コンピュータサイエンスのための離散数学入門 [1]

— Answers for Recommended Problems —

宮田 高志

1996.05.28–1996.12.25
1997.04.23–1997.10.09
1998.05.30–

1 集合と命題

- 1996 年度の勉強会でやった問題: 1, 17, 26, 29, 32, 39, 59, 73
- 1997 年度の勉強会でやった問題: 20, 52, 62, 74
- 1998 年度の勉強会でやった問題: 2, 16, 19, 48 (52)
- 1999 年度の勉強会でやった問題: 3, 15, 21, 27, 51, 68

1.73: ある国には、常に本当のことをいうかあるいは、常に嘘しかいわない人しか住んでいない。そして、これらの人々は、質問に対して、“はい” か “いいえ” しか答えない。1 人の旅人が、道がふたまたにわかれているところにさしかかった。この時、一方は首都に通じているが、他方は通じていない。そこには、どちらの道が首都に通じているかを示す標識はなかったが、この国の住人 Z 氏が立っていた。どちらの道をいけば首都につくかを判断するために、旅人は、Z 氏にどのような質問をすればよいか。ただし、質問は 1 回だけである。

解答: p で “Z 氏はいつも真実をいう” を表し、q で “左側の道は首都に通じている” を表す。p と q を含む、次のような命題 A を構成すればよい。「“A は真であるか？” という問いに対して、Z 氏が “はい” と答えるのは、q が真である時、かつその時に限る」すなわち、p, A, q に関する真理値表を書くと次のようにならなければならない。

p	A	q	comment
T	T	T	Z 氏が真実を言って A が真なら yes と言うから q は真でなければならない。
T	F	F	Z 氏が真実を言って A が偽なら no と言うから q は偽でなければならない。
F	T	F	Z 氏が嘘を言って A が真なら no と言うから q は偽でなければならない。
F	F	T	Z 氏が嘘を言って A が偽なら yes と言うから q は真でなければならない。

これより、$A \equiv p \leftrightarrow q$ であることがわかる。

1.52: n 組のカップルが、パーティーに出席した。かれらは、会場の入口でパーティーのホストとホステスに迎えられた。皆が握手をして、あいさつをしおわったあとに、ホストは、客全員とかれの妻 (ホステス) に、おのおの何人と握手したかを尋ねてまわったところ、$2n+1$ 個の異なる答えが得られた。どの人も、自分のパートナーとは握手しなかったとする。ホステスは何人の人と握手したのだろうか。答えを求め、帰納法で、それを証明せよ。

解答: 自分のパートナーとは握手しなかったことから、得られた答えは 0 人, 1 人, ..., $2n$ 人の $2n+1$ 通りであったはずである。$2n-k$ 人と握手した人と k 人と握手した人がカップルであることが数学的帰納法で証明できるので、どちらも n 人と握手したようなカップルがちょうど一組あることが分かる。このことから (尋ねてまわった) ホスト自身は n 人と握手していなければならないので、その相手であるホステスも n 人と握手したことになる。

2 計算可能性と形式言語

- 1996 年度の勉強会でやった問題: 8, 12, 16
- 1997 年度の勉強会でやった問題: 7, 17
- 1998 年度の勉強会でやった問題: 4, 5, 10, 11
- 1999 年度の勉強会でやった問題: 6, 9, 14

2.12(a): 言語 (省略) の各文は、a と b の個数が等しい文字列である。

解答: 本文にはやや複雑な文法が示してあるが、$S \to aSb \,|\, bSa \,|\, SS \,|\, \epsilon.$ で十分である。題意を満たす言語 L の任意の文がこの文法 G で生成できることを、数学的帰納法によって示す。L の最小の文 ab および ba は明らかに G で生成できる。長さ $2n$ までの L のすべての文が G で生成できたと仮定する。この時、長さ $2n+2$ の L の文で、a で始まる文 s について、左から a, b の個数を比較していって、ちょうど $k < 2n+2$ 番目で同じ個数になったとする。すると帰納法の仮定により、s を最初から k 番目の部分および $k+1$ 番目から最後の部分の二つに分けることによりどちらも G で生成できるので、これと $S \to SS.$ の規則を使うことにより s を生成できる。もし最後まで a と b の個数が同じにならなかった場合は (最初の文字は a と仮定したので) 最後の文字は b でなければならない。よってこの時も真中の部分については帰納法の仮定により G で生成でき、残りの部分について規則 $S \to aSb.$ を使うことによって生成できる。

2.17(b): 次の言語を生成するタイプ 2 の文法を与えよ。

$$L = \{x \,|\, x \in (a,b)^*, x \text{ は } b \text{ の } 2 \text{ 倍の } a \text{ を含む}\} \tag{1}$$

略解: 考え方としては「a, a, b の任意の順列を A とすると、A の任意の位置に A が入り得る」とするか、もしくは「a と a, b という『組』が同数含まれる」と考えてこの二つの任意の順列を生成するように文法を設計すればよい。

3 順列、組合せと離散的確率

- 1996 年度の勉強会でやった問題: 15, 67, 69, 70
- 1997 年度の勉強会でやった問題: 63, 71
- 1998 年度の勉強会でやった問題: 12, 37, 62, 64
- 1999 年度の勉強会でやった問題: 6, 36, 56, 68

3.64: 公正なコインを、2 回続けて表が出るか、あるいは 2 回続けて裏が出るまで投げるという試行について考察する。

(a) 標本空間を決定せよ。

(b) 6 回投げる前に、この試行が終了する確率はいくつか。

(c) 偶数回投げた後に、この試行が終了する確率はいくつか。

(d) 2 回表が出て試行が終了したことがわかっているとする。このとき、試行が、6 回投げる前に終了する確率はいくつか。

(e) 3 回投げる前には、試行が終了しないことがわかっているとする。このとき、6 回投げた後では、試行が終了しない確率はいくつか。

解答: (a) 表が出たことを H, 裏が出たことを T と表すと、

$$\Omega = \{(HT)^i HH \mid 0 \le i\} \cup \{(HT)^i T \mid 0 < i\} \cup \{(TH)^i TT \mid 0 \le i\} \cup \{(TH)^i H \mid 0 < i\} \tag{2}$$

(b) 次の 8 つのうちのいずれかであればよい。

$$\{HH, HTHH, HTT, HTHTT, TT, THTT, THH, THTHH\} \tag{3}$$

すなわち、

$$\Pr(6 \text{ 回投げる前に終了}) = \frac{1}{4} \times 2 + \frac{1}{8} \times 2 + \frac{1}{16} \times 2 + \frac{1}{32} \times 2 = \frac{7}{8} \tag{4}$$

(c) 式 (2) の右辺第一項か第二項に属す試行であればよいので、

$$\Pr(\text{偶数回で終了}) = 2\sum_{i=0}^{\infty} \left(\frac{1}{4}\right)^i \frac{1}{4} = \frac{2}{3} \tag{5}$$

(d) 2 回表が出て試行が終了する確率は、式 (2) の右辺第一項か第四項に属す試行がおきる確率であるから、

$$\Pr(HH \text{ で終了}) = \sum_{i=0}^{\infty} \left(\frac{1}{4}\right)^i \frac{1}{4} + \sum_{j=1}^{\infty} \left(\frac{1}{4}\right)^j \frac{1}{2} = \frac{1}{3} + \frac{1}{6} = \frac{1}{2} \tag{6}$$

である。一方、2 回表が出て試行が終了してかつ 6 回投げる前に試行が終了する確率は、式 (3) のうちの HH, $HTHH$, THH, $THTHH$ の四つであるから $\Pr(6 \text{ 回投げる前に } HH \text{ で終了}) = 1/4 + 1/8 + 1/16 = 7/16$。よって、

$$\Pr(6 \text{ 回投げる前に終了} \mid HH \text{ で終了}) = \frac{\Pr(6 \text{ 回投げる前に } HH \text{ で終了})}{\Pr(HH \text{ で終了})} = \frac{7}{8} \tag{7}$$

(e) 3 回投げる前に試行が終了する確率は、

$$\Pr(3 \text{ 回投げる前に終了}) = \Pr(X \in \{HH, TT\}) = \frac{1}{2} \tag{8}$$

(3 回以上投げてかつ) ちょうど 6 回目で試行が終了する確率は、

$$\Pr(6 \text{ 回目で終了}) = 4 \times \frac{1}{64} = \frac{1}{16} \tag{9}$$

よって、

$$\begin{aligned}
& \Pr(6 \text{ 回投げた後では終了しない} \mid 3 \text{ 回投げる前には終了しない}) \\
= \; & 1 - \Pr(6 \text{ 回目で終了} \mid 3 \text{ 回投げる前には終了しない}) \\
= \; & 1 - \frac{\Pr(6 \text{ 回目で終了})}{1 - \Pr(3 \text{ 回投げる前に終了})} \\
= \; & 1 - \frac{1}{8} = \frac{7}{8}
\end{aligned}$$

3.69 (注): Bayesian Network との関係に注意

番外編 一つ買うとおまけにバッチが一つついてくるお菓子がある。バッチの種類は全部で k 種類で、お菓子を買う時にどのバッチがついているかは分からないが、どの種類も等確率であたるとする。n 個のお菓子を買った時にちょうど全種類のバッチが揃う確率を求めよ。

解答: n 個のお菓子を買った時にちょうど k 種類のバッチが揃う場合の数を $f(n,k)$ と書くことにすると、$f(n,k)$ に対して次のような漸化式が成り立つ。

$$f(n,k) = k^n - \binom{k}{1} f(n,k-1) - \binom{k}{2} f(n,k-2) - \ldots - \binom{k}{k-1} f(n,1) \tag{10}$$

すなわち、n 個のお菓子を、ついてきたバッチの種類で分類することを考える。お菓子の買い方は k^n 通りだが、この中にはバッチが k 種類未満しかない場合も含まれるのでそれらを引いたのが式 (10) である。$f(n,1) = 1$ から順に計算してゆくと $f(n,k)$ は次のような式で表されることがわかる。

$$f(n,k) = \sum_{i=0}^{k-1} (-1)^i \binom{k}{i} (k-i)^n \tag{11}$$

これを使うと、求める確率 $\Pr(n;k)$ は次のように計算できる。

$$\begin{aligned}
\Pr(n;k) &= \Pr(n \text{ 個買ってちょうど } k \text{ 種類揃う}) \\
&= k\Pr(n-1 \text{ 個買って特定の } k-1 \text{ 種類揃う}) \times \Pr(\text{残った一種類をあてる}) \\
&= k\frac{1}{k}\Pr(n-1 \text{ 個買って特定の } k-1 \text{ 種類揃う}) \\
&= \frac{f(n-1,k-1)}{k^{n-1}} \\
&= k\sum_{i=0}^{k-2}(-1)^i\binom{k-1}{i}\left(\frac{k-1-i}{k}\right)^n \\
&= k\sum_{j=1}^{k-1}(-1)^{j-1}\binom{k-1}{j-1}\left(\frac{k-j}{k}\right)^n
\end{aligned}$$

4 関係と関数

- 1996 年度の勉強会でやった問題: 15, 24, 39, 47
- 1997 年度の勉強会でやった問題: 20, 42, 53
- 1998 年度の勉強会でやった問題: 2, 8, 15, 26, 32
- 1999 年度の勉強会でやった問題: 9, 10, 25, 31, 38

4.15 (類題): 10 個の要素を持つ集合 A 上の推移的な二項関係はいくつか？

4.39: 大学には 35,000 人の学生がいる。おのおのの学生は、4 つの (異なる) 科目を履修する。大学は、999 の異なる科目を開設した。離散数学に関係する科目を履修してるある学生が、最大の教室でも 135 人しか収容できないと知ったとき、ある問題が存在することに気がついた。何が問題であるのだろうか。

解答: 各学生は科目登録の申請書を一科目につき一枚、その科目の箱に入れるとすると、999 個の箱のうち少なくとも一つには 140 枚以上の登録申請書が入っているはず。

4.47: $x_1, x_2, \ldots, x_n$ を n 個の任意の整数とする。$x_i + x_{i+1} + \ldots + x_{i+k}$ が n で割り切れるような i と k ($i \geq 1$, $k \geq 0$) が存在することを示せ。

解答: $y_k = \sum_{i=1}^{k} x_x$ なる n 個の数を考える。このうちのどれかが n で割り切れるならば、題意は満たされている。どれも n で割り切れない時は y_k を n で割った余りを考えると、少なくとも一組、余りが等しいものがあるはずである (余りの種類は $n-1$ 通りで y_k は n 個あるから)。それらを y_i, y_j ($i < j$) とおくと $y_i \equiv y_j \pmod{n}$ であるから、その差 $y_j - y_i = x_{i+1} + \ldots + x_j$ は n で割り切れる。

4.42(注): 鎖は増加部分列を、反鎖は減少部分列を表す。

4.53: $a_1, a_2, \ldots, a_n$ と $b_1, b_2, \ldots, b_n$ を $a_i < b_i$ ($i = 1, 2, \ldots, n$) を満たす $2n$ 個の相異なる数とする。$a_1, a_2, \ldots, a_n$ を、$a'_1 > a'_2 > \ldots > a'_n$ となるように $a'_1, a'_2, \ldots, a'_n$ と並べ直し、そして、$b_1, b_2, \ldots, b_n$ を、$b'_1 > b'_2 > \ldots > b'_n$ となるように $b'_1, b'_2, \ldots, b'_n$ と並べ直す。このとき、$a'_i < b'_i$ ($i = 1, 2, \ldots, n$) となることを示せ。

解答: 題意を満たすことを示すには、任意の k について少なくとも k 個の (相異なる) b_i が a'_k より大きいことを示せばよい。そうすれば、b'_j は b_i を大きいものから並べたものだから a'_k に対応する b'_k は a'_k より大きいことになる。ところが、a'_k より '左の' a'_i ($i = 1, 2, \ldots, k-1$) に対してはすべて自分より大きい b_j を少なくとも一つずつ持っており、かつこれらは相異なるので、a'_k より大きい b'_k は少なくとも k 個ある。よって題意は満たされる。

4.26(c): π_1, π_2 を f に関して代入性を持つ 2 つの分割とする。このとき、$\pi_1 \cdot \pi_2$ と $\pi_1 + \pi_2$ はともに f に関して代入性を持つことを示せ。

解答: 集合 A の分割 π に対して二つの要素 $a, b \in A$ が π の同じブロックに属すとき、$a =_\pi b$ と書くことにする。すると、A から A への関数 f が代入性を持つことは次のように書ける。

$$\forall a, \forall b \in A : \ a \overset{\pi}{=} b \ \Rightarrow \ f(a) \overset{\pi}{=} f(b) \tag{12}$$

$\pi_1 \cdot \pi_2$ が代入性を持つことの証明 分割の積の定義から、

$$\forall a, \forall b \in A : \ a \overset{\pi_1 \cdot \pi_2}{=} b \ \Leftrightarrow \ (a \overset{\pi_1}{=} b) \wedge (a \overset{\pi_2}{=} b) \tag{13}$$

が成り立つ。一方、π_1 と π_2 はともに代入性を持つことから、

$$\forall a, \forall b \in A : \ a \overset{\pi_1}{=} b \ \Rightarrow \ f(a) \overset{\pi_1}{=} f(b) \tag{14}$$

$$\forall a, \forall b \in A : \ a \overset{\pi_2}{=} b \ \Rightarrow \ f(a) \overset{\pi_2}{=} f(b) \tag{15}$$

が成り立つ。(13) と (14), (15) から

$$\forall a, \forall b \in A : \ a \overset{\pi_1 \cdot \pi_2}{=} b \ \Rightarrow \ (f(a) \overset{\pi_1}{=} f(b)) \wedge (f(a) \overset{\pi_2}{=} f(b)) \tag{16}$$

が成り立つ。(13) の a, b をそれぞれ $f(a), f(b)$ として右から左が導けることを使うと、最後の命題は

$$\forall a, \forall b \in A : \ a \overset{\pi_1 \cdot \pi_2}{=} b \ \Rightarrow \ f(a) \overset{\pi_1 \cdot \pi_2}{=} f(b) \tag{17}$$

となる。

$\pi_1 + \pi_2$ が代入性を持つことの証明 分割の和の定義から、

$$\forall a, \forall b \in A : \ a \overset{\pi_1 + \pi_2}{=} b \ \Leftrightarrow \ \exists c_i \in A \text{ s.t. } (a \overset{\pi_*}{=} c_1) \wedge (c_1 \overset{\pi_*}{=} c_2) \wedge \ldots \wedge (c_k \overset{\pi_*}{=} b) \tag{18}$$

が成り立つ。ただし、関係 $\overset{\pi_*}{=}$ は π_1 か π_2 のどちらかを意味する。一方、π_1 と π_2 はともに代入性を持つことから、

$$\begin{aligned} a \overset{\pi_*}{=} c_1 \quad &\Rightarrow \quad f(a) \overset{\pi_*}{=} f(c_1) \\ c_1 \overset{\pi_*}{=} c_2 \quad &\Rightarrow \quad f(c_1) \overset{\pi_*}{=} f(c_2) \\ &\cdots \\ c_k \overset{\pi_*}{=} b \quad &\Rightarrow \quad f(c_k) \overset{\pi_*}{=} f(b) \end{aligned}$$

が成り立つ。(18) とこれらより

$$\forall a, \forall b \in A : \ a \overset{\pi_1 + \pi_2}{=} b \ \Rightarrow \ \exists c_i \in A \text{ s.t. } (f(a) \overset{\pi_*}{=} f(c_1)) \wedge (f(c_1) \overset{\pi_*}{=} f(c_2)) \wedge \ldots \wedge (f(c_k) \overset{\pi_*}{=} f(b)) \tag{19}$$

が成り立ち、$\pi_1 \cdot \pi_2$ に関する証明と同様に

$$\forall a, \forall b \in A : \ a \overset{\pi_1 + \pi_2}{=} b \ \Rightarrow \ f(a) \overset{\pi_1 + \pi_2}{=} f(b) \tag{20}$$

となる。

4.32(d): $g \circ f$ が次のそれぞれの関数となるための f と g についての必要十分条件を述べよ。

1. $g \circ f$ は上への関数
2. $g \circ f$ は 1 対 1 関数
3. $g \circ f$ は 1 対 1 で上への関数

解答: 二項関係 f が集合 A から集合 B への関数であるとは、A の任意の要素 a に対して $(a,b) \in f$ となるような B の要素がただ一つ定まることをいう。このとき $b = f(a)$ と書く。

f が A から B の上への関数であるとは、(21) が成り立つことをいう。また、f が A から B の 1 対 1 関数であるとは、(22) が成り立つことをいう。

$$\forall b \in B:\ \exists a \in A \text{ s.t. } b = f(a) \tag{21}$$

$$\forall a_1, a_2 \in A:\ a_1 \neq a_2 \ \Rightarrow\ f(a_1) \neq f(a_2) \tag{22}$$

また、A の部分集合 A' に対して B の部分集合 $B' = \{b \in B \mid \exists a \in A \,\text{s.t.}\, b = f(a)\}$ を A' の**像**という。

以下では f, g の定義域と値域をそれぞれ X, Y, Y, Z とする (i.e. $f : X \to Y$, $g : X \to Z$)。また、X の f に関する像を $\hat{Y}$ とおく。

1. $g \circ f$ は上への関数
   $\Leftrightarrow\ \forall z \in Z:\ \exists x \in X \text{ s.t. } z = g \circ f(x) = g(f(x))$
   $\Leftrightarrow\ \forall z \in Z:\ \exists y \in \hat{Y} \text{ s.t. } z = g(y)$ $\quad$ ($f(x)$ を y とおいた)
   $\Leftrightarrow\ g : \hat{Y} \to Z$ は上への関数 $\quad$ ($\Rightarrow g$ は上への関数)
2. $g \circ f$ は 1 対 1 関数
   $\Leftrightarrow\ [\forall x_1, x_2 \in X:\ x_1 \neq x_2 \ \Rightarrow\ g \circ f(x_1) \neq g \circ f(x_2)]$
   $\Leftrightarrow\ [\forall x_1, x_2 \in X:\ x_1 \neq x_2 \ \Rightarrow\ f(x_1) \neq f(x_2)]$ $\quad$ かつ $\quad$ $[\forall y_1, y_2 \in \hat{Y}:\ y_1 \neq y_2 \ \Rightarrow\ g(y_1) \neq g(y_2)]$
   $\Leftrightarrow\ f : X \to \hat{Y}$ は 1 対 1 かつ上への関数で、$g : \hat{Y} \to Z$ は 1 対 1 関数
   ($\Leftrightarrow\ f$ と $g : \hat{Y} \to Z$ は 1 対 1 関数)
3. $g \circ f$ は 1 対 1 で上への関数
   $\Leftrightarrow\ f : X \to \hat{Y}$ と $g : \hat{Y} \to Z$ が 1 対 1 かつ上への関数
   ($\Leftrightarrow\ f$ が 1 対 1 関数で、$g : \hat{Y} \to Z$ が 1 対 1 かつ上への関数)

4.38 (注): この問題は、「選ぶ時の確率が数によって異なっており、かつ選んだ数が〜の条件を $1 - \epsilon$ 以上の確率で満たすためには少なくともいくつ選ばなければならないか」という問題に一般化できる。そして、このような条件を満たす数の集合は ϵ-ネットとよばれる。ϵ-ネットに関する詳細は [3] を参照。

5 グラフと平面グラフ

- 1996 年度の勉強会でやった問題: 11, 12, 14, 36
- 1997 年度の勉強会でやった問題: 2, 16, 17
- 1998 年度の勉強会でやった問題: 8, 10, 18, 27
- 1999 年度の勉強会でやった問題: 1, 21, 34, 39

5.8: n 個の非不整数からなる順序づけられた組 $(d_1, d_2, \ldots, d_n)$ が**グラフ的** (graphical) であるというのは、n 個の頂点からなるループを持たない線形グラフで、それらの頂点の次数が d_1,...,d_n であるものが存在することである。

(c) 一般性を欠くことなく、$d_1 \geq d_2 \geq \ldots \geq d_n$ と仮定できる。このとき、$(d_1, d_2, \ldots, d_n)$ がグラフ的であるための必要十分条件は、$(d_2 - 1, d_3 - 1, \ldots, d_{d_1} - 1, d_{d_1+1} - 1, d_{d_1+2}, \ldots, d_n)$ がグラフ的であることを示せ。

解答: 二つの異なる頂点 α, β に対して隣接する頂点の集合をそれぞれ V_α, V_β と書くことにする。いま、V_β の要素であって V_α の要素でない頂点 u を一つとる。$|V_\alpha| \geq |V_\beta|$ ならば V_α の要素であって V_β の要素でない頂点 v が少なくとも一つ存在する。よって二つの辺 (u, β) と (v, α) を取り去って代わりに (u, α) と (v, β) を加えれば、各頂点の次数を変化させることなく、β に隣接していて α に隣接していない頂点を、α に隣接していて β に隣接していないようにすることができる (図 1)。この性質を使うと、$(d_1, d_2, \ldots, d_n)$ がグラフ的である

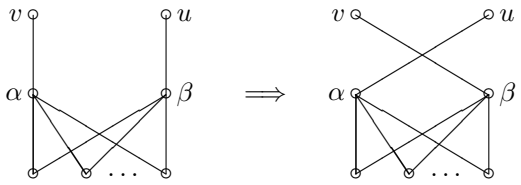


図 1: 二本の辺の「入れ換え」

とき、対応するグラフの、次数 d_1 を持つ頂点 u が $N = \{d_2, d_3, \ldots, d_{d_1+1}\}$ のどれとも隣接していなくても、(上記のように二本の辺を入れ換えることで) N の要素と隣接するようにグラフを書き換えることが必ずできる (α が N の要素、β が N 以外の頂点に相当する)。よって $(d_1, d_2, \ldots, d_n)$ がグラフ的であるときこの書き換えを繰り返せば、次数 d_1 を持つ頂点 u が N のすべての要素と隣接しているようにすることができる。この状態で u と u からの辺を取り除けば、次数の組は $(d_2 - 1, d_3 - 1, \ldots, d_{d_1} - 1, d_{d_1+1} - 1, d_{d_1+2}, \ldots, d_n)$ となるので、これもグラフ的であるといえる。また逆は明らかに成り立つ。

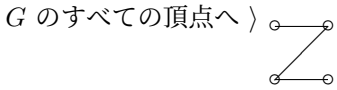
5.10(c): 自己補グラフは、$4k$ または $4k + 1$ 個の頂点を持つことを示せ。

解答: グラフ G が自己補グラフであるためには、G と同じ数の頂点をもつ完全グラフの辺の数が偶数本でなければならない。ところが、頂点の数が $4k + 2$ のときは、その完全グラフは ${}_{4k+2}C_2 = (2k + 1)(4k + 1)$ 本すなわち奇数本の辺を持つので自己補グラフにはなり得ない。頂点の数が $4k + 3$ のときも同様に自己補グラフにはなり得ない。

逆に、$4k$ または $4k + 1$ 個の頂点があれば必ず自己補グラフを作れることが、次のように数学的帰納法で示せる。

- $k = 1$ の時: 4 および 5 個の頂点を持つ自己補グラフは次のように作ることができる。

- $k = n$ の時に自己補グラフが作れると仮定する。そのグラフを G とおくと、次のように G に四つの頂点を加えれば $k = n + 1$ のときも自己補グラフが作れることが分かる。



よって頂点の数が $4k$ または $4k + 1$ 個であるということは自己補グラフを作れることの必要十分条件となっている。

5.12, 5.14 (参考): 次の perfect graph theorem が有名。

Perfect Graph Theorem (Lovász): α-perfect $\Leftrightarrow$ χ-perfect

任意のグラフ G に対して、(1) 最小彩色の色数を $\chi(G)$, (2) 最大独立点集合のサイズを $\alpha(G)$, (3) 最小クリークカバー (点集合をクリークに分割) のクリーク数を $\kappa(G)$, (4) 最大クリークのサイズを $\omega(G)$ と書く。これらの間には自明な大小関係 $\omega(G) \leq \chi(G)$, $\alpha(G) \leq \kappa(G)$ がある。

Def. $G(V, E)$ の点誘導部分グラフ (vertex induced subgraph) とは $V' \subseteq V$ に対して、$G'_{V'} = (V', E \cap (V' \times V'))$ をいう。

Def. G が α-perfect $\Leftrightarrow$ G の任意の点誘導部分グラフ G' に対して $\alpha(G') = \kappa(G')$。

Def. G が χ-perfect $\Leftrightarrow$ G の任意の点誘導部分グラフ G' に対して $\omega(G') = \chi(G')$。

Def. G の ($K_{|V|}$ に対する) 補グラフ $\bar{G}$ とは $G(V, E)$ の時、$\bar{G}(V, V \times V \setminus E)$ のことである。

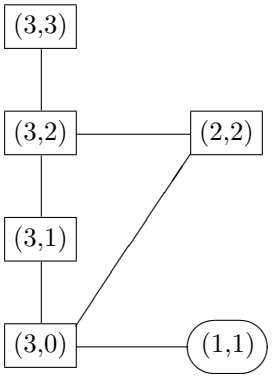


図 2: 3 組の夫婦の状態遷移グラフ (自分自身に戻る遷移は省略した)

5.36: n **次元立方体 (n-cube)** とは、n 桁の 2 進数で標識づけられた 2^n 個の頂点を持ち、2 つの頂点の 2 進数が 1 つの桁だけ異なるとき、その頂点間に辺が存在する無向グラフのことである。$n \geq 1$ に対して、n 次元立方体はハミルトン閉路を持つことを示せ (隣接する 2 数が、ちょうど 1 つの桁だけ値が異なるような 2^n 個の n 桁 2 進数の系列的な配置は、**グレイ・コード (Gray code)** として知られている)。

解答: 2^{n+1} 個のノードのうち、2^n 個は頭に 0 を、その他の 2^n 個は頭に 1 をつけ、後ろの $n-1$ bit が同じもの同士をつなぐ。こうすれば帰納法の仮定からそれぞれのグループについてハミルトン閉路が存在し、どちらのグループ中のノードも相手側とちょうど一つリンクを持っている。よってそれらのリンクを使って両方のハミルトン閉路をつなげればよい。

5.2: (a) 3 組の夫婦が旅の途中で河に出会った。そこには、2 人乗りボートが 1 隻しかなかった。3 人の夫は全員嫉妬深く、自分の妻を他の男のいる中に残しておくことを許さないとする。3 組の夫婦が河を渡る方法をグラフを用いて決定せよ。

(b) (a) のパズルにおいて、4 組の夫婦がいると仮定すると、解がないことを証明せよ。

(c) (a) のパズルにおいて、4 組の夫婦がいてボートが 3 人乗りとすれば、解があることを証明せよ。

解答: (a) こちら側の岸にいる夫と妻の人数を一つの状態として、状態の遷移を「適当な人数でボートを向こう側へこいでゆき、さらに適当な人数で**こちら側へ戻ってくる**」と定める。問題の条件から、どちらの岸でも夫の人数が妻の人数以上でなければならないので、状態遷移グラフは次のようになる。各状態はこちら側の (夫の人数, 妻の人数) を表す。丸で囲った状態が最終状態 (の一歩手前) である。

(b) 同様の考え方で可能な状態を数え上げると、(4,4),...,(4,0),(3,3),(2,2),(1,1) の 8 通りある。ところが一回の遷移でこちら側の人数は高々一人しか減らないので、(1,1) へ遷移するためには合計 3 人の状態がなければならないが、そのような状態はないので解はない。

5.16: 無向グラフにおいて 2 頂点間の**距離** (distance) をその頂点間を結ぶ道に含まれる辺の個数の最小数と定義する。無向グラフの**直径** (diameter) とは、すべての 2 頂点間の距離のうちの最大値のことである。

(a) 図 5 P.4 (省略) のグラフの直径を求めよ。

(b) グラフの頂点はコンピュータを表わし、辺はコンピュータ間のデータ通信回線を表わすものとする。この場合グラフの直径は具体的に何を意味するか。

(c) d を n 頂点を持つグラフの直径とし、δ を頂点の次数の最大数とする。

$$1 + \delta + \delta(\delta-1) + \delta(\delta-1)^2 + \ldots + \delta(\delta-1)^{d-1} \geq n \tag{23}$$

を示せ。

解答 (c): 直径の定義から、ある頂点から距離 d 以内でたどれるすべての頂点に印をつけると、グラフのすべての頂点に印がつかなければならないことに着目する。

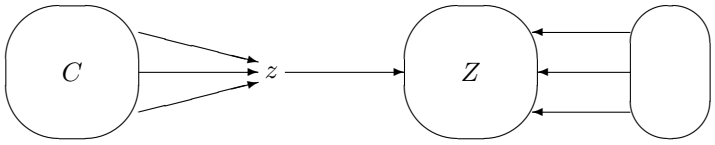


図 3: C のどの頂点も z に向かう辺をもつ時

1. $d = 1$ の時:
   どの頂点 v に関しても、高々 δ 個の頂点と隣り合っている。直径が 1 であるから、v 自身を含めて $1 + \delta$ でグラフ中のすべての頂点を尽くしていなければならない。すなわち $1 + \delta \geq n$ が成り立つ。
2. $d = 2$ の時:
   同様に、どの頂点 v に関しても距離 1 でたどれる頂点は高々 δ 個、距離 2 でたどれる頂点は高々 $\delta(\delta-1)$ 個 (距離 1 でたどれる頂点の各々が v を除いて高々 $\delta - 1$ 個の頂点と隣り合っているから) なので、v 自身を含めて $1 + \delta + \delta(\delta - 1)$ 個でグラフ中のすべての頂点を尽くしていなければならない。すなわち $1 + \delta + \delta(\delta - 1) \geq n$ がなりたつ。
3. 同様の議論から $d = k$ の時は $1 + \delta + \delta(\delta - 1) + \delta(\delta - 1)^2 + \ldots + \delta(\delta - 1)^{k-1} \geq n$ が成り立つ。

5.34: G を有向完全グラフとする。G の頂点集合の空でない部分集合 S が次の条件をみたすとき、**高位集合** (outclassed group) とよばれる。すなわち、S の頂点と S に含まれない頂点とを結ぶどの有向辺も、必ず S に含まれない頂点から S の頂点へと向きがついているときである。G に高位集合が存在しないならば、G はすべての頂点を含む有向初等閉路をもつことを示せ。

解答: G の適当な有向閉路を C とおく。まず、G が高位集合をもたないことから、C 以外の点 z で辺の向きが C の点 x_0 から z であるものが存在する。そのような点がなければ C が高位集合になってしまうからである。さらに、C において x_0 の直後の点 x_1 に対して、もし辺の向きが (z, x_1) ならば $x_0 \to z \to x_1 \to \ldots$ と辿ることによって C に z を含めることができる。辺の向きが (x_1, z) の時は C において x_1 の直後の点 x_2 を考える。(z, x_2) ならば $x_0 \to x_1 \to z \to x_2 \to \ldots$ z と辿ることによってやはり C に z を含めることができる。(x_2, z) の時は C において x_2 の直後の点 x_3 に関して同様の議論を繰り返すと、結局次の二つの可能性がある。

1. (x_i, z) かつ (z, x_{i+1}) であるような i が存在する。
2. C のどの頂点 x_i に対しても辺の向きは (x_i, z) である。

前者の場合は C に z を含めることができる。また後者の場合は z から C 以外の点を辿って到達できるすべての点の集合 Z に着目する (図 3)。Z が高位集合にならないことから、Z 中の点 z' で C 中の点 x_j へ向かう辺をもつものが必ず存在する。この時、$x_{j-1} \to z \to \ldots \to z' \to x_j \to x_{j+1} \to \ldots$ と辿ることにより、C に z と Z の中のいくつかの点を含めることができる。以上より、上記二つのいずれの場合においても、C に対して C 以外の点を含むように拡張できる。よって G はハミルトン閉路をもつ。

5.39: 5.8 節で扱った巡回セールスマン問題に対して、必ずしも最良とはかぎらないが、良い結果を導く方法を以下に示す。再び、$G = (V, E, w)$ を n 頂点からなる完全グラフとし、w を E から正実数の集合への写像で、三角不等式をみたすものとする。T を G の最小全域木とする。

(a) V' で部分グラフ T において奇次数である頂点の集合とする。V' の頂点の個数は偶数でなければならない。理由を述べよ。

(b) G' で V' の頂点すべてからなる G の完全部分グラフを表す。M で G' の 1 因子で重みが最小のものを表す。$T \cup M$ で、T と M のグラフを重ね合わせたグラフを表す。(T と M の両方に現れている辺は、$T \cup M$ では 2 回現れる。) $T \cup M$ がオイラー閉路を含むことを示せ。

(c) T の重みが、最小ハミルトン閉路の重みより小さいことを示せ。

(d) M の重みが、最小ハミルトン閉路の重みの半分以下であることを示せ。

(e) $T \cup M$ のオイラー閉路から、すでに訪れた頂点を訪れることを避けることによって、そのオイラー閉路の重み以下の重みとなるハミルトン閉路が得られることを示せ。

解答: **(a)** 頂点 v の次数を $d(v)$ と書くことにすると、すべての頂点の次数の和 $\sum_v d(v)$ は辺の数の二倍に等しい。よって次数が奇数の頂点 v_i と偶数の頂点 v_j をわけて和をとると、以下の式が成り立つ。

$$\sum_i d(v_i) + \sum_j d(v_j) = 2|E| \tag{24}$$

左辺第一項 $\sum_i d(v_i)$ は各 $d(v_i)$ が偶数であることから偶数である。よって第二項全体も偶数でなければならない。すなわち、v_j の個数は偶数である。

(b) M の辺はすべて、もとの T において奇次数であった頂点を結んでいる。よって $M \cup T$ のすべての頂点の次数は偶数となるのでオイラー閉路を含む。

(c) 最小ハミルトン閉路から一つだけ辺を除いたグラフは G に対する全域木になっている。よって T が最小全域木ならばこれよりもさらに重みは少ないはずである。

(d) G' に対する最小ハミルトン閉路 H' から一つおきに辺を除くと、G' に対する 1 因子が二通り構成できる。M が G' に対する重み最小の 1 因子であるならば、M の重みはどちらの 1 因子の重みより小さくなければならない。よって M の重みは H' の重みの半分以下でなければならない。さらに、H' の重みは G に対する最小ハミルトン閉路 H の重みより小さくなければならない。なぜならば、H の頂点を G' に含まれないものはとばしつつ順に辿れば G' に対するハミルトン閉路 H'' が得られるが、H'' の重みは (三角不等式から) もとのハミルトン閉路 H の重みより小さい。H' は G' の最小ハミルトン閉路であるのだから、H' の重みは H'' の重みより小さくなければならない。

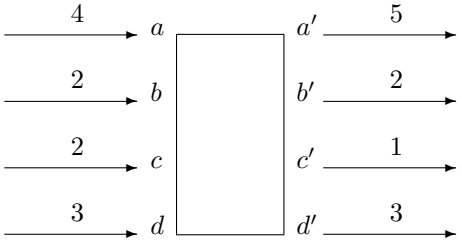
(e) もとのオイラー閉路を $(x_0, x_1, \ldots, x_n)$ とし、構成すべきハミルトン閉路を H とおく。$H = (x_0)$ から始めて、x_i を一つずつ H に追加してゆくが、x_i がすでに H に含まれていたら x_i はとばして x_{i+1} を、x_{i+1} も H に含まれていたら x_{i+2} を、というように順に H に頂点を加えてゆくとする。このようにして H を構成すれば、重みは三角不等式を満たすのでできたハミルトン閉路の重みはもとのオイラー閉路の重みより小さくなる。

6 木と切断集合

- 1996 年度の勉強会でやった問題: 30, 34, 38, 41
- 1997 年度の勉強会でやった問題: 13, 31, 40
- 1998 年度の勉強会でやった問題: 10, 26, 35
- 1999 年度の勉強会でやった問題: 1, 21, 34, 39

6.38: 4 個の頂点を持つ有向グラフで、どの頂点から他のどの頂点への辺も 3 本以上は存在せず、各頂点の出次数と入次数がそれぞれ (5,4), (3,3), (1,2), (2,2) となるものを、対応する輸送回路網の流れの問題を解くことにより構成せよ。

略解: 各頂点を仮想的に二つに分け、出入りしている辺の次数を容量とする輸送回路網を構成する。



この図において四角で囲んだところは完全二部グラフとなっており、各辺の容量は 1 である (自分自身への辺はないとすると a から a' などの辺は除く必要がある)。

6.41: 図のグラフ (省略) で、できるだけ小さい辺の集合を選んですべての頂点がその集合の少なくとも 1 つの辺と接続するようにしたい。この問題を輸送回路網に関係した最小流問題として解け。

略解: まず問題 6.39 の「ある輸送回路網が与えられたとき、各辺の流れが、その辺の容量以上であって、かつ、その値が最小であるような流れを求めたい」を解く必要がある。'自明な' 流れ φ (source から十分多くの量を流すことによって作ることができる) を一つとり、これと最小流 ϕ との差 $\varphi(i,j) - \phi(i,j)$ を各辺に対して考えることにより cut の容量を定義することができる。アルゴリズムに関しても同様で自明な流れからはじめて greedy に流れを減らしてゆけばよい。

6.41 に対する解答は (1) 左頂点集合の各頂点のそれぞれに source から容量 1 の辺を付け加える (2) 右頂点集合の各頂点のそれぞれから sink へ容量 1 の辺を付け加える (3) 与えられた辺集合の容量は 0 とする。としてから最小流を求めればよい。

本文中の最大流を求めるアルゴリズムの説明は直観的に何をやっているのか分かりにくいところがあるので次の説明を補足しておく。

1. 次の条件を満たす source a から sink z までの経路 $P = (v_0, v_1, v_2, \ldots, v_n, v_{n+1})$ (ただし $v_0 = a$, $v_{n+1} = z$) を探す。もしこのような経路がなければ終了である。

   P 中のすべての辺 $e = (v_i, v_{i+1})$ $(0 \le i \le n)$ について、辺 (v_i, v_{i+1}) の flow が容量未満であるか、辺 (v_{i+1}, v_i) の flow が 0 より大きい。前者の場合を「e は順方向である」といい、後者の場合を「e は逆方向である」ということにする。

2. 1 の経路 P の各辺 $e = (v_i, v_{i+1})$ について次の値を求め、それらのうちの最大値を ν とする。

   e が順方向: (e の容量) − (e の flow)
   e が逆方向: (v_{i+1}, v_i) の flow

3. P の各辺の flow を、その辺が順方向なら ν だけ増加、逆方向なら ν だけ減少させ、1 から繰り返す。

7 有限状態機械

- 1996 年度の勉強会でやった問題: 3, 8, 15, 20, 24
- 1997 年度の勉強会でやった問題: 2, 19, 22
- 1998 年度の勉強会でやった問題: 9, 11, 20

7.11: 下記の集合に対して、その集合を認識する決定的有限状態機械を求めよ。

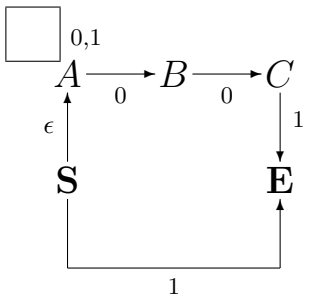
(d) $L = \{001$ で終わる 2 値文字列全体 $\} \cup \{1\}$

略解: 求める解を非決定性有限状態機械を使って記述すると、図 4 のようになる (初期状態が **S** で、終了状態が **E**)。これを決定性有限機械に変換する。表より、必要な状態は 5 つで、それらの遷移関係は図 5 となる (**1** が初期状態で、**3** が終了状態)。

7.15: 同期列 (synchronizing sequence) とは、有限状態機械を特定の最終状態へ移す入力列である。n 個の状態を持つ有限状態機械が同期列を持つならば、長さ $2^n - 2$ 以下の同期列を持つことを示せ。

解答: 与えられた有限状態機械 A の状態の集合を S、入力文字の集合を Σ、状態遷移関数を F とする。A を元に、状態の集合を $T = 2^S \setminus \phi$、入力文字の集合を Σ、状態遷移関数を F' とする次のような有限状態機械 B を考える。

$$\forall s, t \in T,\ \forall w \in \Sigma: \quad F'(s,w) = t \iff \forall a \in s\ \exists b \in t \text{ s.t. } F(a,w) = b \tag{25}$$



	状態の集合	遷移可能性
1	$\{S,A\}$	$0 \to A,B$ (2)
		$1 \to A,E$ (3)
2	$\{A,B\}$	$0 \to A,B,C$ (4)
		$1 \to A$ (5)
3	$\{A,E\}$	$0 \to A,B$ (2)
		$1 \to A$ (5)
4	$\{A,B,C\}$	$0 \to A,B,C$ (4)
		$1 \to A,E$ (3)
5	$\{A\}$	$0 \to A,B$ (2)
		$1 \to A$ (5)

図 4: $L = \{001$ で終わる 2 値文字列全体 $\} \cup \{1\}$ に対する非決定性有限状態機械とその決定化手続き表

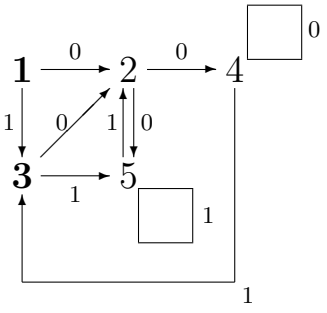


図 5: 図 4 の非決定性有限状態機械を決定化したもの

F' の定義から、A が状態 $x \in S$ への同期列 σ を持つことと、σ によって B を状態 $S \in T$ から状態 $\{x\} \in T$ へ遷移させられることが同値であることが分かる。B は $2^n - 1$ 個の状態を含むので σ の長さは高々 $2^n - 2$ である。

7.20: 次の言語は有限状態言語ではないことを示せ。
$L = \{xx \mid x \text{ は } 0 \text{ と } 1 \text{ からなる文字列 }\}$

解答: L を受理する有限状態機械 M が存在すると仮定する。M の状態の数を n とし、文字列 $\alpha = 0^n 10^n 1 \in L$ を考える。α を受理するまでに訪れた状態の列の前半 $n+1$ 個を $s_0, s_1, \ldots, s_n$ とする。状態の数は全部で n 個しかないから、これらのうち二つは同じものである。それらを s_i, s_j $(i < j)$ とすると、s_i から s_j の間を "近道" することにより、M は $0^i 0^{n-j} 10^n 1$ も受理しなければならない。これは矛盾である。よって L は有限状態言語ではない。

別解: L を受理する有限状態機械 M が存在すると仮定する。M の状態の数を n とし、$2^k > n$ となるような十分大きな k を一つ決め、0 と 1 からなる長さ k の文字列全体 X を考える。L の定義から任意の $x \in X$ に対して M は xx を受理しなければならないが、その途中の状態すなわち、ちょうど前半の x を読んだ状態 s を考える。x としては 2^k 通りの可能性があるので、状態 s は 2^k 個あるはずだが、$2^k > n$ となるように k を決めたので、これらのうちの少なくとも二つは同じ状態でなければならない。例えば $x_i \in X$ を読み終わった状態 s_i と $x_j \in X$ を読み終わった状態 s_j が同じであったとすると、M は $x_i x_i$, $x_j x_j$ だけではなく、$x_i x_j$, $x_j x_i$ も受理することになる。これは矛盾である。よって L は有限状態言語ではない。

8 アルゴリズムの解析

- 1996 年度の勉強会でやった問題: 6, 9
- 1997 年度の勉強会でやった問題: 6, 10
- 1998 年度の勉強会でやった問題: 5, 7
- 1999 年度の勉強会でやった問題: 1, 2

8.6: n 個の数 $x_1, x_2, \ldots, x_n$ をソートする問題を吟味する。一般性を失うことなく、n 個の数は異なっていると仮定する。基本演算が、2 つの数を比較し、比較の結果により枝分かれするものであるソーティング・アルゴリズムのクラスを考える。すなわち、2 つの数値 x_i, x_j を比較するために選び、$x_i > x_j$ ならば、操作の一方のコースが続く。一方、$x_x < x_j$ ならば、他方の操作のコースが続く。このようなアルゴリズムは、2 分木で簡単に表現できる。ここで、内点は比較演算に対応し、葉は n 個の数値の順序が完全に定まった最終結果に対応している。(a) 省略 (b) 4 つの数をソートするアルゴリズムを設計し、その計算量を決定せよ。(c) n 個の数をソートするこのクラスのアルゴリズムの計算量に関する下界を決定せよ。

略解 [2]: (b) 次のように比較すると 13 以外の各ノードでの場合の数が 2^m となる。(簡単のため「左側」だけを示す。(A (B C)) は A が二つの子供 B, C を持っていることを、ij は x_i と x_j を比較して $x_i > x_j$ ならば左の子供を選ぶことをそれぞれ意味している。)

(12 (13 (23 (24 (34 14)) (34 (24 14))) (14 (24 34))) (...))

(c) n 個の数について何も分からない状態では、その並び方について $n!$ 通りの可能性がある。比較をすることでこれらの可能性を分類していき最後に 1 通りとなった時が終了すなわち葉にたどり着いた時である。2 分木を一段下りるごとに場合の数を半分にできればもっとも速く葉にたどり着くことができるから、$\dfrac{n!}{2^k} \leq 1$ となる k が計算に必要な最小の比較回数である。すなわち

$$k \geq \frac{\log n!}{\log 2} = O(n \log n) \tag{26}$$

最後の変形は Staring の公式 $n! \approx \sqrt{2\pi n}\, n^n e^{-n}$ を使った。

追記 (1997 年度): 上のアルゴリズムは最悪の場合の比較回数は 5 回で最低 (証明は略) だが、最良の場合の比較回数が 4 回で効率が悪い。最良の場合の比較回数を 3 回に保ったまま最悪の場合の比較回数を 5 回 (以下) にすることはできるか？

二つずつに分けて、最も大きい要素と最も小さい要素を洗い出す方針でアルゴリズムを設計する。例えば次の通り。

(12 (34 (23 – (41 – 24)) (24 – (14 23 23))) (34 (. . .) (. . .)))

(c) の問題では**最悪の場合でも (うまくアルゴリズムを設計すれば)** $O(n \log n)$ で並べ替え可能だと主張していることに注意。例えば Quick Sort はこの主張を満たすアルゴリズムにはなっていない (Quick Sort の計算量が $O(n \log n)$ なのは平均であって、最悪は $O(n^2)$ であるから)。上の主張を満足するアルゴリズムとしては、Heap Sort などがある。

8.10: ヒープ (heap) は、次の条件を満たすように 2 分木の頂点に数を並べたものである。

> すべての葉は、最低、あるいは、次に低いレベルにある。
> 最低レベルの葉は、すべて一番左の位置にある。
> 内点の数は、その 2 つの息子の数より大きい。

たとえば、図 8 P.3(a) (省略) の 2 分木はヒープであり、図 8 P.3(b) はヒープではない。(a) 上記の初めの二つの条件を満たす n 個の数を持つ 2 分木が与えられているとき、それを、ヒープに変更するアルゴリズムを設計せよ。そのアルゴリズムの計算量はどのくらいか。(b) n 個の数を持つヒープが与えられていると仮定する。根の数と最低レベルの一番左の数を置き換えると、もはやヒープではない。(たとえば、図 8 P.3(c) (省略) は、この方法で図 8 P.3(a) (省略) から得られる。) この木を、ヒープに戻すアルゴリズムを設計せよ。そのアルゴリズムの計算量はどのくらいか。(c) n 個の数のヒープが与えられているとき、根の数について、何がいえるか。(a) と (b) で設計したアルゴリズムを結合して、ソーティング・アルゴリズムを作ることができる。どのようにすればよいか。そのソーティング・アルゴリズムの計算量はどのくらいか。

略解: 条件の内容がつかみにくいが、最初の文は、木の高さのバランスが高々 1 しか違わないということを言っている。つまり、木の高さが h の時、すべての葉は根から h または $h-1$ の距離にある。二つ目の文は根から葉までの距離に違いがあるとき、深い方の葉はすべてより左にあるということである。

(a)「トーナメント」を行ってゆけばよい。すなわち、第一段階では葉の方からより大きな数を親に持ってゆくという操作を繰り返して、根に来る数を決める。この時の計算量は (枝と比較が対応するので) $n-1$ 回の比較が行われる。第二段階では、やはり葉の方からより大きな数を親に持ってゆくという操作を繰り返すが、根の子供までででやめる。この時の比較回数は $n-1-2$ 回である。以下同様に高さ 2, 3, . . . までで打ち切る「トーンナメント」を木の高さまで行えば、ヒープが完成する。この時の比較回数の総和は

$$\sum_{i=1}^{h}(n-1-2^i) < nh \tag{27}$$

ただし、h は木の高さである。元の木は 2 分木でしかも最初の条件からほとんど完全 2 分木なので、$h \leq \log_2 n$ である。よって計算量は $O(n \log n)$ である。

(b) 問題では「置き換える」と書いてあるが、実際には「根を取り除いて代りに一番深いところにある葉を根に移動する」ということである。この場合単純に両方の息子と比較して大きいものを親に移すということを繰り返せばよい。移動してきた新しい根にある数が、一番深いところまで移動したときが最も計算量が多いときだが、この時でも元の木の高さ h を超えない。よって計算量は $O(\log n)$ である。

(a)(b) から前処理に $O(n \log n)$, 数を一つ取り出すのに $O(\log n)$ かかるので n 個の数を順々に取り出してソートするには $O(n \log n)$ の計算量が必要である。これは最悪の場合でも変わらない。

8.7(d): $n = 4$ に対して、天秤を 2 回しか使わない “枝分かれのない” アルゴリズムを見つけられるか。すなわち、最初の結果 (重いか、等しいか、軽いか) によらず、2 回目には、1 回目の結果のどの場合にも同じ重みの組を天秤の左右に載せるようなアルゴリズムが見つけられるか。$n = 13$ に対して、天秤を 3 回使う “枝分かれのない” アルゴリズムが見つけられるか。$n = (3^k - 1)/2$ に対して天秤を k 回使うものが見つけられるか。

解答: $n=2$ および $n=13$ に対するアルゴリズムは図 6 の通りである。ただし、各コインを $c_1, c_2, \ldots$ などと表し、正しいコインを C で表すとする。また、天秤の左に $c_i, c_j, \ldots$ を置き、右に $c_k, c_l, \ldots$ を置くことを「$c_i, c_j, \ldots \mid c_k, c_l, \ldots$」と表記し、傾いた方と同じ枝へ分岐するとする。

$n=13$ の時のアルゴリズムに $n=4$ の時のアルゴリズムの構造が入っていることから分かるように、次のような再帰的なアルゴリズムを用いれば、$n=(3^k-1)/2$ 枚のコインに対して 天秤を k 回使うだけで悪いコインを探せる。

check_bad_coin 入力: $n=(3^k-1)/2$ 枚のコイン

1. 問題のコインを $M_1 \equiv 3^{k-1}$ 枚と $M_2 \equiv (3^{k-1}-1)/2$ 枚の二つのグループに分ける。
2. M_1 のグループと同数の正しいコインを用意し、それぞれを天秤に載せる。
   (a) 天秤が正しいコインの方へ傾いた時: 'light' および M_1 を入力として **find_bad_coin** を呼び出す。
   (b) 天秤が問題のコイン M_1 の方へ傾いた時: 'heavy および M_1 を入力として **find_bad_coin** を呼び出す。
   (c) 天秤が釣り合った時: M_2 を入力として **check_bad_coin** を再帰的に呼び出す。

find_bad_coin 入力: $W \in \{$'light','heavy'$\}$ および $n=3^k$ 枚のコイン

1. コインを三等分し、各グループを N_1, N_2, N_3 とする。そのうち二つのグループ (N_1 および N_2 とする) を左右の天秤に載せる。
   (a) 天秤が N_1 の方に傾いた時:
   W が 'light' なら W と N_2 を、W が 'heavy' なら W と N_1 を入力として **find_bad_coin** を再帰的に呼び出す。
   (b) 天秤が N_2 の方に傾いた時:
   W が 'light' なら W と N_1 を、W が 'heavy' なら W と N_2 を入力として **find_bad_coin** を再帰的に呼び出す。
   (c) 天秤が釣り合った時:
   W と N_3 を入力として **find_bad_coin** を再帰的に呼び出す。
   ただし、各 N_i が 1 枚になっていたら終了である。

9 離散的数値関数と母関数

- 1996 年度の勉強会でやった問題: 11, 12, 22, 31
- 1997 年度の勉強会でやった問題: 10, 23, 30
- 1998 年度の勉強会でやった問題: 9, 12, 22, 25, 27
- 1999 年度の勉強会でやった問題: 8, 22, 35

9.11:

$$a_r = \begin{cases} 1 & r=0 \\ 3 & r=1 \\ 2 & r=2 \\ 0 & r \geq 3 \end{cases} \tag{28}$$

$$c_r = 5^r \qquad r \geq 0 \tag{29}$$

であるとき、**a**∗**b**=**c** を満たす **b** を求めよ。

略解: a_r 及び c_r の母関数 **a**, **c** は次のようになる。

$$\mathbf{a} = 1+3z+2z^2 \tag{30}$$

$$\mathbf{c} = \frac{1}{1-5z} \tag{31}$$

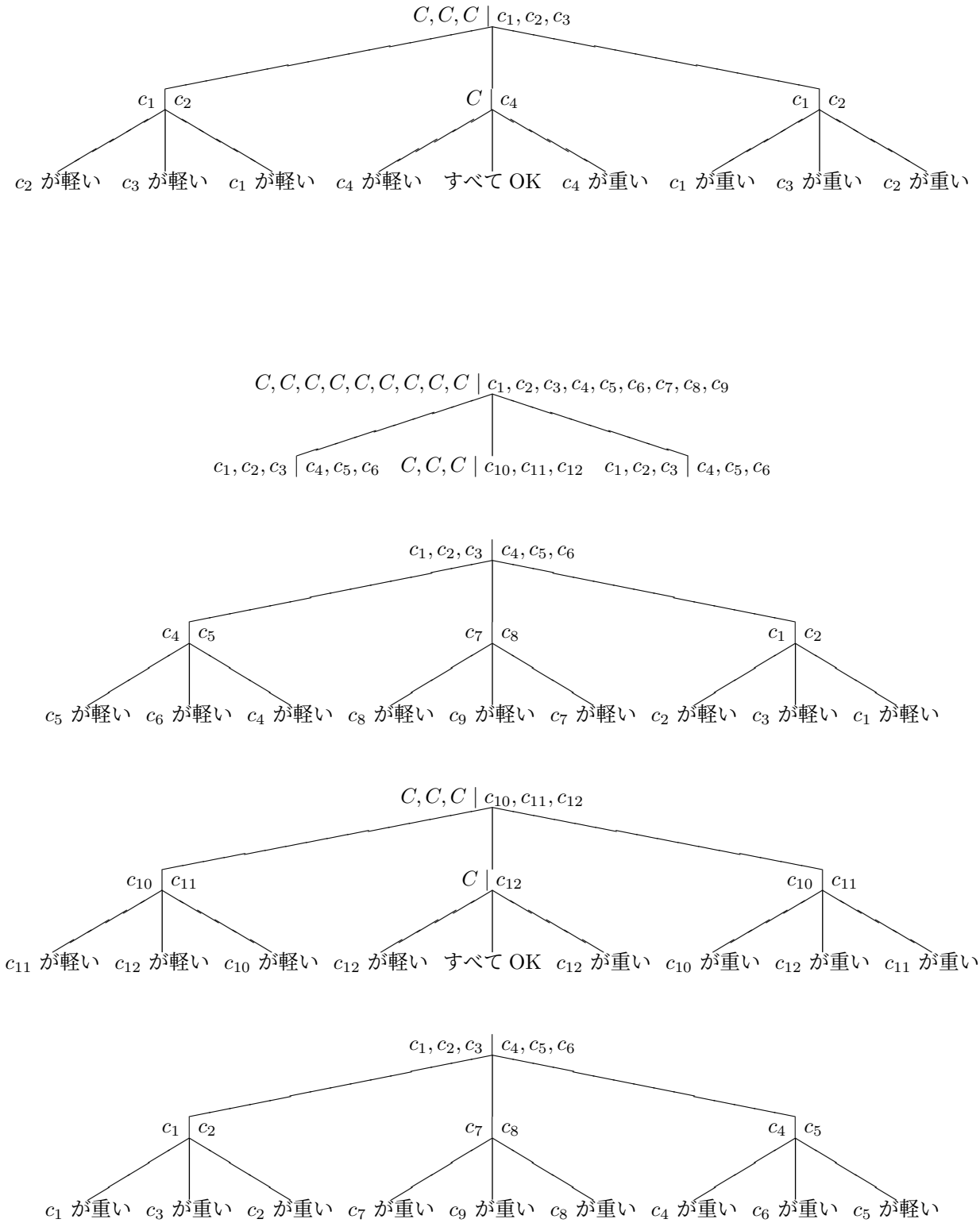


図 6: $n = 4$ および $n = 13$ に対する “枝分かれのない” アルゴリズム

よって $\mathbf{b}$ は $\mathbf{c}/\mathbf{a}=\dfrac{1}{(1-5z)(1+3z+2z^2)}$ となる。

9.12: (a) 原子炉内の各粒子は、1 秒ごとに分裂し 2 つの粒子になるとする。また、時刻 $t=0$ で始まり、1 秒ごとに 1 つの粒子が原子炉内に放出されるとする。この時、時刻 n ではどのくらいの粒子が存在するか。
(b) 1 つの粒子が分裂し 2 つになる時、1 つは、実際、もとの粒子であり、もう 1 つは新たに作られた粒子である。粒子の寿命は 10 秒であるとする。すなわち、粒子は作られてから、10 秒後には消滅してしまう。放出された全ての粒子を新たに作られた粒子とみなし、(a) と同じことを考えよ。

略解: (a) 時刻 n での粒子数を a_n とすると $a_n = 2a_{n-1}+1$, $a_0=0$ と書ける。辺々 z^n をかけて $n=1$ からの無限和をとると、

$$\mathbf{a} - a_0 = 2z\,\mathbf{a} + \frac{1}{1-z} \tag{32}$$

となる。よって $\mathbf{a} = \dfrac{1}{(1-2z)(1-z)} = \dfrac{2}{1-2z} - \dfrac{1}{1-z}$ より $a_n = 2^n - 1$。
(b) 時刻 n に新しく作られる粒子の個数を b_n とすると、$t=9$ までは $b_n = a_n$ で $t=10$ 以降は $b_n = b_{n-1}+b_{n-2}+\ldots+b_{n-9}+1$ となる。b_n の母関数を $\mathbf{b}$, $c_0=c_1=\ldots=c_9=1$, $c_n=0$ $(n\geq 10)$ なる c_n の母関数を $\mathbf{c}$ と置くと、

$$2b_n = b_n + b_{n-1} + b_{n-2} + \ldots + b_{n-9} + 1 \tag{33}$$

$$\text{よって} \qquad 2\,\mathbf{b} = \mathbf{b}\,\mathbf{c} + \frac{1}{1-z} \tag{34}$$

と書ける。時刻 n での粒子数 a'_n の母関数は $\mathbf{bc}$ と書けるから

$$\mathbf{a}' = \mathbf{b}\,\mathbf{c} = \frac{1}{1-z}\,\frac{1+z+z^2+\ldots+z^9}{1-z-z^2-\ldots-z^9} \tag{35}$$

a'_n と b_n の直接の関係を記述すると、

$$b_n = a'_{n-1} - a'_{n-11} \tag{36}$$

$$a'_n = a'_{n-1} + b_{n-1} \tag{37}$$

よって $a'_n = a'_{n-1} + a'_{n-2} - a'_{n-12}$ となる。この漸化式に対する特性方程式は $t^{12}-t^{11}-t^{10}+1=0$。これを解けば一般項が求められる。

参考: $O(\bullet)$, $\Omega(\bullet)$, $\Theta(\bullet)$ **と** $O(\bullet)$, $o(\bullet)$　計算量のオーダでは次のような表記も用いられる。

$$g = o(f) \iff \lim_{n\to\infty}\frac{g}{f} = 0 \tag{38}$$

$$g = O(f) \iff \lim_{n\to\infty}\frac{g}{f} \text{ が有界} \tag{39}$$

10　漸化式と再帰的アルゴリズム

- 1996 年度の勉強会でやった問題: 13, 16
- 1997 年度の勉強会でやった問題: 22, 27
- 1998 年度の勉強会でやった問題: 11, 28, 29
- 1999 年度の勉強会でやった問題: 20, 30, 36

10.13: 電話を通して、r 人の人々の間にゴシップが広がるとする。A と B の間の 1 回の通話で、A は自分の自分の聞いたすべてのゴシップを B に伝え、B も自分の聞いたすべてのゴシップを A に伝える。r 人の人々の間で、すべてのゴシップが、すべての人々に伝わるのに必要な最小通話数を a_r で表す。(a) $a_2=1$, $a_3=3$, $a_4=4$ を示せ。(b) $a_r \leq a_{r-1}+2$ を示せ。(c) $r\geq 4$ のとき $a_r \leq 2r-4$ を示せ。

解答 (b): r 人の時にすべての人々にすべてのゴシップを伝えるひとつの方法は、まず A が B と通話して B の持っているすべてのゴシップを受取り、B 以外の $r-1$ 人の間で互いのゴシップを交換しあう (この状態で B 以外の人はすべてのゴシップを知っている)。最後に A が他の人から受け取ったゴシップを B に伝えてやることで全員がすべてのゴシップを知ることができる。この時の通話総数は $a_{r-1}+2$ であるから、$a_r \geq a_{r-1}+2$ である。

11 群と環

- 1996 年度の勉強会でやった問題: 14, 29, 35, 48, 49
- 1997 年度の勉強会でやった問題: 16, 34, 43
- 1998 年度の勉強会でやった問題: 13, 19, 26, 51
- 1999 年度の勉強会でやった問題: 6, 28, 39, 50

11.14: 中心的亜群 (central groupoid) とは、2 項演算 $*$ を持つ代数系 $(A,*)$ で、A の任意の要素 a, b, c に対して、次の式が成り立つものをいう。

$$(a*b)*(b*c)=b \tag{40}$$

(a) 中心的亜群では、次の式が成り立つことを示せ。

$$a*((a*b)*c) = a*b \tag{41}$$

$$(a*(b*c))*c = b*c \tag{42}$$

(b) $(A,*)$ を代数系とする。ただし、$*$ は 2 項関係で、A の任意の要素 a, b, c, d に対して、次の式が成り立つとする。

$$(a*((b*c)*d))*(c*d)=c \tag{43}$$

このとき、$(A,*)$ は中心的亜群であることを示せ。
(c) 4 つの頂点を持つ有向グラフで、任意の 2 頂点の間に、長さ 2 の道が 1 個だけ存在するものをつくれ。
(d) $G=(V,E)$ は有向グラフで、任意の 2 頂点の間に、長さ 2 の道が 1 個だけ存在するものとする。V の任意の 2 つの要素 a, b に対して、a から b への長さ 2 の道に含まれる 2 つの辺を (a,c), (c,b) とする。このとき、代数系 $(V,*)$ を $a*b=c$ によって定義する。$(V,*)$ は中心的亜群であることを示せ。
(e) $(A,*)$ を中心的亜群とする。有向グラフ $G=(A,E)$ を次のように構成する。辺 (a,c) が E に含まれるのは、$a*b=c$ をみたす要素 b が存在するときかつこのときに限る。このとき、A の任意の 2 つの頂点の間には、長さ 2 の道がちょうど 1 個だけ存在することを示せ。
(f) $(A,*)$ を中心的亜群とし、この亜群に対応する (e) で定義した有向グラフを $G=(A,E)$ とする。$a\in A$ に対して、

$$R(a) = \{b \mid (a,b)\in E\} \tag{44}$$

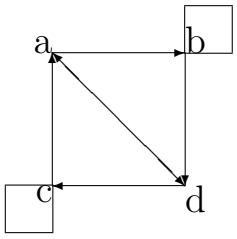
$$L(a) = \{b \mid (b,a)\in E\} \tag{45}$$

とおく。A の任意の要素 a, b に対して、$R(a)$ と $L(b)$ の要素の個数は等しいことを示せ。また、$R(a)$ と $R(b)$ の要素の個数も等しいことを示せ。
(g) $(A,*)$ を中心的亜群とする。A の要素の個数は、ある整数 m に対して m^2 であることを示せ。

略解: (a) 式 $((x*a)*(a*b))*((a*b)*c)$ を考える。第一項は式 (40) より $(x*a)*(a*b)=a$ であるから、

$$((x*a)*(a*b))*((a*b)*c)=a*((a*b)*c) \tag{46}$$

他方、$(x*a)$ を y とおけば、$((x*a)*(a*b))*((a*b)*c)=(y*(a*b))*((a*b)*c)=a*b$ であるから、$((x*a)*(a*b))*((a*b)*c)=a*((a*b)*c)=a*b$ となる。



$*$	a	b	c	d
a	d	b	d	b
b	d	b	d	b
c	c	a	c	a
d	c	a	c	a

図 7: 中心的亜群と対応するグラフの例 (b と c は自分自身への辺を持つ)

(b) 与えられた式 (43) の c に $c' * b$ を代入すれば、

$$(a * ((b * (b * c')) * d)) * ((b * c') * d) = b * c' \tag{47}$$

よって、

$$\begin{aligned}(b * c') * (c' * d) &= ((a * ((b * (b * c')) * d)) * ((b * c') * d)) * (c' * d) &(48)\\ &= (a' * ((b * c') * d)) * (c' * d) &(49)\\ &= c' &(50)\end{aligned}$$

式 (48) から式 (49) は、$a * ((b * (b * c')) * d) = a'$ と置いた。

(c) 例えば図 7 左のグラフは、題意を満たす。このグラフに対して問題のような対応を考えた時の演算表は、図 7 右のようになる。

(d) 代数系の構成の仕方から「$a \to c \to b$ なる道が存在 $\Leftrightarrow a * b = c$」である。任意の三つの頂点 a, b, c について $a * b = d$, $b * c = e$ だったとすると、$a \to d \to b \to e \to c$ なる道があることがわかる。つまり $d \to b \to e$ なる道があることから $d * e = b$ すなわち $(a * b) * (b * c) = b$ である。

(e) 任意の三つの要素 a, b, c について「$a * b = c \Rightarrow a \to c \to b$ なる道が存在する」がいえる。(辺 $a \to c$ が存在するのはグラフの定義から。辺 $c \to b$ が存在するのは、元の代数系が中心的亜群であることから $(a*b)*(b*c) = b$ すなわち $c*(b*c) = b$ であるから。) 逆に $a \to c \to b$ の時は、定義から $\exists x.a * x = c$ かつ $\exists y.c * y = b$ が成り立つ。さらに a, x, y について (a) の結果から $a * x = a * ((a * x) * y)$ すなわち $c = a * b$ でなければならない。

(f) まず、任意の $x \in R(a)$ に対して、$x * b \in L(b)$ である。(なぜなら適当な u に対して $b * u$ なる値を考えると、$(x * b) * (b * u) = b$ であるから) よって、$R(a) \subseteq L(b)$ がいえる。同様に、任意の $y \in L(b)$ に対して、$a * y \in R(a)$ である。($a * y = v$ とおくと $v \in R(a)$ であるから) よって、$L(b) \subseteq R(a)$。以上より $R(a) = L(b)$ である。また、$a = b$ のとき $R(a) = L(a)$ であるから、$R(a) = R(b)$ もいえる。

(g) (f) で定義した $R(a)$ の要素の個数を m とし、$R(a) = \{b_1, b_2, \ldots, b_m\}$ とする。この時、互いに異なるどの二つ b_i, b_j についても $R(b_i) \cap R(b_j)$ である。(もし、$c \in R(b_i) \cap R(b_j)$ ならば a と c の間に b_i もしくは b_j を通る二つの長さ 2 の道が存在することになり、(e) の結果と矛盾する。) さらにどの $R(b_i)$ も 要素の個数は m であるから、A は m^2 個の要素を持つ。

11.16: (a) 2 個の要素からなる群は、必ず $(Z_2, \oplus)$ に同型であることを示せ。

(b) 3 個の要素からなる群は、必ず $(Z_3, \oplus)$ に同型であることを示せ。

(c) 4 個の要素からなる群は、同型を除いていくつあるか。

解答: 群は必ず単位元を含むので、2 個および 3 個の要素をそれぞれ $\{e, a\}$, $\{e, a, b\}$ (e は単位元) とおいて演算表を作る。群の逆元の存在から、$xy = xz \Longleftrightarrow y = z$ が言えるので、演算表の各行・各列には同じ元はちょうど一回しか現れないことに注意すると、それぞれ表 1 のものしかあり得ないことがわかる。要素数 4 の場合も同様にしらみつぶしに調べると 4 通りしかないことがわかる。

$+$	e	a
e	e	a
a	a	e

$+$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

表 1: 要素数 2 および 3 の群

11.29: $(A, *)$ を群とする。A の任意の要素 a, b に対し、$a^3 * b^3 = (a*b)^3$, $a^4 * b^4 = (a*b)^4$, かつ $a^5 * b^5 = (a*b)^5$ が成り立てば、$(A, *)$ はアーベル群となることを示せ。

解答: 与えられた各式の辺々に左右から a^{-1}, b^{-1} をかけてやると、

$$a^2b^2 = (ba)^2 \tag{51}$$
$$a^3b^3 = (ba)^3 \tag{52}$$
$$a^4b^4 = (ba)^4 \tag{53}$$

を得る。これらより、$(ba)^6 = a^3b^3a^3b^3 = a^2b^2a^4b^4$ すなわち $ab^3a^3 = b^2a^4b$ となる。これより、

$$ab^3a^3 = b^2a^4b \tag{54}$$
$$aababab = abababaab \tag{55}$$
$$abab = baba = aabb \tag{56}$$

式 (54) では b^3a^3 及び b^2a^2 を書き換えた。よって $ba = ab$ が得られる。

11.34: $(H, *)$, $(K, *)$ を群 $(G, *)$ の部分群とする。$H \times K$ から G への関数 f を、H の任意の要素 h と K の任意の要素 k に対して、$f[(h, k)] = h * k$ で定める。このとき、f が $(H, *)$ と $(K, *)$ の直積から $(G, *)$ への同型写像となるのは、次の条件をみたすときかつこのときに限ることを示せ。

1. H と K は正規部分群である。
2. $\{h * k \mid h \in H, k \in K\} = G$
3. $H \cap K = \{e\}$, ただし、e は単位元である。

解答: 問題では $H \times K$ 上の演算が定義されていないが、次のように $+$ として定義することにする。

$$\forall\, h_1, h_2 \in H, k_1, k_2 \in K : (h_1, k_1) + (h_2, k_2) = (h_1 * h_2, k_1 * k_2) \tag{57}$$

$\Longrightarrow$: $f[(h_1, k_1) + (h_2, k_2)] = f[(h_1, k_1)] * f[(h_2, k_2)]$ より、$h_1 * h_2 * k_1 * k_2 = h_1 * k_1 * h_2 * k_2$。すなわち $\forall h \in H, \forall k \in K : h * k = k * h$ が成り立つ。k を固定して考えると、これは任意の $k \in K$ に対して $kH = Hk$ を意味する。

他方、f が同型写像であることから、任意の $x \in G$ に対して $x = h * k$ なる $h \in H$, $k \in K$ が存在する。$h \in H \Longleftrightarrow h^{-1} \in H$ より、H の x に関する左剰余類を考えると、

$$xH = (hk)H = h(Hk) = H'k, \qquad Hk = kH = khh^{-1}H = xH', \qquad \text{i.e. } xH = Hk = kH \tag{58}$$

また H の x に関する右剰余類を考えると、

$$Hx = H(hk) = H'k, \qquad Hk = Hh^{-1}hk = H'x, \qquad \text{i.e. } Hx = kH \tag{59}$$

よって $xH = Hx$、すなわち H は G の正規部分群である。また $H \cap K$ が単位元以外の元 x を含むとすると、$H \times K$ の二つの異なる元 (e, x) と (x, e) がどちらも x に写像されることになるので、f が同型写像であることと矛盾する。

$\Longleftarrow$: H, K が G の正規部分群であることから、$\forall h \in H, \forall k \in K : \exists h' \in H, \exists k' \in K$ s.t. $h*k = k'*h = k*h'$ が成り立つ。最後の $k'*h = k*h'$ より $k^{-1}k' = h'h^{-1}$。$K \cap H = \{e\}$ であるから、$k^{-1}k' = h'h^{-1} = e$ すなわち $k' = k$, $h' = h$。よって、任意の $h \in H$, $k \in K$ に対して $h*k = k*h$ が成り立つ。これから $f[(h_1, k_1) + (h_2, k_2)] = f[(h_1, k_1)] * f[(h_2, k_2)]$ が成り立つ。

11.35: $(H, *)$ を群 $(G, *)$ の正規部分群とする。部分群 $(H, *)$ によって誘導される $(G, *)$ の準同型写像がアーベル群となるのは、G の任意の要素 a, b に対して、$a*b*a^{-1}*b^{-1}$ が H に含まれるときかつこのときに限ることを示せ。

解答: G の各要素 $a \in G$ に対して、H の (左) 剰余類 $aH = \{a * H \,|\, h \in H\}$ は G を分割する。これらを $G/H = \{aH \,|\, a \in G\}$ と書くことにする。(問題の "準同型像" とはこの G/H のことで、写像 $f : a \mapsto aH \in G/H$ を考えていることになる) G/H 上の演算 $\bullet$ を次のように定義する。

$$aH \bullet bH = cH \quad \Leftrightarrow \quad \exists x \in aH \; \exists y \in bH \text{ s.t. } x * y \in cH \tag{60}$$

上の定義は代表元 x, y のとり方によらないことに注意。代数系 $(G/H, \bullet)$ がアーベル群であること、すなわち次の 5 つを示せばよい。

1. $\bullet$ は G/H において閉じている。
2. $\bullet$ は結合則を満たす。
3. $\bullet$ に関して単位元が存在する。
4. 任意の $aH \in G/H$ に対して逆元が存在する。
5. $\bullet$ が可換である。

演算が閉じていること、および結合則が成り立つことは $(G, *)$ が群であることから明らかである。また、eH が単位元であることは、H が G の正規部分群であることから次のように示せる。

$$eh_1 * ah_2 = eah_1'h_2 = ah_3 \tag{61}$$

逆元の存在についても、aH に対して $(a^{-1})H$ をとればよいので明らかである。さらに、$\bullet$ が可換であることは、G/H の任意の二つの元の要素 xh_1 と yh_2 に対して、$(xh_1) * (yh_2)$ と $(yh_2) * (xh_1)$ が同じ分割に含まれることをいえばよい。まず、H が正規部分群であることから、任意の $h \in H, y \in G$ に対して、$hy = yh'$ なる $h' \in H$ が存在する。特に $h = xyx^{-1}y^{-1}$ とする。この時、(yH については代表元として yh' をとることにすると)

$$\begin{aligned} yh' * xh_1 &= hyxh_1 && (62)\\ &= xyx^{-1}y^{-1}yxh_1 && (63)\\ &= xyh_1 \in (xy)H && (64) \end{aligned}$$

となる。同様に $xh_1 * yh_2$ についても $(xy)H \in G/H$ に含まれることがわかるので、$\bullet$ は可換である。

11.48: $n \times n$ **ラテン方陣** (Latin square) とは、n 個の異なる記号を $n \times n$ の行列の形に並べ、どの記号も各行、各列に 1 回以下しか現れないようにしたものである。ラテン方陣 A に対して、第 i 行、第 j 列の要素を a_{ij} で表すことにする。2 つの $n \times n$ ラテン方陣 A, B は、$a_{ij} = a_{kl}$, $b_{ij} = b_{kl}$ がともに成り立つような i, j, k, l が 1 組も存在しないとき、**直交している** (orthogonal) という。ラテン方陣の集合は、それらのうちの任意の 2 つの要素が直交しているとき、直交しているという。

(a) 4×4 ラテン方陣をつくれ。

(b) 直交する 2 つの 3×3 ラテン方陣をつくれ。

(c) $(\{b_0, b_1, \ldots, b_{n-1}\}, +, \cdot)$ を体とする。ただし、b_0 は加法に関する単位元である。次のような $(n-1)$ 個の $n \times n$ 方陣 $A_1, A_2, \ldots, A_{n-1}$ をつくるとする。

$$a_{ij}^{(r)} = b_r \cdot b_i + b_j \qquad \begin{matrix} i, j = 0, 1, 2, \ldots, n-1 \\ r = 1, 2, \ldots, n-1 \end{matrix} \tag{65}$$

a	b	c	d
b	c	d	a
c	d	a	b
d	a	b	c

a	b	c
b	c	a
c	a	b

a	b	c
c	a	b
b	c	a

図 8: 4×4 ラテン方陣と、直交する二つの 3×3 ラテン方陣

ただし、$a_{ij}^{(r)}$ は方陣 A_r の第 ij 要素を表わす。どの方陣もラテン方陣であることを示せ。このラテン方陣の集合は直交していることを示せ。

解答: **(a),(b)** 図 8 の通り。

(c) $a_{ij}^{(r)} = b_r \cdot b_i + b_j$ であるから、もし同じ方陣の同じ行の二つの要素 $a_{ij}^{(r)}$ と $a_{kj}^{(r)}$ が一致したとすると、$b_i = b_k$ でなければならず、矛盾する。行についても同様。直交性については、ある r について $a_{ij}^{(r)} = a_{kl}^{(r)}$ なる任意の i, j, k, l について、別の r' については $a_{ij}^{(r')} \neq a_{kl}^{(r')}$ であることを示せばよい。最初の式から、

$$b_r b_i + b_j = b_r b_k + b_l \tag{66}$$

$$b_r(b_i - b_k) = b_l - b_j \tag{67}$$

$$b_r = (b_l - b_j)/(b_i - b_k) \tag{68}$$

である。もし $a_{ij}^{(r')} = a_{kl}^{(r')}$ とすると (同様の計算から) $b_{r'} = b_r$ となって $r \neq r'$ に矛盾する。よって $a_{ij}^{(r')} \neq a_{kl}^{(r')}$ である。

11.49: 環 $(A, +, \cdot)$ は、$(A, \cdot)$ が可換モノイドであるとき、**単位元を持つ可換環** (commutative ring with unity) とよばれる。

(a) 環のイデアル H が次の性質を持つとき、**素イデアル** (prime ideal) とよばれる。H に含まれない任意の 2 つの要素 a, b に対して、$a \cdot b$ もまた H に含まれない。単位元を持つ可換環のあるイデアルから誘導される準同型像が整域となるのは、そのイデアルが素イデアルのときかつそのときに限ることを示せ。

(b) イデアル H は、その環のイデアルで H を含むものが H とその環自身以外に存在しないとき、**極大イデアル** (maximal ideal) とよばれる。単位元を持つ可換環のあるイデアルから誘導される準同型像が体となるのは、そのイデアルが極大イデアルのときかつこのときに限ることを示せ。

解答: 群 $(A, +)$ において、$a \in A$ に関する H の (左) 剰余類を $aH = \{a + h \,|\, h \in H\}$ と書くことにする。環 $(A, +, \cdot)$ のイデアル H から誘導される準同型像とは、H の (左) 剰余類の集合 $A/H = \{aH \,|\, a \in A\}$ のことである。この上に二つの演算 $\oplus$ と $\odot$ を次のように定義する。

$$aH \oplus bH = cH \quad \Leftrightarrow \quad \exists x \in aH, \exists y \in bH \text{ s.t. } x + y \in cH \tag{69}$$

$$aH \odot bH = cH \quad \Leftrightarrow \quad \exists x \in aH, \exists y \in bH \text{ s.t. } x \cdot y \in cH \tag{70}$$

(a) 代数系 $(A/H, \oplus, \odot)$ において、$\oplus$ の単位元は H であるから、これが整域となることを示すには、次の三つを示せばよい。

1. $(A/H, \oplus)$ は可換群である。($(A, +, \cdot)$ が環、すなわち $(A, +)$ が可換群であることから明らか)
2. $\odot$ は可換で、かつ $cH \neq H$ なる cH に対して $cH \odot aH = cH \odot bH$ ならば $aH = bH$ が成り立つ。
3. $\odot$ は $\oplus$ に関して分配的である。($(A, +, \cdot)$ が環であることから明らか)

二つ目を示すために、$z \in cH$, $x \in aH$, $y \in bH$ とおく。$z \cdot x = z \cdot y$ より、$z \cdot (x - y) = 0 \in H$ と書ける。問題の条件 $\forall a, b : a \notin H \wedge b \notin H \Rightarrow a \cdot b \notin H$ より z または $x - y$ のどちらかは H の要素である。cH は H ではないので $z \notin H$, よって $x - y \in H$ である。すなわち $x \in yH = bH$ となり、$aH = bH$ である。

(b) 代数系 $(A/H, \oplus, \odot)$ において、$\oplus$ の単位元は H であるから、これが体となることを示すには次の三つを示せばよい。

1. $(A/H, \oplus)$ は可換群である。($(A, +, \cdot)$ が環、すなわち $(A, +)$ が可換群であることから明らか)
2. $(A/H - \{H\}, \odot)$ は可換群である。
3. $\odot$ は $\oplus$ に関して分配的である。($(A, +, \cdot)$ が環であることから明らか)

二つ目を示すためには、(1) $\odot$ が単位元をもち、(2) 任意の $aH \neq H$ に対して $\odot$ に関する逆元が存在し、(3) $\odot$ が可換である、の三つを示す必要がある。(1) に関しては、$(A, \cdot)$ の単位元を 1 とすると (可換モノイドであるからこれは存在する)、あきらかに $1H$ が単位元になる。

(2) に関してはまず、$x \notin H$ なる x を一つとり、$H' := \{h + a \cdot x \mid h \in H, a \in A\}$ という集合を考える。もし、$1 \notin H'$ ならば、$H' \supset H$ がイデアルになって H の極大性に矛盾することを示す。任意の $b \in A$ と任意の $y \in H'$ に対して、

$$\begin{aligned} b \cdot y &= b \cdot (h + a \cdot x) = b \cdot h + b \cdot (a \cdot x) && (71) \\ &= h' + a' \cdot x \in H' \qquad (h' \in H,\ a' \in A) && (72) \end{aligned}$$

と書けるので、H' はイデアルであり、$1 \notin H'$ であるから $H' \neq A$ である。[1] 以上より、任意の $a \notin H$ に対してある $h \in H$ と $b \in A$ が存在して $h + a \cdot b = 1$ となることが分かる。すなわち、任意の $a \notin H$ に対して $aH \odot bH = 1H$ となる $b \in A$ が存在することがいえた。

(3) に関しては、$(A, \cdot)$ が可換モノイドであることから明らか。

11.13: $(A, *)$ を次のような代数系とする。A の任意の要素 a, b に対して、

$$\begin{aligned} (a * b) * a &= a && (73) \\ (a * b) * b &= (ba)a && (74) \end{aligned}$$

が成立する。

(c) 任意の a, b に対して、$a * a = b * b$ を示せ。

解答 問題の式 (73), (74) を $*$ を省略し、変数を変えて書き直すと、

$$\begin{aligned} (xy)x &= x && (75) \\ (xy)y &= (yx)x && (76) \end{aligned}$$

となる。(75) の x に ab を、y に a をそれぞれ代入すると、

$$\begin{aligned} \{(ab)a\}(ab) &= ab \qquad && (ab)a = a \text{ より} \\ a(ab) &= ab \end{aligned}$$

同様に、(76) の x に a を、y に ab をそれぞれ代入すると、

$$\begin{aligned} \{a(ab)\}(ab) &= \{(ab)a\}a \qquad && a(ab) = ab \text{ より} \\ (ab)(ab) &= aa \\ \text{すなわち} \qquad (xy)(xy) &= xx \end{aligned}$$

が得られる。ここで、$\{(ab)b\}\{(ab)b\}$ という式を考えると、

$$\begin{aligned} \{(ab)b\}\{(ab)b\} &= (ab)(ab) = aa && (xy)(xy) = xx \text{ より} \\ &= \{(ba)a\}\{(ba)a\} && \text{式 (76) より} \\ &= (ba)(ba) = bb && (xy)(xy) = xx \text{ より} \end{aligned}$$

[1] 逆にイデアル H が 1 を含むときは、任意の $a \in A$ に対して $a \cdot 1 = a \in H$ でなければならないので、$H = A$ となることに注意。

12 ブール代数

- 1996 年度の勉強会でやった問題: 21, 22, 23, 27
- 1997 年度の勉強会でやった問題: 17, 24, 25
- 1998 年度の勉強会でやった問題: 10, 18, 19
- 1999 年度の勉強会でやった問題: 11, 13, 24

12.10: 束 $(A, \leq)$ が**モジュラ束** (modular lattice) とは、$a \leq c$ なる A の任意の要素 a, b, c に対して $a \vee (b \wedge c) = (a \vee b) \wedge c$ が成立することである。

束がモジュラーであることと、

$$a \vee (b \wedge (a \vee c)) = (a \vee b) \wedge (a \vee c) \tag{77}$$

が成立することとは同値であることを証明せよ。

解答: $a \leq a \vee c$ であるから、$(A, \leq)$ がモジュラー束ならば与式の c に $a \vee c$ $(\geq a)$ を代入すれば式 (77) が得られる。逆に、任意の a, b, c に対して式 (77) が成立すると仮定すると、$a \leq c$ ならば $a \vee c = c$ なので、式 (77) は

$$a \vee (b \wedge c) = (a \vee b) \wedge c \tag{78}$$

となり、$(A, \leq)$ はモジュラー束となる。

12.11: モジュラー束の任意の要素 a, b, c について、

$$(a \vee b) \wedge c = b \wedge c \tag{79}$$

が成立するならば、

$$(c \vee b) \wedge a = b \wedge a \tag{80}$$

が成立することを示せ。(テキスト中では式 (80) の右辺が $\wedge$ ではなく $\vee$ になっているが、誤植であろう)

解答: 任意の x,y,z に対して $x \vee (y \wedge (x \vee z)) = (x \vee y) \wedge (x \vee z)$ が成り立つこと (問題 12.10 より) と、$(a \vee b) \wedge c = b \wedge c$ の二つから $(c \vee b) \wedge a = b \wedge a$ を示せばよい。

12.13: $(A, \leq)$ を分配束とし、a と b を A の任意の 2 つの要素とする。$I(a, b)$ を次のような集合とする。

$$I(a, b) = \{x \mid x \in A, a \wedge x = b \wedge x\} \tag{81}$$

$I(a, b)$ はイデアルであることを示せ (イデアルの定義については問題 12.12 を参照)。

解答: A の部分集合 I がイデアルであるとは次の二つの条件が成り立つことである。

1. I の任意の要素 a, b に対して、$a \vee b$ も I の要素である。
2. I の任意の要素 a と A の任意の要素 x に対して、$a \wedge x$ も I の要素である。

最初の条件については、$c, d \in I$ とすると I の定義から

$$a \wedge c = b \wedge c, \qquad a \wedge d = b \wedge d \tag{82}$$

が成り立つ。よって $c \vee d$ に対して、

$$\begin{aligned} a \wedge (c \vee d) &= (a \wedge c) \vee (a \wedge d) \qquad (A \text{ が分配束であることから}) && (83)\\ &= (b \wedge c) \vee (b \wedge d) \qquad (I \text{ の定義から}) && (84)\\ &= b \wedge (c \vee d) && (85) \end{aligned}$$

となるので、$c \vee d$ は I の要素である。

二つ目の条件については、$c \in I$, $x \in A$ とすると $c \wedge x$ に対して、

$$\begin{aligned} a \wedge (c \wedge x) &= (a \wedge c) \wedge x && (86)\\ &= (b \wedge c) \wedge x \qquad (c \in I \text{ より}) && (87)\\ &= b \wedge (c \wedge x) && (88) \end{aligned}$$

となるので $c \wedge x$ は I の要素である。

12.24: 12.7 節において、2 値ブール代数上のブール表現に対する加法標準形と乗法標準形を定めた。この問題において、これらの概念が一般のブール代数に拡張できることを示す。$E(x_1, x_2, \ldots, x_n)$ をブール代数 $(A, \vee, \wedge, ^-)$ 上のブール表現とする。$E(x_1, x_2, \ldots, x_n)$ の x_i に A の要素 a を代入したブール表現を $E(x_i = a)$ で表わす。

(a) 任意の x_i に対して、次の等式を示せ。

$$E(x_1, x_2, \ldots, x_n) = (\bar{x}_i \wedge E(x_i = 0)) \vee (x_i \wedge E(x_i = 1)) \tag{89}$$

ヒント: 与式の成立することは、表現 $E(x_1, x_2, \ldots, x_n)$ の長さに関する帰納法を用いて証明される。ここで、表現の長さとは、表現内に現われる A の要素の数、変数名、演算子 $\vee, \wedge, ^-$ について重複したものも数えて得られる総数のことである。したがって、長さ 1 の表現とは、A の要素と変数 $x_1, x_2, \ldots, x_n$ である。

(b) (a) の結果を用いて、$c_{\delta_1\delta_2\ldots\delta_n}$ を A の要素とし、$\tilde{x}_i$ が x_i または $\bar{x}_i$ を表わすとき、任意のブール表現は、次の形の式

$$c_{\delta_1\delta_2\ldots\delta_n} \wedge \tilde{x}_1 \wedge \tilde{x}_2 \wedge \ldots \wedge \tilde{x}_n \tag{90}$$

の結びで書き表わせることを示せ。ブール表現のこのような書き表わし方を加法標準形という。

(c) $E(x_1, x_2) = (2 \wedge x_1) \wedge (x_1 \vee \bar{x}_2)$ をブール代数 $(\{0, 1, 2, 3\}, \vee, \wedge, ^-)$ 上のブール表現とする。$E(x_1, x_2)$ を加法標準形に書き改めよ。

(d) f を、あるブール代数 $(A, \vee, \wedge, ^-)$ における A^n から A への関数とする。もし、f がブール関数ならば、どのようにして関数 f を表示するブール表現を決定できるか。
ヒント: その表現の加法標準形を考えよ。

(e) 図 12.8 に示される関数がブール関数でないことを示せ。

	f		f		f		f
(0,0)	1	(1,0)	1	(2,0)	2	(3,0)	3
(0,1)	0	(1,1)	1	(2,1)	0	(3,1)	0
(0,2)	0	(1,2)	0	(2,2)	1	(3,2)	0
(0,3)	3	(1,3)	3	(2,3)	1	(3,3)	2

図 12.8

(f) 任意の x_i について、次の等式が成り立つことを示せ。

$$E(x_1, x_2, \ldots, x_n) = (x_i \vee E(x_i = 0)) \wedge (\bar{x}_i \vee E(x_i = 1)) \tag{91}$$

(g) (f) の結果を用いて、$d_{\delta_1\delta_2\ldots\delta_n}$ を A の要素とし、$\tilde{x}_i$ が x_i または $\bar{x}_i$ を表わすとき、任意のブール表現は、次の形の式

$$c_{\delta_1\delta_2\ldots\delta_n} \vee \tilde{x}_1 \vee \tilde{x}_2 \vee \ldots \vee \tilde{x}_n \tag{92}$$

の交わりで書き表わせることを示せ。ブール表現のこのような書き表わし方を乗法標準形という。

解答: (a) 表現 $E(x_1, x_2, \ldots, x_n)$ の長さ k に関する数学的帰納法によって証明する。

1. $k = 1$ の時: $E(x_1, x_2, \ldots, x_n) = x_j$ または $E(x_1, x_2, \ldots, x_n) = c$ である ($1 \le j \le n$, c は A の定数)。この時、与式が成り立つのは明らかである (例えば $E(x_1, x_2, \ldots, x_n) = x_1$ として $i = 2$ とすると、$E(x_2 = 0) = E(x_2 = 1) = x_1$ であるから、$(\bar{x}_2 \wedge E(x_2 = 0)) \vee (x_2 \wedge E(x_2 = 1)) = (\bar{x}_2 \wedge x_1) \vee (x_2 \wedge x_1) = (\bar{x}_2 \vee x_2) \wedge x_1 = x_1$ である)。

2. $k \leq m$ の全てに対して与式が成り立つと仮定する。まず、

$E(x_i = 0) \neq E(x_i = 1)$ ならば $E(x_i = 0) \vee E(x_i = 1) = 1$

であることに注意 (これも E の長さに関する数学的帰納法で証明できる)。この時、

- $E(x_1, x_2, \ldots, x_n) = \overline{E'(x_1, x_2, \ldots, x_n)}$ (E' は長さ m 以下) とする。$E'(x_i = 0) = E'(x_i = 1)$ ならば、$k = 1$ の場合の例と同様に与式は成り立つ。$E'(x_i = 0) \neq E'(x_i = 1)$ の時は、

$$E' = (\bar{x}_i \wedge E'(x_i = 0)) \vee (x_i \wedge E(x_i = 1)) \tag{93}$$

と書き表わせるので、

$$\begin{aligned}
E(x_1, x_2, \ldots, x_n) &= \overline{E'(x_1, x_2, \ldots, x_n)} \\
&= \overline{(\bar{x}_i \wedge E'(x_i = 0)) \vee (x_i \wedge E(x_i = 1))} \\
&= (x_i \vee \overline{E'(x_i = 0)}) \wedge (\bar{x}_i \vee \overline{E'(x_i = 1)}) \\
&= (x_i \wedge \bar{x}_i) \vee (x_i \wedge \overline{E'(x_i = 1)}) \vee (\overline{E'(x_i = 0)} \wedge \bar{x}_i) \\
&\qquad \vee (\overline{E'(x_i = 0)} \wedge \overline{E'(x_i = 1)}) \\
&= (\bar{x}_i \wedge \overline{E'(x_i = 0)}) \vee (x_i \wedge \overline{E'(x_i = 1)}) \\
&= (\bar{x}_i \wedge \overline{E(x_i = 0)}) \vee (x_i \wedge \overline{E(x_i = 1)})
\end{aligned}$$

となり、与式が成立する。

- $E(x_1, x_2, \ldots, x_n) = E_1(x_1, x_2, \ldots, x_n) \wedge E_2(x_1, x_2, \ldots, x_n)$ (E_1, E_2 は長さ m 以下) ならば、

$$\begin{aligned}
E(x_1, x_2, \ldots, x_n) &= E_1(x_1, x_2, \ldots, x_n) \wedge E_2(x_1, x_2, \ldots, x_n) \\
&= \{(\bar{x}_i \wedge E_1(x_i = 0)) \vee (x_i \wedge E_1(x_i = 1))\} \\
&\qquad \wedge \{(\bar{x}_i \wedge E_2(x_i = 0)) \vee (x_i \wedge E_2(x_i = 1))\} \\
&= (\bar{x}_i \wedge E_1(x_i = 0) \wedge E_2(x_i = 0)) \\
&\qquad \vee (x_i \wedge \bar{x}_i \wedge E_1(x_i = 1) \wedge E_2(x_i = 0)) \\
&\qquad \vee (\bar{x}_i \wedge x_i \wedge E_1(x_i = 0) \wedge E_2(x_i = 1)) \\
&\qquad \vee (x_i \wedge E_1(x_i = 1) \wedge E_2(x_i = 1)) \\
&= (\bar{x}_i \wedge E(x_i = 0)) \vee (x_i \wedge E(x_i = 1))
\end{aligned}$$

となり、与式が成立する。

- $E(x_1, x_2, \ldots, x_n) = E_1(x_1, x_2, \ldots, x_n) \vee E_2(x_1, x_2, \ldots, x_n)$ (E_1, E_2 は長さ m 以下) ならば、

$$\begin{aligned}
E(x_1, x_2, \ldots, x_n) &= E_1(x_1, x_2, \ldots, x_n) \vee E_2(x_1, x_2, \ldots, x_n) \\
&= \{(\bar{x}_i \wedge E_1(x_i = 0)) \vee (x_i \wedge E_1(x_i = 1))\} \\
&\qquad \vee \{(\bar{x}_i \wedge E_2(x_i = 0)) \vee (x_i \wedge E_2(x_i = 1))\} \\
&= \{\bar{x}_i \wedge (E_1(x_i = 0) \vee E_2(x_i = 0))\} \\
&\qquad \vee \{x_i \wedge (E_1(x_i = 1) \vee E_2(x_i = 0))\} \\
&= (\bar{x}_i \wedge E(x_i = 0)) \vee (x_i \wedge E(x_i = 1))
\end{aligned}$$

となり、与式が成立する。

(b)

(c)

(d)

(e)

(f), (g) 問題 (a), (b) に対して双対原理を適用すれば明らか。

12.27: 5 人の候補者 a, b, c, d, e から委員が選ばれることになっている。この人選は、次の全条件をみたさなければならない。

1. a または b のどちらかを含まねばならない、しかし両方を含んではいけない。
2. c または e のどちらか、または、両方を含まねばならない。
3. もし d が含まれるならば、b も含まれねばならない。
4. a と c の両方とも含まれるか、または、両方とも含まれない。
5. もし e が含まれるならば、c と d も含まれねばならない。

この人選はどのように行なわれるべきか。

解答: a で「候補者 a が選ばれる」を表して (b, c,... も同様)、各条件を論理式で表現しそれらの積を充足させる組合せを探せばよい。

1. $(a \wedge \neg b) \vee (\neg a \wedge b)$
2. $c \vee e$
3. $d \Rightarrow b \quad (= \neg d \vee b)$
4. $(a \wedge c) \vee (\neg a \wedge \neg c)$
5. $e \Rightarrow (c \wedge d) \quad (= \neg e \vee (c \wedge d))$

これらの積を簡単化すると $a \wedge \neg b \wedge c \wedge \neg d \wedge \neg e$ となるので、a と c を選出すればよいことがわかる。

参考文献

[1] “コンピュータのための離散数学入門”, C. L. Liu 著, 成嶋 弘/秋山 仁 共訳, 1995, オーム社.

[2] “アルゴリズムとデータ構造”, 石畑清 著, 岩波講座ソフトウェア科学シリーズ 第 3 巻, 岩波書店.

[3] “計算幾何学”, 今井 浩, 今井 桂子 共著, 情報数学講座 第 12 巻, 共立出版, 1994.