集中講義 応用数学特論 II

Day 5 巡回デザインとその応用

担当：盧　暁南 (山梨大学)
xnlu@yamanashi.ac.jp

2021 年 8 月 31 日

本日の内容

本日は巡回準差集合 (cyclic ADS)，巡回準直交配列 (CAOA) およびその応用 (自己相関関数マグニチュードが小さい最適系列，fMRI 実験における最適計画) について最新の研究結果を紹介する．

0　記号

- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$: 位数 n の巡回群
- $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$: $\mathbb{Z}_n$ の非 0 要素全体の集合
- $\mathbb{F}_q$: 位数 q の有限体

1　二元系列とその自己相関関数

定義 1.1. 無限二元系列 $\mathbf{s} = (s_0, s_1, \ldots, a_{n-1}, a_n, a_{n+1}, \ldots)$ において，次の式が満たされるとき $\mathbf{s}$ が**周期** (period) n を持つという．

$$s_i = s_{i+n} \qquad \forall i \geq 0.$$

注 1.2. 便宜上，周期 n の無限系列は長さ n の (有限) 系列として取り扱うことができる．

定義 1.3. 系列 $\mathbf{s} = (s_t) \in \{0,1\}^n$ の巡回シフト w に関する**周期的自己相関関数** (periodic autocorrelation) は以下に定義する．

$$\rho_{\mathbf{s}}(w) = \sum_{t=0}^{n-1} (-1)^{s_{t+w} - s_t}.$$

ここで，s_{t+w} の添字 $t+w$ は mod n で計算する．

注 1.4. シフト w が n で割り切れる場合，$\rho_{\mathbf{s}}(w) = n$ となり，$w \not\equiv 0 \pmod{n}$ (非自明なシフト，または off-peak なシフトと呼ばれる) だけを考えば良い．

定義 1.5. 系列 $\mathbf{s}$ の非自明なシフトにおける自己相関関数値の絶対値の最大値は，**自己相関のマグニチュード** (autocorrelation magnitude) といい，次式で表される．

$$\max_{\tau \not\equiv 0 \pmod{N}} |\rho_{\mathbf{s}}(\tau)|$$

注 1.6. 無線情報通信，レーダシステム，ストリーム暗号 (stream cipher) などの応用において，**自己相関のマグニチュードが低い系列**が望ましい．

定義 1.7. 任意の $w \not\equiv 0 \pmod n$ に対して，次の条件を満たす 2 元系列 $\mathbf{s}$ は**最適な** (optimal) 自己相関を持つという．([1, 2] 参照).

$$\rho_{\mathbf{s}}(w) \in \begin{cases} \{-1\} & \text{if } n \equiv 3 \pmod 4, \\ \{1, -3\} & \text{if } n \equiv 1 \pmod 4, \\ \{2, -2\} & \text{if } n \equiv 2 \pmod 4, \\ \{0, -4\} \text{ or } \{0, 4\} & \text{if } n \equiv 0 \pmod 4. \end{cases} \tag{1}$$

簡単化するため，これから最適な自己相関マグニチュードを持つ系列を**最適系列**という．

本日の講義では $n \equiv 2 \pmod 4$ の場合を中心に議論する．

定理 1.8. 以下の n に対して周期 n の最適系列が存在する．

(i) $n = q - 1$．ここで $q \equiv 3 \pmod 4$ は素数冪である．このような系列は SLCE 系列 (論文著者の頭文字) と呼ばれる．(cf. Sidelnikov [12], Lempel-Cohn-Eastman [6])

(ii) $n = 2p$．ここで $p \equiv 5 \pmod 8$ は素数である．このような系列は DHM 系列 (論文著者の頭文字) と呼ばれる．(cf. Ding-Helleseth-Martinsen [4])

2 準差集合

定義 2.1. $\mathbb{Z}_n$ の部分集合 D において，D の**差リスト** (list of differences) ΔD は次に定義する．

$$\Delta D = \{a - b \mid a, b \in D, a \neq b\}$$

ここで，ΔD は重複した要素が認められる**多重集合** (multiset) として扱う．

定義 2.2. $\mathbb{Z}_n$ の k 元部分集合 D において，ΔD に $\mathbb{Z}_n$ のすべての非 0 要素がちょうど λ 回現れるとき，D を $\mathbb{Z}_n$ 上の (n, k, λ) **差集合** (difference set; DS) という．また，群構造として $\mathbb{Z}_n$ を考えるため，(n, k, λ) **巡回差集合** (cyclic difference set) ともいう．

定義 2.3. $\mathbb{Z}_n$ の k 元部分集合 D において，ΔD に $\mathbb{Z}_n^*$ の中の t 個の要素が λ 回ずつ現れ，残りの $n - t - 1$ 個の要素が $\lambda + 1$ 回ずつ現れるとき，D は $\mathbb{Z}_n$ 上の (n, k, λ, t) **準差集合** (almost difference set; ADS) という．また，群構造として $\mathbb{Z}_n$ を考えるため，(n, k, λ, t) **巡回準差集合** (cyclic almost difference set) ともいう．

命題 2.4. 周期 $n \equiv 2 \pmod 4$ の最適系列 $\iff$ $\mathbb{Z}_n$ 上の $(n, \frac{n}{2}, \frac{n-2}{4}, \frac{3n-2}{4})$-ADS.

定義 2.5. 有限体 $\mathbb{F}_q$ において $C_i^{(e,q)} = \{g^{et+i} : 0 \le t \le (q-1)/e\}$ は**円分剰余類** (cyclotomic coset) という．ここで，$e \mid (q-1)$ であり，g は $\mathbb{F}_q$ の生成元である．例えば，

- $C_1^{(2,q)} = \{g^{2t+1} : 0 \le t < (q-1)/2\}$.
- $C_i^{(4,q)} = \{g^{4t+i} : 0 \le t < (q-1)/4\}$ $(0 \le i \le 3)$.

定理 2.6 (Sidelnikov [12], Lempel-Cohn-Eastman [6])**.** $q \equiv 3 \pmod 4$ を素数冪とし，g を有限体 $\mathbb{F}_q$ の生成元とする．(有限体の乗法群に同型となる群) $\mathbb{Z}_{q-1}$ の部分集合 D を $\log_g(C_1^{(2,q)} - 1)$ で定義する．ここで，$\log_g$ は $\mathbb{F}_q$ 上で底 g における離散対数を表す．以上で定義した D は $\mathbb{Z}_{q-1}$ 上の $(q-1, \frac{q-1}{2}, \frac{q-3}{4}, \frac{3q-5}{4})$ ADS になる．

定理 2.7 (Ding-Helleseth-Martinsen [4])**.** $p \equiv 5 \pmod 8$ を素数とする．有限体 $\mathbb{F}_p$ に適切な生成元を選んで，整数 $i, j, l \in \{0, 1, 2, 3\}$ を以下の組合せから選ぶことにする．

(i) $p-4$ が平方数であるとき，$(i,j,l) \in \{(0,1,3),(0,2,3),(1,2,0),(1,3,0)\}$ ([4, Theorem 3]) ;

(ii) $p-1$ が平方数であるとき，$(i,j,l) \in \{(0,1,2),(0,3,2),(1,0,3),(1,2,3)\}$ ([4, Theorem 4]).

集合 C_0, C_1 を次に定義する．

$$C_0 = C_i^{(4,p)} \cup C_j^{(4,p)}, \qquad C_1 = C_j^{(4,p)} \cup C_l^{(4,p)}.$$

このとき，以下の D は ($\mathbb{Z}_{2p}$ に同型となる群) $\mathbb{Z}_2 \times \mathbb{Z}_p$ 上の $(n, \frac{n}{2}, \frac{n-2}{4}, \frac{3n-2}{4})$-ADS である．

$$D = \big(\{0\} \times C_0\big) \cup \big(\{1\} \times C_1\big) \cup \big\{(0,0)\big\}$$

3 巡回準直交配列

定義 3.1 (Lin–Phoa–Kao [7]). $k \times n$ の 2 元巡回配列 $\mathbf{A}$ において，以下の条件が満たされるとき，$\mathbf{A}$ は $(n,k,2,t,b)$ **巡回準直交配列** (circulant almost orthogonal array; CAOA) という．

- $\mathbf{A}$ の任意の $t \times n$ 部分配列において，2 つの t タプル $\mathbf{a}_1, \mathbf{a}_2 \in \{0,1\}^t$ に対して $|\lambda(\mathbf{a}_1) - \lambda(\mathbf{a}_2)| \le b$ が成り立つ．ここで $\lambda(\mathbf{a})$ は列ベクトル $\mathbf{a}$ の出現回数を表す．

命題 3.2 (盧–三嶋–宮本–神保 [8]). 周期 $n \equiv 2 \pmod 4$ の最適系列 $\implies$ CAOA$(n, n-1, 2, 2, 1)$

レポート課題

課題 1. 定理 2.6 を用いて長さ $n = 18$ の SLCE 系列を構成せよ．

課題 2. $100 \le n \le 200$ の $n \equiv 2 \pmod 4$ の整数の中に，SLCE 系列 (定理 2.6) または DHM 系列 (定理 2.7) が存在するようなパラメータ n をすべて列挙せよ．

レポート提出期限：9 月 6 日 (月) 23:59 まで

参考文献

[1] K. T. Arasu, C. Ding, T. Helleseth, P. V. Kumar, and H. M. Martinsen. Almost difference sets and their sequences with optimal autocorrelation. *IEEE Trans. Inform. Theory*, 47(7):2934–2943, 2001.

[2] Y. Cai and C. Ding. Binary sequences with optimal autocorrelation. *Theoret. Comput. Sci.*, 410(24-25):2316–2322, 2009.

[3] T. W. Cusick, C. Ding, and A. R. Renvall. *Stream Ciphers and Number Theory*. Elsevier, revised edition, 2004.

[4] C. Ding, T. Helleseth, and H. Martinsen. New families of binary sequences with optimal three-level autocorrelation. *IEEE Trans. Inform. Theory*, 47(1):428–433, 2001.

[5] S. W. Golomb and G. Gong. *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*. Cambridge University Press, 2005.

[6] A. Lempel, M. Cohn, and W. Eastman. A class of balanced binary sequences with optimal autocorrelation properties. *IEEE Trans. Inform. Theory*, IT-23(1):38–42, 1977.

[7] Y.-L. Lin, F. K. H. Phoa, and M.-H. Kao. Optimal design of fMRI experiments using circulant (almost-) orthogonal arrays. *The Annals of Statistics*, 45(6):2483–2510, 2017.

[8] X.-N. Lu, M. Mishima, N. Miyamoto, and M. Jimbo. Optimal and efficient designs for fMRI experiments via two-level circulant almost orthogonal arrays. *Journal of Statistical Planning and Inference*, 213:33–49, 2021.

[9] K. Momihara, Q. Wang, and Q. Xiang. Cyclotomy, difference sets, sequences with low correlation, strongly regular graphs, and related geometric substructures. In K.-U. Schmidt and A. Winterhof, editors, *Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications*, volume 23 of *Radon Series on Computational and Applied Mathematics*, pages 178–205. De Gruyter, 2019.

[10] E. H. Moore and H. S. K. Pollatsek. *Difference Sets: Connecting Algebra, Combinatorics, and Geometry*. American Mathematical Society, 2013.

[11] X. Niu, H. Cao, and K. Feng. Binary periodic sequences with 2-level autocorrelation values. *Discrete Mathematics*, 343(3):111723, 2020.

[12] V. M. Sidelnikov. Some k-valued pseudo-random sequences and nearly equidistant codes. *Probl. Peredachi Inf.*, 5(1):16–22, 1969.