様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　１９　日現在

機関番号：　３２６８６
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2017
課題番号：　１５Ｋ０５００８

研究課題名（和文）グレブナー基底の高速計算法、検証法とその応用

研究課題名（英文）Efficient methods for Groebner basis computation, verification and thier applications

研究代表者

野呂　正行（NORO, Masayuki）

立教大学・理学部・教授

研究者番号：５０３３２７５５

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：グレブナー基底関連計算の高速化法であるモジュラー計算に関する研究成果を論文としてまとめて発表した。算法の正当性、停止性などに疑問点が多かったsignature based algorithm (SBA) について、ある程度満足の行く算法を開発し、2論文として発表した。楕円曲線暗号やPQCへの攻撃方法として主要な方法であるF4, SBAについて、これらで解読を試みた場合の計算量の解析について研究し、発表した。Wishart行列の累積分布関数が満たす方程式系を対角領域に制限した方程式系の計算方法を考案した。これは、最近盛んに研究されているグレブナー基底の統計への応用の１例である。

研究成果の概要（英文）：We published a paper describing various modular methods for efficient Groebner basis computation. We published two papers concerned with the signature based algorithm (SBA). In these papers we proposed several variants of SBA and showed their correctness and termination. F4 and SBA are main methods for attacking elliptic curve cryptography and post-quantum cryptography. We analyzed the complexity when we applied these methods to cryptanalysis. We studied the system of partial differential equations (PDE) satisfied by the cumulative distribution function (CDF) of Wishart matrices and proposed an efficient method for deriving a system of PDE satisfied by the restriction of the CDF on diagonal regions. This is an application of Groebner basis theory to statistics that is a very active research area.

研究分野：　計算代数

キーワード：　応用数学　計算代数　グレブナー基底　モジュラー計算

１．研究開始当初の背景

代数方程式系，微分方程式系は物理・工学など様々な分野に現れるもので，その解を求めることや，その解たちの性質を調べることは，数学的には方程式に現れる多項式，微分作用素の生成するイデアルを調べることになる．グレブナー基底はイデアルの本質をあらわにする重要なツールであり，その計算は，アルゴリズムの改良および，計算機ハードウェアの進歩により近年急速に実用性を増し，応用も広がっている．しかし，有理数体，有理関数体など無限体上での計算はまだ困難が多い．J. -C. Faugere による F4, F5 など，新世代のグレブナー基底計算アルゴリズムが提案されているが，有理数体上で F4 を飛び抜けて高速に実行するとされる Maple, Magma などのソフトウェアはすべて実装が非公開で，実際には正当性のない基底候補を出力していることが知られている．また F5 についてはその正当性，有効性研究対象となっていた．

２．研究の目的

代数方程式系，微分方程式系の解を求めることや，その解たちの性質を調べることは，数学的には方程式に現れる多項式，微分作用素の生成するイデアルを調べることになる．イデアルの本質は，グレブナー基底により与えられる．本研究においては，今までの研究で得たモジュラー技法に基づく計算によるグレブナー基底候補の高速生成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，実装する．これらをもとに，イデアル分解の高速アルゴリズムを開発，実装する．また，暗号などへの応用をもつ有限体上のグレブナー基底計算の高速計算法，微分作用素イデアルの制限イデアルについても研究する．

(1)グレブナー基底の高速計算と計算機実装

① 有限体上のグレブナー基底計算
有限体上のグレブナー基底計算は，係数膨張の困難がないため，F4 アルゴリズムが有効に働くが，F5 はさらに高速であるとの結果が発表されている．しかし，F5 の正当性，真の高速性について不明の点が多く，これについて理論，実装両面から検討し，有用なアイディアがあれば取り入れて，アルゴリズムに改良を加えてより高速な実装を実現する．

② 無限体上のグレブナー基底計算
有理数体，有理関数体などの無限体上のグレブナー基底を，その体上で直接高速に計算することは一般に限界があり，基底候補を計算し，その後で計算した候補が正しい基底であることを示す方法が現実的である．これらについて，これまでの研究成果に基づき，並列計算も併用した真に実用的な検証法の理論と計算法の開発，実装を目指す．

(2) グレブナー基底計算の応用

① イデアルの根基の素イデアル分解の高速計算法の研究とその計算機実装
イデアル I に対し，I の根基の素イデアル分解は代数方程式系の求解の重要なステップであり，解の構造を数学的に調べる基本となる．また，イデアル準素分解アルゴリズムの核心部分でもある．しかし，その計算は，種々の消去イデアルの計算を含み困難であることが多い．この困難を克服するため，1)で開発する方法，および分解自体を有限体上で行い，それらを張り合わせる方法の両面から研究し，実装する．

② 暗号研究への応用
有限体上のグレブナー基底の高速計算は，無限体上のグレブナー基底計算で重要であるだけでなく，それ自身，ある種の公開鍵暗号方式に現れる代数方程式系の求解の主要ツールとしても重要であるが，現状では効率面から非オープンなソフトを用いざるを得ない．本研究で，これらに匹敵するオープンな実装を実現することにより，有用な研究ツールを提供する．

③ 微分方程式系の部分多様体への制限
微分方程式系を満たす関数の値の計算法は holonomic 勾配法として確立されたが，方程式の特異点における値の計算には，方程式系を，特異点を含む部分多様体に制限することが必要となる．一般には D-加群の制限アルゴリズムによるが，これを，グレブナー基底の基底変換を効率的に行う FGLM 法に類似した方法により求める方法の実用化を目指す．

３．研究の方法

(1)グレブナー基底の高速計算と計算機実装

① 有限体上のグレブナー基底計算
F4 アルゴリズムは，係数膨張の生じない有限体上で特に有効である．Risa/Asir には既に実装され，それなりの効率を達成しているが，FGb (Maple に含まれる，現在最高速とされる実装)と比較すると不満足である．これを，FGb と匹敵するレベルに改良する．FGb に実装されているとされる F5 アルゴリズムについて詳細に調査，及び計算機実験を行い，有効と考えられる場合に本格的な実装を行う．

② 無限体上のグレブナー基底計算
i) 有限体上での分解の張り合わせによる候補計算
前研究の成果および前項の成果も応用して，

中国剰余定理による有理数体上の基底候補計算の高速化，並列化を達成する．この方法をさらに発展させ，候補計算の高速化を図る．

ii) グレブナー基底計算候補の正当性検証
非斉次イデアルのグレブナー基底候補の正当性の検証について，斉次化変数に関する saturation を用いたモジュラー計算法の有効性の検証および改良を行う．また，生成関係式のモジュラー計算によるグレブナー基底候補の検証法をさらに発展させ，並列化も含めた高速実装を行う．

③有理関数体上のグレブナー基底計算の効率化
イデアルを 0 次元化したあと必要となる有理関数体上のグレブナー基底計算について，その効率化方法を検討する．これに関しては，係数体を実際に有理関数体にする方法，ブロック項順序により通常の多項式環で計算する方法ともに一長一短がある．これらを適切にアルゴリズム選択する方法を考える．

(2)グレブナー基底の応用

① 微分方程式系の部分多様体への制限
行列変数 1F1 と呼ばれる多変数関数は Wishart 行列の最大固有値の分布関数に現れる．その関数値をホロノミック勾配法で計算する方法が与えられているが，変数のいくつかが等しい領域(対角領域)には適用できず，微分方程式系を対角領域に制限した方程式系のグレブナー基底が必要となる．この問題の場合，方程式は 0 次元だがホロノミックでないため D-加群における制限アルゴリズムは適用できない．我々は，この制限がロピタル則および FGLM 類似の方法により行えることを実験的に発見した．この方法を精密化，理論化し，より変数が多い場合，あるいは一般の 0 次元微分方程式系の場合に制限を計算する方法として確立する．

②根基の素イデアル分解
有限体上でのイデアル分解を，中国剰余定理を用いて貼り合わせ，有理数体上での分解に持ち上げる方法について研究し，効率的な計算法を提案する．有限体ごとに分解パターンが異なる場合の処理など，解決すべき困難は多いが，多項式因数分解と共通する点もあるので，その経験を元に有効な方法を確立したい．

③ 暗号研究用へのグレブナー基底の応用
グレブナー基底の理論は公開鍵暗号の安全性評価に利用されており，特に楕円曲線暗号や多変数公開鍵暗号の解読への応用が近年報告されている．これらの双方の解読では標数が 2 である有限体を係数とする代数方程式系のグレブナー基底の計算を行い，これらのグレブナー基底を計算するための計算量の理論値や実際の計算時間から，解読可能な暗号パラメータ（有限体の拡大次数や変数の個数など）を評価する．そのために，それぞれの代数方程式系に特化して F4 や F5 などを改良することで，それぞれのグレブナー基底を計算するアルゴリズムを構築し，それらに適した実装を行う．

４．研究成果

(1)グレブナー基底の高速計算と計算機実装

① 有限体上のグレブナー基底計算
signature based algorithm の研究に着手し，T. Vaccon 氏と共同で斉次イデアルの場合に，停止性と正当性を保証するアルゴリズムを構築した．成果を国際会議 ISSAC2017 で発表し（論文 3)，フルペーパーを雑誌に投稿した． さらに一般のイデアルに拡張し国際会議 ISSAC2018 に投稿し受理された(論文 7)．

② 無限体上のグレブナー基底計算
i）有限体上での分解の張り合わせによる候補計算
有限体上で F4 によりグレブナー基底を計算し，それらを中国剰余定理で張り合わせ，有理数に引き戻して有理数体上でのグレブナー基底候補を計算するための Risa/Asir パッケージ noro_grcrt.rr を開発した．これを楕円曲線間の同種写像に関する公式を与えるためのグレブナー基底計算に応用し，l=89 までの公式を作成できた．この結果は論文投稿中である．

ii）グレブナー基底計算候補の正当性検証
グレブナー基底計算の高速化のためのモジュラー技法をまとめた論文が受理された(論文 5)．本論文においては，まずこれまで定義されてきた様々な形の luckiness と呼ばれる概念の関係を明らかにした．これらは主として initial イデアルの対応に関するものであるが，我々は effective luckiness という概念をここで新たに定義した．これは，有理数体上の多項式イデアルの生成系の有限体上への準同型像が生成するイデアルのグレブナー基底と，元のイデアルのグレブナー基底が対応するという条件であり，この概念を用いることで，準同型像から得られた元のイデアルのグレブナー基底候補の正当性の検証法を種々の場合に明らかにすることができた．さらに，Hilbert luckiness という概念を定義し，懸案であった非斉次イデアルのグレブナー基底候補のための有用な十分条件を与えた．また，グレブナー基底計算の上位演算である種々のイデアル演算（イデアル商，saturation，イデアル分解）などについても，検証法を含めた統一的なモジュラー計算の枠組みを与えた．

③ 有理関数体上のグレブナー基底計算の効率化
有理関数体上のグレブナー基底計算の困難性によりしばしばボトルネックとなる有理関数体上での最小多項式計算において，種々の消去法を同時に競争的に実行し，最速で返ってきた計算結果を用いて計算を続行する方法を実装した．これは Risa/Asir の OpenXM による競争的実行機能の応用である．これにより，これまで続行が困難であったある種の素イデアル分解が最後まで遂行可能になった(発表 13)．

(2)グレブナー基底の応用

① 微分方程式系の部分多様体への制限
行列変数 1F1 が満たす微分方程式の対角領域への制限を，簡約化ルールをロピタル則を用いて機械的に生成し，再帰的に用いることで 36 変数までのすべての対角領域パターンに対し計算できることを示した．この結果は国際会議 ISSAC2016 に受理され，発表することができた(論文 1)．また，この結果を含む Wishart 行列の最大固有値の分布関数を対角領域上で計算する Risa/Asir 上のパッケージ n_wishartd．rr を公開した．さらに，同様の方法が行列変数 2F1 が満たす微分方程式にも適用できることがわかり，Wishart 行列の比の最大固有値の分布関数の計算も同パッケージで計算できるよう機能追加を行った(発表 8)．

②根基の素イデアル分解
研究協力者である青山暢氏の，２項式イデアルの根基の素イデアル分解に関する結果が ISSAC2017 に受理された(論文 2)．また，青山氏と研究代表者の共著の，有理関数体上でのイデアルの根基の素イデアル分解において，パラメタ変数に値を代入して得られるイデアルの分解結果を中国剰余定理で結合し，多項式-有理式変換で分解の候補を得る算法の論文が ISSAC2018 に受理された(論文 6)．

③ 暗号研究へのグレブナー基底の応用
公開鍵暗号の安全な暗号パラメータはその解読アルゴリズムの計算量から算出される．楕円曲線暗号やいくつかの耐量子計算機暗号(PQC)への攻撃方法として，F4 アルゴリズムや F5 アルゴリズムが挙げられる．しかし，それらの計算量は未解決な部分があり，また実際にそれらで解読を試みた場合の影響を評価する課題がある．本研究ではそれらの課題に取り組み，その成果を招待講演等（発表 9，12）及び電子政府推奨暗号を評価するプロジェクト(CRYPTREC)の技術報告書(論文 4)において発表した．

５．主な発表論文等

（研究代表者，研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　7 件）

① V. Tristan, K. Yokoyama, On Affince Tropical F5 Algorithms, Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation (ISSAC 2018), 査読有, 2018, 印刷中.
② T. Aoyama, M. Noro, Modular Algorithms for Computing Minimal Associated Primes and radicals of Polynomial Ideals, Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation(ISSAC 2018), 査読有, 2018, 印刷中.
③ M. Noro, K. Yokoyama, Usage of Modular Techniques for Efficient Computation of Ideal Operations, Mathematics in Computer Science, 査読有, 2018, 12, pp1-32, DOI https://doi.org/10.1007/s11786-017-0325-1
④ 篠原直行，野呂正行，横山和弘，楕円曲線上の離散対数問題に関する指数計算法，CRYPTREC Report 2016，査読有，2017，pp71-100.
⑤ T. Vaccon, K. Yokoyama, A Tropical F5 Algorithm. 4 Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation (ISSAC 2017), 査読有, 2017, pp429-436.
⑥ T. Aoyama, An Algorithm for Computing Minimal Associated Primes of Binomial Ideals without Producing Redundant Components, Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation (ISSAC 2017), 査読有, 2017, pp21-27.
⑦ M. Noro, System of Partial Differential Equations for the Hypergeometric Function 1F1 of a Matrix Argument on Diagonal Regions, Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation (ISSAC 2016), 査読有, 2016, pp381-388.

〔学会発表〕（計　14　件）

① 横山和弘，楕円曲線の同種写像の公式作成における計算機代数の利用，Risa/Asir Conference 2018, 2018.
② 野呂正行，有理関数体上の最小多項式の

計算について，Risa/Asir Conference 2018，2018.

③ 篠原直行，耐量子計算機暗号の最新動向と NICT の取り組み，SecurityDay2017 (招待講演) 2017.

④ 横山和弘，楕円曲線の同種写像の公式生成について，九州代数的整数論 2017（招待講演），2017.

⑤ 横山和弘，近年の数式処理と将来の展望，RIMS 研究集会「数式処理の新たな発展」（招待講演），2016.

⑥ 篠原直行，楕円離散対数問題に対する指数計算法，代数幾何学と暗号数理の展開 (国際学会，招待講演)，2017.

⑦ 野 呂 正 行 ， Risa/Asir 2016-2017，Risa/Asir conference 2017，2017.

⑧ M. Noro，System of Partial Differential Equations for the Hypergeometric Function 1F1 of a Matrix Argument on Diagonal Regions，ISSAC2016 (国際学会)，2016.

⑨ K. Yokoyama，M. Noro，Modular Techiniques for Efficient Computation of Ideal Operation，ICIAM 2015（招待講演）(国際学会），2015.

⑩ 篠原直行，小標数の有限体上の離散対数問題の解法，第 11 回「代数学と計算」研究集会 (AC2015)（招待講演），2015.

⑪ 横山和弘，グレブナー基底計算の効率化，RIMS 研究集会「数式処理研究の新たな発展」(招待講演），2015.

⑫ K. Yokoyama，Stabilityu of Parametric Decomposition，Dagstuhl Seminar 15471 Symbolic Computation and Satisfiability (招待講演) (国際学会)，2015.

⑬ 野呂正行，matrix 1F1 が対角領域上で満たす微分方程式系を用いた分布関数の値の計算，Risa/Asir Conference 2016，2016.

⑭ 野呂正行，行列変数 1F1 の対角領域への制限が満たす微分方程式系の計算，RIMS 研究集会「数式処理とその周辺分野の研究 ― Computer Algebra and Related Topics」，2015.

〔図書〕（計 件）

〔産業財産権〕

○出願状況（計 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計 件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等
http://www2.rikkyo.ac.jp/web/noro

６．研究組織

(1)研究代表者
野呂正行 （NORO Masayuki）
立教大学・理学部・教授
研究者番号：50332755

(2)研究分担者
横山和弘 （YOKOYAMA Kazuhiro）
立教大学・理学部・教授
研究者番号：30333454
篠原直行 (SHINOHARA Naoyuki)

国立研究開発法人情報通信研究機構・サイバーセキュリティ研究所セキュリティ基盤研究室・主任研究員
研究者番号 ： 70565986

(3)連携研究者
( )
研究者番号：

(4)研究協力者
青山暢（AOYAMA Toru）
神戸大学・理学研究科・博士後期課程