J. Symbolic Computation (1988) **6**, 287–304

A p-adic Approach to the Computation of Gröbner Bases

FRANZ WINKLER

Institut für Mathematik and Research Institute for Symbolic Computation, Johannes Kepler Universität, A-4040 Linz, Austria

(*Received* 5 *March* 1987, *and in revised form* 27 *November* 1987)

A method for the p-adic lifting of a Gröbner basis is presented. If F is a finite vector of polynomials in $\mathbb{Q}[x_1, \ldots, x_v]$ and p is a lucky prime for F (it turns out that there are only finitely many unlucky primes) then in a first step the normalized reduced Gröbner basis $G^{(0)}$ for F modulo p is computed, together with matrices $Y^{(0)}$ and $R^{(0)}$ such that $Y^{(0)} . G^{(0)} \equiv F$ (mod p) and $R^{(0)} . G^{(0)} \equiv 0$ (mod p), where the rows of $R^{(0)}$ are the syzygies of $G^{(0)}$ derived from the reduction of the S-polynomials of $G^{(0)}$ to 0. These congruences can be lifted to congruences modulo p^i, for any natural number i, finally leading to the normalized reduced Gröbner basis for F in $\mathbb{Q}[x_1, \ldots, x_v]$.

Introduction

p-adic methods have been successfully applied to a variety of problems in computer algebra, such as the computation of greatest common divisors of multivariate polynomials over the integers (Moses & Yun, 1973; Miola & Yun, 1974), and factorization of multivariate integral polynomials (Zassenhaus, 1969; Musser, 1975; Wang & Rothschild, 1975; Wang, 1978). For an introduction to p-adic lifting and an overview of applications we refer to (Lauer, 1983).

In all these applications the p-adic methods help to control the otherwise enormous growth of coefficients. A similar problem with coefficient growth is encountered in the computation of Gröbner bases of polynomial ideals over the rational number field $\mathbb{Q}$. Trinks remarks in (Trinks, 1984): "Dealing with $K = \mathbb{Q}$, we usually start with a system $f_1, \ldots, f_m$ having coefficients of modest size, but during the algorithm the size of coefficients tends to increase and often makes results unattainable due to space and time limits." So it is just natural to develop a p-adic method for the computation of Gröbner bases over $\mathbb{Q}$. However, to our knowledge, this problem has not received much attention yet. A method for a special case (solution of a system of algebraic equations with finitely many, simple solutions) is treated in (Trinks, 1984; Malle & Trinks, 1984) and used for the solution of an example in (Matzat & Zeh-Marschke, 1986). In this paper we report some new results on p-adic lifting of Gröbner bases, extending (Winkler, 1987a).

For future reference we review some standard definitions and facts. Throughout this paper we assume that K is a field, $K[x_1, \ldots, x_v]$ the ring of polynomials in $x_1, \ldots, x_v$ over K, and $\lhd$ is an admissible ordering of the power products in the variables $x_1, \ldots, x_v$ (as defined in Buchberger, 1985). If $f \in K[x_1, \ldots, x_v]$, then $lpp(f)$ denotes the leading power

Work reported herein has been supported by the *Österreichische Forschungsgemeinschaft*.

0747–7171/88/020287 + 18 $03.00/0

product of f w.r.t. $\lhd$ and $lc(f)$ the leading coefficient of f, i.e. the coefficient of $lpp(f)$ in f. If $F \subset K[x_1, \ldots, x_v]$, then $lpp(F) = \{lpp(f) \mid f \in F\}$. $pp(f)$ denotes the set of power products occurring in f and $pp(F) = \{pp(f) \mid f \in F\}$.

Every subset F of $K[x_1, \ldots, x_v]$ generates an ideal in $K[x_1, \ldots, x_v]$, namely

$$ideal(F) = \left\{ \sum_{i=1}^{n} h_i \,.\, f_i \mid 0 \leqslant n,\ h_i \in K[x_1, \ldots, x_v], f_i \in F \right\}.$$

F is called a *basis* of the ideal generated by F. In fact, from Hilbert's basis theorem (Hilbert, 1980; van der Waerden, 1967) we know that every ideal in $K[x_1, \ldots, x_v]$ has a finite basis. For convenience we will often write a basis F for a polynomial ideal as a vector $(F_1, \ldots, F_m)^T$ rather than a set $\{F_1, \ldots, F_m\}$.

Every set $F \subseteq R[x_1, \ldots, x_v]$, R a commutative ring, induces a *reduction relation* $\to_F$ on $R[x_1, \ldots, x_v]$ in the following way:

$$g_1 \to_F g_2 \quad \text{iff } g_2 = g_1 - \frac{a}{lc(f)} \,.\, u \,.\, f$$

for some $f \in F$, u a power product in $x_1, \ldots, x_v$, such that $u \,.\, lpp(f)$ occurs in g_1 with coefficient a and $lc(f)$ is invertible in R. In words: g_1 *is reducible to* g_2 *w.r.t.* F. If no such u and f exist, then g_1 is *irreducible w.r.t.* F. This reduction relation $\to_F$ is Noetherian. A polynomial f is reducible w.r.t. F if and only if f contains a term which is in $ideal(lpp(F))$. If $g \to_F^* h$ (g is reducible to h w.r.t. F in finitely many steps) and h is irreducible w.r.t. F then h is called a *normal form of* g *w.r.t.* F. Whenever $g_1 \to_F^* g_2$, $F = (F_1, \ldots, F_m)^T$, then $g_1 - g_2 = (h_1, \ldots, h_m) \,.\, F$ for some polynomials $h_1, \ldots, h_m$. But not every vector $(h_1, \ldots, h_m)$ corresponds to a reduction w.r.t. F. A vector $(h_1, \ldots, h_m)$ such that $(h_1, \ldots, h_m) \,.\, F = 0$ is called a *syzygy* of F. The set of syzygies of F form a module over $R[x_1, \ldots, x_v]$, the module of syzygies of F.

For $f, g \in R[x_1, \ldots, x_v]$ such that $lc(f)$ and $lc(g)$ are invertible, the *S-polynomial* of f and g is defined as follows:

$$Spol(f, g) = \frac{1}{lc(f)} \cdot \frac{lcm(lpp(f), lpp(g))}{lpp(f)} \,.\, f - \frac{1}{lc(g)} \cdot \frac{lcm(lpp(f), lpp(g))}{lpp(g)} \,.\, g.$$

A finite basis F of an ideal I in $K[x_1, \ldots, x_v]$ is a *Gröbner basis* for I iff every polynomial f in I is reducible to 0 (in finitely many steps) w.r.t. F. If $ideal(F') = I$, then in abuse of notation we also say "F is a Gröbner basis for F'" instead of "F is a Gröbner basis for I". The Gröbner basis F is called *reduced* iff, for every polynomial $f \in R$, f is irreducible w.r.t. $F \backslash \{f\}$. F is *normalized* iff every polynomial f in F is *monic*, i.e. $lc(f) = 1$. The normalized reduced Gröbner basis for an ideal I is uniquely determined (Buchberger, 1976).

There are many characterizations of Gröbner bases; we only list some of them as far as they are relevant for this paper. Let $F = (F_1, \ldots, F_m)^T$ be a finite basis of the ideal I.

—F is a Gröbner basis for I if and only if

—every S-polynomial $Spol(f, g)$ of elements $f, g \in F$ is reducible to 0 w.r.t. F if and only if

—every polynomial has a unique normal form w.r.t. F.

These and other characterizations can be found in Buchberger (1985) and Möller & Mora (1986). For an introduction to the theory of Gröbner bases we refer to Buchberger (1985). If F is a Gröbner basis, then the set $S(F)$, consisting of the vectors $(h_1, \ldots, h_m)$

derived from a reduction of the S-polynomials of F to 0 w.r.t. F, is a basis for the module of syzygies of F, see (Winkler, 1986). Whenever F is a sequence of polynomials in $K[x_1, \ldots, x_v]$ and G is a Gröbner basis for F, then there are matrices X, Y, R over $K[x_1, \ldots, x_v]$ such that $G = X \cdot F, F = Y \cdot G, R \cdot G = 0$, where the rows of R are the elements of $S(G)$. We call the matrices X and Y transformation matrices and we call the matrix R a syzygy matrix of F and G.

The notion of a Gröbner basis can be extended to modules over the polynomial ring (Galligo, 1979). All the properties of a Gröbner basis mentioned above carry over to this generalization.

In the following we will be dealing primarily with Gröbner bases in the ring $\mathbb{Q}[x_1, \ldots, x_v]$, which we will denote $\mathscr{A}$. By $\mathbb{Z}_m$ we mean the ring of integers modulo m. The ring $\mathbb{Z}_m[x_1, \ldots, x_v]$, $m \in \mathbb{N}$, will be denoted $\mathscr{A}_m$. The aim of this paper is to approximate the Gröbner basis G of a polynomial ideal in $\mathscr{A}$ by a basis G' in $\mathscr{A}_{p^n}$, p a prime. If p^n is sufficiently large, then we will be able to recover the "true" coefficients of G from their approximations in G'. The coefficients which we want to approximate will be *Farey rationals*. The *N-Farey rationals*, $N \in \mathbb{N}$, are defined as

$$\mathscr{F}_N = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z}, \ -N \leqslant a \leqslant N, \ 1 \leqslant b \leqslant N, \ gcd(a, b) = 1 \right\}.$$

Furthermore, for a prime p, $\mathscr{F}_{p,N} = \mathscr{F}_N \cap \{a/b \in \mathbb{Q} \mid gcd(b, p) = 1\}$. The elements of $\mathscr{F}_{p,N}$ can be encoded uniquely in the integers modulo m for a suitable m. More specifically, if p is a prime, $m = p^k$, N such that $N \leqslant \sqrt{(m-1)/2}$, then for any $n \in \mathbb{Z}_m$ there exists at most one $a/b \in \mathscr{F}_{p,N}$ such that $a \equiv b \cdot n \bmod m$. A proof of this fact is given, for instance, in (Trinks, 1984). The usual canonical mapping is used for mapping $\mathscr{F}_{p,N}$ into $\mathbb{Z}_m$. For the inverse mapping from $\mathbb{Z}_m$ to $\mathscr{F}_{p,N}$ one can use a suitably extended Euclidean algorithm, as described in (Kornerup & Gregory, 1983). Whenever we say that p does not divide q for a prime p and a rational number q, we mean that p divides neither the numerator nor the denominator of q, i.e. the p-adic norm of q is one, $|q|_p = 1$, and when we say that q' is the image of $q = a/b \in \mathscr{F}_{p,N}$ modulo $m = p^k$, we mean that $a \equiv b \cdot q' \bmod m$.

The structure of the paper is as follows. Section 1 contains a short discussion of lucky primes, i.e. those primes with respect to which the p-adic approximation of a Gröbner basis is possible. In Section 2 existence and uniqueness of such an approximation are investigated, giving rise to the lifting algorithm of Section 3. In Section 4 we draw some conclusions and list open problems.

1. Lucky Primes

W. S. Brown (1971) calls a prime p lucky for the computation of the greatest common divisor of two integral polynomials f and g, if p does not divide the leading coefficient of f and g and the degree of the gcd of f and g modulo p equals the degree of the gcd of f and g over the integers (the gcd of f and g modulo p cannot be less than the degree of the gcd over the integers, as long as p does not divide any of the leading coefficients of f and g). Only such lucky primes can be used in the modular computation of the polynomial greatest common divisor. We need a similar condition on the prime p.

EXAMPLE 1. (a) (from Ebert, 1983) Let $F = \{xy^2 - 2y, x^2y + 3x\} \subset \mathbb{Q}[x, y]$. Let the power products be ordered according to the graduated lexicographic ordering with $x < y$.

The normalized reduced Gröbner basis for F in $\mathbb{Q}[x, y]$ is $G = \{x, y\}$. $G \bmod 5 = \{x, y\}$, but that is not a Gröbner basis for *ideal*(F) in $\mathbb{Z}_5[x, y]$. Actually, the normalized reduced Gröbner basis for *ideal*(F) in $\mathbb{Z}_5[x, y]$ is $\{xy^2 - 2y, x^2y - 2x\}$. So 5 is not "lucky" for F.

(b) Let $F = \{7xy + y + 4x, y + 2\} \subset \mathbb{Q}[x, y]$. Let the power products be ordered according to the graduated lexicographic ordering with $x < y$. The normalized reduced Gröbner basis for F in $\mathbb{Q}[x, y]$ is $G = \{x + \frac{1}{5}, y + 2\}$. 5 divides the second coefficient of the first polynomial in G, so 5 is not "lucky" for F. The normalized reduced Gröbner basis for F in $\mathbb{Z}_5[x, y]$ is $\{1\}$.

(c) Let $F = \{16x^2 + 4xy^2 - 4z + 1, 4x + 2y^2z + 1, -2x^2z + x + 2y^2\} \subset \mathbb{Q}[x, y, z]$. Let the power products be ordered according to the lexicographic ordering with $z < y < x$. The normalized reduced Gröbner basis for F in $\mathbb{Q}[x, y, z]$ has the leading power products $\{z^7, y^2, x\}$ (see Winkler *et al.*, 1985). The normalized reduced Gröbner basis for F in $\mathbb{Z}_7[x, y, z]$ has the leading power products $\{z^6, zy^2, y^4, x\}$. So 7 is not "lucky" for F.

(d) Let $F = \{x^2y + 9x^2 - y, xy + 4x^2 + 3x\} \subset \mathbb{Q}[x, y]$. Let the power products be ordered according to the graduated lexicographic ordering with $x < y$. The normalized reduced Gröbner basis for F in $\mathbb{Q}[x, y]$ is $\{xy + 4x^2 + 3x, y^2 - 16x^2 + 3y - 12x, x^3 - \frac{3}{2}x^2 + \frac{1}{4}y\}$. The normalized reduced Gröbner basis for F in $\mathbb{Z}_5[x, y]$ is $\{xy - x^2 - 2x, y^2 - x^2 - 2y - 2x, x^3 + x^2 - y\}$. So 5 is "lucky" for F.

Ebert (1983) observes that in general the number of polynomials in the normalized reduced Gröbner basis G for some $F \subset \mathbb{Q}[x_1, \ldots, x_v]$ can be greater than, equal to, or less than the number of polynomials in the normalized reduced Gröbner basis G_p for F in $\mathbb{Z}_p[x_1, \ldots, x_v]$, for some prime p. In Example 1 we see that also the leading power products of G can be greater than, equal to, less than, or incomparable to the leading power products of G_p. From Example 1(a) we also see, that it is not sufficient to just require that p not provide any coefficient of F and G. Fortunately, there are only finitely many such "unlucky" primes.

THEOREM 1. *Let $F = (F_1, \ldots, F_m)^T$ be a finite sequence of polynomials in $\mathscr{A}$, $G = (G_1, \ldots, G_m)^T$ the normalized reduced Gröbner basis for F in $\mathscr{A}$. For almost all primes p the images $\bar{F} = F \bmod p$, $\bar{G} = G \bmod p$ exist and $\bar{G}$ is the normalized reduced Gröbner basis for $\bar{F}$ in $\mathscr{A}_p$.*

PROOF. Let X, Y, R be matrices over $\mathscr{A}$ such that

$$G = X \,.\, F \quad \text{and} \quad F = Y \,.\, G,$$

and the rows of R are the elements of $S(G)$, i.e. the syzygies of G derived from reductions of the S-polynomials of G to 0 w.r.t. G.

$$R \,.\, G = 0.$$

Let p be such that it does not divide any coefficient of F, G, X, Y and R. Then $\bar{F} = F \bmod p$, $\bar{G} = G \bmod p$, $\bar{X} = X \bmod p$, $\bar{Y} = Y \bmod p$ exist and

$$\bar{G} \equiv \bar{X} \,.\, \bar{F}, \qquad \bar{F} \equiv \bar{Y} \,.\, \bar{G} \pmod{p}.$$

So $\bar{G}$ and $\bar{F}$ generate the same ideal in $\mathscr{A}_p$.

Furthermore, $\bar{R} = R \bmod p$ exists.

$$\bar{R} \,.\, \bar{G} \equiv 0 \pmod{p}$$

and the rows of the matrix $\bar{R}$ correspond to reductions of the S-polynomials of $\bar{G}$ to 0 w.r.t. $\bar{G}$ in $\mathscr{A}_p$. So $\bar{G}$ is the normalized reduced Gröbner basis for $\bar{F}$ in $\mathscr{A}_p$.

For a given F there are only a finite number of primes that divide some coefficient of F, G, X, Y or R. □

After Example 1(a) we have remarked that it is not sufficient to require that the prime p not divide any coefficient of F and G. In this case the transformation matrix X is

$$\begin{pmatrix} \frac{1}{15}x^2 & \frac{1}{3}-\frac{1}{15}xy \\ -\frac{1}{2}-\frac{1}{10}xy & \frac{1}{10}y^2 \end{pmatrix}.$$

X has no representation in $\mathscr{A}_5$.

Definition 1. Let F be a finite sequence of polynomials in $\mathscr{A}$, G the normalized reduced Gröbner basis for F. Let p be a rational prime. p is *lucky* for F iff there are transformation matrices X, Y and a syzygy matrix R for F and G such that p does not divide any coefficient in F, G, X, Y and R. □

2. The Lifting of a Gröbner Basis

From now on we assume that p is a rational prime. Let F be a finite sequence of polynomials in $\mathscr{A}$. Let $G^{(0)}$ be a Gröbner basis for F in $\mathscr{A}_p$, and $X^{(0)}$, $Y^{(0)}$ transformation matrices and $R^{(0)}$ a syzygy matrix for F and $G^{(0)}$ over $\mathscr{A}_p$.

$$\begin{aligned} X^{(0)} \,.\, F &\equiv G^{(0)} \\ Y^{(0)} \,.\, G^{(0)} &\equiv F \pmod p \\ R^{(0)} \,.\, G^{(0)} &\equiv 0. \end{aligned} \tag{2.1}$$

The first two congruences in (2.1) guarantee that F and $G^{(0)}$ generate the same ideal in $\mathscr{A}_p$ and the third congruence guarantees that $G^{(0)}$ is a Gröbner basis. In fact various criteria can be used for eliminating unnecessary S-polynomials or rows of $R^{(0)}$, respectively (see Buchberger, 1979; Winkler, 1984). In addition to the usual requirement for such a criterion, namely that checking only the necessary S-polynomials for reducibility to 0 suffices to ensure the reducibility to 0 of all S-polynomials, we demand that it should work uniformly for coefficient domains $\mathbb{Z}_{p^i}$, $i \geqslant 1$. I.e. if $G^{(0)}$ is a sequence of polynomials over $\mathbb{Z}_p$ and $G^{(i)}$ a sequence of polynomials over $\mathbb{Z}_{p^i}$ such that $G^{(0)} \equiv G^{(i)} \pmod p$ and $pp(G_i^{(0)}) = pp(G_j^{(i)})$ for $1 \leqslant j \leqslant length(G^{(0)})$, then $Spol(G_k^{(0)}, G_l^{(0)})$ is necessary if and only if $Spol(G_k^{(i)}, G_l^{(i)})$ is necessary, $1 \leqslant k, l \leqslant length(G^{(0)})$. From now on we will assume such a criterion (which could, of course, be trivial in the sense that all S-polynomials are deemed necessary). For instance the criteria given in (Buchberger, 1979; Winkler, 1984) satisfy our requirements. If $R^{(0)}$ is such that it contains only rows corresponding to necessary S-polynomials of $G^{(0)}$, then it is also called a syzygy matrix of $G^{(0)}$.

Now one could try to lift the congruences (2.1) to congruences modulo p^i for large enough i. The work required in the lifting process depends, of course, on the number of congruences that have to be lifted. The matrix $X^{(0)}$ can contain very high power products, since F is not a Gröbner basis and therefore the representation of $G^{(0)}$ in terms of F is not just a reduction. This problem does not occur with $Y^{(0)}$ and $R^{(0)}$, since $G^{(0)}$ is a Gröbner basis. The following theorem shows that actually we don't really have to consider the equivalence $X^{(0)} . F \equiv G^{(0)} \pmod{p}$.

THEOREM 2. *Let G and G' be Gröbner bases in $K[x_1, \ldots, x_v]$, $lpp(G) = lpp(G')$ and $G \subseteq ideal(G')$. Then $ideal(G) = ideal(G')$.*

PROOF. Every nonzero polynomial $f \in ideal(G')$ is reducible w.r.t. G' and, since $lpp(G') = lpp(G)$, it is also reducible w.r.t. G and the reduction result is again in $ideal(G')$. Since the reduction w.r.t. G is Noetherian, we get that every nonzero $f \in ideal(G')$ can be reduced to 0 w.r.t. G. Therefore, $ideal(G') \subseteq ideal(G)$. □

Suppose that the prime p is lucky for F in $\mathscr{A}$. So the normalized reduced Gröbner basis G for F contains the same leading power products as the normalized reduced Gröbner basis $G^{(0)}$ for F in $\mathscr{A}_p$. Then in the lifting process it suffices to lift the congruences $Y^{(0)} . G^{(0)} \equiv F$ and $R^{(0)} . G^{(0)} \equiv 0$. By Theorem 2, if one finally gets a Gröbner basis G' in $\mathscr{A}$, then G' will automatically be a Gröbner basis for F. This provided that in the lifting process the leading power products of the approximations to the basis G' remain unchanged. So (2.1) is reduced to

$$\begin{array}{l} Y^{(0)} . G^{(0)} \equiv F \\ R^{(0)} . G^{(0)} \equiv 0 \end{array} \pmod{p}. \tag{2.2}$$

The following technicality will be used in subsequent proofs.

LEMMA 1. *Let $\mathscr{A}'$ be the set of polynomials in $\mathscr{A}$ no coefficient of which has a denominator divisible by p. Let I be an ideal in $\mathscr{A}$, $I' = I \cap \mathscr{A}'$ and I_p the set of polynomials f in $\mathscr{A}_p$ such that $f \equiv g \pmod{p}$ for some $g \in I'$. (I_p is an ideal in $\mathscr{A}_p$.) Let $h \in I'$, $h' \in \mathscr{A}_p$ be such that $p^{i-1} . h' \equiv h \pmod{p^i}$. Then $h' \in I_p$.*

PROOF. h is a multiple of p^{i-1}, so for some $g \in \mathscr{A}'$ we have $h = p^{i-1} . g$ and $h' = g \bmod p$. Since $h \in I'$, also $g \in I'$, so $h' \in I_p$. □

DEFINITION 2. Let $F \in \mathscr{A}^m$, p lucky for F, $G^{(0)}$ the normalized reduced Gröbner basis for F in $\mathscr{A}_p$, $R^{(0)}$ a syzygy matrix for $G^{(0)}$ over $\mathscr{A}_p$; specifically, let the jth row of $R^{(0)}$ be the syzygy of $G^{(0)}$ derived from the reduction of $Spol(G^{(0)}_{l(j)}, G^{(0)}_{r(j)})$ to 0 w.r.t. $G^{(0)}$. Let t be a positive integer or ∞, and for $0 \leqslant i < t$ let $G^{(i)}$, $Y^{(i)}$, $R^{(i)}$ be matrices over $\mathscr{A}_{p^{i+1}}$ such that

$$\begin{array}{l} Y^{(i)} . G^{(i)} \equiv F \\ R^{(i)} . G^{(i)} \equiv 0 \end{array} \pmod{p^{i+1}},$$

$$G^{(i)} \equiv G^{(i-1)}, \quad Y^{(i)} \equiv Y^{(i-1)}, \quad R^{(i)} \equiv R^{(i-1)} \pmod{p^i} \quad \text{if } i \geqslant 1,$$

every element of $G^{(i)}$ is monic, and $pp(G^{(i)}_k) = pp(G^{(i-1)}_k)$ for $0 < i < t$, $1 \leqslant k \leqslant n$. Then $L = ((G^{(i)}, Y^{(i)}, R^{(i)}))_{0 \leqslant i < t}$ is a *lifting sequence for F* modulo p.

For $0 \leqslant j < t$ the lifting sequence L is called *reducing up to j* iff for all $0 \leqslant i \leqslant j$ the rows of $R^{(i)}$ are the syzygies of $G^{(i)}$ corresponding to reductions of the necessary S-polynomials of $G^{(i)}$ to 0 in $\mathscr{A}_{p^{i+1}}$; specifically, the jth row of $R^{(i)}$ is the syzygy of $G^{(i)}$ corresponding to the reduction of $Spol(G^{(i)}_{l(j)}, G^{(i)}_{r(j)})$ to 0 w.r.t. $G^{(i)}$. □

THEOREM 3. (existence of a lifting sequence): *Let m, n, l be natural numbers, $F \in \mathscr{A}^m$, p a lucky prime for F, $G \in \mathscr{A}^n$ the normalized reduced Gröbner basis for F, and $G^{(0)} \in \mathscr{A}_p^n$ the normalized reduced Gröbner basis for F in $\mathscr{A}_p$. If*

$$\begin{matrix} Y^{(0)} \,.\, G^{(0)} \equiv F \\ R^{(0)} \,.\, G^{(0)} \equiv 0 \end{matrix} \quad (\operatorname{mod} p)$$

holds for some (m, n)-matrix $Y^{(0)}$ over $\mathscr{A}_p$, and some (l, n)-matrix $R^{(0)}$ over $\mathscr{A}_p$, then for every $i \in \mathbb{N}$ there exist $G^{(i-1)}$, $Y^{(i-1)}$, $R^{(i-1)}$ over $\mathscr{A}_{p^i}$ such that

$$\begin{matrix} Y^{(i-1)} \,.\, G^{(i-1)} \equiv F \\ R^{(i-1)} \,.\, G^{(i-1)} \equiv 0 \end{matrix} \quad (\operatorname{mod} p^i) \tag{2.3}$$

and

$$Y^{(i-1)} \equiv Y^{(i-2)}, \qquad R^{(i-1)} \equiv R^{(i-2)} \quad (\operatorname{mod} p^{i-1}), \quad \textit{if } i > 1 \tag{2.4}$$

and

$$G^{(i-1)} = G \bmod p^i. \tag{2.5}$$

The increments

$$\frac{1}{p^{i-1}}(G^{(i-1)} - G^{(i-2)}), \qquad \frac{1}{p^{i-1}}(Y^{(i-1)} - Y^{(i-2)}), \qquad \frac{1}{p^{i-1}}(R^{i-1)} - R^{(i-2)})$$

can be chosen as a solution of a system of linear equations in $\mathscr{A}_p$, the polynomials in $G^{(i)}$ are monic, and $pp(G_k^{(i-1)}) = pp(G_k^{(i-2)})$ for $1 \leqslant k \leqslant n$.

PROOF. By induction on i. For $i = 1$ the statements (2.3) and (2.5) obviously hold. (2.4) is void. Now let $i > 1$. By the induction hypothesis there exist $G^{(i-2)}$, $Y^{(i-2)}$, $R^{(i-2)}$ over $\mathscr{A}_{p^{i-1}}$ such that (2.3), (2.4) and (2.5) hold for $i - 1$. Let $G' \in A_p^n$, $G^{(i-1)}) \in \mathscr{A}_{p^i}^n$ be such that

$$G^{(i-1)} = G^{(i-2)} + p^{i-1} \,.\, G' = G \bmod p^i.$$

So (2.5) obviously holds. We need to construct matrices Y', R' over $\mathscr{A}_p$ such that for

$$Y^{(i-1)} = Y^{(i-2)} + p^{i-1} \,.\, Y',$$
$$R^{(i-1)} = R^{(i-2)} + p^{i-1} \,.\, R'$$

the congruence (2.3) hold (the definition of $Y^{(i-1)}$ and $R^{(i-1)}$ directly implies that (2.4) holds). So we have to solve

$$\begin{aligned} F &\equiv Y^{(i-1)} \,.\, G^{(i-1)} \\ &\equiv Y^{(i-2)} \,.\, G^{(i-2)} + p^{i-1} \,.\, Y' \,.\, G^{(i-2)} + p^{i-1} \,.\, Y^{(i-2)} \,.\, G' \quad (\operatorname{mod} p^i). \end{aligned} \tag{2.6}$$

Rewriting (2.6) as

$$F - Y^{(i-2)} \,.\, G^{(i-2)} - p^{i-1} \,.\, Y^{(0)} \,.\, G' \equiv p^{i-1} \,.\, Y' \,.\, G^{(0)} \quad (\operatorname{mod} p^i), \tag{2.7}$$

we see that the image modulo p^i of the left hand side of (2.7) is a vector.

$$\begin{pmatrix} h_1^{(i-1)} \\ \vdots \\ h_m^{(i-1)} \end{pmatrix}$$

where each component $h_k^{(i-1)}$ is the image modulo p^i of a polynomial h_k in *ideal*(F) = *ideal*(G), no coefficient of which has a denominator divisible by p. Because of (2.3) for $i-1$, the left hand side of (2.7) is divisible by p^{i-1}. So we have to solve

$$\frac{1}{p^{i-1}} \cdot \begin{pmatrix} h_1^{(i-1)} \\ \vdots \\ h_m^{(i-1)} \end{pmatrix} \equiv Y' \,.\, G^{(0)} \pmod{p}.$$

For every k, $1 \leqslant k \leqslant m$, $h_k \in$ *ideal*(G), so by Lemma 1 $h_k^{(i-1)}/p^{i-1} \in$ *ideal*$(G^{(0)})$ and therefore we can take the elements of Y' as the multiplicands used in the reductions of $h_1^{(i-1)}/p^{i-1}, \ldots, h_m^{(i-1)}/p^{i-1}$ to 0 w.r.t. $G^{(0)}$.

We still have to find a matrix R' such that

$$(R^{(i-2)} + p^{i-1} \,.\, R') \,.\, (G^{(i-2)} + p^{i-1} \,.\, G') \equiv 0 \pmod{p^i}.$$

So we have to solve

$$R^{(i-2)} \,.\, G^{(i-2)} + p^{i-1} \,.\, R^{(i-2)} \,.\, G' \equiv -p^{i-1} \,.\, R' \,.\, G^{(i-2)} \pmod{p^i}. \tag{2.8}$$

The image modulo p^i of the left hand side of (2.8) is a vector of images of polynomials in *ideal*(G) = *ideal*(F). Because of (2.3) for $i-1$, the left hand side of (2.8) is divisible by p^{i-1}. So we have to solve

$$\frac{1}{p^{i-1}} \cdot (R^{(i-2)} \,.\, G^{(i-2)} + p^{i-1} \,.\, R^{(i-2)} \,.\, G') \equiv -R' \,.\, G^{(0)} \pmod{p}.$$

All the images modulo p of the polynomials on the left hand side are in *ideal*$(G^{(0)})$ (by Lemma 1), so the reduction to 0 modulo $G^{(0)}$ yields the matrix R'.

Observe that $G' = (G'_1, \ldots, G'_n)^T$, $Y' = (Y'_{ij})_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n}$ and $R' = (R'_{ij})_{1 \leqslant i \leqslant l, 1 \leqslant j \leqslant n}$ are a solution to the system of linear equations

$$G^{(0)} \,.\, Y' + Y^{(0)} \,.\, G' \equiv \frac{1}{p^{i-1}} \cdot (F - Y^{(i-2)} \,.\, G^{(i-2)}) \pmod{p}$$

$$G^{(0)} \,.\, R' + R^{(0)} \,.\, G' \equiv \frac{1}{p^{i-1}} \cdot (-R^{(i-2)} \,.\, G^{(i-2)}) \pmod{p},$$

the polynomials in $G^{(i)}$ are monic, and $pp(G'_k) \subseteq pp(G_k^{(i-2)})$ for $1 \leqslant k \leqslant n$. □

From Theorem 3 we know that for every lucky prime p for F a lifting sequence for F modulo p exists. The next theorem deals with the uniqueness of such a lifting sequence. It turns out that the components $G^{(i)}$ are indeed uniquely determined, whereas the components $Y^{(i)}$, $R^{(i)}$ are usually not. Starting from the normalized reduced Gröbner basis $G^{(0)}$ modulo p, after i lifting steps we get $G^{(i)}$, a sequence of polynomials in $\mathscr{A}_{p^{i+1}}$. $\mathbb{Z}_{p^{i+1}}$ is not a field, and since we have not introduced the notion of a Gröbner basis over a ring, we have to prove (a), (b), (c) in Theorem 4.

THEOREM 4 (uniqueness of lifting sequences): *Let $m, n \in \mathbb{N}$, $F \in \mathscr{A}^m$, $G \in \mathscr{A}^n$ the normalized reduced Gröbner basis for F, p lucky for F, and $i \geqslant 0$. Let $L = ((G^{(j)}, Y^{(j)}, R^{(j)}))_{0 \leqslant j < i+1}$ be a lifting sequence for F modulo p. Then*

(*a*) *all the S-polynomials of $G^{(i)}$ can be reduced to 0 w.r.t. $G^{(i)}$,*
(*b*) *every polynomial h in ideal$(G^{(i)})$ ($\subseteq \mathscr{A}_{p^{i+1}}$) is reducible w.r.t. $G^{(i)}$,*

(*c*) *ideal*$(F) =$ *ideal*$(G^{(i)})$ *as ideals in* $\mathscr{A}_{p^{i+1}}$,
(*d*) $G^{(i)} = G \bmod p^{i+1}$.

PROOF. (a) Since $G^{(0)}$ is a Gröbner basis, we know that all the S-polynomials of $G^{(0)}$ can be reduced to 0 w.r.t. $G^{(0)}$, and actually the rows of $R^{(0)}$ are just the syzygies derived from the reductions of the necessary S-polynomials of $G^{(0)}$.

If L is reducing up to i, then obviously the S-polynomials of $G^{(i)}$ are reducible to 0 w.r.t. $G^{(i)}$.

Otherwise let j, $1 \leqslant j \leqslant i$, be the smallest index such that the rows of $R^{(j)}$ do not correspond to the syzygies derived from reductions of the necessary S-polynomials of $G^{(j)}$ to 0 w.r.t. $G^{(j)}$. Let R' be the matrix over $\mathscr{A}_p$ such that

$$R^{(j)} = R^{(j-1)} + p^j \,.\, R'.$$

The elements of $R^{(j-1)}$ can be considered as the multiplicands used in an "incomplete" reduction of the necessary S-polynomials of $G^{(j)}$ w.r.t. $G^{(j)}$. A step in this incomplete reduction consists of partially reducing an occurring term, possibly leaving a coefficient which is a multiple of p^j. The result of this incomplete reduction is a vector of the form

$$p^j \,.\, h = p^j \,.\begin{pmatrix} h_1 \\ \vdots \\ h_l \end{pmatrix}$$

for some $h_1, \ldots, h_l \in \mathscr{A}_p$. Because of $R^{(j)} \,.\, G^{(j)} \equiv 0 \pmod{p^{j+1}}$ we have

$$p^j \,.\, h \equiv -p^j \,.\, R' \,.\, G^{(0)} \pmod{p^{j+1}},$$

or equivalently,

$$h \equiv -R' \,.\, G^{(0)} \pmod{p}.$$

Obviously $h_k \in$ *ideal*$(G^{(0)})$ for $1 \leqslant k \leqslant l$, so h_k can be reduced to 0 w.r.t. $G^{(0)}$. Actually, whenever a term has to be reduced which is also reduced in the incomplete reduction above, then corresponding basis polynomials can be used in corresponding reduction steps. Let the elements of the matrix $\bar{R}'$ be the multiplicands used in this reduction of h to 0, so that $h \equiv -\bar{R}' \,.\, G^{(0)} \pmod{p}$. For the matrix

$$S^{(j)} := R' - \bar{R}'$$

we have

$$S^{(j)} \,.\, G^{(0)} \equiv 0 \pmod{p}.$$

If we now let

$$\bar{R}^{(j)} := R^{(j)} - p^j \,.\, S^{(j)},$$

then the rows of $\bar{R}^{(j)}$ correspond to the syzygies derived from reductions of the necessary S-polynomials of $G^{(j)}$ to 0 w.r.t. $G^{(j)}$.

In the sequel we construct matrices $\bar{R}^{(j+1)}, \ldots, \bar{R}^{(i)}$ such that

$$\bar{L} = ((G^{(0)}, Y^{(0)}, R^{(0)}), \ldots, (G^{(j-1)}, Y^{(j-1)}, R^{(j-1)}),$$
$$(G^{(j)}, Y^{(j)}, \bar{R}^{(j)}), \ldots, (G^{(i)}, Y^{(i)}, \bar{R}^{(i)}))$$

is a lifting sequence for F modulo p. Actually we prove the following: for every k with

$j \leqslant k \leqslant i$ there exists a matrix $S^{(k)}$ over $\mathscr{A}_p$ such that for

$$\bar{R}^{(k)} := R^{(k)} - \sum_{r=j}^{k} p^r \,.\, S^{(r)},$$
$$\bar{R}^{(j-1)} := R^{(j-1)}$$

we have

$$\left\{ \begin{array}{c} \bar{R}^{(k)} \,.\, G^{(k)} \equiv 0 \pmod{p^{k+1}}, \\ \bar{R}^{(k)} \equiv \bar{R}^{(k-1)} \pmod{p^k}, \qquad \text{and} \\ \left(\sum_{r=j}^{k} p^r \,.\, S^{(r)} \right) . \, G^{(k-j)} \equiv 0 \quad (\bmod\, p^{k+1} \end{array} \right\} . \tag{2.9}$$

Induction on k.
For $k = j$, we have

$$\bar{R}^{(j)} \,.\, G^{(j)} = R^{(j)} \,.\, G^{(j)} - p^j \,.\, S^{(j)} \,.\, G^{(j)} \equiv 0 \pmod{p^{j+1}},$$
$$\bar{R}^{(j)} = R^{(j)} - p^j \,.\, S^{(j)} \equiv R^{(j-1)} = \bar{R}^{(j-1)} \pmod{p^j},$$
$$p^j \,.\, S^{(j)} \,.\, G^{(0)} \equiv 0 \pmod{p^{j+1}}.$$

Now consider k such that $j < k \leqslant i$. Let the matrix R over $\mathscr{A}_p$ be such that

$$R^{(k)} = R^{(k-1)} + p^k \,.\, R.$$

By the induction hypothesis we have

$$(\bar{R}^{(k-1)} + p^k \,.\, R) \,.\, G^{(k)} \equiv (R^{(k-1)} + p^k \,.\, R) \,.\, G^{(k)} - \left(\sum_{r=j}^{k-1} p^r \,.\, S^{(r)} \right) . \, G^{(k)} \equiv 0 \pmod{p^k}.$$

So

$$-\left(\sum_{r=j}^{k-1} p^r \,.\, S^{(r)} \right) . \, G^{(k-j)} \equiv p^k \,.\begin{pmatrix} g_1 \\ \vdots \\ g_l \end{pmatrix} =: p^k \,.\, g \pmod{p^{k+1}}$$

for some $g_1, \ldots, g_l \in \mathscr{A}_p$. Observe that $k - j < i$. So by the assumption of the theorem and Lemma 1, every g_t, $1 \leqslant t \leqslant l$, is the homomorphic image of a polynomial in *ideal*(G) modulo p, so it can be reduced to 0 w.r.t. $G^{(0)}$. Collecting the multiplicands used in these reductions in the matrix $S^{(k)}$, we get

$$g \equiv S^{(k)} \,.\, G^{(0)} \pmod{p}.$$

For this definition of $S^{(k)}$ the condition (2.9) holds.

$$\bar{R}^{(k)} \,.\, G^{(k)} \equiv \left(R^{(k)} - \sum_{r=j}^{k} p^r \,.\, S^{(r)} \right) . \, G^{(k)} \equiv R^{(k)} \,.\, G^{(k)} - \left(\sum_{r=j}^{k-1} p^r \,.\, S^{(r)} \right) . \, G^{(k)} - p^k \,.\, S^{(k)} \,.\, G^{(k)}$$
$$\equiv R^{(k)} \,.\, G^{(k)} + p^k \,.\, g - p^k \,.\, g \equiv 0 \pmod{p^{k+1}},$$
$$\bar{R}^{(k)} = R^{(k)} - \sum_{r=j}^{k} p^r \,.\, S^{(r)} \equiv R^{(k-1)} - \sum_{r=j}^{k-1} p^r \,.\, S^{(r)} = \bar{R}^{(k-1)} \pmod{p^k},$$
$$\left(\sum_{r=j}^{k} p^r \,.\, S^{(r)} \right) . \, G^{(k-j)} = \left(\sum_{r=j}^{k-1} p^r \,.\, S^{(r)} \right) . \, G^{(k-j)} + p^k \,.\, S^{(k)} \,.\, G^{(k-j)}$$
$$\equiv -p^k \,.\, g + p^k \,.\, g = 0 \pmod{p^{k+1}}.$$

So we have constructed a lifting sequence $\bar{L}$ which is reducing up to j. Repeating this process, we finally get a lifting sequence which is reducing up to i. Thus, all the necessary S-polynomials of $G^{(i)}$ are reducible to 0 w.r.t. $G^{(i)}$, and therefore all S-polynomials are reducible to 0 w.r.t. $G^{(i)}$. This completes the proof of (a).

(b) A polynomial h in $ideal(G^{(i)})$ can be written as

$$h \equiv \sum_{k=1}^{n} h_k \, . \, G_k^{(i)} \pmod{p^{i+1}}, \tag{2.10}$$

for some $h_k \in \mathcal{A}_{p^{i+1}}$. Let u be the highest power product w.r.t. $\lhd$ occurring in some summand on the right hand side of (2.10). If $lpp(h) \lhd u$, then the coefficients of u on the right hand side of (2.10) cancel. Subtracting proper multiples of syzygies of $G^{(i)}$, derived from reducing S-polynomials of $G^{(i)}$ to 0, we can decrease u by a process analogous to that described in (Winkler, 1986), proof of Theorem 5. So, finally, the leading power products on both sides of (2.10) will be the same, and therefore h is reducible w.r.t. $G^{(i)}$.

(c) Since p is lucky, $\bar{G}^{(i)} = G \bmod p^{i+1}$ exists and $ideal(\bar{G}^{(i)}) = ideal(F)$ as ideals in $\mathcal{A}_{p^{i+1}}$. Certainly $ideal(F) \subseteq ideal(G^{(i)})$, since $Y^{(i)} \, . \, G^{(i)} \equiv F \pmod{p^{i+1}}$. Assume that $ideal(G^{(i)}) \nsubseteq ideal(F)$. Let h be a polynomial in $ideal(G^{(i)}) \backslash ideal(F)$. By (b), h is reducible w.r.t. $G^{(i)}$. But every polynomial which is reducible w.r.t. $G^{(i)}$ is also reducible w.r.t. $\bar{G}^{(i)}$, since the leading power products in both bases are the same and the basis elements are monic. Say $h \rightarrow_{\bar{G}^{(i)}} g$. Then $g \in ideal(G^{(i)})$, since $ideal(\bar{G}^{(i)}) = ideal(F) \subseteq ideal(G^{(i)})$. But $g \notin ideal(F)$, for otherwise $h \in ideal(F)$. So $g \in ideal(G^{(i)}) \backslash ideal(F)$, and by the same reasoning as for h we get that g can be reduced w.r.t. $\bar{G}^{(i)}$. That process can be repeated indefinitely, leading to an infinite chain of reductions. This, however, is impossible.

(d) Assume that there exists a k, $1 \leqslant k \leqslant n$, such that $G_k^{(i)} \neq \bar{G}_k^{(i)}$. $\bar{G}_k^{(i)}$ can be reduced by $G_k^{(i)}$ to some nonzero polynomial h in $\mathcal{A}_{p^{i+1}}$, and h is irreducible w.r.t. $G^{(i)}$ (because the same power products occur in $G_k^{(i)}$ and $\bar{G}_k^{(i)}$ and $G^{(i)}$ is reduced). So, by (b), $h \notin ideal(G^{(i)})$, and therefore $ideal(G^{(i)}) \neq ideal(\bar{G}^{(i)}) = ideal(F)$ in $\mathcal{A}_{p^{i+1}}$. This, however, is a contradiction to (c). □

If p is a lucky prime for F, then by Theorem 3 the congruence (2.2) can be extended to a lifting sequence of arbitrary length and by Theorem 4 such a lifting sequence guarantees that we get the correct approximation of the normalized reduced Gröbner basis G for F. In order to compute $(G^{(i)}, Y^{(i)}, R^{(i)})$ from $(G^{(i-1)}, Y^{(i-1)}, R^{(i-1)})$ we have to solve the system

$$U \, . \, c = v^{(i)} \tag{2.11}$$

over $\mathcal{A}_p$, where

$$v^{(i)} = \frac{1}{p^i} \cdot \begin{pmatrix} F - Y^{(i-1)} \, . \, G^{(i-1)} \\ \cdots\cdots\cdots\cdots \\ -R^{(i-1)} \, . \, G^{(i-1)} \end{pmatrix}$$

and U is the matrix

$$\begin{array}{cc}
 & \begin{array}{ccc} \text{column } n \, . \, m & \qquad\qquad & \text{column } n \, . \, (m+1) \\ \downarrow & & \downarrow \end{array} \\
\begin{array}{c} \\ \\ \text{row } m \\ \\ \\ \\ \text{row } m+l \end{array} &
\left(\begin{array}{ccccc|ccccc|c}
G_1^{(0)} & \dots & G_n^{(0)} & & & & & & & & \\
 & 0 & \ddots & 0 & & & & 0 & & & Y^{(0)} \\
 & & G_1^{(0)} & \dots & G_n^{(0)} & & & & & & \\
\hline
 & & & & & G_1^{(0)} & \dots & G_n^{(0)} & & & \\
 & & 0 & & & & 0 & \ddots & 0 & & R^{(0)} \\
 & & & & & & & G_1^{(0)} & \dots & G_n^{(0)} &
\end{array}\right)
\end{array}$$

If

$$(y'_{11}, \ldots, y'_{1n}, \ldots, y'_{m1}, \ldots, y'_{mn}, r'_{11}, \ldots, r'_{1n}, \ldots, r'_{l1}, \ldots, r'_{ln}, g'_1, \ldots, g'_n)^T$$

is a solution such that $pp(g'_j) \subseteq pp(G_j^{(0)}) \setminus \{lpp(G_j^{(0)})\}$ for $1 \leqslant j \leqslant n$, then

$$G^{(i)} = G^{(i-1)} + p^i \cdot \begin{pmatrix} g'_1 \\ \vdots \\ g'_n \end{pmatrix},$$

$$Y^{(i)} = Y^{(i-1)} + p^i \cdot \begin{pmatrix} y'_{11} & \cdots & y'_{1n} \\ \vdots & & \vdots \\ y'_{m1} & \cdots & y'_{mn} \end{pmatrix},$$

$$R^{(i)} = R^{(i-1)} + p^i \cdot \begin{pmatrix} r'_{11} & \cdots & r'_{1n} \\ \vdots & & \vdots \\ r'_{l1} & \cdots & r'_{ln} \end{pmatrix}.$$

For the computation of a basis

$$C' = \left\{ \begin{pmatrix} \vdots \\ g'^{(1)}_1 \\ \vdots \\ g'^{(1)}_n \end{pmatrix}, \ldots, \begin{pmatrix} \vdots \\ g'^{(q)}_1 \\ \vdots \\ g'^{(q)}_n \end{pmatrix} \right\}$$

for the module of solutions of the homogeneous system

$$U \,.\, c = 0 \tag{2.12}$$

and a solution to the inhomogeneous system (2.11) we refer to (Möller & Mora, 1986; Furukawa *et al.*, 1986; Winkler, 1986). Observe that for every $1 \leqslant j, k \leqslant n$ there exists a solution $c' = (\ldots, c'_{n(m+l)+1}, \ldots, c'_{n(m+l)+n})^T$ of (2.12) such that $c'_{n(m+l)+j} = G_k^{(0)}$ and $c'_{n(m+1)+t} = 0$ for $1 \leqslant t \leqslant n, t \neq j$.

The only remaining complication is that during the lifting process no new power products are allowed to be introduced in the basis and the basis polynomials should stay monic. In order to satisfy this requirement, the basis C' of the solution module of the homogeneous system is transformed to a basis

$$C = \left\{ \begin{pmatrix} \vdots \\ g^{(1)}_1 \\ \vdots \\ g^{(1)}_n \end{pmatrix}, \ldots, \begin{pmatrix} \vdots \\ g^{(r)}_1 \\ \vdots \\ g^{(r)}_n \end{pmatrix} \right\}$$

in which the last n components constitute a Gröbner basis for the module generated by these components (see Möller & Mora, 1986; Winkler, 1987b).

LEMMA 2. *Let $i \in \mathbb{N}$, $G^{(0)} = (G_1^{(0)}, \ldots, G_n^{(0)})^T$ the normalized reduced Gröbner basis for $F = (F_1, \ldots, F_m)^T$ in $\mathscr{A}_p$, p lucky for F. Let C be a basis for the module of solutions of* (2.12) *such that the last n components of the vectors in C constitute a Gröbner basis for the module generated by these components. Let $L = ((G^{(j)}, Y^{(j)}, R^{(j)}))_{0 \leqslant j < i}$ be a lifting sequence for F modulo p.*

(*a*) *There exists a vector* $g' = (g'_1, \ldots, g'_n)^T$ *over* $\mathscr{A}_p$ *such that the last* n *components of every solution*

$$\bar{c} = (\bar{c}_1, \ldots, \bar{c}_{n(m+l)}, \bar{c}_{n(m+l)+1}, \ldots, \bar{c}_{n(m+l)+n})^T$$

of (2.11) satisfying the additional requirement

$$pp(\bar{c}_{n(m+l)+k}) \subseteq pp(G_k^{(0)}) \setminus \{lpp(G_k^{(0)})\} \quad \text{for } 1 \leqslant k \leqslant n \tag{2.13}$$

are equal to g'.

(*b*) *From an arbitrary solution* $\bar{\bar{c}}$ *of* (2.11) *a solution* $\bar{c}$ *of* (2.11) *which satisfies the additional requirement* (2.13) *can be computed.*

Proof: (a) By Theorems 3 and 4.

(b) Let $\bar{\bar{c}} = (\ldots, h_1, \ldots, h_n)^T$. Then $h - g' = (h_1 - g'_1, \ldots, h_n - g'_n)^T$ are the last n components of a solution of (2.12). So they can be reduced to 0 w.r.t. the last n components of

$$C = \{ \underbrace{\begin{pmatrix} \vdots \\ g_1^{(1)} \\ \vdots \\ g_n^{(1)} \end{pmatrix}}_{C_1}, \ldots, \underbrace{\begin{pmatrix} \vdots \\ g_1^{(r)} \\ \vdots \\ g_n^{(r)} \end{pmatrix}}_{C_r} \}.$$

If we let the possible coefficients in g' be parameters and reduce $h - g'$ w.r.t. the last n components of C, we get linear equations for these parameters that have a unique solution (by (a)), and we get a representation of $h - g'$ as a linear combination of the vectors consisting of the last n components of C,

$$g' = h + \sum_{j=1}^{r} a_j \cdot \begin{pmatrix} g_1^{(j)} \\ \vdots \\ g_n^{(j)} \end{pmatrix}.$$

Then

$$\bar{c} = \bar{\bar{c}} + \sum_{j=1}^{r} a_j \cdot C_j$$

is a solution of (2.11) which satisfies (2.13). □

The left hand side U of (2.11) remains the same throughout the lifting process. The right hand side varies and it can be efficiently computed as

$$v^{(i+1)} = \frac{1}{p} \cdot \left(v^{(i)} - \begin{pmatrix} Y'G^{(i-1)} + Y^{(i-1)}G' + p^i Y'G' \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ R'G^{(i-1)} + R^{(i-1)}G' + p^i R'G' \end{pmatrix} \right),$$

where G', Y', R' are the matrices over $\mathscr{A}_p$ such that $G^{(i)} = G^{(i-1)} + p^i G'$, $Y^{(i)} = Y^{(i-1)} + p^i Y'$, $R^{(i)} = R^{(i-1)} + p^i R'$.

3. The Lifting Algorithm

Suppose we knew how to determine a reasonable bound B for the coefficients of the normalized reduced Gröbner basis G for a given F and how to select a lucky prime p.

Then the following algorithm could be used to compute G by lifting the corresponding Gröbner basis modulo p just high enough so that every coefficient in G has a unique representation. If such a bound B is not known, then the algorithm *lift* can be considered as p-adically approximating G.

Algorithm *lift* (**in:** $F = (F_1, \ldots, F_m)^T$ in $\mathscr{A}^m$,
p, a lucky prime for F,
B, a bound on the coefficients in the normalized reduced Gröbner basis G for F, i.e. every coefficient of G is in $\mathscr{F}_{p,B}$;
out: G, the normalized reduced Gröbner basis for F);

(1) [length of lifting sequençe] Compute K such that $2B^2 + 1 \leqslant p^K$.

(2) [initialization] Set $i \leftarrow 1$. Compute the normalized reduced Gröbner basis $G^{(0)} = (G_1^{(0)}, \ldots, G_n^{(0)})^T$ for F modulo p and matrices $Y^{(0)}$, $R^{(0)}$ over $\mathscr{A}_p$ such that

$$Y^{(0)} \,.\, G^{(0)} \equiv F \quad \text{and} \quad R^{(0)} \,.\, G^{(0)} \equiv 0 \pmod{p},$$

and the rows of $R^{(0)}$ are the syzygies of $G^{(0)}$ derived from the reductions of the necessary S-polynomials of $G^{(0)}$ to 0 w.r.t. $G^{(0)}$.

(3) [solution of homogeneous system] Let the matrix U be as in (2.11). Compute a basis

$$C = \begin{pmatrix} \vdots \\ g_1^{(1)} \\ \vdots \\ g_n^{(1)} \end{pmatrix}, \ldots, \begin{pmatrix} \vdots \\ g_1^{(k)} \\ \vdots \\ g_n^{(k)} \end{pmatrix}$$

for the module of solutions of $U \,.\, c = 0$ in $\mathscr{A}_p$, such that the last n components of the basis vectors in C constitute a Gröbner basis for the module generated by these components.

(4) [finished?] If $i = K$ then go to (6).

(5) [lift to congruence modulo p^{i+1}] Compute a particular solution

$$(y'_{11}, \ldots, y'_{1n}, \ldots, y'_{m1}, \ldots, y'_{mn}, r'_{11}, \ldots, r'_{1n}, \ldots, r'_{l1}, \ldots, r'_{ln}, g'_1, \ldots, g'_n)^T$$

of

$$U \,.\, c = \frac{1}{p^i} \,.\, \begin{pmatrix} F - Y^{(i-1)} \,.\, G^{i-1)} \\ \cdots\cdots\cdots\cdots\cdots \\ -R^{(i-1)} \,.\, G^{(i-1)} \end{pmatrix}$$

over $\mathscr{A}_p$, such that $pp(g'_j) \subseteq pp(G_j^{(0)}) \setminus \{lpp(G_j^{(0)})\}$ for $1 \leqslant j \leqslant n$. Set

$$G^{(i)} \leftarrow G^{(i-1)} + p^i \,.\, (g'_1, \ldots, g'_n)^T,$$

$$Y^{(i)} \leftarrow Y^{(i-1)} + p^i \,.\, (y'_{kj})_{\substack{1 \leqslant k \leqslant m, \\ 1 \leqslant j \leqslant n}} \qquad R^{(i)} \leftarrow R^{(i-1)} + p^i \,.\, (r'_{kj})_{\substack{1 \leqslant k \leqslant i \cdot \\ 1 \leqslant j \leqslant n}}$$

Set $i := i + 1$. Go to (4).

(6) [convert the coefficients back to $\mathbb{Q}$] Compute the unique coefficients in $\mathscr{F}_{p,B}$ corresponding to the coefficients in $G^{(K)}$, getting the normalized reduced Gröbner basis G for F over $\mathbb{Q}$. □

EXAMPLE 2. We carry out the algorithm *lift* for computing a p-adic approximation of a Gröbner basis in $\mathbb{Q}[x, y]$. As the ordering $<$ of the power products we choose the lexicographic ordering with $x < y$. Let the input basis F be

$$F = \begin{pmatrix} x^2y^2 - \frac{14}{3}x^3y \\ xy^3 - \frac{12}{7}x^2y^2 + 8x \\ y^4 + 8y - 24x^3 \end{pmatrix}.$$

The normalized reduced Gröbner basis for F over $\mathbb{Q}$ is

$$G = \begin{pmatrix} x^2 \\ xy^3 + 8x \\ y^4 + 8y \end{pmatrix}.$$

So the coefficients of both F and G are relatively small, whereas the highest coefficient appearing in the computation of G is 1098247/1190896.

As the prime p we choose 5, which is indeed a lucky prime for F. The Gröbner basis for F modulo 5 is

$$G^{(0)} = \begin{pmatrix} x^2 \\ xy^3 - 2x \\ y^4 - 2y \end{pmatrix},$$

the transformation matrix from $G^{(0)}$ to F modulo 5 is $Y^{(0)}$ and the rows of $R^{(0)}$ are the syzygies derived from the necessary S-polynomials $Spol(G_1^{(0)}, G_2^{(0)})$, $Spol(G_2^{(0)}, G_3^{(0)})$ of $G^{(0)}$.

$$Y^{(0)} = \begin{pmatrix} y^2 + 2xy & 0 & 0 \\ -y^2 & 1 & 0 \\ x & 0 & 1 \end{pmatrix}, \qquad R^{(0)} = \begin{pmatrix} y^3 - 2 & -x & 0 \\ 0 & y & -x \end{pmatrix}.$$

In lifting the Gröbner basis $G^{(0)}$ modulo 5 to a basis modulo some higher power of 5 we have to solve a system of inhomogeneous linear equations. The left hand side of this system is the matrix U, whose transposed is

$$\begin{pmatrix}
x^2 & 0 & 0 & 0 & 0 \\
xy^3 - 2x & 0 & 0 & 0 & 0 \\
y^4 - 2y & 0 & 0 & 0 & 0 \\
0 & x^2 & 0 & 0 & 0 \\
0 & xy^3 - 2x & 0 & 0 & 0 \\
0 & y^4 - 2y & 0 & 0 & 0 \\
0 & 0 & x^2 & 0 & 0 \\
0 & 0 & xy^3 - 2x & 0 & 0 \\
0 & 0 & y^4 - 2y & 0 & 0 \\
0 & 0 & 0 & x^2 & 0 \\
0 & 0 & 0 & xy^3 - 2x & 0 \\
0 & 0 & 0 & y^4 - 2y & 0 \\
0 & 0 & 0 & 0 & x^2 \\
0 & 0 & 0 & 0 & xy^3 - 2x \\
0 & 0 & 0 & 0 & y^4 - 2y \\
y^2 + 2xy & -y^2 & x & y^3 - 2 & 0 \\
0 & 1 & 0 & -x & y \\
0 & 0 & 1 & 0 & -x
\end{pmatrix}$$

We compute a basis C for the module of solutions of $U \,.\, c = 0$ in $\mathbb{Z}_5[x, y]$, such that the last 3 components of the basis vectors in C constitute a Gröbner basis for the module generated by these components. C includes the vectors

$$\begin{pmatrix} \vdots \\ x^2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} \vdots \\ xy^3 - 2x \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} \vdots \\ y^4 - 2y \\ 0 \\ 0 \end{pmatrix},$$

$$\begin{pmatrix} \vdots \\ 0 \\ x^2 \\ 0 \end{pmatrix}, \begin{pmatrix} \vdots \\ 0 \\ xy^3 - 2x \\ 0 \end{pmatrix}, \begin{pmatrix} \vdots \\ 0 \\ y^4 - 2y \\ 0 \end{pmatrix},$$

$$\begin{pmatrix} \vdots \\ 0 \\ 0 \\ x^2 \end{pmatrix}, \begin{pmatrix} \vdots \\ 0 \\ 0 \\ xy^3 - 2x \end{pmatrix}, \begin{pmatrix} \vdots \\ 0 \\ 0 \\ y^4 - 2y \end{pmatrix}.$$

In the first lifting step we compute a particular solution $\bar{\bar{c}}$ to the system

$$U \,.\, c = \frac{1}{5} \cdot \begin{pmatrix} F - Y^{(0)} \,.\, G^{(0)} \\ \cdots\cdots\cdots\cdots \\ -R^{(0)} \,.\, G^{(0)} \end{pmatrix} \tag{3.1}$$

over $\mathbb{Z}_5[x, y]$. The basis vectors in C are used to reduce $\bar{\bar{c}}$ to a solution $\bar{c}$ of (3.1) satisfying the requirement that none of the last 3 components of $\bar{c}$ contains any power product that does not already appear in the corresponding element of $G^{(0)}$ and, moreover, the coefficient of $lpp(G_j^{(0)})$ in $\bar{c}_{15+j}$ is 0, for $1 \leqslant j \leqslant 3$. As the vector $\bar{c}$ we get

$$\bar{c} = \begin{pmatrix} 2xy \\ 0 \\ 0 \\ -xy^4 + 2x^2y^3 + 2y^2 + 2xy + x^2 \\ x^2y - 2x^3 \\ 0 \\ 0 \\ 0 \\ 0 \\ 2 \\ 0 \\ 0 \\ -xy^5 + 2x^2y^4 + 2xy^2 + x^2y \\ 0 \\ x^3y - 2x^4 \\ 0 \\ 2x \\ 2y \end{pmatrix}$$

Now we use the components of $\bar{c}$ to update the approximations to G, Y, and R, getting

$$G^{(1)} = \begin{pmatrix} x^2 \\ xy^3 + 8x \\ y^4 + 8y \end{pmatrix},$$

$$Y^{(1)} = \begin{pmatrix} y^2 + 12xy & 0 & 0 \\ -5xy^4 + 10x^2y^3 + 9y^2 + 10xy + 5x^2 & 5x^2y - 10x^3 + 1 & 0 \\ x & 0 & 1 \end{pmatrix},$$

$$R^{(1)} = \begin{pmatrix} y^3 + 8 & -x & 0 \\ -5xy^5 + 10x^2y^4 + 10xy^2 + 5x^2y & y & 5x^3y - 10x^2 - x \end{pmatrix}.$$

$G^{(1)}$ (with its coefficients mapped back to $\mathbb{Q}$) is already the normalized reduced Gröbner basis for F in $\mathbb{Q}[x, y]$. □

4. Conclusion

As we have shown, it is possible to give a lifting algorithm that computes a p-adic approximation to the normalized reduced Gröbner basis G for the ideal generated by a finite set of polynomials F in $\mathbb{Q}[x_1, \ldots, x_v]$. For the lifting process to be valid, we have to guarantee that the prime p is not one of finitely many unlucky primes. Unfortunately, up to now we do not have an effective criterion for determining luckyness. What we would like to have is a criterion similar to the one for the polynomial factorization problem, where we only have to check that p does not divide the leading coefficient and the resultant of the primitive squarefree polynomial f, and f remains squarefree modulo p. So determining luckyness remains an open problem.

Another open problem is the computation of a reasonable upper bound on the coefficients of the normalized reduced Gröbner basis for the ideal generated by a set of polynomials F. Such a bound is essential for the termination criterion of the algorithm *lift*.

Although we cannot yet present a totally effective procedure for the problem of lifting a Gröbner basis, we hope that this is the starting point for further investigation into the subject.

References

Brown, W. S. (1971). On Euclid's algorithm and the computation of polynomial greatest common divisors. *JACM*, **18/4**, 478–504.

Buchberger, B. (1976). Some properties of Gröbner bases for polynomial ideals. *ACM SIGSAM Bull.* **10**(4), 19–24.

Buchberger, B. (1979). A criterion for detecting unnecessary reductions in the construction of Gröbner-Bases. *Proc. EUROSAM 79*, Marseille, 1979, LNCS **72**, 3–21. E. W. Ng, ed., Springer-Verlag, Heidelberg.

Buchberger, B. (1985). Gröbner bases: An algorithmic method in polynomial ideal theory. In (Bose, N. K., ed.) *Multidimensional Systems Theory*. D. Reidel Publ. Comp. pp. 184–232.

Ebert, G. L. (1983). Some comments on the modular approach to Gröbner-bases. *ACM SIGSAM Bull.* **17**(2), 28–32.

Furukawa, A., Sasaki, T., Kobayashi, H. (1986). Gröbner basis of a module over $K[x_1, \ldots, x_n]$ and polynomial solutions of a system of linear equations. In (Char, B. W., ed.) *Proc. SYMSAC'86*. ACM 1986. pp. 222–224.

Galligo, A. (1979). Théorème de division et stabilité en géométrie analytique locale. *Ann. Inst. Fourier*, **29**, 107–184.

Hilbert, D. (1890). Über die Theorie der algebraischen Formen. *Math. Annalen*. **36,** 473–534.

Kornerup, P., Gregory, R. T. (1983). Mapping integers and Hensel codes onto Farey fractions. *BIT* **23,** 9–20.

Lauer, M. (1983). Computing by homomorphic images. In (Buchberger. B. *et al.*, eds.) *Computer Algebra — Symbolic and Algebraic Computation*. 2nd edition. Springer-Verlag, Heidelberg.

Malle, G., Trinks, W. (1984). *Zur Behandlung algebraischer Gleichungssysteme mit dem Computer*. Mathematisches Institut, Universität Karlsruhe, unpublished manuscript.

Matzat B. H., Zeh-Marschke, A. (1986). Realisierung der Mathieugruppen M_{11} und M_{12} als Galoisgruppen über Q. *J. Number Theory* **23,** 195–202.

Miola, A., Yun, D. Y. Y. (1974). The computational aspects of Hensel-type univariate greatest common divisor algorithms. In (Jenks, R. D., ed.) *Proc. EUROSAM'74. SIGSAM Bulletin* **8/3**, 46–54.

Möller, H. M., Mora, F. (1986). New constructive methods in classical ideal theory. *J. of Algebra*, **100,** 138–178.

Moses, J., Yun, D. Y. Y. (1973). The EZGCD algorithm. *Proc. ACM Annual Conference*, Atlanta, pp. 159–166.

Musser, D. R. (1975). Multivariate polynomial factorization. *JACM* **22,** 291–308.

Trinks, W. (1984). On improving approximate results of Buchberger's algorithm by Newton's method. *SIGSAM Bull.* **18**(3), 7–11.

van der Waerden, B. L. (1967). *Algebra II*. Springer-Verlag, Heidelberg.

Wang, P. S. H. (1978). An improved multivariate polynomial factorization algorithm. *Math. Comp.* **32,** 1215–1231.

Wang, P. S. H., Rothschild, L. P. (1975). Factoring multivariate polynomials over the integers. *Math. Comp.* **29,** 935–950.

Winkler, F. (1984). *The Church-Rosser Property in Computer Algebra and Special Theorem Proving: An Investigation of Critical-Pair/Completion Algorithms*. Dissertation, Institut für Mathematik, J. Kepler Universität, Linz.

Winkler, F. (1986). Solution of Equations I: Polynomial Ideals and Gröbner Bases. Lecture notes, Short Course "Symbolic and Algebraic Computation". *Conf. on "Computers & Mathematics"*. Stanford University, 1986, Series in Computational Mathematics, R. D. Jenks, ed., Springer-Verlag.

Winkler, F. (1987a). p-adic methods for the computation of Gröbner bases, extended abstract. *EUROCAL'87*, Leipzig, GDR.

Winkler, F. (1987b). A recursive method for computing a Gröbner basis of a module in $K[x_1, \ldots, x_v]^r$. *A.A.E.C.C.-5*, Menorca, Spain.

Winkler, F., Buchberger, B., Lichtenberger, F., Rolletschek, H. (1985). "Algorithm 628 — An algorithm for constructing canonical bases of polynomial ideals. *ACM Trans. on Math. Software* **11,** 66–78.

Zassenhaus, H. (1969). On Hensel factorization, I. *J. Number Theory* **1,** 291–311.