第 8 回情報数理セミナー プログラム

日時：2024 年 12 月 21 日 (土) ～ 12 月 22 日 (日)
会場: 茨城大学 水戸キャンパス 共通教育棟 2 号館 24 番教室

プログラム

12 月 21 日 (土)

8:30～ 会場準備・諸注意

10:00～11:30 高橋 裕太 (沼津工業高等専門学校)
スーパー形式群の構造について

13:30～15:00 中川 皓平 (NTT 社会情報研究所)
non-smooth な次数の同種写像計算手法とその暗号応用

15:30～17:00 佐竹 翔平 (熊本大学)
RIP matrices, Ramsey graphs and randomness extractors

～18:30 自由討論

12 月 22 日 (日)

8:30～ 会場準備・諸注意

10:00～11:30 磯部 遼太郎 (千葉大学)
On strict closure of rings

13:30～15:00 岡崎 勝男 (小山工業高等専門学校)
一般化された重み付き高さに関する Northcott 数

～18:30 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。

第 8 回情報数理セミナー アブストラクト

日時：2024 年 12 月 21 日 (土) ～ 12 月 22 日 (日)
会場: 茨城大学 水戸キャンパス 共通教育棟 2 号館 24 番教室

アブストラクト

12 月 21 日 (土)

高橋 裕太 (沼津工業高等専門学校)
スーパー形式群の構造について

物理学におけるスーパー・ストリング理論の発展に伴い，スーパー対称性に基づく幾何学が注目を集めている．数学においては標数が 2 でない体上の $\mathbb{Z}_2 = \{0, 1\}$ により次数付けられたベクトル空間の圏は，特殊な対称性（スーパー対称性）により対称テンソル圏となりスーパー・ベクトル空間の圏と呼ばれる．代数やスキームなどの対象は，このスーパー・ベクトル空間の圏上で定義されることでスーパー代数，スーパー・スキームへ一般化される．本講演では，スキームや形式群の関手による定義を紹介し，形式群のスーパー化であるスーパー形式群についてホップ代数的手法による研究成果について述べる．

中川 皓平 (NTT 社会情報研究所)
non-smooth な次数の同種写像計算手法とその暗号応用

耐量子暗号の一つである同種写像暗号の分野では近年, 高次元同種写像を利用した新方式が数多く提案されている．そのうちの一つである暗号方式 QFESTA の論文では, これまで効率的に計算することが困難だった non-smooth な次数の同種写像計算を, 2 次元同種写像と四元数代数を利用して効率的に行うアルゴリズムが提案された．本発表ではこのアルゴリズムについての解説を行い, 時間が許せばそのアルゴリズムを用いた暗号方式 (QFESTA, SQIsign2D 等) を紹介する．

佐竹 翔平 (熊本大学)
RIP matrices, Ramsey graphs and randomness extractors

RIP 行列はもともとは圧縮センシングの理論で登場したが, 今日では理論計算機科学, 組合せ論, 整数論などの様々な文脈で研究されている．本講演では, RIP 行列と組合せ論および理論計算機科学との関係性に焦点を当て, 特定の RIP 行列から Ramsey グラフおよび乱数抽出器が構成できることを紹介する．

12 月 22 日 (日)

磯部 遼太郎 (千葉大学)

On strict closure of rings

可換環 R とその整閉包 $\overline{R}$ に対して，

$$R^* = \left\{\alpha \in \overline{R} \mid \alpha \otimes 1 = 1 \otimes \alpha \text{ in } \overline{R} \otimes_R \overline{R}\right\}$$

は R と $\overline{R}$ の中間環となり，これを R の strict closure と呼ぶ。環の strict closure の概念は，1971 年に J. Lipman によって Arf 環の概念と同時に導入され，今日まで Arf 環や weakly Arf 環の理論と密接に関係しながら発展してきた。

本講演では，strict closure の持つ基礎的な性質や Arf 環との関係を説明しつつ，近日得られた研究成果をいくつか紹介する。また，整閉環の構造・理論と対比しながら，strict closure に関する理論の今後の課題や展望について説明する。

岡崎 勝男 (小山工業高等専門学校)

一般化された重み付き高さに関する Northcott 数

有理数体の無限次代数拡大のある種の有限性を測る量として, Northcott 数と呼ばれる非負の整数が知られています. Northcott 数は計算することすらも困難な対象であり, 実際に Northcott 数を導入した Vidaux と Videla は, 当該論文中でその分布の決定を問として出題していました. 少し昔ですが, 講演者は現 NTT 基礎数学センタの佐野薫さんとの共同研究で, この Vidaux と Videla の問を一般化した上で解決しましたので, 周辺事項と併せて紹介します。