The Proper Basis for Polynomial Ideals

Sheng-Ming Ma

Abstract

We define a new type of ideal basis called the proper basis that improves both Gröbner basis and Buchberger’s algorithm. Let $x_1$ be the least variable of a monomial ordering in a polynomial ring $K[x_1, \ldots, x_n]$ over a field $K$. The Gröbner basis of a zero-dimensional polynomial ideal contains a univariate polynomial in $x_1$. The proper basis is defined and computed in the variables $\bar{x} := (x_2, \ldots, x_n)$ with $x_1$ serving as a parameter in the algebra $K[x_1][\bar{x}]$. Its algorithm is more efficient than not only Buchberger’s algorithm whose elimination of $\bar{x}$ unnecessarily involves the least variable $x_1$ but also Möller’s algorithm due to its polynomial division mechanism. This is corroborated by a series of benchmark testings herein. The proper basis is in a modular form and neater than Gröbner basis and hence reduces its coefficient swell problem. It is expected that all the state of the art algorithms improving Buchberger’s algorithm over the last decades can be further improved if we apply them to the proper basis.

1 Introduction

After Buchberger initiated his celebrated algorithm in his remarkable PhD thesis [5], the theory of Gröbner basis had been established as a standard tool in computer algebra, yielding algorithmic solutions to many significant problems in mathematics, science and engineering [4]. As a result, there have been many excellent textbooks on the subject such as [3, 30, 1, 27, 23, 13, 20, 9].

The computation of Gröbner basis is often plagued with a high complexity. A typical phenomenon is the intermediate coefficient swell problem (ICSP) over the rational number field $\mathbb{Q}$ and especially with respect to the LEX ordering. This stimulates decades of ardent endeavors to improve the efficiency of Buchberger’s algorithm. The methods of normal selection strategies and signatures have been quite successful in this respect [6, 22, 3, 18, 24, 12, 17]. The modular and $p$-adic methods based on the “lucky primes” and Hensel lifting are adopted to control the rampant growth of the intermediate coefficients [15, 40, 39, 34, 25, 2]. There are also the conversion methods among Gröbner bases such as the FGLM algorithm [16] and Gröbner Walk [7], a detailed description of which can be found in [8, 38].

The Gröbner basis over a field had also been generalized to over rings. In particular, the Gröbner basis over a principal ideal ring (PIR) was developed by Möller in [31] and elucidated in [1, Chapter 4]. Nonetheless these generalizations have never been applied to polynomial ideals over a field.

The method of characteristic set [30, 42] based on the pseudo-division is more efficient than Gröbner basis. However the pseudo-division usually loses too much algebraic information of the original ideal. After the computation we only have information on the zero locus or radical ideal that is insufficient to solve algebraic problems. This is also the deficiency associated with a few other methods such as the rational univariate representation [35].

In this article we define a new type of ideal basis called proper basis that reduces the computational complexity of Gröbner basis while retains the algebraic information of the original ideal. Let $I \subset K[x]$ be a zero-dimensional polynomial ideal over a field $K$ with $x := (x_1, \ldots, x_n)$. Suppose that $I \cap K[x_1]$ is a principal ideal $(\chi)$ that is generated by the eliminant $\chi \in K[x_1] \setminus K$ of $I$. We obtain $\chi$ after eliminating all the other variables $\bar{\chi} := (x_2, \ldots, x_n)$ with respect to, e.g., the LEX ordering $x_1 < \cdots < x_n$. Nonetheless it is literally excessive computations for Buchberger’s elimination process to involve the variable $x_1$. Hence
it is natural for us to treat \( K[x] \) as the algebra \( K[x_1][\bar{x}] \) such that the variable \( x_1 \) serves as a parameter when we eliminate the variables \( \bar{x} \). In this way we define a new type of ideal basis for \( I \) called the proper basis. Moreover, the proper basis is based on a new type of polynomial division called the proper division, which improves the division mechanism in Möller’s algorithm over a PIR for Gröbner bases. Our benchmark testings corroborate that the proper basis algorithm is distinctively more efficient than both Buchberger’s classical algorithm over \( K \) and Möller’s one over \( K[x_1] \) for Gröbner bases.

In Definition 3.2 and Theorem 3.4 we define the proper division using least multipliers in \( K[x_1] \). The purpose of Lemma 3.7 and Lemma 3.8 is to trim down the number of \( S \)-polynomials for computational efficiency. The algorithm in Lemma 3.9 parallels that of Buchberger for Gröbner basis except that it uses the least multiplier in \( K[x_1] \). Based on Lemma 3.12, we derive in Corollary 3.13 (2) that the prebasis obtained in Lemma 3.9 satisfies Definition 2.3 for the proper basis.

The content of Section 4 parallels Section 3 except that we contrive a modular algorithm over a PIR \( K[x_1]/(q) \) that might contain zero divisors.

In Section 6 we conduct benchmark testings on the timings of the respective algorithms. It is clear that the proper basis algorithm has a distinctive advantage over both Buchberger’s and Möller’s classical algorithms for Gröbner bases in the textbooks.

Throughout the article all our discussions are with respect to the \( \text{LEX} \) ordering \( x_1 < \cdots < x_n \) since it is typical to have the highest level of computational complexity compared with other monomial orderings. We use \( K \) to denote a field that is not necessarily algebraically closed unless specified. As usual, let us denote the sets of rational, integral and natural numbers by \( \mathbb{Q} \), \( \mathbb{Z} \) and \( \mathbb{N} \) respectively.

## 2 The Definition for Proper Basis

Let \( K \) be a field and \( x \) denote the variables \( (x_1, \ldots, x_n) \). We consider two types of algebras that determine the notations in this article. The first one is \( K[x_1][\bar{x}] \) over \( K[x_1] \) with the variables \( \bar{x} \) denoting \( (x_2, \ldots, x_n) \). The second one is \( R_q[\bar{x}] \) over a PIR \( R_q \) that is isomorphic to \( K[x_1]/(q) \). Here \( (q) \) denotes a nontrivial principal ideal in \( K[x_1] \) that is generated by \( q \).

In order to clarify the notations, in what follows let us use \( R \) to denote \( K[x_1] \) or \( R_q \). In this way the algebra \( R[\bar{x}] \) over \( R \) denotes the above algebra \( K[x_1][\bar{x}] \) or \( R_q[\bar{x}] \). We also adopt the following notations for a ring \( R \); we denote \( R^* := R \setminus \{0\} \) as the set of nonzero elements in \( R \), and \( R^\times \) as the set of units in \( R^* \).

With \( \alpha = (\alpha_2, \ldots, \alpha_n) \in \mathbb{N}^{n-1} \), we denote a monomial \( x_2^\alpha_2 \cdots x_n^\alpha_n \) by \( \bar{x}^\alpha \) and a term by \( c\bar{x}^\alpha \) with the coefficient \( c \in R^* \). Let us denote the set of monomials in \( \bar{x} \) by \( [\bar{x}] := \{ \bar{x}^\alpha : \alpha \in \mathbb{N}^{n-1} \} \). The notation \( \langle A \rangle \) denotes an ideal generated by a nonempty subset \( A \subset R[\bar{x}] \).

**Notation 2.1** (\( \text{supp}(f) \), \( \text{LT}(f) \), \( \text{LM}(f) \), \( \text{LC}(f) \), \( \text{LM}(B) \), \( \langle \text{LM}(B) \rangle \), \( \text{LT}(B) \), \( \langle \text{LT}(B) \rangle \)).

Let \( R \) denote a PIR such as \( K[x_1] \) or \( R_q \cong K[x_1]/(q) \) as above. Suppose that \( f = \sum \alpha c\bar{x}^\alpha \) is a polynomial in \( R[\bar{x}] \). We denote the support of \( f \) by \( \text{supp}(f) := \{ \bar{x}^\alpha \in [\bar{x}] : c_\alpha \neq 0 \} \). In particular, we define \( \text{supp}(f) := \{1\} \) if \( f \in R^* \) and \( \text{supp}(f) := \emptyset \) if \( f = 0 \).

Let \( \succ \) be a monomial ordering on the monomial set \([\bar{x}]\). The leading term of \( f \) is a term \( c\beta \bar{x}^\beta \) that satisfies \( \bar{x}^\beta := \max_\succ \{ \bar{x}^\alpha \in \text{supp}(f) \} \) and is denoted by \( \text{LT}(f) := c\beta \bar{x}^\beta \). The leading monomial of \( f \) is the monomial \( \bar{x}^\beta \) of \( \text{LT}(f) = c\beta \bar{x}^\beta \) and is denoted by \( \text{LM}(f) := \bar{x}^\beta \). The leading coefficient of \( f \) is the coefficient \( c_\beta \) of the leading term \( \text{LT}(f) = c\beta \bar{x}^\beta \) and is denoted by \( \text{LC}(f) := c_\beta \in R^* \).

Let \( B := \{b_j : 1 \leq j \leq s\} \) be a polynomial set in \( R[\bar{x}] \setminus \{0\} \). We denote the leading monomial set \( \{\text{LM}(b_j) : 1 \leq j \leq s\} \) by \( \text{LM}(B) \), and the ideal generated by \( \text{LM}(B) \) in \( R[\bar{x}] \) by \( \langle \text{LM}(B) \rangle \). Similarly, we can define \( \text{LT}(B) \) and \( \langle \text{LT}(B) \rangle \).

For \( q \in K[x_1] \setminus K \), consider the set \( R_q := \{ r \in K[x_1] : \deg(r) < \deg(q) \} \) with \( \deg(r) = 0 \) for every \( r \in K \) including \( r = 0 \). We define binary operations on \( R_q \) such that it is a PIR isomorphic to \( K[x_1]/(q) \). For every \( f \in K[x_1] \), there exist a quotient \( h \in K[x_1] \) and unique remainder \( r \in R_q \) such that \( f = hf + r \). We define an epimorphism as follows.

\[
\sigma_q : K[x_1] \to R_q : \quad \sigma_q(f) := r.
\]

Since \( R_q \) is a subset of \( K[x_1] \), for every \( r \in R_q \), we define an injection as follows.

\[
\iota_q : R_q \hookrightarrow K[x_1] : \quad \iota_q(r) := r.
\]
If we extend the ring epimorphism $\sigma_q$ in (2.1) such that it is the identity map on the variables $\tilde{x}$, then $\sigma_q$ induces an epimorphism from $K[x_1][\tilde{x}]$ to $R_q[\tilde{x}]$ which we still denote by $\sigma_q$ as follows.

$$\sigma_q: K[x_1][\tilde{x}] \to R_q[\tilde{x}]: \quad \sigma_q\left(\sum_{j=1}^s c_j \tilde{x}^{\alpha_j}\right) := \sum_{j=1}^s \sigma_q(c_j) \tilde{x}^{\alpha_j}.$$  \hspace{1cm} (2.3)

Similarly the injection $\iota_q$ in (2.2) can be extended to an injection from $R_q[\tilde{x}]$ into $K[x_1][\tilde{x}]$ in the way that it is an identity map on the variables $\tilde{x}$ as follows.

$$\iota_q: R_q[\tilde{x}] \hookrightarrow K[x_1][\tilde{x}]: \quad \iota_q\left(\sum_{j=1}^s c_j \tilde{x}^{\alpha_j}\right) := \sum_{j=1}^s \iota_q(c_j) \tilde{x}^{\alpha_j}.$$  \hspace{1cm} (2.4)

**Definition 2.2** (Eliminant $\chi$; multiplicity $\text{mult}_p(f)$).

For a zero-dimensional polynomial ideal $I \subset K[x_1][\tilde{x}]$, let us denote the monic generator of the principal ideal $I \cap K[x_1]$ by $\chi$, i.e., $I \cap K[x_1] = (\chi)$. We call $\chi$ the *eliminant* of $I$ henceforth.

For an irreducible factor $p$ of a univariate polynomial $f \in K[x_1] \setminus K$, we use $\text{mult}_p(f)$ to denote the multiplicity of $p$ in $f$. That is, $\text{mult}_p(f) := \max\{i \in \mathbb{N} : f \in (p^i)\}$. \hfill $\Box$

Suppose that the above eliminant $\chi$ has the following factorization whose pairwise relatively prime factors are in $\Omega \subset K[x_1] \setminus K$:

$$\chi = \prod_{q \in \Omega} q.$$  \hspace{1cm} (2.5)

It is evident that the above factorization corresponds to a decomposition of $I$ as follows.

$$I = \bigcap_{q \in \Omega} (I + (q)).$$  \hspace{1cm} (2.6)

**Definition 2.3** (Proper basis).

Let $I \subset K[x_1][\tilde{x}]$ be a zero-dimensional polynomial ideal whose eliminant $\chi$ has a pairwise coprime factorization as in (2.5). For each $q \in \Omega$, let $I_q := \sigma_q(I) \subset R_q[\tilde{x}]$ denote its image under $\sigma_q$ in (2.3). Also suppose that there exists a subset $B_q \subset I_q$ that satisfies:

$$\langle \text{lt}(I_q) \rangle = \langle \text{lt}(B_q) \rangle.$$  \hspace{1cm} (2.7)

Then we define the following set:

$$\bigcup_{q \in \Omega} (B_q \cup \{q\})$$  \hspace{1cm} (2.8)

as the *proper basis* of the zero-dimensional polynomial ideal $I$.

### 3 The First Algorithmic Step in $K[x_1][\tilde{x}]$

Our algorithm for the proper basis is divided into two steps. The first step is in $K[x_1][\tilde{x}]$ over $K[x_1]$ whereas the second one is in $R_q[\tilde{x}]$ over $R_q$ as in Section 4.

**Notation 3.1** ($\text{gcd}(a, b)$, $\text{lcm}(a, b)$).

For a univariate polynomial $f = \sum_{k=0}^d c_k x^k \in K[x_1]$ with $c_d \in K^*$ being nonzero, recall that we use $\text{lt}(f)$, $\text{lm}(f)$ and $\text{lc}(f)$ to denote the leading term $c_d x^d$, leading monomial $x^d$ and leading coefficient $c_d$ of $f$ over the field $K$ respectively. In what follows we use $\text{gcd}(a, b)$ and $\text{lcm}(a, b)$ to denote the greatest common divisor (GCD) and least common multiple (LCM) of $a, b \in (K[x_1])^*$ respectively. In particular, we always choose the monic polynomials for GCDs such that $\text{lc}(<\text{gcd}(a, b)>)$ = 1. However we always choose the LCMs such that $\text{lc}(<\text{lcm}(a, b)>)$ = $\text{lc}(a) \cdot \text{lc}(b)$. This is a different choice from that of [20, §3.4] so that the identity $a/\text{gcd}(a, b) = \text{lcm}(a, b)/b$ holds, which is convenient for our later discussions.
Definition 3.2 (Proper term reduction in the algebra $K[x_1][\hat{x}]$).

Let $\succ$ be a monomial ordering on $[\hat{x}]$. For $f \in K[x_1][\hat{x}] \setminus K[x_1]$ and $g \in K[x_1][\hat{x}] \setminus \{0\}$, suppose that $f$ has a term $c_\alpha x^\alpha$ satisfying $x^\alpha \in \supp(f) \cap (\text{LM}(g))$. We define a proper term reduction of $c_\alpha x^\alpha$ by $g$ as follows.

$$h = \mu f - \frac{m c_\alpha}{\text{LT}(g)} g$$

with the least multiplier $\mu := m/c_\alpha \in R^*$ and multiplier $m := \text{lcm}(c_\alpha, \text{LC}(g))$.

Definition 3.3 (Properly reduced polynomial in $K[x_1][\hat{x}]$).

A polynomial $r \in K[x_1][\hat{x}]$ is properly reduced with respect to a polynomial set $B = \{b_j : 1 \leq j \leq s\} \subset K[x_1][\hat{x}] \setminus K[x_1]$ if $\supp(r) \cap (\text{LM}(B)) = \emptyset$ holds. In particular, this includes the special case when $r = 0$ and hence $\supp(r) = \emptyset$. Otherwise we say that $r$ is properly reducible with respect to $B$.

Theorem 3.4 (Proper division or reduction in $K[x_1][\hat{x}]$).

Suppose that $B = \{b_j : 1 \leq j \leq s\} \subset K[x_1][\hat{x}] \setminus K[x_1]$ is a finite polynomial set. For every $f \in K[x_1][\hat{x}]$, there exist a multiplier $\lambda \in (K[x_1])^*$, a remainder $r \in K[x_1][\hat{x}]$ and quotients $q_j \in K[x_1][\hat{x}]$ for $1 \leq j \leq s$ such that

$$\lambda f = \sum_{j=1}^s q_j b_j + r,$$

where $r$ is properly reduced with respect to $B$, and the multiplier $\lambda$ is literally a product of the least multipliers as in (3.1). Moreover, the polynomials in (3.2) satisfy the following condition:

$$\text{LM}(f) = \max\{\max_{1 \leq j \leq s}\{\text{LM}(q_j b_j)\}, \text{LM}(r)\}. \tag{3.3}$$

Proof. If $f$ is properly reducible with respect to $B$, we define $x^\alpha := \max\{\supp(f) \cap (\text{LM}(B))\}$ and make a proper term reduction of $c_\alpha x^\alpha$ by some $b_j \in B$ as in (3.1). This repeats and then terminates in finite steps since the monomial ordering is a well-ordering. The equality in (3.3) follows from the fact that it holds for the proper term reduction in (3.1).

Remark 3.5. There is a stark difference between the proper reduction herein and Möller’s reduction over a PIR in [31]. With the notations as in Theorem 3.4, Möller’s reduction requires that the linear equation

$$\text{LC}(f) = \sum_{j=1}^s c_j \cdot \text{LC}(b_j) \tag{3.4}$$

be solvable for the $c_j$’s in $K[x_1]$. Please refer to [31, P349, (1)] or [1, P204, (4.1.1)]. This is the major difference between the proper reduction and Möller’s reduction.

Definition 3.6 (S-polynomial in $K[x_1][\hat{x}]$).

Suppose that $f, g \in K[x_1][\hat{x}] \setminus K[x_1]$. The $S$-polynomial of $f$ and $g$ is defined as:

$$S(f, g) := \frac{m \hat{x}^\gamma}{\text{LT}(f)} f - \frac{m \hat{x}^\gamma}{\text{LT}(g)} g \tag{3.5}$$

with $m := \text{lcm}(\text{LC}(f), \text{LC}(g)) \in (K[x_1])^*$ and $\hat{x}^\gamma := \text{lcm}(\text{LM}(f), \text{LM}(g)) \in [\hat{x}]$.

In particular, when $g \in (K[x_1])^*$ and $f \in K[x_1][\hat{x}] \setminus K[x_1]$, we take $\text{LM}(g) = 1$ and $m = \text{lcm}(\text{LC}(f), g)$ and the special $S$-polynomial satisfies $dS(f, g) = f_1 g$ with $d := \text{gcd}(\text{LC}(f), g) \in K[x_1]$ and $f_1 := f - \text{LT}(f)$.

It is easy to verify that the $S$-polynomial satisfies $\text{LM}(S(f, g)) = \hat{x}^\gamma = \text{lcm}(\text{LM}(f), \text{LM}(g))$.

Lemma 3.7 and Lemma 3.8 are generalizations of Buchberger’s first and second criteria respectively. Please refer to [3, P222, §5.5] or [1, P124, §3.3] for Buchberger’s two criteria.

Lemma 3.7. For $f, g \in K[x_1][\hat{x}] \setminus K[x_1]$, suppose that $\text{LM}(f)$ and $\text{LM}(g)$ are relatively prime. Let us denote $d := \text{gcd}(\text{LC}(f), \text{LC}(g))$. Then the $S$-polynomial in (3.5) satisfies $dS(f, g) = f_1 g - g_1 f$ with $f_1 := f - \text{LT}(f)$ and $g_1 := g - \text{LT}(g)$. Moreover, we have $\text{LM}(S(f, g)) = \max\{\text{LM}(f_1 g), \text{LM}(g_1 f)\}$. 

4
Proof. With \( m \) denoting \( \text{lcm}(\text{LC}(f), \text{LC}(g)) \), the conclusion follows from the identities \( m/\text{LC}(f) = \text{LC}(g)/d \) and \( m/\text{LC}(g) = \text{LC}(f)/d \). Moreover, the identity for \( \text{LM}(S(f, g)) \) follows from \( dS(f, g) = f_1 \cdot \text{LT}(g) - g_1 \cdot \text{LT}(f) \) that is easy to prove. \( \square \)

Let us denote \( \text{lcm}(\text{LT}(f), \text{LT}(g)) := \text{lcm}(\text{LC}(f), \text{LC}(g)) \cdot \text{lcm}(\text{LM}(f), \text{LM}(g)) \). The following lemma is evident.

**Lemma 3.8.** For \( f, g, h \in K[x_1][\bar{x}] \setminus K[x_1] \), if \( \text{lcm}(\text{LM}(f), \text{LM}(g)) \) is divisible by \( \text{LM}(h) \), then we have the following triangular identity among the \( S \)-polynomials:

\[
\lambda S(f, g) = \frac{\lambda \cdot \text{lcm}(\text{LT}(f), \text{LT}(g))}{\text{lcm}(\text{LT}(f), \text{LT}(h))} S(f, h) - \frac{\lambda \cdot \text{lcm}(\text{LT}(f), \text{LT}(g))}{\text{lcm}(\text{LT}(g), \text{LT}(h))} S(g, h),
\]

(3.6)

where the multiplier is defined as \( \lambda := \text{LC}(h)/d \) with \( d := \text{gcd}(\text{lcm}(\text{LC}(f), \text{LC}(g)), \text{LC}(h)) \in K[x_1] \).

**Lemma 3.9** (The algorithm computing a temporary prebasis for the proper basis).

Let \( F \subset K[x_1][\bar{x}] \setminus K[x_1] \) be a finite polynomial set generating a zero-dimensional polynomial ideal. Then the algorithm that consists of the following sequence of instructions terminates in finite steps.

A1 Start with a prebasis set \( G := F \), multiplier set \( \Lambda := \emptyset \) in \( K[x_1] \), temporary set \( S := \emptyset \) of \( S \)-polynomials, and temporary pre-eliminant \( \chi_0 := 0 \).

A2 For each pair \( f, g \in G \) with \( f \neq g \), execute the instructions in A3.

A3 If \( \text{LM}(f) \) and \( \text{LM}(g) \) are relatively prime, add \( d := \text{gcd}(\text{LC}(f), \text{LC}(g)) \) into the multiplier set \( \Lambda \) if \( d \in K[x_1] \setminus K \);

Else if there exists an \( h \in G \setminus \{ f, g \} \) such that \( \text{lcm}(\text{LM}(f), \text{LM}(g)) \in (\text{LM}(h)) \), add \( \lambda \) as defined in (3.6) into the multiplier set \( \Lambda \) if \( \lambda \in K[x_1] \setminus K \);

Else, compute the \( S \)-polynomial \( S(f, g) \) as in (3.5) and add it into the set \( S \).

A4 For every \( S \)-polynomial \( S \in S \), make a proper reduction of \( S \) by the prebasis set \( G \) to obtain a remainder that is denoted as \( r \) like in Theorem 3.4. If the multiplier \( \lambda \) satisfies \( \lambda \in K[x_1] \setminus K \) in the proper reduction (3.2), add \( \lambda \) into the multiplier set \( \Lambda \). Delete \( S \) from the set \( S \).

If \( r \in K[x_1] \setminus K \), redefine \( \chi_0 := \text{gcd}(r, \chi_0) \);

Else if \( r \in K[x_1][\bar{x}] \setminus K[x_1] \), add \( r \) into \( G \). For every \( f \in G \setminus \{ r \} \), execute the instructions in A3 to compute the \( S \)-polynomial \( S(f, r) \);

Else if \( r \in K^* \) is a unit, halt the algorithm and output \( G = \{ 1 \} \).

A5 Repeat the instructions in A4 until \( S = \emptyset \).

A6 For every \( f \in G \), if \( d := \text{gcd}(\text{LC}(f), \chi_0) \in K[x_1] \setminus K \), add \( d \) into the multiplier set \( \Lambda \).

A7 Return the pre-eliminant \( \chi_0 \in (K[x_1])^* \), prebasis \( G \subset K[x_1][\bar{x}] \setminus K[x_1] \), multiplier set \( \Lambda \subset K[x_1] \setminus K \).

**Proof.** The termination of the algorithm follows from the fact that the algebra \( K[x_1][\bar{x}] \) is Noetherian. \( \square \)

Please note the step A6 is for the reduction of the special \( S \)-polynomial \( S(f, \chi_0) \) as in Definition 3.6.

**Notation 3.10** (Compatible part \( \chi_0^* \) of the pre-eliminant \( \chi_0 \)).

Let \( \chi_0 \) and \( \Lambda \) be the pre-eliminant and multiplier set that are obtained in the algorithm of Lemma 3.9. Let us denote \( \Theta := \{ p \in K[x_1] \setminus K \colon p \) is an irreducible factor of \( \chi_0 \) and relatively prime to every multiplier in \( \Lambda \} \). If \( \Theta \neq \emptyset \), we define the compatible part of \( \chi_0 \) as \( \chi_0^* := \prod_{p \in \Theta} p^{\text{mult}(p, \chi_0)} \). Otherwise \( \chi_0^* := 1 \).

**Lemma 3.11.** Let \( F = \{ f_j \colon 1 \leq j \leq s \} \subset K[x_1][\bar{x}] \setminus K[x_1] \) be a finite polynomial set. Suppose that each \( f_j \) has the same leading monomial \( \text{LM}(f_j) = \bar{x}^\alpha \in [\bar{x}] \) for \( 1 \leq j \leq s \).

(1) If \( f = \sum_{j=1}^s f_j \) satisfies \( \text{LM}(f) \prec \bar{x}^\alpha \), then there exist multipliers \( b, b_j \in (K[x_1])^* \) for \( 1 \leq j < s \) such that

\[
b f = \sum_{1 \leq j < s} b_j S(f_j, f_s).
\]

(3.7)
(2) For each irreducible polynomial \( p \in K[x_1] \setminus K \), we can always relabel the subscripts of the polynomial set 
\[ F = \{ f_j : 1 \leq j \leq s \} \] 
such that the multiplier \( b \in (K[x_1])^* \) in (3.7) is not divisible by \( p \).

Proof. (1) Let us denote \( l_j := \text{LC}(f_j) \) for \( 1 \leq j \leq s \) and \( m_j := \text{lcm}(l_j, l_\ast) \) for \( 1 \leq j < s \). Then the condition \( \text{LM}(f) \prec \bar{x}^\beta \) implies that \( \sum_{j=1}^s l_j = 0 \). It is easy to check that the identity (3.7) holds for the definition of multipliers as \( b := \text{lcm}(m_j/l_j : 1 \leq j < s) \) and \( b_j := b_j/m_j \) for \( 1 \leq j < s \).

(2) Let us relabel the subscripts of \( f_j \) for \( 1 \leq j \leq s \) such that \( \text{mult}_p(l_j) = \min_{1 \leq j \leq s} \{ \text{mult}_p(l_j) \} \). Then \( \text{mult}_p(m_j/l_j) = \text{mult}_p(l_j/\gcd(l_j, l_\ast)) = 0 \) for \( 1 \leq j < s \). Thus the multiplier \( b \) is not divisible by \( p \). \( \square \)

Lemma 3.12. For a finite polynomial set \( F \subset K[x_1][\bar{x}] \setminus K[x_1] \) generating a zero-dimensional polynomial ideal, let \( G = \{ g_k : 1 \leq k \leq s \} \) and \( \chi_0 \) be the prebasis and pre-eliminant that are obtained in the algorithm of Lemma 3.9. For every \( f \in \langle F \rangle \), there exist \( \{ q_k : 0 \leq k \leq s \} \subset K[x_1][\bar{x}] \) and a multiplier \( \lambda \in (K[x_1])^* \) being relatively prime to the compatible part \( \chi_0^\lambda \) of \( \chi_0 \) such that:

\[ \lambda f = \sum_{k=1}^s q_k g_k + q_0 \chi_0. \] (3.8)

Moreover, the polynomials in (3.8) satisfy the following condition:

\[ \text{LM}(f) = \max \left\{ \max_{1 \leq k \leq s} \{ \text{LM}(q_k g_k) \}, \text{LM}(q_0) \} \right\}. \] (3.9)

In particular, the eliminant \( \chi \in \langle F \rangle \) also satisfies (3.8) with \( q_0 \in (K[x_1])^* \) and \( \gcd(\lambda, \chi_0^\lambda) = 1 \) as follows:

\[ \lambda \chi = q_0 \chi_0. \] (3.10)

Proof. Let us fix an irreducible factor \( p \) of the compatible part \( \chi_0^\lambda \), i.e., \( p \in \Theta \) as in Notation 3.10.

For \( F = \{ f_k : 1 \leq k \leq t \} \), suppose that \( f \) can be written as \( f = \sum_{k=1}^t h_k f_k \) with \( h_k \in K[x_1][\bar{x}] \) for \( 1 \leq k \leq t \) and \( \bar{x}^\beta := \max_{1 \leq k \leq t} \{ \text{LM}(h_k f_k) \} \). Assume that \( \text{LM}(f) < \bar{x}^\beta \) since the conclusion already holds otherwise. Let us denote \( \text{LT}(h_k) := c_k \bar{x}^\alpha_k \) with \( c_k \in (K[x_1])^* \) for \( 1 \leq k \leq t \). Without loss of generality, suppose that \( \text{LM}(\bar{x}^\alpha_k f_k) = \bar{x}^\beta \) holds for \( 1 \leq k \leq t \). And we have:

\[ f = \sum_{k=1}^t c_k \bar{x}^\alpha_k f_k + \sum_{k=1}^t (h_k - \text{LT}(h_k)) f_k. \] (3.11)

As per Lemma 3.11 (1), there exist multipliers \( b, b_k \in (K[x_1])^* \) for \( 1 \leq k < t \) that satisfy the identity:

\[ b \sum_{k=1}^t c_k \bar{x}^\alpha_k f_k = \sum_{1 \leq k < t} b_k S(c_k \bar{x}^\alpha_k f_k, c_k \bar{x}^\alpha f_k) = \sum_{1 \leq k < t} b_k m_k \bar{x}^{\beta - \gamma_k} S(f_k, f_k). \] (3.12)

where \( \bar{x}^{\gamma_k} := \text{lcm}(\text{LM}(f_k), \text{LM}(f_k)) \) and \( m_k := \text{lcm}(c_k \cdot \text{LC}(f_k), c_k \cdot \text{LC}(f_k))/\text{lcm}(\text{LC}(f_k), \text{LC}(f_k)) \) for \( 1 \leq k < t \). Moreover, by Lemma 3.11 (2), we can relabel the subscripts of the elements in \( F \) such that \( \text{mult}_p(b) = 0 \).

Each \( S \)-polynomial \( S(f_k, f_k) \) in (3.12) has a proper reduction by the prebasis set \( G \) as in the steps A4 of the algorithm in Lemma 3.9. Further, we have \( \text{LM}(S(f_k, f_k)) < \bar{x}^{\gamma_k} \). These proper reductions together with the second summation in (3.11) yield a new representation \( \mu f_k = \sum_{k=0}^s a_k g_k \) with \( g_0 := \chi_k \) such that \( \max_{0 \leq k \leq s} \{ \text{LM}(a_k g_k) \} = \bar{x}^{\beta} \). Here the quotient \( a_k \) is in \( K[x_1][\bar{x}] \) for \( 0 \leq k \leq s \). The multiplier \( \mu \in (K[x_1])^* \) satisfies \( \gcd(\mu, \chi_0^\lambda) = 1 \). It is evident that \( \text{mult}_p(\mu b) = 0 \).

We repeat the above procedure on the new representation \( \mu f = \sum_{k=0}^s a_k g_k \). The repetition halts in finite steps since the monomial ordering on \( \bar{x} \) is a well-ordering. We obtain a representation in the form of either (3.8) satisfying (3.9), or (3.10) when \( f = \chi \). However for the time being we just denote the multiplier in (3.8) or (3.10) as \( \lambda_p \) since it satisfies \( \text{mult}_p(\lambda_p) = 0 \).

Finally we define the multiplier \( \lambda := \gcd(\{ \lambda_p : p \in \Theta \}) \) such that \( \gcd(\lambda, \chi_0^\lambda) = 1 \) and \( \lambda = \sum_{p \in \Theta} d_p \lambda_p \) with \( d_p \in K[x_1] \). By \( f = \sum_{p \in \Theta} d_p \lambda_p f \) and the above representations of \( \lambda_p f \) for \( p \in \Theta \), we obtain the final conclusion. \( \square \)
Corollary 3.13. (1) The eliminant \( \chi \) is divisible by the compatible part \( \chi_0^\alpha \) of the pre-eliminant \( \chi_0 \).

(2) Let \( I := (F) \) be the zero-dimensional polynomial ideal as in Lemma 3.12 together with its pre-eliminant \( \chi_0 \) and prebasis \( G \). When \( \chi_0^\alpha \neq 1 \), let us denote \( \chi_0^\alpha \) simply as \( q \) and define the PIR \( R_q \) that is isomorphic to \( K[x_1]/(\chi_0^\alpha) \) as in (2.1). Under the epimorphism \( \sigma_q \) as in (2.3), we denote \( I_q := \sigma_q(I) \) and \( B_q := \sigma_q(G) \). Then holds the identity (2.7) that defines the proper basis.

Proof. (1) A direct consequence of (3.10).

(2) Let \( \iota_q \) be the injection defined in (2.4). For every \( f \in I_q \) with \( \text{lcm}(f) \in R_q^* \) being nonzero, \( \exists g \in I \) such that \( \sigma_q(g) = f \). Then \( g - \iota_q(f) \in (\chi) \) and thus \( (\chi/q)(g - \iota_q(f)) \in (\chi) \). Hence \( (\chi/q)\iota_q(f) \in I \).

As per Lemma 3.12, there exist \( \{q_k : 0 \leq k \leq s \} \subset K[x_1][\widehat{x}] \) as well as a multiplier \( \lambda \in (K[x_1])^* \) satisfying \( \gcd(\lambda, q) = 1 \) such that both (3.8) and (3.9) hold for \( (\chi/q)\iota_q(f) \). For \( 1 \leq k \leq s \), we collect the subscript \( k \) into a set \( \Lambda \) if it satisfies both \( \text{lcm}(q_k g_k) = \text{lcm}(\iota_q(f)) \) and \( \sigma_q(\text{lcm}(q_k g_k)) \in R_q^* \) being nonzero. Since \( \sigma_q(\lambda \chi/q) \in R_q^* \) is a unit, we have \( \Lambda \neq \emptyset \) due to the equality (3.9). Then (2.7) follows from the identity:

\[
\text{lt}(f) = \sigma_q(\lambda \chi/q)^{-1} \cdot \sum_{k \in \Lambda} \sigma_q(\text{lt}(q_k)) \cdot \text{lt}((\sigma_q(g_k))) \in \langle \text{lt}(B_q) \rangle.
\]

When the compatible part \( \chi_0^\alpha = 1 \), we simply ignore the partial proper basis \( B_q \) in the above Corollary 3.13 (2) and continue with the algorithm in the following Section 4.

4 The Final Algorithmic Step in \( R_q[\widehat{x}] \)

In this section we complete the construction of the proper basis. This is based on a modular algorithm which involves unorthodox computations in PIRs with zero divisors. The content of this section totally parallels that of Section 3.

Let \( \chi_0 \) be the pre-eliminant that is obtained in Lemma 3.9. Let \( \chi_0^\alpha \) be its compatible part as before. Suppose that \( \chi_0/\chi_0^\alpha = \prod g_i^\alpha \) is a squarefree factorization. More specifically, \( g_i \in K[x_1] \) is not a constant. For \( 1 \leq i, j \leq s \) and \( i \neq j \), \( g_i \) and \( g_j \) are coprime if neither of them is a unit. For \( 1 \leq i \leq s \), if \( p \in K[x_1] \) is a monic irreducible polynomial that divides \( g_i \), then \( \text{mult}_p(g_i) = 1 \) and \( \text{mult}_p(\chi_0/\chi_0^\alpha) = i \).

Notation 4.1 (The modulus \( q \) as the factor \( g_i \) of \( \chi_0/\chi_0^\alpha \)).

For \( 1 \leq i \leq s \), if the squarefree factor \( g_i \) of \( \chi_0/\chi_0^\alpha \) is not a unit, let us simply denote the factor \( g_i \) as \( q \).

We define the PIR \( R_q \) that is isomorphic to \( K[x_1]/(g_i) \) together with the epimorphism \( \sigma_q \) and injection \( \iota_q \) like in (2.3) and (2.4).

Definition 4.2 (Modular proper term reduction in the algebra \( R_q[\widehat{x}] \)).

For \( f \in R_q[\widehat{x}] \setminus R_q \) and \( g \in (R_q[\widehat{x}])^* \setminus R_q^* \) with \( \text{lcm}(g) \in R_q^* \), suppose that \( f \) has a term \( c_\alpha \widehat{x}^\alpha \) with \( \widehat{x}^\alpha \in \text{supp}(f) \cap (\text{lcm}(g)) \). We define the multipliers \( \mu := \sigma_q(\text{lcm}(\iota_q(f), l_\alpha)/l_\alpha) \) and \( m := \sigma_q(\text{lcm}(l_\alpha, l_g)/l_g) \) with \( l_\alpha := \iota_q(c_\alpha) \) and \( l_g := \iota_q(\text{lcm}(g)) \). If the multiplier \( \mu \) satisfies \( m \in R_q^* \) being a unit, we make a modular proper reduction of the term \( c_\alpha \widehat{x}^\alpha \) by \( g \) as follows.

\[
h = \mu f - \frac{m \widehat{x}^\alpha}{\text{lcm}(g)} g.
\]

We call \( h \) the remainder of the reduction and \( \mu \) the least multiplier with respect to \( g \).

Definition 4.3 (Properly reduced polynomial in \( R_q[\widehat{x}] \)).

A nonzero term \( c_\alpha \widehat{x}^\alpha \in R_q[\widehat{x}] \) is said to be properly reducible with respect to \( F = \{f_1, \ldots, f_s\} \subset R_q[\widehat{x}] \setminus R_q \) if \( \widehat{x}^\alpha \) is divisible by \( \text{lcm}(f_j) \) for some \( f_j \in F \) and moreover, \( \text{the least multiplier } \mu \) with respect to \( f_j \) is a unit in \( R_q^* \) as in (4.1). A polynomial \( f \in R_q[\widehat{x}] \) is properly reduced if it has no properly reducible terms with respect to \( F \).

The proof for the following conclusion is almost a verbatim repetition of that for Theorem 3.4.

Theorem 4.4 (Modular proper division or reduction in \( R_q[\widehat{x}] \)).

Suppose that \( F = \{f_1, \ldots, f_s\} \) is a finite polynomial set in \( R_q[\widehat{x}] \) \( \setminus R_q \). For every \( f \in R_q[\widehat{x}] \), there exist a multiplier \( \lambda \in R_q^* \) being a unit as well as a remainder \( r \in R_q[\widehat{x}] \) and quotients \( q_j \in R_q[\widehat{x}] \) for \( 1 \leq j \leq s \) such that:

\[
\lambda f = \sum_{j=1}^s q_j f_j + r,
\]
Lemma 4.8. (The algorithm computing a partial proper basis)
Here the multiplier $d := \gcd_{q}(\text{LC}(f), \text{LC}(g))$ is nonzero, i.e., $d \in R_q^{\times}$ and $l_h := \iota_q(\text{LC}(h))$ and $d := \gcd(\text{lcm}(l_f, l_g), l_h)$.

Definition 4.5. ($S$-polynomial in $R_q[\bar{x}]$).
Suppose that $f$ and $g$ are in $R_q[\bar{x}] \setminus R_q$. Let us denote $l_f := \iota_q(\text{LC}(f))$ and $l_g := \iota_q(\text{LC}(g))$. We define the multipliers $m_f := \sigma_q(\text{lcm}(l_f, l_g)/l_f)$ and $m_g := \sigma_q(\text{lcm}(l_f, l_g)/l_g)$ as well as the monomial $\hat{\chi} := \text{lcm}(\text{LM}(f), \text{LM}(g))$. Then the following polynomial:

$$S(f, g) := \frac{m_f \hat{\chi}}{\text{LM}(f)} f - \frac{m_g \hat{\chi}}{\text{LM}(g)} g$$

is called the $S$-polynomial of $f$ and $g$ in $R_q[\bar{x}]$.

There are two special $S$-polynomials as follows.
1. For every $f \in R_q[\bar{x}] \setminus R_q$, we have $S(f, g) = n_f f_1$ with $n_f := \sigma_q(g/\gcd(l_f, q))$ and $f_1 := f - \text{LT}(f)$.
2. For $f \in R_q[\bar{x}] \setminus R_q$ and $g \in R_q^{\times}$, we take $\text{LM}(g) = 1$ and $\text{LC}(g) = g$ in (4.4). The $S$-polynomial satisfies $dS(f, g) := f_1 g$ with $d = \gcd_{q}(\text{LC}(f), g)$ and $f_1 := f - \text{LT}(f)$.

The following two conclusions are modular versions of Lemma 3.7 and Lemma 3.8 and we omit their trivial proofs here.

Lemma 4.6. For $f, g \in R_q[\bar{x}] \setminus R_q$, suppose that $\text{LM}(f)$ and $\text{LM}(g)$ are relatively prime. Let us denote $d := \gcd_{q}(\text{LC}(f), \text{LC}(g))$. Then the $S$-polynomial $S(f, g)$ satisfies $dS(f, g) = f_1 g - g_1 f$ with $f_1 := f - \text{LT}(f)$ and $g_1 := g - \text{LT}(g)$. Moreover, we have $\text{LM}(S(f, g)) = \max\{\text{LM}(f_1) \cdot \text{LM}(g), \text{LM}(g_1) \cdot \text{LM}(f)\}$. For $f, g \in (R_q[\bar{x}])^* \setminus R_q^{\times}$ without both of them being in $R_q^{\times}$, we define the relative common multiplier of $g$ versus $f$ as $\text{rcm}(g|f) := m_f \hat{\chi}/\text{LM}(f)$ with $m_f$ and $\hat{\chi}$ being defined as in Definition 4.5.

Lemma 4.7. For $f, g, h \in (R_q[\bar{x}])^* \setminus R_q^{\times}$ with at most one of them being in $R_q^{\times}$, if $\text{lcm}(\text{LM}(f), \text{LM}(g))$ is divisible by $\text{LM}(h)$, then holds the following triangular identity among the $S$-polynomials:

$$\lambda S(f, g) = \frac{\lambda \cdot \text{rcm}(g|f)}{\text{rcm}(h|f)} S(f, h) - \frac{\lambda \cdot \text{rcm}(f|g)}{\text{rcm}(h|g)} S(g, h).$$

Here the multiplier $\lambda := \sigma_q(l_h/d)$ is nonzero, i.e., $\lambda \in R_q^{\times}$ with $l_h := \iota_q(\text{LC}(h))$ and $d := \gcd(\text{lcm}(l_f, l_g), l_h)$.

The following algorithm is a slight revision of the one in Lemma 3.9.

Lemma 4.8. (The algorithm computing a partial proper basis $B_q$ in $R_q[\bar{x}]$).
Let $F \subset R_q[\bar{x}] \setminus R_q$ be a finite polynomial set. Then the algorithm that consists of the following sequence of instructions terminates in finite steps.

B1. Start with a prebasis set $G := F$, temporary set $S := \emptyset$ of $S$-polynomials, and temporary pre-eliminant $\chi_q \in R_q$ as $\chi_q := 0$.

B2. For each pair $f, g \in G$ with $f \neq g$, execute the instructions in B3.

B3. If $\text{LM}(f)$ and $\text{LM}(g)$ are relatively prime, and the multiplier $d := \gcd_{q}(\text{LC}(f), \text{LC}(g))$ is a unit, continue; else if there exists an $h \in G \setminus \{f, g\}$ such that $\text{lcm}(\text{LM}(f), \text{LM}(g)) \in (\text{LM}(h))$, and the multiplier $\lambda$ as in (4.5) is a unit, continue;

Else, compute the $S$-polynomial $S(f, g)$ as in (4.4) and add it into the set $S$. 

8
The proof is almost a verbatim repetition of that for Lemma 3.12.

(2) For every irreducible factor $p$ of the modulus $q$, we can always relabel the subscripts of the polynomial set $F = \{f_j : 1 \leq j \leq s\}$ such that the multiplier $b_j \in R_q^*$ in (4.6) is not divisible by $p$.

Proof. (1) Let us denote $l_j := \text{lcm}(\text{LC}(f_j))$ for $1 \leq j \leq s$. We define the multipliers $m_j := \text{lcm}(l_j, l_s)/l_j$ for $1 \leq j < s$ and a multiplier $a := \text{lcm}_{1 \leq j \leq s}(m_j)$. With $a_j := a/m_j \in R_q^*$ for $1 \leq j < s$, we can easily verify that $b_j := \sigma_q(a_j)$ and $b := \sigma_q(a)$ in $R_q^*$ satisfy the identity (4.6).

(2) Given an irreducible factor $p$ of the modulus $q$, we can always change the order of the elements in the polynomial set $F = \{f_j : 1 \leq j \leq s\}$ such that $\text{mult}_p(l_s) = \min_{1 \leq j \leq s}\{\text{mult}_p(l_j)\}$. Hence $\text{mult}_p(m_j) = \text{mult}_p(l_s/\text{gcd}(l_j, l_s)) = 0$ for $1 \leq j < s$, from which we can deduce that $\text{mult}_p(b) = 0$.

Lemma 4.10. For a finite polynomial set $F \subset R_q[\tilde{x}] \setminus R_q$, let $G = \{g_k : 1 \leq k \leq s\}$ and $\chi_q$ be the prebasis and pre-eliminator that are obtained in the algorithm of Lemma 4.8. For every $f \in \langle F \rangle$, there exist $\{q_k : 0 \leq k \leq s\} \subset R_q[\tilde{x}]$ and a unit multiplier $\lambda \in R_q^*$ such that:

$$\lambda f = \sum_{k=1}^{s} q_k g_k + q_0 \chi_q.$$  \hfill (4.7)

Moreover, the polynomials in (4.7) satisfy the following condition:

$$\text{LM}(f) = \max\{\max_{1 \leq k \leq s}\{\text{LM}(g_k) \cdot \text{LM}(g_k)\}, \text{LM}(q_0 \chi_q)\}.$$  \hfill (4.8)

In particular, the identities (4.7) and (4.8) still hold in the case of $\chi_q = 0$.

Suppose that $I$ is a zero-dimensional polynomial ideal in $K[x_1][\tilde{x}]$ satisfying $\sigma_q(I) = \langle F \rangle$. Then its eliminant $\chi$ also satisfies (4.7) with $q_0 \in R_q$ and $\lambda \in R_q^*$ as follows:

$$\lambda \sigma_q(\chi) = q_0 \chi_q.$$  \hfill (4.9)

Proof. The proof is almost a verbatim repetition of that for Lemma 3.12.
Corollary 4.11. (1) In the case of \( \chi_q = 0 \), the eliminant \( \chi \) is divisible by \( q \); Otherwise it is divisible by \( \iota_q(\chi_q) \).

(2) Let \( F \subset R_q[\tilde{x}] \setminus R_q \) be a finite polynomial set as in Lemma 4.10 together with its pre-eliminant \( \chi_q \) and prebasis \( G \). Suppose that \( I \) is a zero-dimensional polynomial ideal such that \( \sigma_q(I) = \langle F \rangle \). In the case of \( \chi_q = 0 \), we denote \( I_q := \sigma_q(I) \) and \( B_q := G \). Then holds the identity (2.7) that defines the proper basis; Otherwise we substitute \( \iota_q(\chi_q) \) for \( g_i^1 \) as the modulus \( q \) in Notation 4.1. Then still holds the identity (2.7) that defines the proper basis.

Proof. (1) The conclusion readily follows from the identity (4.9).

(2) In the case of \( \chi_q = 0 \), for every \( f \in I_q \), the identity (4.7) and (4.8) holds. Then the identity (2.7) follows from the nonempty subscript set \( \Lambda := \{ 1 \leq k \leq s : LM(q_k) \cdot LM(q_k) = LM(f), LC(q_k) \cdot LC(q_k) \in R_q \} \).

In the case when \( \chi_q \in R_q^* \) is nonzero, consider the natural epimorphism \( \sigma : R_q \to R_q/(\chi_q) \) with \( \chi_q \) being the principal ideal generated by \( \chi_q \in R_q \). It induces an epimorphism \( \sigma : R_q[\tilde{x}] \to (R_q/(\chi_q))[\tilde{x}] \) like in (2.3). After we apply \( \sigma \) to (4.7), the proof of (2.7) is a verbatim repetition of the above case.

5 An Example

In the following example it is conspicuous that the coefficients of the proper basis are of moderate sizes and swell like neither those of Gröbner basis over \( \mathbb{Q} \) nor those of Möller’s Gröbner basis over \( \mathbb{Q}[z] \).

Example 5.1. Suppose that we have a zero-dimensional polynomial ideal \( I = \langle f, g, h \rangle \subset \mathbb{Q}[x, y, z] \) with \( f = -z^2(z + 1)^3x + y; g = z^3(z + 1)^6x - y^2; h = x^2y + z^3(z - 1)^5 \).

For the purpose of comparison, let us list its reduced Gröbner basis \( G = \{ \chi, g_1, g_2, g_3, g_4 \} \) over \( \mathbb{Q} \) with respect to the LEX ordering \( x > y > z \) as follows:

\[
\begin{align*}
\chi &= z^6(z - 1)^5(z^{13} + 9z^{12} + 36z^{11} + 84z^{10} + 126z^9 + 126z^8 + 85z^7 + 31z^6 + 19z^5 - 9z^4 + 4z^3 \\
&\quad - 4z^2 - 3z - 1); \\
g_1 &= 20253807z^2y + 264174124z^{23} + 1185923612z^{22} + 850814520z^{21} - 3776379304z^{20} \\
&\quad - 6824277548z^{19} + 1862876196z^{18} + 12815317453z^{17} + 3550475421z^{16} + 2124010581z^{15} \\
&\quad - 35582561480z^{14} + 4291843554z^{13} - 41728834070z^{12} + 35649844325z^{11} - 17049238505z^{10} \\
&\quad + 3388659963z^9 + 930240431z^8 - 61146095z^7 - 518331181z^6; \\
g_2 &= 20253807y^2 + 903303104z^{23} + 4102316224z^{22} + 3140448384z^{21} - 1268348798z^{20} \\
&\quad - 2399669428z^{19} + 480472920z^{18} + 4373994786z^{17} + 1490642335z^{16} + 9051639768z^{15} \\
&\quad - 12140061331z^{14} + 13997060534z^{13} - 138071007235z^{12} + 118589702914z^{11} \\
&\quad - 55199680030z^{10} + 1192745234z^9 + 2021069107z^8 - 38017822z^7 - 176286683z^6; \\
g_3 &= 2592487926z^2x + (7777461888z - 2592487926)y + 108083949263z^{23} + 486376518055z^{22} \\
&\quad + 349575751130z^{21} - 1558206505718z^{20} - 282017901021z^{19} + 78826739707z^{18} \\
&\quad + 535042098351z^{17} + 1476923019345z^{16} + 68933055575z^{15} - 14602936038043z^{14} \\
&\quad + 17386123487861z^{13} - 16350032901517z^{12} + 13787524468420z^{11} - 623568320715z^{10} \\
&\quad + 78699720594z^9 + 628350552934z^8 - 64382649679z^7 - 206531313875z^6; \\
g_4 &= 20253807x^2 + 1037040736z^{23} + 4686773132z^{22} + 3455561112z^{21} - 14868243976z^{20} \\
&\quad - 2470438972z^{19} + 6731446644z^{18} + 51651585868z^{17} + 16267315284z^{16} + 7429467573z^{15} \\
&\quad - 14163619691z^{14} + 63168836472z^{13} - 15545190640z^{12} + 13570646958z^{11} \\
&\quad - 62903516282z^{10} + 11263864699z^9 + 2500312823z^8 + 197272975z^7 - 1682438629z^6 \\
&\quad - 101269035z^5 + 20253807z^4.
\end{align*}
\]

According to [1, P254, Theorem 4.5.12], this is also Möller’s strong Gröbner basis in \( \mathbb{Q}[z][x, y] \).
We begin the computation of the proper basis by listing the prebasis elements $G = \{ f, g, h \}$ in increasing order of their leading terms.

We disregard the $S$-polynomial $S(g, h)$ based on Lemma 3.8 since $\text{lc}(LT(g), LT(h)) = z^4(z + 1)^6 x^2 y$ is divisible by $LT(f) = -z^2(z + 1)^3 x$ and the multiplier $\lambda = 1$. Then we compute the $S$-polynomials $S(f, g)$ and $S(f, h)$ and make proper reductions. The remainders are $e := -y^2 + 2 z^2(z + 1)^3 y$ and $d := z^2(z + 1)^3 [(z^2(z + 1)^6 - 1) y + z^4(z + 1)^5]$. The prebasis set $G$ becomes $\{ d, e, f, g, h \}$.

We disregard the $S$-polynomials $S(e, f)$ and $S(e, g)$ based on Lemma 3.7 since $\text{lc}(LT(e))$ is relatively prime to both $LT(f)$ and $LT(g)$. We also disregard the $S$-polynomial $S(e, h)$ since $\text{lc}(\text{LM}(e), \text{LM}(h)) = x^2 y^2$ is divisible by $LM(f) = x$. Now the multiplier $\lambda$ in the identity (3.6) equals $-z^2(z + 1)^3 y$ and we add it into the multiplier set $\Lambda$.

We disregard the $S$-polynomials of $S(d, f)$ and $S(d, g)$ since the leading monomial $\text{LM}(d) = y$ is relatively prime to $\text{LM}(d) = y$. Moreover, we also disregard the $S$-polynomial $S(d, h)$ since $\text{lc}(LT(d), LT(h)) = -z^2(z + 1)^3(z^4(z + 1)^6 - 1) x^2 y$ is divisible by $LT(f) = -z^2(z + 1)^3 x$.

Let us compute and then make a proper reduction of the $S$-polynomial $S(d, e) = -z^4(x + 1)^3(z + 11 + 36 z^2 + 126 z^2 + 85 z^2 + 31 z^2 + 9 z^2 + 4 z^3 - 4 z^2 - 3 z - 1) y$. We obtain the pre-eliminant $\chi_0 = (z + 1)^3 z^8(z + 1)^3(z + 1)^3 + 36 z^2 + 126 z^2 + 85 z^2 + 31 z^2 + 9 z^2 + 4 z^3 - 4 z^2 - 3 z - 1) y$ with the multiplier $\mu = z^4(z + 1)^6 - 1$. We add $\mu$ into the multiplier set $\Lambda = \{ z^2(z + 1)^3, z^4(z + 1)^6 - 1 \}$.

By a comparison between $\chi_0$ and $\Lambda$, we obtain the compatible part $\chi_0^0 = (z + 1)^5(z + 1)^3(z + 1)^3 + 36 z^2 + 126 z^2 + 85 z^2 + 31 z^2 + 9 z^2 + 4 z^3 - 4 z^2 - 3 z - 1) y$. The squarefree factors of $\chi_0^0$ are $z^8(z + 1)^3$. For the modulus $q = (z + 1)^3$ and hence over $R_q = \mathbb{Q}[z]/((z + 1)^3)$, our computation shows that the ideal $\sigma_q(I) = \{ 1 \}$ and thus it should be disregarded.

For the modulus $q = z^6$ and hence over $R_q = K[z]/(z^6)$, we abuse the notations a bit and still use $f, g, h$ to denote $\sigma_q(f), \sigma_q(g), \sigma_q(h)$. The squarefree part of $\text{LC}(g)$ equals $(z + 1)^6$. Hence we use it as a simple representation of $g$ and the same for $h$. We disregard the $S$-polynomial $(g, h)$ by the triangular identity with respect to $f$.

We compute and then make a modular proper reduction of the $S$-polynomials $S(f, g)$ and $S(f, h)$ to obtain the remainders $e := -y^2 + 2 z^2(z + 1)^3 y$ and $d := -z^2(z + 1)^3(z^4(z + 1)^6 + 1) y - 2 z^3 + z^4$. We add $d, e$ into the prebasis $G = \{ d, e, f, g, h \}$.

We disregard the $S$-polynomials $S(e, f)$ and $S(e, g)$ since $\text{LC}(e)$ is relatively prime to both $LT(f)$ and $LT(g)$. We also disregard the $S$-polynomials $S(d, g)$ and $S(d, h)$ by the triangular identities with respect to $f$. Moreover, the remainder of modular proper reduction of the $S$-polynomial $S(d, e)$ equals 0.

The modular proper reduction of the $S$-polynomial $S(d, f)$ yields the pre-eliminant $\chi_4 = z^6$. We substitute $q = z^6$ for the old modulus $q = z^8$. Then we compute and make a modular proper reduction of the $S$-polynomial $S(e, h)$ to obtain 0. The same for the special $S$-polynomials $S(f, q), S(g, q), S(h, q)$.

After removing the redundancies of the prebasis $G$, we obtain a partial proper basis over $R_q \cong K[x]/(z^6)$ as follows. It corresponds to the pre-eliminant $\chi_4 = z^6$ as above.

$$B_q : \begin{cases} b_1 := z^2(z + 1)^3 y; & b_2 := y^2; \\ b_3 := z^2(z + 1)^3 y - x & b_4 := x^2 y - z^4(z + 1)^5. \end{cases}$$ (5.2)

The partial proper basis over $R_q \cong K[x]/(\chi_4^0)$ is as follows. It corresponds to the compatible part $\chi_4^0$ that is also a factor of the eliminant $\chi$ by Corollary 3.13 (1).

$$B_q : \begin{cases} a_1 := z^2(z + 1)^3(z^4(z + 1)^6 - 1) y + z^6(z + 1)^3(z + 1)^5; \\ a_2 := z^4(z + 1)^6(z^4(z + 1)^6 - 1) x + z^6(z + 1)^3(z + 1)^5. \end{cases}$$ (5.3)

Hence the eliminant is $\chi = \chi_4^0 \cdot t_q(\chi_4)$, which coincides with the one obtained via the Gröbner basis in (5.1). The partial proper bases in (5.2) and (5.3) constitute the proper basis of $I$ as in (2.8).

6 Benchmark Testings in a Cascade of Complexity

In order to corroborate the distinctive computational advantage of the proper basis algorithm over Buchberger’s and Möller’s classical algorithms for Gröbner bases, we conducted a cascade of benchmark testings.
that are in increasing order of complexity. The programming language is Maple 18. The timings were conducted on an 11th Gen Intel Core i7 3.30 GHz system with 32.0 GB RAM under a 64-bit version of Windows 10 operating system. All the computations are over the rationals $\mathbb{Q}$ with respect to the typical LEX ordering $x \succ y \succ z$.

**Example 6.1.** (1) $I = \langle x^2 + x - zy, \; -zx + y^3 + 2, \; -x + y + z^2 - 1 \rangle$;

(2) $I = \langle x^2 + x - zy^2, \; -zx + y^4 + 2, \; -x + y^2 + z^2 - 1 \rangle$;

(3) $I = \langle x^2 + x - zy^3, \; -zx + y^4 + 2, \; -x + y^2 + z^2 - 1 \rangle$;

(4) $I = \langle x^2 + x - zy^3, \; -zx + y^5 + 2, \; -x + y^2 + z^2 - 1 \rangle$;

(5) $I = \langle x^2 + x - z^2y^3, \; -z^2x + y^5 + 2, \; -x + y^2 + z^3 - 1 \rangle$;

(6) $I = \langle x^2 + x - z^2y^3, \; -z^3x + y^6 + 2, \; -x + y^2 + z^3 - 1 \rangle$;

(7) $I = \langle x^2 + x - zy^3, \; -zx + y^5 + 2, \; -x + y^3 + z^2 - 1 \rangle$;

(8) $I = \langle x^2 + x - zy^3, \; -zx + y^5 + 2, \; -x + y^3 + z^2 - 1 \rangle$;

(9) $I = \langle x^2 + x - z^2y^4, \; -z^2(z^3 - 2)x^2 + y^6 + 2z^4, \; -x^2 + y^4 + z^4 - z \rangle$;

(10) $I = \langle x^2 + x - z^2y^3, \; -z(z - 1)x^2 + y^6 + z^4, \; -x + y^5 + z^2 - 1 \rangle$;

(11) $I = \langle x^3 + x - z^2y^4, \; -z(z - 1)x^2 + y^5 + z^4, \; -x + y^5 + z^2 - 1 \rangle$;

(12) $I = \langle x^2 + x - z^2y^4, \; -z(z - 1)x^2 + y^6 + z^4, \; -x + y^5 + z^2 - 1 \rangle$;

(13) $I = \langle x^3 + x - z^2y^4, \; -z(z - 1)x^2 + y^6 + z^4, \; -x + y^5 + z^2 - 1 \rangle$;

In the following tables the unit for the timings is in second. The symbol “N/A” means that either Maple crashed or the running time was more than 86400.000 seconds (24 hours).

| Example 6.1 | Proper basis | Möller’s basis | Buchberger’s basis |
|-------------|--------------|----------------|--------------------|
| (1)         | 0.016        | 0.032          | 0.453              |
| (2)         | 0.000        | 0.016          | 0.047              |
| (3)         | 0.750        | 1.594          | 79.250             |
| (4)         | 2.172        | 7.547          | 442.125            |
| (5)         | 1.953        | 112.391        | 9569.672           |
| (6)         | 2.000        | 145.703        | 14694.797          |
| (7)         | 2.000        | 36229.156      | N/A                |
| (8)         | 2.953        | 12516.609      | N/A                |
| (9)         | 5.829        | N/A            | N/A                |
| (10)        | 15.390       | N/A            | N/A                |
| (11)        | 32.203       | N/A            | N/A                |
| (12)        | 75.297       | N/A            | N/A                |
| (13)        | 194.735      | N/A            | N/A                |

**Remark 6.2.** The above implementations for all the three algorithms are primitive in the sense that we only make basic optimizations like in Lemma 3.7 and Lemma 3.8, or Lemma 4.6 and Lemma 4.7. This leaves room for further improvements and optimizations on the proper basis algorithm. In fact, it is a natural expectation that all the state of the art algorithms that improves Buchberger’s algorithm over the last decades can be applied to the proper basis for further improvements and optimizations.
7 Conclusion and Acknowledgement

We defined the proper basis based on the proper division in Definition 2.3 for zero-dimensional polynomial ideals. The proper basis algorithm is more efficient than Buchberger’s and Möller’s classical algorithms for Gröbner bases. This is corroborated by the benchmark testings with respect to the typical LEX ordering over the rationals \( \mathbb{Q} \) in Section 6. We shall address the significant progress in generalizing the proper basis to the polynomial ideals of positive dimensions. It shall be interesting to make further efficiency improvements on the proper basis algorithm in the future.

References

[1] Adams, W., Loustaunau, P., 1994. An Introduction to Gröbner Bases. Grad. Stud. Math. 3, Amer. Math. Soc.

[2] Arnold, E., 2003. Modular algorithms for computing Gröbner bases. J. Symbolic Comput. 35, 403-419.

[3] Becker, T., Weispfenning, V., 1993. Gröbner Bases. A computational approach to commutative algebra. Grad. Texts in Math. 141, Springer.

[4] Buchberger, B., Winkler, F., 1998. Gröbner Bases and Applications. London Math. Soc. Lecture Note Ser. 251, Cambridge Univ. Press.

[5] Buchberger, B., 2006. 1965 Ph.D. Thesis: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. J. Symbolic Comput. 41 (3-4), 475-511.

[6] Buchberger, B., 1985. Gröbner bases: an algorithmic method in polynomial ideal theory, in: Bose, N. (Eds.), Multidimensional Systems Theory. D. Reidel Publishing, pp. 184-232.

[7] Collart, S., Kalkbrener, M., Mall, D., 1997. Converting bases with the Gröbner walk. J. Symbolic Comput. 24, 465-469.

[8] Cox, D., Little, J., O’Shea, D., 2005. Using Algebraic Geometry, second ed. Grad. Texts in Math. 185, Springer-Verlag.

[9] Cox, D., Little, J., O’Shea, D., 2015. Ideals, Varieties, and Algorithms. An introduction to computational algebraic geometry and commutative algebra, fourth ed. Springer-Verlag.

[10] Decker, W., Lossen, C., 2006. Computing in Algebraic Geometry. Springer-Verlag.

[11] Dubé, T., 1990. The structure of polynomial ideals and Gröbner bases. SIAM J. Comput, 19 (4), 750-773.

[12] Eder, C., Faugère, J., 2017. A survey on signature-based algorithms for computing Gröbner bases. J. Symbolic Comput. 80, 719-784.

[13] Ene, V., Herzog, J., 2012. Gröbner Bases in Commutative Algebra. Grad. Stud. Math. 130, Amer. Math. Soc.

[14] Eder, C., Hofmann, T., 2021. Efficient Gröbner bases computation over principal ideal rings. J. Symbolic Comput. 103, 1-13.

[15] Eberle, G., 1983. Some comments on the modular approach to Gröbner-bases. ACM SIGSAM Bulletin 17, 28-32.

[16] Faugère, J., Gianni, P., Lazard, D., Mora, T., 1993. Efficient computation of zero-dimensional Gröbner bases by change of ordering. J. Symbolic Comput. 16, 329-344.

[17] Francis, M., Verron, T., 2020. A signature-based algorithm for computing Gröbner bases over principal ideal domains. Math. Comput. Sci. 14, 515-530.
[18] Faugère, J., 2002. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5), in: ISSAC 2002, Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, ACM Press, 75-83.

[19] Fröberg, R., 1997. An Introduction to Gröbner Bases. John Wiley & Sons.

[20] von zur Gathen, J., Gerhard, J., 2013. Modern Computer Algebra, third ed. Cambridge Univ. Press.

[21] Gebauer, R., Möller, M., 1988. On an installation of Buchberger’s algorithm. J. Symbolic Comput. 6, 275-286.

[22] Giovini, A., Mora, T., Niesi, G., Robbiano, L., Traverso, C., “One sugar cube, please,” or selection strategies in the buchberger algorithm, in: Watt, S. (Eds.), ISSAC 1991, Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation, ACM Press, 49-54.

[23] Greuel, G., Pfister, G., 2008. A Singular Introduction to Commutative Algebra. Springer-Verlag.

[24] Gao, S.H., Volny IV, F., Wang, M.S., 2016. A new framework for computing Gröbner bases. Math. Comp. 85 (297), 449-465.

[25] Gräbe, H., 1993. On lucky primes. J. Symbolic Comput. 15, 199-209.

[26] Harvey, D., van der Hoeven, J., 2022. Polynomial multiplication over finite fields in time $O(n \log n)$. J. ACM. 69 (2), 12:1-12:40.

[27] Kreuzer, M., Robbiano, L., 2000. Computational Commutative Algebra 1. Springer-Verlag.

[28] Lazard, D., 1992. Solving zero-dimensional algebraic systems. J. Symbolic Comput. 13 (2), 117-131.

[29] Lichtblau, D., 2012. Effective computation of strong Gröbner bases over euclidean domains. Illinois J. Math. 56 (1), 177-194.

[30] Mishra, B., 1993. Algorithmic Algebra. Texts Monogr. Comput. Sci. Springer-Verlag.

[31] Möller, H., 1988. On the construction of Gröbner bases using syzygies. J. Symbolic Comput. 6 (2), 345-359.

[32] Norton, G., Sălăgean, A., 2001. Strong Gröbner bases for polynomials over a principal ideal ring. Bull. Aust. Math. Soc. 64, 505-528.

[33] Nabeshima, K., 2009. Reduced Gröbner bases in polynomial rings over a polynomial ring. Math. Comput. Sci. 2, 587-599.

[34] Pauer, F., 1992. On lucky ideals for Gröbner basis computations. J. Symbolic Comput. 14, 471-482.

[35] Rouillier, F., 1999. Solving zero-dimensional systems through the rational univariate representation. Appl. Algebra Engrg. Comm. Comput. 9, 433-461.

[36] Suzuki, A., Sato, Y., 2006. A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases, in: ISSAC 2006, Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation, ACM Press, 326-331.

[37] Sasaki, T., Takeshima, T., 1989. A modular method for Gröbner-basis construction over $\mathbb{Q}$ and solving system of algebraic equations. J. Information Processing 12, 371-379.

[38] Sturmfels, B., 1995. Gröbner Bases and Convex Polytopes. Univ. Lecture Ser. 8, Amer. Math. Soc.

[39] Traverso, C., 1989. Gröbner trace algorithms, in: Symbolic and Algebraic Computations (Rome 1988). Lecture Notes in Comput. Sci. 358, Springer-Verlag, 125-138.

[40] Winkler, F., 1988. A $p$-adic approach to the computation of Gröbner bases. J. Symbolic Comput. 6, 287-304.
[41] Wu, W.T., 1983. On the decision problem and the mechanization of theorem-proving in elementary geometry, in: Automated Theorem Proving: After 25 Years. Bledsoe, W., Loveland, D. (Eds.) Contemp. Math. 29, Amer. Math. Soc., 213-234.

[42] Wu, W.T., 2000. Mathematics Mechanization: Mechanical Geometry Theorem-Proving, Mechanical Geometry Problem-Solving and Polynomial Equations-Solving. Math. Appl. 489, Kluwer Dordrecht and Science Press Beijing.