公開

研 究 終 了 報 告 書

「Square-root bottleneck を超える RIP 行列と関連する組合せ論」

研究期間： 2021 年 10 月～ 2024 年 3 月
研 究 者： 佐竹 翔平

1. 研究のねらい

制限等長性 (Restricted Isometry Property, RIP)をもつ行列 (RIP 行列)の構成は，圧縮センシングの理論における最重要問題の 1 つである．特に，数学的にも応用上の観点からも，できるだけ大きな sparsity level に対応する RIP 行列の構成が興味深く重要な問題となる．RIP 行列の構成の方法の 1 つとして，ランダム行列にもとづく確率論的な構成があげられる．実際，ランダム行列は高い確率でほぼ最適な sparsity level を達成することがよく知られている．しかしながら，圧縮センシングへの応用のためには明示的な RIP 行列が望まれるが，ランダム行列は明示的な行列を与えるものではない．

こうした背景から，RIP 行列の明示的構成とその RIP を保証する問題が研究されてきた．本問題は，整数論，組合せ論，関数解析などの数学の様々な分野とも関連しており，数学と情報科学との境界領域に位置する．ただし，明示的構成から得られる$M \times N$行列に関して，従来のほとんどの研究で，sparsity level が$O(\sqrt{M})$の場合の RIP しか保証できていなかったという状況がある．Sparsity level に対するこの制約は square-root bottleneck とよばれる．この制約を超える RIP 行列は極めて限られた場合にしか与えられておらず，保証された RIP は$\sqrt{M}$のオーダーをわずかに超えるに留まり，理論的最適値に未だ及ばない．

一方で，いくつかの先行研究や報告者の研究により，エクスパンダーグラフや乱数抽出器などの擬ランダム性を持つ組合せ論的対象の構成・性質評価や，Ramsey グラフの構成などの Ramsey 理論への貢献，Erdős-Falconer 問題への sharp な解の構成などを通した有限体上の加法的組合せ論への応用などの組合せ論的な貢献が積み上げられてきた．特に，square-root bottleneck は乱数抽出器の min-entropy rate や Ramsey グラフにおけるクリーク数の評価における理論的な bottleneck とも直結することが平方剰余上のグラフ (Paley グラフ)や乱数抽出器 (Paley 抽出器)などで観察されている．

以上の背景から以下の 2 つの目標を研究のねらいとする．

目標 1. Square-root bottleneck を超える新たな RIP 行列の明示的構成
目標 2. RIP 行列の擬ランダム性の研究，Ramsey 理論，加法的組合せ論などへの応用

2. 研究成果

(1)概要

まず，目標 2 に関して，新たに構成した可換群上の Cayley graph または Cayley sum graph のエクスパンダー性の評価を通して，漸近的に最適な coherence を実現する明示的な RIP 行列も新たに構成した論文 (同様式内，5．主な研究成果リスト，論文 1.)が国際学術誌 Designs, Codes and Cryptography に採択された．グラフのエクスパンダー性は擬ランダム性の研究の

公開

中心的役割を果たしており，純粋数学，理論計算機科学の双方で重要であり，RIP を通した擬ランダム性へのアプローチを目指す目標 2 に対して一つの進展を与えたものと言える．また，今回構成したグラフの第 2 固有値は最小のオーダーを達成し，実際にはスパースではないものの Ramanujan グラフの一例にもなっている．

さらに，本課題の副産物としてエクスパンダーグラフを用いた non-malleable code の構成をまとめた別の論文も国際会議 WAIFI2022 に採択された．本課題に関係するのは Section 5 でのグラフの構成であり，非可換群上の Cayley グラフからの RIP 行列の構成を検討した際に，報告者が構成したグラフが本論文で応用されている．残念ながら，非可換群上の Cayley グラフからの RIP 評価の見通しが完全に立っていないが，今後も引き続き検討を進めていく．

その他の成果，進捗については「(2) 詳細」を参照されたい．

（2）詳細

1. Square-root bottleneck を超える新たな RIP 行列の明示的構成

まず，Bourgain et.al. (2011, Duke Math.), Bandeira-Mixon-Moreira (2017, Int. Math. Res. Not.), 提案者らがこれまでに構成した RIP 行列を参考に，代数的手法で構成された種々の行列を調査し，候補となる行列の情報を収集した．

有望と思われるクラスの 1 つは，フレーム理論，符号理論，代数的組合せ論などの文脈で研究されてきた equiangular tight frame (ETF)とよばれる行列のクラスである．実際，サイズが$M \times N$の ETF は，少なくとも，sparsity level が$\sqrt{M}$のオーダーの RIP をもつことが保証される．また，Bandeira-Mixon-Moreira (2017, Int. Math. Res. Not.)および報告者 (2021, Linear Algebra Appl.)による Paley 行列は ETF の 1 つの例であり，報告者-Gu (ITW2020)が構成した RIP 行列の系列の一部も ETF となる．ETF のジェネリックな構成法は，König (1995, in ``Panoramas of Mathematics''), Strohmer-Heath (2003, Appl. Comput. Harmon. Anal.), Ding-Feng (2007, IEEE Trans. Inf. Theory) などで与えられている．これらの構成法では，Hadamard 行列の構成に応用される conference 行列の固有ベクトル，または有限可換群上の difference set とその指標値を並べた列ベクトルを並べた行列を構成することで ETF が構成される．Conference 行列や difference set は代数的組合せ論，特に組合せデザイン論における主要な研究対象であり，これらの構成に関しては非常に多くの研究成果があり，構成例が蓄積されていた．

研究期間内では特に，Singer difference set から得られる ETF (Singer ETF)を調べた．実際に Jasper et al. (IEEE Trans. Inf. Theory, 2014) により ETF が目標 1 を達成する RIP 行列であることは予想されてはいるものの，具体的な研究自体はほとんど行われてこなかったように思われる．報告者は Singer ETF の RIP が square-root bottleneck を超えるための十分条件を得た．ただし，この十分条件は整数論の未解決問題に密接に関係しており，square-root bottleneck を超える RIP の証明には至っていない．しかし，今回導出した十分条件によって，square-root bottleneck を超える RIP の証明に関してもおおむねの見通しが見えてきており，引き続き検討を進めていく．また，有限素体上の平方剰余から構成される RIP 行列である Paley 行列に関しては，報告者 (2021, Linear Algebra Appl.) らによって Paley グラフ予想の下で square-root bottleneck を超える RIP が証明されていたが，いかなる予想の仮定も置かない状況では，その RIP が square-root bottleneck を超えることは予想されているもの，証明は与えられていない．そこで RA との共同での計算機実験により，ある程度以下のサイズの有限素体に関しては，やはり Paley 行列の

公開

sparsity level は square-root bottleneck を超えることを示唆する実験結果を得た.

2. RIP 行列の擬ランダム性の研究, Ramsey 理論, 加法的組合せ論などへの応用

本テーマに関する研究の進捗がより得られたと報告者は考える. まず, 論文 1. (同様式内, 5. 主な研究成果リスト) では, 新たに構成した可換群上の Cayley graph または Cayley sum graph のエクスパンダー性の評価を通して, 漸近的に最適な coherence を実現する明示的な RIP 行列も新たに構成した. この構成における鍵は, 代表者と Y. Gu 氏によって ISIT2020 で指摘されていた, 同じ群上で構成される特定の複素行列の coherence の最小化とエクスパンダー性に直結するグラフの第 2 固有値の最小化との同値性であった. その RIP が square-root bottleneck を超えるか否かは現在も未解決だが, 新たな課題として今後も研究を進めていく. なお, この課題に関連して, 今回構成した行列は, Turan 数や Ramsey 数の下界の証明などで重要な役割を果たす projective norm graph と呼ばれるグラフを一般化した構成によって与えており, グラフ理論的にも意義のある結果であると考える. 以上の成果は, RIP を通した擬ランダム性へのアプローチを目指す目標 2 に対して一定の進展を与えたものと言える.

3. 今後の展開

まず目標 1.に関して, Singer ETF を含め ETF などに着目し, 引き続き RIP の評価を進めていきたい. 一方で, 計算機実験による RIP の数値実験についても継続し, 結果をさらに蓄積していく. さらに, 今回の RIP はいわばℓ_2-ノルムの設定での等長性について着目しているが, 実際はより一般的なℓ_p-ノルムの設定での RIP も定義されており, やはり圧縮センシングなどへの重要な応用をもつ. ℓ_p-ノルムの設定での RIP 行列の明示的構成は, 報告者の知る限りほとんど前例がなく, 今年になって Fourcart によるプレプリントが発表されているにとどまっている. しかも, RIP 評価に関してはℓ_2-ノルムの設定よりも sparsity level の評価がはるかに悪くなってしまい, やはり技術的な bottleneck が立ちはだかっている. そこで, 目標 1.に向けての研究で着目してきた RIP 行列なども応用し, ℓ_p-ノルムの設定での RIP 行列の明示的構成にも取り組みたい.

目標 2.に関し, 今後の究極的な目標として, RIP 行列の構成・評価の困難性の数学的理解や RIP という性質そのものの組合せ論的な「意味」を, エクスパンダーグラフや Ramsey グラフの構成・性質評価や加法的組合せ論などにおける問題の解の構成などへの帰着, または関係性の探究により, 得ていきたいと考えている.

4. 自己評価

全体としては, コロナ禍や報告者の業務等の都合で, 当初予定より研究が遅れ気味ではあったものの, 論文の採択や研究発表なども研究期間内に行うことができたため, 概ね良好な進捗状況であったと考えている. 反省点としては, コロナ禍や業務等の関係で予定していた海外への研究訪問等ができなかった点と, RA を継続的に雇用できず計算機実験の進捗が予定より遅れてしまった点が挙げられる. 一方で, サイトビジットや領域会議等でのアドバイザー, ACT-X 採択者との研究交流により, 報告者自身の研究の視野と領域が採択前に比べて大幅に拡張できたことは非常に大きな収穫であった. 実際に, 本課題と直接的な関係は必ずしもないものの ACT-X 採択者との共同研究も行うことができた. 今後は本課題に関連する共同研究も積極的に行っていきたいと考える.

公開

５．　主な研究成果リスト

（１）代表的な論文（原著論文）発表

研究期間累積件数：　2　件

1. Shohei Satake, Yujie Gu, Cayley sum graphs and their applications to codebooks, Des. Codes Cryptogr., 2023 年, vol.91, 1315–1333.
2.
3.

（２）特許出願

研究期間全出願件数：　0　件（特許公開前のものは件数にのみ含む）

（３）その他の成果（主要な学会発表、受賞、著作物、プレスリリース等）

・学会発表

1. 佐竹　翔平, RIP 行列, グラフ　&　組合せデザイン,
研究集会「実験計画法と関連する組合せ構造および統計教育」, 2023 年 11 月 24 日,
広島大学東広島キャンパス.

2. 佐竹　翔平, エクスパンダーグラフと RIP 行列 (招待講演),
令和 5 年度情報数理ワークショップ, 2023 年 11 月 21 日, 九州大学西新プラザ.

3. 佐竹　翔平, Paley グラフ予想と Renes–Zauner の equiangular tight frame がもつ RIP II,
2021 年度応用数学合同研究集会, 2021 年 12 月 19 日, オンライン.

4. Shohei Satake, The restricted isometry property of the Paley ETF and Paley graph conjecture,
43rd Australasian Combinatorics Conference, 17th December 2021, online

.・開催したワークショップ

5. 研究集会　直交デザインと関連する組合せ論, 2023 年 1 月 21 日, 明治大学中野キャンパス.