数式処理 *J.JSSAC (2007)*
Vol. 14, No. 1, pp. 41 - 65

CGB 特集

Comprehensive Gröbner bases and von Neumann regular rings

Katsusuke Nabeshima *

Research Institute for Symbolic Computation (RISC-Linz), Johannes Kepler Universität Linz

Abstract

There is a close relation between comprehensive Gröbner bases and non-parametric Gröbner bases over commutative von Neumann regular rings. By this relation, Gröbner bases over a commutative von Neumann regular ring can be viewed as an alternative to comprehensive Gröbner bases. (Therefore, this Gröbner basis is called an "alternative comprehensive Gröbner basis (ACGB)".) In the first part of this paper, we treat the theory of Gröbner bases in polynomial rings over a commutative von Neumann regular ring. In the second part, we describe the special type of comprehensive Gröbner bases which is called alternative comprehensive Gröbner bases on varieties (ACGB-V).

1 Introduction

We describe the relations between comprehensive Gröbner bases and non-parametric Gröbner bases over commutative von Neumann regular rings. Commutative von Neumann regular rings can be viewed as certain subdirect products of fields. So in some sense they can code arbitrary sets of fields. In 1987, Weispfenning studied and constructed the theory of Gröbner bases in polynomial rings over a commutative von Neumann regular ring. In 1992, Weispfening also introduced, constructed and studied comprehensive Gröbner bases for parametric polynomial ideals. Here, we show that there is a surprisingly close relationship between his two works. Thus, we show that Gröbner bases over commutative von Neumann regular rings do in fact cover parametric Gröbner bases over commutative von Neumann rings. We call the parametric Gröbner bases "alternative comprehensive Gröbner bases (ACGB)". In the papers [SS02, SS03, SSN02, SSN03b, SSN03a, SS04, Wei02b, Wei06], these results are shown. In the second part of this paper, we present the special type of comprehensive Gröbner bases. In construction of parametric Gröbner bases, we usually assume that parameters can take arbitrary values. In case, however, there exist some constraints among parameters, it is more natural to construct comprehensive Gröbner bases for only parameters satisfying such constraints. Using this idea, we formalized comprehensive Gröbner bases in terms of ACGB. In the papers [SSN03a, SSN03b, Nab05a, Nab05b], these results were presented.

*Katsusuke.Nabeshima@risc.uni-linz.ac.at

2 Von Neumann regular rings and Boolean algebra

In this section we describe relations between commutative von Neumann regular rings and Boolean algebra. Some of the facts of this section are presented in Saracino and Weispfenning [SW75, Lou79], and some books of "Boolean algebra", for instance [BS80]. First, we give a definition of "commutative von Neumann regular rings".

Definition 1 (commutative von Neumann regular rings [SW75, Wei87])
A commutative ring R with identity 1 is called a commutative **von Neumann regular ring** if it has the following property:

$$\forall a \in R \ \ \exists b \in R \text{ such that } \ \ a^2 b = a.$$

For such b, $a^* := ab$ and $a^{-1} := ab^2$ are uniquely determined and satisfy $aa^* = a$, $aa^{-1} = a^*$ and $(a^*)^2 = a^*$ is idempotent of a, a^{-1} the quasi inverse of a.

Note that every direct product of fields is a commutative von Neumann regular ring. Conversely, any commutative von Neumann regular ring is known to be isomorphic to a subring of a direct product of fields [SW75].
In this chapter, we assume that R is a commutative von Neumann regular ring.

Example 2
Take $R = \mathbb{Q}^3$ and define for $a = (a_1, a_2, a_3) \in \mathbb{Q}^3$, $a^{-1} := (y_1, y_2, y_3)$ where for $i \in \{1, 2, 3\}$

$$y_i = \begin{cases} 0, & \text{if } a_i = 0, \\ \frac{1}{a_i}, & \text{otherwise.} \end{cases}$$

We see that for all $a \in \mathbb{Q}^3$ there exists $b \in \mathbb{Q}^3$, namely

$$b := a^{-1} \text{ such that } a^2 b = a.$$

Therefore, $\mathbb{Q}^3$ is a von Neumann regular ring. (We consider $0^{-1} := 0$.)

A definition of Boolean algebra is the following.

Definition 3
$\mathbb{B} := \langle B, \wedge, \vee, \neg, 0, 1 \rangle$ is called a **Boolean algebra** if $\mathbb{B}$ satisfies the following property;

1. $x \vee x = x \wedge x = x$, for $x \in B$,
2. $x \vee y = y \vee x$, $x \wedge y = y \wedge x$, for $x, y \in B$,
3. $(x \vee y) \vee z = x \vee (y \vee z)$, $(x \wedge y) \wedge z) = x \wedge (y \wedge z)$, for $x, y, z \in B$,
4. $(x \vee y) \wedge x = x$, $(x \wedge y) \vee x = x$, for $x, y \in B$,
5. $(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z)$, $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$, for $x, y, z \in B$,
6. $x \vee \neg x = 1$, $x \wedge \neg x = 0$, for $x \in B$.

Definition 4
Let R be a commutative von Neumann regular ring. Let $A = \{x \in R | x^2 = x\}$ be a set of idempotents of R. Define on A the operations $\neg, \wedge, \vee$ by $\neg a = 1 - a$, $a \wedge b = ab$ and $a \vee b = a + b - ab$. Then $B(R) := \langle A, \neg, \wedge, \vee, 1, 0 \rangle$ is called the **Boolean algebra** of R. The set A is called the **carrier set** of $B(R)$.

Note that the carrier set of $B(\mathbb{Q}^3)$ is $\{(x_1, x_2, x_3) \mid x_1, x_2, x_3 \in \{0, 1\}\}$.

Definition 5 ([BS80])
Let $\mathbb{B} = \langle B, \wedge, \vee, \neg, 0, 1\rangle$ be a Boolean algebra. A subset I of B is called an **ideal** of $\mathbb{B}$ if

1. $0 \in I$,
2. $a, b \in I \Rightarrow a \vee b \in I$,
3. $(a \in I \text{ and } b = a \wedge b) \Rightarrow b \in I$.

Note that definition 5 property (3) is equivalent to ;

$$a \in I \text{ and } b \in B \Rightarrow a \wedge b \in I.$$

It is important to consider prime ideals of Boolean algebra in order to construct an algorithm for computing Gröbner bases in polynomial rings over a commutative von Neumann regular ring. We give a definition of prime ideals of Boolean algebra and the examples.

Definition 6 ([BS80])
An ideal I of a Boolean algebra is called a **prime ideal** if $1 \notin I$ and $a \wedge b \in I$ implies $a \in I$ or $b \in I$.

Example 7
Let $B(\mathbb{Q}^3) := \langle B, \wedge, \vee, \neg, 0, 1\rangle$. Then, prime ideals of $B(\mathbb{Q}^3)$ are

$$\begin{aligned} P_1 &:= \{(0, x_2, x_3) \mid x_2, x_3 \in \{0, 1\}\}, \\ P_2 &:= \{(x_1, 0, x_3) \mid x_1, x_3 \in \{0, 1\}\}, \\ P_3 &:= \{(x_1, x_2, 0) \mid x_1, x_2 \in \{0, 1\}\}. \end{aligned}$$

The set $Q_i := \{(x_1, 0, 0) \mid x_1 \in \{0, 1\}\}$ is not a prime ideal in $B(\mathbb{Q}^3)$, because $(1, 0, 1) \wedge (1, 1, 0) = (1, 0, 0) \in Q_1$, but $(1, 0, 1), (1, 1, 0) \neq Q_1$.

Proposition 8
For $i = 1, \ldots, n$ let $P_i = \{(x_1, \ldots, x_n) \in \{0, 1\}^n \mid x_i = 0\}$. The set of all prime ideals of $B(\mathbb{Q}^n) = \langle B, \wedge, \vee, \neg, 0, 1\rangle$ is $\{P_1, \ldots, P_n\}$ where $B = \{(x_1, \ldots, x_n) \mid x_i \in \{0, 1\}\}$.

Proof Let S be an arbitrary non-empty subset of $\{1, \cdots, n\}$. We denote for all $j \in S$,

$$I_j := \left\{(x_1, \ldots, x_n) \in \{0, 1\}^n \,\middle|\, x_j = 1\right\}.$$

Then, I_j is not an ideal in $B(\mathbb{Q}^n)$, because I_j does not satisfy definition 5 (3). Let L be an arbitrary subset of $\{1, \cdots, n\}$. Then we denote $I_L := \left\{(x_1, \ldots, x_n) \in \{0, 1\}^n \,\middle|\, x_j = 0, j \in L\right\}$. First we prove that if $|L| = 1$ ($|L|$ is the cardinality of L), then I_L is a prime ideal. Let $L = \{i\} \subseteq \{1, \ldots, n\}$, then a_i and b_i are the ith coordinate of $a, b \in B$. Take $a \wedge b \in I_L$, then $a_i \wedge b_i = 0$. Hence a_i or b_i must be 0. Therefore $a \in I_L$ or $b \in I_L$ and thus I_L is a prime ideal. Second, we prove that if $|L| > 1$, then I_L is not a prime ideal. Take $j_1, j_2 \in L$, $j_1 \neq j_2$. Let a_j be the jth coordinate of $a \in B$. Take $f \in \left\{(x_1, \ldots, x_n) \in \{0, 1\} \,\middle|\, x_{j_1} = 1, x_{j_2} = 0\right\}$ and $g = \left\{(x_1, \ldots, x_n) \in \{0, 1\}^n \,\middle|\, x_{j_1} = 0, x_{j_2} = 1\right\}$. Then $f \wedge g \in I_L$, but $f_{j_1} \wedge g_{j_1} = f_{j_2} \wedge g_{j_2} = 0$. Hence $f, g \notin I_L$. Therefore I_L is a prime ideal of $B(\mathbb{Q}^n)$. The set of all prime ideals of $B(\mathbb{Q}^n)$ is $\{P_1, \ldots, P_n\}$. ∎

Definition 9
An ideal I of a Boolean algebra B is called a **maximal** if there exists no ideal J with $I \subsetneq J \subsetneq B$.

Theorem 10 (Theorem 3.12 [BS80])
Let I be an ideal of $\mathbb{B} := \langle B, \wedge, \vee, \neg, 0, 1\rangle$. Then, I is a maximal ideal of $\mathbb{B}$ if and only if for any $a \in B$, exactly one of $a, \neg a$ belongs to I.

Lemma 11 (Corollary 3.13 [BS80])
Let I is an prime ideal of Boolean algebra $\langle B, \wedge, \vee, \neg, 0, 1\rangle$ if and only if I is a maximal ideal.

Proof (⇐) Suppose I is a maximal ideal with

$$a \wedge b \in I, \text{ for } a, b \in B.$$

As

$$(a \wedge b) \vee (\neg a \vee \neg b) = 1 \notin I,$$

we have

$$\neg a \vee \neg b \notin I,$$

hence,

$$\neg a \notin I \text{ or } \neg b \in I.$$

By theorem 10 either

$$a \in I \text{ or } b \in I.$$

(⇒) Since $0 \in I$, given $a \in B$ we have

$$a \wedge \neg a \in I.$$

Since I is a prime ideal,

$$a \in I \text{ or } \neg a \in I.$$

As

$$a \vee \neg a = 1 \notin I,$$

one of $a, \neg a$ belong to I. By theorem 10, I is a maximal ideal. ∎

For a Boolean algebra B, $\mathrm{Spec}(B)$ denotes the prime spectrum of B, i.e., the set of all prime ideals of B. The set of all maximal ideals of B is denoted by $\mathrm{St}(B)$. (Actually, in this case, by Lemma 11 we can say $\mathrm{Spec}(B) = \mathrm{St}(B)$.)

Theorem 12 (Saracino-Weispfenning[SW75])
For a maximal ideal I of $B(R)$, $I_R = \{xy \mid x \in R, y \in I\}$ (then I_R is a maximal ideal of R). If we define a map Φ from R into $\prod_{I \in St(B(R))} R/I_R$ by $\Phi(x) = \prod_{I \in \mathrm{St}(B(R))} [x]_{I_R}$, then Φ is a ring isomorphism.

An example of the theorem is the following.

Example 13
Let's consider $\mathbb{Q}^3$. From Proposition 8 and Lemma 11, we know $\mathrm{St}(B(\mathbb{Q}^3)) = \mathrm{Spec}(B(\mathbb{Q}^3)) = \{P_1, P_2, P_3\}$. Let $S_i := \{xy | x \in \mathbb{Q}^3, y \in P_i\}$ for each $i = 1, 2, 3$. Then, by Theorem 12, $\mathbb{Q}^3 \cong \mathbb{Q}^3/S_1 \times \mathbb{Q}^3/S_2 \times \mathbb{Q}^3/S_3$. Obviously, $\mathbb{Q}^3/S_3$ is isomorphic to $\mathbb{Q}$. By this identification Φ can be seen as the identity map on $\mathbb{Q}^3$.

Let $R_p := R/(p_R)$ where $p \in \mathrm{Spec}(B(R))$. Then for a subset Q of R and $p \in \mathrm{Spec}(B(R))$ we let $\Phi_p : R \longrightarrow R_p$ be the canonical homomorphism, and Q_p the image of Q under Φ_p.

Remark: Let P_1 be as in example 7. Obviously ${\mathbb{Q}^3}_{P_1}$ is isomorphic to $\mathbb{Q}$ and thus Φ_{P_1} can be seen as the projection map

$$\begin{aligned} \Phi_{P_1} : \mathbb{Q}^3 &\to \mathbb{Q}, \\ (a, b, c) &\mapsto (c), \end{aligned}$$

where $a, b, c \in \mathbb{Q}$.

3 Gröbner bases over von Neumann regular rings

Here, we describe the theory of Gröbner bases in polynomial rings over a commutative von Neumann regular ring. The theory has been studied by Weispfenning [Wei87]. Before describing the theory, we define the notations for $R[\bar{X}]$.

Definition 14
Let f be a non zero polynomial in $R[\bar{X}]$ and $\succ$ be an arbitrary order on the set of power products.

1. The **set of power products** of f that appear with a non-zero coefficient, is written $\mathrm{pp}(f)$.
2. The biggest power product of $\mathrm{pp}(f)$ with respect to $\succ$ is denoted by $\mathrm{lpp}(f)$ and is called the **leading power product** of g with respect to $\succ$.
3. The coefficient corresponding to $\mathrm{lpp}(f)$ is called **leading coefficient** of f with respect to $\succ$.
4. The product $\mathrm{lc}(f)\,\mathrm{lpp}(f)$ is called the **leading monomial** of f with respect to $\succ$.

Example 15
To illustrate, let $f = (2, 0, \frac{2}{3})xy^2z + (-1, -3, 0)z^2 + (\frac{1}{2}, 0, 5)x^3 + (3, 4, 0)x^2z^2$ in $\mathbb{Q}^3[x, y, z]$ and let $\succ$ denote the lexicographic order with $x \succ y \succ z$. Then, $\mathrm{pp}(f) = \{xy^2z, z^2, x^3, x^2z^2\}$, $\mathrm{lc}(f) = \left(\frac{1}{2}, 0, 5\right)$, $\mathrm{lpp}(f) = x^3$ and $\mathrm{lm}(f) = \left(\frac{1}{2}, 0, 5\right)x^3$.

In this section and the next section, Greek letters α, β, γ are used for power products, Roman letters a, b, c for elements of R, f, g, h for polynomials over a commutative von Neumann regular ring R. In order to describe the theory, we need a reduction system as the normal polynomial ring $K[\bar{X}]$. Note that R is not an integral domain.

Definition 16 (reduction [Wei87])
For a polynomial $f = a\alpha + g$ with $\mathrm{lm}(f) = a\alpha$, a monomial **reduction** $\to_f$ is defined as follows:

$$b\alpha\beta + h \to_f b\alpha\beta + h - ba^{-1}\beta(a\alpha + g) = (b\alpha\beta - ba^*\alpha\beta) + h - g$$

where $ab \neq 0$ (and $b\alpha\beta$ need not be the leading monomial of $b\alpha\beta + h$). (See Definition 1 for the notation a^*.)
Actually, we can repeat this reduction step until we have a polynomial which can not reduced by f. In this case, we use the notation $\overset{*}{\longrightarrow}_f$.

An example of the reduction is the following.

Example 17
Let $f = (2,0)x^2y + (2,1)y$, $g = (3,2)x^2y^2 \in \mathbb{Q}^2[x,y]$ with the lex-order $x \succ y$.

$$\begin{aligned} g &\longrightarrow_f g - (3,2)\cdot\left(\frac{1}{2},0\right)\cdot y \cdot f \\ &= (3,2)x^2y^2 - \left((3,0)x^2y^2 + (3,0)y^2\right) \\ &= (0,2)x^2y^2 + (-3,0)y^2 \end{aligned}$$

In the above example, we have $\mathrm{lpp}(g) = x^2y^2$, but after reduction by f, we have still $\mathrm{lpp}((0,2)x^2y^2 + (-3,0)y^2) = x^2y^2$. (Note that the first coordinate was reduced by f.) This property is not good for computing Gröbner bases in the ring, and thus we need the following definition.

Definition 18 (boolean closed [Wei87])
A polynomial f is called **boolean closed** if $(\mathrm{lc}(f))^* f = f$.

Example 19
Let $f = (0,-1)x^2y + (0,3)xy + (0,2)$ in $\mathbb{Q}^2[x,y]$. Then $(\mathrm{lc}(f))^* = (0,1)$, and $(\mathrm{lc}(f))^* f = f$. Hence f is a boolean closed polynomial.

A reduction $\rightarrow_F$ by a set F of polynomials in also naturally defined.

Remark: If polynomial g is not a boolean closed polynomial, then we have a problem which we have already seen in Example 17. Therefore, we need only boolean closed polynomials to compute reductions. If we have a non-boolean closed polynomial g, then we have to classify g into a set of boolean closed polynomials for computing reductions.

We are able to construct a set of boolean closed polynomials H from a given finite set of polynomials $F \subset R[\bar{X}]$ such that ideal $\langle F\rangle = \langle H\rangle$. Though H is not determined uniquely, we use the notation $\mathrm{BC}(F)$ (boolean closure of F) to denote one of such H. We need a set of boolean closed polynomials for reductions. The following algorithm provides a set $\mathrm{BC}(F)$ of boolean closed polynomials for a given subset F of $R[\bar{X}]$ such that $\langle F\rangle = \langle \mathrm{BC}(F)\rangle$.
Let q be a polynomial in $R[\bar{X}]$. We denote by $q - (\mathrm{lc}(q)^*)q$ the **boolean remainder** $\mathrm{br}(q)$ of q, and by $\mathrm{lc}(q)^* q$ the **boolean closure** $\mathrm{bc}(q)$ of q. So for $q \neq 0$, $\deg_{\bar{X}}(\mathrm{br}(q)) \leq \deg_{\bar{X}}(q)$ and $q = \mathrm{bc}(q) + \mathrm{br}(q)$.

Algorithm 20 ($\mathsf{BC}(F,\succ)$ **(Boolean Closure[Wei87]))**
Input: F: a finite set of polynomials in $R[\bar{X}]$, $\succ$: a term order on $\mathrm{pp}(\bar{X})$,
Output: Q: a finite set of boolean closed polynomials in $R[\bar{X}]$ with $\langle F\rangle = \langle Q\rangle$.
begin
$Q \longleftarrow \emptyset$; $H \longleftarrow F$
  while $H \neq \emptyset$ **do**
    Select g from H; $H \leftarrow H \backslash \{g\}$
    $Q \longleftarrow Q \cup \{\mathrm{bc}(g)\}$
    if $\mathrm{br}(g) \neq 0$ **then**
      $H \longleftarrow H \cup \{\mathrm{br}(g)\}$
    end-if
  end-while
return(Q)
end

Example 21
Let $f := (1,3,0)x^2y + (3,1,1)xy + (0,0,1)y + (-1,3,-2)$ and $g := (-1,0,2)x^2 + (-1,2,2)xy + (3,2,0)x + (2,0,0)$ in $\mathbb{Q}^3[x,y]$ and $\succ$ is the lexicographic order such that $x \succ y$. Then by the algorithm, we have

$$\begin{aligned} \mathrm{BC}(\{f\}) &= \{(1,3,0)x^2y + (3,1,0)xy + (-1,3,0), (0,0,1)xy + (0,0,1)y + (0,0,-2)\}, \\ \mathrm{BC}(\{g\}) &= \{(-1,0,2)x^2 + (-1,0,2)xy + (3,0,2)x + (2,0,0), (0,2,0)xy + (0,2,0)x\}. \end{aligned}$$

Hence, $\mathrm{BC}(\{f,g\}) = \mathrm{BC}(\{f\}) \cup \mathrm{BC}(\{g\})$.

Theorem 22 ([Wei87])
For any finite set F of polynomials, we can construct a finite set H of boolean closed polynomials such that ideal $\langle F \rangle = \langle H \rangle$.

We can naturally define Gröbner bases in $R[\bar{X}]$, like the case polynomial rings over a field $K[\bar{X}]$, as follows.

Definition 23
Gröbner bases]Fix a term order on $\mathrm{pp}(\bar{X})$. A finite set $G = \{g_1, \ldots, g_s\}$ of an ideal I is said to be a **Gröbner basis** for I with respect to $\succ$ if $\langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_l) \rangle = \mathrm{lm}(I)$.

Definition 24 (S-polynomial [Wei87])
For each pair of polynomials $f = a\alpha + f'$ and $g = b\beta + g'$ where $\mathrm{lm}(f) = a\alpha$, $\mathrm{lm}(g) = b\beta$. An **S-polynomial** of f and g (written : $\mathrm{SP}(f,g)$) is defined as follows:

$$\begin{aligned} \mathrm{SP}(f,g) &= b\frac{\mathrm{lcm}(\alpha,\beta)}{\beta} \cdot f - a\frac{\mathrm{lcm}(\alpha,\beta)}{\alpha} \cdot g \\ &= b\frac{\mathrm{lcm}(\alpha,\beta)}{\beta} \cdot f' - a\frac{\mathrm{lcm}(\alpha,\beta)}{\alpha} \cdot g'. \end{aligned}$$

Example 25
Let $f = (1,0,2)x^2y + (2,3,-1)xy + (2,1,0)y$, $g = (2,1,1)x^2 + (2,3,0)x + (1,1,1)y$ in $\mathbb{Q}^3[x,y]$. Then the S-polynomial of f and g are is:

$$\begin{aligned} \mathrm{SP}(f,g) &= (2,1,1) \cdot f - (1,0,2) \cdot g \\ &= (4,3,-1)xy + (4,1,0)y + (1,0,0)xy + (1,0,2)y^2 \\ &= (5,3,-1)xy + (1,0,2)y^2 + (4,1,0)y. \end{aligned}$$

Theorem 26 ([Wei87])
Let $G \subset R[\bar{X}]$ be a finite set of boolean closed polynomials. Then G is a Gröbner basis if and only if $\mathrm{SP}(f,g) \longrightarrow_G 0$ for any pair f and g of polynomials in G.

Now, we can construct an algorithm for computing Gröbner bases in $R[\bar{X}]$. This algorithm is essentially same as the Buchberger algorithm [Buc65]. We remark again that R is not an integral domain.

Algorithm 27 ($\mathsf{GBovN}(F, \succ)$ **(Gröbner basis over a von Neumann regular ring))**
Input: F: a finite list of polynomials in $R[\bar{X}]$, $\succ$: a term order on $\mathrm{pp}(\bar{X})$,
Output: G: Gröbner basis of $\langle F \rangle$ with respect to $\succ$ in $R[\bar{X}]$ with $\langle F \rangle = \langle G \rangle$
begin

$G \longleftarrow \mathrm{BC}(F, \succ)$; $C \longleftarrow \{\{g, f\} | g, f \in G\}$
while $C \neq \emptyset$ **do**
Select $\{h_1, h_2\}$ from C; $C \leftarrow C \backslash \{\{h_1, h_2\}\}$
if $\mathrm{SP}(h_1, h_2)\downarrow_G \neq 0$ **then**
$G \longleftarrow G \cup \mathrm{BC}(\mathrm{SP}(h_1, h_2)\downarrow_G, \succ)$ (see below $(*)$)
$B \longleftarrow \{(f, k) | k \in \mathrm{BC}(\mathrm{SP}(h_1, h_2)\downarrow_G, \succ), f \in G\}$
$C \longleftarrow C \cup B$
end-if
end-while
return(G)
end
($(*)$ $h\downarrow_F$ denotes a normal form of h modulo $\rightarrow_F$, i.e., $h\downarrow_F$ is irreducible modulo $\rightarrow_F$.)

If a finite set G is a Gröbner basis and reduced, then G is called **reduced Gröbner basis** (i.e., $\forall p \in G$, p cannot be reduced by $G \backslash \{p\}$). We have the following property.

Theorem 28 ([Wei87])
Let G be a reduced Gröbner basis, then any element of G is boolean closed.

In $K[\bar{X}]$, reduced Gröbner bases serve us as canonical forms of Gröbner bases, however we have to be careful in $R[\bar{X}]$.

Definition 29 ([Sat98])
A polynomial f is called **monic** if it satisfies $\mathrm{lc}(f) = (\mathrm{lc}(f))^*$.

Definition 30 ([Sat98, Wei87])
A reduced Gröbner basis $G \subset R[\bar{X}]$ is called a **stratified** Gröbner basis, when it satisfies the following two properties.

1. Every element of G is monic.
2. $\mathrm{lpp}(f) \neq \mathrm{lpp}(g)$ for any distinct elements f and g of G.

Theorem 31 ([Wei87])
A stratified Gröbner basis is determined uniquely, i.e., two stratified Gröbner bases $G, G' \subset R[\bar{X}]$ with $\langle G \rangle = \langle G' \rangle$ must be identical.

Remember that in Theorem 12, I_R depends on I. So let $R_p := R/(p_R)$ where $p \in \mathrm{Spec}(B(R))$. Then for a subset Q of R and $p \in \mathrm{Spec}(B(R))$ we let $\Phi_p : R \rightarrow R_p$ be the canonical homomorphism, and Q_p the image of Q under Φ_p. The following theorem is quite important for constructing (alternative) comprehensive Gröbner bases. In the next theorem, we use the notations R_p and $G_p := \Phi(G)$.

Theorem 32 (Weispfenning [Wei87])
Let G be a finite set of non-zero polynomials in $R[\bar{X}]$.

1. If G is a set of boolean closed polynomials, then G is a Gröbner basis if and only if for all $p \in \mathrm{Spec}(B(R))$, G_p in a Gröbner basis in $R_p[\bar{X}]$.
2. G is a reduced Gröbner basis if and only if G is a set of boolean closed polynomials and for all $p \in \mathrm{Spec}(B(R))$, G_p is a reduced Gröbner basis in $R_p[\bar{X}]$.
3. If for all $h \in R[\bar{X}]$, G is a Gröbner basis, then $(h\downarrow_G)_p = h_p \downarrow_{G_p}$.

4 Criteria for computing Gröbner bases

In [Buc79, Buc70], Buchberger has introduced criteria for computing Gröbner bases in $K[\bar{X}]$. It is possible to generalize the criteria to $R[\bar{X}]$. In this section, we present criteria for computing Gröbner bases in $R[\bar{X}]$. That is, we describe techniques for removing unnecessary critical pairs. By the criteria, we can improve algorithm 27 for computing Gröbner bases efficiently.

Theorem 33 (First Criterion)
Let f and g be non-zero boolean closed polynomials in $R[\bar{X}]$. If f and g have $\mathrm{lc}(f)\,\mathrm{lc}(g) = 0$ or disjoint leading power products, then $\mathrm{SP}(f,g) \xrightarrow{*}_{\{f,g\}} 0$.

Proof If $\mathrm{lc}(f)\,\mathrm{lc}(g) = 0$, then by Definition 24, $\mathrm{SP}(f,g) = 0$. Assume that f and g have disjoint leading power products. For all $p \in \mathrm{Spec}(B(R))$, then we have f_p, g_p in $R_p[\bar{X}]$. If one of f_p and g_p is 0, then $\mathrm{SP}(f,g)_p = 0$ in $R_p[\bar{X}]$. (R is not an integral domain.) If $f_p \neq 0$ and $g_p \neq 0$, then we can apply the original Buchberger's criterion [Buc79]. Hence, we have $\mathrm{SP}(f_p, g_p) \xrightarrow{*}_{\{f_p,g_p\}} 0$ in $R_p[\bar{X}]$. Therefore, $\{f_p, g_p\}$ is a Gröbner basis for ideal $\langle f_p, g_p\rangle$ in $R_p[\bar{X}]$. By Theorem 32, $\{f,g\}$ is a Gröbner basis in $R[\bar{X}]$. Therefore, $\mathrm{SP}(f,g) \xrightarrow{*}_{\{f,g\}} 0$. ∎

Theorem 34 (Second Criterion)
Let p, g_1 and g_2 be non-zero boolean closed polynomials in $R[\bar{X}]$ such that the following hold:

1. $\mathrm{lpp}(p) | \mathsf{LCM}(\mathrm{lpp}(g_1), \mathrm{lpp}(g_2))$, and
2. $\mathrm{lc}(g_1)^* \,\mathrm{lc}(p)^* \,\mathrm{lc}(g_2)^* = \mathrm{lc}(g_1)^* \,\mathrm{lc}(g_2)^*$.

Then, $\mathrm{SP}(g_1, g_2)$ is generated by an ideal $\langle \mathrm{SP}(g_1,p), \mathrm{SP}(g_2,p)\rangle$ in $R[\bar{X}]$. That is, $\mathrm{SP}(g_1,g_2) \in \langle \mathrm{SP}(g_1,p), \mathrm{SP}(g_2,p)\rangle$.

Proof We have the following equation (which is an easy exercise).

$$\begin{aligned}
&\mathrm{lc}(p)^* \frac{\mathsf{LCM}(\mathrm{lpp}(g_1), \mathrm{lpp}(g_2), \mathrm{lpp}(p))}{\mathsf{LCM}(\mathrm{lpp}(g_1), \mathrm{lpp}(g_2))}\,\mathrm{SP}(g_1,g_2) \\
&\quad + \mathrm{lc}(g_2)^* \frac{\mathsf{LCM}(\mathrm{lpp}(g_1), \mathrm{lpp}(g_2), \mathrm{lpp}(p))}{\mathsf{LCM}(\mathrm{lpp}(g_1), \mathrm{lpp}(p))}\,\mathrm{SP}(g_1,p) \\
&\quad + \mathrm{lc}(g_1)^* \frac{\mathsf{LCM}(\mathrm{lpp}(g_1), \mathrm{lpp}(g_2), \mathrm{lpp}(p))}{\mathsf{LCM}(\mathrm{lpp}(g_2), \mathrm{lpp}(p)}\,\mathrm{SP}(g_2,p) = 0.
\end{aligned}$$

Since $\mathrm{lpp}(p) | \mathsf{LCM}(\mathrm{lpp}(g_1), \mathrm{lpp}(g_2))$, we have

$$\mathsf{LCM}(\mathrm{lpp}(g_1), \mathrm{lpp}(g_2), \mathrm{lpp}(p)) = \mathsf{LCM}(\mathrm{lpp}(g_1), \mathrm{lpp}(g_2)).$$

By the above equations, we have

$$\begin{aligned}
&\mathrm{lc}(p)^*\,\mathrm{SP}(g_1,g_2) + \mathrm{lc}(g_2)^* \frac{\mathsf{LCM}(\mathrm{lpp}(g_1), \mathrm{lpp}(g_2), \mathrm{lpp}(p))}{\mathsf{LCM}(\mathrm{lpp}(g_1), \mathrm{lpp}(p))}\,\mathrm{SP}(g_1,p) \\
&\quad + \mathrm{lc}(g_1)^* \frac{\mathsf{LCM}(\mathrm{lpp}(g_1), \mathrm{lpp}(g_2), \mathrm{lpp}(p))}{\mathsf{LCM}(\mathrm{lpp}(g_2), \mathrm{lpp}(p)}\,\mathrm{SP}(g_2,p) = 0. \qquad (*)
\end{aligned}$$

By the definition of S-polynomial and the assumption 2, we have

$$\mathrm{lc}(p)^*\,\mathrm{SP}(g_1,g_2) = \mathrm{SP}(g_1,g_2).$$

Hence, the equation $(*)$ can be transformed as follows :

$$\begin{aligned}\mathrm{SP}(g_1,g_2) &= -\mathrm{lc}(g_2)^* \frac{\mathsf{LCM}(\mathrm{lpp}(g_1),\mathrm{lpp}(g_2),\mathrm{lpp}(p))}{\mathsf{LCM}(\mathrm{lpp}(g_1),\mathrm{lpp}(p))}\,\mathrm{SP}(g_1,p)\\ &\quad -\mathrm{lc}(g_1)^* \frac{\mathsf{LCM}(\mathrm{lpp}(g_1),\mathrm{lpp}(g_2),\mathrm{lpp}(p))}{\mathsf{LCM}(\mathrm{lpp}(g_2),\mathrm{lpp}(p)}\,\mathrm{SP}(g_2,p)\\ &\quad \in \langle \mathrm{SP}(g_1,p),\mathrm{SP}(g_2,p)\rangle.\end{aligned}$$

∎

We have the next corollary which directly follows from theorem 34

Corollary 35
Let g_1, p, g_2 and p_i be polynomials in $R[\bar{X}]$ for each $i = 1, 2, \ldots l$ such that the following holds:

1. $\mathrm{lpp}(p_i)|\mathsf{LCM}(\mathrm{lpp}(g_1),\mathrm{lpp}(g_2))$ for each $i = 1, 2, \ldots l$, and
2. $(\mathrm{lc}(p_1)^* \vee \mathrm{lc}(p_2)^* \vee \ldots \vee \mathrm{lc}(p_l)^*)\,\mathrm{lc}(g_1)^*\,\mathrm{lc}(g_2)^* = \mathrm{lc}(g_1)^*\,\mathrm{lc}(g_2)^*$.

Then, $\mathrm{SP}(g_1,g_2)$ is generated by an ideal
$\langle \mathrm{SP}(g_1,p_1),\ldots,\mathrm{SP}(g_1,g_l),\mathrm{SP}(g_2,p_1),\ldots,\mathrm{SP}(g_2,p_l)\rangle$ in $R[\bar{X}]$. Note that notation $\vee$ is sum of boolean algebra. i.e. $a \vee b = a + b - ab$.

The next algorithm is required by algorithm 37 ImprovedGB, and contains two criteria above. The following algorithm removes unnecessary critical pairs in $R[\bar{X}]$. The foundation algorithm of algorithm 36 is UPDATE of [BW93](pp.230). The original algorithm UPDATE [BW93] is improved for the polynomial ring $R[\bar{X}]$ by the two criteria. The new algorithm which is the following, is called UPDATE, again. The termination argument follows the original UPDATE.

Algorithm 36 (UPDATE($G_{old}, B_{old}, h, \succ$) **(Update of a set of critical pairs and basis))**
Input: G_{old}: a finite subset in $R[\bar{X}]$, B_{old}: a finite set of critical pairs in $R[\bar{X}]$,
h : a non-zero polynomial $\in R[\bar{X}]$, $\succ$: a term order on $\mathrm{pp}(\bar{X})$,
Output: G_{new}: updates of G_{old}, B_{new}: update of B_{old}.
begin
$C \longleftarrow \{\{h,g\}|g \in G_{old}\}$; $D \longleftarrow \emptyset$; $E \longleftarrow \emptyset$
while $C \neq \emptyset$ **do**
Select $\{h,g\}$ from C
  if $\mathrm{lc}(h)^*\,\mathrm{lc}(g)^* = 0$ **then**
    $C \leftarrow C\backslash\{\{h,g\}\}$
  else
    $E \leftarrow E \cup \{\{h,g\}\}$; $C \leftarrow C\backslash\{\{h,g\}\}$
  end-if
end-while
while $E \neq \emptyset$ **do**
Select $\{h,g_1\}$ from C; $E \leftarrow E\backslash\{\{h,g_1\}\}$
  if lpp(h) and lpp(g_1) are disjoint **or**
  $\Big(\mathsf{LCM}(\mathrm{lpp}(h),\mathrm{lpp}(g_2)) \nmid \mathsf{LCM}(\mathrm{lpp}(h),\mathrm{lpp}(g_1))\forall\{h,g_2\} \in E$ **and**
    $\mathsf{LCM}(\mathrm{lpp}(h),\mathrm{lpp}(g_2)) \nmid \mathsf{LCM}(\mathrm{lpp}(h),\mathrm{lpp}(g_1))\forall\{h,g_2\} \in D\Big)$ **then**
  $D \leftarrow D \cup \{\{h,g_1\}\}$
  end-if
end-while
$F \longleftarrow \emptyset$
while $D \neq \emptyset$ **do**
select $\{h,g\}$ from D ; $D \leftarrow D\backslash\{\{h,g\}\}$

if lpp(h) and lpp(g) are not disjoint **then**
$F \leftarrow F \cup \{\{h, g\}\}$
end-if
end-while
$B_{new} \leftarrow \emptyset$
while $B_{old} \neq \emptyset$ **do**
Select $\{g_1, g_2\}$ from B_{old}; $B_{old} \leftarrow B_{old} \backslash \{\{g_1, g_2\}\}$
if $\mathrm{lpp}(h) \nmid \mathsf{LCM}(\mathrm{lpp}(g_1), \mathrm{lpp}(g_2))$ **or** $\mathsf{LCM}(\mathrm{lpp}(g_1), \mathrm{lpp}(h)) = \mathsf{LCM}(\mathrm{lpp}(g_1), \mathrm{lpp}(g_2))$
or $\mathsf{LCM}(\mathrm{lpp}(h), \mathrm{lpp}(g_2)) = \mathsf{LCM}(\mathrm{lpp}(g_1), \mathrm{lpp}(g_2))$ **then**
$B_{new} \leftarrow B_{new} \cup \{\{g_1, g_2\}\}$
elif $\mathrm{lc}(h)^* \mathrm{lc}(g_1)^* \mathrm{lc}(g_2)^* \neq \mathrm{lc}(g_1)^* \mathrm{lc}(g_2)^*$ **then**
$B_{new} \leftarrow B_{new} \cup \{\{g_1, g_2\}\}$
end-elif
end-if
$B_{new} \leftarrow B_{new} \cup F$; $G_{new} \leftarrow \emptyset$
while $G_{old} \neq \emptyset$ **do**
select g from G_{old}; $G_{old} \leftarrow G_{old} \backslash \{g\}$
if $\mathrm{lpp}(h) \nmid \mathrm{lpp}(g)$ **then**
$G_{new} \leftarrow G_{new} \cup \{g\}$
end-if
end-while
$G_{new} \leftarrow G_{new} \cup \{h\}$
end-while
return(G_{new}, B_{new})
end

Finally, we construct an algorithm which is more efficient than algorithm 27. Let F be a finite subset of $R[\bar{X}]$ with a order and $\succ$ a term order on $\mathrm{pp}(\bar{X})$. Then, the following algorithm outputs a reduced Gröbner basis G in $R[\bar{X}]$ such that $\langle F \rangle = \langle G \rangle$, and eliminates superfluous critical pairs according to the first and second criterion.

Algorithm 37 (ImprovedGB($F, \succ$))
Input: F : a finite list of polynomials in $R[\bar{X}]$, $\succ$: a term order on $\mathrm{pp}(\bar{X})$,
Output: G : Gröbner bases of F in $R[\bar{X}]$ with $\langle F \rangle = \langle G \rangle$.
begin
$L \leftarrow \mathrm{BC}(F, \succ)$; $G \leftarrow \emptyset$; $B \leftarrow \emptyset$
while $L \neq \emptyset$ **do**
Select g from L; $L \leftarrow L \backslash \{g\}$; $(G, B) \leftarrow \mathrm{UPDATE}(G, B, g, \succ)$
end-while
while $B \neq \emptyset$ **do**
Select $\{g_1, g_2\}$ from B; $B \leftarrow L \backslash \{\{g_1, g_2\}\}$; $h \leftarrow \mathrm{SP}(g_1, g_2)\downarrow_G$
if $h \neq 0$ **then**
$H \leftarrow \mathrm{BC}(\{h\}, \succ)$
while $H \neq \emptyset$ **do**
Select h_1 from H; $H \leftarrow H \backslash \{h_1\}$; $(G, B) \leftarrow \mathrm{UPDATE}(G, B, h_1, \succ)$
end-while
end-if end-while
return(G)
end

5 Alternative comprehensive Gröbner bases

Here we describe alternative comprehensive Gröbner bases (ACGB). Alternative comprehensive Gröbner bases are based on the theory of polynomial rings over commutative von Neumann regular rings. The idea is the following. In this section, we assume that K **is always an infinite field**. Let $f_1(\bar{A}, \bar{X}), \ldots, f_k(\bar{A}, \bar{X})$ be polynomials in $K[\bar{A}, \bar{X}]$ with parameters $\bar{A} = \{A_1, \ldots, A_m\}$ and variables $\bar{X} = \{X_1, \ldots, X_n\}$. Consider each polynomial $f(\bar{A})$ in $K[\bar{A}]$ as function from K^m to K, then $f_1(\bar{A}, \bar{X}), \ldots, f_k(\bar{A}, \bar{X})$ become polynomials in the polynomial ring $K^{K^m}[\bar{X}]$ over a von Neumann regular ring K^{K^m}.
This idea leads us to define an alternative Comprehensive Gröbner basis (ACGB).

Definition 38 ([SS03])
Let F be a finite set of polynomials in a polynomial ring $K[\bar{A}, \bar{X}]$ over K with variables $\bar{A} = \{A_1, \ldots, A_m\}$ and $\bar{X} = \{X_1, \ldots, X_n\}$. Let G be a Gröbner basis of $\langle F \rangle$ in a polynomial ring $\bar{K}^{\bar{K}^m}[\bar{X}]$. G is called an **alternative comprehensive Gröbner basis (ACGB)** of F with parameters $\bar{A}$ in $\bar{K}[\bar{X}]$. ($\bar{K}$ is an algebraic closure of K.)

Remark: In order to enable the above Gröbner bases computation, it suffices to establish a way to handle the smallest commutative von Neumann regular ring extending the canonical image of $K[\bar{A}]$. If the rational field $K(\bar{A})$ would correspond to it, the situation would be very nice. Unfortunately, it does not work. Consider the inverse ${A_1}^{-1}$ of A_1 in the commutative von Neumann regular ring K^{K^m}. Since $A_1(a_1, \ldots, a_m) = a_1$ for any $a_1, \ldots, a_m \in K$, ${A_1}^{-1}$ should be the function ϕ from $K^m \to K$ such that $\phi(0, a_2, \ldots, a_m) = 0$ and $\phi(a_1, \ldots, a_m) = \frac{1}{a_1}$ if $a_1 \neq 0$. Certainly ϕ is not a member of $K(\bar{A})$.

Example 39 ([SS03])
Let t be a function $\mathbb{C}^2$ to $\mathbb{C}$ defined by

$$t(a,b) = \begin{cases} a-b, & \text{if } (a,b) \in \mathbb{C}^2 \backslash \mathbb{V}(a-b), \\ 0, & \text{otherwise.} \end{cases}$$

The inverse is

$$t(a,b) = \begin{cases} \frac{1}{a-b}, & \text{if } (a,b) \in \mathbb{C}^2 \backslash \mathbb{V}(a-b), \\ 0, & \text{otherwise.} \end{cases}$$

The addition of t and t^{-1} is

$$(t + t^{-1})(a,b) = \begin{cases} \frac{a^2-2ab+b^2+1}{a-b}, & \text{if } (a,b) \in \mathbb{C}^2 \backslash \mathbb{V}(a-b), \\ 0, & \text{otherwise.} \end{cases}$$

The multiplication

$$(t \cdot t^{-1})(a,b) = \begin{cases} 1, & \text{if } (a,b) \in \mathbb{C}^2 \backslash \mathbb{V}(a-b), \\ 0, & \text{otherwise.} \end{cases}$$

Actually, we would like to apply Theorem 32 for constructing an algorithm for computing ACGB in $\bar{K}^{\bar{K}^m}[\bar{X}]$. What is a prime ideal in $B(\bar{K}^{\bar{K}^m})$?

Proposition 40
The form of all prime ideals is the following:

$$\forall \alpha \in \bar{K}^m, T_\alpha := \left\{ t \in \bar{K}^{\bar{K}^m} \,\middle|\, t(\alpha) = 0, t(\beta) \in \{0,1\}, \forall \beta \in K^m \backslash \{\alpha\} \right\} \quad (*).$$

Proof **(Ideal)** First, we prove that T_α is an ideal in $B(\bar{K}^{\bar{K}^m})$. It is obviously $0 \in T_\alpha$. Take f, g from T_α, then $f(\alpha) = 0$ and $g(\alpha) = 0$. Hence, we have $(f \vee g)(\alpha) = (f + g - fg)(\alpha) = f(\alpha) + g(\alpha) - f(\alpha)g(\alpha) = 0$. This fact implies $f \vee g \in T_\alpha$. (Note that K is a infinite field, and the function $K^m \to K$ is a injection.) Take f from T_α and $h \in B(\bar{K}^{\bar{K}^m})$. We have $(h \wedge f)(\alpha) = 0$ since $f(\alpha) = 0$. Therefore, T_α is an ideal in $B(\bar{K}^{\bar{K}^m})$.
(Prime) We prove that T_α is a prime ideal. Take $f \wedge g \in T_\alpha$, then $(f \wedge g)(\alpha) = f(\alpha) \wedge g(\alpha) = 0$. Therefore, $f(\alpha) = 0$ or $g(\alpha) = 0$, this means $f \in T_\alpha$ or $g \in T_\alpha$. T_α is a prime ideal.
Next we prove that all prime ideals of $B(\bar{K}^{\bar{K}^m})$ has the form $(*)$. This means that any function q from T_α is always zero at only **one** point α. This prove is essentially same as Example 8. Let's consider the following set;
$\forall \alpha_1, \ldots, \alpha_i \in K^m$ with $\alpha_j \neq \alpha_l$, $j, l \in \{1, \ldots, i\}$ and $j \neq l$,

$$T_{(\alpha_1,\ldots,\alpha_i)} := \left\{ t \in \bar{K}^{\bar{K}^m} \,\middle|\, t(\alpha_1) = 0, \ldots, t(\alpha_i) = 0, t(\beta) \in \{0,1\}, \forall \beta \in \bar{K}^m \backslash \{\alpha_1, \ldots, \alpha_i\} \right\}.$$

That is, any function q from T_i is always zero at only i points.
Let $i = 2$. Take $f \wedge g \in T_2$, then $f(\alpha_1) \wedge g(\alpha_1) = 0$ and $f(\alpha_2) \wedge g(\alpha_2) = 0$. Let us consider the following function;

$$F := \left\{ h \in \bar{K}^{\bar{K}^m} \,\middle|\, h(\alpha_1) = 0, h(\alpha_2) = 1, t(\beta) \in \{0,1\}, \forall \beta \in \bar{K}^m \backslash \{\alpha_1, \alpha_2\} \right\},$$

and

$$G := \left\{ h \in \bar{K}^{\bar{K}^m} \,\middle|\, h(\alpha_1) = 1, h(\alpha_2) = 0, t(\beta) \in \{0,1\}, \forall \beta \in \bar{K}^m \backslash \{\alpha_1, \alpha_2\} \right\}.$$

Take $f_1 \in F$ and $g_1 \in G$. Then $f_1 \wedge g_1 \in T_2$, but $f_1, g_1 \notin T_2$. Hence, $T_{(\alpha_1,\alpha_2)}$ is not a prime ideal. Even if $i > 2$, $T_{(\alpha_1,\ldots,\alpha_i)}$ is not a prime ideal in $B(\bar{K}^{\bar{K}^m})$. This proof is the same as the case $i = 2$. Therefore, the form T_α is only the prime ideal in $B(\bar{K}^{\bar{K}^m})$. ∎

We define a computable ring T and operations on T which witness that T forms a von Neumann regular ring. For an arbitrary polynomial $f \in K[\bar{A}]$, we can consider it as a mapping $f : \bar{K}^m \to \bar{K}$, i.e., $f \in \bar{K}^{\bar{K}^m}$. Therefore, we can define the canonical embedding

$$\varphi : K[\bar{A}] \to \bar{K}^{\bar{K}^m}.$$

Let T be the closure of the image $\varphi(K[\bar{A}])$ under addition, multiplication, and inverse in the von Neumann regular ring $\bar{K}^{\bar{K}^m}$, thus T becomes a von Neumann regular ring.
Let's define the following map

$$\begin{aligned} \mathrm{ter}_T : K[\bar{A}][\bar{X}] &\to T[\bar{X}], \\ c_1\alpha_1 + \cdots + c_l\alpha_l &\mapsto \mathrm{ter}_T(c_1)\alpha_1 + \cdots + \mathrm{ter}_T(c_l)\alpha_l, \end{aligned}$$

where $c_1, \ldots, c_l \in K[\bar{A}]$ and $\alpha_1, \ldots, \alpha_l \in \mathrm{pp}(\bar{X})$.

We know the form of all prime ideals. Therefore, if we have $B(T)$ in Theorem 32, then the theorem means the following.

Theorem 41
Let $F = \{f_1(\bar{A}, \bar{X}), \ldots, f_s(\bar{A}, \bar{X})\}$ be a set of polynomials in $K[\bar{A}][\bar{X}]$ (where $\bar{A}$ are parameters and $\bar{X}$ are variables). Furthermore, let $G = \{g_1, \ldots, g_l\}$ be the reduced Gröbner basis of $\mathrm{ter}_T(F)$ in $T[\bar{X}]$. Then, for each m-tuple $\bar{a} = (a_1, \ldots, a_m) \in \bar{K}^m$, $G_{\bar{a}}$ becomes the reduced Gröbner basis of the ideal $\langle f_1(\bar{a}, \bar{X}), \ldots, f_s(\bar{a}, \bar{X})\rangle$ in $\bar{K}[\bar{X}]$. Here $G_{\bar{a}}$ denotes the set $\{g_{1\bar{a}}, \ldots, g_{l\bar{a}}\}$ of polynomials $g_{1\bar{a}}, \ldots, g_{l\bar{a}}$ in $\bar{K}[\bar{X}]$ given from $g_1, \ldots, g_l$ by replacing each coefficient c with $c(\bar{a})$. (Remember that c is an element of T).

By the above theorem, Gröbner bases satisfy the main property of comprehensive Gröbner bases. Therefore, they are called "alternative comprehensive Gröbner bases". In fact, we need to define the algebraic structure of T to compute a Gröbner bases in $T[\bar{X}]$. That is, we need addition, multiplication, and inverse in the von Neumann regular ring T. In [SS02, SS03], they are introduced and defined. In this thesis, we do not describe them. If one is interested in the detail, the author strongly recommends to see [SS03]. In the algebraic structure of T, the following definitions are required for computing Gröbner bases in $T[\bar{X}]$. In the next section, the notations of the following definition will be applied for describing the special types of comprehensive Gröbner bases. Therefore, we give the following two definitions.

Definition 42 (preterrace [SS03])
A triple (s, t, r) is called a preterrace on $K[\bar{A}]$ if s and t are finite sets of polynomials in $K[\bar{A}]$ and $r = \frac{g}{h}$ for some $g, h \in K[\bar{A}]$ which satisfy

1. $\mathbb{V}(s) \subseteq \mathbb{V}(t)$,
2. $(\mathbb{V}(\{g\}) \cup \mathbb{V}(\{h\})) \cap (\mathbb{V}(t) \backslash \mathbb{V}(s)) = \emptyset$, i.e., $g(\bar{a}) \neq 0$ and $h(\bar{a}) \neq 0$ for any $\bar{a} \in \mathbb{V}(t) \backslash \mathbb{V}(s)$.

For a given preterrace $p = (s, t, r)$, the **support** of p (written: $\mathrm{supp}(p)$) is the set of $\mathbb{V}(t) \backslash \mathbb{V}(s) \subseteq K^m$. For a preterrace $p = (s, t, \frac{g}{h})$ on $K[\bar{A}]$ and $\bar{a} \in K^m$, we define $p(\bar{a}) \in K$ by

$$p(\bar{a}) = \begin{cases} \frac{g(\bar{a})}{h(\bar{a})}, & \text{if } \bar{a} \in \mathrm{supp}(p) = \mathbb{V}(t) \backslash \mathbb{V}(s), \\ 0, & \text{otherwise.} \end{cases}$$

Therefore, p can be consider as a member of T.

Definition 43 (terrace [SS03])
A finite set $\{p_1, \ldots, p_l\}$ is called a **terrace** on $K[\bar{A}]$ of each p_i (i=1,. . . ,l)is a preterrace on $K[\bar{A}]$ such that $\succ (p_i) \neq \emptyset$ and $\mathrm{supp}(p_i) \cap \mathrm{supp}(p_j) = \emptyset$ for any distinct $i, j \in \{1, \ldots, l\}$. The support of a terrace t is defined by

$$\mathrm{supp}(t) = \bigcup_{p \in t} \mathrm{supp}(p) \subseteq K^m.$$

Example 44
Let $f = abx^2y + x + by$, $g = y^2 + ax + b$ be polynomials in $\mathbb{C}[a, b][x, y]$. We consider the map $\mathrm{ter}_t : \mathbb{C}[a, b][x, y] \to T_{(a,b)}[x, y]$ where $T_{(a,b)}$ is the von Neumann regular ring of equivalence class on terrace on $\mathbb{C}[a, b]$. Then,

$$\begin{aligned} \mathrm{ter}_T(f) &= [(\mathbb{C}^2 - \mathbb{V}(ab), ab)]x^2y + [(\mathbb{C}^2, 1)]x + [(\mathbb{C}^2 - \mathbb{V}(b), b)]y, \\ \mathrm{ter}_T(g) &= [(\mathbb{C}^2, 1)]y^2 + [(\mathbb{C}^2 - \mathbb{V}(a), a)]x + [(\mathbb{C}^2 - \mathbb{V}(b), b)]1. \end{aligned}$$

The one of coefficients $[(\mathbb{C}^2 - \mathbb{V}(ab), ab)]$ means

$$\begin{cases} ab, & \text{if } ab \neq 0, \\ 0, & \text{otherwise.} \end{cases}$$

One can notice that every coefficients has the parametric spaces and elements of $\mathbb{C}[a, b]$. That is, every coefficients has preterraces (see Definition 42).

Now, since we know algorithm 37, Theorem 41 and the structure of $T[\bar{X}]$ (which is from [SS03]), we can construct an algorithm for computing alternative comprehensive Gröbner bases.

Algorithm 45 ($\mathsf{ACGB}(F, \succ)$ **(Alternative Comprehensive Gröbner Bases))**
Input F : a subset of $K[\bar{A}][\bar{X}]$, $\succ$: a term order on $\mathrm{pp}(\bar{X})$,
Output G : an alternative comprehensive Gröbner basis for $\langle F \rangle$ with respect to $\succ$.

1. Compute $\mathrm{ter}_T(F)$.
2. Compute a Gröbner basis G for $\langle \mathrm{ter}_T(F) \rangle$ with respect to $\succ$ in $T[\bar{X}]$ by the algorithm 37 where T is a commutative von Neumann regular ring.
3. G is an alternative comprehensive Gröbner basis for $\langle F \rangle$ with respect to $\succ$.

In Figure 1, we give the rough procedure of algorithm 45.

Alternative comprehensive Gröbner bases have the following nice property, which do not hold in standard comprehensive Gröbner bases [SS03].

"There exists a canonical form of an alternative comprehensive Gröbner basis in a natural way."

Since an alternative comprehensive Gröbner basis is already in a form of a Gröbner basis in a polynomial ring over a commutative von Neumann regular ring, we can use a stratified Gröbner basis as a canonical form an alternative comprehensive Gröbner basis. By the same reason above, we can use reductions of an alternative comprehensive Gröbner basis.

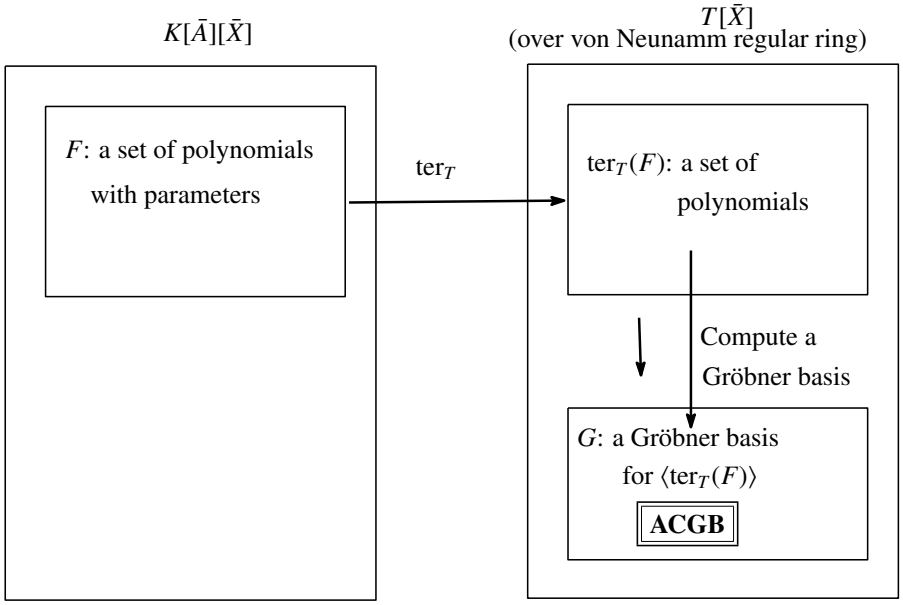

Figure 1 A computation method for ACGB

The algorithm ACGB has been implemented in the computer algebra systems Risa/Asir by Suzuki in [SS03]. In the following example, we give the outputs of the program.

Example 46
Let $F = \{bx^2y + 3, axy^2 + bxy + b\}$ be a set of polynomials in $\mathbb{C}[a, b][x, y]$, a, b parameters, x, y variables and $\succ$ the graded reverse lexicographic order such that $x \succ y$. The Suzuki's program outputs the following as an alternative comprehensive Gröbner basis for $\langle F \rangle$ with respect to $\succ$;

```
[[(V[b],1)]*1,
[(V[b*a]-V[b],1)]*y+[(V[b*a]-V[b],1/3*b)]*1,
[(V[0]-V[b*a],1),(V[b*a]-V[b],1)]*x+[(V[0]-V[b*a],(-3*a)/(b^2))]*y+[(V[0]
-V[b*a],(-3)/(b)),(V[b*a]-V[b],(-3)/(b))]*1,
[(V[0]-V[b*a],1)]*y^3+[(V[0]-V[b*a],(2*b)/(a))]*y^2+[(V[0]-V[b*a],(b^2)/(
a^2))]*y+[(V[0]-V[b*a],(1/3*b^3)/(a^2))]*1].
```

We can understand the output as follows;

$$\begin{cases} \{1\}, & \text{if } b = 0, \\ \{y + \frac{1}{3}b, x - \frac{1}{b}\}, & \text{if } ab = 0, b \neq 0, \\ \{x + y - \frac{3}{b}, y^3 + \frac{2b}{a}y^2 + \frac{b^2}{a^2}y + \frac{b^3}{3a^2}\}, & \text{if } ab \neq 0. \end{cases}$$

6 ACGB on varieties (ACGB-V)

In this section, we present a special type of ACGB which is called ACGB-V (ACGB on Varieties). When there exists a constraint of parameters $\bar{A}$ 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 $\mathbb{V}(f_1(\bar{A}), \ldots,$

$f_l(\bar{A})$) than a whole space K^m. 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 $K[\bar{A}]$ in K^{K^m}. When such constrains exists, we can replace K^{K^m} by $K^{\mathbb{V}(f_1(\bar{A}),\ldots,f_l(\bar{A}))}$. Note that the restriction of $K[\bar{A}]$ on $K^{\mathbb{V}(f_1(\bar{A}),\ldots,f_l(\bar{A}))}$ is isomorphic to a quotient ring $K[\bar{A}]/I(\mathbb{V}(f_1,\ldots,f_l))$, where $I(\mathbb{V}(f_1(\bar{A}),\ldots,f_l(\bar{A})))$ denotes an ideal of $K[\bar{A}]$ that consists of all polynomials vanishing at every point of $\mathbb{V}(f_1(\bar{A}),\ldots,\mathbb{V}(\bar{A}))$. Hence, it is isomorphic to $K[\bar{A}]/\operatorname{rad}(\langle f_1(\bar{A}),\ldots,f_l(\bar{A})\rangle)$ in case K is an algebraically closed field. (Here, $\operatorname{rad}(I)$ denotes a radical ideal of I.) The above observation leads us to the following definition.
The basic notion of this section has been studied in [SSN03b, SSN03a, Nab05a].

Definition 47 (ACGB-V)
Let K be an algebraically closed field, F a set of polynomials in $K[\bar{A}][\bar{X}]$ and I a polynomial ideal in $K[\bar{A}]$. An **ACGB-V** (**A**lternative **C**omprehensive **G**röbner **B**asis on a **V**ariety) of $\langle F\rangle$ with respect to I is defined as follows. Let T be a regular closure of the quotient ring $K[\bar{A}]/\operatorname{rad}(I)$ in the commutative von Neumann regular ring $K^{\mathbb{V}(I)}$. Then, there exists a stratified Gröbner basis of $\langle F\rangle$ in $T[\bar{X}]$. We call G an ACGB-V of $\langle F\rangle$ with respect to the ideal I.

Theorem 48
Using the same notation as in the above definition, let $F = \{f_1(\bar{A},\bar{X}),\ldots,f_l(\bar{A},\bar{X})\}$ and $G = \{g_1(\bar{X}),\ldots,g_k(\bar{X})\}$ an ACGB-V of $\langle F\rangle$ with respect to I of $K[\bar{A}]$. Then following properties hold for any m-tuple $\bar{a} \in K^m$ belonging to the variety $\mathbb{V}(I)$:

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

(Note that $\bar{a}$ is a prime ideal in $B(K^{K^m})$. For $p \in \operatorname{Spec}(B(R))$ we let $\Phi_p : R \to R_p$ be the canonical homomorphism where R is a commutative von Neumann regular ring. Then, $G_p := \Phi(G)$. That is, $G_{\bar{a}} = \Phi(G)$.)

Proof This proof is exactly same as the proof of Theorem 3.2 of [SS02] or Theorem 4.3 [SS03]. ∎

Example 49
Let F be the set of polynomials $\{a-b, axy-bx^3y-3a, bxy-3bx-5b\}$ in $\mathbb{Q}[a,b][x,y]$, a,b parameters and x,y variables. Take a lexicographic order $\succ$ such that $y \succ x$. When we are interested in only values such that the ideal becomes proper, it is more natural to construct an ACGB-V of $\langle F\rangle$ 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 $\{a-b, axy-bx^3y-3a, bxy-3bx-5b\}$ in $T[x,y]$ where T is a regular closure of $\mathbb{Q}[a,b]/\langle a-b\rangle$. This G is the desired $ACGB-V$ of $\langle F\rangle$ and has the following form using terraces:

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

We should note that the ACGB-V of $\langle (a-b) + (axy-bx^2y-3a)^3 + (bxy-3bx-5b)^4, axy-bx^2y-3a, bxy-3bx-5b\rangle$ with respect to $\langle a-b\rangle$ has the same form.

7 Computation methods for ACGB-V

In this section, we present algorithms for computing ACGB-V. As we saw, when there is a constraint of parameters $\bar{A}$ 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 $\mathbb{V}(f_1(\bar{A}), \ldots, f_l(\bar{A}))$ than a whole space K^m. First, we describe the case $\langle f_1(\bar{A}), \ldots, f_l(\bar{A})\rangle$ is a zero-dimensional ideal in $K[\bar{A}]$. Second, we generalize the method of zero-dimensional case to general cases. These computation method is introduced in [SSN03b, SSN03a, Nab05a].

Definition 50 (Definition 6.46 [BW93])
Let I be a proper ideal of $K[\bar{A}]$ and $\bar{U} \subseteq \bar{A}$. Then $\bar{U}$ is called independent modulo I if $I_{\bar{U}} = I \cap K[\bar{U}] = \{0\}$. Moreover, $\bar{U}$ is called **maximally independent** modulo I if it is independent modulo I and not properly contained in any other independent set modulo I. The **dimension** $\dim(I)$ of I is defined as

$$\dim(I) = \left\{ |\bar{U}| \,\middle|\, \bar{U} \subset \bar{A} \text{ independent modulo } I \right\}.$$

We will, rather obviously, call an ideal of $K[\bar{A}]$ **zero-dimensional** if it is proper and has dimension zero.

Definition 51 (DCGB)
Let $F = \{f_1(\bar{A}, \bar{X}), \ldots, f_l(\bar{A}, \bar{X})\}$ in $K[\bar{A}][\bar{X}]$ and S a set of polynomials $\{s_1(A_1), \ldots, s_m(A_m)\}$, where $s_i(A_i)$ is a non-constant univariate polynomial in $K[A_i]$ for each $i = 1, \ldots, m$. A 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** (DCGB) of $\langle F\rangle$ with respect to $(\bar{A}, S)$ if it satisfies the following:
$G(\bar{a}) = \{g_1(\bar{a}, \bar{X}), \ldots, g_k(\bar{a}, \bar{X})\}\backslash\{0\}$ is a Gröbner basis for $\langle f_1(\bar{a}, \bar{X}), \ldots, f_l(\bar{a}, \bar{X})\rangle$ in $\bar{K}[\bar{X}]$ for any elements $\bar{a} = (a_1, \ldots, a_m) \in \bar{K}^m$ satisfying $s_1(a_1) = 0, \ldots, s_m(a_m) = 0$.

Lemma 52
Let 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 $P_1, \ldots, P_k$ of $K[\bar{A}]$. Since I is zero dimensional, each P_i is also zero-dimensional. Therefore, P_i is a maximal ideal, and thus, we can apply the Chinese remainder theorem to obtain an isomorphism $K[\bar{A}]/I \cong K[\bar{A}]/P_1 \times \cdots \times K[\bar{A}]/P_k$. The right-hand side is a direct product of fields, hence it is a commutative von Neumann regular ring. ∎

Theorem 53 ([SSN03a])
Let I be a zero dimensional ideal in a polynomial ring $K[\bar{A}]$, $F = \{f_1(\bar{A}, \bar{X}), \ldots, f_l(\bar{A}, \bar{X})\}$ a set of polynomials in $K[\bar{A}][\bar{X}]$ and $G = \{g_1(\bar{A}, \bar{X}), \ldots, g_k(\bar{A}, \bar{X})\}$ a stratified Gröbner basis for $\langle F\rangle$ in a polynomial ring $(K[\bar{A}]/\operatorname{rad}(I))[\bar{X}]$ over a commutative von Neumann regular ring $K[\bar{A}]/\operatorname{rad}(I)$. Then, we have the following two properties for any m-tuple $\bar{a} = (a_1, \ldots, a_m) \in \bar{K}^m$ belonging to the variety $\mathbb{V}(I)$:

1. $G(\bar{a}) = \{g_1(\bar{a}, \bar{X}), \ldots, g_k(\bar{a}, \bar{X})\}\backslash\{0\}$ is a reduced Gröbner basis of the ideal generated by $F(\bar{a}) = \{f_1(\bar{a}, \bar{X}), \ldots, f_k(\bar{a}, \bar{X})\}$ in $K[\bar{X}]$.
2. For any polynomial $h(\bar{A}, \bar{X}) \in K[\bar{A}][\bar{X}]$, we have $(h(\bar{A}, \bar{X})\downarrow_G)(\bar{a}, \bar{X}) = h(\bar{a}, \bar{X}) \downarrow_{G(\bar{a}, \bar{X})}$.

Like the algorithm ACGB, by Theorem 53 and algorithm 37, we can easily construct an algorithm for computing discrete comprehensive Gröbner bases.

Algorithm 54 (DCGB($F, S, \succ$) **[SSN03a])**
Input F : a subset of $K[\bar{A}][\bar{X}]$,
S: a zero-dimensional ideal in $K[\bar{A}]$,
$\succ$: a term order on $\mathrm{pp}(\bar{X})$,
Output G : a discrete comprehensive Gröbner basis for $\langle F\rangle$ with respect to S.

1. Consider the map $\psi : K[\bar{A}]/\operatorname{rad}(S) \to K^s$ where $s = |\mathbb{V}(\operatorname{rad}(S))|$ (the number of solutions).
2. Compute $\psi(F)$.
3. Compute a Gröbner basis G for $\langle\psi(F)\rangle$ with respect to $\succ$ in $(K[\bar{A}]/\operatorname{rad}(S))([\bar{X}]$ by the algorithm 37.
4. Compute $\psi^{-1}(G)$. There exists a map ψ^{-1} because $K[\bar{A}]/\operatorname{rad}(S)$ is isomorphic to K^s.

In Figure 2, we give the rough procedure of algorithm 54. This algorithm has been implemented by the author in prolog[1)]. In the next example, we give an output of the program.

Example 55
Let $F = \{2xy^2z + x + 2, aby^2z + 2bx + 9, bx + ayz + 2, a^3 + 4a^2 + 3a, 2b^3 - 5b^2 + 3b\}$ be a set of polynomial in $\mathbb{C}[a, b][x, y, z]$, a, b parameters, x, y variables and $\succ$ the graded reverse lexicographic order. Then, $\langle a^3 + 4a^2 + 3a, 2b^3 - 5b^2 + 3b\rangle$ is a zero dimensional ideal in $\mathbb{C}[a, b]$. We can use the algorithm DCGB. The program outputs the following set G;

```
[(2/3*b^2-5/3*b+1),
(-2/9*a^2*b^2+5/9*a^2*b-4/9*a*b^2+10/9*a*b)*y+(32352520/138649329*a^2*b^2
-6228140/15405481*a^2*b+4717108/46216443*a*b^2-2362394/15405481*a*b)*z+(2
29518223/138649329*a^2*b^2-293241527/92432886*a^2*b+319292681/92432886*a*
b^2-394962473/61621924*a*b),
(-2/3*b^2+5/3*b)*x+(25960/104013*a^2*b^2-4860/11557*a^2*b+2692/34671*a*b^
2-1490/11557*a*b)*z+(758285/624078*a^2*b^2-2890075/1248156*a^2*b+785765/3
12039*a*b^2-3051715/624078*a*b-65/18*b^2+247/36*b),
(-2/9*a^2*b^2+5/9*a^2*b-4/9*a*b^2+10/9*a*b)*z^2+(41/24*a^2*b^2+23/6*a^2*b
+61/12*a*b^2+21/2*a*b)*z+(9001/1944*a^2*b^2-4201/1944*a^2*b+54007/3888*a*
b^2-24727/3888*a*b),
(2/9*a^2*b^2-5/9*a^2*b+4/9*a*b^2-10/9*a*b-2/3*b^2+5/3*b)*z*y^2+(1/9*a^2*b
^2-41/234*a^2*b+2/9*a*b^2-41/117*a*b-1/3*b^2+41/78*b)].
```

Therefore, G is a discrete comprehensive Gröbner basis. In fact, a comprehensive Gröbner basis for $\langle F\rangle$ is $G \cup \{a^3 + 4a^2 + 3a, 2b^3 - 5b^2 + 3b\}$. That is, we can understand

$$\begin{cases} G & \text{if the support is } \mathbb{V}(a^3 + 4a^2 + 3a, 2b^3 - 5b^2 + 3) \\ \{1\} & \text{if the support is } \mathbb{C}^2 \backslash \mathbb{V}(a^3 + 4a^2 + 3a, 2b^3 - 5b^2 + 3). \end{cases}$$

[1)]Prolog is a logic programming language. The author used "SICStus Prolog".
http://www.sics.se/isl/sicstuswww/site/index.html

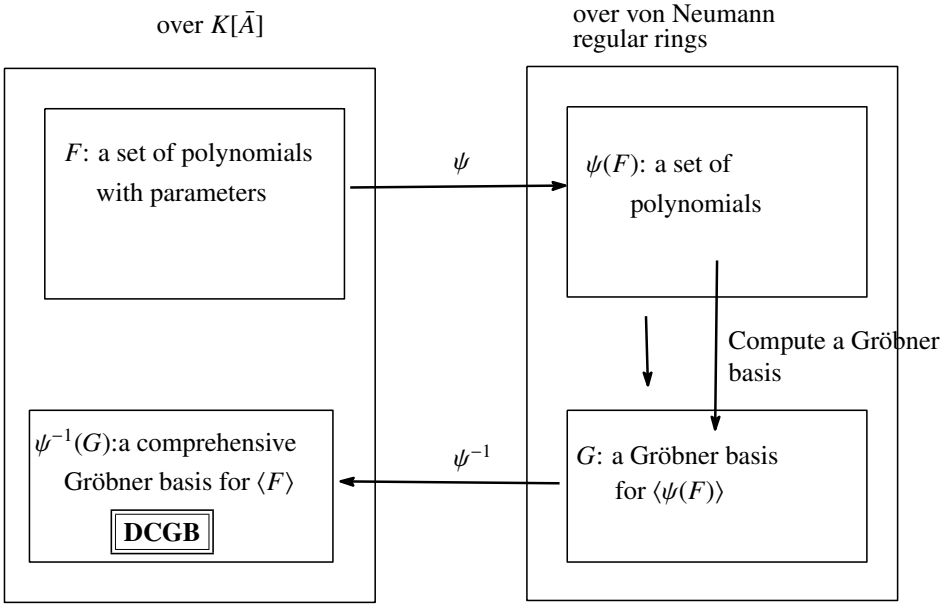

Figure 2 A computation method for DCGB

Second, we describe an algorithm for computing ACGB-V. Namely, we extend the algorithm DCGB to the more general situation of ACGB-V. In order to explain the algorithm we need the following lemma.

Lemma 56 (Lemma 7.47 [BW93])
Let $I \subset K[\bar{A}]$ be an ideal and $\bar{U} \subset \bar{A}$ be a maximal independent set of variables with respect to I. Then, $I \subset K(\bar{U})[\bar{A}\backslash\bar{U}]$ is a zero-dimensional ideal.

In order to compute a maximal independent modulo I, we can apply the algorithm DCGB for computing ACGB-V. However, we can not use the method directly for computing ACGB-V, because we have to regard $\bar{U}$ as a set of parameters. For example, let $I = \langle ab + b + c + 1\rangle$, $F = \{bx + ay + c, cx^2 + ab\}$ where a, b, c are parameters and x, y are variables. Then I is not a zero-dimensional ideal in $\mathbb{Q}[a, b, c]$, but $I_{\{a,c\}}$ is a zero-dimensional ideal in $\mathbb{Q}(a, c)[b]$. However, it is only true if $a \neq -1$. The case $a = -1$ is overlooked, though if should not be. By $I = \langle ab+b+c+1\rangle$, there exists $a = -1$. To solve this problem, we propose the following algorithm. The first key point is to compute ACGB where $\bar{U}$ is a set of parameters and $\{\bar{A}\backslash U\}$ is a set of variables. The second key point is an information of **support** (or preterrace). In the following algorithm, we use the notation supp which is from Definition 42.

Algorithm 57 (Div-zero(I))
Input I : a polynomial ideal in $K[\bar{A}]$,
Output $M = \{(V, Q)|Q$: a set of variables in $\bar{A}$; V: a set of polynomials in $K(Q)[\bar{A}\backslash Q]$ with $\mathrm{supp}(\mathrm{lpp}(h_1)) = \mathrm{supp}(\mathrm{lpp}(h_2)), \forall h_1, h_2 \in V\ \}$.

1. $Z \leftarrow I$; $M \leftarrow \emptyset$;

2. $R \leftarrow$ Compute a radical ideal of Z in $K[\bar{A}]$ $(*1)$

3. $U \leftarrow$ Compute a maximal independent set with respect to R in $K[\bar{A}]$ $(*2)$

4. $A \leftarrow$ Compute ACGB with respect to Z (and the lexicographic order $\succ$) where U is a set of parameters and $\{\bar{A}\backslash U\}$ is a set of variables. (We can obtain a reduced stratified Gröbner basis in $\bar{K}^{\bar{K}^{|U|}}[\bar{A}\backslash U]$.)

5. $N \leftarrow$ Classify A into N which is a set of sets of polynomials in $\bar{K}^{\bar{K}^{|U|}}[\bar{A}\backslash U]$. $N = \{N_1 |$ supports of all monomials p_1 are same, and $\mathrm{supp}(p_1) = \mathrm{supp}(p_2), \forall p_1, p_2 \in N_1\ \}$. That is, N_1 is a set of polynomials in $\bar{K}^{\bar{K}^{|U|}}[\bar{A}\backslash U]$ and all polynomials in N_1 have a same support.
   (We can compute this N by using *supports* (head idempotent). This algorithm is similar to the algorithm BC.)

6. **while** $N \neq \emptyset$ **do**
   Select J from N; $N \leftarrow N\backslash\{J\}$
   if $\langle J\rangle$ is a zero-dimensional ideal in $K(U)[\bar{A}\backslash U]$ **then**
   $M \leftarrow M \cup (J, U)$
   else
   $S \leftarrow$ Compute all combinations of polynomials of T_1 where supports of all element of J is $[\mathbb{V}(T_1) - \mathbb{V}(T_2)]$. $(**)$
   while $S \neq \emptyset$ **do**
   Select s_1 from s; $s \leftarrow s\backslash s_1$
   $Z \leftarrow \{s_1\} \cup Z$
   goto 2
   end-while
   end-if
   end-while

($(**)$ Let $[\mathbb{V}(T_1) - \mathbb{V}(T_2)] \subset \bar{K}^{\bar{K}^{|U|}}$ be a *support* of J where T_1, T_2 are sets of polynomials in $K[U]$. Then we can consider that J is restricted to T_1. So we consider about $Z \cup$ {one of T_1 } in the next step.)

Remark: In $(*1)$ and $(*2)$, there exist algorithms for computing a radical ideal and a maximal independent set U modulo I.
By the algorithm ACGB and the Remark, this algorithm clearly terminates and outputs correctly. By the above algorithm we can obtain zero-dimensional ideals from I in several polynomial rings. Let us consider $I = \langle ab + b + c + 1\rangle$ again. I is already a radical ideal and $\{a, c\}$ is a maximal independent set with respect to I in $\mathbb{Q}[a, b, c]$. We can compute ACGB of I where a, b are parameters and b is variable. Then, the algorithm ACGB outputs the following:

$$[[(\mathbb{V}[(c+1)*(a+1)] - \mathbb{V}[c+1], 1)] * 1,$$
$$[(\mathbb{V}[0] - \mathbb{V}[a+1], 1)] * b + [(\mathbb{V}[0] - \mathbb{V}[(c+1)*(a+1)], (c+1)/(a+1))] * 1]. \ (*)$$

Look at the first polynomial. Then, we have $\{1\}$ when the support is $[[(\mathbb{V}((c+1)*(a+1)) - \mathbb{V}(c+1)]$. So we don't need it. In the second polynomial, we classify the support $[\mathbb{V}(0) - \mathbb{V}(a+1)]$ to $[\mathbb{V}(0) - \mathbb{V}((a+1)(c+1))]$ and $[\mathbb{V}((a+1)(c+1)) - \mathbb{V}(a+1)]$ where $\mathbb{V}(0) = \mathbb{C}^2$. First we consider the support $[\mathbb{V}(0) - \mathbb{V}((a+1)(c+1))]$. In the support $[\mathbb{V}(0) - \mathbb{V}((a+1)(c+1))]$, we have $\langle b + \frac{c+1}{a+1}\rangle$ which is a zero-dimensional ideal in $\mathbb{Q}(a, c)[b]$. Next by the algorithm, we have to consider three supports $v_1 = [\mathbb{V}((a+1)(c+1)) - \mathbb{V}(a+1)]$, $v_2 = [\mathbb{V}((a+1)(c+1)) - \mathbb{V}(c+1)]$ and $v_3 = [\mathbb{V}(a+1, c+1)]$

(because in the support $[\mathbb{V}(0) - \mathbb{V}((a+1)(c+1))]$, I is restricted to $\langle (a+1)(c+1) \rangle$). Actually, now we have

$$\mathbb{V}((a+1)(c+1)) = v_1 \cup v_2 \cup v_3.$$

(1) If we consider the support v_1, then we obtain $\langle b \rangle$ from $(*)$
(2) If we take the support v_2, then we already consider the case.
(3) If we take the support v_3, then we can obtain $\langle ab + b + c, a + 1, c + 1 \rangle = \langle a + 1, c + 1 \rangle$ which is a zero-dimensional ideal in $\mathbb{Q}(b)[a, c]$.

Therefore by the algorithm we obtained:

$$\begin{cases} \langle b + \frac{c+1}{a+1} \rangle, & \text{zero-dim. ideal in } \mathbb{Q}(a,c)[b], \text{ supp. } [\mathbb{V}(0) - \mathbb{V}((a+1)(c+1)], \quad (1) \\ \langle b \rangle, & \text{zero-dim. ideal in } \mathbb{Q}(a,c)[b], \text{ supp. } [\mathbb{V}((a+1)(c+1)) - \mathbb{V}(a+1)], (2) \\ \langle a+1, c+1 \rangle, & \text{zero-dim. ideal in } \mathbb{Q}(b)[a,c], \text{ supp. } [\mathbb{V}(c+1, a+1)]. \quad (3) \end{cases}$$

We already know the method of DCGB (zero-dimensional case) [SSN03b, SSN03a]. By the algorithm Div-zero, we can obtain some zero-dimensional ideals, and we apply DCGB's method for computing ACGB-V. However, note that when we compute DCGB in several polynomial rings, we regard a maximal independent set as parameters. Because these zero-dimensional ideals have parameters which are in the coefficient domain $K(U)$ of their polynomial ring. For example, let $F = \{bx + ay + c, cx^2 + ab\}$ and $\succ$ the lexicographic order such that $x \succ y$.

In case (3), we regard b as a parameter when we compute comprehensive Gröbner basis : (That is, $a + 1 = 0, c + 1 = 0$, the support is $[\mathbb{V}(a + 1, c + 1)]$)

```
[[(V[-b]-V[-1],1)]*y+[(V[-b]-V[-1],1)]*1,
[(V[0]-V[b],1)]*x+[(V[0]-V[-b],(-1)/(b))]*y+[(V[0]-V[-b],(-1)/(b))]*1,
[(V[0]-V[b],1)]*y^2+[(V[0]-V[b],2)]*y+[(V[0]-V[b^4+b],b^3+1)]*1,
[(V[b],1)]*x^2].
```

To obtain comprehensive Gröbner basis for $\{F, I\}$, we have to also compute ACGB in cases (1) and (2).

In case (1) : ($b + \frac{c+1}{a+1} = 0$, the support is $[\mathbb{V}(0) - \mathbb{V}((a+1)(c+1))]$),

```
[[(V[a^2+a,(-c^2-c)*a-c^2-c]-V[c*a+c,a^2+a],1),(V[(-c^2-c)*a^2+(-c^2-c)*a
 ]-V[(-c-1)*a],1),(V[(-c^2-c)*a^2+(-c^2-c)*a]-V[(c^2+c)*a+c^2+c],1)]*1,
[(V[(-c-1)*a^2+(-c-1)*a]-V[a^2+a],1)]*y+[(V[(-c^2-c)*a-c^2-c,(-c-1)*a^2+(
 -c-1)*a]-V[a^2+a,(-c^2-c)*a-c^2-c],(c)/(a))]*1,
[(V[0]-V[(c^2+c)*a^2+(c^2+c)*a],1)]*y^2+[(V[0]-V[(c^2+c)*a^2+(c^2+c)*a],(
 2*c)/(a))]*y+[(V[0]-V[(-c^5-c^4)*a^5+(-4*c^5-4*c^4)*a^4+(-5*c^5-2*c^4+6*
 c^3+4*c^2+c)*a^3+(-3*c^5+6*c^3+4*c^2+c)*a^2+(-c^5-c^4)*a],(c^3*a^3+3*c^3
 *a^2+(2*c^3-3*c^2-3*c-1)*a+c^3)/(c*a^5+3*c*a^4+3*c*a^3+c*a^2))]*1,
[(V[0]-V[(c^2+c)*a^2+(c^2+c)*a],1),(V[-c^2-c,(-c-1)*a]-V[-c-1],1)]*x+[(V
 [0]-V[(c^2+c)*a^2+(c^2+c)*a],(-a^2-a)/(c+1))]*y+[(V[0]-V[(-c^2-c)*a^2+(-
 c^2-c)*a],(-c*a-c)/(c+1))]*1,
[(V[(c^2+c)*a+c^2+c]-V[(c^2+c)*a+c^2+c,c*a^2+c*a],1)]*x^2].
```

In case (2) : ($b = 0$, the support is $[\mathbb{V}((a+1)(c+1)) - \mathbb{V}(a+1)]$),

```
[[(V[c*a]-V[c],1)]*1,
 [(V[0]-V[a],1)]*y+[(V[0]-V[c*a],(c)/(a))]*1,
 [(V[0]-V[c*a],1)]*x^2]
```

Then in each case, we obtained a parametric Gröbner basis for $\langle F \rangle \cup I$ by using ACGB method.

We described a natural idea to generalize the algorithm DCGB. The first key point of this idea is what variables are regarded as parameters (or variables). Then we compute ACGB because we need the information of the support. The second key point is that "add an information of support to an original ideal in $K[\bar{A}]$". By the algorithm Div-zero we can classify the original ideal I to some zero-dimensional ideals in several polynomial rings. Then, we can apply the computation method DCGB (zero-dimensional) for computing comprehensive Gröbner bases. This is the procedure of computing ACGB-V. Since we need to compute a Gröbner basis in a polynomial ring over a von Neumann regular ring, the outputs hold the nice properties of (reduced) Gröbner basis over von Neumann regular rings. For instance, if we substitute any values for parameters of the outputs (reduced Gröbner bases in a polynomial ring over a von Neumann regular ring), then the set computed is always the reduced Gröbner bases.

References

[BS80] Burris, S. and Sankappanavar, H.P. *A Course in Universal Algebra*. Springer-Verlag, 1980.

[Buc65] Buchberger, B. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal*. Universität Innsbruck, Austria, 1965. Ph.D. Thesis.

[Buc70] Buchberger, B. Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. *Aequationes Math*, 4:374–383, 1970.

[Buc79] Buchberger, B. A criterion for detecting unnecessary reductions in the construction of Gröbner bases. In Ng, E.W., editor, *EUROSAM'79*, pages 3–21. Springer, 1979.

[Buc85] Buchberger, B. Gröbner bases: An Algorithmic Method in Polynomial Ideal Theory. In Bose, N., editor, *Multidimensional Systems Theory*, pages 184–232. Reidel Publishing Company, 1985.

[BW93] Becker, T. and Weispfenning, V. *Gröbner Bases, a computational Approach to Commutative Algebra*. Springer New York, 1993.

[Lou79] Loullis, G. Sheaves and boolean valued model theory. *Journal of Symbolic Logic*, 44 (2):153–183, 1979.

[MM05] Manubens, M. and Montes, A. Improving DISPGB algorithm using the discriminant ideal (extended abstract). In Dolzmann, A., Seidl, A., and Thomas, S., editors, *the A3L 2005, conference in Honor of the 60th Birthday of Volker Weispfenning*, pages 159–166. BOD Norderstedt, 2005.

[MM06] Manubens, M. and Montes, A. Improving DISPGB algorithm using the discriminant ideal. *Journal of Symbolic Computation*, 41:1245–1263, 2006.

[Mon02] Montes, A. A new algorithm for discussing Gröbner basis with parameters. *Journal of Symbolic Computation*, 33/1-2:183–208, 2002.

[Nab05a] Nabeshima, K. A computation method for ACGB-V. In Dolzmann, A., Seidl, A., and Thomas, S., editors, *the A3L 2005, conference in Honor of the 60th Birthday of Volker Weispfenning*, pages 171–180. BOD Norderstedt, 2005.

[Nab05b] Nabeshima, K. A Direct Products of Fields Approach to Comprehensive Gröbner Bases over Finite Fields. In Zaharie, D., Petcu, D., Negru, V., Jebelean, T., Ciobanu, G., Cicortas, A., Abraham, A., and Paprzycki, M., editors, *International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, pages 39–47. IEEE Computer Society, 2005.

[Sat98] Sato, Y. A new type of canonical Gröbner bases in polynomial rings over von Neumann regular rings. In Gloor, O., editor, *International Symposium on Symbolic and Algebraic Computation*, pages 317–321. ACM-Press, 1998.

[Sat05] Sato, Y. Stability of Gröbner basis and ACGB. In Dolzmann, A., Seidl, A., and Thomas, S., editors, *the A3L 2005, conference in Honor of the 60th Birthday of Volker Weispfenning*, pages 223–228. BOD Norderstedt, 2005.

[SS02] Suzuki, A. and Sato, Y. An alternative approach to Comprehensive Gröbner bases. In Mora, T., editor, *International Symposium on Symbolic and Algebraic Computation*, pages 255–261. ACM Press, 2002.

[SS03] Suzuki, A. and Sato, Y. An alternative approach to Comprehensive Gröbner bases. *Journal of Symbolic Computation*, 36/3-4:649–667, 2003.

[SS04] Suzuki, A. and Sato, Y. Comprehensive Gröbner Bases via ACGB. In Tran, Q-N., editor, *The 10th Internatinal Conference on Applications of Computer Algebra*, pages 65–73. Lamar University, 2004.

[SSN02] Sato, Y., Suzuki, A., and Nabeshima, K. Generalized discrete Comprehensive Gröbner Bases. In *CA-ALIAS*, pages 105–110. RIMS, Kyoto University, 2002.

[SSN03a] Sato, Y., Suzuki, A., and Nabeshima, K. ACGB on Varieties. In Ganzha, V.F., Mayr, E.W., and Vorozhtsov, E.V., editors, *The 6th International Workshop on Computer Algebra in Scientic Computing (CASC)*, pages 313–318. Technische Universität München, 2003.

[SSN03b] Sato, Y., Suzuki, A., and Nabeshima, K. Discrete Comprehensive Gröbner bases II. In Li, Z. and Sit, W., editors, *Computer Mathematics, Lecture Notes Series on Computing*, pages 240–247. World Scientific, 2003.

[SW75] Saracino, D. and Weispfenning, V. On algebraic curves over commutative regular rings. In Saracino, D. and Weispfenning, V., editors, *Model Theory and Algebra, a memorial tribute to A. Robinson*, pages 307–387. Springer, 1975.

[Wei87] Weispfenning, V. Gröbner bases for polynomial ideals over commutative regular rings. In Davenport, J., editor, *EUROCAL '87, LNCS378*, pages 336–347. Springer, 1987.

[Wei92] Weispfenning, V. Comprehensive Gröbner bases. *Journal of Symbolic Computation*, 14/1:1–29, 1992.

[Wei02a] Weispfenning, V. Canonical Comprehensive Gröbner bases. In Mora, T., editor, *International Symposium on Symbolic and Algebraic Computation*, pages 270–278. ACM Press, 2002.

[Wei02b] Weispfenning, V. Comprehensive Gröbner bases and regular rings. In Nakagawa, K., editor, *Symposium in Honor of Bruno Buchberger's 60th Birthday*, pages 256–264. RISC-Linz, 2002.

[Wei03] Weispfenning, V. Canonical Comprehensive Gröbner bases. *Journal of Symbolic Computation*, 36/3-4:669–683, 2003.

[Wei04] Weispfenning, V. Gröbner bases for binomials with parametric exponents. In Ganzha, V.F., Mayr, E.W., and Vorozhtsov, E.V., editors, *International Workshop on Computer Algebra in Scientic Computing (CASC)*, pages 467–478. Technische Universität München, 2004.

[Wei06] Weispfenning, V. Comprehensive Gröbner bases and regular rings. *Journal of Symbolic Computation*, 41(3-4):285–296, 2006.