九州大学 IMI 共同利用（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

Mathematical sciences and applications of expander graphs

8月25日（月）

14:00-15:00
講演者：見村 万佐人（東北大学）
講演タイトル：幾何学的群論におけるエクスパンダー

アブストラクト：エクスパンダーグラフは理論計算機科学から生まれた概念で、「性質のよい」グラフと思えます。ですが、幾何学的群論（や大尺度幾何学）では、「病的な性質を持つ、"悪い"グラフ」としてしばしば応用されます。また、両分野での "エクスパンダー" の定式化において細部が異なっていたりします。本講演ではエクスパンダーにまつわる異分野交流ということで、幾何学的群論の視点からのエクスパンダーの定式化と応用を紹介します。本集会での尾國新一さんの講演への橋渡しも兼ねています。

15:30-16:30
講演者：尾國 新一（愛媛大学）
講演タイトル：群とグラフの大尺度幾何学とその周辺

アブストラクト：無限の広がりを持つ"図形"を大きな尺度によって考察する幾何学を大尺度幾何学あるいは粗幾何学と呼びます。
例えば大尺度幾何学では「直線」と「直線上に一定の間隔で並んだ点の列」を"図形"として区別しません。
この粗さのおかげで、大尺度幾何学では、代数的な対象である可算無限群を無限の広がりを持つ"図形"として扱うことができます。また、可算無限個からなる有限グラフの族をひとまとめにして無限の広がりを持つ一つの"図形"として扱うこともあります。本講演では、粗バウム・コンヌ予想、エクスパンダー、グラフィカルスモールキャンセレーション理論をキーワードとして、大尺度幾何学、グラフの幾何学、幾何学的群論のつながりについてお話します。

8月26日（火）

10:30-11:30
講演者：峯松 一彦（NEC）
講演タイトル：組み合わせグループテストの改ざん検知への応用

アブストラクト：メッセージ認証コード（Message authentication code, MAC）などの暗号学的な改ざん検知手法では、一般に対象データから改ざんチェック用のタグを一つ生成しておく。この方法はデータ全体の改ざんの有無を明らかにする一方、データのどの位置が改ざんされたかの情報は得られない。
一方、データを適当なブロックに分割して個別にタグをとることでブロック単位の改ざん検知が可能となるが、タグはブロックの数だけ増大し、利用上の障害となる。従ってタグの増加を抑えつつ粒度の高い改ざん検知ができないかが課題となる。
本講演では、この問題に対する、古典的な組み合わせ論の問題である組み合わせグループテスト（Combinatorial group testing, CGT）からのアプローチを紹介する。さらにProperty-preservingハッシュ関数など近年注目される暗号技術とのかかわりについても述べる。

14:00-15:00
講演者：西村 優作（早稲田大学）
講演タイトル：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

アブストラクト：近年、格子同型問題に基づく耐量子計算機暗号が提案されており、格子同型問題は暗号理論の中で重要な問題である。
Ducas-Gibbons によって、LCD 符号から構成法 A で得られる格子に対し、hull 攻撃と呼ばれる格子同型問題解法が考案された。
この手法により、それらの格子の同型問題が$\mathbb{Z}^n$格子の同型問題およびグラフ同型問題へと帰着できることが示された。
ただし、Ducas-Gibbons の研究では有限体上の符号から得られる格子のみが対象とされていた。
本講演では、より一般的な場合として、整数 k に対して有限環$\mathbb{Z}/k\mathbb{Z}$上の自由 LCD 符号から得られる格子に対する hull 攻撃法を考察する。

特に、k が 4 の倍数ではない整数であれば、格子同型問題を$\mathbb{Z}^n$格子の同型問題およびグラフ同型問題へと帰着できることが判明したため、その結果を紹介する。

15:30-16:30
講演者：木本 一史（琉球大学）
講演タイトル：有限グラフ上の Chip-Firing Game と２変数ゼータ関数

アブストラクト：ループを持たない有限連結グラフに対し、有限体上の代数曲線に対する局所ゼータ関数の類似とみなせるような２変数ゼータ関数が定義される（Lorenzini,2012)。２変数ゼータ関数はグラフの sandpile 群（Jacobian）や Tutte 多項式とも密接に関連するグラフ不変量であるものの、これら３つのうちの任意の２つは残り１つを決定しない（Clancy-Leake-Payne, 2015)。本講演では２変数ゼータ関数を中心に、これらの話題について紹介する。

8月27日（水）

10:30-11:30
講演者：小関　健太（横浜国立大学）
講演タイトル：Coloring of graphs on surfaces

アブストラクト：「任意の平面グラフは 4-彩色を持つ」という四色定理は，グラフ理論では最も有名な定理であり，その証明以降も球面以外の閉曲面上のグラフを対象に多くの研究がなされてきた．特に，face-width というパラメータが大きいグラフは「局所平面的」と呼ばれ，平面グラフと類似の性質が成り立つことが知られている．
本発表では，この観点からの研究を紹介する．

IMI Workshop of the Joint Research Projects in Kyushu University

Mathematical sciences and application of expander graphs

Date : August 25-27, 2025
Place : Lecture Room (W1-C-501), West Zone 1,
Ito campus, Kyushu University

August 25 (Mon), 2025

14:00-15:00
Speaker : Masato Mimura (Tohoku University)
Title : Expanders in Geometric Group Theory

Abstract: The concept of expander graphs has been introduced in theoretical computer science, and expander graphs are regarded as "good" graphs. However, in Geometric Group Theory (and Large-scale Geometry), expanders often serve as a source of "pathological" examples. Also, formulations of "expanders" differ in detail between these two research fields. In this talk, I will present an overview of the formulation and applications of expanders in Geometric Group Theory.

15:30-16:30
Speaker : Shin-ichi Oguni (Ehime University)
Title : Large-scale geometry of groups and graphs, and related topics

Large-scale geometry, which is often called coarse geometry, treats unbounded geometric objects in view of large scale. For example, large-scale geometry does not distinguish the Euclidean line and any sequence of points arranged at constant intervals on the line. Thanks to such roughness, we can study infinite countable groups, which are originally algebraic objects, as geometric objects in large-scale geometry.
Also large-scale geometry often treats a family consisting of a countably infinite number of finite graphs as one geometric object.
We talk about relations among large-scale geometry, geometry of graphs and geometric group theory, where the coarse Baum-Connes conjecture, expander and graphical small cancellation theory are key words.

August 26 (Tues), 2025

10:30-11:30

Speaker : Kazuhiko Minematsu（NEC）

Title : Application of combinatorial group testing to message tamper detection

Abstract: Cryptographic tamper detection methods, such as message authentication code (MAC), generate a single authentication tag from the target data.
While this method reveals whether or not the entire data has been tampered with, it does not provide information on which part of the data has been tampered with.
On the other hand, dividing data into appropriate blocks and tagging each block individually enables block-wise detection, but the number of tags increases with the number of blocks, which is often costly in practice. A method with a small number of tags and a high resolution of tamper detection is desirable.
In this talk, I will introduce an approach to this problem from combinatorial group testing (CGT), a classical combinatorial problem. The relationship with advanced cryptographic techniques, such as property-preserving hash function, will also be discussed.

14:00-15:00

Speaker : Yusaku Nishimura (Waseda University)

Title : On Lattice Isomorphism Problems for Lattices from LCD Codes over Finite Rings

Abstract: These days, post-quantum cryptography based on the lattice isomorphism problem has been proposed. Ducas-Gibbons introduced the hull attack, which solves the lattice isomorphism problem for lattices obtained by Construction A from an LCD code over a finite field. Using this attack, they showed that the lattice isomorphism problem for such lattices can be reduced to the lattice isomorphism problem with the trivial lattice $\mathbb{Z}^n$ and the graph isomorphism problem. However, the previous work by Ducas-Gibbons only considered lattices constructed by a code over a finite field. In this talk, we considers lattices constructed by a code over a *finite ring* $\mathbb{Z}/k\mathbb{Z}$, which is a more general case. In particular, when k is not divisible by 4, we show that the lattice isomorphism problem can be reduced to the lattice isomorphism problem for $\mathbb{Z}^n$ and the graph isomorphism problem.

15:30-16:30
Speaker : Kazufumi Kimoto (University of the Ryukyus)
Title : Chip-Firing Games and Two-Variable Zeta Functions on Finite Graphs

Abstract: For a finite connected graph without loops, a two-variable zeta function can be defined that can be regarded as an analog of the local zeta function for algebraic curves over finite fields (Lorenzini, 2012).
Although this two-variable zeta function is a graph invariant closely related to the sandpile group (Jacobian) and the Tutte polynomial, any two of these three do not determine the remaining one (Clancy–Leake–Payne, 2015). In this talk, I will introduce these topics, with a focus on the two-variable zeta function

August 27 (Wed), 2025

10:30-11:30
Speaker : Kenta Ozeki (Yokohama National University)
Title : Coloring of graphs on surfaces

Abstract: The Four Color Theorem, which states that every planar graph is 4-colorable, is one of the most well-known theorems in graph theory.
Since it has been solved, many studies have focused on graphs embedded on nonspherical closed surfaces.
In particular, graphs with large face-width are called “locally planar,” and are known to exhibit properties similar to those of planar graphs.
In this talk, I will introduce research from this perspective.