**立教大学学術推進特別重点資金（立教ＳＦＲ）**
**プロジェクト研究（共同プロジェクト研究）**
**２０１４年度研究【経過・成果】報告書**

| | | |
|---|---|---|
| **研究代表者** | 所属部局･職 | 氏　名 |
| | 理学部・教授 | 野呂　正行　　印 |
| **研究課題** | グレブナー基底候補の高速計算法，検証法および極小付属素イデアル計算への応用 | |
| **研究組織** | 所属研究機関・部局・職 | 氏　名 |
| | 理学部・教授 | 横山　和弘 |
| **研究期間** | ２０１４年度　～　２０１５年度 | |

| **研究経費** | ２０１４年度 | ２０１５年度 | 年度 | 総計 |
|---|---|---|---|---|
| **(上段：支出金額)** | 2,540,630 円 | 円 | 円 | 2,540,630 円 |
| **(下段：採択金額)** | 2,587,000 円 | 1,400,000 円 | 円 | 3,987,000 円 |

**研究の概要**（200～300 字で記入、図･グラフ等は使用しないこと。）

連立代数方程式の解を求めることや、その解の性質を調べることは、方程式に現れる多項式で生成されるイデアルを調べることになる。この多項式イデアルの本質はグレブナー基底と呼ばれるものにより表されるが、係数が有理数の場合には、不用意な計算法は係数膨張を招き計算不能に陥ってしまう。本研究では、モジュラー技法に基づく計算および分散並列計算を用いたグレブナー基底候補の高速計算法および候補の正当性の高速な検証方法をさらに発展させ、グレブナー基底の高速計算法を開発し、実装してその成果を確認する。さらに応用上重要な演算であるイデアルの極小付属素イデアル計算の高速なアルゴリズムを開発、実装する。

キーワード（研究内容をよく表しているものを３項目以内で記入。）

〔グレブナー基底　　〕〔イデアル分解　　〕〔モジュラー計算　　〕

**研究【経過・成果】の概要**（図･グラフ等は使用しないこと。）

本研究では、主としてモジュラー技法と呼ばれる、有限体上で計算したグレブナー基底の張り合わせで有理数体上のグレブナー基底候補を得る方法、および、その候補の正当性を示す方法について、並列化も併用した真に実用的な高速計算法の研究開発および、我々が開発、配布している計算代数システム Risa/Asir 上に計算機実装を行うことを第一の目的とする。さらに、それらを応用して、イデアルの極小付属素イデアル計算の高速計算法の開発およびその計算機実装を行うことも目標とする。本年度は、以下の各テーマにつき、研究開発を行った。

1. グレブナー基底候補の正当性検証法の研究および計算機実装

a) 生成関係式の計算による検証

グレブナー基底候補とは、有限体上のグレブナー基底を中国剰余定理等により張り合わせて、係数を有理数にひき戻して得られる多項式集合である。有理数体上のグレブナー基底の直接計算が中間係数膨張などにより困難な場合に、グレブナー基底候補により代数方程式系の解の候補を高速に得ることができる。もしこのグレブナー基底候補がもとのイデアルの部分集合であることが分かれば、候補の正当性は原理的には容易にわかるが、実際にはこの包含関係のチェックが困難である。本研究においては、このような場合に、基底候補を、もとのイデアルの生成系の多項式係数の積和で直接書きあらわす方法について一般ユーザが使える機能として本格的に実装した。
この応用として、これまで懸案となっていた、あるグレブナー基底候補の正当性を、2 日程度の計算で示すことができた。この成果を国際会議 ICMS2014 (International Congress on Mathematical Software) で発表した (研究発表[1])。

b) グレブナー基底チェックの並列化

グレブナー基底候補の正当性の検証においては、候補が、それ自身が生成するイデアルのグレブナー基底になっていることのチェックが必要となる。これは、候補から作られるすべての S 多項式をその候補で割った余りが 0 になるかどうかのチェックとなるが、この機能 Risa/Asir 上の OpenXM による分散並列計算機能を用いて実装した。負荷分散は S 多項式リストを全次数順に並べて機械的に worker に配布する方法を用いているが、十分な台数効果が実現できている(研究発表[9])。

2. グレブナー基底候補の並列計算の実装

有理数体上のイデアルのグレブナー基底候補を高速に計算するための関数を実装､公開した｡Worker を動的に起動し､それらを指定しての並列計算が容易にできる機能を備えている(研究発表[9])。

3. グレブナー基底候補計算の応用

楕円曲線の同種写像は数論における興味ある対象であると同時に、有限体上の楕円曲線の有理点群の位数計算にも重要な役割を果たす。同種写像は楕円曲線の間の有理写像であり、その写像を楕円曲線の係数により決定することは、ある代数方程式系の求解に帰着される。この計算をグレブナー基底計算による消去法の問題ととらえ、これまでに得た候補計算などの効率化技法がどこまで有効か検証した。ℓ次の同種写像はその次数ごとに計算を行うが、次数が 61 以下の素数に対し公式の作成が可能であることを示した。この計算には、本研究経費で購入したマルチコア計算機が大きな役割を果たした(研究発表[4,5,8])。

研究【経過・成果】の概要　つづき

4.イデアルの極小付属素イデアル計算の応用

本研究の目標であるイデアルの極小付属素イデアル計算は、連立代数方程式の解を、可能な限り分解することに相当する。ランダムに与えられた方程式に対してこのような操作で解を分解することは期待できないが、数学的な背景を持つ問題から生ずる方程式に対してはこのような分解計算が極めて有効に働く場合がある。本年度は、超幾何微分方程式と呼ばれる２階常微分方程式の解で定義される Schwarz 写像および、方程式をある形に変換したものから得られる種々の Schwarz 写像の間の関係、またこれらの写像の像である曲面の特異点の研究に対し、本研究の成果を応用することができた。超幾何方程式はいくつかのパラメタをもち、そのパラメタの値により得られる Schwarz 写像の性質は異なるが、特に monodromy 群が位数 6 の二面体群となる場合にその特異性を厳密に計算した。この計算は、多変数の連立代数方程式を解いて、その実数解の様子を調べることに帰着されるが、この計算を、われわれが開発した極小付属素イデアル計算を行うパッケージを改良しつつ行い、この場合における特異性を完全かつ厳密に調べることができた。この成果は、雑誌 International Journal of Mathematics に掲載予定である(研究発表[2])。

5. $F_5$ アルゴリズムの調査

グレブナー基底の高速計算法として最近注目されている $F_5$ アルゴリズム（最近では signature based アルゴリズムと呼ばれている）について、考案者である J.C. Faugere らのサーベイ論文 C. Eder, J.-C. Faugere, A survey on signature-based Groebner basis computations に基づき調査を行った。結果として、その正当性はある程度理解することはできた。次年度、科研費による研究において、さらに調査を進める。

6. 行列変数超幾何関数 ${}_1F_1$ が対角領域で満たす微分方程式系の計算

本テーマは、微分作用素環におけるグレブナー基底計算を目的とするもので、これまで述べてきた多項式イデアルに対する計算とやや趣を異にするが、統計学へのグレブナー基底の応用という、最近極めて活発に研究されている分野における重要問題であり、またそこに現れる有理関数の計算の効率化は、本研究の目的である極小付属素イデアル計算の高速化にとって大変重要である。行列変数 ${}_1F_1$ は、Wishart 分布と呼ばれる、統計学で基本的な多変量分布の分布関数を記述するもので、その値を高精度に計算することが応用上重要である。この計算については、変数の値がすべて異なる場合に、${}_1F_1$ が満たす偏微分方程式系のグレブナー基底を用いた HGM(Holonomic Gradient Method)を応用した高速計算法が提案されている。しかし、この方程式系は対角領域（変数のいくつかが等しい領域）で特異性を持つため、そこでは HGM を応用できない。我々はこの困難を克服するため、古典的なロピタル則と、グレブナー基底の項順序変換アルゴリズムである FGLM アルゴリズムを応用して、${}_1F_1$ が対角領域で満たす方程式系を計算するアルゴリズムを考案した。この方法により、9 変数までのすべての対角パターン（すなわち、変数が等しいブロックのパターン）について方程式系を計算することができた。この方法は、必ずしもグレブナー基底を与えることを保証しないが、これまで計算したものはすべてグレブナー基底になっていることが確かめられている。この計算を効率よく実現するため、有理式係数の除算アルゴリズムの高速化を、さまざまなデータ表現を用いて試みた。結果として、有理式を、できる限り通分せずに、分母を因数分解した形で保持し、その形を用いて簡約を行うという方法が現時点では最も効率がよいことが分かった。実際には、さらに、部分分数の形で保持して計算するのがより効率が上がることが、手計算の結果などからも予測される。これらの結果は、有理式係数のグレブナー基底計算の高速化に応用できると考えられる(研究発表[6,7])。

**研究発表**（研究によって得られた研究経過・成果を発表した①～④について、該当するものを記入してください。該当するものが多い場合は主要なものを抜粋してください。）

①雑誌論文（著者名、論文標題、雑誌名、巻号、発行年、ページ）
②図書（著者名、出版社、書名、発行年、総ページ数）
③シンポジウム・公開講演会等の開催（会名、開催日、開催場所）
④その他（学会発表、研究報告書の印刷等）

## ① 雑誌論文

[1] M. Noro, K. Yokoyama, Verification of Groebner Basis Candidates. Mathematical Software ICMS 2014, Lecture Notes in Computer Science Volume 8592, 2014, pp 419-424

[2] S. Fujimori, M. Noro, K. Saji, T. Sasaki, M. Yoshida, Schwarz maps for the hypergeometric differential equation. To appear in International Journal of Mathematics.

## ④その他

[3] Masayuki Noro, Verification of Groebner Basis Candidates, ICMS 2014, August 5, 2014, Hanyang University, Seoul, Korea

[4] 横山和弘, 楕円曲線の同種写像の計算公式、RIMS 研究集会「数式処理とその周辺分野の研究」,2014.12.25, 京大数理研

[5] 横山和弘, 楕円曲線の同種写像の計算公式、Workshop on Computational Number Theory with Implementations 2015. 2015.2.21, 九州大学

[6] Masayuki Noro, Computation of a system of partial differential equations satisfied by the hypergeometric function 1F1 of a matrix argument over diagonal region, Theoretical and Computational Aspects of Algebraic Analysis, the workshop on computational and algebraic methods in statistics, 2015.3.4, 東京大学

[7] Masayuki Noro, Computation of a system of partial differential equations satisfied by the hypergeometric function 1F1 of a matrix argument over diagonal region, Theoretical and Computational Aspects of Algebraic Analysis, 2015.3.7, 日本大学

[8] 横山和弘 楕円曲線の同種写像の計算公式（その２） Risa/Asir Conference 2015, 2015.3.19, 金沢大学

[9] 野呂正行, 小原功任 Risa/Asir の最新動向について Risa/Asir Conference 2015, 2015.3.19, 金沢大学