2025年度共同利用研究報告書

2025年12月21日

所属・職名 熊本大学 半導体・デジタル研究教育機構 総合情報学部門・准教授
佐竹 翔平

		整理番号	2025a037	
1.研究計画題目	エクスパンダーグラフにまつわる数理科学と応用			
2.新規・継続	継続			
3.種別	若手・学生研究			
4.種目	短期共同研究			
5.開催方法	ハイブリッド開催			
6.研究代表者	氏名	佐竹 翔平		
	所属 部局名	熊本大学 半導体・デジタル研究教育機構 総合情報学部門	職名	准教授
7.研究実施期間	2025年08月25日(月曜日)～2025年08月29日(金曜日)			
8.キーワード	エクスパンダー、情報科学、数理科学、産学研究			
9.参加者人数	91人			

10.本研究で得られた成果の概要

有限体上のMarkoff方程式に基づくグラフ、いわゆるMarkoff mod p graphのエクスパンダー性に関する共同研究を継続的に進めた。Markoff方程式は3変数のDiophantine方程式であり、Markoffの古典的結果により、非負有理整数解全体はMarkoff moveによって連結な3正則木（Markoff tree）を成すことが知られている。一方、有限素体上で同様の構成を行うと3正則有限無向グラフ（Markoffグラフ）が得られる。Bourgain–Gamburd–SarnakによりMarkoffグラフがエクスパンダーであるとの予想が提示されているが、現時点では十分大きな素数に対する連結性の証明にとどまっており、エクスパンダー性の本質的解明には至っていない。MarkoffグラフはCayleyグラフやSchreierグラフのような有限群に基づく構成ではないため、従来手法が適用できず、新たな解析的・組合せ論的手法の開発が不可欠である。

本共同研究では、昨年度までの成果を拡張し、Markoffグラフおよび一般化Markoffグラフの内部構造を詳細に解析した。その結果、巨大連結成分内に複数の完全2部グラフマイナーが存在することを証明し、低種数閉曲面への埋め込み不可能性や非apex性を導いた。これらはエクスパンダー性を示唆する重要な傍証であり、一般化Markoffグラフに関する近年の研究進展とも整合的である。得られた成果は現在論文として取りまとめており、国際学術誌への投稿を予定している。

さらに産業界への貢献に向けて、暗号理論的な研究も進めてきた。Markoffグラフを用いた暗号学的ハッシュ関数が既に提案されているものの、その安全性評価や数理的基盤は十分に確立されていなかった。本共同研究では、一般化Markoffグラフの巨大連結成分内におけるサイクルの存在性と分布に注目し、特定の短サイクルの構成法や具体的位置を明らかにした。これらの成果は、ハッシュ関数の安全性解析や耐量子計算機暗号への応用に資するものであり、SCIS2026において発表予定である。

2025 年度九州大学マス・フォア・インダストリ研究所
「産業数学の先進的・基礎的共同研究拠点」共同利用研究 若手・学生研究-短期共同研究

「エクスパンダーグラフにまつわる数理科学と応用」

成果報告書

1. 実施状況

本共同研究は 2022 年度から毎年実施しているの若手・学生研究-短期共同研究「エクスパンダーグラフの新しい構成手法の確立とその応用 1, 2, 3」の継続課題として, 2025 年 3 月に採択された. 本項目では, 本共同研究の整理番号, 組織委員, 研究課題ウェブサイト, 実施時期, 事前準備等の状況を記す.

・整理番号

2025a037

・組織委員

佐竹 翔平（熊本大学 半導体・デジタル研究教育機構・准教授）
相川 勇輔（東京大学・助教）
池松 泰彦（九州大学 IMI・准教授）
Reyes Bustos Cid（NTT 基礎数学研究センタ・リサーチアソシエート）
Jo Hyungrok（横浜国立大学 先端科学高等研究院・特任助教）
見村 万佐人（東北大学 理学研究科・准教授）

・研究課題ウェブサイト

https://joint2.imi.kyushu-u.ac.jp/research_chooses/view/2025a037

・研究実施期間

2025 年 8 月 25 日（月）～ 2025 年 8 月 29 日（金）

・事前準備

採択通知後, 3 月から 8 月までの共同研究開始時期までに 各月 1~2 回 ZOOM を使用してオンラインミーティングを行い, 共同研究の実施方式（公開型・非公開型講演会の実施方法), 各講演者の選定, 予算の使用方法, 関連分野へのアナウンス時期・方法などに関して打合せを行った.

2. 共同研究の背景・目的

エクスパンダーは，辺が少なく，局所的な連結性が高いという一見相反する特徴を持つ興味深いグラフであり，効率的な情報伝達や高速攪拌性を活かして，耐量子計算機暗号や量子符号など情報科学の幅広い分野で理論的・応用的に重要視されている．近年では，Google などの企業がエクスパンダーの研究を進めており，暗号技術や機械学習を含む産業分野への応用可能性がますます注目を集めている．このように，エクスパンダーの理論的基盤は情報科学の革新を支える重要な要素である．

エクスパンダー研究の中核となる課題は，次の 2 点に集約される．

(1) エクスパンダーの構成法の確立と高度化.

代数的構成は明示性が高い一方で，群論や整数論といった数学の難解な問題に直面することが多く，第 2 固有値の評価や構造解析が困難である．組合せ論・アルゴリズム的な構成は，数学的な課題を回避できるものの，構造解析や性質の透明性が低下する傾向がある．このため，両者の長所を統合したハイブリッド構成法が必要とされる．

(2) エクスパンダーの応用可能性の拡大と解明.

暗号理論や符号理論，機械学習などの応用において，エクスパンダーの特性がその有用性を左右する．特に，第 2 固有値や構造に関する深い理解が応用可能性を広げる鍵となる．また，エクスパンダーは暗号学的ハッシュ関数，量子LDPC符号，グラフニューラルネットワークなどの分野においても期待されているが，その応用可能性はまだ十分に開拓されていない．特に国内では，産業界との連携が未だ限定的であり，組織的な研究体制や応用の推進が課題である．

以上の背景から，本研究では，以下の 2 つを目的とする．

目的 1: ハイブリッド構成手法の開発.

代数的構成と組合せ論的構成の利点を統合した新たな構成手法を提案し，エクスパンダーの特性を最適化する．これにより，構造解析を容易にしつつ，効率的な構成を実現する．

目的 2: 学術・産業界を巻き込んだ応用可能性の拡大.

エクスパンダーを軸にした暗号技術や機械学習などの新たな応用分野を開拓し，国内外の産業界との連携を強化する．特に，企業との共同研究を促進し，産業利用の具体例を提示することで，エクスパンダーの社会実装を推進する．

本研究によって，エクスパンダーの応用可能性の開拓と拡大，さらに関連研究分野と産

業化との連携体制の確立と応用研究の推進が期待される.

関連する研究の経過として，昨年度までの共同研究において，群論的構成による Ramanujan Cayley グラフに適切な部分グラフ除去などの組合せ的操作を施し，第 2 固有値を評価するハイブリッド手法によって，ほぼ最適な第 2 固有値をもつエクスパンダーの新規構成に成功した．さらに，エクスパンダーの「立方化」による高次元化を通した暗号学的ハッシュ関数の提案や符号理論への応用などに関しても研究が進められている．一方で，有限体上の Markoff 方程式から得られるグラフのエクスパンダー性について，グラフマイナーと数論的手法を融合したアプローチで迫っており，近日中に論文を投稿予定である．他方，国内での産業界へのプレゼンや連携の余地は依然として多く残されており，エクスパンダー研究の産学での継続的な普及活動と研究促進が必要となっていた.

3. 実施状況

「2. 共同研究の背景・目的」で述べた状況に鑑み，数学，計算機科学，情報科学，データサイエンスなどの専門家によるエクスパンダーおよび関連するトピックに関するイントロダクションである 6 講演から構成される公開型講演会を 9 月 9 日から 9 月 11 日まで実施した．公開型講演会は九州大学 伊都キャンパス ウエスト 1 号館 C 棟 5 階 C501 大講義室（W1-C-501）における現地開催と ZOOM によるオンライン開催のハイブリッド形式で実施した．公開型講演会の内容は以下のとおりである.

8 月 25 日（月）

・見村 万佐人（東北大学）
幾何学的群論におけるエクスパンダー

・尾國 新一（愛媛大学）
群とグラフの大尺度幾何学とその周辺

8 月 26 日（火）

・峯松 一彦（NEC）
組み合わせグループテストの改ざん検知への応用

・西村 優作（早稲田大学）
有限環上の自由 LCD 符号から得られる格子の格子同型問題について

・木本 一史（琉球大学）
有限グラフ上の Chip-Firing Game と 2 変数ゼータ関数

8 月 27 日（水）午前

・小関　健太（横浜国立大学）

Coloring of graphs on surfaces

公開型講演会にはのべ 92 名が参加した．昨年度以上に様々なバックグラウンドをもつ参加者からの質問やコメントがあり，活発な議論がなされた．

一方で，8 月 27 日午後から 8 月 29 日に，関連分野の専門家による，より具体的な議論を目的とした非公開型講演会を実施した．エクスパンダーに関連する耐量子計算機暗号，グラフ理論，大域解析学などに関する合計 4 件の講演が実施された．また，前日までの公開型講演会での 3 講演の内容に関してのより詳細な質疑応答や研究に関連する未解決問題の議論のための Open problem session の時間も 8 月 27 日の講演後に設け，関連話題や今後の研究の方向性に関する議論を行った．非公開型講演会は九州大学 伊都キャンパス ウエスト 1 号館 D 棟 4 階 IMI オーディトリアム（W1-D-413）における現地開催と ZOOM によるオンライン開催のハイブリッド形式で実施し，合計で 12 名が参加した．

非公開型講演会の内容は以下のとおりである．

8 月 27 日（木）午後

・相川 勇輔（東京大学）

Lattice Sieving using Graph-based Nearest Neighbor Search

8 月 28 日（木）

・佐竹 翔平（熊本大学）

Markoff mod p-graph の埋め込み可能性

・Cid Reyes Bustos (NTT IFM)

講演タイトル：Heat kernel of certain families of infinite graphs

8 月 29 日（金）

・Semin Oh (慶北大学校)

The non-bipartite integral graphs with bounded spectral radius

・Hyungrok Jo（横浜国立大学）

PoC ハッシュ関数：代数的設計と証明可能な安全性

4. 共同研究で得られた成果

※　以下の研究成果は現在進行中の共同研究の成果を含んでおり，発表前の段階にある．

目的(i)に関して，新たに Markoff mod p graph とよばれる有限体上の Markoff 方程式に基づくグラフのエクスパンダー性に関しての共同研究を継続している．Markoff 方程式は 3 変数の Diophantine 方程式であり，Markoff (1879, 1880)の結果より，非負有理整数上の方程式解の集合（(0, 0, 0)は除く）は Markoff move とよばれる解の集合上の写像によって，連結な 3-正則木（Markoff tree）のグラフ構造を作り出す．一方で，有限素体$\mathbb{F}_p$上の方程式解の集合で同様にグラフ構造を作り出すと 3-正則有限無向グラフ（Markoff グラフ）が構成される．Bourgain-Gamburd-Sarnak (2016) によって，Markoff グラフがエクスパンダー性をもつことが予想されているが，現状では Chen (2024), Fuchs et al. (2024) らによって十分大きな素数pに対して連結性が証明される（この結果も大きなブレイクスルーであったが）にとどまっている．Markoff グラフは既存のエクスパンダーの代数的構成のほとんどで用いられてきた Cayley graph や Schereier graph のような有限群上で構成されるグラフではないため，エクスパンダー性の証明のためには，新しい手法が必要と思われる．エクスパンダー性の予想に迫るという意味でも，新手法の開発に向けての手がかりを模索する意味でもエクスパンダー性の傍証を固める研究は重要であった．一方で，今年に入って一般化した Markoff 方程式および対応するグラフ（一般化 Markoff グラフ）に対しても研究が Martin (2025) によって進展しており，巨大連結成分の存在性などが明らかになってきた．

本共同研究の一環として，昨年度までの研究を拡張し，Markoff グラフのみならず一般化 Markoff グラフの内部構造，とくに完全 2 部グラフ$K_{3,3}$のマイナーが複数存在することを証明しており，一般化 Markoff グラフの巨大連結成分の低種数の閉曲面への埋め込み不可能性，非 apex 性などのエクスパンダー性の傍証となる結果を新たに得ることができた．これらの成果をまとめた論文を国際学術誌に投稿予定である．

上記研究は目的 (ii)に観点からも，産業界でも重要な基礎研究に位置する．実際に，Markoff グラフまたは一般化 Markoff グラフを用いた暗号学的ハッシュ関数が Fuchs et al. (2021) によって提案されており，その安全性評価や高機能化は次世代（耐量子計算機）暗号の開発という面でも重要視されている．現状では，エクスパンダー性によるハッシュ値分布の一様性の証明，セキュリティパラメータの設定，衝突困難性の数学的解析などの暗号学的に不可避な数理課題も，耐量子計算機暗号や整数論における同種写像グラフの研究などに比して，ほとんど手つかずのまま多く残されていた．共同研究では一般化 Markoff グラフの巨大連結成分内のサイクルの存在性や分布に関する研究が進展しており，特定の短サイクルの構成法や具体的な位置について明らかにした．これらの暗号理論的成果は 2026 年暗号と情報セキュリティシンポジウム（SCIS2026）の報告集論文および発表において公表する予定である．

受付中

開催日：2025/08/25〜2025/08/27

エクスパンダーグラフにまつわる数理科学と応用｜2025a037

カテゴリー：イベント　　タグ：若手研究　短期共同研究

開催概要

- **開催方法**：九州大学 伊都キャンパスとZoomミーティングによるハイブリッド開催
- **開催場所**：九州大学 ウエスト1号館
  公　開：C棟 5階 C501大講義室（W1-C-501）
  非公開：D棟 4階 IMIオーディトリアム（W1-D-413）
- **主要言語**：日本語
- **主催**：九州大学マス・フォア・インダストリ研究所
- **種別・種目**：　若手・学生研究-短期共同研究
- **研究計画題目**：エクスパンダーグラフにまつわる数理科学と応用
- **研究代表者**：佐竹 翔平（熊本大学 半導体・デジタル研究教育機構 総合情報学部門・准教授）
- **研究実施期間**：2025年8月25日(月) 〜 2025年8月29日(金)
- **公開期間**：2025年8月25日(月) 〜 2025年8月27日(水)AM
- **研究計画詳細**：https://joint2.imi.kyushu-u.ac.jp/research_chooses/view/2025a037

プログラム

8月25日（月）公開

14:00-15:00

見村 万佐人（東北大学）
幾何学的群論におけるエクスパンダー

15:30-16:30

尾國 新一 (愛媛大学)
群とグラフの大尺度幾何学とその周辺

8月26日（火）公開

10:30-11:30

峯松 一彦（NEC）
組み合わせグループテストの改ざん検知への応用

13:00-14:00

コーヒーブレイク

14:00-15:00

西村 優作 (早稲田大学)
有限環上の自由LCD符号から得られる格子の格子同型問題について

- 15:30-16:30

木本 一史 (琉球大学)
有限グラフ上の Chip-Firing Game と2変数ゼータ関数

8月27日（水）公開　※13:00–16:30 非公開

- 10:30-11:30

小関　健太（横浜国立大学）
Coloring of graphs on surfaces

8月28日（木）※13:00–16:30 非公開

8月29日（金）※10:30–13:00 非公開