科学研究費助成事業　　研究成果報告書

平成　２６　年　　５　月　２６　日現在

機関番号：　１４５０１
研究種目：　若手研究(B)
研究期間：　2010～2013
課題番号：　２２７０００１１

研究課題名（和文）実践的な問題に即した近似代数計算の確立と実用化

研究課題名（英文）Symbolic-Numeric Computations for Practical Situations

研究代表者
長坂　耕作（Nagasaka, Kosaku）

神戸大学・人間発達環境学研究科・准教授

研究者番号：７０３５９９０９

交付決定額（研究期間全体）：（直接経費）　　2,900,000円、（間接経費）　　870,000円

研究成果の概要（和文）：代数的な式の簡単化に用いられるグレブナ基底について，誤差を考慮した近似グレブナ基底の計算方法を，構造化をキーワードに開発し，理論的な背景のある近似グレブナ基底を計算可能とした。整数係数多項式の近似GCDアルゴリズムなど，より広範囲の多項式に対して近似代数演算を拡張した。特に，幅広く使用されているMapleに含まれる近似GCDアルゴリズムのQRGCDを拡張して，ExQRGCDアルゴリズムを提案した。これらの成果について，特定の数式処理システムではなく，ネイティブのアプリケーションから利用可能とするため，C言語による汎用ライブラリLIBSNAPの開発を行い，ウェブサイトにて公開した。

研究成果の概要（英文）：We proposed an algorithm for computing a structured Groebner basis approximately. With this algorithm, even if the input has some numerical error, we can compute their Groebner basis which are widely used for simplifying algebraic relations for example. For approximate polynomial GCD, we extended the concept to polynomials over integers and gave some special lattice to make it being compatible with multiple precision integers. Especially for the well known approximate polynomial GCD algorithm, QRGCD, we extended it with much theoretical considerations and proposed ExQRGCD algorithm. Moreover, for those results, to achieve that many people can use the results, we implemented them with C and published it on the website. The name of library is "LIBSNAP".

研究分野：　総合領域

科研費の分科・細目：　情報学・情報学基礎

キーワード：　アルゴリズム理論　数式処理

１．研究開始当初の背景

近似代数が提唱されてから約 20 年の間に，数多くの研究が行われているため，それぞれのアプローチにより，誤差の取扱い方法（近似の概念）が異なってきているものの，実数や複素数などの連続的に変化する数に対しては，誤差が十分小さければ妥当な結果を求められるようになってきている。しかしながら，誤差を含む代数制約の簡単化（近似 Groebner 基底）については，多くの研究成果が発表されているが実用化レベルに達していない。加えて，実践的な問題への応用を考えた場合，整数計画問題や組合せ最適化などと同じく，離散的に変化する整数に対しても同様の処理（離散的な誤差を離散的に扱えること）を行え得ることが望ましいが，これを可能とするアルゴリズムの研究は進んでいない。既存のアルゴリズムによる最適解は，整数計画問題や組合せ最適化などと同じく，もはや本来の問題である離散的な場合の最適解とはならない。また，これら近似代数の研究成果を社会に還元する，汎用形式のライブラリについては開発されていない。

２．研究の目的

本研究では，最終的な目的である「実践的な近似代数の機能を提供するパッケージやライブラリの開発」の実現のため，これを含む以下の 3 項目について，それぞれの取組目標を次のように定めた。

(1) 近似代数における誤差の概念の拡張
研究代表者は，離散的に変化する整数に対しても近似代数を適用可能とする萌芽的なアルゴリズムを提案していたが，その理論的な解明と更なる高速化を行う。また，同アルゴリズムの適用対象を広げるため，整数誤差を持つ整数係数多項式の近似因数分解などについても理論的な解明に取り組む。

(2) 実践的な機能の提供に不足するアルゴリズムの確立
数式を取り扱う上で代数的な制約条件を簡単化することは非常に重要であるが，誤差を含む代数制約の簡単化（近似 Groebner 基底）については，多くの研究成果が発表されているが実用化レベルに達していない。この問題に対して，研究代表者が近年再発見した新しいアプローチと，近年近似代数で活用されはじめた行列操作で，実用的なレベルのアルゴリズムを提供する。

(3) 実践的な近似代数の機能を提供するパッケージやライブラリの開発
多くの研究開発現場で利用可能とするため，C/C++などから容易に近似代数を利用可能なライブラリを実現する。これは，連続的な誤差に加えて離散的な誤差も扱える，近似代数の実践的な機能を持つライブラリとする。

３．研究の方法

研究目的を実現するための 3 つの取組目標のそれぞれに下記の方法で研究を行った。

(1) 近似代数における誤差の概念の拡張
整数誤差に対する萌芽的なアルゴリズムの理論的な解明と更なる高速化，整数誤差を持つ整数係数多項式の近似因数分解などについての理論的な解明，近似代数計算による数式の簡単化を人間らしく行うアルゴリズムの実現を検討する。

(2) 実践的な機能の提供に不足するアルゴリズムの確立
誤差を含む代数制約の簡単化への STLS の基本的な適用方法の確立，厳密な手法（CGS: 誤差をパラメータとして表現）と STLS による手法との関係を究明，RREF と STLS と組み合わせによる（収束性を考慮した）効率的なアルゴリズムの開発を推進する。

(3) 実践的な近似代数の機能を提供するパッケージやライブラリの開発
上記の研究成果を含む，C/C++などから容易に利用可能な数値数式融合計算の研究成果に関するライブラリを実装し，提供する。

４．研究成果

研究目的に記載の 3 つの取組目標ごとに，その研究成果を述べる。

(1) 近似代数における誤差の概念の拡張
格子算法による整数係数多項式の近似 GCD アルゴリズムを，最新の情報に基づいて修正したものが Journal of Symbolic Computation に掲載された。その成果を整数の近似 GCD アルゴリズムに応用し，準同型暗号との関連性を研究集会で発表した。準同型暗号はクラウドなどにおいて，秘匿すべき情報の処理を実現するために必要不可欠な暗号技術であり，その安全性が整数の近似 GCD に帰着されることがわかっている。本研究では，整数を基数の多項式として表現することで，多項式用のアルゴリズムが整数用にも利用できることを示した。その後，整数に拡張する段階で導入した特殊な整数格子が，多項式の近似 GCD アルゴリズムの誤差の取り扱いを改善することが判明したため，国際研究集会 SNC 2011 で発表した。具体的な研究成果は，多倍長整数などにおける配列毎の誤差への対応を可能にしたことである。これにより，暗号系の安全性にも関係する整数の無平方分解への拡張も試みており，その中間報告を 2011 年 12 月の京都大学数理解析研究所の研究集会で行った。また，近似代数における誤差の概念の拡張として進めている整数上の近似 GCD については，体上の最近特異行列問題に帰着することが出来ないため，関連する厳密な因数分解アルゴリズムである Berlekamp アルゴリズムについて近年のサーベイも実施した。

(2) 実践的な機能の提供に不足するアルゴリズムの確立

① 誤差を含む代数制約の簡単化を，研究代表者が提唱した構造化 Groebner 基底で実現しようとしている。本研究の開始時点では，構造化 Groebner 基底を計算するアルゴリズムの実現には至っていなかったが，研究集会での情報交換などに基づいて，定義に基づく基底の計算を行えるアルゴリズムを開発した。手法としては，厳密な Groebner 基底の高速計算アルゴリズムである F4 に基づいて，構造化 Groebner 基底に必要となる項集合の計算に特化させたものである。その成果は，ISSAC 2011 (International Symposium on Symbolic and Algebraic Computation)で発表している。なお，これら研究実績に基づくプログラムは，Mathematica 上に実装したものを，論文等に記載の URL からダウンロードすることで入手可能となっている。加えて，近似 Groebner 基底に関する招待講演を行ったことで得られたフィードバックから，後退誤差解析の研究が進んでいないものの非常に重要であることが判明した。萌芽的な方法については研究発表をしたが，今後の理論構築が望まれる段階である。なお，実践的な利用に不可欠と思われる近似 Groebner 基底については，2011 年度のフィードバックから後退誤差解析の研究を行い，数学的に今後研究が必要とされる理論などについてまとめたものを，2012 年 7 月，ISSAC2012 においてポスター報告を行っている。

② 実践的な近似代数の機能を提供するライブラリの開発に取り組んだ過程において実施した Maple の SNAP パッケージの調査で，使われている近似 GCD アルゴリズムの正当性と実際の実装に乖離があることを発見した。この実装はもっとも幅広く使われているものであり影響も多い。これを改善するアルゴリズム（ExQRGCD）を導き，その速報を，2012 年 12 月，京都大学数理解析研究所の研究集会で報告し，最終版を国際研究集会の CASC2013 にて発表した。内容としては，QRGCD において適切に取り扱われていなかった摂動量の評価を，より保守的に実施する枠組みを開発したものである。

(3) 実践的な近似代数の機能を提供するパッケージやライブラリの開発

実践的な近似代数の機能を提供するパッケージやライブラリの開発は，既存の SNAP パッケージの改良を行うことよりも，汎用ライブラリの提供を優先した研究推進を行った。2011 年 7 月と 2011 年 9 月に行った研究発表は，この試みの中間報告となっており，次年度以降の汎用ライブラリの設計と実装に先立つ調査や試験実装の結果について取り扱っている（7 月の発表では C++用に，9 月の発表では C 用に試験実装している）。ライブラリの実装については，様々なデータ構造や実装形式において実験を繰り返し行った。その結果に基づき，基本的なデータ構造を確定させ，2013 年 3 月よりウェブで公開を行っている。研究期間の途中においては，API の基本方針や基本データ構造のみの公開となっていたが，研究実施計画に基づき，多くの部分は最終年度に公開を実施した。なお，最終的に公開段階にあるのは，基礎的な多項式や行列の処理（倍精度や多倍長精度）に加えて，近似 GCD の多様なアルゴリズム（QRGCD，ExQRGCD，UVGCD）となっている。非公開版には，本研究推進上，実装した様々なもの（Fastgcd や，これらの改良版）もあるが，これらは今後に公開の予定である。

以上のことから，整数上の誤差への対応，理論的背景を有する近似 Groebner 基底の計算方法の確立，実践的な近似 GCD アルゴリズムの改良と（汎用ライブラリとしての）実装系の提供などが本研究の成果である。どの研究も今後の展開が期待されるが，より実践的なライブラリとするためには，QE などの産業界が必要としている技術を包括した，数値数式融合計算としての実践的なアプローチが求められると考えられる。

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 3 件）

① K. Nagasaka and T. Masui. Extended QRGCD Algorithm. Lecture Notes in Computer Science, Vol. 8136, 257-272. 2013. 査読有
DOI: 10.1007/978-3-319-02297-0_22

② K. Nagasaka. Approximate Polynomial GCD over Integers. Journal of Symbolic Computation, Vol. 46(12), 1306-1317. 2011. 査読有

③ K. Nagasaka. Computing a Structured Groebner Basis Approximately. Proc. International Symposium on Symbolic and Algebraic Computation 2011, 273-280. 2011. 査読有

〔学会発表〕（計 20 件）

① 長坂耕作. 近似 GCD アルゴリズムにおける枢軸選択の影響. RIMS 研究集会「数式処理とその周辺分野の研究」. 2013 年 12 月 25 日～27 日. 京都大学数理解析研究所.

② 長坂耕作. 厳密に与えられた系の Groebner 基底を数値的に求める場合に必要な桁精度の考察. 研究集会「数式処理研究と産学連携の新たな発展」. 2013 年 8 月 21 日～23 日. 九州大学マス・フォア・インダストリ研究所.

③ K. Nagasaka and T. Masui. Revisiting QRGCD and Comparison with ExQRGCD. ISSAC 2013 Poster

presentations. 2013年6月26日～29日. Boston, USA. 査読有

④ K. Nagasaka. Backward error analysis of approximate Groebner basis. ISSAC 2012 Poster presentations. 2012年7月22日～25日. Grenoble, France. 査読有

⑤ K. Nagasaka. A Symbolic-Numeric Approach to Groebner Basis with Inexact Input. Fields Institute Workshop on Hybrid Methodologies for Symbolic-Numeric Computation (Hybrid 2011). 2011年11月16日～19日. Waterloo, Canada. 招待講演

⑥ K. Nagasaka. An improvement in the lattice construction process of Approximate Polynomial GCD over Integers. Symbolic-Numeric Computation (SNC 2011). 2011月6月7日～9日. San Jose, USA. 査読有

⑦ 長坂耕作. 近似 Groebner 基底と SLRA. 第19回日本数式処理学会大会. 2010年6月 11 日～13 日. 名古屋大学ベンチャービジネスラボラトリ.

〔その他〕
ホームページ等
http://wwwmain.h.kobe-u.ac.jp/~nagasaka/research/snap/

６．研究組織

(1)研究代表者

長坂　耕作（NAGASAKA, Kosaku）
神戸大学・人間発達環境学研究科・准教授
研究者番号：７０３５９９０９