ACGB on Varieties

Yosuke Sato* Akira Suzuki† Katsusuke Nabeshima‡

* Department of Mathematical Information Science,
Tokyo University of Science, Japan,
ysato@rs.kagu.tus.ac.jp
† Graduate School of Science and Technology,
Kobe University, Japan,
sakira@kobe-u.ac.jp
‡ Department of Mathematical Sciences,
Ritsumeikan University, Japan
nabe@theory.cs.ritsumei.ac.jp

Abstract. When constructing parametric Gröbner bases, we usually assume that parameters can take arbitrary values. However, in the case there are some constraints among parameters, it is more natural to construct parametric Gröbner bases for parameters satisfying such constraints. Using this idea, we formalized parametric Gröbner bases in terms of ACGB [8, 9]. This natural formalization leads us to the desirable fact that is discrete comprehensive Gröbner bases studied in [4–6] can be naturally defined as special instances of ACGB.

1 Introduction

Comprehensive Gröbner bases or comprehensive Gröbner systems introduced in [11] are uniform representations of Gröbner bases of polynomial ideals with parameters. During their construction, we implicitly assume that parameters can take any value. The following is a computation example of CGB[1]. It computes the comprehensive Gröbner system of the polynomial ideal $\langle a-b, xya-x^2yb-3a, xyb-3xb-5b\rangle$ with parameters a and b.

```
torder({y,x},lex);
on cgbgs;
gsys{a-b,x*y*a-x^2*y*b-3*a,x*y*b-3*x*b-5*b};
{{a - b <> 0 and b <> 0,{a - b}},
 {a <> 0 and b = 0,{a - b}},
 {b <> 0 and a - b = 0,
        2
  {b*y*x  - a*y*x + 3*a,
   b*y*x - (3*b)*x - 5*b,
                    2                   2
   (2*a*b)*y - (15*b )*x + (9*a*b - 25*b ),
       2   2               2
   (3*b )*x  - (3*a*b - 5*b )*x - 2*a*b}},
 {a = 0 and b = 0,{}}}
```

Though there is an obvious constraint $a-b=0$ among parameters a and b, the computation produced case distinctions `{a - b <> 0 and b <> 0,{a - b}}` and `{a <> 0 and b = 0,{a - b}}` where the ideal becomes the whole ring. When we are interested in only values such that the ideal becomes proper, those computations are unnecessary.

It is not very difficult to make an implementation with facilities to handle such constraints among parameters. Actually DisPGB[2] which is an another implementation to compute parametric Gröbner bases has such a tool [1]. We can input two kinds of constraints among parameters. One

[1] http://www.fmi.uni-passau.de/~redlog/cgb/

[2] http://www-ma2.upc.es/~montes/

is in a form of equalities, and the another one is in a form of inequalities. The following is its computation example, where the input ideal $\langle (a-b)+(xya-x^2yb-3a)^3+(xyb-3xb-5b)^4, xya-x^2yb-3a, xyb-3xb-5b\rangle$ has a slightly more complicated form.

```
L := dispgb([(a-b)+(x*y*a-x^2*y*b-3*a)^3+(x*y*b-3*x*b-5*b)^4,
     a*(x*y*a-x^2*y*b-3*a),
     x*y*b-3*x*b-5*b],plex(y,x),plex(a,b),null=[a-b],notnull={a}):

tprint(L);
                            null = [a - b], notnull = {a}

                                                 2
                  Case = [1], [b <> 0], [3 x  + 2 x - 2, 2 y - 15 x - 16]

                           [0] - Not compatible conditions
```

In this example, `null = [a - b]` is a constraint consisting of the set of equalities $\{a-b=0\}$, `notnull = {a}` is a constraint consisting of the set of inequalities $\{a \neq 0\}$.

It is also very easy to add such facilities to an ACGB introduce in [8, 9]. An ACGB (Alternative Comprehensive Gröbner bases) is defined as a Gröbner basis in a polynomial ring over a certain commutative Von Neumann regular ring, it serves as an alternative of a comprehensive Gröbner basis. We generalized an ACGB so that we can handle constraints among parameters. Our rather trivial generalization brings us an interesting and desirable result.

Discrete comprehensive Gröbner bases we have been studying in [2, 4–6] are different kinds of applications of commutative Von Neumann regular rings to comprehensive Gröbner bases. We found that they are special instances of ACGB-V. Consequently, we can give more general alternative proofs of our results in [2, 4–6]. We can extend discrete comprehensive Gröbner bases to more general cases in a natural way.

Our plan is as follows. In Section 2, we describe our formalization. In Section 3, we show how discrete comprehensive Gröbner bases can be naturally defined as special instances of ACGB under our formalization. In Section 4, we discuss further properties of our formalization.

We assume the reader is familiar with comprehensive Gröbner bases introduced in [11] and ACGB introduced in [8, 9]. We also assume the reader is familiar with Gröbner bases in polynomial rings over commutative Von Neumann regular rings, we refer the reader to [3], [10] or [13] for details. The reader is not necessarily required to be acquainted with discrete comprehensive Gröbner bases.

2 ACGB-V

When there is a constraint of parameters $\bar{A} = A_1, \ldots, A_m$ in a form of polynomial equations $f_1(\bar{A}) = 0, \ldots, f_l(\bar{A}) = 0$, it is more natural to consider the range of values for $\bar{A}$ to be the variety $V(f_1(\bar{A}), \ldots, f_l(\bar{A}))$ than a whole space K^m. Here, K is a field we are working in.

One of the main ideas of ACGB is that we consider a polynomial in $\bar{A}$ as a function from K^m to K, i.e. as a member of K^{K^m} that is a commutative Von Neumann regular ring, and then treat it as a member of the regular closure of $K[A_1, \ldots, A_m]$ in K^{K^m}. When such constraints exist, we can replace K^{K^m} by $K^{V(f_1(\bar{A}),\ldots,f_l(\bar{A}))}$. Note that the restriction of $K[A_1, \ldots, A_m]$ on $K^{V(f_1(\bar{A}),\ldots,f_l(\bar{A}))}$ is isomorphic to a quotient ring $K[\bar{A}]/I(V(f_1(\bar{A}), \ldots, f_l(\bar{A})))$, where $I(V(f_1(\bar{A}), \ldots, f_l(\bar{A})))$ denotes an ideal of $K[\bar{A}]$ that consists of all polynomials vanishing at every point of $V(f_1(\bar{A}), \ldots, f_l(\bar{A}))$. Hence, it is isomorphic to $K[\bar{A}]/rad(\langle f_1(\bar{A}), \ldots, f_l(\bar{A})\rangle)$ in case K is an algebraically closed field. Here, $rad(I)$ denotes a radical ideal of I. The above observation leads us to the following definition.

Definition 1. *Let K be an algebraically closed field. Let F be a finite set of polynomials in $K[\bar{A}, \bar{X}]$, where $\bar{A}$ and $\bar{X}$ denote a sequence of indeterminates $A_1, \ldots, A_m$ and $X_1, \ldots, X_n$. Let I be a polynomial ideal in $K[\bar{A}]$. An ACGB-V (Alternative Comprehensive Gröbner Basis on a Variety) of F with respect to I is defined as follows.*

Let T be a regular closure of the quotient ring $K[\bar{A}]/rad(I)$ in the commutative Von Neumann regular ring $K^{V(I)}$. Then there exists a stratified Gröbner basis G of F in $T[\bar{X}]$. We call G an ACGB-V of F with respect to the ideal I.

For the construction of G, we can use the same algorithm as in [8, 9] using terraces to compute T. The only difference is that any preterrace appearing in a computation of T has a form of $\langle s, t, r\rangle$ where s and t include all generators of $rad(I)$. Note that this restriction is imposed in order to assure that $V(I) \supseteq V(s)$ and $V(I) \supseteq V(t)$. The name ACGB-V is derived from the next theorem, where we use the same notations of specializations as in [8, 9].

Theorem 1. *Using the same notations as in the above definition, let $G = \{g_1(\bar{X}), \ldots, g_k(\bar{X})\}$ be an ACGB-V of $F = \{f_1(\bar{A}, \bar{X}), \ldots, f_l(\bar{A}, \bar{X})\}$ with respect to an ideal I of $K[\bar{A}]$, then the following properties hold for any m-tuple $(a_1, \ldots, a_m)$ of elements of K belonging to the variety $V(I)$:*

1. *$G_{(a_1,\ldots,a_m)} = \{g_{1(a_1,\ldots,a_m)}(\bar{X}), \ldots, g_{k(a_1,\ldots,a_m)}(\bar{X})\} \setminus \{0\}$ is a reduced Gröbner basis of the ideal generated by $F(a_1, \ldots, a_m) = \{f_1(a_1, \ldots, a_m, \bar{X}), \ldots, f_k(a_1, \ldots, a_m, \bar{X})\}$ in $K[X_1, \ldots, X_n]$.*
2. *For any polynomial $h(\bar{X}) \in T[\bar{X}]$, we have $(h \downarrow_G)_{(a_1,\ldots,a_m)}(\bar{X}) = h_{(a_1,\ldots,a_n)}(\bar{X}) \downarrow_{G_{(a_1,\ldots,a_m)}}$.*

Proof. The proof is exactly same as the proof of theorem 3.2 of [8] or theorem 4.3 of [9]. □

Example 1. Let F be the set of polynomials $\{a - b, xya - x^2yb - 3a, xyb - 3xb - 5b\}$. Take a lexicographic term order $>$ such that $y > x$. As we saw in the examples of Section 1, when we are interested in only values such that the ideal becomes proper, it is more natural to construct an ACGB-V of F with respect to the ideal $\langle a - b\rangle$. Since $\langle a - b\rangle$ is already a radical ideal, we construct a stratified Gröbner basis G of $\{a - b, xya - x^2yb - 3a, xyb - 3xb - 5b\}$ in $T[x, y]$, where T is a regular closure of $K[a, b]/\langle a - b\rangle$. This G is the desired ACGB-V of F and has the following form using terraces:

$$\begin{aligned} G = \{ & [(V(a-b) - V(a-b,a), 1)]y + [(V(a-b) - V(a-b,a), -15/2)]x \\ & \qquad\qquad\qquad\qquad + [(V(a-b) - V(a-b,a), -8)], \\ & [(V(a-b) - V(a-b,a), 1)]x^2 + [(V(a-b) - V(a-b,a), +2/3)]x \\ & \qquad\qquad\qquad\qquad + [(V(a-b) - V(a-b,a), -2/3)] \,\}. \end{aligned}$$

We should note that the ACGB-V of $\{(a-b) + (xya - x^2yb - 3a)^3 + (xyb - 3xb - 5b)^4, xya - x^2yb - 3a, xyb - 3xb - 5b\}$ with respect to $\langle a - b\rangle$ has the same form.

3 Connection Between Discrete Comprehensive Gröbner Bases

In this section, we show that discrete comprehensive Gröbner bases introduced in [4, 5] and further optimized in [2, 6] are special instances of ACGB-V. Before describing our results, we will give a short review of discrete comprehensive Gröbner bases.

Though the original discrete comprehensive Gröbner bases introduced in [4, 5] works for arbitrary commutative Von Neumann regular ring, we studied them for only fields in [2, 6]. In this paper, we also concentrate on polynomial rings over fields.
We begin with a general definition of discrete comprehensive Gröbner bases employed in [2].

Definition 2. *Let K be an arbitrary field and $F = \{f_1(\bar{A}, \bar{X}), \ldots, f_l(\bar{A}, \bar{X})\}$ be a finite set of polynomials in $K[\bar{A}, \bar{X}]$, where $\bar{A}$ and $\bar{X}$ denote a sequence of indeterminates $A_1, \ldots, A_m$ and $X_1, \ldots, X_n$. Let S be a set of polynomials $\{s_1(A_1), \ldots, s_m(A_m)\}$, where each $s_i(A_i)$ is a non-constant univariate polynomial in $K[A_i]$. A finite set $G = \{g_1(\bar{A}, \bar{X}), \ldots, g_k(\bar{A}, \bar{X})\}$ of polynomials in $K[\bar{A}, \bar{X}]$ is called a discrete comprehensive Gröbner basis of F with respect to $(\bar{A}, S)$ if it satisfies the following:*

$G(\bar{a}) = \{g_1(\bar{a}, \bar{X}), \ldots, g_k(\bar{a}, \bar{X})\} \setminus \{0\}$ is a Gröbner basis of $\{f_1(\bar{a}, \bar{X}), \ldots, f_l(\bar{a}, \bar{X})\}$ in $\overline{K}[\bar{X}]$ for any elements $\bar{a} = a_1, \ldots, a_m$ of $\overline{K}$(an algebraic closure of K) satisfying $s_1(a_1) = 0, \ldots, s_m(a_m) = 0$.

In [2], we showed that we can always construct such a discrete comprehensive Gröbner basis whenever K is a perfect computable field using the fact that the quotient ring $K[\bar{A}]/\langle s_1'(A_1),\dots,s_m'(A_m)\rangle$ becomes a commutative Von Neumann regular ring. Here, $s_i'(A_i)$ denotes a squarefree part of $s_i(A_i)$ for each $i=1,\dots,m$. Our proof was rather elementary, it is simply based on the Chinese remainder theorem, it does not use any sophisticated technique.

In the rest of this section, we show that we can naturally extend discrete comprehensive Gröbner bases to more general situations as a corollary of Theorem 1.

Lemma 1. *Let K be an arbitrary field and I be a zero dimensional radical ideal in a polynomial ring $K[\bar{A}]$. Then $K[\bar{A}]/I$ becomes a commutative Von Neumann regular ring.*

Proof. Present I as an intersection of prime ideals $P_1,\dots,P_k$ of $K[\bar{A}]$. Since I is zero dimensional, each P_i is also zero dimensional. Therefore P_i is a maximal ideal. So we can apply the Chinese remainder theorem to get an isomorphism $K[\bar{A}]/I \simeq K[\bar{A}]/P_1 \times \cdots \times K[\bar{A}]/P_k$. The right-hand side is a direct product of fields, so it becomes a commutative Von Neumann regular ring. □

Using this lemma together with Theorem 1, we can generalize discrete comprehensive Gröbner bases.

Theorem 2. *Let K be an arbitrary field and I be a zero dimensional ideal in a polynomial ring $K[\bar{A}]$. Let $F=\{f_1(\bar{A},\bar{X}),\dots,f_l(\bar{A},\bar{X})\}$ be a finite set of polynomials in $K[\bar{A},\bar{X}]$, where $\bar{A}$ and $\bar{X}$ denote a sequence of indeterminates $A_1,\dots,A_m$ and $X_1,\dots,X_n$.*
Let $G=\{g_1(\bar{A},\bar{X}),\dots,g_k(\bar{A},\bar{X})\}$ be a stratified Gröbner basis of F in a polynomial ring $(K[\bar{A}]/rad(I))[\bar{X}]$ over a commutative Von Neumann regular ring $K[\bar{A}]/rad(I)$. Then we have the following two properties for any m-tuple $(a_1,\dots,a_m)$ (denoted by $\bar{a}$) of elements of $\overline{K}$ belonging to the variety $V(I)$:

1. *$G(\bar{a})=\{g_1(\bar{a},\bar{X}),\dots,g_k(\bar{a},\bar{X})\}\setminus\{0\}$ is a reduced Gröbner basis of $F(\bar{a})=\{f_1(\bar{a},\bar{X}),\dots,f_l(\bar{a},\bar{X})\}$ in $\overline{K}[X_1,\dots,X_n]$.*
2. *For any polynomial $h(\bar{A},\bar{X})\in K[\bar{A},\bar{X}]$, we have $(h(\bar{A},\bar{X})\downarrow_G)(\bar{a},\bar{X})=h(\bar{a},\bar{X})\downarrow_{G(\bar{a})}$.*

Proof. Though, K might not be algebraically closed, we can work in its algebraic closure $\overline{K}$ and have a ACGB-V of F with respect to I by Theorem 1. Since $K[\bar{A}]/rad(I)$ is already a commutative Von Neumann regular ring, its regular closure in $K^{V(I)}$ is the ring itself. Therefore, any element of T has a representative in $K[\bar{A}]$. This assures that we can have G inside of $K[\bar{A},\bar{X}]$. Such a G clearly satisfies the above two properties. □

4 Some Properties of ACGB-V

As we saw in Section 1, we should use information about constraints on parameters in construction of parametric Gröbner bases. A natural way to get such constraints from a finite set of polynomials $F=\{f_1(\bar{A},\bar{X}),\dots,f_l(\bar{A},\bar{X})\}$ with parameters $\bar{A}$ is first to compute an elimination ideal I of $\langle F\rangle$ with respect to $\bar{A}$, i.e. $I=\langle F\rangle\cap K[\bar{A}]$, then construct an ACGB-V of F with respect to I.
It might happen that there exist some hidden constraints even if the elimination ideal I is equal to $\{0\}$.

Example 2. Let $F=\{AX+1, X+Y\}$ with a parameter A. Though its elimination ideal is equal to $\{0\}$, there is a hidden constraint $A\neq 0$, that is $\{a\in\mathbf{C}\mid \exists x,y\in\mathbf{C}\ ax+1=0 \text{ and } x+y=0\} = \{a\in\mathbf{C}\mid a\neq 0\}$.

In this example, there does not exists any nontrivial ideal I of $\mathbf{Q}[A]$ such that $V(I)\supseteq\{a\in\mathbf{C}\mid a\neq 0\}$. Therefore there is no proper ideal I of parameter A such that we could construct a ACGB-V of F with respect to I. Fortunately this is not a coincidence. The following theorem is an easy consequence of a well-known fact of varieties, from which we know the above natural construction is the best effort by ACGB-V's.

Theorem 3. *Let K be an algebraically closed field and $F = \{f_1(\bar{A}, \bar{X}), \dots, f_l(\bar{A}, \bar{X})\}$ be a finite set of polynomials in $K[\bar{A}, \bar{X}]$ with parameters $\bar{A}$. Let I be an elimination ideal of $\langle F \rangle$ with respect to $\bar{A}$. Then there does not exists an ideal I' in $K[\bar{A}]$ such that $V(I)$ properly includes $V(I')$ and any constraint of $\bar{A}$ resides inside of the variety $V(I')$ that is $V(I') \supseteq \{\bar{a} \in K^m \mid \exists\, \bar{x} \in K^n\ f_i(\bar{a}, \bar{x}) = 0$ for $i = 1, \dots, l\}$.*

Proof. This is simply a restatement of a well-known fact that $V(I)$ is the Zariski closure of the projection of $V(F)$ i.e. $\{\bar{a} \in K^m \mid \exists\, \bar{x} \in K^n\ (\bar{a}, \bar{x}) \in V(F)\}$. □

We conclude the section with the following interesting fact.

Theorem 4. *Let I be a zero dimensional ideal of a polynomial ring $K[A_1, \dots, A_m]$ with an arbitrary field K. Let $s_i(A_i)$ be a univariate polynomial of A_i for each $i = 1, \dots, m$. Then we have a polynomial $f(A_1, \dots, A_m)$ in $K[A_1, \dots, A_m]$ such that $f(a_1, \dots, a_m) = 0$ if $(a_1, \dots, a_m) \in V(I)$ and $f(a_1, \dots, a_m) = 1$ if $(a_1, \dots, a_m) \notin V(I)$. Where each a_i runs over any element of $\overline{K}$ that satisfies $s_i(a_i) = 0$.*

Proof. This is a special instance of Theorem 2 with $I = \langle s_1(A_1), \dots, s_m(A_m) \rangle$, although there does not appear any variable X_i. □

Example 3. Let I be an ideal $\langle A^2 - 2, A - B \rangle$ of $\mathbf{Q}[A, B]$, $s_1(A) = A^2 - 1$ and $s_2(B) = B^2 - 1$. The $f(A, B)$ has the following form $-\frac{1}{4}\,AB + \frac{1}{2}$.

5 Conclusion and Remarks

Though we have not implemented ACGB-V yet, we can expect the following.
When an ideal I is zero dimensional, ACGB-V of F with respect to I is a generalization of our discrete comprehensive Gröbner basis as we saw in Section 3. Once we get a prime ideal decomposition $I = \cap_{i=1}^{l} P_i$ with zero dimensional maximal ideals P_i's, what we have to do is essentially computation of each field $K[\bar{A}]/P_i$. We think that the computation of ACGB-V of F is much more efficient than the computation of ACGB of F. We can even use a distributive computation for $K[\bar{A}]/P_i$'s.
When an ideal I is not zero dimensional, an ACGB-V of F with respect to I is constructed by using terraces and its computation is essentially same as the computation of an ACGB of F as we have explained right after Definition 1. In this case we do not think we can expect much advantage of ACGB-V for most cases, although we can expect drastic reduction of computation time in some case such as the second example of Section 1.

References

1. Montes, A. (2002). A new algorithm for discussing Gröbner basis with parameters, J. Symb. Comp. 33, 1-2, 183–208.
2. Nabeshima, K., Sato, Y. and Suzuki, A. (2003). On extension of Discrete Comprehensive Gröbner Bases(in Japanese). Submitted for publication.
3. 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
4. Sato, Y. and Suzuki, A. (2000). Gröbner Bases in polynomial rings over Von Neumann regular rings – their applications – (Extended Abstract). Proceedings of the Fourth Asian Symposium in Computer Mathematics (ASCM 2000). Lecture Notes Series on Computing Vol. 8, World Scientific, 59–62
5. Sato, Y. and Suzuki, A. (2001). Discrete Comprehensive Gröbner Bases. International Symposium on Symbolic and Algebraic Computation (ISSAC 2001), Proceedings, 292–296.
6. Sato, Y., Suzuki, A. and Nabeshima, K. (2003). Discrete Comprehensive Gröbner Bases II. Proceedings of the Sixth Asian Symposium in Computer Mathematics (ASCM 2003). Lecture Notes Series on Computing Vol. 10, World Scientific, 240–247.
7. 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.

8. 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.
9. Suzuki, A. and Sato, Y. (2002). An Alternative approach to Comprehensive Gröbner Bases. To appear in J. Symb. Comp. 2003.
10. Weispfenning, V. (1989). Gröbner bases in polynomial ideals over commutative regular rings, EUROCAL '87, J. H. Davenport Ed., Springer LNCS 378, 336–347.
11. Weispfenning, V. (1992). Comprehensive Gröbner bases, J. Symb. Comp. 14/1, 1–29.
12. Weispfenning, V. (2002). Canonical Comprehensive Gröbner bases, International Symposium on Symbolic and Algebraic Computation (ISSAC 2002), Proceedings, 270–276.
13. Weispfenning, V. (2003). Comprehensive Gröbner bases and regular rings, To appear in J. Symb. Comp. 2003.