■12 群（電子情報通信基礎）- 2 編（離散数学）

2 章 組合せ数学

（執筆者：松林 昭）［2009 年 6 月 受領］

■概要■

組合せ数学（combinatorial mathematics）は，有限個の対象のうちで，ある条件を満たすものの数え上げと構成にかかわる問題を扱うものである．ただし最近では，構成問題は最適化問題〔本編 4,5,6 章参照〕の枠組で取り扱われることが多い．本章では，主に数え上げにかかわる問題について述べる．

数え上げの手法は，数え上げる対象の性質と，代数・解析・幾何などで扱われる対象に内在する組合せ的構造との関連づけに基づく．それらの概要を以下に述べる．

一つの典型的な手法は，求めようとする数列を母関数，すなわち，数列の第 n 項を第 n 次項の係数としたべき級数で表現して取り扱うものである．数列の性質を導くのに多項式の代数演算ないし解析的計算手法を用いることができるようになる．

求めようとする数列 $a_1,\ldots,a_n$ が $\mathbb{R}^n$ 上の可逆な線形変換 f で別の数列 $b_1,\ldots,b_n$ に写るならば，$a_1,\ldots,a_n$ を $b_1,\ldots,b_n$ の f^{-1} の像として表すことができる．この考え方を局所有限半順序集合上に拡張したものがメビウスの反転公式であり，数論におけるメビウスの反転公式や包除原理などの一般化となっている．

数え上げに際し，同じとみなすべき 2 対象間の関係が置換群と関連づけられるならば，数え上げはその置換群が誘導する同値類の総数を求める問題に帰着できる．そのような数を求めるための有用な方法としてバーンサイドの定理やポリアの数え上げ法などが知られている．

確率的手法は，数え上げる対象を事象とする確率空間を定めたうえで条件を満たす対象の数や存在性，存在条件などを確率によって評価するものであり，近年幅広い問題に対して適用されている．

【本章の構成】

2-1 節では基本的な順列・組合せ，及びこれらと関連する 2 項定理と多項定理について述べる．更に，集合分割数の結果を示す．2-2 節では反転公式について述べる．また，メビウスの反転公式の応用例としてふるいの公式と包除原理を示す．2-3 節では母関数について述べ，よく知られるいくつかの数列を母関数を用いて求める例を示す．2-4 節では置換群によって誘導される同値類の数え上げについて述べる．2-5 節では確率的手法について，いくつかの典型的な手法を紹介する．

2-1 節から 2-4 節の内容は多くの教科書で扱われている．代表的なものには文献 1, 2, 3, 4, 5, 6) などがある．2-5 節の内容を解説している文献としては 7, 8) などがある．特に 8) では確率的手法に関する幅広い話題が扱われている．

■12 群 - 2 編 - 2 章

2-1 順列・組合せ・集合分割数

（執筆者：松林 昭）[2009 年 6 月 受領]

2-1-1 順　列

n 元集合 A の各要素を 1 回ずつ選び出し，それらを並べて得られる順序列を順列（permutation）と呼ぶ．順列の総数は全単射 $A \to A$，すなわち A 上の置換の総数と等しく，$n! = \prod_{i=1}^{n} i$ である．A から m 個の要素を 1 回ずつ選び，それらを並べて得られる順序列は A に対する長さ m の順列などと呼ばれる．その総数 ${}_n\mathrm{P}_m$ は単射 $\{1,\ldots,m\} \to A$ の総数と等しく，

$$ {}_n\mathrm{P}_m = \prod_{i=0}^{m-1}(n-i) \qquad (n \geq 0,\ m \geq 0) \tag{2·1} $$

である．式 (2·1) は $n \geq m \geq 0$ のとき ${}_n\mathrm{P}_m = n!/(n-m)!$ と表すことができ，$m > n \geq 0$ のとき ${}_n\mathrm{P}_m = 0$ である．A の各要素を 0 回以上，全体で m 回選び出し，それらを並べて得られる順序列を重複順列（permutation with repetition）と呼ぶ．重複順列の総数は写像 $\{1,\ldots,m\} \to A$ の総数と等しく，n^m である．

2-1-2 組合せ

n 元集合 A の部分集合を，特にその選び方に注目しているとき，組合せ（combination）と呼ぶ．m 個の要素からなる組合せを選ぶ方法の総数，すなわち A の m 元部分集合の総数 ${}_n\mathrm{C}_m$ は，単調増加な単射 $\{1,\ldots,m\} \to \{1,\ldots,n\}$ の総数に等しく，

$$ {}_n\mathrm{C}_m = \frac{{}_n\mathrm{P}_m}{m!} = \frac{\prod_{i=0}^{m-1}(n-i)}{m!} \qquad (n \geq 0,\ m \geq 0) \tag{2·2} $$

である．式 (2·2) は $n \geq m \geq 0$ のとき ${}_n\mathrm{C}_m = n!/(m!(n-m)!)$ と表せる．組合せ数について，次の関係が成り立つ．

$$ {}_n\mathrm{C}_m = {}_n\mathrm{C}_{n-m} \qquad (n \geq m \geq 0) \tag{2·3} $$

$$ {}_n\mathrm{C}_m = {}_{n-1}\mathrm{C}_m + {}_{n-1}\mathrm{C}_{m-1} \qquad (n \geq 1,\ m \geq 1) \tag{2·4} $$

A の各要素を 0 回以上，全体で m 回選び出して得られる多重集合（A の各要素が複数回現れることを許す集合）を重複組合せ（combination with repetition）と呼ぶ．重複組合せの総数 ${}_n\mathrm{H}_m$ は単調非減少な写像 $\{1,\ldots,m\} \to \{1,\ldots,n\}$ の総数に等しく，

$$ {}_n\mathrm{H}_m = \frac{\prod_{i=0}^{m-1}(n+m-1-i)}{m!} \qquad (n \geq 0,\ m \geq 0) \tag{2·5} $$

である．$n \geq 0$，$m \geq 0$，$n+m \geq 1$ のとき式 (2·5) は ${}_n\mathrm{H}_m = {}_{n+m-1}\mathrm{C}_m$ と表せる．

2-1-3 2 項定理と多項定理

非負整数 n に対して，n 次多項式 $(1+x)^n$ の第 i 次項 $(0 \leq i \leq n)$ は ${}_n\mathrm{C}_i x^i$ に等しい．この

事実は 2 項定理として知られる．

2 項定理（binomial theorem）：非負整数 n と実数 x に対して，

$$(1+x)^n = \sum_{i=0}^{n} {}_n\mathrm{C}_i x^i. \tag{2·6}$$

この定理に由来して ${}_n\mathrm{C}_m$ は 2 項係数（binomial coefficient）とも呼ばれ，$\binom{n}{m}$ で表されることもある．なお，2 項係数を任意の実数 y と非負整数 m に対して $\binom{y}{m} = (1/m!)\prod_{i=0}^{m-1}(y-i)$ と定義すると，$\binom{y}{m}$ は x の関数 $(1+x)^y$ のマクローリン展開における第 m 次項の係数に等しい．したがって $(1+x)^y = \sum_{i=0}^{\infty}\binom{y}{i}x^i$ が成り立ち，これは一般化 2 項定理と呼ばれる．

2 項定理を多変数多項式に一般化したものが次の定理である．

多項定理（multinomial theorem）：非負整数 n と実数 $x_1, \ldots, x_k$ に対して，

$$(x_1 + \cdots + x_k)^n = \sum_{\substack{m_1+\cdots+m_k=n \\ m_i \geq 0,\ i=1,\ldots,k}} \binom{n}{m_1, \ldots, m_k} x_1^{m_1} \cdots x_k^{m_k}. \tag{2·7}$$

ただし，$\binom{n}{m_1,\ldots,m_k}$ は多項係数（multinomial coefficient）と呼ばれ，$n!/(m_1! \cdots m_k!)$ に等しい．

多項係数は k 元集合 $\{a_1, \ldots, a_k\}$ から a_i $(1 \leq i \leq k)$ を $m_i \geq 0$ 回，全体で n 回選び出し，それらを並べて得られる順序列*の総数に等しい．

2-1-4 集合分割数

n 元集合 A を m 個の非空の集合に分割する方法の総数 $S(n,m)$ は第 2 種スターリング数（Stirling numbers of the second kind）と呼ばれ，

$$S(n,m) = \frac{1}{m!}\sum_{i=0}^{m}(-1)^{m-i}{}_m\mathrm{C}_i\, i^n \qquad (n \geq 0,\ m \geq 0) \tag{2·8}$$

で与えられる．$m > n$ のとき $S(n,m) = 0$ が成り立つ．A を非空の集合に分割する方法の総数 B_n はベル数（Bell numbers）と呼ばれ，

$$B_n = \sum_{m=0}^{\infty} S(n,m) = \frac{1}{e}\sum_{i=0}^{\infty}\frac{i^n}{i!} \qquad (n \geq 0) \tag{2·9}$$

で与えられる．

* このような順序列も重複順列（permutation with repetition）と呼ばれる．

■12 群 - 2 編 - 2 章

2-2 反転公式

（執筆者：松林 昭）[2009 年 6 月 受領]

半順序集合 $(P,\preceq)$ は，任意の $p,q\in P$ に対して $\{u\in P\mid p\preceq u\preceq q\}$ が有限集合になるとき局所有限という．最小元をもつ局所有限半順序集合 $(P,\preceq)$ に対し，次の 2 条件を満たす関数 $f:P^2\to\mathbb{R}$ 全体を $\mathcal{F}$ とする．

1. $p=q$ ならば $f(p,q)\neq 0$
2. $p\not\preceq q$ ならば $f(p,q)=0$

$p\in P$ に対して，$\{q\in P\mid q\preceq p\}=\{p_1,\ldots,p_n\}$ かつ $p_i\preceq p_j\Rightarrow i\leq j\,(1\leq i,j\leq n)$ とするとき，$m_{ij}=f(p_i,p_j)$ で定義される $n\times n$ 行列 (m_{ij}) を $M_{f,p}$ とする．$\mathcal{F}$ の条件より $M_{f,p}$ は逆行列 $(M_{f,p})^{-1}$ をもち，しかも $M_{g,p}=(M_{f,p})^{-1}$ であるような $g\in\mathcal{F}$ が存在する．したがって，P 上の関数 a,b が $a(p)=\sum_{q\preceq p}f(q,p)b(q)$ を満たすならば，$b(p)=\sum_{q\preceq p}g(q,p)a(q)$ が成り立つ．

2-2-1 2 項反転公式

2 項定理より，任意の非負整数 n と実数 x に対して $x^n=(1+(x-1))^n=\sum_{i=0}^n{}_n\mathrm{C}_i(x-1)^i$ 及び $(x-1)^n=\sum_{i=0}^n{}_n\mathrm{C}_i(-1)^{n-i}x^i$ が成り立つ．このことは，$(P,\preceq)$ として非負整数集合と $\leq$ をとり，$i,j\in P$ に対して $f(i,j)={}_j\mathrm{C}_i$ 及び $g(i,j)={}_j\mathrm{C}_i(-1)^{j-i}$ と定めると，$f,g\in\mathcal{F}$ かつ任意の $n\in P$ に対して $M_{g,n}=(M_{f,n})^{-1}$ であることを意味する．ゆえに次の公式を得る．

2 項反転公式（binomial inversion formula）：数列 $a_0,a_1,\ldots$ と $b_0,b_1,\ldots$ が $a_n=\sum_{i=0}^n{}_n\mathrm{C}_ib_i$ $(n\geq 0)$ を満たすならば，$b_n=\sum_{i=0}^n{}_n\mathrm{C}_i(-1)^{n-i}a_i$ が成り立つ．

2-2-2 スターリングの反転公式

非負整数 n に対して，x の n 次多項式 $\prod_{j=0}^{n-1}(x-j)$ の第 i 次項 $(0\leq i\leq n)$ の係数 $s(n,i)$ は第 1 種スターリング数（Stirling numbers of the first kind）と呼ばれる．すなわち，

$$\prod_{j=0}^{n-1}(x-j)=\sum_{i=0}^{n}s(n,i)x^i \tag{2・10}$$

である．2-1 節より，写像 $f:\{1,\ldots,n\}\to\{1,\ldots,m\}$ の総数は m^n である．一方，$|f(\{1,\ldots,n\})|=i$ であるような f の数は第 2 種スターリング数を用いて $S(n,i)_m\mathrm{P}_i=S(n,i)\prod_{j=0}^{i-1}(m-j)$ と表せるから，$m^n=\sum_{i=0}^n S(n,i)\prod_{j=0}^{i-1}(m-j)$ が成り立つ．これは m の多項式として恒等的に成り立つので，実数 x に対しても

$$x^n=\sum_{i=0}^{n}S(n,i)\prod_{j=0}^{i-1}(x-j) \tag{2・11}$$

が成り立つ．式 (2・10) と (2・11) は，$(P,\preceq)$ として非負整数集合と $\leq$ をとり，$i,j\in P$ に対

して $f(i,j) = s(j,i)$ 及び $g(i,j) = S(j,i)$ と定めると，$f, g \in \mathcal{F}$ かつ任意の $n \in P$ に対して $M_{g,n} = (M_{f,n})^{-1}$ であることを意味する．ゆえに次の公式を得る．

スターリングの反転公式（Stirling inversion formula）：数列 $a_0, a_1, \ldots$ と $b_0, b_1, \ldots$ が $a_n = \sum_{i=0}^{n} s(n,i) b_i$ $(n \geq 0)$ を満たすならば，$b_n = \sum_{i=0}^{n} S(n,i) a_i$ が成り立つ．

2-2-3 メビウスの反転公式

$(P, \preceq)$ を最小元をもつ局所有限半順序集合とする．$p, q \in P$ に対して，

$$\mu(p,p) = 1$$
$$\mu(p,q) = -\sum_{p \preceq u \prec q} \mu(p,u) \qquad (p \prec q)$$
$$\mu(p,q) = 0 \qquad (p \not\preceq q)$$

と再帰的に定義される関数 μ は $(P, \preceq)$ 上のメビウス関数（Möbius function）と呼ばれる．また，

$$\zeta(p,q) = 1 \qquad (p \preceq q)$$
$$\zeta(p,q) = 0 \qquad (p \not\preceq q)$$

とすると，$\mu, \zeta \in \mathcal{F}$ かつ任意の $p \in P$ に対して $M_{\zeta,p} = (M_{\mu,p})^{-1}$ が成り立つ．したがって，次の公式を得る．

メビウスの反転公式（Möbius inversion formula）：P 上の実関数 a, b が $a(p) = \sum_{q \preceq p} b(q)$ $(p \in P)$ を満たすならば，$b(p) = \sum_{q \preceq p} \mu(q,p) a(q)$ が成り立つ．

(1) 例：ふるいと包除原理

有限加法的集合関数 m をもつ集合 S を考える*．S の n 個の部分集合を $A_1, \ldots, A_n$ とし，$K = \{1, \ldots, n\}$ とする．$(2^K, \subseteq)$ は局所有限半順序集合であり，この上でメビウス関数は $J \subseteq I \subseteq K$ に対して $\mu(J,I) = (-1)^{|I-J|}$ となる．2^K 上の関数 a, b を $a(I) = m(\bigcap_{i \in K-I} A_i)$, $b(I) = m(\bigcap_{i \in K-I} A_i - \bigcup_{i \in I} A_i)$ と定義する．特に，$a(K) = m(\bigcup_{i \in K} A_i)$, $b(K) = m(\emptyset) = 0$ である．定義より $a(I) = \sum_{J \subseteq I} b(J)$ が成り立つので，メビウスの反転公式より $b(K) = \sum_{J \subseteq K} (-1)^{|K-J|} a(J) = \sum_{I \subseteq K} (-1)^{|I|} a(K-I) = m(\bigcup_{i \in K} A_i) + \sum_{\emptyset \neq I \subseteq K} (-1)^{|I|} m(\bigcap_{i \in I} A_i) = 0$ が成り立つ．ゆえに次の公式を得る．

ふるいの公式（sieve formula）：有限加法的集合関数 m をもつ集合 S，$A_1, \ldots, A_n \subseteq S$，$K = \{1, \ldots, n\}$ に対し，$m(\bigcup_{i \in K} A_i) = \sum_{\emptyset \neq I \subseteq K} (-1)^{|I|-1} m(\bigcap_{i \in I} A_i)$.

有限集合 A に対して $m(A) = |A|$ とすると，次の包除原理を得る．

包除原理（principle of inclusion-exclusion）：有限集合 $A_1, \ldots, A_n$，$K = \{1, \ldots, n\}$ に対し，$|\bigcup_{i \in K} A_i| = \sum_{\emptyset \neq I \subseteq K} (-1)^{|I|-1} |\bigcap_{i \in I} A_i|$.

---

* すなわち m は $m(\emptyset) = 0$ であるようなモジュラ関数であり，任意の $A, B \subseteq S$ に関して $m(A) + m(B) = m(A \cup B) + m(A \cap B)$ が成り立つ．

■12 群 - 2 編 - 2 章

2-3 母関数

（執筆者：松林 昭）[2009 年 6 月 受領]

数列 $a_0, a_1, \ldots$ に対して，べき級数

$$a(x) = \sum_{n=0}^{\infty} a_n x^n \tag{2・12}$$

をこの数列の母関数（generating function）と呼ぶ．数列が有限列 $a_0, \ldots, a_m$ の場合は，$n > m$ に対して $a_n = 0$ と考える．母関数の取扱いには 2 種類のアプローチがある．

2-3-1 代数的取扱い

$a(x)$ を形式的べき級数として取り扱い，級数の代数演算のみを考える．$a(x)$ の収束性が問題とならない代わりに，$a(x)$ の値を利用したり，$a(x)$ を微積分したりすることは正当でない*．

ある整数 m 未満の i に対して $a_i = 0$ であるようなべき級数 $\sum_{n=-\infty}^{\infty} a_n x^n$ 全体は，$\sum_{n=-\infty}^{\infty} b_n x^n + \sum_{n=-\infty}^{\infty} c_n x^n \equiv \sum_{n=-\infty}^{\infty} (b_n + c_n) x^n$ を和，$(\sum_{n=-\infty}^{\infty} b_n x^n)(\sum_{n=-\infty}^{\infty} c_n x^n) \equiv \sum_{n=-\infty}^{\infty} \sum_{i+j=n} b_i c_j x^n$ を積とし，実数 0 と 1 をそれぞれ零元と単位元にもつ体〔1 編 3 章 3-1 参照〕をなす．このような体は（実数体上の）べき級数体あるいはローラン級数体と呼ばれる．

(1) 例: 等比数列

数列 $a_n = sr^n$ $(s \neq 0, n \geq 0)$ の母関数 $a(x)$ は，べき級数体上で $(\sum_{n=0}^{\infty} sr^n x^n)(1 - rx)/s = 1$ であることから，（x とは関係なく）

$$a(x) = \sum_{n=0}^{\infty} sr^n x^n = \frac{s}{1 - rx} \tag{2・13}$$

である．

(2) 例: フィボナッチ数

$f_0 = 0$，$f_1 = 1$，$f_n = f_{n-2} + f_{n-1}$ $(n \geq 2)$ と再帰的に定義されるフィボナッチ数（Fibonacci numbers）の母関数を $f(x)$ とすると，$f(x) = \sum_{n=0}^{\infty} f_n x^n = x + \sum_{n=2}^{\infty} (f_{n-1} + f_{n-2}) x^i = x + x f(x) + x^2 f(x)$ より，

$$f(x) = \frac{x}{1 - x - x^2} = \frac{1}{\sqrt{5}} \left(\frac{1}{1 - \alpha x} - \frac{1}{1 - \beta x} \right) \tag{2・14}$$

を得る．ただし $\alpha = (1 + \sqrt{5})/2$ (黄金比)，$\beta = (1 - \sqrt{5})/2$ である．したがって，式 (2・13) より $f_n = (\alpha^n - \beta^n)/\sqrt{5}$ と求められる．

(3) 例: 整数分割数

正整数 n が単調非増加な正整数列 $r_1, \ldots, r_k$ の和であるとき，数列 $r_1, \ldots, r_k$ を n の分割と呼ぶ．$p(n)$ を n の分割の総数とすると（ただし $p(0) = 1$ とする），$p(n)$ は $\prod_{i=1}^{\infty} (\sum_{j=0}^{\infty} x^{ij})$ の第 n 次項の係数に等しい．したがって，$p(n)$ の母関数は

* 形式的な微積分を定義することは可能である．

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{i=1}^{\infty}\left(\sum_{j=0}^{\infty} x^{ij}\right) = \prod_{i=1}^{\infty}\frac{1}{1-x^i} \tag{2･15}$$

で与えられる．$p(n)$ の閉じた簡単な式は知られていないが，母関数に基づいて漸化式

$$p(n) = \sum_{\substack{i\geq 1\\ i(3i-1)\leq 2n}} (-1)^{i-1} p\left(n - \frac{i(3i-1)}{2}\right) + \sum_{\substack{i\geq 1\\ i(3i+1)\leq 2n}} (-1)^{i-1} p\left(n - \frac{i(3i+1)}{2}\right) \quad (n \geq 1) \tag{2･16}$$

が得られることが知られている[9]．

2-3-2 解析的取扱い

コーシー・アダマールの公式より，$a(x)$ の収束半径 r は $1/\overline{\lim}_{n\to\infty}\sqrt[n]{|a_n|}$ で与えられる．$r > 0$ であるとき，$a(x)$ を $x \in (-r, r)$ 上で定義される関数として取り扱う．これにより $a(x)$ は代数的な取扱いに加えて解析的な取扱い，特に項別微積分が可能となる．ゆえに $a^{(n)}(x)$ を $a(x)$ の第 n 階導関数とすると，$a_n = a^{(n)}(0)/n!$ と表せる．

なお，増加率の大きい数列でも解析的に扱える母関数を得る目的で，式 (2･12) の代わりに

$$a(x) = \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n \tag{2･17}$$

のかたちの級数が考えられることもある．この級数は特に指数型母関数（exponential generating function）と呼ばれる．これに対して式 (2･12) の級数は常母関数（ordinary generating function）と呼ばれることもある．

(1) 例：カタラン数

n 対の括弧からなる “正しい” 文字列を考える．これは $n = 0$ のとき空列，$n \geq 1$ のときは $0 \leq i \leq n-1$ 対括弧の正しい文字列を新しい一つの括弧で囲み，別の $n-1-i$ 対括弧の正しい文字列を後に連結して得られる文字列である．n 対括弧の正しい文字列の総数を b_n とすると，定義より $b_0 = 1$ 及び $n \geq 1$ に対して $b_n = \sum_{i=0}^{n-1} b_i b_{n-1-i}$ が成り立つ．また明らかに $0 < b_n \leq 2^{2n}$ であるので，b_n の母関数 $b(x) = \sum_{n=0}^{\infty} b_n x^n$ は少なくとも 1/4 の収束半径をもち，この内部で解析的に取り扱える．

b_n の漸化式より，$b(x) = 1 + \sum_{n=1}^{\infty}\sum_{i=0}^{n-1} b_i b_{n-1-i} x^n = 1 + x\sum_{n=0}^{\infty}\sum_{i=0}^{n} b_i b_{n-i} x^n = 1 + xb(x)^2$ を得る．このことと $\lim_{x\to 0} b(x) = 1$ より

$$b(x) = \begin{cases} \dfrac{1-\sqrt{1-4x}}{2x} & (x \neq 0) \\ 1 & (x = 0) \end{cases} \tag{2･18}$$

が成り立つ．ここで $n \geq 1$ に対して $c_n = b_{n-1}$，$c_0 = 0$ とすると，c_n の母関数として $c(x) = \sum_{n=1}^{\infty} b_{n-1}x^n = xb(x) = (1-\sqrt{1-4x})/2$，これをマクローリン展開することにより $c(x) = \sum_{n=1}^{\infty}({}_{2(n-1)}\mathrm{C}_{n-1}/n)x^n$ が得られ，$b_n = c_{n+1} = {}_{2n}\mathrm{C}_n/(n+1)$ と求められる．この値はカタラン数（Catalan numbers）と呼ばれ，順序木の総数などとしても知られる．

■12 群 - 2 編 - 2 章

2-4 同値類の数え上げ

（執筆者：松林 昭）[2009 年 6 月 受領]

2-4-1 置換群

n 元集合上の置換全体は，合成（積）を 2 項演算とし，恒等置換（恒等写像）を単位元にもつ群〔1 編 3 章 3-1 参照〕をなす．このような群は n 次対称群 S_n と呼ばれ，対称群の部分群は置換群と呼ばれる．$\Gamma \subseteq S_n$ をある置換群とする．$\gamma \in \Gamma$ を巡回置換の積に分解したとき，長さ i $(1 \le i \le n)$ の巡回置換が現れる回数を $l_i(\gamma)$ で表す．特に，$l_1(\gamma)$ は γ の不動元（$\gamma(a) = a$ であるような a）の数に等しい．このとき，

$$P_\Gamma(x_1, \ldots, x_n) = \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} \prod_{i=1}^{n} x_i^{l_i(\gamma)} \tag{2·19}$$

と定義される $x_1, \ldots, x_n$ の多項式を Γ の巡回置換指数（cycle index）と呼ぶ．

2-4-2 置換群が誘導する同値類

有限集合 A 上の置換群を Γ とする．$a, b \in A$ に対して，$\gamma(a) = b$ となるような $\gamma \in \Gamma$ が存在するとき $a \overset{\Gamma}{\sim} b$ と表すと，関係 $\overset{\Gamma}{\sim}$ は A 上の同値関係となる．$a \in A$ を不動元にもつ置換の集合を Γ_a とすると，各 $b \overset{\Gamma}{\sim} a$ に対して $|\{\gamma \in \Gamma \mid \gamma(a) = b\}| = |\Gamma_a|$ であることが分かるので，a を含む同値類の要素数は $|\Gamma|/|\Gamma_a|$ に等しい．したがって，同値類の総数は $\sum_{a \in A} |\Gamma_a| = \sum_{\gamma \in \Gamma} l_1(\gamma)$ を $|\Gamma|$ で割ったものに等しい．ゆえに次の定理を得る．

バーンサイドの定理（Burnside's Theorem）： A 上の同値関係 $\overset{\Gamma}{\sim}$ が定める同値類の総数は

$$\frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} l_1(\gamma) \tag{2·20}$$

に等しい．

(1) 例：正 n 角形の彩色

正 n 角形の頂点を k 色で彩色する方法の総数を考える．ただし回転によって一致するものは同一と考える．A を彩色の集合，すなわち写像 $\{1, \ldots, n\} \to \{1, \ldots, k\}$ の集合とし，$\Gamma = \{\gamma_1, \ldots, \gamma_n\}$ を彩色を $360i/n$ 度回転させる置換 γ_i の集合とすると，Γ は γ_n を単位元にもつ置換群をなす．γ_i の不動元数は正 n 角形の特定の $\gcd(n, i)$ 頂点からなるパスの彩色の総数に等しい．ただし，$\gcd(n, i)$ は n と i の最大公約数である．したがって $\overset{\Gamma}{\sim}$ が定める A 上の同値類の総数は，式 (2·20) より

$$\frac{1}{n} \sum_{i=1}^{n} k^{\gcd(n,i)} \tag{2·21}$$

で与えられる．

2-4-3 写像上の同値類

彩色のような写像の総数を数えるのにバーンサイドの定理を適用すると，写像（彩色）集合上の置換を考える必要がある．しかし回転などでは彩色そのものよりも彩色される頂点の方を置換すると考えることで複雑な場合が扱いやすくなり，より詳細な置換群の性質が得られることがある．

有限集合 A 上の置換群を Γ とし，A から有限集合 C への写像 $f : A \to C$ 全体を Φ とする．$f, g \in \Phi$ に対して，すべての $a \in A$ で $f(a) = g(\gamma(a))$ となるような $\gamma \in \Gamma$ が存在するとき $f \overset{\Gamma}{\approx} g$ と表すと，関係 $\overset{\Gamma}{\approx}$ は Φ 上の同値関係となる．

ポリアの数え上げ法（Pólya's method of enumeration）：各 $c \in C$ に対して重み $w(c)$ が定義されているとし，Φ 上の同値関係 $\overset{\Gamma}{\approx}$ が定める各同値類 F の重みを $W(F) = \prod_{a \in A} w(f(a))$（ただし $f \in F$）とする．$W(F)$ は f の選び方によらず定まることに注意する．このとき，

$$\sum_F W(F) = P_\Gamma\left(\sum_{c \in C} w(c), \sum_{c \in C} w(c)^2, \ldots, \sum_{c \in C} w(c)^{|A|}\right) \tag{2・22}$$

が成り立つ．

すべての $c \in C$ に対して $w(c) = 1$ とすることにより，次の系を得る．

系：Φ 上の同値関係 $\overset{\Gamma}{\approx}$ が定める同値類の総数は

$$P_\Gamma(|C|, \ldots, |C|) \tag{2・23}$$

に等しい．

(1) 例：正 n 角形の各色の使用回数を限定した彩色

正 n 角形の頂点を，色 $c_1, \ldots, c_k$ をそれぞれ $d_1, \ldots, d_k$ 回ずつ（$\sum_{j=1}^{k} d_j = n$）使って彩色する方法の総数を考える．ただし回転によって一致するものは同一と考える．A を n 頂点集合，$C = \{c_1, \ldots, c_k\}$ とし，$\Gamma = \{\gamma_1, \ldots, \gamma_n\}$ を頂点を $360i/n$ 度回転させる置換 γ_i の集合とすると，Γ は γ_n を単位元にもつ置換群をなす．

$$l_j(\gamma_i) = \begin{cases} \gcd(n, i) & (j = n/\gcd(n, i)) \\ 0 & (\text{otherwise}) \end{cases} \tag{2・24}$$

であるので，式 (2・22) の右辺は

$$\frac{1}{n} \sum_{i=1}^{n} \left(\sum_{j=1}^{k} w(c_j)^{n/\gcd(n,i)} \right)^{\gcd(n,i)} \tag{2・25}$$

となる．また式 (2・22) は $w(c)$ の多項式として恒等的に成り立つので，c_j を d_j 回使う彩色の総数は式 (2・25) における項 $\prod_{j=1}^{k} w(c_j)^{d_j}$ の係数と等しい．なお，$w(c_j) = 1$ $(1 \le j \le k)$ とすることにより，式 (2・25) から式 (2・21) が得られる．

■12 群 - 2 編 - 2 章

2-5 確率的手法

（執筆者：松林 昭）[2009 年 6 月 受領]

確率的手法（probabilistic method）では，ある性質を満たす組合せ対象の総数や存在性，あるいは存在条件などを確率の技法を用いて示す．典型的には，組合せ対象を事象とする確率空間を設計し，目的の性質をもつ事象の生起確率が正であることを示すことによって，そのような性質をもつ対象が存在することを主張する．もし，対象や確率空間の性質などから生起確率に対する精密な情報が得られる場合には，存在性だけでなくその量についての知見が得られることもある．いずれにせよ，ここで設計する確率空間は恣意的なものであって，考える対象そのものが確率的な側面をもっている必要はない．また，この論法は所望の対象の存在を明らかにするけれども，そのような対象の構成については何も言及しないことに注意する必要がある．しかしながら，所望の事象が高確率で起こるように確率空間を設計できる場合には単純なランダム構成が高確率で所望の構成を与える．更にこのような確率的な構成から決定的構成アルゴリズムを設計する研究も行われている[10]．事象の生起確率を評価するために確率の様々な概念を利用できる．本節ではいくつかの典型的な方法を紹介する．以下では，標本空間 Ω の事象 $A \subseteq \Omega$ の確率を $\Pr[A]$ で表す．

2-5-1 数え上げのふるい

所望の組合せ対象が，ある事象 $\{A_i\}$ の余事象の積 $\bigcap_i \overline{A_i}$ で表せるとする．もし $\sum_i \Pr[A_i] < 1$ であるように確率空間を設計できたならば，$\Pr[\bigcap_i \overline{A_i}] = \Pr[\overline{\bigcup_i A_i}] \geq 1 - \sum_i \Pr[A_i] > 0$ が成り立つので，所望の対象が存在することが示される．

(1) 例：ラムゼー数の下界

正整数 k, l に対して，全ての n 頂点グラフ G が k 点クリーク〔本編 3 章 3-4-3 参照〕か l 点独立集合〔本編 3 章 3-4-2 参照〕をもつような最小の n はラムゼー数（Ramsey number）$R(k,l)$ と呼ばれる．$k \geq 3$ ならば $R(k,k) > \lfloor 2^{k/2} \rfloor$，すなわち $n \leq \lfloor 2^{k/2} \rfloor$ ならば k 点クリークも k 点独立集合ももたないような n 頂点グラフが存在する．これを以下に示す．

n 頂点の各点対を確率 1/2 で辺で結んでグラフ G をつくる．各 k 頂点集合 U がクリークか独立集合であるという事象を A_U で表すと，

$$\sum_U \Pr[A_U] = {}_n\mathrm{C}_k 2^{1-{}_k\mathrm{C}_2} < \frac{n^k}{k!} \cdot \frac{2}{2^{(k^2-k)/2}} \leq \frac{2 \cdot 2^{k/2}}{k!} < 1 \qquad (2\cdot26)$$

が成り立つ．したがって，$\Pr[\bigcap_U \overline{A_U}] > 0$ であり，$\bigcap_U \overline{A_U}$ が起こるような n 頂点グラフが存在する．なお，式 (2･26) の $2 \cdot 2^{k/2}/k!$ は k の増加にともなって急速に 0 に収束するので，G は $k \geq 2\log_2 n$ に対して高い確率で k 点クリークも k 点独立集合ももたない*．

(2) 例：ハイパーグラフの 2-彩色

有限集合 V と集合族 $E_1, \ldots, E_m \subseteq V$ は，単色になる E_i が存在しないような V の彩色 $V \to \{1,2\}$ が存在するとき，2-彩色可能であるという．$|E_i| \geq n\ (1 \leq i \leq m)$ で $m < 2^{n-1}$ ならば常に 2-彩色可能である．これを以下に示す．

* しかしそれにもかかわらず，このようなグラフを明示的かつ効率的に構成する方法は知られていない．

V の各元を確率 1/2 で色を選んで彩色する．E_i が単色になるという事象を A_i で表すと，

$$\sum_{i=1}^{m} \Pr[A_i] \le m2^{1-n} < 1 \tag{2·27}$$

が成り立つ．したがって $\Pr[\bigcap_{i=1}^{m} \overline{A_i}] > 0$ であり，$\bigcap_{i=1}^{m} \overline{A_i}$ が起こるような 2-彩色が存在する．

2-5-2 期待値・分散

目的の性質がパラメータ（例えばグラフの不変量など）を含む場合，そのパラメータは確率空間の上で確率変数となる．確率変数 X の期待値 $\mathrm{E}[X]$ に対して，$X \le \mathrm{E}[X]$ であるような事象と $X \ge \mathrm{E}[X]$ であるような事象の生起確率がともに正であることが分かるので，そうした性質をもつ対象の存在が示される．更にマルコフの不等式やチェビシェフの不等式などを偏差の大きい事象の生起確率を制限するために利用することで，事象の存在条件などの上下界が得られることもある．

(1) 例：独立集合

グラフ (V, E) の各頂点 $v \in V$ の次数を $d(v)$ で表すと，G の独立数 (最大独立集合の要素数) は少なくとも $\sum_{v\in V} 1/(d(v)+1)$ である．これを以下に示す．

$\prec$ を V 上のすべての全順序から等確率で選んだ一つの全順序とする．$I = \{u \in V \mid (u,v) \in E \Rightarrow u \prec v\}$ とすると，$\prec$ が全順序であることから I は独立集合となる．X_v を $v \in I$ という事象の指示変数，すなわち $v \in I$ ならば $X_v = 1$，そうでなければ $X_v = 0$ とすると，$\mathrm{E}[|I|] = \mathrm{E}[\sum_{v\in V} X_v] = \sum_{v\in V} \mathrm{E}[X_v] = \sum_{v\in V} \Pr[v \in I] = \sum_{v\in V} 1/(d(v)+1)$ が成り立つ．したがって，$|I| \ge \sum_{v\in V} 1/(d(v)+1)$ であるような独立集合が存在する．

2-5-3 分　布

分散の小さい確率分布を設計できれば，偏差の大きい事象の生起確率をチェビシェフの不等式などから得られるものよりも更に制限できる．これを利用することで，より精密な存在条件などを示すことができる．

(1) 例：discrepancy

有限集合 V の部分集合族 $\mathcal{A}$ に対して，V の彩色 $\chi : V \to \{-1, 1\}$ を考える．$A \subseteq V$ に対して $\chi(A) = \sum_{v\in A} \chi(v)$ とし，$\mathcal{A}$ の discrepancy を $\mathrm{disc}(\mathcal{A}) = \min_\chi \max_{A\in\mathcal{A}} |\chi(A)|$ と定義する．$|V| = m$，$|\mathcal{A}| = n$ のとき，$\mathrm{disc}(\mathcal{A}) \le \sqrt{2m\ln(2n)}$ が成り立つ．これを以下に示す．

各 $v \in V$ に対して $\chi(v) \in \{-1, 1\}$ を確率 1/2 で選ぶ．$\alpha = \sqrt{2m\ln(2n)}$ とし，各 $A \subseteq V$ が $|\chi(A)| > \alpha$ を満たす事象の指示変数を X_A とする．$|A| = a$ とすると，$\chi(A)$ は $B(a, 1/2) - a/2$（ただし $B(a, 1/2)$ は 2 項分布．すなわち, 成功確率 1/2 の独立なベルヌーイ試行を a 回行うときの成功回数が従う確率分布）の分布に従い, チェルノフ限界と同様の不等式 $\Pr[|\chi(A)| > \alpha] < 2e^{-\alpha^2/(2a)}$ が成り立つ．したがって $\mathrm{E}[X_A] = \Pr[|\chi(A)| > \alpha] < 2e^{-\alpha^2/(2a)} \le 2e^{-\alpha^2/(2m)} = 1/n$ であり，ゆえに $\mathrm{E}[\sum_{A\in\mathcal{A}} X_A] = \sum_{A\in\mathcal{A}} \mathrm{E}[X_A] < n \cdot 1/n = 1$．これは $\sum_{A\in\mathcal{A}} X_A = 0$ であるような χ が存在することを意味するので，$\mathrm{disc}(\mathcal{A}) \le \sqrt{2m\ln(2n)}$ が成り立つ．

2-5-4 独立性

数え上げのふるいによる確率の評価方法では，$\Pr[\bigcap_i \overline{A_i}] \ge 1 - \sum_i \Pr[A_i]$ を正とするた

めに $\sum_i \Pr[A_i] < 1$ の前提を必要としていた．もし $\{A_i\}$ が互いに独立ならば，$\Pr[\bigcap_i \overline{A_i}] = \prod_i (1 - \Pr[A_i]) > 0$ を得るには各 i に対して $\Pr[A_i] < 1$ でさえあればよい．このアイディアの一般の場合への拡張は Lovász local lemma と呼ばれ，Erdös と Lovász（1975）によって示された．

事象 $A_1, \ldots, A_n$ に対し，頂点集合 $V = \{1, \ldots, n\}$ と有向辺集合 E からなるグラフは，A_i が $(i, j) \notin E$ であるようなすべての A_j と独立であるとき従属有向グラフと呼ばれる．

Lovász Local Lemma：事象 $A_1, \ldots, A_n$ の従属有向グラフ (V, E) に対して，$\Pr[A_i] \le x_i \prod_{(i,j)\in E}(1 - x_j)$（$1 \le i \le n$）であるような実数 $0 \le x_i < 1$（$1 \le i \le n$）が存在するならば，$\Pr[\bigcap_{i=1}^n \overline{A_i}] \ge \prod_{i=1}^n (1 - x_i)$.

系：$A_1, \ldots, A_n$ を事象とする．各 $1 \le i \le n$ に対して A_i がたかだか d 個の例外を除く A_j（$j \ne i$）と独立で，$\Pr[A_i] \le p$ であり，かつ $ep(d + 1) \le 1$ （e は自然対数の底）ならば，$\Pr[\bigcap_{i=1}^n \overline{A_i}] > 0$.

（1）例：次数が制限されたハイパーグラフの 2-彩色

有限集合 V と集合族 $E_1, \ldots, E_m \subseteq V$ が，各 $1 \le i \le m$ に対して $|E_i| \ge n$ と $|\{E_j \mid E_i \cap E_j \ne \emptyset\}| \le d$ を満たし，かつ $e(d+1) \le 2^{n-1}$ であるとする．V の各元を確率 1/2 で色を選んで彩色し，E_i が単色になるという事象を A_i で表すと，A_i はたかだか d 個の例外を除く A_j $(j \ne i)$ と独立で，$\Pr[A_i] \le 2^{1-n}$ が成り立つ．したがって Lovász local lemma の系より (V, E) は 2-彩色可能である．

■参考文献

1) C. Berge, “Principes de Combinatoire,” Dunod, 1968; 野崎明弘（訳）, “組合せ論の基礎,” サイエンス社, 1973.
2) R.P. Grimaldi, “Discrete and Combinatorial Mathematics – An Applied Introduction（5th Edition）,” Pearson Education/Addison-Wesley, 2003.
3) C.L. Liu, “Introduction to Combinatorial Mathematics,” McGraw-Hill, 1968; 伊理正夫, 伊理由美（訳）, “組合せ数学入門,” 共立出版, 1972.
4) L. Lovász, “Combinatorial Problems and Exercises,” Akadémiai Kiadó, 1979; 成嶋 弘, 土屋守正（訳）, “数え上げの手法,” 東海大学出版会, 1988.
5) J. Matoušek and J. Nešetřil, “Invitation to Discrete Mathematics,” Oxford University Press, 1998; 根上生也, 中本敦浩（訳）, “離散数学への招待,” シュプリンガー・ジャパン, 2002.
6) 高橋磐郎, 藤重悟, “離散数学,” 岩波書店, 1981.
7) R.L. Graham, M. Grötschel, and L. Lovász（Ed.）, “Handbook of Combinatorics,” The MIT Press/Elsevier, 1995.
8) N. Alon and J.H. Spencer, “The Probabilistic Method（3rd Edition）,” Wiley, 2008.
9) G.E. Andrews and K. Eriksson, “Integer Partitions,” Cambridge University Press, 2004; 佐藤文広（訳）, “整数の分割,” 数学書房, 2006.
10) R. Motwani and P. Raghavan, “Randomized Algorithms,” Cambridge University Press, 1995.