Московский государственный университет
имени М. В. Ломоносова

Кафедра Математических методов прогнозирования

Конспект лекций
по курсу

ПРИКЛАДНАЯ АЛГЕБРА

группа 417, осенний семестр 2019/20 уч. года

Лектор к.ф.-м.н., доц. *С. И. Гуров*

2019

Оглавление

Глава 1

Булевы алгебры

1.1 Аксиоматика булевой алгебры

Определение 1.1. *Булевой алгеброй* $\mathfrak{B}$ называется множество B, содержащее по крайней мере два элемента — *нуль* o и *единица* ι, с заданными на нём бинарными операциями *объединения* $\sqcup$, *пересечения* $\sqcap$ и унарной операцией *дополнения* $'$, таких, что для любых элементов $x, y, z \in B$ выполняются следующие *законы* (или *аксиомы*) *булевой алгебры*:

1) $x \sqcup y = y \sqcup x$,
2) $x \sqcap y = y \sqcap x$,
3) $(x \sqcup y) \sqcap z = (x \sqcap z) \sqcup (y \sqcap z)$,
4) $(x \sqcap y) \sqcup z = (x \sqcup z) \sqcap (y \sqcup z)$,
5) $x \sqcup o = x$,
6) $x \sqcap \iota = x$,
7) $x \sqcup x' = \iota$,
8) $x \sqcap x' = o$,
9) $(x')' = x$,
10) $\iota' = o$,
11) $o' = \iota$,
12) $(x \sqcup y)' = x' \sqcap y'$,
13) $(x \sqcap y)' = x' \sqcup y'$,

14) $x \sqcup \iota = \iota$,
15) $x \sqcap o = o$
16) $x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z$,
17) $x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z$,
18) $x \sqcup x = x$,
19) $x \sqcap x = x$,
20) $x \sqcap (x \sqcup y) = x$,
21) $x \sqcup (x \sqcap y) = x$.

Множество B называется *носителем* булевой алгебры $\mathfrak{B}$, а o и ι — *выделенными элементами* или *универсальными гранями*.

Аксиомы 1) и 2) — законы коммутативности (Com), 3) и 4) — дитрибутивности (Dtr). Аксиомы 5) и 6) — законы нейтральности универсальных граней. Аксиомы 7) и 8) — *основные законы, описывающие свойства дополнения*; они постулируют, соответственно, его полноту и обособленность. Аксиома 9) — закон инволютивности дополнения. Далее приведены законы 10) и 11) — взаимной дополнительности o и ι, 12) и 13) — 1-й и 2-й законы Де Мóргана (DeM), 14) и 15) — поглощающих свойств универсальных граней, 16) и 17) — ассоциативности (Ass). Аксиомы 18) и 19) — законы идемпотентности[1)] Наконец, аксиомы 20) и 21) — законы поглощения (Abs).

[1)] Идемпотентность — свойство операции при повторном применении давать тот же результат, что и при первом (от лат. *idem* — тот же самый и *potens* — способный; термин введён Ч. Пирсом.

Понятно, что в булевой алгебре определены объединения и пересечения *любой конечной совокупности* элементов.

Введённые операции называют *абстрактными*, поскольку ни они сами, ни носитель, на котором они определены, никак не конкретизируются и никаких иных требований, кроме удовлетворения данным законам, к ним не предъявляется.

Основные соотношения булевой алгебры

Утверждение 1.1 (*основные свойства элементов булевой алгебры*). *Для любых элементов x и y булевой алгебры справедливы следующие утверждения.*

1. $x \sqcup y = o \Leftrightarrow x = y = o$ *и*

   $x \sqcap y = \iota \Leftrightarrow x = y = \iota$;

2. *Следующие четыре соотношения эквивалентны:*

$$(1)\ x \sqcap y = x\,, \qquad (2)\ x \sqcup y = y,$$
$$(3)\ x' \sqcup y = \iota\,, \qquad (4)\ x \sqcap y' = o.$$

3. *Лемма о единственности дополнения*[2)]*:*

$$\begin{cases} x \sqcap y = o \\ x \sqcup y = \iota \end{cases} \Leftrightarrow\ y = x'$$

[2)] В некоторых аксиоматизациях дополнение вводится как элемент, удовлетворяющий законам 7) и 8), и тогда необходимо доказывать его единственность, чем и объясняется данное традиционное название леммы.

Доказательство. При пояснении выкладок применение законов коммутативности и ассоциативности специально указывать не будем.

1. $x = x \sqcap (\underbrace{x \sqcup y}_{=o}) = o$; $x = x \sqcup (\underbrace{x \sqcap y}_{=\iota}) = \iota$
   и аналогично для y. Обратные следования очевидны.

2. Выведем требуемые соотношения циклически выведены друг из друга.

   (1) $\xrightarrow{\sqcup y}$ (2) : $x \sqcap y = x \Rightarrow$

   $$\Rightarrow y \sqcup (x \sqcap y) = y \sqcup x \Rightarrow y = y \sqcup x;$$

   (2) $\xrightarrow{\sqcup x'}$ (3) : $x' \sqcup y = x' \sqcup y \sqcup x = \iota$;

   (3) $\xrightarrow{DeM}$ (4) : $x' \sqcup y = \iota \Rightarrow x \sqcap y' = o$;

   (4) $\xrightarrow{\sqcup (x \sqcap y)}$ (1) : $(x \sqcap y') \sqcup (x \sqcap y) = x \sqcap y \Rightarrow$

   $$\Rightarrow x \sqcap (y \sqcup y') = x = x \sqcap y.$$

3. *Достаточность.*

$$y = y \sqcap (\underbrace{x \sqcup x'}_{=\iota}) = (\underbrace{y \sqcap x}_{=o}) \sqcup (y \sqcap x') =$$
$$= (y \sqcap x') \sqcup (\underbrace{x \sqcap x'}_{=o}) = x' \sqcap (\underbrace{x \sqcup y}_{=\iota}) = x'.$$

Необходимость очевидна. □

Пусть V — выражение или равенство булевой алгебры. Обозначения для результата одновременной замены всех символов в V:

$V^\sharp$ — $\sqcap \leftrightarrow \sqcup$ и $\iota \leftrightarrow o$;

$V^\flat$ — $x \leftrightarrow x'$, где $x \notin \{o, \iota\}$;

V^* — когда производятся обе указанные замены.

Утверждение 1.2 (Принцип двойственности).

1. *Если V — булево равенство, истинное для любых входящих в него элементов, то равенства $V^\sharp$, $V^\flat$ и V^* также истинны.*

2. *Если V — выражение булевой алгебры, то $V^* = V'$.*

Доказательство.

1. Приведённые выше законы, кроме 9) — инволютивности дополнения — разбиваются на пары *взаимодвойственных*, переходящих друг в друга при замене $^\sharp$; а указанный закон *самодвойственен.*

   Преобразование $^\flat$ переводит все законы, кроме 9), или с точностью до обозначений в себя, или в двойственные, а закон инволютивности дополнения — в тождество $x' = x'$.

   Поэтому и при замене * истинность булева равенства сохранится.

2. Справедливость этого утверждения следует из равенства $V = z$, где z — соответствующий элемент булевой алгебры: $V = z \Rightarrow V^* = z' = V'$. □

Об аксиоматике булевой алгебры. Приведённая система из 21-ой аксиомы избыточна.

Например, законы идемпотентности вытекают из законов поглощения: для любого $x \in B$ справедливо

$$18)\ x \sqcup x \overset{18)}{=} x \sqcup (x \sqcap (x \sqcup x)) \overset{19)}{=} x.$$

19) — по принципу двойственности.

Также можно показать, что законы де Мóргана выводимы из остальных аксиом булевой алгебры и т. д.

Приведём две «рабочие» системы аксиом.

1. Пары аксиом коммутативности, дистрибутивности, нейтральных свойств особых элементов, а также основные законы дополнения — *первые 8 из приведенных выше законов.*

   Данная система не является независимой: например, каждый из законов нейтральности универсальных граней (14) и 15) в определении 1.1) выводим из остальных семи.

2. Пары законов дистрибутивности, поглощения и основных свойств дополнения.

   Это единственная кратчайшая (6 аксиом) известная на сегодняшний день безызбыточная система двойственных аксиом булевой алгебры.

Известны и весьма «экзотические» системы аксиом для булевой алгебры (с одним символом операции, одной аксиомой и др.).

Алгебраические системы. Булева алгебра — пример *алгебраической системы (АС)* или *структуры*, точнее, частного случая АС — *алгебры*. АС $\mathfrak{A}$ задается парой $\mathfrak{A} = \langle A, \sigma_A \rangle$, где

A — *носитель* или *базовое множество* ($A \neq \varnothing$); упрощая, АС часто обозначают символом базового множества;

σ_A — *сигнатура* на A — упорядоченная совокупность символов операций, отношений и особых элементов на A.

- Все операции АС должны быть *устойчивы* на её носителе.
- Если σ_1 и σ_2 — две сигнатуры на A и $\sigma_1 \subset \sigma_2$, то
  АС $\langle A, \sigma_1 \rangle$ является *редуктом* АС $\langle A, \sigma_2 \rangle$.

Однако полного перечня аксиом и точного определения предложенной им алгебры Буль не дал. АС, эквивалентная булевой алгебре в современном её понимании, впервые приведена в вышедшем в том же году 3-м томе трактата А. де Моргана «Формальная логика».

1.2 Алгебры множеств

Алгебры на множествах. Пусть $A \neq \varnothing$ — множество, $\mathcal{P}(A)$ — множество всех подмножеств (*булеан*) A; $\mathcal{S}(A)$ — некоторая совокупность подмножеств

A, устойчивая относительно объединения $\cup$, пересечения $\cap$ и дополнения до A $(^-)$, а также содержащая $\varnothing$ и A. Понятно, что $\{\varnothing, A\} \subseteq \mathcal{S}(A) \subseteq \mathcal{P}(A)$.

АС $\langle \mathcal{S}(A), \cup, \cap, {}^-, \varnothing, A \rangle$ — *алгебра множеств.*

Алгебра множеств с носителем $\mathcal{P}(A)$ — *тотальная (над A)*, а с двухэлементным носителем $\{\varnothing, A\}$ — *тривиальная.*

Утверждение 1.3. *Всякая алгебра множеств $\mathcal{S}(A)$ есть булева алгебра с нулём $\varnothing$ и единицей A.*

Доказательство. Убедимся, что в алгебре множеств выполняются первые восемь законов булевой алгебры определения 1.1.

в формулировке которых произведены подстановки

$$\sqcup \mapsto \cap, \quad \sqcap \mapsto \cap, \quad {}' \mapsto {}^-, \quad \iota \mapsto A, \quad o \mapsto \varnothing.$$

1. Законы коммутативности, нейтральности универсальных граней и основные законы дополнения, очевидно, справедливы.
2. Покажем справедливость одного из законов дистрибутивности (второй будет справедлив по двойственности), а именно то, что для любых подмножеств $X, Y, Z \in \mathcal{S}(A)$ справедливо

$$(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z).$$

Докажем это *методом двух включений.*

$\Rightarrow$ Произвольный элемент w из $(X \cup Y) \cap Z$ принадлежит Z, а также либо X, либо Y, то есть справедливо «либо $w \in X \cap Z$, либо $w \in Y \cap Z$» и, следовательно, $w \in (X \cap Z) \cup (Y \cap Z)$.

$\Leftarrow$ Если $w \in (X \cap Z) \cup (Y \cap Z)$, то $w \in X \cap Z$ или $w \in Y \cap Z$, то есть «$w \in Z$ и либо $w \in X$, либо $w \in Y$» $\Leftrightarrow$ $w \in (X \cup Y) \cap Z$. □

Другим способом доказательства теоретико–множественных тождеств является *метод характеристичских функций*. Он состоит в сопоставлении каждому множеству A функции

$$\chi_X(w) = \begin{cases} 1, & x \in X, \\ 0, & x \notin X \end{cases}.$$

Тогда функции, соответствующие операциям, будут равны:

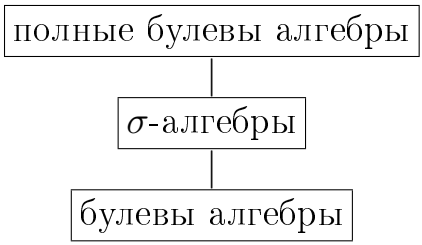
$$\begin{aligned} \chi_{X\cap Y} &= \chi_X \chi_Y; \\ \chi_{X\cup Y} &= \chi_X + \chi_Y - \chi_X \chi_Y; \\ \chi_{X'} &= 1 - \chi_X. \end{aligned}$$

Метод эквивалентных преобразований заключается в последовательной подстановке известных тождеств в формулу для получения правой части доказываемого утверждения из левой или наоборот.

Алгебра множеств, замкнутая относительно операции *счётного* объединения, называется *σ-алгеброй* и, следовательно, является булевой алгеброй. *Например*, аксиоматика А. Н. Колмогорова теории вероятностей построена на σ-алгебре подмножеств пространства элементарных событий.

Булева алгебра, в которой операции $\sqcup$ и $\sqcap$ определены для *произвольной совокупности* её элементов называется *полной*.

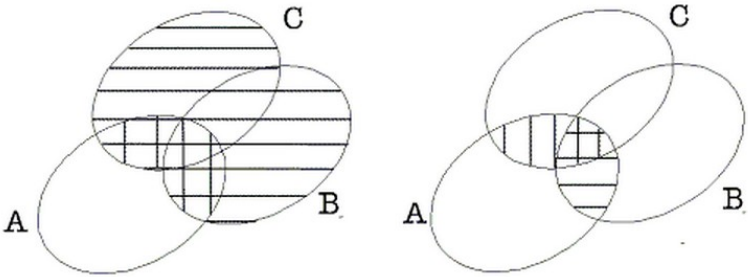
Любая алгебра множеств — полная, а σ-алгебра (где эти операции могут быть взяты лишь по счётной совокупности множеств), является “промежуточной” между обычной и полной булевыми алгебрами:



Формально для булевой алгебры с носителем B и объединения $S = \bigsqcup_{x \in X \subseteq B} x$ считают, что $S = x$ при одноэлементном множестве $X = \{x\}$ и $S = o$ при пустом X. Для пересечения элементов — $\bigsqcap_{x \in \varnothing} x = \iota$.

Составляющие системы множеств. Проверку равенств булевой алгебры $\mathcal{P}(A)$ проводят, используя известные *диаграммы Эйлера-Венна*.

Пример 1.1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ —



Это будет являться доказательством, если диаграмма *правильно построена*. Формализуем данное понятие.

Определение 1.2. Пусть дано множество $U \neq \varnothing$ и система $X = \{X_1, \ldots, X_n\}$ его подмножеств.
Составляющие данной системы множеств задаются индуктивным определением:

1) у одноэлементной системы $\{X_1\}$ — две составляющие: X_1 и $\overline{X}_1$;

2) если s — составляющая системы $\{X_1, \ldots, X_{n-1}\}$, то $s \cap X_n$ и $s \cap \overline{X}_n$ — составляющие системы $\{X_1, \ldots, X_{n-1}, X_n\}$.

Система множеств X называется *независимой*, если все её составляющие непусты.

Пример 1.2. Рассмотрим множество $U = \{a, b, c, d\}$.

1. Найдём составляющие системы $X_1 = \{a, b\}$, $X_2 = \{b\}$.

Шаг 1: $X_1 = \{a, b\}$, $\overline{X}_1 = \{c, d\}$;
Шаг 2: $X_1 \cap X_2 = \{b\}$, $\overline{X}_1 \cap X_2 = \varnothing$,
$\overline{X}_2 = \{a, c, d\}$, поэтому
$X_1 \cap \overline{X}_2 = \{a\}$, $\overline{X}_1 \cap \overline{X}_2 = \{c, d\}$,

и, следовательно, данная система множеств *не является независимой*.

2. Составляющие системы $X_1 = \{a, b\}$, $X_2 = \{b, c\}$ суть $\{b\}$, $\{c\}$, $\{a\}$, $\{d\}$, и, следовательно, данная система множеств *независима*.

Утверждение 1.4. *1. Объединение всех составляющих совпадает со всем множеством U.*

2. Различные составляющие независимой системы множеств не пересекаются.

3. Независимая система из n множеств имеет 2^n различных составляющих.

Доказательство. — пп. (1) и (2) легко проводятся по индукции, (3) следует из (1). □

Теорема 1.1 (*Венн*). *Если в алгебре множеств булево равенство выполнено для некоторой независимой системы подмножеств, то оно справедливо для любой системы подмножеств.*

Доказательство. Рассмотрим непустое множество M, представленное нормальной формой Кантора F_M над независимой системой множеств $X = \{X_1, \ldots, X_n\}$:

$$M = F_M = \bigcup_{\sigma=(\sigma_1,\ldots,\sigma_n)\in N_M \subseteq B^n} \bigcap_{j=1}^{n} X_j^{\sigma_j} = \bigcup_{k\in I_M \subseteq \{1,\ldots,2^n\}} s_k,$$

где N_M и I_M — соответствующие множеству M совокупности вершин n-мерного единичного куба B^n и множества $\{1, \ldots, 2^n\}$ номеров составляющих системы X. Заметим, что для зависимой системы X указанное представление может отсутствовать, оно единственно с учётом введённой выше эквивалентности.

Заметим, что если $s \neq \varnothing$ — составляющая какой-либо независимой системы множеств, то либо $s \subseteq M$, либо $s \cap M = \varnothing$ и справедливость $x \in s$ полностью определяет истинность $x \in X_i$ для всех $i = 1, \ldots, n$.

В силу этого представление для M остаётся справедливым и единственным для любой произвольной

независимой системы множеств (для зависимой системы могут появиться и другие представления). Поэтому если в независимой системе два булевых выражения F_1 и F_2 имеют одни и те же составляющие, то справедливость или несправедливость равенства $F_1 = F_2$ сохранится и в любой другой независимой системе. □

Следствие. Диаграммы Венна будут являться доказательством булева равенства, если несвязанным условиями элементам булевой алгебры соответствуют независимая система областей (области общего положения).

1.3 Изоморфизмы булевых алгебр

Примеры булевых алгебр

1. *Алгебра логики* или *алгебра высказываний* — АС $\mathbf{2} = \langle B, \sigma \rangle$, где $B = \{1, 0\}$ («истина» и «ложь»), а $\sigma = \langle \vee, \&, \neg, 0, 1 \rangle$ является булевой алгеброй; она играет фундаментальную роль в логике.

7) $x \vee \neg x = 1$ — *закон исключенного третьего;*

8) $x \,\&\, \neg x = 0$ — *закон противоречия.*

2. *Булева алгебра n-мерных двоичных векторов* —
АС $\mathbf{2}^n = \langle B^n, \vee, \&, \neg, \widetilde{0}, \widetilde{1} \rangle$, где B^n — n-мерный единичный куб, $\widetilde{0} = (0, \ldots, 0)$ и $\widetilde{1} = (1, \ldots, 1)$, а

сигнатурные операции применяются к булевым векторам покомпонентно (многомерный вариант алгебры **2**).

3. *Булева алгебра логических функций* — АС $\langle P_2, \vee, \&, \neg, \mathbf{0}, \mathbf{1} \rangle$, где P_2 — множество всех двузначных булевых функций, а $\mathbf{0}$ и $\mathbf{1}$ — функции «тождественный нуль» и «тождественная единица».

4. Пусть N — *свободное от квадратов* натуральное число (то есть справедливо *примарное разложение* $N = p_1 \cdot \ldots \cdot p_k$, где $p_1, \ldots, p_k$ — различные простые числа) и $D(N)$ — совокупность всех натуральных делителей N.
Например, для $N = 30 = 2 \cdot 3 \cdot 5$ имеем
$D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$.

Обозначим: $m \vee n$ — наименьшее общее кратное чисел, $m \wedge n$ — наибольший общий делитель чисел m и n, $m' = \frac{N}{m}$. Тогда АС $\langle D(N), \vee, \wedge, ', 1, N \rangle$ — булева алгебра, широко используемая в теории чисел.

5. *Алгебра контактных схем.*
Рассмотрим множество электрических выключателей, или контактов, которые могут находиться в одном из двух состояний — замкнутом (проводящем) или разомкнутом (не проводящем).

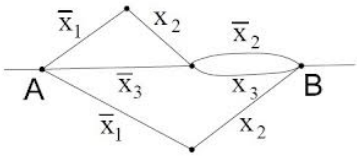
У таких контактов различают входной и выходной полюсы, которые можно соединять с полюсами других контактов, строя электрические двухполюсные (один вход и один выход) цепи.

Если соединять друг с другом только входные и

выходные полюсы, то имеется только два способа объединения таких цепей: *последовательное* и *параллельное*. В результате получаем π-*схемы*.

Под произведением $A \cdot B$ понимаем цепь, образованную последовательным, а под суммой $A + B$ — параллельным соединением цепей A и B. Под цепью $\overline{A}$ понимаем цепь, полученную размыканием всех замкнутых контактов A и замыканием всех её разомкнутых контактов.

Проводимость двухполюсной цепи может быть описана формулой над множеством логических связок $\{ \vee, \&, \neg \}$ ($\&$ опускают), в которой каждому контакту цепи соответствует своя пропозициональная переменная с отрицанием или без, выражающая его проводимость.



$$(\overline{x}_1 x_2 \vee \overline{x}_3)(\overline{x}_2 \vee x_3) \vee \overline{x}_1 x_2 \;=\; \overline{x}_1 x_2 \vee \overline{x}_2 \overline{x}_3$$

Две цепи одинаковы, если можно так сопоставить контактам переменные, что при одном и том же состоянии контактов обе рассматриваемые цепи являются одновременно либо проводящими, либо не проводящими. Это — отношение эквивалентности на множестве цепей.

Обозначим I постоянно замкнутую, O — постоянно разомкнутую цепи.

Если C — множество всех попарно неэквивалентных π-схем (последовательно-параллельных двухполюсных электрических цепей), то АС $\langle C, +, \cdot, {}^{-}, O, I \rangle$ — булева *алгебра переключательных схем.*

Применение формульного аппарата булевых алгебр для анализа и синтеза электрических схем имеет огромное прикладное значение.

Кроме параллельно-последовательных, существуют ещё т.н. *мостиковые схемы.*

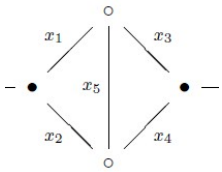


Рис. 1.1. Мостиковая схема

Такие схемы не может быть построена указанными операциями последовательного и параллельного соединения цепей — формула

$$F = x_1 \,\&\, (x_3 \vee (x_4 \,\&\, x_5)) \vee x_2 \,\&\, (x_4 \vee (x_3 \,\&\, x_5)),$$

не является бесповторной[3)], и никакое эквивалентное преобразование F не приведёт к бесповторной форме над множеством связок $\{\vee, \&, \neg\}$.

Для описания подобных схем язык булевой алгебры оказывается недостаточным: *не удаётся так усовершенствовать обычный булев аппарат алгебры ло-*

[3)] Формула над данным множеством связок называется *бесповторной*, если каждая переменная встречается в ней не более одного раза.

гики, добавив к нему ещё несколько (конечное число!) операций так, чтобы он стал содержать средства для описания строения не только параллельно-последовательных, но и мостиковых схем, притом описания адекватного, то есть такого, при котором каждому контакту в схеме соответствует ровно одна буква в формуле, выражающая проводимость данной схемы (Кузнецов А.В.).

В 1960-х гг. российский логик и философ *Е. К. Войшвилло* построил алгебру для адекватного описания двухполюсных цепей общего вида.

6. *Алгебра случайных событий.* Пусть в ходе некоторых экспериментов могут наблюдаться или не наблюдаться определённые события. Такие события называют *случайными*, не различая при этом события, которые в данном эксперименте появляются/не появляются только одновременно.

Введём три операции на таких событиях в данном эксперименте:

- $+$ — *сложение* двух событий означающее, что наблюдается хотя бы одно из указанных событий;
- $\cdot$ — *умножение* двух событий, означающее, что наблюдаются оба этих события;
- $^-$ — *отрицание* события, означающее, что данное событие не наблюдалось.

Зафиксируем также никогда не наступающее событие $\varnothing$ и всегда наступающее при проведении данного эксперимента событие $\mathbf{1}$. Совокупность всех случайных

событий, связанных с данным экспериментом, является булевой алгеброй относительно введённых операций и выделенных элементов $\varnothing$ и $\mathbf{1}$.

Далее вводят понятие вероятностной меры $P(\cdot)$ на элементах алгебры событий, однако это не предмет нашего рассмотрения.

Вышеприведенные АС являются *представлениями* или *реализациями* булевой алгебры.

Максиминная алгебра. Для действительных чисел a, b из отрезка $[\,0,\,1\,]$ положим

$$a \oplus b = \max\{a,\,b\},\ a \otimes b = \min\{a,\,b\},\ \ominus a = 1 - a.$$

АС $\langle\,[\,0,\,1\,],\,\oplus,\,\otimes,\,\ominus,\,0,\,1\,\rangle$ — *максиминная алгебра.*

Она *не будет являться булевой алгеброй*: в ней не выполняются, например, основные законы дополнения. Кстати, это доказывает их независимость от остальных и необходимость присутствия этих законов в любой системе аксиом для булевой алгебры введённой сигнатуры.

Дополнения в максиминной алгебре единственны и, таким образом, максиминная алгебра *чрезвычайно близка к булевой алгебре*, но ей всё-таки не является.

Изоморфизм булевых алгебр: определение

Определение 1.3. Пусть B и B_1 — булевы алгебры и $\varphi\colon B \to B_1$ — такая биекция, что для всех $x, y \in B$ справедливы равенства

1) $\varphi(x \sqcup y) = \varphi(x) \sqcup \varphi(y)$,

2) $\varphi(x \sqcap y) = \varphi(x) \sqcap \varphi(y)$,
3) $\varphi(x') = (\varphi(x))'$.

Тогда говорят, что φ — *булев изоморфизм* между B и B_1, а данные алгебры *булево изоморфны* (символически $B \cong B_1$).

Замечание. Из данных свойств следует

$$4)\ \ \varphi(o) = o, \quad 5)\ \ \varphi(\iota) = \iota.$$

Действительно:

$$\varphi(o) = \varphi(x \sqcap x') = \varphi(x) \sqcap \varphi(x') = \varphi(x) \sqcap \varphi(x)' = o$$

и аналогично для $\varphi(\iota)$.

Неформально булев изоморфизм — взаимно-однозначное отображение носителей булевых алгебр, сохраняющее операции и особые элементы o и ι.

Примеры 1.1 (*изоморфных булевых алгебр*).

1. Алгебра высказываний изоморфна тривиальной алгебре множеств: $\mathbf{2} \cong \{\varnothing, A\}$.
2. $|A| = n \Rightarrow \mathcal{P}(A) \cong B^n$. Булев изоморфизм — биекция элементов A и векторов первого слоя B^n.

Теорема 1.2 (*критерий изоморфности тотальных алгебр множеств*). *Две тотальные алгебры множеств $\mathcal{P}(A)$ и $\mathcal{P}(B)$ изоморфны, если и только если A и B имеют одинаковую мощность.*

Доказательство. Необходимость. Пусть существует изоморфизм φ между алгебрами $\mathcal{P}(A)$ и $\mathcal{P}(B)$.

Тогда φ — взаимно-однозначное соответствие между $\mathcal{P}(A)$ и $\mathcal{P}(B)$ и, следовательно, между множествами A и B, откуда следует их равномощность.

Достаточность. Если множества A и B равномощны, то между их элементами можно установить взаимно-однозначное соответствие f.

Однако элементами $\mathcal{P}(A)$ и $\mathcal{P}(B)$ служат подмножества A и B соответственно, и f не является искомым изоморфизмом.

Поэтому распространим отображение f на подмножества данных множеств:

$$\varphi(X) = \bigcup_{a \in X} f(a) \subseteq B.$$

Простая проверка показывает, что φ является булевым изоморфизмом между $\mathcal{P}(A)$ и $\mathcal{P}(B)$. □

1.4 Теорема Стоуна

Атомы. Справедлива следующая фундаментальная теорема о представлении произвольных булевых алгебр алгебрами множеств.

Теорема 1.3 (*Стоун*). *Всякая булева алгебра изоморфна подходящей алгебре множеств.*

Мы докажем эту теорему для *конечного случая*, для чего введём новое понятие.

Определение 1.4. Ненулевой элемент a булевой алгебры B называется *атомом*, если для любого элемента $x \in B$ справедливо

$$a \sqcap x = \left[\begin{array}{l} \text{либо } 0, \\ \text{либо } a. \end{array} \right.$$

В последнем случае говорят, что *элемент x содержит атом a*.

Например, атомы в B^n — двоичные наборы первого слоя, в $\mathcal{P}(A)$ — *одноэлементные* подмножества A.

Утверждение 1.5 (*основное свойство атомов*). *Если a_1 и a_2 — различные атомы булевой алгебры, то*

$$a_1 \sqcap a_2 = o.$$

Доказательство. Если $a_1 \sqcap a_2 = b \neq o$, то согласно определению должно быть и $b = a_1$, и $b = a_2$. □

Лемма 1.1. *В конечной булевой алгебре каждый ненулевой элемент содержит хотя бы один атом.*

Доказательство. Приведём алгоритм нахождения атома, содержащегося в элементе $x \in B$.

1. Для $x \neq o$ полагаем сначала $a = x$.
2. Упорядочим произвольным образом элементы из $B \setminus \{o\}$, получив конечную последовательность, которую обозначим B_x.
3. Последовательно $k = 1, 2, \ldots$ перебирая элементы этой последовательности, вычисляем $z = a \sqcap b_k$, полагая
   - если $z = 0$, то исключаем b_k из B_x;
   - если $z \neq o$, то полагаем $a = z$.

В результате получим элемент

$$a = x \sqcap \prod_{b \in B_x \subset B} b \neq o,$$

причём для любого $b \in B$ пересечение $a \sqcap b$ равно либо o, либо a, а B_x соответствующее подмножество то есть a — искомый атом.

Заметим, что если x содержит более одного атома, при разных упорядочениях элементов в указанной последовательности в качестве a будут получаться, вообще говоря, различные атомы. □

Булева алгебра называется

- *атомной* (или *дискретной*), если каждый её ненулевой элемент содержит атом,
- *безатомной* (или *непрерывной*) если она не содержит ни одного атома.

Все конечные (и рассмотренные ранее) алгебры — атомные.

Пример 1.3 (*безатомной булевой алгебры*). Пусть S — совокупность всех конечных объединений всевозможных полуинтервалов вида $(x, y]$ из промежутка $I = (0, 1]$: $0 < x \leqslant y \leqslant 1$. S устойчива относительно теоретико-множественных операций $\cup$, $\cap$ и дополнения до I, и в ней *выполняются все законы булевой алгебры*. Единица в S — весь интервал I, нуль — пустое множество $(x, x]$.

Алгебра S является *безатомной*: любой интервал $(x, y] \neq \varnothing$ содержит в себе ненулевой подынтервал.

Обозначения для булевой алгебры B:

$At(x)$ — совокупность всех атомов, содержащихся в элементе $x \in B$.

$At(B)$ — совокупность всех атомов B.

Лемма 1.2 (о разложении ненулевого элемента на атомы). *Всякий ненулевой элемент атомной булевой алгебры может быть представлен в виде объединения содержащихся в нём атомов:*

$$x = \bigsqcup_{a \in At(x)} a. \tag{1.1}$$

Пример 1.4. В $\mathcal{P}(\{a, b, c, d\})$ элемент $x = \{a, b, c\}$ содержит атомы $\{a\}$, $\{b\}$, $\{c\}$ и равен их объединению: $x = \{a\} \cup \{b\} \cup \{c\}$.

При $At(a) = \{a\}$ формально полагают

$$x = \bigsqcup_{\{a\}} a \quad \text{и} \quad o = \bigsqcup_{\varnothing} a.$$

Доказательство леммы будет дано позднее.

Единица ι есть объединение всех атомов булевой алгебры: равенство $\iota \sqcap a = a$ справедливо для всех атомов.

Для конечного случая теорема Стоуна допускает следующее *усиление*.

Теорема 1.4. *Всякая конечная булева алгебра изоморфна некоторой тотальной алгебре множеств.*

Доказательство. Пусть B — конечная булева алгебра.

Покажем, что тотальная алгебра множеств над $At(B)$ изоморфна B, то есть $B \cong \mathcal{P}(At(B))$.

Рассмотрим функцию $\varphi(x) = At(x)$, сопоставляющую каждому элементу x из B множество $At(x)$ содержащихся в нём атомов и покажем, что она является искомым изоморфизмом. Также считаем, что $\varphi(o) = \varnothing$.

Убедимся сначала, что $\varphi(x)$ — биекция между B и $\mathcal{P}(At(B))$.

Из разложения элемента на атомы следует, что

1) элемент x однозначно определяется множеством $At(x)$ своих атомов и наоборот, то есть отображение $\varphi(x)$ *инъективно*;
2) для произвольного подмножества $A \subseteq At(B)$ можно определить элемент x как

$$x = \bigsqcup_{a \in A} a,$$

тогда $\varphi(x) = A$ и φ — *сюръективно*.

Биективность отображения φ показана.

Теперь удостоверимся, что для φ выполнены свойства (1)–(3) изоморфизма булевых алгебр.

1. Очевидно, что

$$x \sqcup y = \bigsqcup_{a_1 \in At(x)} a_1 \sqcup \bigsqcup_{a_2 \in At(y)} a_2 = \bigsqcup_{a \in At(x) \cup At(y)} a,$$

откуда $\varphi(x \sqcup y) = \varphi(x) \cup \varphi(y)$.

2. Покажем, что $\varphi(x \sqcap y) = \varphi(x) \cap \varphi(y)$

$$x \sqcap y = \bigsqcup_{a_1 \in At(x)} a_1 \sqcap \bigsqcup_{a_2 \in At(y)} a_2 = \bigsqcup_{\substack{a_1 \in At(x) \\ a_2 \in At(y)}} (a_1 \sqcap a_2) = \bigsqcup_{a \in At(x) \cap At(y)} a\,.$$

Второе равенство здесь — по дистрибутивности, а последнее — по основному свойству атомов.

3. Подставляя в полученные выше равенства $y = x'$ с учётом $At(\iota) = At(B)$ получим

$$At(x) \cup At(x') = At(B) \quad \text{и} \quad At(x) \cap At(x') = \varnothing,$$

откуда по лемме о единственности дополнения —

$$At(x') = At(B) \setminus At(x) \text{ и } \varphi(x') = \overline{\varphi(x)}.$$

□

Следствие. Конечная n-атомная булева алгебра содержит 2^n элементов, т. к. мощность множества всех подмножеств совокупности из n атомов есть 2^n.

Теорема Стоуна показывает, что элементы любой булевой алгебры можно представлять подмножествами некоторого множества, а булевы операции отождествлять с одноимёнными теоретико-множественными.

Заметим, что для доказательства теоремы Стоуна в случае бесконечных булевых алгебр используется понятие ультрафильтра.

Глава 2

Отношения и соответствия

2.1 Декартово произведение множеств и отношения

Определение 2.1. *Декартовым* или *прямым произведением* непустых множеств $A_1, \ldots, A_n$, символически $A_1 \times A_2 \times \ldots \times A_n$, называют совокупность всех конечных последовательностей вида $(a_1, a_2, \ldots, a_n)$, где $a_i \in A_i$, $i \in \overline{1,n}$.

Декартово произведение n экземпляров множества A обозначают A^n и называют *n-ой декартовой степенью* множества A: $A^1 = A$, под A^0 понимают некоторое одноэлементное подмножество A.

Определение 2.2. *Отношения* — подмножества декартовых произведений множеств; символически $\rho \subseteq A_1 \times \ldots \times A_n$.

Число множеств в соответствующем декартовом произведении есть *местность* или *арность* отношения.

Определение 2.3. Если ρ — отношение на $A_1 \times \ldots \times A_n$, то совокупность всех элементов $a_1 \in A_1$ для которых существуют такие $a_2 \in A_2, \ldots, a_n \in A_n$, что

$(a_1, a_2, \ldots, a_n) \in \rho$, называют *проекцией отношения* ρ *на множество* A_1 или *первой проекцией* ρ.

Аналогично определяются вторые, третьи и т.д. проекции. Символически i-я проекция ρ обозначается $Pr_i\,\rho$.

Отношения можно рассматривать как предикаты (функции, принимающие два значения — «истина» и «ложь»): $\rho\,(a_1, \ldots, a_n) = 1$ (истинно), если $(a_1, \ldots, a_n) \in \rho$ и ложно $(= 0)$ в противном случае. Поэтому к отношениям можно применять операции алгебры логики: дизъюнкции $(\vee)$, конъюнкции $(\&)$, отрицания $(\neg)$, тождества $(\equiv)$, импликации $(\supset)$ и др.

Унарные отношения — описывают различные свойства его элементов.

Бинарные отношения — будут рассматриваться далее.

Тернарные отношения (пример): отношение «*между*»: $\rho(x, y, z) = 1 \Leftrightarrow x < y < z$ на $\mathbb{R}$.

Соответствия. Бинарные отношения на декартовом произведении множеств A и B называют отношениями *между* A *и* B или *соответствиями* между данными множествами.

Для соответствия $\rho \subseteq A \times B$:

- обозначение — $a\rho b$, если $(a, b) \in \rho$;
- задание — направленным двудольным графом $\overrightarrow{G}(\rho)$, с долями A и B, вершинами которого служат

элементы этих долей, причём, если $a\rho b$, то из вершины, соответствующей $a \in A$, дуга ведёт в вершину, соответствующую $b \in B$.

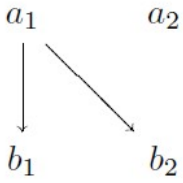


Рис. 2.1. Граф отношения $\{(a_1, b_1), (a_1, b_2)\}$ на $\{a_1, a_2\} \times \{b_1, b_2\}$

Соответствие ρ —

образ элемента $a \in A$ — множество

$$\rho(a) = \{b \in B \mid a\rho b\};$$

образ множества X — множество $\rho(X) = \bigcup\limits_{x \in X} \rho(x)$.

Свойства теоретико-множественных операций, применённые к соответствиям $\alpha, \beta \subseteq A \times B$ ($a \in A$, $b \in B$):

1) $a(\alpha \cup \beta)b \Leftrightarrow$
$\Leftrightarrow a\alpha b \vee a\beta b \Leftrightarrow (a, b) \in \alpha$ или $(a, b) \in \beta$;

2) $a(\alpha \cap \beta)b \Leftrightarrow a\alpha b \& a\beta b \Leftrightarrow (a, b) \in \alpha$ и $(a, b) \in \beta$;

3) $a\overline{\alpha}b \Leftrightarrow \neg(a\alpha b) \Leftrightarrow (a, b) \notin \alpha$.

Введём две новые операции для бинарных отношений (соответствий): унарную *псевдообращения* и бинарную *произведения*.

Определение 2.4. Унарная операция $^\sharp$ *псевдообращения* соответствия $\rho \subseteq A \times B$ задаёт *псевдообратное* к нему соответствие $\rho^\sharp \subseteq B \times A$: $b\rho^\sharp a \Leftrightarrow a\rho b$ для любых $a \in A$, $b \in B$.

Свойства псевдообращения:

$$(\rho^\sharp)^\sharp = \rho, \quad \overline{\rho^\sharp} = (\overline{\rho})^\sharp, \quad \alpha \subseteq \beta \Rightarrow \alpha^\sharp \subseteq \beta^\sharp,$$
$$(\alpha \cup \beta)^\sharp = \alpha^\sharp \cup \beta^\sharp, \quad (\alpha \cap \beta)^\sharp = \alpha^\sharp \cap \beta^\sharp.$$

Прообразы соответствия $\rho \subseteq A \times B$:

элемента $b \in B$ — множество $\rho^\sharp(b) = \{\, a \in A \mid a\rho b \,\}$;

множества $Y \subseteq B$ — множество $\rho^\sharp(Y) = \bigcup\limits_{y \in Y} \rho^\sharp(y)$.

Определение 2.5. Пусть A, B и C — непустые множества, $\alpha \subseteq A \times B$, $\beta \subseteq B \times C$. Тогда *произведение* или *умножение* $\alpha \diamond \beta$ соответствий α и β определяется для произвольных $a \in A$, $c \in C$ как

$$a(\alpha \diamond \beta)c \Leftrightarrow \exists\limits_B b : (a\alpha b) \,\&\, (b\beta c).$$

Часто знак $\diamond$ опускают и вместо $\alpha \diamond \beta$ пишут $\alpha\beta$.

Свойства произведения соответствий (в случае существования):

- $\alpha(\beta\gamma) = (\alpha\beta)\gamma$;
- $(\alpha\beta)^\sharp = \beta^\sharp \alpha^\sharp$;

- $\left\{ \begin{array}{l} \alpha \subseteq \beta \\ \gamma \subseteq \delta \end{array} \right. \Rightarrow \alpha\gamma \subseteq \beta\delta$
- $\alpha(\beta \cup \gamma) = \alpha\beta \cup \alpha\gamma, \quad (\alpha \cup \beta)\gamma = \alpha\gamma \cup \beta\gamma\,;$
- $\alpha(\beta \cap \gamma) \subseteq \alpha\beta \cap \alpha\gamma, \quad (\alpha \cap \beta)\gamma \subseteq \alpha\gamma \cap \beta\gamma.$

Доказательства. Соотношения

$$\alpha(\beta\gamma) = (\alpha\beta)\gamma \quad \text{и} \quad \left\{ \begin{array}{l} \alpha \subseteq \beta \\ \gamma \subseteq \delta \end{array} \right. \Rightarrow \alpha\gamma \subseteq \beta\delta$$

доказываются элементарно.

Покажем, что $(\alpha\beta)^\sharp = \beta^\sharp\alpha^\sharp$. Пусть $\alpha \subseteq A \times B$, $\beta \subseteq B \times C$, тогда для любых $a \in A$, $c \in C$ справедливо:

$$\begin{aligned} c(\alpha\beta)^\sharp a = a(\alpha\beta)c = \underset{B}{\exists} b : a\alpha b \,\&\, b\beta c = \\ = \underset{B}{\exists} b : c\beta^\sharp b \,\&\, b\alpha^\sharp a = c(\beta^\sharp\alpha^\sharp)a. \end{aligned}$$

Докажем, что $(\alpha \cap \beta)\gamma \subseteq \alpha\gamma \cap \beta\gamma$. Для произвольных элементов a и c соответствующих множеств получим

$$\begin{aligned} a[(\alpha \cap \beta) \diamond \gamma]c = \exists\, b : (a(\alpha \cap \beta)b) \,\&\, (b\gamma c) = \\ = \exists\, b : a\alpha b \,\&\, a\beta b \,\&\, \underline{b\gamma c} = \\ = \exists\, b : a\alpha b \,\&\, b\gamma c \,\&\, a\beta b \,\&\, b\gamma c \Rightarrow \\ \Rightarrow (\exists\, x : a\alpha x \,\&\, x\gamma c) \,\&\, (\exists y : a\beta y \,\&\, y\gamma c) = \\ = a(\alpha\gamma)c \,\&\, a(\beta\gamma)c = a(\alpha\gamma \cap \beta\gamma)c\,. \end{aligned}$$

$\alpha(\beta \cap \gamma) \subseteq \alpha\beta \cap \alpha\gamma$ — доказывается аналогично.

Представление соответствий (0,1)-матрицами. $\rho \subseteq \{a_1, \ldots, a_m\} \times \{b_1, \ldots, b_n\}$ — соответствие на конечных множествах. Матрица $M(\rho)$ отношения ρ:

$$M(\rho) = \| r_{ij} \|_{i=1,\,j=1}^{m,\,n} = \begin{cases} 1, & a_i \,\rho\, b_j, \\ 0, & \text{иначе.} \end{cases}$$

$\mathcal{M}_{m\times n}$ — множество всех (0,1)-матриц размера $m \times n$, I — матрица из 1, 0 — нуль-матрица из 0. К матрицам из $\mathcal{M}$ поэлементно применяют логическую операцию $\neg$, а к матрицам одинакового размера — логические операции $\vee$ и $\&$ по правилам алгебры высказываний **2**.

$$\begin{aligned} M(\alpha \cup \beta) &= M(\alpha) \vee M(\beta); \\ M(\alpha \cap \beta) &= M(\alpha) \,\&\, M(\beta); \\ M(\overline{\alpha}) &= \neg\, M(\alpha). \end{aligned}$$

Пусть $M_1 \in \mathcal{M}_{m\times n}$, $M_2 \in \mathcal{M}_{n\times k}$.
Произведение $M_1 \times M_2 \in \mathcal{M}_{m\times k}$ данных матриц — обычное матричное произведение с заменой операции суммирования на $\vee$, а умножения — на $\&$.

Для квадратных матриц обычным образом вводится натуральная степень M^n матрицы M.

Для конечных множеств A, B, C и $\alpha \subseteq A \times B$ и $\beta \subseteq B \times C$ справедливы равенства

$$M(\alpha \diamond \beta) = M(\alpha) \times M(\beta), \quad M(\alpha^n) = M^n(\alpha).$$

Образ $\rho(X)$ подмножества X находится умножением слева вектора-строки, задающей X, на матрицу $M(\rho)$.

2.2 Однородные отношения

Определение 2.6. Отношение $\rho \subseteq A^2$ называется *бинарным на* A или *однородным*.

$\mathcal{R}(A)$ — совокупность всех однородных на A отношений.

Элемент $a \in A$ такой, что $a\overline{\rho}a$ для некоторого отношения $\rho \in \mathcal{R}(A)$ назовём *ρ-нерефлексивным*.

Утверждение 2.1 (*канторовость отношений*). *Совокупность всех ρ-нерефлексивных элементов множества A не является образом $\rho(x)$ какого-либо элемента $x \in A$.*

Доказательство. Обозначим $N = \{\, a \in A \mid a\overline{\rho}a \,\}$. Тогда $x \in N \Leftrightarrow x \notin \rho(x)$ и $x \notin N \Leftrightarrow x \in \rho(x)$, то есть $N \neq \rho(x)$. □

Однородные отношения $\rho \in \mathcal{R}(A)$ удобно (особенно в случае, когда A — конечное множество с небольшим числом элементов) изображать в виде ориентированного графа $\overrightarrow{G}(\rho)$, вершинам которого соответствуют элементы A, а дуга ведёт из x в y, если $x\rho y$. Если $x\rho x$, то у вершины x рисуют петлю. Когда $x\rho y$ и $y\rho x$, вместо пары дуг противоположной направленности между x и y рисуют (ненаправленное) ребро.

Отношения $\sigma_\alpha = \alpha \cup \alpha^\sharp$ и $\iota_\alpha = A^2 \setminus \sigma_\alpha = \overline{\alpha \cup \alpha^\sharp}$ называют соответственно отношениями *сравнимости* и *несравнимости* для отношения $\alpha \in \mathcal{R}(A)$.

Если $\rho \in \mathcal{R}(A)$ и $\varnothing \neq B \subseteq A$, то отношение $\rho \cap B^2$ называют *сужением* или *ограничением отношения* ρ *на подмножество* B и обозначают $\rho\,|_B$.

Обозначение для натурального k: $\alpha^k = \overbrace{\alpha \diamond \ldots \diamond \alpha}^{k \text{ символов } \alpha}$.

Разумеется, $\alpha \subseteq \beta \Rightarrow \alpha^k \subseteq \beta^k, \quad k = 1, 2, \ldots$.

Покажем, что квадрат пересечения однородных отношений лежит в пересечении их квадратов. По свойства произведения соответствий и теоретико-множественного пересечения имеем

$$(\alpha \cap \beta)^2 \subseteq \alpha^2 \cap \beta^2 \cap \alpha\beta \cap \beta\alpha \subseteq \alpha^2 \cap \beta^2.$$

Пример 2.1 (*операции над однородными отношениями*). Пусть $\alpha = <$ — отношение *строго меньше* на $\mathbb{N}$.

$\alpha^\sharp$: $\quad m <^\sharp n \Leftrightarrow n < m \Leftrightarrow m > n$.

α^2: $\quad m <^2 n \Leftrightarrow \underset{\mathbb{N}}{\exists} x : (m < x) \& (x < n) \Leftrightarrow m+1 < n$;

$\alpha \diamond \alpha^\sharp$: $\quad m(< \diamond >)n \Leftrightarrow \underset{\mathbb{N}}{\exists} x : (m < x) \,\&\, (x > n) \Leftrightarrow$

$$\Leftrightarrow \underset{\mathbb{N}}{\exists} x : x > \max\{m, n\} \Leftrightarrow 1,$$

то есть отношение $< \diamond >$ на $\mathbb{N}$ *истинно всегда*.

$\alpha^\sharp \diamond \alpha$: $\quad m(> \diamond <)n \Leftrightarrow \underset{\mathbb{N}}{\exists} x : (m > x) \,\&\, (x < n) \Leftrightarrow$

$$\Leftrightarrow \underset{\mathbb{N}}{\exists} x : x < \min\{m, n\} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} 1, \text{ если } \min\{m, n\} > 1, \\ 0, \text{ иначе.} \end{cases}.$$

Убеждаемся, что, вообще говоря, $\alpha\beta \neq \beta\alpha$.

При $\alpha\beta = \beta\alpha$ отношения α и β называют *перестановочными*.

Специальные однородные отношения

Определение 2.7. Однородное на множестве A отношение ρ называется:

∇ : *универсальным*, если $\rho = A^2$.

$\triangle$: *диагональным* (*единичным*), если $x\rho y \Leftrightarrow x = y$.

Для единичного отношения на A используют также обозначение 1_A.

По определению для $\rho \in \mathcal{R}(A)$ полагают $\rho^0 = \triangle$.

F : *полным*, если $\rho \cup \rho^\sharp = \nabla$, то есть $x\rho y \vee x\rho^\sharp y$, или из любых двух элементов A *по крайней мере один находятся в отношении* ρ *с другим*;

R : *рефлексивным*, если $\triangle \subseteq \rho$, что означает $x\rho x$;

AR : *антирефлексивным* или *иррефлексивным*, если $\rho \cap \triangle = \varnothing$, то есть $x\bar{\rho}x$;

S : *симметричным*, если $\rho^\sharp \subseteq \rho$;

Поскольку $(\rho^\sharp)^\sharp = \rho$, то $\rho^\sharp = \rho$;

AS : *антисимметричным*, если $\rho \cap \rho^\sharp \subseteq \triangle$, то есть $x\rho y \,\&\, y\rho x \Rightarrow x = y$;

$\rho \cap \rho^\sharp$ — *симметрическая часть* данного отношения ρ;

NS : *несимметричным* или *асимметричным*, если $\rho \cap \rho^\sharp = \varnothing$, то есть *из двух соотношений* ρ *и* $\rho^\sharp$ *хотя бы одно не выполнено* (симметрическая часть пуста);

T : *транзитивным*, если $\rho^2 \subseteq \rho$, то есть $x\rho y \,\&\, y\rho z \;\Rightarrow\; x\rho z$;

Поскольку $\rho^2 \subseteq \rho \;\Rightarrow\; \rho^3 \subseteq \rho^2 \subseteq \rho$, то для транзитивного ρ имеем $\rho^n \subseteq \rho$, $n = 1, 2, \ldots$;

C : *содержащим цикл*, если для некоторых x и $k > 1$ справедливо $x\rho^k x$; в противном случае говорят, что ρ — отношение *без циклов* или *ациклическое*.

Обозначения с указанием множества — ∇_A.

Понятно, что ни отношение $\rho\rho^\sharp$, ни $\rho^\sharp\rho$ могут не быть равными единичному, что объясняет выбор термина “псевдообратное” для отношения $\rho^\sharp$.

Теорема 2.1. *Симметричное и транзитивное отношение на множестве* A*, первая проекция которого совпадает с* A*, рефлексивно.*

Доказательство. Пусть $\rho \in \mathcal{R}(A)$ обладает указанными свойствами.

$Pr_1\,\rho = A$ означает существование для любого x такого y, что $x\rho y$, откуда по симметричности и $y\rho x$. Поэтому для произвольного x справедливо

$$\forall\, x\, \exists\, y : (x\rho y)\,\&\,(y\rho x) \;\Leftrightarrow\; x\rho^2 x \;\Rightarrow\; x\rho x,$$

что и означает $\Delta \subseteq \rho$. □

Теорема 2.2 (*свойства произведения отношений*). *Для однородных отношений* α, β *и* γ *справедливы следующие утверждения.*

1. *Если* β *рефлексивно, то* $\alpha \subseteq \alpha\beta$ *и* $\alpha \subseteq \beta\alpha$.

   Отсюда $\Delta \subseteq \alpha^n$ *для рефлексивного* α, $n = 0, 1, \ldots$.

2. *Если* α *рефлексивно и транзитивно, то* $\alpha^n = \alpha$, $n = 1, 2, \ldots$.

3. *Если* $\alpha, \beta \subseteq \gamma$ *и* γ *транзитивно, то* $\alpha\beta \subseteq \gamma$.

Доказательство.

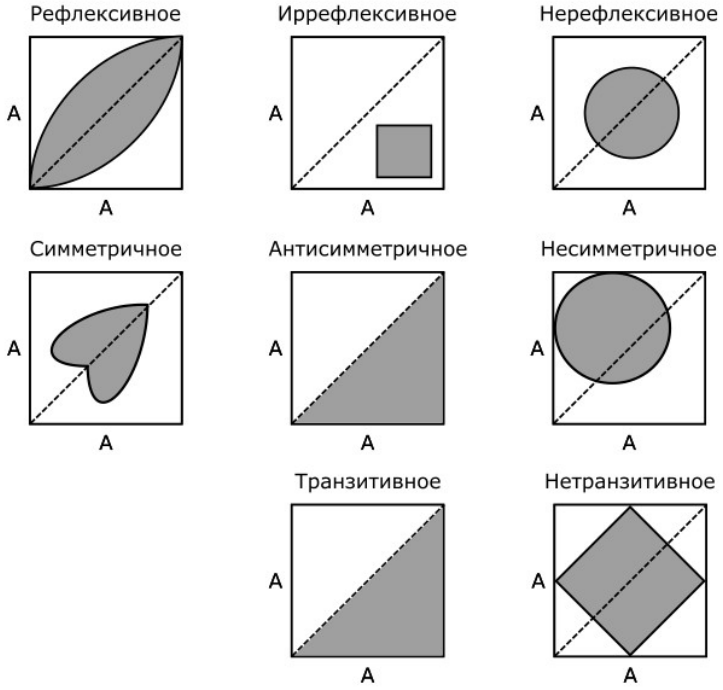


Рис. 2.2. Примеры отношений с указанными свойствами

1. $\underline{\beta - (R) \;\Rightarrow\; \alpha \subseteq \alpha\beta \;\&\; \alpha \subseteq \beta\alpha}$

   $\alpha = \alpha\Delta \subseteq \alpha\beta$ и аналогично для другого включения.
   $\Delta \subseteq \alpha^n$ следует из доказанного при $\alpha = \beta$.

2. $\underline{\alpha - (R), (T) \;\Rightarrow\; \alpha^n = \alpha}$

   Подставляя $\beta = \alpha$ в (1) получим $\alpha \subseteq \alpha^2$, а т. к. α транзитивно, то $\alpha^2 \subseteq \alpha$, откуда $\alpha = \alpha^2$ и требуемое.

3. $\underline{\alpha, \beta \subseteq \gamma \;\&\; \gamma - (T) \;\Rightarrow\; \alpha\beta \subseteq \gamma}$

   $$\left\{ \begin{array}{l} \alpha \subseteq \gamma \\ \beta \subseteq \gamma \end{array} \right. \Rightarrow \alpha\beta \subseteq \gamma\gamma = \gamma^2 \subseteq \gamma. \qquad \square$$

Инвариантность свойств однородных отношений

Определение 2.8. Данное свойство *инвариантно* относительно некоторой операции, если при условии, что операнды обладают данным свойством, то им обладает и результат операции.

Теорема 2.3 (*об инвариантности "положительных" свойств отношений*). *Для однородных отношений*

1) *рефлексивность инвариантна относительно* $\cup$, $\cap$, $^\sharp$ *и* $\diamond$;
2) *симметричность инвариантна относительно* $^-$, $\cup$, $\cap$ *и* $^\sharp$, *а относительно* $\diamond$ *— если и только если отношения перестановочны;*

3) *транзитивность инвариантна относительно* $\cap$ *и* $^\sharp$, *а относительно* $\diamond$ — *если отношения перестановочны.*

Доказательство может быть найдено в [9].

Теорема 2.4 (*об инвариантности "отрицательных" свойств отношений*). *Для однородных отношений* α *и* β

1) *антирефлексивность инвариантна относительно* $\cup$, $\cap$, $^\sharp$; *а относительно произведения* $\alpha\beta$ — *если и только если*
$$\alpha \cap \beta^\sharp = \varnothing;$$

2) *антисимметричность инвариантна относительно* $\cap$, $^\sharp$;

3) *несимметричность инвариантна относительно* $\cap$, $^\sharp$; *а относительно* $\cup$ — *если и только если*
$$\alpha \cap \beta^\sharp = \alpha^\sharp \cap \beta = \varnothing.$$

Доказательство может быть найдено в [9].

2.3 Отношение эквивалентности

Определение и основные свойства эквивалентности

Определение 2.9. Однородные рефлексивные, симметричные и транзитивные отношения называют *отношениями эквивалентности.*

Классы эквивалентности элементов или совпадают, или не пересекаются. Каждому $a \in A$ эквивалентности $\sim \in \mathcal{E}(A)$ сопоставляют множество $[a]_\sim$ эквивалентных ему элементов — *классов эквивалентности* или *смежных классов*:

$$[a]_\sim = \{\, x \in A \mid x \sim a \,\}.$$

Если эквивалентность фиксирована, то смежный класс элемента a обозначаем $[a]$.

Формирование смежных классов происходит в ходе выполнения операции *абстракции отождествления* по данной эквивалентности, при которой отвлекаются от индивидуальных характеристик элементов, выделяя лишь их общность.

Совокупность $\mathcal{D} = \{\, A_1, A_2, \ldots \}$ непустых подмножеств множества A образует его разбиение, если объединение всех подмножеств из $\mathcal{D}$ совпадает с A и все они попарно не пересекаются:

$$A = A_1 + A_2 + \ldots, \qquad A_i \cap A_j = \varnothing \ \text{ при } \ i \neq j.$$

Элементы $A_1, A_2, \ldots$ разбиения $\mathcal{D}$ — блоки; символически — $(\, A_1 \mid A_2 \mid \ldots)$. Разбиение $\mathcal{D}$ множества задает отношение эквивалентности $\sim$ на нём: *смежные классы* $\sim$ *есть блоки разбиения* $\mathcal{D}$.

Теорема 2.5 (*о классах эквивалентности*). *1. Если на множестве $A \neq \varnothing$ задана эквивалентность, то множество смежных классов образует разбиение A.*

2. Разбиение множества $A \neq \varnothing$ на блоки единственным образом определяет эквивалент-

ность $\sim$ *так, что для любой пары* a, b *элементов* A

$a \sim b \Leftrightarrow$ *a и b находятся в одном блоке разбиения.*

Определение 2.10. Множество, элементами которого являются классы эквивалентности множества A по отношению эквивалентности $\sim$, называется *фактормножеством* и обозначается $A/\sim$.

Пример 2.2. 1. Если A — множество *зёрен, насыпанных в мешки*, и для зёрен a и b положить $a \sim b$, если они *лежат в одном мешке*, то

- классами эквивалентности являются множества зёрен, *лежащих в одном мешке*,
- фактормножеством $A/\sim$ — *множество мешков.*

2. Если W — множество *слов русского языка*, и для слов u и v положить $u \sim v$, если они *начинаются с одной и той же буквы* (в русском языке 33 буквы), то

- классами эквивалентности будут множества слов, *начинающихся на данную букву*,
- а фактормножеством $W/\sim$ — *множество* соответствующих *букв* ($|W/\sim| = 31$).

Из теоремы инвариантности "положительных" свойств вытекает

Теорема 2.6 (*об инвариантности пересечения эквивалентностей*). *Отношение эквивалентности инвариантно относительно пересечения.*

Следствие. Пересечение эквивалентностей из произвольной непустой (возможно бесконечной) совокупности есть эквивалентность.

Эквивалентности α и β называют *когерентными*, если для любой пары смежных классов по α и по β соответственно справедливо утверждение «*либо один из данных классов лежит в другом, либо они не пересекаются*».

Теорема 2.7. *Пусть α и β — эквивалентности. Тогда*

1) *объединение $\alpha \cup \beta$ является эквивалентностью, если и только если α и β когерентны;*
2) *если $\alpha \cup \beta$ — эквивалентность, то $\alpha \cup \beta = \alpha\beta$ и, следовательно эквивалентности α и β перестановочны.*
3) *произведение эквивалентностей будет эквивалентностью, если и только если они перестановочны.*

Доказательство может быть найдено в [9].

Если S — некоторое свойство элементов множества A, то *наименьшим подмножеством, обладающим свойством S* называется *пересечение всех подмножеств A*, элементы которых обладают данным свойством.

Теорема 2.8 (о произведении перестановочных эквивалентностей). *Для перестановочных эквивалентностей произведение является наименьшей эквивалентностью, их содержащей.*

Это следствие предыдущей теоремы.

Оператор замыкания. Укажем способ построения наименьшей эквивалентности, содержащей данное отношение. Оно использует фундаментальное понятие *замыкания*.

Определение 2.11. *Оператором замыкания* на непустом множестве M называют отображение C множества всех подмножеств M в себя, обладающее для всех X, $Y \subseteq M$ следующими свойствами:

1. $X \subseteq C(X)$ — рефлексивность,
2. $X \subseteq Y \Rightarrow C(X) \subseteq C(Y)$ — монотонность,
3. $C(C(X)) = C(X)$ — идемпотентность.

Множество X называется *замкнутым*, если $C(X) = X$.

Наименьшее *рефлексивное* ρ^r [*симметричное* ρ^s, *транзитивное* ρ^t, *эквивалентное* ρ^e] отношение, содержащее данное отношение ρ, называется *рефлексивным [симметричным, транзитивным, эквивалентным] замыканием* ρ.

Замыкание совокупности отношений есть замыкание их *объединения*.

Замыкания однородного отношения ρ.

Рефлексивное, симметричное: $\rho^r = \rho \cup \Delta$, $\rho^s = \rho \cup \rho^\sharp$.

Транзитивное. Введём отношение $\rho^+ \stackrel{\text{def}}{=} \bigcup\limits_{n=1}^{\infty} \rho^n$.

Ясно, что, во-первых,

$a\rho^+b \Leftrightarrow \exists n\, \exists x_1, \ldots, x_n : a\rho x_1 \,\&\, x_1\rho x_2 \,\&\, \ldots \,\&\, x_n\rho b,$
во-вторых, ρ^+ транзитивно
и, в-третьих, $\alpha \subseteq \beta \Rightarrow \alpha^+ \subseteq \beta^+$.

Легко видеть, что $\rho^{\,t} = \rho^+$. Действительно, применяя операцию $^+$ к

$$\rho \subseteq \rho^t \subseteq \rho^+,$$

получим $\rho^+ \subseteq \rho^t \subseteq \rho^+$, что означает $\rho^{\,t} = \rho^+$.

Эквивалентное (ρ^e). Очевидно для любого $\rho \in \mathcal{R}(A)$

$$\rho^* \stackrel{\text{def}}{=} (\rho^t)^r = (\rho^r)^t = \triangle \cup \rho^+ = \bigcup_{n=0}^{\infty} \rho^n.$$

ρ^* — рефлексивно-транзитивным замыкание ρ.

Обозначение: $\rho^= \stackrel{\text{def}}{=} (\rho \cup \rho^\sharp \cup \triangle)^t$; ясно, это эквивалентность и $\alpha \subseteq \beta \Rightarrow \alpha^= \subseteq \beta^=$.

Легко показать, что $\rho^e = \rho^=$. Для этого применим операцию $^=$ к

$$\rho \subseteq \rho^e \subseteq \rho^=,$$

и получим $\rho^= \subseteq \rho^e \subseteq \rho^=$, что означает $\rho^e = \rho^=$.

Теорема 2.9. *Эквивалентное замыкание совокупности эквивалентностей совпадает с объединением всевозможных произведений этих эквивалентностей.*

Доказательство может быть найдено в [9].

Следствия. *1. Эквивалентное замыкание* $\{\alpha, \beta\}^e$ *двух эквивалентностей* α *и* β *совпадает с объединением всевозможных произведений вида* $\alpha\beta$, $\beta\alpha$, $\alpha\beta\alpha$, $\beta\alpha\beta \ldots$.

2. *Если* α *и* β *— перестановочные эквивалентности, то*

$$\{\alpha, \beta\}^e = \alpha\beta = \alpha \cup \beta$$

(последнее равенство есть утверждение теоремы 2.7).

Определение 2.12. Пусть A и B — непустые множества и $\rho \subseteq A \times B$ — непустое соответствие между ними.

Тогда *ядром соответствия* ρ называется однородное на A отношение $\operatorname{Ker}\rho$, определяемое соотношением для $a_1, a_2 \in A$.

$$a_1(\operatorname{Ker}\rho)\, a_2 \;\Leftrightarrow\; \rho(a_1) = \rho(a_2).$$

Очевидно $\operatorname{Ker}\rho$ есть эквивалентность на соответствующих множествах (наследуются свойства $=$), её называют *ядерной*. Смежные классы данной эквивалентности называются *ядрами*, используют обозначение $\operatorname{Core}(a) = [a]_{Ker\rho}$.

При задании отношения матрицей, *ядрам* будут соответствовать *совокупности одинаковых строк*.

2.4 Пространства толерантности

Определение 2.13. Однородные *рефлексивные и симметричные* отношения называют *отношениями толерантности*, символически $\simeq$, τ.

Пример 2.3. Следующие отношения τ суть толерантности.

1. A и B — точки евклидова пространства и $A\tau B \Leftrightarrow |A - B| \leqslant r > 0$.
2. Слова русского языка находятся в отношении τ, если они *отличаются не более, чем на одну букву*.

Определение 2.14. Пару $\langle A, \simeq \rangle$, где A — непустое множество, а $\simeq$ — толерантность на нём, называют *пространством толерантности*.

Пример 2.4. Пусть A — непусто и $\mathcal{P}^*(A)$ — совокупность всех его *непустых* подмножеств. Для $X, Y \in \mathcal{P}^*(A)$ положим

$$X \simeq Y \stackrel{\text{def}}{=} X \cap Y \neq \varnothing.$$

Тогда $\langle \mathcal{P}^*(A), \simeq \rangle$ — пространство толерантности.

Представление толерантности $(0,1)$*-матрицами* — матрица будет симметрична и содержать единицы на главной диагонали, а любая такая матрица — задавать толерантность.

Представление толерантности графами — как и любое бинарное отношение. При этом вершины x и y графа $G(\tau)$ при $x\tau y$ соединяют неориентированным ребром (симметричность), а петли при каждой вершине (рефлексивность) опускают.

Пример 2.5. Задание матрицей и графом толерантности на трёхэлементном множестве $\{1, 2, 3\}$:

$$M(\tau) = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \qquad 1 \text{ —— } 2 \text{ —— } 3$$

Утверждение 2.2. *Если $\simeq$ — толерантность, а $\sim$ — эквивалентность на некотором множестве такие, что $\simeq \subseteq \sim$, то $\simeq^t \subseteq \sim$.*

Доказательство: применяем операцию $\simeq^t$ к $\simeq \subseteq \sim$.

Следствие. *Транзитивное замыкание толерантности есть минимальная её включающая эквивалентность.*

Симметризованное произведение $\circ$ однородных отношений α и β:

$$\alpha \circ \beta \stackrel{\text{def}}{=} \alpha\beta \cup \beta\alpha.$$

Теорема 2.10 (*о свойствах толерантности*).

1. *Толерантность инвариантна относительно $\cup$, $\cap$, $^\sharp$, а относительно $\diamond$ — если и только если толерантности перестановочны (и в этом случае $\alpha \diamond \beta = \alpha \circ \beta$).*
2. *Толерантность инвариантна относительно $\circ$.*
3. *Если τ — толерантность, то и $\overline{\tau} \cup \triangle$ — толерантность.*
4. *Если α — рефлексивное однородное отношение, то отношения $\alpha \cup \alpha^\sharp$, $\alpha \cap \alpha^\sharp$ и $\alpha \circ \alpha^\sharp$ суть толерантности.*

Доказательство.

1. Все утверждения следуют из пп. (1) и (2) теоремы об инвариантности "положительных" свойств однородных отношений.
2. Пусть α и β — толерантности. Тогда

   R: рефлексивность $\alpha \circ \beta$ следует из рефлексивности $\alpha\beta$ и $\beta\alpha$ (п. (1) упомянутой теоремы);

   S: $(\alpha \circ \beta)^\sharp = (\alpha\beta \cup \beta\alpha)^\sharp = (\alpha\beta)^\sharp \cup (\beta\alpha)^\sharp = \\ = \beta^\sharp\alpha^\sharp \cup \alpha^\sharp\beta^\sharp = \beta\alpha \cup \alpha\beta = \alpha \circ \beta.$
3. Дополнение сохраняет свойство симметричности, но превращает рефлексивное отношение антирефлексивное.
4. Отношения, являющиеся результатами указанных операций наследуют рефлексивность α и приобретают свойство симметричности.

□

Расщепление понятий при переходе от частного к общему:

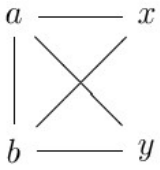
эквивалентность	$\longleftrightarrow$	ядро = класс
толерантность	$\longleftrightarrow$	ядро $\neq$ класс

Ядра толерантности суть классы $\mathrm{Core}(\cdot)$ по эквивалентности $\mathrm{Ker}\,\tau$, то есть элементы принадлежат одному ядру, если они толерантны одним и тем же элементам. Ясно, что они образуют разбиение носителя пространства толерантности.

Пример 2.6.

1. Ядра толерантности 1—2—3 суть $\{1\}$, $\{2\}$ и $\{3\}$.

2. Для толерантности



имеем
$\tau(a) = \{a, b, x, y\} = \tau(b)$, $\tau(x) = \{a, b, x\}$, $\tau(y)\{a, b, y\}$;
в результате ядрами будут
$\mathrm{Core}(a) = \mathrm{Core}(b) = \{a, b\}$, $\mathrm{Core}(x) = \{x\}$
и $\mathrm{Core}(y) = \{y\}$.

Определение 2.15. Пусть $\langle A, \tau \rangle$ — пространство толерантности.

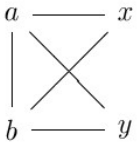
Подмножество $K \subseteq A$ называют *предклассом толерантности в* A или *τ-предклассом*, если в нём все пары элементов толерантны.

Максимальный (по включению) предкласс называют *классом толерантности в* A или *τ-классом*.

Пример 2.7. 1. Любое одноэлементное множество пространства толерантности — тривиальный пример предкласса.

2. Для толерантности 1—2—3 классы суть $K_1 = \{1, 2\}$ и $K_1 = \{2, 3\}$.

3. Для толерантности



классы толерантности суть $\{a, b, x\}$ и $\{a, b, y\}$.

Свойства толерантности[1)]

- Совокупность всех предклассов толерантности пространства $\langle A, \tau \rangle$ образует *покрытие* множества A, т. к. объединение всех одноэлементных предклассов уже образует покрытие A.
- Если задано *покрытие* непустого множества A его подмножествами, то тем самым задана и *толерантность* τ на нём: все элементы, принадлежащих данному подмножеству, считаем толерантными друг другу.

  При этом данные подмножества будут τ-классами толерантности.

Лемма 2.1. *Для всякого предкласса существует содержащий его класс.*

Доказательство для конечного случая. Рассмотрим некоторый τ-предкласс K и все τ-предклассы, его содержащие. Любая цепь вложенных друг в друга таких предклассов, начинающаяся с K, будет конечной, а заключительный предкласс будет уже классом. □

[1)] Ср. с теоремой о классах эквивалентности.

Как следствие, получаем что для всякой пары элементов пространства толерантности $\langle A, \tau \rangle$, находящихся в отношении τ, существует класс толерантности, их содержащий (эта пара элементов образует предкласс; начинаем с него).

Разложение толерантности на квадраты

Утверждение 2.3. *Если* $K_1, \ldots, K_m$ *— все классы толерантности* τ, *то*

$$\tau = \bigcup_{i=1}^{m} K_i^2.$$

Пример 2.8. Для толерантности 1—2—3:

$K_1 = \{1, 2\}$, $K_2 = \{2, 3\}$.

$K_1^2 = \{(1,1), (1,2), (2,1), (2,2)\}$,

$K_2^2 = \{(2,2), (2,3), (3,2), (3,3)\}$.

Или при задании толерантности $(0,1)$-матрицами:

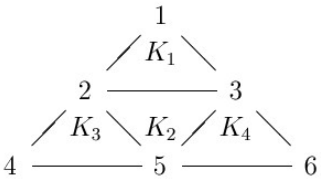
$$M(\tau) = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \vee \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Разложение толерантности на квадраты *неприводимо*, если из него нельзя исключить ни один квадрат.

Пример 2.9. Рассмотрим толерантность τ на 6-элементном множестве, задаваемую графом Классы толерантности:

$$K_1 = \{1, 2, 3\}, \quad K_2 = \{2, 3, 5\},$$
$$K_3 = \{2, 4, 5\}, \quad K_4 = \{3, 5, 6\}.$$

Разложения



- полное $\tau = K_1^2 \cup K_2^2 \cup K_3^2 \cup K_4^2$ — избыточно;
- $\tau = K_1^2 \cup K_3^2 \cup K_4^2$ — неприводимо.

Определение 2.16. *Базисом* $\mathcal{B}(\tau)$ толерантности τ на конечном множестве называется всякий *набор классов*, определяющий её неприводимое разложение на квадраты.

Толерантность может иметь *несколько базисов с различным числом входящих в них классов.*

Пример 2.10. Рассмотрим толерантность на 8-элементном множестве, заданную графом на рис. 2.3 с обозначенными классами.

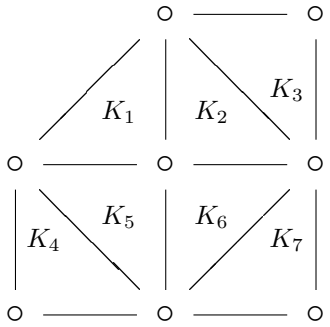


Рис. 2.3. Толерантность на 8-элементном множестве

Здесь классы
$K_1, \ldots, K_5$ и K_7 образуют 6-элементный, а классы

K_1, K_3, K_4, K_6 и K_7 — 5-элементный базисы данного пространства толерантности.

Определение 2.17. *Фактормножеством пространства толерантности* $\langle A, \tau \rangle$ *по его базису* $\mathcal{B}(\tau)$ называется множество, элементами которого являются классы из $\mathcal{B}(\tau)$ и их всевозможные (не обязательно попарные) непустые пересечения.

Обозначение: $A/\mathcal{B}(\tau)$, а в случае единственного базиса — A/τ.

Пример 2.11.

Для пространства толерантностьи 1—2—3 классы суть $K_1 = \{1, 2\}$ и $K_2 = \{2, 3\}$; они и составляют его единственный базис.

Добавив к этим классам

$$K_3 = K_1 \cap K_2 = \{2\},$$

получим *факторможество по базису* — $\{K_1, K_2, K_3\}$.

Напомним, что фактормножество по ядру есть $\{\{1\}, \{2\}, \{3\}\} = \{K_1 \setminus K_3, K_2 \setminus K_3, K_3\}$.

Понятие фактормножества пространства толерантности по его базису оказывается особенно полезном в случаях, кода базис содержит небольшое число элементов. Оно используется, в частности, при минимизации конечных автоматов.

2.5 Соответствия

Для непустых соответствий $\rho, \alpha, \beta \subseteq A \times B$ и справедливо соотношение:

$$\rho \subseteq \rho\rho^\sharp\rho.$$

Действительно,

$$a\rho b \;=\; (a\rho b)\,\&\,(b\rho^\sharp a)\,\&\,(a\rho b) \;\Rightarrow\; a(\rho\rho^\sharp\rho)b.$$

Типы соответствий

Определение 2.18. Соответствие ρ между множествами A и B называется —

- *многозначным отображением* или *всюду определённым соответствием*, если $\triangle_A \subseteq \rho\rho^\sharp$, что эквивалентно $\mathrm{Dom}\,\rho = A$;
- *частичным отображением* A *в* B, если $\rho^\sharp\rho \subseteq \triangle_B$, что эквивалентно $a\rho b_1 \,\&\, a\rho b_2 \;\Rightarrow\; b_1 = b_2$.
- *функциональным* или *отображением* A *в* B, если $\left(\triangle_A \subseteq \rho\rho^\sharp\right) \& \left(\rho^\sharp\rho \subseteq \triangle_B\right)$, что эквивалентно $\forall\, a \in A\ \exists!\, b \in B : a\rho b$;

  Отображение φ из A в B называют *функцией из* A *в* B или *операцией на* A;
- *дифункциональным* или *квазиоднозначным* отображением, если $\rho\rho^\sharp\rho \subseteq \rho$, или, по доказанному выше, $\rho\rho^\sharp\rho = \rho$.

2.6 Основные свойства отображений

Обозначения для отображений:

$$\varphi : A \to B, \quad A \xrightarrow{\varphi} B, \quad x\varphi = b.$$

Множество всех отображений $A \to B$ будем обозначать $Fun\,(A, B)$ или B^A, при $A = B$ — $Fun\,(A)$.

Пусть $\mathfrak{B} = \langle\, B, \sqcup, \sqcap, ', o, \iota \,\rangle$ — булева алгебра. Множество B^{B^n} всех функций из B^n в B образует булеву алгебру с носителем B^{B^n}, где операции и выделенные элементы заданы следующим образом:

$$\begin{aligned}
\text{объединение} &- (f \sqcup g)(a) = f(a) \sqcup g(a),\\
\text{пересечение} &- (f \sqcap g)(a) = f(a) \sqcap g(a),\\
\text{дополнение} &- (f(a))' = f'(a),\\
\text{нуль} &- \mathbf{0}(a) \equiv o,\ \text{единица} - \mathbf{1}(a) \equiv \iota,\\
&(\text{везде } a = (a_1, \ldots, a_n) \in B^n).
\end{aligned}$$

Утверждение 2.4. *Объединение [пересечение] двух отображений $\varphi\colon A \to B$ и $\psi : A \to B$ является отображением, если и только если $\varphi = \psi$.*

Доказательство. Поскольку φ и ψ — отображения из A в B, для каждого $a \in A$ φ и ψ содержат лишь по одной паре (a, b_1) и (a, b_2) соответственно, где $b_1, b_2 \in B$.

Если предположить, что $b_1 \neq b_2$, то $\varphi \cup \psi$ содержит две, а $\varphi \cap \psi$ — не содержит ни одной пары с первым элементом a. □

Отрицание отображения, очевидно, отображением не является. Т.о. применение к отображениям обычных теоретико-множественных операций *интереса не представляет.*

Утверждение 2.5. *Если множества A, B и C непусты, φ — отображение из A в B, а ψ — отображение из B в C, то $\varphi\psi$ — отображение из A в C.*

Доказательство.

$$\left\{\begin{array}{l} \triangle_A \subseteq \varphi\varphi^\sharp,\ \varphi^\sharp\varphi \subseteq \triangle_B \\ \triangle_B \subseteq \psi\psi^\sharp,\ \psi^\sharp\psi \subseteq \triangle_C \end{array}\right. \Rightarrow \quad \triangle_A \subseteq \varphi\varphi^\sharp =$$

$$= \varphi\ \triangle_B\ \varphi^\sharp \subseteq \varphi(\psi\psi^\sharp)\varphi^\sharp = (\varphi\psi)(\psi^\sharp\varphi^\sharp) = (\varphi\psi)(\varphi\psi)^\sharp.$$

$(\varphi\psi)^\sharp(\varphi\psi) \subseteq \triangle_C$ — показывается аналогично. □

Произведение функций как отображений принято записывать как их композицию $*$:

$$(\varphi * \psi)(x) = (\varphi \diamond \psi)(x) = \psi(\varphi(x)),$$

или в альтернативной нотации

$$(x\varphi)\psi = x(\varphi\psi) = x\varphi\psi.$$

Виды отображений. Единичное отношение $\triangle_A$, рассматриваемое как отображение A на себя, называют *тождественным*, для которого будем употреблять обозначение id_A.

Определение 2.19. Отображение $\varphi\colon A \to B$ называется

- *вложением* или *инъективным отображением* A *в* B, если $\mathrm{id}_A = \varphi\varphi^\sharp$, символически $A \overset{\varphi}{\hookrightarrow} B$;

при этом различные элементы A отображаются в различные элементы B.

Если $A \subseteq B$, то вложение $A \overset{\varphi}{\hookrightarrow} B$ такое, что $\varphi(x) = x$, называется *естественным вложением* множества A в множество B.

С инъекцией связан *принцип Дирихле*: *не существует инъекции множества с бóльшим числом элементов во множество с меньшим числом элементов.*

- *наложением* или *сюръективным отображением A в B, сюръекцией*, если $\varphi^\sharp\varphi = \mathrm{id}_B$, то есть каждый элемент множества B имеет свой прообраз.

  Отображения проектирования — сюръективные отображения $A_1 \times \ldots \times A_n \overset{\pi_i}{\to} A_i$, определяемые как $(a_1, \ldots, a_i, \ldots, a_n) \overset{\pi_i}{\mapsto} a_i,\ i = \overline{1,n}$.

- *биекцией* или *взаимно-однозначным отображением*, если $\bigl(\mathrm{id}_A = \varphi\varphi^\sharp\bigr)\,\&\bigl(\varphi^\sharp\varphi = \mathrm{id}_B\bigr)$, то есть оно является одновременно и вложением, и наложением.

  Множество всех биекций из A в B обозначаем $Bij\,(A, B)$, а в случае $A = B$ — $Bij\,(A)$.

Псевдообратное к отображению $\varphi\colon A \to B$ соответствие $\varphi^\sharp$, может и не быть отображением из B в A. Единственный тип отображений, имеющих обратное — биекции.

Пусть дано отображение $\varphi\colon A \to B$. Его *ядром* называется отношение $\operatorname{Ker}\varphi \in \mathcal{R}(A)$, заданное как

$$a_1(\operatorname{Ker}\varphi)a_2 \;\Leftrightarrow\; \varphi(a_1) = \varphi(a_2).$$

Ядро отображения есть частный случай понятия ядра соответствия и является *ядерной эквивалентностью*:

$$\operatorname{Ker}\varphi \;=\; \varphi\varphi^{\sharp}.$$

Покажем, что $\operatorname{Ker}\varphi$ — эквивалентность:

R: $\triangle_A \in \varphi \;\Rightarrow \triangle_A \in \varphi\varphi^{\sharp}$;
S: $(\varphi\varphi^{\sharp})^{\sharp} = (\varphi^{\sharp})^{\sharp}\varphi^{\sharp} = \varphi\varphi^{\sharp}$;
T: $(\varphi\varphi^{\sharp})^2 = \varphi\varphi^{\sharp}\varphi\varphi^{\sharp} = \varphi(\varphi^{\sharp}\varphi)\varphi^{\sharp} \subseteq \varphi\ \triangle_B\ \varphi^{\sharp} = \varphi\varphi^{\sharp}$.

Покажем, что $a_1(\varphi\varphi^{\sharp})a_2 \;\Leftrightarrow\; \varphi(a_1) = \varphi(a_2)$:

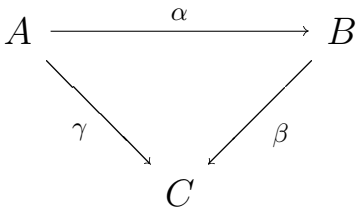
$$a_1\varphi\varphi^{\sharp}a_2 \;\Leftrightarrow\; \underset{B}{\exists}\, b : (a_1\varphi b)\ \&\ (b\varphi^{\sharp}a_2) \;\Leftrightarrow$$
$$\Leftrightarrow\; \underset{B}{\exists}\, b : (a_1\varphi b)\ \&\ (a_2\varphi b) \;\Leftrightarrow\; \varphi(a_1) = \varphi(a_2).$$

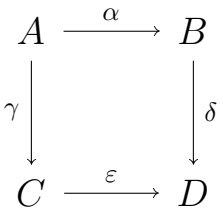
С ядерной эквивалентностью отображения φ из A связано фактормножество $A/\operatorname{Ker}\varphi$ и натуральное отображение $nat(A, \operatorname{Ker}\varphi)$, для которого $nat(A, \operatorname{Ker}\varphi)(x) = [x]_{\operatorname{Ker}\varphi}$.

Отображения $\varphi\colon A \to B$ и $nat(A, \operatorname{Ker}\varphi)$ имеют общую ядерную эквивалентность, но отображают A в разные множества: соответственно в B и в $A/\operatorname{Ker}\varphi$.

Коммутативные диаграммы. Если A, B, C, D — некоторые множества и

$$\alpha : A \to B, \quad \beta : B \to C, \quad \gamma : A \to C,$$
$$\delta : B \to D, \quad \varepsilon : C \to D,$$

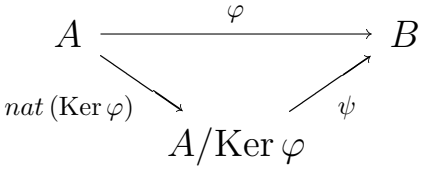




то данные отображения задают в виде диаграмм:
Говорят, что эти диаграммы коммутативны, если $\gamma = \alpha\beta$ и $\alpha\delta = \gamma\varepsilon$ соответственно. Аналогично определяется коммутативность и для более сложных диаграмм.

Биективные отображения будем обозначать на диаграммах двунаправленными стрелками $\leftrightarrow$.

Теорема 2.11 (основное свойство отображений). *Пусть даны непустые множества A, B и отображение $\varphi\colon A \to B$. Тогда имеется единственное отображение $\psi : A/\operatorname{Ker}\varphi \to B$, являющееся вложением, и такое, что нижеследующая диаграмма коммутативна:*



Доказательство. Имеем $\psi([a]_{\operatorname{Ker}\varphi}) = \varphi(a)$ — однозначно определённое вложение $\operatorname{Ker}\varphi$ в B, то есть $\varphi = \pi * \psi$. □

Основное свойство отображений: любое отображение $\varphi : A \to B$ (A и B непусты) может быть представлено в виде композиции *наложения* π и *вложения* ψ:

$$\varphi = \pi * \psi,$$

где $\pi = nat\,(\mathrm{Ker}\,\varphi)$ и $\mathrm{Ker}\,\varphi \overset{\psi}{\hookrightarrow} B$.

Очевидно ψ — *биекция* при *сюръективности* φ.

Глава 3

Частично упорядоченные множества

3.1 Предпорядки и порядки

Основные понятия

Определение 3.1. *Предпорядками* называют рефлексивные и транзитивные однородные отношения.

Пример 3.1. Предпорядками, например, являются следующие отношения:

1) отношение делимости $\mid$ на множестве $\mathbb{Z} \setminus \{0\}$;
2) отношение выводимости $\vdash$ в логике: если из логической формулы A выводится формула B, то пишут $A \vdash B$;

Определение 3.2. Антисимметричные *(AS)* предпорядки называют отношениями *частичного порядка*.

Пример 3.2. Все предпорядки из предыдущего примера не являются частичными порядками.

1. Для элементов $\mathbb{Z} \setminus \{0\}$ из $m \mid n$ и $n \mid m$ следует не $m = n$, а лишь $|m| = |n|$.

2. Возможно $A \vdash B$ и $B \vdash A$, но $A \neq B$ (формулы A и B не совпадают как строки символов): например, для $A = x \supset y$ и $B = (\neg x \vee y) \,\&\, (z \vee \neg z)$;

Пример 3.3. Частичными порядками являются:

- Отношение включения $\subseteq$ на совокупности $\mathcal{A} \subseteq \mathcal{P}(A)$ подмножеств некоторого множества A — важнейший пример частичного порядка. Говорят, что совокупность $\mathcal{A}$ *упорядочена по включению*.

  Это — важнейший пример частичного порядка.

- Отношение $\leqslant$ на множествах чисел.

- Диагональное отношение $\triangle$ на произвольном множестве можно рассматривать не только как эквивалентность, но и как частичный порядок. Множество с таким порядком называют *тривиально упорядоченным*.

Из предпорядка несложно построить порядок. Действительно, пусть на множестве P задан предпорядок $\preceq$. Отождествим элементы a и b, для которых одновременно и $a \rho b$ и $b \rho a$. Ясно, что этим будет задана некоторая эквивалентность ε на P, а на фактормножестве P/ε — частичный порядок

$$[a]_\varepsilon \leq [b]_\varepsilon \Leftrightarrow a \preceq b,$$

индуцированный предпорядоком $\preceq$.

Пример 3.4. 1. В наших обозначениях $[n]_\varepsilon = \{n, -n\}$ и частичный порядок $\leq$ есть отношение делимости $\mid$ на фактормножестве $\{\mathbb{Z} \setminus \{0\}\}/\varepsilon$.

2. Если на множестве всех логических формул $\mathcal{A}$ ввести отношение $\simeq$ *дедуктивной эквивалентности* по правилу

$$(A \vdash B) \,\&\, (B \vdash A) \;\Leftrightarrow\; A \simeq B,$$

то $\mathcal{A}/\simeq$ — фактормножество классов дедуктивно эквивалентных формул, являющееся, более того, булевой алгеброй и называемой *алгеброй Линденбаума–Тарского* (символически L^*).

- Символы отношения частичного порядка: $\sqsubseteq$, $\leqslant$, $\preccurlyeq$ ....
- Если $a \sqsubseteq b$, то говорят, что a *предшествует* b, b *следует за* a, *содержит* a.
- *Интервал*: $[a, b] = \{x \mid (a \sqsubseteq x) \,\&\, (x \sqsubseteq b)\}$.
- Если $[a, b] = \{a, b\}$, то говорят, что a *непосредственно предшествует* b и что b *непосредственно следует за* a или *покрывает*, символически $a \lessdot b$.
- Элементы a и b *сравнимы*, если $(a \sqsubseteq b) \vee (b \sqsubseteq a)$, и *несравнимы* иначе; символически $a \sim b$ и $a \nsim b$ соответственно.
- Отношение *строгого порядка*: $x \sqsubset y \;\Leftrightarrow\; x \sqsubseteq y$ и $x \neq y$,

- *Двойственный порядок*: $x \sqsupseteq y \Leftrightarrow y \sqsubseteq x$ и аналогично для строгого порядка.

Определение 3.3. Пару $\langle P, \sqsubseteq \rangle$, где P — непустое множество, а $\sqsubseteq$ — частичный порядок на нём, называют *частично упорядоченным множеством* (сокращённо *ч. у. множеством*).

Ч.у. множество представляет собой пример особого типа алгебраической системы — *модели*. АС является моделью, если в ней отсутствуют операции на носителе, но имеются отношения на нём.

Любое множество можно превратить в частично упорядоченное, задав на нём некоторый порядок. *Например*, на двухэлементном множестве $\{x, y\}$ можно построить 3 различных порядка: вместе с рефлексивностью положить $x \nsim y$ (тривиальный порядок), $x \sqsubseteq y$ и $y \sqsubseteq x$.

Пример 3.5. Ч.у. множествами являются:

- модели $\langle \mathbb{R}, \leqslant \rangle$, $\langle \mathbb{N}, \leqslant \rangle$, $\langle \mathbb{N}, | \rangle$, $\langle B^n, \preccurlyeq \rangle$ и $\langle \mathcal{P}(\cdot), \subseteq \rangle$;
- для $A \neq \varnothing$ модель $\langle \mathcal{E}(A), \subseteq \rangle$ есть ч. у. множество, состоящее из разбиений множества A (имея в виду взаимно-однозначную связь между разбиениями множества и отношениями эквивалентности на нём); при этом говорят, что A *упорядоченно по измельчению*.

Если на множестве P заданы порядки $\sqsubseteq_1$ и $\sqsubseteq_2$ и $\sqsubseteq_1 \subseteq \sqsubseteq_2$ (из $x \sqsubseteq_1 y$ следует $x \sqsubseteq_2 y$ для всех

$x, y \in P$), то говорят, что *порядок* $\sqsubseteq_1$ *содержится в порядке* $\sqsubseteq_2$. При построении порядка, содержащего данный, говорят о *продолжении* последнего. *Например*, тривиальный порядок на неодноэлементном множестве содержится в любом другом и может быть продолжен до него.

В зависимости от мощности P различают *конечные* и *бесконечные* ч. у. множества.

Бесконечное ч.у. множество, все *интервалы* которого конечны, называется *локально конечным*. *Например*, ч. у. множества $\langle \mathbb{N}, \leqslant \rangle$ и $\langle \mathbb{Q}, \leqslant \rangle$ бесконечны, но первое локально конечно, а второе — нет.

Определение 3.4. Если любые два элемента неединичного ч. у. множества P сравнимы, то оно называется *линейно упорядоченным* или *цепью*.

Для линейного порядка будем использовать обозначение $\leqslant$.

- n-элементную цепь будем обозначать $\mathbf{n}$. *Длина цепи* $\mathbf{n}$ есть число $n-1$.
- Цепь $v_1 < \ldots < v_n$ будем записывать как $[v_1, \ldots, v_n]$. Обозначим $[n] = [1, \ldots, n]$.
- Цепь в ч. у. множестве называется *максимальной* или *насыщенной*, если её объединение с любым, не принадлежащим ей элементом, цепью не является.

  Например, B^n содержит $n!$ максимальных цепей.

Диаграммы Хассе — используют для наглядного представления ч. у. множеств. На них изображают элементы ч. у. множеств, и, если элемент a предшествует элементу b, то a рисуют ниже b и соединяют их отрезком, если это предшествование непосредственное.

Диаграмма Хассе *не есть* представление ч. у. множества в виде направленного графа.

Рис. 3.1. Диаграммы 3-элементных ч. у. множеств

Точных эффективных (не содержащих суммирования и не подразумевающих перебора всех или почти всех элементов) формул для числа неизоморфных диаграмм, помеченных частичных порядков и предпорядков соответственно на n-элементном множестве неизвестно и вряд ли они существуют.

Множество всех ч. у. множеств структурно необозримо: неизвестно никакой удобной его характеризации. В нём выделяют лишь отдельные классы, которые, с одной стороны — в сумме далеко не исчерпывают всех ч. у. множеств, а с другой — сами содержат ч. у. множества с трудно определяемыми характеристиками.

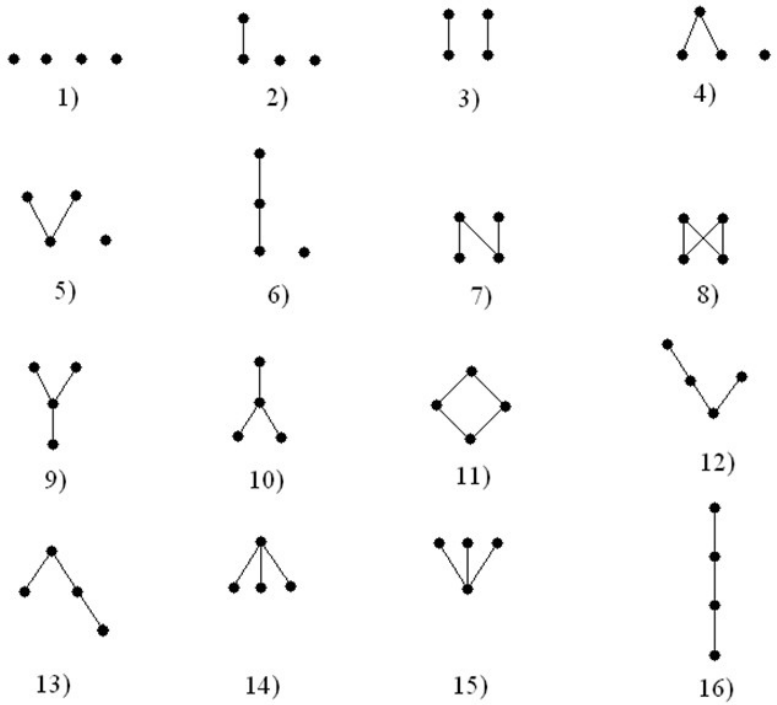


Рис. 3.2. Диаграммы всех 4-элементных ч. у. множеств

3.2 Особые элементы и основные свойства ч. у. множеств

Особые элементы

Определение 3.5. Элемент u ч. у. множества $\langle P, \sqsubseteq \rangle$ называют:

- *максимальным*, если $u \sqsubseteq x \Rightarrow u = x$,
- *минимальным*, если $u \sqsupseteq x \Rightarrow u = x$,
- *наибольшим*, если $x \sqsubseteq u$,
- *наименьшим*, если $x \sqsupseteq u$

для любых $x \in P$.

Ч.у. множество может иметь не более, чем по одному наибольшему и наименьшему элементу. Их называют соответственно *единицей* (ι) и *нулём* (o), а также *универсальными гранями* данного ч. у. множества. Если ч. у. множество имеет обе универсальные грани, то оно называется *ограниченным*.

Ясно, что наибольший элемент, если он есть, одновременно является и максимальным и обратное не верно: максимальных элементов может быть несколько. Аналогично для наименьшего и минимальных элементов.

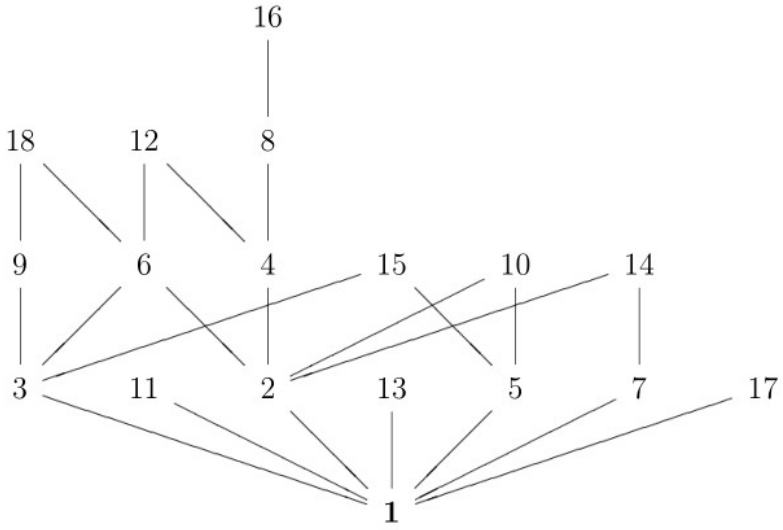
Пример 3.6 (*особые элементы ч. у. множеств*).

1. Рассмотрим ч. у. множество $\langle N_f^1, \preccurlyeq \rangle$,
   где N_f^1 — множество единичных наборов монотонной булевой функции
   $f(x_1, \ldots, x_5) = x_1 \vee x_2x_3 \vee x_3x_4x_5$.

   Для N_f^1

   - нижние единицы (10000), (01100) и (00111) функции f — *минимальные* элементы,
   - $\widetilde{1} = (11111)$ — *наибольшим* элементом,
   - наименьший элемент отсутствует.

2. Диаграмма ч. у. множества $\langle \{1, \ldots, 18\}, | \rangle$:
   1 — наименьший элемент, $10, \ldots, 18$ — максимальные, а наибольшего элемента нет.



3. В ограниченном ч. у. множестве $\langle \mathcal{P}(A), \subseteq \rangle$ наименьшим элементом является пустое множество $\varnothing$, а наибольшим — само множество A.
4. Во множестве $\mathcal{P}^*(A)$ всех непустых подмножеств непустого множества A при $|A| > 1$ нет наименьшего элемента, а минимальными являются все *одноэлементные подмножества*.

Утверждение 3.1 (*о максимальных и минимальных элементах конечного ч. у. множества*). *В конечном ч. у. множестве каждый элемент содержится в некотором максимальном элементе и содержит некоторый минимальный элемент.*

Доказательство. Пусть x — произвольный элемент ч. у. множества $\langle P, \sqsubseteq \rangle$. Если x не максимален, то найдётся такой элемент $x_1 \in P$, что $x \sqsubseteq x_1$. Повторяя рассуждения для новых элементов, получаем возрастающую цепь $x \sqsubseteq x_1 \sqsubseteq \ldots$.

Поскольку множество P конечно, то и данная цепь конечна, а её последний элемент x_n, по определению будет максимальным элементом P и $x \sqsubseteq x_n$.

Нахождения минимального элемента аналогично, при этом строится убывающая цепь. □

Определение 3.6. *Высотой* ч. у. множества P, символически $h(P)$, называют длину самой длинной его цепи.

Высотой элемента v (символически $h(v)$) в конечном упорядоченном множестве называется наибольшая из длин цепей $[v_0, \ldots, v]$, где v_0 — минимальный элемент.

n-элементное тривиально упорядоченное ч. у. множество будем обозначать $n\mathbf{1}$.

Антицепи в ч. у. множестве

Определение 3.7. *Антицепь* есть непустое подмножество A ч. у. множества P, в котором любые два элемента несравнимы.

Антицепь, перестающая быть таковой при добавлении к ней произвольного элемента, называют *насыщенной*.

Максимальной называют антицепь с наибольшим числом элементов.

Например, в ч. у. множестве $\langle \mathbb{N}, | \rangle$ антицепью является произвольное подмножество попарно некратных чисел, а в множестве $\langle B^n, \preccurlyeq \rangle$ — совокупности верхних нулей либо нижних единиц некоторой

(не тождественной константам) монотонной булевой функции.

Проблема Дедекинда — задача определения количества $\psi(n)$ антицепей в B^n, ей посвящена обширная литература. Таблица первых значений $\psi(n)$:

n	1	2	3	4	5	6
$\psi(n)$	3	6	20	168	7 581	7 828 354

Точной формулы для $\psi(n)$ неизвестно и вряд ли она существует; однако, найдена асимптотика: например, для чётных n для $\psi(n)$ справедливо

$$\psi(n) \sim 2^{\binom{n}{n/2}} e^{\binom{n}{n/2-1}\left(\frac{1}{2^{n/2}}+\frac{n^2-2n}{2^{n+5}}\right)}.$$

(по ней, например, $\psi(6) \approx 7\,996\,118$).

Шириной ч. у. множества P, символически $w(P)$, называют мощность его максимальной антицепи.

Используя понятия высоты и ширины ч. у. множества можно показать, что в ч. у. множестве из $uv+1$ элементов есть либо цепь из $u+1$ элементов, либо антицепь из $v+1$ элементов.

Цепное условие Жордана–Дедекинда. *Все насыщенные цепи между двумя данными элементами локально конечного ч. у. множества имеют одинаковую длину.*

Определение 3.8. Если ч. у. множество P удовлетворяет условию Жордана–Дедекинда и имеет наименьший элемент, то говорят, что P — *градуированное (ранжированное).*

Для градуированных множеств существует единственная определённая на их элементах *ранговая функция* ρ такая, что $\rho(x) = 0$, если x — минимальный элемент и $\rho(y) = \rho(x) + 1$, если $x \lessdot y$.

Если $\rho(x) = k$, то говорят, что элемент x *имеет ранг* k. Элементы одного ранга образуют *слой* ч. у. множества. Например, ч. у. множество $\langle \mathbb{N}, | \rangle$ ранжировано: $\rho(1) = 0$ и его k-й $(k > 0)$ слой состоит из всех натуральных чисел, примарное разложение которых содержит k простых сомножителей, не обязательно различных.

Мощность W_k k-го слоя ранжированного ч. у. множества — *число Уитни*. Слой градуированного есть насыщенная антицепь; обратное неверно:

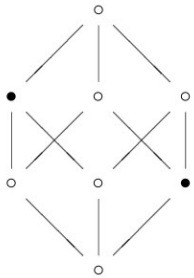


Рис. 3.3. Два элемента • — насыщенная антицепь

***LYM*-свойство.** Конечное градуированное ч. у. множество P с ранговой функцией ρ обладает *LYM-свойством* (Любеля-Ямамото-Мешалкина), если неравенство

$$\sum_{x \in A} \frac{1}{W_{\rho(x)}} \leqslant 1$$

выполняется для любой антицепи A в P.

Например, ч. у. множество на рис. 3.4 не обладает LYM-свойством: для выделенной антицепи имеем

$$2 \cdot \frac{1}{3} + 2 \cdot \frac{1}{3} = \frac{4}{3} > 1.$$

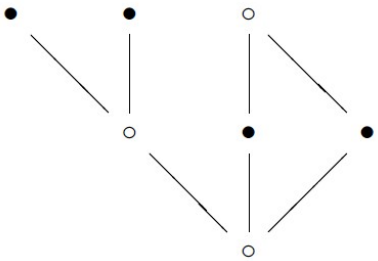


Рис. 3.4. 3-слойное ч. у. множество

В то же время справедлива

Теорема 3.1. *B^n обладает LYM-свойством.*

Доказательство. Пусть A — некоторая антицепь в кубе B^n, k-й в котором будем обозначать B_k^n.

Переходя от суммирования по элементам антицепи к суммированию по слоям B^n получим, что необходимо показать справедливость

$$\sum_{x \in A} \frac{1}{W_{\rho(x)}} = \sum_{k=0}^{n} \frac{|A \cap B_k^n|}{C_n^k} \leqslant 1.$$

Рассмотрим множество всех $n!$ насыщенных цепей, содержащих наборы $(0, \ldots, 0)$ и $(1, \ldots, 1)$. Каждая такая цепь содержит не более одного элемента антицепи A. В то же время, через любую вершину на

k-м слое куба B^n проходит ровно $k!(n-k)!$ рассматриваемых цепей. Поэтому

$$\sum_{k=0}^{n} |A \cap B_k^n| \cdot k!(n-k)! \leqslant n!$$

Разделив обе части неравенства на $n!$, получаем требуемое. □

Теорема 3.2. *Минимальное число антицепей, на которые может быть разбито конечное ч. у. множество P, есть $h(P)+1$ (наибольшая мощность цепи в P).*

Доказательство. Если $h(P) = 0$, то P — тривиально упорядоченное множество, то есть антицепь. Пусть $h(P) \geqslant 1$ и теорема справедлива для $h-1$. Обозначим через A_1 множество максимальных элементов P. Поскольку A_1 — антицепь, и $P' = P \setminus A_1$ имеет высоту $h-1$ (т. к. из каждой максимальной цепи было удалено по элементу), то ч. у. множество P' может быть разложено в антицепи $A_2, \ldots, A_{h+1}$ и $P = A_1 + \ldots + A_{h+1}$ — искомое разбиение. □

Атомы ч. у. множеств. Если ч. у. множество имеет наименьший элемент, то элементы, непосредственно следующие за ним, называют *атомами*.

Двойственно определяются *коатомы*: это элементы, непосредственно предшествующие наибольшему элементу.

Пример 3.7. 1. Конечная нетривиальная цепь содержит единственные атом и коатом.

2. В цепи $[0, \ldots, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, 1]$ атомы отсутствуют.

3. Положим формально, что $0|0$. Тогда в ч. у. множестве $\langle \mathbb{N}_0, | \rangle$ наименьшим элементом является 1, наибольшим — 0, атомы суть простые числа, а коатомы отсутствуют.

Трёхслойные ч. у. множеств. Ч.у. множество P, все элементы которого находятся в трёх непересекающихся антицепях X_1, X_2 и X_3 таких, что

- $|X_1| \approx |X_3| \approx |P|/4$;
- для всех $a \in X_1$, $c \in X_3$ имеет место $a < c$ (то есть все элементы из X_3 содержат все элементы X_1);
- если $a < b$ и $a \in X_i$, $b \in X_j$, то $i < j$.

называют *трёхслойным*.

Введём равномерное распределение вероятности на множестве всех n-элементных ч. у. множеств.

Теорема 3.3. *При $n \to \infty$ с вероятностью 1 все n-элементные ч. у. множества являются трёхслойными.*

Этот результат радикально расходится с обычным представлением о «типичном» ч. у. множестве.

3.3 Грани, изотонные отображения и порядковые идеалы

Определение 3.9. Пусть $\langle P, \sqsubseteq \rangle$ — ч. у. множество и $A \subseteq P$.
Множества $A^{\triangle}$ и $A^{\triangledown}$ определяемые условиями

$$A^{\triangle} = \{x \in P \mid \forall a \in A : a \sqsubseteq x\} \text{ и}$$
$$A^{\triangledown} = \{x \in P \mid \forall a \in A : x \sqsubseteq a\}.$$

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

Если $A = \{a\}$ одноэлементно, то пользуются обозначениями $a^{\triangle}$ и $a^{\triangledown}$.

Из определения вытекают следующие основные свойства верхнего и нижнего конусов. Пусть $\langle P, \sqsubseteq \rangle$ — ч. у. множество, $A, B \subseteq P$ и $x, y \in P$. Тогда

1. $A \subseteq B \Rightarrow B^{\triangledown} \subseteq A^{\triangledown}$ и $B^{\triangle} \subseteq A^{\triangle}$;
2. $(A \cup B)^{\triangle} = A^{\triangle} \cap B^{\triangle}$; $(A \cup B)^{\triangledown} = A^{\triangledown} \cap B^{\triangledown}$;
3. $x \sqsubseteq y \Leftrightarrow x^{\triangledown} \subseteq y^{\triangledown}$.

Определение 3.10. Пусть $\langle P, \sqsubseteq \rangle$ — ч. у. множество и $A \subseteq P$.

Если в $A^{\triangle}$ существует наименьший элемент, то он называется *точной верхней гранью множества* A и обозначается $\sup A$.

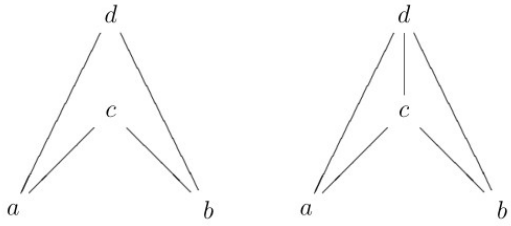


Рис. 3.5. Два порядка на $\{a, b, c, d\}$

Если в $A^{\triangledown}$ существует наибольший элемент, то он называется *точной нижней гранью множества* A и обозначается $\inf A$.

Пример 3.8. 1. Пусть $P = \{a, b, c, d\}$ и два различных порядка на P задаются диаграммами на рис. 3.5: Для $A = \{a, b\}$ на рис. 3.5 имеем $A^{\triangle} = \{c, d\}$ в обоих случаях, но в первом $\sup A$ отсутствует, а во втором $\sup A = c$ [1)].

2. Если S — совокупность подмножеств некоторого множества, то, по включению, $\sup S$ совпадает с объединением, а $\inf S$ — с *пересечением* всех подмножеств из совокупности S.

Отображения ч. у. множеств

Определение 3.11. Пусть $\langle P, \sqsubseteq_P \rangle$ и $\langle Q, \sqsubseteq_Q \rangle$ — ч. у. множества и x, y — произвольные элементы из P.
Отображение $\varphi\colon P \to Q$ называется соответственно

[1)] вторая диаграмма не есть диаграмма Хассе: линии, соединяющие d с a и b здесь излишни

- *изотонным*, (*монотонным*, *порядковым гомоморфизмом*), если

$$x \sqsubseteq_P y \;\Rightarrow\; \varphi(x) \sqsubseteq_Q \varphi(y);$$

- *обратно изотонным*, если

$$\varphi(x) \sqsubseteq_Q \varphi(y) \;\Rightarrow\; x \sqsubseteq_P y;$$

- *антиизотонным*, если

$$x \sqsubseteq_P y \;\Rightarrow\; \varphi(x) \sqsupseteq_Q \varphi(y).$$

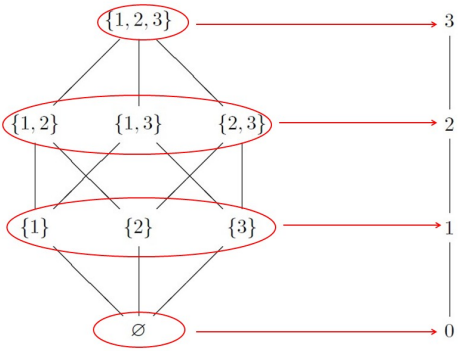
- Если φ *изотонно, обратно изотонно и инъективно*, то его называют *вложением* или *(порядковым) мономорфизмом* ч. у. множества P в ч. у. множество Q, что обозначают $P \overset{\varphi}{\hookrightarrow} Q$.

- Сюръективный мономорфизм ч. у. множеств называют *(порядковым) изоморфизмом*, символически $P \cong Q$ или $P \overset{\varphi}{\cong} Q$.
  Ясно, что φ — биекция и для любых $x, y \in P$ справедливо

$$x \sqsubseteq_P y \;\Leftrightarrow\; \varphi(x) \sqsubseteq_Q \varphi(y).$$

- Изоморфизм ч. у. множества в себя называют *(порядковым) автоморфизмом*.

- Если отображение $\varphi\colon P \to Q$ между носителями ч. у. множеств P и Q биективно и для любых $x, y \in P$ справедливо $x \sqsubseteq_P y \;\Leftrightarrow\; \varphi(x) \sqsupseteq_Q \varphi(y)$, то говорят, что P и Q *антиизоморфны*.



Примеры 3.1. 1. Отображение $\mathcal{P}(\{1,2,3\}) \xrightarrow{\varphi} \mathbf{4}$, $\varphi(x) = |x|$ — *изотонно, но не инъективно* и, следовательно, вложением не является.

2. Тождественное отображение $\langle \mathbb{N}, | \rangle$ в $\langle \mathbb{N}, \leqslant \rangle$ *изотонно, но не обратно изотонно* и, следовательно, вложением также не является.

3. Если P — неодноэлементное ч. у. множество с *тривиальным порядком*, а P' — то же самое множество *с произвольным нетривиальным порядком*, то тождественное отображение P на себя является *изотонным* и *взаимнооднозначным*, но *не обратно изотонным*.

4. Отображение $\mathcal{P}(X) \xrightarrow{\varphi} \mathcal{P}(X)$, $\varphi(A) = \overline{A}$, $A \subseteq X \neq \varnothing$ *антиизотонно*.

Порядковые идеалы и фильтры

Определение 3.12. Пусть $\langle P, \sqsubseteq \rangle$ — ч. у. множество. Подмножество I элементов P называется его *порядковым идеалом*, если

$$(x \in I) \,\&\, (y \sqsubseteq x) \;\Rightarrow\; y \in I.$$

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

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

Согласно определению, $\varnothing$ — порядковый идеал любого ч. у. множества.

Из определения следует, что объединение и пересечение порядковых идеалов есть порядковый идеал.

Понятно, что $x^{\triangledown}$ и $x^{\triangle}$ — порядковый идеал и фильтр соответственно, $x \in P$. Такие идеалы и фильтры называют *главными*.

Обозначения:

- $J(P)$ — множество всех порядковых идеалов ч. у. множества $\langle P, \sqsubseteq \rangle$, упорядоченное по включению — также ч. у. множество.

  Крайние случаи: если P — n-элементные

  цепь — $J(\mathbf{n}) \cong (\mathbf{n}+\mathbf{1})$;
  антицепь — $J(n\mathbf{1}) \cong B^n$.

- $J_0(P)$ — совокупность всех главных порядковых идеалов ч. у. множества P, упорядоченное по включению — также ч. у. множество.
  Понятно, что $J_0(P) \subseteq J(P)$.

Теорема 3.4 (о представлении ч. у. множеств). *Любое ч. у. множество P изоморфно $J_0(P)$ и, следовательно, может быть вложено в булеан подходящего множества.*

Доказательство. Пусть $\langle P, \sqsubseteq \rangle$ — ч. у. множество.

Докажем, что $\varphi(x) = x^{\triangledown}$ — искомый изоморфизм.

1) Покажем, что φ — *биекция*.

а) φ — *вложение*, поскольку

$$\varphi(x) = \varphi(y) \Leftrightarrow (x^{\triangledown} = y^{\triangledown}) \Leftrightarrow$$
$$\Leftrightarrow (x^{\triangledown} \subseteq y^{\triangledown}) \,\&\, (y^{\triangledown} \subseteq x^{\triangledown}) \Leftrightarrow$$
$$\Leftrightarrow (x \sqsubseteq y) \,\&\, (y \sqsubseteq x) \Leftrightarrow x = y\,.$$

б) φ — *наложение*, т. к. каждому главному идеалу $x^{\triangledown}$ соответствует порождающий его элемент x.

2) Изотонность и обратная изотонность φ устанавливается свойств нижнего конуса:

$$x \sqsubseteq y \Leftrightarrow x^{\triangledown} \subseteq y^{\triangledown} \Leftrightarrow \varphi(x) \subseteq \varphi(y).$$

Таким образом, $P \overset{x^{\triangledown}}{\cong} J_0(P) \overset{\mathrm{id}}{\hookrightarrow} J(P) \overset{\mathrm{id}}{\hookrightarrow} \mathcal{P}(P)$. □

Между антицепями и порядковыми идеалами конечного ч. у. множества существует взаимнооднозначное соответствие.

Пусть $\langle P, \sqsubseteq \rangle$, A — антицепь в P, $I \in J(P)$. Если $I = \bigcup_{a \in A} a^{\triangledown}$, то говорят, что A порождает I. В случае $A = \{a_1, \ldots, a_k\}$ пишут $I = \langle a_1, \ldots, a_k \rangle$ и говорят, что идеал I *конечнопорождённый*.

3.4 Операции над ч. у. множествами

Двойственность. Ч.у. множества $\langle P, \sqsubseteq \rangle$ и $\langle P, \sqsubseteq \rangle$ называют *двойственным* или *дуальным*.

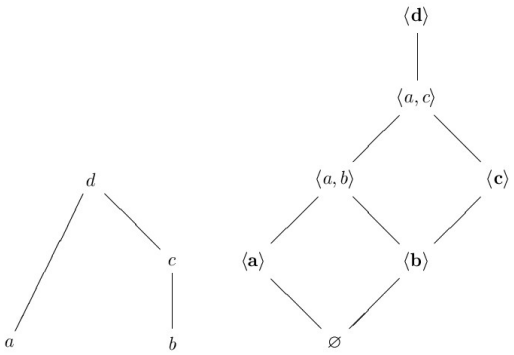


Рис. 3.6. Ч.у. множества P и $J(P)$; подмножество $J_0(P)$ выделено.

Если $P \cong P^\sharp$, то P — *самодвойственное* ч. у. множество.

Принцип двойственности для ч. у. множеств: Любое утверждение, истинное для произвольных элементов ч. у. множества, остаётся таковым в ч. у. множестве, дуальном к нему при замене $\sqsubseteq \leftrightarrow \sqsupseteq$.

Пересечение. Если $\langle P, \sqsubseteq_1 \rangle$ и $\langle P, \sqsubseteq_2 \rangle$ — два ч. у. множества с общим носителем, то их *пересечением* будет ч. у. множество $\langle P, \sqsubseteq_1 \cap \sqsubseteq_2 \rangle$.

Свойства ч. у. множеств могут не сохраняются при пересечении, например свойство «быть линейным порядком»: пусть P — цепь, тогда $P^\sharp$ — также цепь, а $P \cap P^\sharp$ — тривиально упорядоченное множество.

Прямая сумма. Если $\langle P, \sqsubseteq_P \rangle$ и $\langle Q, \sqsubseteq_Q \rangle$ — два ч. у. множества, $P \cap Q = \varnothing$, то их *прямой суммой*, символически $P + Q$, называется множество $P \cup Q$ с частичным порядком $\sqsubseteq$ таким, что

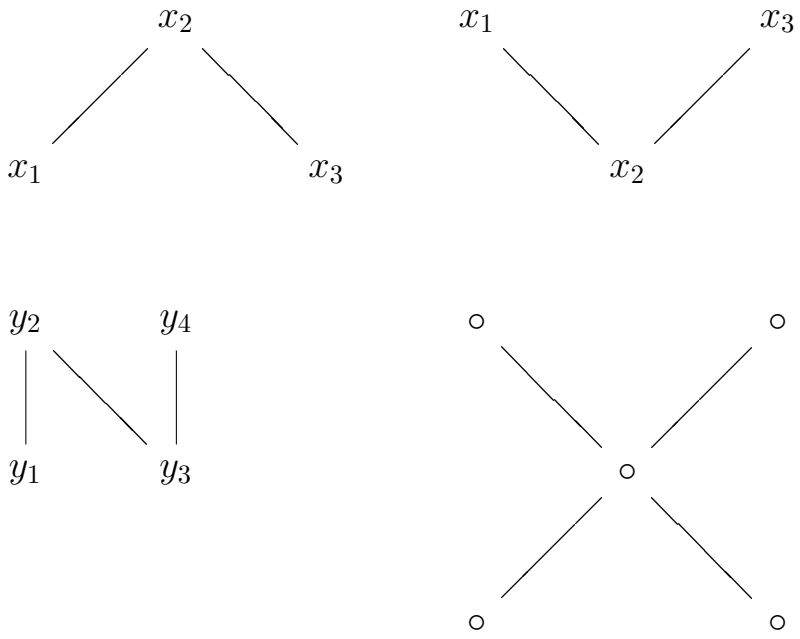


Рис. 3.7. Зигзаги или заборы Z_3 (или Λ;) $Z_3^\sharp$ (или V); Z_4 (или N) двойственны друг другу. Под ними — самодвойственные ч. у. множества (первое — N)

$$x \sqsubseteq y \Leftrightarrow (x \sqsubseteq_P y) \vee (x \sqsubseteq_Q y).$$

Диаграмма прямой суммы состоит из двух диаграмм соответствующих ч. у. множеств, рассматриваемых как единая диаграмма.

Обозначение: $\underbrace{P + \ldots + P}_{n} \cong nP$.

Любая n-элементная антицепь изоморфна $n\mathbf{1}$.

Порядковая сумма. Если $\langle P, \sqsubseteq_P \rangle$ и $\langle Q, \sqsubseteq_Q \rangle$ — два ч. у. множества, $P \cap Q = \varnothing$, то их *порядковой суммой*, символически $P \oplus Q$, называется множество

$P \cup Q$ с частичным порядком $\sqsubseteq$ таким, что

$$x \sqsubseteq y \Leftrightarrow \left[\begin{array}{l} x \sqsubseteq_P y, \\ x \sqsubseteq_Q y, \\ x \in P,\ y \in Q. \end{array}\right.$$

Ясно, что операция $\oplus$ ассоциативна, но не коммутативна. Обозначение: $\mathbf{n} \cong \underbrace{\mathbf{1} \oplus \ldots \oplus \mathbf{1}}_{n}$.

Диаграмма порядковой суммы $P \oplus Q$ состоит из диаграмм соответствующих ч. у. множеств, причём диаграмма P располагается под диаграммой Q, и между ними добавлены отрезки, соединяющие максимальные элементы P с минимальными элементами Q.

Пример см. на рис. 3.8.

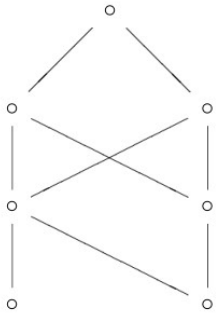


Рис. 3.8. Порядковая сумма $Z_4 \oplus Z_3$

Прямое произведение. Если $\langle P, \sqsubseteq_P \rangle$ и $\langle Q, \sqsubseteq_Q \rangle$ — два ч. у. множества, то их *прямым* или *декартовым произведением* называется множество $P \times Q$ с частичным порядком $\sqsubseteq$ таким, что

$$(p, q) \sqsubseteq (p', q') \Leftrightarrow (p \sqsubseteq_P p') \& (q \sqsubseteq_Q q').$$

Легко видеть, что $P \times Q \cong Q \times P$.
Обозначение: $P^n = P \times \ldots \times P$.
Справедливо соотношение

$$P \times R \cong Q \times R \;\Rightarrow\; P \cong Q\,, \quad \text{откуда}$$
$$P^n \cong Q^n \;\Rightarrow\; P \cong Q.$$

Построение диаграммы ч. у. множества $P \times Q$:

1) строят диаграмму ч. у. множества P;
2) отбрасывают отрезки между элементами P;
3) заменяют каждый элемент x диаграммой Q_x;
4) соединяют отрезками копии элементов из Q в Q_x и Q_y, если x непосредственно предшествует y.

Пример см. на рис. 3.9.

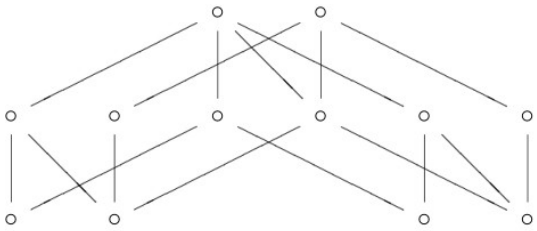


Рис. 3.9. Прямое произведение $Z_3 \times Z_4$

Диаграммы изоморфных ч. у. множеств $P \times Q$ и $Q \times P$ обычно выглядят совершенно не похожими друг на друга.

Если ч. у. множества P и Q градуированы и их ранговые функции суть ρ_P и ρ_Q, то их прямое произведение также градуировано. При этом

$$\rho\left((x_1, x_2)\right) = \rho_P(x_1) + \rho_Q(x_2).$$

Для чисел Уитни W_k справедливо равенство

$$W_k(P \times Q) = \sum_{i=0}^{k} W_i(P) \cdot W_{k-i}(Q).$$

Отсюда следует известное равенство $W_k(\mathbf{2}^n) = C_n^k$.

Если два ч. у. множества обладают *LYM*-свойством, то их прямое произведение этим свойством может и не обладать.

Определение 3.13. *Мультипликативной размерностью* ч. у. множества P называется наименьшее число k линейных порядков L_i таких, что существует вложение $P \hookrightarrow L_1 \times \ldots \times L_k$.

Степень. Если $\langle P, \sqsubseteq_P \rangle$ и $\langle Q, \sqsubseteq_Q \rangle$ — два ч. у. множества, то обозначим через Q^P множество всех изотонных отображений из P в Q. $\langle Q^P, \sqsubseteq \rangle$ — ч. у. множество с порядком $\sqsubseteq$ для $f, g \in Q^P$ таким, что

$$f \sqsubseteq g \Leftrightarrow \forall x \in P : f(x) \sqsubseteq_Q g(x).$$

Легко показывается справедливость соотношения

$$\mathbf{2^n} \cong (\mathbf{n+1}).$$

(мы заключаем $\mathbf{n+1}$ в скобки, чтобы отличить n+1-элементную цепь от прямой суммы n-элементной цепи и тривиального ч. у. множества). Действительно, $\mathbf{2^n} \cong [f_0, \ldots, f_n]$, и данные функции задаются таблицами значений

$f(x) \diagdown x$	1	2	...	$n-2$	$n-1$	n
$f_0(x)$	0	0	...	0	0	0
$f_1(x)$	0	0	...	0	0	1
$f_2(x)$	0	0	...	0	1	1
...	...	...	...	...	...	...
$f_n(x)$	1	1	...	1	1	1

Арифметика ординалов

- Для ч. у. множеств — P и произвольных Q и R справедливо

$$R^P \cong R^Q \Rightarrow P \cong Q, \quad (Q^P)^\sharp \cong (Q^\sharp)^{P^\sharp}.$$

- Для введённых операций $+$, $\times$ над ч. у. множествами выполняются законы ассоциативности, коммутативности и первый дистрибутивный закон —

$$P \times (Q + R) \cong (P \times Q) + (P \times R),$$

и для степени — соотношения

$$R^{P+Q} \cong R^P \times R^Q, \ (P^Q)^R \cong P^{Q \times R},$$
$$(P \times Q)^R \cong P^R \times Q^R.$$

- Также справедливы соотношения для «единицы»:

$$\mathbf{1} \times P \cong P, \quad \mathbf{1}^P \cong \mathbf{1}.$$

- Важное для практических приложений соотношение —

$$\mathbf{n}^P \cong \left(\mathbf{2^{n-1}}\right)^P \cong \mathbf{2}^{P \times (\mathbf{n-1})}.$$

3.5 Линеаризация

Принцип продолжения порядка

Теорема 3.5 (*Шпильрайн-Дашник-Миллер*, принцип продолжения порядка).

1. *Любой частичный порядок на том же множестве может быть продолжен до линейного, который называют его линейным продолжением).*
2. *Каждый порядок есть пересечение всех своих линейных продолжений.*

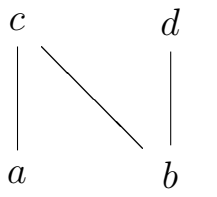
Доказательство для конечного случая. Пусть $\langle P, \sqsubseteq \rangle$ — ч. у. множество и P — не цепь. Построим линейный порядок $\leqslant$, содержащий данный частичный.

В P найдутся несравнимые элементы a и b. Произвольно определим порядок на них: 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.

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. □



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

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

Рис. 3.10. Ч. у. множество Z_4 и 5 его линейных расширений

Линейный порядок $\leqslant$, включающий в себя данный частичный порядок $\sqsubseteq$ (то есть $\sqsubseteq \subseteq \leqslant$) на некотором множестве, называют *линеаризацией* или *линейным продолжением* исходного порядка[2)]. В современной аксиоматической теории множеств принцип продолжения порядка играет роль, сопоставимую с аксиомой выбора.

Обозначение: $\mathcal{L}(P)$ — совокупность всех линейных продолжение ч. у. множества P. По принципу продолжения порядка:

$$P = \bigcap_{L \in \mathcal{L}(P)} L.$$

[2)] Показано, что любое отношение без циклов может быть продолжено до линейного порядка.

Поиск такого продолжения для конечных ч. у. множеств, заданных парами непосредственно следующих друг за другом вершин в теоретическом программировании называют *топологической сортировкой*[3)].

Алгоритмы, решающие данную задачу за *линейное время* появились лишь в начале нашего века.

Счётно-бесконечные ч. у. множества такие, что нижние конусы любых элементов конечны, называется *казуальными*. Примерами являются $\langle \mathbb{N}, \leqslant \rangle$, $\langle \mathbb{N}, | \rangle$.

Алгоритм построения линейного расширения казуального ч. у. множества P

1) Выделяем множество M_1 минимальных элементов P и произвольно его линейно упорядочиваем;
2) Рассматриваем множество $P_1 = P \setminus M_1$; множество его минимальных элементов — M_2;
3) Произвольно линейно упорядочиваем элементы из M_2;
4) и т. д.

(среди множеств M_1, M_2, ... могут быть и бесконечные).

[3)] Термин крайне неудачен: указанная процедура не имеет никакого отношения ни к сортировке (упорядочение элементов в списке по возрастанию/убыванию значений какого-либо атрибута), ни к топологии (раздел математики, изучающий в самом общем виде понятие непрерывности).

Например, при построении линейного расширения казуального множества $\langle \mathbb{N}, | \rangle$ минимальным элементом будет 1, затем в произвольном порядке на каждом шаге располагаем все простые числа, потом в произвольном порядке — все числа, представимые в виде произведения *двух* (не обязательно неравных) простых, *трёх* простых и т.д.

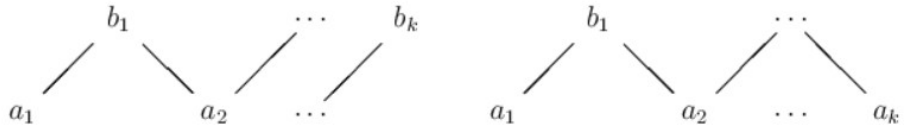
Известны эффективные алгоритмы построения *всех* линейных расширений конечного ч. у. множества.

Число скачков в некотором линейном расширении L ч. у. множества P есть минимальное количество пар несравнимых элементов P в L. Например, линеаризации $[b, d, a, c]$ зигзага Z_4 (см.рис. 3.10) один скачок — пара (d, a). Все остальные линеаризации имеют два скачка. Задача нахождения линейного расширения ч. у. множества с минимальным числом скачков NP-трудна.

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.

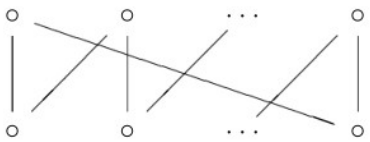
Ранее уже были указаны ч. у. множества, называемые *заборами*. Обобщим это понятие: *заборами* или *зигзагами* будем называть двудольные ч. у. множества, состоящие из $n > 2$ элементов $\{v_1, \ldots, v_n\}$ с отношениями включения $v_{2i-1} \lessdot v_{2i}$ и $v_{2i} \gtrdot v_{2i+1}$

(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.



a) Z_{2k} *b)* Z_{2k-1}

Если в $2n$-элементном заборе при $n \geqslant 3$ добавить условие «*последний элемент покрывает первый*», то получим *малую корону* $\mathbf{S}_n$:



Полная корона S_n — это $2n$-элементное двудольное ч. у. множество, то есть $S_n = A \cup B$, 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 $b_j \in B$ полагают $a_i \sqsubseteq b_j$ для всех $i \neq j$, $i, j = 1, \ldots, n$ (и, естественно, $\sqsubseteq$ рефлексивен).

Число всевозможных линеаризаций конечного ч. у. множества P обозначают $e(P)$. Это число может

интерпретироваться как некоторая оценка сложности P. Ясно, что $e(n\mathbf{1}) = n!$, $e(C) = 1$ для цепи C и это максимально и минимально возможные значения $e(\cdot)$.

Справедливы формулы:

- $e(P \oplus Q) = e(P)\, e(Q)$;
- $e(P{+}Q) = \binom{n+m}{n} e(P)\, e(Q), \quad n = |P|,\ m = |Q|.$
- $e(\mathbf{2} \times \mathbf{n}) = \dfrac{1}{n+1} C_{2n}^n$ — числа Каталана.
- $\displaystyle\sum_{n\geqslant 0} \frac{e(Z_n)\, x^n}{n!} = \sec x{+}\operatorname{tg} x$ (*производящая функция* для последовательности значений $\{Z_n\}_{n\geqslant 0}$).

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

$$\begin{aligned}\operatorname{tg} x &= x + \frac{1}{3}x^3 + \frac{2}{15}x^5 + \ldots \\ &\quad \ldots + \frac{2^{2n}(2^{2n}-1)B_n}{(2n)!}x^{2n-1} + \ldots, \\ \sec x &= 1 + \frac{x^2}{2} + \frac{5}{24}x^4 + \frac{61}{720}x^6 + \ldots + \\ &\quad \ldots + \frac{E_n}{(2n)!}x^{2n} + \ldots,\end{aligned}$$

  где B_n и E_n — *числа Бернулли и Эйлера* соответственно. Например,

$$e(Z_5) = \frac{2}{15} \cdot 5! = 16. \qquad (3.1)$$

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.

- Легко найти, что $e(S_n) = (n+1)!(n-1)!$.
- $$\sum_{n \geqslant 1} \frac{e(\mathbf{s}_n)}{n!}\, x^n = \frac{x}{\cos^2 x}$$
- $$\frac{\log(e(B^n))}{2^n} = \log_n \lfloor n/2 \rfloor - \frac{3}{2} \log e + o(1).$$
- Вычисление значения $e(P)$ — $\#P$-полная задача. Точное решена лишь для очень немногих типов ч. у. множеств.

Для ч. у. множества $\langle \{ v_1, \ldots, v_n \}, \sqsubseteq \rangle$ в n-мерном евклидовом пространстве определим многогранник $\mathcal{P}$:

$$\mathcal{P} = \Big\{ (x_1, \ldots, x_n) \in \mathbb{R}^n \mid 0 \leqslant x_i \leqslant 1,\ v_i \sqsubseteq v_j \Rightarrow x_i \leqslant x_j \Big\}$$

Если $vol(\mathcal{P})$ — объём $\mathcal{P}$, то $e(P) = n! \cdot vol(\mathcal{P})$.

Вероятностное пространство, связанное с ч. у. множеством. *Дискретное вероятностное пространство* на множестве $\mathcal{L}(P)$ всех линеаризаций ч. у. множества $\langle P, \sqsubseteq \rangle$: каждой его линеаризаций приписывают *равную вероятность*.

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

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

Теорема 3.6 (*XYZ*-теорема). *Пусть* $\langle P, \sqsubseteq \rangle$ — *ч. у. множество и* $x, y, z \in P$. *Тогда*

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

Пример 3.9. Ч.у. множество на рис. 3.10 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

$$\Pr[a < b] = \frac{2}{5}, \quad \Pr[a < d] = \frac{4}{5},$$
$$\Pr[(a < b)\&(a < d)] = \frac{2}{5} \text{ и } \frac{8}{25} \leqslant \frac{2}{5}.$$

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

Ясно, что, оптимальная процедура поиска L включает в себя нахождение элементов x и y, для которых $\Pr[x < y]$ наиболее близка к $\frac{1}{2}$.

«1/3 – 2/3 предположение»: *Любое не являющееся цепью ч. у. множество содержит пару несравнимых элементов x и y, для которых*

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

Пример **2+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.*

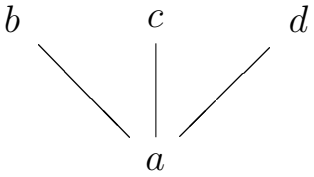
Наиболее сильный результат на сегодняшний день:

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

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

3.6 Размерность ч. у. множеств

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.

Определение 3.14. Наименьшее число линейных порядков, дающих в пересечении данное ч. у. множество P, называется его *(порядковой) размерностью* последнего и обозначается $\dim(P)$.

Для вышепреведённого ч. у. множества $\dim(P) \leqslant 3$.

Теорема 3.7 (*Ope*). *Порядковая и мультипликативная размерности ч. у. множества совпадают.*

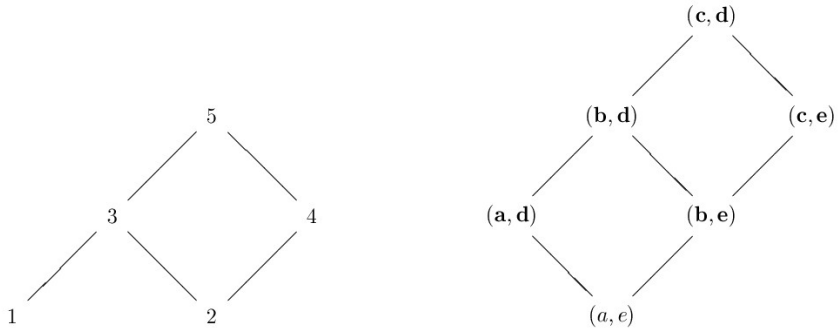


Рис. 3.11. Ч. у. множество P (слева), его вложение в $[a, b, c] \times [d, e]$ (справа, P выделено) и представление в виде пересечения своих линейных продолжений — $P \hookrightarrow [a, b, c] \times [d, e]$

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

Размерность 1 имеют только цепи. Размерность — 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.

- Размерность 1 имеют только цепи.
- Размерность 2 имеют:
  - *тривиально упорядоченные* неодноэлементные множества;
  - все отличных от цепей ч. у. множеств, имеющие не более 5 элементов;
  - зигзаги любой длины;
  - все 6-элементные ч. у. множества, за исключением *короны* s_3, *«шеврона»* sh и $sh^\sharp$ (см. рис. 3.12), имеющими размерность 3.
- Стандартный пример ч. у. множества размерности n — полная корона $S_n \quad (\dim(S_n) = n)$.

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

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

Для ч. у. множеств P и Q справедливо:

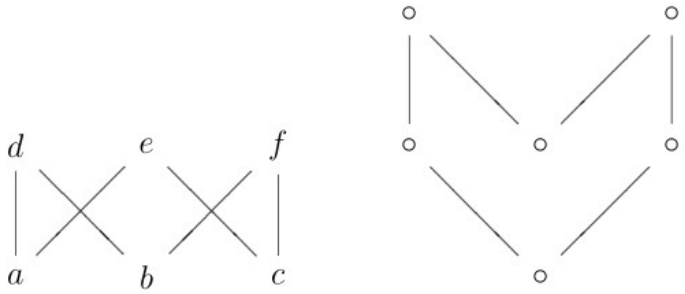


Рис. 3.12. Малая корона s_3 и «шеврон» sh

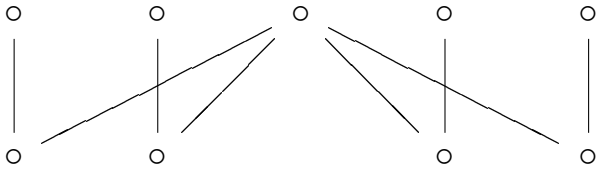


Рис. 3.13. Ч.у. множество P размерности 3

- $\varnothing \neq Q \subseteq P \Rightarrow \dim(Q) \leqslant \dim(P)$ и при удалении из ч. у. множества одного элемента его размерность уменьшается не более, чем на 1.
- $\dim(P \times Q) \leqslant \dim(P) + \dim(Q)$, 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 декар-

тово произведение линейных порядков $\mathbb{R}$ равна n;
  - $\dim(\mathbf{2}^n) = n$;
  - $\dim(S_n \times S_n) = 2n - 2$.

- $\dim(P) \leqslant \dfrac{|P|}{2}$ 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.

Пример 3.10. Размерность упорядоченной по включению совокупности 1- и 2-элементных подмножеств n-элементного множества неограниченно растёт при $n \to \infty$.

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.

d-несводимые ч. у. множества и проблема Ногина. Ч.у. множество P размерности $d \geqslant 2$ называется *d-несводимым*, если $\dim(P') < d$ для любого собственного ч.у. подмножества $P' \subseteq P$.

- Единственное 2-несводимое множество — 2-элементная антицепь.
- 3-несводимые ч. у. множества: s_3, sh, $sh^\sharp$, ...

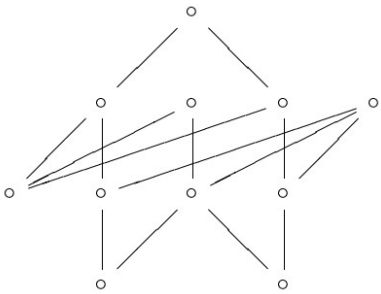


Рис. 3.14. 4-несводимое ч. у. множество

- Единственное $2n$-элементное n-несводимое множество — корона S_n.

Общепринятая точка зрения:
3-несводимые множества редки, хорошо изучены и регулярны, в то время как 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 3.2. $\pi(d, n) \leqslant n - d$.

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 $w(P) \leqslant n - \dim(P)$. Очевидно, $\pi(P) \leqslant w(P)$, откуда $\pi(P) \leqslant n - \dim(P)$. □

3.7 Вполне упорядоченные множества и смежные вопросы

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

Принцип Хаусдорфа: всякая цепь ч. у. множества содержится в некоторой его максимальной цепи.

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*.

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

Аксиома выбора предложена Э. Цéрмело при разработке *аксиоматической теории множеств*.

AC утверждает, что для каждого непустого множества A найдётся такая функция f_A, что $f_A(B) \in B$ для любого $B \in \mathcal{P}^*(A)$. Иными словами: для любого всюду определённого соответствия можно построить вложенное в него функциональное.

Определение 3.15. Линейно упорядоченное множество называют *вполне упорядоченным* (*в. у. множество*), если каждое его непустое подмножество содержит наименьший элемент.

Ясно, что в. у. множество всегда содержит *наименьший* элемент. Элементы в.у. множества традиционно обозначают строчными греческими булавами α, β, ...

Во в.у. 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, элемент α называется *предельным*.

Пример 3.11. 1. Вполне упорядочены все конечные цепи, а также 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. $\left[0,\ \frac{1}{2},\ \frac{2}{3},\ \frac{3}{4},\ \ldots,\ 1,\ 1+\frac{1}{2},\ 1+\frac{2}{3},\ \ldots,\right.$
$\left.\ldots,\ m,\ m+\frac{1}{2},\ m+\frac{2}{3},\ \ldots\right]$

является вполне упорядоченной, её предельные элементы — натуральные числа.

4. Линейное расширение казуального множества $\langle \mathbb{N}, | \rangle$ по ранее рассмотренному алгоритму (см. с. 93) является вполне упорядоченным.

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

Вопрос: принцип полного упорядочения очень похож на принцип продолжения порядка, применённый к тривиально упорядоченному множеству. Так в чём разница?

Пример 3.12. На счётных множествах частичный порядок указать легко.

Множество целых чисел $\mathbb{Z}$ можно вполне упорядочить считая, например, что

$$0 < 1 < -1 < 2 < -2 < 3 < -3 \ldots \quad \text{или}$$
$$1 < 2 < \ldots < 0 < -1 < -2 < \ldots$$

Утверждения, эквивалентные приведённым: о равномощности множеств X и $X \times X$; о непустоте

декартова произведения произвольной совокупности непустых множеств и др.

Т.о. 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.

Замечания об аксиоме выбора AC:

- Для *конечных* множеств её справедливость очевидна, но при рассмотрении *бесконечных совокупностей бесконечных множеств* эта очевидность теряется.

  Бертран Рассел об аксиоме выбора: — Сначала она кажется очевидной; но чем больше вдумываешься, тем более странными кажутся выводы из этой аксиомы; под конец же вообще перестаешь понимать, что же она означает.

- *все попытки свести AC к другим фундаментальным принципам оказались безуспешными.*

  Доказательство невозможности опровергнуть AC в аксиоматике NBG дал в 1940 г. К. Гёдель. В 1963 г. П. Коэн доказал независимость AC от остальных аксиом ZFC. Аксиоматики теории множеств NBG и ZFC *равнообъёмны*: любая теорема, доказуемая в одной системе, также доказуема и в другой.

- 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.

Поэтому при не связанных с вопросами оснований математики и теории множеств исследованиях можно *как принять аксиому выбора, так и отказаться от неё.*

Отклонение AC — обеднение содержания конкретных математических теорий: не удаётся, например, доказать —

- наличие базиса у произвольного векторного пространства;
- эквивалентности двух определений непрерывности функции в точке (по Коши и по Гейне: на языке ε–δ и через пределы последовательностей соответственно).

Принятие AC влечёт существование объектов с парадоксальными свойствами, например:

- 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.

К. Гёдель показал:

- присоединение AC к системе аксиом теории множеств не увеличивает опасности впасть в противоречие (то есть 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 (то есть 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*.

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*).

Пример 3.13 (Парадокс Рассела). *Множество Рассела* — $R = \{\, x \mid x \notin x \,\}$, то есть $z \in R \Leftrightarrow z \notin z$.

При подстановке $z \mapsto R$ получаем

$$R \in R \Leftrightarrow R \notin R \quad \text{— противоречие.}$$

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

Если α — элемент в.у. множества, то интервал

$$[\, o,\, \alpha\,) \stackrel{\text{def}}{=} \alpha^{\triangledown} \setminus \{\alpha\}$$

называют *начальным отрезком* α. Символ $[\, o,\, o\,)$ понимается как пустое множество.

Сравнение в.у. множеств и кардинальные числа

Теорема 3.8 (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) $A \cong$ *некоторому начальному отрезку* B;

3) $B \cong$ *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 $\overline{\overline{X}}$ (обозначение ввёл Г. Кантор) понимается новый объект, связанный с множеством X, называемый *кардинальным числом* X или *кардиналом*.

Теорема 3.9 (*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 2)–3), либо выполняются условия теоремы Кантора-Шрёдера-Бернштейна (если каждое из множеств равномощно подмножеству другого, то множества равномощны), что влечёт выполнение условия (1) . □

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 (2) и (3) теоремы.

Теорема 3.10 (*Кантор*). $\overline{\overline{A}} < \overline{\overline{\mathcal{P}(A)}}$.

Доказательство. Предположим противное, то есть что существует биекция $\varphi : A \to \mathcal{P}(A)$. Данную биекцию можно рассматривать как всюду определённое однородное отношение на A.

В множестве-степени $\mathcal{P}(A)$ существует подмножество N всех φ-нерефлексивных элементов из A:

$$N = \{a \in A \mid a \notin \varphi(a)\} \subseteq A.$$

Однако по свойству канторовости (утверждение 2.1) множество N не имеет прообраза. Противоречие. □

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*, то есть дело в аксиоме свёртки).

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

Теорема 3.11 (*принцип трансфинитной индукции*). *Пусть имеется вполне упорядоченное множество, с каждым элементом α которого связано утверждение S_α, которые образуют совокупность S.*

Тогда, если из справедливости S_β для всех $\beta \in [o, \alpha) \neq o$ 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 данном вполне упорядоченном множестве. Но тогда, поскольку S_β справедливо для всех $\beta \in [o, \alpha)$, справедливо и S_α — противоречие. □

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

3.8 Некоторые применения теории ч. у. множеств

Применение ч. у. множеств в математике

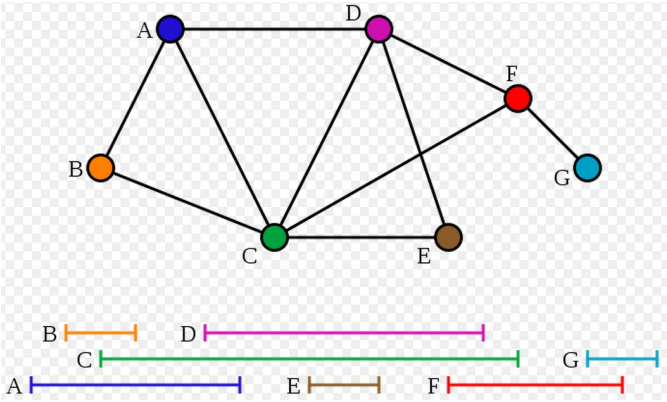
1) Использование частичных порядков в *теории чисел, теории множеств и комбинаторике* (теория разбиений и др.) уже были упомянуты.
2) Рассматривают АС, носители которых частично упорядочены.

   Наиболее исследованы *частично упорядоченные группы, кольца и полугруппы.*
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.).

   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:

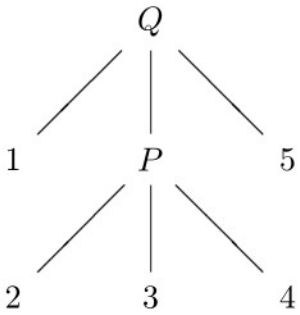
   PQ-деревья — корневые планарные деревья, висячие вершины в которых представляют пе-



реставляемые 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 среди элементов 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 каждого из данных критериев желательно *максимизировать.*

В экономике решение $x^* \in X$ называется *оптимальным по Парето*, если не существует такого возможного решения $x \in X$, для которого $y_i(x^*) \leqslant y_i(x)$ для всех $i = 1, \ldots, n$, причём хотя бы одно неравенство выполняется строго.

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

Нахождение множества Парето в простейшем случае, когда множество возможных векторов $Y = \{ y(x) \mid x \in X \}$ состоит из конечного числа N элементов, то есть 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).

Пример: Задача о выборе наилучшего проектного решения

Для участия в конкурсе представлено 5 вариантов строительства на территории, непосредственно прилегающей к жилому району предприятий различного типа (например, x^1 — машиностроительный завод, x^2 — текстильная фабрика, x^3 — молочный завод и т.п.).

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.

	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 $5-z$ на противоположные, произведём попарное сравнение полученных векторов. В результате удаления доминируемых элементов, получим множество Парето $\Pi = \{x^1, x^2, x^5\}$, то есть осуществлять окончательный выбор следует из 1, 2 и 5-го проектов.

Применение ч. у. множеств в математической логике: модели Крипке как общий способ установления истинности формул логических исчислений.

Зафиксируем множества

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

Определение 3.16. *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.

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: $\{\,\mathbf{И},\, \mathbf{Л}\,\}$ и выделенное — **И**.

Схемы 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.

В ИИВ имеется единственное правило вывода, обозначаемое *MP* (лат. *modus ponens*), 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 $\nvdash A$.

Пример 3.14 (*вывод формулы в ИИВ*). Покажем

$$\vdash x \vee y \supset y \vee x.$$

(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)

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 (*объектной*) теории: корректность, непротиворечивость, различные виды полноты теории, разрешимость, независимость систем аксиом и правил вывода и др.

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.

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

Примеры тавтологий: 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, то есть 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 $\nvdash F$.

- 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*.

Построение шкал Крипке. 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 будем записывать символически $w \Vdash x$, ложности — $w \nVdash x$.
При формировании шкалы Крипке требуется, чтобы

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

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

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 3.17. *Шкала Крипке* есть тройка

$$\langle W, \leqslant, \Vdash \rangle,$$

где: редукт $\langle W, \leqslant \rangle$ — ч. у. множество,

$\Vdash \subseteq W \times Var$ — соответствие «один ко многим», ставящее каждому миру совокупность истинных в нём логических переменных и удовлетворяющее условию наследования истинности.

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 $u \nVdash A$;

$w \Vdash \neg A \;\Leftrightarrow\; \forall (u \geqslant w)\; u \nVdash A$ (то есть если $\Vdash \neg A$, то ни в этом, ни в каком-либо большем мире невозможно $\Vdash A$).

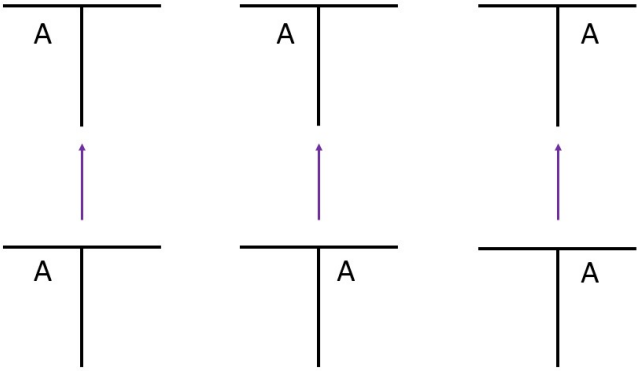
Введённые шкалы Крипке задают *семантику* ИИВ, придавая смысл формулам — разделяя их на истинные и ложные *в данном мире*.

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. Каждому миру соответствует таблица из 2 столбцов. Если $w \Vdash A$, то помещаем формулу A в левый столбец мира w, если $w \nVdash A$, то в правый.



Теорема 3.12 (*корректность 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 $w \Vdash A \Rightarrow w \nVdash B$.

Первое: проверяем истинность всех аксиом ИИВ.

1-*я аксиома* $A \supset (B \supset A)$.

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

2-*я аксиома* $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$.

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. □

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 3.15. 1. 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 $v \Vdash x \vee \neg x$).

2. Та же шкала будет контрмоделью для формулы $\neg\neg x \supset x$:
положив $u \nVdash x$ и $v \Vdash x$, по вышеприведённым правилам получим, что $u \nVdash \neg x$, $u \Vdash \neg\neg x$ и $u \nVdash \neg\neg x \supset x$.

3. Постоим контрмодель для формулы $\neg x \vee \neg\neg x$.

Пусть в мире u она ложна: $u \nVdash \neg x \vee \neg\neg x$. Тогда в это мире ложны оба члена дизъюнкции: $u \nVdash \neg x$, $u \nVdash \neg\neg x$.

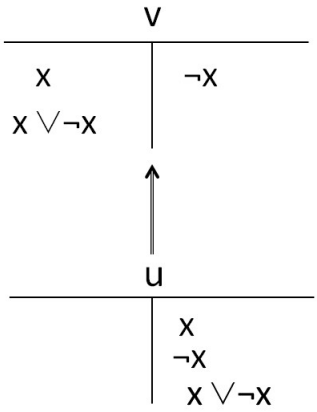


Рис. 3.15. Контрмодель для $u \nVdash x \vee \neg x$

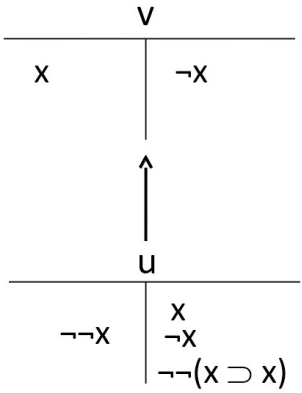


Рис. 3.16. Контрмодель для $\neg\neg x \supset x$

В соответствии с правилами истинности и ложности формул в шкалах, пусть в $v \nVdash \neg x$ и $v \Vdash \neg\neg x$ в мире v, бóльшим u, а в бóльшим u мире w — $w \nVdash \neg\neg x$ $w \Vdash \neg\neg x$. При этом миры v и w несравнимы: $u \leqslant v$, $u \leqslant w$, $u \nsim w$.

Искомая контрмодель построена. В ней формула x будет истинна только в мире v.

Шкалы Крипке: применение

1) Метод автоматической верификации параллельных вычислительных систем (англ. model checking), позволяет

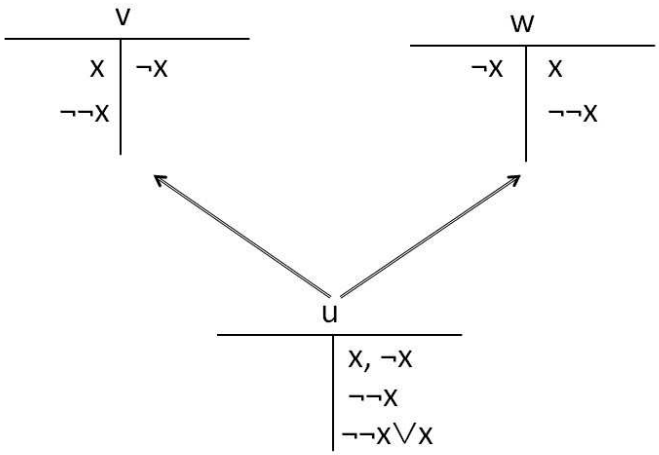


Рис. 3.17. Контрмодель для формулы $\neg x \vee \neg\neg x$

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.

2) *Модальные логики* формализуют *сильные* и *слабые модальные* выражения вида «необходимо/возможно», «всегда/иногда» 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.

Глава 4

Решётки

4.1 Определение и основные свойства

Определение 4.1. Ч. у. множество, в котором для любых элементов a и b существуют и $\inf\{a, b\}$, и $\sup\{a, b\}$, называют *решёточно упорядоченным* (р. у. множеством).

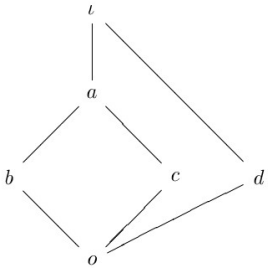
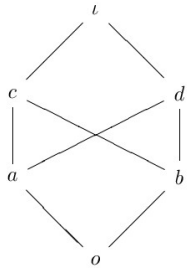


Рис. 4.1. Р. у. м.



Не-р. у. м.

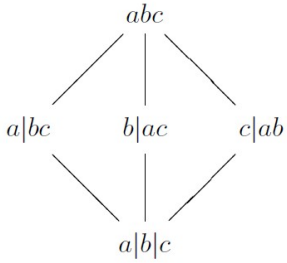
Определение 4.2. Тройка $\langle L, \sqcup, \sqcap \rangle$, где L — непустое множество, а $\sqcup$ (*объединение*), $\sqcap$ (*пересечение*) — бинарные операции на нём, подчиняющимися двойственным парам законов *коммутативности, ассоциативности, идемпотентности и поглощения*

$$x \sqcup y = y \sqcup x, \qquad x \sqcap y = y \sqcap x,$$
$$x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z, \qquad x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z,$$
$$x \sqcup x = x, \qquad x \sqcap x = x,$$
$$x \sqcap (x \sqcup y) = x, \qquad x \sqcup (x \sqcap y) = x.$$

называют *алгебраической решёткой*.

Решётка называется *полной*, если *любое подмножество* её элементов имеет точные верхнюю и нижнюю грани.

Принцип двойственности для решёток: любое утверждение, истинное для *любых произвольных* элементов решётки, остаётся таковым при замене $\sqcap \leftrightarrow \sqcup$.



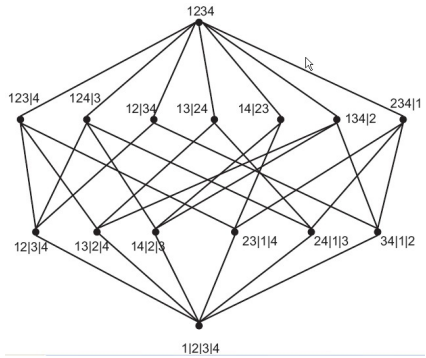


Рис. 4.2. Примеры алгебраических решёток: беллианы множеств $\{a, b, c\}$ и $\{1, 2, 3, 4\}$

Теорема 4.1 (эквивалентность р. у. множеств и решёток).

1) *Пусть* $\langle P, \sqsubseteq \rangle$ — *решёточно упорядоченное множество. Если для любых элементов* x *и* y *из* P *положить*

$$x \sqcup y = \sup\{x, y\}, \qquad x \sqcap y = \inf\{x, y\},$$

то структура $\langle P, \sqcup, \sqcap \rangle$ *будет решёткой.*

2) *Пусть* $\langle L, \sqcup, \sqcap \rangle$ *— решётка. Если для любых элементов* x *и* y *из* L *положить*

$$x \sqsubseteq y \;=\; x \sqcap y = x \quad (\textit{или}\ x \sqsubseteq y \;=\; x \sqcup y = y),$$

то структура $\langle L, \sqsubseteq \rangle$ *будет решёточно упорядоченным множеством.*

Теорема устанавливает взаимно-однозначное соответствие между решёточно упорядоченными множествами и решётками: *из одной* AC *всегда можно получить другую.*

Поэтому термин «решётка» применяют для обоих понятий: любую решётку можно представить либо как упорядоченное множество, либо как алгебру.

р.у. множества	решётки
$\langle \mathbb{R}, \leqslant \rangle$	$\langle \mathbb{R}, \max, \min \rangle$
$\langle \mathbb{N}, \mid \rangle$	$\langle \mathbb{N}, \text{НОК}, \text{НОД} \rangle$
$\langle \mathcal{P}(A), \subseteq \rangle$	$\langle \mathcal{P}(A), \cup, \cap \rangle$

Возможность такого рассмотрения решёток позволяет вводить в них как порядковые, так и алгебраические операции, что приводит к богатой и многообразной в приложениях теории.

Наименьший элемент решётки (как р. у. м.) — её ноль (o), наибольший — единица (ι) — это её *универсальные грани*. Решётка может и не иметь универсальных граней: $\mathbb{Z}$, у $\langle \mathbb{N}, \mid \rangle$ — только $o = 1$. Все конечные решётки содержат o и ι.

Если решётка содержит o, то она может содержать атомы. Определение атома решётки совпадает с приведённым для булевой алгебре (см. определение 1.4).

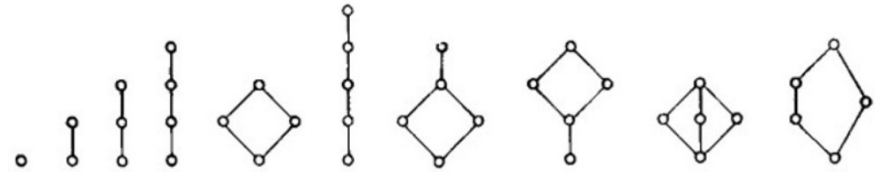


Рис. 4.3. Все решётки, содержащие не более 5 элементов.
5 элементные решётки: цепь, «ракетка вниз», «ракетка вверх», M_3 (бриллиант) и N_5 (пятиугольник).

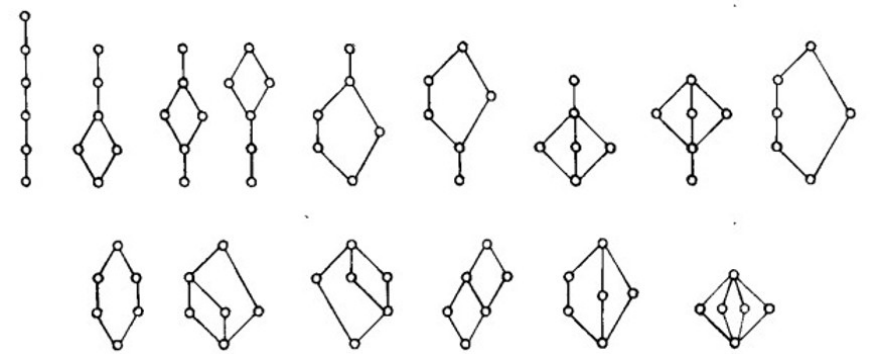


Рис. 4.4. Все 15 решёток, содержащих 6 элементов.

Теорема 4.2. *Ч. у. множество является полной решёткой, если и только если*

1) *оно имеет наибольший элемент* ι *и*
2) *для любого его непустого подмножества* A *существует точная нижняя грань* $\inf A$.

Доказательство. Необходимость. Пусть $\langle P, \sqsubseteq \rangle$ — полная решётка. Тогда каждое непустое подмножество $A \subseteq P$ имеет и точную нижнюю грань $\inf A$, и точную верхнюю грань $\sup A$. В частности, существует $\sup P = \iota$.

Достаточность. Покажем, что в условиях теоремы каждое непустое подмножество $A \subseteq P$ имеет точную верхнюю грань.

Рассмотрим $A^\triangle$ — совокупность всех верхних граней A. Очевидно, $\iota \in A^\triangle$, так что $A^\triangle \neq \varnothing$.

По условию теоремы существует элемент $b = \inf A^\triangle$, но по определению, $b = \sup A$, откуда следует, что P — полная решётка. □

Следствия. Конечное ч. у. множество P является решёткой если и только если

1) *оно имеет наибольший элемент и*
2) *для любых двух его элементов существует точная нижняя грань.*

Обычно на практике проверка наличия у подмножеств ч. у. множества *точных нижних граней* — не вызывает затруднений, а *верхних граней* — требует значительных усилий. Данная теорема является *эффективным критерием решёточности порядков*, например:

Утверждение 4.1. *Решётка всех эквивалентностей множества является полной.*

Доказательство. Точной нижней гранью любой совокупности эквивалентностей является их пересечение, а единицей решётки всех эквивалентностей множества служит универсальная *аморфная* эквивалентность ∇. □

4.2 Гомоморфизмы, идеалы, фильтры

Утверждение 4.2. *Для любых элементов x, y, u, v решётки $\langle L, \sqcup, \sqcap \rangle$ справедливо*

$$\begin{cases} x \sqsubseteq y \\ u \sqsubseteq v \end{cases} \Rightarrow \begin{cases} x \sqcup u \sqsubseteq y \sqcup v \\ x \sqcap u \sqsubseteq y \sqcap v \end{cases}.$$

Доказательство.

$$\begin{cases} x \sqsubseteq y \\ u \sqsubseteq v \end{cases} \Leftrightarrow \begin{cases} x \sqcap y = x \\ u \sqcap v = u \end{cases} \Rightarrow x \sqcap y \sqcap u \sqcap v = x \sqcap u \Leftrightarrow$$
$$\Leftrightarrow (y \sqcap v) \sqcap (x \sqcap u) = x \sqcap u \Leftrightarrow x \sqcap u \sqsubseteq y \sqcap v,$$

и $x \sqcup y \sqsubseteq u \sqcup v$ по двойственности. □

Теорема 4.3. *Элементы x, y и z любой решётки удовлетворяют следующим неравенствам полудистрибутивности*

$$Dtr \sqsupseteq: \quad (x \sqcup y) \sqcap z \sqsupseteq (x \sqcap z) \sqcup (y \sqcap z);$$
$$Dtr \sqsubseteq: \quad (x \sqcap y) \sqcup z \sqsubseteq (x \sqcup z) \sqcap (y \sqcup z)$$

и полумодулярности

$$Mod \sqsubseteq: \quad x \sqsubseteq y \Rightarrow x \sqcup (y \sqcap z) \sqsubseteq y \sqcap (x \sqcup z);$$
$$Mod \sqsupseteq: \quad x \sqsupseteq y \Rightarrow x \sqcap (y \sqcup z) \sqsupseteq y \sqcup (x \sqcap z).$$

Лемма 4.1 (о четырёх элементах). *Для любых элементов x, y, u, v решётки $\langle L, \sqcup, \sqcap \rangle$ справедливо соотношение*

$$x, y \sqsubseteq u, v \Rightarrow (x \sqcup y) \sqsubseteq (u \sqcap v).$$

Доказательство. По $Dtr\,\sqsubseteq$:

$$(u \sqcap v) \sqcup x \sqsubseteq (\underbrace{u \sqcup x}_{u}) \sqcap (\underbrace{v \sqcup x}_{v}) = u \sqcap v \Rightarrow x \sqsubseteq u \sqcap v.$$

Аналогично и $y \sqsubseteq u \sqcap v$; применяя операцию $\sqcup$ к обеим частям полученных включений, получаем требуемое. □

Гомоморфизмы решёток

Определение 4.3. Отображение φ решётки L в решётку L' называется *алгебраическим* или *решёточным гомоморфизмом*, если для любых $x, y \in L$ справедливы равенства

$$\varphi(x \sqcup y) = \varphi(x) \sqcup \varphi(y) \quad \text{и} \quad \varphi(x \sqcap y) = \varphi(x) \sqcap \varphi(y).$$

Биективный решёточный гомоморфизм есть *решёточный изоморфизм*, символически $L \cong L'$.

Изоморфизм решётки в себя называется *автоморфизмом*.

Инъективные и сюръективные решёточные гомоморфизмы называют *решёточными* (или *алгебраическими*) *мономорфизмами* (вложениями) и *эпиморфизмами* соответственно.

1. Порядковые гомоморфизмы решёток как ч. у. множеств, вообще говоря, *не являются алгебраическими* (см. рис. 4.5).

2. Напротив, любое отображение одной решётки на другую, сохраняющее *хотя бы одну из решёточных*

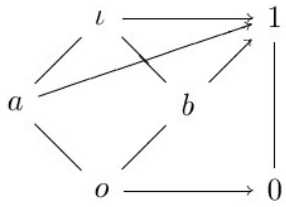


Рис. 4.5. Порядковый, но не решёточный гомоморфизм решёток: $\varphi(a) \sqcap \varphi(b) = 1 \sqcap 1 = 1 \neq \varphi(a \sqcap b) = \varphi(o) = 0$.

операций, является порядковым гомоморфизмом: если φ сохраняет пересечение, то для любых $x, y \in L$ справедливо

$$x \sqsubseteq y \Leftrightarrow x = x \sqcap y \overset{(*)}{\Rightarrow}$$
$$\Rightarrow \varphi(x) = \varphi(x \sqcap y) = \varphi(x) \sqcap \varphi(y) \Leftrightarrow \varphi(x) \sqsubseteq \varphi(y),$$

и, значит, φ изотонно (аналогично изотонность φ следует и из сохранения объединения).

В случае изоморфизма проблемы снимаются.

Теорема 4.4 (об эквивалентности двух видов изоморфизма решёток). *Две решётки алгебраически изоморфны, если и только если они изоморфны как ч. у. множества.*

Доказательство. Необходимость. Пусть φ — *алгебраический изоморфизм* решётки L на некоторую другую решётку. Так как отображение φ взаимно-однозначно и изотонно, остаётся убедится в его обратной изотонности.

Это устанавливается обращением следования $\overset{(*)}{\Rightarrow}$ в предыдущем выражении, что можно сделать в силу взаимно-однозначности φ.

Достаточность. Пусть L_1 и L_2 — две решётки, *изоморфные как порядки.* Докажем согласованность операции $\sqcap$ относительно порядкового изоморфизма φ, то есть что

$$\varphi(x \sqcap y) = \varphi(x) \sqcap \varphi(y),$$

при условии $x \sqsubseteq y \;\Leftrightarrow\; \varphi(x) \sqsubseteq \varphi(y)$ и биективности φ.

Для произвольных $x, y \in L_1$ в силу изотонности φ

$$\left\{ \begin{array}{l} x \sqcap y \sqsubseteq x \\ x \sqcap y \sqsubseteq y \end{array} \right. \Rightarrow \left\{ \begin{array}{l} \varphi(x \sqcap y) \sqsubseteq \varphi(x) \\ \varphi(x \sqcap y) \sqsubseteq \varphi(y) \end{array} \right.$$

Пусть b — есть нижняя грань $\{\, \varphi(x), \varphi(y) \,\}$ в L_2. Тогда в силу сюръективности φ, в L_1 найдется $a = \varphi^{-1}(b)$ и

$$\left\{ \begin{array}{l} b = \varphi(a) \sqsubseteq \varphi(x) \\ b = \varphi(a) \sqsubseteq \varphi(y) \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} a \sqsubseteq x \\ a \sqsubseteq y \end{array} \right. .$$

Отсюда далее имеем

$$a \sqsubseteq x \sqcap y \;\Leftrightarrow\; b = \varphi(a) \sqsubseteq \varphi(x \sqcap y).$$

Таким образом, $\varphi(x \sqcap y)$ будет наибольшей нижней гранью для $\{\, \varphi(x), \varphi(y) \,\}$, или, что то же, $\varphi(x \sqcap y) = \varphi(x) \sqcap \varphi(y)$.

Согласованность операции $\sqcup$ относительно φ справедлива по двойственности. $\square$

Подрешётки

Определение 4.4. Непустое подмножество P решётки $\langle L, \sqcup, \sqcap \rangle$ называется её *подрешёткой*, символически $P \leqslant L$, если

$$a, b \in P \;\Rightarrow\; \begin{cases} a \sqcup b \in P, \\ a \sqcap b \in P. \end{cases}$$

Из определения следует, что подмножество элементов решётки L может быть решёткой относительно наследуемого частичного порядка, но не её подрешёткой (см. рис. 4.6).

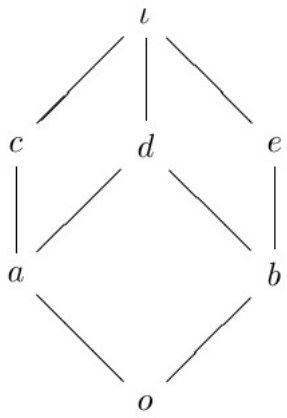


Рис. 4.6. Ч. у. подмножество o, a, c, ι, e — подрешётка, но ч. у. подмножество o, a, c, ι, b — решётка, но не подрешётка исходной

Подрешётки: некоторые свойства

- Каждое подмножество решётки L является подрешёткой, если и только если L — цепь.
- Любой интервал решётки есть её подрешётка.

- Пересечение подрешёток либо пусто, либо является подрешёткой.

  В силу этого, удобно считать подрешёткой и пустое множество: тогда пересечение любой совокупности — подрешётка.

- Если определить объединение двух интервалов решётки L как наименьший интервал, их содержащий (он, очевидно, единственен), то совокупность $Si(L)$ всех интервалов L вместе с пустым интервалом есть *решётка интервалов*.

- Если φ — гомоморфизм решётки L в решётку L', то $\operatorname{Im}\varphi \leqslant L'$.

Идеалы и фильтры решёток

Определение 4.5. *Непустой* порядковый идеал I решётки называется её *решёточным идеалом*, если

$$x,\, y \in I \;\Rightarrow\; x \sqcup y \in I\,.$$

Непустой порядковый фильтр F решётки называется её *решёточным фильтром*, если

$$x,\, y \in F \;\Rightarrow\; x \sqcap y \in F\,.$$

Непустое подмножество I оказывается решёточным идеалом, если и только если справедлива эквивалентность

$$x,\, y \in I \;\Leftrightarrow\; x \sqcup y \in I,$$

и аналогично для фильтров —

$$x,\, y \in F \;\Leftrightarrow\; x \sqcap y \in F.$$

Множество $J(L)$ всех идеалов решётки L упорядочено по включению, то есть является ч. у. множеством.

Множество $\{L\}$ всех элементов решётки L — её (*несобственный*) идеал. Это — наибольший элемент $J(L)$.

Все другие идеалы и фильтры L называют *собственными* Множество всех несобственных идеалов решётки L обозначают $J_*(L)$.

Если решётка содержит наименьший элемент o, то он принадлежит любому её идеалу. Так что множество $\{o\}$ является наименьшим её идеалом.

В случае, когда решётка не имеет наименьшего элемента, в число её идеалов договариваются включать пустое множество $\varnothing$.

Идеалы решёток: свойства и примеры

- Если a — элемент решётки, то *главные порядковые* идеал $J(a) = a^{\triangledown}$ и фильтр $a^{\triangle}$ являются, также и *главными решёточными* идеалом и фильтром.
- В конечной решётке все идеалы и фильтры — главные: если I — идеал конечной решётки, то рассмотрим элемент $x = \bigsqcup_{a \in I} a$, для которого будем иметь $x \in I$ и $I = x^{\triangledown}$; и аналогично для фильтров.
- В бесконечных решётках могут существовать и неглавные решёточные идеалы и фильтры.

В цепи $\left[0, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \ldots, 1\right]$ неглавный идеал — $[0, 1)$.

- Если A — бесконечное множество, то совокупность $\mathcal{P}_0(A)$ всех его *конечных подмножеств* будет неглавным идеалом решётки $\mathcal{P}(A)$.

Максимальные элементы $J_*(L)$ называют *максимальными идеалами* решётки L (то есть максимальный идеал решётки не содержится ни в каком другом её собственном идеале).

Теорема 4.5 (о собственных идеалах решётки с единицей). *Всякий собственный идеал решётки с единицей содержится в некотором её максимальном идеале.*

Доказательство. Пусть $\langle L, \sqsubseteq \rangle$ — решётка с единицей ι, и $C = [J_1, J_2, \ldots]$ — некоторая (конечная или бесконечная) цепь собственных идеалов L. Обозначим $J = \bigcup_{J_k \in C} J_k$.

Если $x \in J$, то $x \in J_k \in C$ для некоторого k и для любого $y \sqsubseteq x$ имеем $y \in J_k \subseteq J$. Пусть $x, y \in J$, тогда $x \in J_k \in C$ и $y \in J_l \in C$ для некоторых k, l.

Поскольку C — цепь, то J_k и J_l сравнимы в $J_*(L)$.

Без ограничения общности считаем, что $J_k \subseteq J_l$.

Тогда $x, y \in J_l$ и, поскольку J_l — идеал, то $x \sqcup y \in J_l \subseteq J$.

Таким образом, J — идеал решётки L.

Более того, он собственный, поскольку $\iota \notin J_k \in C \Rightarrow \iota \notin J$.

С другой стороны, поскольку $J_k \subseteq J$ для всех $J_k \in C$, то J будет верхней гранью цепи C.

Отсюда по лемме Куратовского-Цорна вытекает утверждение теоремы. □

Диаграммы Хассе остаются удобным способом описания решёток, однако если решётка устроена слишком сложно, такие диаграммы становятся малонаглядными.

Теорема 4.6 (о представлении решёток). *Всякая решётка может быть вложена в булеан подходящего множества с сохранением всех точных нижних граней.*

Доказательство. Пусть L — решётка. Отображение $\varphi(x) = x^\nabla$ осуществляет вложение L в $\mathcal{P}(L)$ как ч. у. множество. Осталось удостовериться, что φ сохраняет пересечения, то есть $\varphi(x \sqcap y) = \varphi(x) \cap \varphi(y)$ или $(x \sqcap y)^\nabla = x^\nabla \cap y^\nabla$.

$$z \in (x \sqcap y)^\nabla \Leftrightarrow z \sqsubseteq (x \sqcap y) \Rightarrow \begin{cases} z \sqsubseteq x \\ z \sqsubseteq y \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} z \in x^\nabla \\ z \in y^\nabla \end{cases} \Leftrightarrow z \in (x^\nabla \cap y^\nabla).$$

Поэтому φ — искомое вложение. □

Данная теорема позволяет представлять элементы любой решётки подмножествами некоторого множества A, пользуясь аналогами диаграмм Эйлера-Венна. В таких диаграммах результат операции пересечения отождествляют с теоретико-множественным

пересечением в A, наибольшему элементу решётки (если он существует) соответствует само множество A, а наименьшему (если он есть) сопоставляют пустое множество.

Выясним, как следует обозначать результат объединения (точные верхние грани) на таких диаграммах.

$$z \in \varphi(x) \cup \varphi(y) = x^{\triangledown} \cup y^{\triangledown} \Leftrightarrow \left[\begin{array}{l} z \in x^{\triangledown} \\ z \in y^{\triangledown} \end{array} \right. \Leftrightarrow \left[\begin{array}{l} z \sqsubseteq x \\ z \sqsubseteq y \end{array} \right. \Rightarrow$$
$$\Rightarrow z \sqsubseteq x \sqcup y \Leftrightarrow z \in (x \sqcup y)^{\triangledown} = \varphi(x \sqcup y).$$

Таким образом, $\varphi(x) \cup \varphi(y) \subseteq \varphi(x \sqcup y)$, причём равенство в этом выражении, как нетрудно видеть, будет лишь в случае сравнимости x и y. Поэтому при обозначении объединения элементов, изображаемых в виде связных выпуклых областей, необходимо рисовать выпуклую область, покрывающую "с запасом" области, соответствующие данным элементам (см.рис. 4.7).

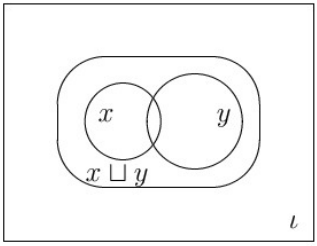


Рис. 4.7. Диаграмма, изображающая объединение и пересечение элементов решётки

4.3 Модулярные и дистрибутивные решётки

Модулярные решётки

Определение 4.6. Решётка $\langle L, \sqcup, \sqcap \rangle$ называется *модулярной*, если для любых x, y, $z \in L$ в ней выполняется следующий *модулярный закон*

$$Mod: \; x \sqsubseteq y \;\Rightarrow\; x \sqcup (y \sqcap z) \;=\; y \sqcap (x \sqcup z).$$

Примеры 4.1. 1) Модулярными являются все цепи, решётка $\langle \mathbb{N}, | \rangle$, булевы алгебры. Впоследствии мы увидим, что для этих решёток справедливо более сильное условие дистрибутивности.

2) Решётка $NSub\,G$ всех *нормальных* подгрупп группы G образует модулярна (пересечение групп всегда группа, а объединение нормальных подгрупп — их произведение).

3) Решётка всех эквивалентностей на данном множестве в общем случае *не модулярна*: см. рис. 4.8.

$$\alpha = (1|2|34),\ \beta = (12|34),\ \gamma = (1|23|4),\ \alpha \subset \beta.$$
$$Mod: \; \alpha \subset \beta \;\Rightarrow\; \alpha \cup (\beta \cap \gamma) = \beta \cap (\alpha \cup \gamma),$$
$$\alpha \cup (\beta \cap \gamma) = \alpha \cup o = \alpha \neq \beta \cap (\alpha \cup \gamma) = \beta \cap \iota = \beta.$$

Немодулярность N_5 оказывается ключевой:

Теорема 4.7 (критерий модулярности решётки). *Решётка модулярна, если и только если никакая её подрешётка не изоморфна пятиугольнику N_5.*

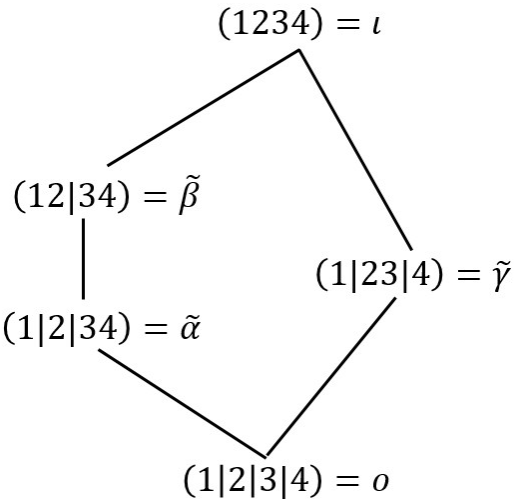


Рис. 4.8. Подрешётка решётки всех разбиений множества $\{1, 2, 3, 4\}$, изоморфная N_5

Невыполнение условия Жордана–Дедекинда для решётки влечёт существование подрешётки, изоморфной N_5, а это в свою очередь — её немодулярность.

Напротив, выполнение условие Жордана–Дедекинда ещё *не означает* модулярности решётки.

Для решётки на рис. 4.9 цепное условие Жордана–Дедекинда выполняется, однако она немодулярна, т. к. содержит подрешётку $\{o, a, c, e, \iota\} \cong N_5$.

Правило сокращения в решётках

$$Abbr(x, y) : \forall z \begin{cases} x \sqcup z = y \sqcup z \\ x \sqcap z = y \sqcap z \end{cases} \Rightarrow x = y.$$

Теорема 4.8 (правило сокращения в модулярных решётках). *Решётка модулярна, если и только если* $x \sim y \Rightarrow Abbr(x, y)$.

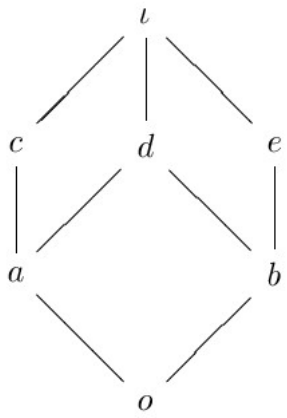


Рис. 4.9. Немодулярная решётка с выполненным условием Жордана–Дедекинда

Доказательство. *Достаточность.* Пусть для элементов x, y, z модулярной решётки справедливо

$$x \sqsubseteq y \quad \text{и} \quad (x \sqcup z = y \sqcup z) \,\&\, (x \sqcap z = y \sqcap z).$$

Тогда

$$x \overset{Abs}{=} x \sqcup (x \sqcap z) \overset{Abbr}{=} x \sqcup (y \sqcap z) \overset{Mod}{=} y \sqcap (x \sqcup z) \overset{Abbr}{=} \\ = y \sqcap (y \sqcup z) \overset{Abs}{=} y.$$

Необходимость — опустим. □

Также для модулярных решёток модулярны: (1) гомоморфный образ, (2) любая подрешётка, (3) прямое произведение.

Дистрибутивные решётки

Определение 4.7. Решётка $\langle L, \sqcup, \sqcap \rangle$ называется *дистрибутивной*, если в ней выполняются дистрибутивные законы

$$(x \sqcup y) \sqcap z = (x \sqcap z) \sqcup (y \sqcap z);$$
$$(x \sqcap y) \sqcup z = (x \sqcup z) \sqcap (y \sqcup z).$$

Примеры 4.2. 1. Дистрибутивны цепи, булевы алгебры и их подрешётки.

Из 5-элементных решёток, изображённых на рис. 4.3 модулярны цепь **5** и обе «ракетки».

2. Решётка всех подпространств векторного пространства (упомянутая ранее в качестве примера модулярной решётки) не дистрибутивна.

3. Решётка $\mathrm{Sub}\, C$ всех подгрупп *циклической* группы C дистрибутивна.

Всякая дистрибутивная решётка модулярна: модулярный закон — ослабленная форма второго дистрибутивного закона.

Поэтому и пятиугольник N_5 недистрибутивен (проверьте).

Решётка $Sub\, V_4 \cong M_3$ модулярна, но не дистрибутивна: см. рис. 4.10.

Обозначим $E = o$, $V_4 = \iota$, $\langle x \rangle = a$, $\langle xy \rangle = b$, $\langle y \rangle = c$ и тогда:

$$(a \sqcup b) \sqcap c = \iota \sqcap c = c \neq$$
$$\neq (a \sqcap c) \sqcup (b \sqcap c) = o \sqcup o = o.$$

Недистрибутивность M_3, оказывается ключевой.

Теорема 4.9. *Модулярная решётка является дистрибутивной, если и только если никакая её подрешётка не изоморфна ромбу* M_3.

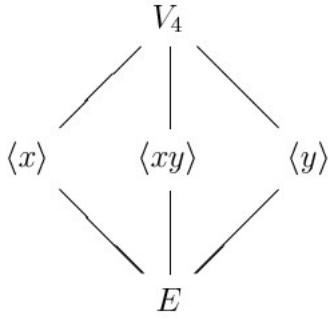


Рис. 4.10. Решётка подгрупп четверной группы Клейна $V_4 = \langle\, e, x, y, xy \,\rangle$

Следствие (критерий дистрибутивности решётки). *Решётка дистрибутивна, если и только если никакая её подрешётка не изоморфна ни пятиугольнику N_5, ни ромбу M_3.*

Лемма 4.2. *Порядковые идеалы ч. у. множества P образуют подрешётку решётки $\langle\, \mathcal{P}(P), \cup, \cap \,\rangle$.*

Доказательство. Достаточно показать, что совокупность $J(P)$ устойчива относительно теоретико-множественных операций объединения и пресечения.

Пусть $I_1, I_2 \in J(P)$. Тогда для всех элементов $a, x \in P$ имеем

$$(x \sqsubseteq a) \,\&\, (a \in I_1 \cup I_2) \;\Rightarrow\; \left[\begin{array}{l} (x \sqsubseteq a) \,\&\, (a \in I_1) \\ (x \sqsubseteq a) \,\&\, (a \in I_2) \end{array}\right. \;\Rightarrow$$

$$\Rightarrow \left[\begin{array}{l} x \in I_1 \\ x \in I_2 \end{array}\right. \;\Rightarrow\; x \in I_1 \cup I_2$$

и аналогично для $I_1 \cap I_2$. Следовательно, и $I_1 \cup I_2$, и $I_1 \cap I_2$ являются порядковыми идеалами. $\square$

Следствие. *Решётка* $\langle J(P), \cup, \cap \rangle$ *дистрибутивна.*

Пример дистрибутивности $J(Z_3)$ см. на рис. 4.11.

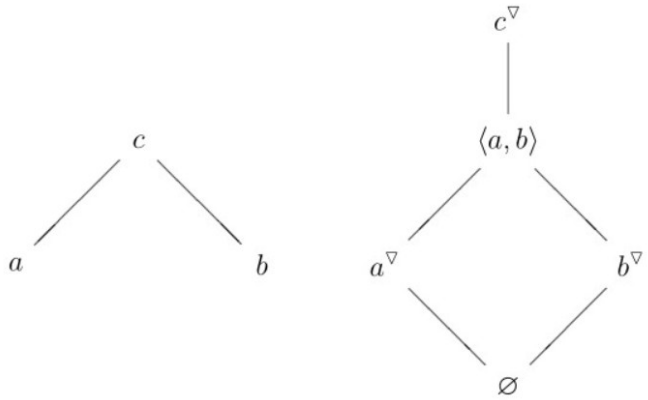


Рис. 4.11. Z_3 и $J(Z_3)$

В конечных дистрибутивных решётках важную роль играют не атомы (например, в конечной цепи всего один атом), а *неразложимые в объединение элементы.*

Определение 4.8. Элемент $a \neq o$ решётки с нулём o называют *неразложимым в объединение*, если из $a = b \sqcup c$ следует, что либо $a = b$, либо $a = c$.

Ясно, что если элемент a разложим и $a = b \sqcup c$, то оба элемента b и c строго содержатся в a.

Примеры 4.3. 1. Атомы любой решётки неразложимы, и в атомной булевой алгебре нет других неразложимых элементов.

2. В решётке $\langle \mathbb{N}, | \rangle$ неразложимы только *степени простых чисел.*
3. В цепи ни один элемент не является разложимым.

Утверждение 4.3. *В конечной решётке каждый ненулевой элемент может быть представлен в виде объединения неразложимых элементов.*

Доказательство. Пусть $a = a_1 \sqcup a_2$ и $a_1 \neq a \neq a_2$.

Если и a_1, и a_2 неразложимы, то лемма доказана. Иначе представляем a_1 и/или a_2 в виде объединения строго содержащихся в них элементов, и т.д.; в силу конечности решётки указанный процесс закончится. □

Следствие. Всякий ненулевой элемент атомной булевой алгебры представим в виде объединения содержащихся в нём атомов.

Действительно, булева алгебра — решётка, а неразложимы в ней — её атомы и только они.

Обозначения для подмножеств элементов (дистрибутивной) решётки L:

- $\operatorname{Irr} L$ — множество неразложимых в объединение элементов L;
- $\operatorname{Irr}(x) = \{ y \in \operatorname{Irr} L \mid y \sqsubseteq x \}$ — множество неразложимых элементов L, содержащихся в x.
- Для решётки с нулём o формально положим $\operatorname{Irr}(o) = \varnothing$.

Доказанная лемма утверждает, что в конечной решётке каждый ненулевой элемент x допускает представление (ср. с 1.1):

$$x = \bigsqcup_{a \in \operatorname{Irr}(x)} a.$$

Построение решётки $J(P)$ казуального ч. у. множества P.

1. Построим диаграмму булевой алгебры $\mathcal{P}(M) = J(M)$ для множества M минимальных элементов P.
2. Выберем некоторый минимальный элемент x множества $P \setminus M$ и пусть S_x — множество непосредственно предшествующих ему элементов.

   Присоединим к $J(M)$ такой элемент $\langle x \rangle$, который неразложим в объединение и непосредственно следует за порядковым идеалом, порождённым S_x.
3. Добавим все объединения имеющихся и вновь построенных элементов с $\langle x \rangle$ так, чтобы они образовали *булеву алгебру*.
4. Выберем новый минимальный элемент y множества $\{P \setminus M\} \setminus \{x\}$ и достроим диаграмму аналогичным способом.
5. Продолжаем так, пока не получим диаграмму $J(P)$.

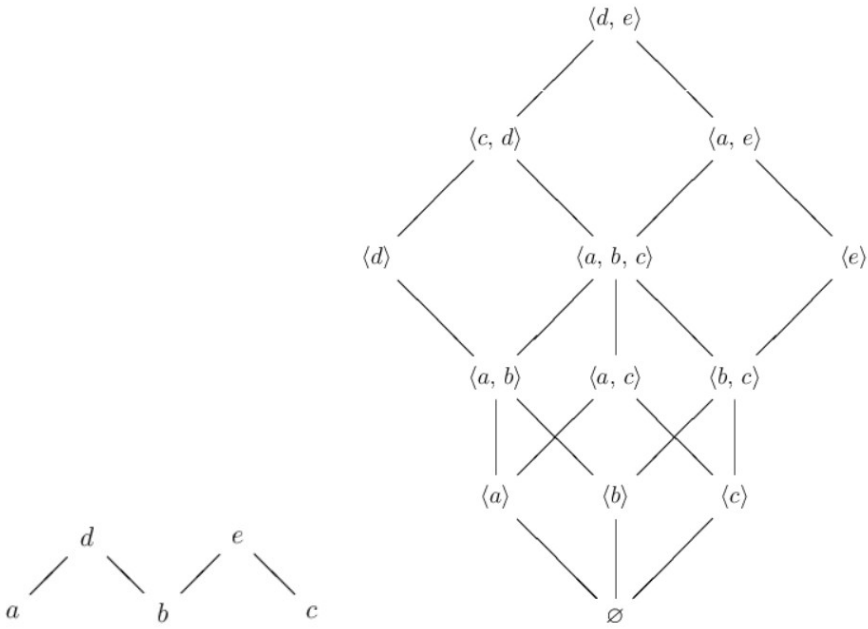


Рис. 4.12. Ч. у. множество Z_5 и решётка $J(Z_5)$ его порядковых идеалов

Пример 4.1.

Продемонстрируем на построенной решётке вычисление некоторых характеристических чисел исходного ч. у. множества Z_5.

$|J(\mathcal{P})|$ — Известно, что Z_n имеет F_{n+2} ($(n+2)$-е число Фибоначчи) порядковых идеалов.

Например, в нашем случае $|J(Z_5)| = F_7 = 13$.

$e(\mathcal{P})$ — Ясно, что каждая максимальная восходящая от наименьшего элемента $\varnothing$ к наибольшему $P^{\triangledown}$ цепь соответствует некоторой линеаризации множества P. Поэтому $e(P)$ равно числу

таких цепей.

Подсчитываем, что таких цепей — 16 (ср. с результатом (3.1):

$$e(Z_5) = \frac{2}{15} \cdot 5! = 16.$$

Лемма 4.3. $\operatorname{Irr} J(P) \cong P$.

Доказательство. Пусть P — ч. у. множество и $J(P)$ — (дистрибутивная) решётка его порядковых идеалов. Порядковый идеал решётки неразложим, если и только если он является главным, откуда:

$$\operatorname{Irr} J(P) \cong J_0(P) = \{ x^\nabla \mid x \in P \}.$$

Ранее был установлен изоморфизм между ч. у. множеством и совокупностью его главных идеалов:

$$\varphi : P \to J(P), \quad \varphi(x) = x^\nabla,$$

поэтому $P \cong J_0(P) = \operatorname{Irr} J(P)$. □

Фундаментальная теорема о конечных дистрибутивных решётках. Следствие из леммы 4.2 утверждает, что если P — ч. у. множество, то $\operatorname{Irr} J(P)$ — дистрибутивная решётка.

Зададимся вопросом, обратимо ли это утверждение, то есть если имеется дистрибутивная решётка L, можно ли подобрать такое ч. у. множество P, чтобы $L \cong J(P)$? Это оказывается возможным в случае конечности L.

Теорема 4.10 (ФТКДР, *Г. Биркгоф*). *Всякая конечная дистрибутивная решётка L изоморфна решётке порядковых идеалов ч. у. множества её неразложимых элементов: $L \cong J(Irr\, L)$.*

Доказательство. Рассмотрим отображение

$$\psi : L \to J(\mathrm{Irr}\ L)\,, \quad \psi(x) = \mathrm{Irr}(x),$$

и покажем сначала его биективность.

Инъективность. Любому ненулевому элементу $x \in L$ сопоставлено множество $\mathrm{Irr}(x)$ содержащихся в нём неразложим элементов и, формально, $\mathrm{Irr}(o) = \varnothing$.

Сюръективность. Пусть $I \subseteq \mathcal{P}(L)$ — множество неразложимых в объединение элементов L.

В рассматриваемом случае конечности L образуем их объединение, и тогда существует элемент $x \in L$ такой, что

$$x = \bigsqcup_I a.$$

Таким образом, ψ — биекция.

С другой стороны,

$$x \sqsubseteq y \;\Leftrightarrow\; \mathrm{Irr}(x) \subseteq \mathrm{Irr}(y) \;\Leftrightarrow\; \psi(x) \subseteq \psi(y).$$

Поэтому ψ — порядковый, а по теореме 4.4 — и решёточный изоморфизм между L и $J(\mathrm{Irr}\ L)$. □

ФТКДР позволяет представлять элементы любой дистрибутивной решётки подмножествами некоторого множества и пользоваться диаграммами Эйлера-Венна.

Решётки с дополнениями

Определение 4.9. Если в решётке $\langle L, \sqcup, \sqcap \rangle$ с универсальными гранями для элемента x существует элемент y такой, что

$$x \sqcap y = o \quad \text{и} \quad x \sqcup y = \iota,$$

то y называется *дополнением элемента* x.

Решётка называется *решёткой с дополнениями*, если в ней каждый элемент имеет хотя бы одно дополнение.

Если каждый элемент решётки обладает в точности одним дополнением, то её называют *решёткой с единственными дополнениями*.

Примеры см. на рис. 4.13.

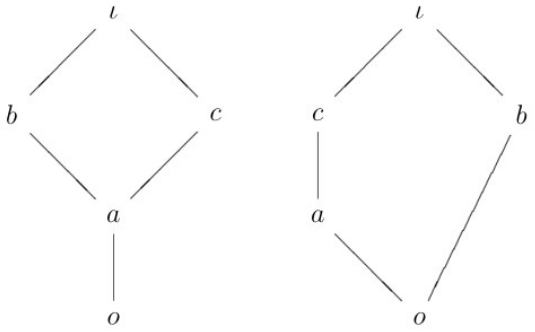


Рис. 4.13. В первой решётке элементы a, b, c не имеет дополнения;
N_5 — решётка с дополнениями: a и c — дополнения b

Утверждение 4.4. *Если ограниченная решётка дистрибутивна, то каждый её элемент имеет не более одного дополнения.*

Доказательство. Пусть элемент x дистрибутивной решётки имеет два дополнения — y_1 и y_2:

$$\begin{cases} x \sqcup y_1 = x \sqcup y_2 = \iota \\ x \sqcap y_1 = x \sqcap y_2 = o \end{cases}$$

Тогда

$$y_1 = y_1 \sqcap (\underbrace{x \sqcup y_2}_{=\iota}) = (\underbrace{y_1 \sqcap x}_{=o}) \sqcup (y_1 \sqcap y_2) =$$
$$= (y_1 \sqcap y_2) \sqcup (\underbrace{x \sqcap y_2}_{=o}) = y_2 \sqcap (\underbrace{y_1 \sqcup x}_{=\iota}) = y_2.$$

□

4.4 Применение теории решёток к задаче классификации

Классификация по прецедентам: постановка задачи

1. Множество *объектов* $\mathcal{X}$ разделено на несколько подмножеств (*классов*).
2. *Информация о таком разбиении содержится только в указании о принадлежности к данным классам элементов конечной обучающей последовательности* (*выборки*) из $\mathcal{X}$, элементы которой называют *прецедентами.*
3. Объекты имеют описание на некотором формальном языке, указывающем степень обладания объектами конечным числом признаков из множества $M = \{x_1, \ldots, x_n\}$.

Классификация: подходы к решению задачи

- статистические методы (ЛДФ, ...);
- метрические методы (NN, ...);
- разделяющие поверхности (SVM, ...);
- потенциальные функции;
- логические методы;
- коллективные решающие правила (области компетенции, голосование, алгебраический подход);
- структурные методы;
- реляционный подход (АФП (FCA), ...)
- ...

Соответствия Галуа. Далее запись отображений: $f(a)$ записывается как af, а $f(A)$ записывается как Af.

Определение 4.10. Пусть $\langle P, \sqsubseteq_P \rangle$ и $\langle Q, \sqsubseteq_Q \rangle$ — ч. у. множества. Пара отображений

$$(\varphi, \psi), \quad \varphi : P \to Q, \ \ \psi : Q \to P,$$

удовлетворяющая свойствам

1) φ и ψ антиизотонны;
2) $\varphi = \varphi\psi\varphi$, $\psi = \psi\varphi\psi$.

называется *соответствием Галуа* между P и Q.

Понятие: философское отступление
Понятие — совокупность суждений об отличительных признаках вещей (объектов) и отношений между ними

Примеры: искусство, наука, ...

Объём понятия — множество всех объектов, обладающих зафиксированными в данном понятии свойствами.

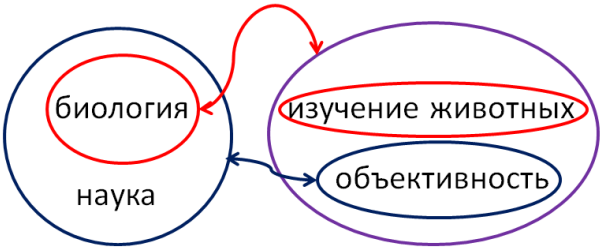
Примеры: искусство: литература, живопись, архитектура,...; наука: биология, физика, химия...

Содержание понятия — совокупность свойств, присущих всем объектам данного понятия.

Примеры: искусство: результат отражения действительности в форме чувственных образов, создание выразительных форм, ...

наука: познавательная деятельность, объективность, систематичность, ...

Закон обратного отношения между содержанием и объёмом понятия: бóльшее по объёму понятие имеет меньшее содержание. Антимонотонность соответствий Галуа отражает этот закон.



Решётка формальных понятий. Обозначения

G — *множество объектов*;

M — *множество признаков*;

I — соответствие между G и M называемое *отношением инцидентности*, то есть gIm означает, что объект $g \in G$ обладает признаком $m \in M$.

Определение 4.11. Тройка $K = (G, M, I)$ называется *формальным контекстом*.

В конечном случае контекст может быть задан в виде *объектно-признаковой* $(0,1)$*-матрицы*.

Утверждение 4.5. *Если для произвольных* $A \subseteq G$ *и* $B \subseteq M$ *формального контекста* (G, M, I) *ввести отображения*

$$\varphi : \mathcal{P}(G) \to \mathcal{P}(M) \quad и \quad \psi : \mathcal{P}(M) \to \mathcal{P}(G)$$

такие, что

$$A\varphi = I(A) \stackrel{\text{def}}{=} A', \qquad B\psi = I^{\sharp}(B) \stackrel{\text{def}}{=} B,$$

то пара (φ, ψ) *будет соответствием Галуа между ч.у. множествами* $\mathcal{P}(G)$ *и* $\mathcal{P}(M)$*, упорядоченными по включению.*

Штрихи над подмножествами $A \subseteq G$ и $B \subseteq M$ называют *операторами Галуа*.

Определение 4.12. Пусть дан контекст $K = (G, M, I)$.
Пара подмножеств (A, B), где $A \subseteq G$, $B \subseteq M$, и таких, что $A' = B$ и $B' = A$, называется *формальным понятием* данного контекста с *формальным объёмом* A и *формальным содержанием* B.

Если контекст представлен в виде объектно-признаковой $(0,1)$-матрицы, то формальному понятию соответствует максимальная её подматрица, заполненная единицами.

Теорема 4.11 (основная АФП). *Множество всех формальных понятий данного контекста* $K = (G, M, I)$ *образует полную решётку, обозначаемую* $\mathfrak{B}(K)$, *относительно операций* $\sqcup$ *(объединение) и* $\sqcap$ *(пересечение):*

$$(A_1,\, B_1) \sqcap (A_2,\, B_2) \;=\; (\, A_1 \cap A_2,\, (A_1 \cap A_2)'\,),$$
$$(A_1,\, B_1) \sqcup (A_2,\, B_2) \;=\; (\, (B_1 \cap B_2)',\, B_1 \cap B_2\,),$$

и называемую решёткой формальных понятий.

В решётке $\mathfrak{B}(K)$ формального контекста $K = (G, M, I)$, если нет разных объектов с одинаковым содержанием:

- $(A_1,\, B_1) \sqsubseteq (A_2,\, B_2) \Rightarrow (A_1 \subseteq A_2)\ \&\ (B_1 \supseteq B_2)$;
- единица ι — формальное понятие $(G,\, G')$;
- атомы — формальные понятия вида $(g,\, g')$, если $g'' = g$;
- нуль o — формальное понятие $(\varnothing,\, M)$ с пустым объёмом.

Пример 4.2. Для объектно–признаковой $(0,1)$-матрицы, представленной на рис. 4.14 построить множество формальных понятий K и решётку $\mathfrak{B}(K)$.
Решение.

$$K \;=\; \{\, (\varnothing \mid M)\,,$$

$G \diagdown M$	a	b	c	d	e	f	g
P	×	×	×	×	×	×	
Q	×	×	×	×	×		×
R	×	×	×	×		×	×
S	×	×	×				
T	×	×			×		
U	×		×			×	
V		×	×				×

Рис. 4.14

$$(P \mid abcdef),\ (Q \mid abcdeg),\ (R \mid abcdfg),$$
$$(PQ \mid abcde),\ (PR \mid abcdf),\ (QR \mid abcdg),$$
$$(PQR \mid abcd),$$
$$(PQT \mid abe),\ (PQRU \mid acf),\ (QRV \mid bcg),$$
$$(PQRS \mid abc),$$
$$(PQTRS \mid ab),\ (PQRSU \mid ac),\ (PQRSV \mid bc),$$
$$(PQRSTU \mid a),\ (PQRSTV \mid b),\ (PQRSUV \mid c),$$
$$(G \mid \varnothing)\}$$

Пояснение: $(S \mid abc)$ не есть формальное понятие, т. к. $S' = \{abc\}$, но $\{abe\}' = \{PQRS\} \neq S$.
Также $(T \mid abe)$ не есть формальное понятие, т. к. $T' = \{abe\}$, но $\{abe\}' = \{PQT\} \neq T$.

Решётка формальных понятий изображена на рис. 4.15.

Пример 4.3 (модель социальной стратификации). Допустим, что по некоторой репрезентативной выборке были проведены социологические исследования, в ко-

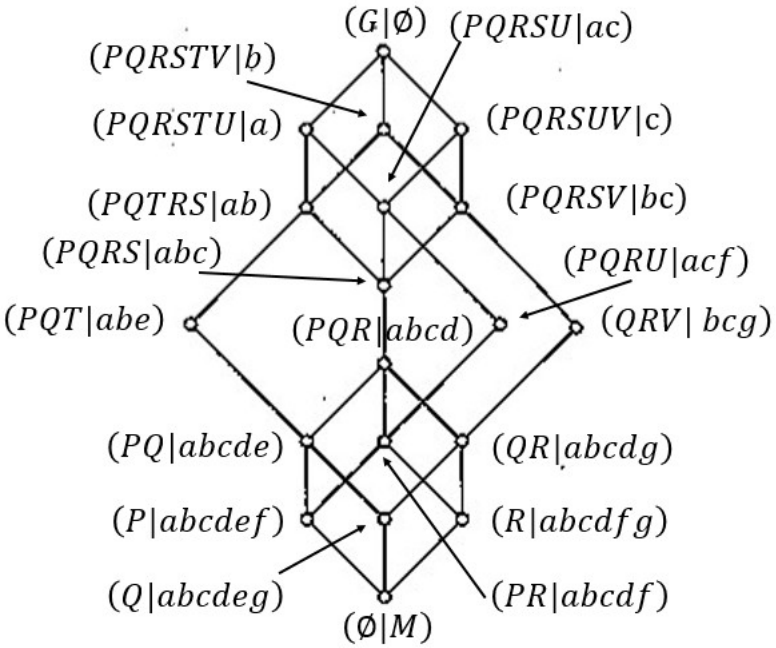


Рис. 4.15

торых получали данные о (1) доходах, (2) числе подчинённых, (3) профессии и (4) хобби населения.

Значения количественных данных (1) и (2) объединены в интервалы

Доход (руб.)	символ
5 000...8 000	a_2
12 000...20 000	a_4
80 000...100 000	a_8
100 000...150 000	a_{14}

# подчинённых (чел.)	символ
0	b_0
до 5	b_1
5...20	b_2
20...100	b_3
500 000...1 000 000	b_7

и получена соответствующая база данных:

Фамилия	(1)	(2)	(3)	(4)
1. Иванов И. И.	a_4	b_1	рабочий	рыбалка
2. Петров В. Г.	a_4	b_1	рабочий	рыбалка
3. Сидоров К. П.	a_4	b_0	рабочий	пение
4. Печкин О. В.	a_8	b_7	чиновник	футбол
5. Березин А. С.	a_{14}	b_3	бизнесмен	шахматы
6. Орлов С. И.	a_2	b_2	учитель	туризм
7. Воробьёв М. В.	a_2	b_0	дьякон	пение
8. Галкин Л. Ю.	a_2	b_0	дворник	рыбалка
# градаций	4	5	6	5

Построить решётку формального контекста понятий $\mathfrak{B}$ для множества объектов, совпадающих с множеством опрошенных и множеством свойств-атрибутов (1)...(4).

Решение. Штрихом $'$ обозначаем соответствия Галуа — антиизотонные отображения множества объектов G во множество содержаний M и обратно такие, что тройное их применение к эквивалентно однократному.

Пара подмножеств $(A,\, B)$, где $A \subseteq G$, $B \subseteq M$, и таких, что $A' = B$ и $B' = A$, называется *формальным понятием* данного контекста с *формальным объёмом* A и *формальным содержанием* B.

Теорема 4.12 (основная АФП). *Множество всех формальных понятий данного контекста K образует полную решётку, обозначаемую $\mathfrak{B}(K)$, относительно операций $\vee$ (объединение) и $\wedge$ (пересечение):*

$$(A_1,\, B_1) \vee (A_2,\, B_2) = \big((B_1 \cap B_2)',\, B_1 \cap B_2\big),$$

$$(A_1,\, B_1) \wedge (A_2,\, B_2) \;=\; (\, A_1 \cap A_2,\, (A_1 \cap A_2)'\,)$$

и называемую решёткой формальных понятий.

Справедливы свойства: в решётке $\mathfrak{B}(K)$ формального контекста $K = (G, M, I)$ —

- $(A_1,\, B_1) \sqsubseteq (A_2,\, B_2) \Rightarrow (A_1 \subseteq A_2)\ \&\ (B_1 \supseteq B_2)$;
- единица ι — формальное понятие $(G,\, G')$;
- атомы — формальные понятия вида $(g,\, g')$, если нет разных объектов с одинаковым содержанием;
- нуль o — формальное понятие $(\varnothing,\, M)$ с пустым объёмом.

Строим формальные понятия.

Имеем $G = \{\, 1,\, 2,\, \ldots,\, 8\,\}$ — множество объектов.

Образуем по базе данных бинарные (1 — имеет место, 0 — не имеет места) 20-мерные векторы номинальных атрибутов объектов $(j_1,\, \ldots,\, j_{20})$, координаты которых соответствуют следующим группам атрибутов.

Данные (1) и (2)

j_1	j_2	j_3	j_4	j_5	j_6	j_7	j_8	j_9
a_2	a_4	a_8	a_{14}	b_0	b_1	b_2	b_3	b_7

Данные (3)

j_{10}	j_{11}	j_{12}	j_{13}	j_{14}	j_{15}
рабочий	чиновник	бизнесмен	учитель	дьякон	дворник

Данные (4)

j_{16}	j_{17}	j_{18}	j_{19}	j_{20}
рыбалка	пение	футбол	шахматы	туризм

Понятия будем обозначать

$$\underbrace{i_1, \ldots, i_k}_{\text{объекты}} \mid \underbrace{j_1, \ldots, j_m}_{\text{атрибуты}}$$

$$i_1 < \ldots < i_k,\ i_1, \ldots, i_k \in \{1, \ldots, 8\},$$
$$j_1 < \ldots < j_m,\ j_1, \ldots, j_m \in \{1, \ldots, 4\}.$$

Нуль решётки $\mathfrak{B}$ есть понятие с нулевым объёмом:

$$\varnothing \mid \underset{(1)}{\underline{1111}}, \underset{(2)}{\underline{11111}}, \underset{(3)}{\underline{111111}}, \underset{(4)}{\underline{11111}}$$

Далее в каждом типе данных персоны 1 будет находится не более, чем в единственной позиции. Для краткости будем указывает только эту позицию. — будет означать что данной множеству персон не присущ ни один признак данной группы.

1. Объекты 1 и 2 неразличимы по атрибутом, им соответствует понятие с объёмом $\{1, 2\}$, итого:

$$1, 2 \mid 0100, 01000, 100000, 10000$$

или сокращённо —

$$\begin{aligned}
1, 2 &\mid [2], [2], [1], [1] \\
3 &\mid [2], [1], [1], [2] \\
4 &\mid [3], [6], [2], [3] \\
5 &\mid [4], [5], [3], [4] \\
6 &\mid [1], [3], [4], [5] \\
7 &\mid [1], [1], [5], [2] \\
8 &\mid [1], [1], [6], [1]
\end{aligned}$$

Это понятия 1-го уровня.

2. Строим понятия 2-го уровня, объединяя понятия 1-го уровня (для удобства — в лексикографическом порядке).

$$1,2,3 \mid [3],\ -,\ [1],\ -$$

Попытка построить понятие с объёмом $\{1,2,4\}$ даёт

$$1,2,4 \mid -,\ -,\ -,\ - \qquad (*)$$

Однако любой набор объектов, содержащий объекты 1, 2 и 4 не будет иметь общих атрибутов, и, таким образом, получено

$$\{1,2,4\}' = G' = \{\,0000, 00000, 000000, 00000\,\},$$

и, таким образом, $(*)$ — **не есть** формальное понятие.

То же имеем для наборов объектов $(1,2,5)$, $(1,2,6)$, $(1,2,7)$ и только для набора $(1,2,8)$ получим

$$1,2,8 \mid -,\ -,\ -,\ -.$$

Далее для объекта 3 новое формальное понятие образует только объединение с 7-м объектом:

$$3,7 \mid -,\ [1],\ -,\ [2]$$

Объединения 4, 5 и 6-го объектов с остальными даёт единицу ι. Объединение 7-го объекта с 8-м даёт новое формальное понятие

$$7,8 \mid [1],\ [1],\ -,\ -$$

3. Строим понятия 3-го уровня, объединяя уже построенные. Здесь получаются два новых понятия:

$$3,7,8 \mid -,\ [1],\ -,\ -$$

$$6,7,8 \mid [1],\ -,\ -,\ -$$

Понятие 4-го уровня только одно — единица ι.

Строим решётку формальных понятий $\mathfrak{B}$ (обозначены, для простоты только множества объектов формальных понятий и понятия ранжируются по числу объектов) — см. рис. 4.16.

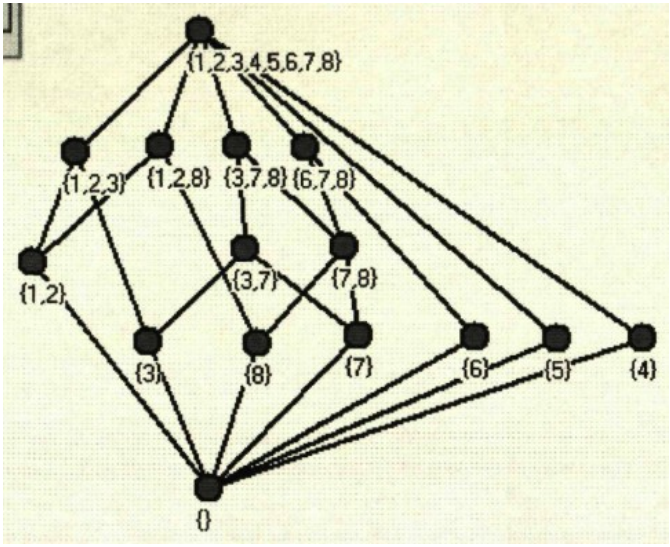


Рис. 4.16. Решение задачи 4.3

Классификация: положительные и отрицательные примеры.

Рассматриваются задачи, в которых множество $\mathcal{X}$ разбито на два непересекающихся класса: $\mathcal{X}^+$ (*положительный*) и $\mathcal{X}^-$ (*отрицательный*) относительно обладания/необладания их объектами некоторым *целевым признаком* $z \notin M$.

Прецеденты из данных классов называются, соответственно, *положительными* и *отрицательными примерами*. Имеем 2 класса и $z = "x \in \mathcal{X}^+"$

Данные для обучения классификации описываются *положительным* $K_+ = (G_+, M, I_+)$ и *отрицательным* $K_- = (G_-, M, I_-)$ *контекстами*.

Операторы Галуа в этих контекстах обозначаются соответствующими *верхними индексами*: A^+, A^-, B^+ и т.д.

Формальное понятие $(A_+, B_+) \in K_+$ будем называть *положительным* с положительными формальным объёмом A_+ и содержанием B_+.

Аналогично определяются *отрицательные* формальные объём и содержание для контекста K_-.

Определение 4.13. Содержание B_+ положительного формального понятия (A_+, B_+) называется:

- *положительной* $\oplus-$*предгипотезой*, если
$$\forall (A_-, B_-) \in K_- : B_+ \neq B_-,$$
т. е. оно не является формальным содержанием ни одного отрицательного понятия;
- *положительной* $\oplus-$*гипотезой*, если
$$\forall (g, g^-) \in K_- : B_+ \not\subseteq g^-,$$
т. е. оно не является подмножеством содержания понятия какого-либо отрицательного примера g;
- фальсифицированной положительной $\oplus-$гипотезой, если
$$\exists (g, g^-) \in K_- : B_+ \subseteq g^-.$$

Отрицательные ($\ominus$—предгипотезы, ...) определяются аналогично.

Гипотеза является также и предгипотезой.

Гипотезы используются для классификации новых объектов

Простейшее решающее правило
Пусть $g \notin \{G_+ \cup G_-\}$ — новый (неопределённый) объект.

Если его формальное содержание g' содержит хотя бы одну

- $\oplus$—гипотезу и не содержит ни одной отрицательной гипотезы, то он относится к положительному классу;
- $\ominus$—гипотезу и не содержит ни одной положительной гипотезы, то он относится к отрицательному классу.

Отказ от классификации происходит, если g':

- либо не содержит никаких гипотез (недостаток данных);
- либо содержит как положительные, так и отрицательные гипотезы (противоречие в данных).

Многозначные контексты.
Для получения бинарной информации о признаках из количественных и качественных признаков используется процедура шкалирования.

Многозначный контекст — это четвёрка (G, M, Z, I), где

- G, M, Z — множества объектов, признаков и значений признаков соответственно,

- I — тернарное отношение $I \subseteq G \times M \times Z$, задающее значение $z \in Z$ признака $m \in M$ объекта $g \in G$,

причем отображение $G \times M \to Z$ функционально.

Шкалирование — это представление многозначных контекстов двузначными.

Пример «Фрукты». *Задача:* построить классификатор по целевому свойству z = «*являться фруктом*» и следующей объектно-признаковой таблице положительных и отрицательных примеров:

№	G \ M	цвет	жёсткий	гладкий	форма	z
1	**яблоко**	жёлтое	нет	да	круглое	+
2	**грейпфрут**	жёлтый	нет	нет	круглый	+
3	**киви**	зелёное	нет	нет	овальное	+
4	**слива**	синяя	нет	да	овальная	+
5	**кубик**	зелёный	да	да	кубический	−
6	**яйцо**	белое	да	да	овальное	−
7	**теннисный мяч**	белый	нет	нет	круглый	−

Результат шкалирования

G \ M	w	y	g	b	f	$\bar{f}$	s	$\bar{s}$	r	$\bar{r}$	z
1		×				×	×		×		+
2		×				×		×	×		+
3			×			×		×		×	+
4				×		×	×			×	+
5			×		×		×			×	−
6	×				×		×			×	−
7	×					×		×	×		−

$G_+ = \{1, 2, 3, 4\}$, $G_- = \{5, 6, 7\}$ $\Rightarrow$ отношение I_+ представлено верхней частью таблицы, а отношение I_- — нижней.

Признаки означают:
w — *белый*, y — *жёлтый*, g — *зелёный*, b — *синий*;
f — *твёрдый*, $\overline{f}$ — *мягкий*,
s — *гладкий*, $\overline{s}$ — *шероховатый*;
r — *круглый*, $\overline{r}$ — *некруглый*.

Формальные понятия $(\{g_1, \ldots, g_q\}, \{m_1, \ldots, m_p\})$ будем обозначать $(g_1, \ldots, g_q \mid m_1, \ldots, m_p)$.

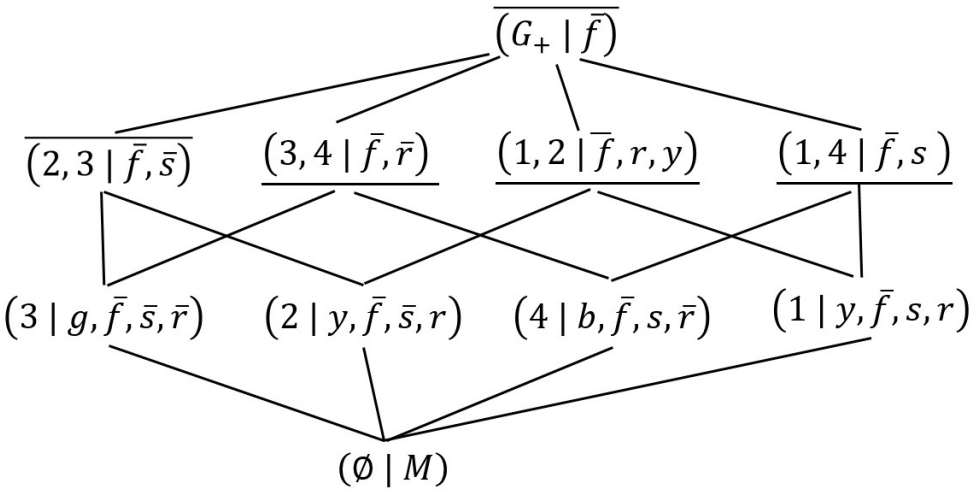


Рис. 4.17. Решётка $\mathfrak{B}(K_+)$. Подчеркнуты положительные $\oplus-$гипотезы, надчёркнуты — фальсифицированые $\oplus-$гипотезы.

Формирование гипотез.
Формальные содержания

- $\{\overline{f}, \overline{r}\}$ (*мягкий*, *некруглый*),
  $\{\overline{f}, r, y\}$ (*мягкий*, *круглый*, *жёлтый*) и
  $\{\overline{f}, s\}$ (*мягкий*, *гладкий*)
  — являются $\oplus-$гипотезами;

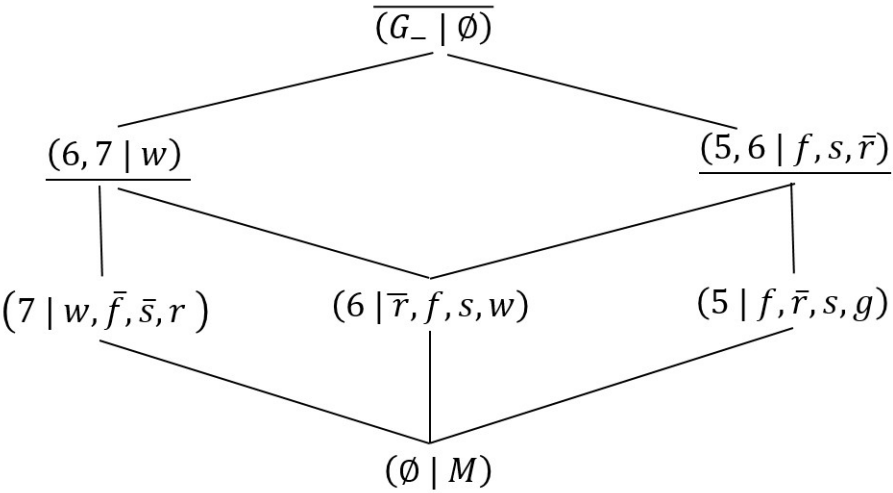


Рис. 4.18. Решётка $\mathfrak{B}(K_-)$

- $\{\overline{f},\overline{s}\}$ (*мягкий*, *шероховатый*) — является фальсифицированной $\oplus$–гипотезой, т. к. она — часть содержания $\{w,\overline{f},\overline{s},r\}$ отрицательного примера 7 (теннисный мяч);

- $\{w\}$ (*белый*) и $\{f,s,\overline{r}\}$ (*твёрдый*, *гладкий*, *некруглый*) — являются $\ominus$–гипотезами.

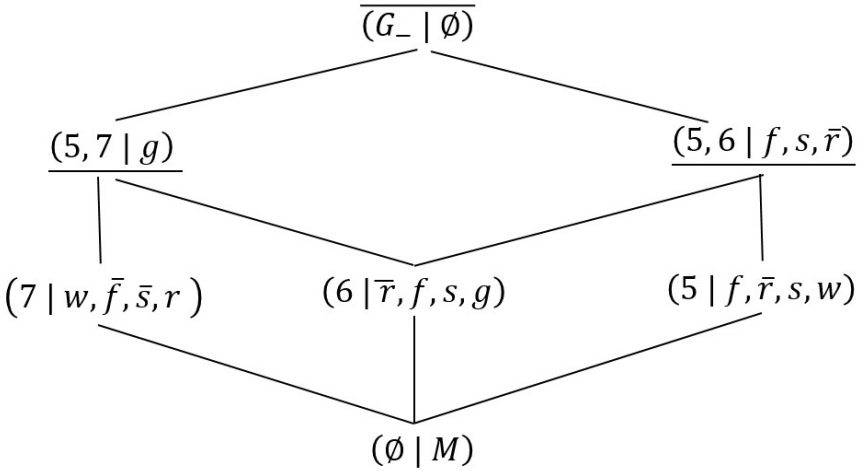
Классификация. Неопределённый объект g

- *мирабель*[1)] будет классифицирован как *фрукт*, т. к. его формальное содержание *жёлтый*, *мягкий*, *гладкий* $\{y,\overline{f},s\}$ содержит $\oplus$–гипотезу $\{\overline{f},s\}$ и не содержит ни одной из $\ominus$–гипотез);

[1)] небольшая круглая слива золотистого цвета

- *кусок сахара* со свойствам *белый*, некруглый, твёрдый будет классифицирован как *не-фрукт*;
- *брикет пломбира* со свойствами *белый*, *мягкий*, *некруглый* вызовет отказ от классификации, поскольку $g' = \{w, \overline{f}, \overline{r}\}$ содержит как положительную $\{\overline{f}, \overline{r}\}$, так и отрицательную $\{w\}$ гипотезы.

Дополнение. Если считать, что теннисный мяч — зелёный[2)], то при таком изменении свойств объекта № 7 изменятся только отрицательный контекст. Теперь $\mathfrak{B}(K_-)$ —



- $\{g\} = \{5, 7\}'$ является фальсифицированной $\ominus$–гипотезой, поскольку она содержится в формальном содержании $\{g, \overline{f}, \overline{s}, \overline{r}\}$ положительного понятия $\{3\}$.

[2)] требование телекомпаний

- $\{f, s, \overline{r}\} = \{5, 6\}'$ является $\ominus-$гипотезой.

Поэтому

- объекты со свойствами *жёлтый*, *мягкий*, *гладкий* и *белый*, *мягкий*, *некруглый* будет классифицированы как *фрукт*;
- на объекте с единственным свойством *белый* произойдёт отказ от классификации.

Недостатки метода:

- построение решётки формальных понятий в реальных случаях чрезвычайно трудоёмко.
- Во-вторых сила алгебраической системы — решётки — недостаточна, в ней отсутствуют отрицания. В ней, например, не может произойти парадокс, подобный парадоксам Рассела или Карри.

  Парадокс Рассела невозможен, поскольку в модели невыразимо отрицание: дополнение формального понятия не является, вообще говоря, формальным понятием.

Глава 5

Булевы алгебры (продолжение)

5.1 Булевы алгебры как решётки

Определение 5.1. Дистрибутивная решётка с дополнениями называется *булевой алгеброй*.

Нетрудно видеть, что оба, вышеприведённое и данное на первой лекции 1.1, определения эквивалентны.

Нетрудно установить следующие два свойства, справедливых для произвольных элементов x и y булевой алгебры с нулевым и единичным элементами с нулём.

1. $x \sqsubseteq y \Leftrightarrow x \sqcap y' = o \Leftrightarrow x' \sqcup y = \iota \Leftrightarrow$
   $\Leftrightarrow x \sqcap y = x \Leftrightarrow x \sqcup y = y$;

   Следует из определения отношения $\sqsubseteq$ —

   $$x \sqsubseteq y \stackrel{\text{def}}{=} x \sqcap y = x \,(\text{или } x \sqsubseteq y \stackrel{\text{def}}{=} x \sqcup y = y)$$

   — и леммы 1.1 об основных соотношениях в булевой алгебре.

2. $x \sqsubseteq y \Leftrightarrow x' \sqsupseteq y'$ — закон антиизотонности дополнения.

$$x \sqsubseteq y \;\Leftrightarrow\; x \sqcap y = x \;\Leftrightarrow\; (x \sqcap y)' = x' \;\Leftrightarrow$$
$$\Leftrightarrow\; x' \sqcup y' = x' \;\Leftrightarrow\; y' \sqsubseteq x' \;\Leftrightarrow\; x' \sqsupseteq y'.$$

Теорема 5.1. *Пусть* $\langle B, \sqcup, \sqcap, ', o, \iota \rangle$ *— булева алгебра и* A *— непустое множество. Тогда множество* B^A *также будет булевой алгеброй относительно операций* $\sqcup, \sqcap$ *и* $'$*, определённых на функциях* $f, g \in B^A$ *поточечно,* $x \in A$*:*

$$(f \sqcup g)(x) = f(x) \sqcup g(x),$$
$$(f \sqcap g)(x) = f(x) \sqcap g(x),$$
$$(f')(x) = (f(x))'.$$

Нулём и единицей B^A *будут постоянные отображения* $f_0(x) \equiv o$ *и* $f_1(x) \equiv \iota$ *соответственно.*

Доказательство — проверка аксиом булевой алгебры. □

При $A = B^n$ получим булеву алгебру B^{B^n} всех функций из B^n в B, и если $B = \mathbf{2}$ — булеву алгебру $\mathbf{2}^{\mathbf{2}^n}$ всех булевых функций от n переменных.

Определение 5.2. *Булевым гомоморфизмом* называют решёточный гомоморфизм φ из булевой алгебры B_1 в булеву алгебру B_2, обеспечивающий равенство

$$\varphi(x') = \varphi(x)' \quad \text{для всех } x \in B_1.$$

То есть булев гомоморфизм — это отображение одной булевой алгебры в другую, согласованное со всеми пятью $(\sqcup,\ \sqcap,\ ',\ o,\ \iota)$ булевыми операциями.

Произвольный решёточный гомоморфизм одной булевой алгебры в другую может и не быть булевым гомоморфизмом (см. п. 2 следующего приимера).

Определение 5.3. Булева алгебра B' называется *подалгеброй булевой алгебры* B, символически $B' \leqslant B$, если $B' \subseteq B$ и на B' устойчивы сужения всех операций B.

Пример 5.1.
1. Булева алгебра $P_{\mathbf{2}}^n$ логических функций от n переменных является подалгеброй алгебры $P_{\mathbf{2}}$ всех логических функций.
2. Пусть $A \subset B$. Тогда $\mathcal{P}(A) \nleqslant \mathcal{P}(B)$, поскольку эти булевы алгебры имеют, например, разные единичные элементы (что повлечёт и несовпадение дополнений в них).

Кольца: определение, основные свойства

Определение 5.4. Абелева группа $\langle R, +, 0 \rangle$ называется *кольцом*, символически $\langle R, +, \cdot, 0 \rangle$, если на ней определена операция умножения $\cdot$, связанная со сложением *дистрибутивными законами*

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{и} \quad (y + z) \cdot x = y \cdot x + z \cdot x.$$

Если умножение обладает свойством ассоциативности и/или коммутативности то и кольцо называют *соответствующе*.

Если в кольце имеется единичный элемент 1 по умножению ($x \cdot 1 = 1 \cdot x = x$), то кольцо называется

кольцом с единицей или *унитальным*, символически $\langle R, +, \cdot, 0, 1 \rangle$.

Элемент a унитального кольца называется *обратимым*, если существует элемент b такой, что

$$a \cdot b = b \cdot a = 1.$$

Определение 5.5. Ассоциативное кольцо, обладающие свойством $x^2 = x$ для любого своего элемента называется *булевым кольцом*.

Теорема 5.2. *Булево кольцо R коммутативно и в нём $-x = x$ для любого элемента $x \in R$.*

Доказательство. Докажем сначала второе, а потом первое утверждения:

$$\begin{aligned} x + x &= (x+x)^2 = x^2 + x^2 + x^2 + x^2 = \\ &= (\underbrace{x+x}_{=0}) + (x+x) \;\Rightarrow\; x = -x; \end{aligned}$$

$$\begin{aligned} x + y &= (x+y)^2 = x^2 + xy + yx + y^2 = \\ &= x + \underbrace{xy + yx}_{=0} + y \;\Rightarrow\; xy = -yx = yx. \end{aligned}$$

□

Теорема 5.3. *Пусть $\mathfrak{B} = \langle B, \sqcup, \sqcap, ', o, \iota \rangle$ — булева алгебра. Для любых $x, y \in B$ положим*

$$x + y = (x \sqcap y') \sqcup (x' \sqcap y), \quad x \cdot y = x \sqcap y.$$

Тогда $AC\,\mathfrak{B}^* = \langle B, +, \cdot, o, \iota \rangle$ — булево кольцо с единицей ι.

Доказательство. Покажем, что введённая операция $+$ образует на носителе B абелеву группу.

Коммутативность + очевидна. Покажем ассоциативность + (далее не различаем операции умножения и пересечения):

$$\begin{aligned}(x+y)+z &= (xy' \sqcup x'y)z' \sqcup (xy' \sqcup x'y)'z = \\ &= xy'z' \sqcup x'yz' \sqcup (x' \sqcup y)(x \sqcup y')z = \\ &= xy'z' \sqcup x'yz' \sqcup x'y'z \sqcup xyz\,, \\ x+(y+z) &= x(yz' \sqcup y'z)' \sqcup x'(yz' \sqcup y'z) = \\ &= x(y' \sqcup z)(y \sqcup z') \sqcup x'yz' \sqcup x''y = \\ &= xy'z' \sqcup xyz \sqcup x'yz' \sqcup x'y'z\,,\end{aligned}$$

и ассоциативность операции + показана.

Свойство нуля: $x+o = xo' \sqcup x'o = x\iota = x$ и тебуемое показано.

Для операции $\cdot = \sqcap$ необходимо показать только её дистрибутивность относительно сложения:

$$\begin{aligned}(x+y)z &= (xy' \sqcup x'y)z = xy'z \sqcup x'yz\,, \\ xz+yz &= xz(yz)' \sqcup (xz)'(yz) = \\ &= xz(y' \sqcup z') \sqcup (x' \sqcup z')yz = xy'z \sqcup x'yz.\end{aligned}$$

□

Основным примером булева кольца и является как раз кольцо $\langle\, \mathcal{P}(A),\, +,\, \cap,\, \varnothing,\, A \,\rangle$, получаемое указанным способом из тотальной алгебры множеств.

Теорема 5.4. *Пусть* $\mathfrak{R} = \langle\, R,\, +,\, \cdot,\, 0,\, 1 \,\rangle$ *— булево унитальное кольцо. Для любых* $x,\, y \in R$ *положим*

$$x \sqcup y = x + y + x \cdot y, \quad x \sqcap y = x \cdot y\,, \quad x' = x + 1.$$

Тогда $AC\ \mathfrak{R}^* = \langle\, R,\, \sqcup,\, \sqcap,\, ',\, 0,\, 1 \,\rangle$ *— булева алгебра.*

Доказательство. Нужно показать справедливость законов 1)–8) в определении 1.1 булевой алгебры. Очевиды выполнения всех законов, кроме дистрибутивных.

Выкладка

$$(x \sqcup y) \sqcap z \;=\; (x + y + xy)z \;= \\ = \; xz + yz + xyz \;=\; (x \sqcap z) \sqcup (y \sqcap z)$$

доказывает справедливость в $\mathfrak{B}^*$ первого дистрибутивного закона, и аналогичго – второго. □

Т.о. любое булево кольцо с единицей может быть задано с помощью булевой алгебры и наоборот.

Следствие $\mathfrak{B}^{**} = \mathfrak{B}$ и $\mathfrak{R}^{**} = \mathfrak{R}$ устанавливает *стоуновскую двойственность* между булевыми алгебрами и булевыми кольцами.

Определение 5.6. АС $\langle\, B, \sqcup, \sqcap, ', \sqsubseteq, o, \iota \,\rangle$ такая, что $\langle\, B, \sqcup, \sqcap, ', o, \iota \,\rangle$ — булева алгебра, а отношение $\sqsubseteq$ задаются по правилу

$$x \sqsubseteq y \;\stackrel{\text{def}}{=}\; x \sqcap y = x \;\; (\text{или} \;\; x \sqsubseteq y \;\stackrel{\text{def}}{=}\; x \sqcup y = y)$$

называется *булевой структурой.*

Утверждение 5.1. *Элемент a булевой алгебры B является атомом, если и только если $o \lessdot a$.*

Доказательство. Пусть a и b — ненулевые элементы булевой алгебры B. Тогда

- $o \lessdot a \;\Rightarrow\; \left[\begin{array}{l} a \sqsubseteq b, \\ a \not\sim b, \end{array}\right. \;\Leftrightarrow\; \left[\begin{array}{l} a \sqcap b = a, \\ a \sqcap b = o. \end{array}\right. \;\Leftrightarrow\; a \in At(B);$

- если $a \in At(B)$ и найдётся такое b, что $b \sqsubset a$, то

$$a \sqcap b = b \left\{ \begin{array}{l} b \neq, \\ b \neq o, \end{array} \right. \Rightarrow a \notin At(B).$$

□

5.2 Идеалы и фильтры

Определение 5.7. *Идеалом* [фильтром] I булевой алгебры B называют её решёточные идеалы, символически $I \trianglelefteqslant B$ [фильтры].

Каждый булев идеал I и фильтр F булевой алгебры B обладает всеми свойствами решёточных, и, кроме этих, ещё и

$$\left\{ \begin{array}{l} x \in I \\ x' \in I \end{array} \right. \Rightarrow I = B \quad \text{и} \quad \left\{ \begin{array}{l} x \in F \\ x' \in F \end{array} \right. \Rightarrow F = B.$$

Действительно, по определению идеала $\iota = x \sqcup x' \in I$, откуда $I = B$ и аналогично для фильтров.

На идеалы и фильтры булевой алгебры переносятся понятия собственных, несобственных и главных идеалов и фильтров. Поскольку булева алгебра есть решётка, то в конечной булевой алгебре все идеалы и фильтры — главные.

Пример 5.2. 1. Пусть $B \subseteq A$. Тогда совокупность всех подмножеств множества A, содержащихся в B, есть идеал булевой алгебры $\mathcal{P}(A)$, а содержащих

B — фильтр $\mathcal{P}(A)$. Это — *главные идеалы и фильтры в бесконечной булевой алгебре.*

2. Приведём пример неглавных идеалов и фильтров. Пусть A — бесконечное множество. Совокупность $\mathcal{P}_0(A)$ всех конечных подмножеств A есть неглавный идеал, а неглавный фильтр булевой алгебры $\mathcal{P}(A)$ — совокупность подмножеств, имеющих конечное дополнение до A. Его называют *фильтром Фреше.*

Определение 5.8. Идеал [фильтр] булевой алгебры называется *максимальным*, если он не содержится ни в каком другом собственном идеале [фильтре].

Фильтр булевой алгебры B называется *ультрафильтром* если для любого $b \in B$ ему принадлежит в точности один из элементов b и b'.

Понятно, что если x — атом [коатом] конечной булевой алгебры, то $x^{\triangle}$ [$x^{\triangledown}$] — её максимальный фильтр [идеал]. В конечных булевых алгебрах ультрафильтры других видов, очевидно (как в решётках), отсутствуют.

5.3 Булевы уравнения

Булевы многочлены. Полиномиальная функция

Определение 5.9. Пусть заданы n-множество *переменных* $X_n = \{ x_1, \ldots, x_n \}$ и *константы* 0, 1.

Тогда

1) $x_1, \ldots, x_n, 0, 1$ — *булевы многочлены*;
2) если p и q — булевы многочлены, то таковыми являются и $(p \sqcup q)$, $(p \sqcap q)$, (p').

Множество всех булевых многочленов от переменных из X_n обозначим M_n.

Ясно, что булевы многочлены — это формулы из переменных и констант над множеством символов операций $\{\sqcup, \sqcap, '\}$.

Отношение равенства элементов из M_n вводится как *синтаксическое тождество*: многочлены p и q равны, символически $p = q$, если p и q *совпадают как строки символов*. Далее пользуемся известными правилами экономии скобок.

Очевидно, M_n не есть булева алгебра: например, $x_1 \sqcup x_2 \neq x_2 \sqcup x_1$.

Определение 5.10. Пусть B — булева алгебра и p — булев многочлен из M_n. Обозначим через $\widehat{p}_B(b_1, \ldots, b_n)$ элемент из B, который получается из p заменой

$$x_i \mapsto b_i \in B,\ i = \overline{1, n},$$

а отображение

$$\widehat{p}_B : B^n \to B,$$

сопоставляющее вектор $(b_1, \ldots, b_n) \in B^n$ элемент $\widehat{p}_B(b_1, \ldots, b_n) \in B$ назовём *полиномиальной функцией, индуцированной булевым многочленом* p.

Если булева алгебра B фиксирована, то нижний индекс у символов элемента $\widehat{p}_B(b_1, \ldots, b_n)$ и полиномальной функции $\widehat{p}_B$ будем опускать.

Пример 5.3 (везде $n = 2$). 1. Пусть $B = \mathbf{2} = \{0, 1\}$, $p = x_1 \sqcup x_2$ и $q = x_2 \sqcup x_1$.

Тогда $p \neq q$, но полиномиальные функции этих многочленов совпадают: $\widehat{p} = a \vee b = b \vee a = \widehat{q}$ и при любой замене в них аргументов a и b элементами $\{0, 1\} \in \mathbf{2}$ получим один и тот же элемент.

2. Пусть A — множество, $B = \mathcal{P}(A)$, $p = (x_1 \sqcup x_2)'$ и $q = {x_1}' \sqcap {x_2}'$.

Тогда опять $p \neq q$, а $\widehat{p} = \overline{X \cup Y}$ и $\widehat{q} = \overline{X} \cap \overline{Y}$, где $X, Y \subseteq A$, то есть снова $\widehat{p} = \widehat{q}$.

Введём обозначение $P_B^n = \{\, \widehat{p}_B \mid p \in M_n \,\}$ — множество всех полиномиальных функций, индуцированных многочленами из M_n на B. Ясно, что $P_B^n \subseteq B^{B^n}$.

Теорема 5.5. *P_B^n — булева подалгебра B^{B^n}.*

Доказательство. Убеждаемся в очевидной устойчивости помножества P_B^n множества B^{B^n} относительно операций булевой алгебры. Также P_B^n и B^{B^n} содержат функции $f_0 \equiv 0$ и $f_1 \equiv 1$. □

Определение 5.11. Два булевых многочлена $p, q \in M_n$ называются *эквивалентными*, символически $p \sim q$, если равны их полиномиальные функции на $\mathbf{2}$, то есть $p \sim q \;\Leftrightarrow\; \widehat{p}_{\mathbf{2}} = \widehat{q}_{\mathbf{2}}$.

Действительно, $\sim$ есть отношение эквивалентности на M_n (все свойства $\sim$ наследуются из свойств $=$).

Теорема 5.6. *Пусть* $p, q \in M_n$ *и* B *— произвольная булева алгебра. Тогда* $\widehat{p}_{\mathbf{2}} = \widehat{q}_{\mathbf{2}} \Rightarrow \widehat{p}_B = \widehat{q}_B$.

Теорема 5.7. $M_n/\sim \cong_b P_{\mathbf{2}}^n$.

То есть $M_n/\sim$ есть булева алгебра, изоморфная $P_{\mathbf{2}}^n$.

Доказательство. Определим отображение

$$\varphi\colon P_{\mathbf{2}}^n \to M_n/\sim,$$

переводящее полиномиальную функцию $P_{\mathbf{2}}^n$, индуцированную многочленом p на $\mathbf{2}$, в класс эквивалентности $[p]_\sim$. Определение корректно, т. к.

$$\widehat{p}_{\mathbf{2}} = \widehat{q}_{\mathbf{2}} \Rightarrow p \sim q \Rightarrow [p]_\sim = [q]_\sim.$$

Ясно, что φ и есть искомый булев изоморфизм. □

Таким образом для произвольной булевой алгебры B имеем цепочку

$$B^{B^n} \geqslant P_B^n \cong_b P_{\mathbf{2}}^n \cong_b M_n/\sim .$$

Если $P_B^n \cong B^{B^n}$, то назовём булеву алгебру B *полиномиально полной*; это означает, что каждую её функцию можно представить полиномом.

Из единственности представления булевых функций в виде совершенных ДНФ, КНФ или АНФ (полиномов Жегалкина), следует, что

$$|M_n/\sim| = 2^{2^n}.$$

Отсюда:

- поскольку $M_n/\sim \cong P_{\mathbf{2}}^n$, то алгебра $\mathbf{2}$ полиномиально полна.

- если $|B| = m > 2$, то

$$|P_B^n| = |M_n/\sim| = 2^{2^n} < m^{m^n} = |B^{B^n}|,$$

то есть $\mathbf{2}$ — единственная полиномиально полная булева алгебра.

Определение 5.12. Пару (p, q), где $p, q \in M_n$ назовём *булевым уравнением.*

Пусть B — произвольная булева алгебра. Элемент $(b_1, \ldots, b_n) \in B^n$ называется *решением уравнения* (p, q) *в булевой алгебре* B, если

$$\widehat{p}_B(b_1, \ldots, b_n) = \widehat{q}_B(b_1, \ldots, b_n).$$

Совокупность $\{ (p_i, q_i) \mid i = \overline{1, m} \}$ образует систему из m уравнений.

Уравнение (p, q) допустимо записывать в виде $p = q$. Например, $x_1{}'x_2 \vee x_3 = x_1(x_2 \vee x_3)$ — булево уравнение в $\mathbf{2}$, а (101) — его решение. Эквивалентное преобразование булева уравнения

Теорема 5.8. *Уравнения*

$$p = q \quad и \quad (p \sqcap q') \sqcup (p' \sqcap q) = 0$$

имеют одни и те же решения.

Доказательство. Пусть B — булева алгебра и $b \in B^n$. Положим $x = \widehat{p}(b)$ и $y = \widehat{q}(b)$.

Тогда, с одной стороны,

$$x = y \Rightarrow (x \sqcap y') \sqcup (x' \sqcap y) = (x \sqcap x') \sqcup (x' \sqcap x) = 0 \sqcup 0 = 0,$$

а с другой —

$$(x \sqcap y') \sqcup (x' \sqcap y) = 0 \Rightarrow \begin{cases} x \sqcap y' = 0 \\ x' \sqcap y = 0 \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} x \sqcap y' = 0 \\ x \sqcup y' = 1 \end{cases} \Rightarrow a = y'' \Leftrightarrow x = y\,.$$

□

По данной теореме система уравнений

$$\{\,(p_i,\, q_i) \mid i = 1,\, \ldots,\, m\,\}\,.$$

эквивалентна единственному уравнению

$$\bigsqcup_{i=1}^{m} ((p_i \sqcap q_i') \sqcup (p_i' \sqcap q_i)) = 0 \qquad (*).$$

Если решение ищется в алгебре $\mathbf{2}$, то выразив левую часть в КНФ, получим, что уравнение $(*)$ имеет решение, когда хотя бы один из сомножителей принимает значение 0 и, приравнивая их последовательно к 0, находят все решения системы.

Пример 5.4. Решим в $\mathbf{2}$ систему

$$\{\,(x_1x_2,\, x_1x_3 \vee x_2),\, (x_1 \vee x_2',\, x_3)\,\}\,.$$

Перепишем систему в привычном виде

$$\begin{cases} x_1x_2 = x_1x_3 \vee x_2\,, \\ x_1 \vee x_2' = x_3. \end{cases}$$

Она эквивалентна единственному уравнению

$$x_1x_2(x_1x_3 \vee x_2)' \vee (x_1x_2)'(x_1x_3 \vee x_2) \vee$$
$$\vee (x_1 \vee x_2')x_3' \vee (x_1 \vee x_2')'x_3 = 0.$$

Преобразуя левую часть в КНФ, получим уравнение

$$(x_1 \vee x_2 \vee x'_3)(x'_1 \vee x'_2 \vee x'_3) = 0.$$

Таким образом, решения рассматриваемой системы — элементы $(b_1, b_2, b_3) \in \mathbf{2}^3$ удовлетворяющие соотношениям $(b_1 \vee b_2 \vee \bar{b}_3)(\bar{b}_1 \vee \bar{b}_2 \vee \bar{b}_3) = 0$, то есть это (001) и (111).

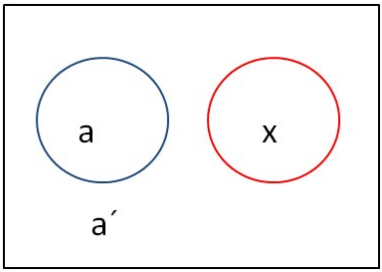
Системы булевых уравнений. В общем случае, когда решение ищется не в простейшей, а в произвольной булевой алгебре $B \neq \mathbf{2}$, то приведение уравнения $(*)$ к КНФ приводит к потере решений, поскольку B не обладает свойством полиномиальной полноты, и в ней из $a \sqcap b = o$ *не следует*, что либо $a = o$, либо $b = o$.

Выкладки в булевой структуре $\langle B, \sqcup, \sqcap, ', \sqsubseteq, o, \iota \rangle$

1. $a \sqcap x = 0 \Leftrightarrow (a \sqcap x) \sqcup a' = a' \Leftrightarrow$

$$\Leftrightarrow (a \sqcup a') \sqcap (x \sqcup a') = a' \Leftrightarrow x \sqcup a' = a' \Leftrightarrow x \sqsubseteq a' \ (\Leftrightarrow a \sqsubseteq x').$$

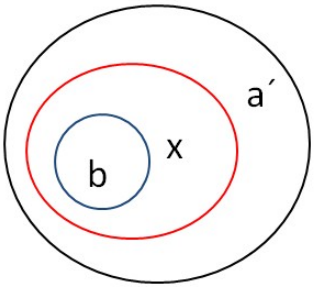
Аналогично $b \sqcap x' = 0 \Leftrightarrow b \sqsubseteq x$.

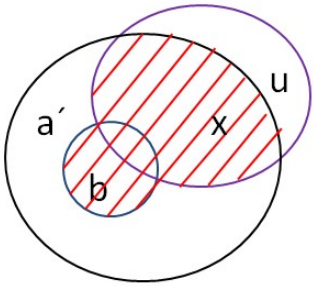


2.

$$\left\{\begin{array}{l} b \sqsubseteq x \\ x \sqsubseteq a' \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} \exists\, u \in B : x = b \sqcup u, \\ x \sqcap a' = x, \end{array}\right. \Leftrightarrow$$

$$\Leftrightarrow\ x = (b \sqcup u) \sqcap a' \ \Leftrightarrow\ x = (a' \sqcap u) \sqcup b.$$





Решение булева уравнения с одним неизвестным. Пусть в булевой структуре $\langle\, B, \sqcup, \sqcap, ', \sqsubseteq, o, \iota \,\rangle$ задано уравнение $p = q$, где $p, q \in P_1$.

Метод его решения состоит в выполнении следующих шагов.

1. Приводим данное уравнение к равносильному уравнению с o в правой части.
2. Приводим полученное уравнение к равносильному уравнению вида $(a \sqcap x) \sqcup (b \sqcap x') = o$, где a и b — известные элементы B.
3. Заменяем полученное уравнение на эквивалентную систему
$$a \sqcap x = o, \qquad b \sqcap x' = o.$$
4. Если $b \not\sqsubseteq a'$, то исходное уравнение решения не имеет. Иначе, искомое решение — x такой, что

$b \sqsubseteq x \sqsubseteq a'$ или $x = (b \sqcup u) \sqcap a' = (a' \sqcap u) \sqcup b$,

где u — произвольный элемент B.

Пример 5.5. Решим в булевой структуре уравнение

$$x \sqcup c = d.$$

1. $x \sqcup c = d \Leftrightarrow \big((x \sqcup c)' \sqcap d\big) \sqcup \big((x \sqcup c) \sqcap d'\big) = o.$

2. $\big((x \sqcup c)' \sqcap d\big) \sqcup \big((x \sqcup c) \sqcap d'\big) =$
$= (x' \sqcap c' \sqcap d) \sqcup (x \sqcap d') \sqcup (c \sqcap d') =$
$= (x' \sqcap c' \sqcap d') \sqcup \underline{(x \sqcap d') \sqcup (x \sqcap c \sqcap d')} \sqcup (x' \sqcap c \sqcap d') =$
$= \big(x \sqcap \underbrace{(d' \sqcup (c \sqcap d'))}_{d'}\big) \sqcup \big(x' \sqcap ((c' \sqcap d) \sqcup (c \sqcap d'))\big) = o.$

3. Имеем $d' \sqcap x = o$, $\big((c' \sqcap d) \sqcup (c \sqcap d)'\big) \sqcap x' = o.$

4. Исходное уравнение имеет решение если и только если
$$(c' \sqcap d) \sqcup (c \sqcap d') \sqsubseteq d.$$
Покажем, что данное условие эквивалентно $c \sqsubseteq d$:
$$\begin{aligned}
\big((c' \sqcap d) \sqcup (c \sqcap d')\big) &\sqsubseteq d;\\
(c' \sqcap d) \sqcup (c \sqcap d') \sqcup d &= d;\\
(c' \sqcap d) \sqcup \big((c \sqcup d) \sqcap (\underbrace{d' \sqcup d}_{=\iota})\big) &= d;\\
(c' \sqcap d) \sqcup c \sqcup d &= d;\\
\big((\underbrace{c' \sqcup c}_{=\iota}) \sqcap (d \sqcup c)\big) \sqcup d &= d;\\
d \sqcup c &= d;\\
c &\sqsubseteq d.
\end{aligned}$$

Общее решение исходного уравнения —

$$x \;=\; \big(c' \sqcap d) \;\sqcup\; (c \sqcap d') \sqcup u\big) \sqcap d \;= \\ = \;(c' \sqcap d) \;\sqcup\; (u \sqcap d) \;=\; d \sqcap (c' \sqcup u),$$

где u — произвольный элемент булевой структуры B.

Необязательная проверка:

$(d \sqcap (c' \sqcup u)) \sqcup c \overset{Dtr}{=} (d \sqcup c) \sqcap \iota \;=\; d \sqcup c \overset{c \sqsubseteq d}{=} d.$

Глава 6

Идемпотентная алгебра

6.1 Тропическая математика

Тропическая (идемпотентная) математика — область прикладной математики, связанная с изучением полуколец с идемпотентным сложением[1)].

За последние десятилетия эта область превратилась в один из наиболее быстро развивающихся разделов математики.

Причинами интереса к идемпотентной математике является то, что многие классические задачи оптимизации могут быть описаны при помощи линейных векторных уравнений идемпотентной алгебры. Это открывает новые возможности для исследования таких систем на основе подходящим образом определенных идемпотентных аналогов математических объектов, методов классической линейной алгебры и теории линейных динамических систем.

[1)] Название «тропическая» отсылает к бразильской школе — пионерским работам бразильского математика венгерского происхождения Имре Ши́мона (1943–2009).

6.2 Идемпотентные полукольцо и полуполе

Определение, примеры и свойства. Рассмотрим АС $\langle\, \mathbb{X};\, \oplus,\, \otimes,\, \mathbb{O},\, \mathbb{I}\,\rangle$, где носителем $\mathbb{X}$ является некоторое числовое множество с выделенными нулевым $\mathbb{O}$ и единичным $\mathbb{I}$ элементами, а операции сложения $\oplus$ и умножения $\otimes$ обладают следующими свойствами (далее x, y, z — произвольные элементы $\mathbb{X}$).

1. Относительно сложения множество $\mathbb{X}$ *идемпотентный коммутативный моноид*:

1) $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ — ассоциативность,
2) $x \oplus y = y \oplus x$ — коммутативность,
3) $x \oplus \mathbb{O} = x$ — свойство $\mathbb{O}$,
4) $x \oplus x = x$ — идемпотентность (Id)[2)].

2. Относительно умножения множество $\mathbb{X} \setminus \{\mathbb{O}\}$ — коммутативная группа:

5) $x \otimes (y \otimes z) = (x \otimes y) \otimes z$ — ассоциативность,
6) $x \otimes y = y \otimes x$ — коммутативность,
7) $x \otimes \mathbb{I} = x$ — свойство $\mathbb{I}$,
8) если $x \neq \mathbb{O}$, то существует элемент x^{-1} такой, что $x \otimes x^{-1} = \mathbb{I}$ — существование *обратного*.

3. Сложение и умножение связаны свойствами:

9) $x \otimes (y \oplus z) = x \otimes y \oplus x \otimes z$ — дистрибутивность,

[2)] Если бы вместо 4) стояло условие существования противоположного элемента, по сложению мы имели бы коммутативную группу.

10) $x \otimes \mathbb{O} = \mathbb{O}$ — закон поглощения (нуль по сложению является нулём по умножению)[3].

Данную АС можно назвать *идемпотентным полуполем*. Если свойство 8) не имеет места, получаем *идемпотентное полукольцо*.

В силу ассоциативности $\otimes$ на $\mathbb{X}$ естественным образом вводится операция *возведения в натуральную степень любого его элемента*, которая также естественно распространяется на случай рационального показателя степени (при записи показателя степени применяются обычные арифметические операции). Далее в алгебраических выражениях знак умножения $\otimes$, как обычно, будем опускать.

Введём на $\mathbb{X}$ бинарное отношение $\leq$ по правилу

$$x \leq y \;\Leftrightarrow\; x \oplus y = y,$$

которое является отношением частичного порядка; покажем это.

R: $\quad x \leq x \;\Leftrightarrow\; x \oplus x = x;$

AS:

$$\left\{ \begin{array}{l} x \leq y, \\ y \leq x, \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} x \oplus y = y, \\ y \oplus x = x, \end{array} \right. \Leftrightarrow\; x = y;$$

T:

$$\left\{ \begin{array}{l} x \leq y, \\ y \leq z, \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} x \oplus y = y, \\ y \oplus z = z, \end{array} \right. \Rightarrow$$

$$\Rightarrow\; x \oplus (\underbrace{y \oplus z}_{=z}) = \underbrace{y \oplus z}_{=z} \;\Leftrightarrow\; x \leq z.$$

[3] нужно в связи с отсутствием элемента, противоположного по сложению.

Элементарно показываются следующие свойства отношения $\leq$ для любых $x, y, z \in \mathbb{X}$:

накопление — $x \leq x \oplus y$:

$$x \oplus y = x \oplus y \overset{Id}{\Rightarrow} x \oplus (x \oplus y) = x \oplus y \Rightarrow x \leq x \oplus y;$$

монотонность по $\oplus$ *и* $\otimes$ — из $x \leq y$ следует

$$x \oplus z \leq y \oplus z \text{ и } xz \leq yz;$$

неотрицательность — $\mathbb{O} \leq x$, откуда $\mathbb{O} < \mathbb{I}$.

Во многих задачах, включая рассматриваемые ниже примеры и приложения, введенный порядок оказывается *линейным*.

Примеры 6.1 (полуполей).

1. $\mathbb{R}_{\max,+} = \langle \underbrace{\mathbb{R} \cup \{-\infty\}}_{\mathbb{X}}; \underbrace{\max}_{\oplus}, \underbrace{+}_{\otimes}, \underbrace{-\infty}_{\mathbb{O}}, \underbrace{0}_{\mathbb{I}} \rangle$.

Свойства:

- для каждого $x \in \mathbb{X}$ существует *обратный элемент* x^{-1}, равный $-x$ в обычной арифметике;
- для любых $x, y, \in \mathbb{R}$ определена *степень* x^y, равная xy в обычной арифметике;
- *порядок* $\leq$ совпадает с обычным линейным.

2. Введём обозначение $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$.
$\mathbb{R}_{\min,\times} = \langle \mathbb{R}_+ \cup \{+\infty\}; \min, \times, +\infty, 1 \rangle$.

Свойства:

- *обратный элемент* и *степень* имеют обычный смысл;
- *порядок* $\leq = \geqslant$, то есть он двойственен обычному линейному, а максимальным элементом служит 0.

3. $\mathbb{R}_{\max,\times} = \langle\, \mathbb{R}_+ \cup \{0\};\ \max,\ \times,\ 0,\ 1 \,\rangle$.
4. $\mathbb{R}_{\min,+} = \langle\, \mathbb{R} \cup \{+\infty\};\ \min,\ +,\ +\infty,\ 0 \,\rangle$.

Легко видеть, что рассмотренные полуполя изоморфны друг другу, и на рис. 6.1 приведена соответствующая диаграмма.

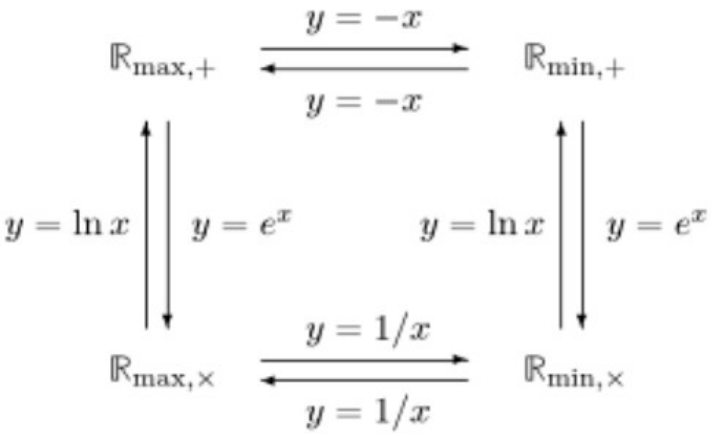


Рис. 6.1. Изоморфизм полуполей

Пример 6.1 (идемпотентного полукольца, не являющегося полуполем).

$$\mathbb{R}_{\max,\min} = \langle\, \mathbb{R} \cup \{-\infty\} \cup \{+\infty\},\ \max,\ \min,\ -\infty,\ +\infty \,\rangle.$$

Свойства:

- *обратного элемента* по отношению к операции «умножения» min не существует;
- понятие *степени* не определяется;
- *порядок* $\leq$ совпадает с обычным линейным, максимальным элементом является $+\infty$, а минимальным — $-\infty$.

Метрика. На полукольце $\mathbb{X}$ определим функцию расстояния ρ следующим образом: для любых $x, y \neq \mathbb{O}$ положим

$$\rho(x,y) \;=\; xy^{-1} \oplus x^{-1}y.$$

Легко убедится, что тогда функция ρ принимает значения на интервале $[\mathbb{I}, \infty)$. Поэтому естественно положить

$$\rho(x,y) \;=\; \begin{cases} \mathbb{I}, & \text{если } x = y = \mathbb{O}, \\ \infty, & \text{если один из аргументов} \\ & \text{равен нулю, а другой} \\ & \text{отличен от нуля.} \end{cases}$$

Функция ρ удовлетворяет условию *симметрии и неравенству треугольника*, что позволяет использовать её в качестве метрики на $\mathbb{X}$. Например, в полуполе $\mathbb{R}_{\max,+}$ она совпадает с обычным расстоянием

$$\rho(x,y) \;=\; \max\{\, x-y,\, y-x \,\} \;=\; |x-y|.$$

Заметим, что введение метрики позволяет естественным образом определить на полукольце $\mathbb{X}$ понятия непрерывности и сходимости относительно этой метрики.

Для любых $x, y \in \mathbb{X}$ и рационального числа $\alpha \geq 0$ справедливо *биномиальное тождество*

$$(x \oplus y)^{\alpha} \;=\; x^{\alpha} \oplus y^{\alpha}. \tag{6.1}$$

Если порядок на $\mathbb{X}$ линейный, то для доказательства тождества достаточно проверить его в каждом из случаев $x \leq y$ и $x > y$. При условии частичного порядка докажем (6.1) для целого показателя $\alpha = p \geq 0$. Если одно из чисел x или y равно нулю, то тождество становится тривиальным. Предположим, что $x, y, \neq 0$.

Проверим (6.1) но индукции. При $p = 0, 1$ имеем очевидные равенства. Допустим, что тождество верно при некотором p. Тогда, в частности, $x^p \oplus y^p \geq x^q y^{p-q}$ при всех $q = 0, 1, \ldots, .$

Покажем, что оно сохраняется и при $p + 1$. Ясно, что всегда справедливо неравенство $(x \oplus y)^{p+1} \geq x^{p+1} \oplus y^{p+1}$. Поверим выполнение противоположного неравенства. Рассмотрим величину

$$\begin{aligned}(x \oplus y)^{p+1}(x \oplus y) \;&=\; (x^p \oplus y^p)\,(x \oplus y)^2 \;= \\ &= x^{p+2} \oplus x^{p+1}y \oplus x^p y^2 \oplus x^2 y^p \oplus xy^{p+1} \oplus y^{p+2} \;\leq \\ &\leq x^{p+2} \oplus x^{p+1}y \oplus xy^{p+1} \oplus y^{p+2} \;=\; \left(x^{p+1} \oplus y^{p+1}\right)(x \oplus y).\end{aligned}$$

После сокращения на $x \oplus y \neq \mathbb{O}$ имеем $(x \oplus y)^{p+1} \leq x^{p+1} \oplus y^{p+1}$.

Применяя тождество (6.1) легко показать, что для всех $x, y \in \mathbb{X}$ и рациональных чисел $\alpha, \beta \geq > 0$ выполняется

$$x^\alpha y^\beta \;\leq\; (x \oplus y)^{\alpha+\beta}. \tag{6.2}$$

Действительно, из (6.1) следует, что

$$(x \oplus y)^\alpha \;=\; x^\alpha \oplus y^\alpha \geq x^\alpha, \quad (x \oplus y)^\beta \;=\; x^\beta \oplus y^\beta \geq y^\beta,$$

Заметим, что при $\alpha = \beta = 1/2$ из (6.2) получаем аналог неравенства между геометрическим и арифметическим средними

$$\sqrt{xy} \;=\; x \oplus y. \tag{6.3}$$

6.3 Идемпотентный векторный полумодуль

Определение и свойства. Над идемпотентным полуполем $\mathbb{X}$ образуем m-мерное координатное пространство $\mathbb{X}^m$, элементы которого $\overline{a} = (\; a_1 \;\ldots\; a_m \;)^T$ будем рассматривать как векторы-столбцы. Ясно, что дня любых векторов из $\mathbb{X}^m$ определены операции $\oplus$

покоординатного сложения и покоординатного умножения на число $x \in \mathbb{X}$.

Вектор $\overline{\mathbb{O}} = (\mathbb{O}, \ldots, \mathbb{O})$ назовём *нулевым*. Далее $\overline{a}, \overline{b}$ — произвольные элементы $\mathbb{X}^m$, а x, y — произвольные элементы $\mathbb{X}$.

Для умножение вектора на скаляр справедливы свойства

$$x(y\overline{a}) = (xy)\overline{a}, \quad \mathbb{I}\overline{a} = \overline{a}.$$

В силу покомпонентного определения операций сложения векторов, на пространство $\mathbb{X}^m$ распространяются свойства сложения полуполя $\mathbb{X}$: *ассоциативность*, *коммутативность*, *существование нуля* $\overline{\mathbb{O}}$ *и идемпотентность*.

Как следствие, справедливыми оказывается свойства *накопления, неотрицательности и монотонности* по $\oplus$ и $\otimes$; например последнее записывается в виде

$$\overline{a} \le \overline{b} \;\Rightarrow\; \overline{a} \oplus \overline{c} \le \overline{b} \oplus \overline{c} \;\text{ и }\; x\overline{a} \le x\overline{b}.$$

И, наконец, сложение векторов и умножение вектора на скаляр связаны свойствами дистрибутивности

$$x(\overline{a} \oplus \overline{b}) = x\overline{a} \oplus x\overline{b}, \quad (x \oplus y)\overline{a} = x\overline{a} \oplus y\overline{a}.$$

Поэтому можно сказать, что пространство $\mathbb{X}^m$ с указанными операциями образует *векторный полумодуль* над полукольцом $\mathbb{X}$.

Линейная зависимость векторов. Рассмотрим в $\mathbb{X}^m$ произвольную систему векторов

$S = \{\, \overline{a}_1, \ldots, \overline{a}_n \,\}$ и вектор $\overline{b} \in \mathbb{X}$. Последний *линейно зависит* от S, если его можно представить в виде *линейной комбинации*

$$\overline{b} \;=\; x_1\overline{a}_1 \oplus \ldots \oplus x_n\overline{a}_n$$

с *коэффициентами* $x_1, \ldots x_n \in \mathbb{X}$.

Система векторов является *линейно зависимой*, если хотя бы один из её векторов линейно зависит от других, и *линейно независимой* — в противном случае.

Определение 6.1. Если вектор $\overline{b}$ линейно зависит от некоторой системы векторов S, но не зависит от любой её подсистемы, то S называется *минимальной системой, порождающей* $\overline{b}$.

Нетрудно проверить, что представление любого вектора в виде разложения по векторам его минимальной порождающей системы является единственным. Действительно, предположим, что имеется два разложения вектора $\overline{b}$ по векторам его минимальной порождающей системы $S = \{\, \overline{a}_1, \ldots, \overline{a}_n \,\}$

$$x_1\overline{a}_1 \oplus \ldots \oplus x_n\overline{a}_n \;=\; y_1\overline{a}_1 \oplus \ldots \oplus y_n\overline{a}_n \;=\; \overline{b},$$

причем $x_i \neq y_i$, для некоторого $i = 1, \ldots, n$, для определенности, $x_i < y_i$. Отсюда

$$x_i\overline{a}_i < y_i\overline{a}_i \leq \overline{b}$$

и по свойству *накопления* вытекает, что величина $x_i\overline{a}_i$, не влияет на значение $\overline{b}$ и её можно отбросить. Следовательно, вектор $\overline{b}$ является линейной комбинацией системы $S \setminus \{a_i\}$, что противоречит условию минимальности системы S.

Метрика. Для всякого вектора $\overline{a} = (\ a_1\ \ldots\ a_m\ )^T$ из $\mathbb{X}^m$ определим *носитель* $\operatorname{supp}(\overline{a})$ как множество индексов ненулевых компонент этого вектора:

$$\operatorname{supp}(\overline{a}) \ = \ \{\, i \in \{1, \ldots, m\} \mid a_i \neq \mathbb{O} \,\}.$$

Для любых ненулевых векторов $\overline{a}, \overline{b} \in \mathbb{X}^m$ при условии $\operatorname{supp}(\overline{a}) = \operatorname{supp}(\overline{b})$ определим расстояние между ними как идемпотентную сумму покоординатных расстояний:

$$\rho(\overline{a}, \overline{b}) \ = \bigoplus_{i \in \operatorname{supp}(\overline{a})} \rho(a_i, b_i).$$

Положим также

$$\rho(\overline{a}, \overline{b}) \ = \ \begin{cases} \infty, & \text{если } \operatorname{supp}(\overline{a}) \neq \operatorname{supp}(\overline{b}), \\ \mathbb{I}, & \text{если } \overline{a} = \overline{b} = \mathbb{O}. \end{cases}$$

Заметим, что в $\mathbb{R}^m_{\max,+}$ введённая метрика совпадает с обычной метрикой

$$\rho_\infty(\overline{a}, \overline{b}) \ = \max_{1 \leqslant i \leqslant m} |a_i - b_i|.$$

Идемпотентная алгебра матриц. Будем рассматривать $(m \times n)$-матрицы с элементами из *идемпотентного полуполя* $\mathbb{X}$.

Определение 6.2. Матрица не имеющая ненулевых строк, называется *регулярной*, а не имеющая ни ненулевых строк, ни ненулевых столбцов — *правильной*.

Матрица, все элементы которой равны нулю $\mathbb{O}$, называется *нулевой*, символически также $\mathbb{O}$.

Для любых матриц соответствующих размеров и $x \in \mathbb{X}$ определены операции сложения $\oplus$ и умножения $\otimes$, а также операция умножения матрицы на скаляр, аналогичные соответствующим в обычной линейной алгебре с заменами $+ \mapsto \oplus, \quad \times \mapsto \otimes$.

Из свойств операций полуполя $\mathbb{X}$ следует, что на матрицы переносятся все свойства идемпотентного векторного полумодуля. Таким образом, множество матриц над полуполем $\mathbb{X}$ также является над ним *идемпотентным полумодулем.*

Квадратные матрицы. Рассмотрим $n \times n$-матрицы A над полуполем $\mathbb{X}$.

Как обычно, матрица A называется *диагональной*, если все её недиагональные элементы равны $\mathbb{O}$. Диагональная матрица A с диагональными элементами $a_1, \ldots, a_n$ обозначается $A = \operatorname{diag}(a_1, \ldots, a_n)$.

Матрица $I = \operatorname{diag}(\mathbb{I}, \ldots, \mathbb{I})$ называется *единичной.*

Ясно, что множество рассматриваемых квадратных матриц устойчиво относительно операций сложения и умножения матриц и удовлетворяет условиям их ассоциативности, дистрибутивности, а также (свойство единицы)

$$AI = IA = A.$$

Поэтому можно сказать, что множество всех квадратных матриц над полуполем $\mathbb{X}$ образует над ним *ассоциативное идемпотентное полукольцо с единицей.*

Обратная и псевдообратная матрицы. Пусть A — квадратная матрица. Матрица A^{-1} называется *обратной к* A, если

$$A^{-1}A = AA^{-1} = I.$$

Теорема 6.1. *Для того, чтобы матрица имела обратную, необходимо и достаточно, чтобы в каждом её столбце и в каждой её строке стоял ровно один элемент, отличный от нуля.*

Доказательство. Рассматриваем квадратные порядка n матрицы над идемпотентным полуполем $\mathbb{X}$.

Достаточность. Рассмотрим матрицу A у которой в каждом столбце и в каждой строке имеется ровно один отличный от нуля элемент. Транспонируем A и заменим каждый её ненулевой элемент на обратный. Нетрудно видеть, что получена матрица, обратная к A.

Необходимость. Пусть для матрицы $A = (a_{ij})$ существует матрица $B = (b_{ij})$ такая, что $AB = BA = I$.

Зафиксируем i-е строку матрицы A и столбец матрицы B, $i \in \{1, \ldots, n\}$. Для данного индекса i выполняется равенство

$$a_{i1}b_{1i} \oplus \ldots \oplus a_{in}b_{ni} = \mathbb{I}.$$

Отсюда следует, что в матрице A найдётся столбец, а в матрице B — строка с индексом j такие, что $a_{ij}b_{ji} > \mathbb{O}$, откуда $a_{ij} > \mathbb{O}$ и $b_{ji} > \mathbb{O}$.

Допустим, что в столбце j матрицы A имеется ещё один ненулевой элемент, например $a_{kj} \neq \mathbb{O}$, $k \neq i$. Тогда

$$a_{kj}b_{ji} > \mathbb{O},$$

и по свойству накопления операции сложения, (k,i)-й недиагональный элемент I окажется строго больше $\mathbb{O}$, что невозможно. Следовательно, матрица A не может иметь два ненулевых элемента в одном *столбце*.

Используя равенство $BA = I$, аналогично доказывается, что A не может иметь двух ненулевых элементов в одной *строке*. □

Например, при $d_1, \ldots, d_n \neq \mathbb{O}$ —

$$\big(\operatorname{diag}(d_1, \ldots, d_n)\big)^{-1} = \operatorname{diag}(d_1^{-1}, \ldots, d_n^{-1}).$$

Ясно, что в полукольце $\mathbb{X}^{n\times n}$ обратимы только диагональные матрицы и матрицы, полученные из них путем перестановки строк или столбцов.

Для любой матрицы $A = (a_{ij}) \in \mathbb{X}^{m\times n}$ можно определить *псевдообратную матрицу* $A^- = (a_{ij}^-) \in \mathbb{X}^{n\times m}$ с элементами

$$a_{ij}^- = \begin{cases} a_{ji}^{-1}, & \text{если } a_{ji} \neq \mathbb{O}, \\ \mathbb{O}, & \text{иначе.} \end{cases}$$

Таким образом, псевдообратная матрица получается из исходной транспонированием и заменой ненулевых элементов на обратные.

Легко видеть, что дня правильной матрицы A выполняются неравенства

$$A^-A \geqslant I \quad \text{и} \quad A^-A \geqslant I.$$

Если для матрицы A существует обратная, то очевидно, что $A^- = A^{-1}$.

Для любой матрицы A её *носителем* называется *множество пар индексов ненулевых компонент* A.

Для матриц A и B одинакового размера с общим носителем из $A \le B$ следует $A^- \ge B^-$.

Применяя к векторам описанную выше операцию преобразования $A \to A^-$ матриц заключаем, что для любого *вектора-столбца* $\overline{x} = (\ x_1\ \ \dots\ \ x_m\ )^T$ над $\mathbb{X}$ определён *вектор-строка* $\overline{x}^- = (\ x_1^-\ \ \dots\ \ x_n^-\ )$, где

$$x_i^- = \begin{cases} x_i^{-1}, & \text{если } x_i \neq \mathbb{O}, \\ \mathbb{O}, & \text{иначе.} \end{cases}, \quad i = \overline{1,n}.$$

Из неравенства $\overline{x} \le \overline{y}$ для векторов $\overline{x}$ и $\overline{y}$ с общим носителем следует $\overline{x}^- \ge \overline{y}^-$.

6.4 Линейные уравнения

Основные понятия. Пусть $A, C \in \mathbb{X}^{m\times n}$ — матрицы, а $\overline{b}, \overline{d} \in \mathbb{X}^m$ — векторы.

Общим линейным уравнением относительно неизвестного вектора $\overline{x} \in \mathbb{X}^n$ называется уравнение

$$A\,\overline{x} \oplus \overline{b} = C\,\overline{x} \oplus \overline{d}.$$

Заметим, что в силу отсутствия противоположного по сложению, данному уравнению нельзя, как в обычной алгебре, придать форму, при которой все слагаемые, содержащие неизвестный вектор $\overline{x}$, оказываются слева, а слагаемые без $\overline{x}$ — справа.

Будем рассматривать следующие частные случаев уравнения общего линейного уравнения

$$1)\ A\,\overline{x} = \overline{b}, \qquad 2)\ A\,\overline{x} \oplus \overline{d} = \overline{b}.$$

Наряду с данными уравнениями, будем рассматривать неравенство

$$A\,\overline{x} \leq \overline{b}.$$

Будем называть уравнения (неравенства), возможно, представленные в терминах различных полуколец, *эквивалентными*, если множества их отличных от нуля решений совпадают. Например, эквивалентны следующие пары уравнений и неравенств:

$$\begin{array}{lcl} A\,\overline{x} = \overline{b} & \longleftrightarrow & \overline{x}^{-}A^{-} = \overline{b}^{-} \\ A\,\overline{x} \leq \overline{b} & \longleftrightarrow & \overline{x}^{-}A^{-} \leq \overline{b}^{-} \\ \mathbb{R}_{\max,+} & \longleftrightarrow & \mathbb{R}_{\min,+} \\ \mathbb{R}_{\max,\times} & \longleftrightarrow & \mathbb{R}_{\min,\times} \end{array}$$

Расстояние от вектора до множества. Расстояние между произвольным вектором $\overline{b} \in \mathbb{X}^m$ и множеством векторов $S \subset \mathbb{X}^m$ определяется величиной

$$\rho(S, \overline{b}) = \inf_{\overline{a} \in S} \rho(\overline{a}, \overline{b}).$$

Пусть имеется система векторов $S = \{\ \overline{a}_1,\ \ldots,\ \overline{a}_n\ \}$ из $\mathbb{X}^m$. Для системы S введем $(m \times n)$-матрицу $A = (\ \overline{a}_1\ \ldots\ \overline{a}_n\ )$ составленную из векторов-столбцов системы S и линейную оболочку

$$\begin{aligned} \mathcal{A} &= \operatorname{span}\{\ \overline{a}_1, \ldots, \overline{a}_n\ \} = \\ &= \{\ x_1\overline{a}_1 \oplus \ldots \oplus x_n\overline{a}_n \mid x_1, \ldots, x_n \in \mathbb{X}\ \}. \end{aligned}$$

Очевидно, что если в системе S имеется нулевой вектор $\mathbb{O}$, то его удаление оставит оболочку $\mathcal{A}$ без изменений, поскольку $\mathbb{O}$ всегда будет в ней присутствовать.

Найдём расстояния от произвольного вектора $\overline{b} \in \mathbb{X}^m$ до линейной оболочки $\mathcal{A}$. В силу того, что каждый вектор $\overline{a} \in \mathcal{A}$ можно представить в виде

$$\overline{a} = A\,\overline{x}, \quad \overline{x} \in \mathbb{X}^n,\ A \in \mathbb{X}^{m\times n},$$

получаем

$$\rho(S,\overline{b}) \;=\; \rho(\mathcal{A},\overline{b}) \;=\; \min_{\overline{x}\in\mathbb{X}^n} \rho(A\,\overline{x},\overline{b}).$$

Будем интересоваться также расстоянием от $\overline{b}$ до множеств

$$\mathcal{A}_1 \;=\; \{\ \overline{a} \in \mathcal{A} \mid \overline{a} \le \overline{b}\ \}, \quad \mathcal{A}_2 \;=\; \{\ \overline{a} \in \mathcal{A} \mid \overline{a} \ge \overline{b}\ \}.$$

В случае $\overline{b} = \mathbb{O}$ будем всегда иметь $\rho(\mathcal{A},\mathbb{O}) = \mathbb{I}$, поскольку $\mathcal{A}$ всегда содержит нулевой вектор.

Также, поскольку в этом случае

$$\mathcal{A}_1 = \{\mathbb{O}\} \ \text{ и } \ \mathcal{A}_2 = \mathcal{A},$$

то и $\rho(\mathcal{A}_1,\overline{b}) = \rho(\mathcal{A}_2,\overline{b}) = \mathbb{I}$.

Если же $A = \mathbb{O}$ (нулевая матрица), но $\overline{b} \ne \mathbb{O}$, то $\rho(\mathcal{A},\overline{b}) = \infty$.

Далее будем считать, что система $S = \{\ \overline{a}_1,\ldots,\overline{a}_n\ \}$ *не имеет нулевых векторов, а вектор* $\overline{b}$ *не имеет нулевых координат.*

Для *регулярной* (не имеющей нулевых строк) матрицы A определим величину

$$\triangle(A,\overline{b}) \;=\; \left(A(\overline{b}^{\,-}A)^{\,-}\right)^{-}\overline{b},$$

а для нерегулярной положим $\triangle(A,\overline{b}) = \infty$.

Смысл введённой величины раскрывает

Лемма 6.1. *Для любых матрицы A и вектора $\overline{b} > \mathbb{O}$ выполняется равенство*

$$\rho(\mathcal{A},\overline{b}) \;=\; \sqrt{\triangle(A,\overline{b})}.$$

Отсюда $\triangle(A,\overline{b}) \geqslant \mathbb{I}$.

Лемма 6.2. *Вектор $\overline{b}$ принадлежит линейной оболочке столбцов регулярной матрицы A, если и только если $\triangle(A,\overline{b}) = \mathbb{I}$.*

Максимальное решение уравнения 1-го рода. Псевдорешение. Пусть заданы матрица $A \in \mathbb{X}^{m\times n}$ и вектор $\overline{b} \in \mathbb{X}^m$. Рассмотрим задачи решения относительно $\overline{x} \in \mathbb{X}^n$ уравнения

$$A\,\overline{x} \;=\; \overline{b} \tag{6.4}$$

и неравенства

$$A\,\overline{x} \;\leq\; \overline{b}. \tag{6.5}$$

Определение 6.3. Решение $\overline{x}_m$ уравнения (6.4) или неравенства (6.5) называют *максимальным*, если $\overline{x} \leq \overline{x}_m$ для любого решения $\overline{x}$.

Теорема 6.2. *Уравнение $A\,\overline{x} = \overline{b}$ имеет решение если и только если $\triangle(A,\overline{b}) = \mathbb{I}$.*

В этом случае его максимальным решением является $\overline{x}_m = (\overline{b}^{-} A)^{-}$.

Если столбцы матрицы A *образуют минимальную систему, порождающую* $\overline{b}$, *то других решении нет.*

Если разрешимость уравнения (6.4) не гарантируется, рассмотрим вспомогательное уравнение

$$A\,\overline{x} = \sqrt{\triangle(A, \overline{b})} \otimes A\,(\overline{b}^{-} A)^{-}.$$

Его решением будет, очевидно,

$$\overline{x}_0 = \sqrt{\triangle(A, \overline{b})} \otimes \overline{x}_m.$$

Оно, очевидно, всегда существует и при $\triangle(A, \overline{b}) = \mathbb{I}$ превращается в решение исходного уравнения (6.4).

Можно показать, что среди всех векторов линейной оболочки столбцов матрицы A оно обеспечивает *минимум расстояния до вектора* $\overline{b}$ *в смысле метрики* ρ.

Назовем $\overline{x}_0$ *псевдорешением* уравнения $A\,\overline{x} = \overline{b}$. В силу своих свойств его можно взять в качестве решения, если последнее не гарантируется.

Пусть теперь установлено, что $\triangle(A, \overline{b}) > \mathbb{I}$, то есть уравнение $A\,\overline{x} = \overline{b}$ не имеет решений. В этом случае может представлять интерес определение таких векторов $\overline{x}_1$ и $\overline{x}_2$, которые, являясь оптимальными с точки зрения невязки обеих частей уравнения, в то же время обеспечивают выполнение соответствующих неравенств $A\,\overline{x} \le \overline{b}$ и $A\,\overline{x} \ge \overline{b}$.

Можно показать, что такие векторы имеют вид

$$\overline{x}_1 = \overline{x}_m, \qquad \overline{x}_2 = \triangle(A, \overline{b}) \cdot \overline{x}_m$$

и при $\triangle(A, \overline{b}) = \mathbb{I}$ они совпадают.

Решение неравенства $A\,\overline{x} \le \overline{b}$. Можно показать, что решение неравенства всегда существует и записывается в виде $\overline{x} \le \overline{x}_m = (\overline{b}^{-} A)^{-}$.

Общее решение уравнения $A\,\overline{x} = \overline{b}$. Предположим, что вектор $\overline{b} \in \mathbb{X}^m$ линейно зависит от некоторого подмножества столбцов матрицы $A \in \mathbb{X}^{m\times n}$.

Пусть I — набор индексов столбцов, *образующих минимальную порождающую $\overline{b}$ систему векторов*, а $\mathcal{I} = \{I_1, \ldots, I_k\}$ — множество всех таких наборов индексов. Очевидно, если $\mathcal{I} \neq \varnothing$, то уравнение имеет решение.

Для каждого набора $I \in \mathcal{I}$ введём диагональную матрицу порядка n

$$G_I = \operatorname{diag}\,\big(\, g_1(I)\ \ldots\ g_n(I)\,\big),\ g_i(I) = \begin{cases} \mathbb{O}, & \text{если } i \in I, \\ \mathbb{I}, & \text{иначе.} \end{cases}$$

Пример 6.2. Пусть $A \in \mathbb{X}^{4\times 5}$ и вектор $\overline{b}$ порождается только 2, 3 и 5-м векторами-столбцами матрицы A.

Тогда $I = \{2, 3, 5\}$, и диагональная матрица G_I порядка 5 имеет $\mathbb{I}$ на 1 и 4-й позициях $\mathbb{O}$ на остальных.

Теорема 6.3. *Общим решением уравнения*

$$A\,\overline{x} = \overline{b}, \quad \textit{где}\ \ A \in \mathbb{X}^{m\times n},\ \overline{b} \in \mathbb{X}^m$$

в случае его разрешимости ($\triangle(A, \overline{b}) = \mathbb{I}$ или, что то же, $\overline{b}$ принадлежит линейной оболочке столбцов A) является совокупность векторов

$$\overline{x}_I = \big(\overline{b}^{-} A \oplus \overline{v}^T G_I\big)^{-}, \quad \overline{v} \in \mathbb{X}^n, \quad I \in \mathcal{I}.$$

Рассмотрим частный случай, когда семейство сокращается до одного множества решений: $|\mathcal{I}| = 1$.

Пусть столбцы матрицы A линейно независимы. Тогда существует только одно подмножество столбцов I, которое образует минимальную систему для $\overline{b}$, одна матрица G, и общее решение принимает вид

$$\overline{x} = \left(\overline{b}^{-} A \oplus \overline{v}^T G\right)^{-}, \qquad \overline{v} \in \mathbb{X}^n.$$

Если же I совпадает с множеством всех столбцов матрицы A, то G — нулевая матрица, а общее решение сводится к ранее приведённому единственному решению $\overline{x} = (\overline{b}^{-} A)^{-}$.

Решение уравнения $A\,\overline{x} \oplus \overline{d} = \overline{b}$. Рассмотрим задачу решения относительно $\overline{x} \in \mathbb{X}^n$ уравнения

$$A\,\overline{x} \oplus \overline{d} = \overline{b} \tag{6.6}$$

где A — матрица, а $\overline{b}$ и $\overline{d}$ — векторы подходящего размера. Будем предполагать, что $\overline{d} \leq \overline{b}$. Очевидно, что при нарушении этого условия уравнение решений не имеет.

Введем множества индексов строк

$$I_1 = \{\, i \mid d_i < b_i \,\} \quad \text{и} \quad I_2 = \{\, i \mid d_i = b_i \,\}.$$

Обозначим через A_1 и A_2 подматрицы, составленные из *строк* матрицы A с индексами из множеств I_1 и I_2 соответственно.

Аналогичным образом векторы $\overline{b}$ и $\overline{d}$ разбиваются на части $\overline{b}_1$, $\overline{b}_2$ и $\overline{d}_1$, $\overline{d}_2$ соответственно.

Тогда уравнение (6.6) согласно свойству накопления будет равносильно системе

$$\begin{cases} A_1\overline{x} = \overline{b}_1, \\ A_2\overline{x} \leq \overline{d}_2. \end{cases}$$

Найдем множество $\mathcal{I}_1$ — всех наборов I минимальных подмножеств столбцов матрицы A_1 относительно $\overline{b}_1$. Далее найдём подмножество $\widetilde{\mathcal{I}}_1 \subseteq \mathcal{I}_1$ — наборов, которые определяют общие решения для уравнения и неравенства.

Лемма 6.3. *Уравнение* $A\,\overline{x} \oplus \overline{d} = \overline{b}$ *имеет решение если и только если выполняются условия*

$$\triangle(A_1, \overline{b}_1) = \mathbb{I} \quad и \quad \widetilde{\mathcal{I}}_1 \neq \varnothing.$$

При этом общим решением является семейство

$$\overline{x}_I = \left(\overline{b}^{\,-} A \oplus \overline{v}^T G_I\right)^-, \quad \overline{v} \in \mathbb{X}^n, \quad I \in \widetilde{\mathcal{I}}_1.$$

6.5 Приложения и примеры

Рассмотрим некоторые примеры применения полученных результатов в различных приложениях.

1. Сетевое планирование. Пусть имеется проект, который состоит в параллельном выполнении n работ. Для завершения каждой из работ могут потребоваться промежуточные результаты некоторых других работ, время получения которых задано. Для каждой работы $i = 1, \ldots, n$ и введем обозначения:

x_i — время начала работы;

y_i — время завершения работы;

a_{ij} — время получения промежуточного результата работы j, который необходим для завершения работы i.

Время завершения каждой работы i определяется выражением

$$y_i = \max\{ x_1 + a_{i1}, \ldots, x_n + a_{in} \}. \qquad (6.7)$$

Пусть для всех работ заданы директивные сроки завершения их выполнения. Требуется определить сроки начала работ, при которых время завершения совпадает с директивными сроками. Если такие сроки начала работ определить невозможно, то следует найти приближенные решения задачи, которые являются оптимальными с точки зрения минимального нарушения директивных сроков.

Обозначим через $\overline{b} = (\ b_1\ \ldots\ b_n\ )^T$ вектор директивных сроков завершения работ.

Будем решать задачу в полуполе

$$\mathbb{R}_{\max,+} = \langle\, \mathbb{R} \cup \{-\infty\};\ \max,\ +,\ -\infty,\ 0 \,\rangle.$$

В нём уравнения (6.7) принимает вид

$$y_i = a_{i1}x_1 \oplus \ldots \oplus a_{in}x_n.$$

Введя обозначения

$$\overline{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},\ \overline{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix},\ A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix},$$

получим равенство

$$\overline{y} = A\,\overline{x}.$$

Тогда рассматриваемая задача планирования сводится к исследованию в полукольце $\mathbb{R}_{\max,+}$ уравнения (6.4):

$$A\,\overline{x} = \overline{b}.$$

Вычислим величину $\triangle = \triangle(A, \overline{b})$.

Если $\triangle = \mathbb{I} = 0$, то решение уравнения существует и выполнение сроков $\overline{b}$ обеспечивает, например, максимальное решение $\overline{x}_m = (\overline{b}^{-} A)^{-}$, задающее самые поздние допустимые сроки начала работ.

При условии $\triangle > 0$ решения не существует, но можно найти приближенные решения

$$\overline{x}_0 = \sqrt{\triangle}\,\overline{x}_m, \quad \overline{x}_1 = \overline{x}_m, \quad \overline{x}_2 = \triangle\,\overline{x}_m.$$

Этим решениям отвечают сроки окончания работ

$$\overline{y}_0 = A\,\overline{x}_0, \quad \overline{y}_1 = A\,\overline{x}_1 \le \overline{b}, \quad \overline{y}_2 = A\,\overline{x}_2 \ge \overline{b},$$

отклонения которых от директивных сроков определяют величины

$$\rho(\overline{y}_0, \overline{b}) = \sqrt{\triangle}, \qquad \rho(\overline{y}_1, \overline{b}) = \rho(\overline{y}_2, \overline{b}) = \triangle.$$

Если возможна корректировка первоначальных директивных сроков, то определения новых сроков завершения работ можно взять, например, любой вектор $\overline{b}'$ такой, что $\overline{y}_1 \le \overline{b}' \le \overline{y}_2$. Тогда отклонения новых сроков от первоначальных не будет превосходить $\triangle$, а их минимум $\sqrt{\triangle}$ будет достигаться при $\overline{b}' = \overline{y}_0$.

Все вычисления выполняем по правилам идемпотентной математики.

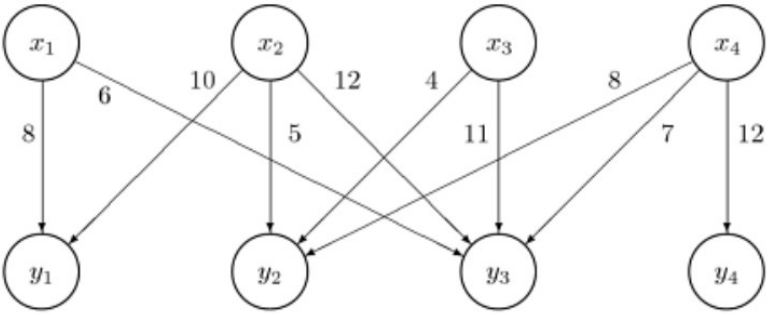


Рис. 6.2. Сетевая модель проекта

1. Пусть $n = 4$ и сетевая модель некоторого проекта имеет вид, представленный на рис. 6.2.

Для рассматриваемого проекта найдем самые поздние допустимые сроки начала работ для набора директивных сроков окончания $\overline{b} = (\ 14\ 11\ 16\ 15\ )^T$.

Для решения задачи при традиционном подходе необходимо решить систему неравенств

$$\begin{cases} \max\{\, x_1 + 8,\, x_2 + 10,\, x_3,\, x_4 \,\} & \leqslant 14, \\ \max\{\, x_1,\, x_2 + 5,\, x_3 + 4,\, x_4 + 8 \,\} & \leqslant 11, \\ \max\{\, x_1 + 6,\, x_2 + 12,\, x_3 + 11,\, x_4 + 7 \,\} & \leqslant 16, \\ \max\{\, x_1,\, x_2,\, x_3,\, x_4 + 12 \,\} & \leqslant 15, \end{cases}$$

$$x_1,\, x_2,\, x_3,\, x_4 \geqslant 0.$$

Матрица A имеет вид

$$A = \begin{pmatrix} 8 & 10 & 0 & 0 \\ 0 & 5 & 4 & 8 \\ 6 & 12 & 11 & 7 \\ 0 & 0 & 0 & 12 \end{pmatrix}.$$

Вычисляем величину $\triangle$.

$$\overline{b}^{-}A = (\,-14\ \ -11\ \ -16\ \ -15\,) \otimes \begin{pmatrix} 8 & 10 & 0 & 0 \\ 0 & 5 & 4 & 8 \\ 6 & 12 & 11 & 7 \\ 0 & 0 & 0 & 12 \end{pmatrix} =$$

$$\Big[\text{ для первой компоненты вектора } \overline{b}^{-}A:$$
$$-14+8=-6, \quad -11+0=-11,$$
$$-16+6=-10, \ -15+0=-15\Big]$$
$$= \big(\max\{-6,\,-11,\,-10,\,-15\}$$
$$\max\{-4,\,-6,\,-4,\,-15\}$$
$$\max\{-14,\,-7,\,-5,\,-15\}$$
$$\max\{-14,\,-3,\,-9,\,-3\}\big) =$$
$$= (\,-6\ \ -4\ \ -5\ \ -3\,); \quad (\overline{b}^{-}A)^{-} = (\,6\ 4\ 5\ 3\,)^{T} = \overline{x}_m;$$

$$A\,\overline{x}_m = A \otimes \begin{pmatrix} 6 \\ 4 \\ 5 \\ 3 \end{pmatrix} =$$

$$= \begin{pmatrix} \max\{14,\,14,\,5,\,3\} \\ \max\{6,\,9,\,9,\,11\} \\ \max\{12,\,16,\,16,\,10\} \\ \max\{6,\,4,\,5,\,15\} \end{pmatrix} = \begin{pmatrix} 14 \\ 11 \\ 16 \\ 15 \end{pmatrix};$$

$$(A\,\overline{x}_m)^{-}\overline{b} = (\,-14\ \ -11\ \ -16\ \ -15\,) \otimes \begin{pmatrix} 14 \\ 11 \\ 16 \\ 15 \end{pmatrix} =$$

$$= \max\{0,\,0,\,0,\,0\} = 0 = \mathbb{I} = \triangle.$$

Таким образом, $\triangle = \mathbb{I}$, уравнение (6.4) разрешимо и

максимальное его решение есть

$$\overline{x} = \overline{x}_m = \begin{pmatrix} 6 & 4 & 5 & 3 \end{pmatrix}^T.$$

Сроки окончания работ:

$$A\,\overline{x}_m = (\ 14\ 11\ 16\ 15\ )^T = \overline{b}.$$

2. Найдем сроки начала работ для нового вектора $\overline{b} = (\ 15\ 15\ 15\ 15\ )^T$ директивных сроков окончания.

Сначала находим $\triangle = \triangle(A, \overline{b})$:

$$\overline{b}^{-}A = (\ -15\ \ -15\ \ -15\ \ -15\ ) \otimes A =$$
$$= \begin{pmatrix} \max\{-7,\ -15,\ -9,\ -15\} \\ \max\{-5,\ -10,\ -3,\ -15\} \\ \max\{-15,\ -11,\ -4,\ -15\} \\ \max\{-15,\ -7,\ -8,\ -3\} \end{pmatrix} =$$
$$= (-7\ \ -3\ \ -4\ \ -3\ ); \quad (\overline{b}^{-}A)^{-} = (\ 7\ 3\ 4\ 3\ )^T = x_m;$$

$$A\,\overline{x}_m = A \otimes \begin{pmatrix} 7 \\ 3 \\ 4 \\ 3 \end{pmatrix} =$$

$$= \begin{pmatrix} \max\{15,\ 13,\ 4,\ 3\} \\ \max\{7,\ 8,\ 8,\ 11\} \\ \max\{13,\ 15,\ 15,\ 10\} \\ \max\{7,\ 3,\ 4,\ 15\} \end{pmatrix} = \begin{pmatrix} 15 \\ 11 \\ 15 \\ 15 \end{pmatrix};$$

$$(A\,\overline{x}_m)\overline{b} = (\ -15\ \ -11\ \ -15\ \ -15\ ) \otimes \begin{pmatrix} 15 \\ 15 \\ 15 \\ 15 \end{pmatrix} =$$

$$= \max\{0,\, 4,\, 0,\, 0\} = 4.$$

Поскольку $\triangle = 4 \neq \mathbb{I} = 0$, уравнение (6.4) не имеет решений. Но можно найти приближенные решения и соответствующие им сроки окончания работ:

$$\sqrt{4} = \frac{4}{2} = 2;$$

$$\overline{x}_0 = \sqrt{\triangle} \otimes \overline{x}_m = 2 + (\,7\;3\;4\;3\,)^T = (\,9\;5\;6\;5\,)^T;$$

$$\overline{y}_0 = A\,\overline{x}_0 = A \otimes (\,9\;5\;6\;5\,)^T =$$

$$= \begin{pmatrix} \max\{17,\, 15,\, 6,\, 5\} \\ \max\{9,\, 10,\, 10,\, 13\} \\ \max\{15,\, 17,\, 17,\, 17\} \\ \max\{9,\, 5,\, 6,\, 17\} \end{pmatrix} = \begin{pmatrix} 17 \\ 13 \\ 17 \\ 17 \end{pmatrix};$$

$$\overline{x}_1 = \overline{x}_m = (\,7\;3\;4\;3\,)^T;$$

$$\overline{y}_1 = A\,\overline{x}_1 = A \otimes \begin{pmatrix} 7 \\ 3 \\ 4 \\ 3 \end{pmatrix} =$$

$$= \begin{pmatrix} \max\{15,\, 13,\, 4,\, 3\} \\ \max\{7,\, 8,\, 8,\, 11\} \\ \max\{13,\, 15,\, 15,\, 10\} \\ \max\{7,\, 3,\, 9,\, 15\} \end{pmatrix} = \begin{pmatrix} 15 \\ 11 \\ 15 \\ 15 \end{pmatrix};$$

$$\overline{x}_2 = \triangle \otimes \overline{x}_m = 4 + (\,7\;3\;4\;3\,)^T = (\,11\;7\;8\;7\,)^T;$$

$$\overline{y}_2 = A\,\overline{x}_2 = A \otimes \begin{pmatrix} 11 \\ 7 \\ 8 \\ 7 \end{pmatrix} =$$

$$= \begin{pmatrix} \max\{19,\,17,\,7,\,8\} \\ \max\{11,\,12,\,12,\,15\} \\ \max\{17,\,19,\,19,\,14\} \\ \max\{11,\,7,\,8,\,19\} \end{pmatrix} = \begin{pmatrix} 19 \\ 15 \\ 19 \\ 19 \end{pmatrix}.$$

2. Исследование надежности. Пусть некоторое техническое устройство может работать в одном из m режимов. Его работоспособность зависит от исправности некоторого узла, которое выпускается n различными производителям и определяется заданным для каждого режима и производителя набором вероятностей выхода из строя устройства при неисправности узла.

Для каждого режима работы i-го устройства $i = 1, \ldots, m$ введем обозначения:

y_i — максимальная по всем производителям узла вероятность выхода данного устройства из строя при неисправности узла;

a_{ij} — вероятность выхода из строя устройства при неисправности узла от производителя j.

Для каждого j-го производителя $j = 1, \ldots, n$ определим величину

x_j — вероятность выхода узла из строя.

Максимальная вероятность выхода из строя устройства в режиме i определяется выражением в смысле полукольца $\mathbb{R}_{\max,\times}$ (напомним, с обычными 0 и 1)

$$y_i = a_{i1}x_1 \oplus \ldots \oplus a_{in}x_n.$$

Перейдём к векторным обозначениям:

$$\overline{y} = A\,\overline{x}.$$

Пусть $\overline{b}$ — вектор допустимых для каждого режима вероятностей выхода устройства из строя. Составим неравенство

$$A\,\overline{x} \le \overline{b},$$

решение $\overline{x} = (\overline{b}^{-} A)^{-} = \overline{x}_m$ которого определяет максимально допустимые для каждого производителя вероятности выхода из строя узла.

Найдем максимальное решение неравенства при условии $(m = 3,\ n = 4)$

$$A = \begin{pmatrix} 0{,}15 & 0{,}2 & 0{,}2 & 0{,}3 \\ 0{,}2 & 0{,}2 & 0{,}4 & 0{,}5 \\ 0{,}3 & 0{,}5 & 0{,}6 & 0{,}6 \end{pmatrix}, \quad \overline{b} = \begin{pmatrix} 0{,}025 \\ 0{,}02 \\ 0{,}01 \end{pmatrix}.$$

После выполнения вычислений в $\mathbb{R}_{\max,\times}$ получим

$$\overline{x}_m = \begin{pmatrix} 0{,}03 & 0{,}04 & 0{,}04 & 0{,}06 \end{pmatrix}^T.$$

3. Планирование производства. Пусть имеется n видов сырья, которые должны использоваться в каждом из m производственных процессов. Для всех процессов заданы нормы времени на потребление каждого вида сырья. Процесс останавливается, когда сырье хотя бы одного вида оказывается исчерпанным.

Для каждого процесса $i = \overline{1, m}$ введем обозначения:

y_i — максимальная продолжительность процесса;

a_{ij} — среднее время потребления единицы сырья вида j.

Для каждого вида сырья $j = \overline{1,n}$ определим величину

x_j — начальное количество сырья.

Максимальная продолжительность процесса i определяется равенством в полуполе $\mathbb{R}_{\min,\times}$ (в котором $\mathbb{O} = +\infty$, $\mathbb{I} = 1$ и порядок обратный обычному)

$$y_i = a_{i1}x_1 \oplus \ldots \oplus a_{in}x_n.$$

В векторных обозначениях имеем равенство

$$\overline{y} = A\,\overline{x}.$$

Пусть для каждого процесса i запланирована определенная продолжительность b_i. Необходимо установить такой минимальный начальный запас каждого вида сырья, чтобы при запуске любого из процессов обеспечить требуемую продолжительность процесса.

Зададимся $\overline{b} = (\ b_1\ \ldots\ b_n\ )^T$. Решение задачи сводится к нахождению максимального (минимального в смысле обычного порядка) решения уравнения

$$A\,\overline{x} = \overline{b}.$$

Найдем решение при условии, что ($m = 3$, $n = 4$)

$$A = \begin{pmatrix} 2 & 1 & 4 & 3 \\ 2 & 3 & 4 & 4 \\ 3 & 2 & 5 & 6 \end{pmatrix}, \qquad \overline{b} = \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix}.$$

Вычислим величину $\triangle = \triangle(A, \overline{b})$ в полуполе $\mathbb{R}_{\min,\times} = \langle\, \mathbb{R}_+ \cup \{+\infty\};\ \min,\ \times,\ +\infty,\ 1\,\rangle$:

$$\overline{b}^{-}A = (\ 1/3\ \ 1/4\ \ 1/5\ ) \otimes \begin{pmatrix} 2 & 1 & 4 & 3 \\ 2 & 3 & 4 & 4 \\ 3 & 2 & 5 & 6 \end{pmatrix} =$$

$$= \big(\ \min\{\,2/3,\ 1/2,\ 3/5\,\}\ \min\{\,1/3,\ 3/4,\ 2/5\,\}$$
$$\min\{\,4/3,\ 1,\ 1\,\}\ \min\{\,1,\ 1,\ 6/5\,\}\ \big) =$$

$$= (\ 1/2\ \ 1/3\ \ 1\ \ 1\ ); \quad (\overline{b}^{-}A)^{-} = (\ 2\,3\,1\,1\ )^{T} = x_m;$$

$$A\,\overline{x}_m = \begin{pmatrix} 2 & 1 & 4 & 3 \\ 2 & 3 & 4 & 4 \\ 3 & 2 & 5 & 6 \end{pmatrix} \otimes \begin{pmatrix} 2 \\ 3 \\ 1 \\ 1 \end{pmatrix} =$$

$$= \begin{pmatrix} \min\{\,4,\ 3,\ 4,\ 3\,\} \\ \min\{\,4,\ 9,\ 4,\ 4\,\} \\ \min\{\,6,\ 6,\ 5,\ 6\,\} \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix};$$

$$(A\,\overline{x}_m)^{-}\overline{b} = (\ 1/3\ \ 1/4\ \ 1/5\ ) \otimes \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix} =$$

$$= \min\{\,1,\ 1,\ 1\,\} = 1 = \mathbb{I}.$$

Таким образом, $\triangle = \mathbb{I}$, уравнения (6.4) разрешимо и максимальное его решение есть

$$\overline{x}_m = (\ 2\,3\,1\,1\ )^{T}.$$

Сроки окончания работ выдерживаются:

$$A\,\overline{x}_m = (\ 3\,4\,5\ )^{T} = \overline{b}.$$

Допустим, что продолжительность процесса i, например, по технологическим причинам, не может превышать некоторой величины d_i.

Введем вектор

$$\overline{d} = (\ d_1\ \ \ldots\ \ d_m\ )^T.$$

Тогда в полукольце $\mathbb{R}_{\min,\times}$ имеем уравнение:

$$A\,\overline{x} \oplus \overline{d}\ =\ \overline{b}.$$

Пусть матрица A определена так же, как в предыдущей задаче. Найдем решение этого уравнения при

$$\overline{b}\ =\ (\ 2\ 4\ 2\ )^T, \quad \overline{d}\ =\ (\ 4\ 5\ 2\ )^T.$$

В предположении, что данное уравнение имеет решение, найдём его максимальное решение.

$$\overline{b}^{\,-} A\ =\ \begin{pmatrix} \frac{1}{2} & \frac{1}{4} & \frac{1}{2} \end{pmatrix} \otimes \begin{pmatrix} 2 & 1 & 4 & 3 \\ 2 & 3 & 4 & 4 \\ 3 & 2 & 5 & 6 \end{pmatrix}\ =$$

$$=\ (\ \min\{\,1,\,1/2,\,3/2\,\}\ \ \min\{\,1/2,\,3/4,\,1\,\}$$

$$\min\{\,2,\,1,\,5/2\,\}\ \ \min\{\,3/2,\,1,\,3\,\}\ )\ =\ \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 1 & 1 \end{pmatrix}.$$

$$\overline{x}\ =\ (\overline{b}^{\,-} A)^-\ =\ (\ 2\ 2\ 1\ 1\ )^T = x_m$$

является решением задачи.

Непосредственной подстановкой легко убедиться в том, что вектор $\overline{x}$ является решением уравнения:

$$A\,\overline{x}\ =\ \begin{pmatrix} 2 & 1 & 4 & 3 \\ 2 & 3 & 4 & 4 \\ 3 & 2 & 5 & 6 \end{pmatrix} \otimes \begin{pmatrix} 2 \\ 2 \\ 1 \\ 1 \end{pmatrix}\ =$$

$$=\ \begin{pmatrix} \min\{\,4,\,2,\,4,\,3\,\} \\ \min\{\,4,\,6,\,4,\,4\,\} \\ \min\{\,6,\,4,\,5,\,6\,\} \end{pmatrix}\ =\ \begin{pmatrix} 2 \\ 4 \\ 4 \end{pmatrix};$$

$$A\,\overline{x} \oplus \overline{d} = \begin{pmatrix} \min\{\,2,\,4\,\} \\ \min\{\,4,\,5\,\} \\ \min\{\,4,\,2\,\} \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \\ 2 \end{pmatrix} = \overline{b}.$$

4. Анализ цен предложения товарного рынка. Предположим, что на рынке представлен товар одного и того же назначения от n различных производителей. В зависимости от наличия дополнительных опций соответствующий вариант товара предлагается в одной из m ценовых категорий по цене, пропорциональной некоторой базовой цене производителя.

Для каждой категории $i = 1, \ldots, m$ определим величины

y_i — минимальная цена предложения товара по всем производителям;

z_i — максимальная цена предложения товара по всем производителям.

Для каждого производителя $j = 1, \ldots, n$ введем обозначения:

x_j — базовая цена товара;

a_{ij} — коэффициент, определяющий цену предложения варианта товара в ценовой категории i.

Для всех $i = 1, \ldots, m$ имеем в полукольцах $\mathbb{R}_{\min,\times}$ и $\mathbb{R}_{\max,\times}$ равенства

$$\begin{aligned} y_i &= a_{i1}x_1 \oplus \ldots \oplus a_{in}x_n \quad (\mathbb{R}_{\min,\times}), \\ z_i &= a_{i1}x_1 \oplus \ldots \oplus a_{in}x_n \quad (\mathbb{R}_{\max,\times}), \end{aligned}$$

или, в векторных обозначениях,

$$\begin{aligned} \overline{y} &= A\,\overline{x} \quad (\mathbb{R}_{\min,\times}), \\ \overline{z} &= A\,\overline{x} \quad (\mathbb{R}_{\max,\times}). \end{aligned}$$

Предположим, что для каждой ценовой категории заданы её нижняя и верхняя границы. Определим величину базовой цены товара для каждого производителя, при которой цена варианта товара во всех ценовых категориях удовлетворяет указанным границам.

Обозначим через $\overline{b}$ и $\overline{c}$ векторы нижних и верхних границ соответственно. Имеем неравенства

$$\begin{aligned} A\,\overline{x} &\le \overline{b} \quad (\mathbb{R}_{\min,\times}), \\ A\,\overline{x} &\le \overline{c} \quad (\mathbb{R}_{\max,\times}). \end{aligned}$$

Учитывая, что первое неравенство эквивалентно неравенству $\overline{x}^{-}A^{-} \le \overline{b}^{-}$ в полукольце $\mathbb{R}_{\max,\times}$ получим в этом полукольце систему неравенств

$$\begin{cases} \overline{x}^{-}A^{-} & \le \overline{b}^{-}, \\ A\,\overline{x} & \le \overline{c}. \end{cases}$$

Совместное решение неравенств приводит к

$$\overline{x}_{\mu} = A^{-}\overline{b} \le \overline{x} \le (\overline{c}^{-}A)^{-} = x_m.$$

Найдем границы для базовых цен товара в случае $n = 4$ производителей и $m = 3$ ценовых категорий в условиях

$$A = \begin{pmatrix} 1{,}0 & 1{,}2 & 1{,}5 & 1{,}0 \\ 2{,}7 & 3{,}2 & 2{,}5 & 4{,}1 \\ 4{,}0 & 5{,}0 & 4{,}0 & 6{,}4 \end{pmatrix}, \ \overline{b} = \begin{pmatrix} 10 \\ 40 \\ 60 \end{pmatrix}, \ \overline{c} = \begin{pmatrix} 40 \\ 60 \\ 80 \end{pmatrix}.$$

Вычисление нижних и верхних границ дает

$$\overline{x}_{\mu} = \begin{pmatrix} 15{,}0 & 12{,}5 & 16{,}0 & 10{,}0 \end{pmatrix}^T,$$
$$\overline{x}_{m} = \begin{pmatrix} 20{,}0 & 16{,}0 & 20{,}0 & 12{,}5 \end{pmatrix}^T.$$

Программные средства, предназначенных для работы с методами тропической математики:

1) Gfan — *http* : *//home.math.au.dk/jensen /software/gfan/gfan.html*

2) Библиотека на Haskell — *https* : *//github.com/pharpend/tropical*

3) Библиотека на Java (для полуполя $\mathbb{R}_{\max,+}$) — *http* : *//se.math.spbu.ru/SE/diploma/*2014*/m /Puzikov_Aleksandr_Juryevich − code.zip*

Глава 7

Линейные рекуррентные последовательности

7.1 Основные понятия

Определение 7.1. Числовая последовательность (вещественных чисел)

$$\overline{a} = \{a_i\}_{i \geqslant 0} = (\ a_0,\ a_1,\ \ldots\ ),$$

для которой при $n \geqslant k \geqslant 1$ выполняется *линейное рекуррентное соотношение (л. р. с.) порядка* k

$$a_n + C_1\, a_{n-1} + C_2 a_{n-2} + \ldots + C_k a_{n-k} = C, \qquad (*)$$

где $C_1, \ldots, C_k \neq 0$, C — некоторые константы, называется *линейной рекуррентной последовательностью (л. р. п.) порядка* k, причём в случае $C = 0$ говорят об *однородном соотношении*, и о *неоднородном*, в случае $C \neq 0$.

Очевидно, соотношение $(*)$ содержит $k+1$ слагаемых и л. р. п. порядка k однозначно задаётся своим рекуррентным соотношением и совокупностью из k её последовательных элементов, которые называют *начальными условиями (Н.У.)*; обычно это элементы $a_0, \ldots, a_{k-1}$.

Поставим в соответствие вышеприведённому однородному л. р. с. $(*)$ *характеристический многочлен*

$$P(x) = x^k + C_1 x^{k-1} + \ldots + C_{k-1}x + C_k.$$

Пример 7.1. Последовательность чисел Фибоначчи

$$1,\ 1,\ 2,\ 3,\ 5,\ 8,\ \ldots$$

является однородной линейной рекуррентной последовательностью 2-го порядка, задаваемую соотношением и Н.У.

$$a_n - a_{n-1} - a_{n-2} = 0,\ \ n \geqslant 1,\ \ a_0 = a_1 = 1.$$

Характеристическим многочленом для последовательности Фибоначчи будет

$$P(x) = x^2 - x - 1.$$

Ясно, что множество $\mathcal{L} = \{\overline{a}\}$ всех линейных рекуррентных последовательностей с операциями поэлементного *суммирования* $\overline{a} + \overline{b}$ и *умножения* всех элементов на константу $r \in \mathbb{R}$ $\overline{b} = r \cdot \overline{a}$ является бесконечномерным *линейным векторным пространством (л.в.п.)* над $\mathbb{R}$ относительно введенных операций.

Теорема 7.1. *Последовательности из $\mathcal{L}$, для которых выполняется некоторое линейное рекуррентное соотношение порядка k, образуют k-мерное подпространство L подпространства $\mathcal{L}$.*

Доказательство. Если $\overline{a}, \overline{b} \in L \subset \mathcal{L}$ удовлетворяют л. р. с. порядка k, то ему удовлетворяет и

$$\alpha\overline{a} + \beta\overline{b} \in L,\ \alpha, \beta \in \mathbb{R}.$$

Равенство $\dim L = k$ очевидно. □

Для k некоторых л. р. п. $\overline{a}^1, \ldots, \overline{a}^k$ введём квадратную матрицу A порядка k:

$$A(\overline{a}^1, \ldots, \overline{a}^k) = A = \begin{pmatrix} a_0^1 & a_0^2 & \ldots & a_0^k \\ a_1^1 & a_0^2 & \ldots & a_1^k \\ \ldots & \ldots & \ldots & \ldots \\ a_{k-1}^1 & a_{k-1}^2 & \ldots & a_{k-1}^k \end{pmatrix}.$$

Теорема 7.2. *Последовательности $\overline{a}^1, \ldots, \overline{a}^k$ образуют базис k-мерного подпространства линейного пространства $\mathcal{L}$, если и только если*

$$\det\left(A(\overline{a}^1, \ldots, \overline{a}^k)\right) \neq 0.$$

7.2 Решение однородных л. р. с.

Утверждение 7.1. *Если заданы однородное л. р. с. порядка k*

$$a_n + C_1 a_{n-1} + C_2 a_{n-2} + \ldots + C_k a_{n-k} = 0 \qquad (**)$$

и начальные условия $a_0, \ldots, a_{k-1}$, то единственная удовлетворяющая им л. р. п. имеет вид

$$\overline{a} = \beta_1 \overline{a}^1 + \ldots + \beta_k \overline{a}^k,$$

где $\overline{a}^1, \ldots, \overline{a}^k$ — некоторый базис линейного под пространства решений L, а коэффициенты $\beta_1, \ldots, \beta_k$ однозначно определяются СЛАУ порядка k

$$A \times \begin{pmatrix} \beta_1 \\ \dots \\ \beta_k \end{pmatrix} = \begin{pmatrix} a_0 \\ \dots \\ a_{k-1} \end{pmatrix}.$$

Таким образом задача нахождения л. р. п. сводится к нахождению базиса линейного подпространства L, образованного множеством всех последовательностей, удовлетворяющих данному л. р. с. и решению приведённой СЛАУ. Базисные последовательности строят с помощью корней характеристического многочлена $P(x)$.

Случай действительных корней

Лемма 7.1 (о корнях характеристического многочлена). *Пусть задано однородное л. р. с. порядка k. Тогда если λ — корень его характеристического многочлена*

$$P(x) = x^k + C_1 x^{k-1} + \ldots + C_{k-1}x + C_k,$$

то последовательность $\overline{\lambda} = (1, \lambda, \lambda^2, \ldots)$ удовлетворяет соотношению $(**)$.

Доказательство. Подставим члены $\overline{\lambda}$ в $(**)$: поскольку $C_k \neq 0$ влечёт $\lambda \neq 0$, получим

$$\lambda^n + C_1\lambda^{n-1} + \ldots + C_k\lambda^{n-k} = \\ = \lambda^{n-k} \underbrace{\left(\lambda^k + C_1\lambda^{k-1} + \ldots + C_k\right)}_{P(\lambda)=0} = 0.$$

□

Будем искать базис подпространства L в виде набора последовательностей, образованных степенями корней характеристического многочлена $P(x)$.

Теорема 7.3. *Пусть характеристический многочлен* $P(x)$ *однородного л. р. с.* $(**)$ *порядка* k *имеет* k *различных корней* $\lambda_1, \ldots, \lambda_k$. *Тогда последовательности* $\overline{\lambda}_1, \ldots, \overline{\lambda}_k$ *образуют базис* k*-мерного подпространства решений* L.

Доказательство. По лемме о корнях характеристического многочлена, все последовательности $\overline{\lambda}_i, i = \overline{1,k}$ удовлетворяют соотношению $(**)$, то есть лежат в пространстве L.

Для последовательностей $\overline{\lambda}_1, \ldots, \overline{\lambda}_k$ матрица A принимает вид

$$A_\lambda = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \lambda_1 & \lambda_2 & \ldots & \lambda_k \\ \ldots & \ldots & \ldots & \ldots \\ \lambda_1^{k-1} & \lambda_2^{k-1} & \ldots & \lambda_k^{k-1} \end{pmatrix}.$$

Её определитель является определителем Вандермонда, поэтому

$$|A_\lambda| = \prod_{1 \leqslant i < j \leqslant k} (\lambda_j - \lambda_i) \neq 0,$$

поскольку все корни $\lambda_1, \ldots, \lambda_k$ различны и отсюда следует утверждение теоремы.

Поэтому общее решение линейного однородного рекуррентного соотношения $(**)$ выглядит следующим образом:

$$\overline{a} = \beta_1 \overline{\lambda}_1 + \ldots + \beta_k \overline{\lambda}_k.$$

□

Утверждение 7.2. *Если некоторый корень λ многочлена $P(x)$ имеет кратность m, ему будут соответствовать следующие базисные последовательности*

$$\overline{\lambda},\ n\overline{\lambda},\ \ldots,\ n^{m-1}\overline{\lambda},$$

или последовательность $\left(1+n+\ldots+n^{m-1}\right)\overline{\lambda}$.

Уравнение $P(x)=0$ назовём *характеристическим* для данного характеристического многочлена $P(x)$ соответствующего л. р. с.

Пример 7.2. 1. Найти л. р. п., удовлетворяющую однородному л. р. с.

$$a_{n+2}-4a_{n+1}+3a_n\ =\ 0.$$

Решение. Характеристическое уравнение данного соотношения есть

$$P(x)\ =\ x^2-4x+3\ =\ 0.$$

Оно имеет два простых вещественных корня $\lambda_1=1,\ \lambda_2=3$ и решение данного соотношения в общем виде есть

$$a_n\ =\ \beta_1+\beta_2\cdot 3^n.$$

2. Найти однородную л. р. п., удовлетворяющую л. р. с.

$$a_{n+3}+3a_{n+2}+3a_{n+1}+a_n\ =\ 0.$$

Решение. Характеристическое уравнение данного соотношения:

$$P(x)\ =\ x^3+3x^2+3x+1\ =\ (x+1)^3\ =\ 0.$$

Таким образом данное характеристическое уравнение имеет один вещественный корень $\lambda = -1$ кратности 3, и решение данного л.о.р.с. в общем виде есть

$$a_n \;=\; (-1)^n \left(\beta_1 + \beta_2 n + \beta_3 n^2\right).$$

Из доказанного ранее следует, что если заданы начальные условия $a_0, \ldots, a_{k-1}$ однородного л. р. с. порядка k

$$a_n + C_1\, a_{n-1} + C_2\, a_{n-2} + \ldots + C_k\, a_{n-k} \;=\; 0,$$

то коэффициенты $\beta_1, \ldots, \beta$ в общем решении

$$\overline{a} \;=\; \beta_1 \overline{\lambda}_1 + \ldots + \beta_k \overline{\lambda}_k$$

находят из СЛАУ k-го порядка

$$A_\lambda \times \begin{pmatrix} \beta_1 \\ \ldots \\ \beta_k \end{pmatrix} \;=\; \begin{pmatrix} a_0 \\ \ldots \\ a_{k-1} \end{pmatrix}.$$

Пример 7.3. 1. Ранее было найдено, что л. р. п.

$$a_n \;=\; \beta_1 + \beta_2 \cdot 3^n$$

при любых β_1, β_2 удовлетворяет л. р. с.

$$a_{n+2} - 4a_{n+1} + 3a_n \;=\; 0.$$

Найти конкретную однородную л. р. п., если $a_1 = 10$, $a_2 = 16$.

Решение. Для начала найдём a_0 (полагая $n = 0$):

$$16 - 4 \cdot 10 + 3a_0 = 0 \;\Rightarrow\; a_0 = (40 - 16)/3 = 8.$$

Далее:

$$\begin{cases} \beta_1 + \beta_2 &= 8, \\ \beta_1 + 3\beta_2 &= 10, \end{cases} \Rightarrow \begin{cases} \beta_1 &= 7, \\ \beta_2 &= 1, \end{cases}$$

то есть искомая л. р. п. есть $a_n = 7 + 3^n$.

2. Ранее было найдено, что л. р. п.

$$a_n = (-1)^n \left(\beta_1 + \beta_2 n + \beta_3 n^2\right)$$

при любых β_1, β_2, β_3 удовлетворяет л. р. с.

$$a_{n+3} + 3a_{n+2} + 3a_{n+1} + a_n = 0.$$

Найдём конкретную такую л. р. п., если $a_0 = 0$, $a_1 = 2$, $a_2 = -10$.

Решение.

$$\begin{cases} \beta_1 & & & = 0, \\ -\beta_1 & -\beta_2 & -\beta_3 & = 2, \\ \beta_1 & +2\beta_2 & +4\beta_3 & = -10, \end{cases} \Rightarrow \begin{cases} \beta_1 &= 0, \\ \beta_2 &= 1, \\ \beta_3 &= -3, \end{cases}$$

то есть искомая л. р. п. есть $a_n = (-1)^{n+1}(3n^2 - n)$.

Случай комплексных корней. Если характеристический многочлен $P(x)$ имеет пару комплексных корней, то и соответствующая пара базисных комплексных последовательностей имеет вид

$$\begin{aligned} \overline{\lambda}_1 &= \left\{ \rho^n(\cos n\varphi + i \sin n\varphi) \right\}_{n \geqslant 0}, \\ \overline{\lambda}_2 &= \left\{ \rho^n(\cos n\varphi - i \sin n\varphi) \right\}_{n \geqslant 0}. \end{aligned}$$

Известно, что если к системе базисных векторов л.в.п. применить невырожденное линейное преобразование, то преобразованная система векторов также будет базисной. После применения к пространству L некоторого преобразование поворота, вместо пары комплексных последовательностей $(\overline{\lambda}_1, \overline{\lambda}_2)$ получим пару действительных последовательностей

$$\overline{\lambda}'_1 = \{\rho^n \cos n\varphi\}_{n\geqslant 0}, \qquad \overline{\lambda}'_2 = \{\rho^n \sin n\varphi\}_{n\geqslant 0}.$$

Аналогично поступают с другими парами комплексно сопряженных корней.

Пример 7.4. Найти л. р. п., удовлетворяющую л. р. с.

$$a_{n+2} - 2\cos\alpha \cdot a_{n+1} + a_n = 0, \quad a_1 = \cos\alpha,\ a_2 = \cos 2\alpha.$$

Решение. Для начала найдём a_0 $(\cos^2\alpha = \frac{1+\cos 2\alpha}{2})$:

$$\cos 2\alpha - 2\cos^2\alpha + a_0 = 0 \ \Rightarrow\ a_0 = 1.$$

Характеристическим уравнением для заданной последовательности является

$$x^2 - 2x\cos\alpha + 1 = 0,$$

которое имеет два комплексно сопряжённых корня

$$\lambda_1 = \cos\alpha - i\sin\alpha, \qquad \lambda_2 = \cos\alpha + i\sin\alpha.$$

Переходя в действительную область, получим последовательности

$$\overline{\lambda}'_1 = \{\cos n\alpha\}_{n\geqslant 0}, \qquad \overline{\lambda}'_2 = \{\sin n\alpha\}_{n\geqslant 0},$$

то есть общее решение данного л.о.р.с. записывается в виде

$$a_n = \beta_1 \cos n\alpha + \beta_2 \sin n\alpha.$$

Из начальных условий получаем

$$\begin{cases} \beta_1 = 1, \\ \beta_1 \cos\alpha + \beta_2 \sin\alpha = \cos\alpha, \end{cases} \Rightarrow \begin{cases} \beta_1 = 1, \\ \beta_2 = 0, \end{cases}$$

то есть искомая л. р. п. есть $a_n = \cos n\alpha$.

7.3 Решение неоднородных л. р. с.

В случае $C \neq 0$ записанное в общем виде неоднородное линейное рекуррентное соотношение

$$a_n + C_1 a_{n-1} + C_2 a_{n-2} + \ldots + C_k a_{n-k} = C$$

задаёт *неоднородную л. р. п.*.

Теорема 7.4. *Общее решение* $\overline{a}$ *неоднородного л. р. с. представляется в виде суммы некоторого его частного решения* $\overline{a}'$ *и общего решения* $\overline{a}^0$ *соответствующего однородного соотношения:* $\overline{a} = \overline{a}^0 + \overline{a}'$.

Доказательство. Пусть $\overline{a}'$ и $\overline{a}''$ — два частных решения неоднородного соотношения. Очевидно последовательность $\overline{a}' \pm \overline{a}''$ удовлетворяет соответствующему однородному соотношению. □

Частное решение неоднородного р.с. можно, например, искать в виде постоянной последовательности

$$\overline{a}' = (\ a,\ a,\ \ldots\ )$$

и в этом случае

$$a + C_1\, a + \ldots + C_k\, a \;=\; C.$$

1. При условии $1 + C_1 + \ldots + C_k \neq 0$ получим

$$a \;=\; \frac{C}{1 + C_1 + \ldots + C_k}.$$

2. Если же

$$\sum_{i=1}^{k} C_i = -1, \quad \text{но} \quad \sum_{i=1}^{k} i \cdot C_i \neq 0,$$

то существует частное решение вида

$$\overline{a}\,' = \{na\}_{n \geqslant 0},$$

где константа a находится из уравнения

$$a \cdot n + C_1\, a \cdot (n-1) + \ldots + C_k \cdot a \cdot (n-k) \;=\; C \quad (\star)$$

(результат подстановки $a_n = an$ в неоднородное л. р. с.).

Поскольку $-C_1 - \ldots - C_k = 1$, то в соответствии с $(\star)$ получим

$$\frac{C}{a} = (-C_1 - \ldots - C_k) \cdot n + C_1 \cdot (n-1) + \ldots + C_k \cdot (n-k) =$$
$$= -C_1 n - \ldots - C_k n + (C_1 n - 1 \cdot C_1) + (C_2 n - 2 \cdot C_2) + \ldots$$
$$\ldots + (C_k n - k \cdot C_k) \;=\; -\sum_{i=1}^{k} i \cdot C_i.$$

Отсюда

$$a \;=\; -\frac{C}{\sum_{i=1}^{k} i \cdot C_i},$$

и частное решение неоднородного линейного рекуррентного соотношения в этом случае имеет вид

$$a_n{}' = na.$$

умножением на $x - 1$:

Пример 7.5. Решить рекуррентное соотношение

$$a_{n+3} - 7a_{n+1} + 6a_n = 20$$

при $a_0 = 2$, $a_1 = -6$, $a_2 = 3$.

Решение. Характеристическое уравнение данного неоднородного л. р. с. есть:

$$x^3 - 7x + 6 = 0.$$

Для его решения переберём делители свободного члена: $D(6) = \pm 1, \pm 2, \pm 3, \pm 6$.

1. Убеждаемся, что $\lambda_1 = 1$ — корень данного л. р. с. Далее имеем

$$x^3 - 7x + 6 = (x - 1)\left(x^2 + x - 6\right)$$

и корни последнего квадратного трёхчлена суть $\lambda_2 = 2$, $\lambda_3 = -3$. Следовательно, общее решение однородного л. р. с.

$$a_{n+3} - 7a_{n+1} + 6a_n = 0$$

есть $a_n^0 = \beta_1 + \beta_2 2^n + \beta_3(-3)^n$.

2. Найдём частное решение $\overline{a}{}'$ исходного неоднородного л. р. с.

Имеем: сумма его коэффициентов $1-7+6 = 0$, однако

$$\sum_{i=1}^{k} i\,C_i = 0 + 2\cdot(-7) + 3\cdot 6 \;=\; -14 + 18 \;=\; 4 \;\neq\; 0,$$

и поэтому частное решение исходного неоднородного л. р. с. —

$$a'_n \;=\; -\frac{20n}{4} \;=\; -5n,$$

и общее решение $a_n \;=\; \beta_1 + \beta_2 2^n + \beta_3(-3)^n - 5n$.

3. Определим по начальным условиям множители β_1, β_2, β_3:

$$\begin{cases} \beta_1 + \beta_2 + \beta_3 & = a_0 \;=\; 2, \\ \beta_1 + 2\beta_2 - 3\beta_3 - 5 & = a_1 \;=\; -6, \\ \beta_1 + 4\beta_2 + 9\beta_3 - 10 & = a_2 \;=\; 3, \end{cases}$$

Вычитаем из 2-го уравнения 1-е: $\beta_2 - 4\beta_3 = -3$, то есть $\beta_2 = 4\beta_3 - 3$, что влечёт

$$\begin{cases} \beta_1 + 8\beta_3 - 6 - 3\beta_3 & = -1, \\ \beta_1 + 16\beta_3 - 12 + 9\beta_3 & = 17 \end{cases} \;\Rightarrow\; \begin{cases} \beta_1 + 5\beta_3 & = 5, \\ \beta_1 + 25\beta_3 & = 25 \end{cases}$$

Вычитая из 2-го уравнения 1-е:

$$20\beta_3 = 20 \;\Rightarrow\; \beta_3 = 1 \;\text{ и }\; \beta_1 = 0,\; \beta_2 = 1.$$

Ответ: $a_n \;=\; 2^n + (-3)^n - 5n$.

Решение неоднородных линейных рекуррентных соотношений со «стандартной» правой частью — полином или экспонента от n — рассмотрено на примерах в конце следующего раздела.

7.4 Задачи с решениями

Задача 7.1. *Найти решение однородного л. р. с.*

$$a_{n+2} + 3a_n = 0, \quad a_0 = 1,\ a_1 = 2\sqrt{3}.$$

Решение. Характеристическое уравнение

$$x^2 + 3 = 0$$

имеет комплексно сопряжённые корни

$$\lambda_1 = -i\sqrt{3}, \quad \lambda_1 = i\sqrt{3}.$$

Им соответствует общее решение

$$a_n = \beta_1 3^{\frac{n}{2}} \cos\frac{\pi n}{2} + \beta_2 3^{\frac{n}{2}} \sin\frac{\pi n}{2} = \\ = 3^{\frac{n}{2}} \left(\beta_1 \cos\frac{\pi n}{2} + \beta_2 \sin\frac{\pi n}{2}\right).$$

Найдём β_1, β_2:

$$\begin{cases} \beta_1 = 1, \\ \sqrt{3}\beta_2 = 2\sqrt{3} \end{cases} \Rightarrow \beta_2 = 2.$$

Ответ: $a_n = 3^{\frac{n}{2}} \left(\cos\frac{\pi n}{2} + 2\sin\frac{\pi n}{2}\right)$

Задача 7.2. *Найти общее решение однородного л. р. с.*

$$a_{n+2} + 2a_{n+1} + a_n = 0.$$

Решение. Характеристическое уравнение

$$x^2 + 2x + 1 = 0$$

имеет единственный вещественный корень $\lambda = -1$ кратности 2.

Таким образом, решение есть

$$a_n = (-1)^n (\beta_1 + \beta_2 n).$$

Задача 7.3. *Найти общее решение однородного л. р. с.*

$$a_{n+3} + 10a_{n+2} + 32a_{n+1} + 32a_n = 0.$$

Решение. Характеристическое уравнение есть

$$P(x) = x^3 + 10x^2 + 32x + 32 = 0.$$

Пробуем подобрать корень из делителей
$32 : \pm 1, \pm 2, \pm 4, \ldots, \pm 32$.

Имеем $P(\pm 1) = \pm 1 + 10 \pm 32 + 32 \neq 0$,
$P(\pm 2) = \pm 8 + 40 + \pm 64 + 32$ и $P(-2) = 0$.

Далее —

$$x^3 + 10x^2 + 32x + 32 = (x+2)\left(x^2 + 8x + 16\right) = \\ = (x+2)(x+4)^2,$$

то есть $P(x)$ имеет корень -2 кратности 1 и -4 кратности 2.

Поэтому решение есть

$$a_n = \beta_1(-2)^n + (\beta_2 + \beta_3 n)(-4)^n = \\ = (-2)^n\left(\beta_1 + (\beta_2 + \beta_3 n)2^n\right).$$

Задача 7.4. *Найти общий член рекуррентной последовательности, удовлетворяющей соотношению*

$$a_{n+2} = 6a_{n+1} - 8a_n + 6n + 1, \quad a_0 = 4,\ a_1 = 5.$$

Решение. Представим соотношение в виде

$$a_{n+2} - 6a_{n+1} + 8a_n = 6n + 1.$$

Характеристическое уравнение есть

$$P(x) = x^2 - 6x + 8 = 0,$$

его корни суть $\lambda_1 = 2$, $\lambda_2 = 4$ и общее решение соответствующего однородного л. р. с. есть

$$a_n^0 = \beta_1 2^n + \beta_2 4^n.$$

Поскольку справа — полином 1-й степени, частное решение будем искать в виде $a'_n = \alpha_1 n + \alpha_0$.

Подставляя a'_n в исходное соотношение, получим

$$\begin{gathered}(\alpha_1(n+2)+\alpha_0) - 6\,(\alpha_1(n+1)+\alpha_0) + 8\,(\alpha_1 n + \alpha_0) = \\ = \alpha_1 n + 2\alpha_1 + \alpha_0 - 6\alpha_1 n - 6\alpha_1 - 6\alpha_0 + 8\alpha_1 n + 8\alpha_0 = \\ = 3\alpha_1 n + (2\alpha_1 + \alpha_0 - 6\alpha_1 - 6\alpha_0 + 8\alpha_0) = 6n + 1,\end{gathered}$$

Откуда

$$\alpha_1 = 2,\ -4\alpha_1 + 3\alpha_0 = -8 + 3\alpha_0 = 1 \ \Rightarrow\ \alpha_0 = 3$$

и $a'_n = 2n + 3$.

Получено общее решение

$$a_n = \beta_1 2^n + \beta_2 4^n + 2n + 3.$$

Найдём коэффициенты β_1, β_2:

$$\left\{\begin{array}{llll}\beta_1 & +\beta_2 & +3 & = 4 \\ 2\beta_1 & +4\beta_2 & +5 & = 5\end{array}\right. \Rightarrow$$

$$\Rightarrow \left\{\begin{array}{lll}\beta_1 & +\beta_2 & = 1 \\ 2\beta_1 & +4\beta_2 & = 0\end{array}\right. \Rightarrow \left\{\begin{array}{l}\beta_1 = 2 \\ \beta_2 = -1\end{array}\right.$$

Ответ: $a_n = 2^{n+1} - 4^n + 2n + 3$.

Задача 7.5. *Решить рекуррентное соотношение*

$a_{n+3}-6a_{n+2}+11a_{n+1}-6a_n = 4n,\ a_0 = 1,\ a_1 = 3,\ a_2 = 4.$

Решение. Характеристическое уравнение есть

$$P(x) \;=\; x^3 - 6x^2 + 11x - 6 \;=\; 0.$$

Пробуем подобрать корень из $D(6):\ \pm1,\ \pm2,\ \pm3,\ \pm6$. Находим, что $x_1 = 1$ — корень,

$$P(x) \;=\; (x-1)\left(x^2 - 5x + 6\right)$$

и $x_2 = 2$, также корни $x_3 = 3$ характеристического уравнения.

Таким образом общее решение однородного соотношения есть

$$a_n^0 \;=\; \beta_1 + \beta_2 2^n + \beta_3 3^n.$$

Частное решение ищем в виде $a'_n \;=\; n(\alpha_1 n + \alpha_2)$.

Подставляя его в исходное соотношение

$$\alpha_1(n+3)^2 + \alpha_2(n+3) - 6\big[\alpha_1(n+2)^2 + \alpha_2(n+2)\big] + \\ + 11\big[\alpha_1(n+1)^2 + \alpha_2(n+1)\big] - 6[\alpha_1 n^2 + \alpha_2 n] \;=\; 4n$$

Приравниваем коэффициенты перед степенями n:

$$n^2 : \alpha_1(1 - 6 + 11 - 6) \;=\; \alpha_1 \cdot 0 \;=\; 0;$$

$$n^1 : 6\alpha_1 + \alpha_2 - 24\alpha_1 - 6\alpha_2 + 22\alpha_1 + 11\alpha_2 - 6\alpha_2 \;= \\ = \; 4\alpha_1 \;=\; 4n, \quad \text{откуда } \alpha_1 = 1;$$

$$1 : 9\alpha_1 + 3\alpha_2 - 24\alpha_1 - 12\alpha_2 + 11\alpha_1 + 11\alpha_2 \;= \\ = \; -4\alpha_1 + 2\alpha_2, \quad \text{откуда } \alpha_2 = 2.$$

То есть $a'_n \;=\; n^2 + 2n$.

Определяем теперь константы $\beta_1, \beta_2, \beta_3$ исходя из Н.У.:

$$\left\{\begin{array}{rcl}\beta_1+\beta_2+\beta_3+0 &=& 1,\\ \beta_1+2\beta_2+3\beta_3+3 &=& 3,\\ \beta_1+4\beta_2+9\beta_3+8 &=& 4,\end{array}\right. \Rightarrow \left\{\begin{array}{rcl}\beta_1 &=& 1,\\ \beta_2 &=& 1,\\ \beta_3 &=& -1.\end{array}\right.$$

Окончательно имеем $a_n = 1 + 2^n - 3^n + n(n+2)$.

Задача 7.6. *Решить рекуррентное соотношение (с линейной правой частью)*

$$a_{n+1} - a_n = n, \qquad a_1 = 1.$$

Решение. Очевидно $a_0 = 1$.

Характеристическое уравнение для данного соотношения есть $x - 1 = 0$ и оно имеет корень $x = 1$, откуда общее решение однородного соотношения есть $a_n^0 = \beta$.

Частное решение ищем в виде

$$a'_n = n(\alpha_1 n + \alpha_2).$$

Подставляя его в исходное соотношение, имеем

$$\alpha_1(n+1)^2 + \alpha_2(n+1) - \alpha_1 n^2 - \alpha_2 n = n,$$

откуда $\alpha_1 = 1/2$ и $\alpha_2 = -1/2$, то есть

$$a'_n = (n^2 - n)/2 \text{ и } a_n = \beta + (n^2 - n)/2.$$

Из начальных условий: $a_0 = \beta = 1$ и окончательно — $a_n = 1 + C_n^2$.

Задача 7.7. *Решить рекуррентное соотношение (с экспоненциальной правой частью)*

$$a_{n+2} + 2a_{n+1} - 8a_n = 27 \cdot 5^n, \quad a_1 = -9,\ a_2 = 45.$$

Решение. Определяем, что $(n = 0)$:

$$45 - 2 \cdot 9 - 8a_0 = 27 \ \Rightarrow \ a_0 = 0.$$

Характеристическое уравнение для данного соотношения есть

$$x^2 + 2x - 8 = 0$$

и оно имеет корни $\lambda_1 = -4$ и $\lambda_2 = 2$, откуда общее решение однородного соотношения есть

$$a_n^0 = \beta_1(-4)^n + \beta_2 \cdot 2^n.$$

Частное решение ищем в виде $a'_n = \alpha \cdot 5^n$.

Подставляя его в исходное соотношение, имеем

$$\alpha \cdot 25 \cdot 5^n + 2\alpha \cdot 5 \cdot 5^n - 8 \cdot 5^n = 27 \cdot 5^n,$$

откуда $\alpha(35 - 8) = 27$ и $\alpha = 1$, то есть

$$a_n = \beta_1(-4)^n + \beta_2 \cdot 2^n + 5^n.$$

Из начальных условий находим, что $\beta_1 = 2,\ \beta_2 = -3$ и окончательно —

$$a_n = 2 \cdot (-4)^n - 3 \cdot 2^n + 5^n.$$

Задача 7.8. *Дано*

$$u_{k+2} - u_{k+1} - 2u_k + 4 = 0, \quad u_0 = 0,\ u_1 = 1.$$

Найти явное выражение для u_k.

Решение. Характеристическое уравнение:

$$x^2 - x - 2 = 0,$$

корни которого — $\lambda_1 = 2$, $\lambda_2 = -1$, откуда

$$u_n^0 = \beta_1 \cdot 2^n + \beta_2 \cdot (-1)^n.$$

Ищем частное решение $u'_n = a = const$:

$$a = 3a - 4 \Rightarrow a = 2 \Rightarrow u'_n = 2,$$

откуда $u_n = \beta_1 \cdot 2^n + \beta_2 \cdot (-1)^n + 2$.

$$\begin{cases} u_0 = \beta_1 + \beta_2 + 2 = 0, \\ u_1 = 2\beta_1 - \beta_2 + 2 = 1, \end{cases} \Rightarrow \begin{cases} \beta_1 + \beta_2 = -2, \\ 2\beta_1 - \beta_2 = -1. \end{cases}$$

$$3\beta_1 = -3 \Rightarrow \beta_1 = -1 \Rightarrow \beta_2 = -1.$$

Ответ: $u_n = -2^n - (-1)^n + 2$.

Задача 7.9. *Решить систему линейных рекуррентных соотношений*

$$\begin{cases} a_{n+1} = -b_n + n, \\ b_{n+1} = a_n + 2b_n + 1, \\ a_0 = 1,\ b_0 = -2. \end{cases}$$

Решение. Сразу находим, что $b_1 = -2$.

Далее, выражая из второго уравнения

$$b_{n+2} = a_{n+1} + 2b_{n+1} + 1,$$

и подставляя туда $a_{n+1} = -b_n + n$, получаем л. р. с. относительно b_n:

$$b_{n+2} - 2b_{n+1} + b_n = n + 1.$$

Его характеристическое уравнение $x^2 - 2x + 1 = 0$ имеет корень $x = 1$ кратности 2, поэтому общее решение соотношения есть

$$b_n^0 = \beta_1 + \beta_2 n,$$

а частное можно искать в виде

$$b'_n = n^2(\alpha_1 n + \alpha_2) = \alpha_1 n^3 + \alpha_2 n^2.$$

Подставляя выражение для b_n в исходное соотношение, находим $\alpha_1 = 1/6$, $\alpha_2 = 0$, и, таким образом

$$b_n = \beta_1 + \beta_2 + n^2/6.$$

Используя Н.У. на b_n, получим

$$\beta_1 = -2,\ \beta_2 = -1/6.$$

Итого решение —

$$b_n = -2 - \frac{n}{6} + \frac{n^3}{6},$$
$$a_n = 2 + \frac{7(n-1)}{6} - \frac{(n-6)^3}{6} = 1 + \frac{2}{3}n + \frac{1}{2}n^2 - \frac{1}{6}n^3.$$

Глава 8

Алгебраические основы криптографии

8.1 Основные понятия

Термины. *Криптография*[1)] — наука о способах преобразования (зашифрования) информации с целью её защиты от незаконных пользователей, обеспечения целостности и реализации методов проверки подлинности.

Таким образом, если помехоустойчивое кодирование защищает информацию от естественных, природных воздействий, то криптографические методы призваны защитить информацию от осмысленных воздействий человека-злоумышленника.

Открытый текст (plaintext) — сообщение, подлежащее зашифрованию. Будем считать, что это двоичное слово.

Например, тексты на английском языке обычно представляют, используя *стандартную кодировку*

$$a = 01,\ b = 02,\ \ldots,\ z = 26,\ \text{ пробел } = 00.$$

[1)] от др.-греч. *тайнопись*

Шифртекст (ciphertext) или *криптограмма* — результат зашифрования открытого текста. Так же считаем, что шифртекст есть двоичное слово.

Шифр (cipher) — семейство обратимых отображений множества последовательностей открытых текстов во множество последовательностей шифртекстов. Алгоритм шифрования тщательно разрабатывается и меняется в редких случаях.

Ключ (key) или *криптопеременная* — параметр (обычно составной), определяющий выбор конкретного отображения из входящих в шифр, его сменная часть.

Зашифрование (encryption) — процесс преобразования открытого текста в шифрованный с помощью шифра и ключа к данному тексту.

Расшифрование (decryption) — процесс, обратный к зашифрованию, реализуемый при известном значении ключа.

Дешифрование — процесс раскрытия криптограммы без знания секретного ключа.

Определения шифра и его ключа соответствуют принятому в современной криптографии правилу стойкости Керкгоффса[2)], согласно которому *в секре-*

[2)] Огюст Керкгоффс (Auguste Kerckhoffs, 1835–1903) — нидерландский криптограф, лингвист, историк, математик, автор фундаментального труда «Военная криптография» (1883), в котором сформулированы общие требования к криптосистемам. Является одним из создателей и популяризаторов искусственного языка Волапюк.

те держится только ключ, а сам алгоритм шифрования открыт.

Таким образом, *надёжность зашифрования определяется не секретностью шифра, а исключительно значением его секретного ключа*, известному только легальным пользователям. По необходимости ключ легко меняется.

В современных шифрсистемах ключ задается двоичным числом длиной не менее 128 и до 4096 бит.

Шифры подразделяются на:

блочные — сообщение разбивается на блоки фиксированной длины, которые зашифровываются независимо друг от друга (обычно блоки имеют длину 64 или 128 бит);

поточные — сообщение шифруется последовательно посимвольно (символом может быть как бит, так и произвольное число битов), и каждый символ шифруется в зависимости и от его расположения в тексте.

Типы шифрсистем. Сложность алгоритмов. Зашифрование открытого текста и его расшифровывание проводят с использованием, как правило, различных ключей, которые мы будем обозначать k_e и k_d соответственно. Множество возможных значений k_e и k_d называют *пространством ключей.*

Если $k_d = k_e$, или один ключ может быть легко получен из другого, то соответствующая криптосистема называется *симметрической*, а в противном случае — *асимметрической.*

Понятно, что при использовании симметрической системы оба ключа должны быть известны только легальным абонентам. Поэтому такие системы называют ещё *криптосистемами с секретным ключом или одноключевыми).* Основная проблема симметрической криптографии — обеспечение секретности при передаче ключей.

Примером системы с совпадающими ключами является шифрсистема *гаммирования* (или *шифр Вернама*), когда криптограмму $\widetilde{\beta}$ получают из открытого текста $\widetilde{\alpha}$ путём сложения его по $\bmod 2$ с некоторым случайным двоичным ключём $\widetilde{\gamma}$ той же длины, а вторичное такое сложение её расшифровывает. В этом случае, очевидно, криптограмма может оказаться результатом зашифрования любого открытого текста при подходящем выборе ключа $\widetilde{\gamma}$. Такая система обладает *абсолютной криптостойкостью*[3)], если ключ не содержит длинных повторяющихся битовых последовательностей и используется однократно.

При асимметрическом шифровании ключ расшифрования k_d остаётся секретным (private key), а ключ зашифрования k_e делается общедоступным (public key). Поэтому ассимметрические системы называют ещё *криптосистемами с открытым ключом* или *двуключевыми.* Расшифровать криптограм-

[3)] Под «абсолютной» понимается стойкость к дешифрованию, обеспеченная фундаментальными законами природы, а не текущими технологическими возможностями.

Использование данной и аналогичных криптосистем с *одноразовым шифрблокнотом* (содержащим наборы ключей $\widetilde{\gamma}_1$, $\widetilde{\gamma}_2$, ...) требует выработки длинных последовательностей двоичных ключей требуемого качества, решения проблем их хранения, передачи и уничтожения. На каждом из этих этапов жизненного цикла ключей имеется угроза их раскрытия. Все это делает данные системы непрактичными, дорогостоящими, и они применяется в исключительных случаях.

му может только абонент, которому известен секретный ключ. Шифрсистема проектируется так, чтобы секретный ключ нельзя было определить (вычислить, подобрать) за приемлемое время.

Последнее означает, что неизвестен полиномиальный алгоритм решения соответствующей задачи. Напомним, что *полиномиальным* называется алгоритм, время работы которого в зависимости от длины входного слова ℓ ограничено сверху величиной ℓ^c для некоторой константы c, не зависящей от ℓ.

Всегда существует экспоненциальный алгоритм подбора ключа k_d, заключающийся в полном переборе (brute force) возможных секретных ключей. *Экспоненциальным* называют алгоритм, имеющий оценку времени исполнения вида $exp(\ell)$.

Обычно существует и *субэкспоненциальный* алгоритм подбора ключа k_d. Время работы субэкспоненциального алгоритма асимптотически меньше любой экспоненты, но больше любого полинома.

На практике используют гибридные криптографические системы, когда обмен ключами производится с использованием асимметричной криптографии, а шифрование/расшифрование данных — более быстрыми симметричными алгоритмами.

Теоремы и алгоритмы. В конечном поле возможно сильное упрощение вычисления степеней сумм.

Теорема 8.1 (тождество Фробениуса). *В поле характеристики $p > 0$ выполнено тождество*

$$(a + b)^p = a^p + b^p.$$

Доказательство. В любом коммутативном кольце верна формула степени бинома

$$(a+b)^p = a^p + \underbrace{C_p^1 a^{p-1}b + \ldots + C_p^{p-1}ab^{p-1}}_{=0} + b^p,$$

в которой при $i = 1, \ldots, p-1$ числители коэффициентов $C_p^i = \frac{p!}{i!\cdot(p-i)!}$ делятся на p, а знаменатели — нет, и поэтому все они равны $0 \pmod p$. □

Следствие. В поле характеристики $p > 0$ для любого натурального n справедливо

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

Обобщённый алгоритм Евклида GE-InvZm нахождения элемента c^{-1}, обратного к c в кольце $\mathbb{Z}_m$ при условии НОД$(c, m) = 1$ (что гарантирует существование решения).

1. Запишем исходные данные в виде двухстрочной таблицы

$$\begin{array}{cc} m & 0 \\ c & 1 \end{array}$$

2. Вычислим частное q от деления друг на друга элементов первого столбца, то есть m на c: $m = q \cdot c + r$, $0 \leqslant r < c$.
3. Вычтем из 1-й строки 2-ю, домноженную на q и запишем результат в качестве 3-й строки таблицы.

4. Проводим аналогичные действия с двумя последними строками таблицы, пока в очередной строке не получим первый элемент 0. Тогда второй элемент *предпоследней* строки есть c^{-1}.

Пример 8.1. Решим в поле $\mathbb{Z}/(101)$ сравнение

$$4y = 1.$$

Применим алгоритм GE-InvZm, для удобства нумеруя строки и записывая значения частных и вычитаемые строки:

1	101	0	
2	4	1	$q = 25$ (100 25)
3	1	$\mathbf{-25}$	$q = 4$
4	0		

Найдено $y^{-1} = -25 \equiv_{101} 76$.
Действительно, $76 \cdot 4 = 304 = 3 \cdot 101 + 1$.

Алгоритм быстрого возведения в степень позволяет эффективно использовать в криптографии арифметику вычетов. позволяет эффективно использовать в криптографии арифметику вычетов.

При возведении в натуральную степень x некоторого числа используют двоичную запись степени:

$$x = x_k 2^k + x_{k-1} 2^{k-1} + \ldots + x_0 2^0,\ x_i \in \{0, 1\},\ i = \overline{0, k}.$$

Пусть, например, требуется вычислить a^{53}. Поскольку $53 = 2^5 + 2^4 + 2^2 + 1$, то

$$a^{53} = a^{2^5} \cdot a^{2^4} \cdot a^{2^2} \cdot a^{2^0}.$$

Вычисление первого сомножителя требует пяти умножений: $a^{2^5} = ((((a^2)^2)^2)^2)^2$. В процессе его вычисления запоминаются значения второго и третьего сомножителей. Их перемножение требует ещё трёх умножений. Таким образом, для вычисления a^{53} требуется только $5 + 3 = 8$ умножений, а не 52.

При вычислении степени элемента по модулю n возводят в квадрат не само число, а его остаток от деления на n, что существенно проще. Поэтому вычисляют вектор

$$[\ x_0\ \ldots\ x_k\ ]$$

двоичного представления x и тогда

$$a^x\ =\ a_0^{x_0} \cdot a_1^{x_1} \cdot \ldots \cdot a_k^{x_k} \pmod n,$$

где $a_0 = a$ и $a_{i+1} \equiv_n a_i^2$, $i = 0, \ldots, k-1$.

Пример 8.2. Вычислим $3^{11} \pmod 5$.

1. Находим вектор двоичного представления показателя степени 11: $11 = 2^0 + 2^1 + 2^3 \leftrightarrow [\ 1\ 1\ 0\ 1\ ]$. Поэтому $3^{11} \equiv_5 a_0^1 \cdot a_1^1 \cdot a_2^0 \cdot a_3^1$.

2. Находим a_i, $i = 0, 1, 2, 3$:

$$a_0 = 3 \equiv_5 3, \qquad a_1 = 3^2 = 9 \equiv_5 4,$$
$$a_2 = 4^2 = 16 \equiv_5 1, \qquad a_3 = 1^2 \equiv_5 1.$$

3. Окончательно $3^{11} \equiv_5 3 \cdot 4 = 12 \equiv_5 2$.

Теорема 8.2 (Ферма, малая). *Если целое a не делится на простое число p, то $a^{p-1} \equiv_p 1$.*

Доказательство. Требуемое сравнение выполняется для $a \equiv_p 1$ и всегда для $p = 2$ (тогда a нечётно).

Для остальных случаев оно доказывается для данного $p > 2$ индукцией по a, $a + 1 \not\equiv_p 0$. По тождеству Фробениуса и индуктивному предположению $a^p \equiv_p a$ имеем

$$(a+1)^{p-1} = (a+1)^p(a+1)^{-1} \equiv_p (a^p+1)(a+1)^{-1} = \\ = (a+1)(a+1)^{-1} \equiv_p 1.$$

□

Обобщением малой теоремы Ферма является следующая

Теорема 8.3 (*Эйлер*). *Если* $n > 1$ *и* $(a, n) = 1$, *то*

$$a^{\varphi(n)} \equiv_n 1. \tag{8.1}$$

Задача о рюкзаке: выбрать такие элементы вектор-строки $\boldsymbol{a} = [\, a_1 \ \ldots \ a_n \,]$ *различных* целых, чтобы их сумма равнялась данному z («размер рюкзака»)[4].

Например, в векторе

$$\boldsymbol{a} = [\, 43 \ \underline{129} \ 215 \ \underline{473} \ \underline{903} \ 302 \ \underline{561} \ \underline{1165} \ 697 \ 1523 \,],$$

подчёркнуты элементы, дающие в сумме $z = 3231$, то есть решением задачи для данного z будет вектор-столбец $\boldsymbol{x} = [\, 0\,1\,0\,1\,1\,0\,1\,1\,0\,0 \,]^T$ позиций выбранных чисел: $\boldsymbol{a} \times \boldsymbol{x} = z$. Неизвестны полиномиальные алгоритмы решения задачи о рюкзаке.

[4] Предполагается, что решение существует и единственно; другое название задачи — *проблема подмножества суммы*

Односторонняя функция — центральное понятие криптографии.

Определение 8.1. *Односторонней* (или *однонаправленной*, one-way function) называется обратимая функция $f : X \to Y$, обладающая свойствами:

1) существует полиномиальный алгоритм вычисления значений $f(x)$;
2) не существует полиномиального алгоритма обращения функции f (то есть нахождения x по значению $y = f(x)$).

Неформально: имеющая обратную функция $f(x)$ называется однонаправленной, если для всех $x \in X$ достаточно легко вычислить $y = f(x)$, но почти для всех $y \in Y$, нахождение любого $x \in X$, для которого $y = f(x)$, *вычислительно не осуществимо* (невозможно за полиномиальное время).

До сих пор не доказано, что однонаправленные функции вообще существуют (проблема их существования эквивалентна проблеме $P \stackrel{?}{=} NP$). Однако было предложено много функций, претендующие на односторонность. Они использует сложность решения задач теории чисел или комбинаторного анализа. Приведем некоторые из таких задач.

- Найти примарное разложение большого натурального числа (задача FACT).
- Для известных a, b, n найти такое значение x, что $a^x = b \pmod n$ (задача DLOG нахождения *дискретного логарифма*).

- Решить задачу о рюкзаке для общего случая.
- Декодировать исправляющий ошибки линейный код общего вида.

Односторонняя функция с секретом (с лазейкой; trapdoor one-way function) — функция $f_k(x) : X \to Y$ зависящая от параметра k, называемым *секретным ключом* или *лазейкой* и такая, что

1) вычисление значения $f_k(x)$ относительно несложно и при этом не требуется знание параметра k;
2) вычисление значения $f_k^{-1}(y)$ для всех $y \in Y$ при известном k относительно несложно;
3) почти для всех k и $y \in Y$, нахождение $f_k^{-1}(y)$ вычислительно неосуществимо без знания k.

Один из примеров, претендующих на то, чтобы являться односторонней функцией с лазейкой — функция $f(x) = x^m \pmod n$, m и n известны. Действительно, вычисление $f(x) = y$ производится методом быстрого возведения в степень, а эффективный алгоритм обратного преобразования $f^{-1}(y)$, то есть *вычисления корня m-й степени по* $\bmod n$, требует знания примарного разложения n. Эта информация может считаться лазейкой.

Применение односторонних функций с секретом позволяет, например, организовать обмен шифрованными сообщениями по открытым каналов связи, снабдить документ электронной подписью и др.

8.2 Криптографические протоколы

Криптографический протокол (cryptographic protocol) — набор правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах.

Электронная цифровая подпись (ЭЦП) — позволяет проверить авторство документа и отсутствие в нём искажений.

Идея организации электронной подписи на основе односторонних функций с секретом проста:

1. Автор документа a вычисляет значение y его хэш-функции преобразования a в битовую строку установленной длины[5)].
2. Используя свой секретный ключ k к односторонней функции с секретом f_k, автор вычисляет значение $x = f_k^{-1}(y)$ и посылает документ a, его хэш y и вычисленное значение x адресатам.
3. Проверку авторства документа a легко проводит любой адресат, вычисляя без знания k значение $f_k(x)$ и сравнивая результат с y.
4. Снабдить ЭЦП данного автора какой-либо документ без знания секрета k трудновыполнимо.

В России федеральным законом определяются три вида электронных подписей: простая, усиленная неквалифициро-

[5)] Понятно, что хэш-функции осуществляют необратимые преобразование информации. *Хэш* (или *дайджест*) y выступает как компактный представитель (паспорт) документа a. К хэш-функциям предъявляются специфические требования, которые мы не будем здесь обсуждать.

ванная и усиленная квалифицированная. Отличия заключаются в степени защищенности и юридически представляемых возможностях.

Обмен шифртекстами по открытому каналу связи. Приведём пример использования односторонней функции с лазейкой при решении задачи о рюкзаке[6)], задаваемую вектор-строкой $\boldsymbol{a}$.

Пусть открытый текст состоит из двоичных векторов $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^n$. Умножая $\boldsymbol{a}$ на эти векторы-столбцы, получим шифртекст $\boldsymbol{y} = [\, y_1 \ \ldots \ y_n \,]$. Таким образом, шифрование осуществляется элементарно.

Для расшифрования полученного сообщения потребуется решать задачу о рюкзаке: по значению y_i находить вектор $\boldsymbol{x}^i$ такой, что $\boldsymbol{a} \times \boldsymbol{x}^i = y_i$, $i = \overline{1,n}$, что без знания лазейки трудновыполнимо.

Покажем, в чём здесь состоит лазейка. Рассмотрим *сверхрастущие векторы* $\boldsymbol{a}$, в которых каждый элемент *больше суммы всех предыдущих элементов*. В этом случае задача решается очень просто.

Действительно, пусть, например,

$$\boldsymbol{a} = [\, \underline{25}\ 27\ \underline{56}\ 112\ 231\ \underline{452}\ \underline{916}\ 1803 \,] \quad \text{и} \quad z = 1449.$$

Поскольку $z < 1803$, то последний элемент данного вектора не входит в решение. Далее, поскольку $z > 916$, то 916 обязательно входит в решение, так как сумма всех предыдущих элементов меньше 916. Рассуждая аналогично, получаем код позиций выбираемых элементов: [1 0 1 0 0 1 1 0].

[6)] На ней основаны системы шифрования Меркля–Хеллмана и Шора–Ривеста.

Преобразуем сверхрастущий вектор $\boldsymbol{a}$ в некоторый вектор $\boldsymbol{b}$. Для этого выберем *модуль* m, больший суммы всех элементов $\boldsymbol{a}$ и возьмем некоторое u, взаимно простое с m. Это даст возможность далее определить элемент $v = u^{-1} \pmod m$.

Вектор $\boldsymbol{b}$ будем вычислять по правилу

$$\boldsymbol{b} = u \cdot \boldsymbol{a} \pmod m.$$

Он уже не является сверхрастущим, и может быть опубликован в качестве открытого ключа, а лазейкой будут значения m и u.

Пример 8.3. Рассмотрим сверхрастущий вектор $\boldsymbol{a} = [\ 1\ 2\ 4\ 8\ 16\ ]$ с суммой элементов 31.

Пусть передаваемые сообщения представляют собой 5-разрядные двоичные коды

$\boldsymbol{x}^1 = [\ 1\,0\,1\,1\,0\ ]^T$, $\boldsymbol{x}^2 = [\ 0\,1\,1\,0\,1\ ]^T$, $\boldsymbol{x}^3 = [\ 1\,0\,0\,0\,1\ ]^T$, образующие матрицу $X = [\ \boldsymbol{x}^1\ \boldsymbol{x}^2\ \boldsymbol{x}^3\ ]$.

Для преобразования вектора $\boldsymbol{a}$ в вектор $\boldsymbol{b}$ выберем $m = 37 > 31$ и взаимно простое с ним значение $u = 40$. Тогда открытым вектором будет

$$\boldsymbol{b} = [\ 3\ 6\ 12\ 24\ 11\ ].$$

Умножив $\boldsymbol{b}$ на матрицу X, получаем шифртекст:

$$\boldsymbol{b} \times X = \begin{bmatrix} 3 & 6 & 12 & 24 & 11 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} =$$

$$= \begin{bmatrix} 39 & 29 & 14 \end{bmatrix} = \boldsymbol{y}.$$

Легальный получатель сообщения:

1) зная лазейку $(m, u) = (37, 40)$, находит элемент v, обратный к u по mod m: $u \cdot v \equiv_m 1$; в нашем случае $u = 25$;
2) восстанавливает вектор $\boldsymbol{a} \equiv_m v \cdot \boldsymbol{b}$ —

$$25 \cdot [\ 3\ 6\ 12\ 24\ 11\ ] \equiv_{37} [\ 1\ 2\ 4\ 8\ 16\ ] = \boldsymbol{a};$$

3) находит вектор $\boldsymbol{z} \equiv_m v \cdot \boldsymbol{y} = [\ z_1\ z_2\ z_3\ ]$ —

$$\boldsymbol{z} = 25 \cdot [\ 39\ 29\ 14\ ] \equiv_{37} [\ 13\ 22\ 17\ ];$$

4) легко решает три задачи о рюкзаке со сверхрастущим $\boldsymbol{a}$ и $z_1 = 13$, $z_2 = 22$, $z_3 = 17$, определяя передаваемые сообщения $\boldsymbol{x}^1$, $\boldsymbol{x}^2$, $\boldsymbol{x}^3$.

Выработка общего секретного ключа по открытому каналу связи — покажем, как это можно сделать на примере протокола DH Диффи–Хеллмана[7)].

Два лица — традиционно A (Алиса) и B (Боб) — обмениваются сообщениями по открытому каналу. Чтобы обеспечить секретность переписки, A и B должны выработать общий секретный ключ.

Для этого они выбирают простое число p и в поле Галуа $GF(p)$ — некоторый примитивный элемент α; эти значения не являются секретом. Затем A и B независимо друг от друга выбирают по одному случайному натуральному числу x и y соответственно,

[7)] Предложен в 1976 г. сотрудниками MTI У. Диффи (Bailey Whitfield 'Whit' Diffie, 1944) и М. Хеллманом (Martin Edward Hellman, 1945) и независимо от них Р. Мерклем (Ralph Charles Merkle, 1952).

Этот протокол положил начало криптографии открытого ключа.

которые держат в секрете. Далее каждый из них вычисляет новый элемент поля $GF(p)$:

$$X = \alpha^x, \quad Y = \alpha^y, \qquad (\mathrm{mod}\ p), \qquad (*)$$

которыми обмениваются по открытому каналу.

Абонент A, получив Y, вычисляет ключ:

$$K = Y^x \qquad (\mathrm{mod}\ p),$$

и аналогично поступает абонент B:

$$K = X^y \qquad (\mathrm{mod}\ p).$$

Тем самым у Алисы и Боба появился общий секретный ключ $K = \alpha^{xy} \in GF(p)$, который в дальнейшем используется в алгоритмах симметричного шифрования.

Пассивный злоумышленник, перехватывающий, но не изменяющий сообщений (традиционно E, Ева, от англ. eavesdropper, подслушивающий) не может определить ключ K: его определение связано с решением одного из уравнений $(*)$, а это вычислительно трудная задача DLOG.

Заметим, что задача DLOG принадлежит классу NP, но её NP-полнота не доказана.

Протокол DH устойчив к пассивной атаке, но при беззащитен от активного вмешательства типа «*человек посередине*» (man-in-the-middle attack): при обмене сообщениями ни A, ни B не могут достоверно определить, кем является их собеседник. Действительно, если к каналу связи имеет доступ *активный злоумышленник* (традиционно M, Меллори от англ. malicious, злонамеренный), который может перехватывать сообщения, изменять или полностью подменять их, то, выра-

ботав два ключа: общий с A и общий с B, он может представляться Алисе Бобом, а Бобу — Алисой[8)].

Таким образом, протокол DH позволяет передавать секретный ключ по *частично защищенному каналу связи*, защищённому подмены и незащищеному от прослушивания.

8.3 Система шифрования RSA

RSA — классическая асимметрическая криптосистема. В ней открытым ключом шифрования является пара (n, e) значений *модуля* n и *экспоненты* e. По данному шифртексту $y = x^e \pmod n$ требуется найти открытый тест x. Таким образом, функция шифрования f, использующаяся в RSA, есть

$$f_e : x \to x^e \pmod n. \tag{8.2}$$

Для расшифрования сообщения y нужно решить сравнение $x^e \equiv_n y$.

Искомое решение может быть представлено в виде

$$x = y^d \pmod n, \tag{8.3}$$

которое будет единственным, когда модуль n свободен от квадратов, а значения экспоненты e и $\varphi(n)$ взаимно просты. Пара $(\varphi(n), d)$ является секретным ключом криптосистемы RSA.

Функция $f_e(x)$ легко вычисляется с помощью алгоритма быстрого возведения в степень, также как и при известном d — обратная к ней функция $f_d(y)$.

[8)] Вспоминаем *Сказку о царе Салтане А. С. Пушкина*: «... И в суму его пустую // Суют грамоту другую...»

Покажем, как можно было бы найти секретный ключ расшифрования d. Ясно, что он должен удовлетворять условию

$$x^{e\cdot d} \equiv_n x.$$

По теореме 8.3 Эйлера имеем

$$x^{\varphi(n)} \equiv_n 1, \quad \text{откуда} \quad x^{k\cdot\varphi(n)} \equiv_n 1$$

для любого целого k. Отсюда

$$x^{1+k\cdot\varphi(n)} = x = x^{e\cdot d} \pmod{n},$$

и заключаем, что для ключа d должно выполняться условие

$$d \cdot e = 1 \pmod{\varphi(n)}. \tag{8.4}$$

Решить это сравнение можно было бы, например, с помощью алгоритма 8.1 со с. 252. Но для этого надо знать $\varphi(n)$. В свою очередь, $\varphi(n)$ легко вычислить, найдя факторизацию несекретного модуля n. А вот эта задача чрезвычайно трудоёмка.

Таким образом, *схема RSA основана на сложности задачи FACT*. Также как и DLOG, эта задача принадлежит классу NP, но её NP-полнота не доказана.

Система RSA опубликована в 1978 г. и её название есть аббревиатура от фамилий авторов Р. Ривéста, А. Шамира и Л. Адлемана (Ronald Linn Rivest, 1947; Adi Shamir, 1952; Leonard Adleman, 1945) из MTI[9)].

[9)] Однако согласно рассекреченным британским правительством в 1997 г. сведениям, идея основных принципов криптографии с открытым ключём принадлежит сотруднику Главного управления связи Великобритании (GCHQ) Джеймсу Х. Эллису, который высказал её в 1970 г., но не смог найти для неё практической реализации. Первооткрывателем алгоритма RSA в 1973 г. стал Клиффорд Кокс, а впервые реализовал то, что известно как протокол Диффи–Хеллмана, — в следующем году Малкольм Дж. Уильямсон (все из GCHQ).

Алгоритм RSA используется в большом числе криптографических приложений.

Конкретно, авторы этой схемы предложили выбирать число n в виде произведения двух больших простых множителей p и q, $p \neq q$. Тогда

$$\varphi(n) = \varphi(pq) = (p-1)(q-1), \qquad (8.5)$$

и условием на выбор экспоненты e будет её взаимная простота с $p-1$ и $q-1$. Отметим, что число, представимое в виде произведения двух простых чисел, называют *полупростым*.

Утверждение 8.1. *Пусть $n = pq$, где p, q — простые числа. Тогда знание p, q равносильно знанию $\varphi(n)$.*

Доказательство. Зная p и q, легко находят $\varphi(n) = (p-1)(q-1)$.

Обратно, зная $\varphi(n) = pq - (p+q) + 1$, имеем

$$\begin{cases} p+q = n+1-\varphi(n), \\ pq = n \quad \text{(это значение открыто)}. \end{cases}$$

Теперь p и q могут быть получены как корни квадратного уравнения $z^2 + (\varphi(n) - n - 1)\, z + n = 0$. □

Итак, организация шифрованной переписки с помощью схемы RSA происходит следующим образом.

1. Организатор системы выбирает два достаточно больших простых числа p и q таких, что значение $|p-q|$ также не мало, и находит произведение $pq = n$.

2. Затем он выбирает экспоненту $e < n$, достаточно большую, взаимно простую с числами $p-1$ и $q-1$ и для упрощения зашифрования — с малым числом единиц. Перемножая $p-1$ и $q-1$ организатор получает $\varphi(n)$ и по (8.4) — определяет d.
3. Числа n и e публикуются, числа d и $\varphi(n)$ остаются секретными.
4. Теперь любой абонент может отправлять зашифрованные с помощью (8.2) сообщения организатору этой системы, а организатор легко сможет расшифровывать их с помощью (8.3), что без знания секретного ключа d вычислительно неосуществимо.

Заметим, что алгоритм RSA намного медленнее алгоритмов симметричного шифрования.

Пример 8.4. Пусть $p = 11$, $q = 13$, тогда $n = pq = 143$.

Выберем значение $e = 13$, оно простое, и, очевидно, заведомо взаимно просто с

$$p - 1 = 10 \quad \text{и} \quad q - 1 = 12.$$

Вычисляем $\varphi(143) = 10 \cdot 12 = 120$.

Возьмём фрагмент текста, соответствующий, например, числу $x = 42$, и зашифруем его:

$$y \;=\; 42^{13} \;=\; 1\,265\,437\,718\,438\,866\,624\,512 \;\equiv_{143}\; 3.$$

Для получения ключа расшифрования легальный пользователь зная $\varphi(n) = 120$ решает сравнение

$$d \cdot 13 \;=\; 1 \pmod{120}.$$

Применим для этого алгоритм GE-InvZm:

1	120	0	
2	13	1	$q = 9 \quad (\ 117\ 9\ )$
3	3	-9	$q = 4 \quad (\ 12\ \ -36\ )$
4	1	**37**	$q = 3$
5	0		

и получим $d = 37$.

Получив криптограмму y, легальный получатель расшифровывает её:

$$3^{37} \;=\; 450\,283\,905\,890\,997\,363 \;\equiv_{143}\; 42 \;=\; x.$$

Перескажем близко к тексту отрывок из [31].

Для иллюстрации своего метода Ривест, Шамир и Адлеман в 1977 г. зашифровали предложенным ими способом некоторую английскую фразу. Сначала она стандартным образом была представлена числом в 27-ричной системе исчисления, записана в виде целого x, а затем зашифрована с помощью отображения (8.2) при

$$n \;=\; 114381625757888867669325779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541 \quad (129 \text{ знаков, RSA-129}),$$

и $e = 9007$. Эти два числа были опубликованы, причем дополнительно сообщалось, что $n = pq$, где p и q — простые числа, записываемые соответственно 64 и 65-ю десятичными знаками.

Первому, кто дешифрует криптограмму

$$y \;=\; 968696137546220614771409222543558829057599911245743198746951209308162982251457083569314766228839896280133919905518294945157815154 \quad (123 \text{ знака}),$$

была обещана награда в \$100.

Предполагалось, что для расшифровки понадобится порядка 40 квадрильонов лет. Однако в 1994 г., то есть всего через 17 лет, задача была решена: были определены числа p и q и в результате дешифровки получилась фраза «*The magic words are squeamish ossifrage*»[10)].

Выполнение вычислений потребовало огромных по тем временам ресурсов: в работе, возглавлявшейся четырьмя авторами проекта дешифровки и продолжавшейся после предварительной теоретической подготовки примерно 220 дней, на добровольных началах участвовало около 600 человек и примерно 1600 компьютеров, объединенных в интернете.

То, что за 17 лет никто не смог дешифровать указанную фразу считалось подтверждением стойкости системы RSA-129. Однако в последние десятилетия были найдены эффективные алгоритмы факторизации, и в 2015 г. для дешифрования этого сообщения при использовании облачных вычислений потребовалось около одного дня. С 2013 г. браузеры Mozilla перестали поддерживать сертификаты удостоверяющих центров с ключами RSA меньше 2048 бит.

8.4 Факторизация натуральных чисел

Тесты на простоту числа. Элементарный *метод пробных делений* проверки простоты натурального N состоит в проверке делимости N на все простые числа от 2 до $\lfloor\sqrt{N}\,\rfloor$. Однако для чисел порядка 10^{40} и более этот метод уже неприменим.

Несложной является проверка на основе малой теоремы Ферма.

[10)] «*Волшебные слова — привередливая скопа*» (скопа — крупная хищная птица) — по-видимому, нарочито бессмысленная фраза.

Тест Ферма проверки простоты числа N.

Выбирается случайное $a \in [\ 2,\ N-1\ ]$, символически $a \xleftarrow{\$} [\ 2,\ N-1\ ]$.

N — составное, если окажется, что либо $a \mid N$, либо сравнение

$$a^{N-1} \equiv_N 1 \tag{8.6}$$

не выполняется. Иначе вопрос остаётся открытым и N испытывается при другом значении a.

Имеется, однако, бесконечно много составных чисел, для которых сравнение (8.6) выполняется при всех a, взаимно простых с N, т. е. они не будут выявлены данной проверкой. Эти числа называют *псевдопростыми* или *числами Кармайкла*[11)].

Отметим, что

- для составления *таблиц простых чисел* наилучшим является известный метод решета Эратосфена, несмотря на то, что он требует большого объёма памяти;
- на сегодняшний день разработаны быстрые и эффективные детерминированные алгоритмы определения простоты числа, основанные на эллиптических кривых.

Генерация ключей. Линейный конгруэнтный метод. Один из способов получения ключа шифрования — использовать генератор псевдослучайных чисел. Хорошие по статистическим свойствам последовательности псевдослучайных чисел получаются по формуле *линейного конгруэнтного метода*:

$$r_{i+1} \equiv_m a \cdot r_i + b, \quad i = 1, \ldots, N,$$

[11)] Роберт Дэниэл Кармайкл (R. D. Carmichael, 1879–1967) — американский математик, $561 = 3 \cdot 11 \cdot 17$ — пример числа Кармайкла.

где a, b, m — некоторые целые взаимно простые числа, от которых и зависит качество такой последовательности.

Очевидно, рассматриваемая последовательность будет периодической и показано, что её длина может достигать значения m. Часто данный генератор используют с параметрами

$$a = 214\,013, \quad b = 2\,531\,011, \quad m = 2^{32},$$

а в качестве r_1 берут текущее время с точностью до тика таймера компьютера.

Ясно, что значение r_1 однозначно определяет значения всех следующих членов последовательности. Например, если каждое r_i есть короткое целое число (16 бит), то различных ключей будет только 2^{16} вне зависимости от длины ключа N. Отсюда следует вывод, что псевдослучайные последовательности в качестве ключей использовать нельзя.

Сегодня специалисты сходятся во мнении, что источником истинно случайной последовательности может быть только какой-нибудь физический процесс: радиоактивный распад, тепловое движение атомов или молекул и т. п. Процесс оцифровывается и после определенной обработки используется. Различные методы типа вычисления адреса памяти или номера сектора на диске с извлечением данных оттуда, использование интервалов между последовательными нажатиями клавиш пользователя и т. д. раскритикованы как непригодные для применения в криптографии.

Построение больших простых чисел. На сегодняшний день созданы быстрые и эффективные алгоритмы для решения этой задачи. Опишем наиболее

простой из них.

Пусть уже имеется большое простое число S. Для построения существенно большего простого N:

1) выберем *четное* число $R \xleftarrow{\$} [\, S,\, 4S+2\,]$ и положим $N = SR + 1$;
2) проверим число N на отсутствие малых простых делителей;
3) испытаем N на простоту каким-либо не слишком трудоёмким тестом достаточно много раз;
4) если выяснится, что N — составное, то выберем новое значение R и повторим вычисления.

Если N, выдерживает испытания данным алгоритмом, то возможно, что N — простое. Тогда следует попытаться доказать это с помощью более мощных и трудоёмких тестов[12)].

Факторизация и сплиттинг. *Факторизация* натурального числа n — это нахождение его *примарного разложения*:

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s},$$

где p_i — разные простые числа, α_i — натуральные, $i = \overline{1, s}$.

Стойкость многих криптосистем основывается на трудности решения задачи FACT (криптосистема RSA, некоторые схемы цифровой подписи и др.).

[12)] см. теорему 4 на с. 102 книги *Введение в криптографию / Под общ. ред. В. В. Ященко. — М.: МЦНМО, 2012.*

Отметим, что на существующих компьютерах распознавание простоты целого числа с 125 десятичными цифрами может быть выполнено за несколько минут, в то время как его факторизация потребует миллионы лет компьютерных вычислений, то есть практически неосуществима[13)].

Сплиттингом натурального числа n называют представление его в виде

$$n = a \cdot b, \quad a, b \in [\ 2,\ n-1\ ],$$

а числа a и b — *нетривиальными факторами* n.

ρ-алгоритм сплиттинга составного целого n, которое не есть степень простого числа

Шаг 0. Полагаем $a = 2,\ b = 2,\ f(x) = x^2 + 1$.

Шаг 1. Перевычисляем

$$a := f(a),\ b := f(f(b)) \pmod{n}.$$

Шаг 2. Вычисляем $d = \text{НОД}\,(a - b, n)$.

Шаг 3. Если $d \in [\ 2,\ n-1\ ]$, то d — делитель n.
Если $d = 1$, то переход к Шагу 1.
Если $d = n$, то алгоритм заканчивает работу и вопрос о нетривиальных факторах в n остается открытым.

ρ-алгоритм Полларда[14)] для сплиттинга числа n

[13)] но с появлением квантовых компьютеров сможет быть решена за приемлемое время

[14)] Предложен в 1975 г. британским математиком Джоном Поллардом (John M. Pollard, 1941). Название связано с тем, что алгоритм строит числовую последовательность, элементы которой, начиная с некоторого номера n образуют цикл, что иллюстрируется расположением чисел в виде греческой буквы ρ.

требует $O\left(n^{1/4}\right)$ модулярных умножений и эффективен при поиске малых делителей. Его основная идея очень проста: если период последовательности $x_i \pmod n$ может быть порядка n, то период последовательности $x_i \pmod p$ для простого делителя p числа n не превосходит p. Это значит, что x_j и x_k могут быть различными по модулю n, но совпадать по модулю p, то есть $p \mid \text{НОД}\,(x_j - x_k, n)$.

Пример 8.5. 1. Пусть $n = 163\,829$.

Шаг 1. $a = 5,\ b = 26$.

Шаг 2. $a - b = 5 - 26 = -21 \equiv_{163\,829} = 163\,808$ и

$$d = \text{НОД}\,(163\,808, 163\,829) = 23.$$

Шаг 3. Поскольку $d \in [\ 2,\ n-1\ ]$, то $23 \mid 163\,829$.

Дальнейший анализ показывает, что $n/23 = 7\,123 = 17 \cdot 419$.

2. Пусть $n = 455\,459$. Результаты вычислений по ρ-алгоритму Полларда приведены в таблице

	a	b	d
1	5	26	1
2	26	2871	1
3	677	179 685	1
4	2871	155 260	1
5	44 380	416 250	1
6	179 685	43 670	1
7	121 634	164 403	1
8	155 260	247 944	1
9	44 567	68 343	743

Следовательно, 743 и $455\,459/743 = 613$ есть два нетривиальных делителя 455 459.

8.5 Дискретное логарифмирование

Задача DLOG. Криптосистема ЭльГамаля. Пусть G — мультипликативная абелева группа порядка n, $a, b \in G$. Задача нахождения решения уравнения

$$a^x \equiv_n b$$

называется *задачей (проблемой) дискретного логарифмирования* в группе G. Её решение x называется *дискретным логарифмом элемента b по основанию a*, символически $\log_a b$, если решение существует.

На сложности этой задачи DLOG базируется ряд шифрсистем с отрытым ключом, в частности рассмотренная ранее система Диффи–Хелмана DH и система ElGamal, разработанная ЭльГамалем[15)].

Рассмотрим вариант последней, когда G есть мультипликативная группа простого поля $\mathbb{F}_p$, то есть $|G| = n = p - 1$. Пусть также α — порождающий элемент G. Будем далее использовать изоморфизм групп $\mathbb{F}_p^*$ (по умножению) и $\mathbb{Z}_{p-1}$ (по сложению).

Для организации обмена Алиса и Боб выбирают в группе G каждый соответственно по своему секретному ключу

$$x_A,\, x_B \overset{\$}{\leftarrow} [\, 2,\ p-2\,]$$

[15)] Taher ElGamal (1955) — американский криптограф египетского происхождения.

и вычисляют значения

$$d_A = \alpha^{x_A} \quad \text{и} \quad d_B = \alpha^{x_B}.$$

Открытыми ключами, которыми обмениваются Алиса и Боб, являются тройки (p, α, d_A) и (p, α, d_B).

Пусть абонент A хочет передать абоненту B сообщение $m \in \mathbb{F}_p^*$. Для этого A выбирает ещё одно случайное число

$$s \xleftarrow{\$} [\, 2,\ p-2\,],$$

называемое *сеансовым ключом*, вычисляет по $\bmod p$ пару чисел

$$a = \alpha^s \quad \text{и} \quad b = m \cdot (d_B)^s,$$

и передаёт шифртекст (a, b) абоненту B по открытому каналу. Поэтому длина криптограммы в схеме ЭльГамаля вдвое длиннее исходного сообщения m.

Для расшифрования криптограммы, B вычисляет по $\bmod p$ значение m:

$$m = b(d_B)^{-s} = b(\alpha^{x_B})^{-s} = b(\alpha^s)^{-x_B} = ba^{p-1-x_B}.$$

Очевидно, шифросистема фактически является ЭльГамаля одним из способов выработки открытых ключей Диффи-Хеллмана.

Пример 8.6. Алиса передаёт Бобу своё сообщение BUJ, используя шифрсистему ЭльГамаля.

Вычисление ключей. Боб

1) выбирает простое $p = 2357$ и находит генератор $\alpha = 2$ мультипликативной группы поля $\mathbb{F}_p$;

2) выбирает свой секретный улюч — случайное число $x_B = 1751 \in [\,2,\, p-2\,]$ и вычисляет

$$d_B = \alpha^{x_B} \equiv_{2\,357} 1\,185;$$

3) передаёт Алисе свой открытый ключ

$$(\,p,\, \alpha,\, d_B\,) \;=\; (\;2\,357,\;2,\;1\,185\;).$$

Зашифрование. Алиса

1) получает открытый ключ Боба;

2) представляет свой текст BUJ в виде натурального числа $m \in [\,0,\, p-1\,]$ с помощью 27-ричной системы счисления:

$$m \;=\; \underbrace{2}_{B}\cdot 27^2 + \underbrace{21}_{U}\cdot 27^1 + \underbrace{10}_{J} \;=\; 2\,035;$$

3) выбирает случайный сеансовый ключ

$$s = 1520 \in [\,2,\, p-2\,];$$

4) вычисляет по $\bmod 2\,357$ числа $a = \alpha^s = 1\,430$ и

$$b = m \cdot (d_B)^s = 2\,035 \cdot 1\,185^{1520} = 697;$$

5) посылает шифртекст $(\,1\,430,\, 697\,)$ Бобу.

Расшифрование. Боб

1) получает криптограмму от Алисы;

2) вычисляет значение

$$a^{p-1-x_B} \;=\; 1\,430^{605} \;\equiv_{2\,357}\; 872$$

и получает $m \;=\; 872 \cdot 697 \;\equiv_{2\,357}\; 2\,035$;

3) представляет m в 27-ричной системе счисления: $m = 2\,035_{10} = [\;2\;21\;10\;]_{27}$ и получает исходный текст BUJ.

На практике значение p выбирают длиной не менее, чем 2048 бит.

Заметим, что сложность решения задачи DLOG зависит от конкретной группы G, на которой она задана. Например, для аддитивной группы $\mathbb{Z}_m$ эта задача сводится к решению линейного сравнения первой степени вида $ax \equiv_m b$, и не представляет трудности. Гораздо сложнее решение этой задачи в группе по умножению кольца $\mathbb{Z}_p$, где p — большое простое число[16)]. Так же ясно, что найти такой элемент x в группе $\mathbb{Z}_m$, что $a^x = b$ можно лишь если b принадлежит подгруппе, порожденной элементом a.

Алгоритм согласования. Рассмотрим сравнение

$$a^x \equiv_p b \tag{8.7}$$

в мультипликативной группе простого поля Галуа $G = \mathbb{F}_p^*$, где p — простое число. Будем предполагать, что a — примитивный элемент группы G, то есть $\operatorname{ord} a = p - 1$.

С помощью перебора можно решить уравнение (8.7) за $O(p)$ арифметических операций.

Известна формула $\log_a b \equiv \sum_{j=1}^{p-2} (1 - a^j)^{-1} b^j \pmod{p-1}$, однако сложность вычисления по ней, очевидно, хуже, чем для простого перебора.

Алгоритм согласования решения уравнения (8.7)

[16)] В настоящее время размер этого простого числа должен составлять порядка 1000 бит, чтобы эта задача была трудно решаема и ее можно было использовать при построении стойких криптосистем. Понятно, что реализация таких систем требует больших объемов машинной памяти.

1. Положить $H = \lceil \sqrt{p} \rceil$.
2. Найти $c = a^H \pmod p$.
3. Составить таблицу степеней $c^u \pmod p$ для $u = 1, \ldots, H$.
4. Составить таблицу значений $b \cdot a^v \pmod p$ для $v = 0, \ldots, H$.
5. Найти совпавшие элементы данных таблиц. Для них $c^u \equiv_p b \cdot a^v$ откуда $a^{Hu-v} \equiv_p b$. Выдать $x \equiv_{p-1} Hu - v$.

Докажем, что алгоритм работает корректно. Любое целое число $x \in [\ 0,\ p-2\ ]$ можно представить в виде $x \equiv_{p-1} Hu - v$, где $u \in [\ 1,\ H\ ]$, $v \in [\ 0,\ H\ ]$. Действительно, набор из $H(H+1)$ чисел вида

$$\begin{gathered} H,\ H-1,\ H-2,\ \ldots,\ H-H=0, \\ 2H,\ 2H-1,\ \ldots,\ 2H-H,\ \ldots, \\ H^2,\ H^2-1,\ \ldots,\ H^2-H \end{gathered}$$

содержит в себе, в частности, все числа $0,\ 1,\ \ldots,\ p-2$, поскольку $H^2 > p$.

На практике после выполнения Шагов 3 и 4 проводят упорядочение таблиц по возрастанию выходных значений. Поскольку набор из N элементов можно упорядочить за $O(N \log N)$ операций, оценка сложности алгоритма согласования — $O\left(\sqrt{p} \cdot \log p\right)$ арифметических операций.

Пример 8.7. Решим сравнение $6^x \equiv_{11} 8$.

Имеем $p = 11,\ a = 6,\ b = 8$.

1. $H = \lceil \sqrt{11} \rceil = 4$.
2. $6^4 = 1\,296 \equiv_{11} 9 = c \quad (1\,296 = 117 \cdot 11 + 9)$.
3. $u = 1, 2, 3, 4$

u	1	2	3	4
9^u	9	$9 \cdot 9 = 81$	$4 \cdot 9 = 36$	$3 \cdot 9 = 27$
$9^u \pmod{11}$	9	4	3	5

4. $v = 0, 1, \ldots, 4$

v	0	1	2	3	4
6^v	1	6	36	216	1 296
$8 \cdot 6^v$	8	48	288	1 728	10 368
$8 \cdot 6^v \pmod{11}$	8	4	2	1	6

5. Совпал элемент 4 таблиц при $u = 2$, $v = 1$, поэтому $x = Hu - v = 7 \equiv_{10} 7$.

Алгоритм согласования применим для вычисления дискретного логарифма в произвольной циклической группе.

Пример 8.8. Пусть требуется решить сравнение

$$2^x \equiv 17 \pmod{25}.$$

Для этого рассмотрим группу $G = \mathbb{Z}_{25}^*$. Понятно, что $|G| = \varphi(25) = \varphi(5^2) = 5 \cdot \varphi(5) = 20 = n$, конкретно,

$$G = \mathbb{Z}_{25} \setminus \{\, 0,\ 5,\ 10,\ 15,\ 20 \,\},$$

и легко убедится, что $G = \langle 2 \rangle$. Далее применяем описанный алгоритм, заменяя p на основание сравнения 25, кроме первого шага, где заменяем p на $n = 20$.

1. $H = \lceil 20 \rceil = 5$.
2. $c = 2^5 \equiv 7 \pmod{25}$.
3. $u = 1, 2, 3, 5$

u	1	2	3	4	5
$7^u \pmod{25}$	7	24	18	1	7

4. $v = 0, 1, \ldots, 5$

v	0	1	2	3	4	5
$17 \cdot 2^v \pmod{25}$	17	9	18	11	22	19

5. Совпал элемент 18 таблиц при $u = 3$, $v = 2$, поэтому $x = Hu - v = 13 \equiv_{24} 13$.

Разработаны и другие достаточно быстрые (субэкспоненциальные) алгоритмы дискретного логарифмирования, основанные на различных идеях.

8.6 Криптосистемы МакЭлиса и Ниддеррайтера

Криптосистема МакЭлиса. Данная система зашифрования с открытым ключом основана на задаче декодирования линейного кода, исправляющего ошибки[17)]. Исторически первая система, использующая в процессе шифрования рандомизацию — преобразование данных во время зашифрования с помощью генератора псевдослучайных чисел. Кратко опишем её простейший данной криптосистемы.

[17)] Разработана в 1978 г. американским математиком и инженером Р. Мак-Элисом (Robert J. McEliece, 1942).

Для получения секретных сообщений от Боба Алиса выбирает исправляющий r ошибок линейный $(n, k, 2r+1)$-код C, задающийся порождающей матрицей $G_{n\times k}$. Далее Алиса генерирует две квадратные матрицы:

P порядка n — перестановочную;

S порядка k — случайную невырожденную.

Вычисляя $n \times k$-матрицу

$$\widetilde{G} = P \times G \times S,$$

Алиса «маскирует» матрицу G.

Закрытым ключом является тройка матриц (S^{-1}, G, P^{-1}), а открытым — пара $(\widetilde{G}, r)$, который передаётся Бобу.

Боб, желая зашифровать своё сообщение $\boldsymbol{u}$ длины k, вычисляет вектор $\widetilde{G}\boldsymbol{x}$, добавляя к нему случайный n-вектор $\boldsymbol{e}$ с r единицами. В этом и состоит рандомизация информации.

Полученный шифртекст

$$\boldsymbol{w} = \widetilde{G}\boldsymbol{x} + \boldsymbol{e}.$$

Боб посылает Алисе.

Для расшифрования этой криптограммы Алиса вычисляет вектор

$$\widehat{\boldsymbol{w}} = P^{-1}\boldsymbol{w},$$

и, используя какой-либо алгоритм декодирования кода C, получает из $\widehat{\boldsymbol{w}}$ вектор $\widehat{\boldsymbol{u}}$. Исходно переданное сообщение Алиса получает, вычисляя

$$\boldsymbol{u} = S^{-1}\widehat{\boldsymbol{u}}.$$

По сравнению с RSA криптосистема МакЭлиса имеет преимущество в скорости зашифрования и расшифрования, а также более высокую степень защиты при данной длине ключа.

При этом она не свободна и от недостатков. К ним относятся большие размеры открытого ключа и криптограммы $\boldsymbol{w}$, которая оказывается значительно длиннее сообщения $\boldsymbol{u}$. Пример значений реально используемых параметров шифрсистемы МакЭлиса: $n = 6960$, $k = 5413$, $r = 119$, размер открытого ключа — 8 373 911 бит.

Криптосистема Нидеррайтера — предложенная в 1986 г. Х. Нидеррайтером[18)] модификация системы Мак-Элиса.

В отличие от неё, криптосистема Нидеррайтера использует проверочную H, а не порождающую матрица $(n, k, 2r + 1)$-кода, и не использует рандоминзацию данных.

Открытым ключом является пара (H_{pub}, r), где $H_{pub} = S \times H \times P$, а S и P — выбранные квадратные матрицы: случайная невырожденная порядка $n - k$ и перестановок P соответственно. Секретный ключ — тройка (S^{-1}, H, P^{-1}). В данной системе сообщениями являются все n-векторы с весом, не превосходящим r.

Поскольку система не использует случайные параметры, результат шифрования одного и того же текста будет одинаковым, что позволяет использовать её

[18)] Харальд Нидеррайтер (Harald G. Niederreiter, 1944) — австрийский математик.

именно систему для создания ЭЦП.

Размер открытого ключа в криптосистеме Нидеррайтера в $\frac{n}{n-k}$ раз меньше, чем в системе Мак-Элиса, а по сравнению с RSA скорость шифрования выше приблизительно в 50 раз, а дешифрования — в 100 раз.

Однако для её использования необходим алгоритм перевода исходного сообщения в n-вектор веса r и размер криптограммы намного больше, чем размер открытого текста.

Для ряда частных случаев системы МакЭлиса и Нидеррайтера взломаны российскими криптоаналитиками, однако они остаются стойкими при условии использовании *кодов Гоппы*[19)].

8.7 Задачи

Задача 8.1. *1. Решить комбинаторную задачу.*

Пусть p — простое число, большее 2. Сколько существует способов C раскрасить вершины правильного p-угольника в a цветов, если раскраски, получающиеся совмещением при вращении многоугольника вокруг своего центра, считать одинаковыми?

2. На основе полученного решения доказать малую теорему Ферма.

Задача 8.2. *Докажите справедливость сравнения*

[19)] Криптосистема МакЭлиса на кодах Гоппы рассматривается Еврокомиссией как перспективная.

$x^{(p-1)(q-1)} \equiv_n 1$ *с использованием только малой теоремы Ферма.*

Задача 8.3. *В системе шифрования RSA по данным модулю* $n = 91$ *и экспоненте* $e = 29$ *найти ключ расшифрования* d.

Задача 8.4. *Пусть в шифрсистеме RSA организатор (получатель сообщений) опубликовал открытый ключ* ($n = 21$, $e = 11$). *На стороне отправителя используя стандартную кодировку кириллического алфавита (А=01, Б=02, ...) зашифровать сообщение АБВ и расшифровать полученную криптограмму на стороне получателя.*

Задача 8.5. *Решить сравнения*

$$а)\ 6^x \equiv_{11} 2; \quad б)\ 8^x \equiv_{11} 3; \quad в)\ 2^x \equiv_{13} 3.$$

Задача 8.6. *Алиса A, Боб B и Кирилл C ведут секретную переписку, используя протокол DH, в качестве параметров которого они выбрали значения* $p = 23$ *и* $\alpha = 2$. *Секретные ключи Алисы, Боба и Кирилла суть*

$$x_A = 5,\ x_B = 17;\ и\ \ x_C = 12\ соответственно.$$

Определить их открытые X_A, X_B *и* X_C *и общие секретные ключи* K_{AB}, K_{AC} *и* K_{BC}.

Задача 8.7. *В системе RSA выбраны простое числа* $p = 11$ *и* $q = 17$ *и экспонента* $e = 13$. *Определить открытый и секретный ключи и расшифровать шифртексты* $y_1 = 02$ *и* $y_2 = 03$.

Список литературы

1. *Алескеров Ф.Т., Хабина Э.Л., Шварц Д.А.* Бинарные отношения, графы и коллективные решения: учеб. пособие для вузов. — М.: Изд. дом ГУ ВШЭ, 2006.

2. *Анализ формальных понятий.* [HTML] (http://www.machinelearning.ru/wiki/index.php?title=Анализ формальных понятий).

3. *Богомолов А.М., Салий В.Н.* Алгебраические основы теории дискретных систем. — М.: Наука, 1997.

4. *Биркгоф Г.* Теория решёток. — М.: Наука, 1984.

5. *Биркгоф Г., Барти Т.* Современная прикладная алгебра. — М.: Лань, 2005.

6. *Вагнер В.В.* Теория отношений и алгебра частичных отображений. / Теория полугрупп и её приложений. Сборник статей. Вып. 1. — Изд-во Сарат. ун-та, 1965. — С. 3–178.

7. *Владимиров Д.А.* Булевы алгебры. — М.: Наука, 1969.

8. *Гретцер Г.* Общая теория решёток. — М.: Мир, 1982.

9. *Гуров С.И.* Булевы алгебры, упорядоченные множества, решётки: определения, свойства, примеры. — М.: КРАСАНД, 2012.

10. *Кривулин Н.* Кривулин Н. Методы идемпотентной алгебры в задачах моделирования сложных систем. — СПб.: Изд-во С-Петерб. ун-та, 2009.

11. *Кузнецов С. О.* Теория решёток для интеллектуального анализа данных. [HTML] (http://vorona.hse.ru/sites/infospace/podrazd/facul/facul_bi/opm/DocLib3/ИОПF/book.pdf).

12. *Кузнецов С. О.* Автоматическое обучение на основе анализа формальных понятий. // Автоматика и телемеханика, 2001, № 10, С. 3–27.

13. *Курош А.Г.* Лекции по общей алгебре: Учебник. — СПб.: Издат-во «Лань», 2005[20)].

14. *Курош А.Г.* Общая алгебра (лекции 1969–1970 учебного года). — М.: Наука, 1974.

15. *Непейвода Н.Н.* Прикладная логика. — Новосибирск: НГУ, 2000.

16. *Оре О.* Теория графов. — М.: Наука, 1980.

17. *Пензов Ю.Е.* Элементы математической логики и теории множеств. — Саратов: Издат-во Саратовск. ун-та, 1968.

18. *Плоткин Б.И.* Универсальная алгебра, алгебраическая логика и базы данных. — М.: Наука, 1991.

[20)] Это издание включает и записи лекций [14], которые автор намеревался объединить с данным учебником.

19. *Скорняков Л.А.* Элементы теории структур. — М.: Наука, 1970.

20. *Стенли Р.* Перечислительная комбинаторика (Volume I). — М.: Мир, 1990.

21. *Столл Р.Р.* Множество. Логика. Аксиоматические теории. — М.: Просвещение, 1968.

22. *Теория* выбора и принятия решений: Учебное пособие. / Макаров И.М., Виноградская Т.М., Рубчинский А.А., Соколов В.Б. — М.: Наука, 1982.

23. *Шрейдер Ю.А.* Пространства толерантности. // Кибернетика, № 2, 1970. — С. 124–128.

24. *Яблонский С.В.* Введение в дискретную математику. — М.: Наука, 1986.

25. *Яглом И.М.* Булева структура и её модели. — М.: Сов. радио, 1980.

26. *Davey B.A., Priestley H.A.* Introduction to Lattices and Order. — Cambridge University Press, 1990.

27. *Finite Ordered Sets.* Concepts, Results and Uses. (Encyclopedia of Mathematics and its applications). / Caspard N., Leclerc B., Monjardet B. — Cambrige University Press. 2012.

28. *Handbook* of discrete and combinatorial mathematics. / Kenneth H. Rosen, editor in chief, John G. Michaels, project editor...[et al.]. CRC Press LLC. — 2000.

29. *Kuznetsov S.O.* Mathematical aspects of concept analysis. // Journal of Mathematical Science, Vol. 80, Issue 2, pp. 1654–1698, 1996.

30. *Ordered* Sets. Proc. NATO Adv. Study Inst. Banff (1981) (I. Rival, ed.). (Banff, Alta., Canada, 1981), NATO Ser. C: Math. Phys. Sci. Vol. 83, Dordrecht-Boston, Mass., 1982. pp. 171–211.

31. *Введение* в криптографию / Под общ. ред. В. В. Ященко. — 4-е изд., доп. М.: МЦНМО, 2012.

32. *Применко Э. А.* Алгебраические основы криптографии: Учебное пособие. — М.: Книжный дом «Либроком», 2014.

33. *Токарева Н. Н.* Симметричная криптография. Краткий курс: учебное пособие / Новосиб. гос. ун-т. Новосибирск, 2012.