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　　元 年　　６ 月 １８ 日現在

機関番号：１２１０２
研究種目：基盤研究(C)（一般）
研究期間：2015～2018
課題番号：１５Ｋ００００５

研究課題名（和文）疎な多変数多項式・系に対する近似代数算法の開発と安定・効率化

研究課題名（英文）Development, stabilization and enhancement of approximate algebraic algorithms for sparse multivariate polynomials and systems

研究代表者

佐々木　建昭（Sasaki, Tateaki）

筑波大学・数理物質系（名誉教授）・名誉教授

研究者番号：８００８７４３６

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：拡張ヘンゼル構成(ＥＨＣ)を利用して、疎で主係数特異な多変数多項式のＧＣＤの効率的算法を開発するとともに、ＥＨＣ自体の効率化を目指した。ＥＨＣは互いに素な多変数多項式GとHから主変数を消去した終結式Sを分母因子とするので、Sを最小化することが望ましい。
最小なSはイデアル<G,H>の最小元であるので、イデアル<G,H>のグレブナー基底を用いてＥＨＣの定式化を行ったが、グレブナー基底の計算量は変数の個数について2重指数的で重い。そこで、計算が速い剰余列を工夫するうち、剰余列を余因子で正規化すればイデアルの最小元が得られることを発見し、定理化した。

研究成果の学術的意義や社会的意義
多変数多項式の因数分解とGCD計算については、蜜な多項式に関しては算法はほぼ完成の域に達しているが、疎な多項式で特に主係数が原点で０になるなどの特異なものに対しては、算法は効率化の余地が多くある。その中でも、拡張ヘンゼル構成法は本研究グループの発案であり、拡張ヘンゼル構成に基づく効率化は日本がやるべき仕事であろう。
多変数多項式の変数消去は古い研究テーマだが、旧来の多項式剰余列や終結式に基づく方法では消去結果が最小にならないことが大部分である。一方、グレブナー基底法は最小元を与えるが極めて遅い。したがって、イデアルの最小元を剰余列法で高速に計算する方法の発見は画期的だと思う。

研究成果の概要（英文）：We first developed an efficient algorithm for the GCD of sparse multivariate singular polynomials, by using the extended Hensel construction (EHC), then aimed at enhancing the EHC algorithm itself. The EHC is a power series in main variable with coefficients of rational functions in sub-variables, and it is critical to make the denominators small. The smallest denominator can be computed by the Groebner basis which is very heavy. So, we aimed at computing the smallest denominator by the polynomial remainder sequence (PRS) which is quite fast.
We found that, if we make the resultant obtained by PRS smallest by normalizing it with the cofactors, then the obtained resultant becomes equal to the smallest element of the Groebner basis, uo to a constant. This result is very useful in the practical computation, so we made this fact in a theorem.

研究分野：計算機代数と数式処理

キーワード：拡張ヘンゼル構成　疎で主係数特異な多変数多項式　多変数多項式系の変数消去　多変数多項式系の消去イデアル　多変数多項式イデアルの最低元　多変数多項式の剰余列　多項式剰余列と余因子

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

因数分解やＧＣＤ等の基本演算では、次数に飛びのない密多項式に関する算法はほぼ完成の域に達していたが、多変数多項式では従変数に０を代入したときに主係数や多項式そのものが０になる場合(これを特異な場合という)があり、まだまだ研究の余地が十分あった。たとえば、従来の算法では多変数用の一般ヘンゼル構成が多くの場面で用いられているが、特異な場合に対しては原点の位置を移動して非特異多項式に変換する必要がある。すると、疎な多項式では項数が爆発的に増加することが多く、計算時間が一気に増加するのである。さらに、浮動小数係数の多変数多項式では原点の位置を移動するだけで誤差が一気に拡大することも多々ある。

本研究代表者とその共同研究者は、従来の整数や有理数を係数とする数式に対する代数的演算を浮動小数や誤差を含む数係数を持つ数式に拡張する、いわゆる『近似代数』を提唱して、多項式の近似ＧＣＤや近似因数分解、近似グレブナー基底や近似特異系などの概念を提唱するとともに、それらの算法を考案・インプリメントしてきた。その延長として、ヘンゼル構成を特異な多項式にも原点移動なく適用できる拡張ヘンゼル構成を提案した。拡張ヘンゼル構成は主係数特異な多変数多項式に適用されて、大成功を収めるとともに、疎な多変数多項式に対しては、世界の主流である『疎多項式補間法』と並ぶ地位を占めるまでになった。しかし、研究は緒についたばかりで、近似グレブナー基底など多くの困難な課題がひしめいていた。

２．研究の目的

(1) 疎な多変数多項式の[厳密および近似]ＧＣＤ計算と因数分解に対して、本研究代表者らが考案し発展させた拡張ヘンゼル構成を用いた効率的算法を開発する。
(2) (疎な)多変数多項式系に対して、[厳密および近似]シジジー(線形従属関係)の効率的な算法を開発し、本研究代表者らが考案した近似グレブナー基底算法、悪条件連立代数方程式の良条件化、近似特異系の特異化法を安定化する。
(3) パラメータ係数の疎な線形微分方程式に対し、パラメータの最適値決定などに対する効率的算法を開発し、パラメータ係数の疎な微分代数方程式系への拡張を計る。
(4) 上記が当初の目的だったが、「拡張ヘンゼル構成での最小の分母因子の効率的決定」の研究で、最小分母因子が「互いに疎な２多変数多項式系の消去イデアルの最小元」であり、剰余列法で高速に計算できると判明したので、研究目的を『多変数多項式系の主変数消去における最小元を多項式剰余列で高速に計算する』との課題に変更した。

３．研究の方法

基本的には研究代表者が理論を展開して方向性を定め、共同研究者がアイデアを計算機に実装するものとするが、もちろん、各研究者の創意工夫を最大限尊重する。

理論の展開はとことん考え抜くことだが、具体的にプログラムを書いて例題をテストすることも理論の進展を大きく促す。そのため、研究代表者もプログラムを書く。

４．研究成果

(１)<u>拡張ヘンゼル構成による疎な多変数多項式のＧＣＤ算法の開発</u>：　拡張ヘンゼル構成による主係数特異な多変数多項式の因数分解は、2005 年に当時大学院生だった稲葉が計算機に実装し、当時主流の Wang-Rothschild 法に比べて圧倒的に優勢であることを実証した。一方、GCD の方は手つかずだった。その間、米国で考案された「疎多項式補間法」の研究が進展して、欧米ではその方法による特異多項式の因数分解や GCD の効率化が精力的に行われた。それらの算法と拡張ヘンゼル法による算法とを性能比較するため、稲葉のプログラムを参考に、讃岐が「拡張ヘンゼル法による主係数特異な多項式の GCD 算法」を実装し、カナダで開発された数式処理システム Maple と性能を比較した。その結果、拡張ヘンゼル法によるプログラムは Maple グループが実装したプログラム(当然ながら、プログラムは粋をこらして効率化されている)と比べて大差ない計算速度を出したが、数倍遅かった。

(２)<u>拡張ヘンゼル構成算法の効率化の研究</u>：　上記の実験結果は、本研究代表者らに拡張ヘンゼル構成算法の効率化を強く決意させた。実は、拡張ヘンゼル構成に関する研究は 10 年以上昔に算法を実装して以来、多変数代数関数の特異点とその近傍での拡張ヘンゼル級数の収束性の研究に精力を注ぎ、算法の効率化は行っていなかったのだ。まず、稲葉のプログラムを主変数に関して疎な多変数多項式に適用して驚いた。拡張ヘンゼル構成で得られるのは、従変数の有理式を係数とする主変数のべき級数だが、有理式の分母因子が必要な因子のべき乗になっており、稲葉は有理式を計算するたび GCD 演算で分子分母の簡約を行っていたのだ。稲葉はプログラムを数式処理システム Mathematica 上に実装したが、分母因子は Mathematica の終結式ルーチンで計算した。そこで、まず疎な多項式の終結式計算のため、「疎な多項式用の剰余列算法」を開発した(この算法は(1)に述べた讃岐のプログラムには組み込まれている)。すると分母因子が最小かどうか気になった。最小の終結式はグレブナー基底法で計算できるので、２多項式系のグレブナー基底で最小の分母因子を計算すると共に、有理式の簡約まで

グレブナー基底で定式化してみた。実は有理式の簡約はなかなか厄介な課題であり、種々の方法を試した結果、同一分母にそろえることが最も有用だと判明した。すると今度は、グレブナー基底計算の遅さが非常に気になった。よく知られていることだが、グレブナー基底の計算量は変数の個数について二重指数的で、変数の個数が増えると致命的になるのだ。この点は本研究代表者も当然気付いていたが、論文の査読者から嘲笑的に指摘される始末であった。

(３) 互いに素な２多変数多項式の消去イデアルの最小元を剰余列で高速に計算する算法：上記で述べたように、分母因子をグレブナー基底で計算することは致命的制約があり、別の手段で計算しなければならない。そこで、昔馴染みの剰余列法に戻ったが、昔に比べて多くの知見を得ている。まず、疎多項式用の剰余列算法を開発したことは上に述べた。疎多項式用の剰余列算法は、Loos が 1982 年に提唱したものの、彼は具体的算法を提示するに至らなかった。剰余列算法では、２番目以降の剰余に二つ以上前の剰余の主係数のべき乗が因子として入り込むので、それを除くことが必要だが、彼は部分終結式理論に代わる理論を提示できなかったのである。本研究代表者は、Hearn の「試し除算法」を用いることで、この課題をあっと言う間にクリアした。その方法で多くの終結式を(剰余列法で可能な限り小さく)計算するうちに気付いた：終結式がグレブナー基底で計算されるものと数係数を除いて一致するのだ。グレブナー基底法で得られる終結式は、数学的にいうと「互いに素な二つの多項式 G,H から主変数を消去した消去イデアルの最小元」である。一方、剰余列法は余因子も計算し、余因子の共通因子を除くよう規格化して、各剰余をイデアルの元としつつ最小化している。そこで、余因子を経由すれば剰余列法とグレブナー基底法で計算される終結式が一致することを証明できるのでは？、と証明に取り組んだ。余因子は、剰余列法ではある次数条件を満たして計算されるが、グレブナー基底法では次数条件が満たさないことが大部分である。しかし、次数条件を満たない余因子も H と G で割ると余りが従変数の多項式となった。すなわち、次数条件を満たす余因子に変換されたのである。この変換が可能なことは、与多項式 G と H の主係数が互いに素な場合は直ちに証明できるが、素でない場合は一筋縄ではいかない。だが、G と H の主係数の共通因子が余因子の主係数にどう入り込むかをみると、G と H が互いに素なので、剰余計算が進むたびにその共通因子は剰余の主係数から消えていき、代わりに余因子の主係数に移動するのである。主変数が消去された時点では、共通因子は全て余因子の主係数に移動する。このため、余因子で各項で H と G の次数以上の高次項は係数が H と G 主係数の倍数となり、H と G の次数低減が可能になるのである。すなわち、『剰余列の規格化により、剰余列法で計算される終結式と２多項式系のグレブナー基底法で計算される終結式は定数倍を除き一致する』との定理が得られた。

この定理は初等的で簡単ながら非常に有用な定理である。実際、従変数が３～６個の疎な多変数多項式の最小終結式の計算で、Mathematica(M)のグレブナー基底法と国産のシステム GAL(G)に実装した剰余列法で計算時間を比較したところ(単位はミリ秒)、３個では M:46.33，G:78.0、４個では M:12040，G:218、５個では M:>90 分，G:649、６個では M:>90 分，G:22040 だった。

(４) 多変数多項式の剰余列計算における中間式膨張を抑止する算法の開発：　上述のように剰余列法が非常に有用なことが判明したので、余勢をかって剰余列計算の徹底的な効率化に取り組んだ。剰余列算法は 1960～70 年代に部分終結式算法として(密多項式に対しては)完成したが、一度計算した剰余からその不要因子を除算で除去している。すなわち、中間式膨張を起こしている。この中間式膨張は大したことはないが効率を数倍落としており、算法開発者としてはそれすらも解決したい。本研究代表者は過去、このような問題に対してべき級数除算で解決してきた。今の場合も部分終結式理論が使えるならば、除多項式があらかじめ分るので、商となる多項式がギリギリ計算可能な限界の次数より上の項は捨てて被除多項式を計算し、商をべき級数除算で計算するのである。今の場合、部分終結式理論が使えず除多項式が分らないので、二つ前以前の剰余の主係数で試し割りしている。そこで、従変数に二桁程度の異なる素数を代入した「簡単系」で剰余列計算を試行して除多項式を推定し、その後で元の系の剰余列をべき級数除算で実行するのである。算法を上記のシステム GAL に実装して実験したところ、望み通りの性能が得られた。

５．主な発表論文等

〔雑誌論文〕（計１０件）

① 佐々木建昭, 稲葉大樹：疎な多変数多項式系の高速な変数消去法の探究. 査読無, 数理解析研究所講究録 2104 巻, 65-77 (2019), ISSN 1880-2818.

② Tateaki Sasaki: A Theory and an Algorithm for Computing Sparse Multivariate Polynomial Remainder Sequences. 査読有, Computer Algebra in Scientific Computing (CASC 2018); Springer LNCS 11077, 345-360 (2018). DOI: 10.1007/978-3-319-99639-4_24.

③ Tateaki Sasaki, Daiju Inaba: Simple Relation Between the Lowest-order Element of Ideal <G,H> and the Last Element of Polynomial Remainder Sequence. **査読有**, SYNASC 2017, IEEE Computer Society, 55-62 (2018). DOI: 10.1109/SYNASC2017.00019.

④ Tateaki Sasaki, Daiju Inaba: Various Enhancements for Extended Hensel Construction of Sparse Multivariate Polynomials. **査読有**, SYNASC 2016, IEEE Computer Society, 83-86 (2017). DOI: 10.1109/SYNASC.2016.025.

⑤ **佐々木建昭**, **稲葉大樹：疎な多変数多項式の拡張** Hensel **構成算法の再構築**. **査読無**, **数理解析研究所講究録** 2019 **巻**, 3-17 (2017). ISSN 1880-2818.

⑥ **佐々木建昭**:**浮動小数グレブナー基底の安定な算法を目指して**. **査読無**, **数理解析研究所講究録** 2054 **巻**, 42-54 (2017). ISSN 1880-2818.

⑦ **讃岐勝**, **稲葉大樹**, **佐々木建昭**:**拡張** Hensel **構成による近似** GCD **計算とその安定化**. **査読無**, **数理解析研究所講究録** 2019 **巻**, 28-38 (2017). ISSN 1880-2818.

⑧ **佐々木建昭**, **稲葉大樹：疎な多変数多項式の拡張** Hensel **構成の効率化**. **査読無**, **数理解析研究所講究録** 2054 **巻**, 55-67 (2017). ISSN 1880-2818.

⑨ Tateaki Sasaki, Daiju Inaba: Enhancing the Extended Hensel Construction by Using Groebner Bases. **査読有**, Computer Algebra in Scientific Computing (CASC 2016), Springer LNCS 9890, 457-472 (2016). DOI; 10.1007/978-3-319-45641-6.

⑩ Masaru Sanuki, Daiju Inaba, Tateaki Sasaki: Computation of GCD of Sparse Multivariate Polynomials by Extended Hensel Construction. **査読有**, SYNASC 2015, IEEE Computer Society, 34-41 (2016). DOI: 10.1109/SYNASC.2015.15.

〔**学会発表**〕(**計１５件**)

① Tateaki Sasaki: A Theory and an Algorithm for Computing Sparse Multivariate Polynomial Remainder Sequences. CASC 2018: 20th International Workshop on Computer Algebra in Scientific Computing, Sep. 17-21, 2018. Lille, France.

② **佐々木建昭**:**疎な多変数多項式の剰余列計算の新算法**. **第** 47 **回数値解析シンポジウム**, June 6-8, 2018, **福井県 あわら市**.

③ **佐々木建昭**, **稲葉大樹：疎な多変数多項式系の高速な変数消去法の探究**. RIMS **共同研究（公開型）**「Computer Algebra – Theory and Applications」, Dec. 20-22, 2017、**京都市**.

④ Tateaki Sasaki, Daiju Inaba: Simple Relation Between the Lowest-order Element of Ideal <G,H> and the Last Element of Polynomial Remainder Sequence. SYNASC 2017: 19th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, Sep. 21-24, 2017, Timisoara, Romania.

⑤ **佐々木建昭**, **稲葉大樹：イデアル**<G,H>**の最低元と剰余列の最終元の簡単な関係**. **第** 46 **回数値解析シンポジウム**, June 28-30, 2017, **滋賀県 高島市**.

⑥ Tateaki Sasaki, Daiju Inaba: Various Enhancements for Extended Hensel Construction of Sparse Multivariate Polynomials. SYNASC 2016: 18th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, Sep. 24-26, 2016, Timisoara, Romania.

⑦ Tateaki Sasaki, Daiju Inaba: Enhancing the Extended Hensel Construction by Using Groebner Bases. CASC 2016: 18th International Workshop on Computer Algebra in Scientific Computing, Sep. 19-23, 2016, Bucharest, Romania.

⑧ **佐々木建昭**, **稲葉大樹**:**疎な多変数多項式の拡張** Hensel **構成算法の再構築**. RIMS **共同研究（グループ型）「数式処理の新たな発展 –その最新研究と基礎理論の再構成」**, Sep. 7-9, 2016, **京都市**.

⑨ **讃岐勝**, **稲葉大樹**, **佐々木建昭**：**拡張** Hensel **構成による近似** GCD **計算とその安定化**. RIMS **共同研究（グループ型）「数式処理の新たな発展 –その最新研究と基礎理論の再構成」**, Sep. 7-9, 2016, **京都市**.

⑩ **佐々木建昭**, **稲葉大樹：拡張** Hensel **構成のグレブナー基底による効率化**. **第** 45 **回数値解析シンポジウム**, June 08-10, 2016, **鹿児島県 霧島市**.

⑪ **佐々木建昭**：**浮動小数グレブナー基底の安定な算法を目指して**. RIMS **研究集会「数式処理とその周辺分野の研究」**, Dec. 2-4, 2015, **京都市**.

⑫ **佐々木建昭**, **稲葉大樹：疎な多変数多項式の拡張** Hensel **構成の効率化**. RIMS **研究集会「数式処理とその周辺分野の研究」**, Dec. 2-4, 2015, **京都市**.

⑬ Masaru Sanuki, Daiju Inaba, Tateaki Sasaki: Computation of GCD of Sparse Multivariate Polynomials by Extended Hensel Construction. SYNASC 2015: 17th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, Sep. 22-24, 2015, Timisoara, Romania.

⑭ 讃岐勝, 稲葉大樹, 佐々木建昭：疎な多変数多項式の厳密/近似ＧＣＤ計算について. 第 44 回数値解析シンポジウム, June 08-10, 2015, 山梨県 甲州市.
⑮ 佐々木建昭：浮動小数グレブナー基底の安定的計算に向けて. 第 44 回数値解析シンポジウム, June 08-10, 2015, 山梨県 甲州市.

〔図書〕（計　０件）

〔産業財産権〕
○出願状況（計　０件）

○取得状況（計　０件）

〔その他〕
ホームページ等

６．研究組織

(1)研究分担者
研究分担者氏名：讃岐 勝
ローマ字氏名：Masaru Sanuki
所属研究機関名：筑波大学
部局名：医学医療系
職名：助教
研究者番号（8 桁）：40524880

(2)研究協力者
研究協力者氏名：
ローマ字氏名：