# 科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　２０　日現在

機関番号：　１４５０１
研究種目：　挑戦的萌芽研究
研究期間：　2011～2013
課題番号：　２３６５４０３５

研究課題名（和文）高い確率でグレブナー基底を高速に計算するアルゴリズムの開発

研究課題名（英文）Algorithm for efficiently computing a Groebner basis with high probability

研究代表者
野呂　正行（NORO, Masayuki）

神戸大学・理学（系）研究科（研究院）・教授

研究者番号：５０３３２７５５

交付決定額（研究期間全体）：（直接経費）　　1,900,000円、（間接経費）　　570,000円

研究成果の概要（和文）：有限体上のグレブナー基底を中国剰余定理により貼り合わせて有理数体上のグレブナー基底を計算する際に、全次数ごとにまとめて変換することで変換コストが下げられることを発見した。
入力イデアルが非斉次の場合にグレブナー基底候補がグレブナー基底であること示すために、有限体上での生成関係式を未定係数に置き換えて得た線形方程式を有理数体上で解くことにより生成関係式を計算する方法を考案し、実装した。巨大な方程式を有限体上でいったん解いた情報を用いて小さくすることで、解が一意となり、Hensel構成が適用でき、効率よい求解が可能になった。

研究成果の概要（英文）：We found that the cost of integer-rational number conversion in the procedure for computing Groebner bases over the rationals by combining modular Groebner bases by Chinese remainder theorem can be reduced by converting all the polynomials with the same degree together.
In order to show the correctness of a Groebner basis candidate, we developed an algorithm which computes an exact generating relation for each element in the candidate. We first compute a generating relation over a finite field. Then we replace the coefficients with variables to obtain a huge system of linear equations. By using the information obtained by solving the system over the finite field, we can reduce the size of the system and the solution is made unique. Then we can apply Hensel lifting for solving the system and we can efficiently solve the system.

研究分野：　数物系化学

科研費の分科・細目：　数学・数学一般（含確率論・統計数学）

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

グレブナー基底計算は近年急速に実用性を増してきているが、有理数体上の計算を厳密に行うと係数膨張などの困難を生じる。これを避けるために、必ずしも結果の正当性を保証しないが、多くの場合正しいグレブナー基底が得られるような実装を用いることは時として有効である。たとえば、イデアル分解計算など、候補による計算結果が別の方法でチェックできる場合には、グレブナー基底候補自身の正当性チェックは必ずしも必要ではなく、候補を高速に生成できることは、実用上重要である。一方で、数学的な定理の証明などにグレブナー基底を用いる場合、計算した結果がたしかに入力されたイデアルのグレブナー基底であることを保証する必要がある。しかし、広く用いられているソフトウェアである Maple, Magma などにおいては、その出力が単なるグレブナー基底候補であることを明示していない。このようなソフトウェアは本来数学的な事実の保証に使うことはできないが、知らずにそのような主張をしている論文も見受けられる。

## ２．研究の目的

(１)正当性を必ずしも保証しないが高速にグレブナー基底候補を計算できるアルゴリズムを開発する。さらに、研究代表者らが開発、公開している計算代数システム Risa/Asir 上に実装し、その内部を明らかにしたうえで公開する。それにより、ユーザはブラックボックス化されたプログラムを使わずに済み、数学的事実の検証のための厳密な実装と、実験のための確率的な実装をユーザの意思で使い分けることができる。

(2) 分散並列計算の応用可能性を検討、実装する。中国剰余定理を応用するグレブナー基底計算は自明に並列化できるが、実際に行ってみると、必ずしも台数効果が得られない場合が多い。これを克服するために、実装上の工夫を随所で行う。また、イデアル分解アルゴリズムは、得られた分解候補の正当性が、イデアルの交わりが元のイデアルと等しいことを示すことで保証できるため、必ずしも各ステップでのグレブナー基底の正当性が必要でない。この特性を生かして、新しいタイプの並列計算方法を模索する。

(3)得られたグレブナー基底候補が実際にグレブナー基底であることを効率よく示す方法を研究、実装する。本研究の最初の目的はグレブナー基底候補の高速生成であったが、その後に発表された、正当性の保証に対する誤った論文の定理の改良に関連して、正当性保証をモジュラー計算で行うという方向性が見えてきた。この方法を発展させて、新しいグレブナー基底候補の検証法を開発する。

## ３．研究の方法

(1) モジュラー計算の応用
有理数体上のグレブナー基底候補を計算する上で最も有効と考えられる方法は、有限体上のグレブナー基底を中国剰余定理により貼り合わせて、係数を有理数に引き戻す方法である。この方法について、真に効率的な方法を模索し、実装する。

(2) F4 アルゴリズム実装の効率化
グレブナー基底計算法として、現在最も有効と考えられる F4 アルゴリズムについて、Risa/Asir 上の実装をさらに効率化する。この実装中で、簡約計算など下位レベルの計算の効率化を行う。

(3)グレブナー基底候補の検証方法の開発
モジュラー計算で得たグレブナー基底候補が、入力イデアルのグレブナー基底であることを確認するための方法について研究し、Risa/Asir 上に実装する。

(4)並列計算の応用
すでに、Risa/Asir には OpenXM と呼ばれる分散並列計算を行うためのメカニズムが装備されている。有限体上の結果の貼り合わせをはじめとして、並列化可能な部分は多く存在するが、研究の進展に応じてさらに多くの部分に並列化を適用し、実時間での高速化を目指す。

## ４．研究成果

以下で述べる研究成果は、ごく最近のものを除いてすべて Risa/Asir に実装され、

http://www.math.kobe-u.ac.jp/OpenXM/

から入手可能である。

(1) モジュラー計算によるショートカット
ある有限体上での Buchberger あるいは F4 アルゴリズムの実行において必要になった S ペアのリストを用いて、その他の有限体上での実行の無駄を省く方法を実装した。

(2) 中国剰余定理の適用における最適化
有限体上のグレブナー基底を貼り合わせて有理数体上のグレブナー基底候補を求める際、整数有理数変換を行う必要があるが、この場合に、分母が推測できれば変換の手間が少なくてすむ。これまでは、すべての係数に対する操作を逐次的に行い、分母をインクリメンタルに更新していく方法だったが、多項式の全次数ごとに変換を行い、分母は全次数が変わるご

とにリセットする方法を考案した。これにより、変換の効率が格段に向上した．
表は、著名なベンチマーク問題である cyclic -9 のグレブナー基底候補生成を、ここで述べたリセットあり/なしで行った結果を示す。Worker 数は並列計算に用いたプロセッサの個数である。リセットありの計算は、プロセッサ数が少ないにも関わらず、実計算時間が大幅に短縮されていることがわかる。

| イデアル | リセット | worker 数 | 計算時間 | CRT | IR | 有限体の個数 |
|---|---|---|---|---|---|---|
| $\langle C_9\rangle$ | なし | 62 | $5.0\times10^4$ | $2.4\times10^4$ | $1.5\times10^4$ | 1736 |
| $\langle C_9\rangle$ | あり | 30 | $2.0\times10^4$ | 2400 | 740 | 450 |
| $\langle C_9^h\rangle$ | なし | 64 | $7.8\times10^4$ | $4.5\times10^4$ | $1.7\times10^4$ | 640 |
| $\langle C_9^h\rangle$ | あり | 54 | $2.9\times10^4$ | 9000 | 3000 | 486 |

(3)グレブナー基底候補の検証法の研究
横山和弘氏（立教大学）との共同研究により、非斉次のグレブナー基底候補の正当性が、有限体上でのある saturation 計算で得られる整数 k に対する斉次化変数のベキ t^k を、もとの生成系の斉次化に添加した生成系から計算するグレブナー基底から判定できることを示した。得られた定理は次の通りである。

定理 ($I\subset\langle G\rangle$ なる GB 候補 $G$ の検証)
$G$ が $I=\langle F\rangle$ の全次数付き順序 $\prec$ に関する $p$-GB 候補で $I\subset\langle G\rangle$, $G$ は $\langle G\rangle$ のグレブナー基底とする. 自然数 $k$ が $\langle\phi_p(F)^h\rangle : t^k = \langle\phi_p(F)^h\rangle : t^\infty$ を満たすとする. このとき, $p$ が $F^h\cup\{t^k\}$, $\prec^h$ ($\prec$ の斉次化) について, $p$ が $F^h\cup\{t^k\}$ のグレブナー基底の先頭係数を割らないならば, $I=\langle G\rangle$.

(4)グレブナー基底候補の生成係数の計算
(3)で述べた方法が適用できない場合に各グレブナー基底候補を入力多項式集合から生成する係数を計算することで直接示す方法を考案した。具体的には、有限体上の計算で得た、有限体上での生成係数の係数を未定係数に置き換えて得られる有理数体上の線形方程式系を解く。この際、いったん有限体上で解いてみることで、0にできる係数をすべて0にするという方法で、方程式のサイズを格段に小さくすることができる。また、解が一意化することで、有理数体上での求解に Hensel lifting を用いることができる。この方法により、数年来の懸案であった、物理学に由来するあるグレブナー基底候補の正当性検証に成功した。得られたアルゴリズムは以下の通りである。
このアルゴリズムにより、10 か月間計算しても計算が終了しなかった生成関係式の計算が１日半程度で終了するようになり、問題のグレブナー基底候補が実際にグレブナー基底であることを示すことができた。

**Algorithm 1** `generating_relation`$(F,G,g)$

Input : $F=\{f_1,\dots,f_m\}, G\subset\mathbb{Z}[X]$ s.t. $G$ is a $F$ の $p$-GB 候補, $F\subset\langle G\rangle$, $g\in G$
Output : $g=h_1f_1+\cdots+h_mf_m$ を満たす $h_1,\dots,h_m\subset\mathbb{Q}[X]$, または **failure**
$G_p=\phi_p(G)\leftarrow\langle\phi_p(F)\rangle$ の簡約グレブナー基底
$(H_1,\dots,H_m)\leftarrow H_i=\sum_j a_{ij}t_{ij}$ s.t.
$\phi_p(g)=H_1\phi_p(f_1)+\cdots+H_m\phi_p(f_m)$
$(i=1,\dots,m,\ a_{ij}\in\mathbb{F}_p,\ t_{ij}$ は単項式)
$E\leftarrow(\sum_j c_{1j}t_{1j})f_1+\cdots+(\sum_j c_{lj}t_{mj})f_m-g$
($c_{ij}$ は未定係数)
$E$ を $E=\sum_{i=1}^{k}e_it_i$ と表す ($t_i$ は単項式, $e_i$ は $c_{ij}$ の一次式)
$Z\leftarrow e_1=\cdots=e_k=0$ の $\mathbb{F}_p$ 上の解において, 自由変数に関する, 定数項を持たない一次式で表される変数
$\bar{E}\leftarrow(\sum_{j,c_{1j}\notin Z}c_{1j}t_{ij})f_1+\cdots+(\sum_{j,c_{mj}\notin Z}c_{mj}t_{ij})f_m-g$
$\bar{E}$ を $\bar{E}=\sum_{i=1}^{k}\bar{e}_is_i$ と表す ($s_i$ は単項式, $\bar{e}_i$ は $c_{ij}\notin Z$ の一次式)
**if** $\bar{e}_1=\cdots=\bar{e}_l=0$ が解 $c_{ij}=b_{ij}$ を $\mathbb{Q}$ 上で持つ **then**
return $(\sum_{j,c_{1j}\notin Z}b_{1j}t_{ij},\dots,\sum_{j,c_{mj}\notin Z}b_{mj}t_{ij})$
**else**
return **failure**
**end if**

(5)並列計算の応用
グレブナー基底の正当性検証においては、与えられた多項式集合が、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を示す必要がある場合が生じる。この計算は、多数の多項式の、この多項式集合による剰余がすべて０であることを示す計算で、明らかに並列化できる。この計算を並列化して台数効果が得られることが示せた。例として、斉次化 cyclic-9 のグレブナー基底候補のチェックを 1CPU で行うと４か月程度かかるが、これを２６CPU で 10 日程度で行うことができた。また、整数計算ライブラリ GMP を導入することで、各剰余計算も数倍程度高速化した。たとえば、ベンチマーク問題 McKay のグレブナー基底計算は１CPU で 360 秒から 100 秒へ、ilias13 は 600 秒から 250 秒へそれぞれ短縮された。

## 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３件）


① 野呂正行、横山和弘、グレブナー基底候補の正当性検証について、数理解析研究所講究録、査読無、1843, 2013, pp.38-50.
② M. Noro, Implementation of a primary decomposition package, T. Hibi, Ed., Harmony of Groebner Bases and the Modern Industrial Society, 査読有, 2012, pp.213-227.
③ T. Kawazoe, M. Noro, Algorithms for computing a primary ideal decomposition without producing intermediate redundant components, J. Symb. Comp., 査読有,6, 2011, pp.1158-1172, DOI:10.1016/j.jsc.2011.06.001

〔学会発表〕（計７件）

① 野呂正行、グレブナー基底計算、検証および並列化、Risa/Asir Conference2014, 2014 年 3 月 6 日、神戸大学瀧川記念学術交流会館
② 野呂正行、横山和弘、グレブナー基底候補の高速生成法とその検証について、RIMS 研究集会「数式処理とその周辺分野の研究」、2013 年 12 月 26 日、数理解析研究所
③ 野呂正行、matrix 1F1 が対角領域で満たす微分方程式系について、Risa/Asir Conference 2013, 2013 年 3 月 17 日、神戸大学理学部
④ 野呂正行, Modular 計算の応用によるイデアル諸演算の計算法と検証法について、計算による数理科学の展開 2013, 2012 年 12 月 27 日、神戸大学理学部
⑤ 野呂正行、横山和弘、グレブナー基底候補の正当性検証について、CALLING 2012, 2012 年 12 月 27 日、数理解析研究所.
⑥ M. Noro, Primary decomposition of polynomial ideals and its efficient implementation, SCA2012, 招待講演, 2012 年 5 月 18 日, RWTH Aachen, Germany.
⑦ 野呂正行、数式処理の理論概説、第２０回日本数式処理学会大会、招待講演、2011 年 9 月 10 日、神戸大学理学部

〔図書〕（計 3 件）

① M. Noro et al., Groebner Bases – Statistics and Software Systems, Springer, 2013, 474 (107-164)
② 野呂正行他、応用数理ハンドブック、朝倉書店、2013,704 (332-335)
③ 野呂正行他、グレブナー道場、共立出版、2011, 557 (213-227)

〔産業財産権〕

○出願状況（計　0　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　0　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://www.math.kobe-u.ac.jp/OpenXM/

６．研究組織

(1)研究代表者

野呂　正行　（NORO, Masayuki）
神戸大学・大学院理学研究科・教授
研究者番号：50332755

(2)研究分担者

（　　）

研究者番号：

(3)連携研究者

（　　）

研究者番号：