研究集会

マトロイド理論と暗号理論の交差点

離散構造・符号・情報理論・計算

アブストラクト集

開催日	2026 年 8 月 3 日（月）・4 日（火）
会場	九州大学 伊都キャンパス ウエスト 1 号館 D 棟 4 階 IMI コンファレンスルーム（W1-D-414）
開催方法	対面・Zoom ミーティングによるハイブリッド開催
主催	九州大学マス・フォア・インダストリ研究所
研究代表者	今村 浩二
研究計画番号	2026a022

https://joint.imi.kyushu-u.ac.jp/post-20894/

目次

開催概要

研究計画題目	マトロイド理論と暗号理論の交差点（離散構造・符号・情報理論・計算）
種別	若手・学生研究—研究集会（II）
研究実施期間	2026 年 8 月 3 日（月）・4 日（火）
開催場所	九州大学 伊都キャンパス ウエスト 1 号館 D 棟 4 階 IMI コンファレンスルーム（W1-D-414）
開催方法	対面・Zoom ミーティングによるハイブリッド開催
主要言語	日本語
主催	九州大学マス・フォア・インダストリ研究所
研究代表者	今村 浩二
研究計画番号	2026a022

趣旨

本研究集会では，線形独立性や代数的独立性を抽象化するマトロイド・ポリマトロイド理論と，暗号・情報セキュリティを支える符号理論，情報理論，計算量理論との接点に焦点を当てる．

両分野の構造理論と安全性概念を相互に理解するための共通語彙を整え，具体例，計算手法，未解決問題を共有することを目的とする．さらに，グラフ，組合せデザイン，最適化，秘匿計算，ネットワーク符号化などの隣接分野も含めた交流を通じて，将来の共同研究につながる課題を見いだすことを目指す．

公式ウェブサイト

https://joint.imi.kyushu-u.ac.jp/post-20894/

プログラム

8 月 3 日（月）

時刻	内容
9:50–10:00	オープニング
10:00–11:00	**西村 優作**（早稲田大学・D1） 均等分割を用いた符号の平滑化限界
11:00–11:20	休憩
11:20–12:20	**城本 啓介**（熊本大学） 符号とマトロイドの臨界問題について
12:20–13:20	昼休み
13:20–14:20	**相馬 輔**（統計数理研究所） クイバー表現の半安定性と劣モジュラ最適化
14:20–14:40	休憩
14:40–15:40	**盧 暁南**（岐阜大学） 組合せデザイン・グループテスト行列とマトロイドとの接点
15:40–16:00	休憩
16:00–17:00	**神戸 祐太**（三菱電機） AI 時代の数学と暗号：機械学習による記号計算理論を通じた視点から

8 月 4 日（火）

時刻	内容
10:00–11:00	**中村 周平**（茨城大学） NIST 耐量子計算機暗号標準化計画における多変数多項式署名方式に対する攻撃の推移
11:00–11:20	休憩
11:20–12:20	**河瀬 康志**（中央大学） 離散凹評価をもつ二部市場における公平かつ事前安定な確率的割当
12:20–13:40	昼休み
13:40–14:40	**藤井 海斗**（京都大学） 局所探索の近似保証と均衡の社会的最適性
14:40–15:00	休憩
15:00–16:00	**品川 和雅**（筑波大学） PSM プロトコルの通信量について

2026 年 8 月 3 日（月）10:00–11:00

均等分割を用いた符号の平滑化限界

西村 優作

早稲田大学・D1

概要

耐量子暗号の観点から、符号ベース暗号の安全性に関する研究が注目を集めている。近年、Debris-Alazard らによって「平滑化限界」と呼ばれる符号の不変量が定義され、平滑化限界を最悪時平均時帰着といった安全性証明へ応用する試みがなされている。特に、Debris-Alazard らは有限アーベル群上での調和解析を用いて平滑化限界について示している。本講演では、グラフ上で定義されている均等分割を用いて、先行研究では扱われていなかった初期状態を持つ確率分布や非線形な符号に対しても、同様の平滑化限界に関する不等式が成立することを紹介する。本研究は、高島克幸氏（早稲田大学）と三枝崎剛氏（早稲田大学）との共同研究である。

2026 年 8 月 3 日（月）11:20–12:20

符号とマトロイドの臨界問題について

城本 啓介

熊本大学

概要

符号理論とマトロイド理論の関係については，主に有限体上の線形符号を用いたマトロイドの構成や符号のハミング重み多項式とマトロイドの Tutte 多項式に関する Greene 恒等式等が広く知られている．本講演では，上記の関係を紹介した上で，マトロイドの古典的問題である臨界問題の符号理論的解釈を紹介する．また，近年の結果として有限体上の行列を符号語とし 2 つの行列差の階数を符号語間の距離とした階数距離符号について，対応するマトロイド構造としてポリマトロイドの q-類似を導入し，符号の階数重み多項式と関係した Tutte 型多項式との恒等式の紹介，臨界問題の q-類似とそれに対応した階数距離符号の問題について紹介する．また，一般化階数重みに関する双対性を表す Wei 型恒等式についての概要を紹介する．

2026 年 8 月 3 日（月）13:20–14:20

クイバー表現の半安定性と劣モジュラ最適化

相馬 輔

統計数理研究所

概要

劣モジュラ性は，マトロイドをはじめとして，工学上の諸問題に現れ，効率的なアルゴリズム設計の鍵となる重要な性質である．近年，従来の劣モジュラ性を拡張した「部分空間上の劣モジュラ性」と呼ぶべき性質が，作用素スケーリング，共分散行列の推定，Brascamp-Lieb 多面体，クイバー（箙）の表現論などの問題に現れることが分かってきた．

本発表では，特にクイバー表現の半安定性に現れる「部分空間上の劣モジュラ性」に着目して，1) 半安定性の判定条件である King の条件に劣モジュラ基多面体のような多面錐（King 錐）が現れること，2) King 錐の組合せ構造を調べることで半安定性に関する様々な問題への効率的なアルゴリズムが得られること，について紹介する．

本発表は，岩政勇仁氏（神戸大），大城泰平氏（北大）との共同研究に基づく．

2026 年 8 月 3 日（月）14:40–15:40

組合せデザイン・グループテスト行列とマトロイドとの接点

盧 暁南

岐阜大学

概要

組合せデザインは，有限集合上の「均整性」をもつ部分集合族を対象とし，その構成法や代数的・幾何的性質を研究する分野であり，統計的実験計画法，符号理論，有限幾何学などと深く関係している．一方，グループテストは，多数のアイテムの中から少数の陽性アイテムを，できるだけ少ないテスト回数で特定することを目的とする手法である．特に非適応型グループテストでは，各テストで調べるアイテム集合をあらかじめ定め，そのテスト計画を，行をテスト，列をアイテムとする 0-1 行列として表す．本講演では，組合せデザインとグループテスト行列を題材として，マトロイド理論との接点を概観する．特に，デザインやテスト行列からマトロイド的構造を見出す方向と，マトロイドの視点からデザインやテスト行列を構成・解析する方向の双方について，基本例を交えながら紹介する．関連する符号理論・情報理論的な背景にも適宜触れる．

2026 年 8 月 3 日（月）16:00–17:00

AI 時代の数学と暗号：機械学習による記号計算理論を通じた視点から

神戸 祐太

三菱電機

概要

近年、AI、特に機械学習や大規模言語モデルの発展により、数学や暗号の研究方法は大きく変わりつつある。AI は定理証明、脆弱性発見、記号計算の高速化などに応用され、従来は人間が主に担っていた探索や検証の一部を補助する存在として注目されている。特に記号計算の文脈においては、こうした応用は単なる実装上の高速化にとどまらず、計算問題の学習のためのデータ生成アルゴリズムとその評価のための新たな理論開発を押し進め、純粋数学、応用数学、計算機科学など多岐にわたる分野に影響を及ぼしている。

本講演では機械学習によるグレブナー基底計算およびボーダー基底計算の高速化研究を中心に、機械学習技術の計算代数や暗号解析への応用理論を紹介する。さらに、そこで用いられている基本的な学習理念である、数学問題の End-to-End Formula-Driven 教師あり学習について紹介し、この学習理念が広く様々な数学問題に活用できること、またその活用に伴って生じる新しいタイプの数学的課題について説明する。

2026 年 8 月 4 日（火）10:00–11:00

NIST 耐量子計算機暗号標準化計画における多変数多項式署名方式に対する攻撃の推移

中村 周平

茨城大学

概要

暗号分野における課題の一つとして, 大規模な量子計算機が実現すると, 素因数分解問題や離散対数問題を基にした公開鍵暗号が危殆化することが知られている. この課題に対する対策の一つとして, 量子計算機を用いても求解困難と考えられる数学問題を基に暗号を設計する方法があり, このように設計された暗号は耐量子計算機暗号 (PQC) と呼ばれている. 米国国立標準技術研究所 (NIST) は, PQC 標準化プロジェクトを 2016 年に開始しており, これまでの成果として, 2022 年には格子暗号から 3 方式, ハッシュ暗号から 1 方式, 2025 年には符号暗号から 1 方式を標準化することを決定している. 多変数多項式暗号は, その安全性を連立二次方程式問題 (MQ 問題) の求解困難性に依存する暗号であり, 標準化プロジェクトにおいて候補方式として検討されている. 実際, 多変数多項式署名方式である UOV とその変種である MAYO, QR-UOV, SNOVA は, NIST PQC 追加デジタル署名プロジェクトの第 3 ラウンドにおいて現在検討が進められている. 本講演では, UOV を含む多変数多項式暗号に対してしばしば現れる, MinRank 問題への帰着に基づく攻撃を紹介し, NIST PQC 標準化計画における攻撃手法の推移を概観することを目指す.

2026 年 8 月 4 日（火）11:20–12:20

離散凹評価をもつ二部市場における公平かつ事前安定な確率的割当

河瀬 康志

中央大学

概要

学校選択や労働市場のような二部マッチング市場では，タイや無差別が自然に生じるため，抽選を用いて割当を決めることが多い．しかし，ランダムタイブレーキングによって事後的に安定な割当を選んでも，抽選前の確率的な割当として見ると，安定性や公平性が失われることがある．本研究では，複数の相手や契約の組合せに対する評価が離散凹性を満たす二部市場を対象に，公平かつ安定な確率的割当が常に存在することを示す．ここでの公平性とは，タイや無差別がある場合に，対称な立場にあるエージェントや選択肢を確率の意味で対称に扱うことを要求するものである．さらに，得られた分数的な割当は，安定な決定的割当上の抽選として実装できることを示す．加えて，数値的な効用ではなく順位選好のみを用いる設定を，マトロイド制約付きの契約マッチングとして定式化する．この枠組みは，定員制約やタイプ別制約を含む学校選択型の応用を包含し，マトロイド応答的な選好のもとで同様の存在結果が得られることを示す．本講演の内容は，今村謙三氏との共同研究成果に基づくものである．

2026 年 8 月 4 日（火）13:40–14:40

局所探索の近似保証と均衡の社会的最適性

藤井 海斗

京都大学

概要

局所探索とは、解の小さな変更を繰り返すことで目的関数値を徐々に改善していく組合せ最適化の汎用的な手法です。本講演では、目的関数や制約が劣モジュラ性やマトロイド性をもつ場合に得られる局所探索の近似保証を紹介します。一方で、ゲーム理論における均衡とは、プレイヤーたちが誰も逸脱することを望まないような状態のことです。局所探索の近似保証と近い技法によって、均衡において社会厚生が近似的に最大化されることを示し、局所探索と均衡の関連性を議論します。

2026 年 8 月 4 日（火）15:00–16:00

PSM プロトコルの通信量について

品川 和雅

筑波大学

概要

Private Simultaneous Messages（PSM）とは、各参加者が自分の入力と共有乱数に基づいて一度だけメッセージを送信し、受信者がそれらのメッセージから関数値のみを得る秘密計算モデルである。本講演では、PSM プロトコルの通信量に関する上下界について、既存研究と我々の研究を紹介する。

運営

研究代表者

今村 浩二（九州大学マス・フォア・インダストリ研究所・特任助教）

組織委員

- 縫田 光司（九州大学マス・フォア・インダストリ研究所・教授）
- 池松 泰彦（九州大学マス・フォア・インダストリ研究所・准教授）
- 中島 規博（名古屋工業大学 工学部・准教授）
- 佐竹 翔平（福岡大学 理学部応用数学科・准教授）
- 長峰 孝典（日本大学 理工学部・助教）
- 齋藤 琢弥（北海道大学 化学反応創成研究拠点・特任助教）

主催

九州大学マス・フォア・インダストリ研究所