2024年度共同利用研究報告書

2025年01月14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	2024a028		
1.研究計画題目	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3			
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	2024年09月09日(月曜日)～2024年09月13日(金曜日)			
8.キーワード	エクスパンダーグラフ, 組合せ論・組合せ最適化, 群論, 整数論, 耐量子計算機暗号, 符号理論, 理論計算機科学, 学習理論			
9.参加者人数	97人			

10.本研究で得られた成果の概要

目的(i)に関して, 新たにMarkoff mod p graphとよばれる有限体上のMakoff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が進行中である. 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 mod p graph G_p) が構成される. Bourgain-Gamburd-Sarnak (2016) によって, G_p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, G_pの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. G_p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, G_pの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G_pのエクスパンダー性の傍証を固める研究は重要であった.

本共同研究の一環として, 現在Markoff mod p graph G_pの内部構造, とくにグラフマイナーに関する研究を進めてきており, G_p内の完全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, G_pの非 (射影) 平面性, 木幅, 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ている. 証明の要点は, K_3,3-マイナーの存在性をF_p上の代数方程式系の解の存在性に帰着させ, 解の存在性を直交多項式や線形代数的手法を用いて示す点にある. 以上の結果は共著論文として, 近日中に国際数学誌に投稿予定である. 一方で, G_pの (グラフの) 全自己同型群の位数や群構造を決定することで, エクスパンダー性に対する連結性よりも強い傍証が与えられることも観察しており, 数値実験の結果からG_pの (グラフの) 全自己同型群の位数と群構造に関する予想を立てることができた. こちらの研究も引き続き実施していく.

以上の研究は目的 (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 mod p graph G_p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手つかずのまま多く残されており, 今回のMarkoff mod p graphのグラフマイナーなどの内部構造の研究はサイクル分布の解明による衝突困難性の解析にも貢献している.

報告書は 2028 年 4 月に公開予定