Title	Generalized Discrete Comprehensive Grobner Bases (Computer Algebra : Algorithms, Implementations and Applications)
Author(s)	Sato, Yoske; Suzuki, Akira; Nabeshima, Katsusuke
Citation	数理解析研究所講究録 (2003), 1335: 105-110
Issue Date	2003-07
URL	http://hdl.handle.net/2433/43345
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録 1335 巻 2003 年 105-110

Generalized Discrete Comprehensive Gröbner Bases

Yosuke Sato
Department of Mathematical Sciences,
Ritsumeikan University *

Akira Suzuki
Graduate School of Science and Technology,
Kobe University †

Katsusuke Nabeshima
Department of Mathematical Sciences,
Ritsumeikan University ‡

Abstract

We showed special types of comprehensive Gröbner bases can be defined and calculated as the applications of Gröbner bases in polynomial rings over commutative Von Neumann regular rings in [5] and [6]. We called them discrete comprehensive Gröbner bases, since there is a strict restriction on specialization of parameters, that is parameters can take values only 0 and 1. In this paper, we show that our method can be naturally generalized to the cases where parameters can take any value from a given finite set.

1 Introduction

In [5] and [6], we proposed special types of comprehensive Gröbner bases called discrete comprehensive Gröbner bases using Weispfenning's theory of Gröbner bases in polynomial rings over commutative Von Neumann regular rings [9]. Roughly speaking, discrete comprehensive Gröbner bases are comprehensive Gröbner bases with parameters the specializations of which are restricted to only 0 and 1. One of the key facts for constructing discrete comprehensive Gröbner bases is that the quotient ring $R[X]/(X^2-X)$ for a given Von Neumann regular ring R also becomes a Von Neumann regular ring. We gave an elementary direct proof of this fact in [6]. However, this fact essentially follows from the Chinese remainder theorem. That is $R[X]/(X^2-X)$ is isomorphic to the direct product $R[X]/(X)\times R[X]/(X-1)$. This observation leads us to generalize discrete comprehensive Gröbner bases as follows.

Let K be a field and $S_1,\ldots,S_n$ be non-empty finite subsets of K. Let $A_1,\ldots,A_n$ be indeterminates and for each $i=1,\ldots,n$, let $p_i(A_i)$ be the polynomial $\prod_{k\in S_i}(A_i-k)$. Then the quotient ring

*ysato@theory.cs.ritsumei.ac.jp
†sakira@kobe-u.ac.jp
‡nabe@theory.cs.ritsumei.ac.jp

$K[A_1,\ldots,A_n]/(p_1(A_1),\ldots,p_n(A_n))$ becomes a commutative Von Neumann regular ring. Let F be a finite set of polynomials in $K[A_1,\ldots,A_n,\overline{X}]$, where $\overline{X}$ are indeterminates distinct from $A_1,\ldots,A_n$. Considering F to be a finite set of polynomials in $(K[A_1,\ldots,A_n]/(p_1(A_1),\ldots,p_n(A_n)))[\overline{X}]$, construct a stratified Gröbner basis G of the ideal (F). Then G becomes a discrete comprehensive Gröbner basis of (F) in the following sense. For each $i=1,\ldots,n$, let a_i be an element of S_i. Then the set of polynomials $G(a_1,\ldots,a_n)=\{g(a_1,\ldots,a_n,\overline{X})|g\in G\}$ is the reduced Gröbner basis of the ideal generated by the set of polynomials $F(a_1,\ldots,a_n)=\{f(a_1,\ldots,a_n,\overline{X})|f\in F\}$ in $K[\overline{X}]$.

We made an implementation to compute the above revised version of discrete comprehensive Gröbner bases for the case that K is the field of rational numbers. Through our computation experiments, we found that they are sufficiently practical.

The rest of the paper is organized as follows. In Section 2, we describe some mathematical facts which play important roles for the construction of our revised discrete comprehensive Gröbner bases. Our main results are shown in Section 3. In Section 4, we give some computation examples of our implementation. The reader is assumed to be familiar with the theory of Gröbner bases in polynomial rings over commutative Von Neumann regular rings. We refer the reader to [9],[4] or [6].

2 Some basic facts

In this section, we show some mathematical facts which are easy consequences of the Chinese remainder theorem.

Lemma 1
Let K be a field and $a_1,a_2,\ldots,a_\ell$ be distinct elements of K. Let $p(X)$ be a polynomial defined by $p(X)=(X-a_1)(X-a_2)\cdots(X-a_\ell)$. Let R be a commutative ring which extends K. Then $R[X]/(p(X))$ is isomorphic to R^ℓ. Actually the mapping Φ from $R[X]/(p(X))$ to R^ℓ defined by $\Phi(h(X))=(h(a_1),h(a_2),\ldots,h(a_\ell))$ is an isomorphism.

Proof The ideals $(X-a_1),(X-a_2),\ldots,(X-a_\ell)$ are clearly co-maximal in $K[X]$. Hence, they are also co-maximal in $R[X]$. By the Chinese remainder theorem, we have an isomorphism Φ from $R[X]/(p(X))$ to $\prod_{i=1\ldots\ell}R[X]/(X-a_i)$ defined by $\Phi(h(X))=(h(a_1),h(a_2),\ldots,h(a_\ell))$. $R[X]/(X-a_i)$ is clearly isomorphic to R for each i. ∎

Using the above lemma we have the following.

Lemma 2
Let K be a field and $S_1,S_2,\ldots,S_n$ be non-empty finite subsets of K. Let $A_1,\ldots,A_n$ be indeterminates and $p_i(A_i)$ be a polynomial $\prod_{k\in S_i}(A_i-k)$ for each $i=1,\ldots,n$. Then $K[A_1,\ldots,A_n]/(p_1(A_1),\ldots,p_n(A_n))$ is isomorphic to K^M, where $M=|S_1||S_2|\ldots|S_n|$ and $|S_i|$ denotes the cardinality of S_i.

Proof We prove by induction on n. When n is 1, it follows directly from Lemma 2.1. Note that $K[A_1,\ldots,A_n]/(p_1(A_1),\ldots,p_n(A_n))$ is isomorphic to $R[A_n]/(p_n(A_n))$ with
$R=K[A_1,\ldots,A_{n-1}]/(p_1(A_1),\ldots,p_{n-1}(A_{n-1}))$. By the induction hypothesis, R is isomorphic to $K^{M'}$, where $M'=|S_1||S_2|\ldots|S_{n-1}|$. Since R clearly includes K, we can apply Lemma 2.1 to have an isomorphism between $R[A_n]/(p_n(A_n))$ and $R^{|S_n|}$ which is isomorphic to K^M. ∎

By this lemma, we can see $K[A_1,\ldots,A_n]/(p_1(A_1),\ldots,p_n(A_n))$ is a commutative Von Neumann regular ring. This is the key fact in this paper. In order to have our discrete comprehensive Gröbner bases, we need to describe the isomorphism explicitly.

Lemma 3
With the same notations in Lemma 2.2, let $\overline{\alpha}_1,\overline{\alpha}_2,\ldots,\overline{\alpha}_M$ be an enumeration of the set $\{(a_1,a_2,\ldots,a_n)|a_i \in S_i$ for each $i\}$. Let $\overline{\alpha}_j = (\alpha_1^j,\alpha_2^j,\ldots,\alpha_n^j)$ for each $j = 1,2,\ldots,M$. The mapping Φ from $K[A_1,\ldots,A_n]/(p_1(A_1),\ldots,p_n(A_n))$ to $\prod_{j=1\ldots M} K[A_1,\ldots,A_n]/(A_1-\alpha_1^j,\ldots,A_n-\alpha_n^j)$ defined by $\Phi(h(A_1,A_2,\ldots,A_n)) = (h(\overline{\alpha}_1),h(\overline{\alpha}_2),\ldots,h(\overline{\alpha}_M))$ is an isomorphism.

Proof We actually showed this fact in the proof of Lemma 2.2 by applying Lemma 2.1 iteratively. ∎

3 Discrete comprehensive Gröbner bases

For any polynomial h of $R[\overline{X}]$, let h^i denotes the polynomial in $K[\overline{X}]$ obtained from h by replacing each coefficient c in h by the ith coordinate of c, which belongs to K^M after identifying R with K^M. The following lemma is a directly consequence of Theorem 2.3 of [9].

Lemma 4
Let K be a field and R be a commutative Von Neumann regular ring defined as a finite direct product K^M of K for some natural number M. Fix a term order for the terms in the indeterminates $\overline{X}$ and let $G = \{g_1,\ldots,g_k\}$ be the stratified reduced Gröbner basis of an ideal $(f_1,\ldots,f_\ell)$ in a polynomial ring $R[\overline{X}]$. Then, $\{g_1^i,\ldots,g_k^i\}$ becomes the reduced Gröbner basis of the ideal $(f_1^i,\ldots,f_\ell^i)$ in the polynomial ring $K[\overline{X}]$ for each $i = 1,2,\ldots,M$.

We also have the following lemma.

Lemma 5
With the same notations and conditions in Lemma 3.1, let $G_i = \{g_1^i,\ldots,g_k^i\}$ for each i. Then for any polynomial h in $R[\overline{X}]$, we have $(h\downarrow_G)^i = h^i\downarrow_{G_i}$ for each i. Here, $h\downarrow_G$ denotes the normal form of h with respect to the Gröbner basis G.

Proof The proof is essentially same as the proof for Property (2) of Theorem 3.3 [6] or the proof for Property (2) of Theorem 3.2 [7]. ∎

Now we are ready to state our revised discrete comprehensive Gröbner bases.

Theorem 6
Let K be a field and $S_1,\ldots,S_n$ be non-empty finite subsets of K. Let $A_1,\ldots,A_n$ be indeterminates and $p_i(A_i)$ be a polynomial $\prod_{k\in S_i}(A_i-k)$ for each $i = 1,\ldots,n$. Then, the quotient ring $K[A_1,\ldots,A_n]/(p_1(A_1),\ldots,p_n(A_n))$ becomes a commutative Von Neumann regular ring as is shown in Lemma 2.2. Let F be a finite set of polynomials in $K[A_1,\ldots,A_n,\overline{X}]$, where $\overline{X}$ are indeterminates distinct from $A_1,\ldots,A_n$.
Fix a term order of terms of indeterminates $\overline{X}$. Considering F to be a finite set of polynomials in $(K[A_1,\ldots,A_n]/(p_1(A_1),\ldots,p_n(A_n)))[\overline{X}]$, construct the stratified Gröbner basis G of the ideal (F) in this polynomial ring. Then we have the following properties.

(1) For any n-tuple $(a_1, a_2, \ldots, a_n)$ *of elements of* K *such that* $a_i \in S_i$ *for each* i*, the set of polynomials* $G(a_1, \ldots, a_n) = \{g(a_1, \ldots, a_n, \overline{X}) | g \in G\}$ *is the reduced Gröbner basis of the ideal generated by the set of polynomials* $F(a_1, \ldots, a_m) = \{f(a_1, \ldots, a_n, \overline{X}) | f \in F\}$ *in* $K[\overline{X}]$.

(2) For any $h(A_1, \ldots, A_n, \overline{X})$ *in* $(K[A_1, \ldots, A_n]/(p_1(A_1), \ldots, p_n(A_n)))[\overline{X}]$,
$(h(A_1, \ldots, A_n, \overline{X})\downarrow_G)(a_1, \ldots, a_n, \overline{X}) = h(a_1, \ldots, a_n, \overline{X})\downarrow_{G(a_1, \ldots, a_n)}$.

Here, $r(a_1, \ldots, a_n, \overline{X})$ *denotes the polynomial in* $K[\overline{X}]$ *given from a polynomial* $r(A_1, \ldots, A_n, \overline{X})$ *in* $(K[A_1, \ldots, A_n]/(p_1(A_1), \ldots, p_n(A_n)))[\overline{X}]$ *by substituting each* A_i *with* a_i.

Proof The first property follows from Lemma 2.3 and Lemma 3.1, the second property follows from Lemma 2.3 and Lemma 3.2. ∎

Let G be as in Theorem 3.3. Then we call G a *discrete comprehensive Gröbner basis*. Remember that G is nothing but our original discrete comprehensive Gröbner basis, when each set S_i is $\{0, 1\}$.

4 Computation Examples

We made an implementation to compute the revised version of discrete comprehensive Gröbner bases for the case that the coefficient field is the field of rational numbers. Though our program is very naive and written in prolog, it is sufficiently practical. The following are examples of our computation experiments.

Example 1

Let F *be a set of polynomials* $\{A_1^2 A_2 X_1^2 X_2 + A_3 X_1 + A_2,\ A_1 A_3 X_1 X_2^2 + A_2 X_1 X_2 X_3^2 + X_1 + A_1,\ A_1^2 X_1 X_3 + A_1 X_2 + A_3 X_3\}$ *with parameters* A_1, A_2, A_3. *Let* $S_1 = \{-1, 0, 2\}, S_2 = \{-1, 0, 1\}, S_3 = \{-1, 1, 3\}$. *Our program calculated the following discrete comprehensive Gröbner basis with the graded reverse lex order* $>$ *such that* $X_1 > X_2 > X_3$.

$-A1^2 * A2^2 + 1/2 * A1^2 + A1 * A2^2 - 1/2 * A1 + A2^2,$
$(1/2 * A1^2 * A2^2 - 1/2 * A1^2 - 1/2 * A1 * A2^2 + 1/2 * A1 - A2^2 + 1) * X3,$
$(1/2 * A1^2 * A2^2 - 1/2 * A1^2 - 1/2 * A1 * A2^2 + 1/2 * A1 - A2^2 + 1) * X1,$
$(1/2 * A1^2 * A2^2 - 1/2 * A1 * A2^2) * X3 * X1 + (-1/4 * A1^2 * A2^2 + 3/4 * A1 * A2^2) * X2 + (3/8 * A1^2 * A2^2 * A3 - 5/8 * A1 * A2^2 * A3) * X3,$
$\vdots$
$(1/24*A1^2*A2^2*A3^2 - 1/12*A1^2*A2^2*A3 + 3/8*A1^2*A2^2 + 1/24*A1^2*A2*A3^2 - 1/12*A1^2*A2*A3 - 1/8*A1^2*A2 - 1/12*A1*A2^2*A3^2 + 1/6*A1*A2^2*A3 - 1/4*A1*A2^2 - 1/12*A1*A2*A3^2 + 1/6*A1*A2*A3 + 1/4*A1*A2) * X2^2 * X1 + (-1/24*A1^2*A2^2*A3^2 - 7/24*A1^2*A2^2*A3 + 1/8*A1^2*A2^2 - 1/24*A1^2*A2*A3^2 + 1/12*A1^2*A2*A3 + 1/8*A1^2*A2 + 1/12*A1*A2^2*A3^2 + 11/24*A1*A2^2*A3 - 1/4*A1*A2^2 + 1/12*A1*A2*A3^2 - 1/6*A1*A2*A3 - 1/4*A1*A2) * X2^2 + (17/48*A1^2*A2^2*A3^2 - 1/12*A1^2*A2^2*A3 - 1/8*A1^2*A2^2 + 1/24*A1^2*A2*A3^2 - 1/12*A1^2*A2*A3 - 1/8*A1^2*A2 - 37/48*A1*A2^2*A3^2 + 1/6*A1*A2^2*A3 + 1/4*A1*A2^2 - 1/12*A1*A2*A3^2 + 1/6*A1*A2*A3 + 1/4*A1*A2) * X3 * X2 + (1/24*A1^2*A2^2*A3^2 - 1/12*A1^2*A2^2*A3 - 1/8*A1^2*A2^2 + 1/24*A1^2*A2*A3^2 + 7/24*A1^2*A2*A3 - 1/8*A1^2*A2 - 1/12*A1*A2^2*A3^2 + 1/6*A1*A2^2*A3 + 1/4*A1*A2^2 - 1/12*A1*A2*A3^2 - 11/24*A1*A2*A3 + 1/4*A1*A2) * X2 + (1/4*A1^2*A2^2 - 5/16*A1^2*A2*A3^2 - 3/4*A1*A2^2 + 11/16*A1*A2*A3^2) * X3$

The computation time was a few seconds by a personal computer with a CPU of Pentium III 1200 MHZ. We can of course get a similar result by calculating a full comprehensive Gröbner basis of $F \cup \{(A_1 + 1)A_1(A_1 - 2), (A_2 + 1)A_2(A_2 - 1), (A_3 + 1)(A_3 - 1)(A_3 - 3)\}$. *However, cgb of CGB [1] and dispgb of DisPGB [3] that are the only available existing comprehensive Gröbner bases computation packages did not terminate within one hour.*

Example 2

Let F *be the same set of polynomials as the above example. Let* $S_1 = \{-3, -1, 0, 2, 5\}, S_2 = \{-3, -1, 0, 1, 5\}, S_3$ $\{-7, -1, 1, 3, 6\}$. *Our program calculated the discrete comprehensive Gröbner basis within 10 seconds and produced the following polynomial that consists of only parameters.*

$-1/225 * A1^4 * A2^4 + 2/225 * A1^4 * A2^3 + 16/225 * A1^4 * A2^2 - 2/225 * A1^4 * A2 - 1/30 * A1^4 + 1/75 * A1^3 * A2^4 - 2/75 * A1^3 * A2^3 - 16/75 * A1^3 * A2^2 + 2/75 * A1^3 * A2 + 1/10 * A1^3 + 1/15 * A1^2 * A2^4 - 2/15 * A1^2 * A2^3 - 16/15 * A1^2 * A2^2 + 2/15 * A1^2 * A2 + 1/2 * A1^2 - 19/225 * A1 * A2^4 + 38/225 * A1 * A2^3 + 304/225 * A1 * A2^2 - 38/225 * A1 * A2 - 19/30 * A1 - 1/15 * A2^4 + 2/15 * A2^3 + 16/15 * A2^2 - 2/15 * A2$

We can also get an information of parameters by calculating a Gröbner basis of $F \cup \{(A_1 + 3)(A_1 + 1)A_1(A_1 - 2)(A_1 - 5), (A_2 + 3)(A_2 + 1)A_2(A_2 - 1)(A_2 - 5), (A_3 + 7)(A_3 + 1)(A_3 - 1)(A_3 - 3)(A_3 - 6)\}$ in the polynomial ring $\mathbf{Q}[X_1, X_2, X_3, A_1, A_2, A_3]$ with the block term order such that $[X_1, X_2, X_3] > [A_1, A_2, A_3]$. We, again, were not able to compute the Gröbner basis even by using RISA/ASIR [2] that has a very fast and sophisticated Gröbner bases computation package.

5 Conclusion and Remarks

Though we do not give a description in this paper, we can generalize Theorem 3.3 for an arbitrary polynomial $p_i(A_i)$. In order to construct discrete comprehensive Gröbner bases for such cases, we further need factorizations in polynomial rings over algebraically extended fields and have to handle fields which are represented as quotient rings of some polynomial rings. Since we have not made an implementation for such cases at this point we do not know if they are feasible.

References

[1] Dolzmann, A., Sturm, T., Neun, W. (1999). CGB: Computing Comprehensive Gröbner Bases. http://www.fmi.uni-passau.de/ redlog/cgb/

[2] Noro, M. and Takeshima, T. (1992). Risa/Asir – A Computer Algebra System. International Symposium on Symbolic and Algebraic Computation (ISSAC 92), Proceedings, 387–396.

[3] Montes, A. (2002). A new algorithm for discussing Gröbner basis with parameters, J. Symb. Comp. 33, 1-2, 183–208.

[4] 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, 317–321.

[5] Sato, Y. and Suzuki, A. (2000). Gröbner Bases in Polynomial Rings over Von Neumann Regular Rings - Their applications -(Extended Abstract) Proceedings of The 4th Asian Symposium on Computer Mathematics(ASCM 2000), Lecture Notes Series on Computing Vol.8, World Scientific, pp 59–62.

[6] Sato, Y. and Suzuki, A. (2001). Discrete Comprehensive Gröbner bases. International Symposium on Symbolic and Algebraic Computation (ISSAC 2001), Proceedings, 292–296.

[7] Suzuki, A. and Sato, Y. (2002). An alternative approach to Comprehensive Gröbner bases. International Symposium on Symbolic and Algebraic Computation (ISSAC 2002), Proceedings, 255–261.

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

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

[10] Weispfenning, V. (1992). Comprehensive Gröbner bases, J. Symb. Comp. 14/1, 1–29.