学位論文要旨

Point arrangements on some combinatorial objects
(いくつかの組合せ論的対象上の点配置について)

梶浦 大起

本論文では，いくつかの数学的対象上の点配置について研究した。Chapter 1 では立方体上の点配置として digital net を，Chapter 2 では有限群やさらに一般的に association scheme 上の点配置である equi-distributed subset を論じた。

■Chapter 1 の概要　本章は [3] の内容をもとに議論を行う。Digital $(0, m, 3)$-net（in base 2）と呼ばれる立方体 $[0, 1)^3$ 上の点配置について考察する。$\mathbb{F}_2 = \{\overline{0}, \overline{1}\}$ を 2 元体，$\varphi : \mathbb{F}_2 \longrightarrow \mathbb{R}$ を $\overline{0}$ を 0，$\overline{1}$ を 1 に対応させる全単射，$\varphi_m : \mathbb{F}_2^m \longrightarrow \mathbb{R}$ を $\varphi_m((x_0, \ldots, x_{m-1})) = \sum_{i=0}^{m-1} \varphi(x_i)/2^{i+1}$ で定められる写像とする。

定義 1 (digital (t, m, s)-net in base 2)**.** $C_0, \ldots, C_{s-1}$ を $\mathbb{F}_2$ 係数の $m \times m$-行列として，$\mathcal{P} \subset [0, 1)^s$ を以下で定める:

$$\mathcal{P} := \{(\varphi_m(C_0\boldsymbol{x}), \ldots, \varphi_m(C_{s-1}\boldsymbol{x})) \in [0, 1)^s \mid \boldsymbol{x} \in \mathbb{F}_2^m\}.$$

このとき，点集合 $\mathcal{P}$ が $(C_0, \ldots, C_{s-1})$ を生成行列とする digital (t, m, s)-net (in base 2) であるとは，$\#\mathcal{P} = 2^m$ かつ任意の $(\boldsymbol{d}, \boldsymbol{a}) \in \{(d_0, \ldots, d_{s-1}, a_0, \ldots, a_{s-1}) \in \mathbb{Z}_{\geq 0}^{2s} \mid 0 \leq a_i < 2^{d_i},\ \sum_{i=0}^{s-1} d_i = m - t\}$ に対して以下を満たすこと:

$$\#(E_{\boldsymbol{d},\boldsymbol{a}} \cap \mathcal{P}) = 2^t.$$

ただし，$E_{\boldsymbol{d},\boldsymbol{a}} := \prod_{i=0}^{s-1} \left[a_i 2^{-d_i}, (a_i + 1)2^{-d_i}\right)$ とする。

Digital net は準モンテカルロ法という有限部分集合を用いた数値積分法と深い関係がある。(Hardy と Krause の) 全変動有界な函数について，m を固定すれば，digital (t, m, s)-net は t が小さいほど積分をよく近似する点集合になる。特に $t = 0$ の場合が最良であり，我々は興味がある。s が以下の値のときは $t = 0$ となる同値条件は古典的によく知られている:

$s = 1$ **の場合** 生成行列 C_0 が可逆行列であることと同値。
$s \geq 4$ **の場合** digital $(0, m, s)$-net (in base 2) は存在しない。

上記を踏まえて我々は $s = 2$ or 3 の場合に digital $(0, m, s)$-net (in base 2) を生成する行列に興味がある。ここで，$(C_0, \ldots, C_{s-1})$ が digital (t, m, s)-net を生成する場合は $(C_0, \ldots, C_{s-2})$ は digital $(t, m, s-1)$-net を生成することが知られているため，特に $s = 3$ の場合を詳しく知りたい。

本論文では特に擬似乱数生成法でよく用いられる線型極大周期列によって生成される digital net が $t = 0$ の場合について議論した。線型極大周期列とは，位数が $2^m - 1$ となる $\mathbb{F}_2$ 係数 $m \times m$ 行列 B で定義される線形漸化式 $\boldsymbol{x}_{n+1} = B\boldsymbol{x}_n$ と 0 でない初期値ベクトル $\boldsymbol{x}_0 \in \mathbb{F}_2^m$ により生成されるベクトルの列 $\{\boldsymbol{x}_n\}$ である。本論文では線型極大周期列を用いて以下のように定義される点集合 $\mathcal{P}$ について考える:

$$\mathcal{P} := \{(\varphi_m(\boldsymbol{x}_i), \varphi_m(\boldsymbol{x}_{i+1}), \varphi_m(\boldsymbol{x}_{i+2})) \in (\mathbb{F}_2^m)^3 \mid 0 \leq i < 2^m - 1\} \cup \{0\}.$$

このとき，$\mathcal{P}$ は (I, B, B^2) で生成される digital net (in base 2) となる。本論文では主定理として以下の定理を示した:

定理 2. $m \geq 1$ を正の整数として，B を $\mathbb{F}_2$ 係数の $m \times m$ 行列とする。このとき，以下が同値:

1. m 次の単位行列を I として，(I, B, B^2) は digital $(0, m, 3)$-net (in base 2) を生成する，
2. ある正則下三角行列 L を用いて，$B = LPJL^{-1}$ とかける。ここで，P と J は以下で定める $\mathbb{F}_2$ 係数の行列である:

$$P := \begin{pmatrix} \binom{0}{0} & \cdots & \binom{m-1}{0} \\ & \ddots & \vdots \\ & & \binom{m-1}{m-1} \end{pmatrix}, \quad J := \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}.$$

この定理と $(LPJL^{-1})^3 = I$ を合わせて，最初の興味であった線型極大周期列による生成法について以下のことがわかる:

系 3. 定理と同じ記号を用いる。(I, B, B^2) で生成される digital net が $t = 0$ の場合，B の位数は 3 である。i.e., $m > 2$ の場合には，線型極大周期列による生成法で digital $(0, m, 3)$-net (in base 2) は生成できない。

最後に，$s = 3$ の場合に $t = 0$ な digital net (in base 2) は [3] の後，[1] によって完全に分類されたことを紹介しておく。

■Chapter 2 の概要　本章は [2] の内容をもとに議論を行う。有限群 G の空でない真部分集合 D は，G の任意の非単位元 a に対して，$a = d_1^{-1} d_2$ となる $(d_1, d_2) \in D \times D$ の個数が a によらず一定の場合に difference set と呼ばれる。difference set は有限群の群軌道を用いて対称 2-design を構成する強力な方法として導入された。以来，導入から 60 年近く経った現在でも，様々な difference set の系列が構成されたり，具体的な群での存在・非存在が調べられている。本博士論文では，difference set の一般化として，以下のように概念を導入する。

定義 4 (Equi-distributed subset)**.** X を v 点集合，$(X, \{R_i\}_{i=0}^{d})$ を unital relation partiton（有向完全グラフの分割）とする。このとき，k 点部分集合 $Y \subset X$ について，任意の $i \neq 0$ に対して $\lambda = \#(R_i \cap (Y \times Y))/\#R_i$ のとき，(v, k, λ)-equi-distributed subset と呼ぶ。

台集合が有限群 G である unital relation partiton を構成する方法は様々に知られている。その中でも，thin association scheme と群 association scheme と呼ばれるふたつが代表的である。G の thin association scheme 上の equi-distributed subset は G の difference set の概念に他ならない。G の群 association scheme 上の equi-distributed subset を G の pre-difference set と呼ぶ。一般に G の difference set は G の pre-difference set でもある。

本論文では equi-distributed subset の一般論を展開し，存在・非存在性を中心に幾つかの定理を示した。それらの系として幾つかの有限群に対して具体的に pre-difference set を構成した。特に，以下の結果が得られた:

定理 5. G を有限群として，N をその部分群，A を部分アーベル群とする。写像 $\varphi : N \times A \longrightarrow G$ を $\varphi(n, a) := na$ として定める。φ が全単射（i.e., $N \cap A = \{e\}$ かつ全射）であるとき，もし $N \times A$ に difference set D が存在すれば，$\varphi(D)$ は G の pre-difference set である。

系 6. 位数 16 の正二面体群 D_{16} や $\mathbb{F}_3$ 係数 3×3 上三角行列のなす群 $UT(3, 3)$ に対して，pre-difference set が構成できる。特に，非自明な difference set を持たないが非自明な pre-difference set を持つような群の例を発見した。

定理 7. G_1 と G_2 を有限群，D_i を (v_i, k_i, λ_i)-pre-difference set（$i = 1$ or 2）とする。このとき，以下が同値:

1. $(D_1 \times D_2) \sqcup (D_1^c \times D_2^c)$ が $G_1 \times G_2$ 上の pre-difference set
2. $v_1 = 4(k_1 - \lambda_1)$ かつ $v_2 = 4(k_2 - \lambda_2)$。

系 8. 位数 16 の正二面体群 D_{16} の n 回直積の列 $\{D_{16}^n\}_{n=1}^{\infty}$ に対して，pre-difference set であるが difference set でない無限系列をひとつ構成した。

定理 9. G を指数 2 の部分群を含む群とする。G の (v, k, λ)-pre-difference set が存在するならば，$k - \lambda$ は平方数である。

定理 10. 以下の群には非自明な pre-difference set が存在しない:

1. G の位数が奇素数 p と正の整数 α を用いて $2p^\alpha$ とかける場合，
2. G の位数が素数 p と奇数 α を用いて $4p^\alpha$ とかけて，しかも指数 2 の部分群を持つ場合。

参考文献

[1] R. Hofer, K.Suzuki, *A complete classification of digital (0,m,3)-nets and digital (0,2)-sequences in base 2*, Unif. Dist. Theo., Vol. 14, 2019(43-51).

[2] H. Kajiura, M. Matsumoto, T. Okuda, *Non-existence and construction of pre-difference sets, and equi-distributed subsets in association schemes*, Grph. & Comb., Vol. 37, 2021 (1531-1544).

[3] H. Kajiura, M. Matsumoto, K. Suzuki, *Characterization of matrices B such that* (I, B, B^2) *generates a digital net with t-value zero*, Fin. Fld. Thr. Appl., Vol. 52, 2018 (289-300).