科学研究費助成事業　　研究成果報告書

平成　２６　年　　４　月　１７　日現在

機関番号：１７１０２
研究種目：若手研究(B)
研究期間：2012～2013
課題番号：２４７０００１４

研究課題名（和文）グレブナー基底の構造と分解

研究課題名（英文）Interpolation and structure of Groebner bases

研究代表者
Ｄａｈａｎ　Ｘａｖｉｅｒ（Dahan, Xavier）

九州大学・システム情報科学研究科（研究院・研究員

研究者番号：５０５６７５１８

交付決定額（研究期間全体）：（直接経費）　　1,700,000円、（間接経費）　　510,000円

研究成果の概要（和文）：多変数多項式系を用いていろいろな物理学的な現象を記述でき、この方程式系の高率的な求解は基礎的な位置を占めている。辞書式順序グレブナー基底（lex Gbで略記）はこの目的を達成するために主流な方法である。残念ながら、この辞書式順序によるグレブナー基底を計算するのは一番難しいである。
本研究計画の目的は、lex Gbの構造を一層把握することで、高速なアルゴリズムへの進歩を与えることである。新しい補間式を設置した後、lex Gbの構造が簡単にわかった。その構造を生かして、lex Gbの分解に対して新しい高率なアルゴリズムを提案した。それで、より小さい方程式が出力されることから、より高速に求解できる。

研究成果の概要（英文）：Systems of multivariate polynomial equations allow to describe a variety of physical phenomenon and solving them efficiently is thus a fundamental problem. Lexicographic Groebner bases (later on "lex Gb") are the mainstream tool to achieve this task. The particular lexicographic order is unfortunately the most difficult order to compute Groebner bases. The aim of this project was to grasp furthermore the structure of these lex Gb and to open the way to new improvements for their computation. After having set up new interpolation formulas, we could easily deduce the structure and obtain the first upper bounds on the bit-size of their coefficients.
Then, from the structure we have understood how to set up a new efficient decomposition algorithm of lex Gb, in order to get smaller and thus easier to solve polynomial systems. Moreover, with Prof. Yokoyama (Rikkyo University) we found out how to derive a new efficient algorithm to remove multiple solutions.

研究分野：数式処理

科研費の分科・細目：情報学・情報学基礎

キーワード：グレブナー基底　補間式　ビット長の見積もり　多変数多項式　三角形方

１．　　研究開始当初の背景

(1) 辞書式順序グレブナー基底（次に lex Gb で略記）は多変数多項式連立法手式の救解の主流な主流である。Lex Gb に対する先行研究が、lex Gb の構造を含めていろいろ存在していた。だが、lex Gb の補間方式はまだ簡明でおらず、構造から結果を得るために不十分な状況であった。

(2) 不十分の例外としては、2 変数の lex Gb の場合、構造も補間式も完全に理解されていた。3 変数の場合、補間式を設置でき、本研究のきっかけであった。その時点、期待できる結果のすべてを代数的に得られるか、あるいは根の集合の幾何を利用するか、不明であった。

(3)　lex Gb の「分解」アルゴリズムに関しては、1992 年に一つが発表された。一方任意の lex Gb を扱うことができ、一方重いグレブナー基底のルーチンに基づいている。上記の 3 変数に対する予備研究によると、ずいぶんより速い多項式の割り算だけを利用するアルゴリズムが存在する可能性がわかった。ということは、進歩の余地がたくさんある状況であった。

２．　　研究の目的

(1)まず、より明確な lex Gb の「構造」を紹介してから、それに依存している新たな lex Gb の「分解」アルゴリズムを設定するという主要な目的である。

(2) その構造と身近な関係がある補間式も明らかにし、自分の先行論文の工夫を適用して明確な（ある程度）lex Gb のビット長の上界を計算することを計画した。

(3)　その後、lex Gb の一般化としての block order という単項式順序によるグレブナー基底に上記の構造と補間式に適用することを計画した。このような順序によるグレブナー基底は、パラメータを含む多変数多項式系を適切に扱うことができるから重要である。

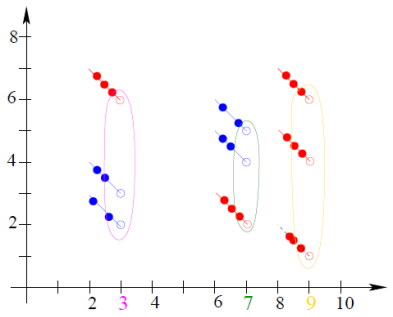
３．　　研究の方法

(1) 応募の時点には、主要な lex Gb の構造を 2 変数の lex Gb 同様に代数的に得ると考えたが、実際に重複根がある場合に、特別な構造が表示されない反例を見つけた。応募の「研究実施目的」に掲載した方法（代数的に）と違い、「研究が当初計画どおりに進まない時の対応」に掲載した方法(補間式、根の集合の幾何を用いて)により進んだ。目的に影響が概ねおらず、結果の範囲は重複根なしの lex Gb(次に、radical lex Gb で略記)に制限されることになった。

(2)　主要な補間式から、「研究計画・方法」に説明した通りに進んだ：構造、係数のビット長に対する上界、分解アルゴリズムの設定などを設置した。

４．研究成果

(1) radical lex Gb に対する簡明な補間式と構造を得た。
(発表①、関連論文は投稿中。図 1 を参照)



$$f=(x_1-9)\left[(x_2-2)\left((x_3-\bullet)(x_3-\bullet)\frac{x_2-5}{6-5}+(x_3-\bullet)(x_3-\bullet)\frac{x_2-6}{5-6}\right)\frac{x_1-3}{7-3}\right.$$
$$\left.+(x_2-6)\left((x_3-\bullet)(x_3-\bullet)\frac{x_2-2}{3-2}+(x_3-\bullet)(x_3-\bullet)\frac{x_2-3}{2-3}\right)\frac{x_1-7}{3-7}\right]$$

図 1：補間式の例(3 変数)

(2) lex Gb を計算する際に、係数のビット長が増大し、メモリ不足となる恐れがあり、入力された多変数多項式連立方程式のパラメータから、出力される lex Gb の係数に対するビット長の上界を計算した。入出される方程式系の変数の個数を n、最大の次数 d、最大の係数のビット長を h とすれば、出力される lex Gb の係数は最大

$$O(n\ h\ d^{2n})$$

ビット長がある。この上界は、被約グレブナー基底に適用されず、補間式から自然に推定される特殊な lex Gb のみに適用される。実際によく使われている被約グレブナー基底に対する上界を計算するのはより複雑であり、記載するのも難しいである。
（表③、関連論文を大分完成した）。

(3) lex Gb を分解するアルゴリズムに関しては、明らかにした構造を生かすことで、多項式割り算だけを利用する初の lex Gb 分解ゴリズムを設定した。分解された部分は、幾つかのより小さい lex Gb を成し、その幾つかの方程式の解からなる集合を計算するために、より効率である。先行研究はグレブナー基底のルーチンに基づいているから、計算量を見積もりにくいのに対して、提案したアルゴリズムの計算量を以下通りに大まかに見積もることができた：

$$O(n\ s^2\ d^2)、$$

ただし、変数の個数を n、最大の次数 d、lex Gb にある多項式の個数を s とする。
(発表②、④、関連論文は準備中。図２を参照)。

(4)本研究計画の「２.研究目的（３）」の一般化については、実際、この目的を達成するのに 2 年間は短かった。なぜならば、応募の時に想定していたエフォート 70%は楽観的過ぎ、実際に 2012 年１１月から、教育などで 20%程度に減少した。

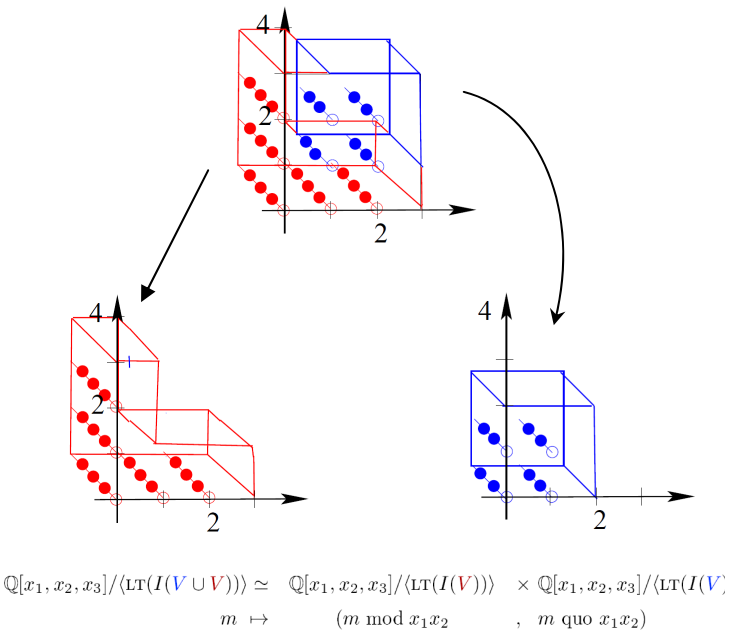


図 2: 根の集合の分解の例(3 変数)とその数式

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 1 件）
(1) DAHAN Xavier、Regular graphs of large girth and arbitrary degree. To appear in Combinatorica.

〔学会発表〕（計 6 件）
① DAHAN Xavier、On the structure of lexicographic Groebner bases in dimension zero. ISSAC 2012 ポスターセッション, Grenoble, France.
② DAHAN Xavier、Gcd-based decomposition algorithm of lexicographic Groebner bases. Workshop on Solving multivariate polynomial systems and related topics, 福岡、2013 年 3 月 2 日。
③ DAHAN Xavier、Application of height theory to some modular algorithm in Symbolic Computation. FORUM “Math-for-Industry”、福岡、2012 年 10 月 22 日.
④ DAHAN Xavier、最大公多項式に基づく辞書式順序のグレブナー基底の分解アルゴリズム。Risa/Asir conference 2013、2013 年 3 月 17 日。神戸大学。
⑤ DAHAN Xavier、Computation of eigenvalues of Cayley graphs and applications. The 16th Korea-Japan workshop on algorithms and computations. Suwon、Korea。2013 年 7 月 12 日。
⑥ DAHAN Xavier、Attacks on the ECDLP using Groebner bases.IMI 共同研究、安全・安心社会基盤構造のための代数構造、福岡 2013 年 8 月 27 日。

〔図書〕（計 0 件）

〔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://itslab.inf.kyushu-u.ac.jp/~dahan/index_j.html

６．研究組織
(1)研究代表者
ダハングザヴィエ（DAHAN XAVIER）
九州大学システム情報科学研究院
特任助教
研究者番号：50567518

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者

(　　)

研究者番号：