関係と順序

離散数学・オートマトン
2024 年後期
佐賀大学理工学部　只木進一

二項関係: Binary relations

- 2 つのモノを結びつける関係
- 集合 A と B の直積 $A \times B$ の部分集合 R
  - A から B への二項関係（A から B への関係）
  - $R : A \to B$
  - $(a, b) \in R$: a と b は R の関係にある: aRb
  - $R(a) = \{b \mid aRb\}$: a と R の関係にある全体
- $R : A \to A$: A の上への関係
- 写像、関数との違い
  - A の一つの要素から B の複数の要素への関係も含む
  - 写像と関数は関係の特殊な場合

関係の定義域、値域

$$R : X \to Y \tag{1.1}$$

- 定義域 (domain): X
- 値域 (range): Y
- 関数の場合と同じ

逆関係: Inverse relations

aRb の逆関係

- B から A への関係

$$R^{-1} = \{(b, a) \mid a \in A, b \in B, aRb\} \tag{1.2}$$

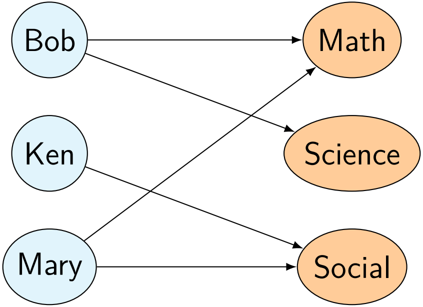
- $b \in B$ と aRb の関係にある a の全体

$$R^{-1}(b) = \{a \in A \mid aRb\} \tag{1.3}$$

- 逆関数との違いに注意

例 1.1: 生徒と得意科目

- $A = \{\text{Bob}, \text{Ken}, \text{Mary}\}$: **生徒の集合**
- $B = \{\text{Math}, \text{Science}, \text{Social}\}$: **科目の集合**



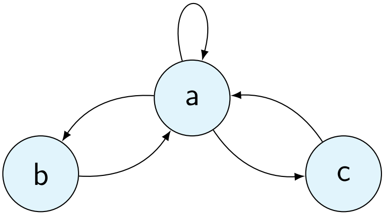
- $R : A \to B$
  - 生徒 $a \in A$ は、科目 $b \in B$ が得意である
- $R^{-1} : B \to A$
  - 科目 $b \in B$ を得意な生徒は $a \in A$ である

例 1.2: 関係とグラフ

- $X = \{\mathrm{a}, \mathrm{b}, \mathrm{c}\}$ 上の二項関係

$$R = \{(\mathrm{a}, \mathrm{a}), (\mathrm{a}, \mathrm{b}), (\mathrm{a}, \mathrm{c}), (\mathrm{b}, \mathrm{a}), (\mathrm{c}, \mathrm{a})\} \tag{1.4}$$

$$\begin{aligned} R(\mathrm{a}) &= \{\mathrm{a}, \mathrm{b}, \mathrm{c}\} \\ R(\mathrm{b}) &= R(\mathrm{c}) = \{\mathrm{a}\} \\ R^{-1}(\mathrm{a}) &= \{\mathrm{a}, \mathrm{b}, \mathrm{c}\} \\ R^{-1}(\mathrm{b}) &= R^{-1}(\mathrm{c}) = \{\mathrm{a}\} \end{aligned}$$



例 1.3: 包含関係

- 集合 X の部分集合上の包含関係 $\subseteq = \{(A, B) \mid A \subseteq B \subseteq X\}$
- $\subseteq^{-1}(B) = 2^B$:B のべき集合
  - B の部分集合全体

$$X = \{\mathsf{a}, \mathsf{b}\} \tag{1.5}$$

$$2^X = \{\emptyset, \{\mathsf{a}\}, \{\mathsf{b}\}, \{\mathsf{a}, \mathsf{b}\}\} \tag{1.6}$$

$$\begin{array}{cccc}
\emptyset \subseteq \emptyset & \emptyset \subseteq \{\mathsf{a}\} & \emptyset \subseteq \{\mathsf{b}\} & \emptyset \subseteq \{\mathsf{a}, \mathsf{b}\} \\
\{\mathsf{a}\} \subseteq \{\mathsf{a}\} & \{\mathsf{a}\} \subseteq \{\mathsf{a}, \mathsf{b}\} & & \\
\{\mathsf{b}\} \subseteq \{\mathsf{b}\} & \{\mathsf{b}\} \subseteq \{\mathsf{a}, \mathsf{b}\} & & \\
\{\mathsf{a},\mathsf{b}\} \subseteq \{\mathsf{a}, \mathsf{b}\} & & &
\end{array}$$

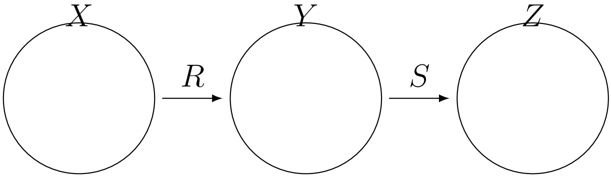
$$\begin{aligned}
\{a, b\} &\subseteq^{-1} \{\emptyset, \{a\}, \{b\}, \{a, b\}\} \\
\{a\} &\subseteq^{-1} \{\emptyset, \{a\}\} \\
\{b\} &\subseteq^{-1} \{\emptyset, \{b\}\} \\
\emptyset &\subseteq^{-1} \{\emptyset\}
\end{aligned}$$

関係と関数: Relations and Functions

- 関係 $R : X \to Y$ が以下を満たすとき、関数と呼ぶ
  - $\forall x \in X$ に対して $|R(x)| = 1$、つまり x に対して一つの $y \in Y$ が定まる
- つまり、関数は、関係の特別な場合

関係の結合: Compositions

- 集合 X、Y、Z に対する関係 $R : X \to Y$ 及び $S : Y \to Z$



- 関係の結合

$$S \circ R : X \to Z \tag{2.1}$$

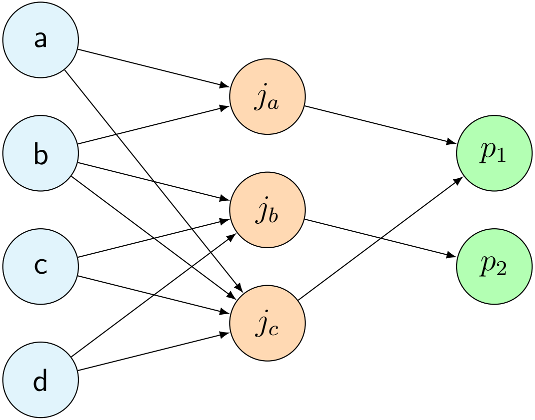
$$S \circ R = \{(x, z) \in X \times Z \mid \exists y \in Y,\ xRy \land ySz\} \tag{2.2}$$

- 結合律

$$R_3 \circ (R_2 \circ R_1) = (R_3 \circ R_2) \circ R_1 \tag{2.3}$$

例 2.1: 論文著者 $\rightarrow$ 学術誌 $\rightarrow$ 出版社

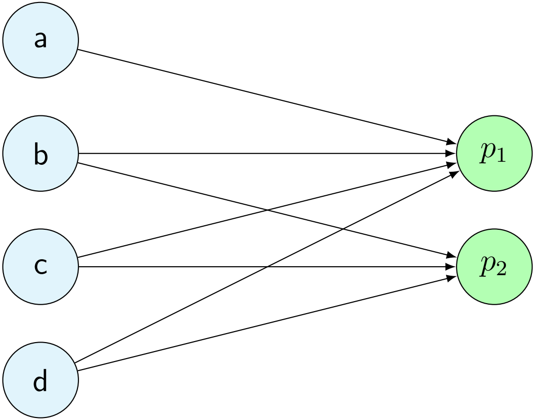
- $R : A \rightarrow J$: 著者 $a \in A$ は $j \in J$ の学術誌に論文を出版した
- $S : J \rightarrow P$: 学術誌 $j \in J$ は $p \in P$ という出版社が出版している。



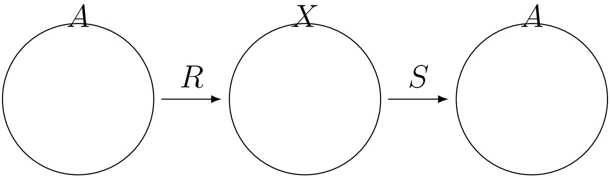
$$R = \{(\mathsf{a}, j_a), (\mathsf{a}, j_c), (\mathsf{b}, j_a), (\mathsf{b}, j_b), (\mathsf{b}, j_c), (\mathsf{c}, j_b), (\mathsf{c}, j_d), (\mathsf{d}, j_b), (\mathsf{d}, j_d)\} \tag{2.4}$$

$$S = \{(j_a, p_1), (j_b, p_2), (j_c, p_1)\} \tag{2.5}$$

$$S \circ R = \{(\mathsf{a}, p_1), (\mathsf{b}, p_1), (\mathsf{b}, p_2), (\mathsf{c}, p_1), (\mathsf{c}, p_2), (\mathsf{d}, p_1), (\mathsf{d}, p_2)\} \tag{2.6}$$



例 2.2:

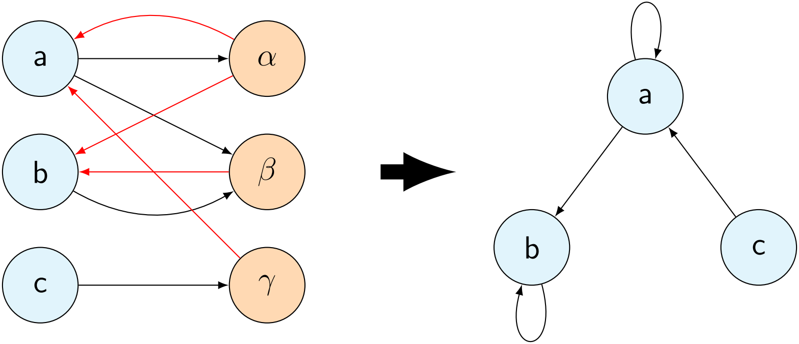


- $A = \{\mathsf{a}, \mathsf{b}, \mathsf{c}\}$ と $X = \{\alpha, \beta, \gamma\}$ に対して

$$R = \{(\mathsf{a}, \alpha), (\mathsf{a}, \beta), (\mathsf{b}, \beta), (\mathsf{c}, \gamma)\} \tag{2.7}$$

$$S = \{(\alpha, \mathsf{a}), (\alpha, \mathsf{b}), (\beta, \mathsf{b}), (\gamma, \mathsf{a})\} \tag{2.8}$$

$$\begin{aligned} S \circ R &= \{(x, z) \in A \times A \mid \exists y \in X,\ xRy \wedge ySz\} \\ &= \{(\mathsf{a}, \mathsf{a}), (\mathsf{a}, \mathsf{b}), (\mathsf{b}, \mathsf{b}), (\mathsf{c}, \mathsf{a})\} \end{aligned} \tag{2.9}$$


a
b
c
α
β
γ
a
b
c

恒等関係、関係のべき乗

- $R : A \to A$
  - $R^0 = \Delta_A = \{(a, a) \mid a \in A\}$: **恒等関係**: identity
  - $R^{n+1} = R \circ R^n$: **べき乗**: exponentiation

関係の和、共通部分

- 定義域と値域が共通の二つの関係 $R, S : A \to B$
  - 和 (union): $R \cup S$
  - 共通部分 (intersection): $R \cap S$
- 反射的推移閉包: reflexive transitive closures

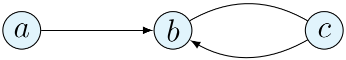
$$R^* = \bigcup_{n=0}^{\infty} R^n \tag{2.10}$$

- 推移閉包: transitive closures

$$R^+ = \bigcup_{n=1}^{\infty} R^n \tag{2.11}$$

例 2.3:

$$R = \{(\mathsf{a}, \mathsf{b}), (\mathsf{b}, \mathsf{c}), (\mathsf{c}, \mathsf{b})\} \tag{2.12}$$



- R^2

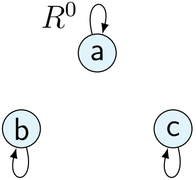
$$\mathsf{a}R\mathsf{b} \wedge \mathsf{b}R\mathsf{c} \Rightarrow \mathsf{a}R^2\mathsf{c}$$
$$\mathsf{b}R\mathsf{c} \wedge \mathsf{c}R\mathsf{b} \Rightarrow \mathsf{b}R^2\mathsf{b}$$
$$\mathsf{c}R\mathsf{b} \wedge \mathsf{b}R\mathsf{c} \Rightarrow \mathsf{c}R^2\mathsf{c}$$

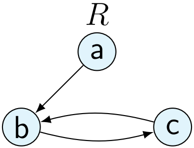
- R^3

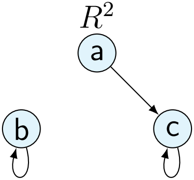
$$\mathsf{a}R\mathsf{b} \wedge \mathsf{b}R^2\mathsf{b} \Rightarrow \mathsf{a}R^3\mathsf{b}$$
$$\mathsf{b}R\mathsf{c} \wedge \mathsf{c}R^2\mathsf{c} \Rightarrow \mathsf{b}R^3\mathsf{c}$$
$$\mathsf{c}R\mathsf{b} \wedge \mathsf{b}R^2\mathsf{b} \Rightarrow \mathsf{c}R^3\mathsf{b}$$

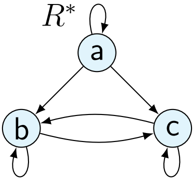
- $R = R^3$ を得る

$$
\begin{aligned}
R^* &= R^0 \cup R \cup R^2 \\
&= \{(\mathsf{a},\mathsf{a}), (\mathsf{a},\mathsf{b}), (\mathsf{a},\mathsf{c}), (\mathsf{b},\mathsf{b}), (\mathsf{b},\mathsf{c}), (\mathsf{c},\mathsf{b}), (\mathsf{c},\mathsf{c})\}
\end{aligned}
$$


R^0
a
b
c


R
a
b
c


R^2
a
b
c


R^*
a
b
c

例 2.4: N 上の二項関係 $nRm \Leftrightarrow n = m + 1$

$$
\begin{aligned}
nR^0m &\Leftrightarrow n = m \\
nR^1m &\Leftrightarrow n = m + 1 \\
nR^2m &\Leftrightarrow n = m + 2 \\
nR^km &\Leftrightarrow n = m + k \\
nR^*m &\Leftrightarrow \exists k \geq 0,\ nR^km \Leftrightarrow n \geq m \\
nR^+m &\Leftrightarrow \exists k > 0,\ nR^km \Leftrightarrow n > m
\end{aligned}
$$

同値関係: Equivalence relations

- $R : A \to A$
- 以下の三つの性質を全て満たす関係: 同値関係
  - 反射律 (reflexive): $\forall a \in A$ に対して aRa
  - 対称律 (symmetric): $\forall a, b \in A$ に対して $aRb \Leftrightarrow bRa$
  - 推移律 (transitive): $\forall a, b, c \in A$ に対して $aRb \wedge bRc \Leftrightarrow aRc$

例 3.1: m を法とする合同

- $x, y \in N \cup \{0\}$ を $m \in N$ で除した余りが等しい

$$R = \{(x, y) \mid x \equiv y \pmod{m}\} \tag{3.1}$$

- 反射律: xRx は自明
- 対称律: $xRy \Rightarrow yRx$ も自明
- 推移律: $xRy \wedge yRz \Rightarrow xRz$
  - $k, \ell \in Z$ が存在し、$x - y = km$ かつ $y - z = \ell m$

$$x - z = (x - y) + (y - z) = (k + \ell)\, m \tag{3.2}$$

同値類: equivalence classes

- 集合 A 上の同値関係 R によって、集合 A を分ける
- $a \in A$ に対して
$$[a]_R = \{b \in A \mid aRb\} \tag{3.3}$$
    - R によって定まる a と同値なものの全体
    - a を代表元という
- 重複は無い

同値類の性質

- 集合 A 上の同値関係 R
- $\forall a, b, c \in A$
- $a \in [a]_R$
- $b, c \in [a]_R \Rightarrow bRc$
- $aRb \Leftrightarrow [a]_R = [b]_R$
- $[a]_R = [b]_R$ と $[a]_R \cap [b]_R = \emptyset$ のいずれか一方だけが必ず成り立つ
- $\bigcup_{a \in A} [a]_R = A$

m を法とする剰余類

- $R = \{(x, y) \mid x \equiv y \pmod{m}\}$
- $m = 3$ の場合 $(k \in N \cup \{0\})$

$$
\begin{aligned}
[0] &= \{n \mid n = 3k\} \\
[1] &= \{n \mid n = 3k + 1\} \\
[2] &= \{n \mid n = 3k + 2\}
\end{aligned}
$$

有限体: Finite fields

- 素数 p で除した余りからなる集合

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \cdots, p-1\} \tag{3.4}$$

- 加法について $\mathrm{mod} p$ で閉じており、0 を単位元として、全ての要素に逆元がある。
- 乗法について $\mathrm{mod} p$ で閉じており、1 を単位元として、0 以外の要素の逆元がある。
- $\mathrm{mod} p$ の交換則、結合則、分配則が成り立つ。
- Fermat の小定理: p と互いに素な $a \in \mathbb{F}_p$ に対して

$$a^{p-1} \equiv 1 \bmod p$$

  - 暗号理論の基礎

Fermat の小定理: 証明

- $a^p \equiv a \bmod p$ を証明
  - $1^p \equiv 1 \bmod p$ は明らか
  - a に対して $a^p \equiv a \bmod p$ を仮定

$$
\begin{aligned}
(a+1)^p &\equiv \sum_{k=0}^{p} \binom{p}{k} a^k 1^{p-k} \bmod P \\
&\equiv \left(a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k 1^{p-k} + 1^p \right) \bmod p \\
&\equiv (a^p + 1) \bmod p \\
&\equiv (a+1) \bmod p
\end{aligned} \tag{3.5}
$$

- $\binom{p}{k} \equiv 0 \bmod p$ for $k \in [1, p-1]$

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \tag{3.6}$$

分子は p の倍数、一方分母には因子 p を含まない

- $a^{p-1} \equiv 1 \bmod p$

$$\begin{aligned} a^p - a &\equiv 0 \bmod p \\ &\equiv a\left(a^{p-1} - 1\right) \bmod p \quad (3.7) \\ a^{p-1} &\equiv 1 \bmod p \quad (3.8) \end{aligned}$$

例 3.2: $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$

$$1 + 4 \equiv 0 \bmod 5 \qquad 2 + 3 \equiv 0 \bmod 5$$
$$2 \times 3 \equiv 1 \bmod 5 \qquad 4 \times 4 \equiv 1 \bmod 5$$

$$\begin{array}{llll}
a = 2 & a^2 \equiv 4 \bmod 5 & a^3 \equiv 3 \bmod 5 & a^4 \equiv 1 \bmod 5 \\
a = 3 & a^2 \equiv 4 \bmod 5 & a^3 \equiv 2 \bmod 5 & a^4 \equiv 1 \bmod 5 \\
a = 4 & a^2 \equiv 1 \bmod 5 & &
\end{array}$$

順序: Order

- 反対称律: anti-symmetric
  - $\forall a, b \in A$ に対して $aRb \wedge bRa \Rightarrow a = b$
- 関係が反射律、推移律、反対称律を満たすとき、半順序 (partial-order) または順序という
  - 大小関係 $\leq$ は半順序
  - 半順序が定義された集合を半順序集合という

全順序: total order

- 全順序: 半順序に加えて、任意の二つの要素について比較可能であるとき
- 全順序集合: 全順序を定義された集合

例 4.1:

- 自然数、整数、有理数、実数に対する大小関係 $\leq$ は全順序
  - 任意の要素を大小関係 $\leq$ で比較可能
- 集合の包含関係 $\subseteq$ は半順序
  - 任意の集合の間に包含関係は成り立たない

例 4.2:

$n, m \in N$ 対する関係「$n \mid m$: n は m を割り切る」は半順序

- 反射律: $n \mid n$ は自明
- 推移律: $n \mid m \wedge m \mid \ell \Rightarrow n \mid \ell$

$$
\begin{aligned}
&(n \mid m \Rightarrow m = an,\ \ m \mid \ell \Rightarrow \ell = bm) \\
&\Rightarrow \ell = bm = abn
\end{aligned} \tag{4.1}
$$

- 反対称律

$$
\begin{aligned}
n \mid m \wedge m \mid n \Rightarrow m = an \wedge n = bm \\
\Rightarrow a = b = 1 \Rightarrow n = m
\end{aligned} \tag{4.2}
$$

- n と m が互いに素の場合には、関係が成り立たないため、全順序ではない