The Generalized Rabinowitsch Trick

Deepak Kapur, Yao Sun, Dingkang Wang and Jie Zhou

Abstract The famous Rabinowitsch trick for Hilbert's Nullstellensatz is generalized and used to analyze various properties of a polynomial with respect to an ideal. These properties include, among others, (i) checking whether the polynomial is a zero divisor in the residue class ring defined by the associated ideal and (ii) checking whether the polynomial is invertible in the residue class ring defined by the associated ideal. Just like using the classical Rabinowitsch's trick, its generalization can also be used to decide whether the polynomial is in the radical of the ideal. Some of the byproducts of this construction are that it is possible to be more discriminatory in determining whether the polynomial is a zero divisor (invertible, respectively) in the quotient ring defined by the ideal, or the quotient ideal constructed by localization using the polynomial. This method also computes the smallest integer which gives the saturation ideal of the ideal with respect to a polynomial. The construction uses only a single Gröbner basis computation to achieve all these results.

Keywords Rabinowitsch trick · Zero divisor · Invertible · Radical membership

1 Introduction

The classical Rabinowitsch trick was first proposed by J.L. Rabinowitsch in his 1-page paper *Zum Hilbertschen Nullstellensatz* in 1929 [9]. This ingenious trick was used to prove the famous Hilbert's Nullstellensatz theorem. Based on this proof, the

The authors were supported by the NSF DMS-1217054 and NSFC 11371356.

D. Kapur
Department of Computer Science, University of New Mexico, Albuquerque, NM, USA

Y. Sun
SKLOIS, Institute of Information Engineering, CAS, Beijing, China

D. Wang · J. Zhou (✉)
KLMM, Academy of Mathematics and Systems Science, CAS, Beijing, China
e-mail: jiezhou@amss.ac.cn

I.S. Kotsireas and E. Martínez-Moro (eds.), *Applications of Computer Algebra*,
Springer Proceedings in Mathematics & Statistics 198,
DOI 10.1007/978-3-319-56932-1_14

radical membership problem can be solved. Let $k[X]$ be a polynomial ring over a field k, f be a polynomial and I be an ideal in $k[X]$, where $X = [x_1, \ldots, x_n]$ is a set of variables. The classical Rabinowitsch trick involves adding $fy - 1$ for performing radical membership test of f in I, where y is a new indeterminate different from X. In 2009, Sato and Suzuki [12] used this trick to compute the inverse of a polynomial f in the residue class ring $k[X]/(I : f^\infty)$.

A general construction to determine whether a given polynomial f is a zero divisor or invertible in the quotient ring $k[X]/I$, is proposed. It is proved that all this can be done using a single Gröbner basis construction of I augmented with a generalization of the classical Rabinowitsch trick, $fy - z$, where y, z are new indeterminates not appearing in X. It is also possible to perform radical membership test on f in I using the generalized construction. The generalized construction can be also used to compute the Gröbner bases of a family of related ideals–$I, I : f, I : f^2, \ldots, I : f^\infty$, $I + \langle f \rangle, I : f + \langle f \rangle, I : f^2 + \langle f \rangle, \ldots$, or $I : f^\infty + \langle f \rangle$ simultaneously, where $I : f^s = \{h \mid hf^s \in I\}$.

These results provide a necessary and sufficient condition for deciding whether f is invertible in $k[X]/(I : f^i)$ or whether f is a zero divisor in $k[X]/(I : f^i)$, where i is a nonnegative integer.

This paper is organized as follows. We review the properties of the classical Rabinowitsch trick in Sect. 2; we also relate it to Spear's trick of introducing a tag variable for studying properties of polynomial ideals; Bayer's further exploited the tag variable construction. In Sect. 3, we give two main results about the structure of the Gröbner basis of $I \cup \{fy - z\}$ and discuss how to check invertibility of f, radical membership of f, or f being a zero divisor in the residue class ring defined by I. An application of the generalized Rabinowitsch trick is presented in Sect. 4. Section 5 includes concluding remarks; as said there, constructions proposed in this paper generalize in a natural way to parameterized system using the comprehensive Gröbner system construction [7, 8].

2 Rabinowitsch Trick and Tag Variables

2.1 The Classical Rabinowitsch Trick

The classical Rabinowitsch trick was proposed to prove the famous Hilbert's Nullstellensatz theorem. Given polynomials $f, f_1, \ldots, f_s$ in $k[X]$, if f vanishes on the common zeros of $f_1, \ldots, f_s$, then there exists polynomials $a_0, a_1, \ldots, a_s$ in $k[X, y]$, such that

$$a_0(fy - 1) + a_1 f_1 + \cdots + a_s f_s = 1,$$

where y is an extra variable different from X. Substituting y by $1/f$, there exists an integer m such that f^m in the ideal generated by $f_1, \ldots, f_s$. For details, the reader can refer to [4]. The classical Rabinowitsch's trick can be used to solve the radical membership problem of an ideal by the following proposition (page 176, [3]).

Proposition 1 *Let k be an arbitrary field and let $I = \langle f_1, \ldots, f_s \rangle \subset k[X]$ be an ideal. Then $f \in \sqrt{I}$ if and only if the constant polynomial 1 belongs to the ideal $I + \langle fy - 1 \rangle$.*

Sato and Suzuki [12] used the classical Rabinowitsch trick to compute the inverse of a polynomial f in residue class ring $k[X]/(I : f^\infty)$.

Proposition 2 *Let I be an ideal and f be a polynomial in $k[X]$. If G is a Gröbner basis of the ideal $I + \langle fy - 1 \rangle$ in $k[X, y]$ w.r.t. a term order such that $y >> X$, then f is invertible in $k[X]/(I : f^\infty)$ if and only if G has a form $G = \{y - h, g_1, \ldots, g_l\}$. Further, h is an inverse of f in $k[X]/(I : f^\infty)$ and $I : f^\infty = \langle g_1, \ldots, g_l \rangle$.*

Proposition 2 can only be used to decide whether f is invertible in $k[X]/(I : f^\infty)$ directly. To decide whether f is invertible in $k[X]/I$, however, the equality of the two ideals I and $I : f^\infty$ needs to be checked.

2.2 Tag Variable

Spear [14] introduced the concept of a *tag* variable and showed how various ideal theoretic operations can be performed with Gröbner basis computations using lexicographic ordering and the associated elimination ideals; please refer to [10] for many interesting comments about Spear's contributions to Gröbner basis theory. In [13], Shannon, and Sweedler used tag variables to test if a given polynomial g of $k[x_1, \ldots, x_n]$ lay in $k[f_1, \ldots, f_s]$.

In [10], Mora credited Bayer [1] for using a tag variable and reverse lexicographic ordering to analyze the properties of a polynomial f with respect to a polynomial ideal $I = \langle f_1, \ldots, f_s \rangle$.

If a Gröbner basis $G = \langle g_1, \ldots, g_t \rangle$ of ideal $I + \langle f - z \rangle$ over $k[X, z]$ is computed w.r.t. a reverse lexicographical ordering such that $X >> z$, then each g_i can be uniquely expressed as

$$g_i = z^{d_i} h_i, \qquad z \nmid h_i, \;\; h_i \in k[X, z],$$

where d_i is a nonnegative integer. If z divides g_i, let $a_i(X, z) = g_i/z$; otherwise, $a_i = g_i$. Substitute $z = f$ into a_i and h_i, and let

$$A_i(X) = a_i(X, f), \qquad H_i(X) = h_i(X, f).$$

Proposition 3 [10] *Using the above definitions of A_i's and H_j's,*

1. *$\{A_1, \ldots, A_t\}$ is a basis of $I : f$, and*
2. *$\{H_1, \ldots, H_t\}$ is a basis of $I : f^\infty$.*

Since the reverse lexicographical (rev-lex) ordering is not a well-ordering, the procedure of computing a Gröbner basis of an ideal w.r.t. the rev-lex ordering may not terminate as illustrated by the following example.

Example 1 Consider $I = \langle x_1, x_2^2 + x_2 \rangle$; let $f = x_1 - x_2$ be a polynomial.

Bayer's method advocates computing a Gröbner basis of $\langle x_1, x_2 + x_2^2, x_1 - x_2 - z \rangle = \langle f_1, f_2, f_3 \rangle$ w.r.t. the rev-lex ordering $x_1 > x_2 > z$. Assuming that the Buchberger's algorithm [2] is used, let $\overline{f}^F$ be the remainder on division of f by the ordered tuple F, and the $S - polynomial$ of f and g is

$$S(f, g) = \frac{x^r}{\mathrm{lt}(f)} f - \frac{x^r}{\mathrm{lt}(g)} g,$$

where $\mathrm{lt}(f)$ is the leading term of polynomial f w.r.t. the rev-lex ordering $x_1 > x_2 > z$, and x^r is the least common multiple of $\mathrm{lt}(f)$ and $\mathrm{lt}(g)$.

Initial: $F = (f_1, f_2, f_3)$;

Step1: $S(f_1, f_2) = x_2 \cdot f_1 - x_1 \cdot f_2 = -x_1 x_2^2 := f_4, \quad \overline{f_4}^F = 0$;

Step2: $S(f_1, f_3) = f_1 - f_3 = x_2 + z := f_5$.

In F, only the leading term of f_2 can divide $\mathrm{lt}(f_5)$. Let $f_5 - f_2 = -x_2^2 + z$, which is still only reduced by f_2. Sequentially, it gives an infinite sequence

$$x_2 + z, -x_2^2 + z, x_2^3 + z, \ldots, (-1)^{k+1} x_2^k + z, \ldots.$$

The procedure of computing a Gröbner basis of $\langle x_1, x_2 + x_2^2, x_1 - x_2 - z \rangle$ w.r.t. the rev-lex ordering $x_1 > x_2 > z$ does not terminate. So Bayer's method can not be used directly in this case.

Mora claimed a way to overcome this problem by homogenizing an ideal. For homogeneous ideals, the Gröbner basis of an ideal w.r.t. rev-lex ordering exists. A nonhomogeneous ideal can thus first be homogenized; use then Proposition 3 on the homogenized ideal basis and then dehomogenize the result. It should be noted however that the dehomogenization does not produce a Gröbner basis of the nonhomogeneous ideal. Moreover, we want to emphasize that Proposition 3 only guarantees as its output, a basis of $I : f$ or $I : f^\infty$, not a Gröbner basis.

Example 2 Let the ideal $I = \langle x_2^2, x_1 x_2 + x_3^2 \rangle$, the polynomial $f = x_1 x_2$.

The Gröbner basis of $I + \langle f - z \rangle$ w.r.t. the rev-lex ordering $x_1 > x_2 > x_3 > z$ is $G = \langle z^2, x_2 z, x_3^2 + z, x_2^2, x_1 x_2 - z \rangle$. By the Proposition 3, $I_1 = \{x_1 x_2, x_2, x_1 x_2 + x_3^2, x_2^2\}$ is a basis of $I : f$. It is easy to check x_3^2 is in $I : f$, but $\mathrm{lt}(x_3^2) = x_3^2$ is not divided by any leading term of polynomials in G. So I_1 is not a Gröbner basis.

3 The Generalized Rabinowitsch Trick

In this section, we generalize the Rabinowitsch trick and discuss properties of f in a quotient ring such as $k[X]/I$, $k[X]/(I : f)$. Specifically, we provide necessary and sufficient conditions to check whether f is invertible or a zero divisor in $k[X]/I$, $k[X]/(I : f)$,..., $k[X]/(I : f^s)$,..., and $k[X]/(I : f^\infty)$. We can also check whether

f is in $\sqrt{I}$, the radical of ideal I, as well as find the smallest integer m such that $I : f^m = I : f^\infty$.

A polynomial f is **invertible** in $k[X]/I$, if $f \notin I$ and there exists g in $k[X]$ such that $fg - 1 \in I$. Moreover, such g is called an inverse of f in $k[X]/I$. A polynomial f is a **zero divisor** in $k[X]/I$, if $f \notin I$ and there exists h in $k[X]$ such that $h \notin I$ and $fh \in I$.

The generalized Rabinoswitsch's trick can be interpreted as integration of Rabinowitsch's trick with that of tag variable as illustrated below. Consider, the following ideal

$$J = I + \langle fy - z \rangle \subset k[X, y, z],$$

associated with I and f, where y and z are two new variables different from X.

Firstly, we analyze some special polynomials in J, which can be expressed as $g = p_t y z^t + p_{t-1} y z^{t-1} + \cdots + p_0 y + q_r z^r + q_{r-1} z^{r-1} + \cdots + q_1 z + q_0$, where $p_0, \ldots, p_t, q_0, \ldots, q_r$ are polynomials in $k[X]$.

Lemma 1 *Let $I = \langle f_1, \ldots, f_s \rangle$ be an ideal, f be a polynomial in $k[X]$, and $J = I + \langle fy - z \rangle$ be an ideal in $k[X, y, z]$. Given a polynomial $g = p_t y z^t + \cdots + p_0 y + q_r z^r + \cdots + q_1 z + q_0$ in J, where $p_0, \ldots, p_t, q_0, \ldots, q_r \in k[X]$, then*

$$p_{i-1} f^{i-1} + q_i f^i \in I,$$

where i is a nonnegative number, $p_j = 0$ when $j > t$, and $q_k = 0$ when $k > r$. Moreover, $p_{i-1} \in I : f^{i-1} + \langle f \rangle$, and when $p_{i-1} = 0$, $q_i \in I : f^i$.

Proof Since g is a polynomial in J, there exists $a_1, \ldots, a_s, a_{s+1} \in k[X, y, z]$, such that

$$p_t y z^t + \cdots + p_0 y + q_r z^r + \cdots + q_1 z + q_0 = a_1 f_1 + \cdots + a_s f_s + a_{s+1}(fy - z). \tag{1}$$

Now setting $z = fy$ in the above Eq. (1) gives

$$p_t (fy)^t y + \cdots + p_0 y + q_r (fy)^r + \cdots + q_1 (fy) + q_0 = a'_1 f_1 + \cdots + a'_s f_s,$$

where $a_j{}' \in k[X, y]$ for $j = 1, \ldots, s$. Viewing the right side of the above equation as a polynomial in $k[X][y]$, it is possible to reformulate it as $a_1{}' f_1 + \cdots + a_s{}' f_s = b_k y^k + \cdots + b_1 y + b_0$, where $b_0, \ldots, b_k \in k[X]$. Note that each b_j can also be arranged as an expression of the form $b_j = c_1 f_1 + \cdots + c_t f_t$ for some $c_1, \ldots, c_t \in k[X]$, so $b_0, \ldots, b_k \in I$. Thus,

$$p_t (fy)^t y + \cdots + p_0 y + q_r (fy)^r + \cdots + q_1 (fy) + q_0 = b_k y^k + \cdots + b_1 y + b_0.$$

Comparing each coefficient of y^i, $b_i = p_{i-1} f^{i-1} + q_i f^i$. So $p_{i-i} f^{i-1} + q_i f^i \in I$, i.e. $p_{i-1} + q_i f \in I : f^{i-1}$. It is obvious that p_{i-1} in $I : f^{i-1} + \langle f \rangle$, and $q_i \in I : f^i$ when $p_{i-1} = 0$. □

Lemma 2 *Let I, J be defined as in Lemma 1. For a polynomial h in $k[X]$, $hf^s \in I$ if and only if $hz^s \in J$, where s is any nonnegative integer.*

Proof $(\Rightarrow)$: If $hf^s \in I$, then $hz^s = h(fy - (fy - z))^s = hf^s y^s + hp(fy - z) \in J$, where $p \in k[X, y, z]$. $(\Leftarrow)$: It is obvious from Lemma 1.

□

We analyze the ideal J by studying its Gröbner basis using a block ordering in which $y \gg z \gg X$. Using the structure of this Gröbner basis, we give below the main theoretical result.

Let g be a polynomial in $k[X, y, z]$ and "$\prec$" be an admissible monomial ordering on the set of power products of $X \cup \{y, z\}$. We use notations $\mathrm{lpp}(g)$ and $\mathrm{lc}(g)$ to represent the leading power product and leading coefficient of g with respect to "$\prec$," respectively. The notation "$\prec_{y,z}$" is a restriction of "$\prec$" on the set of power products of $\{y, z\}$. We use the notations $\mathrm{lpp}_{y,z}(g)$ and $\mathrm{lc}_{y,z}(g)$ to represent the leading power product and leading coefficient of g with respect to "$\prec_{y,z}$" respectively. The notation $\mathrm{tail}(g)$ represents the part of $g - \mathrm{lc}(g)\mathrm{lpp}(g)$, i.e., g can be expressed as $g = \mathrm{lc}(g)\mathrm{lpp}(g) + \mathrm{tail}(g)$. For example, let $g = 2x^2yz + x^3z$, and "$\prec$" be the lexicographic ordering w.r.t. $z > y > x$, $\mathrm{lpp}(g) = x^2yz$, $\mathrm{lc}(g) = 2$, $\mathrm{lpp}_{y,z}(g) = yz$, $\mathrm{lc}_{y,z}(g) = 2x^2$ and $\mathrm{tail}(g) = x^3z$. And $\mathrm{lc}_{y,z}(g)$ is in $k[X]$.

Theorem 4 *Let I be an ideal and f be a polynomial in $k[X]$. Let G be a Gröbner basis of ideal $J = I + \langle fy - z\rangle \subset k[X, y, z]$ with respect to a block ordering "$\prec$" such that $y \gg z \gg X$.*

1. *Let* $P_s = \{\mathrm{lc}_{y,z}(g) \mid g \in G \cap k[X][z], \mathrm{lpp}_{y,z}(g) = z^k \text{ and } 0 \le k \le s\} \subset k[X]$. *For any integer $s \ge 0$, P_s is a Gröbner basis of $I : f^s$.*
2. *Let* $Q_s = P_s \cup \{\mathrm{lc}_{y,z}(g) \mid g \in G, \mathrm{lpp}_{y,z}(g) = yz^t, \text{ and } 0 \le t \le s\} \subset k[X]$. *For any integer $s \ge 0$, Q_s is a Gröbner basis of $I : f^s + \langle f\rangle$.*

Proof (1) First, we prove $P_s \subset I : f^s$. For any $q \in P_s$, by the construction of P_s, there exists a polynomial $g \in G$, such that $g = qz^k + \mathrm{tail}(g)$, where $0 \le k \le s$. From Lemma 1, we know $qf^k \in I$. So $q \in I : f^k \subset I : f^s$. Therefore, we have proved $P_s \subset I : f^s$.

Second, we prove P_s is a Gröbner basis of $I : f^s$, or equivalently, we need to prove that for any $h \in I : f^s$, there exists $q \in P_s$, such that $\mathrm{lpp}(q)$ divides $\mathrm{lpp}(h)$. Let h be any polynomial in $I : f^s$, we have $hf^s \in I$. Hence, we have $hz^s \in J$ by Lemma 2. Since G is a Gröbner basis of J, there exists a polynomial $g \in G$, such that $\mathrm{lpp}(g)$ divides $\mathrm{lpp}(hz^s)$. So g must have the form of $g = qz^k + \mathrm{tail}(g)$, where $q \in k[X]$ and $0 \le k \le s$. Thus, $\mathrm{lpp}(g) \mid \mathrm{lpp}(hz^s)$ means $\mathrm{lpp}(q) \mid \mathrm{lpp}(h)$, and we also have $q \in P_s$ by the construction of P_s.

(2) First, we prove $Q_s \subset I : f^s + \langle f\rangle$. For any $p \in Q_s \subset k[X]$, if $p \in P_s$, then $p \in I : f^s \subset I : f^s + \langle f\rangle$ by (1). Otherwise, if $p \notin P_s$, then there exist a polynomial $g \in G$ having the form of $g = pyz^t + \mathrm{tail}(g)$, where $0 \le t \le s$. By Lemma 1, we have $p \in I : f^t + \langle f\rangle \subset I : f^s + \langle f\rangle$. So we have proved $Q_s \subset I : f^s + \langle f\rangle$.

Second, we show Q_s is a Gröbner basis of $I : f^s + \langle f \rangle$. For any $h \in I : f^s + \langle f \rangle$, there exists $q \in I : f^s$ and $a_1, a_2 \in k[X]$ such that $h = a_1 q + a_2 f$ by the definition of $I : f^s + \langle f \rangle$. Since $q \in I : f^s$, we have $qf^s \in I$, and hence, $qz^s \in J$ by Lemma 2. Next, we construct the polynomial $T = hyz^s - a_2 z^{s+1} = (a_1 q + a_2 f)yz^s - a_2 z^{s+1} = a_1 qyz^s + a_2(fy - z)z^s \in J$. Since G is a Gröbner basis of J and $\text{lpp}(T) = \text{lpp}(h)yz^s$, there exists a polynomial $g \in G$, such that $\text{lpp}(g)$ divides $\text{lpp}(h)yz^s$. This g must have the form of $g = py^k z^t + \text{tail}(g)$, where $0 \le k \le 1$ and $0 \le t \le s$. So we have $\text{lpp}(p) \mid \text{lpp}(h)$. Due to the form of g we also have $p \in Q_s$. This shows that for any $h \in I : f^s + \langle f \rangle$ there exists $p \in Q_s$ such that $\text{lpp}(p) \mid \text{lpp}(h)$. □

If G is a minimal Gröbner basis[1] of J, it is easy to see that $I : f^{i-1} \subsetneqq I : f^i$ if and only if $P_{i-1} \subsetneqq P_i$, and $I : f^{i-1} + \langle f \rangle \subsetneqq I : f^i + \langle f \rangle$ if and only if $Q_{i-1} \subsetneqq Q_i$.

The following result serves as the basis for checking if a polynomial is invertible or a zero divisor in a residue class ring as well as for checking its membership in the radical of an ideal.

Theorem 5 *Let I be an ideal and f be a polynomial in $k[X]$. Let G be a minimal Gröbner basis of ideal $J = I + \langle fy - z \rangle \subset k[X, y, z]$ with respect to a block ordering "$\prec$" such that $y \gg z \gg X$, and P_s, Q_s are constructed from G as stated in Theorem 4. The following properties hold:*

1. *f is **invertible** in $k[X]/(I : f^s)$ if and only if $1 \in Q_s$ and $1 \notin P_{s+1}$, i.e., $I : f^s + \langle f \rangle = \langle 1 \rangle$ and $f \notin I : f^s$. The inverse of f in $k[X]/(I : f^s)$ can be obtained from G.*
2. *f is a **zero divisor** in $k[X]/(I : f^s)$ if and only if $P_s \subsetneqq P_{s+1}$ and $1 \notin P_{s+1}$, i.e. $I : f^s \subsetneqq I : f^{s+1}$ and $f \notin I : f^s$.*
3. *f is **in the radical ideal** $\sqrt{I}$ if and only if there exists an integer s such that $1 \in P_s$, i.e. $I : f^s = \langle 1 \rangle$.*
4. *m is the **smallest** integer such that $I : f^\infty = I : f^m$, if and only if $P_{m-1} \subsetneqq P_m = P_s$ for all $s > m$. Further, P_m is a Gröbner basis of $I : f^\infty$.*

Proof (1). $(\Rightarrow)$: If f is invertible in $k[X]/(I : f^s)$, then $f \notin I : f^s$ and there exists h such that $fh - 1 \in I : f^s$. So $1 \notin I : f^{s+1}$ and $1 \in I : f^s + \langle f \rangle$. By Theorem 4 (1) and (2), we have $1 \in Q_s$ and $1 \notin P_{s+1}$.

$(\Leftarrow)$: If $1 \notin P_{s+1}$ and $1 \in Q_s$, then $f \notin I : f^s$ and there exists $g \in G$ having the form of $g = yz^t + p_{t-1}yz^{t-1} + \cdots + p_0 y + q_r z^r + \cdots + q_1 z + q_0$, where $p_0, \ldots, p_{t-1}, q_0, \ldots, q_r \in k[X]$ and $0 \le t \le s$. By Lemma 1, $1 + q_{t+1} f \in I : f^t \subset I : f^s$, so f is invertible in $k[X]/(I : f^s)$ and $-q_{t+1}$ is its inverse.

(2). $(\Rightarrow)$: If f is a zero divisor in $k[X]/(I : f^s)$, then $f \notin I : f^s$ and there exists $h \notin I : f^s$ such that $fh \in I : f^s$. So $1 \notin I : f^{s+1}$ and $h \in (I : f^{s+1}) \setminus (I : f^s)$. Then $I : f^s \subsetneqq I : f^{s+1}$. By Theorem 4 (1), P_s, P_{s+1} are Gröbner bases of $I : f^s$ and $I : f^{s+1}$ respectively. So $P_s \subsetneqq P_{s+1}$ and $1 \notin P_{s+1}$.

[1]A set G is a minimal Gröbner basis of I if (1) G is a Gröbner basis of I, and (2) for each $g \in G$, $\text{lpp}(g)$ is not divisible by any leading power products of $G \setminus \{g\}$.

($\Leftarrow$) : If $1 \notin P_{s+1}$ and $P_s \subsetneqq P_{s+1}$, then $f \notin I : f^s$ and there exists $h \in P_{s+1}$ and $h \notin P_s$. From Theorem 4 (1), there exists $g = hz^{s+1} + \text{tail}(g) \in G$. Then $hf^{s+1} \in I$ by Lemma 1. So $hf \in I : f^s$, and f is a zero divisor in $k[X]/(I : f^s)$.

(3). ($\Rightarrow$) : If $f \in \sqrt{I}$, then there exists an integer t such that $f^t \in I$. So $z^t \in J$ from Lemma 2. Since G is a minimal Gröbner basis of J, there exists $g \in G$, such that $\text{lpp}(g) \mid z^s$. So g must have the form of $g = z^s + \text{tail}(g)$, where $0 \le s \le t$. By Theorem 4 (1), $1 \in P_s$.

($\Leftarrow$) : If there exists an integer s such that $1 \in P_s$, then there exists a polynomial $g = z^k + \text{tail}(g)$, where $0 \le k \le s$. By Lemma 1, $f^k \in I$, and hence, $f \in \sqrt{I}$.

(4). Since G is a minimal Gröbner basis of J, by Theorem 4 (1), $I : f^{m-1} \subsetneqq I : f^m = I : f^\infty$ if and only if $P_{m-1} \subsetneqq P_m = P_s$, for all $s > m$. Since P_m is a Gröbner basis of $I : f^m$ by Theorem 4 (1), P_m is also a Gröbner basis of $I : f^\infty$.

□

In case f is invertible in $k[X]/(I : f^s)$, the above proof shows how to construct the inverse of f. In particular, f is invertible in $k[X]/I$ if and only if $1 \in Q_0$, implying that G contains a polynomial of the form $y - h$, where $h \in k[X]$. In that case, h is an inverse of f in $k[X]/I$. Similarly, f is a zero divisor in $k[X]/I$ if and only if $P_0 \subsetneqq P_1$ and $1 \notin P_1$.

The following example illustrates Theorems 4 and 5.

Example 3 Let $I = \langle x_1^2(x_1x_2 - 1)\rangle \subset \mathbb{Q}[x_1, x_2]$, and $f = x_1$. Decide the properties of f in $\mathbb{Q}[x_1, x_2]/I$, $\mathbb{Q}[x_1, x_2]/(I : f)$, ..., and $\mathbb{Q}[x_1, x_2]/(I : f^\infty)$.

A minimal Gröbner basis of $I + \langle fy - z\rangle \subset \mathbb{Q}[x_1, x_2, y, z]$ using a lexicographic ordering with ($y > z > x_1 > x_2$) is

$$G = \{x_1^3x_2 - x_1^2, (x_1^2x_2 - x_1)z, (x_1x_2 - 1)z^2, x_1y - z, yz^2 - x_2z^3\}.$$

As per Theorem 4, we construct the following sets:

$$P_0 = \{x_1^3x_2 - x_1^2\},\ Q_0 = P_0 \cup \{x_1\},$$

$$P_1 = \{x_1^3x_2 - x_1^2, x_1^2x_2 - x_1\},\ Q_1 = P_1 \cup \{x_1\},$$

$$P_2 = \{x_1^3x_2 - x_1^2, x_1^2x_2 - x_1, x_1x_2 - 1\},\ Q_2 = P_2 \cup \{x_1, 1\}.$$

From Theorems 4 and 5, we have:

1. P_0 is a Gröbner basis of I; P_1 is a Gröbner basis of $I : f$; P_2 is a Gröbner basis of $I : f^2$.
2. Q_0 is a Gröbner basis of $I + \langle f\rangle$; Q_1 is a Gröbner basis of $I : f + \langle f\rangle$; Q_2 is a Gröbner basis of $I : f^2 + \langle f\rangle$.
3. f is invertible in $\mathbb{Q}[x_1, x_2]/(I : f^2)$, and x_2 is its inverse.
4. f is a zero divisor in $\mathbb{Q}[x_1, x_2]/I$ and $\mathbb{Q}[x_1, x_2]/(I : f)$.
5. The integer 2 is the smallest integer m such that $I : f^\infty = I : f^m$, and P_2 is a Gröbner basis of $I : f^\infty$.

4 Application in Dynamic Evaluation

It is well known that an ideal I can be decomposed using a polynomial f as follows:

$$I = (I : f^\infty) \cap (I + \langle f^m \rangle),$$

where m is the smallest number such that $I : f^\infty = I : f^m$. From Theorem 4, the smallest m and a Gröbner basis of $I : f^\infty = I : f^m$ can be derived from a Gröbner basis of ideal $I + \langle fy - z \rangle$. This means we get a decomposition of I from G. Particularly, this decomposition is not trivial if f is a zero divisor in $k[X]/I$.

In [11], Noro gave a modular method of decomposing a radical and zero-dimensional ideal I into $I : f$ and $I + \langle f \rangle$ to do dynamic evaluation a la Duval [5], where f is a zero divisor in $k[X]/I$. Note that, Noro considered only the case when m is 1 since I is radical. His method needs to compute Gröbner basis for $I : f$ and $I + \langle f \rangle$ separately. In contrast, our approach can produce these two Gröbner bases simultaneously. The following example is taken from [5].

Example 4 Let $\mathbb{Q}(a, b, c, d)$ be ring defined by a, b, c, d, which are the roots of $x^2 - 2$, $x^2 + 3$, $x^2 + 6$, and $x^2 + 1 - 2c$, respectively. Check whether $a + b - d$ is invertible in $\mathbb{Q}(a, b, c, d)$, and compute an inverse if it exists.

The ring $\mathbb{Q}(a, b, c, d)$ is isomorphic to the quotient ring $\mathbb{Q}[X]/I$ where $X = \{x_1, x_2, x_3, x_4\}$ and $I = \langle x_1^2 - 2, x_2^2 + 3, x_3^2 + 6, x_4^2 - 2x_3 + 1 \rangle$. Note that $\mathbb{Q}(a, b, c, d)$ is not a field since I is not maximal, which means $a + b - d$ may not be invertible in $\mathbb{Q}(a, b, c, d)$.

Let $f = x_1 + x_2 - x_4$. Compute a minimal Gröbner bases G of $J = I + \langle fy - z \rangle$ in $\mathbb{Q}[x_1, x_2, x_3, x_4, y, z]$ using a lexicographic ordering with $y > z > x_4 > x_3 > x_2 > x_1$. We get $G = \{x_1^2 - 2, x_2^2 + 3, x_3^2 + 6, x_4^2 - 2x_3 - 1, (x_3x_4 + x_1x_2x_4 + x_2x_3 + x_1x_3 + 2x_2 - 3x_1)z, (x_3 - x_1x_2)y + (1/2)(x_4 + x_2 + x_1)z, (x_4 - x_2 - x_1)y + z, zy + (1/120)(5x_1x_2x_4 + 2x_2x_3 + 3x_1x_3 + 16x_2 - 21x_1)z^2\}$.

As Theorem 4, we construct the following sets:

$Q_0 := \{x_1^2 - 2, x_2^2 + 3, x_3^2 + 6, x_4^2 - 2x_3 - 1\}$,
$P_0 := Q_0 \cup \{x_3 - x_1x_2, x_4 - x_2 - x_1\}$,
$Q_1 := Q_0 \cup \{x_3x_4 + x_1x_2x_4 + x_2x_3 + x_1x_3 + 2x_2 - 3x_1\}$,
$P_1 := Q_1 \cup \{1\}$.

By Theorem 5, f is a zero divisor in $\mathbb{Q}[X]/I$ and hence, not invertible in $\mathbb{Q}[X]/I$. Further, $I : f^\infty = I : f$. A nontrivial decomposition of I is thus $I = (I : f) \cap (I + \langle f \rangle) = \langle Q_1 \rangle \cap \langle P_0 \rangle$.

Again using Theorem 5 (1), f is in fact invertible in $\mathbb{Q}[X]/(I : f)$, and an inverse can be obtained from the polynomial $zy + (1/120)(5x_1x_2x_4 + 2x_2x_3 + 3x_1x_3 + 16x_2 - 21x_1)z^2$, i.e. an inverse of f in $\mathbb{Q}[X]/(I : f)$ is $-(1/120)(5x_1x_2x_4 + 2x_2x_3 + 3x_1x_3 + 16x_2 - 21x_1)$.

5 Conclusions

Using a generalization of the classical Rabinowitsch trick, we have proposed a method for checking whether a given polynomial f is invertible or a zero divisor in a residue class ring $k[X]/I$, where I is a polynomial ideal. This check is performed by computing a Gröbner basis of $I \cup \{fy - z\}$ by using a block ordering in which $y \gg z \gg X$, where y, z are new variables different from the variables in X. If f is not invertible in $k[X]/I$, it can be determined using the same Gröbner basis construction whether there is an s such that f is invertible in the residue class ring defined by the colon ideal $I : f^s$ on $k[X]$. As a byproduct, the smallest number s can be computed such that $I : f^s = I : f^\infty$, the saturation ideal of I with respect to f. The method can also be used to determine whether f is invertible or a zero divisor in $k[X]/(I : f)$, $k[X]/(I : f^2)$, $k[X]/(I : f^3)$, etc.

A nice aspect of the proposed construction is that it naturally generalizes to parametric systems using a comprehensive Gröbner system by an algorithm such as in [7, 8]. A paper on this generalization is under preparation; preliminary results on the findings were presented as an invited talk at *the International Workshop on Automated Deduction in Geometry (ADG),* Coimbra, Portugal, in July 2014.

Acknowledgements The authors are grateful to Professors Teo Mora and Yosuke Sato for their helpful discussions and suggestions.

References

1. Bayer, D.: The Division Algorithm and the Hilbert Scheme. Ph.D. thesis, Harvard (1981)
2. Buchberger, B.: Groebner bases: an algorithmic method in polynomial ideal theory. In: Bose, N.K. (ed.) Multidimensional Systems Theory, pp. 184–232. D. Reidel Publishing, Dordrecht (1985)
3. Cox, D., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms, 3rd edn. Springer, New York (2007)
4. Brownawell, W.D.: Rabinowitsch trick. In: Encyclopedia of Mathematics. Springer, Berlin (2001)
5. Duval, D.: Algebraic numbers: an example of dynamic evaluation. J. Symb. Comput. **18**, 429–445 (1994)
6. Kapur, D.: Geometry theorem proving using Hilbert's Nullstellensatz. In: Proceedings of the ISSAC 1986, pp. 202–208. ACM Press, New York (1986)
7. Kapur, D., Sun, Y., Wang, D.: An efficient algorithm for computing comprehensive Gröbner system for a parametric polynomial system. J. Symb. Comput. **49**, 27–44 (2013)
8. Kapur, D., Sun, Y., Wang, D.: An efficient method for computing comprehensive Gröbner bases. J. Symb. Comput. **52**, 124–142 (2013)
9. Rabinowitsch, J.L.: Zum Hilbertschen Nullstellensatz. Mathematische Annalen **102**(1), 520 (1929)
10. Mora, T.: Solving Polynomial Equation Systems II. Cambridge University Press, New York (2005)
11. Noro, M.: Modular dynamic evaluation. In: Proceedings of the ISSAC 2006, pp. 262–268. ACM Press, New York (2006)

12. Sato, Y., Suzuki, A.: Computation of inverses in residue class rings of parametric polynomial ideal. In: Proceedings of the ISSAC 2009, pp. 311–316. ACM Press, New York (2009)
13. Shannon, D., Sweedler, M.: Using Gröbner bases to determine algebra membership, splitting surjective algebra homomorphisms and determine birational equivalence. J. Symb. Comput. **6**, 267–273 (1988)
14. Spear, D.A.: A constructive approach to commutative ring theory. In: Proceedings of the 1977 MACSYMA Users Conference, pp. 369–376 (1977)