組合せデザインと高次元 PTE 問題

東京都立大学　大学院理学研究科　数理科学専攻
松村英樹 (Hideki MATSUMURA) *

概要

代数的組合せ論においてデザインとは,「全体を近似する良い部分集合」である．一方，加法的整数論において Prouhet—Tarry—Escott（PTE）問題とは，ある次数までの冪和が一致するような整数の多重集合を求めるディオファントス問題である．本稿では「組合せデザイン」という離散的な空間上のデザインから高次元 PTE 問題の解を構成する手法を紹介する．

1　導入

加法的整数論において，Prouhet–Tarry–Escott（PTE）問題というディオファントス問題が古くから研究されてきた（問題 2 参照）．Matsumura–Sawa [7] は，2 次元 PTE 問題と楕円デザインを初めて関連付け，それらの相互間研究を提案した．楕円デザインとは，Pandey [10] による球面デザインの一般化であり，「ある次数までの多項式の重み付き積分を有限個の点での関数値の算術平均として与える楕円上の集合」である．楕円デザインは「幾何的デザイン」という連続的な空間上のデザイン構造である．

2024 年 11 月の早稲田整数論セミナーにおいて上記の研究について講演した際，雪江明彦氏より以下の質問を頂いた．

問題 1 (雪江)**.** PTE 問題と離散的な空間上のデザインを関連付けられるか？

本研究では，問題 1 への回答の 1 つとして，高次元 PTE 問題と組合せデザインを関連付けた ([8])．本稿では特に直交配列（orthogonal array, OA）及びブロックデザインとの関連について得られた結果を中心に解説する．

2　Prouhet–Tarry–Escott（PTE）問題

本節では，PTE 問題の一般化である r 次元 PTE 問題（PTE_r）について述べる．

問題 2 ([1], **次数 m サイズ n の r 次元 PTE 問題 ($\mathbf{PTE}_r$)).** 与えられた自然数 m, n に対して以下を満たす互いに素な多重集合

$$A := \{(a_{11}, \ldots, a_{1r}), \ldots, (a_{n1}, \ldots, a_{nr})\}, B := \{(b_{11}, \ldots, b_{1r}), \ldots, (b_{n1}, \ldots, b_{nr})\} \subset \mathbb{Z}^r$$

* hmatsumura@tmu.ac.jp

を求めよ：$1 \leq k_1 + \cdots + k_r \leq m$ なる任意の $(k_1, \ldots, k_r) \in \mathbb{Z}^r_{\geq 0}$ に対し，

$$\sum_{i=1}^{n} a_{i1}^{k_1} \cdots a_{ir}^{k_r} = \sum_{i=1}^{n} b_{i1}^{k_1} \cdots b_{ir}^{k_r}.$$

m を**次数**，n を**サイズ**といい，PTE_r の解（以下 PTE_r 解）を

$$[(a_{11}, \ldots, a_{1r}), \ldots, (a_{n1}, \ldots, a_{nr})] =_m^n [(b_{11}, \ldots, b_{1r}), \ldots, (b_{n1}, \ldots, b_{nr})]$$

または

$$[A] =_m^n [B]$$

と表す.

PTE 問題の歴史は Goldbach や Euler の時代に遡る．彼らは 1750 年から 1751 年にかけて以下の PTE_1 解の無限系列を発見した：

$$[a, b, c, a+b+c] =_2^4 [0, a+b, a+c, b+c].$$

1910 年代に Tarry や Escott らが研究し，この問題は Tarry–Escott 問題と呼ばれるようになった. Wright [12] が 1959 年に Prouhet [11] による 1851 年の貢献を指摘して以来, Prouhet–Tarry–Escott 問題と呼ばれるようになった．この辺りの歴史は Dickson の本（[3]）に詳しくまとめられている．PTE_1 は，Alpers–Tijdeman [1] により PTE_r へと拡張された（問題 2）．さらに，この構成法は Ghiglione [4] により PTE_r へと拡張された.

PTE_1 は暗号理論における巨大な連続する滑らかな整数の探索（[2]）やグラフ理論における彩色多項式の零点の整数性 （[6]）等の様々な応用もある．また，PTE_r は離散トモグラフィーに応用されている（[1, 4]）.

3 直交配列（OA）

本節では，直交配列（OA）という組合せデザインについて説明する.

定義 3 ([5, p. 1], 直交配列（orthogonal array, OA）)**.** s, t, λ, r, $N \in \mathbb{N}$ とする．$N \times r$ 行列が**水準 s，強さ t，指数 λ，制約数 r，サイズ N の直交配列（OA）**であるとは，任意の $N \times t$ 行列に対して，全ての s シンボルからなる順序付 t 対（s^t 個）が丁度 λ 回ずつ現れることである．そのような OA を $\mathrm{OA}(N, r, s, t)_\lambda$ と書く.

OA は実験計画法において，少ない実験回数で各因子の効果や因子間の交互作用の効果を測定するために応用されている（[5, Chapter 11]）.

主結果では，互いに素な OA から PTE_r 解を構成した（定理 10）.

定義 4 (互いに素な OA)**.** 同じパラメータを持つ $\mathrm{OA}(N, r, s, t)_\lambda$ X_1, X_2 が**互いに素**であるとは，共通する行を持たないことである.

例 5. 2 つの 4×3 の配列

$$X_1 := \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}^\top, \quad X_2 := \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}^\top$$

は互いに素な $\mathrm{OA}(4,3,2,2)_1$ である．実際，X_1, X_2 のどの 2 列に着目しても $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$ が丁度 $\lambda = 1$ 回ずつ現れており，共通する行を持たない．

注意 6 (Cf. [5, p. 244])**.** $\{0,1\}$ を有限体 $\mathbb{F}_2$ とみなすと例 5 の OA X_1 は $\mathbb{F}_2^3$ の 2 次元部分空間である．このような OA を**線形な OA** といい，線形な OA を平行移動することで互いに素な OA を構成できる．

4　ブロックデザイン

本節では，ブロックデザインのうち，t-(r,k,λ) デザインという組合せデザインについて説明する．以下では，有限集合 D の k 元部分集合全体を $D^{\{k\}}$ と表す．

定義 7 (t-(r,k,λ) デザイン（組合せ t デザイン）)**.** λ, t, k, r を $t \le k \le r$ を満たす非負整数とする．r 個の要素からなる有限集合 R と $\mathcal{B} \subset R^{\{k\}}$ の組 $(R,\mathcal{B})$ が $\boldsymbol{t}$**-**$(\boldsymbol{r},\boldsymbol{k},\boldsymbol{\lambda})$ デザイン（組合せ $\boldsymbol{t}$ デザイン） であるとは，任意の $\boldsymbol{T} \subset \boldsymbol{R}^{\{\boldsymbol{t}\}}$ に対し，

$$|\{\boldsymbol{B} \in \boldsymbol{\mathcal{B}} \mid \boldsymbol{T} \subset \boldsymbol{B}\}| = \boldsymbol{\lambda}$$

となることである．$\boldsymbol{R}$ の元を**点**, $\boldsymbol{\mathcal{B}}$ の元を**ブロック**という．特に, $\boldsymbol{t = 2}$ のときは **BIBD (balanced incomplete block design)** と呼ばれる．

主結果では，互いに素な t-(r,k,λ) デザインから PTE_r 解を構成した（定理 12）．

定義 8 (互いに素な t-(r,k,λ) デザイン)**.** 同じパラメータを持つ t-(r,k,λ) デザイン $(R,\mathcal{B}_1), (R,\mathcal{B}_2)$ が**互いに素**であるとは，$\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$ となることである．

例 9 (Fano 平面)**.** $R = \mathbb{Z}/7\mathbb{Z}$ とし，$\mathcal{B}$ を

$$\mathcal{B} = \{\{i, i+1, i+3\} \mid i \in R\},$$

で定めると，$(R,\mathcal{B})$ は 2-$(7,3,1)$ デザインである．実際,

$$\mathcal{B} = \{\{0,1,3\}, \{1,2,4\}, \{2,3,5\}, \{3,4,6\}, \{4,5,0\}, \{5,6,1\}, \{6,0,2\}\}$$

の各ブロックは以下の図の同じ数字からなる辺（円を含む）に対応しており，任意の 2 点を通る辺はただ 1 本である．$(R,\mathcal{B})$ を **Fano 平面**という．また，ブロック集合は下図のように同じ色の $(0,1)$ ベクトル（**特性ベクトル**）と同一視される．

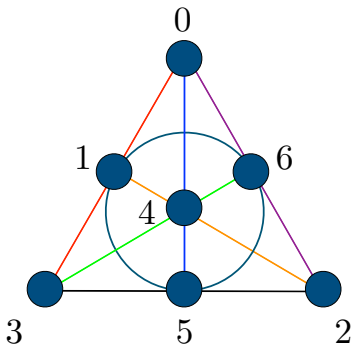

図 1: Fano 平面

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

図 2: Fano 平面の特性ベクトル

同様に，$\mathcal{B}'$ を

$$\mathcal{B}' = \{\{i, i+2, i+3\} \mid i \in R\},$$

で定めると，$(R, \mathcal{B}')$ は $(R, \mathcal{B})$ と互いに素な 2-$(7,3,1)$ デザインである．

5　主結果

本節では，OA を用いた PTE$_r$ 解の構成法とブロックデザインを用いた PTE$_r$ 解の構成法を紹介する．

定理 10 ([8], OA-based construction)**.** X_1, X_2 を互いに素な OA$(N, r, s, t)_\lambda$ の行ベクトルの集合とする．このとき，(X_1, X_2) は次数 t サイズ N の PTE$_r$ 解を与える．

例 11. X, Y を例 5 の OA$(4,3,2,2)_1$ の行ベクトルの集合とすると，これらは互いに素なので，定理 10 より，$[X] =_2^4 [Y]$ は PTE$_4$ 解である．

定理 12 ([8], t-design-based construction)**.** $(R, \mathcal{B}_1)$, $(R, \mathcal{B}_2)$ を b ブロックからなる互いに素な t-(r, k, λ) デザインの組とし，X_1, X_2 をそれぞれ $\mathcal{B}_1$, $\mathcal{B}_2$ の特性ベクトルの集合とする．このとき，(X_1, X_2) は次数 t サイズ b の PTE$_r$ 解を与える．

例 13 ([9, Example 1.3])**.** G を巡回置換 $(1234567) \in S_7$ で生成される位数 7 の巡回群，$\mathrm{Orb}_G(\mathbf{x}) := \{g\mathbf{x} \mid g \in G\}$ をベクトル $\mathbf{x} \in \mathbb{Q}^7$ の G 軌道，

$$X := \mathrm{Orb}_G(1,1,0,1,0,0,0),\ Y := \mathrm{Orb}_G(0,0,1,0,1,1,0)$$

とする．このとき，X, Y は例 9 の互いに素な 2-$(7,3,1)$ デザインに対応する特性ベクトルなので，定理 12 より，$[X] =_2^7 [Y]$ は PTE$_7$ 解である．

より一般に講演者らは，group divisible design と呼ばれる組合せデザインに対し，定理 12 を拡張した．

参考文献

[1] Andreas Alpers and Robert Tijdeman, *The two-dimensional Prouhet-Tarry-Escott problem*, J. Number Theory **123** (2007), no. 2, 403–412, DOI 10.1016/j.jnt.2006.07.001. MR2301222

[2] Craig Costello, Michael Meyer, and Michael Naehrig, *Sieving for twin smooth integers with solutions to the Prouhet-Tarry-Escott problem*, Advances in cryptology—EUROCRYPT 2021. Part I, Lecture Notes in Comput. Sci., vol. 12696, Springer, Cham, [2021] ©2021, pp. 272–301, DOI 10.1007/978-3-030-77870-5_10. MR4284266

[3] Leonard Eugene Dickson, *History of the theory of numbers. Vol. II: Diophantine analysis*, Chelsea Publishing Co., New York, 1966. MR0245500

[4] Viviana Ghiglione, *Switching Components in Discrete Tomography: Characterization, Constructions, and Number-Theoretical Aspects*, Ph.D. Thesis, Technische Universität München, 2019.

[5] A. Samad Hedayat, Neil J. A. Sloane, and John Stufken, *Orthogonal arrays*, Springer Series in Statistics, Springer-Verlag, New York, 1999. Theory and applications; With a foreword by C. R. Rao. MR1693498

[6] Santos Hernández and Florian Luca, *Integer roots chromatic polynomials of non-chordal graphs and the Prouhet-Tarry-Escott problem*, Graphs Combin. **21** (2005), no. 3, 319–323, DOI 10.1007/s00373-005-0617-0. MR2190791

[7] Hideki Matsumura and Masanori Sawa, *Ellipsoidal designs and the Prouhet–Tarry–Escott problem*, Ramanujan J. (published online) **68** (2025), no. 96, DOI 10.1007/s11139-025-01247-8.

[8] Munenori Inagaki, Hideki Matsumura, Masanori Sawa, and Yukihiro Uchida, *Combinatorial designs and the Prouhet–Tarry–Escott problem (in preparation)* (2025).

[9] ———, *On a group of normalized solutions of the higher-dimensional Prouhet–Tarry–Escott problem* (2025), available at `arXiv:2508.20733`.

[10] Badri Vishal Pandey, *Modular forms and ellipsoidal T-designs*, Ramanujan J. **58** (2022), no. 4, 1245–1257, DOI 10.1007/s11139-022-00572-6. MR4451518

[11] E. Prouhet, *M'emoire sur quelques relations entre les puissances des nombres*, C. R. Math. Acad. Sci. Paris **33** (1851), 224.

[12] Edward Maitland Wright, *Prouhet's 1851 solution of the Tarry-Escott problem of 1910*, Amer. Math. Monthly **66** (1959), 199–201, DOI 10.2307/2309513. MR0104622