2026年度共同利用研究報告書

2026年10月27日

所属・職名 九州大学 マス・フォア・インダストリ研究所・特任助教
今村 浩二

		整理番号	2026a022	
1.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）			
2.新規・継続	新規			
3.種別	若手・学生研究			
4.種目	研究集会（Ⅱ）			
5.開催方法	ハイブリッド開催			
6.研究代表者	氏名	今村 浩二		
	所属部局名	九州大学 マス・フォア・インダストリ研究所	職名	特任助教
7.研究実施期間	2026年08月03日(月曜日)～2026年08月04日(火曜日)			
8.キーワード	マトロイド, 誤り訂正符号, グラフ, 超平面配置, 暗号, 秘密分散, 秘匿計算, 情報セキュリティ			
9.参加者人数	67人			

10.本研究で得られた成果の概要

本研究集会では，マトロイド・ポリマトロイド理論と，暗号理論および符号理論，情報理論，計算量理論との接点を探ることを目的に，2日間で計9件の講演を行った．大学・研究機関および企業の研究者が参加し，対面30名，オンライン37名の計67名が集まった．

符号とマトロイドの対応，部分空間上の劣モジュラ性，暗号の安全性・通信量の評価を同一のプログラムで扱い，離散構造を異なる目的に用いる研究を比較するための具体的な題材を共有した．特に，階数距離符号とq-ポリマトロイド，クイバー表現の半安定性，MinRank問題に基づく暗号解析を通じて，行列や部分空間の構造を共通の対象として捉える視点を得た．また，符号の平滑化や秘密計算の通信量に関する講演は，組合せ論的な手法と暗号の安全性・効率との関係を考察する機会となった．

さらに，公平かつ事前安定な割当と局所探索の講演では，マトロイド性や劣モジュラ性が解の構成や質の保証に関わることが示された．機械学習を用いた記号計算や多変数多項式署名方式の解析も取り上げ，構造理論と具体的な計算手法を併せて考える題材を提供した．

大学院生や企業研究者による講演を組み合わせ，若手・学生が専門分野や所属を越えて研究内容に触れられる交流の場を設けた．今後は，小規模な符号や行列の具体例を通じて不変量や評価量，必要な仮定を比較し，秘密分散のアクセス構造や安全性評価も視野に入れながら，継続的な研究交流と共同研究につなげていきたい．

2026 年度 IMI 共同利用研究成果報告書

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）

整理番号：2026a022　　種別：若手・学生研究－研究集会（Ⅱ）
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）
実施期間：2026 年 8 月 3 日（月）〜8 月 4 日（火）
開催場所：九州大学伊都キャンパス IMI コンファレンスルーム（W1-D-414）
開催方法：対面と Zoom ミーティングによるハイブリッド開催

1　研究集会の目的

本研究集会は，マトロイド・ポリマトロイド理論と，暗号理論およびその基盤となる符号理論，情報理論，計算量理論との接点を探ることを目的として開催した．線形符号とマトロイドの対応に加え，秘密分散や情報理論的安全性の問題には，独立性，階数，劣モジュラ性などの離散構造が現れる．これらを異なる専門分野の研究者が共通の視点から捉え，今後の共同研究につながる問題を検討できる場を設けることを目指した．

そのため，符号とマトロイドの構造理論に関する講演と，暗号の安全性解析，秘密計算，組合せ最適化などの講演を組み合わせた．各分野で用いられる数学的知見や計算手法を，具体例を交えながら紹介していただくことで，理論間の対応と応用上の課題を共有する構成とした．

2　実施内容

2 日間にわたり，大学・研究機関および企業の研究者による計 9 件の講演を行った．参加者は対面 30 名，オンライン 37 名の計 67 名であった．各講演は 60 分の枠とし，基礎的な背景から研究上の課題までを紹介するプログラムとした．主な内容は以下のとおりである．

西村優作氏は，符号ベース暗号の安全性に関係する符号の平滑化限界を取り上げ，グラフの均等分割を用いた評価法を紹介した．非線形符号も含む設定を扱う内容であり，組合せ論的な手法と暗号の安全性解析との接点を示す講演となった．

城本啓介氏は，線形符号とマトロイドの関係を出発点に，臨界問題の符号理論的な解釈を解説した．さらに，階数距離符号と q-ポリマトロイド，多項式不変量，一般化階数重みの双対性を取り上げ，古典的な対応を q-類似へ広げる研究を紹介した．

相馬輔氏は，クイバー表現の半安定性を題材に，部分空間上の劣モジュラ性とアルゴリズムの関係を紹介した．盧暁南氏は，組合せデザインおよびグループテスト行列に現れるマトロイド的構造を取り上げ，構造の抽出と構成・解析の両方向から分野間の接点を解説した．

神戸祐太氏は，機械学習によるグレブナー基底・ボーダー基底計算の高速化を中心に，記号計算と暗号解析に関する研究を紹介した．中村周平氏は，多変数多項式署名方式に対する攻撃手法の推移を概観し，MinRank 問題への帰着に基づく解析を取り上げた．これらの講演では，代数的構造を計算する手法と，暗号の安全性を評価する課題が示された．

河瀬康志氏は，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と，マトロイド制約を用いた定式化を紹介した．藤井海斗氏は，劣モジュラ性やマトロイド性のもとでの局所探索の近似保証と，ゲーム理論における均衡の社会的最適性との関係を解説した．

品川和雅氏は，秘密計算のモデルである Private Simultaneous Messages（PSM）を取り上げ，通信量に関する上界・下界の研究を紹介した．PSM では，各送信者が自分の入力と共有乱数に基づくメッセージを一度だけ送り，受信者が関数値以外の情報を得ないことを要求する．この制約のもとで必要となる通信量を評価する問題を通じ，情報の秘匿と計算資源の関係を考えるための題材が提供された．

3　本研究集会で得られた成果

本研究集会では，符号とマトロイドの構造的な対応，劣モジュラ性に基づく計算手法，暗号の安全性と通信量の評価を，同一のプログラムの中で取り上げた．これにより，離散構造を分類・記述する研究と，その構造を利用して計算や情報処理を行う研究を比較するための具体的な題材を共有した．

特に，階数距離符号と q-ポリマトロイド，部分空間上の劣モジュラ性，MinRank 問題への帰着に基づく暗号解析という話題は，行列や部分空間の構造を異なる目的で扱う研究として位置づけられる．また，符号の平滑化や PSM の通信量に関する講演は，組合せ論的な対象や評価手法が暗号の安全性・効率とどのように関わるかを考える機会となった．

最適化に関する講演では，構造上の仮定がアルゴリズムや解の性質にどう反映されるかという視点が示された．クイバー表現の半安定性を判定する問題，公平性と安定性を満たす割当を構成する問題，局所探索で得られる解の質を保証する問題は，それぞれ異なる目的をもつ．これらを併せて扱うことで，マトロイド性や劣モジュラ性が，対象の構造の記述から，計算可能性や解の評価にまで関わることを具体例に即して捉える材料が得られた．

大学院生による講演に加え，企業研究者による記号計算と暗号解析の講演も取り入れ，若手・学生が専門分野や所属を越えて研究内容に触れられる場を設けた．対面とオンラインを併用したことで，遠隔地からも講演を聴講できる機会を確保した．マトロイド理論と暗号理論の関係を，符号理論や最適化などの隣接分野も含めて考察するための研究交流の機会を提供できた．

4　今後の課題と展望

今後の課題として，符号とマトロイドの対応を通じた不変量の計算や評価，部分空間に関する構造理論と計算手法の比較が挙げられる．とりわけ，q-ポリマトロイドの臨界問題や重み構造と，符号理論側の具体的な問題との対応を詳しく調べることは，研究代表者が進める研究とも接続する方向である．

これらの方向を具体化するためには，小規模な符号や行列，部分空間の例について，対応する離散構造と評価量を整理することが有用である．例えば，線形符号の重み分布を計算する方法として，符号語の列挙と多項式不変量の利用を比較したい．既知の結果を共通の例に適用して比較し，手法を移せる範囲と追加の検討が必要な点を見極めることを，今後の研究の出発点としたい．

また，当初の研究計画で掲げた秘密分散のアクセス構造やポリマトロイド不等式による安全性評価については，対象とする構造やプロトコルを絞り，具体例と既存手法の適用範囲を検討することが今後の課題となる．その際には，情報理論的な安全性を扱う場合と，特定の計算問題の困難性を仮定する場合を区別し，離散構造から導ける制約と追加の仮定が必要な部分を明確にしたい．本集会で紹介された研究を踏まえて具体的な問題を定め，継続的な研究交流や短期共同研究につなげていきたい．

開催日：2026/08/03〜2026/08/04

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）｜2026a022

カテゴリー：イベント　タグ：若手研究　研究集会II

開催概要

- **開催方法**：九州大学 伊都キャンパスとZoomミーティングによるハイブリッド開催
- **開催場所**：九州大学 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）
- **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
- **種別・種目**： 若手・学生研究-研究集会（Ⅱ）
- **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）
- **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）
- **研究実施期間**：2026年8月3日（月）〜2026年8月4日（火）
- **公開期間**：2026年8月3日（月）〜2026年8月4日（火）
- **研究計画詳細**：https://joint2.imi.kyushu-u.ac.jp/research_chooses/view/2026a022

プログラム

8月3日（月）

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

11:20-12:20

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

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

14:40-15:40

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

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）

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

11:20-12:20

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

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

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

申込方法

事前申込制（組織委員，講演者のかたも登録が必要です）
参加無料
定員になり次第，参加登録を締め切らせていただく場合がございます．

＼下記URLより参加登録をお願いいたします／

参加登録フォーム

Zoom（オンライン）からご参加の方

Zoomを使ったオンライン開催，ハイブリッド開催の場合

参加登録後に件名［九大IMIより］Zoom用URLのお知らせというメールがimikyoten@gmail.comから自動配信されます．
届いていない方は，お手数をおかけしますがもう一度ご登録いただくか下記にメールにてご連絡をお願い申し上げます．
（迷惑メールフォルダもご確認お願いいたします）

＜九州大学マス・フォア・インダストリ研究所 共同利用・共同研究拠点事務室＞
imikyoten(at)jimu.kyushu-u.ac.jp
(at)を@に変更してください

Zoomについて

開催日までにZoomアプリをインストールしてください．
Zoomアプリは無料版で問題なくご視聴いただけます．

ミーティング用Zoomクライアントのダウンロードは下記からお願いします．
すでにインストールされている方は最新版にアップデートをお願いいたします．
https://zoom.us/download#client_4meeting

パソコンやスマホへのインストール方法は下記をご参照ください．
https://zoom.nissho-ele.co.jp/blog/manual/zoom-install.html

Copyright © Institute of Mathematics for Industry, Kyushu University.