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

令和　６ 年　 ５ 月 ２８ 日現在

機関番号：３２６８６
研究種目：基盤研究(C)（一般）
研究期間：2021～2023
課題番号：２１Ｋ０３３７７

研究課題名（和文）グレブナー基底計算の理論計算量解析とその効率的な実装

研究課題名（英文）Complexity analysis and effective implementation of computation of Groebner bases

研究代表者
横山　和弘（Yokoyama, Kazuhiro）

立教大学・理学部・名誉教授

研究者番号：３０３３３４５４

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：計算量理論解析においては、基本的かつ暗号等に現れるイデアルの生成系がアフィン半正則になる場合に既存の計算量解析の検証を行い、その改良およびSBAの観点よるグレブナー基底計算過程の正確な記述に成功した。
SBAアルゴリズム実装の改良においては、ヒルベルト関数値を利用した基底変換の効率化、S多項式やreducerのベクトル化を用いた簡約操作の効率化などに成功し、F4アルゴリズム実装のマルチスレッド化なども行なった。グレブナー基底計算の応用では、多変数公開鍵暗号の安全性の基礎となるMQ問題解法、楕円曲線の同種写像問題解法、実験計画法における実施計画の決定などに適用した。

研究成果の学術的意義や社会的意義
グレブナー基底は、代数学に留まらずに様々な分野に応用されているが、一般には計算量が大きく、大規模な問題等には有効には適用できないこともあり、その計算の効率化が強く求められている。この効率化の基盤として、正確な計算量の解析が不可欠であり、同時に効率的な実装による検証も重要である。また、効率的な実装では、工学等の実際の問題への適用事例研究が適している。本研究では、この３課題を同時並行に行い、それぞれに関して独自かつ有効な結果が得られたことは、今後のグレブナー基底計算の応用を含めた発展に貢献できたものと考える。

研究成果の概要（英文）：As to the complexity analysis, we dealt with ideals whose generators are affine semi-regular, which are considered as basic cases but frequently appear in engineering science such as public-key cryptography. Inspecting existing results, we succeeded in improving them and in describing the behavior of Groebner bases computation accurately.
As to efficient implementation of SBA algorithms, we applied it successfully to efficient change of basis with help of Hilbert functions, to efficient S-polynomial reduction based on vectorization of polynomials, and to parallelization of F4 type reductions.
As to the application of Groebner basis computation, we also applied it efficiently to engineering problems, such as MQ-problems from multivariate polynomial cryptosystems, problems from elliptic curve isogenies, and problems from the design of experiments.

研究分野：代数学

キーワード：計算機代数　数理情報科学　グレブナー基底

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

研究代表者・分担者らは独自に開発している数式処理システム Risa/Asir の中心的機能としてのグレブナー基底計算の効率化に長年取り組んできた。基本アルゴリズムであるブッフバーガーアルゴリズムとその改良型とされる F4 アルゴリズムに対して、様々な効率化テクニックを積極的に取り入れることで、数学的正当性を保ちつつ実用に耐えうるような機能を提供してきた。それでもなお、計算が困難となるような入力イデアルは存在している。J.C.フォジェールが signature と呼ばれる多項式に紐付けした概念を利用した F5 アルゴリズムを発表し、従来法と比較して、計算上で無駄な S 多項式(0 に簡約されるもの)を大きく減らすことに成功し、結果として圧倒的な高速化が達成できることを示した。しかし、その正当性や停止性の証明は不正確であった。以来、正当性や停止性の研究をきっかけとして数多くの変種が考案されそれらはまとめて signature based algorithm(SBA)と呼ばれている。研究開始時点においては、ある構成法に従えば停止性や正当性は保証されることが示されてはいるが、F5 論文で示されたほどの高速性は、一般に利用可能なソフトウェア上では実現されていなかった。すなわち、SBA は計算困難な場合の状況を改善できるアルゴリズムの一つとして期待されるものであるが、その実用化、すなわち正当性や停止性を保証しつつ実際の計算時間を短縮する詳細なアルゴリズム設計とその実装が必要と思われていた。担当者らは 「グレブナー基底計算アルゴリズムの深化」(科研費基盤(C)2018 年度-2020 年度 18K03432)において SBA のある構成法を考案し、それに従った実装を行ったところ、いくつかの例に対して、従来のアルゴリズムより計算時間が短縮できることが確認できた。この先行研究が SBA の実用化に向けての明るい見通しとなり、この方向の研究をさらに深めることに意味があると考えた。実際、SBA の理論的解析に関しては、研究代表者が富士通研究所との共同研究において、グレブナー基底計算の計算量の下限の導出に統計的な仮定の下で、signature を用いた計算法が多項式の GCD における部分終結式に該当することを発見し、理論的に計算に必要となる S-多項式の個数の評価ができたことかも重要な成功事例になっている。 また、研究代表者と T.バッコン氏との一連の共同研究が大きなポイントになっている。そこでは tropical case という特殊な場合への SBA の拡張を行なったが、この研究で signature に対する深い考察に基づく一般の場合の SBA アルゴリズムの構成法が構築され、このアルゴリズムをベースとする実装により SBA による計算時間の短縮が実現できた。実装面では、既に数式処理システム Risa/Asir に実装済みの多項式演算および F4 用の行列演算関数の存在がある。これらに signature 操作を付け加えることで SBA に対応することができ、計算効率化技法であるモジュラー計算法にも対応できると考えている。

２．研究の目的

我々は、本研究に入る前にある種の SBA を提案し、それに基づいた実装実験により、ある種の入力に対しては、我々の SBA 構成法が従来法より効率的であることを確認した。しかし、その優位性の理論的な説明が不明であった。実際、SBA では除算に制限があるため、無駄な基底の元を生成している可能性が残っていた。これは冗長な基底の生成、S 多項式の増加を招く要因となるるため、精密な解析が必要である。また、正当性や停止性が保証された構成法のもとで、F5 論文に示された「高速性」と同等なものを達成する方法も明らかではない。 以上により、

・理論面では、SBA がなぜ従来法より無駄な簡約となる S 多項式を多く排除できるのか、さらに、全体としての計算の手間をなぜ下げることができるのか、

・実装面では、F5 論文に示された結果に匹敵する性能をもつ SBA 実装がいかにして可能か、

を明らかにすることを本研究の目標とした。さらに、これらの解析において、同じ計算システム上で各アルゴリズムの実装を行って計算時間を比較することや応用事例として暗号安全性解析に関する実際のグレブナー基底計算での、SBA の実用性を調べることも目的とした。

３．研究の方法

上記の目的のため、研究を３テーマ(理論的解析、効果的実装、応用)に分け、研究代表者（横山）が統括を行った。

(1) SBA アルゴリズムの優位性の理論的解析

SBA が生成する S-多項式の個数が signature を使わない他の高速計算法で生成される S 多項式の個数より少ないことを理論的に解明するための第 1 段階として、単純ではあるが暗号安全性解析等の応用とも深く関係がある設定の下で解析を行った。

・イデアルが 0 次元である。

・イデアルの生成集合の syzygy が利用できる。

ここで解析の鍵となるものは、signature と先頭項の関係である。理論的に扱いやすい minimal signature を用いることで、同じ signature を持つ元の中でΣ既約、すなわちイデアルの他の元でΣ簡約できないものが最小の先頭項を持ち、それが signature によって一意に定まる性質を使うことができる。また、正確な理論構築のため、公開鍵暗号等で使われるイデアルの生成系が

正則・半正則である場合を考えた。
(2) SBA アルゴリズム実装の改良
すでに実験版の SBA アルゴリズムが実装されてる Risa/Asir 上で以下の改良や新実装を行った。
①signature の順序の最適化：signature の順序(加群項順序)は全体の計算に大きな影響を及ぼす。POT 順序や Schreyer 型の順序などが知られているが、多くの種類の順序に対する実験を行なって、入力生成系に最適な順序の確認を行った。
② F4 タイプ実装の改良：実験版では、最小の sugar を持つ S 多項式を全て選んで行列上で簡約する F4 タイプの実装を行った。この方法で通常の F4 より大幅に高速化する場合もあるが、冗長な基底が多数生成され、通常の SBA より効率が落ちる場合もある。S 多項式を構成する S ペアの集合を選ぶ最適な方法についてさらなる検討を加え、より高速な実装を目指した。
③ モジュラー計算法の導入：従来のアルゴリズムで有効だったモジュラー計算法を SBA に応用する方法について研究した。
(3) 応用研究
公開鍵系の暗号の安全性解析を取り上げた。安全性解析では、連立代数方程式の解法に帰着されるタイプのものがいくつかある。多変数多項式を用いた暗号系や、楕円曲線離散対数問題、さらには同種写像暗号に対しての代数的攻撃では、有限体上でのグレブナー基底計算が重要なパートを占めており、その実際的な実装や正確な計算量解析が求められている。SBA は最も高速にグレブナー基底計算をする方法と信じられているので、これらの実例に対し計算機実験を行い、その実用性を検証した。

４．研究成果
(1) 理論解析：
①イデアルの生成系がアフィン半正則になる場合に既存の計算量解析の検証を行い、その改良およびグレブナー基底の計算過程の正確な記述に成功した。いわゆる過剰決定系（変数の個数より生成系 F の多項式の個数が多い場合）で、項順序を全次数逆辞書式と設定した場合に、生成系の最大斉次成分全体 F_top が半正則になる場合がアフィン半正則と呼ばれる。この場合に、最大斉次成分のなすイデアルの正則次数を D とした場合に、D-1 次以下までのグレブナー基底計算において F と F_top および F の斉次化 F_hom のグレブナー基底計算のプロセスに完全な一致があることを厳密に証明し、SBA を用いた場合には、ここまでには無駄な S 多項式は現れないこと、さらには F_hom のグレブナー基底に現れる最大次数の元の上からのより正確な評価を与えることに成功した。これらの成果として、1 件が欧文雑誌に投稿し採択され、もう 1 件が計算代数幾何の権威ある国際会議 MEGA に採択された。(7 月に口頭発表予定。)
②第 2 段階と考えている「より一般的な形での SBA 理論」に関し、非可換代数である交代代数におけるグレブナー計算に SBA を適用しその実験を行なった。成果を国際会議で発表した。
(2) SBA アルゴリズム実装の改良：
① 多項式環の項順序と整合しない(compatible でない)加群項順序を用いた SBA アルゴリズムは停止性が保証されないが、入力イデアルをある項順序に関するグレブナー基底とすることで、ヒルベルト-ポワンカレ級数による停止条件を用いて目的項順序に関するグレブナー基底を有限回 の手間で計算する方法を考案した。この方法では syzygy criterion により 0 簡約が生じないため、モジュラー計算法を用いなくても効率よく有理数体上のグレブナー基底が求められた。当初は、非 0 次元イデアルに対してのみ有効であると予想したが、実際には 0 次元でも有効な場合があることがわかった。計算機実験では、さまざまな例に対し全次数逆辞書式順序グレブナー基底を入力として辞書式順序グレブナー基底の計算を行い、計算時間・中間基底の係数の大きさなどを調べた。結果として、多くの場合に先頭項のみの簡約が計算時間の短縮において有利だが、少数の例で係数の大きさが影響して多項式全体を簡約する場合ほうが有利な場合があることが分かった。これらの成果は国際会議や国内会議で発表した。
② 簡約操作の効率化：SBA は、ブッフバーガー算法と同様に S 多項式を中間基底で簡約することで計算が進行するが、S 多項式の選択順序および簡約に条件がつくため、F4 アルゴリズムのように、「一度に多くの S 多項式を取り出して、それを簡約するのに十分な reducer(簡約に使う多項式) を用意してベクトル化を行い、最終的に行列の形に直した上で簡約を行う」という方法が取りにくい。そこで、SBA における S 多項式の選択順序に従って、毎回 1 つの S 多項式を簡約するが、簡約自体は S 多項式やそれを簡約する reducer をベクトル化して、ベクトルに対する簡約で行う方法を考案した。計算機 代数システム Risa/Asir 上での計算機実験を行い、全次数辞書式順序でのグレブナー基底計算において、最大 10 倍程度高速化する場合があることがわかった。これらの成果は国内会議で発表した。
③ F4 アルゴリズムの実装における Risa/Asir のマルチスレッド化：ここでは reducer set(簡約に使う多項式集合)を固定したベクトル形式での多項式除算(簡約)とモジュラー計算による行列簡約の部分を並列化した。実験の結果、8 スレッド程度までの並列化では十分な台数効果が得られることが分かった。
(3)応用研究：SBA の適用までは至らなかったが、グレブナー基底計算の応用事例を扱い、その有効性を検証した。
①多変数公開鍵暗号の安全性の基礎となる MQ 問題と呼ばれる「連立 2 次多変数代数方程式の解

を求める問題」をグレブナー基底計算を使って効率的に解くことを検討し，ここでは F4 型のアルゴリズムを適用し、MQ 問題を効率良く解くために S 多項式及び reducer の選択を多項式の 2 番目に大きな項に注目した新たな方法を考案し、効率よく計算できることを数値実験的に確認した。これらの成果は欧文論文誌、和文論文誌や国内会議で発表した。
②実験計画法におけるある条件を満たす一部実施計画の決定を、あるイデアルの零点計算に帰着させ、それを実際に解くことにより解決した。これらの成果は欧文論文誌で発表した。
③ 楕円曲線の同種写像問題について、グレブナー基底計算によって得られた同種写像公式を利用した方法を構築し、効率化を達成した。これらの成果は欧文論文誌や国際会議で発表した。

５．主な発表論文等

〔雑誌論文〕　計10件（うち査読付論文　9件／うち国際共著　0件／うちオープンアクセス　2件）

１．著者名 Ito Takuma, Hoshi Yuta, Shinohara Naoyuki, Uchiyama Shigenori	４．巻 14
２．論文標題 Polynomial selection of F4 for solving the MQ problem	５．発行年 2022年
３．雑誌名 JSIAM Letters	６．最初と最後の頁 135～138
掲載論文のDOI（デジタルオブジェクト識別子） 10.14495/jsiaml.14.135	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 野呂正行	４．巻 2224
２．論文標題 Non-compatible な加群項順序の下でのsignature-based algorithm について	５．発行年 2022年
３．雑誌名 京都大学数理解析研究所講究録	６．最初と最後の頁 1-9
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Aoki Satoshi, Noro Masayuki	４．巻 -
２．論文標題 Use of primary decomposition of polynomial ideals arising from indicator functions to enumerate orthogonal fractions	５．発行年 2022年
３．雑誌名 Japanese Journal of Statistics and Data Science	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s42081-022-00149-z	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Ito Takuma, Nitta Atsushi, Hoshi Yuta, Shinohara Naoyuki, Uchiyama Shigenori	４．巻 13
２．論文標題 Polynomial selection for computing Groebner bases	５．発行年 2021年
３．雑誌名 JSIAM Letters	６．最初と最後の頁 72～75
掲載論文のDOI（デジタルオブジェクト識別子） 10.14495/jsiaml.13.72	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Kambe Yuta, Yasuda Masaya, Noro Masayuki, Yokoyama Kazuhiro, Aikawa Yusuke, Takashima Katsuyuki, Kudo Momonari	４．巻 1
２．論文標題 Solving the constructive Deuring correspondence via the Kohel-Laurer-Petit-Tignol algorithm	５．発行年 2022年
３．雑誌名 Mathematical Cryptology	６．最初と最後の頁 10~24
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Kudo Momonari, Yokoyama Kazuhiro	４．巻 -
２．論文標題 On Hilbert-Poincare series of affine semi-regular polynomial sequences and related Groebner bases	５．発行年 2024年
３．雑誌名 Mathematical Foundations for Post-Quantum Cryptography, Mathematics for Industry	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Yokoyama Kazuhiro	４．巻 -
２．論文標題 On factorization of parametric polynomials	５．発行年 2024年
３．雑誌名 Commentarii Mathematici Universitatis Sancti Pauli	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 青木 敏、野呂 正行	４．巻 53
２．論文標題 直積構造をもたない内側・外側配置	５．発行年 2023年
３．雑誌名 品質	６．最初と最後の頁 252～261
掲載論文のDOI（デジタルオブジェクト識別子） 10.20684/quality.53.4_252	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Aoki Satoshi, Noro masayuki	4．巻 -
2．論文標題 Use of indicator functions to enumerate cross-array designs without direct product structure	5．発行年 2024年
3．雑誌名 Algebraic Statistics	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Ito Takuma, Kobayashi Koutaro, Kurokawa Takashi, Shinohara Naoyuki, Uchiyama Shigenori	4．巻 15
2．論文標題 A technique to reduce memory usage of M4GB algorithm	5．発行年 2023年
3．雑誌名 JSIAM Letters	6．最初と最後の頁 125～128
掲載論文のDOI（デジタルオブジェクト識別子） 10.14495/jsiaml.15.125	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計19件（うち招待講演　1件／うち国際学会　6件）

1．発表者名 Sakata Kosuke, Kudo Momonari, Kato Taku, Kazuhiro Yokoyama
2．発表標題 Implementation report on computing Groebner bases over exterior algebra
3．学会等名 25th International Workshop on Computer Algebra in Scientific Computing（国際学会）
4．発表年 2022年

1．発表者名 Kazuhiro Yokoyama
2．発表標題 Implemention report on parametric factorization of multi-variate polynomials
3．学会等名 Application of Computer Algebra（国際学会）
4．発表年 2022年

１．発表者名
横山和弘

２．発表標題
多変数多項式のパラメトリック因数分解

３．学会等名
RIMS共同研究（公開型）「Computer Algebra -Foundation and Applications」

４．発表年
2022年

１．発表者名
野呂正行

２．発表標題
Signature based algorithm における F4 スタイルの簡約アルゴリズムの実装について

３．学会等名
RIMS共同研究（公開型）「Computer Algebra -Foundation and Applications」

４．発表年
2022年

１．発表者名
野呂正行

２．発表標題
Signature based algorithm における F_4 スタイルの簡約の実装（非斉次，有理数体上への拡張）

３．学会等名
Risa/Asir Conference 2022

４．発表年
2022年

１．発表者名
Kambe Yuta, Yasuda Masaya, Noro Masayuki, Yokoyama Kazuhiro, Aikawa Yusuke, Takashima Katsuyuki, Kudo Momonari

２．発表標題
Solving the constructive Deuring correspondence via the Kohel-Lauter-Petit-Tignol algorithm

３．学会等名
MathCrypt2021（国際学会）

４．発表年
2021年

１．発表者名
野呂正行

２．発表標題
non-compatible な加群項順序の元での signature based algorithm について

３．学会等名
RIMS共同研究（公開型）「Computer Algebra - Foundations and Applications」

４．発表年
2021年

１．発表者名
野呂正行

２．発表標題
Risa/Asir における種々の change of ordering algorithm の実装について

３．学会等名
Risa/Asir Conference 2022

４．発表年
2022年

１．発表者名
篠原直行

２．発表標題
国内外における耐量子計算機暗号の標準化動向

３．学会等名
2022年度電子情報通信学会総合大会（招待講演）

４．発表年
2022年

１．発表者名
伊藤琢真，黒川貴司，篠原直行，内山成憲

２．発表標題
F4-styleアルゴリズムのMQ問題に対する多項式選択方法

３．学会等名
2022 Symposium on Cryptography and Information Security

４．発表年
2022年

１．発表者名
Yokoyama Kazuhiro

２．発表標題
On the complexity of Groebner basis computation

３．学会等名
10th International Congress on Industrial and Applied Mathematics（国際学会）

４．発表年
2023年

１．発表者名
工藤桃成，横山和弘

２．発表標題
アフィン半正則な多項式系の定める Hilbert 級数と関連する Groebner 基底

３．学会等名
RIMS共同研究(公開型)「Computer Algebra-Foundations and Applications」

４．発表年
2023年

１．発表者名
工藤桃成，横山和弘

２．発表標題
半正則な非斉次多項式列に付随するHilbert級数とGroebner基底の計算量の評価

３．学会等名
日本応用数理学会・研究部会連合発表会「数論アルゴリズムとその応用」

４．発表年
2024年

１．発表者名
Kudo Momonari, Yokoyama Kazuhiro

２．発表標題
The solving degree for computing Groebner bases for affine semi-regular polynomial sequences

３．学会等名
MEGA 24 (Effective Methods in Algebraic Geometry, 2024)（国際学会）

４．発表年
2024年

１．発表者名
Noro Masayuki

２．発表標題
Signature-based algorithm and change of ordering for Groebner basis

３．学会等名
10th International Congress on Industrial and Applied Mathematics（国際学会）

４．発表年
2023年

１．発表者名
野呂正行

２．発表標題
Risa/Asir 2023-2024

３．学会等名
Risa/Asir Conference 2024

４．発表年
2024年

１．発表者名
伊藤 琢真、黒川 貴司、篠原 直行、内山成憲

２．発表標題
Groebner 基底計算における第二先頭単項式の有用性

３．学会等名
2024 Symposium on Cryptography and Information Security

４．発表年
2024年

１．発表者名
鈴木 俊博、伊藤 琢真、黒川 貴司、篠原 直行、内山成憲

２．発表標題
複合的な多項式選択法を用いたグレブナー基底計算によるMQ 問題の求解

３．学会等名
2024 Symposium on Cryptography and Information Security

４．発表年
2024年

１．発表者名 鈴木 俊博、伊藤 琢真、黒川 貴司、篠原 直行、内山成憲
２．発表標題 グレブナー基底計算を用いたMQ問題の解法におけ多項式選択の混合戦略について
３．学会等名 日本応用数理学会・研究部会連合発表会「数論アルゴリズムとその応用」
４．発表年 2024年

〔図書〕　計2件

１．著者名 高山 信毅、野呂 正行、小原 功任、藤本 光史、高山 信毅、濱田 龍義	４．発行年 2022年
２．出版社 共立出版	５．総ページ数 252
３．書名 数学ソフトウェアの作り方	

１．著者名 横山 和弘	４．発行年 2022年
２．出版社 朝倉書店	５．総ページ数 244
３．書名 多項式と計算機代数	

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	野呂　正行 (Noro Masayuki) (50332755)	立教大学・理学部・教授 (32686)	

６．研究組織（つづき）

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	篠原　直行 (Shinohara Naoyuki) (70565986)	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・室長 (82636)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関