第 7 回情報数理セミナー

日時：2024 年 8 月 20 日 (火) ～ 8 月 21 日 (水)
会場: 日本大学理工学部駿河台キャンパス タワー・スコラ 2 階 S201

プログラム

8 月 20 日 (火)
9:00～ 会場準備

10:30～12:00 澤原 雅知 (弘前大学)
　高々星形特異点をもつアフィン平面の極小コンパクト化について

14:00～15:30 伊城 慎之介 (群馬工業高等専門学校)
　ネーター的パーフェクトイド理論について

16:00～17:30 青木 利隆 (神戸大学)
　パーシステントホモロジー入門

～18:00 自由討論

8 月 21 日 (水)
9:00～ 会場準備

10:30～12:00 神戸 祐太 (三菱電機株式会社)
　暗号応用を見据えた機械学習によるグレブナー基底計算

14:00～15:30 池松 泰彦 (九州大学)
　多変数署名方式とその安全性解析について

16:00～17:30 Jo Hyungrok (横浜国立大学)
　多重正則グラフ（multi-regular graph）に基づいたハッシュ関数について

～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 (大阪工業大学工学部 一般教育科)
品川 和雅 (茨城大学大学院 理工学研究科)
長峰 孝典 (日本大学理工学部 数学科)
宮本 賢伍 (茨城大学大学院 理工学研究科)

本セミナーは, 独立行政法人国立高等専門学校機構研究ネットワーク形成事業「数学分野と暗号分野の連携ネットワーク」および JSPS 科研費 JP21K13782 の助成を受けています。

アブストラクト

澤原 雅知 (弘前大学)

高々星形特異点をもつアフィン平面の極小コンパクト化について

複素数体上に定義されたアフィン平面の極小コンパクト化を考える．アフィン平面の極小コンパクト化において，高々対数的標準特異点をもつものは良く研究されている．特に，小島秀雄先生 (新潟大学) と高橋剛先生 (新潟大学) により，高々対数的標準特異点をもつアフィン平面の極小コンパクト化に現れる特異点は，星形特異点に限ることが示されている．本講演では，対数的標準特異点より悪い特異点をもつアフィン平面の極小コンパクト化を考察し，高々星形特異点をもつアフィン平面の極小コンパクト化の分類が得られたことについて報告する．

伊城 慎之介 (群馬工業高等専門学校)

ネーター的パーフェクトイド理論について

Yves André 氏による直和因子予想の解決以降，パーフェクトイド理論は混標数の可換環論を研究するための重要な手法の一つとして確立されてきた．一方で，パーフェクトイド理論において自然に表れる可換環は非ネーター環であるため，ネーター環論の手法を適用できない．講演者はパーフェクトイド理論とネーター環論の融合を目指し，パーフェクトイド塔とその傾化を導入した（仲里渓氏，下元数馬氏との共同研究）．本講演では，この理論のネーター的側面を中心に解説し，最近の進展についても紹介したい．

青木 利隆 (神戸大学)

パーシステントホモロジー入門

位相的データ解析（TDA）は、近年急速に発展しているデータ科学の分野であり、現在では様々な領域（材料科学、生命科学、宇宙論等）において大きな成功を収めている。中でも、パーシステントホモロジー解析（PH 解析）はデータの持つ位相的特徴の持続性（＝パーシステンス）に焦点を当てた解析手法であり、データの持つ隠れた情報への新たな洞察をもたらす。実際にはホモロジー群の列を用いてデータの形（連結成分、穴、空洞、etc.）を捉え、それらを一まとめにしたパーシステンス図を不変量として扱う。表現論の観点からは、このホモロジー群の列は A 型クイバーの表現とみなせることから、クイバー（多元環）の表現論が PH 解析において基礎となる。さらには、近年ではとりわけ「PH 解析の多パラメータ化」が時系列解析を含めた応用上の観点から重要な課題の一つとされている。本講演では、PH 解析を主に代数的・表現論的な観点から紹介する。標準 1 パラメータ解析における一連の構成をクイバー表現を基に理解し、計算アルゴリズムや活用例を見る。加えて、多パラメータ化に向けた理論（半順序集合上のパーシステンス加群）における主要なトピックや最近得られた結果についても紹介したい。

神戸 祐太 (三菱電機)
暗号応用を見据えた機械学習によるグレブナー基底計算

現代の暗号解読は、与えられた情報を基に数学問題を立式し、その求解を行うことで達成される。暗号解読を代数問題の求解に帰着させる方法を代数攻撃といい、代数攻撃はさらにグレブナー基底計算に帰着されることが多い。したがって、グレブナー基底計算量は暗号の安全性を評価するために重要である。一方、近年様々な数学問題において、機械学習モデルを用いることで、従来と比べて低い計算量で解を与える例が報告されている。そこで、グレブナー基底計算を機械学習モデルに学習させることにより、高速なグレブナー基底が実現され、従来の暗号の安全性評価が覆される可能性がある。本発表では千葉大計良先生を中心とした共同研究において得られた、グレブナー基底計算の機械学習理論研究の現状を報告し、上記の暗号攻撃シナリオがどれだけ現実的であるか、また、背景にある数学問題について紹介する。

池松 泰彦 (九州大学)
多変数署名方式とその安全性解析について

多変数多項式を利用した署名方式として UOV が再注目されている。この講演では、UOV の基本的な構成を説明し、UOV の安全性を測るための攻撃について解説する。さらに時間が許せば UOV が生成するイデアルの構造についての結果も紹介する。

Jo Hyungrok (横浜国立大学)
多重正則グラフ（multi-regular graph）に基づいたハッシュ関数について

1991 年、Zemor は Cayley グラフに基づいた暗号学的ハッシュ関数を初めて提案した。これを Cayley ハッシュ関数と呼ぶ。Cayley グラフは、有限体上に定義された群とその生成集合から構成されている。グラフの頂点は群の元を表し、辺は生成元によって作用される元のペアを表す。Cayley ハッシュ関数は、任意の長さの入力メッセージのビットを Cayley グラフの歩道（ウォーク）に変換し、任意の始点からグラフ上を歩道に従って歩き、最終的に到達した終点をハッシュ値として出力する決定的アルゴリズムである。衝突耐性を保証するために、Cayley ハッシュ関数の安全性は群論の Group word problem に依存する。特に、Cayley ハッシュ関数の衝突耐性は、Group word problem のグラフ理論的な観点から見ると、与えられたグラフで見つけられる最小サイクル長の拡張性と密接に関連している。

本講演では、Cayley グラフの一般化された概念を紹介し、従来の単一正則グラフとは異なり、多重次数を持つグラフを導出することを示す。これらの多重正則 Cayley グラフに基づいた暗号学的ハッシュ関数を提案し、その安全性問題に関連するいくつかの考察を述べる。本研究は、Cid Bustos-Reyes（NTT）氏との共同研究の結果であり、現在進行中である。