数理解析研究所講究録
1038巻 1998年 40-48

Von Neumann regular ring 上の多項式環におけるグレブナー基底について

佐藤洋祐
立命館大学理工学部情報学科
ysato@theory.cs.ritsumei.ac.jp

1. はじめに

筆者らは、ブール環上の多項式環において、独特の M-reduction を用いることでグレブナー基底が計算できることを証明した ([S 88,S 90]) が、ほぼ同時期に V. Weispfenning によっても同様の研究がされていた ([W 89]). 彼の研究においても、基本的なアイデアである、M-reduction はわれわれのものと全く同じものが使われている. ただ、彼の仕事は、ブール環よりもより一般的な Von Neumann regular ring (簡単に言うと、体の直積が成す環) 上で理論を構築している点ですぐれている. [S 90] で筆者らは、ブール環上の多項式環においては、既約グレブナー基底以外にもグレブナー基底のある種の標準形が存在することを示した. この標準形は [S 95,Sa 96,Sb 96,S 97] 等における筆者らの研究に利用されている. 最近、筆者はわれわれのこの標準形が、一般の Von Neumann regular ring においても拡張できることを示した ([S 9?]). 今回の発表では、Von Neumann regular ring 上の多項式環におけるグレブナー基底について、われわれの仕事も含めて紹介する. 2節の定理は、[SW 75] からの引用である. 3節の定理は [W 89] からの引用 (かなり解り易い表現に変えてある) であるが、基本的には、[S 88, S 90] でわれわれも同様の結果を得ている. 4節の内容はわれわれのオリジナルである. 尚、定理の証明を述べるとかなり長くなってしまうので、結果のみを記述した.

2. Von Neumann regular ring

単位元をもつ可換環 R が以下の性質を持つとき、これを Von Neumann regular ring とよぶ.

$$\forall a \in R\, \exists b \in R\, a^2 b = a$$

この b にたいして、ab と ab^2 はユニークに定まるが、これをそれぞれ a^*、a^{-1} で表す. これにたいして、$aa^* = a$ 、$aa^{-1} = a^*$ および $(a^*)^2 = a^*$ がなりたつ.

すべての Von Neumann regular ring は体の直積の成す環の部分環と同型になることが以下のようにして示される.

定義 2.1
$\{x \in R | x^2 = x\}$ の要素 a、b にたいして、$\neg a = 1 - a$、$a \wedge b = ab$ で $\neg$ と $\wedge$ を定めると、$(\{x \in R | x^2 = x\}, \neg, \wedge)$ はブール代数になるが、これを $B(R)$ で表す.

$B(R)$ をブール環とみなして、ストーンの表現定理を用いると、
B から $\prod_{I \in St(B(R))} B(R)/I$ の中への同型写像 Φ が $\Phi(x) = \prod_{I \in St(B(R))} [x]_I$ で得られる.
ここで、$St(B(R))$ は $B(R)$ の極大イデアル全体の集合を表す.
この表現は、以下のように R の表現へと拡張される.

定理 2.1
$B(R)$ の極大イデアル I にたいして、$I_R = \{xy | x \in R, y \in I\}$ と定めると、I_R は R の極大イデアルになり、$\Phi(x) = \prod_{I \in St(B(R))} [x]_{I_R}$ で R から $\prod_{I \in St(B(R))} R/I_R$ の中への写像 Φ を定めると、Φ は同型写像になる.

3. グレブナー基底

Von Neumann regular ring R は、一般にネーター環にはならないが、R 上の多項式環の有限生成イデアルを扱う場合は、R の部分環でネーター環になるものの中で考えることができるので、そのグレブナー基底は存在する.しかしながら、R はそれが体でない場合には整域にすらならないので、[Mo 88] 等の方法はグレブナー基底の計算には利用できない.しかしながら、R 上の多項式環では以下で定義する特別のモノミアルリダクションを利用して、Buchberger のアルゴリズムによってグレブナー基底を計算することができる.

以下では、単項を表す記号としてギリシャ文字 α、β、γ 等を、R の要素を表す記号として a、b、c 等を、多項式を表す記号として f、g、h 等を用いる. また、単項上のアドミシブル順序を 1 つ固定し、これによる f の最大の単項を $lt(f)$、その係数を $lc(f)$、最大の単項式すなわち $lc(f)lt(f)$ を $lm(f)$ 、$f - lm(f)$ を $rm(f)$ で表す.

定義 3.1
多項式 $f = a\alpha + g$(ただし $lm(f) = a\alpha$) にたいして、f によるモノミアルリダクション $\rightarrow_f$ を以下で定義する.

$$b\alpha\beta + h \rightarrow_f b\alpha\beta + h - ba^{-1}\beta(a\alpha + g) \ \text{(ただし、} ab \neq 0\text{)}$$

例 3.1

$R = \mathbf{Q}^2$ とし、$a = (2,0)$、$b = (3,2)$ とする. $ab = (6,0) \neq 0$、$a^{-1} = (1/2,0)$ なので
$(3,2)\alpha\beta + h \rightarrow_f (3,2)\alpha\beta + h - (3,2)(1/2,0)\beta((2,0)\alpha + g) = (0,2)\alpha\beta + h - (3/2,0)\beta g$

a^{-1} は a の各成分の内、0 でないものだけを、逆数にしたものに他ならない.したがって、

モノミアルリダクションは、0 でない成分にたいして普通の体上の多項式環におけるモノミアルリダクションをおこなうことに他ならない. また、a^* は a の各成分の内、0 でないものを 1 で置き換えたものである.

このモノミアルリダクションによってグレブナー基底を計算することができるのであるが、体上の多項式環における Buchberger のアルゴリズムをそのまま適用したのではうまくいかない. 体上の多項式環においては、多項式の集合 F によるモノミアルリダクション $\rightarrow_F$ の対称・推移閉包 $\overset{*}{\leftrightarrow}_F$ による同値関係とイデアル (F) による同値関係が一致するが、Von Neumann regular ring 上の多項式環においては、一般には一致しない.

例 3.2
上の例の R による多項式環 $R[X]$ において、$F = \{(1,0)X + (0,1)\}$ と置くと、$(0,1) = (0,1)((1,0)X + (0,1))$ なので、$(0,1) \equiv 0 \bmod(F)$. しかるに、$(0,1) \overset{*}{\leftrightarrow}_F 0$ は成り立たない.

しかしながら、F の要素がある性質をもつとき、この同値関係は一致する.

定義 3.2
多項式 f が、$(lc(f))^*f = f$ をみたすとき、f はブール閉であるという. $(lc(f))^*f$ を f のブール閉包とよび、$bc(f)$ で表す.(注意 任意の多項式のブール閉包はブール閉である.)

定理 3.1
F をブール閉な多項式の集合とすると、$\overset{*}{\leftrightarrow}_F$ による同値関係とイデアル (F) による同値関係は一致する.

$lm(f) = lm(bc(f))$ なので、多項式の任意の有限集合 F にたいして、$(F) = (H)$ をみたすブール閉な多項式の有限集合 H を計算することができる. H は一意には定まらないが、このような H の一つを $bc(F)$ で表すことにする.

グレブナー基底の定義には、いろいろな方法があるが、上のモノミアルリダクションによって以下のように定義する.

定義 3.3
多項式の有限集合 G が以下の条件をみたすとき、G はグレブナー基底であるとよばれる.
・ $\overset{*}{\leftrightarrow}_G$ による同値関係とイデアル (G) による同値関係が一致する.
・ $\rightarrow_G$ はこの同値関係の完備化システムである. すなわち、任意の多項式 f、g にたいして、$f \equiv g \Longleftrightarrow f\downarrow_G = g\downarrow_G$.

定義 3.4
多項式 $f = a\alpha\gamma + f'$、$g = b\beta\gamma + g'$ (ただし $lm(f) = a\alpha\gamma$、$lm(g) = b\beta\gamma$、$GCD(\alpha,\beta) = 1$) にたいし、$b\beta f - a\alpha g = b\beta f' - a\alpha g'$ を f と g の S-多項式とよび、$SP(f,g)$ で表す.

体上の多項式環と同様に、S-多項式を用いてグレブナー基底を述べることができる.

定理 3.2
ブール閉な多項式の有限集合 G にたいして、
G がグレブナー基底である $\Longleftrightarrow$ G の任意の多項式 f、g にたいして、$SP(f,g) \xrightarrow{*}_G 0$
(G の多項式がブール閉であることが重要である. 一般の多項式の集合にたいしては、この定理は成り立たない.)

この定理によって、与えられた多項式の有限集合 F にたいして、ブール閉包の計算とS-多項式の計算を順々に繰り返すことによって、$(F) = (G)$ をみたすブール閉な多項式を要素とするグレブナー基底 G を計算することができる.

以下にグレブナー基底に関する重要な性質を述べる.

定義 3.5
$lc(f) = (lc(f))^*$ をみたす多項式、すなわち、$lc(f)$ の 0 でない各成分が 1 になるとき、f はモニックであるとよばれる.

任意の多項式 f にたいし、$lc(f)^{-1}f$ はモニックであり、f がブール閉であるとき、
$(f) = (lc(f)^{-1}f)$ が成り立つ.

例 3.3
例 3.1 の多項式環のブール閉な多項式 $f = (2,0)X+(3,0)$ にたいして、$lc(f)^{-1}f = (1,0)X+(3/2,0)$ となる. また、$lc(f)^{-1}f = (1/2,0)f$、$(2,0)lc(f)^{-1}f = f$ なので $(f) = (lc(f)^{-1}f)$

定義 3.6
グレブナー基底 G にたいし、G の任意の要素 f が自分以外の G の要素によるモノミアルリダクションによって書き換えられないとき、G を既約グレブナー基底とよぶ.

定理 3.3
G を既約グレブナー基底とするとき、G のすべての要素はブール閉な多項式である.

定義 3.7
既約グレブナー基底 G が、
・ G の任意の要素はモニックな多項式である
・ G の二つの要素で、最大単項が一致するものはない
をみたすとき、これを正規グレブナー基底とよぶ.

定理 3.4
正規グレブナー基底はユニークに定まる. すなわち、$(G) = (G')$ なる正規グレブナー基底 G と G' は一致しなければならない.

例 3.4
$G = \{(1,0)X + (2,0), (0,1)X + (0,2)\}$ は既約グレブナー基底であるが、正規ではない. これと (イデアルとして) 同じ正規なグレブナー基底は $\{(1,1)X + (2,2)\}$ である.

R を体 K_i、$i \in S$ の 直積 $\prod_{i \in S} K_i$ の部分環とする. R 上の多項式 f にたいし、f のすべての係数 r を $r(i)$ で置き換えて得られる K_i 上の多項式を f_i で表す. R 上の多項式の集合 F にたいしても、$\{f_i | f \in F\}$ を F_i で表す.

定理 3.5
ブール閉な多項式の集合 G にたいして、以下の条件は同値になる.
・ G は既約グレブナー基底である.
・ S の各要素 i にたいして、G_i は既約グレブナー基底である.

例 3.5
$R = \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5 \times \mathbf{Z}_7 \times \mathbf{Z}_{11} \times \mathbf{Z}_{13}$ とする.
$R[X, Y]$ において、

$$\begin{cases} XY + (1,2,0,5,5,5)X + (1,2,1,4,0,11) \\ XY^2 + (1,1,2,0,7,7)X + (1,1,3,6,2,0) \end{cases}$$

の正規グレブナー基底を求めると、

$$\begin{cases} (1,1,0,0,1,1)XY + (1,2,0,0,5,5)X + (1,2,0,0,0,11) \\ (1,1,0,0,1,1)X^2 + (1,1,0,0,0,10)X + (1,1,0,0,3,9)Y + (1,1,0,0,4,0) \\ (1,1,1,0,1,1)Y^2 + (1,1,0,0,0,6)X + (0,0,4,0,10,5)Y + (0,0,3,0,3,8) \\ (0,0,1,0,0,0)X + (0,0,3,0,0,0)Y + (0,0,2,0,0,0) \\ (0,0,0,1,0,0) \end{cases}$$

となる.

4. 最適グレブナー基底

一般に、体上の多項式環においては、グレブナー基底の標準形は正規グレブナー基底によってのみ与えられる. 定理 3.4 により、Von Neumann regular ring 上の多項式環でも、正規グレブナー基底によってグレブナー基底の標準形が与えられるが、これ以外にも、グレブナー基底の標準形が存在する.

定義 4.1
ブール閉でモニックな多項式からなるグレブナー基底 G が以下の性質をみたすとき、最適グレブナー基底とよばれる.
・ G の任意の要素 f にたいして、$rm(f)$ は $\rightarrow_G$ によって書き換えられない.
・ G の二つの要素で、最大単項が一致するものはない・
・ G の任意の要素 f と g にたいし、もし $lt(f) | lt(g)$、すなわち $lt(g)$ が $lt(f)$ で割り切れるなら、$lc(g)lc(f) = lc(f)$ でなければならない.

定理 4.1
最適グレブナー基底はユニークに定まる. すなわち、$(G) = (G')$ なる最適グレブナー基底 G と G' は一致しなければならない.

“最適グレブナー基底” という名前は、リダクションを最適におこなうという理由で用いた.

例 4.1
$R = \mathbf{Q}^3$ とし、$R[X]$ の正規グレブナー基底

$$G = \begin{cases} (1,0,0)X^3 \\ (0,1,0)X^2 \\ (0,0,1)X \end{cases}$$

によって、$X^3 \rightarrow_{(1,0,0)X^3} (0,1,1)X^3 \rightarrow_{(0,1,0)X^2} (0,0,1)X^3 \rightarrow_{(0,0,1)X} 0$ となるが、これの最適グレブナー基底

$$G' = \begin{cases} X^3 \\ (0,1,1)X^2 \\ (0,0,1)X \end{cases}$$

を用いると、$X^3 \rightarrow_{X^3} 0$ がただちに得られる.

グレブナー基底は等式問題の解の標準形としてもしばしば使われるが、ある種の制約問題においても、最適グレブナー基底は有効である.
次の例は [S 95] における集合制約のある問題にたいする解の標準形を最適グレブナー基底と正規グレブナー基底で求めたものである.

例 4.2
最適グレブナー基底による標準形

```
x8*x9 = 0
x7*x9 = 0
x7*x8 = 0
x6*x9 = 0
x6*x8 = 0
x6*x7 = 0
x4*x7 = 0
x4*x6 = 0
x3*x7 = 0
x3*x6 = 0
x3*x4 = 0
x2*x9 = 0
x2*x8 = 0
x2*x7 = 0
x2*x6 = 0
x2*x4 = 0
x2*x3 = 0
x1*x9 = 0
x1*x8 = 0
x1*x7 = 0
x1*x6 = 0
x1*x4 = 0
x1*x3 = 0
x1*x2 = 0
```

```
[s10,s2,s7,s8,s9]*x9 = 0
[s10,s2,s7,s8,s9]*x8 = 0
[s10,s7,s8,s9]*x7 = 0
[s10,s7,s8,s9]*x6 = 0
[s2*x5] = [s2]
[s1,s2,s3,s6,s7,s8]*x4 = 0
[s1,s2,s3,s6,s7,s8]*x3 = 0
[s1,s2,s3,s4,s5,s6]*x2 = 0
[s1,s2,s3,s4,s5,s6]*x1 =0
```

正規グレブナー基底による標準形

```
~[s10,s2,s7,s8,s9]*x8*x9 = 0
~[s10,s2,s7,s8,s9]*x7*x9 = 0
~[s10,s2,s7,s8,s9]*x7*x8 = 0
~[s10,s2,s7,s8,s9]*x6*x9 = 0
~[s10,s2,s7,s8,s9]*x6*x8 = 0
~[s10,s7,s8,s9]*x6*x7 = 0
~[s1,s10,s2,s3,s6,s7,s8,s9]*x4*x7 = 0
~[s1,s10,s2,s3,s6,s7,s8,s9]*x4*x6 = 0
~[s1,s10,s2,s3,s6,s7,s8,s9]*x3*x7 = 0
~[s1,s10,s2,s3,s6,s7,s8,s9]*x3*x6 = 0
~[s1,s2,s3,s6,s7,s8]*x3*x4 = 0
~[s1,s10,s2,s3,s4,s5,s6,s7,s8,s9]*x2*x9 = 0
~[s1,s10,s2,s3,s4,s5,s6,s7,s8,s9]*x2*x8 = 0
~[s1,s10,s2,s3,s4,s5,s6,s7,s8,s9]*x2*x7 = 0
~[s1,s10,s2,s3,s4,s5,s6,s7,s8,s9]*x2*x6 = 0
~[s1,s2,s3,s4,s5,s6,s7,s8]*x2*x4 = 0
~[s1,s2,s3,s4,s5,s6,s7,s8]*x2*x3 = 0
~[s1,s10,s2,s3,s4,s5,s6,s7,s8,s9]*x1*x9 = 0
~[s1,s10,s2,s3,s4,s5,s6,s7,s8,s9]*x1*x8 = 0
~[s1,s10,s2,s3,s4,s5,s6,s7,s8,s9]*x1*x7 = 0
~[s1,s10,s2,s3,s4,s5,s6,s7,s8,s9]*x1*x6 = 0
~[s1,s2,s3,s4,s5,s6,s7,s8]*x1*x4 = 0
~[s1,s2,s3,s4,s5,s6,s7,s8]*x1*x3 = 0
~[s1,s2,s3,s4,s5,s6]*x1*x2 = 0
[s10,s2,s7,s8,s9]*x9 = 0
[s10,s2,s7,s8,s9]*x8 = 0
[s10,s7,s8,s9]*x7 = 0
[s10,s7,s8,s9]*x6 = 0
[s2]*x5 = [s2]
[s1,s2,s3,s6,s7,s8]*x4 = 0
[s1,s2,s3,s6,s7,s8]*x3 = 0
[s1,s2,s3,s4,s5,s6]*x2 = 0
[s1,s2,s3,s4,s5,s6]*x1 = 0
```

5. おわりに

定理 3.5 によって、Von Neumann regular ring 上の多項式環におけるグレブナー基底

は、各成分の体上のグレブナー基底を計算して求めることができる. Von Neumann regular ring の直積としての次元が、使用できる計算機の個数にたいして小さい場合は、並列計算によって、より高速に求めることができる.
例えば、例 3.5 の正規グレブナー基底は、

$$\begin{cases} XY + 5X + 11 \\ XY^2 + 7X + 13 \end{cases}$$

の $\mathbf{Z}_2[X,Y]$、$\mathbf{Z}_3[X,Y]$、$\mathbf{Z}_5[X,Y]$、$\mathbf{Z}_7[X,Y]$、$\mathbf{Z}_{11}[X,Y]$、$\mathbf{Z}_{13}[X,Y]$ における、それぞれのモジュラーグレブナー基底を、6 台の計算機を用いて並列計算すれば、より高速に求められる.
しかしながら、直積としての次元が、使用できる計算機の個数よりもはるかに大きい場合は、われわれの方法が有効である. 使用できる計算機の個数に応じて、直積を適当に分割することによって、より最適の並列計算も可能になる.
Von Neumann regular ring の構造が、体の直積として容易に表現できる場合は、このような計算も可能になるが、一般には体の直積表現が容易に得られるとは限らない. [S 95] の comprehensive ブーリアングレブナー基底の計算に現れるブール環を直積として表現するのは、できないことはないが大変複雑 (パラメーターの変数の個数 n にたいして、2^n 個の直積として表現される) になるので、実用的ではない.

参 考 文 献

[B 65] Buchberger, B. (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal. PhD thesis, Universität Innsbruck.

[B 85] Buchberger, B. (1985). Gröbner bases: An algorithmic method in polynomial ideal theory, chap 6 in Recent Trends in Multidimentional System Theory, N. K. Bose Ed., Reidel Publ. Comp.

[Mo 88] Möller, H.M. (1988). On the Construction of Gröbner Bases Using Syzygies *J.Symbol.Comput.* **6**, 345–359.

[S 88] Sakai, K., Sato, Y. (1988). Boolean Gröbner bases. Proceeding of LA-Symposium in winter, RIMS, Kyoto Univ., 29–40

[S 90] Sakai, K., Sato, Y., Menju, S. (1990). Boolean Gröbner bases(revised). ICOT Technical Report 613.

[S 95] Sato, Y. (1995). Set Constraint Solver (a free software developed as a Research Funding Program of AITEC, Research Institute For Advanced Information Technology). ftp://ftp.icot.or.jp/ifs/contract-reserarch/95/DH7-13/H7-13.tgz.

[Sa 96] Sato, Y. (1996). Application of Groebner basis in constraint of non-numerical domains. presented in The 2nd IMACS Conference on Applications of Computer Algebra.

[Sb 96] Sato, Y. (1996). Nonstandard Canonical Forms of Set Constraints. presented in Second International Conference on Principles and Practice of Constraint Programming Set Constraints Workshop.

[S 97] Sato, Y. (1997). Set Constraint Solver - Groebner bases for non-numerical domains -. International Symposium on Symbolic and Algebraic Computation(ISSAC 97), Poster Abstracts pp 13-14.

[S 9?] Sato, Y. (199?). New type of a canonical Gröbner basis in polynomial rings over commutative Von Neumann regular rings. in preparation.

[SW 75] Saracino, D., Weispfenning, V. (1975). On algebraic curves over commutative regular rings, Model Theory and Algebra, a memorial tribute to A.Robinson, Springer LNM vol 498, pp 307-387.

[W 89] Weispfenning, V. (1989). Gröbner bases in polynomial ideals over commutative regular rings, EUROCAL '87, J.H. Davenport Ed., Springer LNCS Vol 378, 336–347.