数理解析研究所講究録
1085 巻 1999 年 34-41

Von Neumann regular ring 上の多項式環の Gröbner bases の応用 - 特別な場合の comprehensive Gröbner bases -

立命館大学理工学部 佐藤洋祐 (Yosuke SATO) *

1 はじめに

Commutative Von Neumann regular ring 上の多項式環における Gröbner bases は [W 89] で提案され、[S 93] や [Sa 98,Sb 98] 等でより詳細な研究がされている．しかしながら、そこで扱われた commutative Von Neumann regular ring の例は、ブール環や体の直積のなす環等の非常に単純な構造のものに限られていた．本論文では、もう少し複雑な例を紹介する．これを用いることによって、非常に制限された形ではあるが、一般の体上の comprehensive Gröbner bases の容易な計算が可能になる．

2 Commutative Von Neumann regular ring

以下の性質を持つ単位元をもつ可換環 R は commutative Von Neumann regular ring とよばれる．

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

このような環は体の直積のなす環の部分環に同型になることが知られており ([SW 75])、その構造から自然に定義されるモノミアルリダクションによって、この環上の多項式環における Gröbner bases が計算できる ([W 89, Sa 98, Sb 98]).

Commutative Von Neumann regular ring の idempotent な要素全体のなすブール環が、直積構造を決定する際に重要な役割を果たすが、idempotent な要素は環の拡大に関しても、以下に述べる重要な性質を有する．

*ysato@theory.cs.ritsumei.ac.jp

定理 1 R を *commutative Von Neumann regular ring* とするとき、剰余環 $R[X]/(X^2-X)$ もまた *commutative Von Neumann regular ring* になる.

証明 $aX+b$ $(a,b\in R)$ を $R[X]/(X^2-X)$ の任意の要素とする. R は commutative Von Neumann regular ring なので、$(a+b)^2c=a+b$、 $b^2d=b$ をみたす R の要素 c 、d が存在する. $f\in R[X]/(X^2-X)$ を $f=(c-d)X+d$ とおくと、$(aX+b)^2f=aX+b$ がなりたつ. ∎

この定理により、commutative Von Neumann regular ring のそれほど自明ではない例が得られたが、実は、これによりある種の comprehensive Gröbner bases(非常に制限された場合に限定されるが) の計算が可能になる.

定理 2 $H=R[X_1,X_2,\ldots,X_n]/(X_1^2-X_1,X_2^2-X_2,\ldots,X_n^2-X_n)$ とおくと、上の定理により H は *commutative Von Neumann regular ring* になるが、この環上の多項式環における *Gröbner bases* に関して次がなりたつ.
$H[Y_1,Y_2,\ldots,Y_m]$ の多項式 f にたいし、R の *idempotent* な要素 $a_1,a_2,\ldots,a_n$ をそれぞれ $X_1,X_2,\ldots,X_n$ に代入して得られた $R[Y_1,Y_2,\ldots,Y_m]$ の多項式を $f(a_1,a_2,\ldots,a_n)$ で表す. $H[Y_1,Y_2,\ldots,Y_m]$ の多項式の集合 F にたいしても

$$F(a_1,a_2,\ldots,a_n)=\{f(a_1,a_2,\ldots,a_n)|f\in F\}$$

と定義する.
G を $H[Y_1,Y_2,\ldots,Y_m]$ におけるイデアル I の *Gröbner basis* とするとき、

(1) $G(a_1,a_2,\ldots,a_n)$ は $R[Y_1,Y_2,\ldots,Y_m]$ におけるイデアル $I(a_1,a_2,\ldots,a_n)$ の *Gröbner basis* になる.

さらに任意の多項式 $f\in H[Y_1,Y_2,\ldots,Y_m]$ と R の *idempotent* な要素 $a_1,a_2,\ldots,a_n$ にたいして、

(2) $f\downarrow_G(a_1,a_2,\ldots,a_n)=f(a_1,a_2,\ldots,a_n)\downarrow_{G(a_1,a_2,\ldots,a_n)}$ がなりたつ.

G が $X_1,X_2,\ldots,X_n$ をパラメーターとする *comprehensive Gröbner basis* である. ただし、代入できる値は *idempotent* なものに限られる.

3 計算例

われわれは定理 2.2 の R として有理数体の場合の G を計算するプログラムを作成した. 以下にその計算例をいくつか紹介する.

使用言語は、多倍長整数がサポートされていて研究用としては非常に使いがってがよいSICStus Prolog を用いた. `neumann_gb(F,P)` の F に多項式のリスト、P には、パラメーターとする変数のリストを入力する. 次の例では、多項式環 $(Q[a,b]/(a^2-a,b^2-b))[x,y]$ におけるイデアル $(x*y^2+a*x+1, x^2*y+b*y+1)$ の 既約 Gröbner basis を計算している. 最初の数 6 は計算された S-多項式の数、次の数 0 は冗長であることが検知され計算せずにすんだ S-多項式の数 (0 ということは、この例では無かったということになるが)、最後の数 3 は計算されたブール閉包の数である.

例 1

```
?- neumann_gb([x*y^2 + a*x + 1, x^2*y + b*y + 1],[a,b]).

a*b*x^2*y + a*b*y + a*b
((1 - a) + a*b)*x^3 - a*b*x*y + a*b*x^2 + (1 - a)*b*y + b*x
        + ((1 - a) + a*b)
(a + (1 - a)*b)*y^2 + (- a + a*b)*x*y - a*b*x^2 + b*y - b*x + (a - a*b)
(1 - a)*b*x*y + (- 1 + a)*b*x^2 + (- 1 + a)*b
(a - a*b)*x^2 + (- a + a*b)*y + (a - a*b)*x
((1 - a) + (- 1 + a)*b)*y + ((- 1 + a) + (1 - a)*b)*x

6    s-polynomials are created
0    s-polynomials are detected to be redundant
3    boolean closures are created
```

例 2

```
?- neumann_gb([a*x^2*y*z + 4*b*x*y^2 - c*z^2*y*w - 5*d + 5,
               x*y*z - a*x*w - b*3*y - 5*d,
               x*y*z^2 - a + 3*b - z*w,
               x*y*z*w*a - c*x + d],
               [a,b,c,d]).

a*b*c*d*w^3*y + 2*a*b*c*d*w^2*y + 64/99*a*b*c*d*w^3 + 5/3*a*b*c*d*z^2
+ 5*a*b*c*d*y*z + 227/33*a*b*c*d*y^2 - 1/3*a*b*c*d*x*z
- 872/297*a*b*c*d*x*y + 326/297*a*b*c*d*x^2 - 887/198*a*b*c*d*w*z
- 223/66*a*b*c*d*w*y + 2902/297*a*b*c*d*w*x + 283/99*a*b*c*d*w^2
+ 604/99*a*b*c*d*z + 3467/99*a*b*c*d*y - 628/297*a*b*c*d*x
```

```
- 1099/198*a*b*c*d*w + 2293/54*a*b*c*d
          .
          .
       途中略
          .
          .
(a*b + (a - 2*a*b)*c*d)*z^2 + (3*a*b*c - 3*a*b*c*d)*y*z
+ (8/3*a*b*c - 8/3*a*b*c*d)*x*y + (4/3*a*b*c - 4/3*a*b*c*d)*x^2
+ (- a*b*c + (- 15/8*a + 23/8*a*b)*c*d)*w*z
+ (- 1/40*a + 1/40*a*b)*c*d*w*x + (9/200*a - 9/200*a*b)*c*d*w^2
+ (- 5*a*b*c + (2171034/6401333*a*b
   + (217/40*a - 195664021/256053320*a*b)*c)*d)*z
+ (- 152272/376549*a*b + (- 1/325*a + 49864949/122378425*a*b)*c)*d*y
+ ((16/45*a*b + 14/45*a*b*c) + (- 89701808/288059985*a*b
    + (- 5517/2600*a + 264629532809/149791192200*a*b)*c)*d)*x
+ (- 797944/6401333*a*b + (14/65*a -37752302/416086645*a*b)*c)*d*w
+ ((- 6/5*a*b + 16/5*a*b*c) + (40506358/32006665*a*b
+ (- 2733/2600*a - 36855394671/16643465800*a*b)*c)*d)
          .
          .
       途中略
          .
          .
((1 - b) + (- a + b)*c) + ((1 - a)*b + (- 2 + 2*a)*b*c)*d

235    s-polynomials are created
277    s-polynomials are detected to be redundant
22   boolean closures are created
```

出力された式が膨大な大きさなので大部分を省略している．出力は既約 Gröbner basis なので、最後のパラメーターのみを含む式が 1 になるようなパラメーターの値にたいして、上の式はすべて 0 になる．参考までに、$a=1, b=1, c=1, d=1$ としたときの Gröbner basis は以下のようになる．

```
w^3*y + 2*w^2*y + 64/99*w^3 + 5/3*z^2 + 5*y*z + 227/33*y^2 - 1/3*x*z
- 872/297*x*y + 326/297*x^2  - 887/198*w*z - 223/66*w*y + 2902/297*w*x
+ 283/99*w^2 + 604/99*z + 3467/99*y - 628/297*x  - 1099/198*w + 2293/54
```

```
w^4 - 6*w^2*y + 12*w^3 + 60*y^2 - x*z - 110/3*x*y + 23/3*x^2 - 10*w*z
- 39*w*y + 251/6*w*x  + 77/2*w^2 - 24*z + 355/2*y - 203/6*x - 3/2*w
+ 451/3

z^3 + 6/5*w^2*y + 1448/825*w^3 - 73/5*z^2 - 297/5*y*z + 3556/275*y^2
+ x*z - 88798/2475*x*y  + 8506/2475*x^2 + 38977/825*w*z - 586/275*w*y
- 1598/495*w*x + 16736/825*w^2 - 18872/165*z  - 37781/825*y
- 45773/2475*x + 9634/165*w - 30227/225

y*z^2 - 34/99*w^3 + 10/3*z^2 + 10*y*z - 68/33*y^2 - 2/3*x*z
+ 1280/297*x*y - 266/297*x^2  - 626/99*w*z + 2/33*w*y - 1/297*w*x
- 370/99*w^2 + 2018/99*z + 463/99*y + 1039/297*x - 1009/99*w + 457/27

y^2*z - 14/297*w^3 + 5/9*z^2 + 10/3*y*z - 28/99*y^2 - 1/9*x*z
+ 760/891*x*y - 28/891*x^2 - 316/297*w*z + 28/99*w*y + 547/891*w*x
- 164/297*w^2 + 994/297*z + 971/297*y + 719/891*x - 497/297*w + 419/81

y^3 + 1/9*w^2*y - 23/594*w^3 - 1/9*y*z + 142/99*y^2 - 1/18*x*z
- 953/1782*x*y - 1445/3564*x^2 + 145/1188*w*z + 4/33*w*y
- 4501/3564*w*x - 97/297*w^2 + 74/297*z - 4343/1188*y + 514/891*x
- 709/1188*w - 2045/324

x*z^2 - 4/33*w^3 - z^2 + 3*y*z + 124/11*y^2 + 5*x*z + 368/99*x*y
+ 124/99*x^2 + 37/33*w*z + 8/11*w*y + 887/99*w*x - 28/33*w^2
+ 185/33*z + 1555/33*y - 2/99*x - 10/33*w + 451/9

x*y*z - w*x - 3*y - 5

x*y^2 - 1/2*w^2*y + 5/66*w^3 + 1/2*y*z + 43/22*y^2 + 35/198*x*y
+ 43/198*x^2 - 5/66*w*z - 16/11*w*y + 203/198*w*x + 35/66*w^2
- 25/66*z + 325/66*y - 73/99*x + 29/66*w + 73/18

x^2*z + 14/33*w^3 - 5*z^2 - 15*y*z + 28/11*y^2 - x*z - 760/99*x*y
+ 28/99*x^2 + 481/33*w*z - 28/11*w*y - 349/99*w*x + 164/33*w^2
```

```
- 961/33*z - 773/33*y - 422/99*x + 497/33*w - 446/9

x^2*y + 5/33*w^3 - 23/11*y^2 + 1/2*x*z - 293/198*x*y + 53/198*x^2
- 5/33*w*z + 13/22*w*y - 353/198*w*x + 103/66*w^2 - 83/66*z
- 302/33*y + 85/99*x + 289/66*w - 74/9

x^3 - 7/33*w^3 + 283/11*y^2 - x*z + 677/99*x*y + 269/198*x^2
- 85/66*w*z - 19/11*w*y + 5101/198*w*x - 82/33*w^2 + 68/33*z
+ 6911/66*y - 581/99*x - 893/66*w + 1859/18

w*z^2 + 74/165*w^3 - 5*z^2 - 15*y*z + 148/55*y^2 - x*z - 5884/495*x*y
+ 148/495*x^2 + 2401/165*w*z - 148/55*w*y - 335/99*w*x + 848/165*w^2
- 965/33*z - 3803/165*y - 2174/495*x + 499/33*w - 2216/45

w*y*z - 14/99*w^3 + 5/3*z^2 + 5*y*z - 28/33*y^2 - 1/3*x*z + 760/297*x*y
- 28/297*x^2 - 316/99*w*z + 28/33*w*y + 547/297*w*x - 164/99*w^2
+ 994/99*z + 773/99*y + 422/297*x - 497/99*w + 446/27

w*y^2 - 1/3*x*y - 1/6*x^2 + 7/6*w*y - 1/6*w^2 + 1/3*y + 1/2*x - 5/6*w
    - 1/3

w*x*z + 3*y*z - w*z + 5*z + 2

w*x*y + 3*y^2 + 2/3*x*y + 1/3*x^2 + 5/3*w*x + 10*y - 2/3*x + 26/3

w*x^2 - 6*y^2 + 5/3*x*y - 2/3*x^2 - 16/3*w*x - 23*y + 19/3*x + w - 67/3

w^2*z - x*z + z - 2*w

w^2*x + 3*w*y - x + 5*w + 1
```

最後の例では S-多項式とブール閉包に関する出力のみを示すことにする.

例 3

```
?- neumann_gb([a*x^2*y*z + 4*e*x*y^2 - c*z^2*y*w - 5*d + 5,
               x*y*z - g*x*w - b*3*y - 5*d,
```

```
          x*y*z^2 - a + 3*b - z*w,
          x*y*z*w*f - c*x + d],
          [a,b,c,d,e,f,g]).

690    s-polynomials are created
581    s-polynomials are detected to be redundant
72    boolean closures are created
```

4 おわりに

$R[X_1, X_2, \ldots, X_n]/(X_1^2 - X_1, X_2^2 - X_2, \ldots, X_n^2 - X_n)$ は R^{2^n} と同型になることが容易に示される．したがって、この直積構造を利用して Gröbner basis の計算をすることができる．すなわち R 上の多項式環における Gröbner bases を 2^n 個計算して、それからもとの Gröbner basis が構成できる．特に、R が体の場合は commutative Von Neumann regular ring 特有のモノミアルリダクションを用いないで、通常の体上の多項式環における Gröbner bases の計算のみによってもとの Gröbner basis が構成できる．パラメーターの個数 n が非常に小さい場合はこの方法も有効であるが、2^n 個の Gröbner bases の計算が必要になるので、n が大きい場合は実用的ではない．例えば、$H = Q[X_1, X_2, \ldots, X_{20}]/(X_1^2 - X_1, X_2^2 - X_2, \ldots, X_{20}^2 - X_{20})$ として、$H[Y, Z]$ におけるイデアル $((X_1 + X_2 + \cdots + X_{20}) * (Y^2 * Z + 1), (X_1 + X_2 + \cdots + X_{20}) * (Y * Z^2 + 1))$ の Gröbner basis $\{(X_1 + X_2 + \cdots + X_{20}) * (Z - Y), (X_1 + X_2 + \cdots + X_{20}) * (Y^3 + 1)\}$ は、 commutative Von Neumann regular ring 特有のモノミアルリダクションを用いれば $S-$ 多項式を 1 つ計算するだけで求めることができるが、体 Q の直積構造を利用した場合は 2^{20} 個の同じ Gröbner bases $\{Z - Y, Y^3 + 1\}$ を計算しなければならない．

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 93] 佐藤洋祐、毛受哲、相場亮 (1995). ブーリアン・グレブナー基底の Syzygy 基底による特徴付け. 「情報処理学会論文誌」第 34 巻 第 7 号 pp 1549-1554.

[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). http://www.icot.or.jp/AITEC/FGCS/funding/itaku-H7-index-J.html http://www.icot.or.jp/AITEC/FGCS/funding/itaku-H8-index-J.html

[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.

[Sa 98] 佐藤 洋祐 (1998). Von Neumann regular rings 上の多項式環におけるグレブナー基底について. 数理解析研究所講究録 1038 「数式処理における理論と応用の研究」pp 40-48.

[Sb 98] Sato, Y. (1998). A new type of canonical Gröbner bases in polynomial rings over Von Neumann regular rings. International Symposium on Symbolic and Algebraic Computation(ISSAC 98), Proceedings pp 317-321.

[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.