2022年度共同利用研究報告書

2022年12月19日

所属・職名 明治大学総合数理学部・助教
佐竹 翔平

		整理番号	2022a017	
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			
2.新規・継続	新規			
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	明治大学総合数理学部	職名	助教
7.研究実施期間	2022年08月22日(月曜日)～2022年08月26日(金曜日)			
8.キーワード	エクスパンダーグラフ, 組合せ最適化, 組合せ論, 群論, 整数論, 情報科学			
9.参加者人数	105人			

10.本研究で得られた成果の概要

本共同研究の目的として以下の2点を挙げていた.

(i) 代数的な構成と組合せ論・アルゴリズム的な構成をハイブリッドさせ, 両者の利点を抽出した新しい構成手法を編み出す.
(ii) エクスパンダーの暗号理論や機械学習などの情報科学への応用にも目を向け, 構成したエクスパンダーの応用を検討する.

これらの目的達成のためには, まずエクスパンダーに関連する分野の研究者が研究交流を行い, 共同研究を行うための下地作りが不可欠であった. 本共同研究によって, グラフ理論, 整数論, 確率論, 計算機代数, 暗号理論, 制御理論などの様々な関連分野からの研究者が講演の質疑応答や議論を通して研究交流を行うことができた点は大きな成果であったと考える. また本共同研究によって, エクスパンダーの構成と暗号理論などの情報科学とのインタラクションに関する複数の共同研究がスタートしており, 今後も引き続き研究を行っていく予定である.

報告書は 2024 年 4 月に公開予定

九州大学 IMI 共同利用・短期共同研究　公開プログラム

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

Toward a New Method for Constructing Expander Graphs and Their Applications

8月22日（月）（公開型講演会）

13:20-13:30: 趣旨説明

13:30-14:30 講演 1

講演者： 見村 万佐人（東北大学）

講演タイトル：エクスパンダーと有限群と無限群

(English title) Expanders, finite groups and infinite groups

14:45-15:45 講演 2

講演者：清水 伸高（東京工業大学）

講演タイトル：エクスパンダーグラフと脱乱択化

(English title) Derandomization and Expander Graphs

16:00-17:00 講演 3

講演者：田村 光太郎（野村総合研究所）

講演タイトル： 社会データ分析におけるグラフアルゴリズムの適用

(English title) Application of Graph Algorithms in Social Data Analysis

講演 1： 見村 万佐人（東北大学） Masato Mimura (Tohoku University)

タイトル：「エクスパンダーと有限群と無限群」

概要：有限群とその生成系の組の列のケイリーグラフからエクスパンダー族を構成する手法は有名である。本講演では、有限群の列を固定し生成系の列を変更したときに、できる有限ケイリーグラフの列がどの程度変わりうるかを述べる。その際、有限群の極限として現われる無限群が効いてくる。

Title: “Expanders, finite groups and infinite groups”

Abstract: One well-known way of constructing expanders is to take Cayley graphs of a certain sequence of pairs of finite groups and generating sets. In this talk, I will discuss how changing generating sets affects the resulting Cayley graphs for a fixed sequence of finite graphs. Here, the "limit groups" of finite marked groups play a key role.

講演 2: 清水 伸高（東京工業大学） Nobutaka Shimizu (Tokyo Institute of Technology)

タイトル:「エクスパンダーグラフと脱乱択化」

概要: ランダムネスを用いると様々な問題に対して効率的なアルゴリズムが設計できることが知られている. 例えば グラフ到達性判定, 多項式同一性判定, 行列積判定, 数え上げの近似などは効率的な乱択アルゴリズムが知られている. 一方で, これらの問題を同等の時間で決定的に解けるかどうかはよく分かっていない. このように, 乱択アルゴリズムを決定的なアルゴリズムに変換する手法は脱乱択化と呼ばれ, ランダムネスが本質的に必要かどうかという理論計算機科学の基本的な問いと密接に関連するため盛んに研究されている. 本発表ではエクスパンダーグラフの理論計算機科学への応用の一つとして脱乱択化に焦点を当てて紹介していく.

Title: “Derandomization and Expander Graphs”

Abstract: We can design efficient randomized algorithms for various problems including graph reachability, polynomial identity testing, checking matrix multiplication, and approximate counting. On the other hand, it is not known whether there exists a deterministic algorithm with the same running time for them. One possible way to obtain such a deterministic algorithm is to eliminate the randomness of randomized algorithms. This transformation is called derandomization, which has been a fundamental topic in theoretical computer science. In this talk, as an application of expanders in theoretical computer science, we introduce the technique of derandomization based on expanders.

講演 3:　田村 光太郎（野村総合研究所）　Kotaro Tamura (Nomura Research Institute)

タイトル：　「社会データ分析におけるグラフアルゴリズムの適用」

概要：　経済社会データにおけるトランザクションデータの解析が増えている。我々は 100 万社の企業間取引データを大規模なグラフ構造データとみなすことで、その構造を数値解析するとともにモデル化した。

グラフの数値解析では、グラフが疎性であるときにグラフアルゴリズムを効率的に適用できる。たとえば、隣接行列の固有解析は、グラフの疎性を利用することで効率的に行えて、ノードのランキングの計算に利用されている。また、関節点や橋のような連結性に重要なノードやエッジを抽出するなど、グラフの特徴点の抽出にも活かされる。これら解析の結果から、企業間の取引構造は、グラフ上において非常に短距離であることや、モチーフ構造に偏りがあること、取引数分布がべき分布に従うことを得ている。

また、我々は、企業間の取引を介して流れる財やサービスの流れを非線形の輸送方程式としてモデル化した。この輸送方程式は定常解の性質として、非線形性から来る解の不安定性がグラフ構造に起因して発現する。グラフの線形化や不安定性を遷移行列から評価するための固有解析を行った。

本講演では、解析に用いたグラフアルゴリズムの利用とその特徴の紹介を含める形で行う。

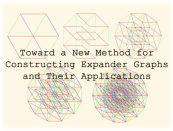
Title：　“Application of Graph Algorithms in Social Data Analysis”

Abstract：　Transactional data related to economic and social activities are increasingly being analyzed. We have numerically analyzed data of one million Japanese firms' transaction as large-scale graph-structured data and modeled its money flow as a transport system.

In numerical analysis of graph data, algorithms can be applied efficiently if the graph is sparse. For example, we can apply the eigenanalysis of adjacency matrices efficiently by taking advantage of the sparsity of the graph, and it has been used to compute node rankings or some centrality analysis. We can also use the sparsity to extract feature points of the graph, such as articulation points and edges. These analysis brought us the results that the network is small-world network, which means distance between firms is short, that the motif structure is significantly biased comparing to the random graph, and that the distribution of the number of transactions follows a power distribution.

Also, we model a nonlinear transport equation defined on the inter-firm transaction network, based on the real data of the money-flow between firms. The steady-state solution of this transport equation emerges instability depending on the nonlinear parameter and graph structure. We evaluated the linear stability of the solution by performing the eigenanalysis to the transition matrix.

This presentation will take the form of including an introduction to　the graph algorithm used in the analysis



九州大学 IMI 共同利用・短期共同研究　非公開講演会

エクスパンダーグラフの構成手法の確立とその応用

Toward a New Method for Constructing Expander Graphs and Their Applications

- 場所：九州大学IMIウェスト1号館オーディトリアム
- 日程：2022年8月23日（火）～　8月26日（金）
- 開催方法：現地参加、またはオンライン（zoom）参加

8月23日（火）

- 13:30-14:30
- 講演者：蔡 凱（大阪公立大学・情報学研究科）
- 講演タイトル：Types of Graph Laplacian Matrices and their Roles in Cooperative Control of Multi-Agent Systems

（20 分自由討論 ＋ 20 分休憩）

- 15:10-16:10
- 講演者：白髪 丈晴（中央大学）
- 講演タイトル：Voting processes on expander graphs

（20 分自由討論）

16:30-17:00「エクスパンダーと有限群と無限群」-見村先生への質疑応答 -

17:00 終了

8月24日（水）

- 10:30-11:30
- 講演者：相川 勇輔（三菱電機）
- 講演タイトル：エクスパンダーグラフ in 耐量子計算機暗号

（20 分自由討論）

11:50~13:30 お昼休み

- 13:30-14:30
- 講演者：久保田 匠（横浜国立大学）
- 講演タイトル：Mixed regular graphs to induce periodic quantum walk

（20 分自由討論 ＋ 20 分休憩）

- 15:10-16:10
- 講演者：瀬川 悦生（横浜国立大学）
- 講演タイトル：Generalized Laplacian induced by Grover walk

（20 分自由討論）

16:30-17:00「エクスパンダーグラフと脱乱択化」 -清水先生への質疑応答 -

17:00 終了

8月25日（木）

- 10:30-11:30
- 講演者：安永 憲司（東京工業大学）
- 講演タイトル：Complexity of Explicit Constructions and Range Avoidance Problems

（20 分自由討論）

11:50~13:30 お昼休み

- 13:30-14:30
- 講演者：金澤 秀（京都大学高等研究院）
  講演タイトル：A limit theorem for Betti numbers of random simplicial complexes

（20 分自由討論 ＋ 20 分休憩）

- 15:10-16:10
- 講演者：齋藤 正顕（工学院大学　教育推進機構）
- 講演タイトル：A central limit theorem for the number of non-backtracking cycles on regular graphs

（20 分自由討論）

16:30-17:00「社会データ分析におけるグラフアルゴリズムの適用」
-田村先生への質疑応答 -

17:00 終了

8月26日（金）

- 10:00-11:00
- 講演者：DAHAN Xavier（東北大学　高度教養教育学生支援機構）
- 講演タイトル：Construction of high-girth expander graphs based on quaternions, generalization to octonions and their implementation

(20 分自由討論)

11:20 終了

発表講演概要一覧

- 講演者：蔡 凱（大阪公立大学・情報学研究科）
- 講演タイトル：Types of Graph Laplacian Matrices and their Roles in Cooperative Control of Multi-Agent Systems
- 概要：In the field of systems and control, many cooperative control problems of multi-agent systems have been actively studied in the past two decades. Common in the formulation and resolution of these problems, a graph Laplacian matrix plays a key role. A graph Laplacian matrix is an important representation of graph topology, which describes the interconnection structure of the agents. Depending on the field of the entries, there are three types of Laplacian matrices: standard Laplacian (nonnegative diagonal entries and nonpositive off-diagonal entries), signed Laplacian (arbitrary real entries), and complex Laplacian (arbitrary complex entries). This talk will introduce these different types of Laplacian matrices, and their roles in modeling and solving different sets of cooperative control problems. Particular attention will be given to their algebraic properties that are fundamental in characterizing stability and performance of the respective solution algorithms.

- 講演者：白髪 丈晴（中央大学）
- 講演タイトル：Voting processes on expander graphs
- 概要：複数のエージェント(プロセッサ，ロボット，etc.)が協調して何らかの処理を行おうとする際，エージェント間での“合意”は欠かすことの出来ない基本的かつ重要な計算である．Voting process は合意計算への単純・低コストかつ高速で頑健なアプローチとして近年活発に研究が行われており，特に“Two-sample voting”と呼ばれるモデルについて，完全グラフ上において高速な収束時間，優れた耐故障性を持つことが示されていた．本研究ではエキスパンダーグラフ上における Two-sample voting の収束時間解析を行い，複数のグラフ構造上で既存研究と同様の性質を示した．本発表ではその解析技法，また近年の成果である voting process の合意以外への応用について述べる．

- 講演者：相川 勇輔（三菱電機）
- 講演タイトル：エクスパンダーグラフ in 耐量子計算機暗号
- 概要：あらゆるものがネットワークで繋がることが前提となった社会では、情報セキュリティは社会インフラを構築する必須技術である。その中核をなす要素技術一つに暗号技術がある。現在我々は公開鍵暗号として RSA 暗号や楕円曲線暗号を日常的に利用しているが、しかし、これらは大規模な量子コンピュータの実現によって危殆化することが Shor によって理論的に証明されている。そこで、量子技術の発展によるセキュリティ上の脅威に備えて、量子コンピュータでも解読できないような次世代暗号の研究や標準化がすすめられている。そのような暗号は耐量子計算機暗号と総称される。その構成の一つに、楕円曲線と同種写像から作られるエクスパンダーグラフを用いるものが知られている。今回は、その方式のアイデアを紹介するとともに、最近の研究の進展について皆様と共有する。

- 講演者：久保田 匠（横浜国立大学）
- 講演タイトル：Mixed regular graphs to induce periodic quantum walk
- 概要：本講演では正則な有向グラフ（混合グラフ）上の量子ウォークの周期性を調べる。正則な無向グラフの場合、隣接行列の固有値が明示的に分かっていれば量子ウォーク（Grover walk）の固有値も明示的に分かり、したがって周期性を調べることができる。有向グラフの場合も、原理的にはエルミート隣接行列の固有値が分かっていれば量子ウォークの周期性を調べられるが、エルミート隣接行列の固有値を明示的に計算することは難しいために周期性の研究が無向グラフと同様には進められない。しかし、エルミート隣接行列の固有値の基本対称式に注目することで、グラフの幾何構造から周期性を調べることができる。本講演では、まず無向グラフ上の典型的な量子ウォークである Grover walk を紹介し、周期性の先行研究をいくつか紹介する。その後、有向グラフ上の量子ウォークを定義し、いくつかの有向グラフのクラスについて周期性に関する最新の結果を論じる。

- 講演者：瀬川 悦生（横浜国立大学）
- 講演タイトル：Generalized Laplacian induced by Grover walk
- 概要：複素パラメータzをもつ入力を、外部から受け続ける量子ウォークモデルの定常状態について考察する。このパラメータzに依存する拡張されたラプラシアン行列$L(z)$を導入し、量子ウォークの定常状態が満たすべき回路方程式を得た。そのことにより、長時間における流出入を示す散乱行列や、エネルギーが、$L(z)$の逆行列を用いて表現できる。この行列を非正則にするようなzは、実はこの量子ウォークのユニタリ時間発展作用素の内側のグラフに対する部分行列の固有値の逆数であり、特に、内側のグラフが正則でそのすべての頂点が外部と直接つながっている状況では、ラマヌジャングラフなどの場合は、その固有値が、複素平面上のある1以下の半径の円周上に乗ることを示した。

- 講演者：安永 憲司（東京工業大学）
- 講演タイトル：Complexity of Explicit Constructions and Range Avoidance Problems
- 概要：値域回避問題（Range Avoidance Problem）とは，回路が入力として与えられ，その回路の出力値として取り得ない値を見つける問題である．与えられる回路は出力が入力よりも短いものに限るため，解が必ず存在する．Korten (FOCS'21) は，この問題が，確率的な手法で存在性が示されるオブジェクト（擬似乱数生成器・乱数抽出器など）の明示的な構成法（explicit construction）を与える問題に関係することを示した．本講演では，この研究やその関連研究について紹介する．

- 講演者：金澤 秀（京都大学高等研究院）
- 講演タイトル：A limit theorem for Betti numbers of random simplicial complexes
- 概要：The Erdős–Rényi graph model has been extensively studied since the 1960s as a typical random graph model. Recently, the study of random simplicial complexes has drawn attention as a higher-dimensional generalization of random graphs. In this talk we introduce a class of homogeneous and spatially independent random simplicial complexes, and discuss the asymptotic behavior of their Betti numbers. This result extends the law of large numbers for Betti numbers of Linial–Meshulam complexes, obtained in an earlier study by Linial and Peled. Time permitting, we will also discuss the

convergence of the empirical spectral distributions of their Laplacians. A key element in the argument is the local weak convergence of simplicial complexes. Inspired by the work of Linial and Peled, we establish the local weak limit theorem for homogeneous and spatially independent random simplicial complexes.

- 講演者：齋藤 正顕（工学院大学　教育推進機構）
- 講演タイトル：A central limit theorem for the number of non-backtracking cycles on regular graphs
- 概要：$(q+1)$-正則グラフの長さmの non-backtracking cycle の個数 N_mについて，絶対値が $2\sqrt{q}$未満の(隣接行列の)固有値が寄与している項t_mを考える（ここでは N_mの誤差項とよぶ）．本研究では，データ t_m（$m = 1,2,\ldots$）の分布について調べ，そのモーメント母関数を与えた．
  また,これを応用して，正則グラフの増大列がある条件をみたすとき，$t_m/\sqrt{n}$（nは絶対値が $2\sqrt{q}$未満の固有値の個数)の極限分布が正規分布となることを示した．尚，本研究は，長谷川武博氏（滋賀大学），西郷甲矢人氏（長浜バイオ大学)，杉山真吾氏（日本大学)，谷口哲也氏（金沢工業大学）との共同研究に基づく．

- 講演者：DAHAN Xavier（東北大学　高度教養教育学生支援機構）
- 講演タイトル：Construction of high-girth expander graphs based on quaternions, generalization to octonions and their implementation
- 概要：Following earlier works by Y. Ihara and then J.-P. Serre, in 1986 Lubotzky-Philips-Sarnak and G. Margulis introduced the breakthrough construction of “Ramanujan graphs”. Based on the arithmetic of quaternions, they provided explicitly the first optimal expanders, in a precise sense. Another remarkable property that these graphs display is their large girth (length of a shortest cycle). They still hold the record of having the largest girth. This property alone has various applications: construction of LDPC error-correcting codes, better design of “local” algorithms, help obtaining better bounds in several instances of algorithms in graphs. In this talk, we will present a variant and a generalization to octonions of the construction of Ramanujan graphs, discuss their new properties, their implementation and show some experimental observations.