ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 42, Number 3, 2012

ρ-HOMOGENEOUS BINOMIAL IDEALS AND PATIL BASES

H. BRESINSKY, F. CURTIS AND J. STÜCKRAD

ABSTRACT. The paper first generalizes the construction of generating sets for binomial ideals as given in [**6**]. For this, ρ-homogeneous binomial ideals are introduced. The resulting generating sets are called Patil bases. It is shown that they are reduced and normalized Gröbner bases. An algorithm for binomials is given to obtain a minimal generating set from a Patil basis. This is applied to the particular case of Patil bases of prime ideals $\mathfrak{p}(n_1, \dots, n_4)$ generated by $\{x^\alpha - x^\beta \mid \alpha, \beta \in \mathbf{N}^4,\ (\alpha - \beta)(n_1, \dots, n_4)^T = 0\}$ in $K[x_1, \dots, x_4]$, K a field. We note that our ideals are toric ideals, see [**7**].

0. Introduction and notation. Assume K is a field and $R := K[x_1, \dots, x_r]$ the polynomial ring in r indeterminates over K, $\mathfrak{m} := (x_1, \dots, x_r)R$. Let $T := \{x_1^{\alpha_1} \cdot \dots \cdot x_r^{\alpha_r} =: x^\alpha \mid \alpha := (\alpha_1, \dots, \alpha_r) \in \mathbf{N}^r\}$ ($\mathbf{N}$ is the set of nonnegative integers) be the set of terms in R and $<$ an admissible term order on T. (For undefined terminology for Gröbner bases we refer the reader to [**2**]).

Remark 1. If clear from the context, we will use interchangeably the symbol $<$ to denote an admissible term order as well on T as on $\mathbf{N}^r$, i.e. $\alpha < \beta$ means the same as $x^\alpha < x^\beta$. $x^\alpha \mid x^\beta$ (or equivalently $\alpha \mid \beta$) denotes monomial division, $x^\alpha \parallel x^\beta$ (or equivalently $\alpha \parallel \beta$) proper division.

Definition 0.1. Assume $f \in R$, $f = \sum_{t \in T} a_t \cdot t$ with $a_t \in K$ and $a_t = 0$ for almost all $t \in T$. Then $\operatorname{supp}(f) := \{t \mid t \in T,\ a_t \neq 0\}$.

Let $n_1, \dots, n_r$ be positive integers with $\gcd(n_1, \dots, n_r) = 1$. Define the weighted degree for R by $\deg x_i := n_i$, $1 \leq i \leq r$. Let

2010 AMS *Mathematics subject classification.* Primary 13F20, 13H10, 13P10.
The first author was supported by the NTZ and the Graduiertenkolleg "Analysis, Geometrie und ihre Verbindung zu den Naturwissenschaften" at the University of Leipzig.
The third author is the corresponding author.
Received by the editors on November 10, 2008, and in revised form on October 23, 2009.

DOI:10.1216/RMJ-2012-42-3-823

$\mathfrak{p}(n_1, \ldots, n_r) =: \mathfrak{p}$ be the ideal in R, generated by

$$\{x^\alpha - x^\beta \mid, \alpha, \beta \in \mathbf{N}^r, (\alpha - \beta)(n_1, \ldots, n_r)^T = 0\} \subseteq R.$$

Assume an admissible lexicographical term order on T (or equivalently on $\mathbf{N}^r$). In this setting Patil bases were introduced by Patil in his thesis [**6**].

In this paper in Section 1 we first introduce the ρ-degree, which includes the usual polynomial degree and the above weighted degree. In Section 2 we then define Patil bases for ρ-homogeneous binomial (toric) ideals $I_L := (\{x^\alpha - x^\beta \mid \alpha, \beta \in \mathbf{N}^r,\ \alpha - \beta \in L\})R$, where L is a subgroup of $\mathbf{Z}^r$ ($\mathbf{Z}$ the integers), for arbitrary admissible term orders. It is then shown that such a Patil basis is a normalized and reduced Gröbner basis with respect to a term order related to the initial term order. In Section 3 we present an algorithm how to obtain a minimal generating set for a ρ-homogeneous binomial ideal from a reduced and normalized Gröbner basis. The algorithm is essential to obtain a minimal generating set for $\mathfrak{p}(n_1, \ldots, n_4)$ in Section 4.

1. ρ-degree. Assume ρ is a map such that:

(i) $\rho : \mathbf{N}^r \to \mathbf{N}$.

(ii) $\rho(\alpha) = 0$ if and only if $\alpha = 0$.

(iii) For all α, β, γ in $\mathbf{N}^r$, $\rho(\alpha) < \rho(\beta)$ implies $\rho(\alpha + \gamma) < \rho(\beta + \gamma)$ and $\rho(\alpha) = \rho(\beta)$ implies $\rho(\alpha + \gamma) = \rho(\beta + \gamma)$.

Definition 1.1. For $\alpha \in \mathbf{N}^r$ $\rho(\alpha)$ is called the ρ-degree of α.

Example 1.1. ρ-degrees, which are not standard.

(a) A map $\varphi : \mathbf{N}^r \to \mathbf{N}$ is linear if $\varphi(\nu_1 + \nu_2) = \varphi(\nu_1) + \varphi(\nu_2)$ for all $\nu_1, \nu_2 \in \mathbf{N}^r$. The ordinary degree mapping δ given by $\delta(\prod_{i=1}^r x_i^{n_i}) := \sum_{i=1}^r n_i$ $(n_1, \ldots, n_r \in \mathbf{N})$ is linear if $\prod_{i=1}^r x_i^{n_i}$ is identified with $(n_1, \ldots, n_r)$. Assume φ satisfies (i)–(iii) and $\psi : \mathbf{N} \to \mathbf{N}$ is such that $\psi(0) = 0$ and $\psi(n_1) < \psi(n_2)$ if $n_1 < n_2$. Then $\psi\varphi$ satisfies (i)–(iii), but $\psi\varphi$ need not be linear if ψ is not linear. For instance if $\psi(n) := n^2$ for all $n \in \mathbf{N}$, then $\psi\varphi$ is not linear.

(b) Let $c_1, \ldots, c_r$ be integers with $c_1, \ldots, c_r > 1$. Define $\varphi : \mathbf{N}^r \to \mathbf{N}$ by

$$\varphi((a_1, \ldots, a_r)) := c_1^{a_1} \cdot \ldots \cdot c_r^{a_r} - 1, \quad a_1, \ldots, a_r \in \mathbf{N}.$$

For φ (i)–(iii) are satisfied. (If the c_i are pairwise distinct prime numbers, then φ is injective.)

Proposition 1.2. *For* $\alpha =: (a_1, \dots, a_r) \in \mathbf{N}^r$, *let* $|\alpha| := \sum_{i=1}^r a_i$. *Then*

$$|\alpha| \leq \rho(\alpha) \quad \textit{for all } \alpha \in \mathbf{N}^r.$$

Proof. We induct on $|\alpha|$. The statement is true if $|\alpha| = 0$ (since $|\alpha| = 0 \Leftrightarrow \alpha = 0$). Let $\alpha \in \mathbf{N}^r$ with $|\alpha| > 0$. If $\alpha =: (a_1, \dots, a_r)$, there is some j, $1 \leq j \leq r$ with $a_j \geq 1$. Let $\alpha' := \alpha - e_j$, $e_j = (0, \dots, 0, 1, 0 \dots, 0)$ with 1 in the jth coordinate. Then $\alpha' \in \mathbf{N}^r$ and $0 = \rho(0) < \rho(e_j)$ implies (by (iii)), $\rho(\alpha') = \rho(0+\alpha') < \rho(e_j+\alpha') = \rho(\alpha)$. By the induction hypothesis

$$|\alpha| = |\alpha'| + 1 \leq \rho(\alpha') + 1 \leq \rho(\alpha). \qquad \square$$

Definition 1.3. By $\#X$ we denote the cardinality of a set X.

Corollary 1.4. *Let* N *be a fixed nonnegative integer. Then*

$$\#\{\alpha \in \mathbf{N}^r \,|\, \rho(\alpha) \leq N\} < \infty, \textit{ in particular } \#\{\alpha \in \mathbf{N}^r \,|\, \rho(\alpha) = N\} < \infty.$$

Proof. Let $\alpha \in \mathbf{N}^r$ with $\rho(\alpha) \leq N$, and assume $\alpha =: (a_1, \dots, a_r)$. Then

$$0 \leq a_i \leq |\alpha| \leq \rho(\alpha) \leq N, \quad 1 \leq i \leq r,$$

from which the claim is derived. $\square$

By Proposition 1.2 and its Corollary 1.4 it follows readily that ρ defines a graded structure on R. Therefore if $f_1, \dots, f_s$ are ρ-homogeneous, then $\{f_1, \dots, f_s\}$ contains a minimal generating set for the ideal $I = (f_1, \dots, f_s)R$.

2. Patil bases.

Definition 2.1. Let L be a subgroup of $\mathbf{Z}^r$ and ρ a ρ-degree such that, for all $\alpha, \beta \in \mathbf{N}^r$, if $\alpha - \beta \in L$, then $\rho(\alpha) = \rho(\beta)$. Let $I_L := \{x^\alpha - x^\beta \mid \alpha, \beta \in \mathbf{N}^r, \alpha - \beta \in L\} \cdot R$ (i.e., I_L is the ideal generated by the indicated binomials which is ρ-homogeneous).

Lemma 2.2. *For* $\alpha \in \mathbf{N}^r$, $\#((\alpha + L) \cap \mathbf{N}^r) < \infty$ *and* $L \cap \mathbf{N}^r = \{0\}$.

Proof. Let $L(\alpha) := \{\lambda \mid \lambda \in L, \alpha + \lambda \in \mathbf{N}^r\}$. Let $\varphi : L(\alpha) \to \mathbf{N}^r$ be defined by $\varphi(\lambda) = \alpha + \lambda \in \mathbf{N}^r$ for all $\lambda \in L(\alpha)$. Clearly φ is injective

and, for $\lambda \in L(\alpha)$, $\rho(\varphi(\lambda)) = \rho(\alpha+\lambda) = \rho(\alpha)$ since $(\alpha+\lambda)-\alpha = \lambda \in L$. Thus, if $\overline{\alpha} := \{\beta \mid \beta \in \mathbf{N}^r, \rho(\beta) = \rho(\alpha)\}$, then $\varphi(\lambda) \in \overline{\alpha}$. Since $\#\overline{\alpha} < \infty$, by Corollary 1.4, and φ is injective, $\#L(\alpha) < \infty$.

Next assume $\alpha = 0$. Then $L(0) = L \cap \mathbf{N}^r$ and, for $\lambda \in L(0)$, $0 + \lambda \in \mathbf{N}^r$. By the previous $\rho(\lambda) = \rho(0 + \lambda) = \rho(0) = 0$, thus $\lambda = 0$. □

Example 2.1. Assume $f : \mathbf{Z}^r \to \mathbf{Z}$ is linear (i.e. $f(z_1 + z_2) = f(z_1) + f(z_2)$ for all $z_1, z_2 \in \mathbf{Z}^r$) such that $n_i := f(e_i) \in \mathbf{N}^+$ for all $i, 1 \leq i \leq r$ ($e_i \in \mathbf{N}^r$ with the ith coordinate 1 and all other coordinates 0). Let $\rho := f|_{\mathbf{N}^r} : \mathbf{N}^r \to \mathbf{N}$ be the restriction of f to $\mathbf{N}^r$, which is a ρ-degree and ρ is linear. If $\alpha := (a_1, \ldots, a_r) \in \mathbf{N}^r$, then $\rho(\alpha) = \sum_{i=1}^r a_i n_i$. For $n_i = 1$, $1 \leq i \leq r$, this ρ-degree is the usual degree. For $n_1 < n_2 < \cdots < n_r$, $\gcd(n_1, \ldots, n_r) = 1$, this ρ-degree is a frequently used weighted degree. For this degree the defining ideal of a curve in affine r-space with parametric representation $x_i = t^{n_i}$, $i = 1, \ldots, r$, is ρ-homogeneous.

Since ρ is linear, condition (iv) is fulfilled with $L = \ker f$.

Assume next that $<$ is an admissible term order on $\mathbf{N}^r$, L as before.

Definition 2.3. For $\alpha \in \mathbf{N}^r$ let $\sigma(\alpha) := \max_<[(\alpha + L) \cap \mathbf{N}^r]$

We now define an admissible term order $<'$ on $\mathbf{N}^r$ as follows.

Definition 2.4. For $\alpha, \beta \in \mathbf{N}^r$ let $\alpha <' \beta$ if

(1) $\rho(\alpha) < \rho(\beta)$ or

(2) $\rho(\alpha) = \rho(\beta)$ and $\beta < \alpha$.

Lemma 2.5. *$<'$ is an admissible term order.*

Proof. Assume $\beta \in \mathbf{N}^r$, $\beta \neq 0$. Then $\rho(\beta) > 0 = \rho(0)$, hence $0 <' \beta$. Next let α, β, γ be in $\mathbf{N}^r$ with $\alpha <' \beta$. If $\rho(\alpha) < \rho(\beta)$, then $\rho(\alpha+\gamma) < \rho(\beta+\gamma)$; thus, $\alpha+\gamma <' \beta+\gamma$. If $\rho(\alpha) = \rho(\beta)$, then $\beta < \alpha$; therefore, $\beta+\gamma < \alpha+\gamma$. And $\rho(\alpha+\gamma) = \rho(\beta+\gamma)$; thus, $\alpha+\gamma <' \beta+\gamma$. □

Assume next that $(\mu_i)_{i\in\mathbf{N}^+}$ is a sequence in $\mathbf{N}^r$ such that:

(1) $\{\mu_i \mid i \in \mathbf{N}^+\} = \mathbf{N}^r\backslash\{0\}$.

(2) $\mu_i - \mu_j \notin \mathbf{N}^r$ for all i, j in $\mathbf{N}^+$ with $i < j$.

We now inductively define subsets of $\mathbf{N}^r$ as follows:

$$M_0 := \varnothing$$

$$M_{i+1} := \begin{cases} M_i, & \text{if } \sigma(\mu_{i+1}) = \mu_{i+1} \text{ or if there exists} \\ & \mu \in M_i \text{ with } \mu_{i+1} - \mu \in \mathbf{N}^r. \\ M_i \cup \{\mu_{i+1}\}, & \text{otherwise.} \end{cases}$$

We have $M_0 \subseteq M_1 \subseteq \cdots$. By Dickson's lemma there exists an $s \in \mathbf{N}$ such that $M_s = M_{s+j}$ for all $j \geq 0$. Let

$$M := \bigcup_{i=0}^{\infty} M_i \subseteq \mathbf{N}^r.$$

Then $M = M_s$, and therefore $\#M \leq s < \infty$.

Definition 2.6. $P_L := \{x^\mu - x^{\sigma(\mu)} \mid \mu \in M\}$ is called a Patil basis of I_L with respect to $<$.

Remark 2. Note that if μ and ν are in M, $\mu \neq \nu$, then $x^\mu \nmid x^\nu$ and $x^\nu \nmid x^\mu$. If $\mu \in M$ and $x^{\mu'} \parallel x^\mu$ for $\mu' \in \mathbf{N}^r \setminus \{0\}$, then $\sigma(\mu') = \mu'$.

Definition 2.7. Let $b = m_1 - m_2$ be a binomial ($m_1, m_2 \in T$). We define

$$|b| := \begin{cases} b & \text{if } m_1 \geq m_2 \\ -b & \text{otherwise.} \end{cases}$$

Moreover, if $m_1 > m_2$ then, as before, the leading term ($\mathrm{lt}_<(b)$) of b is m_1, the lower term, or not the leading term ($\mathrm{nlt}_<(b)$) of b, is m_2. If clear from the context, $<$ will be deleted as subscript.

Proposition 2.8. *P_L is a reduced and normalized Gröbner basis of I_L with respect to $<'$.*

Proof. By Definition 2.3 $P_L \subseteq I_L$. For $x^\mu - x^{\sigma(\mu)}$, $\mu \in M$, $\mathrm{lt}_{<'}(x^\mu - x^{\sigma(\mu)}) = x^\mu$.

Let $\alpha, \beta \in \mathbf{N}^r$ with $0 \neq \alpha - \beta \in L$. We first show that $x^\alpha - x^\beta$ has a reduction modulo P_L. Without loss of generality assume $\mathrm{lt}_{<'}(x^\alpha - x^\beta) = x^\alpha$. Then $\alpha \neq \sigma(\alpha)$. Thus, by construction of M, there exists a $\mu \in M$ with $\alpha - \mu \in \mathbf{N}^r$, i.e., $x^\mu | x^\alpha$. Therefore, $x^{\alpha+\sigma(\mu)-\mu} - x^\beta = x^\alpha - x^\beta - x^{\alpha-\mu}(x^\mu - x^{\sigma(\mu)}) \in I_L$. Since $\alpha + \sigma(\mu) - \mu <' \alpha$ and $\beta <' \alpha$, we have $\mathrm{lt}_{<'}(x^{\alpha+\sigma(\mu)-\mu} - x^\beta) <' x^\alpha = \mathrm{lt}_{<'}(x^\alpha - x^\beta)$, i.e., $x^\alpha - x^\beta$ has a reduction $x^\alpha - x^\beta \overset{x^\mu - x^{\sigma(\mu)}}{\longrightarrow} x^{\alpha+\sigma(\mu)-\mu} - x^\beta$ modulo P_L as claimed.

Therefore P_L is a Gröbner basis of I_L with respect to $<'$. P_L is clearly normalized; thus, it remains to show that P_L is reduced. Suppose this is not the case. Then there exist $\mu, \mu^* \in M, \mu \neq \mu^*$, such that either $x^{\mu^*} | x^\mu$ or $x^{\mu^*} | x^{\sigma(\mu)}$. The first case is impossible by Remark 2. Suppose therefore $x^{\mu^*} | x^{\sigma(\mu)}$, i.e., there exists $\gamma \in \mathbf{N}^r$ such that $\mu^* + \gamma = \sigma(\mu)$. Then since $\mu^* \in M, \sigma(\mu^*) > \mu^*$, thus $\sigma(\mu^*) + \gamma > \mu^* + \gamma = \sigma(\mu)$. Since $\sigma(\mu^*) + \gamma - \sigma(\mu) = \sigma(\mu^*) - \mu^* \in L$, this means $\sigma(\mu^*) + \gamma \in (\mu + L) \cap \mathbf{N}^r$ and $\sigma(\mu^*) + \gamma > \sigma(\mu)$, a contradiction to $\sigma(\mu) = \max_<[(\mu + L) \cap \mathbf{N}^r]$. □

3. Binomial Gröbner bases and minimal generating sets. Assume $I \subseteq R$ is a ρ-homogeneous binomial ideal (i.e., generated by ρ-homogeneous binomials). Also always take $<$ to be an admissible term order on T, which respects the ρ-degree. In the sequel we will consider only ρ-homogeneous binomials.

For the formation of Gröbner bases we specify the following rules:

1. Reduction to a reduced set always takes precedence over s-polynomial formation.

2. For a polynomial p, reduction of $t \in \mathrm{supp}\,(p)$ by an irreducible set F (if possible) is done by selecting $f \in F$ such that $\mathrm{lt}\,(f) | t$ and $\mathrm{lt}\,(f)$ is maximal with respect to this property.

3. If a polynomial p has a term $t \in \mathrm{supp}\,(p)$ such that there exists an $f \in F$ with $\mathrm{lt}\,(f) | t$, then t is taken to be maximal within $\mathrm{supp}\,(p)$ with this property.

We note that by our assumptions above each reduction step and each formation of an s-polynomial leads automatically to a normalized polynomial, provided this polynomial is $\neq 0$.

Also the production of a (normalized) polynomial $b \in R$ by a Buchberger algorithm, starting from a non-empty set F of non-zero

(normalized) polynomials of R, can be described by a directed tree with vertices consisting of (normalized) polynomials of R ending in b such that the vertices of incoming degree zero correspond to elements of F, the vertices of incoming degree one are obtained by reductions and the vertices of incoming degree two indicate s-polynomial formation.

Definition 3.1. Assume $b = m_1 - m_2$ is as in Definition 2.7 with $m_1 > m_2$. If m is a term and $q_2 m_2 = m$ with $q_2 \in T$, then $q_2 m_1$ is a reduction up of m mod b. If $m = q_1 m_1$ with $q_1 \in T$, then $q_1 m_2$ is a reduction down of m mod b (write $m \xrightarrow{b} q_1 m_2$).

Let B be a set of nonzero binomials. A sequence of reductions (up, down or both) of a term m by binomials of B, is said to be a reduction of m modulo B (mod B). We also refer to them as a chain of reductions. If $b^* = m_1^* - m_2^*$ is a binomial, then a reduction of m_1^* or m_2^* (up or down) is said to be a reduction of b^* (up or down) to a binomial $\widetilde{b}$ mod B. (In this setting $\widetilde{b} = 0$ is considered to be a binomial.) For such reductions down we write $b^* = b_0 \to b_1 \to \cdots \to b_n = \widetilde{b}$ mod B. (If required we also indicate the binomials in B by which reduction is achieved.)

Example 3.1. Let $b^* := x_1^2 - x_2^2$, $b := x_1 - x_2$, $x_1 > x_2$. Then $x_1 x_2 - x_2^2$ is a reduction down of b^* by b since $x_1^2 > x_1 x_2$ and $x_1^2 - x_1 x_2$ is a reduction up of b^* by b since $x_1 x_2 > x_2^2$.

Definition 3.2. A term m is lower reduced mod$B$ if $\operatorname{nlt}(b) \nmid m$ for all $b \in B$. Similarly m is defined to be upper reduced mod$B$.

For completeness we define s-polynomials for binominals.

Definition 3.3. Let $b_1 = m_{11} - m_{12}$ and $b_2 = m_{21} - m_{22}$ be binomials, where m_{11}, m_{12}, m_{21}, m_{22} are terms such that $m_{11} > m_{12}$, $m_{21} > m_{22}$. Assume $m_{i1} = q_i d, m_{i2} = q_i' d'$, $i = 1, 2$, with terms q_1, q_2, q_1', q_2', d, d' such that $\gcd(q_1, q_2) = \gcd(q_1', q_2') = 1$. Then the s-polynomial $s(b_1, b_2)$ of b_1 and b_2 is defined to be:

$$s(b_1, b_2) := |q_2 b_1 - q_1 b_2|$$

Remark 3. Let b_1, b_2 be binomials as in Definition 3.3. If $0 \neq s(b_1, b_2)$, then $s(b_1, b_2)$ has a two step reduction up to 0 mod $\{b_1, b_2\}$.

Let G be a reduced and normalized Gröbner basis of I with respect to $<$ (consisting of ρ-homogenous binomials).

Definition 3.4. Let $\prec$ be defined for the binomials of G as follows. For b, b' in G, $b \prec b'$ if and only if either $\rho(b) > \rho(b')$ or $\rho(b) = \rho(b')$ and $\mathrm{lt}\,(b) < \mathrm{lt}\,(b')$.

We now state and prove some lemmata using the previous notation.

Lemma 3.5. *Let G' be a proper subset of G such that $G' \cdot R = I$. Then we have*:

Each $b \in G \setminus G'$ is obtained by a Buchberger algorithm applied to G', i.e., there is a directed tree as described above ending in b having the following additional properties.

(a) *The vertices of this tree consist of ρ-homogeneous normalized binomials contained in I.*

(b) *Each vertex of incoming degree zero is immediately followed by a vertex of incoming degree two.*

Proof. Since G is a reduced and normalized Gröbner basis of I, G is uniquely determined by I and the given term order $<$. Moreover, G is produced by a Buchberger algorithm applied to a generating set of I. This proves the first part of the statement.

Now (a) is clear by our previously stated assumptions for a Gröbner algorithm. Property (b) follows since G' is part of a reduced (and normalized) Gröbner basis. □

Lemma 3.6. *Let $f \in I$, $f \neq 0$. Assume that G' is a subset of G such that $b' \in G'$ for all $b' \in G$ with $\rho(b') \leq \rho(f)$.*

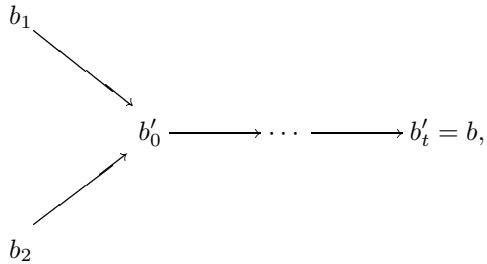
Then f can be reduced by an element of G'. Consequently, f reduces to 0 by elements of G'.

Proof. This is immediate from the definitions of G and G'. □

Remark 4. A consequence of Lemma 3.6 is: If $f \xrightarrow{b} g$ with $b \in G$ and $g \in R$ then $b \in G'$.

Lemma 3.7. *Let G' be a proper subset of G such that $G' \cdot R = I$. Let $b \in G \setminus G'$, and assume that $b' \in G'$ for all $b' \in G$ with $\rho(b') < \rho(b)$. Then*

(a) *The directed reduction tree of Lemma* 3.5 *to produce b by a Buchberger algorithm applied to G' has the form*



where $b_1, b_2 \in G'$, $b_1 \neq b_2$, $t \in \mathbf{N}$ and $b'_0 = s(b_1, b_2)$.

(b) *Let $t > 0$ and assume that the reduction steps $b'_j \to b'_{j+1}$, $0 \leq j < t$, are performed by $b^*_j \in G$. Then $b^*_0, \ldots, b^*_{t-1}, \in G'$ and $b \prec b^*_j$ for all $j = 0, \ldots, t-2$.*

Proof. By Lemma 3.5 (b) the Buchberger algorithm applied to G' must start with an s-polynomial formation of binomials $b_1, b_2 \in G'$, $b_1 \neq b_2$ giving b'_0. Assume this s-polynomial formation would be followed after a possibly empty chain $b'_0 \to \cdots \to b'_t$, $t \in \mathbf{N}$, of reductions by another s-polynomial formation resulting in a binomial b''_0. We then have $\rho(b'_0) = \rho(b'_t) < \rho(b''_0) \leq \rho(b)$. Thus we have $b' \in G'$ for all $b' \in G$ with $\rho(b') \leq \rho(b'_t)$ by our assumption. Since $b'_t \in I$ and $b'_t \neq 0$ (otherwise the s-polynomial formation following the vertex b'_t would be impossible), b'_t is reducible by an element of G' by Lemma 3.6. But this contradicts our preference rule 1. Thus $b'_t = b$, which proves (a).

(b) It is clear by the structure of the Buchberger algorithm and by our preference rules that for the reductions following the first s-polynomial formation we can only use elements of G'. Therefore, $b^*_0, \ldots, b^*_{t-1} \in G'$. Let $0 \leq j < t$, set $b^* := b^*_j$ and consider the reduction step $b'_j \xrightarrow{b^*} b'_{j+1}$.

Case 1. $\mathbf{lt}\,(b'_j) > \mathbf{lt}\,(b)$**.** Then in some step $\mathrm{lt}\,(b'_j)$ has to have a reduction down. By our preference rule 3 this must happen immediately, i.e., $\mathrm{lt}\,(b^*) \mid \mathrm{lt}\,(b'_j)$. If $\mathrm{lt}\,(b^*) \parallel \mathrm{lt}\,(b'_j)$, then $\rho(b^*) < \rho(b'_j) = \rho(b)$. If $\mathrm{lt}\,(b^*) = \mathrm{lt}\,(b'_j)$, then $\rho(b^*) = \rho(b'_j) = \rho(b)$ and also $\mathrm{lt}\,(b^*) = \mathrm{lt}\,(b'_j) > \mathrm{lt}\,(b)$.

In any case $b \prec b^*$.

Case 2. $\mathbf{lt}\,(b'_j) \leq \mathbf{lt}\,(b)$**.** Then $\mathrm{lt}\,(b'_j) = \mathrm{lt}\,(b)$ since reduction lowers terms. Since b is irreducible modulo $G\backslash\{b\}$, $\mathrm{lt}\,(b'_j)$ is irreducible modulo G', i.e., $\mathrm{lt}\,(b^*) \nmid \mathrm{lt}\,(b'_j)$. Therefore $\mathrm{lt}\,(b^*) \mid \mathrm{nlt}\,(b'_j)$. As before we conclude that $\mathrm{lt}\,(b^*) \parallel \mathrm{nlt}\,(b'_j)$ implies $\rho(b^*) < \rho(b'_j) = \rho(b)$, i.e., $b \prec b^*$.

So assume $\mathrm{lt}\,(b^*) = \mathrm{nlt}\,(b'_j)$, i.e., $b'_{j+1} = b'_j + b^*$. Since $b^* \in G' \subseteq G$, $\mathrm{nlt}\,(b^*)$ is reduced mod$G$, and this implies $b'_{j+1} = b'_j + b^* = b$ and therefore $j = t - 1$. □

The following algorithm $\mathfrak{A}$ defines a subset F of G as follows:

begin
  F:=G, H:=G
  while $H \neq \varnothing$ do
    take $b \in H$ minimal with respect to $\prec, F_b := \{b\}$, $H := H\backslash\{b\}$
    while $F_b \neq \varnothing$ do
      if $0 \in F_b$ then $F := F \setminus \{b\}$
      else
        choose $c \in F_b$
        $F_b := (F_b \setminus \{c\}) \cup \{|c - \frac{\mathrm{nlt}\,(c)}{\mathrm{nlt}\,(b')} b'| \mid b' \in H, \mathrm{nlt}\,(b') | \mathrm{nlt}\,(c)\}$
end

Remark 5. By Corollary 1.4, $\mathfrak{A}$ terminates.

Theorem 3.8. *The set F, produced by the algorithm $\mathfrak{A}$ from the given Gröbner basis G, is a minimal ρ-homogeneous generating set of binomials of I.*

Proof. By Remark 5 all that is needed is correctness for $\mathfrak{A}$. F is part of a homogeneous generating set, minimal in number, from

which the uniquely determined reduced and normalized Gröbner basis is obtainable (this follows by Lemmata 3.5, 3.6, 3.7). Therefore F is a minimal generating set. □

In the next corollary we give a slight modification of the algorithm $\mathfrak{A}$. This allows us to finish the inner "while"-loop probably earlier than in the original version.

Corollary 3.9. *Assume F' is obtained from F by also deleting any binomial b, which becomes divisible by an indeterminate during the "while" loop of $\mathfrak{A}$. Then $F'R = FR$.*

Proof. $F'R \neq FR$ contradicts the graded Nakayama lemma. □

Remark 6. We note that our binomial ideal I is of the form $I = I_L$ with L a subgroup of $\mathbf{Z}^r$ (see Definition 2.1); thus, $I : x_i = I$ for all $i = 1, \ldots, r$. Therefore, if a binomial $b \in I$ is divisible by a variable x_i, then $b \in \mathfrak{m}I$.

Remark 7. For completeness there are algorithms for minimal generating sets for some binomial ideals in [**4, 5**]. The results in Section 4 depend strictly upon algorithm $\mathfrak{A}$.

4. An application. Assume throughout this section that $n_1, \ldots, n_r$ are positive integers with $\gcd(n_1, \ldots, n_r) = 1$.

Let $\rho : \mathbf{N}^r \to \mathbf{N}$ be a function as introduced in Section 1. Assume throughout this part of Section 4 that ρ is linear, i.e., $\rho = f|_{\mathbf{N}^r}$, where $f : \mathbf{Z}^r \to \mathbf{Z}$ is a linear map and we have $\rho(e_i) = n_i$ (e_i as before, $i = 1, \ldots, r$).

Let $<$ be an admissible term order on T (or equivalently, on $\mathbf{N}^r$), set $L := \ker f$. Then $I_L = \mathfrak{p}(n_1, \ldots, n_r) =: \mathfrak{p}$ as before. As already mentioned in Section 2, Example 2, $\mathfrak{p}$ is a ρ-homogeneous prime ideal in R with $\dim R/\mathfrak{p} = 1$. (More precisely, $R/\mathfrak{p} \cong K[t^{n_1}, \ldots, t^{n_r}] \subseteq K[t]$, t an indeterminate.)

Assume $P := P_L$ is a Patil basis of $\mathfrak{p}$ with respect to $<$. Since $x_i \notin \mathfrak{p}$ for all $i = 1, \ldots, r$ we can use the version of Corollary 3.9 if we want

to apply our algorithm $\mathfrak{A}$ of Section 3 to P. (Note that P is a reduced and normalized Gröbner basis of $\mathfrak{p}$ with respect to the term order $<'$, see Definition 2.4 and Proposition 2.8.)

If $\mu \in \mathbf{N}^r$ we also will write $\sigma(x^\mu)$ instead of $x^{\sigma(\mu)}$, i.e., if $m \in T$, $m = x^\mu$, then $\sigma(m) := x^{\sigma(\mu)}$, see Definition 2.3.

Definition 4.1. For $i = 1, \ldots, r$ we define

$$\alpha_i := \min\{\alpha \in \mathbf{N}^+ \mid x_i^\alpha - m \in \mathfrak{p} \text{ for some } m \in T \setminus \{x_i^\alpha\}\}.$$

Remark 8. If $n_i = q_i d_{ij}$, $n_j = q_j d_{ij}$, $n_i \neq n_j$, $\gcd(n_i, n_j) = d_{ij}$, then $x_i^{q_j} - x_j^{q_i} \in \mathfrak{p}$; thus, $q_j = \alpha_i$.

Proposition 4.2. (1) *For each $i = 1, \ldots, r$ there exists at least one $m \in T$ such that $|x_i^{\alpha_i} - m| \in P$. If, in addition, $m = \sigma(x_i^{\alpha_i})$ then $x_i^{\alpha_i} - \sigma(x_i^{\alpha_i})$ is the unique binomial in P with a pure power of x_i in its support.*

(2) *Assume $m_1 - m_2 \in \mathfrak{p}$ and $m - \sigma(m) \in P$. If $mm_2 < m_1\sigma(m)$ and $m_2 | \sigma(m)$, then m and m_1 are relatively prime.*

(3) *Let $<$ be the lexicographical term order on T given by $x_1 > x_2 > \cdots > x_r$ and assume $\widetilde{m} - x_i^\gamma \in \mathfrak{p}$, $m - x_i^\beta \in P$, $1 \leq i \leq r$, with $x_i^\beta = \sigma(m)$ and $\gamma \leq \beta$.*

If $\gamma < \beta$ or $m < \widetilde{m}$, then m and $\widetilde{m}$ are relatively prime.

Proof. (1) is immediate since P is a reduced and normalized Gröbner basis of $\mathfrak{p}$ with respect to the term order $<'$ (see Definition 2.4 and Proposition 2.8).

To prove (2) assume $x_j \mid m$ and $x_j \mid m_1$ for some $j, 1 \leq j \leq r$. Then we have with $m' := m_2^{-1}\sigma(m) \in T$ and $b := x_j^{-1}m - x_j^{-1}m_1 m' = x_j^{-1}(m - \sigma(m) - m'(m_1 - m_2)) \in \mathfrak{p} : x_j = \mathfrak{p}$ and $\mathrm{lt}_{<'} b = x_j^{-1}m$. Therefore, $x_j^{-1}m$ possesses a reduction mod$P$, i.e., there is a $\mu \in M$ such that $x^\mu = \mathrm{lt}_{<'}(x^\mu - x^{\sigma(\mu)}) \mid x_j^{-1}m$. But then $x^\mu \parallel m$, a contradiction (see Remark 1).

(3) Since $x_i^\beta = \sigma(m) > m$, we have $i < j$ ($<$ in $\mathbf{N}$) for all $j \in \mathbf{N}$ with $x_j \mid m$. Therefore, $mx_i^\gamma < \widetilde{m}x_i^\beta$ and (3) follows from (2). □

Corollary 4.3. *Let $<$ be a term order with $t < x_1$, for all terms $t \in K[x_2, \ldots, x_r]$. Let $p \in \{2, \ldots, r\}$, and assume that there is an $m \in T$ with $x_1 \mid m$ and $x_p^{\alpha_p} - m \in \mathfrak{p}$.*

Then $x_p^{\alpha_p} < \sigma(x_p^{\alpha_p})$, $x_p^{\alpha_p} - \sigma(x_p^{\alpha_p}) \in P$, and this binomial is the only binomial in P with a pure power of x_p in its support. It is not contained in $K[x_2, \ldots, x_r]$.

Proof. Since $x_1 \mid m$ we have $x_p^{\alpha_p} < m$, and therefore $x_p^{\alpha_p} < m \leq \sigma(m) = \sigma(x_p^{\alpha_p})$. Then $x_1 \mid \sigma(x_p^{\alpha_p})$ by our assumption on $<$.

Let $b' := x_p^{\alpha_p} - m$ $(\in \mathfrak{p})$. Since $\mathrm{lt}_{<'}(b') = x_p^{\alpha_p}$, there is a $b \in P$ with $\mathrm{lt}_{<'} b \mid x_p^{\alpha_p}$, i.e., $\mathrm{lt}_{<'} b = x_p^{\alpha_p}$ by Proposition 4.2 (3) and by the minimality of α_p. Then $b = x_p^{\alpha_p} - \sigma(x_p^{\alpha_p})$, and this is the unique binomial in P with a pure power of x_p in its support by Proposition 4.2 (1). It is clear that $b \notin K[x_2, \ldots, x_r]$ (since $x_1 \mid \sigma(x_p^{\alpha_p})$). □

Assume for the remainder of Section 4 that $r = 4$, $I_L = \mathfrak{p}(n_1, n_2, n_3, n_4) =: \mathfrak{p}$ and P is a Patil bases for $\mathfrak{p}$ with respect to a given term order $<$ on T (or equivalently on $\mathbf{N}^4$). In order to indicate the term order under consideration we sometimes write $P_<$. To obtain minimal generating sets for $\mathfrak{p}$ from P, we consider the following two cases where the situation described in Case 2 is the more general one:

Case 1. There are $i, j, k, l \in \mathbf{N}$ with $\{i, j, k, l\} = \{1, 2, 3, 4\}$ and $m_j, m_k, m_l \in T$ such that $x_i \mid m_j$, $x_i \mid m_k$, $x_i \mid m_l$ and $\{x_j^{\alpha_j} - m_j, x_k^{\alpha_k} - m_k, x_l^{\alpha_l} - m_l\} \subseteq \mathfrak{p}$.

Case 2. For some 3-element subset, say $\{i, k, l\}$ of $\{1, 2, 3, 4\}$ there are $m_k, m_l \in T$ with $x_i \mid m_k$, $x_i \mid m_l$ such that $\{x_k^{\alpha_k} - m_k, x_l^{\alpha_l} - m_l\} \subseteq \mathfrak{p}$.

Using the notation introduced at the beginning of this section we have:

Theorem 4.4. *Let $P_<$ be a Patil basis of $\mathfrak{p}$ with respect to a given term order $<$ on T (or equivalently on $\mathbf{N}^4$), and denote by $F_<$ the minimal set of generators for $\mathfrak{p}$ obtained from $P_<$ by applying algorithm $\mathfrak{A}$ of Section 3. Then we have:*

(1) *Assume we are in Case 1, and let $<$ be any lexicographical term order on T with $x_i > x_j, x_k, x_l$. Then $F_< = P_<$, i.e., the Patil bases of $\mathfrak{p}$ with respect to $<$ is already a minimal generating set for $\mathfrak{p}$.*

(2) *Assume we are in Case* 2 *but not in Case* 1. *Let* $<$ *be a lexicographical term order on* T *with* $x_i > x_j > x_k, x_l$. *Then*

$$F_< = \left\{ b \in P_< \middle| x_j^{\alpha_j} \nmid \mathrm{nlt}_<(b) \right\},$$

i.e., we have for $b \in P_<$, $b = m - \sigma(m)$ $(m \in T)$: $b \notin F_<$ *if and only if* $x_j^{\alpha_j} \mid m$.

(3) *Assume we are not in Case* 2. *Then there are* $i, j, k, l \in \mathbf{N}$ *with* $\{i, j, k, l\} = \{1, 2, 3, 4\}$ *and* $x_i^{\alpha_i} - x_j^{\alpha_j}, x_k^{\alpha_k} - x_l^{\alpha_l} \in \mathfrak{p}$. *Let* $<$ *be the lexicographical term order on* T *given by* $x_i > x_j > x_k > x_l$. *Then there is a uniquely determined* $\gamma \in \mathbf{N}^+$ *with* $x_k^\gamma - \sigma(x_k^\gamma) \in P_<$, *and we have*

$$F_< = \begin{cases} P_< \setminus \{x_k^\gamma - \sigma(x_k^\gamma)\} & \text{if } x_l \mid \sigma(x_k^\gamma) \\ P_< & \text{otherwise.} \end{cases}$$

In order to prove this theorem we state and prove the following lemmata.

Lemma 4.5. *Assume we are in Case* 2, *and let* $<$ *be a lexicographical term order on* T *with* $x_i > x_j > x_k, x_l$.

If $P_< \cap K[x_j, x_k, x_l] \neq \varnothing$ *then* $P_< \cap K[x_j, x_k, x_l] = \{x_k^\gamma x_l^\delta - x_j^{\alpha_j}\}$ *for suitable* $\gamma, \delta \in \mathbf{N}^+$. *Moreover,* $x_k^\gamma x_l^\delta - x_j^{\alpha_j}$ *is the only binomial in* $P_<$ *with* $x_j^{\alpha_j}$ *in its support.*

Proof. Assume without loss of generality that $i = 1$, $j = 2$, $k = 3$, $l = 4$. For $p = 3, 4$ let $b_p := x_p^{\alpha_p} - \sigma(x_p^{\alpha_p})$. By Corollary 4.3 we have: $b_p \in P_< =: P, b_p$ is the only binomial in P with a pure power of x_p in its support and $b_p \notin K[x_2, x_3, x_4]$, $p = 3, 4$.

Assume now that $P \cap K[x_2, x_3, x_4] \neq \varnothing$, and let $b \in P \cap K[x_2, x_3, x_4]$. Since b is irreducible, b contains a pure power in one of the indeterminates x_2, x_3 or x_4 in its support. By our previous considerations b cannot contain a pure power in x_3 or x_4 since otherwise $b = b_3$ or $b = b_4$, and therefore $b \notin K[x_2, x_3, x_4]$, a contradiction. Thus, $b = x_3^\beta x_4^\gamma - x_2^\alpha$ for suitable $\alpha, \beta, \gamma \in \mathbf{N}^+$. It is clear that $\alpha \geq \alpha_2$ and $x_2^\alpha = \sigma(x_3^\beta x_4^\gamma)$ (since $b \in P$). Now let $b' \in P \cap K[x_2, x_3, x_4]$ be another binomial. Then again $b' = x_3^{\beta'} x_4^{\gamma'} - x_2^{\alpha'}$ for suitable $\alpha', \beta', \gamma' \in \mathbf{N}^+$, $\alpha' \geq \alpha_2$ and

$x_2^{\alpha'} = \sigma(x_3^{\beta'} x_4^{\gamma'})$. Now Proposition 4.2 (3) implies $\alpha = \alpha'$ and therefore we have $\sigma(x_3^{\beta} x_4^{\gamma}) = \sigma(x_3^{\beta'} x_4^{\gamma'})$. But then $x_3^{\beta} x_4^{\gamma} = x_3^{\gamma'} x_4^{\beta'}$ by Proposition 4.2 (2), i.e., $b' = b$.

Now by Proposition 4.2 (1) there is an $m \in T$ with $|m - x_2^{\alpha_2}| \in P$. If $x_1 \mid m$, then $x_2^{\alpha_2} - m$ is the only binomial in P with a pure power in x_2 in its support by Proposition 4.2 (1) since then $m > x_2^{\alpha_2}$, and therefore $m = \sigma(x_2^{\alpha_2})$. But this is a contradiction, since $b \in P$ also has a pure power in x_2 in its support, but $b \in K[x_2, x_3, x_4]$, $x_2^{\alpha_2} - m \notin K[x_2, x_3, x_4]$, and therefore $b \neq x_2^{\alpha_2} - m$.

Hence $x_1 \nmid m$, i.e., $m - x_2^{\alpha_2} \in P \cap K[x_2, x_3, x_4]$. Therefore, $m - x_2^{\alpha_2} = b$, i.e., $\alpha = \alpha_2$. □

Lemma 4.6. *Suppose we are in Case* 2 *but not in Case* 1.

(1) *If* $m \in T \setminus \{x_j^{\alpha_j}\}$ *with* $x_j^{\alpha_j} - m \in \mathfrak{p}$, *then* $x_i \nmid m$ *and* $x_k \cdot x_l \mid m$.

(2) *If* $m \in T$ *with* $x_i^{\alpha_i} - m \in \mathfrak{p}$, *then* $x_j^{\alpha_j} \nmid m$.

(3) *Assume* $b \in \mathfrak{p}$, $b = m_1 - m_2$ $(m_1, m_2 \in T)$ *with* $x_j^{\alpha_j} \mid m_1, x_i \mid m_2$. *If* $m_2 \in (x_k, x_l) \cdot R$, *then* $b \in \mathfrak{m} \cdot \mathfrak{p}$.

Proof. Assume without loss of generality $i = 1$, $j = 2$, $k = 3$, $l = 4$.

(1) $x_1 \nmid m$ is immediate since we are not in Case 1. By the minimality of α_2 we have $x_2 \nmid m$, i.e., $m \in K[x_3, x_4]$. If $m = x_3^{\gamma}$ with $\gamma \in \mathbf{N}^+$, then $\gamma \geq \alpha_3$ and $x_j^{\alpha_j} - x_3^{\gamma - \alpha_3} m_3 = x_j^{\alpha_j} - m + x_3^{\gamma - \alpha_3}(x_3^{\alpha_3} - m_3) \in \mathfrak{p}$. But $x_1 \mid m_3$, contradicting the fact proved just before.

Using the same argument we see that m cannot be a pure power of x_4, and therefore $x_3 \cdot x_4 \mid m$.

(2) Suppose there is an $m \in T$ with $x_2^{\alpha_2} \mid m$ and $x_1^{\alpha_1} - m \in \mathfrak{p}$. Let $<$ be the lexicographical term order given by $x_1 > x_2 > x_3 > x_4$. By Proposition 4.2 (1) there is an $m' \in T$ with $|x_2^{\alpha_2} - m'| \in P_<$ and (1) shows $|x_2^{\alpha_2} - m'| \in K[x_2, x_3, x_4]$, i.e., $P_< \cap K[x_2, x_3, x_4] \neq \varnothing$. By Lemma 4.5 there are $\beta, \gamma \in \mathbf{N}^+$ such that $x_3^{\beta} x_4^{\gamma} - x_2^{\alpha_2} \in P_< \subseteq \mathfrak{p}$.

If $x_4 \mid m_3$ or $x_3 \mid m_4$, we are then in Case 1, since $x_1^{\alpha_1} - m x_2^{-\alpha_2} x_3^{\beta} x_4^{\gamma} = x_1^{\alpha_1} - m - m x_2^{-\alpha_2}(x_3^{\beta} x_4^{\gamma} - x_2^{\alpha_2}) \in \mathfrak{p}$ (take $i = 4$ or $i = 3$, $j = 1, m_j = m x_2^{-\alpha_2} x_3^{\beta} x_4^{\gamma}$, $k = 2$, $m_k = x_3^{\beta} x_4^{\gamma}$ and $l = 3$ or $l = 4$), a contradiction.

Therefore, $m_3, m_4 \in K[x_1, x_2]$ since $x_3 \nmid m_3$ and $x_4 \nmid m_4$ by the minimality of α_3 and α_4. Assume $x_2 \nmid m_3$. Then $m_3 = x_1^{\delta}$ with

$\delta \in \mathbf{N}^+$. Clearly $\delta \geq \alpha_1$, and we get with $m_3' := x_1^{\delta-\alpha_1} m : x_3^{\alpha_3} - m_3' = x_3^{\alpha_3} - x_1^{\delta} + x_1^{\delta-\alpha_1}(x_1^{\alpha_1} - m) \in \mathfrak{p}$. Since $x_2 \mid m_3'$, we can assume without loss of generality that $x_2 \mid m_3$ and, using the same argument, $x_2 \mid m_4$. But then we are again in Case 1 with $i = 2$, $j = 1$, $m_j = m$, $k = 3$ and $l = 4$, a contradiction, and this proves (2).

(3) By (1) we have $x_2^{\alpha_2} \parallel m_1$. Let $m' := m_1 x_2^{-\alpha_2} \in T$. Then $m' \in \mathfrak{m}$. Choose $m \in T \setminus \{x_2^{\alpha_2}\}$ with $x_2^{\alpha_2} - m \in \mathfrak{p}$. Then $x_3 x_4 \mid m$ by (1). Now $b = m'(x_2^{\alpha_2} - m) + m'm - m_2$. Assume without loss of generality that $x_3 \mid m_2$. Then $m'm - m_2 = x_3 b'$ with a binomial $b' \in R$, and we get $x_3 b' = b - m'(x_2^{\alpha_2} - m) \in \mathfrak{p}$; therefore, $b' \in \mathfrak{p} : x_3 = \mathfrak{p}$. But this implies $b = m'(x_2^{\alpha_2} - m) + x_3 b' \in \mathfrak{m}\mathfrak{p}$. □

Lemma 4.7. *The following conditions are equivalent*:

(i) *Case* 2 *does not hold for* $\mathfrak{p}$.

(ii) *There are* $i, j, k, l \in \mathbf{N}$ *with* $\{i, j, k, l\} = \{1, 2, 3, 4\}$ *such that* $x_i^{\alpha_i} - x_j^{\alpha_j}$, $x_k^{\alpha_k} - x_l^{\alpha_l} \in \mathfrak{p}$, *and both these binomials are the only ones in* $\mathfrak{p}$ *containing one of the powers* $x_1^{\alpha_1}$, $x_2^{\alpha_2}$, $x_3^{\alpha_3}$ *or* $x_4^{\alpha_4}$ *in their support.*

Proof. (i) ⇒ (ii). For $p \in \{1, 2, 3, 4\}$, let $A_p := \{i_p \mid x_{i_p} \mid m_p, x_p^{\alpha_p} - m_p \in \mathfrak{p}\}$. Since we are not in Case 2, the sets A_p are pairwise distinct and $p \notin A_p$.

Let $j := i_1$. Then $j \neq 1$ and $m_1 = x_j^{\beta}$ with $\beta \in \mathbf{N}^+$, $\beta \geq \alpha_j$. Let $q := i_j$. Then $q \neq j$ and $m_j = x_q^{\gamma}$ with $\gamma \in \mathbf{N}^+$, $\gamma \geq \alpha_q$, and we get $x_1^{\alpha_1} - x_j^{\beta-\alpha_j} x_q^{\gamma} = x_1^{\alpha_1} - x_j^{\beta} + x_j^{\beta-\alpha_j}(x_j^{\alpha_j} - x_q^{\gamma}) \in \mathfrak{p}$.

By the uniqueness of m_1, we therefore have $\beta = \alpha_j, q = 1$ and $\gamma = \alpha_1$, i.e., $x_1^{\alpha_1} - x_j^{\alpha_j} \in \mathfrak{p}$. This is the only binomial in $\mathfrak{p}$ with $x_1^{\alpha_1}$ in its support. Repeating this argument for the remaining indeterminates we get (ii).

(ii) ⇒ (i) is immediate. □

Lemma 4.8. *Assume we are not in Case* 2. *Using the notation of Lemma* 4.7 (ii) *we have*:

(1) *Let* $<$ *be a lexicographical term order on* T *with* $x_i > x_j > x_k, x_l$. *Then* $P_< \cap K[x_j, x_k, x_l] = \{|x_l^{\alpha_l} - x_k^{\alpha_k}|\}$.

(2) *Let* $<$ *be a lexicographical term order on* T *with* $x_i, x_j > x_k > x_l$. *Then* $P_< \cap K[x_i, x_j, x_l] = \{|x_j^{\alpha_j} - x_i^{\alpha_i}|\}$.

Proof. (1) Let $b \in P_< \cap K[x_j, x_k, x_l]$, and assume without loss of generality that $x_k > x_l$. Let $b = m_1 - m_2$ $(m_1, m_2 \in T)$, $m_1 < m_2$. Since $x_i \nmid m_1, x_i \nmid m_2$, we therefore have $x_j \nmid m_1$ (otherwise $m_1 > m_2$). By Proposition 4.2 (1) $x_j^{\alpha_j} - x_i^{\alpha_i}$ and $x_l^{\alpha_l} - x_k^{\alpha_k}$ are contained in $P_< =: P$, and they are the only binomials in P with a pure power of x_j and x_l, respectively, in their support.

Let $m_1 = x_k^\gamma x_l^\delta$ with $\gamma, \delta \in \mathbf{N}$. For $\gamma, \delta > 0$ we have $m_2 = x_j^\beta$ with $\beta \in \mathbf{N}^+$. Then $\beta \geq \alpha_j$, a contradiction, since this would imply that b is reducible $\bmod x_j^{\alpha_j} - x_i^{\alpha_i} \in P$. Therefore, $\gamma = 0$ or $\delta = 0$. If $\gamma > 0$, i.e., $m_1 = x_k^\gamma$, we have $\gamma \geq \alpha_k$ and $m_2 = x_j^\beta x_l^\varepsilon$ with $\beta, \varepsilon \in \mathbf{N}$, and $\beta < \alpha_j$, $\varepsilon < \alpha_l$ (otherwise b would be reducible $\bmod x_j^{\alpha_j} - x_i^{\alpha_i}$ or $x_l^{\alpha_l} - x_k^{\alpha_k}$). But then $x_k^{\alpha_k} x_l^\varepsilon (x_k^{\gamma-\alpha_k} x_l^{\alpha_l - \varepsilon} - x_j^\beta) = x_l^{\alpha_l} b + x_j^\beta x_l^\varepsilon (x_l^{\alpha_l} - x_k^{\alpha_k}) \in \mathfrak{p}$, and therefore $x_k^{\gamma-\alpha_k} x_l^{\alpha_l - \epsilon} - x_j^\beta \in \mathfrak{p}$, a contradiction, since $\beta < \alpha_j$. Thus $\gamma = 0, \delta > 0$, i.e., $b = x_l^{\alpha_l} - x_k^{\alpha_k}$ since $x_l^{\alpha_l} - x_k^{\alpha_k}$ is the only binomial in P with a pure power of x_l in its support by Proposition 4.2 (1).

(2) Assume without loss of generality that $x_i > x_j$, and let $b \in P_< \cap K[x_i, x_j, x_l]$, $b = m_1 - m_2$ $(m_1, m_2 \in T)$, $m_1 < m_2$. Then $x_i \nmid m_1$. If $x_j \nmid m_1$, i.e., $m_1 = x_l^\delta$, $\delta \in \mathbf{N}^+, b$ would be reducible $\bmod x_l^{\alpha_l} - x_k^{\alpha_k} \in P_< =: P$ since then $\delta \geq \alpha_l$, a contradiction. Therefore, $x_j \mid m_1$ and $m_1 = x_j^\beta x_l^\delta$ with $\beta, \delta \in \mathbf{N}$, $\beta > 0$. Clearly, $\beta \leq \alpha_j$ and $\delta < \alpha_l$, since otherwise b would be reducible $\bmod P$. If $\delta > 0$ we have $m_2 = x_i^\alpha$ with $\alpha \in \mathbf{N}^+$ and $\alpha \geq \alpha_i$. But then $x_j^\beta (x_l^\delta - x_i^{\alpha-\alpha_i} x_j^{\alpha_j - \beta}) = b - x_i^{\alpha-\alpha_i}(x_j^{\alpha_j} - x_i^{\alpha_i}) \in \mathfrak{p}$, i.e., $x_l^\delta - x_i^{\alpha-\alpha_i} x_j^{\alpha_j-\beta} \in \mathfrak{p}$, a contradiction, since $\delta < \alpha_l$. Therefore, $\delta = 0$, i.e., $m_1 = x_j^\beta$. By Proposition 4.2 (1) we now get $b = x_j^{\alpha_j} - x_i^{\alpha_i}$ since $x_j^{\alpha_j} - x_i^{\alpha_i}$ is the only binomial in P with a pure power of x_j in its support. □

Proof of Theorem 4.4. (1) Assume without loss of generality that $i = 1$, $j = 2$, $k = 3$, $l = 4$ and that $<$ is given by $x_1 > x_2 > x_3 > x_4$. Suppose there is a $b \in P_< =: P$ with $(P \setminus \{b\}) \cdot R = \mathfrak{p}$. Let $b = m_1 - m_2$, $m_1 < m_2$ $(m_1, m_2 \in T)$. Since $b \in (P \setminus \{b\}) \cdot R$ there must be a $\widetilde{b} \in P \setminus \{b\}$, $\widetilde{b} = \widetilde{m}_1 - \widetilde{m}_2$, $\widetilde{m}_1 < \widetilde{m}_2$ $(\widetilde{m}_1, \widetilde{m}_2 \in T)$ with $\widetilde{m}_2 \mid m_1$. (Note that $\mathrm{lt}_{<'}(b') \nmid m_1$ for all $b' \in P \setminus \{b\}$, since P is a reduced Gröbner basis for $<'$). Since b is irreducible and $m_1 < m_2$, we have $x_1 \nmid m_1$ and therefore $x_1 \nmid \widetilde{m}_2$. Thus, $\widetilde{b} \in P \cap K[x_2, x_3, x_4]$, and hence $\widetilde{b} = x_3^\beta x_4^\delta - x_2^{\alpha_2}$ for suitable $\beta, \gamma \in \mathbf{N}^+$ by Lemma 4.5.

But this contradicts Corollary 4.3 which says that $x_2^{\alpha_2} - \sigma(x_2^{\alpha_2})$ is the only binomial in P with a pure power of x_2 in its support and $x_2^{\alpha_2} - \sigma(x_2^{\alpha_2}) \notin K[x_2, x_3, x_4]$. This proves (1).

(2) Assume without loss of generality that $i = 1$, $j = 2$, $k = 3$, $l = 4$ and that $x_1 > x_2 > x_3 > x_4$. Let $b \in P_< =: P$, $b = m_1 - m_2$, $m_1 < m_2$ $(m_1, m_2 \in T)$. Assume $b \notin F$. By our algorithm $\mathfrak{A}$ there is a sequence of reductions up to b using elements of $P \setminus \{b\}$ ending in 0. Among these reductions a reduction must occur of m_1, since otherwise $m_1 (= \operatorname{lt}_{<'} b)$ would be a multiple of the leading term (with respect to $<'$) of some $b' \in P \setminus \{b\}$ contradicting the fact that P is a reduced Gröbner basis.

Therefore, there is some $\widetilde{b} \in P \setminus \{b\}$, $\widetilde{b} = \widetilde{m}_1 - \widetilde{m}_2$, $\widetilde{m}_1 < \widetilde{m}_2$ $(\widetilde{m}_1, \widetilde{m}_2 \in T)$ with $\widetilde{m}_2 \mid m_1$. Since b is irreducible and $m_1 < m_2$, we get $x_1 \nmid m_1$; therefore, $x_1 \nmid \widetilde{m}_2$, i.e., $\widetilde{b} \in K[x_2, x_3, x_4]$. By Lemma 4.5 we obtain $\widetilde{b} = x_3^{\beta} x_4^{\gamma} - x_2^{\alpha_2}$ for suitable $\beta, \gamma \in \mathbf{N}^+$ and this implies $x_2^{\alpha_2} = \widetilde{m}_2 \mid m_1 = \operatorname{nlt}_< b$. Therefore, $\{b \in P \mid x_2^{\alpha_2} \nmid \operatorname{nlt}_< b\} \subseteq F$.

Next let $b \in P$, $b = m_1 - m_2$, $m_1 < m_2$ $(m_1, m_2 \in T)$, and suppose $x_2^{\alpha_2} | m_1$. Then $x_2 \nmid m_2$ since b is irreducible. If $m_2 \in (x_3, x_4) \cdot R$ then $b \in \mathfrak{mp}$ by Lemma 4.6 (3) and therefore $b \notin F$ by Corollary 3.9. Now assume that $m_2 \notin (x_3, x_4) \cdot R$, i.e., $x_3 \nmid m_2$ and $x_4 \nmid m_2$. Then $m_2 = x_1^{\alpha}$ for some $\alpha \in \mathbf{N}^+$ and $\alpha \geq \alpha_1$. Lemma 4.6 (2) shows that $\alpha > \alpha_1$ (since $x_2^{\alpha_2} \mid m_1$). By Proposition 4.2 (1) there is an $m \in T$ with $|x_1^{\alpha_1} - m| \in P$. Since $x_1 \nmid m$, $m < x_1^{\alpha_1}$, i.e., $m - x_1^{\alpha_1} \in P$. Since $\alpha_1 < \alpha$ we have $\rho(m - x_1^{\alpha_1}) < \rho(b)$, i.e., $b \prec m - x_1^{\alpha_1}$ where $\prec$ is the order on P derived form $<'$, see Definition 3.4.

Therefore, $m - x_1^{\alpha_1}$ can be used for a reduction up of b when b is "tested" in the outer "while"-loop of the algorithm $\mathfrak{A}'$ of Corollary 3.9. The result of such a reduction up of b (via $m_1 = x_1^{\alpha}$) is $b' := m_1 - x_1^{\alpha - \alpha_1} m \in \mathfrak{p}$. If $x_3 \mid m$ or $x_4 \mid m$, then $b' \in \mathfrak{mp}$ by Lemma 4.6 (3) and $b \notin F$ by Corollary 3.9. Suppose $x_3 \nmid m$, $x_4 \nmid m$, i.e., $m = x_2^{\beta}$ with $\beta \in \mathbf{N}^+$. Then $b' = x_2 b''$ with $b'' \in R$ and $b'' \in \mathfrak{p} : x_2 = \mathfrak{p}$. Again $b' \in \mathfrak{mp}$, and therefore $b \notin F$ by Corollary 3.9. This shows (2).

(3) Since $x_k^{n_i} - x_i^{n_k} \in \mathfrak{p}$, there must be a $b \in P_< =: P$ such that $\operatorname{lt}_{<'}(b) | \operatorname{lt}_{<'}(x_k^{n_i} - x_i^{n_k}) = x_k^{n_i}$, i.e., $\operatorname{lt}_{<'}(b) = x_k^{\gamma}$ with $\gamma \in \mathbf{N}^+$. It is then clear that $b = x_k^{\gamma} - \sigma(x_k^{\gamma})$ and $x_k^{\gamma} < \sigma(x_k^{\gamma})$. Since P is a reduced Gröbner basis with respect to $<'$ there is only one binomial in P of this form.

Assume now without loss of generality that $i = 1$, $j = 2$, $k = 3$, $l = 4$. By Lemma 4.8 and Proposition 4.2 (1) we have $x_2^{\alpha_2} - x_1^{\alpha_1}$, $x_4^{\alpha_4} - x_3^{\alpha_3} \in P$. By the minimality of α_3 we have $\gamma \geq \alpha_3$, and since P is a reduced Gröbner basis of $\mathfrak{p}$ with respect to $<'$, $\gamma > \alpha_3$. Assume $x_4 \mid \sigma(x_3^\gamma)$. Then $x_3^\gamma - \sigma(x_3^\gamma) = x_4 b' - x_3^{\gamma-\alpha_3}\,(x_4^{\alpha_4} - x_3^{\alpha_3})$, where $b' := x_3^{\gamma-\alpha_3} x_4^{\alpha_4-1} - x_4^{-1}\sigma(x_3^\gamma)$. Since $x_4 b' \in \mathfrak{p}$ we have $b' \in \mathfrak{p} : x_4 = \mathfrak{p}$, i.e., $x_3^\gamma - \sigma(x_3^\gamma) \in \mathfrak{mp}$, and therefore $x_3^\gamma - \sigma(x_3^\gamma) \notin F_< =: F$ by Corollary 3.9.

Assume now that there is a $b \in P$ with $b \notin F$. We need to show that $b = x_3^\gamma - \sigma(x_3^\gamma)$ and $x_4 \mid \sigma(x_3^\gamma)$. Let $b = m_1 - m_2$ with $m_1, m_2 \in T$, $m_1 < m_2$. Then $x_1 \nmid m_1$. By our algorithm $\mathfrak{A}$ there is a chain of reductions up of b (with respect to $<'$) ending in 0. Since P is a reduced Gröbner basis of $\mathfrak{p}$ with respect to $<'$, $\mathrm{lt}_{<'}(\widetilde{b}) \nmid m_1 = \mathrm{lt}_{<'}(b)$ for all $\widetilde{b} \in P \setminus \{b\}$, i.e., a reduction of m_1 must occur. Assume this reduction step is performed using $\widetilde{b} \in P, \widetilde{b} = \widetilde{m}_1 - \widetilde{m}_2$, with $\widetilde{m}_1, \widetilde{m}_2 \in T$, $\widetilde{m}_1 < \widetilde{m}_2$. Then $\widetilde{m}_2 \mid m_1$, and therefore $x_1 \nmid \widetilde{m}_2$. Since $\widetilde{m}_1 < \widetilde{m}_2$, this implies $x_1 \nmid \widetilde{m}_1$, i.e., $\widetilde{b} \in P \cap K[x_2, x_3, x_4] = \{x_4^{\alpha_4} - x_3^{\alpha_3}\}$ by Lemma 4.8 (1). Hence $x_3^{\alpha_3} \mid m_1$, and thus $x_3 \nmid m_2$. Since P is a reduced Gröbner basis of $\mathfrak{p}$ with respect to $<'$ and $b, x_4^{\alpha_4} - x_3^{\alpha_3}$ are in P, we have $x_3^{\alpha_3} \parallel m_1 = \mathrm{lt}_{<'}(b)$.

Suppose $x_4 \nmid m_2$. Then $m_2 = x_1^\alpha x_2^\beta$ with $\alpha, \beta \in \mathbf{N}$ and $\beta < \alpha_2$ (since P is reduced and b, $x_2^{\alpha_2} - x_1^{\alpha_1} \in P$). Hence $\alpha > 0$ (by the minimality of α_2). Suppose $x_2 | m_1$. Then $\beta = 0$ and $x_1^\alpha = \sigma(m_1)$. Since $x_2^{\alpha_2} - x_1^{\alpha_1} \in P$, and therefore $x_1^{\alpha_1} = \sigma(x_2^{\alpha_2})$, we get by Proposition 4.2 (3) that m_1 and $x_2^{\alpha_2}$ are relatively prime, a contradiction. Thus $x_2 \nmid m_1$, and we have $m_1 = x_3^\varepsilon x_4^\delta$ with $\delta, \varepsilon \in \mathbf{N}$, $\varepsilon \geq \alpha_3$ and $\delta < \alpha_4$ (since P is reduced and $b, x_4^{\alpha_4} - x_3^{\alpha_3}$ are in P). Now m_2 has a reduction up by a binomial $\widetilde{b} \in P \setminus \{b\}$. Let $\widetilde{b} = \widetilde{m}_1 - \widetilde{m}_2$ with $\widetilde{m}_1, \widetilde{m}_2 \in T$, $\widetilde{m}_1 < \widetilde{m}_2$. Then $\widetilde{m}_2 \mid m_2$, and therefore $x_3 \nmid \widetilde{m}_2 = \sigma(\widetilde{m}_1)$. Since $m_2 = \sigma(m_1)$ and $m_1 \widetilde{m}_2 < \widetilde{m}_1 m_2$ if $\widetilde{m}_2 \parallel m_2, m_1$ and $\widetilde{m}_1$ are relatively prime by Proposition 4.2 (2). Since $x_3 \mid m_1$, we therefore get $x_3 \nmid \widetilde{m}_1$, i.e., $\widetilde{b} \in P \cap K[x_1, x_2, x_4] = \{x_2^{\alpha_2} - x_1^{\alpha_1}\}$ by Lemma 4.8 (2). Hence, $\widetilde{b} = x_2^{\alpha_2} - x_1^{\alpha_1}$. Performing p reductions up of m_2 using $x_2^{\alpha_2} - x_1^{\alpha_1}$ ($p \geq 1$), we obtain $x_1^{\alpha - p\alpha_1} x_2^{\beta + p\alpha_2} <' m_1$. But at some stage of the reduction up chain of m_2 (contained in the reduction up chain of b ending in 0) we must obtain a term which is bigger then m_1, i.e., after $p \geq 1$ reductions up of m_2 using $x_2^{\alpha_2} - x_1^{\alpha_1}$ there must occur a reduction up of

$x_1^{\alpha-p\alpha_1}x_2^{\beta+p\alpha_2}$ using a binomial $b^* \in P \setminus \{x_2^{\alpha_2} - x_1^{\alpha_1}\}$, say, $b^* = m_1^* - m_2^*$ with $m_1^*, m_2^* \in T$, $m_1^* < m_2^*$. Then $x_3 \nmid m_2^*$ but $x_3 \mid m_1^*$ (otherwise $b^* = x_2^{\alpha_2} - x_1^{\alpha_1}$) and $x_2 \nmid m_1^*$ (otherwise $x_2 \nmid m_2^*$, and therefore $m_2^* = x_1^{\alpha^*}, \alpha^* \in \mathbf{N}^+$, a contradiction as we have seen above when we proved that $x_2 \nmid m_1$). Therefore, $m_1^* = x_3^{\gamma^*}x_4^{\delta^*}, m_2^* = x_1^{\alpha^*}x_2^{\beta^*}$ with $\alpha^*, \beta^*, \gamma^*, \delta^* \in \mathbf{N}$ and where $\gamma^* > 0$, $0 \le \delta^* < \alpha_4$ (since P is reduced), $0 < \alpha^* \le \alpha - p\alpha_1 \le \alpha - \alpha_1$ (since $b^* \notin K[x_2, x_3, x_4]$, see Lemma 4.8 (1), and $m_2^* \mid x_1^{\alpha-p\alpha_1}x_2^{\beta+p\alpha_2}$) and $0 \le \beta^* < \alpha_2$ (since P is reduced). If $\beta^* \le \beta$, i.e., $m_2^* \parallel m_2$, we would get that m_1 and m_1^* are relatively prime by Proposition 4.2 (2), a contradiction. Hence $\beta < \beta^* < \alpha_2$. Let $c := \alpha_2 - \beta^* + \beta$. Then $0 < c < \alpha_2$, and we get with $b' := m_1x_3^{-1} - x_1^{\alpha-\alpha^*-\alpha_1}x_2^c m_1^* x_3^{-1}$: $\operatorname{lt}_{<'}(b') = m_1x_3^{-1}$ and $x_2^{\beta^*-\beta}x_3b' = x_2^{\beta^*-\beta}b - x_1^{\alpha-\alpha^*-\alpha_1}x_2^{\alpha_2}b^* - x_1^{\alpha-\alpha^*-\alpha_1}m_2^*(x_2^{\alpha_2} - x_1^{\alpha_1}) \in \mathfrak{p}$, i.e., $b' \in \mathfrak{p} : x_2^{\beta^*-\beta}x_3 = \mathfrak{p}$. Therefore, there is a $b'' \in P$ such that $\operatorname{lt}_{<'}(b'') \mid \operatorname{lt}_{<'}(b') = m_1x_3^{-1}$, i.e., $\operatorname{lt}_{<'}(b'') \mid m_1 = \operatorname{lt}_{<'}(b)$, a contradiction, since P is reduced.

Therefore $x_4 \mid m_2$ and, consequently, $x_4 \nmid m_1$.

Finally suppose $x_2 \mid m_1$. Then $b = x_2^\rho x_3^\sigma - x_1^\alpha x_4^\delta$ with $\alpha, \delta, \rho, \sigma \in \mathbf{N}$, $\sigma \ge \alpha_3$, $0 < \rho < \alpha_2$, $0 < \delta < \alpha_4$. Then $x_4^\delta(x_2^\rho x_3^{\sigma-\alpha_3}x_4^{\alpha_4-\delta} - x_1^\alpha) = x_2^\rho x_3^{\sigma-\alpha_3}(x_4^{\alpha_4} - x_3^{\alpha_3}) + b \in \mathfrak{p}$, and therefore $x_2^\rho x_3^{\sigma-\alpha_3}x_4^{\alpha_4-\delta} - x_1^\alpha \in \mathfrak{p} : x_4^\delta = \mathfrak{p}$, i.e., $\alpha \ge \alpha_1$ by the minimality of α_1. But then $m_1 = x_2^\rho x_3^\sigma$ and $x_2^{\alpha_2}$ are relatively prime by Proposition 4.2 (2), a contradiction. Therefore $x_2 \nmid m_1$, i.e., m_1 is a pure power of x_3, and hence $b = x_3^\gamma - \sigma(x_3^\gamma)$ and $x_4 \mid \sigma(x_3^\gamma)$. □

Example 4.1. 1. $n_1 = 5$, $n_2 = 6$, $n_3 = 7$, $n_4 = 9$. Then $\alpha_1 = 3$, $\alpha_2 = \alpha_3 = \alpha_4 = 2$ and $\{x_2^2 - x_1x_3, x_3^2 - x_1x_4, x_4^2 - x_1x_2x_3\} \subset \mathfrak{p} := \mathfrak{p}(5, 6, 7, 9)$.

Hence we are in Case 1 ($i = 1, j = 2, k = 3, l = 4$) and, with a lexicographical term order on T with $x_1 > x_2, x_3, x_4$, we obtain

$$\{x_2^2 - x_1x_3, x_2x_4 - x_1^3, x_3^2 - x_1x_4, x_3x_4 - x_1^2x_2, x_4^2 - x_1x_2x_3\}$$

as a Patil basis (see Remark 9 below) for $\mathfrak{p}$. By Theorem 4.4 (1) this is already a minimal generating set for $\mathfrak{p}$.

2. $n_1 = 6, n_2 = 7, n_3 = 8, n_4 = 9$. Then again $\alpha_1 = 3, \alpha_2 = \alpha_3 = \alpha_4 = 2$ and $\{x_2^2 - x_1x_3, x_4^2 - x_1^3\} \subset \mathfrak{p}(6, 7, 8, 9) =: \mathfrak{p}$. Now it is easy to see

that we are in Case 2 but not in Case 1 (take $i = 1, j = 3, k = 2, l = 4$) and, with a lexicographical term order on T with $x_1 > x_3 > x_2, x_4$, we obtain

$$\{x_2^2 - x_1x_3, x_2x_3 - x_1x_4, x_2x_4 - x_3^2, x_4^2 - x_1^3, x_3^3 - x_1^4, x_3^2x_4 - x_1^3x_2\}$$

as a Patil basis for $\mathfrak{p}$. By Theorem 4.4 (2),

$$F := \{x_2^2 - x_1x_3, x_2x_3 - x_1x_4, x_2x_4 - x_3^2, x_4^2 - x_1^3\}$$

is a minimal generating set for $\mathfrak{p}$. According to Case 2 we can also choose $i = 4, j = 2, k = 1, l = 3$. Now if $<$ is a lexicographical term order on T with $x_4 > x_2 > x_1, x_3$ then $\{x_1x_3 - x_2^2, x_2x_3 - x_1x_4, x_3^2 - x_2x_4, x_1^3 - x_4^2, x_2^3 - x_1^2x_4, x_1^2x_2^2 - x_3x_4^2\}$ is the Patil basis of $\mathfrak{p}$ with respect to $<$, and we again obtain F as a minimal generating set of $\mathfrak{p}$ by Theorem 4.4 (2).

We note that F is already the Patil basis of $\mathfrak{p}$ with respect to the lexicographical term order on T given by $x_1 > x_2 > x_3 > x_4$.

3. (a) $n_1 = 10, n_2 = 15, n_3 = 16, n_4 = 24$. Then $\alpha_1 = 3$, $\alpha_2 = 2$, $\alpha_3 = 3$, $\alpha_4 = 2$ and $\{x_1^3 - x_2^2, x_3^3 - x_4^2\} \subseteq \mathfrak{p}(10, 15, 16, 24) =: \mathfrak{p}$, and both binomials are the only ones in $\mathfrak{p}$ with x_1^3, x_2^2, x_3^3 or x_4^2 in its support. Hence we are not in Case 2 by Lemma 4.7.

$$\{x_2^2 - x_1^3, x_4^2 - x_3^3, x_3x_4 - x_1^4, x_3^4 - x_1^4x_4\}$$

is the Patil basis of $\mathfrak{p}$ with respect to the lexicographical term order on T given by $x_1 > x_2 > x_3 > x_4$. Using the notation of Theorem 4.4 (3) we have $\gamma = 4$ and $x_4 \mid \sigma(x_3^\gamma) = x_1^4x_4$. Therefore

$$\{x_2^2 - x_1^3, x_4^2 - x_3^3, x_3x_4 - x_1^4\}$$

is a minimal generating set of $\mathfrak{p}$ by Theorem 4.4 (3).

We note that the minimal number of generators of $\mathfrak{p}(n_1, n_2, n_3, n_4)$ cannot be 4 when we are not in Case 2 (see, e.g., [**3**]). Another example of a Patil basis not being a minimal generating set was given by Patil in his thesis, see [**6**].

(b) $n_1 = 21$, $n_2 = 24$, $n_3 = 40$, $n_4 = 49$. Then $\alpha_1 = 7$, $\alpha_2 = 5$, $\alpha_3 = \alpha_4 = 3$ and $\{x_1^7 - x_4^3, x_2^5 - x_3^3\} \subseteq \mathfrak{p}(21, 24, 40, 49) =: \mathfrak{p}$, and these

binomials are the only ones in $\mathfrak{p}$ with x_1^7, x_2^5, x_3^3 or x_4^3 in its support. Hence, we are again not in Case 2 by Lemma 4.7.

$$P := \{x_2^3x_3 - x_1^3x_4, x_3^3 - x_2^5, x_2x_4^2 - x_1^2x_3^2, x_3^2x_4 - x_1^5x_2, \\ x_3x_4^2 - x_1^2x_2^4, x_2^4x_4 - x_1^5x_3, x_4^3 - x_1^7, x_2^7 - x_1^8\}$$

is the Patil basis of $\mathfrak{p}$ with respect to the lexicographical term order on T given by $x_1 > x_4 > x_2 > x_3$. We have $\gamma = 7$ and $x_3 \nmid \sigma(x_2^7) = x_1^8$. Therefore, P is already a minimal generating set of $\mathfrak{p}$ by Theorem 4.4 (3).

Remark 9. To obtain Patil bases from a generic zero see [**7**]. For the particular examples above, Apery sequences [**1**] of the numerical semigroup $S := \langle n_1, \dots, n_r\rangle$ can be used. We state without proof: If $A(n_1) = \{\omega_1, \omega_2, \dots, \omega_{n_1}\}$ with $0 = \omega_1 < \omega_2 < \cdots < \omega_{n_1}$ is the Apery sequence of S and $A(n_1, <) = \{(\omega_1, \alpha_1), \dots, (\omega_{n_1}, \alpha_{n_1})\}$ with $\rho(\alpha_i) = \omega_i$ and $\sigma(\alpha_i) = \alpha_i$, $i = 1, \dots, n_1$, then

$$C := \{(i,j) \mid 1 \le i \le n_1, 2 \le j \le r, (\rho(\alpha_i + e_j), \alpha_i + e_j) \notin A(n_1, <), \\ \sigma(\alpha) = \alpha \text{ for all } \alpha \in \mathbf{N}^r \text{ such that } \alpha \parallel \alpha_i + e_j\}$$

is a Patil basis if $a_1 < b_1$ implies $\alpha = (a_1, \dots, a_r) < \beta = (b_1, \dots, b_r)$. Here e_j is as defined in Proposition 1.2 and Example 2.

Acknowledgments. The first named author would like to thank the NTZ and the Graduiertenkolleg "Analysis, Geometrie und ihre Verbindung zu den Naturwissenschaften" at the University of Leipzig for financial support during the preparation of this paper.

REFERENCES

1. G. Angermüller, *Die Wertehalbgruppe einer ebenen irreduziblen algebroiden* , Kurve. Math. Z. **153** (1977), 267–282.

2. T. Becker and V. Weispfenning, *Gröbner bases, A computational approach to commutative algebra*, Grad. Texts Math., Springer Verlag, New York, 1993.

3. H. Bresinsky, *Symmetric semigroups generated by* 4 *elements*, Manuscr. Math. **17** (1975), 205–219.

4. E. Briales, A. Campillo, C. Marijuán and P. Pisón, *Minimal systems of generators for ideals of semigroups*, J. Pure Appl. Algebra **124** (1998), 7–30.

5. S. Eliahou, *Courbes monomiales et algèbre de Rees symbolique*, Ph.D. thesis, Université de Genève, Italy, 1983.

6. D.P. Patil, *Generators for the derivation modules and the defining ideals of certain affine curves*, Ph.D. thesis, Tata Institute of Fundamental Research, Bombay, India, 1989.

7. B. Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series, Amer. Math. Soc. **8** (1996).

University of Maine, Department of Mathematics, Orono, Maine 04469
Email address: bresinsky@math.umaine.edu, dong.nguyenbresinsky@jax.org

800 W. Brown St., Apt. C, Tempe, AZ 85281
Email address: frankcurtis@earthlink.net

Universität Leipzig, Fakultät für Mathematik und Informatik, Augustusplatz 10, 04109 Leipzig, Germany
Email address: stueckrad@mathematik.uni-leipzig.de, susanne.stueckrad@t-online.de