On a number-theoretic problem arsing from designs of efMRI experiments

神戸大学 大学院システム情報学研究科 情報科学専攻
佐竹 翔平 (Shohei SATAKE)

1 導入

efMRI 実験では, MRI 装置に被験者を乗せて画像列を見せたときの脳の反応を測定する. 脳医学においては, 脳の反応を測定する関数として, 血流動態関数が知られており, 実験ではそのピークを推定することが目的となる. 関数のよい推定を行うにあたっては, 統計的によい推定精度をもつと期待される画像列を設計することが求められる. そういった画像列の候補として, m-系列や直交配列による列などが提案されているが, 非常によい推定精度を保証する代わりに, 実験回数 (刺激列の長さ) に強い制約が課されるという実用上の欠点がある. 本稿で扱う巡回的準直交配列 (Circulant almost orthogonal array, CAOA) は, よい推定精度を与え, かつより柔軟な回数の実験を実現する画像列を与えるべく, Lin-Phoa-Kao [8] によって定義された. 最近 Yoshida-Satake-Phoa-Sawa [11] では, 素体上の平方剰余から新しい CAOA の無限系列を構成した. その構成法を考える上では, 平方剰余の分布について考察する必要がある. 本稿では, 整数論においてこれまでの先行研究で取り扱われてきた平方剰余分布の問題のある種の一般化を与え, 関連するいくつかの結果を紹介する. さらにそこから導かれる, [11] の構成法から得られる CAOA が存在するための必要条件についても述べる.

2 巡回的準直交配列とその構成

CAOA の定義は以下のように与えられる.

定義 1. *n, K, s, t, b を自然数とする. M を $0, 1, 2, \ldots, s-1$ を成分にもつ $K \times n$ 巡回行列とする. M の各 $t \times n$ 小行列内に, 長さ t の順序列 $\boldsymbol{a}$ が (小行列によらず) $\lambda(\boldsymbol{a})$ 回出現し, 任意の長さ t の順序列 $\boldsymbol{a}$, $\boldsymbol{b}$ に対して, $|\lambda(\boldsymbol{a}) - \lambda(\boldsymbol{b})| \leq b$ が成り立つとき, M をレベル s, 強さ t, 帯域 b の巡回的準直交配列 (Circulant almost orthogonal array, CAOA) とよぶ. また, そのような CAOA を $CAOA(n, K, s, t, b)$ と表す.*

ここで, CAOA の 1 行目が所望の画像列に対応しており, さらに CAOA から統計的なよさを測る一つの尺度 (D-効率性) が計算される (詳細は [8] を参照). 本稿では, 0 または 1 を成分にもつ $s = 2$ の CAOA に着目する. 最初の CAOA の構成として, [8] では, $CAOA(n, K, 2, 2, 1)$ の構成法が与えられている. これに対し, 最近 Yoshida-Satake-Phoa-Sawa [11] では, [8] での構成例よりも強いある

統計的利点をもつ $CAOA(n, K, 2, 3, 1)$ の構成法を与えることができた. いま, $p \equiv 3 \pmod 4$ を素数とし, σ_p を $\mathbb{Z}/p\mathbb{Z}$ の平方剰余の 0-1 特性ベクトルとおく. すなわち, σ_p の第 i 成分は i が法 p で平方剰余のとき 1, そうでないとき 0 で与えられるとする. さらに, σ_p を第 1 列目にもつ巡回行列を N, その 0 と 1 を反転して得られる巡回行列を $\overline{N}$ とし,

$$N = \begin{bmatrix} \boldsymbol{a}_0 \\ \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{a}_{p-1} \end{bmatrix}, \ \overline{N} = \begin{bmatrix} \boldsymbol{b}_0 \\ \boldsymbol{b}_1 \\ \vdots \\ \boldsymbol{b}_{p-1} \end{bmatrix}$$

とおく. 次に N と $\overline{N}$ からそれぞれ K の連続する行 $\boldsymbol{a}_i$, $\boldsymbol{a}_{i+1}$,..., $\boldsymbol{a}_{i+K-1}$ および $\boldsymbol{b}_j$, $\boldsymbol{b}_{j+1}$, ..., $\boldsymbol{b}_{j+K-1}$ を抜き出す. ただし, それぞれの行は

$$M = \begin{bmatrix} \boldsymbol{a}_i & \boldsymbol{b}_j \\ \boldsymbol{a}_{i+1} & \boldsymbol{b}_{j+1} \\ \vdots & \vdots \\ \boldsymbol{a}_{i+K-1} & \boldsymbol{b}_{j+K-1} \end{bmatrix}. \tag{1}$$

が巡回行列となるように選ばれるとする. このとき, M は以下のパラメータをもつ CAOA となる.

定理 2 (吉田-佐竹-Phoa-澤 [11])**.** *M は $CAOA(2p, K, 2, 3, 1)$ である.*

実際にそのような行たちを求めることは, K が定数であれば, 例えば適当な定数 $l > K$ をとって, $0, 1, 2, \ldots, l$ に対して, p に応じて平方剰余の相互法則を用いて, 具体的に $0, 1, 2, \ldots, l$ 上の分布を計算することで可能となる. 一方で, 素数 p に応じて, K はどこまで大きくなれるかという一つの自然な問題が浮かび上がってくる. この問題は N と $\overline{N}$ が巡回行列である (すなわち, それぞれは第 1 列目で定まる) ことに着目することで, 次のように定式化できる.

問題 3. *σ_p 内の 2 つの連続部分列で, 一方がもう一方の 0-1 反転で得られるような列の最大長 H を求めよ (または評価せよ).*

ここで, $H + 1$ が上記の構成法で得られる $CAOA(2p, K, 2, 3, 1)$ における K の最大値となることに注意せよ.

3 平方剰余の分布と CAOA の存在条件

平方剰余の分布に関しては, 整数論において C. F. Gauss から始まって, 150 年以上の長きにわたって考えられてきた. 中でも σ_p 内の連続する平方剰余 (または非剰余) の部分列の最大長 R (または N) の問題は, 最初は E. Landau, G. Polya, I. Schur らによって考えられ (例えば [2], [5, Chapter 9] を参照), 特に Brauer [1], [2], Davenport-Erdős [4], Gel'fond-Linnik [5, Chapter 9], Hudson [6], Hummel [7], Pollack-Treviño [9] らは, 初等的な組合せ論的手法を用いて, 多くの結果を生み出している. しかしながら, 今回定式化した問題 3 のように一般的な列に焦点を当てた研究は, 講演者の知る限り, これまでなかったように思われる (ただし, [2] の直後のレビューで D. E. Knuth がその問題を提起している). 一方で, $p \equiv 3 \pmod 4$ の場合, $R = N$ であることから, 問題 3 は上記の連続する

平方剰余 (または非剰余) の最長部分列の問題の一般化となっている.

以上を踏まえ, 問題 3 に関する結果を紹介する. まず次の定理は完全に初等的な手法で得られる.

定理 4. 全ての奇素数 p *(*$p \equiv 3 \pmod 4$ でなくてもよい*)* に対して, $H \leq \sqrt{7p} + 1$ が成り立つ.

さらに, 組合せ論的な数え上げのアイデアと Weil の評価式による数え上げを用いることで (したがって初等性が定理 4 に比べて落ちてしまうが), すべての素数 $p \equiv 3 \pmod 4$ に対して, 定理 4 を改良する次の結果が得られる.

定理 5. 全ての素数 $p \equiv 3 \pmod 4$ に対して, $H \leq \sqrt{2p} + 2\sqrt{7}p^{\frac{1}{4}} + 11$ が成り立つ.

ここで, Burgess [3] の部分指標和の評価から, どのような $\delta > 0$ に対しても, 十分大きな p に対して, $H \leq O(p^{1/4+\delta})$ が成り立つ. この評価式は漸近的には, 定理 4 および 5 よりよい評価式であるが, 十分大きな素数に対して成立する評価式である. 我々は CAOA の動機からすべての素数 $p \equiv 3 \pmod 4$ に対して成り立つ評価式に着目していることに注意されたい.

以上から我々の構成法によって作られる CAOA が存在するための下記の必要条件が得られる.

系 6. 定理 2 の $CAOA(2p, K, 2, 3, 1)$ が存在するならば, $K \leq \sqrt{2p} + 2\sqrt{7}p^{\frac{1}{4}} + 12$ である.

謝辞

本研究にあたり, 論文 [9] をご教示くださった Paul Pollack 先生に感謝致します. 本研究は, 科学研究費補助金 (特別研究員奨励費 課題番号 18J11282) の助成を受けています.

参考文献

[1] A. Brauer, Über die Verteilung der Potenzreste, *Math. Z.*, **35** (1932), 39–50.

[2] A. Brauer, Combinatorial methods in the distribution of kth power residues, In *Combinatorial Mathematics and its Applications* (Proc. Conf., Univ. North Carolina, Chapel Hill, N.C., 1967), pp. 14–37 Univ. North Carolina Press, 1969.

[3] D. A. Burgess, The distribution of quadratic residues and non-residues. *Mathematika* **4** (1957), 106–112.

[4] H. Davenport, P. Erdős, The distribution of quadratic and higher residues, *Publ. Math. Debrecen*, **2** (1952) pp. 252–265.

[5] A. O. Gel'fond, Y. V. Linnik, Elementary Methods in the Analytic Theory of Numbers, Pergamon Press, 1966.

[6] R. H. Hudson, On a conjecture of Issai Schur, *J. Reine Angew. Math.*, **289** (1977), 215–220.

[7] P. Hummel, On consecutive quadratic non-residues: a conjecture of Issai Schur, *J. Number Theory*, **103** (2003), no. 2, 257–266.

[8] Y. L. Lin, F. K. H. Phoa, M. H. Kao, Optimal design of fMRI experiments using circulant (almost-)orthogonal arrays, *Ann. Statist.*, **45** (2017), no. 6, 2483–2510.

[9] P. Pollack, E. Treviño, The primes that Euclid forgot, *Amer. Math. Monthly*, **121** (2014), no. 5, 433–437.

[10] Shivarajkumar, Beyond Schur's conjecture, *Amer. Math. Monthly*, **123** (2016), no. 1, 66–70.

[11] K. Yoshida, S. Satake, F. K. H. Phoa, M. Sawa, "Circulant almost-orthogonal arrays with strength 3 and bandwidth 1: Constructions and existence", Submitted.