非可換多項式の因数分解について

6K−3

森 和好　　飯田 三郎
(豊橋技術科学大学 情報工学系)

1 はじめに

最近，数式処理システムの利用が盛んになりつつあり，それにともない数式処理システムは数多くの機能を有するようになった．なかでも因数分解の機能は，数学の理論を適用して多くの改良・発展がなされている．しかしそれらのデータ領域は，ほとんどのシステムにおいてユークリッド整域に属しており，その領域の算法では乗法について非可換な多項式の因数分解を行うことができない．最近Mora[1] らより乗法に関して非可換な多項式の算法についての研究がなされ始めている．一方，Cohn[2] らによる，乗法に関して非可換な多項式の研究もなされたが，因数分解の算法については未だなされていなかった．そこで著者らは，乗法について非可換な多項式(以下，非可換多項式と呼ぶ)を因数分解する算法について考察した．

本稿では，(1)非可換多項式が斉次である場合は，因数分解の一意性，およびその因数分解の算法について，(2)非斉次の場合は，非可換多項式の因数分解の数が高々有限個であること，および非可換多項式の因数分解を多変数連立方程式および単変数可換多項式の整数解の求解に帰着させることができることについて，報告する．

2 準備

非可換多項式(non-commutative polynomial)とは，乗法に関する交換法則の成り立たない多項式を指す．つまり変数u，vについて，$u\cdot v = v\cdot u$が成立しない．非可換多項式は，文字列多項式(string polynomial)あるいは自由結合代数(free associative algebra)とも呼ばれることがある[3]．本稿では，係数としては整数を考える．

非可換多項式と可換多項式との主な違いは次の通りである:

- 可換多項式は一意分解整域に属するが，非可換多項式は一意分解整域には属さず因数分解の結果が複数個有り得る．
- 一意分解整域に属さないことにより，可換多項式の因数分解に用いられるZassenhausらの方法[4]あるいはLenstraらの方法[5]のモジュラアルゴリズムを用いることができない．
- 可換多項式のように除算ができない．つまり非可換多項式の因子の試験でも可換多項式と同様に除算をすることにより確かめることができない．

3 斉次非可換多項式の因数分解

斉次非可換多項式の場合，因子の性質から次の定理が得られる．

[定理1] 斉次非可換多項式の因数分解は一意的である． □

さらに，これにより斉次因数分解ができることが明らかとなる．

4 非可換多項式の因数分解

一般に非可換多項式については，次の定理が得られる．

[定理2] 非可換多項式の因数分解の数は高々有限個である． □

一方，Gröbner基底を用いることにより解が有限個数である多変数連立方程式系は，単変数可換多項式に帰着して解くことができることが知られている[6]．係数を不定元とする連立方程式系を構成した際に，解が有理数の単元について不定であるのでこれを固定する必要があるが，非可換多項式の最高次数の単項式の和は斉次非可換多項式をなすことから因数分解することができる．したがって因数分解された因子の最高次数の単項式は既知とすることができ固定できるならば，2つの因子の項の係数を不定元とする連立方程式系を構成し，それをGröbner基底を用いて単変数可換多項式に帰着し，その整数解を求めることにより非可換多項式を2つの因子に分解することができる．これを既約因子になるまで繰り返すことにより因数分解ができる．

しかし最高次数の単項式の和の係数のg.c.d.が1以外のときには，与えられた非可換多項式の最高次数の因子を一意に定めることができない．そこで最高次数の因子を既知とするために，与えられた非可換多項式の最高次数の単項式の係数のg.c.d.の値($=g$)を非可換多項式に乗じ，2つの因子の最高次数の単項式の係数のg.c.d.の値ともgとなるようにし，因数分解終了後，gを除くこととした．このようにすることにより連立方程式系を構成することにより因数分解ができることが明らかとなった．

5 まとめ

- これまでの結果をもとに，非可換多項式の因数分解の算法をREDUCE 3.3を用いてインプリメントした．REDUCE 3.3では，あらかじめGröbner基底を算出する機能を追加することができる．いくつかの因数分解の実行時間を表1に示す．表1より4次から5次程度の場合には，因数分解が数秒によりできることが判明した．
- このように非可換多項式を因数分解する算法を与えることにより，変数が行列等を指している場合でも因数分解が可能であるという新しい環境が得られ，数式処理システムの扱うことのできる対象を拡大させることができた．しかし，現状では算法の計算量は次数に対して指数的であり，今後の改善が望まれる．

表1 実行時間 (SONY NWS-831,BUG Staff LISP)

非可換多項式	実行時間
$45(u-2v)(u+1)(uu-u+1)(su-12vs)$	9617ms
$(3uw+2)(2uv-2u+121)(23w+125)$	8499ms
$(uvv+29u+v+2)(7uv+3u-5v+2)$	8916ms
$(uv+29u+v+2)(7uv+3u-5v+2)$	2816ms
$(3u+1)(v-7)(w+1)(x+1)$	4350ms
$(3uv+2)uv = u(3vu+2)v = uv(3uv+2)$	1183ms

参考文献
[1] Mora,T., Groebner Bases in Non-Commutative Algebras, *LNCS#358 ISSAC '88*, Springer-Verlag, 150-161(1989)
[2] Cohn,P.M., Free Associate Algebras, *Bull. London Math. Soc.*,1-39(1969).
[3] Knuth,D.E., *The Art of Computer Programming,Seminumerical Algorithms(2nd ed.)*, Addison-Wesley,1981
[4] Zassenhaus,H. et al., A New Algorithm for Factoring Polynomials Over Finite Fields, *Math.Comp.*, Vol.36, No.154, pp. 587-592(1981)
[5] Lenstra,A.K. et al., Factoring Polynomials with Rational Coefficients, *Math.Ann.*, 261, pp.515-534(1982)
[6] Davenport,J.H. et al., *Computer Algebra*, Academic Press(1988)

On the Factorization of Non-Commutative Polynomials
Kazuyoshi Mori (mori@kiku.tutics.tut.ac.jp), Saburou Iida (iida@kiku.tutics.tut.ac.jp)
Toyohashi University of Technology