Для конечных ч.у. множеств заданных парами вида $a \lessdot b$, поиск такого линейного продолжения в теоретическом программировании называют *топологической сортировкой*. Задача решается за линейное время.

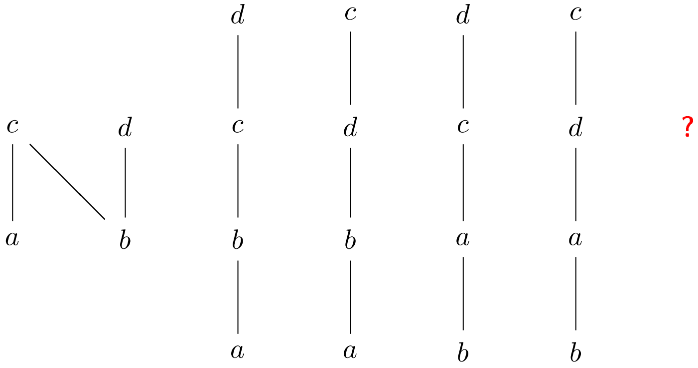
Линейные продолжения ч.у. множеств: примеры...





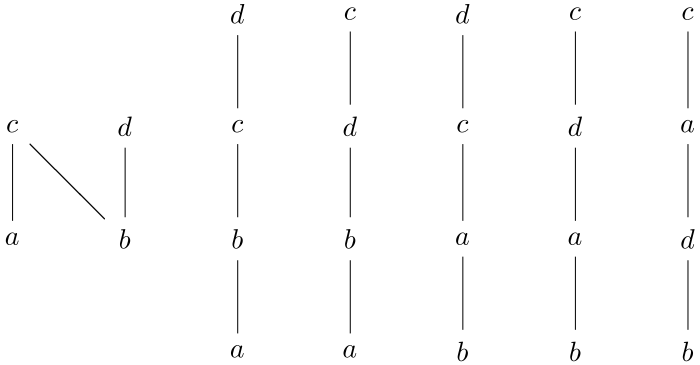
$\mathbf{P}$ $\qquad$ $e(\mathbf{P}) = 3$

Линейные продолжения ч.у. множеств: примеры...



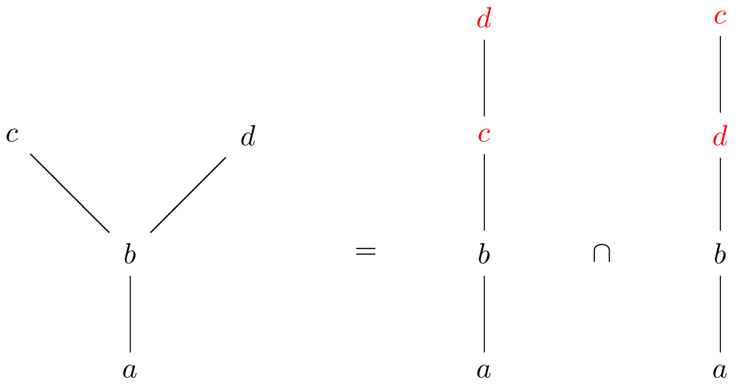
$\mathbf{P}$ $\qquad$ $e(\mathbf{P}) = 5$

Линейные продолжения ч.у. множеств: примеры...

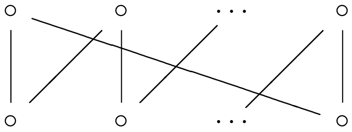


$\mathbf{P}$ $e(\mathbf{P}) = 5$

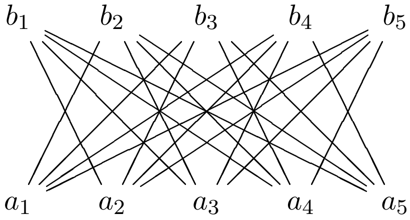
Представление ч.у. множества пересечением цепей



Некоторые ч.у. множества



Малая корона $\mathbf{s}_n$



Корона $\mathbf{S}_5$

«$e(\mathbf{P}) = ?$» — NP-полная задача, но:

- $e(\mathbf{P}+\mathbf{Q}) = \binom{n+m}{n} e(\mathbf{P})e(\mathbf{Q}), \quad n = |\mathbf{P}|,\ m = |\mathbf{Q}|$;
- $e(\mathbf{2}\times\mathbf{n}) = \frac{1}{n+1}\binom{2n}{n}$ — *числа Каталана*;
- $$\sum_{n\geqslant 0} \frac{e(\mathbf{Z}_n)\, x^n}{n!} = \operatorname{tg} x + \sec x\,,$$
  значения $\mathbf{Z}_n$ при чётных n — *числа секанса*, а при нечётных — *числа тангенса*;
- $e(\mathbf{S}_n) = (n+1)!(n-1)!\,$;
- $$\sum_{n\geqslant 1} \frac{e(\mathbf{s}_n)}{n!}\, x^n = \frac{x}{\cos^2 x}\,;$$
- $$\frac{\log(e(B^n))}{2^n} = \log\binom{n}{\lfloor n/2\rfloor} - \frac{3}{2}\log e + o(1)\,.$$

Вероятностное пространство на линеарезациях

При дискретных задач часто рассматривают связанное с ч.у. множеством P *вероятностное пространство* на множестве всех $e(P)$ его линеаризаций, в котором каждая линеаризация *равновероятна*.

В этом пространстве для элементов x, y, z, ... ч.у. множества P рассматривают события E вида $x \leqslant y$, $(x \leqslant y) \,\&\, (x \leqslant z)$ и т.д.

Вероятность $\Pr[E]$ такого события:

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

Теорема (XYZ-теорема)

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

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

Проблема сортировки и «1/3 – 2/3 предположение»

— определить линейный порядк $\mathbf{L}$ с помощью минимального количества вопросов «*верно ли, что $x < y$ в $\mathbf{L}$?*».

Обобщение: $\mathbf{L}$ — зафиксированная, но неизвестная линеаризация ч.у. множества $\mathbf{P}$.

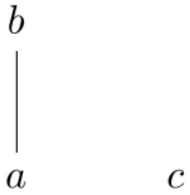
Оптимальная процедура поиска $\mathbf{L}$ включает в себя нахождение элементов x и y, для которых $\Pr[x < y] \approx \frac{1}{2}$.

С.С. Кислицын (1968) высказал «*1/3 – 2/3 предположение*»: "*любое не являющееся цепью ч.у. множество содержит пару несравнимых элементов x и y, для которых*

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

Позднее это утверждение независимо выдвинули американские исследователи М. Фредман и Н. Линал.

1/3 – 2/3 предположение



Пример $\mathbf{2}+\mathbf{1}$ показывает, что указанные границы несужаемы (имеется и пример десятиэлементного ч.у. множества со связанной диаграммой Хассе).

Данное предположение до сих пор успешно противостоит всем попыткам его доказать и *представляет собой одну из наиболее интригующих проблем комбинаторной теории ч.у. множеств* (С. Фелснер и У.Т. Троттер).

На сегодняшний день наиболее сильный результат:

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

Ч.у. множества: спектр

Определение:

$$\underline{Spec\,(\mathbf{P}) \;=\; \{\, \Pr[\, a \leqslant b\,] \mid a, b \in P \,\}}$$

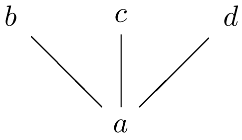
Ясно, что

- поскольку $\Pr[\, a \leqslant b\,] \;=\; 1 - \Pr[\, b \leqslant a\,]$, спектр симметричен относительно $\frac{1}{2}$;
- для всех неодноэлементных тривиально упорядоченных множеств $Spec = \{\, \frac{1}{2} \,\}$;
- $\{\, 0,\ \frac{1}{2},\ 1 \,\}$ — единственный трёхэлементный спектр;
- все четырёхэлементные спектры должны иметь вид $\{\, 0,\ \alpha,\ 1-\alpha,\ 1 \,\}$, где $0 < \alpha < \frac{1}{2}$;
  Гипотеза (2002): $\alpha \;=\; \frac{1}{3}$.

Ч.у. множества: размерность

По теореме Шпильрайна ч.у. множество $\mathbf{P}$ совпадает с пересечением всех $e(\mathbf{P})$ своих линеаризаций, но тот же результат можно получить, взяв значительно меньшее число линейных продолжений.

Например, ч.у. множество $\mathbf{P}$



имеет 6 линеаризаций, но $\mathbf{P} = [a, b, c, d] \cap [a, d, c, b]$.

Пусть $\mathbf{P}$ — ч.у. множество и $\mathcal{R} = \{\mathbf{L}_1, \ldots, \mathbf{L}_k\}$ — совокупность цепей такая, что $\mathbf{P} = \mathbf{L}_1 \cap \ldots \cap \mathbf{L}_k$, то говорят, что $\mathcal{R}$ *реализует* $\mathbf{P}$.

Ч.у. множества: размерность...

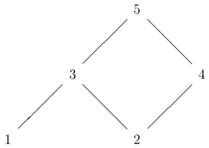
Определение

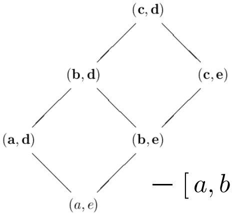
Наименьшее число линейных порядков, дающих в пересечении данное ч.у. множество $\mathbf{P}$ называется его *(порядковой) размерностью* (символически $\dim(P)$).

Теорема (Оре)

Порядковая и мультипликативная размерности ч.у. множества совпадают.

$[1, 2, 3, 4, 5] \cap [2, 4, 1, 3, 5]$:





$— [a, b, c] \times [d, e]$

$\dim(\mathbf{P})$ — более тонкая оценка ч.у. множества, чем $e(\mathbf{P})$

Размерность ... имеют:

1 — только цепи;

2 — тривиально упорядоченные множества

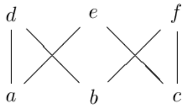
(т.е. размерность не может интерпретироваться как мера отличия данного ч.у. множества от линейного);

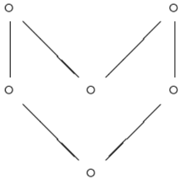
— $\mathbf{Z}_n$;

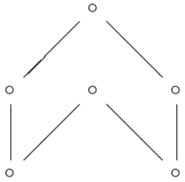
— все отличные от цепей ч.у. множеств, при $|P| \leqslant 6$, кроме

3 — s_3, $\mathbf{sh}$ и $\mathbf{sh}^d$ (см. диаграммы) :

n — $\mathbf{S}_n$







О размерности ч.у. множества $\mathbf{P} = \langle P, \leqslant \rangle$

- $\varnothing \neq Q \subseteq P \Rightarrow \dim(\mathbf{Q}) \leqslant \dim(\mathbf{P})$, при удалении 1-го элемента его размерность уменьшается не более, чем на 1;
- $\dim(\mathbf{P}+\mathbf{Q}) = \max\left\{ \dim(\mathbf{P}), \dim(\mathbf{Q}) \right\}$, если хотя бы одно из множеств не является цепью и $\dim(\mathbf{P}+\mathbf{Q}) = 2$;
- $\dim(\mathbf{P}\times\mathbf{Q}) \leqslant \dim(\mathbf{P}) + \dim(\mathbf{Q})$;
- $\dim(\mathbf{P}) \leqslant |\mathbf{P}|/2$ при $|\mathbf{P}| \geqslant 4$ (теорема Хирагучи).

Теорема («компактности»)

Пусть $\mathbf{P}$ *— такое ч.у. множество, что любое его конечное ч.у. подмножество имеет размерность, не превосходящую* d*.*
Тогда $\dim(\mathbf{P}) \leqslant d$*.*

$$wp1: \quad \frac{n}{4}\left(1-\frac{c_1}{\log n}\right) \leqslant \dim(\mathbf{P}) \leqslant \frac{n}{4}\left(1-\frac{c_2}{\log n}\right), \quad n = |\mathbf{P}|.$$

d-несводимые ч.у. множества

Определение

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

... несводимые множества:

2 — двухэлементная антицепь (единственное);

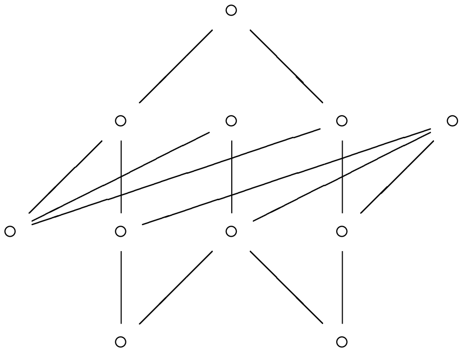
3 — $\mathrm{s}_3, \mathbf{sh}, \mathbf{sh}^d + \ldots$ — описаны, регулярны и хорошо изучены;

4 — достаточно часто встречаются и весьма причудливы;

t — $\mathbf{S}_t$ (единственное $2t$-элементное) $+ \ldots$;

- каждое t-несводимое ч.у. множество является ч.у. подмножеством некоторого $(t+1)$-несводимого.

4-несводимое ч.у. множество



Проблема Ногина

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

Данная проблема до сих пор остаётся открытой.

Утверждение

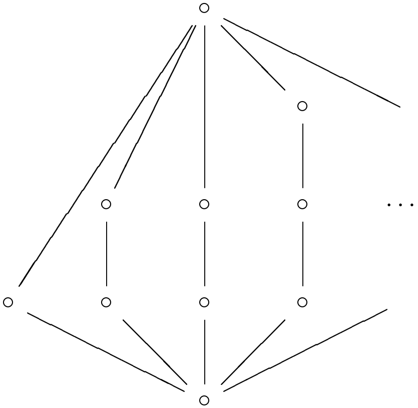
$$\pi(d, n) \leqslant n - d\,.$$

Разделы

Вопрос ЧУМ-1: Есть ли разница между утверждениями

Ч.у. множество содержит (а) бесконечную цепь и (б) цепь, длина которой больше наперёд заданного числа"?

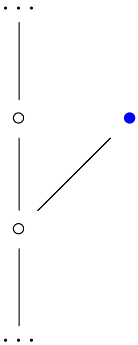
Ответ:



Задача ЧУМ-2

Приведите пример ч.у.м., имеющего в точности один максимальный элемент и не имеющего наибольшего.

Решение.



Задача ЧУМ-3

В ч.у. множестве $\langle \mathbb{N}, | \rangle$ *для подмножества* $A = \{12, 18\}$ *найти*

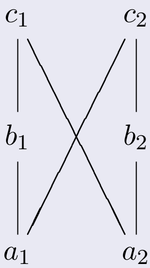
1. $A^{\triangle}$;
2. $A^{\triangledown}$;
3. $\sup A$;
4. $\inf A$.

Решение.

1. $A^{\triangle} = \{ 36n \mid n = 1, 2, \ldots \}$;
2. $A^{\triangledown} = \{ 1, 2, 3, 6 \}$;
3. $\sup A = \text{НОК}\,(12, 18) = 36$;
4. $\inf A = \text{НОД}\,(12, 18) = 6$.

Задача ЧУМ-4

Разложить в пересечение минимального количества цепей ч.у. множество $\mathbf{P}$



Решение.

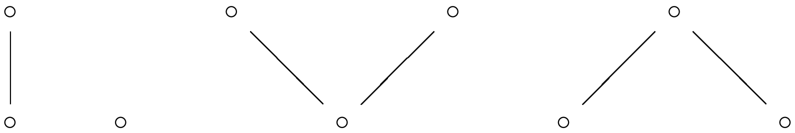
$$\mathbf{P} = [\,a_1,\, b_1,\, a_2,\, c_1,\, b_2,\, c_2\,] \cap [\,a_2,\, b_2,\, a_1,\, c_2,\, b_1,\, c_1\,]\,.$$

Задача ЧУМ-5

1. *Сколько существует частичных порядков на множестве* $\{a, b, c\}$*?*
2. *Сколько среди них неизоморфных?*
3. *Сколько среди них линейных порядков?*

Задача ЧУМ-5...

Решение. Неизоморфных трёхэлементных порядков 5: тривиальный, $\mathbf{3}$ и



Они порождают порядки на $\{\,a,\,b,\,c\,\}$:

тривиальный	— 1,
цепь $\mathbf{3}$	— 6,
$\mathbf{2}+\mathbf{1}$	— 6,
$\mathbf{Z}_3$ и двойственный к нему	— по 3
Всего	— 19

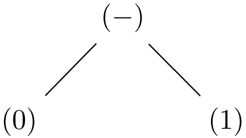
Задача ЧУМ-6

Постройте ч.у. множества $I(1)$ и $I(2)$ всех интервалов булевых единичных кубов размерностей 1 и 2.

Решение.

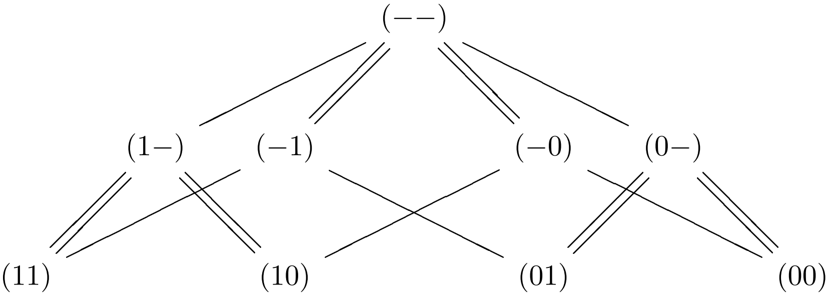
Булев единичный кубов размерности n содержит 3^n различных интервалов, при этом имеется $C_n^k 2^k$ интервалов размерности k, $k = 0,\ 1,\ \ldots,\ n$.

$I(1)$:



Задача ЧУМ-6...

$I(2) = I(1) \times I(1)$
(двойными линиями показаны экземпляры $I(1)$):



Разделы

Интуиционистское исчисление высказываний ИИВ: формулы

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

Приведём вывод формулы $x \vee y \supset y \vee x$.
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 схему 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 конъюнкцию составляющих его формул, 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.

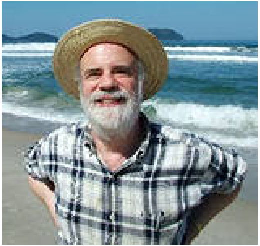
В ИИВ задача радикально усложняется: это исчисление не имеет конечнозначной интерпретации, т.е. если в любом конечном наборе $Tr = \{\mathbf{0}, 1, \ldots, k-1\}$ объявив значение $\mathbf{0}$ выделенным и задав правила оценки формул так, чтобы при всех интерпретациях переменным из Var значений из Tr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

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

$$u \leqslant v \text{ и } u \Vdash x \Rightarrow v \Vdash x,$$

т.е., как говорят, «область истинности переменной наследуется вверх» или «сохраняется в бóльших мирах».

Шкалы Крипке: интерпретация порядка и формальное определение

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 $u \nVdash A$;

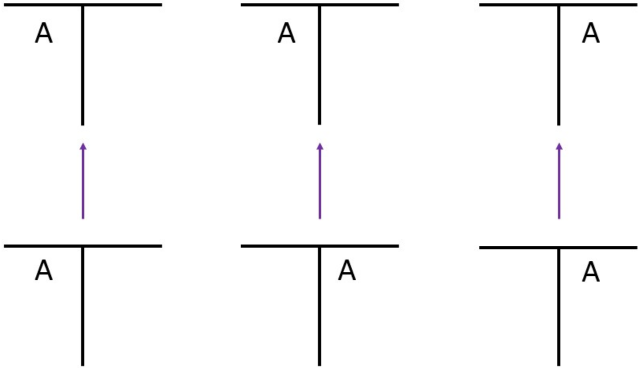
$w \Vdash \neg A \;\Leftrightarrow\; \forall (u \geqslant w)\; u \nVdash A$
(т.е. если $\Vdash \neg A$, то не существует большего мира, в котором бы $\Vdash A$).

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 (бо́льших) 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

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 (продолжение)

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.

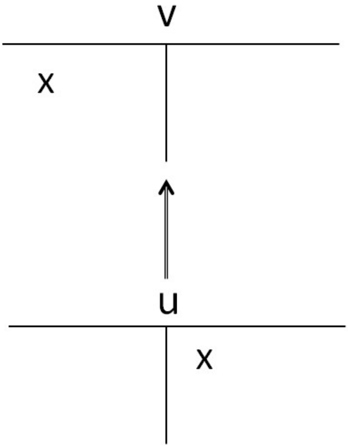
Такая шкала называется *контрмоделью* для данной формулы.

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

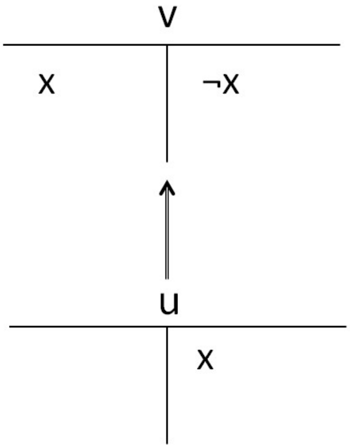
Пример

Постоим шкалу Крипке, содержащую мир, в котором формула $x \vee \neg x$ ложна.
Возьмём два мира u и v такие, что $u \leqslant v$, $u \not\Vdash x$ и $v \Vdash x$.
Тогда $v \not\Vdash \neg x$, откуда $u \not\Vdash \neg x$, что, в свою очередь даёт $u \not\Vdash x \vee \neg x$ (но $v \Vdash x \vee \neg x$).

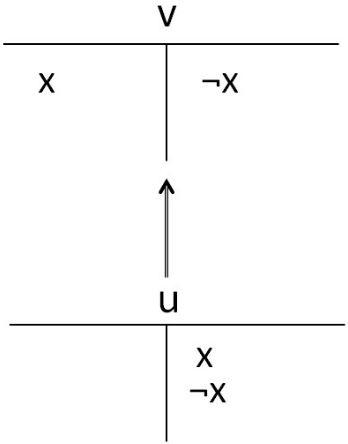
Контрмодель для $x \vee \neg x$ (1)



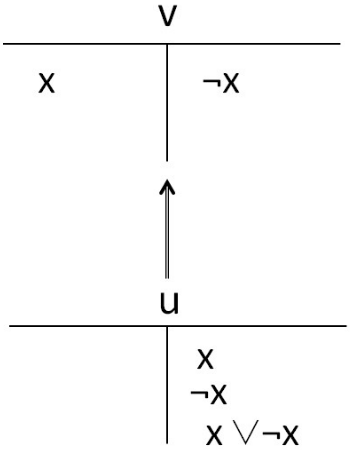
Контрмодель для $x \vee \neg x$ (2)



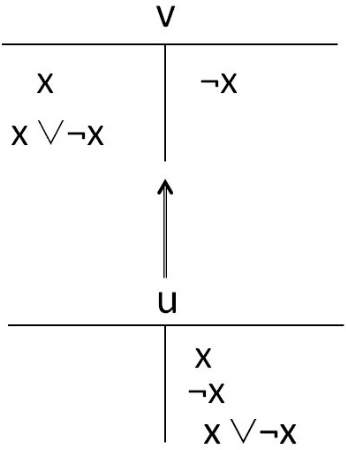
Визуализация контрмодели для $x \vee \neg x$ (3)



Контрмодель для $x \vee \neg x$ (4)



Контрмодель для $x \vee \neg x$ (5)



Контрмодель для $\neg x \vee \neg\neg x$

Пусть в мире u данная формула ложна, т.е. $u \nVdash \neg x \vee \neg\neg x$.
Тогда $u \nVdash \neg x$ и $u \nVdash \neg\neg x$.

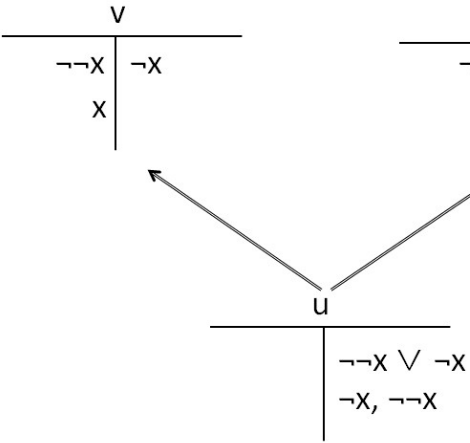
Построим два несравнимых между собой мира v и w, бóльшие u, в которых:

- $v \nVdash \neg x$ и $v \Vdash \neg\neg x$;
- $w \nVdash \neg\neg x$ и $w \Vdash \neg\neg x$.

Искомая контрмодель получена:

- правила истинности и ложности формул в модели соблюдены;
- формула x будет истинна только в мире v.

Контрмодель для $\neg x \vee \neg\neg x$...



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*.