ある equiangular tight frame から得られる conditional な制限等長性と関連するグラフ理論的結果

佐竹 翔平 (熊本大学 大学院先端科学研究部 (工学系))*

概 要

圧縮センシングの理論において, 制限等長性 (RIP) をもつ RIP 行列の構成は重要な研究課題の一つである. Equaingular tight frame (ETF) は最適な coherence をもつため, coherence に基づく RIP の評価のもとでは最良の RIP を保証するが, 一方で RIP に関する square-root bottleneck とよばれる従来課されていた制約はこの方法では超えることができない. Bandeira, Mixon および Moreira は, 有限体の平方剰余から定義される Renes と Zauner による ETF に着目し, 位数が素数 $p \equiv 1 \pmod 4$ である有限体の場合に, Chung による Legendre 指標に関する予想のもとで, この ETF が square-root bottleneck を超える RIP をもつことを示した.

本稿では, Paley グラフ予想の下で, Bandeira らの結果を一般の奇素数 p の場合に拡張する. さらに, Renes と Zauner による ETF のもつ RIP から得られるグラフ理論的な結果についても説明する. 本稿における結果の詳細は, 論文 [25] を参照されたい.

1 序

圧縮センシングの理論は, 少ない観測結果からスパースな原信号の復元可能性を保証するため, 画像処理や MRI などへ幅広く応用されている. 数学的な問題設定は, M, N を $M \leq N$ なる自然数, Φ を複素 $M \times N$ 行列, $\mathbf{x}$ を N 次元複素ベクトル, y を M 次元複素ベクトルとしたとき, $\mathbf{x}$ に関する不定方程式系 $\mathbf{y} = \Phi\mathbf{x}$ から一意に $\mathbf{x}$ を求めるということになる. もちろん $M < N$ の場合, 上述の不定方程式系の解は無数に存在するため, $\mathbf{x}$ を一意的に求めることは一般に不可能である. 一方で $\mathbf{x}$ がスパース, すなわち非ゼロ成分が少ないならば, 適切な行列 Φ を選ぶことで $\mathbf{x}$ を一意的に求められることが証明されており, これが 圧縮センシングの基礎的な結果の 1 つといえる. 特に, 行列 Φ が以下で定義される**制限等長性** (*restricted isometry property*, *RIP*) をもつならば, スパースな $\mathbf{x}$ を一意的に求めることが可能であることが示されている [8]. 以降は, 行列の列ベクトルのノルムはすべて 1 であるとする.

定義 1 (制限等長性) Φ を $M \times N$ 行列とし, 自然数 K, M, N は $K \leq M \leq N$ を満たし, 実数 δ は $0 \leq \delta < 1$ を満たすとする. このとき, 高々 K 個の非ゼロ成分をもつ長さ N の任意のベクトル *(K-**スパース**なベクトル)* に対して,

$$(1-\delta)||\mathbf{x}||^2 \leq ||\Phi\mathbf{x}||^2 \leq (1+\delta)||\mathbf{x}||^2$$

が成り立つならば, Φ は (K, δ)-*restricted isometry property* (*RIP*) をもつという. ここで, $||\cdot||$ はベクトルの ℓ_2 ノルムを表す.

Candès [8] によって, ある $\delta < \sqrt{2} - 1$ に対して Φ が (K, δ)-RIP をもてば, 任意の K-スパースなベクトル $\mathbf{x}$ が $\mathbf{y} = \Phi\mathbf{x}$ から復元できることが示されている. K が大きければ大きい

*日本学術振興会特別研究員 PD 熊本大学 大学院先端科学研究部 (工学系) (〒 860-8555 熊本県熊本市中央区黒髪 2 丁目 39 番 1 号, E-mail: shohei-satake@kumamoto-u.ac.jp)

ほど復元可能性を保証できるベクトルの範囲が広がるため, できるだけ大きな K に対する (K,δ)-RIP をもつ行列の構成が重要となる. 例えば, 各成分が Bernoulli 分布に従う $M \times N$ ランダム行列は, 各 δ に対して, $\delta\frac{M}{\log(2N/M)}$ のオーダーの K に対して (K,δ)-RIP を高い確率でもつことが知られている ([7] など). また, $N \times N$ 離散 Fourier 変換行列 (DFT 行列) から一様ランダムに行を選び, 各列ベクトルを正規化して得られる $M \times N$ ランダム部分行列も, 各 δ とある $C > 0$ に対して, $\frac{M}{\log M} \geq \frac{C}{\delta^2} K \log^2 K \log N \log \varepsilon^{-1}$ が成り立つならば, 確率 $1-\varepsilon$ で (K,δ)-RIP をもつ [21]. しかし, 与えられた行列の制限等長性を評価する問題は NP 困難であり [1], 与えられた行列の制限等長性を判定するための実用的なアルゴリズムも, 講演者の知る限り, 未だ与えられていない. 以上の詳細に関しては [2] などを参照されたい.

こうした状況から, *deterministic* に構成した行列の制限等長性を評価する問題が Tao [29] により提示され, 盛んに研究がなされている. その多くにおいて, 構成した行列の RIP を示す際には, 行列の *coherence* が注目されてきた. 簡単のため, 本稿で登場する行列の列ベクトルの ℓ_2 ノルムはすべて 1 であるとする.

定義 2 (Coherence) $M \times N$ 行列 Φ の列ベクトルを $\phi_1, \phi_2, \ldots, \phi_N$ とおく. このとき, 行列 Φ の *coherence* μ は以下で定義される.

$$\mu(\Phi) := \max_{1 \leq j \neq k \leq N} |\langle \phi_j, \phi_k \rangle|.$$

ただし, $\langle \cdot, \cdot \rangle$ は *Hilbert* 空間 $\mathbb{C}^M$ の標準内積を表す.

定理 3 ([4] など) 任意の $M \times N$ 行列 Φ は, 各 $K \leq M$ に対し, $(K, (K-1)\cdot\mu(\Phi))$-*RIP* をもつ.

定理 3 は, $K < \mu(\Phi)^{-1} + 1$ の場合に Φ の (K,δ)-RIP を保証する. したがって, できるだけ小さな coherence をもつ行列の構成が望まれるが, 一方で coherence に対しては以下の **Welch の不等式**が知られている.

定理 4 (Welch の不等式, [31]) 任意の $M \times N$ 行列 Φ に対して,

$$\mu(\Phi) \geq \sqrt{\frac{N-M}{M(N-1)}}.$$

したがって, coherence によって保証できる RIP には $K = O(\sqrt{M})$ という制約 (*square-root bottleneck*) が課されてしまう. このような状況から, 以下の問題が現れる.

問題 5 ([4] など) ある $\gamma > 1/2$, $C > 0$ に対して, $K \geq CM^\gamma$ および $\delta < \sqrt{2} - 1$ なる (K,δ)-*RIP* をもつ $M \times N$ 行列を *deterministic* に構成せよ.

問題 5 への最初の解は Bourgain ら [4] により与えられ, Mixon [19] による一般化も存在する. 一方で, Welch の不等式の等号を達成する *equiangular tight frame* (*ETF*) ([2], [27] など) たちの中から, 問題 5 への解を見つけ出そうという研究も Bandeira ら [2] らによって行われている. 有望な候補の一つとして, Zauner [32] と Renes [22] による, 有限体上の平方剰余から定義される ETF[1]がある ([2] 参照). Bandeira, Mixon および Moreira [3] は, Legendre 指標に関する Chung [10] の予想のもとで, 素数 $p \equiv 1 \pmod 4$ と位数 p の有限体 $\mathbb{F}_p$ の場合に, Renes と Zauner による ETF が問題 5 の解となることを示した. さらに, このとき強正則グラフの一種である **Paley グラフ**のクリーク数に関して既存の上界が改良できることも示される [3]. しかし, 例えば素数 $p \equiv 3 \pmod 4$ の場合には [3] の議論は一般に通用しない.

[1] [3] では **Paley 行列**ともよばれている.

本稿では, 2 節で説明する **Paley グラフ予想**のもとで, Bandeira らの結果を一般の奇素数の場合に拡張する. 次に Renes と Zauner による ETF が問題 5 の解となる場合には, Paley グラフのクリーク数だけでなく, **Paley トーナメント**内の推移的トーナメントのサイズの上界も改良できることを説明する; これらの結果とグラフ理論, 特に Ramsey 理論との関連は 3 節で説明する. 最後に 4 節では関連する注意と今後の課題について述べる.

2 準備

本稿では, p は奇素数を表すものとする. 位数 p の**有限体** $\mathbb{F}_p$ は, 剰余体 $\mathbb{Z}/p\mathbb{Z}$ と同一視できる. 有限体 $\mathbb{F}_p$ の非ゼロな元 a に対して, $X^2 \equiv a \pmod{p}$ が解をもつとき, a を**平方剰余**とよぶ. 有限体 $\mathbb{F}_p$ 上には全部で $(p-1)/2$ 個の平方剰余が存在する. 有限体 $\mathbb{F}_p$ の **Legendre 指標** χ を以下で定義する.

$$\chi(x) := \begin{cases} 0 & x = 0; \\ 1 & x \text{ が平方剰余}; \\ -1 & \text{その他}. \end{cases}$$

ここで, 任意の $x, y \in \mathbb{F}_p$ に対して, $\chi(xy) = \chi(x)\chi(y)$ が成り立つ.

Renes と Zauner による ETF は以下のように定義される.

定義 6 ([22], [32]) 有限体 $\mathbb{F}_p$ の元を $0 = a_1, a_2, \ldots, a_p$, $\mathbb{F}_p$ の平方剰余を $b_1,\ b_2, \ldots, b_{\frac{p-1}{2}}$ とラベル付けする. 任意の $x \in \mathbb{F}_p$ に対して, $\psi(x) := \exp\Big(\frac{2\pi\sqrt{-1}}{p}x\Big)$ と定義する. このとき, $(p+1)/2 \times (p+1)$ 行列 Φ_p を以下で定義する.

$$\Phi_p := \begin{bmatrix} \frac{1}{\sqrt{p}} & \frac{1}{\sqrt{p}} & \cdots & \frac{1}{\sqrt{p}} & (\sqrt{-1})^r \\ \sqrt{\frac{2}{p}} & \sqrt{\frac{2}{p}}\psi(b_1a_2) & \cdots & \sqrt{\frac{2}{p}}\psi(b_1a_p) & 0 \\ \sqrt{\frac{2}{p}} & \sqrt{\frac{2}{p}}\psi(b_2a_2) & \cdots & \sqrt{\frac{2}{p}}\psi(b_2a_p) & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \sqrt{\frac{2}{p}} & \sqrt{\frac{2}{p}}\psi\big(b_{\frac{p-1}{2}}a_2\big) & \cdots & \sqrt{\frac{2}{p}}\psi\big(b_{\frac{p-1}{2}}a_p\big) & 0 \end{bmatrix}.$$

ただし r は $p \equiv 1\ (3) \pmod 4$ のとき $0\ (1)$ とする.

Bandeira, Mixon および Moreira [3] は Chung [10] による次の予想のもとで, $p \equiv 1 \pmod 4$ の場合に行列 Φ_p が問題 5 に対する解になることを示した.

予想 7 ([10]) 任意の $0 < \alpha \leq 1$ に対し, ある $\beta = \beta(\alpha) > 0$ が存在し, 十分大な素数 $p \equiv 1 \pmod 4$ とサイズが p^α より大きい任意の $S \subset \mathbb{F}_p$ に対し, 以下が成り立つ :

$$\Big|\sum_{s_1,s_2 \in S} \chi(s_1 - s_2)\Big| \leq |S|^{2-\beta}.$$

定理 8 ([3]) 十分大きな素数 $p \equiv 1 \pmod 4$ に対して予想 7が成り立つとき, ある $\gamma > 1/2$ と $\tau > 0$ に対し, 行列 Φ_p は $(p^\gamma, p^{-\tau})$-*RIP* をもつ.

一方で, 素数 $p \equiv 3 \pmod 4$ の場合は, 上記の予想を仮定しても Φ_p の所望の RIP を導出することができない; $p \equiv 3 \pmod 4$ の場合, 任意の $S \subset \mathbb{F}_p$ に対して, $\sum_{s_1,s_2 \in S} \chi(s_1 - s_2) = 0$ が成り立ってしまい, 自明な情報しか得られないためである.

そこで, 一般の奇素数 p の場合を扱うために, 以下の **Paley グラフ予想**に着目する ([8], [9], [15] などを参照).

予想 9 (Paley グラフ予想) 任意の $0 < \alpha \leq 1$ に対し, ある $\beta = \beta(\alpha) > 0$ が存在し, 十分大な奇素数 p とサイズが p^α より大きい任意の $S, T \subset \mathbb{F}_p$ に対して以下が成り立つ :

$$\Big| \sum_{s \in S, t \in T} \chi(s-t) \Big| \leq p^{-\beta} |S||T|.$$

3 Renes と Zauner による ETF の RIP

本稿における最初の主結果は, 次の定理 10 である.

定理 10 十分大きな奇素数 p に対して予想 *9*が成り立つならば, ある $\gamma > 1/2$ と $\tau > 0$ に対し, *Paley* 行列 Φ_p が $(p^\gamma, p^{-\tau})$*-RIP* をもつ.

したがって, 一般の奇素数 p に対して Φ_p が問題 5 の解になることが予想 9 のもとで示されたことになる.

次に定理 10 から得られるグラフ理論的な結果に関して述べる. まず, 序節で登場した Paley グラフと Paley トーナメントの定義を与える.

定義 11 (Paley グラフ) 素数 $p \equiv 1 \pmod 4$ に対して, p 頂点 **Paley グラフ** G_p は, 頂点集合に $\mathbb{F}_p$, 辺集合に $\{\{x, y\} \mid x, y \in \mathbb{F}_p, \chi(x-y) = 1\}$ をもつ無向グラフである.

定義 12 (Paley トーナメント) 素数 $p \equiv 3 \pmod 4$ に対して, p 頂点 **Paley トーナメント** T_p は, 頂点集合に $\mathbb{F}_p$, 辺集合に $\{(x, y) \mid x, y \in \mathbb{F}_p, \chi(x-y) = 1\}$ をもつトーナメント *(*有向完全グラフ*)* である.

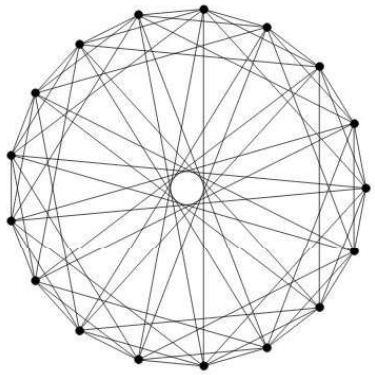

図 1: 17 頂点の Paley グラフ G_{17}

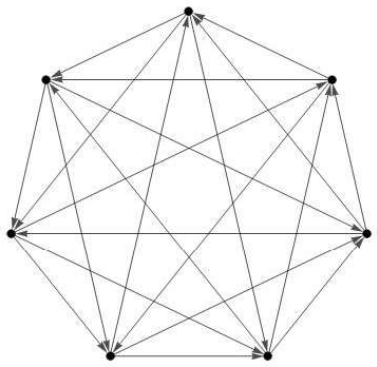

図 2: 7 頂点の Paley トーナメント T_7

グラフ理論において, G_p の**クリーク数** (完全部分グラフの最大サイズ) と T_p 内の**推移的トーナメント** (有向閉路をもたないトーナメント) の最大サイズを上から評価することで, *Ramsey number* ([11], [18] など) や *oriented Ramsey number* ([12], [30] など) に対するよい下界式を与えることが個別の頂点数の場合には経験的に知られている [14], [23], [24]. しか

し, [5], [13], [24] などでの計算機実験は $\sqrt{p}$ より遥かに小さいオーダーとなることを示唆しているにも関わらず, 一般の素数 p に対しては, G_p のクリーク数と T_p の推移的トーナメントの最大サイズのどちらについても, 既存の上界 [16], [20], [28] は $\sqrt{p}$ のオーダーの barrier を超えることができていない.

2 つめの主結果である以下の定理 14 は, 定理 10 が両方の場合において, $O(\sqrt{p})$ の barrier を超えることを示唆する. なお, 定理 13 は本質的には Bandeira, Mixon および Moreira [3] による結果と同じである.

定理 13 ([3]) 素数 $p \equiv 1 \pmod 4$ に対して定理 *10* が成り立つとき, G_p のクリーク数は $o(\sqrt{p})$ である.

定理 14 素数 $p \equiv 3 \pmod 4$ に対し, 定理 *10* が成り立つとき, T_p 内の推移的トーナメントの頂点数は $o(\sqrt{p})$ である.

また, 行列 Φ_p が ETF であることから, 定理 3 のもとでは Φ_p に対して $K = O(\sqrt{p})$ の場合にのみ, ある δ に対して (K, δ)-RIP が保証されるが, 興味深いことに, この RIP に対して定理 13, 14 の証明の議論を用いると, 既存のものとほぼ一致する上界が得られる. これらの状況から, 行列 Φ_p が問題 5 の解であるかどうかという問題は, 単に圧縮センシングにおいてだけではなく, Ramsey 理論においても興味深い課題となることを示唆しており, 今後の研究が期待される.

4 関連する注意と今後の課題

本稿では, Paley グラフ予想の下で, Renes と Zauner による ETF が問題 5 に対する一つの解であることを示した. Renes と Zauner による ETF は平方剰余に基づいて構成されるが, その一般化として, 一般の高次剰余から定義される行列も (一般化) Paley グラフ予想の下で問題 5 の解になることが講演者と Yujie Gu 氏によって最近示された [26]. 一方で, 問題 5 に対する解を与えた結果は依然として少ない. また, Renes と Zauner による ETF を含め, 既存の構成例が square-root bottleneck をどれだけ越えることができるのかを定量的に評価するなど, 興味深い問題が未だに多く残されている.

謝辞

本研究集会における講演の機会をくださった代表者の田邊 顕一朗 准教授 (北海道大学) と研究集会にお誘いくださった城本 啓介 教授 (熊本大学) に厚く御礼申し上げます. また, 本研究に関して有益なコメントをくださった鎌田 祥一 氏 (東京都立大学), 櫻井 幸一 教授 (九州大学), 澤 正憲 准教授 (神戸大学), 田坂 浩二 准教授 (愛知県立大学), 平尾 将剛 准教授 (愛知県立大学), 籾原 幸二 准教授 (熊本大学), Yujie Gu 助教 (九州大学) に感謝申し上げます. 本研究は，科学研究費補助金（特別研究員奨励費 20J00469）の助成を受けております.

参考文献

[1] A. S. Bandeira, E. Dobriban, D. G. Mixon, W. F. Sawin, Certifying the restricted isometry property is hard, *IEEE Trans. Inf. Theory* **59** (2013), 3448–3450.

[2] A. S. Bandeira, M. Fickus, D. G. Mixon, P. Wong, The road to deterministic matrices with the restricted isometry property, *J. Fourier Anal. Appl.* **19** (2013), 1123–1149.

[3] A. S. Bandeira, D. G. Mixon, J. Moreira, A conditional construction of restricted isometries, *Int. Math. Res. Not.* **2017** (2017), 372–381.

[4] J. Bourgain, S. Dilworth, K. Ford, S. Konyagin, D. Kutzarova, Explicit constructions of RIP matrices and related problems, *Duke Math. J.* **159** (2011), 145–185.

[5] A. E. Brouwer, Paley graphs, `https://www.win.tue.nl/~aeb/drg/graphs/Paley.html`.

[6] E. Candès, The restricted isometry property and its implications for compressed sensing, *C. R. Acad. Sci. Paris, Ser. I* **346** (2008), 589–592.

[7] E. J. Candès, J. K. Romberg, T. Tao, Stable signal recovery from incomplete and inaccurate measurements, *Comm. Pure Appl. Math.* **59** (2006), 1207–1223.

[8] M.-C. Chang, On a question of Davenport and Lewis and new character sum bounds in finite fields, *Duke Math. J.* **145** (2008), 409–442.

[9] B. Chor, O. Goldreich, Unbiased bits from sources of weak randomness and probabilistic communication complexity, *SIAM J. Comput.* **17** (1988), 230–261.

[10] F. Chung, Several generalizations of Weil's sums, *J. Number Theory* **49** (1994), 95–106.

[11] D. Conlon, A. Ferber, Lower bounds for multicolor Ramsey numbers, *Adv. Math.* **378** (2021), 107528,

[12] P. Erdős, L. Moser, On the representation of directed graphs as unions of orderings, *Magyar Tud. Akad. Mat. Kutató Int. Közl.* **9** (1964), 125–132.

[13] G. Exoo, Clique numbers for small Paley graphs, `http://cs.indstate.edu/ge/Paley/cliques.html`.

[14] R. E. Greenwood, A. M. Gleason, Combinatorial relations and chromatic graphs, *Canad. J. Math.* **7** (1955), 1–7.

[15] A. M. Güloğlu, M. R. Murty, The Paley graph conjecture and Diophantine m-tuples, *J. Combin. Theory Ser. A* **170** (2020), 105155.

[16] B. Hanson, G. Petridis, Refined estimates concerning sumsets contained in the roots of unity, *Proc. London Math. Soc. (3)* **122** (2021), 353–358.

[17] R. Lidl, H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, 1994.

[18] J. H. van Lint, R. M. Wilson, A course in Combinatorics, Second edition, Cambridge University Press, 2001 (ヴァン・リント, ウィルソン, 組合せ論 上, 神保 雅一 (訳), 澤正憲 (訳), 萩田 真理子 (訳), 丸善出版, 2018 年).

[19] D. G. Mixon, Explicit matrices with the restricted isometry property: breaking the square-root bottleneck, in: Compressed Sensing and Its Applications, 389–417, Birkhäuser/Springer, 2015.

[20] K. Momihara, S. Suda, Upper bounds on the size of transitive subtournaments in digraphs, *Linear Algebra Appl.* **530** (2017), 230–243.

[21] H. Rauhut, Stability results for random sampling of sparse trigonometric polynomials, *IEEE Trans. Inf. Theory* **54** (2008), 5661–5670.

[22] J. M. Renes, Equiangular tight frames from Paley tournaments, *Linear Algebra Appl.* **426** (2007), 497–501.

[23] A. Sánchez-Flores, On tournaments and their largest transitive subtournaments, *Graphs Combin.* **10** (1994), 367–376.

[24] A. Sánchez-Flores, On tournaments free of large transitive subtournaments, *Graphs Combin.* **14** (1998), 181–200.

[25] S. Satake, On the restricted isometry property of the Paley matrix, submitted for publication, arXiv:2011.02907.

[26] S. Satake, Y. Gu, On compressed sensing matrices breaking the square-root bottleneck, To appear in Proceedings of IEEE Information Theory Workshop 2020, arXiv:2010.11179.

[27] T. Strohmer, R. W. Heath, Grassmannian frames with applications to coding and communication, *Appl. Comput. Harmon. Anal.* **14** (2003), 257–275.

[28] C. Tabib, About the inequalities of Erdős and Moser on the largest transitive subtournament of a tournament, in : Combinatoire énumérative, pp. 308–320, Lecture Notes in Math., vol. 1234, Springer, 1986.

[29] T. Tao, Open question: deterministic UUP matrices, `https://terrytao.wordpress.com/2007/07/02/open-question-deterministic-uup-matrices/`.

[30] A. Treglown, A note on some embedding problems for oriented graphs, *J. Graph Theory* **69** (2012), 330–336.

[31] L. R. Welch, Lower bounds on the maximum cross correlation of signals, *IEEE Trans. Inf. Theory* **20** (1974), 397–399.

[32] G. Zauner, Quantum Designs - Foundations of a Non-Commutative Theory of Designs (German), Ph.D. thesis, University of Vienna, 1999.