集中講義 応用数学特論 II

Day 1 ラテン方格・直交配列

担当：盧　暁南 (山梨大学)
xnlu@yamanashi.ac.jp

2021 年 8 月 25 日

本日の内容

1 から n の整数を $n \times n$ のマスに配置し，各行および各列に重複が出ないようにする．このような配置は**ラテン方格**という．また，組合せ論が実用の場に応用される最初の例として，**直交配列**における統計的実験計画法がある．本日はラテン方格と直交配列を中心として，以下の話題について紹介する．

(i) ラテン方格とその関連する代数的構造

(ii) 互いに直交するラテン方格 (MOLS) およびその最大個数

(iii) ラテン方格の transversal (横断線) と Ryser–Brualdi–Stein 予想

(iv) MOLS と直交配列，直交配列の実験計画法への実応用

0　記号

- $[n] := \{1, 2, \ldots, n\}$.
- $\mathbb{Z}$: 整数全体の集合，整数環 (ring of integers)
- 有限集合 A において，$|A|$ または $\#A$ は集合 A の要素数を表す．

1　ラテン方格・擬群・群

定義 1.1. サイズ $n \times n$ の配列 $A = (a_{i,j})$ の各行 i $(1 \le i \le n)$ および各列 j $(1 \le j \le n)$ に，すべてのシンボル $[n]$ が現れるとき，すなわち，

$$\{a_{i,1}, a_{i,2}, \ldots, a_{i,n}\} = \{a_{1,j}, a_{2,j}, \ldots, a_{n,j}\} = [n] \quad (\forall i, j),$$

が成り立つとき，$A = (a_{i,j})$ を**位数** (order) n の**ラテン方格** (Latin square) という．

定義 1.2. 空でない集合 X に対して，直積集合 $X \times X$ から X への写像 $(x, y) \mapsto z = x \circ y$ が定められたとき，$\circ$ を X の**二項演算子** (binary operator) という．このとき，X は二項演算 $\circ$ に関して**閉じている**．$(X, \circ)$ を**亜群** (groupoid) という．

定義 1.3. 亜群 $(X, \circ)$ において，任意の $a, b \in X$ に対して，$a \circ x = b$ および $y \circ a = b$ を満たす $x, y \in X$ が一意的に存在するならば，$(X, \circ)$ は**擬群** (quasigroup) という．

注 1.4. 集合に定まった演算によって決まる構造のことを**代数的構造** (algebraic structure) という．

命題 1.5. ラテン方格 $A = (a_{i,j})$ において，その添字の集合とシンボル集合ともに $X = [n]$ とし，X 上に二項演算子 $\circ$ を以下に定義する．

$$i \circ j = a_{i,j}, \quad (i, j \in X) \tag{1}$$

このとき，$(X, \circ)$ は擬群をなす．

Proof. ラテン方格の定義によって，任意の $a, b \in X$ に対して，$a \circ x = b$ または $x \circ a = b$ の解 $x \in X$ が唯一に存在することが分かる． □

注 1.6. 代数学の文脈で ($|X|$ が有限のとき) 擬群の演算表 (演算結果を表にしたもの) を Cayley table という．命題 1.5 の逆も成り立つ．すなわち，擬群の Cayley table はラテン方格である．

定義 1.7. 擬群 $(X, \circ)$ において，任意の $x \in X$ に対して，$x \circ e = x$ かつ $e \circ x = x$ を満たす $e \in X$ は $(X, \circ)$ の**単位元** (identity) という．単位元をもつ擬群は *loop* という．

定義 1.8. 亜群 $(X, \circ)$ において，**結合律** (associative law)

$$(x \circ y) \circ z = x \circ (y \circ z) \quad (x, y, z \in X)$$

を満たすとき，$(X, \circ)$ が**結合的** (associative) であるという．

定義 1.9. 結合的な loop は**群** (group) という． つまり，単位元をもつ，結合的な擬群は群である．

群は代数学において最も基本的な概念である．整数論や幾何学に現れるたくさんの対称性が群で表現できる．次に，本講義でよく使われる**巡回群** (cyclic group) を整数剰余を用いて紹介する．

定義 1.10. 任意の正整数 n に対して，1 つの文字 1 の累加の全体

$$C_n = \{e = 0 (= 1 \times 0), 1, 1+1, 1+1+1, \ldots, \underbrace{1+1+\cdots+1}_{n-1}\} \quad (\underbrace{1+1+\cdots+1}_{n} = e = 0)$$

は**位数** n の**巡回群** (cyclic group) といい，1 を C_n の**生成元** (generator) という．

命題 1.11. $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$ は mod n の加法で群となり，**巡回群**である．

定義 1.12. 集合 $[n]$ 上の全単射 (実は全射または単射で十分)

$$\sigma : x \mapsto x^\sigma \quad (x \in [n])$$

を X 上の**置換** (permutation) といい，次の 2 行表現で表す．

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1^\sigma & 2^\sigma & \cdots & n^\sigma \end{pmatrix}$$

ここで，x^σ は σ を x に作用させるという．

注 1.13. 巡回的に文字を置き換えるような置換は巡回置換という．すべての置換は巡回置換の積の形で表すことができる．

定義 1.14. 集合 $[n]$ 上のすべての置換の集合 S_n は，置換の積 $x^{\sigma\tau} = (x^\sigma)^\tau$ $(\sigma, \tau \in S_n, x \in [n])$ において群となり，**対称群** (symmetric group) という．一般的に，$\sigma\tau = \tau\sigma$ は成り立たない．対称群 S_n の位数は $n!$ である．

2　ラテン方格の補完問題

定義 2.1. サイズ $k \times n$ $(k < n)$ の配列 $A = (a_{i,j})$ の各行 i $(1 \le i \le n)$ および各列 j $(1 \le j \le n)$ に，すべてのシンボル $[n]$ が高々 1 回現れるとき，すなわち，

$$\{a_{i,1}, a_{i,2}, \ldots, a_{i,n}\} = [n] \quad (\forall i)$$

かつ

$$\#\{a_{1,j}, a_{2,j}, \ldots, a_{k,j}\} = k \quad (\forall j)$$

であるとき，$A = (a_{i,j})$ を $k \times n$ の**ラテン長方形** (Latin rectangle) という．

定理 2.2. 任意の $k \times n$ $(k < n)$ のラテン長方形は $(k+1) \times n$ のラテン長方形に拡張できる．

定理 2.2 の証明は授業で示す．

系 2.3. 任意の $k \times n$ $(k < n)$ のラテン長方形は $n \times n$ のラテン方格に拡張できる．

注 2.4. $k \times n$ のラテン長方形に $n - k$ 行を追加してラテン方格になるように完成させる問題はラテン長方形の補完問題 (completion) と呼ぶ．

3　直交ラテン方格

定義 3.1. $[n]$ 上の位数 n の 2 つのラテン方格 $A = (a_{i,j})$ と $B = (b_{i,j})$ において，$A \boxplus B = ((a_{i,j}, b_{i,j}))$ は A と B を重ね合わせた配列とする．$A \boxplus B$ の成分に $[n] \times [n]$ の要素がすべて現れたとき，A と B は**直交** (orthogonal) するという．

定義 3.2. 位数 n のラテン方格の集合 $\mathcal{L} = \{L_1, L_2, \ldots, L_k\}$ において，任意の L_i と L_j $(i \ne j)$ が直交するなら，すべての L_i $(1 \le i \le k)$ が **互いに直交するラテン方格** (mutually orthogonal Latin squares; MOLS) という．このとき，$\mathcal{L}$ は MOLS 集合という．

定義 3.3. 位数 n のラテン方格において，MOLS 集合の最大サイズを $N(n)$ とする．つまり，

$$N(n) := \max\{k \in \mathbb{N} : \text{位数 } n \text{ の } k \text{ 個の MOLS が存在する }\}$$

定理 3.4. 任意の $n \ge 2$ に対して $N(n) \le n - 1$.

定理 3.4 の証明は授業で示す．

注 3.5. サイズ $n - 1$ の MOLS 集合は完全 (complete) であるという．

定理 3.6. 任意の素数べキ $q \ge 2$ に対して $N(q) = q - 1$.

定理 3.6 の証明は「有限幾何学・有限体」の日に紹介する．

定理 3.7. A_1, A_2 を位数 n の MOLS とし，B_1, B_2 を位数 m の MOLS とする．$A_1 \otimes B_1$, $A_2 \otimes B_2$ が位数 mn の MOLS である．ここで，$\otimes$ は Kronecker 積を表す．

定理 3.7 の詳細は授業で紹介する．

注 3.8. 一般的に，$N(mn) \ge \min\{N(n), N(m)\}$ が成り立つ．

定理 3.9. 任意の $n \equiv 0, 1, 3 \pmod 4$ に対して，$N(n) \ge 2$.

予想 3.10 (Euler, 1782)**.** 任意の $n \equiv 2 \pmod 4$ に対して，位数 n の MOLS が存在しない．

Euler の予想は $n = 2, 6$ に対して正しい．

定理 3.11. 任意の $0 \le u \le t$ に対して，以下の不等式が成り立つ．

$$N(mt+s) \ge \min\{N(m), N(m+1), N(t)-1, N(u)\}$$

定理 3.11 はかなりテクニカルなので，もし時間があれば当日の最後で紹介する．

定理 3.12. 任意の $n \ne 2, 6$ に対して，$N(n) \ge 2$.

定理 3.12 の証明は授業で紹介する．

4 ラテン方格の transversal

定義 4.1. 位数 n のラテン方格 $A = (a_{i,j})$ の要素の部分集合 $T = \{a_{i_1,j_1}, a_{i_2,j_2}, a_{i_t,j_t}\}$ において，

$$\#\{i_1, i_2, \ldots, i_t\} = \#\{j_1, j_2, \ldots, j_t\} = \#T = t$$

であるとき，つまり，T に各行の要素・各列の要素・各シンボルが高々 1 個含まれる場合，T はラテン方格 A の**長さ** (length) t の**部分横断線** (partial transversal) という．

また，$t = n$ のとき，T は**横断線** (transversal) という．

注 4.2. ラテン方格は完全 2 部グラフの辺彩色に対応させることができる．X と Y をそれぞれラテン方格の行番号・列番号の集合とし，完全 2 部グラフ $(X \cup Y, E)$ を考える．E は X と Y の間のすべての辺をなす集合であり，ラテン方格の各要素に対応する．更に，辺 $(x, y) \in X \times Y$ において，ラテン方格の (x, y) 要素が $c \in [n]$ であるとき，辺 (x, y) を色 c で彩色する．このとき，ラテン方格の transversal は辺彩色グラフ $(X \cup Y, E)$ の**完全虹色マーチング** (perfect rainbow matching) (各辺に色が異なるような完成マーチングのこと) に対応する．

ラテン方格の transversal の存在性および最大 partial transversal の決定問題は，ラテン方格の内部構造を解明するための重要な問題として研究されている．

定理 4.3. n が偶数であるとき，有限巡回群 $\mathbb{Z}_n$ の演算表で生成したラテン方格は transversal をもたない．

定理 4.3 は最初に Wanless–Webb [8] によって示した．授業で [8] の証明を紹介する．

すべてのラテン方格に transversal が存在するわけではないから，その次に長さ $n-1$ の partial transversal を見つけたい．

予想 4.4 (Ryser–Brualdi–Stein, 1967)**.** すべての位数 n のラテン方格に対して，長さ $n-1$ の partial transversal が存在する．

定理 4.5 (Hatami–Shor [1], 2008)**.** すべての位数 n のラテン方格に対して，長さ $n - 11.053(\log n)^2$ の partial transversal が存在する．

もし時間があれば，$n = 6$ のラテン方格に必ず長さ 5 の partial transversal が存在することの証明を通して，Hatami–Shor [1] の基本アイデアを簡単に紹介する．

定理 4.6 (Keevash, et. al [3], 2020+)**.** すべての位数 n のラテン方格に対して，長さ $n - O(\log n / \log\log n)$ の partial transversal が存在する．

5 直交配列とその統計的実験計画法への応用

定義 5.1. シンボル集合 S 上の $N \times k$ 配列 A において，任意の $N \times t$ 部分配列にすべての t 次元行ベクトルがちょうど λ 回現れるとき，配列 A は**水準** (level) 数 $s = |S|$，**強さ** (strength) t，**会合数** (index) λ の**直交配列** (orthogonal array; OA) といい，$\mathrm{OA}(N, k, s, t)$ で表す．

命題 5.2. $\mathrm{OA}(N,k,s,t)$ において，$\lambda = N/s^t$.

命題 5.3. $t \geq 2$ のとき，会合数 λ の $\mathrm{OA}(N,k,s,t)$ は会合数 λs の $\mathrm{OA}(N,k,s,t-1)$ である．

命題 5.4. $\mathrm{OA}(N,k,s,t)$ の任意の $N \times k'$ 部分配列は $\mathrm{OA}(N,k',s,t')$ である．ここで，$t' = \min\{k',t\}$.

定理 5.5 (Rao の不等式, 1947)．$\mathrm{OA}(N,k,s,t)$ において，以下が成り立つ．

$$N \geq \sum_{i=0}^{u} \binom{k}{i}(s-1)^i, \qquad \text{if } t = 2u,$$

$$N \geq \sum_{i=0}^{u} \binom{k}{i}(s-1)^i + \binom{k-1}{u}(s-1)^{u+1}. \qquad \text{if } t = 2u+1,$$

もし時間があれば定理 5.5 の証明を紹介する．

統計的実験計画法への応用例 (一部実施要因計画) はスライドで載せておく．

もし時間があれば直交配列の秘密分散法 (secret sharing scheme) への応用も簡単に紹介する．

参考文献

[1] P. Hatami and P. W. Shor. A lower bound for the length of a partial transversal in a Latin square. *Journal of Combinatorial Theory, Series A*, 115(7):1103–1113, 2008.

[2] A. D. Keedwell and J. Dénes. *Latin Squares and Their Applications*. Elsevier, 2nd edition, 2015.

[3] P. Keevash, A. Pokrovskiy, B. Sudakov, and L. Yepremyan. New bounds for Ryser's conjecture and related problems. *arXiv preprint arXiv:2005.00526*, 2020.

[4] C. F. Laywine and G. L. Mullen. *Discrete Mathematics Using Latin Squares*. John Wiley & Sons, 1998.

[5] C. C. Lindner and C. A. Rodger. *Design Theory*. Chapman and Hall/CRC, 2nd edition, 2008.

[6] J. H. van Lint and R. M. Wilson. *A Course in Combinatorics*. Cambridge University Press, 2nd edition, 2001.

[7] I. M. Wanless. Transversals in latin squares: a survey. In *Surveys in Combinatorics 2011*, pages 403–437. Cambridge University Press, 2011.

[8] I. M. Wanless and B. S. Webb. The existence of latin squares without orthogonal mates. *Designs, Codes and Cryptography*, 40(1):131–135, 2006.