パラメータを伴ったGröbner基底の構造的な検出について

— Comprehensive structural Gröbner basis detection —

所属専攻　人間環境学専攻
学籍番号　208D418D
学 生 氏 名　大島谷 遼
指導教員氏名　長坂 耕作 准教授

計算機代数の分野において重要な計算の 1 つに Gröbner 基底の計算がある．Gröbner 基底の計算は Buchberger アルゴリズム [Buc06] に代表されるように，イデアルと項順序を指定して，一定の条件を満たすようなイデアルの基底を求めるものである．F_4 アルゴリズム [Fau99] など他の多くのアルゴリズムでも，Buchberger アルゴリズムの系譜が受け継がれており，基本的なアルゴリズムの考え方は変わっていない．

一方で，以下の例のように，与えられた多項式集合 F がある項順序においてそのままイデアル $\langle F \rangle$ の Gröbner 基底となっているような場合が存在する．

例.
以下の多項式集合 F は，$z \succ y \succ x$ の全次数辞書式順序及び全次数逆辞書式順序においてイデアル $I = \langle F \rangle$ の Gröbner 基底となっている．

$$F = \left\{ 2xy + yz,\ x^2 + y + z \right\} \subset \mathbb{C}[x, y, z]$$

このように，直接 Gröbner 基底の計算をする前に，計算対象である F 自身がそのまま Gröbner 基底となっているような項順序を求めることができれば，項順序を指定しない Gröbner 基底が必要な場面では有効な計算方法であることが考えられる．また，仮に一定の項順序が必要な場面でも，FGLM アルゴリズム [FGLM93] や Gröbner walk[CKM93] などに代表される change of ordering のアルゴリズムを活用することによって，有用な計算手段となることが考えられる．

例えば，連立代数方程式の求解のための計算では，多くの場合で辞書式順序（一般的には消去順序）での Gröbner 基底が必要となるが，辞書式順序での計算は遅くなることが知られており，入力の多項式集合の大きさによっては莫大な時間がかかってしまう可能性も否定できない．そこで，多項式集合がそのまま Gröbner 基底となっているような項順序が存在していれば，その項順序を求めたあとに change of ordering により辞書式順序の Gröbner 基底を求めることができる．これらの 2 つの計算の計算量が，元々行おうとしていた計算の計算量に比べて少なくなっているのであれば，この計算は有用な計算であったと言える．

このように「そのまま Gröbner 基底である」ような項順序を検出する問題は，Sturmfels らによって解かれた既知の問題であり，*Gröbner basis detection*[GS93] や *Structural Gröbner basis detection*[SW97] という名前が付けられている．

一方で，パラメータを伴った多項式環において，場合分けされたパラメータ空間と，それぞれに対応する Gröbner 基底を組にしたものを**包括的 *Gröbner* 基底系** [Wei92] と呼ぶ．包括的 Gröbner 基底系は，Gröbner 基底計算の中で，S-polynomial の計算が行われる際にパラメータの付いた係数が 0 か否かで場合分けを行い，項を確定させながら Gröbner 基底の計算を行っている．

これら 2 つの議論を踏まえ，本論文では，(Structural) Gröbner basis detection において，問題の設定をパラメータを伴った多項式環へと拡張し，それに付随して発見された定理についても取り上げる．まず第 1 章では，Sturmfels らとは違ったアプローチから，Structural Gröbner basis detection の問題を捉え，そこで新たに発見された定理を紹介する．次に，第 2 章では，Gröbner basis detection と Structural Gröbner basis detection について，既に知られている部分について述べる．第 3 章では，これらの問題をパラメータを伴っ

た多項式環へと拡張するために，パラメータ空間を分割するためのアルゴリズムの直接的な方法を紹介する．最後に，第 4 章では，パラメータ空間の分割を効率化するための議論を行い，最終的なアルゴリズムを完成させる．

第 1 章

はじめに

1.1　背景

多項式集合 F が与えられ Gröbner 基底の計算を行う際，Buchberger アルゴリズムなどによりイデアルと項順序を固定し，Gröbner 基底を得るための計算を行うのが一般的である．しかし，計算を行う前に F がそのまま Gröbner 基底であるような項順序を得ることができれば，従来の計算を行わずに Gröbner 基底を得ることができる．また，ここで得た項順序を change of ordering のアルゴリズムによって変換することで，任意の項順序での Gröbner 基底を得ることも可能である．

定理 1.1.1 (Gröbner 基底 [Buc06, theorem1]).
Gröbner 基底 $F = f_1, f_2$

第 2 章

第 3 章

第 4 章

参考文献

[Buc06] Bruno Buchberger. Bruno buchberger’s phd thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of symbolic computation*, 41(3-4):475–511, 2006.

[CKM93] Stephane Collart, Michael Kalkbrener, and Daniel Mall. The gröbner walk. *Dept. of Math., Swiss Federal Inst. of Tech*, 8092, 1993.

[Fau99] Jean-Charles Faugere. A new efficient algorithm for computing gröbner bases (f4). *Journal of pure and applied algebra*, 139(1-3):61–88, 1999.

[FGLM93] Jean-Charles Faugere, Patrizia Gianni, Daniel Lazard, and Teo Mora. Efficient computation of zero-dimensional gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.

[GS93] Peter Gritzmann and Bernd Sturmfels. Minkowski addition of polytopes: computational complexity and applications to gröbner bases. *SIAM Journal on Discrete Mathematics*, 6(2):246–269, 1993.

[SW97] Bernd Sturmfels and Markus Wiegelmann. Structural gröbner basis detection. *Applicable Algebra in Engineering, Communication and Computing*, 8(4):257–263, 1997.

[Wei92] Volker Weispfenning. Comprehensive gröbner bases. *Journal of Symbolic Computation*, 14(1):1–29, 1992.