問題の解

第 1 章 の 解

問 1.1

(1) **象** $\subseteq$ **鼻が長い**，または **象の鼻** $\subseteq$ **長いもの**.

(2) **徳川家光** $\in$ **徳川家康の孫**

(3) $2x + 10 = 2(x + 5)$

(4) $4 \in$ **2 で割り切れる** または $4/2 \in$ **整数**.

問 1.2

(1) $\{2, 3, 5, 7, 11, 13, 17, 19\}$

(2) $\{2\text{ 月}, 4\text{ 月}, 6\text{ 月}, 9\text{ 月}, 11\text{ 月 }\}$

(3) { ロバ，犬，猫，鶏 }

(4) $\{1, 3, 5, \cdots\}$

問 1.3

(1) $\{x \mid x$ は 20 以下の素数 $\}$

(2) $\{x \mid x$ は曜日の名前 $\}$

問 1.4

(1) $1^2 - 4\cdot 1 + 2 = -1 < 0, 2^2 - 4\cdot 2 + 2 = -2 < 0, 3^2 - 4\cdot 3 + 2 = -1 < 0$ より $\{1, 2, 3\} \subseteq \{x \in \mathbb{R} \mid x^2 - 4x + 2 < 0\}$.

(2) $x^2 - 4x + 2 < 0$ を解くと $2 - \sqrt{2} < x < 2 + \sqrt{2}$. ここで，$1 < \sqrt{2} < 2$ だから，$0 < 2 - \sqrt{2} < 1$ かつ $3 < 2 + \sqrt{2} < 4$. よって $\{x \in \mathbb{N} \mid x^2 - 4x + 2 < 0\} \subseteq \{1, 2, 3\}$.

(3) $3 < 3.1 < 2 + \sqrt{2}$ より，$3.1 \in \{x \in \mathbb{R} \mid x^2 - 4x + 2 < 0\} - \{x \in \mathbb{R} \mid x \leq 3\}$.

2

問 1.5

(1) $2x^2 - 3x + 1 = (2x - 1)(x - 1) = 0$ より，$\{1, \frac{1}{2}\} = \{x \in \mathbb{R} \mid 2x^2 - 3x + 1 = 0\}$．よって $\{1\} \subset \{x \in \mathbb{R} \mid 2x^2 - 3x + 1 = 0\}$.

(2) (1) より $\{1\} = \{x \in \mathbb{N} \mid 2x^2 - 3x + 1 = 0\}$.

問 1.6 例えば $\{x \mid x = 0 \text{ かつ } x = 1\}$.

問 1.7 $\{x \mid x \text{ は } 2 \text{ で割り切れる奇数 }\} = \emptyset$ だから，$\{x \mid x \text{ は } 2 \text{ で割り切れる奇数 }\} \subseteq \{x \mid x \text{ は } 6 \text{ で割り切れる自然数 }\}$．よって「2 で割り切れる奇数は 6 で割り切れる」は正しい.

問 1.8 一つはバッグとコートの価格の和より大きな金額を所持している場合で，バッグとコートを同時に買うことができる．もう一つはバッグとコートの高いほうの価格より大きな金額を所持している場合で，バッグを買うこともできるし，コートを買うこともできる.

問 1.9 $\exists x P_A(x) \land \neg P_B(x)$

問 1.10

(1) 任意の自然数は 0 以上である：$\forall x \in \mathbb{N} x \geq 0$

(2) 6 の倍数は 2 の倍数である：$\forall x \in \mathbb{N}$ (x は 6 の倍数 $\rightarrow$ x は 2 の倍数)

(3) 2 で割りきれる奇数は 6 で割りきれる：$\forall x \in \mathbb{N}$ (x は 2 で割り切れる $\land$ x は奇数 $\rightarrow$ x は 6 で割り切れる)

(4) 8 以上 10 以下の素数は存在しない：$\neg(\exists x \in \{8, 9, 10\} x$ は素数)

問 1.11

(1) $\neg(\forall x$ x は玉 $\rightarrow$ x は赤い).

(2) $\forall x$ (x は玉 $\rightarrow \neg(x$ は赤い)).

問 1.12

(1) 例えば,
レポートと試験に合格したものに単位が与えられます.
セットで選べるのはコーヒーと紅茶です.

(2) 前提（仮定）が偽なので結論が真でも偽でも正しい.

(3) 「晴れたら遠足に行く」という約束は雨が降ったときのことを何も約束していない．したがってそこから「雨が降ったから行かない」が数学的に導かれるわけではなく，正しくない．

問 1.13

(1) 以下の真理値表を比べれば $P \to Q$ と $\neg P \vee Q$ は一致するので，これらは同値である．

P, Q	$P \to Q$	$\neg P$	$\neg P \vee Q$
真　真	真	偽	真
真　偽	偽	偽	偽
偽　真	真	真	真
偽　偽	真	真	真

(2) $\neg(\forall x P(x))$ が真になることは，$\forall x P(x)$ が偽になることと同値であり，それは $P(x)$ が偽になる x が存在することと同値である．よって，$\exists x \neg P(x)$ が真になることと同値である．

(3) 上の問と同様.

(4) (2) より，$\neg(\forall x(P(x) \to Q(x)))$ と $\exists x \neg(P(x) \to Q(x))$ は同値である．このことと，ある a が存在して $\neg(P(a) \to Q(a))$ となることは同値である．ここで，$\neg(P(a) \to Q(a))$ と $P(a) \wedge \neg Q(a)$ とは表 1.3 から同値だから，ある a が存在して $\neg(P(a) \to Q(a))$ となること，ある a が存在して $P(a) \wedge \neg Q(a)$ となることとは同値である．したがって，$\exists x \neg(P(x) \to Q(x))$ と $\exists x(P(x) \wedge \neg Q(x))$ とは同値である．

問 1.14 それぞれ，$A \cap B$ は $P_A(x) \wedge P_B(x)$, $A \cup B$ は $P_A(x) \vee P_B(x)$, $\overline{A}$ は $\neg P_A(x)$ で内包的に記述される．

問 1.15 $A \subseteq B \Leftrightarrow (\forall x \in A\ x \in B) \Leftrightarrow (\forall x \in A\ x \notin \overline{B}) \Leftrightarrow A \cap \overline{B} = \emptyset$.

問 1.16 解答省略

問 1.17 $2^{\{a,b\}} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

問 1.18 $|A| = n$ のとき，$|2^A| = 2^n$．$2^\emptyset = \{\emptyset\}$ より，$|2^\emptyset| = 1 = 2^0$ だから，$n = 0$ のときも正しい．

問 1.19 $\bigcup \mathcal{A}$ は $\exists i \in I\ P(i,x)$, $\bigcap \mathcal{A}$ は $\forall i \in I\ P(i,x)$ と記述される.

問 1.20

(1) $A_6 \cup A_9 = \{n > 0 \mid n \mod 6 = 0 \vee n \mod 9 = 0\}$. 実は, $A_6 \cup A_9 = \{n \geq 6 \mid n \mod 3 = 0\}$ が成り立つ.

(2) $A_3 \supseteq A_6 \supseteq A_9 \ldots$ なので $\bigcup_{k \in A_3} A_k = A_3$.

問 1.21

(1) $x \in \overline{\bigcup \mathcal{A}} \Leftrightarrow \neg(\exists A \in \mathcal{A}\ x \in A) \Leftrightarrow \forall A \in \mathcal{A}\ x \notin A \Leftrightarrow x \in \bigcap\{\overline{A} \mid A \in \mathcal{A}\}$

(2) $x \in \overline{\bigcap \mathcal{A}} \Leftrightarrow \neg(\forall A \in \mathcal{A}\ x \in A) \Leftrightarrow \exists A \in \mathcal{A}\ x \notin A \Leftrightarrow x \in \bigcup\{\overline{A} \mid A \in \mathcal{A}\}$

問 1.22

(1) $\{a,b,c\} \times \{0,1\} = \{(a,0),(a,1),(b,0),(b,1),(c,0),(c,1)\}$.

(2) $\{0,1\}^3 = \{(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)\}$.

(3) $\{a,b,c\} \times \{b\} \times \{a,c\} = \{(a,b,a),(a,b,c),(b,b,a),(b,b,c),(c,b,a),(c,b,c)\}$

(4) $|A \times B| = |A| \times |B| = mn$.

問 1.23

鉄道路線		
路線名	駅	駅
東海道本線	東京	神戸
中央本線	神田	名古屋
北陸本線	米原	直江津
東北本線	東京	青森

問 1.24 $\{(0,0),(1,1),(2,4),(3,9),\ldots\} = \{(n,n^2) \mid n \in \mathbb{N}\}$.

問 1.25

(1) $\psi_{学生}(01, 田中和子, 3, 東京都) = 真$

(2) $\psi_{学生}(02, 山口隆, 3, 東京都) = 偽$

問 1.26

(1) $x = y$

(2) $x^2 + y^2 + z^2 \leq 4$

問 1.27

愛する	
人	人
太郎	花子
花子	太郎
和夫	花子
花子	和夫
良子	和夫

愛される	
人	人
花子	太郎
太郎	花子
花子	和夫
和夫	花子
和夫	良子

相思相愛	
人	人
花子	太郎
太郎	花子
花子	和夫
和夫	花子

片思い	
人	人
良子	和夫

三角関係		
人	人	人
太郎	花子	和夫
和夫	花子	太郎
良子	和夫	花子

問 1.28 三角関係の表から第 2 列を削除する.

問 1.29

(1) $\pi(\sigma(学生, x_4 = 神奈川県), 1, 2)$

(2) $\pi(\sigma(成績 \times 学生, (x_1 = x_4) \wedge (x_3 \geq 80)), 2, 5)$

(3) $\pi(\sigma(成績 \times 成績, (x_1 = x_4) \wedge (x_2 = 数学) \wedge (x_5 = 国語) \wedge (x_3 < x_6)), 1)$

問 1.30

(1) 原点を中心とする半径 1 の円を Z 軸の正負の方向に垂直に移動させてできる円柱

(2) xy-平面内で，原点を中心とする単位円とそれへの点 $(2, 0)$ からの接線からなる図形の境界および内部.

問 1.31

(1) SELECT 学籍番号 FROM 成績 WHERE 科目=”数学”

6

(2) SELECT 学生. 学籍番号, 学生. 氏名 FROM 学生, 成績 WHERE 学生. 学籍番号=成績. 学籍番号 AND 成績. 点数 $\leq$50

(3) SELECT 成績. 学籍番号 FROM 成績, 成績$_1$ WHERE 成績. 学籍番号=成績$_1$. 学籍番号 AND 成績. 科目=”数学” AND 成績$_1$. 科目=”国語” AND 成績. 点数 $<$ 成績$_1$. 点数

問 1.32

(1) $\forall y \exists x \exists z\ \psi_{\text{成績}}(x, y, z)$ ：すべての科目に対して履修者（学籍番号とその点数）が存在する．

(2) $\exists x \forall y \forall z\ (\psi_{\text{成績}}(x, y, z) \to z \geq 80)$ ：ある学籍番号が存在して，すべての科目と点数について，成績がついていれば 80 点以上である．$\Leftrightarrow$ すべての科目で 80 点以上をとった学生がいる．

問 1.33

(1) A に最大値が存在する：$\exists x \in A\ \forall y \in A\ y \leq x$

(2) A に最小値が存在しない：$\neg(\exists x \in A\ \forall y \in A\ x \leq y) = \forall x \in A\ \exists y \in A\ x > y$

問 1.34

(1) ペット$^{-1}$:= $\{(\text{ポチ}, \text{太郎}), (\text{タマ}, \text{花子}), (\text{チビ}, \text{和夫})\} \subseteq$ 動物 $\times$ 人

(2) xy-平面上の平面図形の逆関係は x と y を入れ替えて得られるから，直線 $y = x$ に関して対称に移せばよい．

問 1.35

(1) $[<] \circ [<] = \{(x, y) \in \mathbb{N}^2 \mid x + 2 \leq y\}$

(2) $[\leq] \circ [\leq] = [\leq]$

問 1.36 $R \circ S(A) = \{c \mid \exists a \in A\ \exists b \in B\ (a, b) \in R \wedge (b, c) \in S\} = \{c \mid \exists b \in R(a)\ (b, c) \in S\} = S(R(A))$.

問 1.37 $\psi_{R(X)}(y) = \exists x \in X\ R(x, y)$.

問 1.38

(1) $[<](\mathbb{N}) = \mathbb{N} - \{0\}$, $[<]^{-1}(\mathbb{N}) = [>](\mathbb{N}) = \mathbb{N}$

(2) $R(\mathbb{R}) = R^{-1}(\mathbb{R}) = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$

問 1.39 「愛する」は部分写像であり，写像でもある.「愛される」は花子が太郎と和夫の二人から「愛される」ので，部分写像でもない.

問 1.40

(1) $f_1(\mathbb{R}) = \{x \in \mathbb{R} \mid x \geq 0\}$, $f_1^{-1}(\mathbb{R}) = \mathbb{R}$

(2) $f_2(\mathbb{R}) = f_2^{-1}(\mathbb{R}) = \{x \in \mathbb{R} \mid x \geq 0\}$

(3) $f_3(\mathbb{R}) = \mathbb{R}$, $f_3^{-1}(\mathbb{R}) = \mathbb{R} - \{n + \pi/2 \mid n \in \mathbb{Z}\}$

問 1.41 y 軸に平行な任意の直線 $x = c$ との交点が常に 1 個であること.

問 1.42 (1) $f(x, y) = 0$ のグラフを x 軸方向に a, y 軸方向に b 平行移動したグラフの方程式は $f(x - a, y - b) = 0$.

(2) $f(x, y) = 0$ のグラフを c 倍 $(c > 0)$ に拡大したグラフの方程式は $f(x/c, y/c) = 0$.

(3) xy-平面上の 2 次関数 $y = ax^2 + bx + c$ のグラフは頂点が原点 $(0, 0)$ にくるように平行移動すれば $y = ax^2$ のグラフになり，これを $1/a$ 倍に拡張すれば $y = x^2$ のグラフになる.

問 1.43 $R(\{$ 太郎，和夫 $\}) = \{$ 花子，良子 $\}$, $R(\{$ 花子，良子 $\}) = \{$ 太郎，和夫 $\}$

問 1.44 $\forall X \subseteq A\ F(X) = \bigcup_{x \in X} F(x)$. これが必要条件であることは，$A \times B$ 上の関係から写像 $(2^A \to 2^B)$ を定義する仕方から明らか. 十分条件であることは，関係を $R := \{(x, y) \mid y \in F(x)\}$ と定義すれば，R から導かれる写像と F とが一致することから，成り立つ.

問 1.45 xy-平面上のグラフが,

- 上への部分写像：x 軸と平行な直線 $y = c$ との交点が常に 1 個以上であること
- 1 対 1 部分写像：x 軸と平行な直線 $y = c$ との交点が常に 1 個以下であること
- 1 対 1 かつ上への写像：x 軸に平行な直線および y 軸に平行な直線との交点がすべて 1 個であること

問 1.46　A が有限集合のとき，写像 $F \in A^A$ が 1 対 1$\Leftrightarrow |F(A)| = |A| \Leftrightarrow$ 写像 $F \in A^A$ が上への写像 $\Leftrightarrow F$ は 1 対 1 かつ上への写像.

問 1.47　F が 1 対 1 部分写像で $a, b \notin F^{-1}(B)$ のとき，ある $c \in C$ に対する値だけが $G(c) = a, H(c) = b$ と異なり他の要素についてはすべて値が等しい写像 G, H を考えれば，$G \neq H$ かつ $G \circ F = H \circ F$，が成り立つ.

問 1.48　$F \in B^A$ は各要素 $a \in A$ に対し $F(a) \in B$ となる $|B|$ 通りの値を定めることによって一意に定義されるから，全部で $|B|^{|A|}$ 通りある．また部分写像 $F : A \to B$ の個数は，各要素 $a \in A$ に対し B の値または未定義を定めることによって一意に定義されるので，全部で $(|B| + 1)^{|A|}$ 個である.

問 1.49　(1) $ab \cdot ba = abba$, (2) $(ab)^3 = ababab$, (3) $\varepsilon b \varepsilon a = ba$

問 1.50　$(abc)^R = cba$, abc の接頭列は ε, a, ab, abc，接尾列は ε, c, bc, abc，部分列は $\varepsilon, a, b, c, ab, bc, abc$.

問 1.51

(1)　$\{a, ab\}\{a, ba, \varepsilon\} = \{aa, aba, abba, a, ab\}$，$\{a, ba, \varepsilon\}\{a, ab\} = \{aa, baa, a, aab, baab, ab\}$ なので，$\{a, ab\}\{a, ba, \varepsilon\} \neq \{a, ba, \varepsilon\}\{a, ab\}$.

(2)　$B = A^R \cup \{\varepsilon\}$ より，$B^* = (A^R)^*$

問 1.52

(1)　例えば，$\{a, ab\}(\{ba\} \cap \{a\}) = \emptyset \subset \{a, ab\}\{ba\} \cap \{a, ab\}\{a\} = \{aba\}$

(2)　$(AB)^R = \{(xy)^R \mid x \in A \wedge y \in B\} = \{y^R x^R \mid x \in A \wedge y \in B\} = \{y^R \mid y \in B\}\{x^R \mid x \in A\} = B^R A^R$.

(3)　$A \cup B \subseteq A^* \cup B^* \subseteq A^* B^* \subseteq (A \cup B)^*$ より，$(A \cup B)^* \subseteq (A^* B^*)^* \subseteq (A^* \cup B^*)^* \subseteq (A \cup B)^*$.

(4)　$A(A^* B) \cup B = (AA^* \cup \{\varepsilon\})B = A^* B$．同様に，$(BA^*)A \cup B = B(A^* A \cup \{\varepsilon\}) = BA^*$.

問 1.53

(1)　$(\{a\} \cup \{b\})^* \{aba\} (\{a\} \cup \{b\})^*$ に等しいから正規言語である.

(2)　$(\{a\} \cup \{b\})(\{a\} \cup \{b\})^* \{aba\} (\{a\} \cup \{b\})^* \cup (\{a\} \cup \{b\})^* \{aba\} (\{a\} \cup \{b\})(\{a\} \cup \{b\})^*$ に等しいから正規言語である.

問 1.54

(1) $\alpha+ = \alpha\alpha*$

(2) $\alpha? = (|\alpha)$

(3) $\alpha\{m,n\} = \underbrace{\alpha\ldots\alpha}_{m\text{ 個}}|\underbrace{\alpha\ldots\alpha}_{m+1\text{ 個}}|\ldots|\underbrace{\alpha\ldots\alpha}_{n\text{ 個}}$

問 1.55

(1) $0|[1-9][0-9]\{0.2\}|[12][0-9]\{3\}$

(2) $[01]*1$

(3) $10*$

(4) a[a-z]*b

(5) [a-z]+ing

第 2 章 の 解

問 2.1

(1) **基礎** $\sum_{i=0}^{0} i(i+1) = \frac{0(0+1)(0+2)}{3} = 0$ より，$n = 0$ のとき成り立つ.

帰納ステップ $n = k$ のとき成り立つと仮定すると，$\sum_{i=0}^{k+1} i(i+1) = \sum_{i=0}^{k} i(i+1) + (k+1)(k+2) = \frac{k(k+1)(k+2)}{3} + (k+1)(k+2) = \frac{(k+1)(k+2)(k+3)}{3}$ より $n = k+1$ のときも成り立つ.

結論 よって，すべての n に対して与式は成り立つ.

(2) $\sum_{i=0}^{n} i(i+1)\cdots(i+k) = \frac{n(n+1)\cdots(n+k+1)}{(k+2)}$ を数学的帰納法により証明する.

基礎 $\sum_{i=0}^{0} i(i+1)\cdots(i+k) = \frac{0(0+1)\cdots(0+k+1)}{(0+2)} = 0$ より，$n = 0$ のとき成り立つ.

帰納ステップ $n = m$ のとき成り立つと仮定すると，$\sum_{i=0}^{m+1} i(i+1)\cdots(i+$

$k) = \sum_{i=0}^{m} i(i+1)\cdots(i+k) + (m+1)(m+2)\cdots(m+1+k) = \frac{m(m+1)\cdots(m+k+1)}{(k+2)} + (m+1)(m+2)\cdots(m+1+k) = \frac{(m+1)(m+2)\cdots(m+k+2)}{(k+2)}$ より，$n = m+1$ のときも成り立つ．

結論　よって，すべての n に対して与式は成り立つ．

問 2.2

(1)　(a)　$0, 1, 3, 7, 15 \ldots$

(b)　$1, 4, 12, 13, 36, \ldots$

(2)　$f_0 := 0,\ f_1 := 1,\ f_{n+2} := f_{n+1} + f_n\ (n \geq 0)$

問 2.3

基礎　1 は奇数である．

帰納ステップ　k が奇数ならば，$k+2$ も奇数である．

問 2.4

(1)　$\frac{1}{1-2X}$.

(2)　$\frac{1}{(1-X)^2} = 1 + 2X + 3X^2 + \ldots$ より，$2X + 4X^2 + 6X^3 + \cdots = \frac{2X}{(1-X)^2}$.

問 2.5　$A(X) = \sum_{n=0}^{\infty} a_n X^n, B(X) = \sum_{n=0}^{\infty} b_n X^n$ より，

(1)　$cA(X) + dB(X) = \sum_{n=0}^{\infty} ca_n X^n + \sum_{n=0}^{\infty} db_n X^n = \sum_{n=0}^{\infty} (ca_n + db_n) X^n$

(2)　$A(X)B(X) = \left(\sum_{n=0}^{\infty} a_n X^n\right)\left(\sum_{n=0}^{\infty} b_n X^n\right) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} a_{n-k} b_k\right) X^n$

問 2.6　(1)　$a_0 = 5, a_n = 2a_{n-1} + 3\ (n \geq 1)$ より，

$$A(X) - 2XA(X) = 5 + \sum_{n=1}^{\infty} 3X^n = \frac{3}{1-X} + 2$$

よって，

$$A(X) = \frac{3}{(1-2X)(1-X)} + \frac{2}{1-2X} = \frac{8}{1-2X} - \frac{3}{1-X}$$

したがって,

$$a_n = 8 \times 2^n - 3 = 2^{n+3} - 3$$

(2) $a_0 = 0, a_n = 3a_{n-1} + 2^n$ $(n \geq 1)$ より,

$$A(X) - 3XA(X) = a_0 + \sum_{n=1}^{\infty} 2^n X^n = \frac{2X}{1-2X}$$

よって,

$$A(X) = \frac{2X}{(1-2X)(1-3X)} = 2\left(\frac{1}{1-3X} - \frac{1}{1-3X}\right)$$

したがって,

$$a_n = 2(3^n - 2^n)$$

(3) $a_0 = 0, a_1 = 1, a_n = a_{n-1} + a_{n-2}$ $(n \geq 2)$ だから, $1 - X - X^2 = 0$ の解を $1/\alpha, 1/\beta$ $(\alpha < \beta)$ と置くと,

$$A(X) - XA(X) - X^2A(X) = (1-\alpha X)(1-\beta X)A(X) =$$

$$a_0 + (a_1 - a_0)X + \sum_{n=2}^{\infty}(a_n - a_{n-1} - a_{n-2})X^n = X$$

よって,

$$A(X) = \frac{X}{(1-\alpha X)(1-\beta X)} = \frac{1}{\beta - \alpha}\left(\frac{1}{1-\beta X} - \frac{1}{1-\alpha X}\right)$$

したがって,

$$a_n = \frac{\beta^n - \alpha^n}{\beta - \alpha} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

問 2.7

Hanoi(4,A,B,C)：円盤 1〜4 を A から C に移す.

Hanoi(3,A,C,B)：円盤 1〜3 を A から B に移す.

Hanoi(2,A,B,C)：円盤 1〜2 を A から C に移す

Hanoi(1,A,C,B)：円盤 1〜1 を A から B に移す

円盤 1 を A から B に移す

円盤 2 を A から C に移す

Hanoi(1,B,A,C)：円盤 1〜1 を B から C に移す

円盤 1 を B から C に移す

円盤 3 を A から B に移す

Hanoi(2,C,A,B)：円盤 1〜2 を C から B に移す

Hanoi(1,C,B,A,)：円盤 1〜1 を C から A に移す

円盤 1 を C から A に移す

円盤 2 を C から B に移す

Hanoi(1,A,C,B)：円盤 1〜1 を A から B に移す

円盤 1 を A から B に移す

円盤 4 を A から C に移す

Hanoi(3,B,A,C)：円盤 1〜3 を B から C に移す.

Hanoi(2,B,C,A)：円盤 1〜2 を B から A に移す

Hanoi(1,B,A,C)：円盤 1〜1 を B から C に移す

円盤 1 を B から C に移す

円盤 2 を B から A に移す

Hanoi(1,C,B,A)：円盤 1〜1 を C から A に移す

円盤 1 を C から A に移す

円盤 3 を B から C に移す

Hanoi(2,A,B,C)：円盤 1〜2 を A から C に移す

Hanoi(1,A,C,B,)：円盤 1〜1 を A から B に移す

円盤 1 を A から B に移す

円盤 2 を A から C に移す

Hanoi(1,B,A,C)：円盤 1〜1 を B から C に移す

円盤 1 を B から C に移す

問 2.8　数列 $t(n)$ の母関数を $T(X)$ とおくと

$$(1-2X)T(X) = \sum_{n=1}^{\infty} X^n = \frac{X}{1-X}$$

$$T(X) = \frac{X}{(1-2X)(1-X)} = \frac{1}{1-2X} - \frac{1}{1-X}$$

したがって，$t(n) = 2^n - 1$ である．

問 2.9

(1)　$i_w(1) = 0, i_w(n+1) = i_w(n) + n$ を解いて $i_w(n) = n(n-1)/2$.

(2)　$i_a(1) = 0, i_a(n+1) = i_a(n) + n/2$ を解いて $i_a(n) = n(n-1)/4$ を得る．ここで，$i_a(n)$ の値は整数とは限らないことに注意.

(3)　$m(n)$ は $m(0) = 0, m(n+1) = m(\lceil (n+1)/2 \rceil) + m(\lfloor (n+1)/2 \rfloor) + n$ で帰納的に定義される．ここで，$M(n)$ は $M(1) = m(1), M(2) = 2 > m(1) = 1, M(n+1) = 2M((n+1)/2) + n + 1$ を満たすことから，$M(n) \geq m(n)$ が帰納法で証明できる．

問 2.10

(1)　GCD(25,9)=GCD(9,7)=GCD(7,2)=GCD(2,1)=GCD(1,0)=1

(2)　GCD(21,34)=GCD(34,21)=GCD(21,13)=GCD(13,8)=GCD(8,5)=GCD(5,3)=GCD(3,2)=GCD(2,1)=GCD(1,0)=1

問 2.11　以下の表より，$i = -8, j = 13$.

m	n	i	j
1	0	1	0
2	1	0	1
3	2	1	−1
5	3	−1	2
8	5	2	−3
13	8	−3	5
21	13	5	−8
34	21	−8	13

問 2.12 $\mathrm{GCD}(a_n, a_{n+1})$ $=\mathrm{GCD}(a_{n+1}, a_n)$ $=\mathrm{GCD}(a_n, a_{n-1})$ $= \ldots =$ $\mathrm{GCD}(a_3, a_2) =\mathrm{GCD}(1,0)=1$ であるから，n 回.

問 2.13

基礎 $w \in B$ ならば $w \in A^*B$ (すなわち $B \subseteq AB^*$)

帰納ステップ $(w \in AB^*) \wedge (v \in A)$ ならば $vw \in A^*B$ (すなわち $A(A^*B) \subseteq A^*B$)

限定句 このようにして AB^* に含まれることを示せる列のみが AB^* に含まれる．(すなわち，$B \cup AX \subseteq X \Rightarrow A^*B \subseteq X$)

問 2.14 $A \cup (AB^*)B = A(\{\varepsilon\} \cup B^*B) = AB^*$ より，AB^* は言語 X に関する方程式 $X = A \cup XB$ の解である．さらに，AB^* の帰納的定義の限定句より，方程式 $X = A \cup XB$ の任意の解は AB^* を含む．よって最小解である．

問 2.15 n に関する数学的帰納法で，$X_n = \bigcup_{k=0}^{n-1} AB^k$ を示す.

基礎 $n = 0$ のとき，$\bigcup_{k=0}^{n-1} AB^k = \emptyset = X_0$ より成り立つ.

帰納ステップ n のとき成り立つと仮定すると $X_{n+1} = A \cup X_nB = A \cup (\bigcup_{k=0}^{n-1} AB^k)B = A \cup \bigcup_{k=1}^{n} AB^k = \bigcup_{k=0}^{n} AB^k$ より，$n+1$ のときも成り立つ.

したがって，$\lim_{n\to\infty} X_n = \bigcup_{n=0}^{\infty} X_n = AB^*$ である.

問 2.16

(1) $F(X) := aXa \cup bXb \cup \varepsilon$ より $F(\emptyset) = \{\varepsilon\}$，$F^2(\emptyset) = F(\{\varepsilon\}) = \{aa, bb, \varepsilon\}$，$F^3(\emptyset) = F(\{aa, bb, \varepsilon\}) = \{aaaa, baab, abba, bbbb, aa, bb, \varepsilon\}$ である.

(2) $L := \{ww^R \mid w \in \{a, b\}^*\}$ と置くと，$aLa \cup bLb \cup \varepsilon \subseteq L$ だから，$X \subseteq L$. 逆に $w \in L \Rightarrow w = \varepsilon \vee \exists v \in L\ (w = ava \vee w = bvb)$ だから，帰納法により，$L \quad \subseteq X$ が示せる.

(3) $X := aXbX \cup bXaX \cup \varepsilon$

問 2.17 ヒントより，X_0, X_1, X_2 を定義する文法は

$$\begin{cases} X_0 := X_0 0 \cup X_1 1 \cup \varepsilon \\ X_1 := X_2 0 \cup X_0 1 \\ X_2 := X_1 0 \cup X_2 1 \end{cases}$$

である．第 3 式より，$X_2 = X_1 01^*$ であるから，これを第 2 式に代入して，$X_1 := X_1 01^*0 \cup X_0 1$．したがって，$X_1 = X_0 1(01^*0)^*$．これを第 1 式に代入して $X_0 := X_0 0 \cup X_0 1(01^*0)^*1 \cup \varepsilon$ を得るから，求める正規表現は $X_0 = (0 \cup 1(01^*0)^*1)^*$ である．

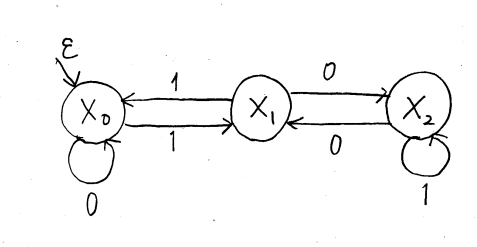

図 1　問の図式表現

問 2.18　$X_0 - \{\varepsilon\} = (0 \cup 1(01^*0)^*1)(0 \cup 1(01^*0)^*1)^*$ だから，求める正規表現は $0 \cup 1(01^*0)^*1(0 \cup 1(01^*0)^*1)^*$

問 2.19　問題を一般化して，$A_{i,j}$ $(i = 1, \ldots, k, j = 0, \ldots, k)$ が正規言語ならば，文法

$$X_i := A_{i,0} \cup \bigcup_{j:=1}^{k} A_{i,j} X_j \ (i = 1, \ldots, k)$$

が定義する言語は正規言語であることを，文法中に現れる変数の個数 k に関する帰納法で証明する．(左線形文法に対しても，変数位置の左右が入れ替わるだけで証明は同様である．)

基礎　変数が 1 個の場合，文法は $X_1 := A_{i,0} \cup A_{i,1} X_1$ だから，$X_1 = A_{i,1}^* A_{i,0}$．$A_{i,1}$, $A_{i,0}$ は正規言語なので，X_1 も正規言語である．

帰納ステップ　X_{k+1} に関する定義式

$$X_{k+1} := (A_{k+1,0} \cup \bigcup_{j:=1}^{k} A_{k+1,j}X_j) \cup A_{k+1,k+1}X_{k+1}$$

を解いて

$$X_{k+1} = A^*_{k+1,k+1}(A_{k+1,0} \cup \bigcup_{j:=1}^{k} A_{k+1,j}X_j)$$

を得る．これを代入して得られる文法

$$X_i := (A_{i,0} \cup A^*_{k+1,k+1}A_{k+1,0}) \cup \bigcup_{j:=1}^{k} (A_{i,j} \cup A^*_{k+1,k+1}A_{k+1,j})X_j$$

の解 X_i $(i = 1, \ldots, k)$ は，帰納法仮定により，正規言語であるから，X_{k+1} も正規言語である．

問 2.20　数式 $x+[2\times x+y]$ の定数は 2，変数は x, y，因子は $2, x, y, [2\times x+y]$，項は $x, 2 \times x, [2 \times x + y]$，式は $2 \times x + y, x + [2 \times x + y]$ である．

第 3 章 の 解

問 3.1　グラフ G_1 と G_2 は同形である．実際，$1 \leftrightarrow a$, $2 \leftrightarrow d$, $3 \leftrightarrow b$, $4 \leftrightarrow e$, $5 \leftrightarrow c$, $6 \leftrightarrow f$ という対応で，同じグラフになる．グラフ G_1 と G_3 は同形でない．実際，三角形（長さ 3 のサイクル）が G_3 には含まれているが，G_1 にはない．したがって，頂点間のどのような 1 対 1 対応を考えても，同じグラフになることはない．ただし，一般に同型性判定は難しい問題で，同じ長さのサイクルの有無等の条件だけでは，判定できないことが知られている．

問 3.2　グラフ G_2 はループ f_1 と多重辺 f_2, f_3 を持つ．G_1 は単純グラフで，G_2 は単純グラフでない．

問 3.3

(1)　各有向辺はその始点の $d_+(v)$ の値を 1 増やし，その終点の $d_-(v)$ の値を 1 増やすので $\sum_{v\in V}\ d_+(v) = \sum_{v\in V}\ d_-(v) = |E|$ が成り立つ．

(2)　グラフが有向グラフならば任意の頂点 v に対し $d(v) = d_+(v) + d_-(v)$ であるから (1) より明らか．無向グラフならば，各辺は始点と終点に対し $d(v)$ の値を 1 ずつ増やすので $\sum_{v \in V} d(v) = 2|E|$ である．

問 3.4　K_5 と $K_{3,3}$ は図 2.

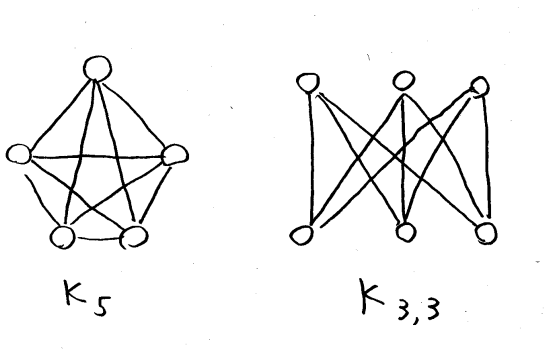

図 2

問 3.5　有向グラフ G_1 の長さ 2 の路は，$e_1e_2, e_2e_3, e_2e_4, e_3e_2, e_4e_5, e_5e_1$ であり，無向グラフ G_2 の長さ 2 の路は，$f_1f_1, f_1f_2, f_1f_3, f_2f_3, f_2f_4, f_3f_4$ とその辺の順番を逆にしたものである．

問 3.6　路は辺の列であるから，1.6 節で定義した真部分列に対応する路を真部分路と呼ぶことにしよう．頂点数を n のグラフ G において，

(1)　u から v への長さ 1 以上の路があれば，その路の真部分閉路を除いた路も u から v への路である．したがって，すべての真部分閉路を除けば u から v への長さ 1 以上の単純路が得られる．

(2)　路の長さが $n+1$ 以上であれば，その路は，$n+2$ 個の頂点を通過するので，真部分閉路を含む．したがって，単純路の長さは n 以下である．

問 3.7　$\sum_{v \in V} d(v) = 2|E|$ より次数の総和は偶数であるから，奇数個の奇頂点を持つことはない．

問 3.8　コラムで取り上げたケーニヒスベルグの橋では，奇頂点の個数が 4 個なので，すべての橋を 1 回ずつ通る路（オイラー路）は存在しない．

問 3.9　証明は無向グラフの場合と同様であるが，復習のため，証明を再構成しよう．

G を連結多重有向グラフであるとする．G が，オイラー路 π を持つとしよう．π は，始点と終点以外の通過頂点に対しては，その頂点に入る辺と出る辺を持つので，出次数と入次数が等しくなる．また，始点 u と終点 v に対しては，それらが異なれば $d_+(u) - d_-(u) = 1 \wedge d_+(u) - d_-(u) = -1$ であり，それらが一致すれば $d_+(u) - d_-(u) = d_+(u) - d_-(u) = 0$ である．オイラー路を構成する辺の集合は G の辺の集合に他ならないので，必要条件であることが示された．

十分条件であることを確かめるために，偶頂点および偶グラフの概念が有向多重グラフでもそのまま定義できることに注意しよう．このとき，偶頂点であることと，出次数と入次数が等しいこととは同値である．必要条件の証明から，偶グラフがオイラー路を持てばそれはオイラー閉路であり，偶グラフでない多重グラフがオイラー路を持てばそれは 出次数 $-$ 入次数 $= 1$ の頂点を始点とし，出次数 $-$ 入次数 $= 1$ の頂点を終点とすることがわかる．

さて，定理の条件を満たす有向多重グラフはオイラー路を持つことを G の辺の本数に関する帰納法で示す．

基礎　辺の本数が 0 のときは，G は連結なので，G の頂点数は 1 で，$G = (\{u\}, \emptyset)$ は長さ 0 のオイラー路を持つ．

帰納ステップ　辺の本数 n は 1 以上だとする．頂点 u として，多重グラフが偶グラフならば任意の頂点を，そうでなければ $d_+(u) - d_-(u) = 1$ の頂点を選ぶ．さらに，u につながる辺 $e{:}(u, v)$ を選び，G から辺 e を除いたグラフを G' とする．G' の奇頂点は，u の選び方から 0 または 2 個であり，G' が偶グラフでなければ，$d_+(v) - d_-(v) = 1$ である．

G' が連結であれば，帰納法の仮定により，G' は頂点 v から始まるオイラー路 π' を持ち，辺 e に路 π' をつなげた路 $e\pi'$ は G のオイラー路である．

G' が連結でないとき，u と v は非連結だから，u を含む連結多重グラフを G_1，v を含む連結多重グラフを G_2 とおく．u の選び方から G_1 は偶グラフである．よって帰納法の仮定より，G_1 は u を始点かつ終点とするオイラー

（閉）路 π_1 を持つ．一方，G_2 が偶グラフでなければ $d_+(v) - d_-(v) = 1$ だから，帰納法の仮定により G が偶グラフであるか否かに関わらず v を始点とする G_2 のオイラー路 π_2 がある．したがって，路 $\pi_1 e \pi_2$ は G のオイラー路である．以上より G' が連結であるか否かに関わらず G のオイラー路が構成できた．

問 3.10　図 3 の通り．

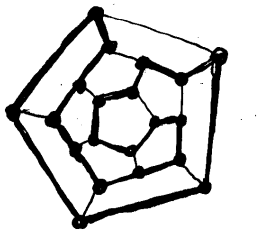

図 3

問 3.11　$K_4, K_{2,3}$ を平面グラフに描いた図 4 を示す．

問 3.12　ハミルトンのグラフの頂点数は 20，辺の数は 30，領域数は 12 である．

問 3.13

(1)　無向多重グラフ G はすべての頂点の次数が 2 以上であるとし，G の頂点 u を任意に選び u を訪問済みとする．u から出発して次々と未訪問の頂点への辺をたどって路を構成していくといくと，いつかこれ以上未訪問の頂点への辺を持たない頂点 v に達する．v の次数は 2 以上であるから，v は路に使われていない辺を持つ．この辺の v 以外の端点はすでに訪問済みで路の上にあるから，G は閉路を持つ．

(2)　閉路を持たない連結無向グラフでは，領域数 $= 1$ であるから 辺の数 $=$ 頂点数 $- 1$ である．

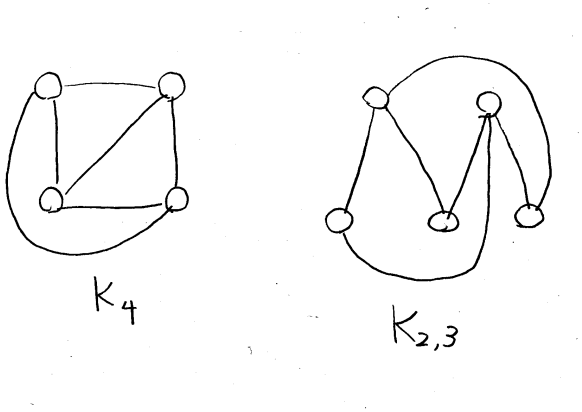

図 4

問 3.14 $A_{G_1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, A_{G_1}^2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ であり，

$A_{G_2} = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, A_{G_1}^2 = \begin{pmatrix} 5 & 2 & 2 \\ 2 & 5 & 0 \\ 2 & 0 & 1 \end{pmatrix}$ である．

問 3.15 A_G に関する定理の証明を，真理値の積と和を用いて以下のようになぞればよい．

基礎 $B_G^0 = E$（単位行列），$B_G^1 = B_G$ であるから，$n = 0, 1$ のときは明らか．

帰納ステップ

$$
\begin{aligned}
(B_G^{n+1})_{i,j} &= \bigcup_{k=1}^{m} (B_G^n)_{i,k} \wedge (B_G)_{k,j} \\
&= \sum_{k=1}^{m} (v_i\text{から } v_k\text{への長さ } n \text{ の路の有無}) \wedge (v_k\text{から } v_j\text{への辺の有無}) \\
&= (v_i\text{から } v_j\text{への長さ } n+1 \text{ の路の有無})
\end{aligned}
$$

なので数学的帰納法により成り立つ． □

問 3.16　定義より，単純路だけ考えれば十分であり，頂点数 m に対しその長さは m 以下である．したがって，$B^+ := \bigvee_{n=1}^{\infty} B_G^n = \bigvee_{n=1}^{m} B_G^n$ の対角成分に真が現れるかどうかをチェックすればよい．$(B^+)_{i,i} =$ 真 ならば頂点 v_i を含む閉路が存在する．

問 3.17　$W_G \cdot W_G^0 = W_G$ を示せば十分だろう．これは実際，$(W_G \cdot W_G^0)_{i,j} = \min_{k=1}^{m} \left((W_G)_{i.k} + (W_G^0)_{k,j}\right) = min((W_G)_{i,j}, \infty) = (W_G)_{i,j}$ より成り立つ．

問 3.18　路の重みはすべて 0 以上の実数であるから，ある路の重みは，そこから部分路を除いた路の重み以上である．したがって，v_i から v_j への路があるとき，その路に含まれる閉路を除いた路の重みは，もとの路の重み以下である．このことから，A_G あるいは B_G において行ったのと同様の議論が成り立つ．

問 3.19　$W_G = \begin{pmatrix} \infty & 1 & \infty & 6 \\ 1 & \infty & 2 & 4 \\ \infty & 2 & \infty & 1 \\ 6 & 4 & 1 & \infty \end{pmatrix}$，$W_G^2 = \begin{pmatrix} 2 & 10 & 3 & 5 \\ 10 & 2 & 5 & 3 \\ 3 & 5 & 2 & 6 \\ 5 & 3 & 6 & 2 \end{pmatrix}$，

$W_G^* = \begin{pmatrix} 0 & 1 & 3 & 4 \\ 1 & 0 & 2 & 3 \\ 3 & 2 & 0 & 1 \\ 4 & 3 & 1 & 0 \end{pmatrix}$

問 3.20　定常分布において状態が i である確率を X_i とおくと以下の連立方程式が成り立つ．

$$\begin{cases} X_1 = (1-p)X_1 + qX_2 \\ X_2 = pX_1 + (1-p-q)X_2 + qX_3 \\ X_3 = pX_2 + (1-q)X_3 \\ X_1 + X_2 + X_3 = 1 \end{cases}$$

第 1 式と第 3 式から $pX_1 = qX_2$,$pX_2 = qX_3$ が導かれるが，これは定常分布において，状態間の移動期待値が相殺されて 0 になることを意味している．このことを利用して方程式を解けば

$$X_1 = \frac{q^2}{q^2+qp+p^2},\ X_2 = \frac{qp}{q^2+qp+p^2},\ X_3 = \frac{p^2}{q^2+qp+p^2}$$

を得る．

問 3.21 $L_G = \begin{pmatrix} a & b & \emptyset \\ a & \emptyset & b \\ \emptyset & a & b \end{pmatrix}$, $L_G^2 = \begin{pmatrix} aa \cup ba & ab & bb \\ aa & ab \cup ba & bb \\ aa & ba & ab \cup bb \end{pmatrix}$

問 3.22 解答省略

問 3.23 図 5.

問 3.24 図 6.

問 3.25 図 7.

問 3.26 正規集合 A を受理する有限オートマトン $\mathcal{M} = (S, E, I, F)$ に対し，その初期状態 I と受理状態 F を交換し，矢印の向きを逆にした有限オートマトン $\mathcal{M}' = (S, \{(s, a, t) \mid (t, a, s) \in E\}, F, I)$ は明らかに A^R を受理するので，A^R も正規集合である．

問 3.27

(1)→(2) 木は連結で閉路をもたないから，どの 2 頂点の間にも単純路がただ一本存在する．

(2)→(3) 条件より連結な平面グラフで領域数 1 だから，オイラーの公式 頂点数 − 辺の数 = 2 − 領域数 より 頂点数 = 辺の数 + 1 である．

(3)→(4) G は連結なので，辺を新たに加えると必ず新たな閉路ができる．さらに，G が平面グラフならばオイラーの公式から領域数 1 で閉路を含まない．一方 G が平面グラフでなければ，G からいくつかの辺（のみ）を除いたグラフが領域数 2 以上の平面グラフになるはずなので，頂点数 − 辺の数 = 1 となることはない．

(4)→(1) 連結でない頂点を結ぶ辺を加えても閉路はできないから，G は連結である．

問 3.28 親の（自分以外の）子を兄弟という．

問 3.29 以下，木は閉路を持たない無向グラフのことであるとする．

基礎 頂点だけからなるグラフは木である．

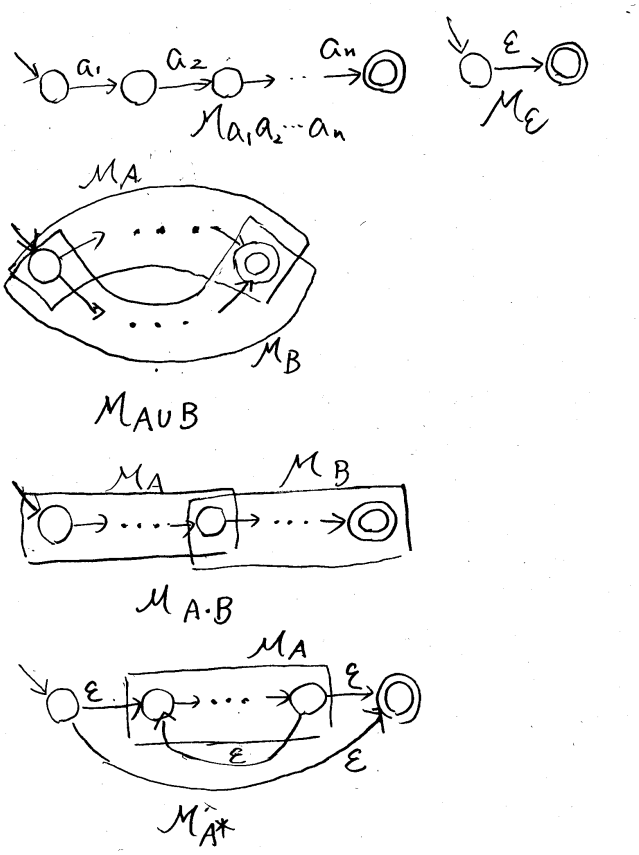

図 5　帰納的証明の有限オートマトン

帰納ステップ　G が木ならば，G の任意の頂点 u に対し新たな頂点 v と無向辺 $[u, v]$ を付け加えたグラフは木である．

問 3.30　$\varepsilon, 0, 00, 01, 1, 10, 100, 101, 2, 20, 21, 210, 22$
これはアドレスをいわゆる辞書式順序で並べていることになっている．

問 3.31　D は接頭性を持つので根 $\varepsilon \in D$ が存在する．また任意の頂点 $i_1 i_2 \ldots i_k$

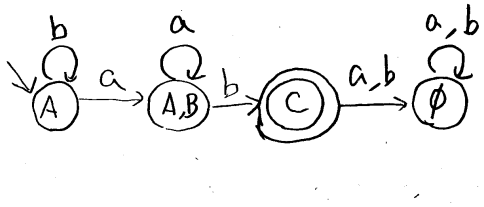

図 6　図 3.10 の決定性有限オートマトンへの変換

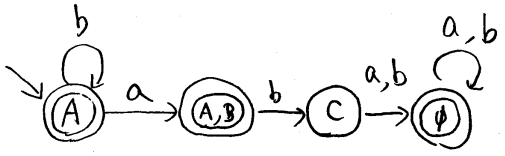

図 7　図 3.10 の補集合を受理する決定性有限オートマトン

は根から唯一つの路 $[\varepsilon, i_1][i_1, i_2] \ldots [i_{k-1} i_k]$ を持つので，木である．

問 3.32

基礎　頂点だけからなるグラフはそれを根とする 2 分木である．

帰納ステップ　t_1, t_2 がそれぞれ節点 v_1, v_2 を根とする 2 分木ならば，これらに新たに節点 v と左の枝 $[v, v_1]$, を付け加えたグラフ，節点 v と右の枝 $[v, v_2]$, を付け加えたグラフ，節点 v と左の枝 $[v, v_1]$, と右の枝 $[v, v_2]$, を付け加えたグラフ，はそれぞれ v を根とする 2 分木である．

問 3.33　図 3.16 のデータを，前順探索で並べると 10, 5, 7, 20, 15, 13, 18, 24, 22, となり，中間順探索では 5, 7, 10, 13, 15, 18, 20, 22, 24, となり，後順探索では 7, 5, 13, 18, 15, 22, 24, 20, 10 となる．

問 3.34

(1) v を根とする 2 分探索木に対して，与えられたデータ d を持つ節点を探索するアルゴリズム search(v, d)

- v のデータ $= d$ ならば，v がその節点である
- v のデータ $< d$ のとき，v に左の子があれば search(v の左の子, d) を適用し，なければデータ d を持つ節点はない
- v のデータ $> d$ のとき，v に右の子があれば search(v の右の子, d) を適用し，なければデータ d を持つ節点はない

(2) v を根とする 2 分探索木に対して，与えられたデータ d を持つ節点を追加するアルゴリズム append(v, d)

- v のデータ $= d$ ならば，なにもしない
- v のデータ $< d$ のとき，v に左の子があれば append(v の左の子, d) を適用し，なければデータ d を持つ節点を作って v の左の子とする
- v のデータ $> d$ のとき，v に右の子があれば append(v の右の子, d) を適用し，なければデータ d を持つ節点を作って v の右の子とする

問 3.35 v を根とする 2 分木で表現された式の値を求める帰納的アルゴリズム calc(v)

- v のデータ が定数ならば，calc(v) の値は定数の値である
- v のデータ $= +$ のとき，calc(v) の値は calc(v の左の子) の値 $+$calc(v の左の子) の値とする
- v のデータ $= -$ のとき，calc(v) の値は calc(v の左の子) の値 $-$calc(v の左の子) の値とする
- v のデータ $= \times$ のとき，calc(v) の値は calc(v の左の子) の値 $*$calc(v の左の子) の値とする
- v のデータ $= /$ のとき，calc(v) の値は calc(v の左の子) の値 /calc(v の左の子) の値とする

問 3.36 v を根とする 2 分木で表現された式を変数 x で微分する帰納的アルゴリズム D(v, x)

- v のデータ が定数または x 以外の変数ならば，D(v, x) は v のデータを定数 0 にした木である

- v のデータが変数 x ならば，$\mathrm{D}(v,x)$ は v のデータを定数 1 にした木である
- v のデータが $+$ または $-$ のとき，木 $\mathrm{D}(v,x)$ は D の左部分木を $\mathrm{D}(v$ の左の子$,x)$，D の右部分木を $\mathrm{D}(v$ の右の子$,x)$ で置き換えたものである．
- v のデータ $=\times$ のとき，$(f(x)\times g(x))' = f'(x)\times g(x) + f(x)\times g'(x)$ であるから，木 $\mathrm{D}(v,x)$ は図 8 の左図の木である．
- v のデータ $=/$ のとき，$(f(x)/g(x))' = f'(x)/g(x) - f(x)\times g'(x)/(g(x)\times g(x))$ であるから，木 $\mathrm{D}(v,x)$ は図 8 の右図の木である．

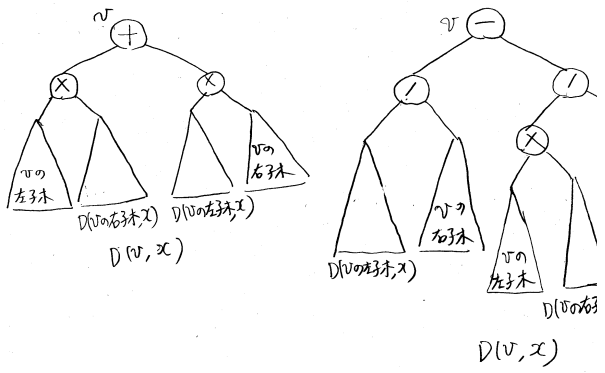

図 8　数式を微分するアルゴリズム

問 3.37　中置記法では $2+3\times5$，前置記法では $+,2,\times,3,5$，後置記法では $2,3,5,\times,+$ となる．

問 3.38　例えば，$10-(3+5)=2$，$10-3+5=12$ であり，括弧がある場合とない場合では，式の意味が異なる．前置記法ではそれぞれ $-,10,+,3,5$ と $+,-,10,3,5$，後置記法ではそれぞれ $10,3,5,+,-$ と $10,3,-,5,+$ となる．

問 3.39　行と列を交換して転置行列を求める操作 $(A^T)_{i,j} = (A)_{j,i}$ である．

問 3.40

(1) $R^2 \subseteq R$ より任意の n に対して $R^n \subseteq R^{n-1} \subseteq \cdots \subseteq R$ だから $R \subseteq R^+ \subseteq R$. このことは,「頂点 u から v への長さ 2 の路があれば辺 (u, v) がある」ならば「頂点 u から v への長さ 1 以上の路があれば辺 (u, v) がある」ことを意味する.

(2) $R^0 \subseteq R$ なので $R = R^+ = R^*$ このことは,「すべての頂点がループを持ち，頂点 u から v への長さ 2 の路があれば辺 (u, v) がある」ならば「頂点 u から v への長さ 0 以上の路があれば辺 (u, v) がある」ことを意味する.

(3) R が反対称的であることは長さ 2 の閉路をもたないことと同値だから，$(R - R^0)^2 \cap R^0 = \emptyset$ であり，さらに推移的なので $R = R^+ \wedge (R - R^0) = (R - R^0)^2 = (R - R^0)+$ である．これは推移的で長さ 2 の閉路を持たなければ，ループ以外の閉路を持たないことを意味する.

(4) 全域的（$\mathrm{dom}(R) = A$）な R が対称的であれば $R^0 \subseteq R \cdot R^{-1} = R^2$. さらに推移的であるから $R = R^{-1} = R^*$ である．この状況では，グラフの互いに連結なすべての頂点の間に両方向の辺がある.

問 3.41 図 9.

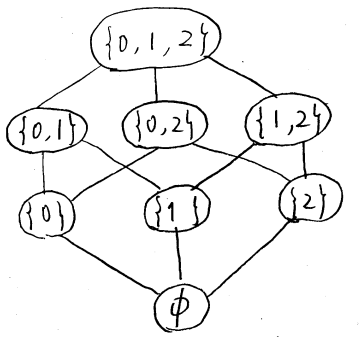

図 9 $\mathbf{2}^{\{0,1,2\}}$ 上の順序関係 $\subseteq$ のハッセ図

問 3.42 図 10.

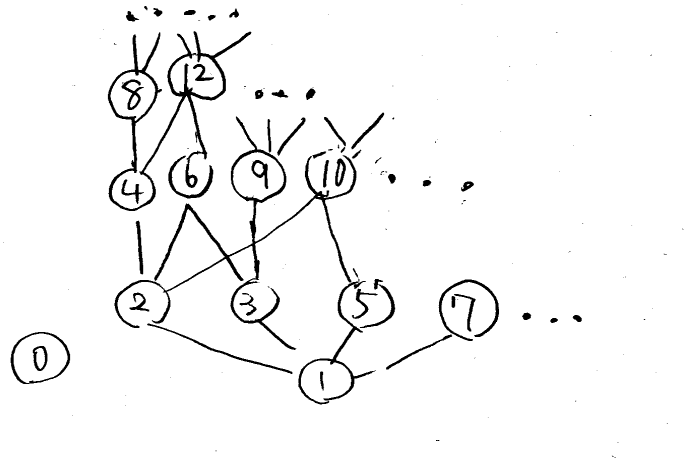

図 10　自然数 $\mathbb{N}$ 上の関係 $\{(a,b) \in \mathbb{N} \times \mathbb{N} \mid a \text{ が } b \text{ を割り切る}\}$ のハッセ図.

問 3.43　3 要素集合 $\{a,b,c\}$ 上の順序関係のハッセ図は図 11 の 5 通りであるから全部で 19 通りである.

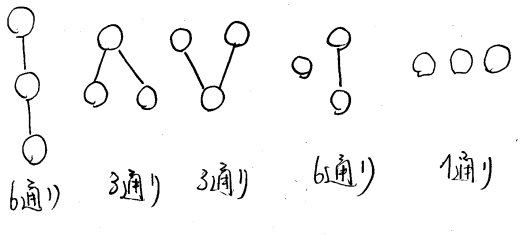

図 11　3 要素集合上の順序関係のハッセ図

問 3.44　R^* は反射的かつ推移的であるから，反対称的であればよい．その必要十分条件は R のグラフが長さ 2 以上の閉路を持たないことである.

問 3.45

(1) R は反射的であるから $\forall a \in A\ a \in R(a)$. よって $\bigcup_{a\in A}\ R(a) = A$.

(2) $c \in R(a) \cap R(b)$ ならば，R は対称的だから $a, b \in R(c)$. さらに R が推移的であるから $R(a) \subseteq R(R(c)) \subseteq R(c) \subseteq R(a)$. b についても同様だから，$R(a) = R(b) = R(c)$.

よって，$R(a) \cup R(b) \neq \emptyset \to R(a) = R(b)$.

問 3.46 R が同値関係ならば，そのグラフは連結成分（同値類）上の完全グラフの和で表されるから，$R = \bigcup_{X\in A/R} X \times X$.

問 3.47 定義から a と b が同値関係 $R_{\mathcal{A}}$ のもとで同値だということは，分割 $\mathcal{A}$ のもとで a と b がともに同じ集合（R の同値類）に属すということであり，それはとりもなおさず同値関係 R のもとで a と b が同値であることに他ならない．形式的に書けば，$(a, b) \in R_{\mathcal{A}} \iff \exists A_i \in \mathcal{A}\ \{a, b\} \subseteq A_i \iff \exists c\ \{a, b\} \subseteq R(c) \iff (a, b) \in R$.

問 3.48 $R^*, (R^*)^{-1} = (R^{-1})^*$ がともに推移律をみたすことから $\widehat{R} := R^* \cap (R^*)^{-1}$ も推移律をみたし，$R^0 \subseteq \widehat{R}$ より $\widehat{R}$ は反射律を満たす．さらに，$(x, y) \in R^* \cap (R^*)^{-1} \Leftrightarrow (y, x) \in R^* \cap (R^*)^{-1}$ であるから，対称律を満たす.

問 3.49 条件より，$\bigwedge_{i=1}^{n}(a_i, b_i) \in R$ ならば

$$\bigwedge_{i=1}^{n}(f(b_1, \ldots, b_{i-1}, a_i, \ldots, a_n), f(b_1, \ldots, b_i, a_{i+1}, \ldots, a_n)) \in R$$

が成り立つ．R は推移的であるので，

$$(f(a_1, \ldots, a_i, \ldots, a_n), f(b_1, \ldots, b_i, \ldots, b_n)) \in R$$

が成り立つ.

問 3.50 定義より，$\bigwedge_{i=1}^{n} b_i \in R(a_i)$ ならば，$f(b_1, \ldots, b_n) \in R(f(a_1, \ldots, a_n))$ なので，$R(f(b_1, \ldots, b_n)) = R(f(a_1, \ldots, a_n))$ である.

問 3.51 ax は p の倍数であるから，p 自身を含めて 2 以上の p の約数はすべて ax の約数である．一方 $\mathrm{GCD}(a, p) = 1$ だから，a と p は 1 以外に共通の約数を持たない．よって p の 2 以上の約数はすべて x の約数であり，x は p の倍数である.

第 4 章 の 解

問 4.1　自然数と k を法とする各同値類との間には $n \longleftrightarrow kn + i$ （$i = 0, \ldots, k-1$）という 1 対 1 対応があり，自然数全体は，これら k 個の同値類と同じ大きさを持つ．したがって，自然数は自分自身の k 倍の大きさを持つ．

問 4.2

反射律　A から A への 1 対 1 上への写像 $f(x) = x$ があるから $|A| = |A|$

対称律　A から B への 1 対 1 上への写像 f があれば，f^{-1} は B から A への 1 対 1 上への写像だから，$|A| = |B| \Rightarrow |B| = |A|$

推移律　A から B への 1 対 1 上への写像 f があり，B から C への 1 対 1 上への写像 g があれば，$g(f(x)$ は A から C への 1 対 1 上への写像だから，$|A| = |B| \wedge |B| = |C| \Rightarrow |A| = |C|$ が成り立つ．

問 4.3　支配人は n 号室の客に $2n$ 号室に移ってもらい、空いた $1, 3, 5, \ldots$ 号室の新しい客を入れたのである．

問 4.4

(1)　A から A への 1 対 1 写像 $f(x) = x$ があるから $|A| \leq |A|$

(2)　A から B への 1 対 1 写像 f があり，B から C への 1 対 1 写像 g があれば，$g(f(x)$ は A から C への 1 対 1 写像だから，$|A| \leq |B| \wedge |B| \leq |C| \Rightarrow |A| \leq |C|$ が成り立つ．

問 4.5　有限集合の濃度はその要素数に等しいから，A が有限集合ならば，明らかにその真部分集合の濃度（要素数）は A の濃度（要素数）より小さい．$A \subseteq \mathbb{N}$ が無限集合ならば，A の要素を小さい順に $a_0, a_1, a_2, \ldots$ と並べることができる．このとき $a_0, a_2, a_4, \ldots$ は A の真部分集合で A と同じ濃度を持つ．

問 4.6　$f : A \to B$ が全単射ならば，$f(X) := \{f(x) \mid x \in X\}$ は 2^A から 2^B への全単射である．

問 4.7　$\dfrac{(i+j)(i+j+1)}{2} + i$

問 4.8　$|\mathbb{N}| = |\mathbb{N}^2|$ より $|\mathbb{N}| = |\mathbb{N}^2| = |\mathbb{N}^3| = \ldots$．厳密な証明は数学的帰納法による．

問 4.9　$A \neq B$ のとき $h(A) \neq h(B)$ であることを示せばよい．このとき，$(A-B)\cup(B-A)$ に属す最小の自然数 N は $A-B$ の要素であると仮定してよい．$C := A\cap\{0,\ldots,N-1\} = B\cap\{0,\ldots,N-1\}$ とおくと，$\displaystyle\sum_{n=N+1}^{\infty} 3^{-n} = \frac{3^{-N}}{2} < 3^{-N}$ なので，$h(B) \leq h(C) + \dfrac{3^{-N}}{2} < h(C) + 3^{-N} \leq h(A)$ である．

問 4.10　全体集合が単要素集合（$U = \{a\}$）のとき，$\cap, \cup, \bar{\cdot}$ の演算表は表 1 のように表 4.1 と一致する．

X, Y	$X \cap Y$	$X \cup Y$
U,U	U	U
U,∅	∅	U
∅,U	∅	U
∅,∅	∅	∅

X	$\overline{X}$
U	∅
∅	U

表 1　$\cap, \cup, \bar{\cdot}$ の演算表

問 4.11

分配法則　$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ は次の表から成り立つ．

$x\ y\ z$	$y \vee z$	$x \wedge (y \vee z)$	$x \wedge y$	$x \wedge z$	$(x \wedge y) \vee (x \wedge z)$
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

$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ も同様に証明できる．

32

吸収法則　$x \wedge (x \vee y) = x \vee (x \wedge y) = x$ は次の表により確認できる．

$x\ y$	$x \vee y$	$x \wedge (x \vee y)$	$x \wedge y$	$x \vee (x \wedge y)$
0 0	0	0	0	0
0 1	1	0	0	0
1 0	1	1	0	1
1 1	1	1	1	1

ド・モルガンの法則　$\neg(x \wedge y) = \neg x \vee \neg y$, $\neg(x \vee y) = \neg x \wedge \neg y$ は次の表により確認できる．

$x\ y$	$\neg(x \wedge y)$	$\neg x \vee \neg y$	$\neg(x \vee y)$	$\neg x \wedge \neg y$
0 0	1	1	1	1
0 1	1	1	0	0
1 0	1	1	0	0
1 1	0	0	0	0

問 4.12　$A \cap B \subseteq A$

問 4.13

定理 1（命題論理の双対原理）　偽 0 と真 1 および命題変数から演算記号 $\wedge, \vee, \neg$ で構成された命題論理式 P に対し，P 中の $\wedge$ と $\vee$，0 と 1 を交換して得られる式を P の**双対式**といい，P^* と書く．このとき，$P \to Q$ ならば $Q^* \to P^*$ であり，$P \Leftrightarrow Q$ ならば $P^* \Leftrightarrow Q^*$ である．

問 4.14　表のように 2 変数論理関数は全部で 16 あり．そのうち本質的に 2 変数関数であるものは 10 ある．

x, y	0, 0	0, 1	1, 0	1, 1
0	0	0	0	0
$x \wedge y$	0	0	0	1
$\neg(x \to y)$	0	0	1	0
x	0	0	1	1
$\neg(x \leftarrow y)$	0	1	0	0
y	0	1	0	1
$\neg(x \leftrightarrow y)$	0	1	1	0
$x \vee y$	0	1	1	1
$\neg(x \vee y)$	1	0	0	0
$x \leftrightarrow y$	1	0	0	1
$\neg y$	1	0	1	0
$x \leftarrow y$	1	0	1	1
$\neg x$	1	1	0	0
$x \to y$	1	1	0	1
$\neg(x \wedge y)$	1	1	1	0
1	1	1	1	1

問 4.15　シャノンの展開定理を使って，変数の個数 n に関する数学的帰納法によって示す.

基礎　$n = 1$ のとき，$f(x_1) = (f(0) \wedge \neg x_1) \vee (f(1) \wedge x_1)$ は 1 変数論理関数であり，$\neg x_1 \wedge x_1$，$\neg x_1$，x_1，$\neg x_1 \vee x_1$ のいずれかに等しいので，$\wedge, \vee, \neg$ 用いて表される.

帰納ステップ　シャノンの定理 $f(x_1, \ldots, x_{n-1}, x_n) = (f(x_1, \ldots, x_{n-1}, 0) \wedge \neg x_n) \vee (f(x_1, \ldots, x_{n-1}, 1) \wedge x_n)$ において，$f(x_1, \ldots, x_{n-1}, 0)$ と $f(x_1, \ldots, x_{n-1}, 1)$ は $n-1$ 変数論理関数なので帰納法の仮定により，$\wedge, \vee, \neg$ 用いて表される．よって，$f(x_1, \ldots, x_{n-1}, x_n)$ も $\wedge, \vee, \neg$ 用いて表される.

問 4.16　最初に $x^{\neg a} = 1 \Leftrightarrow x = \neg a \Leftrightarrow x \neq a$ に注意しよう. $g(x_1, x_2, \ldots, x_n) := \bigwedge_{f(a_1, a_2, \ldots, a_n)=0} \bigvee_{i=1}^{n} x_i^{\neg a_i}$ とおく．$g(x_1, x_2, \ldots, x_n) =$

$1 \Leftrightarrow \bigwedge_{f(a_1,a_2,\ldots,a_n)=0} \left(\left(\bigvee_{i=1}^{n} x_i^{\neg a_i} \right) = 1 \right) \Leftrightarrow \bigwedge_{f(a_1,a_2,\ldots,a_n)=0} \bigvee_{i=1}^{n} (x_i^{\neg a_i} = 1) \Leftrightarrow$
$\bigwedge_{f(a_1,a_2,\ldots,a_n)=0} \bigvee_{i=1}^{n} (x_i \neq a_i) \Leftrightarrow f(x_1, x_2, \ldots, x_n) \neq 0$ よって, $g(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_n)$ である.

問 4.17 加算結果の上の桁（桁上がり）c は，例にとりあげた 3 変数関数であるから $c = (\neg x \wedge y \wedge z) \vee (x \wedge \neg y \wedge z) \vee (x \wedge y \wedge \neg z) \vee (x \wedge y \wedge z)$ である. 下の桁は以下の表で与えられる.

$x\ y\ z$	$f(x,y,z)$	この行だけ 1 の論理式
0 0 0	0	
0 0 1	1	$\neg x \wedge \neg y \wedge z$
0 1 0	1	$\neg x \wedge y \wedge \neg z$
0 1 1	0	
1 0 0	1	$x \wedge \neg y \wedge \neg z$
1 0 1	0	
1 1 0	0	
1 1 1	1	$x \wedge y \wedge z$
$f(x,y,z) = (\neg x \wedge \neg y \wedge z) \vee (\neg x \wedge y \wedge \neg z) \vee (x \wedge \neg y \wedge \neg z) \vee (x \wedge y \wedge z)$		

問 4.18 ド・モルガンの法則 $x \vee y = \neg(\neg x \wedge \neg y)$ を使えば $\vee$ は $\wedge$ と $\neg$ を用いて表すことができるから. 同様に任意の論理関数は $\vee$ と $\neg$ だけを用いて表すこともできる.

問 4.19 $x\mathrm{NAND}y{:=}\neg(x \wedge y)$ だから，$\neg x = x\mathrm{NAND}x$ である. これより，$x \wedge y = (x\mathrm{NAND}y)\mathrm{NAND}(x\mathrm{NAND}y)$. NAND で $\wedge, \neg$ が表されるから，任意の論理関数が NAND で表せる. また，双対性より，同様の議論が $x\mathrm{NOR}y{:=}\neg(x \vee y)$ に対して成り立つ.

問 4.20 $\vee$ や $\wedge$ を計算する回路（図 12）

問 4.21 翻訳すれば以下のようになり，それぞれ妥当であることは明らかだろ

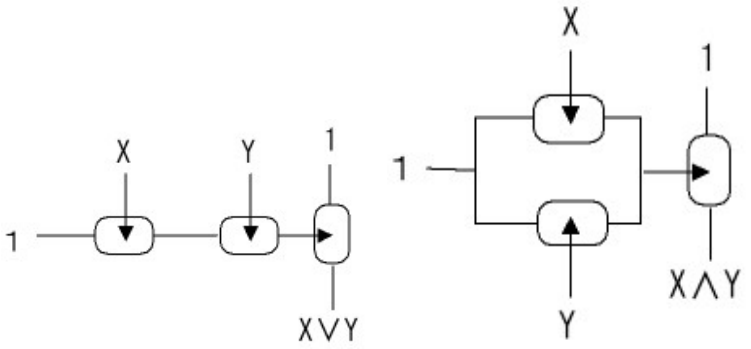

図 12

う.

AAA：すべての A は B である．すべての B は C である．よってすべての A は C である.

AEE：すべての A は B である．すべての B は C でない．よってすべての A は C でない.

IAI：ある A は B である．すべての B は C である．よってある A は C である.

IEO：ある A は B である．すべての B は C でない．よってある A は C でない.

問 4.22　意味を集合で表せば以下のようになるので明らか.

(1)　$A \cap B \neq \emptyset$

(2)　$A \cap B = \emptyset$

(3)　$\neg(A \subseteq B) \Leftrightarrow A - B \neq \emptyset$

(4)　$\neg(A \cap B \neq \emptyset) \Leftrightarrow A \cap B = \emptyset$

第 5 章 の 解

問 5.1　解答省略

問 5.2　$1 \times 5 \times 4 \times 3 \times 2 \times 1$ を計算するので 120．0 からはじめた場合，1 ずつ減らしていくと，$-1, -2, \ldots$ となりレジスタ R1 が 0 になることはないの

で，無限にループして止まらないというのが一つの答え．ただし，7.1.1 節で議論するように，整数が 2 の補数表示されることを考慮するとこの場合も停止して答えは 0 になる．

問 5.3 $q_0012 \vdash q_X X12 \vdash Xq_X12 \vdash X1q_X2 \vdash X12q_XB \vdash X12q_10 \vdash X1q_120 \vdash Xq_1120 \vdash q_2X120 \vdash q_20120 \vdash 0q_0120 \vdash 0q_YY20 \vdash 0Yq_Y20 \vdash 0Y2q_Y0 \vdash 0Y20q_YB \vdash 0Y20q_11 \vdash 0Y2q_101 \vdash 0Yq_1201 \vdash 0q_1Y1201 \vdash 0q_21201 \vdash 01q_0201$
よって出力は 01201 で，頭から 2 までの 0,1 の文字列 01 が 2 の後ろにコピーされる．

問 5.4

(1) $a(x,y) = x + y$

(2) $m(x,y) = x \times y$

(3) $d(xy) = \begin{cases} x/y & x \text{ が } y \text{ の倍数のとき} \\ \text{定義されない} & x \text{ が } y \text{ の倍数でないとき} \end{cases}$

問 5.5

(1) $A(1,0) = A(0,1) = 2, A(1,y+1) = A(0,A(1,y)) = A(1,y)+1$ より $A(1,y) = y+2$

(2) $A(2,0) = A(1,1) = 3, A(2,y+1) = A(1,A(2,y)) = A(2,y)+2$ より $A(2,y) = 2y+3$

(3) $A(3,0) = A(2,1) = 5, A(3,y+1) = A(2,A(3,y)) = 2A(3,y)+3$ より $A(3,y) = 2^{y+3} - 3$

(4) $A(4,0) = A(3,1) = 13, A(4,1) = A(3,A(4,0)) = 2^{16} - 3 = 65533, A(4,2) = A(3,A(4,1)) = 2^{65536} - 3.$

$A(3,y), A(4,y)$ が非常に急激に大きくなることがわかる．

問 5.6 $A(x,y)$ が定義されることを $A(x,y)\downarrow$ と表すことにしよう．アッカーマン関数がすべての自然数の対に対して定義されることは，$\forall x\ (\forall y\ A(x,y)\downarrow)$ を x に関する帰納法で証明するのだが，その際の帰納ステップで y に関する帰納法を使うという，2 重帰納法を用いる．
$\forall x\ (\forall y\ A(x,y)\downarrow)$ の証明.

基礎　$A(0,y)=y+1$ だから，$\forall y\ A(0,y)\downarrow$.

帰納ステップ　$\forall y\ A(m,y)\downarrow\Rightarrow\forall y\ A(m+1,y)\downarrow$ を証明する.

基礎　$A(m+1,0)=A(m,1)\wedge A(m,1)\downarrow$ より明らか.

帰納ステップ　$A(m+1,n)\downarrow$ ならば，$A(m+1,n+1)=A(m,A(m+1,n))\wedge\forall yA(m,y)\downarrow$ より，$A(m+1,n+1)\downarrow$.

結論　数学的帰納法により，$\forall y\ A(m,y)\downarrow\Rightarrow\forall y\ A(m+1,y)\downarrow$

結論　数学的帰納法により，$\forall x\ \forall y\ A(x,y)\downarrow$

問 5.7　Turing 機械は，時点表示の変換機械であるという観点に立てば，文字列中の特定の記号列（状態と入力記号からなる記号列）を別の記号列（動作後の状態とヘッドが見ている記号からなる記号列）に置き換える規則（例えば，$\alpha pX\beta\vdash\alpha qY\beta$）の集合とみなすことができる．このような，記号列の置き換え $\alpha\gamma\beta\vdash\alpha\delta\beta$ を定義する規則 (γ,δ) の集合と開始記号列からなるシステムを Markof のアルゴリズムという.

さらに，Markof のアルゴリズムにおいて，規則 (γ,δ) が記号列の変換 $\alpha\gamma\vdash\delta\alpha$ を定義する（すなわち，接尾列を取り出して規則を適用後に頭に付ける）としたものを Post のタグシステムという.

第 6 章 の 解

問 6.1　$f(3n+k)=n^k\ (k=0,1,2)$ だから，$f(n)\le n^2=O(n^2)$．一方，$\forall N\exists n>N\ n^2\le f(n)$ より，$O(n^2)\preceq f(n)$．よって，$f(n)=O(n^2)$.

問 6.2

(1)　$\forall n>N\ f(n)\le cg(n)$ を満たす $N\in\mathbb{N}$ と $c\in\mathbb{R}$ を用いて

$$h(n)=\begin{cases} f(n) & n\le N\text{ のとき}\\ cg(n) & n>N\text{ のとき}\end{cases}$$

と定義すればよい.

(2)　$\forall n>N\ f(n)\ge cg(n)$ を満たす $N\in\mathbb{N}$ と $c\in\mathbb{R}$ を用いて

$$h(n)=\begin{cases} f(n) & n\le N\text{ のとき}\\ cg(n) & n>N\text{ のとき}\end{cases}$$

と定義すればよい.

(3) $f = O(g) \Rightarrow \exists C_1, C_2 \in \mathbb{R}\ \exists N \in \mathbb{N}\ \forall n > N\ C_1|g(n)| \leq |f(n)| \leq C_2|g(n)| \Rightarrow \exists C_1, C_2 \in \mathbb{R}\ \exists N \in \mathbb{N}\ \forall n > N\ C_1|c_1/c_2||c_2 g(n)| \leq |c_1 f(n)| \leq C_2|c_1/c_2||c_2 g(n)| \Rightarrow c_1 f = O(c_2 g)$

(4) $f = O(h) \wedge g \leq O(h) \Rightarrow f + g = O(h + h) = O(h)$

問 6.3 $f(n) : \mathbb{N} \to \mathbb{R}$ が多項式オーダーであれば，$f(n) = O(n^k)$ より，f $(cn) = O(c^k n^k) = O(n^k)$ である.

問 6.4 n 桁の整数 $a_1 a_2 \ldots a_n$ と $b_1 b_2 \ldots b_n$ との掛け算に対する通常の筆算方法では，各 b_i に対する $a_1 a_2 \ldots a_n \times b_i$ を求めて，これらを桁位置を合わせて足し合わせる．$a_1 a_2 \ldots a_n \times b_i$ の計算では一桁の掛け算と繰り上がりの足し算をそれぞれ n 回行っている．したがって，計算の手間のオーダーは n^2 である．桁数でなく，数値 A, B とした場合，それぞれの桁数は $\log A, \log B$ だから，$O(\log A \log B)$.

問 6.5 $x^2 = x \times x$, $x^4 = x^2 \times x^2$, $x^8 = x^4 \times x^4$, $x^{16} = x^8 \times x^8$ の順に計算すればよい.

問 6.6 帰納的定義で x^n の計算に必要な乗算回数 $t(n)$ は

$$t(1) := 0, t(n) := t(\lfloor n/2 \rfloor) + 1 + n \mod 2$$

で定義される.

$$\log 1 = 0 \wedge \log n \leq \log(n/2) + 1 + n \mod 2$$

かつ

$$2\log 1 = 0 \wedge 2\log(n/2) + 1 + n \mod 2 \leq 2\log n$$

であるから，$\log n \leq t(n) \leq 2\log n$. よって $O(\log n)$ である.

問 6.7 加算回数 $t(n)$ の漸化式は

$$t(0) := 1, t(1) := 0, t(n) := t(n-1) + t(n-2) + 1$$

となる．ここで，$t(n) + 1 = (t(n-1) + 1) + (t(n-2) + 1)$ だから，$t(0) + 1 = a_1, t(1) + 1 = a_2$ に注意すれば，$t(n) = a_{n+1} - 1$ を得る.

問 6.8　帰納的定義 $\mathrm{fib}(a,b,0) := a$, $\mathrm{fib}(a,b,n) :=\mathrm{fib}(b,a+b,n-1)$ にしたがって求めればよい.

問 6.9　　与えられた文字列の対の集合 $\{(x_1,y_1),(x_2,y_2),\ldots,(x_n,y_n)\}$ に対し，言語

$$\{x_{i_1}x_{i_2}\ldots x_{i_k}y_{i_k}^R\ldots y_{i_2}^R y_{i_1}^R \mid i_1,i_1,i_k \in \{1,\ldots,n\}\}$$

を生成する文脈自由文法

$$A := x_1Ay_1^R \cup x_2Ay_2^R \cup \cdots \cup x_nAy_n^R \cup \varepsilon$$

と言語は $\{ww^R \mid w \in \Sigma^+\}$ を生成する文脈自由文法

$$B := \bigcup_{a\in\Sigma} aBa \cup \bigcup_{a\in\Sigma} aa$$

を考える．A と B が定義する文脈自由言語の共通部分は，元の Post の対応問題の解を与える．したがって，共通部分が空でないか否かを判定する問題は，Post の対応問題に還元できるので，決定不能である．

問 6.10　NP 問題を解く非決定性アルゴリズムの計算時間が多項式 $p(n)$ で抑えられるとする．このとき非決定性動作の回数も $p(n)$ で抑えられる．したがって，非決定性動作の候補数（有限）の最大値を a とおけば，ありえる計算過程の個数は $a^{p(n)}$ で抑えられる．したがって，それらをすべて模倣する（決定性）アルゴリズムの計算時間は $O(a^{p(n)})$ で抑えられる．

問 6.11　問題 Q が多項式時間計算量 $t(n)$ を持つ問題 R' に多項式時間アルゴリズム A で還元できるとき，入力 x に対する問題 Q の結果 $Q(x)$ を求めるには $R(A(x))$ を求めればよい．A は多項式時間アルゴリズムなので，P' の入力 $A(x)$ のサイズ $|A(x)|$ は入力 x のサイズ $|x|$ の多項式で抑えられる．したがって，$R(A(x))$ の計算時間 $t(|A(x)|)$ は $|x|$ の多項式で抑えられ，Q は P 問題である。

問 6.12　NP 完全問題 P_1 が多項式時間アルゴリズムで NP 問題 P_2 に還元できるとしよう．このことはまず，P_1 が NP 完全問題であるから，任意の NP 問

題 P の入力 w に対する YES・NO は，それを多項式時間アルゴリズムで変換した $f(w)$ に対する P_1 の YES・NO に一致する．さらに，P_1 が多項式時間アルゴリズムで NP 問題 P_2 に還元できるから，問題 P_1 の入力 $f(w)$ に対する YES・NO は，それを多項式時間アルゴリズムで変換した $g(f(w))$ に対する P_2 の YES・NO に一致する．したがって，任意の NP 問題 P の入力 w に対する YES・NO は，それを多項式時間アルゴリズムで変換した $g(f(w))$ に対する P_2 の YES・NO に一致する．よって P_2 は NP 完全問題である．

問 6.13　巡回セールスマン問題はあきらかに NP 問題であるから，NP 完全問題であるハミルトン閉路問題が巡回セールスマン問題に還元できることを示せばよい．ハミルトン閉路問題の入力グラフ G に対し，各辺の重みをすべて 1 にしたグラフが長さ（頂点数 -1）の巡回路を持つか否か問えばよい．

第 7 章 の 解

問 7.1　$5+3=8$ の 2 進表示は 1000 であるから，-8.

問 7.2

(1)　既約分数 q/p の小数表示が循環小数にならず有限桁で十進表現可能な必要十分条件は，p が 2 と 5 以外の素因数を持たないことである．

(2)　既約分数 q/p が有限桁で n 進表現可能な必要十分条件は，p の素因数がすべて n の素因数であることである．

問 7.3　英小文字を英大文字に変換する式は，

(小文字 c の番号 $-$ 小文字'a' の番号 $+$ 大文字'A' の番号) 番目の文字

である．

問 7.4

(1)　700×1000 画素のカラー画像のデータ量は圧縮しない場合，$\dfrac{700\times1000\times3}{1000\times1000}=$ 2.1MB

(2)　上のデータ量は，日本語（全角文字）の文庫本（700 文字/ページ，200 ページ/冊）$\dfrac{700\times1000\times3}{700\times200\times2}=7.5$ 冊

(3) CD（モノラル）で 1 分あたりのデータ量は $\dfrac{44000 \times 2 \times 60}{1000 \times 1000} = 5.28\text{MB}$ である．

問 7.5 有効数字 3 桁として，$x^2 - 100x + 0.01 = 0$ をの解を，2 解とも解の公式で求めると 100 と 0，解の公式と解と係数の関係を併用すると 100 と 0.0001 である．

問 7.6 有効数字 3 桁として，100 個の 10 と 100 個の 1 の和は，大きい順に加えたとき 1000 であり，小さい順に加えたとき 1100 である．

問 7.7 $\dfrac{\sum_{i=1}^{n}(x_i - m)^2}{n} = \dfrac{\sum_{i=1}^{n}(x_i^2 - 2mx_i + m^2)}{n} = \dfrac{\sum_{i=1}^{n} x_i^2}{n} - 2m\dfrac{\sum_{i=1}^{n} x_i}{n} + m^2 = \dfrac{\sum_{i=1}^{n} x_i^2}{n} - m^2$

問 7.8 $C(a) := 10, C(b) := 1$ なので

(1) $C(ab) = 101$, $C(bba) = 1110$

(2) $C^{-1}(101101) = abab$

問 7.9 条件は $\emptyset \subset X\Sigma^+$ である．実際，この条件を満たす X が接頭条件を満たせば，

$$\forall x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m \in X \; x_1x_2 \ldots x_n = y_1y_2 \ldots y_m$$

$$\Longrightarrow m = n \wedge \forall i \in \{1, \ldots, n\} \; x_i = y_i$$

を満たすことを示せばよい．$x_1x_2 \ldots x_n = y_1y_2 \ldots y_m$ より，x_1 が y_1 の接頭語であるか y_1 が x_1 の接頭語であるかのどちらかである．どちらも X の要素であるから，X の接頭条件より $x_1 = y_1$ である．以下同様の議論を繰り返せば $m = n \wedge \forall i \in \{1, \ldots, n\} \; x_i = y_i$ が成り立つ．

問 7.10 明らかに X が符号であることと $X^R = \{w^R \mid w \in X\}$ が符号であることとは同値である．さらに，X が 2 つ以上の要素をもちかつ接尾条件 $\Sigma^+X \cap X = \emptyset$ をみたせば $\emptyset \subset X \subseteq \Sigma^+$ だから，X は符号である．

問 7.11

(1) $\{1, 01, 10\}$ は $101 = 1 \cdot 01 = 10 \cdot 1$ が 2 通りに切り分けられるので，符号でない．

(2) $\{001, 0001\}$ は反接頭性を持つので接頭符号である．

(3) 0^*1 は (2) 同様反接頭性を持つので接頭符号である．

(4) $\{10, 01, 00\}$ は長さ 2 の定長符号であるから，接頭符号でもある．

問 7.12 $|\Gamma| = n$ のとき，Γ に対する $\{0,1\}$ 上の定長符号に必要な長さは $\lceil \log n \rceil$ である．

問 7.13 木の葉のアドレス集合は，反接頭性を持つので，接頭符号である．

問 7.14 図 13. $1100110111010 = 110 \cdot 0 \cdot 110 \cdot 111 \cdot 0 \cdot 10$

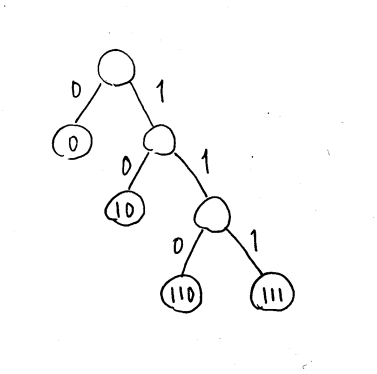

図 13　接頭符号 $X = \{0, 10, 110, 111\}$ を表す 2 分木

問 7.15 1 ビットの誤り確率が 1/1000 であるとする．パリティチェックがある場合に誤りを見逃してしまうのは，2,4,6,8 箇所の誤りがある場合であるから，その確率は ${}_8\mathrm{C}_2/1000^2 + {}_8\mathrm{C}_4/1000^4 + {}_8\mathrm{C}_6/1000^6 + {}_8\mathrm{C}_8/1000^8 = 28/1000^2 + 70/1000^4 + 28/1000^6 + 1/1000^8 = 0.000028000070000028000001$ である．

問 7.16 $d(x,x) = 0$, $d(x,y) \geq 0$, $d(x,y) = d(y,x)$ は定義から明らか．異なる箇所の集合を $D(a_1a_2 \ldots a_n, b_1b_2 \ldots b_n) := \{i \in \{1, \ldots, n\} \mid a_i \neq b_i\}$ で定

義しよう．x と z が異なる箇所では x と y が異なるか y と z が異なるかのどちらかであるから $D(x.z) \subseteq D(x,y) \cup D(y,z)$ よって，$d(x.z) \leq d(x,y) + d(y,z)$.

問 7.17　図 14 のように $m \times n$ ビットのデータを長方形に配置したものに，縦横にパリティビット列（太字）を付加する．このとき，縦および横の 1 ビット誤り検出情報から，1 ビット誤り位置が確定し，誤り訂正が可能になる．

0	1	0	0	**1**
1	1	0	0	**0**
1	0	1	0	**0**
0	**0**	**1**	**0**	**1**

図 14

問 7.18　文字列 abracatabra に対するハフマン符号は最小確率の 2 分木の選び方によって次の二通りある．平均長はどちらも 23/11 である．

記号	出現確率	ハフマン符号 (1)	ハフマン符号 (2)
a	5/11	0	0
b	2/11	100	10
c	1/11	110	1110
r	2/11	101	110
t	1/11	111	1111

問 7.19　例題 7.3 のハフマン符号の平均長は $0.2 \times 2 + 0.2 \times 3 + 0.4 \times 1 + 0.1 \times 3 = 1.9$ であり，定理 7.3 による理論的下限値は $-0.3 \log 0.3 - 0.2 \log 0.2 - 0.4 \log 0.4 - 0.1 \log 0.1 = 1.84644$ である．実際，ハフマン符号の平均長は理論的下限値より 1 以上大きくなることはないということが知られている．

問 7.20

(1)　A は A の錠をかけて箱を B に送る

(2)　B はさらに B の錠をかけて箱を A に送る

(3)　A は自分の鍵で A の錠を外して箱を B に送る

(4) B は B の錠を外して箱を開ける

この方法を暗号通信に適用すると，平文に対して A による暗号化，B による暗号化，A による復号化，B による復号化の順に行われることになるが，一般には，A による暗号化，B による暗号化，B による復号化，A による復号化の順序でなければもとの平文に戻ると限らない．

問 7.21 n 人の間の暗号通信は，共通鍵は $n(n-1)/2$ 個必要であり，一方，公開鍵・秘密鍵の対は n 対で十分である．

問 7.22 $x = 1, 2, \ldots, 9,\ n = 1, 2, \ldots, 9$ に対する $x^n \mod 10$ の表は以下の通り．

x ＼ n	1	2	3	4	5	6	7	8	9
1	1	1	1	1	1	1	1	1	1
2	2	4	8	6	2	4	8	6	2
3	3	9	7	1	3	9	7	1	3
4	4	6	4	6	4	6	4	6	4
5	5	5	5	5	5	5	5	5	5
6	6	6	6	6	6	6	6	6	6
7	7	9	3	1	7	9	3	1	7
8	8	4	2	6	8	4	2	6	8
9	9	1	9	1	9	1	9	1	9

x の n 乗の表 (mod 10)

問 7.23 A 氏の公開鍵を使って復号出来る暗号は秘密鍵を使ったものに限られるので，それを作成できるのは A 氏だけある．

問 7.24 文書が署名した本人しか作成できないことは，上の問で示している．さらに文書が偽造されていないことは，署名を公開鍵で戻した平文が文書と一致している否かを調べれば確認できる．

問 7.25 A の暗号化関数を $f_A(x) := x^{e_A} \mod n_A$，復号化関数を $g_A(y) := y^{d_A} \mod n_A$ とし，B の暗号化関数を $f_B(x) := x^{e_B} \mod n_B$，復号化関数を

$g_B(y) := y^{d_B} \mod n_B$ とする．ここで，公開鍵暗号の場合と異なり，A，B ほそれぞれの暗号化用の鍵 (e_A, n_A) と (e_B, n_B) を公開しない，

(1) A は 52 枚のカード $x_1, x_2, \ldots, x_{52}$ をそれぞれ暗号化した

$$f_A(x_1), f_A(x_2) \ldots, f_A(x_{52})$$

を B に送る．

(2) B はそのうち 5 枚のカードを選び，それぞれ暗号化した

$$f_B(f_A(x_{i_1})), f_B(f_A(x_{i_2})) \ldots, f_B(f_A(x_{i_5}))$$

を A に戻す．

(3) A はカードに復号関数を適用した

$$g_A(f_B(f_A(x_{i_1}))), g_A(f_B(f_A(x_{i_2}))) \ldots, g_A f_B(f_A(x_{i_5})))$$

を B に送る．ここで，問題は $g_A(f_B(f_A(x))) = f_B(x)$ が成り立たなければならない点である．そのためには，$n_A < n_B$ でなければならない．したがって，最初に A は n_A を B に教えて，n_B がそれより大きくなるようにしてもらう．

(4) B は受け取ったカード

$$f_B(x_{i_1}), f_B(x_{i_2}) \ldots, f_B(x_{i_5})$$

に復号関数を適用して，カード $x_{i_1}, x_{i_2} \ldots, x_{i_5}$ を知る．