An algorithm for computing a Gröbner basis of a polynomial ideal over a ring with zero divisors

Deepak Kapur and Yongyang Cai[*]

Department of Computer Science, University of New Mexico,

Albuquerque, NM 87131, USA, {kapur,yycai}@cs.unm.edu.

December 3, 2003

Abstract

An algorithm for computing a Gröbner basis of an ideal of polynomials whose coefficients are taken from a ring with zero divisors, is presented; such rings include $\mathbb{Z}_n$ and $\mathbb{Z}_n[i]$, where n is not a prime number. The algorithm is patterned after (1) Buchberger's algorithm for computing a Gröbner basis of a polynomial ideal whose coefficients are from a field and (2) its extension developed by Kandri-Rody and Kapur when the coefficients appearing in the polynomials are from a Euclidean domain. The algorithm works as Buchberger's algorithm when a polynomial ideal is over a field and as KandriRody-Kapur's algorithm when a polynomial ideal is over a Euclidean domain. The proposed algorithm and the related technical development are quite different from a general framework of reduction rings proposed by Buchberger in 1984 and generalized later by Stifter to handle reduction rings with zero divisors. These different approaches are contrasted along with the obvious approach where for instance, in the case of $\mathbb{Z}_n$,

[*]This research is partially supported by the NSF grants CCR-9996144 and CCR-0203051. The work on this topic was initiated by the first author jointly with Prof. Klaus Madlener of University of Kaiserslautern while Kapur and Madlener were visiting each other in 1986-90. Preliminary results were presented at a workshop at Cornell University organized by the Mathematical Sciences Institute in 1988.

the algorithm for polynomial ideals over $\mathbb{Z}$ could be used by augmenting the original ideal presented by polynomials over $\mathbb{Z}_n$ with n (similarly, in the case of $\mathbb{Z}_n[i]$, the original ideal is augmented with n and $i^2 + 1$).

1 Introduction

An algorithm for computing a Gröbner basis of a polynomial ideal in which the coefficients of monomials in polynomials are taken from a ring with zero divisors (i.e., there exist $c_1, c_2 \neq 0$ in such a ring with $c_1 \cdot c_2 = 0$) is presented. Such coefficient rings include, for examples, $\mathbb{Z}_n$ where n is not a prime number, as well as $\mathbb{Z}_n[i]$ where $i^2 + 1 = 0$, and so on. The proposed algorithm is patterned after (1) Buchberger's algorithm for computing a Gröbner basis of a polynomial ideal where the coefficients of monomials are from a field and (2) its generalization by Kandri-Rody and Kapur [8, 9] when the coefficients of monomials in polynomials are from a Euclidean domain.

The input to the proposed algorithm is an ideal specified by a finite set of polynomials. The algorithm produces another finite basis of the ideal which can be used to reduce polynomials so that (1) every polynomials in the ideal reduces to 0 and (2) every polynomial in the polynomial ring reduces to a unique normal form such that polynomials equivalent with respect to the ideal have the same normal form. An interested reader may wish to refer to a survey article by Buchberger [7] for a brief introduction to the subject as well as numerous applications of a Gröbner basis algorithm. Below, we provide a brief historical background.

The concept of a Gröbner basis of an ideal was introduced by Bruno Buchberger in 1965 in his Ph.D. thesis [4]. Buchberger defined such a specialized basis of an ideal as having the property that any element in the underlying ring has a canonical form (unique normal form) with respect to the ideal, along with the canonical form for the elements in the ideal being 0; furthermore, two elements in the ring modulo a given ideal have the same canonical form. For polynomial ideals over a field, Buchberger not only showed that every polynomial ideal has a Gröbner basis but also gave an algorithm for computing a Gröbner basis from any basis of the ideal. It took some years before the concept became popular among mathematicians and computer scientists. By now, numerous interesting applications of the concept have been found as many computational problems can be solved by computing Gröbner bases of polynomial ideals. Most commercially available computer algebra systems provide implementations of Gröbner basis algorithms. There are highly specialized fast stand-alone software systems available for computing Gröbner basis as well.

Kandri-Rody and Kapur [8, 9] generalized Buchberger's algorithm by defining a rewriting relation induced by a polynomial on a polynomial ring using a division algorithm over a Euclidean domain. They defined a well-founded order on polynomials using the well-founded order on the elements of a Euclidean domain induced by the division algorithm. Using these ideas, they developed a Gröbner basis algorithm to work on polynomial ideals over Euclidean domains. Subsequently, Kapur and Narendran [11] as well as Pan [15] proposed algorithms to compute a Gröbner basis of a ideal in polynomial rings over principal ideal domain (PID). Unlike Buchberger's algorithm as well as KandriRody-Kapur's algorithm which computes canonical forms for elements in the quotient ring defined on a polynomial ring by an ideal, Kapur and Narendran's as well as Pan's algorithms do not have this property. Instead, every polynomial in a given polynomial ideal reduces to 0 using a Gröbner basis of the polynomial ideal; however, different elements in the polynomial ring which are equivalent modulo the polynomial ideal could have different normal forms. In this sense, Kapur and Narendran's algorithm as well as Pan's algorithm compute a *weak* Gröbner basis of an ideal, in contrast to Buchberger's algorithm as well as KandriRody-Kapur's algorithm that compute a *strong* Gröbner basis of an ideal.

KandriRody-Kapur's algorithm cannot, however, work on polynomial ideals over a non-Euclidean domain, for example, a ring with zero divisors. Kapur and Madlener [10] attempted to develop an algorithm to compute a Gröbner basis of polynomial ideals over a ring with zero divisors, which is closely related to the algorithm proposed in the paper[1]. The key new idea due to Kapur and Madlener [10] was that a single polynomial could also generate additional polynomials (the so-called critical pairs) to complete a basis. This idea was subsequently used by Madlener and Reinert [13] in their generalization of Gröbner bases for polynomial ideals over monoid rings; they called it the *saturation* of a given polynomial.

The proposed algorithm works as Buchberger's algorithm when a polynomial ideal is over a field and as KandriRody-Kapur's algorithm when a

[1] Kapur presented the preliminary results of this approach in 1988 at a workshop organized by Mathematical Sciences Institute at Cornell University

polynomial ideal is over a Euclidean domain.

In the next subsection, we discuss different approaches for generalizing Gröbner basis of a polynomial ideal where the coefficients are from a commutative ring. We also contrast how these approaches could be adapted to be used for computing Gröbner basis of a polynomial ideal where the coefficients could be zero-divisors. Section 2 gives basic definitions and lemmas, particularly emphasizing the properties of zero-divisors. The concept of a divisible and annihilable ring (a D-A ring) on which the proposed approach works is defined, and its properties are discussed. In section 3, a well-founded order on polynomials is defined using a well-founded order on the elements of a D-A ring. This leads to the definition of a rewriting relation induced by a polynomial using a division algorithm over a D-A ring. Almost all proofs are patterned after the proofs of related lemmas and properties in [8, 15, 3]. The main differences are that a special attention has to be paid in case the head coefficient of a polynomial in a basis is a zero divisor. These differences are pointed out in subsequent sections before detailed proofs are given. Section 4 gives a Gröbner basis algorithm. The algorithm is illustrated using an example in section 5. The comparison between the reduction ring method and our algorithm is given in section 6. Section 7 extends our algorithm to a polynomial ring over a generalized principle ideal ring (GPIR).

1.1 Related Work: Generalization of Buchberger's Algorithm for Polynomial Ideals over a field

There are at least three different approaches to generalizing Buchberger's algorithm for computing Gröbner bases of polynomial ideals over a commutative Noetherian ring:

- Syzygy method proposed by a number of researchers including Shtokhamer, Trinks, Zacharias, Schaller and Möller which works for polynomial ideals over Noetherian rings in which certain kinds of syzygies can be solved (see [14, 1], etc.).

- KandriRody-Kapur's algorithm for polynomial ideals over a Euclidean domain based on reduction relations, which was subsequently generalized by Pan as well as by Kapur and Narendran for polynomial ideals over a principal ideal domain.

- Buchberger's framework of a reduction ring, which was subsequently generalized by Stifter [16, 17, 18]. A reduction ring satisfies axioms needed for Buchberger's algorithm to be applicable in a general setting.

We briefly discuss each of these approaches and then later, we will discuss how polynomial ideals with coefficients from a ring with zero divisors will be considered. In contrast to Buchberger's approach in which (1) a single polynomial is used to reduce other polynomials and (2) new polynomials to complete a basis are generated by considering pairs of polynomials, approaches proposed by Shtokhamer, Trinks, Zacharias, Schaller and Möller used every finite subset of polynomials in a basis for reduction as well as for generating new polynomials to be added to the basis. As a result, reduction as well as methods for generating new polynomials in their approaches are quite complex. In order to perform these computations, one needs to solve linear nonhomogeneous equations over the coefficient ring as well as compute a basis for syzygies over the coefficient ring. The underlying coefficient ring thus must admit algorithmic solvability of the problem of computing syzygies in the coefficient ring. Furthermore, polynomials which are equivalent modulo a given polynomial ideal need not be reduced to the same canonical form using algorithms based on these approaches. In these respects, their algorithms are not in the spirit of Buchberger's algorithm; see also [5, 6, 9] for comments on differences between their approaches and the approaches based on rewriting techniques.

In 1984, Buchberger also developed a general version of the Gröbner basis algorithm for commutative rings, which satisfy certain conditions. He introduced the notion of a *reduction* ring and described a generalization of his Gröbner basis algorithm for polynomial ideals over a field (1965). Roughly, reduction rings are rings on which the Gröbner basis approach is possible, implying that Gröbner basis computations can be performed. Reduction rings are characterized by axioms that relate the arithmetical operations in the ring with an order. Once a ring $\mathcal{R}$ is shown to be a reduction ring, it is possible to compute a Gröbner basis of ideals over the ring. Buchberger also proved that (1) a polynomial ring over a reduction ring $\mathcal{R}$ is also a reduction ring, (2) there exists a Gröbner basis for every polynomial ideal and furthermore, (3) such a Gröbner basis can be computed. In Buchberger [5], the ring of integers is proven to be a reduction ring. After learning about Kapur and Madlener's approach [private communication, 1988], Stifter [16] generalized the notion of a reduction ring by giving weaker axioms that characterize a wider class of rings, and proved that the ring of integers modulo m (i.e., $\mathbb{Z}_n$), n an arbitrary not necessarily prime number, is a reduction ring in the generalized sense.

In order to show that a ring $\mathcal{R}$ is a reduction ring, one has to choose a Noetherian order on $\mathcal{R}$, finite index sets J_c for each $c \in \mathcal{R}$, and sets of multipliers Mul_c^i for each $c \in \mathcal{R}$ and $i \in J_c$ such that the axioms of a reduction ring are satisfied. The absence of any additional structure on reduction rings makes it necessary to introduce a totally new approach for the formulation of critical pairs that involves only the arithmetical operations and the order. The new concept of a *least common reducible* of two elements (denoted by LCR(.,.)) is defined by first introducing a reduction relation based on the arithmetical operations and the order predicate. As a consequence, the construction for computing critical pairs and a Gröbner basis from the ring operations can be quite involved technically. An algorithm for constructing a Gröbner basis over a reduction ring is given in Buchberger [5] and Stifter [16]: Given a finite set $C \subseteq \mathcal{R}$, find a finite set $D \subseteq \mathcal{R}$ such that $\longleftrightarrow_C^* = \longleftrightarrow_D^*$ and $\longrightarrow_D$ has the Church-Rosser property (see [2]). The key idea is: set $D := C$ and compute $\mathrm{LCR}(c_1, c_2)$ for any $c_1, c_2 \in C$, then reduce $\mathrm{LCR}(c_1, c_2)$ by c_1 and c_2 respectively, while only the multipliers in $Mul_{c_1}^i$ and $Mul_{c_2}^j$ can be quotients for two given indices $i, j \in J_c$. A critical pair is obtained in this way and the normal forms $< b_1, b_2 >$ of the critical pair is computed so that a new element $b_1 - b_2$ can be added into D. The example below illustrates the role of multipliers.

Kandri-Rody and Kapur [9] designed an algorithm for computing a Gröbner basis of a polynomial ideal in which the coefficients of polynomials are from a Euclidean domain, admitting a division algorithm, e.g., such as the ring of integers, Gaussian integers, as well as algebraic integers in quadratic number fields. The algorithm is a generalization of Buchberger's Gröbner basis algorithm for a polynomial ideal over a field, relying only on the existence of a division algorithm over the coefficients. Using the division algorithm, simplification of polynomials by another polynomial is defined in a natural way. A Gröbner basis is then a complete rewriting system when polynomials are viewed as rewrite rules, which can be used to generate canonical forms for equivalence classes in the quotient ring defined by the ideal on a polynomial ring. KandriRody-Kapur's algorithm cannot work, however, on polynomial ideals over a non-Euclidean domain, such as a ring with zero divisors. This paper extends KandriRody-Kapur's algorithm so that a Gröbner basis of a polynomial ideal over a ring with zero-divisors, such as $\mathbb{Z}_n$ and $\mathbb{Z}_n[i]$ ($i^2 = -1$)

for any integer n, can be computed. As will be discussed, the main idea is to generate additional polynomials from a given polynomial whose head coefficient is a zero divisor, and to add these polynomials as well to a given basis. In this sense, critical pairs are generated even from a single polynomial if its head coefficient is a zero divisor, by multiplying it by the *annihilator* of its head coefficient. We now illustrate key differences in various approaches using a simple example of a polynomial ideal with integer coefficients.

Example 1 *Consider an ideal over $\mathbb{Z}[x, y]$ generated by*

$$F = \{f_1 = 6x, f_2 = 32y\}.$$

Buchberger's method defined an order $0 < -1 < 1 < -2 < 2 < \cdots$ over $\mathbb{Z}$, and $\mathrm{LCR}(c_1, c_2) = \max(\mathrm{LCR}(c_1), \mathrm{LCR}(c_2))$, where

$$\mathrm{LCR}(c) = \begin{cases} |c|/2 & \text{if } c \text{ is even} \\ -(|c|+1)/2 & \text{if } c \text{ is odd} \end{cases}$$

for any $c, c_1, c_2 \in \mathbb{Z}$ (see [5]).

1. Since $\mathrm{LCR}(6, 32) = 16$, the superposition of f_1 and f_2 is defined as $16xy$, and the critical pair is obtained: $< p_1 = -2xy,\ p_2 = -16xy >$ as $16 = 3 * 6 - 2 \longrightarrow_6 -2$ and $16 = 1 * 32 - 16 \longrightarrow_{32} -16$.

2. In Buchberger-Stifter's method, there exists an algorithm A such that for all a, c: if $a \longrightarrow_c$, i.e., a is reducible modulo c, then there exists $A(a, c) \in Mul_c$ such that $a - A(a, c)c < a$. Then the polynomial p_2 is reducible modulo f_1 to: $p_3 = 2xy$ as $-16 = (-3) * 6 + 2 \longrightarrow_6 2$.

3. A new polynomial (S-polynomial) can be obtained from p_1 and p_3: $f_3 = p_1 - p_3 = -4xy$.

4. Since $\mathrm{LCR}(6, -4) = 3$, the superposition of f_1 and f_3 is defined as $3xy$, and the critical pair is obtained: $< p_4 = -3xy,\ p_5 = -xy >$ as $3 = 1 * 6 - 3 \longrightarrow_6 -3$ and $3 = (-1) * (-4) - 1 \longrightarrow_{-4} -1$.

5. Since $-3 = 1 * (-4) + 1 \longrightarrow_{-4} 1$, the polynomial p_4 can be further reduced modulo f_3 to: $p_6 = xy$.

6. A new polynomial (S-polynomial) can be obtained from p_5 and p_6: $f_4 = p_5 - p_6 = -2xy$.

7. The polynomial f_3 can be deleted by f_4.

8. No new polynomials can be produced from f_1, f_2, and f_4. A Gröbner basis of the ideal $\mathrm{Id}(F)$ is $\{6x, 32y, -2xy\}$.

Using the syzygy based method for computing a Gröbner basis, F is already a Gröbner basis. While $-2xy$ and $2xy$ cannot be reduced by either $6x$ or $32y$ in Buchberger-Stifter's method and KandriRody-Kapur's algorithm, they can be reduced to 0 using both $6x$ and $32y$ in the method based on syzygies. Since $-2xy = (5y) * (6x) + (-x) * (32y)$, it reduces to 0; similarly, $2xy = (-5y) * (6x) + (x) * (32y)$; it reduces to 0 too.

KandriRody-Kapur's algorithm defined an order $0 < 1 < -1 < 2 < -2 < \cdots$ over $\mathbb{Z}$ (see [9]).

1. Since $\max(6, 32) = 32$, the superposition of f_1 and f_2 is defined as $32xy$, and the critical pair is obtained: $< p_1 = 2xy,\ p_2 = 0 >$ as $32 = 5 * 6 + 2 \longrightarrow_6 2$ and $32 = 1 * 32 + 0 \longrightarrow_{32} 0$.

2. A new polynomial (S-polynomial) can be obtained from p_1 and p_2: $f_3 = p_1 - p_2 = 2xy$.

3. No new polynomials can be produced from f_1, f_2, and f_3. A Gröbner basis of the ideal $Id(F)$ is $\{6x, 32y, 2xy\}$.

The above example computes the Gröbner bases of polynomial ideals over a ring without any zero-divisors. We found that KandriRody-Kapur's algorithm is simpler than Buchberger-Stifter's method, and the syzygy method is quite different from the other two methods.

We know that Buchberger-Stifter's method and the syzygy method can compute Gröbner bases of polynomial ideals over a ring with zero-divisors, but KandriRody-Kapur's algorithm cannot. Our new algorithm extends KandriRody-Kapur's algorithm so that Gröbner bases of polynomial ideals over a ring with zero-divisors can be computed too. The difference between the new method and Buchberger-Stifter's method can be seen in Example 3 in section 6.

2 Basic Definitions and Lemmas

In the following, we assume $\mathcal{R}$ is a commutative ring with an identity element with respect to multiplication $*$, denoted by 1, i.e., for all $a \in \mathcal{R}$, $1 * a = a * 1 = a$.

Definition 1 *An element $\epsilon \in \mathcal{R}$ is called a* **unit** *if there exists an ϵ' in $\mathcal{R}$ such that $\epsilon * \epsilon' = 1$, the units set of $\mathcal{R}$ is denoted as* $\mathrm{Units}(\mathcal{R})$*.*

For example, 1 is a unit. Let $\epsilon, \epsilon' \in \mathrm{Units}(\mathcal{R})$ with $\epsilon * \epsilon' = 1$. If there exists $a \in \mathcal{R}$ such that $a\epsilon = 0$, then

$$a = a * 1 = a * (\epsilon * \epsilon') = (a * \epsilon) * \epsilon' = 0 * \epsilon' = 0,$$

i.e., no unit of $\mathcal{R}$ is a zero divisor.

A ring with an identity element 1 could have more than one unit. In $\mathbb{Z}$, for example, both 1 and -1 are units. For $\mathbb{Z}[i]$, the units are $1, -1, i, -i$. In $\mathbb{Z}_{20}$, the units are $1, 3, 7, 9, 11, 13, 17, 19$. In $\mathbb{Z}_{12}[i]$, the units are $\{a+bi | a, b \in \mathbb{Z}_{12}, \gcd(a^2 + b^2, 12) = 1\}$, for example, $\pm 1 \pm 2i$, $\pm 2 \pm 3i$, etc. For $\mathbb{Z}[s]$ with $s^3 = 1$, the units are $1, -1, s, -s, s^2, -s^2$. For any field $\mathcal{F}$ (such as the rational number field $\mathbb{Q}$), every element in $\mathcal{F} - \{0\}$ is a unit of $\mathcal{F}$, i.e., $\mathrm{Units}(\mathcal{F}) = \mathcal{F} - \{0\}$.

Definition 2 *Two elements, $a, b \in \mathcal{R}$, are called associated if and only if there exists a unit ϵ such that $a = b * \epsilon$.*

It is easy to see that associatedness is an equivalence relation on $\mathcal{R}$. In particular, all units are associated. Moreover, if $a = b * \epsilon$ and $\epsilon * \epsilon' = 1$, then $b = a * \epsilon'$.

2.1 Order on $\mathcal{R}$

Definition 3 *Let* rep*: $\mathcal{R} \longrightarrow \mathcal{R}$ be a selection function, called* **representative***, which picks a unique element for each associatedness equivalence class. We call* $\mathrm{rep}(a)$ *as the representative form of $a \in \mathcal{R}$.*

In the following, we assume that for each element in $\mathcal{R}$, its representative form is computable.

If a and b are associated, then $\mathrm{rep}(a) = \mathrm{rep}(b)$. An element a is called representative if and only if $\mathrm{rep}(a) = a$. In general, for any $u \in \mathrm{Units}(\mathcal{R})$, we set $\mathrm{rep}(u) = 1$. For example, for any field $\mathcal{F}$, if for any $z \in \mathcal{F} - \{0, 1\}$, $0 < 1 < z$ is defined, then the unique representative element is 1.

Given any $a \in \mathcal{R}$ and $b \in \mathcal{R} - \{0\}$, if there exists $q \in \mathcal{R}$ such that $a = q * b$, then we say b is a **divisor** of a, denoted by $b|a$. If $b|a$, i.e., $a = q * b$, then $\mathrm{rep}(b)|a$, because there exists a unit $\epsilon \in \mathcal{R}$ with $\epsilon * \mathrm{rep}(b) = b$ such that $a = (q * \epsilon) * \mathrm{rep}(b)$. Moreover, if $\mathrm{rep}(a) = \mathrm{rep}(b)$, i.e., a and b are associated, then there exist $\epsilon, \epsilon' \in \text{Units}(\mathcal{R})$ with $\epsilon * \epsilon' = 1$ such that $a = \epsilon * b$ and $b = \epsilon' * a$, so $a|b$ and $b|a$.

Definition 4 *Let $<$ be a partial well-founded order on $\mathcal{R}$. It is called a* **representable order** *if and only if (1) $\text{rep}(a) \leq a$ for each $a \in \mathcal{R}$, and (2) for any $a, b \in \mathcal{R} - \{0\}$, if $b|a$ then $\text{rep}(b) \leq \text{rep}(a)$, and (3) for any $a, b \in \mathcal{R}$, $\text{rep}(a)$ and $\text{rep}(b)$ are comparable under $<$.*

2.2 Division Algorithm and RGCD

Let $<$ be a representable order on $\mathcal{R}$ and $b \in \mathcal{R} - \{0\}$; an element b induces an equivalence relation on $\mathcal{R}$ as follows: $a =_b c$ if and only if there exists a q such that $a = q * b + c$. Given $a \in \mathcal{R}$, if a unique minimal element with respect to $<$ exists in the equivalence class induced by the equivalence relation $=_b$, then define the **remainder** r obtained by dividing a by b as the unique minimal element, denoted by $\text{rem}(a, b)$. Obviously $r \leq a$ as $a = 0 * b + a$. We say a can be **reduced** modulo b to r if $r < a$. If $\text{ANN}(b) \neq \{0\}$, then there exists $q' \in \mathcal{R}$ not equal to q, such that $a = q' * b + c$ with $\alpha = q' - q \in \text{ANN}(b)$, as $a = qb + c = (q + \alpha) * b + c = q' * b + c$. With the unique minimal remainder r, if a unique minimal element with respect to $<$ satisfying $a = q * b + r$ exists, then define the **quotient** q as the unique minimal element, denoted by $\text{quot}(a, b)$.

Definition 5 *Let $<$ be a representable order on $\mathcal{R}$, and let $a, b \in \mathcal{R} - \{0\}$. If $\alpha \in \mathcal{R}$ is representative and the greatest among all the representative common divisors of a and b under $<$, then α is called the* **representative greatest common divisor** *of a and b, denoted by $\text{rgcd}(a, b)$.*

Lemma 1 *Assume that there exist a representable order $<$ on $\mathcal{R}$ and a division algorithm, such that for any $a, b \in \mathcal{R} - \{0\}$, both $r = \text{rem}(a, b) < b$ and $q = \text{quot}(a, b)$ are computable such that $a = qb + r$. Then for any $a, b \in \mathcal{R} - \{0\}$, $\text{rgcd}(a, b)$ is computable. Moreover, there exist $\alpha, \beta \in \mathcal{R}$ such that $\text{rgcd}(a, b) = \alpha a + \beta b$.*

Proof: Given $a, b \in \mathcal{R} - \{0\}$, from the definition of D-A rings, we know $r = \text{rem}(a, b) < b$. If $r \neq 0$, then $r_2 = \text{rem}(b, r) < r$. If $r_2 \neq 0$, then $r_3 = \text{rem}(r, r_2) < r_2$. Continue this process, and it will terminate as $<$ is well-founded. Let $r_1 = r$ and $r_0 = b$, we get a finite sequence:

$$0 = r_{k+1} < r_k < \cdots < r_1 < r_0$$

where $r_{i+2} = \mathrm{rem}(r_i, r_{i+1})$ for any $i = 0, 1, \cdots, k-1$.

For any a and b, we show by induction on k that there exist $\alpha, \beta \in \mathcal{R}$ such that $\mathrm{rep}(r_k) = \mathrm{rgcd}(a, b) = \alpha a + \beta b$.

(1) Basis step: $k = 0$, i.e., $r_1 = r = 0$ and there exists $q = \mathrm{quot}(a, b)$ such that $a = q * b$. There exist $\epsilon, \epsilon' \in \mathrm{Units}(\mathcal{R})$ with $\epsilon\epsilon' = 1$ such that $b = \epsilon * \mathrm{rep}(b)$ and $a = q * b = (q\epsilon) * \mathrm{rep}(b)$, so $\mathrm{rep}(b)$ is a representative common divisor of a and b. If there exists another common divisor of a and b, say c, i.e., there exists a $q' \in \mathcal{R}$ such that $b = q' * c$, then $\mathrm{rep}(b) = \epsilon' b = \epsilon' q' c$, i.e., $c | \mathrm{rep}(b)$, so $\mathrm{rep}(c) \leq \mathrm{rep}(b)$. Since $r_0 = b$, we get $\mathrm{rgcd}(a, b) = \mathrm{rep}(b) = \mathrm{rep}(r_0)$, and $\mathrm{rgcd}(a, b) = \alpha a + \beta b$ where $\alpha = 0$ and $\beta = \epsilon'$.

(2) Inductive step: Given any $a', b' \in \mathcal{R} - \{0\}$ such that

$$0 = r'_{k+1} < r'_k < \cdots < r'_1 < r'_0 = b'$$

where $r'_1 = \mathrm{rem}(a', b')$, and $r'_{i+2} = \mathrm{rem}(r'_i, r'_{i+1})$ for any $i = 0, 1, \cdots, k-1$. Assume that there exist $\alpha', \beta' \in \mathcal{R}$ such that $\mathrm{rep}(r'_k) = \mathrm{rgcd}(a', b') = \alpha' a' + \beta' b'$.

Let $a, b \in \mathcal{R} - \{0\}$ such that

$$0 = r_{k+2} < r_{k+1} < \cdots < r_1 < r_0 = b$$

where $r_1 = \mathrm{rem}(a, b)$, and $r_{i+2} = \mathrm{rem}(r_i, r_{i+1})$ for any $i = 0, 1, \cdots, k$.

By the induction hypothesis, there exist $\alpha', \beta' \in \mathcal{R}$ such that $\mathrm{rep}(r_{k+1}) = \mathrm{rgcd}(b, r_1) = \alpha' b + \beta' r_1$. Since $r_1 = \mathrm{rem}(a, b)$, there exists $q = \mathrm{quot}(a, b)$ such that $a = q * b + r_1$, then from $\mathrm{rep}(r_{k+1}) = \mathrm{rgcd}(b, r_1)$ we have $\mathrm{rep}(r_{k+1}) | a$, i.e., $\mathrm{rep}(r_{k+1})$ is a representative common divisor of a and b. If there exists another common divisor of a and b, say c, i.e., $c|a$ and $c|b$, then from $a = qb + r_1$, we have $c|r_1$. Since $\mathrm{rep}(r_{k+1}) = \alpha' b + \beta' r_1$, we get $c|\mathrm{rep}(r_{k+1})$, then $\mathrm{rep}(c) \leq \mathrm{rep}(r_{k+1})$. So $\mathrm{rgcd}(a, b) = \mathrm{rep}(r_{k+1})$. Moreover, let $\alpha = \beta'$ and $\beta = \alpha' - q\beta'$, we get $\mathrm{rgcd}(a, b) = \alpha' b + \beta' r_1 = \alpha' b + \beta'(a - q * b) = \alpha a + \beta b$.

Hence the proof. ■

In fact, an algorithm to compute the rgcd of any two elements in $\mathcal{R}$ follows from the above proof of Lemma 1.

Lemma 2 *Assume that (1) a well-founded order $<$ is defined on $\mathcal{R}$ such that for any $a, b \in \mathcal{R} - \{0\}$, if $b|a$ then $\mathrm{rep}(b) \leq \mathrm{rep}(a)$; and (2) there is a rgcd algorithm such that for any $a, b \in \mathcal{R} - \{0\}$, $\mathrm{rgcd}(a, b)$ is computable. Then $\mathcal{R}$ is Noetherian.*

Proof: At first, there is a unique minimal nonzero representative element in any nonzero ideal of $\mathcal{R}$. If not, say there are at least two minimal nonzero representative elements, a and b. By the assumptions, $\text{rgcd}(a, b) \leq \text{rep}(a) = a$ and $\text{rgcd}(a, b) \leq \text{rep}(b) = b$. Further, since both a and b are minimal, $\text{rgcd}(a, b) < a$ and $\text{rgcd}(a, b) < b$. But $\text{rgcd}(a, b)$ is in the ideal, i.e., a or b is not minimal in the ideal, this leads to a contradiction.

It is shown that any nonzero ideal of $\mathcal{R}$ can be generated by the unique minimal nonzero representative element a in the ideal. If not, say there is a nonzero element b in the ideal, such that $b \neq q * a$ for any $q \in \mathcal{R}$. By the assumptions, $\text{rgcd}(a, b) \leq \text{rep}(a) = a$. Further, since $a \not| b$, $\text{rgcd}(a, b) < a$. But $\text{rgcd}(a, b)$ is in the ideal, i.e., a is not the minimal nonzero representative element in the ideal, there is a contradiction. Thus, any nonzero ideal of $\mathcal{R}$ is principal, which implies that $\mathcal{R}$ is Noetherian. ■

2.3 Annihilators on $\mathcal{R}$

Definition 6 *Let $c \in \mathcal{R} - \{0\}$. An element $a \in \mathcal{R}$ is called an annihilator of c if $c * a = 0$. The set of all annihilators of c is called the annihilator set of c, denoted by* $\text{ANN}(c)$*, i.e.,* $\text{ANN}(c) = \{a \in \mathcal{R} | a * c = 0\}$.

For any $c \in \mathcal{R}$, $0 \in \text{ANN}(c)$, and if c is not a zero divisor, then $\text{ANN}(c) = \{0\}$. Moreover, if $0 \neq a \in \text{ANN}(c)$, then $\text{rep}(a) \in \text{ANN}(c)$.

If c is not a zero divisor, it is easy to see that $\text{ANN}(c)$ is an nonzero ideal of $\mathcal{R}$. Then by Lemma 2, under the assumptions in the lemma, $\text{ANN}(c)$ can be generated by the unique minimal nonzero representative element in $\text{ANN}(c)$, we denote it as $\mathbf{ann(c)}$. If c is not a zero divisor, then define $\text{ann}(c) = 0$.

2.4 D-A rings

Definition 7 *Let $\mathcal{R}$ be a commutative ring with the identity element 1. $\mathcal{R}$ is called a* **divisible and annihilable ring***, simply denoted by a* **D-A ring** *or* **DAR***, if and only if*

(1) For each element in $\mathcal{R}$, its representative form is computable.

(2) There exist a representable order $<$ on $\mathcal{R}$ and a division algorithm, such that for any $a, b \in \mathcal{R} - \{0\}$, both $r = \text{rem}(a, b) < b$ and $q = \text{quot}(a, b)$ are computable such that $a = qb + r$.

(3) For any $c \in \mathcal{R} - \{0\}$, $\text{ann}(c)$ *is computable.*

A field or a Euclidean domain is a D-A ring. A D-A ring can have zero-divisors, whereas there are no zero-divisors in a Euclidean domain; it is easy to see that both the ring of integers modulo n ($\mathbb{Z}_n$) and the ring of Gaussian integers modulo n ($\mathbb{Z}_n[i]$), where n is any non-prime integer, are D-A rings.

A representable order for a D-A ring does not have to be total; instead, it can be partial. For example, for any field $\mathcal{F}$, one possible ordering is $0 < 1 < z$ for any other $z \in \mathcal{F} - \{0, 1\}$, where 1 is picked as the representative form of any nonzero element in $\mathcal{F}$; for the integer ring $\mathbb{Z}$, the ordering $0 < 1 < 2 < 3 < \cdots$ and $a < -b$ for any positive integers a, b (i.e., negative integers are not comparable with each other) works, where positive integer a is picked as the representative form of $\pm a$; and so on.

As the reader saw, there can be distinct multiple representable orders on a D-A ring. But for convenience, we assume below

(1) a representable order $<_{\mathbb{Z}}$ on $\mathbb{Z}$ is always defined as follows: for any $a, b \in \mathbb{Z}$, $a <_{\mathbb{Z}} b$ if and only if (i) $|a| < |b|$ or (ii) $a = -b > 0$. That is,

$$0 < 1 < -1 < 2 < -2 < 3 < -3 < \cdots .$$

(2) a representable order $<_{\mathbb{Z}_n}$ on $\mathbb{Z}_n := \{0, 1, \cdots, n-1\}$ is always defined as follows: for any $a, b \in \mathbb{Z}_n$, $a <_{\mathbb{Z}_n} b$ if and only if $\min_{<_{\mathbb{Z}}}(a, a \pm n) <_{\mathbb{Z}} \min_{<_{\mathbb{Z}}}(b, b \pm n)$. That is,

$$0 < 1 < n-1 < 2 < n-2 < \cdots < [\frac{n+1}{2}].$$

For example, the representable order $<$ on $\mathbb{Z}_6$ is: $0 < 1 < 5 < 2 < 4 < 3$.

(3) a representable order $<_{\mathbb{Z}[i]}$ on $\mathbb{Z}[i]$ with $i^2 = -1$ is always defined as follows: for any $a, b, \alpha, \beta \in \mathbb{Z}$, $a + bi <_{\mathbb{Z}[i]} \alpha + \beta i$ if and only if (1) $a^2 + b^2 < \alpha^2 + \beta^2$ or (2) $a^2 + b^2 = \alpha^2 + \beta^2$ and $b <_{\mathbb{Z}} \beta$ or (3) $b = \beta$ and $a <_{\mathbb{Z}} \alpha$. That is,

$$0 < 1 < -1 < i < -i < 1+i < -1+i < 1-i < -1-i < 2 < -2 < \cdots .$$

(4) a representable order on $\mathbb{Z}_n[i]$ with $i^2 = -1$ is always defined as follows: for any $a, b, \alpha, \beta \in \mathbb{Z}_n$, $a+bi <_{\mathbb{Z}_n[i]} \alpha+\beta i$ if and only if $\min_{<_{\mathbb{Z}}}(a, a\pm n) + \min_{<_{\mathbb{Z}}}(b, b\pm n)i \;<_{\mathbb{Z}[i]}\; \min_{<_{\mathbb{Z}}}(\alpha, \alpha\pm n) + \min_{<_{\mathbb{Z}}}(\beta, \beta\pm n)i$. For example, on $\mathbb{Z}_3[i]$, the order is: $0 < 1 < 2 < i < 2i < 1+i < 2+i < 1+2i < 2+2i$.

2.5 Properties of D-A rings

By Lemma 1, there is a rgcd algorithm on D-A rings. Moreover, by Lemma 2, D-A rings are Noetherian. Below, we assume $\mathcal{R}$ to be a D-A ring with a representable order $<$ on $\mathcal{R}$.

Lemma 3 *Let $c \in \mathcal{R}$, $\mathrm{ann}(c) \neq 0$ and $a \in \mathrm{ANN}(c)$, then $\mathrm{ann}(c)|a$.*

Proof: If there exists an $a \in \mathrm{ANN}(c)$ such that $\mathrm{ann}(c) \not| a$, then from Lemma 1, we have $b = \mathrm{rgcd}(\mathrm{ann}(c), a) \in \mathcal{R}$ such that $b|\mathrm{ann}(c)$, then $b = \mathrm{rep}(b) \leq \mathrm{ann}(c)$.

Moreover, there exist $\alpha, \beta \in \mathcal{R}$ such that $b = \alpha * \mathrm{ann}(c) + \beta a$, then $b * c = (\alpha * \mathrm{ann}(c) + \beta a) * c = 0$, i.e., $b \in \mathrm{ANN}(c)$. According to the definition of $\mathrm{ann}(c)$, we have $\mathrm{ann}(c) \leq b$. Thus $b = \mathrm{ann}(c)$, and this leads to a contradiction with $\mathrm{ann}(c) \not| a$. ■

Further, since the representable order $<$ on $\mathcal{R}$ is Noetherian and $\mathrm{ANN}(c)$ is an ideal of $\mathcal{R}$, $\mathrm{ANN}(c)$ has a finite generating set $\{a_1, \cdots, a_k\}$. By the above lemma 3, we know $\mathrm{ann}(c)$ is a common divisor of $a_1, \cdots, a_k$. By Lemma 1, $\mathrm{rgcd}(a_1, \cdots, a_k) \in \mathrm{ANN}(c)$, then $\mathrm{ann}(c)|\mathrm{rgcd}(a_1, \cdots, a_k)$, so $\mathrm{ann}(c) \leq \mathrm{rgcd}(a_1, \cdots, a_k)$. Since $\mathrm{ann}(c)$ can be generated by $\{a_1, \cdots, a_k\}$, we get $\mathrm{rgcd}(a_1, \cdots, a_k)|\mathrm{ann}(c)$, so $\mathrm{rgcd}(a_1, \cdots, a_k) \leq \mathrm{ann}(c)$. Hence, $\mathrm{ann}(c) = \mathrm{rgcd}(a_1, \cdots, a_k)$.

Lemma 4 *Let $a, b \in \mathcal{R} - \{0\}$, then $\mathrm{rem}(a, b) < \mathrm{rep}(b)$.*

Proof: By the definition of D-A rings, we can assume $a = q * \mathrm{rep}(b) + r'$, where $r' = \mathrm{rem}(a, \mathrm{rep}(b)) < \mathrm{rep}(b)$. Let $\mathrm{rep}(b) = b * \epsilon$, where $\epsilon \in \mathrm{Units}(\mathcal{R})$.

Since $a = q * \mathrm{rep}(b) + r' = (q\epsilon) * b + r'$, it follows that $\mathrm{rem}(a, b) \leq r'$, then $\mathrm{rem}(a, b) < \mathrm{rep}(b)$. ■

If two nonzero elements are comparable, then the bigger element is reducible modulo the smaller from the definition of D-A rings. Further, we have the following lemma:

Lemma 5 *Let $a, b \in \mathcal{R} - \{0\}$, and $\mathrm{rep}(b) \leq \mathrm{rep}(a)$. Then a is reducible modulo b.*

Proof: According to the definition of D-A rings, there exist $q, r \in \mathcal{R}$ such that $a = q * b + r$, where $r = \mathrm{rem}(a, b) < b$. Further, from the definition of the remainder, we have $r \leq a$. If $r < a$, then a is reducible modulo b;

otherwise, $r = a$, by Lemma 4, $\text{rep}(a) \leq a = r = \text{rem}(a, b) < \text{rep}(b)$. This leads to a contradiction with the assumption $\text{rep}(b) \leq \text{rep}(a)$. ■

Lemma 6 *Let $a, b, c_1, c_2 \in \mathcal{R} - \{0\}$ with $b = \text{rem}(a, c_1)$ and $c_2|b$. Then $\text{rep}(c_2) < \text{rep}(c_1)$, and $\text{rem}(c_1, c_2) < b$.*

Proof: By Lemma 4, $b = \text{rem}(a, c_1) < \text{rep}(c_1)$. Since $c_2|b$, it follows that $\text{rep}(c_2) \leq \text{rep}(b) \leq b$. Then $\text{rep}(c_2) < \text{rep}(c_1)$. By Lemma 4, $\text{rem}(c_1, c_2) < \text{rep}(c_2)$. Then $\text{rem}(c_1, c_2) < b$. ■

3 Gröbner basis of a Polynomial Ideal

In the following, we assume that $\mathcal{R}$ is a D-A ring, and $\mathcal{R}[\bar{x}]$ is a polynomial ring in the variables $\bar{x} =< x_1, \cdots, x_d >$. Further, an admissible term order[2] is defined such that we can define the leading (head) term, the leading coefficient, and the leading monomial of a given polynomial $p \in \mathcal{R}[\bar{x}]$, denoted by $\text{lt}(p)$, $\text{lc}(p)$, and $\text{lm}(p)$, respectively. Moreover, we denote $p - \text{lm}(p)$ by $\text{rest}(p)$.

For convenience, if we say $m = ct$ is a monomial in $\mathcal{R}[\bar{x}]$, then usually it means that $c \in \mathcal{R} - \{0\}$ is the coefficient and that t is the term in $\mathcal{R}[\bar{x}]$ of m. Let t_1 and t_2 are terms in $\mathcal{R}[\bar{x}]$, we say $t_1|t_2$ if and only if there exists a term $s \in \mathcal{R}[\bar{x}]$ such that $t_2 = st_1$. Moreover, let $m_1 = c_1t_1$ and $m_2 = c_2t_2$ are monomials in $\mathcal{R}[\bar{x}]$, we say $m_1|m_2$ if and only if $c_1|c_2$ and $t_1|t_2$.

3.1 Well-founded order on a Polynomial Ring

An admissible term order on $\mathcal{R}[\bar{x}]$ and a representable order on $\mathcal{R}$ defines a well-founded order $<$ on polynomials in $\mathcal{R}[\bar{x}]$ in a natural way:

Definition 8 *For any two polynomials $f, g \in \mathcal{R}[\bar{x}]$, $f < g$ if and only if*
(1) $\text{lt}(f) < \text{lt}(g)$
or (2) $\text{lt}(f) = \text{lt}(g)$ *and lc*$(f) < \text{lc}(g)$
or (3) $\text{lm}(f) = \text{lm}(g)$ *and* $\text{rest}(f) < \text{rest}(g)$.

[2] $<$ is an admissible term order iff $<$ is total and for any terms s, t, u: (1) $1 \leq s$; (2) $s \leq t \Rightarrow su \leq tu$

3.2 Polynomials as Rewrite Rules

Let $p = \mathrm{lm}(p) + \mathrm{rest}(p) \in \mathcal{R}[\bar{x}] - \{0\}$. The rewrite rule corresponding to p is:

$$\mathrm{lm}(p) \longrightarrow -\mathrm{rest}(p).$$

If p is a monomial, then the right-hand side of its rule is 0.

Definition 9 *Let $f, g, p \in \mathcal{R}[\bar{x}]$. f* **reduces** *to g* **modulo** *p, denoted by $f \longrightarrow_p g$, if and only if there exists a monomial $m = at$ in f such that $\mathrm{lt}(p)|t$, say $t = s * \mathrm{lt}(p)$, and*

$$g = f - qsp = rt - qs * \mathrm{rest}(p) + f_1,$$

where $q = \mathrm{quot}(a, \mathrm{lc}(p))$, $r = \mathrm{rem}(a, \mathrm{lc}(p)) < \mathrm{lc}(p)$ and $f_1 = f - at$.

Let G be a finite set of polynomials in $\mathcal{R}[\bar{x}]$. A polynomial f reduces to g modulo G, denoted by $f \longrightarrow_G g$, if and only if there exists $p \in G$ such that $f \longrightarrow_p g$.

This definition of a rewriting relation is similar to the definition in [8, 9].

Theorem 1 *Given any finite basis G of polynomials in $\mathcal{R}[\bar{x}]$, the rewriting relation $\longrightarrow_G$ induced by G is Noetherian.*

Proof: Given any polynomial $p \in G$, and let $f, g \in R[\bar{x}]$ and $f \longrightarrow_p g$. Let $f = ct + f_1$, and ct be a monomial in f that can be rewritten using the rule corresponding to p. Let $r = \mathrm{rem}(c, \mathrm{lc}(p))$, then $r < c$.

This $\longrightarrow_p$ either eliminates the monomial ct from f when $r = 0$, in which case $g < f$, or replaces the coefficient c by r upon division by $\mathrm{lc}(p)$ with $r < c$ while leaving all higher monomials unchanged, in which case we see that again $g < f$. Considering that the order on $\mathcal{R}[\bar{x}]$ is well-founded, we have thus proved that $\longrightarrow_G$ is Noetherian. ■

3.3 A-polynomials

Definition 10 *Let $f = ct + \mathrm{rest}(f) \in \mathcal{R}[\bar{x}] - \{0\}$ where $ct = \mathrm{lm}(f)$, and*

$$g = \mathrm{ann}(c) * f = \mathrm{ann}(c) * \mathrm{rest}(f).$$

The polynomial g is called the **A-polynomial** *of f, denoted by $\mathrm{apol}(f)$.*

Let $f \in \mathcal{R}[\bar{x}] - \{0\}$; if $\mathrm{ann}(\mathrm{lc}(f)) = 0$, then $\mathrm{apol}(f) = 0$.

Given $f = ct + \mathrm{rest}(f) \in \mathcal{R}[\bar{x}] - \{0\}$ where $ct = \mathrm{lm}(f)$, let $g_1 = c_1t_1 + \mathrm{rest}(g_1) \neq 0$ be the A-polynomial of f where $c_1t_1 = \mathrm{lm}(g_1)$, i.e.,

$$g_1 = \mathrm{apol}(f) = \mathrm{ann}(c) * \mathrm{rest}(f).$$

We have

$$g_2 = \mathrm{ann}(c_1) * g_1 = \mathrm{ann}(c_1) * \mathrm{rest}(g_1)$$

is the A-polynomial of g_1. We denote $g_2 = \mathrm{apol}(g_1) = \mathrm{apol}^2(f)$. If $g_2 \neq 0$, we can continue this process until $\mathrm{apol}(g_l) = \mathrm{apol}^{l+1}(f) = 0$ for some $l \in \mathbb{N}$. This process will terminate after at most k steps where k is the number of terms in f.

We get a finite sequence of A-polynomials, $g_1, \cdots, g_l$, where $g_i = \mathrm{apol}^i(f) \neq 0$ for all $i = 1, \cdots, l$, and $\mathrm{apol}(g_l) = 0$.

Definition 11 *Let $f \in \mathcal{R}[\bar{x}]$ such that $\mathrm{apol}^i(f) \neq 0$ for $1 \leq i \leq l$, and $\mathrm{apol}^{l+1}(f) = 0$. The set of all the A-polynomials, $\bigcup_{i=1}^{l}\{\mathrm{apol}^i(f)\}$ is called the saturated A-polynomials set generated by f, denoted by $\mathrm{SAP}(f)$.*

Let G be a finite set of polynomials in $\mathcal{R}[\bar{x}]$, the saturated A-polynomials set generated by all polynomials in G is denoted by $\mathrm{SAP}(G) = \{g | \exists f \in G, \ s.t. \ g \in \mathrm{SAP}(f)\}$.

For example, let $f = 15x^4 + 5x^3 - x^2 + 2x - 3 \in \mathbb{Z}_{30}[x]$, we have

$$\begin{aligned} g_1 &= \mathrm{apol}(f) = \mathrm{ann}(15) * (5x^3 - x^2 + 2x - 3) = 10x^3 - 2x^2 + 4x - 6, \\ g_2 &= \mathrm{apol}(g_1) = \mathrm{ann}(10) * (-2x^2 + 4x - 6) = -6x^2 + 12x - 18, \\ g_3 &= \mathrm{apol}(g_2) = \mathrm{ann}(-6) * (12x - 18) = 0. \end{aligned}$$

Then $\mathrm{SAP}(f) = \{g_1, g_2\}$.

Let $f = ct + \mathrm{rest}(f) \in \mathcal{R}[\bar{x}] - \{0\}$ where $ct = \mathrm{lm}(f)$. Let $g_i = c_it_i + \mathrm{rest}(g_i) = \mathrm{apol}^i(f)$ where $c_it_i = \mathrm{lm}(g_i)$. Then

$$g_i = \mathrm{apol}^i(f) = \mathrm{ann}(c_{i-1}) * \cdots * \mathrm{ann}(c_1) * \mathrm{ann}(c) * f$$

for $1 \leq i \leq l$. So $\mathrm{SAP}(f)$ is a subset of the ideal generated by f, i.e., $\mathrm{SAP}(f) \subseteq \mathrm{Id}(f)$, where $\mathrm{Id}(f)$ is the ideal of f. If G is a finite set of polynomials in $\mathcal{R}[\bar{x}]$, then $\mathrm{SAP}(G) \subseteq \mathrm{Id}(G)$, where $\mathrm{Id}(G)$ is the ideal of G.

Lemma 7 *Let $p \in \mathcal{R}[\bar{x}] - \{0\}$ and $f = mp \neq 0$ with a monomial $m = as$. If $a * \mathrm{lc}(p) = 0$, then there exist $k \geq 1$ and $a_k \in \mathcal{R}$ such that $f = a_ks * \mathrm{apol}^k(p)$, and $a_k * \mathrm{lc}(\mathrm{apol}^k(p)) \neq 0$.*

Proof: Since $a * \mathrm{lc}(p) = 0$, by Lemma 3, there exists $a_1 \in \mathcal{R}$ such that $a = a_1 * \mathrm{ann}(c)$. Then $f = mp = a_1 s * (\mathrm{ann}(c) * p) = a_1 s * \mathrm{apol}(p)$.

If $a_1 * \mathrm{lc}(\mathrm{apol}(p)) = 0$, then by Lemma 3, there exists $a_2 \in \mathcal{R}$ such that $a_1 = a_2 * \mathrm{ann}(\mathrm{lc}(\mathrm{apol}(p)))$. Then $f = mp = a_1 s * \mathrm{apol}(p) = a_2 s * \mathrm{apol}^2(p)$.

If $a_2 * \mathrm{lc}(\mathrm{apol}^2(p)) = 0$, continue the above process. This process terminates since $\mathrm{SAP}(p)$ is finite. Since $f \neq 0$, we can assume that

$$f = mp = a_1 s * \mathrm{apol}(p) = \cdots = a_k s * \mathrm{apol}^k(p)$$

such that $a_k * \mathrm{lc}(\mathrm{apol}^k(p)) \neq 0$.

■

3.4 Rewriting Relation and Ideal Congruence

For convenience, we assume below that G is a finite set of polynomials in $\mathcal{R}[\bar{x}]$, rewriting relations $\longrightarrow$ are of modulo G, $\longrightarrow^*$ is the reflexive-transitive closure of $\longrightarrow$, $\longrightarrow^+$ is the transitive closure of $\longrightarrow$, and $\longrightarrow^k$ means k steps of $\longrightarrow$ for some integer k.

Under the assumption that every polynomial in $\mathrm{SAP}(G)$ can reduce to 0 modulo G, it must be shown that the rewriting relation as defined in subsection 3.2 is strong enough to capture the ideal congruence relation, i.e., the reflexive, symmetric and transitive closure of the relation $\longrightarrow$ for G denoted as $\longleftrightarrow_G^*$, is indeed the ideal congruence relation $=_{\mathrm{Id}(G)}$, and $f =_{\mathrm{Id}(G)} g$ if and only if $f = g + \sum_{i=1}^n h_i p_i$ for some $h_1, \cdots, h_n \in \mathcal{R}[\bar{x}]$ and some $p_1, \cdots, p_n \in G$.

Lemma 8 *Let $p \in G$, $f, g \in \mathcal{R}[\bar{x}]$ and $f = g + asp$, where $a \in \mathcal{R} - \mathrm{ANN}(\mathrm{lc}(p))$, s is a term. Then there exist $\alpha \in \mathcal{R}$ and $f', g' \in \mathcal{R}[\bar{x}]$ such that $f \longrightarrow_p^* f'$, $g \longrightarrow_p^* g'$, and $f' - g' = \alpha s * \mathrm{apol}(p)$.*

Proof: Let $p = ct_1 + \mathrm{rest}(p)$ with $ct_1 = \mathrm{lm}(p)$. Then $t = \mathrm{lt}(asp) = st_1$ and $b_1 = \mathrm{lc}(asp) = ac \neq 0$ as $a \in \mathcal{R} - \mathrm{ANN}(\mathrm{lc}(p))$. Let $g = b_2 t + g_1$ such that g_1 has no term t. Let $b_2 = q_2 c + r$, where $r = \mathrm{rem}(b_2, c) \leq b_2$ and $q_2 = \mathrm{quot}(b_2, c)$. Then $f = g + asp = (b_2 t + g_1) + (b_1 t + as * \mathrm{rest}(p)) = (b_1 + b_2)t + (g_1 + as * \mathrm{rest}(p))$.

Let $b = b_1 + b_2 = qc + r'$, where $r' = \mathrm{rem}(b, c) \leq b$ and $q = \mathrm{quot}(b, c)$. Since $b = b_1 + b_2 = (a + q_2)c + r$, $r' = \mathrm{rem}(b, c) \leq r$. Since $b_2 = b - b_1 = (q - a)c + r'$, $r = \mathrm{rem}(b_2, c) \leq r'$. Then $r = r'$, i.e., $b = qc + r$ with $r = \mathrm{rem}(b, c) \leq b$.

Moreover, from $b = qc + r = (a + q_2)c + r$, we get $a + q_2 - q \in \mathrm{ANN}(c)$, then there exists $\alpha \in \mathcal{R}$ such that $a + q_2 - q = \alpha * \mathrm{ann}(c)$.

(1) If $r < b_2$, then $g \longrightarrow_p g' = rt + q_2 s * \mathrm{rest}(p) + g_1$; otherwise, i.e., $r = b_2$ and $q_2 = 0$, let $g' = g$.

(2) If $r < b$, then $f \longrightarrow_p f' = rt + (q + a)s * \mathrm{rest}(p) + g_1$; otherwise, i.e., $r = b$ and $q = 0$, let $f' = f$.

The polynomial $g \longrightarrow_p^* g'$ and $f \longrightarrow_p^* f'$. Moreover, $f' - g' = (q + a - q_2)s * \mathrm{rest}(p) = \alpha s * \mathrm{apol}(p)$. Hence the proof. ■

Lemma 9 *Assume that every polynomial in* $\mathrm{SAP}(G)$ *can reduce to 0 modulo* G*. Let* $p \in G$*, then there exist* $h_1, \cdots, h_k \in \mathcal{R}[\bar{x}]$ *and* $p_1, \cdots, p_k \in G$ *such that* $\mathrm{apol}(p) = \sum_{i=1}^{k} h_i p_i$*, and* $\mathrm{lt}(p_i) < \mathrm{lt}(p)$ *for* $1 \leq i \leq k$*.*

Proof: By the assumption that every polynomial in $\mathrm{SAP}(G)$ can reduce to 0 modulo G, we have $\mathrm{apol}(p) \longrightarrow_G^k 0$ for some $k \geq 0$, it is easy to show by induction on k that there exist $h_1, \cdots, h_k \in \mathcal{R}[\bar{x}]$ and $p_1, \cdots, p_k \in G$ such that $\mathrm{apol}(p) = \sum_{i=1}^{k} h_i p_i$, and $\mathrm{lt}(p_i) \leq \mathrm{lt}(\mathrm{apol}(p)) < \mathrm{lt}(p)$ for $1 \leq i \leq k$. ■

Theorem 2 *Assume that every polynomial in* $\mathrm{SAP}(G)$ *can reduce to 0 modulo* G*. Then* $\longleftrightarrow_G^* = =_{\mathrm{Id}(G)}$*.*

Proof: $(\subseteq)$ $\longleftrightarrow_G^* \subseteq =_{\mathrm{Id}(G)}$: It is trivial to show this by induction that for every k, $\longleftrightarrow_G^k \subseteq =_{\mathrm{Id}(G)}$.

$(\supseteq)$ $\longleftrightarrow_G^* \supseteq =_{\mathrm{Id}(G)}$: Let $G = \{p_1, \cdots, p_n\}$. $f =_{\mathrm{Id}(G)} g$ implies $f = g + \sum_{i=1}^{n} h_i p_i$, where $h_i \in \mathcal{R}[\bar{x}]$ for $1 \leq i \leq n$. Without loss of generality, we assume that $\mathrm{lt}(p_1) \leq \mathrm{lt}(p_2) \leq \cdots \leq \mathrm{lt}(p_n)$ under the order $<$ defined in the subsection 3.1. We show that $f \longleftrightarrow_G^* g$ by induction on n.

(1) Basis Step: $n = 0$: obvious.

(2) Inductive Step: Given $n > 0$, let $\hat{f}, \hat{g} \in \mathcal{R}[\bar{x}]$ such that $\hat{f} = \hat{g} + \sum_{i=1}^{n-1} \hat{h}_i p_i$, where $\hat{h}_1, \cdots, \hat{h}_{n-1} \in \mathcal{R}[\bar{x}]$. Assume that $\hat{f} \longleftrightarrow_G^* \hat{g}$ for such $\hat{f}$ and $\hat{g}$.

Let $f = g + \sum_{i=1}^{n} h_i p_i$, and $g' = g + h_n p_n$, then by the induction hypothesis, we have $f \longleftrightarrow_G^* g'$.

Given any monomial as, and let $f_1, f_2 \in \mathcal{R}[\bar{x}]$ such that $f_1 = f_2 + asp_n$, there are two cases:

Case 1: $a \in \mathrm{ANN}(\mathrm{lc}(p_n))$. Then there exists $\hat{a} \in \mathcal{R}$ such that $a = \hat{a} * \mathrm{ann}(\mathrm{lc}(p_n))$, then $asp_n = \hat{a}s * \mathrm{apol}(p_n)$. By Lemma 9, there exist $h'_1, \cdots, h'_{n-1} \in \mathcal{R}[\bar{x}]$ such that $\mathrm{apol}(p_n) = \sum_{i=1}^{n-1} h'_i p_i$. Then, $asp_n = \hat{a}s * \mathrm{apol}(p_n) = \sum_{i=1}^{n-1} (\hat{a}sh'_i)p_i$. By the induction hypothesis, $f_1 \longleftrightarrow^*_G f_2$.

Case 2: $a \notin \mathrm{ANN}(\mathrm{lc}(p_n))$. By Lemma 8, there exist $\alpha \in \mathcal{R}$ and $f'_1, f'_2 \in \mathcal{R}[\bar{x}]$ such that $f_1 \longrightarrow^*_G f'_1$, $f_2 \longrightarrow^*_G f'_2$, and $f'_1 - f'_2 = \alpha s * \mathrm{apol}(p_n)$. By Lemma 9, there exist $h'_1, \cdots, h'_{n-1} \in \mathcal{R}[\bar{x}]$ such that $\mathrm{apol}(p_n) = \sum_{i=1}^{n-1} h'_i p_i$. Thus, $\alpha s * \mathrm{apol}(p_n) = \sum_{i=1}^{n-1} (\alpha sh'_i)p_i$. Then by the induction hypothesis, $f'_1 \longleftrightarrow^*_G f'_2$, it follows that

$$f_1 \longrightarrow^*_G f'_1 \longleftrightarrow^*_G f'_2 \longleftarrow^*_G f_2.$$

According to the above two cases, it is easy to show that $g' \longleftrightarrow^*_G g$ by induction on the number of terms of h_n. Therefore, $f \longleftrightarrow^*_G g' \longleftrightarrow^*_G g$.

Hence the proof. ■

3.5 Test for a Gröbner basis

Definition 12 *Let G be a finite set of polynomials in $\mathcal{R}[\bar{x}]$. G is a* **Gröbner basis** *of* $\mathrm{Id}(G)$ *if every polynomial in* $\mathrm{Id}(G)$ *can reduce to 0 modulo G.*

Given $c_1, c_2 \in \mathcal{R} - \{0\}$, if $\mathrm{rep}(c_1) \geq \mathrm{rep}(c_2)$, then by Lemma 5, it follows that c_1 is reducible modulo c_2, i.e., $\mathrm{rem}(c_1, c_2) < c_1$. We have the following definition:

Definition 13 *Let $p_i = c_i t_i + \mathrm{rest}(p_i) \in \mathcal{R}[\bar{x}]$, where $c_i t_i = \mathrm{lm}(p_i)$. Let $\mathrm{rep}(c_1) \geq \mathrm{rep}(c_2)$ and $t = \mathrm{lcm}(t_1, t_2) = s_i t_i$ for $i = 1, 2$. Let $q = \mathrm{quot}(c_1, c_2)$ and $r = \mathrm{rem}(c_1, c_2) < c_1$. The* **S-polynomial** *of p_1 and p_2 is $rt - qs_2 * \mathrm{rest}(p_2) + s_1 * \mathrm{rest}(p_1) = s_1 p_1 - qs_2 p_2$, denoted by $\mathrm{spol}(p_1, p_2)$.*

Lemma 10 *Assume that for every pair of polynomials in G, every S-polynomial can reduce to 0 under $\longrightarrow^*$. Then for any $f \in \mathcal{R}[\bar{x}]$ with $f \longrightarrow^* 0$, there exists $p \in G$ such that $\mathrm{lm}(p) | \mathrm{lm}(f)$.*

Proof: Let $f \longrightarrow^* 0$. We show that there exists $p \in G$ such that $\mathrm{lm}(p)|\mathrm{lm}(f)$ by induction on f using the well-founded order $<$ defined in subsection 3.1.

(1) Basis step: $f = 0$, obvious.

(2) Inductive step: For any $g < f$ with $g \longrightarrow^* 0$, assume that there exists $h \in G$ such that $\mathrm{lm}(h)|\mathrm{lm}(g)$.

Let $f = at + \mathrm{rest}(f) \in \mathcal{R}[\bar{x}] - \{0\}$ with $f \longrightarrow^+ 0$. Among all rules used in $f \longrightarrow^+ 0$, there exists $p_1 \in G$ with $c_1t_1 = \mathrm{lm}(p_1)$ such that $at = \mathrm{lm}(f)$ can be rewritten by p_1, i.e., $t_1|t$ and $b_1 = \mathrm{rem}(a, c_1) < a$. That is, we can assume

$$f \longrightarrow^* f' \longrightarrow_{p_1} g \longrightarrow^* 0.$$

If $b_1 \neq 0$, then $\mathrm{lm}(g) = b_1t$. Since $g \longrightarrow^* 0$ with $g < f$, by the induction hypothesis, it follows that there exists $p_2 \in G$ with $c_2t_2 = \mathrm{lm}(p_2)$ such that $\mathrm{lm}(p_2)|\mathrm{lm}(g)$, i.e., $t_2|t$ and $c_2|b_1$. By Lemma 6, $\mathrm{rep}(c_2) < \mathrm{rep}(c_1)$ and $b_2 = \mathrm{rem}(c_1, c_2) < b_1$. Moreover, since $t_1|t$ and $t_2|t$, it follows that $\mathrm{lcm}(t_1, t_2)|t$.

If $b_2 \neq 0$, then $\mathrm{lm}(\mathrm{spol}(p_1, p_2)) = b_2\mathrm{lcm}(t_1, t_2) < at = \mathrm{lm}(f)$, i.e., $\mathrm{spol}(p_1, p_2) < f$. By the assumption, $\mathrm{spol}(p_1, p_2) \longrightarrow^* 0$. By the induction hypothesis, there exists $p_3 \in G$ with $c_3t_3 = \mathrm{lm}(p_3)$ such that $\mathrm{lm}(p_3)|\mathrm{lm}(\mathrm{spol}(p_1, p_2))$, i.e., $t_3|t$ and $c_3|b_2$. By Lemma 6, $\mathrm{rep}(c_3) < \mathrm{rep}(c_2)$ and $b_3 = \mathrm{rem}(c_2, c_3) < b_2$. Moreover, since $t_2|t$ and $t_3|t$, it follows that $\mathrm{lcm}(t_2, t_3)|t$.

If $b_3 \neq 0$, then $\mathrm{lm}(\mathrm{spol}(p_2, p_3)) = b_3\mathrm{lcm}(t_2, t_3) < at = \mathrm{lm}(f)$, i.e., $\mathrm{spol}(p_2, p_3)) < f$. By the assumption, $\mathrm{spol}(p_2, p_3) \longrightarrow^* 0$. By the induction hypothesis, there exists $p_4 \in G$ with $c_4t_4 = \mathrm{lm}(p_4)$ such that $\mathrm{lm}(p_4)|\mathrm{lm}(\mathrm{spol}(p_2, p_3))$, i.e., $t_4|t$ and $c_4|b_3$. By Lemma 6, $\mathrm{rep}(c_4) < \mathrm{rep}(c_3)$ and $b_4 = \mathrm{rem}(c_3, c_4) < b_3$. Moreover, since $t_3|t$ and $t_4|t$, it follows that $\mathrm{lcm}(t_3, t_4)|t$.

Continue the above process until $b_{k+1} = 0$. Since $b_{i+1} < b_i$ and $<$ is Noetherian in $\mathcal{R}$, this process terminates. Let $b_0 = a$; we get a finite sequence:

$$a = b_0 > b_1 > b_2 > b_3 > \cdots > b_k > b_{k+1} = 0,$$

and corresponding polynomials in G: $\{p_1, p_2, \cdots, p_{k+1}\}$ with $\mathrm{lm}(p_i) = c_it_i$ and $t_i|t$ for $1 \leq i \leq k + 1$, such that $b_1 = \mathrm{rem}(a, c_1) < a$ and $b_{j+1} = \mathrm{rem}(c_j, c_{j+1}) < b_i$ and $c_{j+1}|b_j$ for $1 \leq j \leq k$.

Since $b_{k+1} = 0$, $c_{k+1}|c_k$. Since $b_{j+1} = \mathrm{rem}(c_j, c_{j+1})$ and $c_{j+1}|b_j$ for $1 \leq j \leq k$, it is easy to see that $c_{k+1}|c_j$ and $c_{k+1}|b_j$ for each $1 \leq j \leq k$ by induction on k. Since $b_1 = \mathrm{rem}(a, c_1)$, $c_{k+1}|c_1$ and $c_{k+1}|b_1$, we have $c_{k+1}|a$. Together with $t_{k+1}|t$, we get $c_{k+1}t_{k+1}|at$, i.e., $\mathrm{lm}(p_{k+1})|\mathrm{lm}(f)$. It follows that p_{k+1} is the polynomial in G that we were looking for. ■

Lemma 11 *Assume that for every pair of polynomials in G, every S-polynomial can reduce to 0 under $\longrightarrow^*$. Let $p_1, p_2 \in G$ with $c_i t_i = \mathrm{lm}(p_i)$, for $i = 1, 2$. Then there exists $h \in G$ such that $\mathrm{lt}(h)|\mathrm{lcm}(t_1, t_2)$ and $\mathrm{lc}(h)|\mathrm{rgcd}(c_1, c_2)$.*

Proof: Let $t = \mathrm{lcm}(t_1, t_2)$. Assume w.l.o.g. that $\mathrm{rep}(c_2) \leq \mathrm{rep}(c_1)$.

If $b_1 = \mathrm{rem}(c_1, c_2) \neq 0$, then $\mathrm{lm}(\mathrm{spol}(p_1, p_2)) = b_1 t$. By the assumption, $\mathrm{spol}(p_1, p_2) \longrightarrow^* 0$. By Lemma 10, there exists $p_3 \in G$ with $c_3 t_3 = \mathrm{lm}(p_3)$ such that $\mathrm{lm}(p_3)|\mathrm{lm}(\mathrm{spol}(p_1, p_2))$, i.e., $t_3|t$ and $c_3|b_1$. By Lemma 6, $\mathrm{rep}(c_3) < \mathrm{rep}(c_2)$ and $b_2 = \mathrm{rem}(c_2, c_3) < b_1$. Moreover, since $t_2|t$ and $t_3|t$, it follows that $\mathrm{lcm}(t_2, t_3)|t$.

If $b_2 \neq 0$, then $\mathrm{lm}(\mathrm{spol}(p_2, p_3)) = b_2 \mathrm{lcm}(t_2, t_3)$. By the assumption, $\mathrm{spol}(p_2, p_3) \longrightarrow^* 0$. By Lemma 10, there exists $p_4 \in G$ with $c_4 t_4 = \mathrm{lm}(p_4)$ such that $\mathrm{lm}(p_4)|\mathrm{lm}(\mathrm{spol}(p_2, p_3))$, i.e., $t_4|t$ and $c_4|b_2$. By Lemma 6, $\mathrm{rep}(c_4) < \mathrm{rep}(c_3)$ and $b_3 = \mathrm{rem}(c_3, c_4) < b_2$. Moreover, since $t_3|t$ and $t_4|t$, it follows that $\mathrm{lcm}(t_3, t_4)|t$.

Continue the above process until $b_k = 0$. Since $b_{i+1} < b_i$ and $<$ is Noetherian on $\mathcal{R}$, this process terminates. This gives a finite sequence:

$$b_1 > b_2 > \cdots > b_{k-1} > b_k = 0,$$

and corresponding polynomials in G: $\{p_1, p_2, \cdots, p_{k+1}\}$ with $\mathrm{lm}(p_i) = c_i t_i$ and $t_i|t$ for $1 \leq i \leq k+1$, such that $b_i = \mathrm{rem}(c_i, c_{i+1})$ for $1 \leq i \leq k$ and $c_{i+2}|b_i$ for $1 \leq i \leq k-1$.

Since $b_k = 0$, $c_{k+1}|c_k$. Since $b_i = \mathrm{rem}(c_i, c_{i+1})$ for $1 \leq i \leq k$ and $c_{i+2}|b_i$ for $1 \leq i \leq k-1$, it is easy to see that $c_{k+1}|c_j$ and $c_{k+1}|b_j$ for each $1 \leq i \leq k$ by induction on k. Since $c_{k+1}|c_1$ and $c_{k+1}|c_2$, $c_{k+1}|\mathrm{rgcd}(c_1, c_2)$. Together with $t_{k+1}|t$, it follows that p_{k+1} is the polynomial in G that we were looking for. ■

Corollary 1 *Assume that every S-polynomial can reduce to 0 under $\longrightarrow^*$ for every pair of polynomials in G. Let $p_i = c_i t_i + \mathrm{rest}(p_i) \in G$ where $c_i t_i = \mathrm{lm}(p_i)$, for $i = 1, 2, \cdots, k$. Then there exists $h \in G$ such that $\mathrm{lt}(h)|\mathrm{lcm}(t_1, t_2, \cdots, t_k)$ and $\mathrm{lc}(h)|\mathrm{rgcd}(c_1, c_2, \cdots, c_k)$.*

Proof: By Lemma 11, it is easy to show it by induction on k. ■

Definition 14 *Let $f \in \mathcal{R}[\bar{x}]$. A* **standard representation** *of f w.r.t. G is a representation*

$$f = \sum_{i=1}^{N} m_i p_i$$

with monomials m_i and $p_i \in G$ such that $\mathrm{lc}(m_i) * \mathrm{lc}(p_i) \neq 0$ *and* $\mathrm{lt}(m_i p_i) \leq \mathrm{lt}(f)$ *for* $1 \leq i \leq N$*. If $f = 0$, then we say $f = 0$ is the standard representation of f.*

In the above definition, p_i can be same with p_j even if $i \neq j$.

Our aim is to show that G is a Gröbner basis if (1) every A-polynomial in SAP(G) can reduce to 0 under $\longrightarrow^*$, and (2) every S-polynomial can reduce to 0 under $\longrightarrow^*$ for every pair of polynomials in G. With the above definition of standard representation and Lemma 11, at first we will prove below some lemmas and theorems similar to those given in [3, 15] (such as Lemma 10.3, Theorem 10.11, etc. in [3]). Since a D-A ring may not be a PID, we don't have a gcd algorithm though we have a rgcd algorithm. Moreover, we have to consider zero-divisors in a D-A ring $\mathcal{R}$ in the proofs.

Lemma 12 *Let $f \in \mathcal{R}[\bar{x}]$ and assume that $f \longrightarrow^* 0$. Then f has a standard representation w.r.t G.*

Proof: We show it by induction on k, where k is the number of steps, i.e., $f \longrightarrow^k 0$.

(1) Basis step: $k = 0$, obvious.

(2) Inductive step: Given $k > 0$, assume that g has a standard representation w.r.t G if $g \longrightarrow^{k-1} 0$.

Let $f \longrightarrow_p h \longrightarrow^{k-1} 0$, where $p \in G$. Let at be the monomial in f which is rewritten by p, then $h = f - mp$, where $m = qs$ is a monomial, $s * \mathrm{lt}(p) = t$, $q = \mathrm{quot}(a, \mathrm{lc}(p))$, and $\mathrm{rem}(a, \mathrm{lc}(p)) < \mathrm{lc}(p)$. Then $\mathrm{lc}(m) * \mathrm{lc}(p) \neq 0$, $\mathrm{lt}(mp) \leq \mathrm{lt}(f)$, and $\mathrm{lt}(h) \leq \mathrm{lt}(f)$.

By the induction hypothesis, h has a standard representation w.r.t G, i.e.,

$$h = \sum_{i=1}^{N} m_i p_i$$

with monomials m_i and $p_i \in G$ such that $\mathrm{lc}(m_i) * \mathrm{lc}(p_i) \neq 0$ and $\mathrm{lt}(m_i p_i) \leq$

$\mathrm{lt}(h) \leq \mathrm{lt}(f)$ for $1 \leq i \leq N$. Thus,

$$f = mp + h = mp + \sum_{i=1}^{N} m_i p_i$$

is a standard representation of f w.r.t G. ■

The following lemma and its two corollaries are trivial over a PID, but not obvious over a D-A ring because of zero-divisors.

Lemma 13 *Assume that every A-polynomial in* SAP(G) *can reduce to 0 under* $\longrightarrow^*$*. Let* $f = mp$ *with a monomial* m *and* $p \in G$*, then* f *has a standard representation w.r.t.* G*.*

Proof: If $f = mp = 0$, then it is trivial.

Let $f = mp \neq 0$. We will show that f has a standard representation by induction on $p \in G$ using the well-founded order $<$ defined in subsection 3.1.

(1) Basis step: Let p be a minimal nonzero polynomial in G. If $\mathrm{apol}(p) \neq 0$, then by the assumption, we have $\mathrm{apol}(p) \longrightarrow^+ 0$, i.e., $\mathrm{apol}(p)$ is reducible modulo some $g \in G$, then from $\mathrm{lt}(g) \leq \mathrm{lt}(\mathrm{apol}(p)) < \mathrm{lt}(p)$, we get $g < p$. This leads to a contradiction as p is a minimal nonzero polynomial in G. So $\mathrm{apol}(p) = 0$, then by Lemma 3, $\mathrm{lc}(m) * \mathrm{lc}(p) \neq 0$. Thus, $f = mp$ is a standard representation w.r.t. G.

(2) Inductive step: Assume that mg has a standard representation for any monomial m and $g \in G$ with $g < p$.

Let $f = mp$ with $m = as$ and $\mathrm{lm}(p) = ct$. If $\mathrm{lc}(m) * \mathrm{lc}(p) = ac \neq 0$, then $f = mp$ is a standard representation w.r.t. G.

Let $ac = 0$, then by Lemma 7, there exists $k \geq 1$ and $a_k \in \mathcal{R}$ such that

$$f = mp = a_k s * \mathrm{apol}^k(p)$$

and $a_k * \mathrm{lc}(\mathrm{apol}^k(p)) \neq 0$.

By the assumption, $\mathrm{apol}^k(p) \longrightarrow' 0$. Then by Lemma 12, $\mathrm{apol}^k(p)$ has a standard representation

$$\mathrm{apol}^k(p) = \sum_{i=1}^{N} m_i p_i,$$

with monomials m_i and $p_i \in G$ such that $\mathrm{lc}(m_i) * \mathrm{lc}(p_i) \neq 0$ and $\mathrm{lt}(m_i p_i) \leq \mathrm{lt}(\mathrm{apol}^k(p))$ for $1 \leq i \leq N$. Then

$$f = a_k s * \mathrm{apol}^k(p) = \sum_{i=1}^{N} (a_k s m_i) p_i. \tag{3.1}$$

For any index $1 \leq i \leq N$, since $\mathrm{lc}(m_i) * \mathrm{lc}(p_i) \neq 0$, we have $\mathrm{lt}(m_i p_i) = \mathrm{lt}(m_i) * \mathrm{lt}(p_i)$, then by $\mathrm{lt}(m_i p_i) \leq \mathrm{lt}(\mathrm{apol}^k(p))$ and $\mathrm{lt}(\mathrm{apol}^k(p)) < \mathrm{lt}(p)$, we get

$$\mathrm{lt}(p_i) \leq \mathrm{lt}(m_i p_i) \leq \mathrm{lt}(\mathrm{apol}^k(p)) < \mathrm{lt}(p),$$

i.e., $p_i < p$. Moreover, since $a_k * \mathrm{lc}(\mathrm{apol}^k(p)) \neq 0$, we get

$$\mathrm{lt}((a_k s m_i) p_i) \leq s * \mathrm{lt}(m_i p_i) \leq s * \mathrm{lt}(\mathrm{apol}^k(p)) = \mathrm{lt}(f). \tag{3.2}$$

By $p_i < p$ and the induction hypothesis, $(a_k s m_i) p_i$ has a standard representation. Substituting the corresponding standard representation for each $(a_k s m_i) p_i$ in (3.1), then from (3.2), we obtain a standard representation of f w.r.t. G. ■

Corollary 2 *Assume that every A-polynomial in* $\mathrm{SAP}(G)$ *can reduce to 0 under* $\longrightarrow^*$. *Let* $f \in \mathrm{Id}(G)$, *then* f *has a representation* $f = \sum_{i=1}^{N} m_i p_i$ *with monomials* m_i *and* $p_i \in G$ *such that* $\mathrm{lc}(m_i) * \mathrm{lc}(p_i) \neq 0$ *for* $1 \leq i \leq N$.

Proof: Since $f \in \mathrm{Id}(G)$, assume that

$$f = \sum_{i=1}^{N} m_i p_i \tag{3.3}$$

with monomials m_i and $p_i \in G$, where $m_i p_i \neq 0$, for $1 \leq i \leq N$.

By Lemma 13, $m_i p_i$ has a standard representation. Substituting the corresponding standard representation for each $m_i p_i$ in (3.3), we obtain the representation that we were looking for. ■

Corollary 3 *Assume that every A-polynomial in* $\mathrm{SAP}(G)$ *can reduce to 0 under* $\longrightarrow^*$. *Let* $f = mg$ *with a monomial* m *and* $g \in \mathrm{Id}(G)$ *with* $\mathrm{lc}(m) * \mathrm{lc}(g) \neq 0$, *and let* g *has a standard representation w.r.t.* G. *Then* f *has a standard representation w.r.t.* G.

Proof: Let $f = mg$ with a monomial $m = as$ and $g \in \mathrm{Id}(G)$ with $a * \mathrm{lc}(g) \neq 0$, and let the standard representation w.r.t. G of g be

$$g = \sum_{i=1}^{N} m_i p_i \tag{3.4}$$

with monomials m_i and $p_i \in G$ such that $\mathrm{lc}(m_i) * \mathrm{lc}(p_i) \neq 0$ and $\mathrm{lt}(m_i p_i) \leq \mathrm{lt}(g)$, for $1 \leq i \leq N$.

By (3.4), f has a representation

$$f = mg = \sum_{i=1}^{N} (asm_i)p_i. \tag{3.5}$$

For any index $1 \leq i \leq N$, by $\mathrm{lt}(m_i p_i) \leq \mathrm{lt}(g)$, we have

$$\mathrm{lt}((asm_i)p_i) \leq s * \mathrm{lt}(m_i p_i) \leq s * \mathrm{lt}(g) = \mathrm{lt}(asg) = \mathrm{lt}(f) \tag{3.6}$$

since $a * \mathrm{lc}(g) \neq 0$.

By Lemma 13, $(asm_i)p_i$ has a standard representation. Substituting the corresponding standard representation for each $(asm_i)p_i$ in (3.5), we obtain a standard representation w.r.t. G by (3.6). ■

Theorem 3 *Assume that (i) every A-polynomial in* SAP(G) *can reduce to 0 under* $\longrightarrow^*$*, and (ii) every S-polynomial can reduce to 0 under* $\longrightarrow^*$ *for every pair of polynomials in G. Then every polynomial in* Id(G) *has a standard representation w.r.t. G.*

Proof: Let $f \in \mathrm{Id}(G)$. Let

$$f = \sum_{i=1}^{N} m_i p_i \tag{3.7}$$

with monomials $m_i = \alpha_i s_i \neq 0$ and $p_i = c_i t_i + \mathrm{rest}(p_i) \in G$ with $c_i t_i = \mathrm{lm}(p_i)$, for $1 \leq i \leq N$. We may assume that $s = \max\{s_i t_i | 1 \leq i \leq N\}$ is minimal among all such representations of f. Thus $s \geq \mathrm{lt}(f)$. If $s = \mathrm{lt}(f)$, by Corollary 2, f has a standard representation.

We assume that $s > \mathrm{lt}(f)$. Let $J \subseteq \{1, 2, \cdots, N\}$ be the set of all indices with the property that $s = s_i t_i$. Let N_s be the size of J. For a contradiction, we will show that f has a representation

$$f = \sum_{i=1}^{N'} m'_i p'_i$$

of the same kind such that $s' = \max\{\mathrm{lt}(m'_i) \cdot \mathrm{lt}(p'_i) | 1 \leq i \leq N'\} < s$ by induction on N_s.

(1) Basis step: $N_s = 1$. Assume w.l.o.g. that $s_1 t_1 = s$. Since $s > \mathrm{lt}(f)$, s cancels out in the representation in (3.7), then $\mathrm{lm}(m_1 p_1) < s$. By Lemma 13, $m_1 p_1$ has a standard representation, say $m_1 p_1 = \sum_{i=1}^{N''} m''_i p''_i$. Substituting for $m_1 p_1$ in (3.7), we obtain a representation

$$f = \sum_{i=1}^{N''} m''_i p''_i + \sum_{i=2}^{N} m_i p_i \tag{3.8}$$

where the maximum of the leading terms occurring in the first sum is not larger than $\mathrm{lm}(m_1 p_1)$, i.e., less than s since $\mathrm{lm}(m_1 p_1) < s$; the maximum of the leading terms occurring in the first sum is less than s by our assumption $N_s = 1$. The maximum s' of the leading terms in the representation (3.8) satisfies $s' < s$, which means that (3.8) is the s'-representation that we were looking for.

(2) Inductive step: Given $N_s \geq 1$, assume that $g \in \mathrm{Id}(G)$ has a standard representation w.r.t. G if g has a representation (3.7) where the number of the largest terms is not larger than N_s.

Assume that f has a representation (3.7) whose size of the largest terms is $N_s + 1$. Assume w.l.o.g. that $s_1 t_1 = s_2 t_2 = s$, so $\mathrm{lcm}(t_1, t_2) | s$. By Lemma 11, there exists $h = \alpha t' + \mathrm{rest}(h) \in G$ with $\alpha t' = \mathrm{lm}(h)$ such that $t' | \mathrm{lcm}(t_1, t_2)$ and $\alpha | \mathrm{rgcd}(c_1, c_2)$, then $\mathrm{rep}(\alpha) \leq \mathrm{rep}(c_j)$ for $j = 1, 2$.

For any index $j = 1, 2$, let $\mathrm{lcm}(t_j, t') = v_j t_j = v'_j t'$ where v_j, v'_j are terms, and let $c_j = b_j \alpha$ with $b_j = \mathrm{quot}(c_j, \alpha)$. Then

$$\mathrm{spol}(p_j, h) = v_j * \mathrm{rest}(p_j) - b_j v'_j * \mathrm{rest}(h).$$

Since $t' | \mathrm{lcm}(t_1, t_2)$ and $\mathrm{lcm}(t_1, t_2) | s$, we can thus find a term u_j such that $s = u_j * \mathrm{lcm}(t_j, t')$, then

$$s = s_j t_j = (u_j) * \mathrm{lcm}(t_j, t') = (u_j v_j) t_j = (u_j v'_j) t',$$

so $s_j = u_j v_j$. Let $a_j = \beta_j b_j$ and $v = u_j v'_j$, then $a_j \alpha = \beta_j c_j$ and $s_j t_j = vt'$. Thus,

$$\begin{aligned} m_j p_j - a_j vh &= [(\beta_j c_j)(s_j t_j) + \beta_j s_j * \mathrm{rest}(p_j)] - [(a_j \alpha)(vt') + a_j v * \mathrm{rest}(h)] \\ &= \beta_j s_j * \mathrm{rest}(p_j) - a_j v * \mathrm{rest}(h) \\ &= \beta_j u_j (v_j * \mathrm{rest}(p_j) - b_j v'_j * \mathrm{rest}(h)) \\ &= \beta_j u_j * \mathrm{spol}(p_j, h) \end{aligned}$$

for $j = 1, 2$.

We can now modify our representation (3.7) of f as follows:

$$\begin{aligned} f &= \sum_{j=1}^{2} (m_j p_j - a_j vh) + (a_1 + a_2)vh + \sum_{i=3}^{N} m_i p_i \\ &= \sum_{j=1}^{2} \beta_j u_j * \mathrm{spol}(p_j, h) + (a_1 + a_2)vh + \sum_{i=3}^{N} m_i p_i \end{aligned}$$

By the assumption (ii) and Lemma 12, $\mathrm{spol}(p_j, h)$ has a standard representation. By Corollary 3, $\beta_j u_j * \mathrm{spol}(p_j, h)$ has a standard representation, for each $j = 1, 2$; by Corollary 3, $(a_1 + a_2)v * h$ has a standard representation; by the induction hypothesis, $\sum_{i=3}^{N} m_i p_i$ has a standard representation.

If we now add up these representations to obtain, say, $f = \sum_{i=1}^{N'} m'_i p'_i$, then it is easy to see that $s' = \max\{\mathrm{lt}(m'_i) \cdot \mathrm{lt}(p'_i) | 1 \leq i \leq N'\} < s$ as desired. ■

Lemma 14 *Let $f \in \mathrm{Id}(G)$ has a standard representation w.r.t. G. Assume that every S-polynomial can reduce to 0 under $\longrightarrow^*$ for every pair of polynomials in G. Then there exists $h \in G$ such that $\mathrm{lm}(h) | \mathrm{lm}(f)$.*

Proof: Let the standard representation w.r.t. G of f be

$$f = \sum_{i=1}^{N} m_i p_i \tag{3.9}$$

with monomials m_i and $p_i \in G$, where $\mathrm{lc}(m_i) * \mathrm{lc}(p_i) \neq 0$ and $\mathrm{lt}(m_i p_i) \leq \mathrm{lt}(f)$ for $1 \leq i \leq N$.

Let $I \subseteq \{1, 2, \cdots, N\}$ be the set of all indices with the property that $\mathrm{lt}(m'_i p'_i)$ is the largest term in (3.9). Then $\mathrm{lm}(f) = \sum_{i \in I} \mathrm{lm}(m_i p_i)$, and thus

$$\begin{aligned} \mathrm{lcm}(\mathrm{lt}(p_i)|i \in I) &\;\;|\;\; \mathrm{lt}(f), \\ \mathrm{rgcd}(\mathrm{lc}(p_i)|i \in I) &\;\;|\;\; \mathrm{lc}(f). \end{aligned}$$

By Corollary 1, there exists $h \in G$ such that $\mathrm{lt}(h)|\mathrm{lcm}(\mathrm{lt}(p_i)|i \in I)$, and $\mathrm{lc}(h)|\mathrm{rgcd}(\mathrm{lc}(p_i)|i \in I)$. We see that $\mathrm{lm}(h)|\mathrm{lm}(f)$. ∎

Theorem 4 *G is a Gröbner basis if and only if (i) every A-polynomial in* SAP(G) *can reduce to 0 under $\longrightarrow^*$, and (ii) every S-polynomial can reduce to 0 under $\longrightarrow^*$ for every pair of polynomials in G.*

Proof: (⇐) part: This is obvious since every A-polynomial in SAP(G) and every S-polynomial are in Id(G).

(⇒) part: Let $f \in \mathrm{Id}(G)$. We show that $f \longrightarrow^* 0$ by induction on f using the well-founded order $<$ defined in subsection 3.1.

(1) Basis Step: $f = 0$, obvious.

(2) Inductive Step: Assume that $g \longrightarrow^* 0$ for any polynomials $g \in \mathrm{Id}(G)$ with $g < f$.

By Theorem 3, every $f \in \mathrm{Id}(G)$ has a standard representation w.r.t. G. By Lemma 14, there exists $h \in G$ such that $\mathrm{lm}(h)|\mathrm{lm}(f)$, thus $f \longrightarrow_h g$ with $g = f - mh \in \mathrm{Id}(G)$ and $g < f$, where m is a monomial. By the induction hypothesis, $g \longrightarrow^* 0$. Then $f \longrightarrow g \longrightarrow^* 0$. ∎

The above theorem provides a criterion for G to be a Gröbner basis which can be effectively tested. More importantly, we can use it to construct, from a finite subset F of $\mathcal{R}[\bar{x}]$, a Gröbner basis G with $\mathrm{Id}(F) = \mathrm{Id}(G)$ in the next section. Moreover, we can obtain the unique reduced Gröbner basis that allow the computation of unique normal forms[3] by the following theorem similar to Theorem 10.23 in [3].

Theorem 5 *Let G be a Gröbner basis, and $f \in \mathcal{R}[\bar{x}]$. Then f has a unique normal form modulo G.*

[3] A normal form of f modulo G is a polynomial g that is not reducible modulo G and satisfies $f \longrightarrow^*_G g$.

Proof: Let f_1 and f_2 be two normal forms of f modulo G. By Theorem 2, $f - f_1$ are $f - f_2$ are in $\mathrm{Id}(G)$. From

$$f_1 - f_2 = -(f - f_1) + (f - f_2),$$

we have $f_1 - f_2 \in \mathrm{Id}(G)$. Then since G is a Gröbner basis, it follows that

$$f_1 - f_2 \longrightarrow^* 0.$$

Assume that $f_1 \neq f_2$. Let $t = \mathrm{lt}(f_1 - f_2)$, and $f_1 = a_1 t + g_1$, and $f_2 = a_2 t + g_2$, where g_1 and g_2 have no term t. Then $\mathrm{lc}(f_1 - f_2) = a_1 - a_2 \neq 0$. By Theorem 4 and Lemma 10, there exists $p \in G$ such that $\mathrm{lm}(p) | \mathrm{lm}(f_1 - f_2)$, i.e., $\mathrm{lm}(p) | (a_1 - a_2)t$. Then $\mathrm{lt}(p) | t$ and there exists $q \in \mathcal{R}$ such that $a_1 - a_2 = q * \mathrm{lc}(p)$.

Since f_1 and f_2 are normal forms modulo G, it follows that both $a_1 t$ and $a_2 t$ cannot be reduced modulo p, then $\mathrm{rem}(a_1, \mathrm{lc}(p)) = a_1$ and $\mathrm{rem}(a_2, \mathrm{lc}(p)) = a_2$ as $\mathrm{lt}(p) | t$. It follows that $a_1 = \mathrm{rem}(a_1, \mathrm{lc}(p)) \leq a_2$ as $a_1 = q * \mathrm{lc}(p) + a_2$, and $a_2 = \mathrm{rem}(a_2, \mathrm{lc}(p)) \leq a_1$ as $a_2 = -q * \mathrm{lc}(p) + a_1$. Thus $a_1 = a_2$, but this leads to a contradiction with $\mathrm{lc}(f_1 - f_2) = a_1 - a_2 \neq 0$. So $f_1 = f_2$. That is, f has a unique normal form modulo G. ■

4 A Gröbner basis algorithm

If a given basis G of an ideal is not a Gröbner basis, it can be completed to get a Gröbner basis of its ideal. For every polynomial p, we add new rules corresponding to the normal forms of polynomials in $\mathrm{SAP}(p)$, if any. For every pair of polynomial, we compute its S-polynomials and add new rules corresponding to their normal forms, if any. Thus a new basis for the same ideal is generated. This step is repeated until

(1) every f in $\mathrm{SAP}(G)$ can reduce to 0 under $\longrightarrow^*$.

(2) every S-polynomial can reduce to 0 under $\longrightarrow^*$ for every pair of polynomials in G.

By Theorem 4, a Gröbner basis is obtained.

We now give the algorithm:

Algorithm 1 *Given F, a finite set of polynomials in $\mathcal{R}[\bar{x}]$, find G such that the ideal* $\mathrm{Id}(G) = \mathrm{Id}(F)$ *and G is a Gröbner basis.*

```
function $G$ =GRÖBNER_OVER_DAR($F$)
begin
    $G := F$; $P := \emptyset$;
    $B := \{(g_1, g_2) \mid g_1, g_2 \in G$ with $g_1 \neq g_2\}$;
    for all $p \in G$ do
        $A :=$ COMPUTE_APOLs($p$);
        $P := P \bigcup A$;
    end
    $[G, B] :=$ ADD_APOLs_RULEs($P, G, B$);
    while $B \neq \emptyset$ do
        Select $(g_1, g_2)$ from $B$;
        $B := B - \{(g_1, g_2)\}$;
        if $g_i$ is reducible modulo $g_j$ ($i, j = 1, 2$ and $i \neq j$) then
            $G := G - \{g_i\}$;
            $B := B - \{(g_i, g) \mid g \in G\}$;
            $h' := g_i$;
        else
            $h' := \mathrm{spol}(g_1, g_2)$;
        end
        $h :=$ the normal form of $h'$ modulo $G$;
        if $h \neq 0$ then
            $B := B \bigcup \{(g, h) \mid g \in G\}$;
            $G := G \bigcup \{h\}$;
            $A :=$ COMPUTE_APOLs($h$);
            $[G, B] :=$ ADD_APOLs_RULEs($A, G, B$);
        end
    end
    return $G$
end GRÖBNER_OVER_DAR

function $A$ = COMPUTE_APOLs($f$)
begin
    $A := \emptyset$; $g := \mathrm{apol}(f)$;
    while $g \neq 0$ do
        $A := A \bigcup \{g\}$;
        $g := \mathrm{apol}(g)$;
    end
    return $A$
end COMPUTE_APOLs

function $[G, D]$ = ADD_APOLs_RULEs($A, G, D$)
begin
    while $A \neq \emptyset$ do
        Select $f$ from $A$;
        $A := A - \{f\}$;
        $h :=$ the normal form of $f$ modulo $G$;
        if $h \neq 0$ then
            $D := D \bigcup \{(g, h) \mid g \in G\}$;
            $G := G \bigcup \{h\}$;
        end
    end
    return $[G, D]$
end ADD_APOLs_RULEs
```

Theorem 6 *The algorithm* GRÖBNER_OVER_DAR *terminates for every finite subset F of $\mathcal{R}[\bar{x}]$.*

Proof: Assume that the algorithm does not terminate. Let $\{h_n\}_{n\in\mathbb{N}}$ be the non-zero normal form of A-polynomials and S-polynomials in the order that they are being added to G. For $n \in \mathbb{N}$, let $m_n = a_n s_n = \mathrm{lm}(h_n)$, and $G_n = \{F \bigcup \{h_i | i < n\}\}$. Thus, we get two infinite sequences: $\{s_n\}_{n\in\mathbb{N}}$ and $\{a_n\}_{n\in\mathbb{N}}$.

By Dickson's Lemma (Theorem 5.2 in [3]) for the set of all terms and Proposition 4.45 in [3], in the sequence $\{s_n\}_{n\in\mathbb{N}}$, there exists an infinite subsequence $\{s_{n_i}\}_{i\in\mathbb{N}}$ ($n_i < n_j$ iff $i < j$) such that $s_{n_i} | s_{n_j}$ for all $i < j \in \mathbb{N}$. Since $G_{n_i} \subset G_{n_j}$ and h_{n_j} is in normal form modulo G_{n_j}, $\mathrm{lm}(h_{n_j}) = a_{n_j} s_{n_j}$ is not reducible modulo $a_{n_i} s_{n_i}$ for all $i < j$. It follows that a_{n_j} is not reducible modulo a_{n_i} as $s_{n_i} | s_{n_j}$, then $\mathrm{rep}(a_{n_i}) > \mathrm{rep}(a_{n_j})$ for all $i < j$. That is, we obtain an infinite strictly descending sequence $\{\mathrm{rep}(a_{n_i})\}_{i\in\mathbb{N}}$. This leads to a contradiction with that $<$ is a well-founded ordering on $\mathcal{R}$. ■

5 Examples

Example 2 *Given $\mathcal{R}[x, y] = (\mathbb{Z}_{12}[i])[x, y]$ where $i^2 + 1 = 0$, compute a Gröbner basis of $F = \{(5 + 3i)x^2y - y,\ (3 + 2i)xy^2 - x\}$.*

We assume the total degree order induced by $y > x$ and $<_{\mathbb{Z}_n[i]}$. Using this order, polynomials in F are transformed into the following 2 rules:

$$\begin{array}{lll} 1. & (5+3i)x^2y & \longrightarrow y \\ 2. & (3+2i)xy^2 & \longrightarrow x \end{array}$$

1. Since $5 + 3i$ is a zero-divisor with $\text{ann}(5 + 3i) = 6 + 6i$, we get the corresponding rule of the A-polynomial from rule 1:

   $$3.\ \ (6+6i)y \longrightarrow 0.$$

   $3 + 2i$ is not a zero divisor, so no A-polynomial is generated from rule 2.

2. From rules 1 and 2, the superposition is $(5 + 3i)x^2y^2$, which gives the rule:

   $$4.\ \ y^2 \longrightarrow (-3-i)x^2$$

   from $5 + 3i = (-3 - i) * (3 + 2i)$.

3. From rules 1 and 3, the superposition is $(6 + 6i)x^2y$, which gives the rule:

   $$3'.\ \ 6y \longrightarrow 0$$

   from $6 + 6i = 6 * (5 + 3i)$. The rule 3 is deleted.

4. Rule $3'$ can be used to reduce rule 1 to:

   $$1'.\ \ (-1+3i)x^2y \longrightarrow y.$$

   The rule 1 is deleted.

5. From rules $1'$ and $3'$, the superposition is $6x^2y$, which gives the following rule

   $$3''.\ \ (3+3i)y \longrightarrow 0$$

   from $6 = (3 - 3i) * (-1 + 3i)$. The rule $3'$ is deleted.

6. From rules $1'$ and $3''$, the superposition is $(3 + 3i)x^2y$, which gives the following rule

   $$3'''.\ \ 3y \longrightarrow 0$$

   from $3 + 3i = -3 * (-1 + 3i)$. The rule $3''$ is deleted.

7. Rule $3'''$ can be used to reduce rule $1'$ to:

$$1''.\ \ x^2y \longrightarrow -y.$$

The rule $1'$ is deleted.

8. Rule $3'''$ can be used to reduce rule 2 to:

$$2'.\ \ ixy^2 \longrightarrow -x.$$

The rule 2 is deleted.

9. From rules $2'$ and $3'''$, the superposition is $3xy^2$, which gives the rule:

$$5.\ \ 3ix \longrightarrow 0$$

from $3 = -3i * i$.

10. From rules $2'$ and 5, the superposition is $3ixy^2$, which gives the rule:

$$5'.\ \ 3x \longrightarrow 0$$

from $3i = 3 * i$. The rule 5 is deleted.

11. Rule 5 can be used to reduce rule 4 to:

$$4'.\ \ y^2 \longrightarrow -ix^2.$$

The rule 4 is deleted.

12. Rule $4'$ can be used to reduce rule $2'$ to:

$$2''.\ \ x^3 \longrightarrow -x.$$

The rule $2'$ is deleted.

After the above 12 steps, we get a Gröbner basis of rules 1 and 2 over $(\mathbb{Z}_{12}[i])[x, y]$ with $i^2 + 1 = 0$, which consists of polynomials corresponding to rules $1''$, $2''$, $3'''$, $4'$, $5'$, i.e.,

$$\{x^2y + y,\ x^3 + x,\ 3y,\ y^2 + ix^2,\ 3x\}.$$

The reader should note that Gröbner basis can often be computed faster using rgcd.

If a Gröbner basis algorithm over $\mathbb{Z}[i, x, y]$ is used to compute a Gröbner basis of a polynomial ideal over $\mathbb{Z}_{12}[i][x, y]$ by augmenting its basis over $\mathbb{Z}[i, x, y]$ with the polynomials $i^2 + 1$ and 12, in this case we will obtain another basis after a considerably more steps.

6 Comparison with the reduction ring method

For the ring of integers (without zero-divisors), Example 1 was used to illustrate a comparison between Buchberger-Stifter's method and KandriRody-Kapur's algorithm In the following, we give a comparison between our new method and Buchberger-Stifter's method for polynomial ideals over a ring with zero divisor.

We briefly introduce Buchberger-Stifter's method over a reduction ring with zero-divisors at first. Let $\mathcal{R}$ be a reduction ring with $Mul_c, Mul_c^+, Mul_c^- \subset \mathcal{R}$, where Mul_c is the set of all multipliers of c, and let Mul_c^+ and Mul_c^- be two sets of multipliers of c such that $Mul_c^+ \bigcup Mul_c^- = Mul_c$, for each $c \in \mathcal{R}$.

Let $c_1t_1 \longrightarrow f_1$ and $c_2t_2 \longrightarrow f_2$ be two rules (they may be identical such that critical pairs for one rule in the basis can be considered), where c_it_i is a monomial and f_i is a polynomial with terms less than t_i for $i = 1, 2$. Then the superposition of these two rules will be $\mathrm{LCR}(c_1, c_2)\mathrm{lcm}(t_1, t_2)$. Let $t = \mathrm{lcm}(t_1, t_2)$, $\mathrm{LCR}(c_1, c_2) = q_ic_i + r_i$ with $q_i \in Mul_{c_i}$ and $r_i < \mathrm{LCR}(c_1, c_2)$ for $i = 1, 2$, where (q_1, c_1) and (q_2, c_2) are *irrelative*[4]. A critical pair for them is

$$< r_1t + q_1f_1,\ r_2t + q_2f_2 >,$$

and the S-polynomial is $(r_1 - r_2)t + q_1f_1 - q_2f_2$.

For example, over a ring $\mathbb{Z}_n$ with n not a prime number, Stifter [16] defined $Mul_c^+ := \{q | 0 < q < \mathrm{ann}(c)\}$, and $Mul_c^- := \{q | -q \in Mul_c^+\}$, and $Mul_c := Mul_c^+ \bigcup Mul_c^-$ for each $c \in \mathbb{Z}_n - \{0\}$, under the order $0 < 1 < 2 < \cdots < n - 1$. Further, the non-trivial least common reducible of c_1 and c_2 is defined as

$$\mathrm{LCR}(c_1, c_2) = \max(\mathrm{LCR}(c_1),\ \mathrm{LCR}(c_2))$$

for any $c_1, c_2 \in \mathbb{Z}_n$, where $\mathrm{LCR}(c) = \gcd(c, n)$.

Example 3 *Given $\mathcal{R}[x] = \mathbb{Z}_{12}[x]$, compute a Gröbner basis of the following one rule:*

$$\mathit{1.}\quad 3x \longrightarrow 1$$

Using Buchberger-Stifter's reduction ring method, the order is defined as $0 < 1 < 2 < \cdots < 11$.

[4] (q_1, c_1) and (q_2, c_2) are irrelative if and only if (1) $c_1 \neq c_2$; or (2) $c_1 = c_2$, $q_1 \in Mul_{c_1}^+$ and $q_2 \in Mul_{c_1}^-$; (ii) $c_1 = c_2$, $q_1 \in Mul_{c_1}^-$ and $q_2 \in Mul_{c_1}^+$.

1. Since $\mathrm{LCR}(3) = \gcd(3, 12) = 4$, we can get $a = \mathrm{LCR}(c_1, c_1) = 3$ where $c_1 = 3$ is the left-hand-side coefficient of rule 1. By computing $\mathrm{ann}(c_1) = 4$, we get $Mul^+_{c_1} := \{1, 2, 3\}$ and $Mul^-_{c_1} := \{-1, -2, -3\}$. Then by the division algorithm, we get $a = 1 * 3 + 0 \longrightarrow_{c_1} 0$ and $a = (-3) * 3 + 0 \longrightarrow_{c_1} 0$, where two multipliers $q_1 = 1 \in Mul^+_{c_1}$ and $q_2 = -3 \in Mul^-_{c_1}$, i.e., (q_1, c_1) and (q_2, c_1) are irrelative. For the rule 1, the superposition can be set as $3x$, and the critical pair is: 1 and -3. A new rule is obtained:
$$2.\ \ 4 \longrightarrow 0.$$

2. Since $\mathrm{LCR}(3) = \gcd(3, 12) = 4$ and $\mathrm{LCR}(4) = \gcd(4, 12) = 3$, we can get $a = \mathrm{LCR}(c_1, c_2) = 4$ where $c_1 = 3$ and $c_2 = 4$ are the left-hand-side coefficients of rule 1 and rule 2. By computing $\mathrm{ann}(c_1) = 4$ and $\mathrm{ann}(c_2) = 3$, we get $Mul_{c_1} := \{1, 2, 3, -1, -2, -3\}$ and $Mul_{c_2} := \{1, 2, -1, -2\}$. Then by division algorithm, we have $a = 1*3+1 \longrightarrow_{c_1} 1$ and $a = 1 * 4 + 0 \longrightarrow_{c_2} 0$, where two multipliers $q_1 = 1 \in Mul_{c_1}$ and $q_2 = 1 \in Mul_{c_2}$, i.e., (q_1, c_1) and (q_2, c_2) are irrelative. From rule 1 and rule 2, the superposition can be set as $4x$, and the critical pair is: $x+1$ and 0. A new rule is obtained:
$$3.\ \ x \longrightarrow -1.$$

Thus, the Gröbner basis $\{x + 1, 4\}$ is obtained.

In the above example, we found that in each step, for given two rules $c_1t_1 \longrightarrow f_1$ and $c_2t_2 \longrightarrow f_2$, Buchberger-Stifter's method must have the following operations (over $\mathbb{Z}_n$):

(1) Compute $\mathrm{LCR}(c_1)$ and $\mathrm{LCR}(c_2)$ using gcd algorithm, then get $\mathrm{LCR}(c_1, c_2)$.

(2) Compute $\mathrm{ann}(c_1)$ and $\mathrm{ann}(c_2)$, then get Mul_{c_1} and Mul_{c_2}, or $Mul^+_{c_1}$ and $Mul^-_{c_1}$ if $c_1 = c_2$.

(iii) Compute the remainder r_i and the quotient q_i of $\mathrm{LCR}(c_1, c_2)$ divided by c_i for $i = 1, 2$ using a division algorithm, such that (q_1, c_1) and (q_2, c_2) are irrelative.

(iv) Compute a critical pair and get an S-polynomial.

Using the order $<_{\mathbb{Z}_n}$ for this example, each step in our proposed algorithm is simpler though the number of steps is the same.

1. By computing $\mathrm{ann}(c_1)$ where $c_1 = 3$ is the left-hand-side coefficient of rule 1, we get the following A-polynomial rule from rule 1:

   $$2. \quad 4 \longrightarrow 0.$$

2. From rule 1 and 2, the superposition is $4x$, the following rule is obtained by using the division algorithm:

   $$3. \quad x \longrightarrow -1.$$

Thus we have gotten the same Gröbner basis $\{x + 1, 4\}$.

Hence, in our algorithm, for each step, we have the following operations (over $\mathbb{Z}_n$): Given a rule whose leading coefficient is zero-divisor, compute its annihilator, and get the A-polynomial. Otherwise, given two different rules $c_1t_1 \longrightarrow f_1$ and $c_2t_2 \longrightarrow f_2$, assume that c_1 is reducible modulo c_2, then compute the remainder r and the quotient q of c_1 divided by c_2 using a division algorithm, and get an S-polynomial.

By comparison with Buchberger-Stifter's method, our algorithm is quite simple. In particular, Buchberger-Stifter's method computes the A-polynomial quite inefficiently from one rule. Over $\mathbb{Z}_n$, let $c_1t_1 \longrightarrow f_1$ be a rule. By Buchberger-Stifter's method, we observe that we always have $\mathrm{LCR}(c_1, c_1) = \gcd(c_1, n) = q_1c_1 = q_2c_1$ with two multipliers $q_1 = 1 \in Mul^+_{c_1} = \{q|0 < q < \mathrm{ann}(c)\}$ and $q_2 = -(\mathrm{ann}(c_1) - 1) \in Mul^-_{c_1} = \{q|0 < -q < \mathrm{ann}(c)\}$, and then get the S-polynomial $f = (q_1 - q_2)f_1 = \mathrm{ann}(c_1)f_1$. However, the same polynomial, called as A-polynomial in the paper, can be computed by our algorithm much easily.

In fact, there doesn't exist a general approach to compute the $\mathrm{LCR}(c_1, c_2)$ for any c_1 and c_2 in Buchberger-Stifter's reduction ring method for a special reduction ring. Furthermore, we found that Buchberger-Stifter's reduction ring method will have more steps in general. See Example 1 for such an illustration.

7 Extension to other Structures

We have so far discussed how to compute a Gröbner basis of a polynomial ring over a D-A ring; however, this method can be extended to a polynomial ideal over a generalized principle ideal ring (GPIR), which is defined as follows.

Definition 15 *Let $\mathcal{R}$ be a commutative ring with the identity element 1, and assume that for each element in $\mathcal{R}$, its representative form is computable. Let $<$ be a partial well-founded order on $\mathcal{R}$. It is called a* **weak representable order** *if and only if for any $a, b \in \mathcal{R} - \{0\}$, if $b|a$ then $\mathrm{rep}(b) \leq \mathrm{rep}(a)$.*

Now if there exist a weak representable order $<$ and a rgcd algorithm on $\mathcal{R}$, then by Lemma 2, such a $\mathcal{R}$ is Noetherian, thus there is an $\mathrm{ann}(c)$ for any zero divisor $c \in \mathcal{R}$. So we can have the following definition:

Definition 16 *Let $\mathcal{R}$ be a commutative ring with the identity element 1. $\mathcal{R}$ is called a* **generalized principle ideal ring***, simply denoted by a* **GPIR***, if and only if*

(1) For each element in $\mathcal{R}$, its representative form is computable. (2) There exist a weak representable order $<$ on $\mathcal{R}$ and a rgcd algorithm, such that for any $a, b \in \mathcal{R} - \{0\}$, $\mathrm{rgcd}(a, b)$ is computable, and there exist $\alpha, \beta \in \mathcal{R}$ such that $\mathrm{rgcd}(a, b) = \alpha a + \beta b$.

(3) For any $c \in \mathcal{R} - \{0\}$, $\mathrm{ann}(c)$ is computable.

A principle ideal ring (PIR) is a GPIR. Moreover, by Lemma 1, a D-A ring is a GPIR too.

For any $a, b \in \mathcal{R} - \{0\}$, using the rgcd algorithm on $\mathcal{R}$, the representative least common multiple of a and b, rlcm, can be computed as well: $\mathrm{rlcm}(a, b) = \mathrm{rep}(a * b/rgcd(a, b))$.

Definition 17 *Let $\mathcal{R}$ be a GPIR, and let $f, g, p \in \mathcal{R}[\bar{x}]$. We say that f* **G-reduces** *to g* **modulo** *p and write $f \longrightarrow_p g$ if and only if there exists a monomial m in f such that $\mathrm{lm}(p)|m$, say $m = m' * \mathrm{lm}(p)$, and $g = f - m'p$.*

Definition 18 *Let $\mathcal{R}$ be a GPIR, and let G be a finite set of polynomials in $\mathcal{R}[\bar{x}]$. G is a* **weak Gröbner basis** *of $\mathrm{Id}(G)$ (the ideal of G) if every polynomial in $\mathrm{Id}(G)$ can G-reduce to 0 modulo G.*

Definition 19 *Let $p_i = c_i t_i + \mathrm{rest}(p_i) \in \mathcal{R}[\bar{x}]$, where $c_i t_i = \mathrm{lm}(p_i)$. Let $\mathrm{lcm}(t_1, t_2) = s_i t_i$, and $a = q_i c_i = \mathrm{rlcm}(c_1, c_2)$ with $q_i = \mathrm{quot}(a, c_i)$ for $i = 1, 2$.*

(1) The **S-polynomial** *of p_1 and p_2 is defined as $\mathrm{spol}(p_1, p_2) = q_1 s_1 p_1 - q_2 s_2 p_2$.*

(2) Let $b_1, b_2 \in \mathcal{R}$ such that $\mathrm{rgcd}(c_1, c_2) = b_1 c_1 + b_2 c_2$. Then define the **G-polynomial** *of p_1 and p_2 as $\mathrm{gpol}(p_1, p_2) = b_1 s_1 p_1 + b_2 s_2 p_2$.*

Assume that every S-polynomial and G-polynomial can G-reduce to 0 under $\longrightarrow^*$ for every pair of polynomials in G. Then, under the assumption and above new definitions, Lemma 10, Lemma 11, Corollary 1 and Lemma 14 are trivial. Moreover, if we assume that every A-polynomial in $\mathrm{SAP}(G)$ can G-reduce to 0 under $\longrightarrow^*$, then under the assumption and the above modified definitions, we can prove results corresponding to Lemma 12, Lemma 13, Corollary 2, Corollary 3 and Theorem 3. This gives us:

Theorem 7 *G is a weak Gröbner basis if and only if (1) every A-polynomial in $\mathrm{SAP}(G)$ can G-reduce to 0 under $\longrightarrow^*$, and (2) every S-polynomial and G-polynomial can G-reduce to 0 under $\longrightarrow^*$ for every pair of polynomials in G.*

The following algorithm computes a weak Gröbner basis over a GPIR.

Algorithm 2 *Given F, a finite set of polynomials in $\mathcal{R}[\bar{x}]$, find G such that the ideal $\mathrm{Id}(G) = \mathrm{Id}(F)$ and G is a weak Gröbner basis.*

```
function $G$ =GRÖBNER_OVER_GPIR($F$)
begin
    $G := F$; $P := \emptyset$;
    $B := \{(g_1, g_2) \mid g_1, g_2 \in G$ with $g_1 \neq g_2\}$;
    for all $p \in G$ do
        $A :=$ COMPUTE_APOLs($p$);
        $P := P \bigcup A$;
    end
    $[G, B] :=$ ADD_APOLs_RULEs($P, G, B$);
    $C := B$; $D := \emptyset$;
    while $B \neq \emptyset$ do
        while $C \neq \emptyset$ do
            Select $(g_1, g_2)$ from $C$;
            $C := C - \{(g_1, g_2)\}$;
            if $g_i$ is reducible modulo $g_j$ ($i, j = 1, 2$ and $i \neq j$) then
                $G := G - \{g_i\}$;
                $C := C - \{(g_i, g) \mid g \in G\}$;
                $h'_1 := g_i$; $h'_2 := 0$;
            else
                $h'_1 :=$ spol$(g_1, g_2)$; $h'_2 :=$ gpol$(g_1, g_2)$;
            end
            for $i = 1, 2$ do
```

```
                $h_i$ := the G-normal form of $h'_i$ modulo $G$;
                if $h_i \neq 0$ then
                    $D := D \bigcup \{(g, h_i) \mid g \in G\}$;
                    $G := G \bigcup \{h_i\}$;
                    $A :=$ COMPUTE_APOLs($h_i$);
                    $[G, D] :=$ ADD_APOLs_RULEs($A, G, D$);
                end
            end
        end
        $C := D$; $B := D$; $D := \emptyset$;
    end
    return $G$
end GRÖBNER_OVER_GPIR
```

Theorem 8 *The algorithm* GRÖBNER_OVER_GPIR *terminates for every finite subset F of $\mathcal{R}[\bar{x}]$.*

Proof: Assume that the algorithm does not terminate. Let $\{h_n\}_{n\in\mathbb{N}}$ be the non-zero G-normal forms of A-polynomials, S-polynomials and G-polynomials in the order that they are being added to G. For $n \in \mathbb{N}$, let $m_n = a_n s_n = \mathrm{lm}(h_n)$, and $G_n = \{F \bigcup \{h_i | i < n\}\}$. We get two infinite sequences: $\{s_n\}_{n\in\mathbb{N}}$ and $\{a_n\}_{n\in\mathbb{N}}$. Note that at the end of each run through the outer **while**-loop, the new pairs are just added to G, but all S-polynomials of new pairs of elements of G are being treated during the next run. There is a function $\phi : \mathbb{N} \longrightarrow \mathbb{N}$ such that

$$\forall i, n \in \mathbb{N} \text{ with } i < n,\ \mathrm{lm}(\mathrm{gpol}(h_i, h_n)) \text{ is reducible modulo } G_{\phi(n)}. \tag{7.1}$$

By Dickson's Lemma (Theorem 5.2 in [3]) for the set of all terms and Proposition 4.45 in [3], in the sequence $\{s_n\}_{n\in\mathbb{N}}$, there exists an infinite subsequence $\{s_{n_i}\}_{i\in\mathbb{N}}$ ($n_i < n_j$ iff $i < j$) such that

$$s_{n_i} | s_{n_j} \quad \text{for all } i < j \in \mathbb{N}. \tag{7.2}$$

Since $G_{n_i} \subset G_{n_j}$ and h_{n_j} is in G-normal form modulo G_{n_j}, $m_{n_i} \nmid m_{n_j}$. It follows that $a_{n_i} \nmid a_{n_j}$ as $s_{n_i} | s_{n_j}$ for all $i < j$.

We can recursively define a sequence $\{k_i\}_{i\in\mathbb{N}}$ with the following properties:

(1) For any k_i, there exists n_j such that $s_{k_i} | s_{n_j}$;

(2) $\mathrm{rep}(a_{k_j}) < \mathrm{rep}(a_{k_i})$ for all $i < j \in \mathbb{N}$.

Set $k_1 = n_1$, and assume that $k_1, \cdots, k_i$ have been defined. Let $j \in \mathbb{N}$ such that $s_{k_i} | s_{n_j}$. By (7.2), we may assume that $k_i < n_j$ and thus $a_{k_i} \not| a_{n_j}$. By (7.1), $\mathrm{lm}(\mathrm{gpol}(h_{k_i}, h_{n_j}))$ is reducible modulo $G_{\phi(n_j)}$. This means that there exists $n < \phi(n_j)$ such that

$$m_n | \mathrm{lm}(gpol(h_{k_i}, h_{n_j})) = \mathrm{rgcd}(a_{n_j}, a_{k_i}) \cdot s_{n_j}$$

Since $a_{k_i} \not| a_{n_j}$ and $a_n | \mathrm{rgcd}(a_{n_j}, a_{k_i})$, $\mathrm{rep}(a_n) \leq \mathrm{rgcd}(a_{n_j}, a_{k_i}) < \mathrm{rep}(a_{k_i})$. Set $k_{i+1} = n$, then $s_{k_{i+1}} | s_{n_j}$ and $\mathrm{rep}(a_{k_{i+1}}) < \mathrm{rep}(a_{k_i})$. That is, we obtain an infinite strictly descending sequence $\{\mathrm{rep}(a_{k_i})\}_{i \in \mathbb{N}}$. This leads to a contradiction with that $<$ is a well-founded ordering on $\mathcal{R}$. ■

8 Conclusion

An algorithm for computing a Gröbner basis of a polynomial ideal where the coefficients are from a ring with zero divisors is given. The notions of D-A and GPIR rings admitting certain additional properties are introduced so that the algorithm can be applied on polynomial ideals over such rings. Such rings include $\mathbb{Z}_n$ and $\mathbb{Z}_n[i]$ with an arbitrary integer n. The Gröbner basis algorithm for polynomial ideals over a D-A ring is an extension of Buchberger's algorithm for polynomial ideals over a field in the sense that

1. the method is based on the definition of reduction of polynomials using a single polynomial at a time,

2. the algorithm computes a strong Gröbner basis of a polynomial ideal, i.e., not only every polynomial in the ideal simplifies to 0, but all polynomials in the same residue class in the quotient structure induced by the ideal on the polynomial ring has the same normal form, and

3. a reduced unique Gröbner basis can be associated with every polynomial ideal once an admissible ordering is chosen on terms.

In the case of the coefficient ring being GPIR on which a division algorithm cannot be assumed, the algorithm discussed above computes a weak Gröbner basis of a polynomial ideal, i.e., every polynomial in the ideal simplifies to 0 and all polynomials in the polynomial ring have a unique normal form, even though different polynomials in the same residue class in the quotient structure induced by the ideal on the polynomial ring need not have the same normal form. If elements equivalent modulo units are totally ordered in a GPIR, a reduced unique Gröbner basis can be associated with a polynomial ideal as well.

If the coefficient ring is a quotient structure generated by an ideal over a polynomial ring with many noncomparable parameters, then the proposed algorithms do not seem to generalize. It is possible that there may exist non-comparable multi-annihilators for an element in the coefficient ring. For example, in $\mathbb{Z}_2[a, b]$ with $a^2 = a$ and $b^2 = b$ (see also [12] where Boolean rings modeling prepositional calculus are discussed), an annihilator of $ab + a + b + 1 \in \mathbb{Z}_2[a, b]$ can be either a or b. If these parameters cannot be compared, there is no single generator of the annihilator set of $ab+a+b+1$. Furthermore, if there are noncomparable parameters also serving as coefficients of terms in a polynomial, their gcd may not be defined (or it may not be possible to define division of one parameter by another parameter). It is an interesting open question to generalize Buchberger's algorithm for such quotient rings.

ACKNOWLEDGMENT: We thank Birgit Reinert and Sabine Stifter for their help.

References

[1] Adams, W.W. and Loustaunau, P. (1994). An Introduction to Gröbner bases, AMS.

[2] Baader, F. and Nipkow T. (1998). Term Rewriting and All That, Cambridge University Press.

[3] Becker, T. and Weispfenning, V. (1993). Gröbner bases, Springer-Verlag, New York.

[4] Buchberger, B. (1965). An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal (in German). Ph.D. Thesis, Univ. of Innsbruck, Austria, Math., Inst.

[5] Buchberger, B. (1984). A critical-pair/completion algorithm in reduction rings. In: (E. Borger, G. Hasenjaeger, D. Rodding, eds.) Proc. Logic and Machines: Decision Problems and Complexity, Springer LNCS 171, 137-161.

[6] Buchberger, B. (1985). Gröbner bases: An algorithmic method in polynomial ideal theory. In: (N.K. Bose, ed.) Recent Results in Multidimensional Systems Theory, Reidel, 184-232.

[7] Buchberger, B. (1998). Introduction to Gröbner bases. In: (Buchberger, B., Winkler, F., eds.) Gröbner bases and Applications, London Mathematical Society Lecture Note Series 251, Cambridge University Press.

[8] Kandri-Rody, A. and Kapur, D. (1984). An algorithm for computing the Gröbner basis of a polynomial ideal over a Euclidean ring. General Electric Corporate Research and Development Report No. 84CRD045, Schenectady, NY.

[9] Kandri-Rody, A. and Kapur, D. (1988). Computing a Gröbner basis of a polynomial ideal over a Euclidean domain, J. Symbolic Computation 6, 37-57.

[10] Kapur, D. and Madlener, K. (1988). Construction of Gröbner bases in "special" rings, in "Manuscript presented at the Gröbner bases workshop 1988," Cornell.

[11] Kapur, D. and Narendran, P. (1985). Existence and construction of a Gröbner basis of a polynomial ideal. In: Proceedings of a workshop on Combinatorial Algorithms in Algebraic Structures, September 30-October 4, 1985, Europaeische Akademie, Otzenhausen, Fachbereich Informatik Report, Univ. of Kaiserslautern, Germany.

[12] Kapur, D. and Narendran, P. (1985). An Equational Approach to Theorem Proving in First-Order Predicate Calculus. IJCAI 1985: 1146-1153.

[13] Madlener, K., Reinert, B. (1998). String Rewriting and Gröbner bases — A General Approach to Monoid and Group Rings, Proceedings of the Workshop on Symbolic Rewriting Techniques, Monte Verita, 1995, Birkhäuser (printed 1998), 127-180.

[14] Möller, H.M. (1988). On the construction of Gröbner bases using syzygies. J. Symbolic Computation, 6, 345-359.

[15] Pan, L. (1989). On the D-bases of ideals in polynomial rings over principal ideal domains. J. Symbolic Computation, 7, 55-69.

[16] Stifter S. (1987). A generalization of reduction rings. J. Symbolic Computation, 4, 351-364.

[17] Stifter S. (1991). The reduction ring property is hereditary. J. Algebra, 140, 399-414.

[18] Stifter S. (1993). Gröbner bases of modules over reduction rings. J. Algebra, 159, 54-63.