Gröbner Bases for Binomials with Parametric Exponents

Volker Weispfenning
Fakultät für Mathematik und Informatik
Universität Passau
D-94030 Passau, Germany
e-mail: weispfen@uni-passau.de

MIP-0402
January, 2004

Abstract

We study the uniformity of Buchberger algorithms for computing Gröbner bases with respect to a natural number parameter k in the exponents of the input polynomials. The problem is motivated by positive results of T. Takahashi on special exponential parameter series of polynomial sets in singularity theory. For arbitrary input sets uniformity is in general impossible. By way of contrast we show that the Buchberger algorithm is indeed uniform up to a finite case distinction on the exponential parameter k for inputs consisting of monomials and binomials only. Under this hypothesis the case distinction is algorithmic and partitions the parameter range into Presburger sets. In each case the Buchberger algorithm is uniform and can be described explicitly and algorithmically. In the course of the algorithm the exponential parameter k enters also the coefficients as exponent. Thus the uniformity in k is established with respect to parametric exponents in both terms and coefficients. These results are obtained as a consequence of a much more general theorem concerning Buchberger algorithms for sets of monomials and binomials with arbitrary parametric coefficients and exponents, generalizing the construction of Gröbner systems.

1 Introduction

In July 2003, T. Takahashi, K. Yokoyama at RISC-Linz raised the following problem concerning uniformity of Gröbner bases in exponents: Suppose F is a finite set of multivariate polynomials over a field with the property that some of the exponents of terms occurring in the polynomials in F involve a single natural number parameter k. Fix a term order $<_t$. Is it possible to compute by some "parametric Buchberger algorithm" a Gröbner basis G for the ideal I generated by F and the term oder $<_t$ uniformly in k for large enough values of k? More precisely: Is it possible to split the set $\mathbb{N}$ effectively into finitely many blocks such that for all values of k in a single block B the construction of a Gröbner basis G is uniform in k? In particular the number of polynomials in G and the number of terms in each polynomial should be independent of k for $k \in B$, and the shape of each monomial in these polynomials should be uniform in k.

We will give a positive answer to these problems for sets F of binomials and monomials. In fact our positive answer applies to the much more general case, where all exponents and coefficients in F are parametric. The corresponding construction is a a strong generalization of the construction of a Gröbner system in [9, 12]. For the special problem with a single exponential parameter k posed above, we obtain a much more tangible description of the blocks for k as Presburger sets in $\mathbb{Z}$.

The one parameter problem arose from a number of highly complex computations carried out manually with computer support in [6] for examples arising in the classification of singularities for whole series of input polynomials parametrized by an natural number exponential parameter k. For studying the singularities of these series of polynomials f one considers the polynomial system F consisting of f together with all its partial derivatives. In the partial derivatives the parameter k occurs not only in exponents but also in coefficients. Thus the situation is a strong extension of the situation studies in the theory of comprehensive Gröbner bases.

Even if one starts with the apparently simpler problem, where the parameter k occurs only in the exponent, a Gröbner basis computation will automatically move this parameter also into certain coefficients as an exponential parameter:

Consider the following univariate example: $F = \{X^k - 1, X^2 - 2X\}$. Then the normal form of the first polynomial under complete reduction by the second is $2^{k-1}X - 1$ for $k \geq 2$. A slight variation of this example shows that even in the univariate case we cannot expect that the parameter k occurs only polynomially in exponents of polynomials in a Gröbner basis of the ideal generated by F. Consider the following variant of the example above: $F = \{X^k - 1, X^2 - 2\}$. Then the normal form of the first polynomial under complete reduction by the second is $2^{\lfloor k/2 \rfloor} - 1$ for even $k \geq 2$ and $2^{\lfloor k/2 \rfloor}X - 1$ for odd $k \geq 2$. Thus even for arbitrary large values of k the shape of a Gröbner basis is not uniform in k but depends on the parity of k. Changing the polynomial $X^2 - 2$ to $X^3 - 2$, we see that the shape of a Gröbner basis may depend on the residue class of k wrt. to a fixed integer.

Next we show that the problem has a negative answer in general for polynomials in at least two variables involving at least 3 monomials: Consider the polynomial set $F := \{X^k, X - Y - 1\} \in \mathbb{Q}[X, Y]$ for a natural number parameter k, and let the term order be lexicographic with $X > Y$. Then $G := \{(Y + 1)^k, X - Y - 1\}$ is the reduced Gröbner basis of the ideal I generated by F. Notice that the first polynomial $(Y + 1)^k$ has a number of monomials depending on k; moreover every Gröbner basis of I wrt. the given term order must contain a constant multiple of this polynomial. Thus no such Gröbner basis is of the required form.

The one parameter problem stated above has also been studied in [13]. In contrast to this note Yokoyama's lecture notes concentrate on the case of zero-dimensional polynomial ideals. Thus his results are orthogonal to ours and both supplement each other. The author acknowledges stimulating discussions with Prof. Yokoyama on the problem.

2 Binomials with parametric coefficients and exponents

It is well-known [2] that if I is a polynomial ideal generated by a set F of binomials and monomials, then the reduced Gröbner basis of I wrt. to an arbitrary term order consists also of binomials and monomials. In this section we study the dependence of the basic Buchberger algorithm in a denominator-free version for sets of binomials and monomials on the coefficients and exponents of these objects. It involves two kinds of operations: Formation of s-polynomials and reduction of a polynomial to normal form wrt. a finite given finite set of polynomials. We begin by studying iterated denominator-free reduction chains for binomials and monomials.

We consider formal binomials in indeterminates $X_1, \ldots, X_n$. We use tuple notation $X^f := X_1^{f_1} \cdots X_n^{f_n}$ for terms. For n-tuples of natural numbers $c \leq d$ is the component wise partial order $c_i \leq d_i$ for all $1 \leq i \leq n$. We fix an term order $<_t$ on $\mathbb{N}^n$ refining the partial order $\leq$.

Let $F = a_1X^f + b_1X^e$ and $G = a_2X^d + b_2X^c$ be two binomials with parametric coefficients and exponent-tuples. We assume $f \neq e$, $a_2 \neq 0$ and

$d >_t c$, so that a_2X^d is the highest monomial of G. We do not exclude the possibility that some of the other coefficients a_1, b_1, b_2 are zero; so that F or G may be monomials.

To begin with we consider the case (**case 1**) that all formal coefficients are non-zero, so that both F and G are true binomials.

In case $d \leq f$ and $a_1 \neq 0$ the term X^d divides X^f, and so F is reducible modulo G :

$$\begin{aligned} a_2F \xrightarrow[G]{} F_1 &= a_2F - a_1X^{f-d} \cdot G \\ &= a_2a_1X^f + a_2b_1X^e - a_1a_2X^{d+(f-d)} - a_1b_2X^{c+f-d} \\ &= -a_1b_2X^{f-(d-c)} + a_2b_1X^e \end{aligned}$$

Repeating this step for F_1 - provided the analogous assumptions are still satisfied - yields:

$a_2F_1 \xrightarrow[G]{} F_2 = -a_1b_2^2X^{f-(d-c)-(d-c)} + a_2^2b_1X^e = -a_1b_2^2X^{f-2(d-c)} + a_2^2b_1X^e$

Continuing in this way for m reduction steps - provided all these are possible - yields:

$a_2^mF \xrightarrow[G]{m} F_m = (-1)^{par(m)}a_1b_2^mX^{f-m(d-c)} + a_2^mb_1X^e$

Her $par(m)$ denotes the parity of m. Next suppose m is taken maximal such that this iterated m-step reduction is possible. Then three sub-cases can occur:

1.1 The given reductions never interfere with the second monomial of F_i. Then m is minimal with

$$\begin{aligned} f - m(d-c) \ngeq d \quad &\Leftrightarrow \quad f \ngeq m(d-c) + d \\ &\Leftrightarrow \quad f - d \ngeq m(d-c) \\ &\Leftrightarrow \quad \text{exists } 1 \leq i \leq n \text{ with } d_i > c_i \\ &\qquad \text{and } 0 \leq f_i - d_i < m(d_i - c_i) \\ &\Leftrightarrow \quad \tfrac{f_i-d_i}{d_i-c_i} < m \\ &\Leftrightarrow \quad m = \left\lfloor \tfrac{f_i-d_i}{d_i-c_i} \right\rfloor + 1 \end{aligned}$$

1.2 $m-1$ is maximal such that F_{m-1} is is a true binomial; moreover F_m is a non-zero monomial. This is the case iff the following two conditions hold:

$$\begin{aligned} f - m(d-c) = e \quad &\Leftrightarrow \quad f - e = m(d-c) \\ &\Leftrightarrow \quad \text{for all } 1 \leq i \leq n, \\ &\qquad f_i - e_i = m(d_i - c_i) \\ &\Leftrightarrow \quad \text{for all } 1 \leq i \leq n,\ \tfrac{f_i-e_i}{d_i-c_i} = m \end{aligned} \qquad \text{and}$$

$(-1)^{par(m)}a_1b_2^m \neq a_2^mb_1$

Then the final monomial F_m is:
$[(-1)^{par(m)}a_1b_2^m = a_2^m b_1] \cdot X^e$

1.3 $m-1$ is maximal such that F_{m-1} is is a true binomial; moreover F_m zero. This is the case iff the following two conditions hold:

$$\begin{array}{rcl} f - m(d-c) = e & \Leftrightarrow & f - e = m(d-c) \\ & \Leftrightarrow & \text{for all } 1 \le i \le n, \\ & & f_i - e_i = m(d_i - c_i) \\ & \Leftrightarrow & \text{for all } 1 \le i \le n,\ \frac{f_i - e_i}{d_i - c_i} = m \end{array} \quad \text{and}$$

$$(-1)^{par(m)}a_1b_2^m = a_2^m b_1$$

In sub-cases 1.2 and 1.3 we have in particular for some $1 \le i \le n$ $d_i > c_i$ and $\frac{f_i-e_i}{d_i-c_i} = m > 0$, and so $f_i > e_i$, and hence also $m = \left\lfloor \frac{f_i-e_i}{d_i-c_i} \right\rfloor$.

Next we consider the case (**case 2**) that $b_1 = 0$, i. e. that $F = a_1X^f$ is in fact a monomial. Then iterated m-step reduction modulo of F modulo G yields $a_2^m F \xrightarrow[G]{m} F_m = (-1)^{par(m)}a_1b_2^m X^{f-m(d-c)}$

If m is taken maximal such that an iterated m-step reduction modulo G is possible, then m is minimal such that:

$f - m(d-c) \not\geq d$ (as above in sub-case 1.1) $\Leftrightarrow$ exists $1 \le i \le n$ with $d_i > c_i$ and $m = \left\lfloor \frac{f_i-d_i}{d_i-c_i} \right\rfloor + 1$

The last case (**case 3**) to be considered is that $a_1 \neq 0$ and $b_2 = 0$. So F is a binomial or monomial and $G = a_2X^d$ is a monomial with $d \le f$. Then the reduction of F modulo G yields $a_2F \xrightarrow[G]{1} F_1 = a_2b_1X^e$, which may be a monomial or zero.

Notice that in sub-cases 1.2 and 1.3, and in case 3 the final object F_m of the iterated reduction may not yet be in normal form modulo G. Such a normal form can, however, be obtained in the same manner as above by applying:

- case 1 to the second term of F_m in sub-case 1.1.
- case 2 to F_m in sub-case 1.2.
- case 3 to F_1 in case 3 provided $F_1 \neq 0$.

Similarly a normal form of F wrt. a finite set $\mathcal{G}$ of binomials or monomials is obtained by a finite iteration of the reduction chains described above.

Call a function $\varphi : \mathbb{Z}^q \longrightarrow \mathbb{Z}$ a *ipr-function*, if it is obtained from constant functions and projections by superposition with operations $+, -, \cdot, \lfloor \frac{\cdots}{\cdots} \rfloor$ and $\max(\ ,\ )$ and if $\varphi(\mathbb{N}^q) \subseteq \mathbb{N}$. Call a function $\psi : \mathbb{Z}^p \times \mathbb{Z}^q \longrightarrow \mathbb{Z}$ an *exponential ipr-function*, if it is obtained from the first p arguments by means of integer constants, $+$, $-$, $\cdot$ and exponentiation by exponents that are generalized ipr-functions of the second group of q arguments.

Then by the above, we can obtain a normal form F' of F under iterated reduction by $\mathcal{G}$, in such a way that the exponents of X in F' are obtained from the given exponents in F and $\mathcal{G}$ by application of ipr-functions. Moreover the coefficients of F' are exponential ipr-functions in the coefficients occurring in F and in $\mathcal{G}$ and in the exponents of X in F and $\mathcal{G}$. Notice, however, that the concrete form of these ipr-functions and exponential ipr-functions depends on the cases and sub-cases discussed above for iterated reduction chains. Which of these cases does in fact occur depends on the vanishing or non-vanishing of current coefficients, order relations between current exponent tuples both wrt. $\leq$ (for determining reducibility) and wrt. $<_t$ (for selecting correct highest terms). The first type of order relations can be coded into equations by means of the maximum-operation. Thus a complete reduction of F to normal form wrt. $\mathcal{G}$ can be represented as a finitely branching tree, where each node is labeled with an intermediate reduct of F modulo $\mathcal{G}$ and a case description consisting of a finite set of equations and dis-equations on ipr-functions in the exponential parameters, equations and dis-equations on exponential ipr-functions in the coefficients and exponential parameters, and $<_t$-inequalities on ipr-functions in the exponential parameters. By the classical Buchberger theory each branch of this tree is finite; so by König's tree lemma the whole tree is finite. The leaves of this tree contain the respective normal forms of F modulo $\mathcal{G}$ together with the corresponding case description.

Notice the similarity of this finite tree construction with the construction of a Gröbner system for polynomials with parametric coefficient in [9, 12].

Next we study the formation of denominator-free s-polynomials of binomials $F = a_1X^f + b_1X^e$, $G = a_2X^d + b_2X^c$ with $f >_t e$, $d >_t c$. Then under the hypothesis $a_1 \neq 0, a_2 \neq 0$, we have $\mathrm{spol}(F, G) = a_2 \cdot X^{(\max(f,d)-f)} \cdot F - a_1X^{(\max(f,d)-d)} \cdot G = a_2b_1X^{e+\max(f,d)-f} - a_1b_2X^{c+\max(f,d)-d}$.
Here the exponents are obtained from the given ones by the operations $+$, $-$ max, and the coefficients from the given coefficients by $+$, $-$, $\cdot$.

Since in the basic Buchberger algorithm for computing minimal Gröbner bases applied to monomials and binomials the only basic operations are formation of s-polynomials and iterated reductions to normal form, the combined facts found above yield the following theorem:

Theorem 2.1 *Let Φ be a finite set of binomials in $\mathbb{Z}[X] = \mathbb{Z}[X_1, \cdots, X_n]$ with parametric coefficients and exponents, and let $<_t$ be a fixed term order. Then one can construct a finite tree T where each node is labeled with a finite set of monomials and binomials and a case description consisting of a finite set of equations and dis-equations on ipr-functions in the exponential* *parameters, equations and dis-equations on exponential ipr-functions in the coefficients and exponential parameters, and $<_t$-inequalities on ipr-functions in the exponential parameters. The leaves of this tree contain a respective minimal Gröbner basis Ψ_i of the ideal generated by F together with the corresponding case description. The case descriptions cover all cases for the parametric coefficients and exponents in Φ. Each Ψ_i is a finite set of monomials and binomials. The exponents of X in Ψ_i are ipr-functions in the exponential parameters in Φ. The coefficients in Ψ_i are exponential ipr-functions in the coefficients in Φ and the exponential parameters in Φ.*

Notice that this theorem applies as well to all optimized denominator-free versions of the Buchberger algorithm that are obtained from the basic version by deleting the formation of certain s-polynomials according to some criteria like the first and second Buchberger criterion in [1]. Notice also the fact that this theorem forms a strong generalization of the construction of a Gröbner system for polynomials with parametric coefficient in [9, 12] for sets of monomials and binomials.

3 The case of a single exponential parameter

Next we study the consequences of this theorem for the case that the coefficients in Φ are fixed integers and the exponents in Φ depend polynomially on a single natural number parameter k. Then by Theorem 2.1 the exponents occurring in a minimal Gröbner basis Ψ of the ideal generated by Φ are generalized ipr-functions of the parameter k and the coefficients in exponential ipr-functions in k. The same applies if we allow the coefficients in Φ also to be exponential ipr-functions in k.

For definiteness and clarity we repeat the definition of ipr-functions and exponential ipr-functions for the present univariate case:

Call a function $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ a *univariate ipr-function*, if it is obtained from constant functions and the identity by superposition with operations $+, -, \cdot, \lfloor \frac{\cdots}{\cdots} \rfloor$ and $\max(\ ,\ )$. Call a function $\psi : \mathbb{N} \longrightarrow \mathbb{Z}$ an *univariate exponential ipr-function*, if it is obtained from integer constants by means of $+, -, \cdot$ and exponentiation by exponents that are univariate generalized ipr-functions.

Then Theorem 2.1 has the following immediate consequence:

Corollary 3.1 *Let Φ be a finite set of binomials in $\mathbb{Z}[X] = \mathbb{Z}[X_1, \cdots, X_n]$ with exponents that are ipr-functions of a natural number parameter k and coefficients that are exponential ipr-functions of k, and let $<_t$ be a fixed term order. Then one can construct a finite tree T where each node is labeled* *with a finite set of monomials and binomials and a case description consisting of a finite set of equations and dis-equations on ipr-functions of k, equations and dis-equations on exponential ipr-functions of k, and $<_t$-inequalities on ipr-functions of k. The leaves of this tree contain a respective minimal Gröbner basis Ψ_i of the ideal generated by F together with the corresponding case description. The case descriptions cover all cases for the parameter k. Each Ψ_i is a finite set of monomials and binomials. The exponents of X in Ψ_i are ipr-functions of k and the coefficients in Ψ_i are exponential ipr-functions k.*

Our goal is now to simplify both the case distinctions, the ipr-functions and the exponential ipr-functions involved in this result for large enough values of k. It will turn out that for large enough values of k any ipr-function of k can essentially be rewritten as a polynomial function; moreover the case distinctions on k form Presburger sets, i.e. finite or almost periodic subsets of $\mathbb{N}$ (compare [8, 10, 11]).

Definition 3.2 *An* almost integer polynomial function *is a function $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$ with $\varphi(\mathbb{N}) \subseteq \mathbb{N}$ of the form $\varphi(k) = \varphi'(\left\lfloor \frac{k}{p} \right\rfloor)$ for some polynomial $\varphi'(Y) \in \mathbb{Z}[Y]$ and some fixed positive integer p. Any such p is called a* modulus *for φ.*

Notice that moduli are not unique: Any multiple of a modulus is again a modulus. As a consequence any finite number of almost integer polynomial functions has a common modulus, namely the least common multiple of the individual moduli.

Theorem 3.3 *Let $\varphi(k)$ be a generalized ipr-function of a natural number argument k. Then one can compute natural numbers $B(\varphi)$, $p(\varphi)$ and for every residue class $0 \leq i < p(\varphi)$ a polynomial function $\varphi_i(Y) \in \mathbb{Z}[Y]$ such that for all $k \geq B(\varphi)$ with $k \equiv i \bmod p(\varphi)$, we have $\varphi(k) = \varphi_i\left(\left\lfloor \frac{k}{p(\varphi)} \right\rfloor\right)$; in other words, $\varphi(k)$ is an almost integer polynomial function of k with modulus $p(\varphi)$ on the residue class of i modulo $p(\varphi)$.*

Proof. We proceed by induction on the superposition order of φ: For constant functions and the identity function the claim is obvious. If $\varphi(k) = \psi(k) + \vartheta(k)$ or $\varphi(k) = \psi(k) - \vartheta(k)$ or $\varphi(k) = \psi(k) \cdot \vartheta(k)$, then we put $B(\varphi) = \max\,(B(\psi), B(\vartheta))$ and $p(\vartheta) = \mathrm{lcm}\,(p(\psi), p(\vartheta))$. Then the claim is obvious.
If $\varphi(k) = \max(\psi(k), \vartheta(k))$, then we compute $B(\varphi) \geq \max\,(B(\psi), B(\vartheta))$, $p(\varphi) = \mathrm{lcm}\,(p(\psi), p(\vartheta))$, such that for all

$0 \leq i < p(\varphi)$: Either for all $k \geq B(\varphi)$ $\psi_i(\left\lfloor \frac{k}{p(\varphi)} \right\rfloor) \geq \vartheta_i(\left\lfloor \frac{k}{p(\varphi)} \right\rfloor)$, or for all $k \geq B(\varphi)$, $\psi_i(\left\lfloor \frac{k}{p(\varphi)} \right\rfloor) < \vartheta_i(\left\lfloor \frac{k}{p(\varphi)} \right\rfloor)$. Then we may put $\varphi_i(Y) = \psi_i(Y)$, or $\varphi_i(Y) = \vartheta_i(Y)$, depending on the respective case.

Finally let $\varphi(k) = \left\lfloor \frac{\psi(k)}{\vartheta(k)} \right\rfloor$. Put $p'(\varphi) = \mathrm{lcm}\,(p(\psi), p(\vartheta))$. Then by division with remainder we can write for each $0 \leq i < p'(\varphi)$ the polynomial quotient $\frac{\psi_i(Y)}{\vartheta_i(Y)}$ in the form $\frac{\mu_i(Y)}{a^m} + \frac{\psi'(Y)}{\vartheta_i(Y)}$ where $\mu_i(Y)$, $\psi_i'(Y) \in \mathbb{Z}[Y]$, $m \in \mathbb{N}$, a is the highest coefficient of $\vartheta_i(Y)$ and $\psi_i'(Y) = 0$ or $\deg(\psi_i'(Y)) <\ \deg(\vartheta_i(Y))$. Put $p(\varphi) = p'(\varphi)a^m$.
Then for each fixed residue class $0 \leq j < p(\varphi)$ and $k \geq B(\varphi)$ and $k \equiv j \bmod p(\varphi)$ one can rewrite $\frac{\mu_i(\left\lfloor \frac{k}{p'(\varphi)} \right\rfloor)}{a^m} + \frac{\psi_i'(\left\lfloor \frac{k}{p'(\varphi)} \right\rfloor)}{\vartheta_i(\left\lfloor \frac{k}{p'(\varphi)} \right\rfloor)}$ in the form $\nu_j\left(\left\lfloor \frac{k}{p(\varphi)} \right\rfloor\right) + \frac{\psi_j'(\left\lfloor \frac{k}{p'(\varphi)} \right\rfloor)}{\vartheta_j(\left\lfloor \frac{k}{p'(\varphi)} \right\rfloor)}$ with $\nu_j(Y) \in \mathbb{Z}[Y]$. Compute $B(\varphi) \geq \max\ (B(\psi), B(\vartheta))$ such that for all $k \geq B(\varphi)$ and all $0 \leq j < p(\varphi)$, $\left| \frac{\psi_j'(\left\lfloor \frac{k}{p'(\varphi)} \right\rfloor)}{\vartheta_j(\left\lfloor \frac{k}{p'(\varphi)} \right\rfloor)} \right| < 1$. Then we get for $k \geq B(\varphi), k \equiv j \bmod p(\varphi)$, $\left\lfloor \frac{\psi(k)}{\vartheta(k)} \right\rfloor = \nu_j\left(\left\lfloor \frac{k}{p(\varphi)} \right\rfloor\right)$. $\square$

Definition 3.4 *Exponential polynomials of* Y *are functions* $\mathbb{N} \longrightarrow \mathbb{Z}$ *generated from integer constants and* Y *by means of* $+, -, \cdot$ *and exponentiation of integers by almost integer polynomial functions of* Y.

Then by combining Corollary 3.1 with Theorem 3.3 we get:

Theorem 3.5 *Let* Φ *be a finite set of binomials in* $\mathbb{Z}[X] = \mathbb{Z}[X_1, \cdots, X_n]$ *with exponents that are ipr-functions of a natural number parameter* k *and coefficients that are exponential ipr-functions of* k*, and let* $<_t$ *be a fixed term order. Then one can determine a bound* B *and a modulus* q *such that for all* $k > B$ *in a fixed congruence class modulo* q *the following hold:*

One can construct a finite tree T *where each node is labeled with a finite set of monomials and binomials and a case description consisting of a finite set of equations and dis-equations on almost integer polynomial functions of* k*, equations and dis-equations on exponential polynomials of* k*, and* $<_t$*-inequalities between tuples of almost integer polynomial functions of* k*. The leaves of this tree contain a respective minimal Gröbner basis* Ψ_i *of the ideal generated by* F *together with the corresponding case description. The case descriptions cover all cases for the parameter* $k > B$ *in a fixed congruence class modulo* q*. Each* Ψ_i *is a finite set of monomials and binomials. The* *exponents of X in Ψ_i are almost integer polynomial functions in k and the coefficients in Ψ_i are exponential polynomials in k.*

It remains to render case descriptions in this theorem more concrete. For this purpose the next theorem is of decisive importance:

Theorem 3.6 *Let φ be an exponential polynomial of a natural number parameter k, different from the zero function. Then the set $\{k \in \mathbb{N} \mid \varphi(k) = 0\}$ is finite.*

Proof. Rewrite every non-zero integer constant a occurring in the functional definition of φ in the form $2^{\log(a)}$, if $a > 0$ and in the form $-2^{\log(-a)}$, if $a < 0$. We may assume that all the almost integer polynomial functions occurring in $\varphi(k)$ have the same modulus p. Then by the distributive law and the multinomial law, $\varphi(k)$ can be written as a finite sum, whose length depends on k, of summands of the form $\pm 2^{\psi(\lfloor \frac{k}{p} \rfloor)}$ with pairwise different real polynomials $\psi(Y)$, whose coefficients are rational polynomials in logarithms of natural numbers. Since φ is different from the zero function, this sum is non-empty, and hence its sign is determined by the sign of the largest power of 2 occurring in the sum. So for large enough value of k, the value of $\varphi(k)$ is non-zero. □

Corollary 3.7 *Let Φ be a finite set of binomials in $\mathbb{Z}[X] = \mathbb{Z}[X_1, \cdots, X_n]$ with exponents that are ipr-functions of a natural number parameter k and coefficients that are exponential ipr-functions of k, and let $<_t$ be a fixed term order. Then one can determine a bound B and a modulus q such that for all $k > B$ in a fixed congruence class modulo q the following hold: One can construct a minimal Gröbner basis Ψ of the ideal generated by F uniformly in k. Ψ is a finite set of monomials and binomials. The exponents of X in Ψ are almost integer polynomial functions in k and the coefficients in Ψ_i are exponential polynomials in k.*

Proof. By theorem 3.5 it suffices to show the claim that the equations, dis-equations and $<_t$-inequalities occurring in the case descriptions of Theorem 3.5 each hold either on a finite or a co-finite set of natural numbers. Then since the case distinctions cover all of $\mathbb{N}$, at least one case covers a co-finite subset of $\mathbb{N}$. The claim is obvious for equations and disequations involving almost integer polynomial functions of k. For equations and dis-equations involving exponential polynomials of k this follows from Theorem 3.6.

It remains to consider the case of $<_t$-inequalities between tuples of almost integer polynomial functions in k. By the characterization of term orders in

[5, 7, 3] an $<_t$-inequality $c <_t d$ between n-tuples of natural numbers amounts to a certain boolean combination of equations and inequalities between the values of certain real linear forms, evaluated at points c and d. For algorithmic purposes we assume at this point that this characterization of the given to us explicitly. If the entries of c and d are almost integer polynomial functions of k, then the inequalities in such a boolean combination have a satisfaction set in $\mathbb{N}$ that is finite or co-finite; moreover the decision which is the case can be made effectively. Hence the same applies to the given $<_t$-inequality. $\square$

The corollary shows in particular that in the situation of Theorem 3.5 one can partition the set $\mathbb{N}$ of natural numbers into finitely many blocks such that on each block the computation of a minimal Gröbner basis Ψ for the ideal generated by Φ is uniform in k. Moreover every block is a Presburger set, i. e. a subset of $\mathbb{N}$ definable in Presburger arithmetic (compare [4, 8, 10, 11]).

4 Degree bounds for k

Assume in the situation of Corollary 3.7 that the exponential parameter k occurs in exponents in Φ as polynomials of degree bounded by D. Then it is natural to ask, if this bound is preserved under the passage from Φ to a minimal Gröbner basis Ψ as in Corollary 3.7. The next example shows that this is in general not the case:

Example 4.1 *Let $F = X^k, G = X - Y^k \in \mathbb{Z}[X, Y]$ and put $X >_{lex} Y$. Then the monomial F is reduced to normal form modulo G as follows:*

$$F \underset{G}{\longrightarrow} F_1 = X^{k-1}Y^k \underset{G}{\longrightarrow} F_2 = X^{k-2}Y^{2k} \underset{G}{\longrightarrow} \dots \underset{G}{\longrightarrow} F_k = Y^{k^2}.$$

This shows that the degree of exponents in the exponential parameter k can increase from 1 to 2 under reduction of binomials to normal form.
The example can be extended for more indeterminates:

Let $F = X^k, G = X - Y^k, H = Y - Z^k \in \mathbb{Z}[X, Y, Z]$ and put $X >_{lex} Y >_{lex} Z$. Then the monomial F is reduced to normal form Y^{k^2} modulo G as above and the latter monomial is similarly reduces to normal form Z^{k^3}. For n indeterminates we get more generally examples where the degree of exponents in the exponential parameter k can increase from 1 to n under reduction of binomials to normal form.

By way of contrast we show that for weighted total-degree term orders such an increase in degrees does not happen:

Theorem 4.2 *In the situation of Corollary 3.7 assume that the exponential parameter k occurs in exponents in Φ as polynomial functions of k of degree bounded by D. Assume moreover that the term order $<_t$ is a weighted total-degree term order. Consider values of k in an infinite Presburger set. Then k occurs in exponents in Ψ only in almost integer polynomial functions of degree bounded by D.*

Proof. We inspect the change of exponents during the formation of s-polynomials and during reduction to normal form in section 2. Obviously the formation of s-polynomials does not increase the degree of k in exponents. Hence an increase of degrees can only occur in the m-step reduction chains analyzed in section 2, and here only in sub-case 1.1 or in case 2. The critical exponent to consider here is $m(d-c)$, where $m = \left\lfloor \frac{f_i - d_i}{d_i - c_i} \right\rfloor + 1$ for some $1 \leq i \leq n$. Moreover inspection of sub-case 1.1 and case 2 shows that i can be chosen such that $d_i - c_i$ is maximal.

By hypothesis we have $d >_t c$; since $<_t$ is a weighted total-degree term order this implies for large values of k that the degree of k in all entries of c is smaller or equal to the maximal degree d' of k in entries of d. Hence the maximal degree of k in entries of $(d-c)$ is $d_i - c_i$. The maximal degree of k in $(f_i - d_i)$ is bounded by D. For large enough values of k in a fixed residue class modulo a suitable q the values of m can be written as an almost integer polynomial function of k. By the above the degree of this function in k is bounded by $(D - d') + d' = D$. ◻

5 Conclusions

We have shown that for a finite set Φ of monomials and binomials with parametric coefficients *and* exponents corresponding minimal Gröbner bases wrt. a fixed term order can be computed uniformly in all parameters up to a finite case distinction in the parameter space. For arbitrary polynomials this is in general impossible. For the special case of a single exponential natural number parameter k we have computed a finite partition of $\mathbb{N}$ into Presburger sets such that for k in a fixed block of the partition a minimal Gröbner basis Ψ of the ideal generated by F can be computed uniformly in k. Moreover we have explicitly described the dependence of the coefficients and exponents in Ψ on k. For weighted total degree term orders we have moreover shown that the maximal degree of k in exponents occurring in Φ does not grow under the passage to Ψ.

References

[1] T. Becker, V. Weispfenning, and H. Kredel. *Gröbner Bases, a Computational Approach to Commutative Algebra*, volume 141 of *Graduate Texts in Mathematics*. Springer, New York, corrected second printing edition, 1998.

[2] P. Conti and C. Traverso. Buchberger algorithm and integer programming. In *AAECC-9*, volume 539 of *LNCS*, pages 130–139. Springer, 1991.

[3] H. Hong and V. Weispfenning. Algorithmic theory of admissible term orders. Technical report, North Carolina State University, Department of Mathematics and University of Passau, Department of Mathematics, 1999. Submitted for publication.

[4] M. Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik. In *Comptes rendues du 1er Congres des Mathematique des Pays Slaves*, volume 395, pages 92–101, Warsaw, 1929.

[5] L. Robbiano. Term orderings on the polynomial ring. In B. Caviness, editor, *EUROCAL'85, European conference on computer algebra, vol. II*, volume 357 of *Springer LNCS*, pages 31–44. Springer, 1985.

[6] T. Takahashi. An application of Gröbner bases for the moduli of hypersurface simple K3 singularities. Technical report, Kobe University, Kobe, Japan, October 2003.

[7] V. Weispfenning. Admissible orders and linear forms. *ACM SIGSAM Bulletin*, 21(2):16–18, 1987.

[8] V. Weispfenning. The complexity of almost linear Diophantine problems. *Journal of Symbolic Computation*, 10(5):395–403, Nov. 1990.

[9] V. Weispfenning. Comprehensive Gröbner bases. *Journal of Symbolic Computation*, 14:1–29, July 1992.

[10] V. Weispfenning. Complexity and uniformity of elimination in Presburger arithmetic. In W. W. Küchlin, editor, *International Symposium on Symbolic and Algebraic Computation, Maui, Hawaii*, pages 48–53, New York, July 1997. ACM Press.

[11] V. Weispfenning. Mixed real-integer linear quantifier elimination. In S. Dooley, editor, *ISSAC'99*, pages 129–136. ACM-Press, 1999.

[12] V. Weispfenning. Canonical comprehensive Gröbner bases. In T. Mora, editor, *ISSAC 2002*, pages 270–276. ACM Press, 2002.

[13] K. Yokoyama. On systems of polynomial equations with indeterminate exponents. Technical report, Kyushu University, Fukuoka, Japan, October 2003. Lecture notes.