On Lucky Primes*

Hans-Gert Gräbe
Institut für Informatik, Universität Leipzig, Germany

9 February 1993

Abstract

Winkler (1988) and Pauer (1992) present algorithms for a Hensel lifting of a modular Gröbner basis over lucky primes to a rational one. They have to solve a linear system with modular polynomial entries that requires another (modular) Gröbner basis computation.

After an extension of luckiness to arbitrary (commutative noetherian) base rings we show in this paper that for a homogeneous polynomial ideal I one can lift not only its Gröbner basis but also a homogeneous basis of its syzygy module. The same result holds for arbitrary ideals and liftings from $\mathbf{Z}/p$ to $\mathbf{Q}$. Moreover the same lifting can be obtained from a true Gröbner trace by linear algebra over $\mathbf{Q}$ only. Parallel modular techniques allow to find such a true Gröbner trace and a lucky prime with high probability.

All these results generalize in an obvious way to homogeneous modules generated by the rows of matrices with polynomial entries. Since luckiness can be weakened to a condition that transfers from I to higher syzygy modules the lifting theorem generalizes to a lifting theorem for the resolution of I.

1 Introduction

Coefficient growth may have a significant influence on the computational complexity of computing a Gröbner basis for an ideal $I \subset \mathbf{Q}[x_1, \ldots, x_n]$. Modular methods proved to be very useful to limit these expenditures to a necessary minimum. Traverso (1988) observed that it is useful to store a Gröbner trace of the modular computation to lift results to $\mathbf{Q}[x_1, \ldots, x_n]$. Winkler (1988) and Pauer (1992) gave algorithms for a Hensel lifting of a modular Gröbner base over lucky primes to a rational one. The algorithms proposed have to solve a linear system with modular polynomial entries, hence require another (modular) Gröbner basis computation.

The first subject of this paper is an extension of luckiness to arbitrary (commutative noetherian) base rings. We show that the same results as in (Pauer, 1992) can be proved to be valid in a more general context of fibers and localizations of the base ring k. Moreover for (homogeneous) ideals a lifting of the basis of the modular syzygy module is always a basis of the syzygy module over the rationals. A slight modification of Pauer's original definition allows to extend the lifting theorem also to higher syzygy modules.

Then we discuss the concept of multimodular coefficient arithmetic and prove it to be well suited for a search for lucky primes. In the last part of the paper we present a lifting algorithm that requires only linear algebra over $\mathbf{Q}$.

The proposed Gröbner algorithm can briefly be described as follows :

*Appeared in *J. Symb. Comp.* **15** (1993), 199 - 209.

- By parallel modular techniques find at first (with high probability) the minimal reduced modular Gröbner basis, the true Gröbner trace and also a lucky prime.

- Then construct a system of linear equations with coefficients in $\mathbf{Q}$ whose solution gives the unique lifting of the minimal reduced modular Gröbner basis to the rational one in the case we've got indeed the true Gröbner trace. Otherwise the system has no solution.

All these considerations can be generalized in an obvious way to modules generated by the rows of a matrix with polynomial entries (i.e. given by a finite presentation). For the sake of simplicity we restrict our explanations to the case of ideals.

2 Gröbner Bases

Let's begin with some basic definitions. $S := k[x_v : v \in H]$ denotes the (commutative noetherian) polynomial ring in the variables $x_v,\ v \in H$, over the (commutative) ring k. A monomial will be either $\mathbf{x^a} := \prod x_v^{a_v}$ or $\mathbf{a} := (a_v) \in \mathbf{N}^H$.

A total order $<$ on $\mathbf{N}^H$ is a *term order* iff it is monotone and noetherian, i.e. satisfies the conditions

(1) $a < b \Leftrightarrow a + c < b + c$ for all $a, b, c \in \mathbf{N}^H$

(2) $a \geq 0$ for all $a \in \mathbf{N}^H$

Given such an order, $f = \sum c_a x^a \in S$ and a subset $B \subset S$ we define

the initial term $in(f) := c_{a_0} x^{a_0}$ with $a_0 = max\{a : c_a \neq 0\}$,

the degree $deg(f) := a_0$,

the leading coefficient $lc(f) := c_{a_0}$,

the support $supp(f) := \{a \ : \ c_a \neq 0\}$ and
$supp(M) := (supp(f_{ij}))$, if $M = (f_{ij})$ is a matrix with polynomial entries,

$C_a(B) = \{lc(f) \ : \ f \in B \text{ and } deg(f) = a\}$ and

$in(B) := \{in(f) : f \in B\}$.

By convention we let $in(0) = lc(0) = 0$ and $deg(0)$ be undefined. f is *normalized* iff $c_{a_0} = 1$.

Let $k,\ B$ and S be as above, $I = (B)$ the ideal generated by B, and $\Sigma(I) = \{a \ : C_a(I) \neq 0\}$. Denote $Gen(\Sigma)$ the set of monoid generators of $\Sigma \subset \mathbf{N}^H$.

There are several definitions for Gröbner bases which are all equivalent if k is a field, see (Möller, 1988) :

(G − 1) The standard monomials $x^a,\ a \notin \Sigma$, form a free k-module basis of $A = S/I$ and every $x^a,\ a \in \Sigma$, (*non standard monomial*) has a uniquely determined (finite) representation $st(a) := \sum r_{ab} x^b$ such that $x^a \equiv st(a)\ (mod\ I)$ and, for all b, $r_{ab} \neq 0$ implies $a > b$.

(G − 2) $f \in I$ iff there is a representation $f = \sum c_a f_a$ with $deg(f) \geq deg(c_a f_a)$ for all a.

(G − 3) $in(B)$ generates $in(I)$.

In general one has the implications $(G-1) \Rightarrow (G-2) \Leftrightarrow (G-3)$. If k is a field we can assume every $f \in S$ to be normalized, hence $(G-3) \Rightarrow (G-1)$.

Ideals satisfying (G – 1) are called monic in (Pauer, 1992). In (Möller, 1988) the notion of weak and strong reduction was introduced to distinguish between these definitions.

Under the assumption of (G – 1) define $B_0 = \{x^a - st(a) \ : \ a \in Gen(\Sigma)\}$ to be the (uniquely determined) *reduced Gröbner basis* of I.

Since $C_a(I) \subseteq C_b(I)$ if x^a divides x^b and k is noetherian, every ideal I has a finite basis satisfying (G – 3). If k is effective computable then such a *generalized Gröbner basis* can be computed in a finite number of steps. For that purpose normal form algorithm and critical pair definition have to be modified as in thm. II.6 of (Mora, 1988). As in the field case ideal membership can be detected algorithmically using such a basis. Probably the first intensive studies of this generalization are contained in (Zacharias, 1978) and (Trinks, 1978). They were partly rediscovered and extended by several authors, see e.g. (Assi, 1991; Gianni *et al.* , 1988; Möller, 1988; Mora, 1988 and Pauer, 1992).

Under the assumption of (G – 3) a generalized Gröbner basis can be reduced carrying out all possible interreductions. Since k may have syzygies itself the result is no more unique.

3 Lucky Primes

For $p \in Spec(k)$ let's denote $I^{(p)} := I \bigotimes_k k_p/pk_p$ the *fiber* of I over p, $I_p := I \bigotimes_k k_p$ the *localization* of I at p, $\hat{I}_p$ the pS_p-adic completion of I_p and for $c \in k \setminus p$ $I_c := I \bigotimes_k k_c$ the restriction of I to a dense affine open subset of $Spec(k)$. Here k_c denotes the localization of k at the multiplicative set $\{c^n \ : \ n \in \mathbf{N}\}$.

Winkler (1988) investigated connections between the Gröbner bases of special fibers $I^{(p)}$ for maximal primes $p \in Spec(k)$ and the generic fiber $I^{(0)}$ assuming $k = \mathbf{Z}$. (Pauer, 1992) contains a further development of these ideas. Below we extend the corresponding definitions and results to arbitrary (commutative noetherian) base rings.

Lemma 1 *Let $k,\ S,\ I,\ \Sigma = \Sigma(I)$ be as in the preceding paragraph and $p \in Spec(k)$. Then the following conditions are equivalent :*

1) *$C_a(I) \not\subset p$ for all $a \in \Sigma$.*

2) *$C_a(I) \not\subset p$ for all $a \in Gen(\Sigma)$.*

3) *I_p satisfies (G – 1) over k_p and Σ.*

4) *$(S/in(I))_p$ is a free k_p-module with basis $\{x^a : a \notin \Sigma\}$.*

5) *$I^{(p)}$ satisfies (G – 1) over $k^{(p)}$ and Σ.*

If these equivalent conditions are satisfied we conclude moreover

6) *$(S/I)_p$ is a free k_p-module.*

PROOF : 2. $\Rightarrow$ 3. : Since $C_a(I)_p = (1)$ for $a \in Gen(\Sigma)$ we have only to prove the linear independence $(mod\ I_p)$ of x^a, $a \notin \Sigma$. Assume $\sum \frac{c_a}{v} x^a \in I_p$, $\frac{c_a}{v} \in k_p$ and all $a \notin \Sigma$, i.e. $C_a(I) = 0$. Then there exists $u \in k \setminus p$ such that $\sum uc_a x^a \in I$. This yields $uc_a \in C_a(I) = 0$ by noetherian induction, hence $\frac{c_a}{v} = 0$ for all a.

4. follows immediately from 3. since $S/in(I) = \bigoplus_a k/C_a(I)$ and implies 1.

3. $\Rightarrow$ 5. : Again it remains only to prove the linear independence $(mod\ I^{(p)})$ of x^a, $a \notin \Sigma$. But $\sum \overline{c_a} x^a \in I^{(p)}$, i.e. $\sum c_a x^a \in I_p + p \cdot S_p$ for certain liftings $c_a \notin p$ would contradict the uniqueness of normal forms in S_p/I_p guaranteed by (G – 1).

The other assertions are obvious. □

Define $p \in Spec(k)$ to be *lucky* iff $C_a(I) \not\subset p$ for all $a \in \Sigma$. By 2) luckiness is an open condition. Hence there are only finitely many unlucky primes in the case $k = \mathbf{Z}$, that can be read off from the leading coefficients of a generalized $\mathbf{Z}$-Gröbner basis of I, see (Pauer, 1992).

In general one has the following result:

Lemma 2 *Under the assumptions of lemma 1 let k be a domain. Then there exists $c \in k$ such that I_c satisfies (G – 1) over S_c.*

Moreover for finitely many given lucky primes p_i one can choose $c \notin p_i$.

PROOF : Take $0 \neq c \in \bigcap_{a \in Gen(\Sigma)} C_a(I)$. A prime avoidance argument shows the second statement. □

If k is not a domain this intersection may be the zero ideal, hence the restriction to domains is essential.

EXAMPLE : Assume $B := \{x^2 - 2y, y^2 - 2x\} \subset \mathbf{Z}[x, y] =: S$ generates the ideal I. Since B is a Gröbner basis of I with respect to the degreewise lexicographic term order, $(S/I)_p$ is a free $\mathbf{Z}_p$-module for any $p \in Spec\ \mathbf{Z}$. With respect to the pure lexicographic term order I has the (G – 3)-basis

$$B' = \{x^2 - 2y, 2x - y^2, xy^2 - 4y, y^4 - 8y\} \qquad \text{and} \qquad \Sigma' = (x, y^4).$$

Hence 2 is not a lucky prime of I with respect to this term order. Nevertheless the fiber $I^{(2)}$, generated by (x^2, y^2), satisfies (G – 1) over $S^{(2)}$, but not with respect to Σ'.

QUESTION : If $(S/I)_p$ is a free k_p-module, is there always a noetherian term order, with respect to that $p \in Spec\ k$ is lucky for I ? If so, how can it be found ?

The main property of lucky primes used in applications is formulated in the following theorem which is a slight modification of prop. 4.3. in (Pauer, 1992).

Theorem 1 (The Lifting Theorem) *Let k and S be as above, $B \subset S$ a finite basis of the ideal I (or more general of the submodule $I \subseteq S^r$) and $p \in Spec(k)$ such that $(S/I)_p$ (resp. $(S^r/I)_p$) is k_p-free. Denote by overbars the canonical residue maps. Then*

1) *(Lifting Presentations to an Infinitesimal Neighbourhood)*

Assume $h \in I$ and $\{y_f \ : \ f \in B\} \subset S$ are such that $\overline{\sum y_f f} = \overline{h}$ over $S^{(p)}$. Then there is a family $\{z_f \ : \ f \in B\} \subset S_p$ with $\sum z_f f = h$ over S_p and $\overline{y_f} = \overline{z_f}$ for all $f \in B$.

2) *(Lifting Presentations to an Affine Neighbourhood)*

If moreover $c \in k \setminus p$ and $(S/I)_c$ (resp. $(S^r/I)_c$) is k_c-free, then there is even a family $\{z_f \ : \ f \in B\} \subset S_c$ with $\sum z_f f = h$ and $\overline{y_f} = \overline{z_f}$ for all $f \in B$.

3) *(Syzygies at an Infinitesimal Neighbourhood)*

Let $M := \{(y_f^i \ : \ f \in B)\}_i \subseteq S_p^B$ *be a set of syzygies of* B *over* S_p *(i.e.* $\sum y_f^i f = 0$ *for all* i*) such that* $\{(\overline{y_f^i} \ : \ f \in B)\}$ *generates the syzygy module of* $\overline{B}$ *over* $S^{(p)}$*.*

If I *and* M *are homogeneous then* M *generates the syzygy module of* B *over* S_p*.*

In general $M \bigotimes_{S_p} \hat{S}_p$ *generates the syzygy module of* B *over the formal neighbourhood* $\hat{S}_p$ *of* p *and* $(M) \bigotimes_{S_p} \hat{S}_p \bigcap S_p^B = \{m \in S_p^B : \exists f \in 1 + pS_p \text{ with } fm \in M\}$ *is the full syzygy module of* B *over* S_p*.*

PROOF : The first two assertions are prop. 4.3. in (Pauer, 1992) and follow immediately from $I_p \bigcap pS_p/pI_p = Tor_1^{k_p}(S_p/I_p, k^{(p)}) = 0$.

For 3. let M' denote the full syzygy module of B over S_p. If I is homogeneous we get by 1. $(M) + pM' = M'$. The first assertion then follows from Nakayama's lemma since M' decomposes into homogeneous components that are finitely generated over k_p.

The general case is an immediate consequence of thm. 10.17. in (Atiyah, MacDonald, 1969). □

EXAMPLE : Let be $S = \mathbf{Z}[x, y]$, $p \in Spec\ \mathbf{Z}$ and I the ideal generated by $B = \{x, y\}$. $\overline{M} = [-y \ x]$ is the syzygy matrix of $\overline{B}$ over $S^{(p)}$, $M = [-y(1 + px) \ x(1 + px)]$ a lifting of $\overline{M}$ to syzygies of B over S_p, but obviously it doesn't generate the full syzygy module. Hence we cannot expect that arbitrary liftings of inhomogeneous syzygies will generate the full syzygy module at the infinitesimal neighbourhood.

This pathological example suggests that M should be a basis for the full syzygy module provided that it is a "good" lifting from the fiber. We have the following partial result in this direction :

Proposition 1 *With the notation of theorem 1 assume moreover that*

1) $p = (p)$ *is a principal ideal,*

2) $\overline{M}$ *is a Gröbner basis of the syzygy module at the fiber and*

3) $deg\ y^i = deg\ \overline{y^i}$ *for all* i*.*

Then M *is a basis of the syzygy module of* I_p *over* S_p*.*

PROOF : Extend $\{y^i\}$ to a minimal (G - 3)-basis M_1 of M' and assume $v \in M_1 \setminus \{y^i\}$. Since, by 2. and 3., it exists a presentation $\overline{v} = \sum \overline{u_i} \overline{y^i}$ with $deg\ v > deg\ \overline{v} = max(deg\ u_i y^i)$ we may assume moreover that $v = pv_1$ with $v_1 \in M'$ and $deg\ v = deg\ v_1$. But this contradicts the minimality of the Gröbner basis. □

As mentioned already parenthetically the theorem above easily generalizes to homogeneous submodules of free modules instead of ideals. Moreover since

$$Tor_1^{k_p}(S_p^B/M_p, k^{(p)}) = Tor_2^{k_p}(S_p/I_p, k^{(p)}) = 0$$

M_p itself is k_p-free and the theorem applies also to M. This way part 3 generalizes immediately to higher syzygy modules of S/I. Hence one can lift at once a *whole syzygy chain* of the homogeneous ideal I from the fiber to an *infinitesimal* neighbourhood over a lucky prime.

If k is a domain then it follows by general arguments as e.g. presented in thm. 3.4. of (Hochster, Roberts, 1976) that a lucky prime p has also an *affine* neighbourhood, where the lifting M is a basis of the (first) syzygy module. Alternatively this can be shown in the following way : Generalize the definition of C_a to finitely generated submodules of S^B. With the notions from the proof above we get $C_a((M)) \subseteq C_a(M')$, with equality at $p \in Spec\ k$. But since we have on both sides only *finite* families of ideals they will coincide also over an open subset of $Spec\ k$ containing p.

On the other hand one cannot expect that a lifting M is a basis for the syzygy module over a *given* prime $q \not\subset p$. Indeed, for $c_1 \in q \setminus p$ the module $(c_1 M)$ coincides with (M) at p but vanishes at q. Hence there is no analogy of the affine lifting theorem for syzygy modules.

But denote that a whole syzygy chain of I_p over S_p (and also of I_c over S_c) can be pushed down to the fiber $S^{(p)}$:

Lemma 3 *Under the assumptions of theorem 1 let*

$$\mathbf{F}. : \quad \ldots \to F_2 \to F_1 \to I_p \to 0$$

be a free resolution of I_p over S_p. Then $\mathbf{F}. \bigotimes_{k_p} k^{(p)}$ is a free resolution of $I^{(p)}$ over $S^{(p)}$.

Indeed, $(S/I)_p$ is k_p-free, hence $Tor_i^{k_p}(S_p/I_p, k^{(p)}) = 0$ for all $i > 0$.

Let I be as above with basis B. If k is a domain we obtain the following connection between a special fiber over a lucky prime and the generic fiber over (0) :

- A minimal, reduced, and normalized Gröbner basis of $B^{(p)}$ over $S^{(p)}$ can be lifted to a minimal, reduced, and normalized Gröbner basis of B_p over S_p and then pushed down to a minimal, reduced, and normalized Gröbner basis of $B^{(0)}$ over $S^{(0)}$.

  This follows from lemma 1 and the uniqueness of such a Gröbner basis.

- If I is homogeneous then any homogeneous basis of the syzygy module of $B^{(p)}$ over $S^{(p)}$ can be lifted to a homogeneous basis of the syzygy module of B_p over S_p and then pushed down to a basis of the syzygy module of $B^{(0)}$ over $S^{(0)}$.

The first assertion can be generalized to connect two fibers over lucky primes.

4 Multimodular Polynomial Arithmetic

Lets assume for simplicity $k = \mathbf{Z}$ in this chapter although our considerations may be formulated in a more general context. Pauer (1992), Traverso (1988) and Winkler (1988) present no satisfactory solution for the problem to find a lucky prime according to that the computations proposed can be carried out. The only demand on such a prime is that the modular Gröbner algorithm should detect non zero over $\mathbf{Z}$ leading coefficients.

A good approximate solution to this problem can be achieved by a multimodular coefficient arithmetic, i.e. over the base ring $\prod_{i=1}^{N} \mathbf{Z}/p_i\mathbf{Z}$, where $(p_1, \ldots, p_N)$ is an array of primes. In the terminology introduced in the preceding paragraph we will do computations in special fibers of I not individual but in common. By this approach a nonzero coefficient will be

Table 1: Multimodular Gröbner basis computations

	N=1	N=10	N=20	N=30	MCL	PL	a	b	$\frac{b}{a}$	RP	RSP
1	35.3	80.2	130.2	182.0	> 120	3.9	5.1	30	5.9	1063	17
2	1.5	4.5	7.6	10.8	22	0.2	0.32	1.2	3.8	—	9
3	20.9	53.2	89.7	126.3	>120	2.0	2.9	19	6.5	—	18
4	0.12	0.38	0.77	1.04	2	0.02	0.05	0.03	0.7[1]	—	1
5	0.9	2.8	4.8	6.9	4	0.1	0.21	0.6	2.8	—	2
6	12.8	36.8	64.2	91.4	>200	0.9	2.7	10	3.7	—	21
7	1.5	5.1	8.9	12.8	332	0.4	0.4	1.2	3.1	—	9
8	0.7	2.4	4.3	6.0	28	0.1	0.18	0.5	2.8	1051	8

N	the number of primes used
$t = aN + b$	the computational time, hence
a	the time spent for (single modular) coefficient computations and
b	the time spent for (in this concept essentially not parallelizable) polynomial list management overhead
PL	time spent for the pair list management
MCL	lower coefficient bound (in bytes) for the Gröbner computation over $\mathbf{Z}$
RP	rejected (i.e. possibly unlucky) primes among the 30 primes greater than 1000
RSP	the number of rejected small primes during a multimodular Gröbner computation with the first 25 primes $2, \ldots, 97$

detected with probability $1 - \prod \frac{1}{p_i}$ and in contrast to single modular computations considered in the papers cited above even unlucky primes will be found with high probability, since if a leading coefficient detected as nonzero is zero ($mod\ p_i$), the corresponding polynomial can be normalized only switching out p_i. One should control disappearence and renew the array of primes if the number of surviving primes becomes to small. For this purpose one has only to record how new base elements were composed, since only these computations should be repeated. The details are similar to the explanations in (Traverso, 1988) and left to the reader. Moreover this method is well suited for parallelization.

In a (serial) implementation in TURBO-PASCAL (using the compiler's residue arithmetic) I observed that the computation time, as one should expect, depends linear on the number of primes involved in a very accurate way. Table 1 contains the result of sample computations on examples well known to have long (intermediate) integer coefficients. The results given reflect the time spent by the Gröbner algorithm in the S-polynomial reduction part only. They are measured in seconds on an IBM-PC 80386–25. The primes involved are the first primes greater than 1000. All examples are computed with respect to the lexicographic term order induced by the given variable order.

The examples :

The Caprasse example ($z > y > x > t$), (Faugere *et al.* , 1989, ex. 7.3.) :

[1] with great relative error, since the timing is near the measuring bound of the used software

1) $\{\ y^2z + 2xyt - 2x - z,$
$-x^3z + 4xy^2z + 4x^2yt + 2y^3t + 4x^2 - 10y^2 + 4xz - 10yt + 2,$
$2yzt + xt^2 - x - 2z,$
$-xz^3 + 4yz^2t + 4xzt^2 + 2yt^3 + 4xz + 4z^2 - 10yt - 10t^2 + 2\ \}$

The Katsura examples with $u_0 > \ldots > u_n$, (Boege *et al.* ,1986) :

2) for $n = 3$: $\{\ u_0 + 2u_1 + 2u_2 + 2u_3 - 1,$
$u_0^2 + 2u_1^2 + 2u_2^2 + 2u_3^2 - u_0,$
$2u_0u_1 + 2u_1u_2 + 2u_2u_3 - u_1,$
$2u_0u_2 + u_1^2 + 2u_1u_3 - u_2\ \}$

3) for $n = 4$: $\{\ u_0 + 2u_1 + 2u_2 + 2u_3 + 2u_4 - 1,$
$u_0^2 + 2u_1^2 + 2u_2^2 + 2u_3^2 + 2u_4^2 - u_0,$
$2u_0u_1 + 2u_1u_2 + 2u_2u_3 + 2u_3u_4 - u_1,$
$2u_0u_2 + u_1^2 + 2u_1u_3 + 2u_2u_4 - u_2,$
$2u_0u_3 + 2u_1u_2 + 2u_1u_4 - u_3\}$

A class of equations with symmetries :

4) $\{z + y + x^2 - 3,\ z + y^2 + x - 3,\ z^2 + y + x - 3\}$

5) $\{z + y + x^3 - 3,\ z + y^3 + x - 3,\ z^3 + y + x - 3\}$

6) $\{z + y^2 + x^3 - 3,\ z^2 + y^3 + x - 3,\ z^3 + y + x^2 - 3\}$

Trinks' examples with the optimal variable order $w > p > z > t > s > b$.
(Boege *et al.* , 1986) :

7) "Big Trinks'" : $B = \{\ 45p + 35s - 165b - 36,$
$35p + 40z + 25t - 27s,$
$15w + 25sp + 30z - 18t - 165b^2,$
$-9w + 15tp + 20sz,$
$pw + 2tz - 11b^3,$
$99w - 11bs + 3b^2\}$

8) "Little Trinks'" : $B \cup \{10000b^2 + 6600b + 2673\}$

All examples show a time behaviour $t = aN + b$ with time constants a and b depending only on the examples. The ratio $\frac{b}{a}$ ranges between 3 and 7. Hence exploiting the extreme idea of a bimodular arithmetic with an effective updating procedure, if one of the primes is switched out, will add almost nothing to the computing time of the single modular case, but end with high probability at two lucky primes. Even with $N = 10$ in all examples above the true Gröbner trace was obtained without renewing the set of primes.

5 The Lifting Procedure

During the execution of the Gröbner algorithm for B (regarded as a column vector with polynomial entries) we get together with the Gröbner basis G a matrix U with $UB = G$ and a syzygy matrix V of B for free. If B is a Gröbner basis then V is automatically a Gröbner basis with respect to a certain module term order. We will assume this for V in general, applying an appropriate postprocessing if necessary.

For an arbitrary domain k and $p \in Spec(k)$ denote $G^{(p)}$, $U^{(p)}$ and $V^{(p)}$ the corresponding matrices for a Gröbner basis computation over $k^{(p)}$. If p is a lucky prime the sizes of $G^{(p)}$, $U^{(p)}$, $V^{(p)}$ and $G^{(0)}$, $U^{(0)}$, $V^{(0)}$ coincide and, following up the same reduction trace, obviously $supp(G^{(p)}) \subseteq supp(G^{(0)})$, $supp(U^{(p)}) \subseteq supp(G^{(0)})$ and $supp(V^{(p)}) \subseteq supp(V^{(0)})$ (componentwise inclusion).

If $supp(G^{(p)}) = supp(G^{(0)})$ and $supp(U^{(p)}) = supp(U^{(0)})$ we say that p gives a *true Gröbner trace* and if also $supp(V^{(p)}) = supp(V^{(0)})$ we say that p gives a *true extended Gröbner trace.*

Lemma 4 *There is a dense affine open set in $Spec(k)$ defined by $c \in k$ such that all primes $p \in Spec(k_c)$ are lucky and have a true extended Gröbner trace.*

Proof : See thm. 1 in (Winkler, 1988). Obviously the product of all numerators and denominators of all coefficients of all polynomial entries in $G^{(0)}$, $U^{(0)}$ and $V^{(0)}$ and c from lemma 2 will satisfy the condition. □

For $p \in Spec\ \mathbf{Z}$ the lifting theorem and proposition 1 yield that such a lifting of $G^{(p)}$, $U^{(p)}$ resp. $V^{(p)}$ to $G^{(0)}$, $U^{(0)}$ resp. $V^{(0)}$ with $G^{(0)} = U^{(0)}B$ resp. $V^{(0)}B = 0$ will be a Gröbner basis resp. a basis of the syzygy module of B over $\mathbf{Q}$. The most natural way to obtain such a lifting starts from the multimodular result and uses the rational version of the Chinese Remainder Theorem. Any successful lifting of the modular result will be automatically a Gröbner basis over $\mathbf{Q}$. But for a *guaranteed* success of the lifting procedure we need a coefficient bound to estimate the number of surviving primes needed from the multimodular computation.

Below we concentrate on another approach. It is in the spirit of the constructive geometry at the beginning of this century reducing algebraic questions to the solution of big but finite linear systems over $\mathbf{Q}$.

If $M = (f_{ij})$ is a matrix with polynomial entries define a matrix $N = (F_{ij})$ to be a *generic matrix with pattern M* iff F_{ij} are polynomials with indeterminate coefficients and $supp(f_{ij}) = supp(F_{ij})$ for all i, j.

Denote by U_p resp. G_p an arbitrary lifting of $U^{(p)}$ resp. $G^{(p)}$ to k and by U resp. G a generic matrix with pattern U_p resp. $(G_p - in(G_p))$. Then $(U + U_p)B = G + G_p$ defines a system of linear equations in the indeterminate coefficients. If p is a lucky prime with true Gröbner trace this system has a solution in pk_p and hence over $k^{(0)}$, the quotient field of k. Moreover $G^{(0)} = G + G_p$ is uniquely determined as the minimal, reduced, and normalized Gröbner basis of B over $k^{(0)}$. If we suddenly started from a wrong Gröbner trace the pattern of G_p may be wrong. In this case one of the uniquely determined nonzero coefficients of $G^{(0)}$ would disappear and the system becomes inconsistent. If only the pattern of U_p is wrong the system may have a solution $G^{(0)}$, $U^{(0)}$. Since $U^{(0)}B = G^{(0)}$ and $G^{(0)}$ has "the right leading terms", by the uniqueness of reduced, minimal Gröbner bases it is again a Gröbner basis over $k^{(0)}$. Hence we have not to care about the solution to be inside pk_p.

This suggests to consider the system $UB = G_1$ where G_1 is a generic matrix of pattern $G^{(p)}$ with all leading coefficients set equal to 1. If p is a lucky prime with true Gröbner trace this system has a solution over $k^{(0)}$. In any case a solution G_1 over $k^{(0)}$ is a Gröbner basis of B over $k^{(0)}$. On the other hand the pattern of U may not be minimal since U is determined only upto syzygies of B, see below.

EXAMPLE : (Example 4 from above)

$$B = \left[\begin{array}{ccc} x^2+y+z-3 & x+y^2+z-3 & x+y+z^2-3 \end{array} \right]^T$$

A lucky prime with true extended Gröbner trace, obtained by multimodular computations, is $p = 17$. We get

$$G^{(p)} = \left[\begin{array}{c} g_1' \\ g_2' \\ g_3' \\ g_4' \end{array} \right] = \left[\begin{array}{c} x+y+z^2-3 \\ y^2-y-z^2+z \\ yz^2-2y-8z^4+6z^2+3 \\ z^6+7z^4+4z^3+2z^2-8z-6 \end{array} \right] \quad \text{and} \quad U^{(p)} = \left[\begin{array}{ccc} 0 & 0 & 1 \\ 0 & 1 & -1 \\ -8 & 8 & f_1 \\ f_2 & f_3 & f_4 \end{array} \right]$$

with

$f_1 = 8x - 8y - 8z^2 - 1$
$f_2 = -2y + z^2 - 1$
$f_3 = 2y + 3z^2 - 7$ and
$f_4 = 2xy - xz^2 + x - 2y^2 - yz^2 + 3y + z^4 - 7z^2 - 7.$

The corresponding linear system (43 equations in 39 variables) decomposes into four independent systems, one for each entry of $G^{(p)}$. Solving these systems one obtains the **Q**-Gröbner basis $G^{(0)} = \{g_1',\ g_2',\ g_3' + \frac{17}{2}z^4 - \frac{17}{2}z^2,\ g_4' - 17z^4 + 17z^2\}$.

No coefficient bound is involved since we solve the linear equations directly over $Q(k)$.

Assume $k = \mathbf{Z}$, lift $V^{(p)}$ to a matrix V_p over $\mathbf{Z}$ and let V be a generic matrix with pattern V_p. If p is a lucky prime with true extended Gröbner trace, the linear system, obtained from $(V + V_p)B = 0$ in the same way as above, has a solution over $p\mathbf{Z}_p$, too. By proposition 1 the rows of $V^{(0)} = V + V_p$ generate the full syzygy module of B.

For our example we get

$V^{(0)} = V^{(p)} =$

$$\left[\begin{array}{lll} 0 & -x-y-z^2+3 & x+y^2+z-3 \\ y^2-y-z^2+z & \begin{array}{l} -xy^2+xy+xz^2- \\ xz-y^3-y^2z^2+3y^2- \\ yz+2y-z^3+3z^2+ \\ 2z-6 \end{array} & \begin{array}{l} y^4+2y^2z-6y^2+y+ \\ z^2-5z+6 \end{array} \\ -x-y^2-z+3 & x^2+y+z-3 & 0 \end{array} \right].$$

Using a script based on CALI, the author's REDUCE package on commutative algebra, and a (naive) solver for sparse linear systems we lifted this way also the bases of ex. 5 and 8 above from $p = 32003$ to the rationals. Lacking a better solver for sparse linear systems we

generated and solved for ex. 3 systems of $95, 142, 37$ and 156 linear equations with $89, 110, 34$ resp. 149 variables in 77 sec., whereas for ex. 8 systems of $3, 139, 139, 203, 227$ resp. 203 linear equations with $3, 152, 152, 230, 321$ resp. 230 variables in 843 sec. (on an HP 9000/345).

The last example shows an overhead of variables compared to the number of equations. Hence searching for a particular solution of $UB = G_1$ we can set the overhead variables, appearing in the general solution as parameters, equal to 0. This implies that there is a transition matrix U with even smaller pattern satisfying the above equation over $\mathbf{Q}$.

References

[1] Atiyah, M.F, MacDonald I.G. (1969). *Introduction to commutative algebra.* Addison-Wesley, Reading, Massachusetts.

[2] Assi, A. (1991). *Constructions effectives en algèbre commutative.* Thesis, Grenoble.

[3] Boege, W., Gebauer, R., Kredel, H. (1986). Some examples for solving systems of algebraic equations by calculating Gröbner bases. *J. Symb. Comp.* **2**, 83 - 98.

[4] Faugere, J.C., Gianni, P., Lazard, D., Mora, T. (1989). Efficient computation of zerodimensional Gröbner bases by change of ordering. Preprint.

[5] Gianni, P., Trager, B., Zacharias, G. (1988). Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comp.* **6**, 149 - 167.

[6] Gräbe, H.-G. (1993). CALI – A REDUCE package for commutative algebra. Version 1.0. Available through the REDUCE library `redlib@rand.org`.

[7] Hochster, M. Roberts, J.L. (1976). The purity of Frobenius and local cohomology. *Adv. math.* **21**, 117 - 172.

[8] Möller, H.-M. (1988) On the construction of Gröbner bases using syzygies. *J. Symb. Comp.* **6**, 345 - 359.

[9] Mora, T. (1988). Seven variations on standard bases. Preprint, Univ. Genova.

[10] Pauer, F. (1992). On lucky ideals for Gröbner basis computations. *J. Symb. Comp.* **14**, 471 - 482.

[11] Traverso, C. (1988). Gröbner trace algorithms. *Proceedings ISSAC'88, Lecture Notes in Comp. Sci.* **358**, 125 - 138.

[12] Trinks, W. (1978). Über B. Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen. *J. Number Theory* **10**, 475 - 488.

[13] Winkler, F. (1988). A p-adic approach to the computation of Gröbner bases. *J. Symb. Comp.* **6**, 287 - 304.

[14] Zacharias, G. (1978). *Generalized Gröbner bases in commutative polynomial rings.* Bach. thesis, MIT.