第 5 回情報数理セミナー

日時 : 2023 年 6 月 10 日 (土) ～ 6 月 11 日 (日)
会場: 小山工業高等専門学校 専攻科棟 4 階多目的ホール

プログラム

6 月 10 日 (土)
9:00～ 会場準備

10:30～12:00 神戸 祐太 (三菱電機株式会社)
　超特異楕円曲線の自己準同型環の計算法とその実装

13:30～15:00 中川 皓平 (NTT 社会情報研究所)
　Kani の定理を用いた同種写像ベース署名について

15:30～17:00 土谷 昭善 (東邦大学)
　Kempe 同値とトーリックイデアルの 2 次生成性

～18:00 自由討論

6 月 11 日 (日)
9:00～ 会場準備

10:30～12:00 松井 紘樹 (徳島大学)
　Frobenius 押し出し関手の圏論的エントロピー

13:30～15:00 佐藤 謙太 (九州大学)
　基礎体の非分離拡大に対する特異点の振る舞いについて

15:30～17:00 榎園 誠 (立教大学)
　ファイバー曲面のモジュラー不変量について

～18:00 自由討論

世話人
金井 和貴 (呉工業高等専門学校 自然科学系分野)
神代 真也 (小山工業高等専門学校 一般科)
品川 和雅 (茨城大学 大学院 理工学研究科)
長峰 孝典 (小山工業高等専門学校 一般科)
宮本 賢伍 (茨城大学 大学院 理工学研究科)

本セミナーは JSPS 科研費 JP20K14302 および JP21K13782 の助成を受けたものです。

小山高専までのアクセスについては, 下記をご覧ください。
アクセス (小山高専 HP) https://www.oyama-ct.ac.jp/access/
バス時刻表 (小山高専–小山駅東口) https://www.city.oyama.tochigi.jp/uploaded/attachment/221306.pdf

アブストラクト

神戸 祐太 (三菱電機株式会社)
超特異楕円曲線の自己準同型環の計算法とその実装

超特異と呼ばれる楕円曲線の間の準同型写像がなすグラフは計算理論的に複雑であり、その事を利用した暗号方式は超特異同種写像暗号と呼ばれ、耐量子計算機暗号の候補である。本講演では超特異同種写像暗号の安全性解析を背景に、超特異楕円曲線の自己準同型環の計算法とその実装プログラムを紹介する。

中川 皓平 (NTT 社会情報研究所)
Kani の定理を用いた同種写像ベース署名について

昨年、代表的な同種写像暗号の一つである SIDH が、Kani の定理を用いた攻撃により破られることが Castryck&Decru により示された。

その一方で、今年には Robert らにより Kani の定理を用いた新たな署名方式 SQISignHD が発表され注目を浴びている。

このように、近年の同種写像暗号の研究において Kani の定理は重要な役割を担っている。

そこで本講演では、この Kani の定理について簡単に解説をし、それを用いた署名方式である SQISignHD について説明する。

土谷 昭善 (東邦大学)
Kempe 同値とトーリックイデアルの 2 次生成性

Perfect graph はグラフ理論における重要なクラスであり，禁止グラフを用いた perfect graph の特徴づけは strong perfect graph theorem と呼ばれ，グラフ理論における最も有名な定理の一つである．この perfect graph の中で特に重要なクラスとして，perfectly contractile graph というものがある．Perfectly contractile graph の禁止グラフを用いた特徴づけの予想が Everett と Reed によって提唱されたが，未解決のままである．一方，perfect graph は可換環論を使っても特徴づけることが可能である．実際，グラフが perfect となることと，付随する安定集合トーリックイデアルが compressed という性質を持つことは同値である．このようなグラフの可換環論的特徴づけを動機として，大杉氏と柴田氏との共同研究において，perfect graph G が perfectly contractile となることと，付随する安定集合トーリックイデアルが 2 次の二項式で生成されることが同値であることを予想した．

本講演では，perfect graph と perfectly contractile graph の背景から大杉–柴田–土谷予想ができた流れを紹介したあと，perfect graph とは限らないグラフに付随する安定集合トーリックイデアルが 2 次生成となる同値条件を，Kempe 同値と呼ばれるグラフ理論の古典的な概念を使って与え，多くのクラスで予想が正しいことを説明する．

松井 紘樹 (徳島大学)
Frobenius 押し出し関手の圏論的エントロピー

Dimitrov- Haiden-Katzarkov-Kontsevich は与えられた三角圏上の自己完全関手の複雑さを示す普遍量である，圏論的エントロピーを導入した．圏論的エントロピーは様々な分野で現れる種々のエントロピーの共通の類似物であるが，位相的エントロピーについては適切な設定のもとで圏論的エントロピーと一致することが菊田-高橋によって示されている．一方で，可換環論において現れるエントロピーとして局所エントロピーがある．これは Majidi Zolbanin-Miasnikov-Szpiro によって導入されたもので，可換ネーター局所環の自己準同型の複雑さを示すものである．Majidi Zolbanin-Miasnikov は，ある導来圏上の Frobenius 引き戻し関手の圏論的エントロピーと Frobenius 準同型の局所エントロピーの関係を調べている．本講演では，Majidi Zolbanin-Miasniko の結果の双対に相当するものとして，Frobenius 押し出し関手の圏論的エントロピーと Frobenius 準同型の局所エントロピーが一致すること示す．本発表は高橋亮氏との共同研究に基づく．

佐藤 謙太 (九州大学)
基礎体の非分離拡大に対する特異点の振る舞いについて

代数閉体とは限らない体上の代数多様体を, その基礎体の拡大体へと base change した時に, 特異点がどう振舞うか, という問題を考える. 多くの場合, 体の拡大が分離的の場合には特異点は悪くならないことが知られているが, 非分離的の時にはしばしば特異点の様子が大きく変わる. 本講演では, 「2 次元 klt 特異点」という特異点のクラスに関して, この問題を考える.

榎園 誠 (立教大学)
ファイバー曲面のモジュラー不変量について

ファイバー曲面のいくつかのモジュラー不変量の間の不等式 (スロープ不等式) は、代数曲面の分類問題や函数体上の代数曲線の有理点に関する問題、4 次元トポロジーにおけるレフシェッツ束の複素構造に関する問題などと関連して重要である。また半安定なファイバー曲面に関しては、安定曲線のモジュライ空間の交点理論から多くのスロープ不等式が得られることが知られている。本講演では、これらの研究の背景を述べた後、モジュライ空間の議論を拡張することにより、半安定とは限らないファイバー曲面に関して様々なスロープ不等式が得られることを説明する。