Journal of Symbolic Computation 35 (2003) 403–419

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Modular algorithms for computing Gröbner bases

Elizabeth A. Arnold*

Department of Mathematics, Texas A&M University, College Station, TX 77843, USA

Received 5 October 2000; accepted 14 March 2002

Abstract

Intermediate coefficient swell is a well-known difficulty with Buchberger's algorithm for computing Gröbner bases over the rational numbers. p-Adic and modular methods have been successful in limiting intermediate coefficient growth in other computations, and in particular in the Euclidian algorithm for computing the greatest common divisor (GCD) of polynomials in one variable. In this paper we present two modular algorithms for computing a Gröbner basis for an ideal in $\mathbb{Q}[x_1, \ldots, x_\nu]$ which extend the modular GCD algorithms. These algorithms improve upon previously proposed modular techniques for computing Gröbner bases in that we test primes before lifting, and also provide an algorithm for checking the result for correctness. A complete characterization of unlucky primes is also given. Finally, we give some preliminary timings which indicate that these modular algorithms can provide considerable time improvements in examples where intermediate coefficient growth is a problem.

1. Introduction

Intermediate coefficient swell is a notorious difficulty of Buchberger's algorithm for computing Gröbner bases over the rational numbers. During the execution of the algorithm, many intermediate polynomials are computed before the desired Gröbner basis is reached. Unfortunately, the coefficients of these intermediate polynomials can grow to enormous size, even if the coefficients of the polynomials of the original generating polynomials and the Gröbner basis are relatively small. This growth of coefficients can be so great as to significantly slow down the Gröbner basis algorithm or halt it altogether.

Example 1.1.

$$\begin{aligned} f_1 &= 8x^2y^2 + 5xy^3 + 3x^3z + x^2yz \\ f_2 &= x^5 + 2y^3z^2 + 13y^2z^3 + 5yz^4 \end{aligned}$$

* Tel.: +1-979-862-2182; fax: +1-979-279-9226.
E-mail address: barnold@math.tamu.edu (E.A. Arnold).

0014-5793/03/$ - see front matter © 2003 Published by Elsevier Science Ltd.
doi:10.1016/S0747-7171(02)00140-2

$$f_3 = 8x^3 + 12y^3 + xz^2 + 3$$
$$f_4 = 7x^2y^4 + 18xy^3z^2 + y^3z^3.$$

With respect to the DegRevLex ordering with $x > y > z$, the reduced Gröbner basis for the ideal generated by f_1, f_2, f_3, f_4 in $\mathbb{Q}[x, y, z]$ is

$$g_1 = x$$
$$g_2 = y^3 + 1/4$$
$$g_3 = z^2.$$

However, this polynomial appears in the intermediate computations:

$$y^3 - 173590650429045129076474718 2\ldots.$$

In fact, the integer in the second term of the above polynomial contains roughly 80,000 digits. It is the numerator of a rational number with roughly an equal number of digits in the denominator. This six term polynomial has four such coefficients.[1]

Modular and p-adic techniques have been applied successfully to many types of problems where intermediate coefficient growth is significant (Borosh, 1966). These algorithms typically have three basic steps: first, find a "lucky prime" with high probability (roughly, a prime p is lucky for the computation if we do not lose too much algebraic information when viewing the object to be computed modulo p); secondly, compute the object modulo a prime or several primes and then "lift" the coefficients to the integers or rationals; and finally, check that the result is the correct one. The main difficulties are to determine criteria for finding a "lucky" prime, and to find an effective and efficient method for checking the result. In this paper we extend the modular and p-adic algorithms for computing the greatest common divisor (GCD) of polynomials in one variable to algorithms that will compute the Gröbner basis of an ideal of polynomials in several variables with coefficients in the rational numbers.

2. History

The idea of a modular algorithm for computing Gröbner bases was first suggested by Ebert (1983). In this paper he comments that one cannot compare the number of leading terms in two modular Gröbner bases in order to determine the relative unluckiness of the primes. He did, however, prove that one could detect a priori a lucky prime for a Gröbner basis computation involving only binomials and monomials.

Winkler (1987) proposes a p-adic method for lifting a Gröbner basis modulo a prime p to a Gröbner basis with rational coefficients. He presents an effective "step two" for a modular Gröbner basis algorithm. However, Winkler's method is based on two assumptions: (1) that a priori a "lucky prime" is known, and (2) that a bound on the coefficients of the Gröbner basis is known, hence determining when to stop the Hensel lifting. If we were to take a random prime, and lift a given number of times, without a method for checking the result, we would not know if our result was correct. But given a

[1] Computed by Macaulay 2 (Grayson and Stillman, 2000).

lucky prime and a bound on the coefficients, Winkler's method produces a correct rational Gröbner basis for an ideal.

Pauer (1992) and Gräbe (1994) extend Winkler's Step two method to more general rings, but no progress is made on detecting unlucky primes or checking the result. A different approach is taken by Traverso (1988) which avoids the assumptions of knowing a lucky prime and a bound on the coefficients. He proposes a modular "trace" algorithm. But this algorithm is probabilistic. Adding a deterministic check significantly decreases the efficiency of the algorithm. Sasaki (1989) proposes using the Chinese remainder algorithm for computing Gröbner bases.

Our goal in this paper is to extend and improve the Step two lifting method of Winkler, and add both a Step one and a Step three. By introducing the concept of a "Hilbert lucky prime", we will demonstrate an effective method for determining the relative luckiness of two primes and also give an efficient method for checking the result.

3. Preliminaries

In this section we give some definitions and basic Gröbner basis results, as well as introduce notation that will be used throughout the paper. The notation that we use will be the same as in the textbook by Adams and Loustaunau (1994). For more detailed descriptions and proofs, see Adams and Loustaunau (1994) or Buchberger (1985).

Let $X = \{x_1, \ldots, x_v\}$ be a set of indeterminates. We write $\mathcal{R}[X]$ as the ring of polynomials in X with coefficients in a Noetherian ring $\mathcal{R}$. Let $\mathbb{T}^v = \{x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_v^{\alpha_v}\}$ be the set of power products in $\mathcal{R}[X]$. We fix a term order on the power products in $\mathbb{T}^n$. We denote by $\mathrm{lp}(f) \in \mathbb{T}^n$, the leading power product of f, by $\mathrm{lc}(f) \in \mathcal{R}$, the leading coefficient of f, and by $\mathrm{lt}(f) = \mathrm{lc}(f)\mathrm{lp}(f)$, the leading term of f. Moreover, for any subset $S \subseteq \mathcal{R}[X]$, we denote $\mathrm{Lp}(S) = \{\mathrm{lp}(f) \mid f \in S\}$ called the *set* of leading power products of S, and we denote $\mathrm{Lt}(S) = \langle \mathrm{lt}(f) \mid f \in S \rangle \subseteq \mathcal{R}[X]$, the ideal generated by the leading terms of polynomials f in S called the *leading term ideal of* S. Note that $\mathrm{Lp}(S)$ is a set and $\mathrm{Lt}(S)$ is an ideal.

A set of polynomials $G \subseteq I$ is a Gröbner basis for I if and only if $\mathrm{Lt}(G) = \mathrm{Lt}(I)$.

If $\mathcal{R}$ is a field, and G is a Gröbner basis for $I \subseteq \mathcal{R}[X]$, then for every f in I, there exists a $g \in G$ such that $\mathrm{lt}(g)$ divides $\mathrm{lt}(f)$. This is not true in general when $\mathcal{R}$ is not a field. It will always be true that there is a $g \in G$ such that $\mathrm{lp}(g)$ divides $\mathrm{lp}(f)$, but coefficients may present a problem.

If we restrict the ring $\mathcal{R}$ to a principal ideal domain (PID), then we can construct what is called a *strong Gröbner basis*, which will satisfy the previous condition.

Definition 3.1. Let $G = \{g_1, \ldots, g_t\}$ be a set of non-zero polynomials in $\mathcal{R}[X]$, where $\mathcal{R}$ is a PID. We say that G is a *strong Gröbner basis* for $I = \langle g_1, \ldots, g_t \rangle$ if for each $f \in I$, there exists an $i \in \{1, \ldots, t\}$ such that $\mathrm{lt}(g_i)$ divides $\mathrm{lt}(f)$. We say that G is a *minimal strong Gröbner basis* if no $\mathrm{lt}(g_i)$ divides $\mathrm{lt}(g_j)$ for $i \neq j$.

Strong Gröbner bases always exist, but are not usually unique. If the coefficient ring is the integers, it is possible to construct a strong Gröbner basis, G', from a given Gröbner basis, G, such that the set of all primes dividing the leading coefficients of G' is the same as

the set of all primes dividing the leading coefficients of G. This will be useful in Section 5. See Adams and Loustaunau (1994) for a construction.

Note that if $\mathcal{R}$ is a field, then any Gröbner basis is automatically a strong Gröbner basis, although not necessarily unique. We define a *reduced* Gröbner basis, $G = \{g_1, g_2, \ldots, g_t\}$, for an ideal I such that for every i, $\mathrm{lc}(g_i) = 1$, and no power product in g_i is divisible by any leading $\mathrm{lp}(g_j)$ for g_j in the set $G - \{g_i\}$. If $\mathcal{R}$ is a field, then every non-zero ideal in $\mathcal{R}[X]$ has a unique reduced Gröbner basis. Reduced Gröbner bases as defined do not always exist if the coefficient ring is not a field. Gröbner bases for which $\mathrm{lt}(g_i) = 1$ for every i are called *monic* Gröbner bases. If a monic Gröbner basis exists for an ideal, then a reduced Gröbner basis can be constructed from this which is unique.

For our computations involving the Hilbert function, we require the ideal, I, to be homogeneous. However, we would like an algorithm that will compute a Gröbner basis for any ideal, $I \subseteq \mathbb{Q}[X]$. If we chose a graded term order, then it is always possible to homogenize the generators of an arbitrary ideal I, compute a Gröbner basis for the homogeneous ideal, and then dehomogenize and reduce the result to obtain a reduced Gröbner basis for the original ideal I (Möller and Mora, 1984). Therefore, without loss of generality, throughout the rest of this paper, all ideals are assumed to be homogeneous.

4. Modular GCD algorithms

Since the GCD of a set of polynomials in one variable is a Gröbner basis for the ideal generated by these polynomials, we will first examine modular methods for GCD computations. Minor details are omitted in order to present the main ideas which are relevant in a modular Gröbner basis algorithm. For a more complete description, see Davenport et al. (1988).

Let p be a prime integer, $f, g \in \mathbb{Z}[x]$, and $\overline{f}, \overline{g} \in \mathbb{Z}_p[x]$, where $\mathbb{Z}_p$ denotes the field of integers modulo p. Let $d = \gcd(f, g) \in \mathbb{Z}[x]$ and $d_p = \gcd(\overline{f}, \overline{g}) \in \mathbb{Z}_p[x]$. If $d \equiv d_p \mod p$, and $\deg(d_p) = \deg(d)$ then we can use a Hensel algorithm to "lift" d_p to a polynomial, $d_{p^i} \in \mathbb{Z}_{p^i}[X]$ or we can use many such primes and the Chinese remainder theorem to compute $d_n \in \mathbb{Z}_n[x]$ where n is a product of these primes. If the coefficients of d are all less than p^i (respectively n), then d_{p^i} (respectively d_n) (with the appropriate representation of coefficients) is actually the GCD of f and g in $\mathbb{Z}[X]$. This computation will only work if $\deg(d_p) = \deg(d)$ for every prime used in the computation. Unfortunately, this is not true for every prime p.

Definition 4.1. A prime, p, is called *lucky* for f and g if and only if $\deg(d) = \deg(d_p)$.

Since we do not compute d, we cannot tell from d_p whether or not p is a lucky prime. However, it is easy to verify that if p does not divide either of the leading coefficients of f or g, then $\deg(d_p) \geq \deg(d)$. This gives us a method for comparing two primes, p and q, for relative luckiness. If $\deg(d_q) > \deg(d_p)$, then we can discard q as unlucky. This method of testing, however, does not guarantee that p is lucky, only that q is unlucky. Since there are a finite number of unlucky primes (see for example Davenport et al., 1988), after testing several primes, we can find a lucky prime with high probability.

Once we have found a lucky prime with high probability, we can use a Hensel technique to lift d_p to d_{p^i} or the Chinese remainder theorem to compute d_n where n is a product of lucky primes. We have lifted high enough when p^i (respectively n) is larger than all of the coefficients of d. Since the primes used were lucky only with high probability, it is necessary to check the result to determine if it is the correct GCD. This is an easy computation. If d_{p^i} (respectively d_n) divides both f and g, then this together with the fact that $\deg(d_p) = \deg(d_{p^i}) = \deg(d_n)$ can only be larger than the degree of d implies that what we have computed is indeed the correct GCD.

There are three key steps in the modular GCD algorithms presented above.

Step 1. Find a lucky prime with high probability.

Step 2. Use a Hensel algorithm or the Chinese remainder theorem to lift d_p.

Step 3. Check the result.

The goal of this paper is to generalize the p-adic method and the Chinese remainder method for computing GCD's to a p-adic method and Chinese remainder method for computing Gröbner bases. Winkler (1987) effectively has Step two for a p-adic Gröbner basis algorithm. In this paper, we improve and simplify the lifting in Winkler's Step two, and add a Step one and three leading to an implementable p-adic algorithm for computing Gröbner bases. We add the same Step one and three to the basic Step two Chinese remainder algorithm for a fast and deterministic Chinese remainder algorithm for computing Gröbner bases.

5. Step one: lucky primes for Gröbner basis calculations

First we must define what is meant by "lucky" prime in Gröbner basis calculations. Let $I = \langle f_1, \ldots, f_r \rangle$ be an ideal in $\mathbb{Q}[X]$. We scale appropriately so that each f_i is in $\mathbb{Z}[X]$ and each f_i is primitive. We consider the ideal $I_p = \langle \overline{f_1}, \ldots, \overline{f_r} \rangle \subseteq \mathbb{Z}_p[X]$. Let G be the reduced Gröbner basis for I and G_p be the reduced Gröbner basis for I_p. Roughly speaking, a lucky prime is one for which we do not lose too much algebraic information about the ideal $I \subseteq \mathbb{Q}[X]$ when we consider the ideal $I_p \subseteq \mathbb{Z}_p[X]$. For the lifting method presented in this paper, the algebraic information about I that we need to preserve modulo p is the set of leading terms of G. So we have the following definition.

Definition 5.1. A prime integer, p, is called *lucky* for I if and only if $\mathrm{Lp}(G) = \mathrm{Lp}(G_p)$.

Using this definition, we cannot determine whether or not a prime is lucky without computing the actual Gröbner basis for I. We would like to be able to compare two primes, p and q, for relative luckiness, just as in the GCD case. Unfortunately, it is impossible to compare $\mathrm{Lp}(G_p)$ and $\mathrm{Lp}(G_q)$ and determine which of the primes p or q is unlucky. We need another definition of "lucky" prime. Knowledge of the Hilbert function has proved to be useful in Gröbner basis computations (Traverso, 1997), so we next consider the Hilbert function.

5.1. Hilbert lucky primes

In the GCD algorithm, it is the degree of the GCD that allows us to compare primes. Let $I \subseteq \mathbb{Q}[X]$ be a homogeneous ideal. Let $I[n]$ denote the set of polynomials in I of degree n. Then $I[n]$ is a vector space over $\mathbb{Q}$. The Hilbert function of $\mathbb{Q}[X]/I$ is a numerical function $HF_I : \mathbb{N} \longrightarrow \mathbb{N}$ such that $HF_I(n) = \dim_{\mathbb{Q}}(\mathbb{Q}[X][n]/I[n])$. As it turns out, the Hilbert function of $\mathbb{Q}[X]/I$ is the corresponding notion to the degree of the GCD that we seek. We now define the following:

Definition 5.2. A prime p is called *Hilbert lucky* for $I \subseteq \mathbb{Q}[X]$ if and only if $HF_I = HF_{I_p}$.

The following theorem allows us to compare two primes for relative Hilbert luckiness. We see that just like the degree of the GCD, the Hilbert function can only "go up" modulo a prime p.

Theorem 5.3. *For every degree, n, $HF_I(n) \leq HF_{I_p}(n)$.*

In order to prove Theorem 5.3, we need to relate the two ideals, I and I_p. Since there is no clear way to compare them directly, we define another ideal in yet another ring which will serve as a link. Let $J = \langle f_1, \ldots, f_r \rangle$ be the ideal in $\mathbb{Z}[X]$ where $f_1, \ldots, f_r$ are the same generators as in I. Now $I_p \equiv J \mod p$ and $J \subseteq I$ as sets of polynomials.

Proof (Theorem 5.3). Let $I[n]$ (respectively $J[n]$, $I_p[n]$) denote the set of polynomials in I (respectively J, I_p) of degree n, and note that $I[n]$ (respectively $I_p[n]$) is a vector space over $\mathbb{Q}$ (respectively $\mathbb{Z}_p$). $\mathbb{Z}[X][n]$ is a free abelian group of rank $\gamma = \binom{n+\nu-1}{\nu-1}$ (see Eisenbud, 1995, Section 1.9).

Note that $HF_I(n) = \dim_{\mathbb{Q}}(\mathbb{Q}[X][n]) - \dim_{\mathbb{Q}}(I[n])$ and $HF_{I_p}(n) = \dim_{\mathbb{Z}_p}(\mathbb{Z}_p[X][n]) - \dim_{\mathbb{Z}_p}(I_p[n])$. Since $\dim_{\mathbb{Q}}(\mathbb{Q}[X][n]) = \dim_{\mathbb{Z}_p}(\mathbb{Z}_p[X][n])$, to show that $HF_I(n) \leq HF_{I_p}(n)$, it suffices to show that $\dim_{\mathbb{Q}}(I[n]) \geq \dim_{\mathbb{Z}_p}(I_p[n])$. We do this by showing that

$$\dim_{\mathbb{Q}}(I[n]) = \operatorname{rank}_{\mathbb{Z}}(J[n]) \geq \dim_{\mathbb{Z}_p}(I_p[n]).$$

To see this, let $\{f'_1, \ldots, f'_{i_n}\}$ be a $\mathbb{Z}$-basis for $J[n]$. For every $f \in I$, there exists a $c \in \mathbb{Z}$ such that $cf \in J$. Hence $\{f'_1, \ldots, f'_{i_n}\}$ is a $\mathbb{Q}$-basis for $I[n]$, and therefore $\dim_{\mathbb{Q}}(I[n]) = \operatorname{rank}_{\mathbb{Z}}(J[n])$. Since $I_p \equiv J \mod p$, we can show that $\{\overline{f'_1}, \ldots, \overline{f'_{i_n}}\}$ still generate $I_p[n]$ and hence $\operatorname{rank}_{\mathbb{Z}}(J[n]) \geq \dim_{\mathbb{Z}_p}(I_p[n])$. □

To determine the relative Hilbert luckiness of the primes p and q, we compare the Hilbert functions of I_p and I_q. If, for some degree n, we have that $HF_{I_p}(n) < HF_{I_q}(n)$, then we discard q as unlucky. We will see from Theorem 5.13 that there are only a finite number of Hilbert unlucky primes, hence we can find a Hilbert lucky prime with high probability. We note that HF_{I_p} is easily computed from the Gröbner basis, G_p.

As a corollary to Theorem 5.3, we get a complete characterization of Hilbert unlucky primes.

Corollary 5.4. *By the fundamental theorem for finitely generated abelian groups we can write* $\mathbb{Z}[X][n]/J[n] \cong \mathbb{Z}^{r^{(n)}} \oplus \mathbb{Z}_{d_1^{(n)}} \oplus \mathbb{Z}_{d_2^{(n)}} \oplus \cdots \oplus \mathbb{Z}_{d_{s_n}^{(n)}}$, *where* $r^{(n)} \geq 0, d_i \geq 2$ *and* $d_{i+1}^{(n)} \mid d_i^{(n)}$ *for every* $i = 1, \ldots, s_n - 1$. *The Hilbert unlucky primes are precisely the prime divisors of the elements of* $d_1^{(n)}$.

Proof. The free rank of $\mathbb{Z}[X][n]/J[n]$ is equal to $r^{(n)}$. From the previous theorem, we have that $r^{(n)} = \gamma - \text{rank}_{\mathbb{Z}}(J[n]) = \gamma - \dim_{\mathbb{Q}}(I[n]) = HF_I(n)$. If p is a Hilbert unlucky prime, then we must have that $HF_{I_p}(n) > r^{(n)}$ for some n. Since $\mathbb{Z}[X][n]/J[n] \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathbb{Z}_p[X][n]/I_p[n]$, we get $\mathbb{Z}_p[X][n]/I_p[n] = (\mathbb{Z}^{r^{(n)}} \otimes_{\mathbb{Z}} \mathbb{Z}_p) \oplus (\mathbb{Z}_{d_1^{(n)}} \otimes_{\mathbb{Z}} \mathbb{Z}_p) \oplus \cdots \oplus (\mathbb{Z}_{d_{s_n}^{(n)}} \otimes_{\mathbb{Z}} \mathbb{Z}_p)$. If p divides $d_j^{(n)}$, then $\mathbb{Z}_{d_j^{(n)}} \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathbb{Z}_p$. In order for $HF_{I_p}(n)$ to be greater than $r^{(n)}$, we must have the free part of $\mathbb{Z}_p[X][n]/I_p[n]$ to have rank greater than $r^{(n)}$. This will happen if and only if p divides one of the $d_j^{(n)}$'s. □

In the following theorem, we get another very useful characterization of Hilbert unlucky primes.

Theorem 5.5. *p is Hilbert unlucky if and only if there exists a p-torsion element of $\mathbb{Z}[X]/J$.*

Proof. Let $f + J$ be a p-torsion element of $\mathbb{Z}[X]/J$. Since J is homogeneous, we can assume f is homogeneous, say, of degree n. So $f + J[n]$ is a p-torsion element of $\mathbb{Z}[X][n]/J[n]$. We write $\mathbb{Z}[X][n]/J[n] \cong \mathbb{Z}^r \oplus \mathbb{Z}_{d_1^{(n)}} \oplus \mathbb{Z}_{d_2^{(n)}} \oplus \cdots \oplus \mathbb{Z}_{d_{s_n}^{(n)}}$ as in Corollary 5.4. Since there exists a p-torsion element of $\mathbb{Z}[X][n]/J[n]$, we must have that p divides $d_1^{(n)}$. Hence p is Hilbert unlucky by Corollary 5.4.

Conversely, by Corollary 5.4, since p is Hilbert unlucky, p divides $d_1^{(n)}$ for some n where $\mathbb{Z}[X][n]/J[n] \cong \mathbb{Z}^r \oplus \mathbb{Z}_{d_1^{(n)}} \oplus \cdots \oplus \mathbb{Z}_{d_s^{(n)}}$. Therefore, there exists an element in $\mathbb{Z}[X]/J$ of degree n which is p-torsion. □

The Hilbert function corresponds with the degree of the GCD in that it can only "go up" modulo a prime p. But when we extend a unimodular GCD algorithm to a Gröbner basis algorithm, we must take term order into account. It is quite possible for a prime to be Hilbert lucky, but unlucky as we have defined it in Definition 5.1 (see Section 8).

5.2. Lucky primes

Once we have found a Hilbert lucky prime with high probability, we still need to find a lucky prime, one that will give the correct leading power products in G_p.

Let $G = \{g_1, \ldots, g_t\}$ and $G_p = \{g'_1, \ldots, g'_{t_p}\}$ be reduced Gröbner bases for I and I_p, respectively, ordered by increasing leading power products, and let $G_{\mathbf{Z}} = \{h_1, \ldots, h_s\}$ be a minimal strong Gröbner basis for J ordered in the same way.

Theorem 5.6. *For a Hilbert lucky prime, p, we have* $\text{lp}(g'_1) \leq \text{lp}(g_1)$. *Furthermore, if* $\text{lp}(g_j) = \text{lp}(g'_j)$ *for* $1 \leq j \leq i$, *then* $\text{lp}(g'_{i+1}) \leq \text{lp}(g_{i+1})$.

Proof. First we will show that $\mathrm{lp}(g_1') \leq \mathrm{lp}(g_1)$ by considering $G_{\mathbb{Z}}$. Since $\mathrm{Lp}(I) = \mathrm{Lp}(J)$ and $\mathrm{lp}(g_1)$ and $\mathrm{lp}(h_1)$ are both least in G and $G_{\mathbb{Z}}$, respectively, we must have that $\mathrm{lp}(h_1) = \mathrm{lp}(g_1)$. Now we consider $\overline{h_1} \in I_p$. If $\overline{h_1} = 0$, then $h_1 = pf$, for $f \in \mathbb{Z}[x]$. If $f \in J$, then since $G_{\mathbf{Z}}$ is a strong Gröbner basis, there exists $h_i \in G_{\mathbf{Z}}$ such that $\mathrm{lt}(h_i) \mid \mathrm{lt}(f)$. But then $\mathrm{lp}(h_i) \mid \mathrm{lp}(h_1) = \mathrm{lp}(f)$. Since $\mathrm{lp}(h_1)$ is least, we must have that $h_i = h_1$. This is a contradiction, since $\mathrm{lc}(h_1)$ cannot divide $\mathrm{lc}(f)$. Therefore, f cannot be in J. But if $f \notin J$, then $f + J$ is a p-torsion element of $\mathbb{Z}[x]/J$ contradicting the fact that p is Hilbert lucky (Theorem 5.5). So $\overline{h_1} \neq 0$. Since $\overline{h_1} \in I_p$, there exists a $g_j' \in G_p$ such that $\mathrm{lp}(g_j') \mid \mathrm{lp}(\overline{h_1})$. So we have $\mathrm{lp}(g_1') \leq \mathrm{lp}(g_j') \leq \mathrm{lp}(\overline{h_1}) \leq \mathrm{lp}(h_1) = \mathrm{lp}(g_1)$. Therefore $\mathrm{lp}(g_1') \leq \mathrm{lp}(g_1)$.

Now assume that $\mathrm{lp}(g_j) = \mathrm{lp}(g_j')$ for $1 \leq j \leq i$. We will show that $\mathrm{lp}(g_{i+1}') \leq \mathrm{lp}(g_{i+1})$. Let $c \in \mathbb{Z}$ be such that $cg_{i+1} \in J$. Suppose that $\overline{cg_{i+1}} \neq 0$. Then there exists $g_j' \in G_p$ such that $\mathrm{lp}(g_j') \mid \mathrm{lp}(\overline{cg_{i+1}})$. If $j \leq i$, then we get $\mathrm{lp}(g_j') = \mathrm{lp}(g_j) \mid \mathrm{lp}(\overline{cg_{i+1}})$. But then $\mathrm{lp}(g_j)$ divides a term of g_{i+1}, a contradiction to the fact that G is a reduced Gröbner basis for I. So we must have that $j > i$ which implies that $\mathrm{lp}(g_{i+1}') \leq \mathrm{lp}(g_j') \leq \mathrm{lp}(\overline{cg_{i+1}}) \leq \mathrm{lp}(g_{i+1})$ as desired. Now suppose $\overline{cg_{i+1}} = 0$. Then $cg_{i+1} = p^\alpha h$, where $h \in \mathbb{Z}[x]$, $\alpha \geq 1$ and $\overline{h} \neq 0$. Since $p^\alpha h \in J$, if $h \notin J$, then $h + J$ is a p-torsion element of $\mathbb{Z}[x]/J$, contradicting the fact that p is Hilbert lucky (Theorem 5.5). So we have that $h \in J$. Since $\overline{h} \neq 0$, we are in the same situation as above. There exists $g_j' \in G_p$ such that $\mathrm{lp}(g_j') \mid \mathrm{lp}(\overline{h})$. If $j \leq i$, then $\mathrm{lp}(g_j') = \mathrm{lp}(g_j) \mid \mathrm{lp}(\overline{h})$. Since h and g_{i+1} have the same power products, we get a contradiction to the fact that G is a reduced Gröbner basis. Otherwise $j > i$ which implies that $\mathrm{lp}(g_{i+1}') \leq \mathrm{lp}(g_j') \leq \mathrm{lp}(\overline{cg_{i+1}}) \leq \mathrm{lp}(g_{i+1})$. □

Now we can use Theorem 5.6 to compare two primes for luckiness. If two primes p and q generate the same Hilbert function, then we compare the leading terms of G_p and G_q, in increasing order. If, in the first place where the leading terms differ, the leading term in G_p is smaller than the leading term in G_q, we know that p must be unlucky, since by Theorem 5.6, leading terms only "go down" modulo a prime. Note that we can only determine that p is unlucky. We still cannot determine whether or not the prime q is lucky.

Checking that p is Hilbert lucky before comparing leading terms is crucial as the following example shows.

Example 5.7. Let $I = \langle 3y^2x - 5yx^2 + 2x^3, -7y^3x + 5y^2x^2, 7y^6 - 2y^3x^3 + yx^5\rangle \subseteq \mathbb{Q}[y, x]$. Using the degree lexicographical ordering with $y > x$, 5 is a lucky prime, hence Hilbert lucky. $\mathrm{Lp}(G_5) = \{y^2x, yx^3, x^5, y^6\}$. The prime 2 is Hilbert unlucky. $\mathrm{Lp}(G_2) = \{y^2x, y^6\}$. If we were comparing the leading power products of G_2 with G_5 using Theorem 5.6, we would discard 5 as unlucky, since $y^6 > yx^3$.

5.3. *Other definitions of lucky*

Pauer (1992) defines a prime p to be lucky (denoted in this paper as "Pauer-lucky") if p does not divide a leading coefficient of any polynomial in $G_{\mathbf{Z}}$. He shows that for p a Pauer-lucky prime, then $\mathrm{Lp}(G) = \mathrm{Lp}(G_p)$ (we also prove this in Lemma 6.1). Making use of Hilbert lucky primes, we will show in the next several lemmas and theorems, that the

converse is also true for homogeneous ideals, i.e. that if $\mathrm{Lp}(G) = \mathrm{Lp}(G_p)$ then p does not divide a leading coefficient of any polynomial in $G_{\mathbf{Z}}$. Let $d(G)$ denote the least common multiple of the denominators of the coefficients of polynomials in G.

In Proposition 6.1 Pauer (1992) proves that if p does not divide a leading coefficient of any polynomial in $G_{\mathbf{Z}}$, then p does not divide $d(G)$.

With the addition of a hypothesis about Hilbert lucky primes, we can show the converse of this theorem. First we prove two lemmas.

Lemma 5.8. *Let p be a Hilbert lucky prime such that p does not divide $d(G)$. Then for any $g \in G$, there exists a constant $c \in \mathbb{Z}$ such that $cg \in J \subseteq \mathbb{Z}[X]$ and p does not divide c.*

Proof. We know there exists a constant, $c \in \mathbb{Z}$, such that $cg \in J$. We would like to choose this c such that p does not divide c. Since p does not divide a denominator of any coefficient of g, if p divides c, then p divides cg. So if $p \mid c$, then $cg = p^\alpha f$ where α is maximal in the sense that $f \in \mathbb{Z}[X]$ and p does not divide f. Since g is monic, p^α must divide c. If $f \notin J$, then $p^\alpha f \in J$ implies that $f + J$ is a p-torsion element of $\mathbb{Z}[X]/J$, contradicting the fact that p is Hilbert lucky. Therefore $f \in J$. Now choose $c' = c/p^\alpha$ and get $c'g = f \in J$. If $p \mid c'$, then $p \mid c'g = f$, since g is monic and p does not divide a denominator of a coefficient of g. But p does not divide f, so p cannot divide c'. □

Lemma 5.9. *Let $G_{\mathbf{Z}} = \{h_1, \ldots, h_s\}$ be a minimal strong Gröbner basis for J, and let $f \in J$ such that $\mathrm{lp}(f) = \mathrm{lp}(h_i)$ for some $i \in \{1 \ldots s\}$. Then $\mathrm{lc}(h_i)$ divides $\mathrm{lc}(f)$.*

Proof. Given $f \in J$, since $G_{\mathbf{Z}}$ is a strong Gröbner basis, there exists $h_j \in G_{\mathbf{Z}}$ such that $\mathrm{lt}(h_j) \mid \mathrm{lt}(f)$. Suppose $\mathrm{lp}(f) = \mathrm{lp}(h_i)$. Let $\mathrm{lt}(h_i) = c_i X_i$ and $\mathrm{lt}(h_j) = c_j X_j$. So $X_i = \mathrm{lp}(f)$ and $c_j \mid \mathrm{lc}(f)$. We will show that $c_i \mid c_j$. Then we would have that $c_i \mid \mathrm{lc}(f)$, proving the lemma. Let $c = \gcd(c_i, c_j)$. Then $c = a_i c_i + a_j c_j$ for some $a_i, a_j \in \mathbb{Z}$. Let $h = a_j \frac{X_i}{X_j} h_j + a_i h_i \in J$. Note that $\mathrm{lt}(h) = cX_i$ since $X_j \mid X_i$. Again, since $G_{\mathbf{Z}}$ is a strong Gröbner basis, there exists $h_k \in G_{\mathbf{Z}}$ such that $\mathrm{lt}(h_k) \mid \mathrm{lt}(h) = cX_i$. But $cX_i \mid c_i X_i = \mathrm{lt}(h_i)$, so we get $\mathrm{lt}(h_k) \mid \mathrm{lt}(h_i)$. Since $G_{\mathbf{Z}}$ is a minimal Gröbner basis, we must have that $k = i$. So $\mathrm{lc}(h_i) = c_i \mid c$. Therefore $c = c_i$ and $c_i \mid c_j$. We have now shown that $\mathrm{lc}(h_i)$ divides $\mathrm{lc}(f)$. □

Theorem 5.10. *If a prime p is Hilbert lucky and does not divide $d(G)$, then p does not divide a leading coefficient of any polynomial in $G_{\mathbf{Z}}$.*

Proof. Let h be a polynomial in $G_{\mathbb{Z}}$. We must show that p does not divide $\mathrm{lc}(h)$. Since h is also in I, there exists a $g_i \in G$ such that $\mathrm{lp}(g_i)$ divides $\mathrm{lp}(h)$. By Lemma 5.8, we can choose a $c \in \mathbb{Z}$ such that $cg_i \in J$ and p does not divide c. Since g_i is monic, we also have that p does not divide cg_i. Let X be a monomial such that $\mathrm{lp}(h) = \mathrm{lp}(cXg_i)$. Since h is in the strong Gröbner basis for J, by Lemma 5.9, we must have that $\mathrm{lt}(h)$ divides $\mathrm{lt}(cXg_i)$ by Lemma 5.9. Since p does not divide $\mathrm{lc}(cXg_i) = c$, p cannot divide $\mathrm{lc}(h)$. □

The following theorem shows where we find the Hilbert lucky primes that are not lucky. These primes depend on the term order chosen.

Theorem 5.11. *If a prime p is Hilbert lucky, but not lucky, then p must divide $d(G)$.*

Proof. Let G and G_p be ordered by increasing leading power products. Suppose to the contrary that p does not divide $d(G)$. We will show that p is either Hilbert unlucky or p is lucky. If p is Hilbert unlucky, then we are done. So assume that p is Hilbert lucky. We need to show that p is lucky. Let $g_1 \in G$. By Lemma 5.8 choose a $c \in \mathbb{Z}$ such that $cg_1 \in J$ and p does not divide c. Now $\overline{cg_1} \in I_p$ and $\mathrm{lp}(\overline{cg_1}) = \mathrm{lp}(g_1)$. There exists a $g_i' \in G_p$ such that $\mathrm{lp}(g_i') \mid \mathrm{lp}(\overline{cg_1})$. Since p is Hilbert lucky, we cannot have $\mathrm{lp}(g_i') < \mathrm{lp}(g_1)$. Therefore, $\mathrm{lp}(g_i') = \mathrm{lp}(g_1)$. Since g_i' is least in G_p, we must have $i = 1$. Now we assume that $\mathrm{lp}(g_j) = \mathrm{lp}(g_j') \in \mathrm{Lp}(G_p)$ for $1 \le j \le i-1$. Again by Lemma 5.8, there exists a $c_i \in \mathbb{Z}$ such that $c_i g_i \in J$ and p does not divide c_i. We know that $\overline{cg_i} \in I_p$ and $\mathrm{lp}(\overline{cg_i}) = \mathrm{lp}(g_i)$. So there exists $g_l' \in G_p$ such that $\mathrm{lp}(g_l') \mid \mathrm{lp}(\overline{cg_i}) = \mathrm{lp}(g_i)$. If $\deg(g_l') < \deg(g_i)$, then since $\mathrm{lp}(g_j) = \mathrm{lp}(g_j')$ for $1 \le j \le i-1$, for $n = \deg(g_l')$, we would have $HF_{I_p}(n) > HF_I(n)$ contradicting the fact that p is Hilbert lucky. Hence $\mathrm{lp}(g_l') = \mathrm{lp}(g_i) \in \mathrm{Lp}(G_p)$. For every i we can find a g_l' such that $\mathrm{lp}(g_l') = \mathrm{lp}(g_i) \in \mathrm{Lp}(G_p)$. Therefore, we have shown that $\mathrm{Lp}(G) \subseteq \mathrm{Lp}(G_p)$. Since p is Hilbert lucky, this cannot be a strict containment. Hence $\mathrm{Lp}(G) = \mathrm{Lp}(G_p)$, and p is lucky. □

Finally, we have the following theorem.

Theorem 5.12. *If p is a lucky prime, then p does not divide $d(G)$.*

Proof. Suppose to the contrary that p divides the denominator of a coefficient of a polynomial in G. We will show that p is not lucky. If p is Hilbert unlucky, then p is not lucky and we are done. So assume that p is Hilbert lucky. Now suppose p divides the denominator of a coefficient of $g \in G$. Choose c such that $cg \in J$. Since g is monic, and p divides a denominator of a coefficient of g, p must also divide c. If $\overline{cg} \neq 0$, then $\overline{cg} \in I_p$ and $\mathrm{lp}(\overline{cg}) < \mathrm{lp}(g)$. Now $\mathrm{lp}(\overline{cg})$ is in $\mathrm{Lp}(I_p)$, but it is also a power product in $g \in G$. Since G is a *reduced* Gröbner basis of I, $\mathrm{lp}(\overline{cg})$ cannot be in $\mathrm{Lp}(I)$. So, $\mathrm{Lp}(I_p) \neq \mathrm{Lp}(I)$, implying that p is not lucky. Now assume that $\overline{cg} = 0$. Then we can write $cg = p^\alpha f$ for $f \in \mathbb{Z}[X]$ and α is such that p does not divide f. If $f \notin J$, then $f + J$ is a p-torsion element of $\mathbb{Z}[X]/J$ contradicting the fact that p is Hilbert lucky. If $f \in J$, then we are in the same situation as when $\overline{cg} \neq 0$. We have $\overline{f} \in I_p$. Since p divides a denominator of g, then p must also divide $\mathrm{lc}(f)$, since g_i is monic. So $\mathrm{lp}(\overline{f}) < \mathrm{lp}(g_i)$. Now $\mathrm{lp}(\overline{f}) \in \mathrm{Lp}(I_p)$, but $\mathrm{lp}(\overline{f})$ is also a power product in $g_i \in G$. Since G is a *reduced* Gröbner basis of I, $\mathrm{lp}(\overline{f})$ cannot be in $\mathrm{Lp}(I)$. So, $\mathrm{Lp}(I_p) \neq \mathrm{Lp}(I)$, implying that p is not lucky. □

Combining the previous theorems, we now have a complete characterization of lucky primes.

Theorem 5.13. *The following statements are equivalent for a prime, p:*

1. *p is lucky.*
2. *p does not divide a leading coefficient of any polynomial in $G_{\mathbf{Z}}$ (Pauer-lucky).*
3. *p is Hilbert lucky and does not divide $d(G)$.*

6. Step two: lifting of G_p

6.1. p-Adic lifting

First we discuss a p-adic algorithm which uses Hensel lifting techniques. Let $I_{p^i} = \langle \overline{f_1}, \ldots, \overline{f_r} \rangle \subseteq \mathbb{Z}_{p^i}[X]$. The following result is also proved by Pauer (1992) in Proposition 4.1, but we give an alternate proof using the techniques that we have developed so far.

Lemma 6.1. *Let $G_{\mathbb{Z}} = \{h_1, h_2, \ldots, h_s\}$ be a minimal strong $\mathbb{Z}$-Gröbner basis for $J \subseteq \mathbb{Z}[X]$. Let p be a lucky prime. Then $\overline{G_{\mathbb{Z}}} = \{\overline{h_1}, \ldots, \overline{h_s}\}$ is a Gröbner basis for I_{p^i}, although not necessarily reduced.*

Proof. Clearly since $G_{\mathbb{Z}} = \{h_1, h_2, \ldots, h_s\}$ generates J, $\overline{G_{\mathbb{Z}}} = \{\overline{h_1}, \ldots, \overline{h_s}\}$ generates $I_{p^i} \equiv J \bmod p^i$. Since p is lucky, by Theorem 5.13, p does not divide a leading coefficient of any $h_i \in G_{\mathbf{Z}}$. Therefore $\mathrm{Lp}(J) \subseteq \mathrm{Lp}(I_{p^i})$. Let f be a primitive polynomial (in the sense that if $f = ch$, for $c \in \mathbb{Z}$, then h is not in J) in I_{p^i}. We will show that $\mathrm{lt}(f) \in \mathrm{Lt}(\overline{G_{\mathbf{Z}}})$. Since $f \in I_{p^i}$, there exists an $F \in J$ such that $\overline{F} = f$. If $\mathrm{lp}(f) = \mathrm{lp}(F)$, then, since $G_{\mathbb{Z}}$ is a strong Gröbner basis, there exists a j, such that $\mathrm{lp}(h_j)$ divides $\mathrm{lp}(F) = \mathrm{lp}(f)$. Since p does not divide $\mathrm{lc}(h_j)$, we know that $\mathrm{lc}(h_j)$ is a unit in $\mathbb{Z}_{p^i}$. Hence $\mathrm{lt}(f)$ is divisible by $\mathrm{lt}(\overline{h_j})$ and $\mathrm{lt}(f) \in \mathrm{Lt}(\overline{G_{\mathbf{Z}}})$. If $\mathrm{lp}(f) \neq \mathrm{lp}(F)$, and $\mathrm{lp}(f)$ is not in $\mathrm{Lp}(J) = \mathrm{Lp}(I)$, then $\mathrm{Lp}(J)$ is a proper subset of $\mathrm{Lp}(I_{p^i})$. But then $\mathrm{rank}_{\mathbb{Z}}(J[n]) \neq \mathrm{rank}_{\mathbb{Z}_{p^i}}(I_{p^i}[n])$ for $n = \deg(f)$. Using the same reasoning as in the proof of Theorem 5.3, this implies that p is Hilbert unlucky and hence unlucky, which is a contradiction. Therefore $\mathrm{Lp}(J) = \mathrm{Lp}(I_{p^i})$. Since p is lucky, we know that $\mathrm{lp}(h_i) = \mathrm{lp}(\overline{h_i})$ for every i. Since $\mathrm{lc}(\overline{h_i})$ is monic and $\mathrm{Lt}(G_{\mathbf{Z}}) = \langle \mathrm{lt}(h_1), \ldots, \mathrm{lt}(h_s) \rangle$, we get that $\mathrm{Lt}(I_{p^i}) = \langle \mathrm{lt}(\overline{h_1}), \ldots, \mathrm{lt}(\overline{h_s}) \rangle$. Hence $\overline{G_{\mathbb{Z}}}$ is a Gröbner basis for I_{p^i}. □

Note that the proof of Lemma 6.1 tells us that I_{p^i} has a monic Gröbner basis. Recall from Section 3 that if a monic Gröbner basis exists, then we can find a monic reduced Gröbner basis for I_{p^i} that is unique. We denote by $G_{p^i} = \{g_1^{(i)}, \ldots, g_{t_i}^{(i)}\}$, the monic reduced Gröbner basis for $I_{p^i} \subseteq \mathbb{Z}_{p^i}[X]$.

By definition, for a lucky prime p, we have that $\mathrm{Lp}(G) = \mathrm{Lp}(G_p)$. By Lemma 6.1, we also have that $\mathrm{Lp}(G) = \mathrm{Lp}(G_{p^i})$.

Theorem 6.2. *Let $G = \{g_1, g_2, \ldots, g_t\}$ be the reduced Gröbner basis for $I \subseteq \mathbb{Q}[X]$, and let p be a lucky prime. Then $\overline{G} = \{\overline{g_1}, \overline{g_2}, \ldots, \overline{g_t}\} \subseteq \mathbb{Z}_{p^i}[X]$ is the reduced Gröbner basis for I_{p^i}. That is to say $\overline{G} = G_{p^i}$ in $\mathbb{Z}_{p^i}[X]$.*

Proof. Let $G_{p^i} = \{g_1^{(i)}, \ldots, g_t^{(i)}\}$ be the unique monic reduced Gröbner basis for $I_{p^i} \subseteq \mathbb{Z}_{p^i}[X]$. We order G and G_{p^i} by increasing leading power products. First we show that $\overline{g_j} \in I_{p^i}$. Then we show that $\overline{g_j} = g_j^{(i)}$ for $j \in \{1, \ldots, t\}$.

Let $g_j \in G$. By Lemma 5.8, choose $c_j \in \mathbb{Z}$ such that $c_j g_j \in J$ and p does not divide c_j. Since $I_{p^i} = \overline{J}$ in $\mathbb{Z}_{p^i}[X]$, we have that $\overline{c_j g_j} \in I_{p^i}$. Since c_j is invertible in $\mathbb{Z}_{p^i}$, we get

$\overline{c_j}^{-1}\overline{c_j g_j} \equiv \overline{g_j} \in I_{p^i}$ for every $j \in \{1, \ldots, t\}$. From the fact that G is monic, we know that $\mathrm{Lp}(\overline{G}) = \mathrm{Lp}(G) = \mathrm{Lp}(G_{p^i})$.

Now we have that $\overline{g_j} \in I_{p^i}$ and $\mathrm{lp}(\overline{g_j}) = \mathrm{lp}(g_j^{(i)})$ for every j. Consider $g_j^{(i)} - \overline{g_j} \in I_{p^i}$. $\mathrm{lp}(g_j^{(i)} - \overline{g_j}) < \mathrm{lp}(g_j^{(i)})$. In fact, $\mathrm{lp}(g_j^{(i)} - \overline{g_j})$ is a power product in either g_j or $g_j^{(i)}$ (or 0). Since both $g_j^{(i)}$ and $\overline{g_j}$ are reduced with respect to $\mathrm{Lp}(I_{p^i}) = \mathrm{Lp}(I)$, we must have that $g_j^{(i)} - \overline{g_j} = 0 \in I_{p^i}$. Hence $g_j^{(i)} = \overline{g_j}$, and we have shown that $\overline{G} = G_{p^i}$ in $\mathbb{Z}_{p^i}[X]$. □

6.2. *Lifting G_p to $G^{(i)}$*

Now we present a method for lifting G_p, the reduced Gröbner basis for $I_p \subseteq \mathbb{Z}_p[X]$, to G_{p^i}, the monic reduced Gröbner basis for $I_{p^i} \subseteq \mathbb{Z}_{p^i}[X]$.

Assuming that we have a lucky prime p, we first compute G_p. We view G_p and $F = \{f_1, \ldots, f_r\}$ as column matrices and compute the transformation matrix $Z^{(1)}$ with entries in $\mathbb{Z}_p[X]$ such that

$$Z^{(1)}F \equiv G_p \mod p. \tag{1}$$

For each i, we need to find matrices $Z^{(i)}$ and $G^{(i)}$ with entries in $\mathbb{Z}_{p^i}[X]$ such that

$$Z^{(i)}F \equiv G^{(i)} \mod p^i \qquad \text{and} \qquad G^{(i)} \equiv G_p \mod p$$

from which we can compute $G_{p^{i-1}}$, the monic reduced Gröbner basis for I_{p^i}.

This is done by induction. For $i = 1$, we have $Z^{(1)}$ and G_p in Eq. (1). Given $Z^{(i-1)}$ and $G_{p^{i-1}}$, we first compute matrices, Z' and G' such that

$$Z^{(i)} = Z^{(i-1)} + p^{i-1}Z' \tag{2}$$

and

$$G^{(i)} = G_{p^{i-1}} + p^{i-1}G' \tag{3}$$

where

$$Z^{(i)}F \equiv G^{(i)} \mod p^i. \tag{4}$$

To do this, we need to solve the following congruence obtained by substituting Eqs. (2) and (3) into (4).

$$(Z^{(i-1)} + p^{i-1}Z')F \equiv G_{p^{i-1}} + p^{i-1}G' \mod p^i \tag{5}$$

for Z' and G'.

One solution to Eq. (5) is $Z' = \mathbf{0}$, $G' = \frac{1}{p^{i-1}}(Z^{(i-1)}F - G_{p^{i-1}})$. However, we want $G_{p^{i-1}} + p^{i-1}G'$ to be the reduced monic Gröbner basis for I_{p^i}. We use the following technique of Pauer (1992) to obtain the correct power products in G'. We use G_p to reduce G' to a set of polynomials, G'', such that $\mathrm{pp}(G'' \bigcap \mathrm{Lp}(G_p) = \emptyset)$. Let M be the matrix of polynomials used in this reduction. So $G' = MG_p + G''$. Let $Z'' = Z' - MZ^{(1)}$, where $Z^{(1)}$ is as in Eq. (1). Then (Z'', G'') is also a solution to Eq. (5).

Now we show that $G^{(i)} = G_{p^{i-1}} + p^{i-1}G'$ is equal to G_{p^i}, the monic reduced Gröbner basis of I_{p^i}. By construction, we have that $Z^{(i)}F \equiv G^{(i)} \mod p^i$, so $G^{(i)} \subseteq I_{p^i}$. Since p is lucky, $\mathrm{Lp}(G^{(i)}) = \mathrm{Lp}(G_p) = \mathrm{Lp}(G_{p^i})$. Let $\tilde{g} \in G^{(i)}$ and $g' \in G_{p^i}$ such that $\mathrm{lp}(\tilde{g}) = \mathrm{lp}(g')$. Consider $\tilde{g} - g' \in I_{p^i}$. The leading power product of $\tilde{g} - g'$ is strictly less than $\mathrm{lp}(\tilde{g}) = \mathrm{lp}(g')$, and is, hence, one of the lower power products of either $\tilde{g}$ or g'. But both $\tilde{g}$ and g' are reduced with respect to $\mathrm{Lp}(G_p) = \mathrm{Lp}(G_{p^i})$. Therefore, $\tilde{g} - g' = 0$ and $G^{(i)} = G_{p^i}$ in I_{p^i}. So at the ith stage of Step 2, the lifting algorithm computes the reduced monic Gröbner basis of I_{p^i}.

The Farey rational numbers $\mathcal{F}_{p,N} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, |a| \leq N, 1 \leq b \leq N, \gcd(a,b) = 1, \gcd(b,p) = 1\}$ can be used to recover the rational coefficients of G from the $\mathbb{Z}_{p^i}$ coefficients of G_{p^i} (Kornerup and Gregory, 1983). The Farey rational map $\phi : \mathcal{F}_{p,N} \longmapsto \mathbb{Z}_{p^i}$ is one to one if $N \leq \sqrt{p^i/2}$. Let N be a bound on the numerators and denominators of the coefficients of G. Then we can lift G_p to G_{p^i} where i is such that $N \leq \sqrt{p^i/2}$, and pull the coefficients of G_{p^i} back to their unique pre-images in $\mathcal{F}_{p,N} \subseteq \mathbb{Q}$, which are the coefficients of G by Theorem 6.2.

If we knew a bound on the size numerators and denominators of the coefficients of G, we would know when to terminate the lifting algorithm. However, even if such a bound could be computed, it would most likely be too large to be of any use. Instead, we pull back the coefficients of $G^{(i)}$ to rational coefficients at each lift to obtain $\tilde{G}_i$. We say that the computation "stabilizes" to a Gröbner basis candidate, $\tilde{G}$ if $\tilde{G}_{(i-1)} = \tilde{G}_{(i)}$. Once the computation stabilizes, we perform the check in Step three.

6.3. *Chinese remainder lifting*

Let k be a product of lucky primes, and let p be another lucky prime. In this section we discuss an algorithm that uses the Chinese remainder theorem to form the monic reduced Gröbner basis, G_{kp} for the ideal $I_{kp} = \langle \overline{f_1}, \ldots, \overline{f_r} \rangle \subseteq \mathbb{Z}_{kp}[X]$ from the two Gröbner bases, G_k and G_p. Once we have performed a sufficient number of "lifts" , we can then construct the reduced Gröbner basis, G, for I by pulling back the modular coefficients to rational coefficients using the Farey rational map. We recall the Chinese remainder theorem:

Let m and n be two relatively prime odd integers. Then there is a unique solution modulo mn of the simultaneous congruences $x \equiv a \mod m$ and $x \equiv b \mod n$ where $-mn/2 \leq x \leq mn/2$.

In order to apply the Chinese remainder theorem to the coefficients of G_k and G_p, we need the following theorem.

Theorem 6.3. *For any product of lucky primes $n = \prod p_i$, we have that $G \equiv G_n \mod n$ where G_n is the reduced monic Gröbner basis for I_n.*

The proof of this theorem is just a generalization of the proof that $G \equiv G_p \mod p$ for a prime p and can be found in either Arnold (2000) or Pauer (1992).

Now we apply the Chinese remainder algorithm to the coefficients of the polynomials in G_k and G_p to get a new set of polynomials, $G^{(kp)}$, with coefficients in $\mathbb{Z}_{kp}$. By construction, $G^{(kp)}$ is congruent to $G_k \mod k$ and $G_p \mod p$. By Theorem 6.3, we also have that G is congruent to $G_k \mod k$ and $G_p \mod p$. Therefore, by the Chinese remainder

theorem, we must have that $G^{(kp)} \equiv G \bmod kp$, and hence $G^{(kp)} = G_{kp}$. As in the p-adic algorithm, we pull back the coefficients of $G^{(kp)}$ after each lift. Once the computation stabilizes, we have a Gröbner basis candidate $\tilde{G} \in \mathbb{Q}[X]$ and we proceed to Step three.

7. Checking the result

In order to show that our Gröbner basis candidate, $\tilde{G}$, is the correct result, we need to carry out two checks. First we need to show that $\tilde{G}$ is a Gröbner basis for the ideal that it generates, $\langle \tilde{G} \rangle$. This can be done by checking that all of the S-polynomials reduce to zero using $\tilde{G}$, avoiding unnecessary reductions using criteria listed in Buchberger (1979) and Gebauer and Möller (1988). Next we must show that $\langle \tilde{G} \rangle = I$. To show that $I \subseteq \langle \tilde{G} \rangle$, we simply show that the generators of I, $f_1, \ldots, f_r$, reduce to zero using $\tilde{G}$. This method, however, will not work for showing that $\langle \tilde{G} \rangle \subseteq I$, since $F = \{f_1, \ldots, f_r\}$ is not a Gröbner basis. In principle, checking that $\langle \tilde{G} \rangle \subseteq I$ is as difficult a problem as computing a Gröbner basis for I. However, keeping the leading power products constant throughout the lifting process eliminates the need to check this second containment.

Theorem 7.1. *Let $\tilde{G} \subseteq \mathbb{Q}[X]$ be a set of polynomials such that $\mathrm{Lp}(\tilde{G}) = \mathrm{Lp}(G_p)$, $\tilde{G}$ is a Gröbner basis for the ideal that it generates, $\langle \tilde{G} \rangle$ and $I \subseteq \langle \tilde{G} \rangle$. Then $I = \langle \tilde{G} \rangle$.*

Proof. $I \subseteq \langle \tilde{G} \rangle$ implies that $HF_{\langle \tilde{G} \rangle} \leq HF_I$. Since $\tilde{G}$ has the same leading terms as G_p, we have that $HF_{\langle \tilde{G} \rangle} = HF_{I_p}$. By Theorem 5.3, we know that $HF_I \leq HF_{I_p}$. So we have $HF_I \leq HF_{I_p} = HF_{\langle \tilde{G} \rangle} \leq HF_I$. Therefore, $HF_{\langle \tilde{G} \rangle} = HF_I$ which, in addition to the fact that $I \subseteq \langle \tilde{G} \rangle$, implies that $\langle \tilde{G} \rangle = I$. □

So, in fact, once we know that $\tilde{G}$ is a Gröbner basis, and that $I \subseteq \langle \tilde{G} \rangle$, we have that $\tilde{G}$ *is* the reduced Gröbner basis for I. Note that this check does not require that p is a lucky prime.

8. Examples

In this section we provide examples on which we time the Chinese remainder and p-adic Gröbner basis algorithms and also current implementations of Buchberger's algorithm in CoCoA, Macaulay 2 and Maple. We have implemented both the Chinese remainder and the p-adic Gröbner basis algorithms using the programming language of the computer algebra package CoCoA (Capani et al., 2001). Timings were conducted on a Pentium III 500 MHz system with 512 MB memory under the Linux operating system. Each of the examples below are ideals in $\mathbb{Q}[x, y, z]$. Gröbner bases are computed using the degree reverse lexicographical ordering with $x > y > z$.

The examples chosen are those for which there is significant growth in the size of the intermediate coefficients, yet the size of the coefficients in the reduced Gröbner basis are moderate. While intermediate coefficient growth is typical in Gröbner basis calculations, moderate coefficients in the final result are not. We summarize the results of the timings in Table 1.

Table 1
Running times in seconds

Ex	PGB	CRGB	CoCoA	M2	Maple
1	151	4.8	11,090	21,611	–
2	1212	33	4,501	1,246	2059
3	484	10.46	16,433	12,078	–

The first example is from the introduction.

Example 8.1.

$$\begin{aligned} f_1 &= 8x^2y^2 + 5xy^3 + 3x^3z + x^2yz \\ f_2 &= x^5 + 2y^3z^2 + 13y^2z^3 + 5yz^4 \\ f_3 &= 8x^3 + 12y^3 + xz^2 + 3 \\ f_4 &= 7x^2y^4 + 18xy^3z^2 + y^3z^3. \end{aligned}$$

Example 8.2.

$$\begin{aligned} f_1 &= 2xy^4z^2 + x^3y^2z - x^2y^3z + 2xyz^2 + 7y^3 + 7 \\ f_2 &= 2x^2y^4z + x^2yz^2 - xy^2z^2 + 2x^2yz - 12x + 12y \\ f_3 &= 2y^5z + x^2y^2z - xy^3z - xy^3 + y^4 + 2y^2z \\ f_4 &= 3xy^4z^3 + x^2y^2z - xy^3z + 4y^3z^2 + 3xyz^3 + 4z^2 - x + y\ . \end{aligned}$$

The Gröbner basis consists of two polynomials:

$$\begin{aligned} g_1 &= x - y \\ g_2 &= y^3 + 1\ . \end{aligned}$$

In the last example, the four generators in $\mathbb{Q}[x, y, z]$ generate the unit ideal.

Example 8.3.

$$\begin{aligned} f_1 &= 5x^3y^2z + 3y^3x^2z + 7xy^2z^2 \\ f_2 &= 3xy^2z^2 + x^5 + 11y^2z^2 \\ f_3 &= 4xyz + 7x^3 + 12y^3 + 1 \\ f_4 &= 3x^3 - 4y^3 + yz^2. \end{aligned}$$

Table 1 compares The Chinese remainder Gröbner basis algorithm, CRGB, and the p-adic algorithm, PGB, with times in seconds for the current implementations of Buchberger's algorithm in CoCoA, Macaulay 2 and Maple. Maple had the system error: "ran out of memory" for Examples 8.1 and 8.3.

9. Conclusions

These initial timings of the modular algorithms indicate that they perform well in examples where intermediate coefficient growth is problematic and the resulting Gröbner basis is relatively simple. While these modular algorithms are not faster than the current

implementations of Buchberger's algorithm in all examples, the striking differences in timing in these particular examples indicate that the modular algorithms deserve more careful consideration.

The modular algorithms that we tested are coded in the high level programming language of CoCoA. We do not present a detailed description of the code here. Some procedures are implemented by built-in functions in CoCoA and others are implemented in interpreted code. A more accurate comparison would be to implement the modular algorithms in a lower level language such as C++. However, it is clear that the Step three checking can become quite expensive. If the resulting Gröbner basis is simple, as in our examples, then the check is inexpensive. This leads us to conclude that the modular algorithms with the Step 3 check would be especially suited for examples where the Gröbner basis is {1}. Another class of examples for which the resulting Gröbner basis is often relatively simple is made up of elimination examples.

Finally, a very interesting question would be to determine which other classes of examples have significant intermediate coefficient growth with relatively simple Gröbner bases. Even if this problem is not solved, it may be possible to start a traditional Buchberger algorithm and then switch to a modular algorithm when intermediate coefficient growth becomes apparent, saving as much of the information as possible.

Acknowledgements

Some of the results in this paper are from my Ph.D. thesis at the University of Maryland. I would like to thank my advisors Drs William W. Adams and Philippe Loustaunau, Antonio Behn for his help with the code, and also an anonymous referee for helpful comments.

References

Adams, W.W., Loustaunau, P., 1994. An Introduction to Gröbner Bases, American Mathematical Society, Providence, RI.

Arnold, E.A., 2000. Computing Gröbner Bases with Hilbert Lucky Primes, Ph.D. Dissertation, University of Maryland, College Park, MD.

Borosh, I., 1966. Exact solutions of linear equations with rational coefficients by congruence techniques. Mathematics of Computation 20, 107–112.

Buchberger, B., 1979. A criterion for detecting unnecessary reductions in the construction of Gröbner-bases, Lecture Notes in Computer Science, vol. 72, pp. 23–21.

Buchberger, B., 1985. Gröbner-bases: an algorithmic method in polynomial ideal theory, In: Multidimensional Systems Theory, pp. 184–232.

Capani, A., Niesi, G., Robbiano, L., 2001. CoCoA, a system for doing Computations in Commutative Algebra. Available via anonymous ftp from cocoa.dima.unige.it, ed. 4.1.

Davenport, J.H., Siret, Y., Tournier, E., 1988. Computer Algebra: Systems and algorithms for algebraic computation, Academic Press.

Ebert, G.L., 1983. Some comments on the modular approach to Gröbner-bases. ACM SIGSAM Bulletin 17, 28–32.

Eisenbud, D., 1995. Commutative Algebra with a view toward Algebraic Geometry, Springer-Verlag.

Gebauer, R., Möller, H.M., 1988. On an installation of Buchberger's algorithm. Journal of Symbolic Computation 6, 275–286.

Gräbe, H., 1994. On lucky primes. Journal of Symbolic Computation 15, 199–209.
Kornerup, P., Gregory, R., 1983. Mapping integers and Hensel codes onto Farey fractions. Bit 23, 9–20.
Grayson, D., Stillman, M., 2000. Macaulay 2, Available via anonymous ftp from ftp.math.uiuc.edu, ed. 0.8.60.
Möller, H.M., Mora, F., 1984. Upper and lower bounds for the degree of Groebner bases, Eurosam '84, Lecture Notes in Computer Science, vol. 174, pp. 172–183.
Pauer, F., 1992. On lucky ideals for Gröbner basis computations. Journal of Symbolic Computation 14, 471–482.
Sasaki, T., Takeshima, T., 1989. A modular method for Gröbner-basis construction over $\mathbb{Q}$ and solving system of algebraic equations. Journal of Information Processing 12, 371–379.
Traverso, C., 1988. Gröbner Trace Algorithms, Proceedings ISSAC '88, Lecture notes in Computer Science, vol. 358, pp. 125–138.
Traverso, C., 1997. Hilbert functions and the Buchberger's algorithm. Journal of Symbolic Computation 22, 355–376.
Winkler, F., 1987. A *p*-adic approach to the computation of Gröbner bases. Journal of Symbolic Computation 6, 287–304.