Лекции по прикладной универсальной алгебре

Салий

Читались на факультете КНиИТ СГУ с 8 сентября по 1 декабря 2010 года (по средам).
Подготовлены в системе LaTeX с использованием пакета XY-pic.

Оглавление

Часть I

Универсальная алгебра

Глава 1

Множества и отношения

§1 Алгебра множеств

Обозначим через S некоторое фиксированное непустое множество-универсум. Определим *включение* множества A в множество B следующим образом:

$$A \subseteq B \overset{\text{def}}{\Leftrightarrow} (\forall a \in A)(x \in A \Rightarrow x \in B).$$

Будем обозначать $\mathscr{P}(S)$ *множество всех подмножеств* множества S.
Одним из способов изображения множеств являются диаграммы Венна. Базисные диаграммы для множеств S, $\varnothing$ и A приведены на рис. 1.1–1.3.
Операции над множествами ($A, B \in \mathscr{P}(S)$):

1. *Пересечение* множеств (рис. 1.4):

$$A \cap B \overset{\text{def}}{=} \{x \in S \colon x \in A \,\mathcal{AND}\, x \in B\}.$$

2. *Объединение* множеств (рис. 1.5):

$$A \cup B \overset{\text{def}}{=} \{x \in S \colon x \in A \,\mathcal{OR}\, x \in B\}.$$

3. *Дополнение* множества (рис. 1.6):

$$\overline{A} \overset{\text{def}}{=} \{x \in S \colon x \notin A\}.$$

Операции пересечения, объединения и дополнения называются *основными теоретико-множественными операциями.*
Рассмотрим набор подмножеств $\mathscr{A} \subseteq \mathscr{P}(S)$. Система $\mathscr{A}$ называется *замкнутой относительно операции пересечения*, если

$$(\forall A, B \in \mathscr{A})(A \cap B \in \mathscr{A}).$$

Рис. 1.1: Диаграмма для универсума S

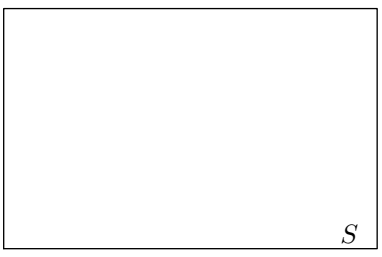


Рис. 1.2: Диаграмма для пустого множества $\varnothing$

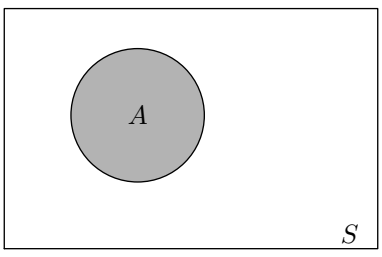


Рис. 1.3: Диаграмма для множества $A \subset S$

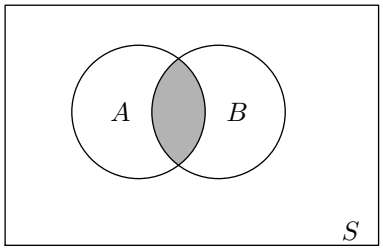


Рис. 1.4: Диаграмма Венна для $A \cap B$

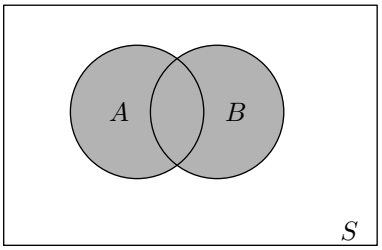


Рис. 1.5: Диаграмма Венна для $A \cup B$

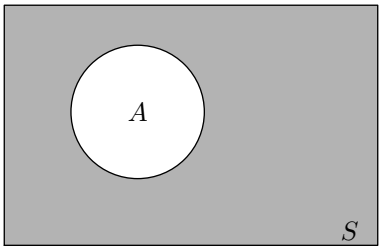


Рис. 1.6: Диаграмма Венна для $\overline{A}$

Система $\mathscr{A}$ называется *замкнутой относительно операции объединения*, если

$$(\forall A, B \in \mathscr{A})(A \cup B \in \mathscr{A}).$$

Система $\mathscr{A}$ называется *замкнутой относительно операции дополнения*, если

$$\left(\forall A \in \mathscr{A}\right)\left(\overline{A} \in \mathscr{A}\right).$$

Алгеброй множеств называется система

$$\left(\mathscr{A}, \cap, \cup, \overline{\ }, \varnothing, S\right),$$

где набор множеств $\mathscr{A} \subseteq \mathscr{P}(S)$ замкнут относительно пересечения, объединения и дополнения и содержит в себе $\varnothing$ и S.
Примеры алгебр.

1. Тотальная алгебра $\left(\mathscr{P}(S), \cap, \cup, \overline{\ }, \varnothing, S\right)$.
2. Тривиальная алгебра $\left(\{\varnothing, S\}, \cap, \cup, \overline{\ }, \varnothing, S\right)$.
3. Алгебра $\left(\left\{\varnothing, S, A, \overline{A}\right\}, \cap, \cup, \overline{\ }, \varnothing, S\right)$, порождённая подмножеством $A \subset S$.

Теорема 1 (основные тождества алгебры множеств)**.**

1. *Законы идемпотентности:*
   (a) $X \cap X = X$.
   (b) $X \cup X = X$.
2. *Законы коммутативности:*
   (a) $X \cap Y = Y \cap X$.
   (b) $X \cup Y = Y \cup X$.
3. *Законы ассоциативности:*
   (a) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$.
   (b) $X \cup (Y \cup Z) = (X \cup Y) \cup Z$.
4. *Законы поглощения:*
   (a) $X \cap (X \cup Y) = X$.
   (b) $X \cup (X \cap Y) = X$.
5. *Законы дистрибутивности:*

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

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

6. *Действия с пустым множеством и универсумом:*

(a) $X \cap \varnothing = \varnothing$, $X \cup \varnothing = X$.

(b) $X \cap S = X$, $X \cup S = S$.

7. *Законы дополнения:*

(a) $X \cap \overline{X} = \varnothing$.

(b) $X \cup \overline{X} = S$.

8. *Закон двойного дополнения:* $\overline{\overline{X}} = X$.

9. *Законы де Моргана:*

(a) $\overline{X \cap Y} = \overline{X} \cup \overline{Y}$.

(b) $\overline{X \cup Y} = \overline{X} \cap \overline{Y}$.

Доказательство.

1. Очевидно.

2. Очевидно.

3. (a) Докажем при помощи диаграмм Венна.
Построим диаграммы Венна для левой (рис. 1.7–1.8) и правой (рис. 1.9–1.10) частей тождества.

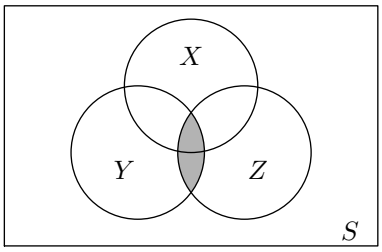


Рис. 1.7: $Y \cap Z$

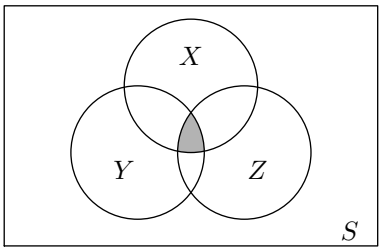


Рис. 1.8: $\boxed{X \cap (Y \cap Z)}$

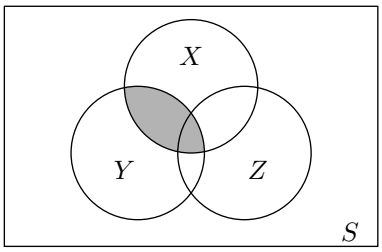


Рис. 1.9: $X \cap Y$

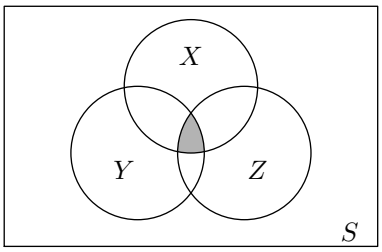


Рис. 1.10: $\boxed{(X \cap Y) \cap Z}$

(b) Доказывается аналогично.

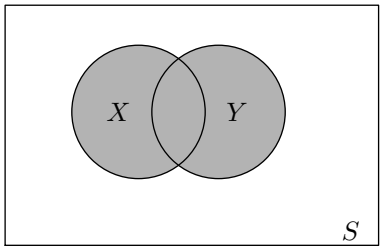


Рис. 1.11: $X \cup Y$

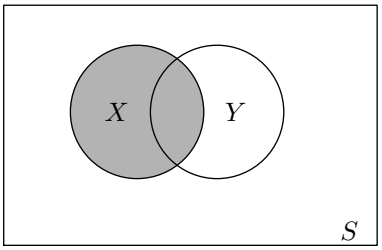


Рис. 1.12: $\boxed{X \cap (X \cup Y)}$

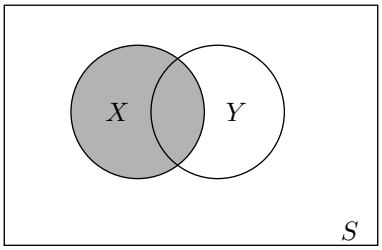


Рис. 1.13: $\boxed{X}$

4. (a) Диаграммы Венна для левой части — рис. 1.11–1.12, для правой — рис. 1.13 [1].
   (b) Аналогично.
5. (a) Левая часть — рис. 1.14–1.15. Правая часть — рис. 1.16–1.18.

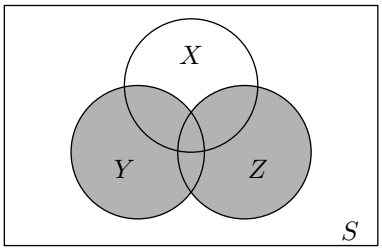


Рис. 1.14: $Y \cup Z$

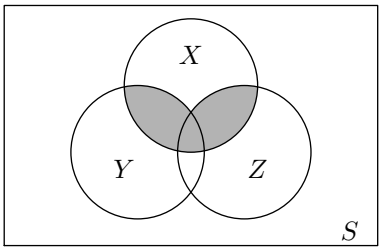


Рис. 1.15: $\boxed{X \cap (Y \cup Z)}$

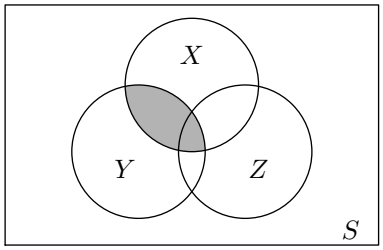


Рис. 1.16: $X \cap Y$

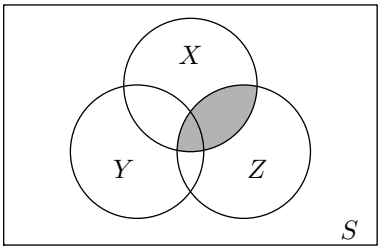


Рис. 1.17: $X \cap Z$

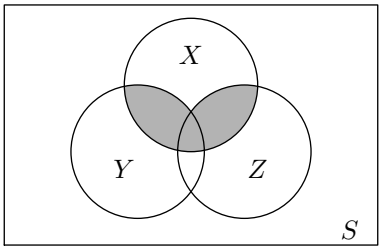


Рис. 1.18: $\boxed{(X \cap Y) \cup (X \cap Z)}$

   (b) Аналогично.
6. Очевидно.
7. Очевидно.
8. Очевидно.

[1] Правило: при доказательстве тождеств на каждой диаграмме нужно рисовать все множества, присутствующие в тождестве.

9. (a) Левая часть — рис. 1.19–1.20. Правая часть — рис. 1.21–1.23.

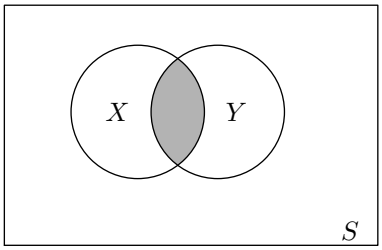


Рис. 1.19: $X \cap Y$

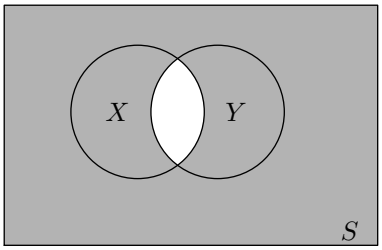


Рис. 1.20: $\boxed{\overline{X \cap Y}}$

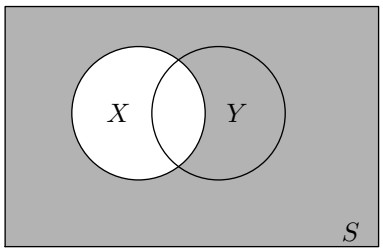


Рис. 1.21: $\overline{X}$

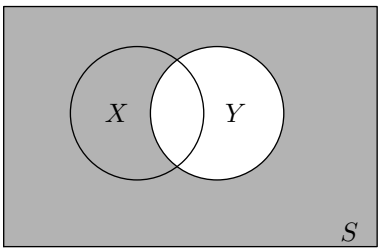


Рис. 1.22: $\overline{Y}$

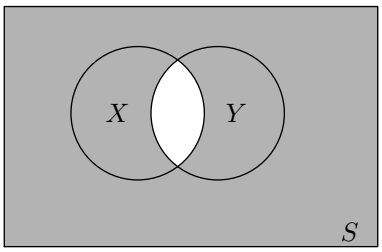


Рис. 1.23: $\boxed{\overline{X} \cup \overline{Y}}$

(b) Аналогично.

□

Операции пересечения и объединения, определённые в алгебре множеств, можно распространить на бесконечные наборы множеств: если $(A_i)_{i\in I} \subseteq \mathscr{P}(S)$, то

$$\bigcap_{i\in I} A_i \stackrel{\text{def}}{=} \{x \in S\colon (\forall i \in I)(x \in A_i)\},$$

$$\bigcup_{i\in I} A_i \stackrel{\text{def}}{=} \{x \in S\colon (\exists i \in I)(x \in A_i)\}.$$

В этом случае по-прежнему выполняются законы де Моргана. Действительно,

$$x \in \overline{\bigcap_{i\in I} A_i} \Leftrightarrow \neg\left(x \in \bigcap_{i\in I} A_i\right) \Leftrightarrow \neg\big((\forall i \in I)(x \in A_i)\big) \Leftrightarrow \big(\exists i \in I\big)\,\big(x \in \overline{A_i}\big) \Leftrightarrow x \in \bigcup_{i\in I} \overline{A_i}.$$

Кроме основных теоретико-множественных операций можно ввести две дополнительные:

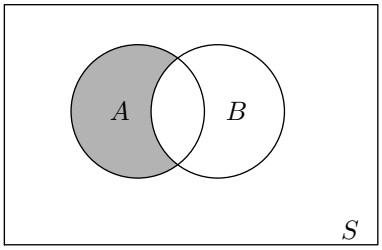


Рис. 1.24: $A - B$

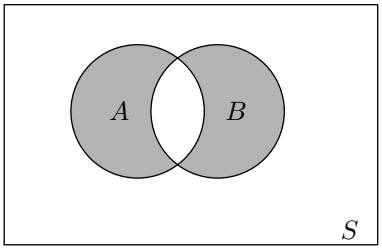


Рис. 1.25: $A \triangle B$

1. *Разность* множеств (рис. 1.24):
$$A - B \stackrel{\text{def}}{=} A \cap \overline{B}.$$

2. *Симметрическая разность* множеств (рис. 1.25):
$$A \triangle B \stackrel{\text{def}}{=} \left(A \cap \overline{B}\right) \cup \left(\overline{A} \cap B\right).$$

Теорема 2 (свойства разности и симметрической разности)**.**

1. $X - (Y - Z) = (X - Y) \cup (X \cap Z)$.
2. $X - (Y \cap Z) = (X - Y) \cup (X - Z)$.
3. $X - (Y \cup Z) = (X - Y) \cap (X - Z)$.
4. $X \triangle (Y \triangle Z) = (X \triangle Y) \triangle Z$.
5. $X \triangle Y = Y \triangle X$.
6. $(X \triangle Y) \cap Z = (X \cap Z) \triangle (Y \cap Z)$.

Доказательство.
Доказательство можно провести при помощи диаграмм Венна. □

§2 Алгебра логики

Алгеброй логики называется система
$$\mathbf{B}_2 = (B_2, \cdot, +, ', 0, 1),$$
где $B_2 = \{0, 1\}$, а операции $\cdot$, $+$, $'$ определены согласно таблицам:

$\cdot$	0	1
0	0	0
1	0	1

Таблица 1.1: Логическое умножение

$+$	0	1
0	0	1
1	1	1

Таблица 1.2: Логическое сложение

x	0	1
x'	1	0

Таблица 1.3: Логическое дополнение

Существует связь между операциями алгебры логики и логическими операторами. Если $\lambda(p)$ — логическое значение высказывания p, т.е.
$$\lambda(p) = \begin{cases} 1, \text{если } p \text{ истинно}, \\ 0, \text{если } p \text{ ложно}, \end{cases}$$
то $\lambda(p \,\mathcal{AND}\, q) = \lambda(p) \cdot \lambda(q)$, $\lambda(p \,\mathcal{OR}\, q) = \lambda(p) + \lambda(q)$, $\lambda(\neg p) = \big(\lambda(p)\big)'$.

Теорема 1 (основные тождества алгебры логики)**.**

1. *Идемпотентность:*
   (a) $x \cdot x = x$.
   (b) $x + x = x$.

2. *Коммутативность:*
   (a) $x \cdot y = y \cdot x$.
   (b) $x + y = y + x$.
3. *Ассоциативность:*
   (a) $x(yz) = (xy)z$.
   (b) $x + (y + z) = (x + y) + z$.
4. *Законы поглощения:*
   (a) $x(x + y) = x$.
   (b) $x + xy = x$.
5. *Дистрибутивность:*
   (a) $x(y + z) = xy + xz$.
   (b) $x + yz = (x + y)(x + z)$.
6. *Действия с 0 и 1:*
   (a) $x0 = 0$, $x + 0 = x$.
   (b) $x1 = x$, $x + 1 = 1$.
7. *Законы дополнения:*
   (a) $xx' = 0$.
   (b) $x + x' = 1$.
8. *Закон двойного дополнения:* $(x')' = x$.
9. *Законы де Моргана:*
   (a) $(xy)' = x' + y'$.
   (b) $(x + y)' = x'y'$.

Доказательство.
Докажем при помощи таблиц. Для всех вариантов значений переменных, входящих в формулу, будем последовательно вычислять левой и правой частей тождества. Если для всех наборов значений переменных значения левой и правой частей равны, то считаем тождество доказанным. Для примера докажем 5a.

x	y	z	$y+z$	$\boxed{x(y+z)}$	xy	xz	$\boxed{xy+xz}$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1

□

Алгебра логики является основным инструментом в приложениях математики, связанных с компьютерной техникой. Все конструкции современных компьютеров сначала выражаются в терминах алгебры логики, затем реализуются в виде физических объектов.

§3 Характеристические функции и векторы

Определим *характеристическую функцию* $\chi_A\colon S \to B_2$ подмножества A универсума S:

$$\chi_A(x) = \begin{cases} 1, \text{если } x \in A; \\ 0, \text{если } x \notin A. \end{cases}$$

Множество всех характеристических функций подмножеств универсума S

$$\mathrm{X}(S) = \{\chi_A\colon A \subseteq S\}.$$

Операции над характеристическими функциями:

1. *Умножение*:
$$(\chi_A \cdot \chi_B)(x) \stackrel{\text{def}}{=} \chi_A(x) \cdot \chi_B(x).$$
2. *Сложение*:
$$(\chi_A + \chi_B)(x) \stackrel{\text{def}}{=} \chi_A(x) + \chi_B(x).$$
3. *Дополнение*:
$$\chi'_A(x) \stackrel{\text{def}}{=} \big(\chi_A(x)\big)'.$$

Алгеброй характеристических функций на S называется система

$$\big(\mathrm{X}(S), \cdot, +, ', \mathbf{0}, \mathbf{1}\big).$$

Теорема 1.

1. $\chi_A = \chi_B \Leftrightarrow A = B$.
2. $\chi_A\chi_B = \chi_{A\cap B}$.
3. $\chi_A + \chi_B = \chi_{A\cup B}$.
4. $\chi'_A = \chi_{\overline{A}}$.
5. $\mathbf{0} = \chi_\varnothing$.
6. $\mathbf{1} = \chi_S$.

Доказательство.
Так как характеристическая функция принимает только значения 0 и 1, то для доказательства равенства двух функций достаточно установить, что значение 1 одна из функций принимает в тех же точках, что и другая. В качестве примера докажем 2:

$(\chi_A\chi_B)(x) = 1 \Leftrightarrow \chi_A(x)\chi_B(x) = 1 \Leftrightarrow \chi_A(x) = 1 \,\mathcal{AND}\, \chi_B(x) = 1 \Leftrightarrow x \in A \,\mathcal{AND}\, x \in B \Leftrightarrow x \in A \cap B \Leftrightarrow \chi_{A\cap B}(x) = 1.$

□

Если универсум $S = \{s_1, \ldots, s_n\}$, то множество $A \subseteq S$ можно закодировать двоичным вектором

$$\big(\chi_A(s_1), \ldots, \chi_A(s_n)\big).$$

Теорема 2. *Если* $|S| = n$, *то* $|\mathscr{P}(S)| = 2^n$.

Доказательство.
Подмножества универсума взаимно однозначно соответствуют кодирующим их двоичным векторам. Число двоичных векторов длины n равно 2^n, поэтому число подмножеств также равно 2^n.

□

§4 Алгебра отношений

1 Отношения

Декартовым произведением непустых множеств A и B называется множество

$$A \times B \stackrel{\text{def}}{=} \{(a,b)\colon a \in A \,\mathcal{AND}\, b \in B\}.$$

Если $a_1, a_2 \in A$, $b_1, b_2 \in B$, то

$$(a_1,b_1) = (a_2,b_2) \stackrel{\text{def}}{\Leftrightarrow} a_1 = a_2 \,\mathcal{AND}\, b_1 = b_2.$$

Если $|A| = m$, $|B| = n$, то $|A \times B| = mn$.
Отношением между множествами A и B называется подмножество произведения $A \times B$. Число всех возможных отношений между A и B равно $|\mathscr{P}(A \times B)| = 2^{mn}$. Для любого отношения ρ выполняется

$$\varnothing \subseteq \rho \subseteq A \times B.$$

Над отношениями можно осуществлять основные теоретико-множественные операции, следовательно, можно рассматривать алгебру множеств

$$\left(\mathscr{P}(A \times B), \cap, \cup, \overline{\ }, \varnothing, A \times B\right).$$

Если $(a,b) \in \rho$, то говорят, что a *находится в отношении* ρ с b.

2 Операции над отношениями

Над отношениями можно ввести две дополнительные операции.

1. *Умножение* отношений.
   Если $\rho \subseteq A \times B$, $\sigma \subseteq B \times C$, то

   $$\rho \circ \sigma \stackrel{\text{def}}{=} \left\{(a,c)\colon \big(\exists b \in B\big)\big((a,b) \in \rho \,\mathcal{AND}\, (b,c) \in \sigma\big)\right\} \subseteq A \times C.$$

   Теорема 1 (ассоциативность умножения)**.** *Если* $\rho \subseteq A \times B$, $\sigma \subseteq B \times C$, $\tau \subseteq C \times D$, *то*

   $$\rho \circ (\sigma \circ \tau) = (\rho \circ \sigma) \circ \tau.$$

   Доказательство.
   $\sigma \circ \tau \subseteq B \times D$, $\rho \circ (\sigma \circ \tau) \subseteq A \times D$. $\rho \circ \sigma \subseteq A \times C$, $(\rho \circ \sigma) \circ \tau \subseteq A \times D$. Таким образом, множества $\rho \circ (\sigma \circ \tau)$ и $(\rho \circ \sigma) \circ \tau$ имеют одинаковую структуру. Покажем, что они состоят из одних и тех же элементов.

   $$\begin{aligned}
   &(a,d) \in \rho \circ (\sigma \circ \tau) \Leftrightarrow \big(\exists b \in B\big)\big((a,b) \in \rho \,\mathcal{AND}\, (b,d) \in \sigma \circ \tau\big) \Leftrightarrow \\
   &\Big(\exists b \in B\Big)\Big((a,b) \in \rho \,\mathcal{AND}\, \big(\exists c \in C\big)\big((b,c) \in \sigma \,\mathcal{AND}\, (c,d) \in \tau\big)\Big) \Leftrightarrow \\
   &\big(\exists b \in B\big)\big(\exists c \in C\big)\big((a,b) \in \rho \,\mathcal{AND}\, (b,c) \in \sigma \,\mathcal{AND}\, (c,d) \in \tau\big) \Leftrightarrow \\
   &\Big(\exists c \in C\Big)\Big(\big(\exists b \in B\big)\big((a,b) \in \rho \,\mathcal{AND}\, (b,c) \in \sigma\big) \,\mathcal{AND}\, (c,d) \in \tau\Big) \Leftrightarrow \\
   &\big(\exists c \in C\big)\big((a,c) \in \rho \circ \sigma \,\mathcal{AND}\, (c,d) \in \tau\big) \Leftrightarrow (a,d) \in (\rho \circ \sigma) \circ \tau.
   \end{aligned}$$

   □

   Тождественным отношением на множестве A называется отношение

   $$\Delta_A = \{(x,y) \in A \times A\colon x = y\}.$$

Теорема 2 (нейтральность тождественного отношения)**.** *Если* $\rho \subseteq A \times B$*, то*

$$\Delta_A \circ \rho = \rho = \rho \circ \Delta_B.$$

Доказательство.
Очевидно, что $\Delta_A \circ \rho \subseteq A \times B$.

$$(a,b) \in \Delta_A \circ \rho \Leftrightarrow \big(\exists x \in A\big)\big((a,x) \in \Delta_A \,\mathcal{ANT}\, (x,b) \in \rho\big) \Leftrightarrow$$
$$(a,a) \in \Delta_A \,\mathcal{ANT}\, (a,b) \in \rho \Leftrightarrow (a,b) \in \rho.$$

Аналогично доказывается, что $\rho = \rho \circ \Delta_B$. □

2. *Обращение* отношений.
Если $\rho \subseteq A \times B$, то

$$\rho^{-1} \stackrel{\text{def}}{=} \big\{(b,a) \in B \times A \colon (a,b) \in \rho\big\}.$$

Теорема 3 (свойства обращения)**.** *Если* $\rho \subseteq A \times B$*,* $\sigma \subseteq B \times C$*, то*

(a) $(\rho^{-1})^{-1} = \rho$.

(b) $(\rho \circ \sigma)^{-1} = \sigma^{-1} \circ \rho^{-1}$.

Доказательство.

(a) Очевидно.

(b) Проведём следующие рассуждения:

$$(c,a) \in (\rho \circ \sigma)^{-1} \Leftrightarrow (a,c) \in \rho \circ \sigma \Leftrightarrow \big(\exists b \in B\big)\big((a,b) \in \rho \,\mathcal{ANT}\, (b,c) \in \sigma\big) \Leftrightarrow$$
$$\big(\exists b \in B\big)\big((c,b) \in \sigma^{-1} \,\mathcal{ANT}\, (b,a) \in \rho^{-1}\big) \Leftrightarrow (c,a) \in \sigma^{-1} \circ \rho^{-1}.$$

□

3 Алгебра отношений

Отношение $\rho \subseteq A \times B$ называется *однородным*, если $A = B$. Если универсум $S \neq \varnothing$, то набор множеств $\mathscr{P}(S \times S)$ замкнут относительно основных теоретико-множественных операций, а также операций умножения и обращения отношений.
Алгеброй отношений на S называется система

$$\big(\mathscr{R}, \cap, \cup, \circ, \overline{\ }, {}^{-1}, \varnothing, S \times S, \Delta_S\big),$$

где набор множеств $\mathscr{R} \subseteq \mathscr{P}(S \times S)$ замкнут относительно всех операций и содержит в себе множества $\varnothing$, $S \times S$, Δ_S.

4 Способы представления отношений

В приложениях используют два основных способа представления отношений:

1. Графы.
Если $S = \{s_1, \ldots, s_n\}$, то отношению $\rho \subseteq S \times S$ соответствует орграф $G(\rho)$, вершины которого обозначены $s_1, \ldots, s_n$, причём дуга из вершины s_i проходит в вершину s_j тогда и только тогда, когда $(s_i, s_j) \in \rho$. И наоборот, если дан орграф G с n вершинами, то ему можно сопоставить отношение $\rho(G)$ на множестве вершин. Это соответствие будет взаимно однозначным, т.е.

$$\rho\big(G(\rho)\big) = \rho,$$
$$G\big(\rho(G)\big) \equiv G.$$

2. Двоичные булевы матрицы.
   Если $S = \{s_1, \ldots, s_n\}$, $\rho \subseteq S \times S$, то отношению ρ можно поставить в соответствие матрицу $M(\rho)$ размера $n \times n$ такую, что

$$[M(\rho)]_{ij} = \begin{cases} 1, \text{если } (s_i, s_j) \in \rho; \\ 0, \text{если } (s_i, s_j) \notin \rho. \end{cases}$$

   Обратно, каждой матрице M с элементами из B_2 можно поставить в соответствие отношение $\rho(M)$. Если пометить строки и столбцы матрицы M элементами из S, то $(s_i, s_j) \in \rho$ тогда и только тогда, когда $M_{ij} = 1$. Таким образом, существует взаимно однозначное соответствие между матрицами M и отношениями ρ.

Обозначим за $\mathscr{M}_n$ множество всех двоичных булевых матриц размерности $n \times n$ над универсумом $S = \{s_1, \ldots, s_n\}$. В множестве $\mathscr{M}_n$ можно ввести следующие операции и объекты ($M, N \in \mathscr{M}_n$):

1. *Пересечение* матриц:
$$(M \wedge N)_{ij} = M_{ij} \cdot N_{ij}.$$
2. *Сложение*:
$$(M + N)_{ij} = M_{ij} + N_{ij}.$$
3. *Умножение*:
$$(M \cdot N)_{ik} = \sum_{j=1}^{n} M_{ij} \cdot N_{jk}.$$
4. *Дополнение*:
$$(M')_{ij} = (M_{ij})'.$$
5. *Транспонирование*:
$$(M^{\mathrm{T}})_{ij} = M_{ji}.$$
6. *Нулевая матрица*:
$$\mathbf{0}_{ij} = 0.$$
7. *Тотальная матрица*:
$$\mathbf{1}_{ij} = 1.$$
8. *Единичная матрица*:
$$E_{ij} = \begin{cases} 1, \text{если } i = j; \\ 0, \text{если } i \neq j. \end{cases}$$

Тогда *алгеброй двоичных булевых матриц* размерности $n \times n$ назовём систему

$$\left(\mathscr{M}_n, \wedge, +, \cdot, ', ^{\mathrm{T}}, \mathbf{0}, \mathbf{1}, E\right).$$

Теорема 4 (представление отношений двоичными булевыми матрицами)**.** *Взаимно однозначное соответствие*

$$\rho \leftrightarrow M(\rho)$$

между отношениями на n-элементном универсуме и двоичными булевыми матрицами размерности $n \times n$ над этим универсумом согласовано со всеми операциями алгебры отношений

$$\left(\mathscr{R}, \cap, \cup, \circ, \bar{}, ^{-1}, \varnothing, S \times S, \Delta_S\right)$$

и операциями алгебры матриц

$$\left(\mathscr{M}_n, \wedge, +, \cdot, ', ^{\mathrm{T}}, \mathbf{0}, \mathbf{1}, E\right)$$

в следующем смысле:

1. $M(\rho \cap \sigma) = M(\rho) \wedge M(\sigma)$.
2. $M(\rho \cup \sigma) = M(\rho) + M(\sigma)$.
3. $M(\rho \circ \sigma) = M(\rho)M(\sigma)$.
4. $M(\overline{\rho}) = M'(\rho)$.
5. $M(\rho^{-1}) = \big(M(\rho)\big)^{\mathrm{T}}$.
6. $M(\varnothing) = \mathbf{0}$.
7. $M(S \times S) = \mathbf{1}$.
8. $M(\Delta_S) = E$.

Иными словами, алгебра отношений и алгебра соответствующих им матриц являются реализациями одного и того же абстрактного объекта.

Доказательство.
В равенствах 1–8 в левых и правых частях стоят двоичные матрицы. Поэтому, чтобы доказать их равенство, достаточно установить, что единицы в них стоят на одних и тех же местах (в остальных будут нули).

1. $$[M(\rho \cap \sigma)]_{ij} = 1 \Leftrightarrow (s_i, s_j) \in \rho \cap \sigma \Leftrightarrow \big((s_i, s_j) \in \rho \,\mathcal{AND}\, (s_i, s_j) \in \sigma\big) \Leftrightarrow$$
$$[M(\rho)]_{ij} = 1 \,\mathcal{AND}\, [M(\sigma)]_{ij} = 1 \Leftrightarrow [M(\rho)]_{ij}[M(\sigma)]_{ij} = 1 \Leftrightarrow [M(\rho) \wedge M(\sigma)]_{ij} = 1.$$
   Таким образом, $M(\rho \cap \sigma) = M(\rho) \wedge M(\sigma)$.
2. Аналогично.
3. $$[M(\rho \circ \sigma)]_{ik} = 1 \Leftrightarrow (s_i, s_k) \in \rho \circ \sigma \Leftrightarrow \big(\exists j\big)\big((s_i, s_j) \in \rho \,\mathcal{AND}\, (s_j, s_k) \in \sigma\big) \Leftrightarrow$$
$$\big(\exists j\big)\big([M(\rho)]_{ij} = 1 \,\mathcal{AND}\, [M(\sigma)]_{jk} = 1\big) \Leftrightarrow \sum_{j=1}^{n} [M(\rho)]_{ij}[M(\sigma)]_{jk} = 1 \Leftrightarrow [M(\rho)M(\sigma)]_{ik} = 1.$$
4. Очевидно.
5. Очевидно.
6. Очевидно.
7. Очевидно.
8. Очевидно.

□

5 Типы отношений

Дан конечный универсум S. На нём возможны следующие типы отношений.

1. Отношение ρ называется *рефлексивным*, если

$$\big(\forall x \in S\big)\big((x,x) \in \rho\big).$$

   В графе $G(\rho)$ каждая вершина имеет петлю. В матрице $M(\rho)$ все элементы главной диагонали равны единице.

2. Отношение ρ называется *иррефлексивным*, если

$$\big(\exists x \in S\big)\big((x,x) \notin \rho\big).$$

   В графе $G(\rho)$ хотя бы одна вершина не имеет петли. В матрице $M(\rho)$ хотя бы один элемент главной диагонали равен 0.

3. Отношение ρ называется *антирефлексивным*, если

$$\big(\forall x \in S\big)\big((x,x) \notin \rho\big).$$

   В графе $G(\rho)$ нет петель. В матрице $M(\rho)$ все элементы главной диагонали равны нулю.

4. Отношение ρ называется *симметричным*, если

$$\big(\forall x \in S\big)\big(\forall y \in S\big)\big((x,y) \in \rho \Rightarrow (y,x) \in \rho\big).$$

   В графе $G(\rho)$ каждая дуга между двумя вершинами имеет встречную дугу между теми же вершинами. Матрица $M(\rho)$ симметрична относительно главной диагонали.

5. Отношение ρ называется *асимметричным*, если

$$\big(\exists x \in S\big)\big(\exists y \in S\big)\big((x,y) \in \rho\, \mathcal{AND}\, (y,x) \notin \rho\big).$$

   В графе $G(\rho)$ найдётся хотя бы одна дуга без встречной дуги. В матрице $M(\rho)$ хотя бы одна единица имеет 0 на симметричном ей относительно главной диагонали месте.

6. Отношение ρ называется *антисимметричным*, если

$$\big(\forall x \in S\big)\big(\forall y \in S\big)\big((x,y) \in \rho\, \mathcal{AND}\, (y,x) \in \rho \Rightarrow x = y\big).$$

   В графе $G(\rho)$ только петли имеют встречные дуги (себя). В матрице $M(\rho)$ вне главной диагонали каждая единица имеет на симметричном ей месте 0.

7. Отношение ρ называется *транзитивным*, если

$$\big(\forall x \in S\big)\big(\forall y \in S\big)\big(\forall z \in S\big)\big((x,y) \in \rho\, \mathcal{AND}\, (y,z) \in \rho \Rightarrow (x,z) \in \rho\big).$$

   Если в графе $G(\rho)$ между вершинами x и z есть путь из двух дуг, смежных с вершиной y, то есть дуга из x в z. Для матриц не существует простого описания транзитивности.

§5 Эквивалентности и разбиения

Отношение ε на S называется *отношением эквивалентности*, если оно рефлексивно, симметрично и транзитивно. Будем писать $x \sim y$, если $(x, y) \in \varepsilon$. Тогда *аксиомы эквивалентности* выглядят следующим образом:

1. $x \sim x$.
2. $x \sim y \Rightarrow y \sim x$.
3. $x \sim y \mathcal{AND} y \sim z \Rightarrow x \sim z$.

Классом эквивалентности отношения ε, соответствующим элементу x, называется множество

$$\varepsilon(x) \stackrel{\text{def}}{=} \{y \in S \colon x \sim y\}.$$

Лемма 1. $(s, t) \in \varepsilon \Leftrightarrow \varepsilon(s) = \varepsilon(t)$.

Доказательство.
Необходимость.
Пусть $(s, t) \in \varepsilon$ и $u \in \varepsilon(s)$.

$(s, t) \in \varepsilon \mathcal{AND} u \in \varepsilon(s) \Rightarrow (s, t) \in \varepsilon \mathcal{AND} (s, u) \in \varepsilon \Leftrightarrow (t, s) \in \varepsilon \mathcal{AND} (s, u) \in \varepsilon \Rightarrow (t, u) \in \varepsilon \Rightarrow u \in \varepsilon(t) \Rightarrow \varepsilon(s) \subseteq \varepsilon(t)$.

Аналогично показываем, что $\varepsilon(t) \subseteq \varepsilon(s)$, откуда $\varepsilon(s) = \varepsilon(t)$.
Достаточность.
Если $t \in \varepsilon(t)$, то $t \in \varepsilon(s)$, т.е. $(s, t) \in \varepsilon$. □

Совокупность множеств

$$\Pi = (A_i)_{i \in I}, A_i \subseteq S$$

называется *разбиением* множества S, если

1. $$\bigcup_{i \in I} A_i = S;$$
2. $$(\forall i, j)(i \neq j \Rightarrow A_i \cap A_j = \varnothing).$$

Множества A_i в этом случае называются Π-*блоками разбиения*.

Теорема 2 (основная теорема об эквивалентностях)**.**

1. *Если ε — отношение эквивалентности на множестве S, то совокупность всех различных классов ε образует разбиение $\Pi(\varepsilon)$ на S.*
2. *Если Π — разбиение множества S, то множество*

$$\varepsilon(\Pi) = \big\{(x, y) \in S \times S \colon x \text{ и } y \text{ находятся в одном } \Pi\text{-блоке}\big\}$$

является эквивалентностью на множестве S.

3. $\varepsilon\big(\Pi(\varepsilon)\big) = \varepsilon$, $\Pi\big(\varepsilon(\Pi)\big) = \Pi$.

Доказательство.

1. Покажем, что совокупность различных классов ε образует разбиение. Отношение ε рефлексивно, т.е.
$$\big(\forall s \in S\big)\big(s \in \varepsilon(s)\big),$$
поэтому
$$\bigcup_{s\in S} \varepsilon(s) = S.$$
Покажем, что классы, имеющие непустое пересечение, совпадают.

$\varepsilon(s) \cap \varepsilon(t) \neq \varnothing \Rightarrow \big(\exists u \in S\big)\big(u \in \varepsilon(s)\ \mathcal{AND}\ u \in \varepsilon(t)\big) \Rightarrow \big(\exists u \in S\big)\big((s,u) \in \varepsilon\ \mathcal{AND}\ (t,u) \in \varepsilon\big) \Rightarrow \big(\exists u \in S\big)\big((s,u) \in \varepsilon\ \mathcal{AND}\ (u,t) \in \varepsilon\big) \Rightarrow (s,t) \in \varepsilon \Rightarrow \varepsilon(s) = \varepsilon(t)$.

2. Рефлексивность и симметричность построенного отношения $\varepsilon(\Pi)$ очевидны. Докажем транзитивность:

$(x,y) \in \varepsilon(\Pi)\ \mathcal{AND}\ (y,z) \in \varepsilon(\Pi) \Rightarrow y \in \varepsilon(x)\ \mathcal{AND}\ (z,y) \in \varepsilon(\Pi) \Rightarrow y \in \varepsilon(x)\ \mathcal{AND}\ y \in \varepsilon(z) \Rightarrow \varepsilon(x) \cap \varepsilon(z) \neq \varnothing \Rightarrow \varepsilon(x) = \varepsilon(z) \Rightarrow (x,z) \in \varepsilon(\Pi)$.

3. Видно по построению.

□

Совокупность всех эквивалентностей на S образует множество $\mathrm{E}(S)$, которое содержит отношения Δ_S и $S \times S$.

Срезы

Дано отношение $\rho \subseteq A \times B$. *Срезом отношения ρ через элемент $a \in A$* называется множество
$$\rho(a) \stackrel{\text{def}}{=} \big\{b \in B\colon (a,b) \in \rho\big\},$$
а *срезом через подмножество* $X \subseteq A$ называется множество
$$\rho(X) \stackrel{\text{def}}{=} \bigcup_{x\in X} \rho(x).$$
Первой проекцией отношения ρ называется множество
$$\mathrm{pr}_1\,\rho \stackrel{\text{def}}{=} \Big\{a \in A\colon \big(\exists b \in B\big)\big((a,b) \in \rho\big)\Big\},$$
второй проекцией — множество
$$\mathrm{pr}_2\,\rho \stackrel{\text{def}}{=} \Big\{b \in B\colon \big(\exists a \in A\big)\big((a,b) \in \rho\big)\Big\}.$$
Очевидно, что вторая проекция представляет собой срез отношения через первую проекцию:
$$\mathrm{pr}_2\,\rho = \rho(\mathrm{pr}_1\,\rho),$$
а также
$$\mathrm{pr}_2\,\rho = \rho(A).$$
Отношения классифицируются по виду срезов:

1. *1-полное* отношение между A и B:
$$\mathrm{pr}_1\,\rho = A.$$

2. *2-полное* отношение между A и B:
$$\mathrm{pr}_2\,\rho = B.$$

3. *Полное* отношение:
$$\mathrm{pr}_1\,\rho = A\,\mathcal{AND}\,\mathrm{pr}_2\,\rho = B.$$

4. *Однозначное* (функциональное) отношение:
$$\big(\forall a \in A\big)\big((a,b_1) \in \rho\,\mathcal{AND}\,(a,b_2) \in \rho \Rightarrow b_1 = b_2\big).$$

5. *Отображение* (однозначное и 1-полное отношение):
$$\rho\colon A \to B.$$

6. *Инъективное* (взаимно однозначное) отображение:
$$\big(\forall a_1, a_2 \in A\big)\big(\rho(a_1) = \rho(a_2) \Rightarrow a_1 = a_2\big).$$

7. *Сюръективное* отображение:
$$\mathrm{pr}_2\,\rho = B.$$

8. *Биективное* (инъективное и сюръективное) отображение.

Теорема 3 (срез произведения)**.** *Если* $\rho \subseteq A \times B$, $\sigma \subseteq B \times C$, *то для всех* $a \in A$
$$(\rho \circ \sigma)(a) = \sigma\big(\rho(a)\big).$$

Доказательство.
Видно, что $(\rho \circ \sigma)(a) \subseteq C$ и $\sigma\big(\rho(a)\big)$.
$$c \in (\rho \circ \sigma)(a) \Leftrightarrow (a,c) \in \rho \circ \sigma \Leftrightarrow \big(\exists b \in B\big)\big((a,b) \in \rho\,\mathcal{AND}\,(b,c) \in \sigma\big) \Leftrightarrow$$
$$\big(\exists b \in B\big)\big(b \in \rho(a)\,\mathcal{AND}\,(b,c) \in \sigma\big) \Leftrightarrow \big(\exists b \in \rho(a)\big)\big((b,c) \in \sigma\big) \Leftrightarrow c \in \sigma\big(\rho(a)\big).$$

□

Фактормножеством множества S по отношению ε из $\mathrm{E}(S)$ называется множество ε-классов S/ε.
Естественное отображение
$$\mathrm{nat}\,\varepsilon\colon S \to S/\varepsilon$$
каждому элементу $s \in S$ ставит в соответствие класс $\varepsilon(s)$.

§6 Отношения порядка

Отношение ω на множестве S называется *отношением порядка*, если оно рефлексивно, транзитивно и антисимметрично.
Граф отношения порядка имеет свойства:

1. В каждой вершине есть петля.

2. В графе нет встречных дуг (кроме петель).

3. Если из вершины x в вершину z существует двудверный путь, то в графе есть дуга (x,z).

Упорядоченным множеством называется пара (S,ω). Одно и то же множество можно упорядочивать по-разному.
В дальнейшем для удобства будем писать $x \leqslant y$ вместо $(x,y) \in \omega$. Тогда *аксиомы порядка* будут иметь вид:

1. $x \leqslant x$.
2. $x \leqslant y \mathcal{AND} y \leqslant x \Rightarrow x = y$.
3. $x \leqslant y \mathcal{AND} y \leqslant z \Rightarrow x \leqslant z$.

Также можно ввести обозначения:

1. $x < y \overset{\text{def}}{\Leftrightarrow} x \leqslant y \mathcal{AND} x \neq y$.
2. $x \geqslant y \overset{\text{def}}{\Leftrightarrow} y \leqslant x$.
3. $x > y \overset{\text{def}}{\Leftrightarrow} x \geqslant y \mathcal{AND} x \neq y$.

Элемент $a \in (S, \leqslant)$ называется *наименьшим*, если

$$(\forall x \in S)(a \leqslant x).$$

Элемент $a \in (S, \leqslant)$ называется *минимальным*, если

$$(\nexists x \in S)(x < a).$$

Наименьший элемент является и минимальным, но не наоборот.
Убывающей цепью в упорядоченном множестве $(S, \leqslant)$ называется последовательность

$$a_1 > \ldots > a_n > \ldots.$$

Возрастающей цепью называется последовательность

$$a_1 < \ldots < a_n < \ldots.$$

Теорема 1 (об экстремальных элементах в конечных упорядоченных множествах)**.**

1. *В конечном упорядоченном множестве каждый элемент содержит некоторый минимальный элемент и содержится в некотором максимальном элементе* [2].
2. *Если в конечном упорядоченном множестве существует единственный минимальный (максимальный) элемент, то он является наименьшим (наибольшим) элементом этого упорядоченного множества.*

Доказательство.

1. Пусть $(S, \leqslant)$ — конечное упорядоченное множество. Если элемент $a \in S$ является минимальным, то a содержит минимальный элемент a, так как $a \leqslant a$.
   Если же a не является минимальным, то существует элемент $a_1 \in S$ такой, что $a > a_1$. Если a_1 является минимальным, то a содержит минимальный элемент. В противном случае найдётся элемент $a_2 \in S$ такой, что $a_1 > a_2$. В силу транзитивности отношения порядка получаем, что $a > a_2$. Если a_2 является минимальным, то a содержит минимальный элемент. Иначе можно продолжить этот процесс до тех пор, пока получаемая убывающая цепь не оборвётся на элементе a_k:

   $$a > a_1 > \ldots > a_k.$$

   Так как a_k минимальный элемент, то a содержит минимальный.
   Аналогично доказывается, что каждый элемент содержится в максимальном.

[2] В бесконечных упорядоченных множествах это утверждение может не выполняться.

2. Пусть $a \in S$ — единственный минимальный элемент. Согласно первому пункту, каждый элемент $x \in S$ содержит a. Это и означает по определению, что a является наименьшим элементом.

□

Для наглядного представления конечных упорядоченных множеств используют *диаграммы Хассе*.
Высотой $h(a)$ элемента a в конечном упорядоченном множестве называется наибольшая из длин убывающих цепей, начинающихся с этого элемента. Под длиной убывающей цепи понимается количество «звеньев» в ней.
Говорят, что элемент b в упорядоченном множестве $(S, \leqslant)$ *непосредственно следует* за элементом a, если

$$a < b \,\mathcal{AND}\, (\nexists x)(a < x < b).$$

В этом случае также говорят, что b является *верхним соседом* для a, а a является *нижним соседом* для b.
Диаграмма Хассе строится следующим образом. Пусть n — наибольшая из высот элементов в упорядоченном множестве $(S, \leqslant)$. Нарисуем $n+1$ горизонталей, пронумерованных снизу вверх соответственно $0, \ldots, n$. Расположим на них элементы множества S в соответствии с их высотами. Элементы одинаковой высоты можно располагать на горизонтали произвольно. Двигаясь снизу вверх, будем соединять прямолинейными отрезками каждый элемент с его нижними соседями.

§7 Автоматы

Автоматом называется система

$$\mathscr{A} = (S, X, \delta),$$

где S — конечное непустое *множество состояний*; X — конечное непустое *множество входных сигналов*; $\delta\colon S \times X \to S$ — *функция переходов*.
Формулой функционирования автомата называется формула вида

$$\delta(s, x) = t,$$

которая означает следующее: автомат, находящийся в состоянии s, под действием сигнала x в следующий момент времени переходит в состояние t. Считается, что автомат функционирует в дискретном времени.
Для задания автоматов используют два способа.

1. Таблица переходов.
   Пусть $S = \{s_1, \ldots, s_m\}$, $X = \{x_1, \ldots, x_n\}$. Таблица переходов имеет вид

$$\begin{array}{c|ccc} \delta & x_1 & \ldots & x_n \\ \hline s_1 & \delta(s_1, x_1) & \ldots & \delta(s_1, x_n) \\ \vdots & \vdots & \ddots & \vdots \\ s_m & \delta(s_m, x_1) & \ldots & \delta(s_m, x_n) \end{array},$$

   где $\delta(s_i, x_j)$ — значение функции переходов при s_i и x_j.

2. Диаграмма переходов.
   Каждому входному сигналу присваивается цвет. Диаграмма переходов представляет собой цветной мультиграф, вершины которого соответствуют состояниям автомата. Если

$$\delta(s_i, x_j) = s_k,$$

   то из вершины s_i в вершину s_k проводится дуга цвета x_j.

Автомат называется *автономным*, если $|X| = 1$. В этом случае функцию переходов рассматривают как отображение

$$\delta\colon S \to S.$$

Подмножество $S' \subseteq S$ называется *устойчивым* в автомате

$$\mathscr{A} = (S, X, \delta),$$

если оно *замкнуто* относительно функции δ, т.е.

$$\big(\forall s \in S'\big)\big(\forall x \in X\big)\big(\delta(s,x) \in S'\big).$$

В любом автомате устойчивы множества S и $\varnothing$.
Если множество $S' \subseteq S$ устойчиво в автомате

$$\mathscr{A} = (S, X, \delta),$$

то *подавтоматом* автомата $\mathscr{A}$, соответствующим множеству S', называется автомат

$$\mathscr{A}' = (S', X, \delta'),$$

где $\delta'\colon S' \times X \to S'$ — ограничение функции δ на $S' \times X$. В дальнейшем будем писать вместо ограниченной функции δ' ту же функцию δ. Подавтомат $\mathscr{A}'$ называется собственным, если он не совпадает с самим автоматом $\mathscr{A}$.
Множество всех подавтоматов автомата $\mathscr{A}$ обозначается $\operatorname{Sub}\mathscr{A}$. Оно включает в себя сам автомат $\mathscr{A}$ и *нулевой автомат*

$$\mathbf{0} = (\varnothing, X, \varnothing).$$

На практике при рассмотрении конкретного автомата интересуются не его эволюцией под действием одиночных входных сигналов, а тем, в какое состояние перейдёт автомат при подаче на вход последовательности входных сигналов. Продолжим функцию δ на множество X^* слов конечной длины над алфавитом X. Определим её индуктивно по длине входного слова:

1. $\delta(s, e) \stackrel{\text{def}}{=} s$, где e — пустое слово;
2. Если $p \in X^*$, $|p| = n$, то для всех $s \in S$ и всех $x \in X$

$$\delta(s, px) \stackrel{\text{def}}{=} \delta\big(\delta(s,p), x\big).$$

Состояние t называется *достижимым* из состояния s в автомате $\mathscr{A}$, если

$$\big(\exists p \in X^*\big)\big(\delta(s,p) = t\big).$$

По определению расширенной функции переходов каждое состояние достижимо из самого себя. Обозначим за $S(s)$ множество состояний, достижимых из состояния s. Для любого s множество $S(s)$ устойчиво, так как если $t \in S(s)$, то все состояния из $S(t)$ будут достижимы из состояния s.
Главным подавтоматом автомата $\mathscr{A}$, порождённым состоянием s, называется автомат

$$\mathscr{A}(s) = \big(S(s), X, \delta\big).$$

Множество главных подавтоматов обозначается $F(\mathscr{A})$.
На множестве подавтоматов $\operatorname{Sub}\mathscr{A}$ можно ввести следующее *отношение порядка*: если автоматы

$$\mathscr{A}_1 = (S_1, X, \delta), \mathscr{A}_2 = (S_2, X, \delta)$$

принадлежат множеству $\operatorname{Sub}\mathscr{A}$, то

$$\mathscr{A}_1 \leqslant \mathscr{A}_2 \overset{\text{def}}{\Leftrightarrow} S_1 \subseteq S_2.$$

По теореме об экстремальных элементах в конечных упорядоченных множествах каждый подавтомат данного автомата содержит некоторый минимальный ненулевой подавтомат и содержится в некотором максимальном собственном подавтомате.
Если порядок $\leqslant$ ограничить на главных подавтоматах, то получим упорядоченное множество

$$\big(F(\mathscr{A}), \leqslant\big),$$

которое называется *каркасом* автомата $\mathscr{A}$.
Когда рисуется диаграмма переходов автомата, следует рисовать её по возможности без самопересечений. В случае автономного автомата это возможно всегда. Его диаграмма будет представлять собой набор контуров с входящими в них деревьями. Такое представление называется *стандартным*.

Глава 2

Основные конструкции универсальной алгебры

§1 Алгебры. Подалгебры и редукты

Пусть дано множество $A \neq \varnothing$ и число $n \in \mathbb{N}$. Тогда *n-й декартовой степенью* множества A называется множество упорядоченных n-систем

$$A^n \stackrel{\text{def}}{=} \big\{(a_1, \ldots, a_n) \colon (\forall i = 1, \ldots, n)(a_i \in A)\big\}.$$

Равенство двух упорядоченных n-систем определяется следующим образом:

$$(a_1, \ldots, a_n) = (b_1, \ldots, b_n) \stackrel{\text{def}}{\Leftrightarrow} (\forall i)(a_i = b_i).$$

n-арной операцией на множестве A называется отображение

$$f \colon A^n \to A.$$

Если $a_1, \ldots, a_n \in A$, то элемент $f(a_1, \ldots, a_n)$ множества A называется *результатом* операции f. Также говорят, что f является *функцией* n аргументов, заданной на множестве A и принимающей значения в A.
В приложениях обычно используются унарные ($n = 1$), бинарные ($n = 2$) и тернарные ($n = 3$) операции, а операции более высокой арности используются в теоретических построениях.
Алгеброй называется система

$$\mathbf{A} = (A, f_1, \ldots, f_m),$$

где непустое множество A называется *носителем* алгебры $\mathbf{A}$, а операции $f_1, \ldots, f_m$ образуют *систему операций* алгебры. Если принять

$$F = \{f_1, \ldots, f_n\},$$

то алгебру можно записать сокращённо

$$\mathbf{A} = (A, F).$$

Подмножество n-арных операций системы F обозначим F_n.
В подробной записи алгебры операции перечисляются в порядке убывания (невозрастания) их арности. Если обозначить через n_i арность операции f_i, то получим вектор

$$(n_1, \ldots, n_m),$$

который называется *типом* алгебры.
В алгебре также выделяют *нульарные операции*. Нульарная операция фиксирует некоторый

элемент носителя A алгебры $\mathbf{A}$, который имеет какие-то особые свойства. Такие операции принято обозначать так же, как и элемент, значение которого они фиксируют.
Алгебра

$$\mathbf{A} = (A, \cdot)$$

типа (2) называется *группоидом*. Вместо $f(a, b)$ в этом случае пишут $a \cdot b$. Эту операцию называют *умножением*.
Полугруппой (ассоциативным группоидом) называется алгебра

$$\mathbf{A} = (A, \cdot)$$

типа (2), в которой выполняется *закон ассоциативности умножения*

$$x(yz) = (xy)z.$$

Моноидом (полугруппой с выделенным нейтральным относительно умножения элементом) называется алгебра

$$\mathbf{A} = (A, \cdot, e)$$

типа $(2, 0)$, где выполняются тождества:

$$x(yz) = (xy)z \text{ (ассоциативность умножения)},$$

$$xe = ex = x \text{ (нейтральность элемента } e).$$

Группой называется алгебра

$$\mathbf{A} = (A, \cdot, ^{-}, e)$$

типа $(2, 1, 0)$, в которой выполняются *аксиомы группы*:

$$x(yz) = (xy)z,$$

$$xe = ex = x,$$

$$x\overline{x} = \overline{x}x = e \text{ (законы обратимости)}.$$

Среди важнейших групп есть такие группы, как *мультипликативная группа положительных действительных чисел*

$$\left(\mathbb{R}^{+}, \cdot, ^{-1}, 1\right),$$

аддитивная группа целых чисел

$$(\mathbb{Z}, +, -, 0),$$

полная линейная группа порядка n

$$\left(M_n^{*}, \cdot, ^{-1}, E\right),$$

где M_n^{*} — множество невырожденных числовых матриц размерности $n \times n$.
Кольцом называется алгебра

$$\mathbf{A} = (A, +, \cdot, ^{-}, 0)$$

типа $(2, 2, 1, 0)$, в которой выполняются *аксиомы кольца*:

$$x + (y + z) = (x + y) + z \text{ (ассоциативность сложения)},$$

$$x(yz) = (xy)z \text{ (ассоциативность умножения)},$$

$$x + 0 = 0 + x = x \text{ (нейтральность нуля по сложению)},$$

$$x + (-x) = (-x) + x = 0 \text{ (обратимость)},$$

$$\begin{matrix} x(y + z) = xy + xz \\ (x + y)z = xz + yz \end{matrix} \text{ (дистрибутивность умножения относительно сложения)}.$$

Алгебра

$$\mathbf{A}^* = (A, F^*),$$

где $F^* \subseteq F$, называется *редуктом* алгебры $\mathbf{A} = (A, F)$.
Множество $A' \subseteq A$ называется *устойчивым* в алгебре $\mathbf{A} = (A, F)$, если оно *замкнуто* относительно всех операций, т.е.

$$\big(\forall x_1, \ldots, x_n \in A'\big)\big(\forall f \in F_n\big)\big(f(x_1, \ldots, x_n) \in A'\big).$$

По определению пустое множество считается устойчивым.
Устойчивое подмножество должно содержать все элементы, соответствующие нульарным операциям.
Если множество A' устойчиво в алгебре $\mathbf{A} = (A, F)$, то *подалгеброй* алгебры $\mathbf{A}$, соответствующей множеству A', называется алгебра

$$\mathbf{A}' = (A', F).$$

Каждая подалгебра должна содержать все нульарные операции. Если в алгебре нет нульарных операций, то одной из её подалгебр будет *нулевая алгебра*

$$\mathbf{0} = (\varnothing, F).$$

Сама алгебра $\mathbf{A}$ также считается подалгеброй.
Определим *порядок* на множестве $\operatorname{Sub}\mathbf{A}$ подалгебр алгебры $\mathbf{A}$: если $\mathbf{A}_1 = (A_1, F)$, $\mathbf{A}_2 = (A_2, F)$, то

$$\mathbf{A}_1 \leqslant \mathbf{A}_2 \overset{\text{def}}{\Leftrightarrow} A_1 \subseteq A_2.$$

Наибольшим элементом в упорядоченном множестве $(\operatorname{Sub}\mathbf{A}, \leqslant)$ является алгебра $\mathbf{A}$. Если в алгебре $\mathbf{A}$ нет нульарных операций, то в упорядоченном множестве $(\operatorname{Sub}\mathbf{A}, \leqslant)$ существует и наименьший элемент (нулевая алгебра $\mathbf{0}$).

§2 Морфизмы

Алгебры $\mathbf{A} = (A, F)$ и $\mathbf{B} = (B, F)$ называются *однотипными*, если они имеют одинаковый тип. Для удобства будем считать, что операции в них обозначены одинаково.
Отображение

$$\varphi\colon A \to B$$

называется *гомоморфизмом* алгебры $\mathbf{A}$ в алгебру $\mathbf{B}$, если оно *согласовано* со всеми операциями, т.е.

$$\Big(\forall x_1, \ldots, x_n \in A\Big)\Big(\forall f \in F_n\Big)\Big(\varphi\big(f(x_1, \ldots, x_n)\big) = f\big(\varphi(x_1), \ldots, \varphi(x_n)\big)\Big).$$

Совокупность всех гомоморфизмов алгебры $\mathbf{A}$ в алгебру $\mathbf{B}$ обозначается $\operatorname{Hom}(\mathbf{A}, \mathbf{B})$. Если отображение $\varphi\colon A \to B$ сюръективно, то говорят, что алгебра $\mathbf{B}$ является *гомоморфным образом* алгебры $\mathbf{A}$, и пишут

$$\mathbf{B} = \varphi(\mathbf{A}).$$

Такой гомоморфизм называют *наложением* алгебры $\mathbf{A}$ на алгебру $\mathbf{B}$.
Если гомоморфизм φ инъективен, то φ называется *вложением* алгебры $\mathbf{A}$ в алгебру $\mathbf{B}$.
Гоморфизмы алгебры $\mathbf{A}$ в себя называются её *эндоморфизмами*. Множество всех эндоморфизмов обозначается $\operatorname{End}\mathbf{A}$.

Теорема 1 (о моноиде эндоморфизмов алгебры)**.** *Система*

$$(\operatorname{End}\mathbf{A}, \circ, \Delta)$$

является моноидом.

Доказательство.
Покажем, что множество $\operatorname{End}\mathbf{A}$ замкнуто относительно операции $\circ$. Пусть $\varphi, \psi \in \operatorname{End}\mathbf{A}$, тогда

$$\big(\varphi\circ\psi\big)\big(f(x_1,\dots,x_n)\big) = \psi\Big(\varphi\big(f(x_1,\dots,x_n)\big)\Big) = \psi\Big(f\big(\varphi(x_1),\dots,\varphi(x_n)\big)\Big) =$$
$$= f\Big(\psi\big(\varphi(x_1)\big),\dots,\psi\big(\varphi(x_n)\big)\Big) = f\big((\varphi\circ\psi)(x_1),\dots,(\varphi\circ\psi)(x_n)\big),$$

т.е. $\varphi\circ\psi \in \operatorname{End}\mathbf{A}$.
Так как умножение преобразований ассоциативно, то система

$$(\operatorname{End}\mathbf{A}, \circ)$$

является полугруппой.
Покажем, что тождественное преобразование Δ является эндоморфизмом:

$$\Delta\big(f(x_1,\dots,x_n)\big) = f(x_1,\dots,x_n) = f\big(\Delta(x_1),\dots,\Delta(x_n)\big).$$

Таким образом, система

$$(\operatorname{End}\mathbf{A}, \circ, \Delta)$$

является моноидом. □

Биективные гомоморфизмы алгебры $\mathbf{A}$ в алгебру $\mathbf{B}$ называются *изоморфизмами*. Множество изоморфизмов алгебры $\mathbf{A}$ в алгебру $\mathbf{B}$ обозначается $\operatorname{Iso}(\mathbf{A},\mathbf{B})$. Изоморфизмы алгебры $\mathbf{A}$ на себя называются её *автоморфизмами*, а их множество обозначается $\operatorname{Aut}\mathbf{A}$. Если существует изоморфизм алгебры $\mathbf{A}$ в алгебру $\mathbf{B}$, то говорят, что алгебра $\mathbf{A}$ *изоморфна* алгебре $\mathbf{B}$, и пишут

$$\mathbf{A} \cong \mathbf{B}.$$

Теорема 2 (об изоморфности алгебр)**.** *Отношение изоморфности является отношением эквивалентности на множестве всех алгебр.*

Доказательство.

1. Так как тождественное преобразование является изоморфизмом, то всякая алгебра изоморфна самой себе, т.е. отношение изоморфности рефлексивно.

2. Если $\mathbf{A} \cong \mathbf{B}$, то между $\mathbf{A}$ и $\mathbf{B}$ существует изоморфизм φ. Покажем, что обратное отображение φ^{-1} является изоморфизмом. Очевидно, что отображение φ^{-1} биективно (так как биективно отображение φ). Теперь покажем, что φ^{-1} является гомоморфизмом: пусть $y_1,\dots,y_n \in B$, $f \in F_n$, тогда

   $$\varphi^{-1}\big(f(y_1,\dots,y_n)\big) = \varphi^{-1}\Big(f\big(\Delta(y_1),\dots,\Delta(y_n)\big)\Big) = \varphi^{-1}\Big(f\big((\varphi^{-1}\circ\varphi)(y_1),\dots,(\varphi^{-1}\circ\varphi)(y_n)\big)\Big) =$$
   $$= \varphi^{-1}\Big(f\Big(\varphi\big(\varphi^{-1}(y_1)\big),\dots,\varphi\big(\varphi^{-1}(y_n)\big)\Big)\Big) = \varphi^{-1}\Big(\varphi\Big(f\big(\varphi^{-1}(y_1),\dots,\varphi^{-1}(y_n)\big)\Big)\Big) =$$
   $$= f\big(\varphi^{-1}(y_1),\dots,\varphi^{-1}(y_n)\big).$$

   Таким образом, $\varphi^{-1} \in \operatorname{Iso}(\mathbf{B},\mathbf{A})$ и $\mathbf{B} \cong \mathbf{A}$, т.е. отношение изоморфности симметрично.

3. Пусть между алгебрами $\mathbf{A}$ и $\mathbf{B}$ существует изоморфизм φ, а между алгебрами $\mathbf{B}$ и $\mathbf{C}$ существует изоморфизм ψ. Очевидно, что произведение двух биекций также является биекцией. Кроме того, было показано, что произведение двух гомоморфизмов является гомоморфизмом. Таким образом, $\varphi\circ\psi \in \operatorname{Iso}(\mathbf{A},\mathbf{C})$ и $\mathbf{A} \cong \mathbf{C}$, т.е. отношение изоморфности транзитивно.

□

В универсальной алгебре изоморфные алгебры не различаются, а считаются лишь конкретными реализациями одного и того же абстрактного объекта.

Теорема 3 (подалгебры и гомоморфизмы)**.**

1. *Гомоморфный образ подалгебры является подалгеброй:*

$$\mathbf{A}' \in \operatorname{Sub}\mathbf{A}\ \mathcal{AND}\ \varphi \in \operatorname{Hom}(\mathbf{A},\mathbf{B}) \Rightarrow \mathbf{B}' = \big(\varphi(A'), F\big) \in \operatorname{Sub}\mathbf{B}.$$

2. *Гомоморфный прообраз подалгебры является подалгеброй:*

$$\mathbf{B}' \in \operatorname{Sub}\mathbf{B}\ \mathcal{AND}\ \varphi \in \operatorname{Hom}(\mathbf{A},\mathbf{B}) \Rightarrow \mathbf{A}' = \big(\varphi^{-1}(B'), F\big) \in \operatorname{Sub}\mathbf{A}.$$

Доказательство.

1. Покажем, что множество $B' = \varphi(A')$ устойчиво относительно всех операций в алгебре $\mathbf{B}$: если $b_1, \ldots, b_n \in B'$, то существуют элементы $a_1, \ldots, a_n \in A'$ такие, что для $i = \overline{1,n}$

$$b_i = \varphi(a_i).$$

Тогда для всех $f \in F_n$

$$f(b_1, \ldots, b_n) = f\big(\varphi(a_1), \ldots, \varphi(a_n)\big) = \varphi\big(f(a_1, \ldots, a_n)\big).$$

Так как $\mathbf{A}' \in \operatorname{Sub}\mathbf{A}$, то множество A' замкнуто относительно операций алгебры $\mathbf{A}$. Поэтому $f(a_1, \ldots, a_n) \in A'$. Учитывая, что $\varphi\colon A' \to B'$, получаем $f(b_1, \ldots, b_n) \in B'$, что и требовалось.

2. Покажем, что множество A' устойчиво в алгебре $\mathbf{A}$: если $a_1, \ldots, a_n \in A'$, то существуют элементы $b_1, \ldots, b_n \in B'$ такие, что для $i = \overline{1,n}$

$$b_i = \varphi(a_i).$$

Так как множество B' замкнуто, то для всех $f \in F_n$ $f(b_1, \ldots, b_n) \in B'$. Но

$$f(b_1, \ldots, b_n) = f\big(\varphi(a_1), \ldots, \varphi(a_n)\big) = \varphi\big(f(a_1, \ldots, a_n)\big),$$

следовательно, $f(a_1, \ldots, a_n) \in \varphi^{-1}(B') = A'$.

□

§3 Конгруэнции и факторалгебры

Дана алгебра $\mathbf{A} = (A, F)$. *Конгруэнцией* алгебры $\mathbf{A}$ называется отношение эквивалентности θ на множестве A, согласованное со всеми операциями алгебры $\mathbf{A}$ в следующем смысле:

$$\Big(\forall a_1, \ldots, a_n, b_1, \ldots, b_n \in A\Big)\Big(\forall f \in F_n\Big)\Big(\big(\forall i = \overline{1,n}\big)\big((a_i, b_i) \in \theta\big) \Rightarrow \big(f(a_1, \ldots, a_n), f(b_1, \ldots, b_n)\big) \in \theta\Big).$$

Совокупность $\operatorname{Con}\mathbf{A}$ конгруэнций алгебры $\mathbf{A}$ вместе с операцией включения $\subseteq$ образует упорядоченное множество $(\operatorname{Con}\mathbf{A}, \subseteq)$.
Факторалгеброй алгебры $\mathbf{A}$ по конгруэнции θ называется однотипная с ней алгебра

$$\mathbf{A}/\theta \stackrel{\text{def}}{=} (A/\theta, F).$$

Операции на ней определены следующим образом: для всех $a_1, \ldots, a_n$ и для всех $f \in F_n$

$$f\big(\theta(a_1), \ldots, \theta(a_n)\big) \stackrel{\text{def}}{=} \theta\big(f(a_1, \ldots, a_n)\big),$$

причём выбор конкретных элементов θ-классов несуществен.

§4 Три теоремы о гомоморфизмах

Ядром отображения

$$\varphi\colon A \to B$$

называется отношение эквивалентности

$$\operatorname{Ker}\varphi \stackrel{\text{def}}{=} \big\{(x,y) \in A \times A\colon \varphi(x) = \varphi(y)\big\}.$$

Теорема 1 (первая теорема о гомоморфизме)**.** *Ядро гомоморфизма является конгруэнцией:*

$$\varphi \in \operatorname{Hom}(\mathbf{A},\mathbf{B}) \Rightarrow \operatorname{Ker}\varphi \in \operatorname{Con}\mathbf{A}.$$

Доказательство.
Пусть $(a_1,a_1'),\ldots,(a_n,a_n') \in \operatorname{Ker}\varphi$. Покажем, что для всех $f \in F_n$

$$\big(f(a_1,\ldots,a_n), f(a_1',\ldots,a_n')\big) \in \operatorname{Ker}\varphi.$$

Так как $(a_i,a_i') \in \operatorname{Ker}\varphi$, то $\varphi(a_i) = \varphi(a_i')$ и

$$\varphi\big(f(a_1,\ldots,a_n)\big) = f\big(\varphi(a_1),\ldots,\varphi(a_n)\big) = f\big(\varphi(a_1'),\ldots,\varphi(a_n')\big) = \varphi\big(f(a_1',\ldots,a_n')\big),$$

откуда

$$\big(f(a_1,\ldots,a_n), f(a_1',\ldots,a_n')\big) \in \operatorname{Ker}\varphi,$$

следовательно, $\operatorname{Ker}\varphi \in \operatorname{Con}\mathbf{A}$. □

Теорема 2 (вторая теорема о гомоморфизме)**.** *Конгруэнция алгебры является ядром некоторого гомоморфизма этой алгебры:*

$$\theta \in \operatorname{Con}\mathbf{A} \Rightarrow \big(\exists\varphi \in \operatorname{Hom}(\mathbf{A},\mathbf{B})\big)\big(\theta = \operatorname{Ker}\varphi\big).$$

Доказательство.
Рассмотрим отображение

$$\operatorname{nat}\theta\colon A \to A/\theta$$

и покажем, что оно является гомоморфизмом:

$$(\operatorname{nat}\theta)\big(f(a_1,\ldots,a_n)\big) = \theta\big(f(a_1,\ldots,a_n)\big) = f\big(\theta(a_1),\ldots,\theta(a_n)\big) = f\big((\operatorname{nat}\theta)(a_1),\ldots,(\operatorname{nat}\theta)(a_n)\big).$$

Теперь убедимся, что $\operatorname{Ker}(\operatorname{nat}\theta) = \theta$:

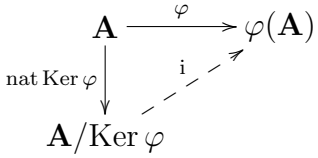
$$(a,a') \in \operatorname{Ker}\varphi \Leftrightarrow (\operatorname{nat}\theta)(a) = (\operatorname{nat}\theta)(a') \Leftrightarrow \theta(a) = \theta(a') \Leftrightarrow (a,a') \in \theta.$$

□

Теорема 3 (третья теорема о гомоморфизме)**.** *Гомоморфный образ алгебры изоморфен её факторалгебре по ядру гомоморфизма:*

$$\varphi \in \operatorname{Hom}(\mathbf{A},\mathbf{B}) \Rightarrow \varphi(\mathbf{A}) \cong \mathbf{A}/\operatorname{Ker}\varphi.$$

Доказательство.
Имеем следующую схему:



Рассмотрим отображение

$$\mathrm{i} : A/\mathrm{Ker}\,\varphi \to \varphi(A),$$

определённое следующим образом:

$$\mathrm{i}\big((\mathrm{Ker}\,\varphi)(a)\big) \stackrel{\mathrm{def}}{=} \varphi(a).$$

Покажем, что $\mathrm{i} \in \mathrm{Iso}\big(\mathbf{A}, \varphi(\mathbf{A})\big)$.
i инъективно:

$$\boxed{\mathrm{i}\big((\mathrm{Ker}\,\varphi)(a)\big) = \mathrm{i}\big((\mathrm{Ker}\,\varphi)(a')\big)} \Rightarrow \varphi(a) = \varphi(a') \Rightarrow (a, a') \in \mathrm{Ker}\,\varphi \Rightarrow \boxed{(\mathrm{Ker}\,\varphi)(a) = (\mathrm{Ker}\,\varphi)(a').}$$

i сюръективно:

$$\boxed{b \in \varphi(A)} \Rightarrow \big(\exists a \in A\big)\big(b = \varphi(a)\big) \Rightarrow \boxed{\Big(\exists a \in A\Big)\Big(b = \mathrm{i}\big((\mathrm{Ker}\,\varphi)(a)\big)\Big).}$$

i — гомоморфизм:

$$\boxed{\mathrm{i}\Big(f\big((\mathrm{Ker}\,\varphi)(a_1), \ldots, (\mathrm{Ker}\,\varphi)(a_n)\big)\Big)} = \mathrm{i}\Big(f\big((\mathrm{nat}\,\mathrm{Ker}\,\varphi)(a_1), \ldots, (\mathrm{nat}\,\mathrm{Ker}\,\varphi)(a_n)\big)\Big) =$$

(пользуемся тем, что $\mathrm{nat}\,\mathrm{Ker}\,\varphi$ — гомоморфизм)

$$= \mathrm{i}\Big((\mathrm{nat}\,\mathrm{Ker}\,\varphi)\big(f(a_1, \ldots, a_n)\big)\Big) = \mathrm{i}\Big((\mathrm{Ker}\,\varphi)\big(f(a_1, \ldots, a_n)\big)\Big) = \varphi\big(f(a_1, \ldots, a_n)\big) =$$
$$= f\big(\varphi(a_1), \ldots, \varphi(a_n)\big) = \boxed{f\Big(\mathrm{i}\big((\mathrm{Ker}\,\varphi)(a_1), \ldots, (\mathrm{Ker}\,\varphi)(a_n)\big)\Big).}$$

□

Гомоморфные образы алгебры в теории систем истолковываются как в той или иной степени «обеднённые» модели системы, которую представляет данная алгебра. Третья теорема о гомоморфизме утверждает, что всякий гомоморфный образ алгебры на самом деле можно рассматривать как факторалгебру этой алгебры по подходящей конгруэнции. Так как конгруэнции относятся к внутренней структуре алгебры, то это значит, что всякая модель системы, которую представляет данная алгебра, может быть описана во внутренних терминах исходной системы. Иными словами, не выходя за пределы системы, можно описать все её внешние модели.

§5 Автоматы как алгебры

Автоматы $\mathscr{A} = (S, X, \delta_{\mathscr{A}})$ и $\mathscr{B} = (T, Y, \delta_{\mathscr{B}})$ [1] называются *сравнимыми*, если $X = Y$.
Отображение

$$\varphi\colon S \to T$$

называется *гомоморфизмом* автомата $\mathscr{A}$ в автомат $\mathscr{B}$, если оно *согласовано* с функциями переходов этих автоматов в следующем смысле:

$$\Big(\forall s \in S\Big)\Big(\forall x \in X\Big)\Big(\varphi\big(\delta(s, x)\big) = \delta\big(\varphi(s), x\big)\Big).$$

Инъективные гомоморфизмы называются *вложениями*, сюръективные — *наложениями*, а биективные — *изоморфизмами*. Два автомата называются *изоморфными*, если между ними существует изоморфизм. Отношение изоморфности автоматов является отношением эквивалентности. Изоморфные автоматы не различаются, а считаются различными копиями одного и того

[1] Будем в дальнейшем для краткости обозначать функции переходов одинаково — δ, подразумевая, что известно, о какой именно функции идёт речь.

же автомата. Гомоморфизмы автомата в себя называются *эндоморфизмами*, а изоморфизмы на себя — *автоморфизмами*.
Отношение $\theta \subseteq S \times S$ называется *конгруэнцией* автомата $\mathscr{A}$, если θ является отношением эквивалентности на S, согласованным с функцией переходов в следующем смысле:

$$\Big(\forall s, s' \in S\Big)\Big((s, s') \in \theta \Rightarrow \Big(\forall x \in X\Big)\Big(\big(\delta(s, x), \delta(s', x)\big) \in \theta\Big)\Big).$$

Факторавтоматом автомата $\mathscr{A}$ по конгруэнции θ называется автомат

$$\mathscr{A}/\theta = (S/\theta, X, \delta),$$

где

$$\Big(\forall s \in S\Big)\Big(\forall x \in X\Big)\Big(\delta\big(\theta(s), x\big) = \theta\big(\delta(s, x)\big)\Big).$$

Определение функции переходов в факторавтомате не зависит от выбора конкретного представителя в классе $\theta(s)$.

Теорема 1 (Скотта)**.** *Каждому автомату $\mathscr{A}$ можно сопоставить унарную алгебру $\mathbf{A}_{\mathscr{A}}$ и каждой конечной унарной алгебре $\mathbf{A}$ можно сопоставить автомат $\mathscr{A}_{\mathbf{A}}$ таким образом, что это соответствие будет взаимно однозначным. При этом будут выполняться соотношения:*

1. $S' \in \operatorname{St}\mathscr{A} \Leftrightarrow S' \in \operatorname{St}\mathbf{A}_{\mathscr{A}}$, *где* St — *совокупность всех устойчивых подмножеств соответствующей структуры.*
2. $\operatorname{Hom}(\mathscr{A}, \mathscr{B}) = \operatorname{Hom}(\mathbf{A}_{\mathscr{A}}, \mathbf{A}_{\mathscr{B}})$.
3. $\operatorname{Con}\mathscr{A} = \operatorname{Con}\mathbf{A}_{\mathscr{A}}$.

Доказательство.
Укажем способ построения алгебры по автомату и автомата по алгебре. Пусть есть автомат

$$\mathscr{A} = (S, X, \delta), X = \{x_1, \ldots, x_n\}.$$

Тогда ему соответствует алгебра

$$\mathbf{A}_{\mathscr{A}} = (S, F), F = \{f_1, \ldots, f_n\},$$

где функции $f_i \colon S \to S$ определены следующим образом:

$$\big(\forall i\big)\big(f_i(s) \stackrel{\text{def}}{=} \delta(s, x_i)\big).$$

Обратно: пусть есть алгебра $\mathbf{A} = (S, F)$ типа $(\underbrace{1, \ldots, 1}_{n})$, где носитель S конечен, а множество функций

$$F = \{f_1, \ldots, f_n\}.$$

Ей соответствует автомат

$$\mathscr{A}_{\mathbf{A}} = (S, X, \delta),$$

где $X = \{x_1, \ldots, x_n\}$, а функция $\delta \colon S \times X \to S$ определена следующим образом:

$$\big(\forall i\big)\big(\delta(s, x_i) \stackrel{\text{def}}{=} f_i(s)\big).$$

Из построения видно, что соответствие взаимно однозначно.
Теперь докажем указанные соотношения:

1.

$$\boxed{S' \in \operatorname{St} \mathscr{A}} \Leftrightarrow \big(\forall s \in S'\big)\big(\forall x \in X\big)\big(\delta(s,x) \in S'\big) \Leftrightarrow \big(\forall s \in S'\big)\big(\forall i\big)\big(\delta(s,x_i) \in S'\big) \Leftrightarrow$$
$$\big(\forall s \in S'\big)\big(\forall i\big)\big(f_i(s) \in S'\big) \Leftrightarrow \boxed{S' \in \operatorname{St} \mathbf{A}_{\mathscr{A}}.}$$

Это соотношение говорит о том, что между подавтоматами автомата $\mathscr{A}$ и подалгебрами алгебры $\mathbf{A}_{\mathscr{A}}$ также существует взаимно однозначное соответствие: каждому подавтомату соответствует подалгебра, носителем которой является множество состояний соответствующего подавтомата.

2. $\operatorname{Hom}(\mathscr{A},\mathscr{B}) = \operatorname{Hom}(\mathbf{A}_{\mathscr{A}}, \mathbf{A}_{\mathscr{B}})$:

$$\boxed{\varphi \in \operatorname{Hom}(\mathscr{A},\mathscr{B})} \Leftrightarrow \Big(\forall s \in S\Big)\Big(\forall x \in X\Big)\Big(\varphi\big(\delta(s,x)\big) = \delta\big(\varphi(s),x\big)\Big) \Leftrightarrow$$
$$\Big(\forall s \in S\Big)\Big(\forall i\Big)\Big(\varphi\big(f_i(s)\big) = f_i\big(\varphi(s)\big)\Big) \Leftrightarrow \boxed{\varphi \in \operatorname{Hom}(\mathbf{A}_{\mathscr{A}}, \mathbf{A}_{\mathscr{B}})\,.}$$

3. $\operatorname{Con}\mathscr{A} = \operatorname{Con}\mathbf{A}_{\mathscr{A}}$:

$$\boxed{\theta \in \operatorname{Con}\mathscr{A}} \Leftrightarrow \Big(\forall s,s' \in S\Big)\Big(\forall x \in X\Big)\Big((s,s') \in \theta \Rightarrow \big(\delta(s,x),\delta(s',x)\big) \in \theta\Big) \Leftrightarrow$$
$$\Big(\forall s,s' \in S\Big)\Big(\forall i\Big)\Big((s,s') \in \theta \Rightarrow \big(f_i(s),f_i(s')\big) \in \theta\Big) \Leftrightarrow \boxed{\theta \in \operatorname{Con}\mathbf{A}_{\mathscr{A}}.}$$

□

Теорема Скотта показывает, что автоматы по существу совпадают с конечными унарными алгебрами. Поэтому все результаты, полученные для алгебр, естественным образом интерпретируются для автоматов.

Глава 3

Решётки

§1 Некоторые общие свойства упорядоченных множеств

Пусть (A, ω) — упорядоченное множество и $A' \subseteq A$. *Ограничением* (*сужением*) порядка ω на A' называется множество

$$\omega' = \omega \cap (A' \times A'),$$

которое также является отношением порядка. Также говорят, что ω является *продолжением* порядка ω' на A. В этом случае пару (A', ω') называют *упорядоченным подмножеством* упорядоченного множества (A, ω).
Порядок ω на множестве A называется *линейным порядком*, если выполняется *условие полноты*:

$$\big(\forall x, y \in A\big)\big((x, y) \in \omega \,\mathcal{OR}\, (y, x) \in \omega\big).$$

Будем говорить, что элементы x и y *сравнимы*, если

$$(x, y) \in \omega \,\mathcal{OR}\, (y, x) \in \omega;$$

в противном случае будем говорить, что они не сравнимы, и писать

$$x \parallel y.$$

Таким образом, *линейным упорядоченным множеством* называется множество, в котором любые два элемента сравнимы.
Диаграмма конечного линейного упорядоченного множества представляет собой цепь. Упорядоченное множество может не быть линейно упорядоченным, но в нём могут содержаться достаточно большие линейные упорядоченные множества, которые называются его цепями. В упорядоченном множестве могут быть цепи, которые не являются ни возрастающими, ни убывающими.

Теорема 1 (о линейных продолжениях порядков)**.** *Любой порядок на произвольном множестве может быть продолжен до линейного порядка на этом множестве.*

Доказательство.
Докажем теорему для конечных множеств.
Построим диаграмму множества (A, ω'). Введём на A порядок ω. Будем писать

$$x \leqslant y,$$

если $(x, y) \in \omega'$, и

$$x \preccurlyeq y,$$

если $(x, y) \in \omega$. Порядок ω должен быть линейным и содержать в себе порядок ω', т.е.

$$(\forall x, y \in A)(x \leqslant y \Rightarrow x \preccurlyeq y).$$

Определим ω следующим образом: $x \preccurlyeq y$, если на диаграмме вершина x расположена левее и ниже (необязательно строго), чем вершина y. Очевидно, что такое отношение ω рефлексивно, транзитивно и антисимметрично, т.е. является отношением порядка. Кроме того, этот порядок является линейным, так как какие бы две точки мы ни взяли на диаграмме упорядоченного множества (A, ω), одна из них будет левее и ниже другой.
Теперь докажем вложенность ω' в ω. Пусть $x < y$. Это значит, что на диаграмме (A, ω') существует восходящая ломаная от вершины x к вершине y, следовательно, вершина x расположена ниже вершины y и $x \preccurlyeq y$. Если же $x = y$, то $x \preccurlyeq x$. □

Пусть $(A, \leqslant)$ и $(B, \leqslant)$ — упорядоченные множества. Отображение

$$\varphi\colon A \to B$$

называется *изотонным*, если оно согласовано с обоими порядками:

$$\big(\forall x, y \in A\big)\big(x \leqslant y \Rightarrow \varphi(x) \leqslant \varphi(y)\big).$$

Упорядоченное множество $(A, \leqslant)$ называется *изоморфным* упорядоченному множеству $(B, \leqslant)$, если существует биекция

$$\varphi\colon A \to B$$

такая, что φ и φ^{-1} изотонны, т.е.

$$\big(\forall x, y \in A\big)\big(x \leqslant y \Leftrightarrow \varphi(x) \leqslant \varphi(y)\big).$$

Можно показать, что два конечных упорядоченных множества изоморфны тогда и только тогда, когда их можно изобразить одной и той же диаграммой Хассе с точностью до обозначений вершин.
Выпишем все различные (неизоморфные) упорядоченные множества с $n \leqslant 3$ элементами.

Рис. 3.1: $n = 1$

Рис. 3.2: $n = 2$

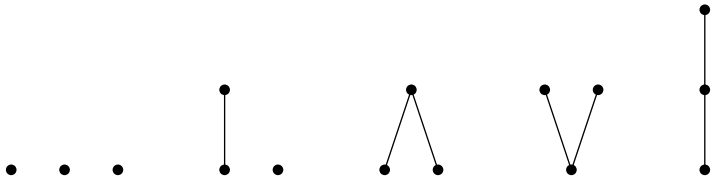


Рис. 3.3: $n = 3$

Перечислим известные значения для P_n — количества неизоморфных упорядоченных множеств с n элементами:

n	P_n	Автор	Год
1	1	-	-
2	2	-	-
3	5	-	-
4	16	-	-
5	63	-	-
6	318	-	-
7	2 045	J. Wright	1972
8	16 999	S.K. Das	1977
9	183 231	R.H. Möhring	1984
10	2 567 284	J.C. Culberson, G.J.E. Rawlins	1990
11	46 749 427	J.C. Culberson, G.J.E. Rawlins	1990
12	1 104 891 746	C. Chaunier, N. Lygeros	1991
13	33 823 827 452	C. Chaunier, N. Lygeros	1992
14	1 338 193 159 771	Heilz, Reinholf	2000

Теорема 2 (равносильные условия для упорядоченных множеств)**.** *В любом упорядоченном множестве* $(A, \leqslant)$ *следующие условия равносильны:*

1. Условие обрыва убывающей цепи: *в* $(A, \leqslant)$ *каждая убывающая цепь конечна.*
2. Условие минимальности: *каждое упорядоченное подмножество в* $(A, \leqslant)$ *содержит по крайней мере один минимальный элемент.*
3. Условие индуктивности: *если некоторым свойством* P *обладают все минимальные элементы упорядоченного множества* $(A, \leqslant)$ *и из того, что свойством* P *обладают все элементы, меньшие некоторого элемента* $a \in A$*, следует, что и элемент* a *обладает свойством* P*, то свойство* P *универсально в упорядоченном множестве* $(A, \leqslant)$*, т.е. им обладают все элементы* $(A, \leqslant)$*.*

Доказательство.
Докажем, что из 1 следует 2. От противного: пусть выполняется условие обрыва убывающей цепи, но не выполняется условие минимальности. Это значит, что существует непустое упорядоченное подмножество $(A', \leqslant)$, в котором не содержатся минимальные элементы. Возьмём элемент $a \in A'$. Так как он не является минимальным в A', то существует элемент $a_1 \in A'$ такой, что $a > a_1$ в $(A', \leqslant)$. a_1 не минимальный, поэтому можно взять элемент $a_2 \in A'$ такой, что $a_1 > a_2$. Продолжая аналогично, получим бесконечную убывающую цепь в $(A', \leqslant)$:

$$a > a_1 > \cdots > a_n > \ldots.$$

Она будет убывающей цепью и в упорядоченном множестве $(A, \leqslant)$. Но по условию в $(A, \leqslant)$ нет бесконечных убывающих цепей. Полученное противоречие доказывает, что в $(A, \leqslant)$ выполняется условие минимальности.
Докажем, что из 2 следует 3. От противного: пусть выполняется условие минимальности, но не выполняется условие индуктивности. Тогда существует свойство P, имеющее смысл для элементов упорядоченного множества $(A, \leqslant)$ и такое, что P выполняется для всех минимальных элементов $(A, \leqslant)$, а из того, что P выполняется для всех элементов, меньших a, следует, что P выполняется для a, но при этом P не является универсальным. Тогда рассмотрим A' — множество элементов, для которых P не выполняется. Так как в $(A, \leqslant)$ выполняется условие минимальности, то в $(A', \leqslant)$ существует минимальный элемент a_0. Элемент a_0 не может быть минимальным в $(A, \leqslant)$, потому что свойством P обладают все элементы, минимальные в $(A, \leqslant)$. Значит, в $(A, \leqslant)$ есть элементы, меньшие a_0, причём они все лежат в $A - A'$. Тогда для всех

них выполняется свойство P. Но по условию элемент a_0 тоже должен обладать свойством P. Полученное противоречие показывает, что условие индуктивности выполняется.
Остаётся доказать, что из 3 следует 1. Имеем: в $(A, \leqslant)$ выполняется условие индуктивности. Будем говорить, что элемент x обладает свойством P, если всякая убывающая цепь, которая начинается с него, конечна. Очевидно, что все минимальные элементы обладают этим свойством. Пусть свойство P выполняется для всех $x < a$. Возьмём убывающую цепь, начинающуюся с a:

$$a > a_1 > \dots.$$

$a_1 < a$, следовательно, a_1 обладает свойством P, и цепь, начинающаяся с a_1, конечна. Но тогда конечна и цепь $a > a_1 > \dots$. В $(A, \leqslant)$ выполняется условие индуктивности, поэтому свойство P универсально, т.е. всякая убывающая цепь конечна. А это и есть условие обрыва убывающей цепи. □

Условие индуктивности, применённое к упорядоченному множеству $(\mathbb{N}, \leqslant)$ натуральных чисел, составляет принцип математической индукции. Таким образом, доказательство по индукции можно проводить во всяком упорядоченном множестве, в котором выполняется условие обрыва убывающей цепи или условие минимальности.
Цепь C в упорядоченном множестве $(A, \leqslant)$ называется *максимальной*, если она не содержится ни в какой другой цепи этого множества. Цепь C называется *ограниченной сверху*, если существует элемент $a \in A$ такой, что для всех $x \in C$ $x \leqslant a$.
Пусть $A \neq \varnothing$ и $\mathscr{P}_0(A)$ — совокупность непустых подмножеств множества A. Отображение

$$\varphi\colon \mathscr{P}_0(A) \to A$$

называется *функцией выбора* для A, если для всех $X \in \mathscr{P}_0(A)$ $\varphi(X) \in X$.
Упорядоченное множество $(A, \leqslant)$ называется *вполне упорядоченным*, если оно линейно упорядочено и удовлетворяет условию минимальности (а вместе с ним условию обрыва убывающей цепи и условию индуктивности).

Рекомендуем

http://erovids-hiphop.ucoz.com — эротика с хип-хопом.
http://hiphop-mashups.ucoz.com — хип-хоп ремиксы.
http://shsd.znanium.ru/register.php?link=21308 — Школа своего дела (бизнес с нуля).