TUM

INSTITUT FÜR INFORMATIK

An Optimal Algorithm for Constructing the Reduced Gröbner Basis of Binomial Ideals

Ulla Koppenhagen
Ernst W. Mayr

TUM-I9605
Januar 1996

TECHNISCHE UNIVERSITÄT MÜNCHEN

TUM-INFO-01-1996-I9605-350/1.-FI

Typescript: ---

Druck: Mathematisches Institut und
Institut für Informatik der
Technischen Universität München

An Optimal Algorithm for Constructing the Reduced Gröbner Basis of Binomial Ideals

Ulla Koppenhagen, Ernst W. Mayr
Institut für Informatik
Technische Universität München
D-80290 München, GERMANY
e-mail: {KOPPENHA|MAYR}@INFORMATIK.TU-MUENCHEN.DE
WWW: HTTP://WWWMAYR.INFORMATIK.TU-MUENCHEN.DE/

January 10, 1996

Abstract

In this paper, we present an optimal, exponential space algorithm for generating the reduced Gröbner basis of binomial ideals. We make use of the close relationship between commutative semigroups and pure difference binomial ideals. Based on the algorithm for the uniform word problem in commutative semigroups exhibited by Mayr and Meyer we first derive an exponential space algorithm for constructing the reduced Gröbner basis of a pure difference binomial ideal. In addition to some applications to finitely presented commutative semigroups, this algorithm is then extended to an exponential space algorithm for generating the reduced Gröbner basis of binomial ideals in general.

1 Introduction

One of the most active areas of research in computer algebra is the design and analysis of algorithms for computational problems in commutative algebra. In particular, computational problems for polynomial ideals occur, as mathematical subproblems, in many areas of mathematics, and they also have a number of applications in various areas of computer science, like language generating and term rewriting systems, tiling problems, algebraic manifolds, motion planing, and several models for parallel systems.

Through the introduction of Gröbner bases (see [Buc65], also [Hi64]) many of the mentioned problems become easily expressible and algorithmically solvable. For practical applications, in particular, the implementation in computer algebra systems, it is important to establish upper complexity bounds for the normal form algorithms which transform a given polynomial ideal basis into a Gröbner basis.

First steps were obtained in [Bay82] and [MoMo84] where upper bounds for the degrees in a minimal Gröbner basis were derived. In [Dub90] Dubé obtained the sharpened degree bound of $2 \cdot (\frac{d^2}{2} + d)^{2^{k-1}}$ (with d the maximum degree of the input basis and k the number of indeterminates) for the degree of polynomials in a reduced Gröbner basis, employing only combinatorial arguments. By transforming a representation of the normal form of a polynomial into a system of linear equations, Kühnle and Mayr exhibited in [KuMa96] an exponential space computation of Gröbner bases. This, however, is based on very complex parallel computations like parallel rank computations of matrices, and the Parallel Computation Thesis [FW78].

In this paper, we make use of the close relationship between commutative semigroups and pure difference binomial ideals (for an investigation of the algebraic structure of general binomial ideals see [EiSt94]). Based on the algorithm in [MM82] for the uniform word problem in commutative semigroups we derive an exponential space algorithm for constructing the reduced Gröbner basis of a general binomial ideal. This algorithm can be implemented without any difficult parallel rank computations of matrices, or any other complex parallel computations. By the results in [MM82] and [Huy86], which give a doubly exponential lower bound (in the size of the problem instance) for the maximal degree of the elements of Gröbner bases as well as for the cardinality of such bases, this algorithm is space optimal.

The remainder of this paper is organized as follows. In Section 2 we briefly introduce the basic notations and fundamental concepts. In Section 3 we derive an exponential space algorithm for constructing the reduced Gröbner basis of a pure difference binomial ideal, and give some applications to finitely presented commutative semigroups. Then, in Section 4, this algorithm is extended to an exponential space algorithm for generating the reduced Gröbner basis of binomial ideals in general.

2 Preliminaries

In this section we briefly review the basic concepts used in the sequel.

2.1 Basic Definitions and Notations

The polynomial ideals which we get by using the relationship of finitely presented commutative semigroups and polynomial ideals are *pure difference binomial ideals*, *i.e.,* each polynomial in the basis of such an ideal is the difference of two terms. By looking at Buchberger's algorithm [Buc65], it is not hard to see that the reduced Gröbner basis of a pure difference binomial ideal still consists only of pure difference binomials.

Let X denote the finite set $\{x_1, \ldots, x_k\}$, and[1] $\mathbb{Q}[X]$ the (commutative) ring of polynomials with indeterminates $x_1, \ldots, x_k$ and rational coefficients.

[1] $\mathbb{N}$ denotes the set of nonnegative integers, $\mathbb{Z}$ the set of integers, and $\mathbb{Q}$ the set of rationals.

A *term* t in $x_1, \ldots, x_k$ is a product of the form

$$t = x_1^{e_1} \cdot x_2^{e_2} \cdots\ x_k^{e_k},$$

with $(e_1, e_2, \ldots, e_k) \in \mathbb{N}^k$ the *degree vector* of t.

By the *degree* $\deg(t)$ of a term t we shall mean the integer $e_1 + e_2 + \ldots + e_k$ (which is ≥ 0).

Each *polynomial* $f(x_1, \ldots, x_k) \in \mathbb{Q}[X]$ is a finite sum

$$f(x_1, \ldots, x_k) = \sum_{1 \leq i \leq n} a_i \cdot t_i,$$

with $a_i \in \mathbb{Q} - \{0\}$ the coefficient of the ith term t_i of f. The product $m_i = a_i \cdot t_i$ is called the ith *monomial* of the polynomial f. The degree of a polynomial is the maximum of the degrees of its terms.

For $f_1, \ldots, f_h \in \mathbb{Q}[X]$, $\langle f_1, \ldots, f_h \rangle \subseteq \mathbb{Q}[X]$ denotes the ideal generated by $\{f_1, \ldots, f_h\}$, that is[2]

$$\langle f_1, \ldots, f_h \rangle := \left\{ \sum_{i=1}^{h} p_i f_i;\ p_i \in \mathbb{Q}[X] \ \text{ for } \ i \in I_h \right\}.$$

If $I = \langle f_1, \ldots, f_h \rangle$, $\{f_1, \ldots, f_h\}$ is called a *basis* of I.

An *admissible term ordering* $\prec$ on $\mathbb{Q}[X]$ is given by any admissible order on $\mathbb{N}^k$, *i.e.,* any total order $<$ on $\mathbb{N}^k$ satisfying the following two conditions:

(T1) $\quad e > (0, \ldots, 0)$ for all $e \in \mathbb{N}^k - \{(0, \ldots, 0)\}$;

(T2) $\quad a < b \quad \Rightarrow \quad a + c < b + c$ for all $a, b, c \in \mathbb{N}^k$.

If $(d_1, \ldots, d_k) > (e_1, \ldots, e_k)$, we say that any monomial $a_1 \cdot x_1^{d_1} \cdots x_k^{d_k}$, $a_1 \in \mathbb{Q} - \{0\}$, is greater in the term ordering than any monomial $a_2 \cdot x_1^{e_1} \cdots x_k^{e_k}$, $a_2 \in \mathbb{Q} - \{0\}$ (written $a_1 \cdot x_1^{d_1} \cdots x_k^{d_k} \succ a_2 \cdot x_1^{e_1} \cdots x_k^{e_k}$).

For a polynomial $f(x_1, \ldots x_k) = \sum_{i=1}^{n} a_i \cdot t_i$ we always assume that $t_1 \succ t_2 \succ \ldots \succ t_n$. For any such nonzero polynomial $f \in \mathbb{Q}[X]$ we define the *leading term* $LT(f) := t_1$.

For the sake of constructiveness, we assume that the term order is given as part of the input by a $k \times k$ integral matrix T such that $a_1 \cdot x_1^{d_1} \cdots x_k^{d_k} \succ a_2 \cdot x_1^{e_1} \cdots x_k^{e_k}$ iff, for the corresponding degree vectors d and e, Td is *lexicographically greater* than Te (see [Rob85, Wei87]).

Let I be an ideal in $\mathbb{Q}[X]$, and let some admissible term ordering $\prec$ on $\mathbb{Q}[X]$ be given. A finite set $\{g_1, \ldots, g_r\}$ of polynomials from $\mathbb{Q}[X]$ is called a *Gröbner* basis of I (w.r.t. $\prec$), if

(G1) $\quad \{g_1, \ldots, g_r\}$ is a basis of I;

[2] for $n \in \mathbb{N}$, I_n denotes the set $\{1, \ldots, n\}$

(G2) $\{LT(g_1),\ldots,LT(g_r)\}$ is a basis of the *leading term ideal* of I, which is the smallest ideal containing the leading terms of all $f \in I$, or equivalently: if $f \in I$, then

$$LT(f) \in \langle LT(g_1),\ldots,LT(g_r)\rangle\,.$$

Let F be a subset of $\mathbb{Q}[X]$ and $\prec$ some fixed admissible term ordering. We say a polynomial p is *reducible* to q modulo F (written $p \triangleright_F q$), if there exists $f \in F$, and a monomial $m \in \mathbb{Q}[X]$ such that $LT(m \cdot f)$ is a monomial of p, and $q = p - m \cdot f$. A polynomial p is *reducible modulo* F if there exists $q \in \mathbb{Q}[X]$ such that $p \triangleright_F q$. If p is not reducible modulo F, then we say p is *in normal form modulo* F. A *normal form* of p modulo F is a polynomial q that is in normal form modulo F and satisfies $p \overset{*}{\triangleright}_F q$, where $\overset{*}{\triangleright}_F$ is the reflexive transitive closure of $\triangleright_F$.

A Gröbner basis $G = \{g_1,\ldots,g_r\}$ is called *reduced* if all polynomials g_i are in normal form modulo $G - \{g_i\}$

For a finite alphabet $X = \{x_1,\ldots,x_k\}$, let X^* denote the free commutative monoid generated by X. An element u of X^* is called a *(commutative) word*. For a word the order of the symbols is immaterial, and we shall in the sequel use an exponent notation: $u = x_1^{e_1}\ldots x_k^{e_k}$, where[3] $e_i = \Phi(u,x_i) \in \mathbb{N}$ for $i = 1,\ldots,k$. We identify any $u \in X^*$ (resp., the corresponding vector $u = (\Phi(u,x_1),\ldots,\Phi(u,x_k))$ $\in \mathbb{N}^k$) with the term $u = x_1^{\Phi(u,x_1)} \cdot x_2^{\Phi(u,x_2)} \cdots x_k^{\Phi(u,x_k)}$ and vice versa any term $u = x_1^{e_1} \cdot x_2^{e_2} \cdots x_k^{e_k} \in \mathbb{Q}[X]$ with the word

$$u = \underbrace{x_1\ldots x_1}_{e_1}\underbrace{x_2\ldots x_2}_{e_2}\ldots\underbrace{x_k\ldots x_k}_{e_k} \in X^*.$$

Now let $\mathcal{P} = \{l_i \equiv r_i;\ i \in I_h\}$ be any (finite) commutative semigroup presentation with l_i, $r_i \in X^*$ for $i \in I_h$. We say a word $v \in X^*$ *is derived in one step* from $u \in X^*$ (written $u \to v(\mathcal{P})$) by application of the congruence $(l_i \equiv r_i) \in \mathcal{P}$ iff, for some $w \in X^*$, we have $u = wl_i$ and $v = wr_i$, or $u = wr_i$ and $v = wl_i$ (note, since '$\equiv$' is symmetric, '$\to$' is symmetric, *i.e.,* $u \to v(\mathcal{P}) \Leftrightarrow v \to u(\mathcal{P})$). The word u *derives* v resp., $u \equiv v \bmod \mathcal{P}$ iff $u \overset{*}{\to} v(\mathcal{P})$, where $\overset{*}{\to}$ is the reflexive transitive closure of $\to$. More precisely we write $u \overset{+}{\to} v(\mathcal{P})$, where $\overset{+}{\to}$ is the transitive closure of $\to$, if $u \overset{*}{\to} v(\mathcal{P})$ with $u \neq v$. A sequence $(u_0,\ldots,u_n)$ of words $u_i \in X^*$ with $u_i \to u_{i+1}(\mathcal{P})$ for $i = 0,\ldots,n-1$ is called a *derivation* (of length n) of u_n from u_0 in $\mathcal{P}$.

By $I(\mathcal{P})$ we denote the pure difference binomial $\mathbb{Q}[X]$-ideal generated by $\{l_1 - r_1,\ldots,l_h - r_h\}$, *i.e.,*

$$I(\mathcal{P}) := \left\{\sum_{i=1}^{h} p_i(l_i - r_i);\ p_i \in \mathbb{Q}[X] \ \text{ for } \ i \in I_h\right\}\,.$$

[3] Let Φ be the Parikh mapping, *i.e.,* $(\Phi(u))_i$ (also written $\Phi(u,x_i)$) indicates, for every $u \in X^*$ and $i \in \{1,\ldots,k\}$, the number of occurrences of $x_i \in X$ in u.

2.2 The Uniform Word Problem and the Corresponding Pure Difference Binomial Ideal Membership Problem

The following proposition shows the connection between the uniform word problem for commutative semigroups and the membership problem for ideals in $\mathbb{Q}[X]$. The *uniform word problem* for commutative semigroups is the problem of deciding for a commutative Thue system $\mathcal{P}$ over X and two words $u, v \in X^*$ whether $u \equiv v \bmod \mathcal{P}$. The *polynomial ideal membership problem* (PIMP) is the problem of deciding for given polynomials $f, f_1, \ldots, f_h \in \mathbb{Q}[X]$ whether $f \in \langle f_1, \ldots, f_h \rangle$.

Proposition 1 [MM82] *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$, and u, $v \in X^*$. Then the following are equivalent:*

(i) There exist $p_1, \ldots, p_h \in \mathbb{Q}[X]$ such that $\quad v - u = \sum_{i=1}^h p_i(l_i - r_i)$.

(ii) There is a derivation $u = \gamma_0 \to \gamma_1 \to \ldots \to \gamma_n = v(\mathcal{P})$ of v from u such that for $j \in I_n$

$$\text{length}(\gamma_j) \le \max\{\deg(l_i p_i),\ \deg(r_i p_i);\ i \in I_h\}.$$

(iii) $u \equiv v \bmod \mathcal{P}$.

In the fundamental paper [Her26], G. Hermann gave a doubly exponential degree bound for the polynomial ideal membership problem:

Proposition 2 [Her26] *Let $X = \{x_1, \ldots, x_k\}$; $g, g_1, \ldots, g_h \in \mathbb{Q}[X]$; and $d := \max\{\deg(g_i);\ i \in I_h\}$. If $g \in \langle g_1, \ldots g_h \rangle$, then there exist $p_1, \ldots, p_h \in \mathbb{Q}[X]$ such that*

(i) $g = \sum_{i=1}^h g_i p_i$;

(ii) $(\forall i \in I_h)\ [\deg(p_i) \le \deg(g) + (hd)^{2^k}]$.

These two propositions yield an exponential space upper bound for the uniform word problem for commutative semigroups.

Proposition 3 [MM82] *Let $X = \{x_1, \ldots, x_k\}$ and $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$. Then there is a (deterministic) Turing machine M and some constant $c > 0$ independent of $\mathcal{P}$, such that M decides for any two words u, $v \in X^*$ whether $u \equiv v \bmod \mathcal{P}$ using at most space* $(\text{size}(u, v, \mathcal{P}))^2 \cdot 2^{c \cdot k}$.

3 Constructing the Reduced Gröbner Basis of a Pure Difference Binomial Ideal in Exponential Space

In this section we derive an exponential space algorithm for generating the reduced Gröbner basis of a pure difference binomial ideal. For this purpose, we first analyze the elements of the reduced Gröbner basis.

3.1 The Reduced Gröbner Basis of Pure Difference Binomial Ideals

Let $\mathcal{P}$ be a commutative semigroup presentation over some alphabet X. If C is some congruence class of $\mathcal{P}$, and $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ $(h_i \succ m_i)$ a Gröbner basis of the pure difference binomial ideal $I(\mathcal{P})$ w.r.t. some admissible term ordering $\prec$, then the minimal element m_C of C w.r.t. $\prec$ is not reducible modulo G. Otherwise, since G is a Gröbner basis and by Proposition 1, there would be some $i \in I_r$, and some $t \in X^*$ with $m_C = h_i \cdot t \xrightarrow{+} m_i \cdot t \prec m_C$ which contradicts the minimality of m_C. Hence m_C is the normal form of any word (considered as a term) $t \in C$ modulo G.

The following theorems characterize the terms of the binomials occuring in the reduced Gröbner basis of $I(\mathcal{P})$, and the leading terms of $I(\mathcal{P})$. The first theorem shows that in each binomial of the reduced Gröbner basis G of $I(\mathcal{P})$ the smaller term (w.r.t. $\prec$) is the minimal element (w.r.t. $\prec$) of the congruence class of the leading term.

Theorem 1 *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$, and $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ be the reduced Gröbner basis of the ideal $I(\mathcal{P})$ w.r.t. some admissible term ordering $\prec$ $(m_i \prec h_i)$. Then m_i is the minimal element (w.r.t. $\prec$) of the congruence class $[h_i]_{\mathcal{P}}$, $i \in I_r$.*

Proof: Assume that $w \neq m_i$ is the minimal element of $[h_i]_{\mathcal{P}}$ (w.r.t. $\prec$). Then $w \prec m_i$ and, by Proposition 1, $m_i - w \in I(\mathcal{P})$ resp., $m_i - w = \sum_{i=1}^{r} p_i(h_i - m_i)$, for some $p_i \in \mathbb{Q}[X]$, $i \in I_r$. Since G is the reduced Gröbner basis of $I(\mathcal{P})$, there must be some $j \in I_r$ with $LT(p_j) \cdot h_j$ divides m_i. But this is a contradiction to the fact that $h_i - m_i$ is an element of the reduced Gröbner basis of $I(\mathcal{P})$. □

The next theorem characterizes the leading terms of the polynomials in $I(\mathcal{P})$, and, in particular, the leading terms of the binomials in the reduced Gröbner basis of $I(\mathcal{P})$.

Theorem 2 *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$, and $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ be the reduced Gröbner basis of the ideal $I(\mathcal{P})$ w.r.t. some admissible term ordering $\prec$ $(m_i \prec h_i)$. Then $LT(I(\mathcal{P}))$ (the set of the leading terms of $I(\mathcal{P})$) is the set of all terms with nontrivial congruence class that are* not *the minimal element in their congruence class w.r.t. $\prec$. $H = \{h_1, \ldots, h_r\}$ is the set of the minimal elements of $LT(I(\mathcal{P}))$ w.r.t. divisibility.*

Proof: Since G is the reduced Gröbner basis of $I(\mathcal{P})$, it is clear that H is the set of the minimal elements of $LT(I(\mathcal{P}))$ w.r.t. divisibility.
Since $h_i - m_i \in I(\mathcal{P})$, there is a derivation in $\mathcal{P}$ of $m_i \prec h_i$ from h_i $(h_i \xrightarrow{+} m_i(\mathcal{P}))$ for all $i \in I_r$. Because G is a Gröbner basis, for any $h \in LT(I(\mathcal{P}))$ there is a $h_j \in H$ and a term t in X with $h = t \cdot h_j$. So from any $h \in LT(I(\mathcal{P}))$ we can start a derivation in $\mathcal{P}$, namely the derivation of $t \cdot m_j \prec h$ $(h \xrightarrow{+} t \cdot m_j(\mathcal{P}))$, and hence the congruence class $[h]_{\mathcal{P}}$ is nontrivial.

Now let $s \in X^*$ be a term with nontrivial congruence class. If s is not the minimal element m_s (w.r.t. $\prec$) of its congruence class $[s]_{\mathcal{P}}$, then s derives m_s ($s \xrightarrow{+} m_s(\mathcal{P})$), and thus $s - m_s \in I(\mathcal{P})$ resp., $s \in LT(I(\mathcal{P}))$. If $s = m_s$, then there is no derivation of some $t_s \prec s$ from s. Furthermore there is no $j \in I_r$ with h_j divides s, because if there is some term $t \in \mathbb{Q}[X]$ and some $j \in I_r$ with $s = t \cdot h_j$, there is a derivation of $t \cdot m_j \prec s$ from s. So if $s = m_s$, then $s \notin LT(I(\mathcal{P}))$ and $s \notin H$. □

If $s \in X^*$ is the minimal element of its congruence class $[s]$ w.r.t. $\prec$, then every subword s' of s, *i.e.,* $s = t \cdot s'$ for some $t \in X^*$, is also the minimal element of its congruence class $[s']$ w.r.t. $\prec$. Otherwise there would be a derivation of some $m_{s'} \prec s'$ from s' and thus a derivation of $t \cdot m_{s'} \prec t \cdot s' = s$ from s which contradicts the minimality of s.

3.2 The Algorithm

In this section we give an exponential space algorithm for generating the reduced Gröbner basis of a pure difference binomial ideal. To show the correctness and the complexity of the algorithm we need the results of the previous sections and the following upper bound for the total degree of polynomials in a Gröbner basis obtained by Dubé in [Dub90]. Note that we use exponential notation in representing words over X.

Proposition 4 [Dub90] *Let $F = \{f_1, \ldots, f_h\} \subset \mathbb{Q}[X]$, $I = \langle f_1, \ldots, f_h \rangle$ the ideal generated by F, and let d be the maximum degree of any $f \in F$. Then for any admissible ordering $\prec$ on $\mathbb{Q}[X]$, the degree of polynomials required in a Gröbner basis for I w.r.t. $\prec$ is bounded by*

$$2 \cdot \left(\frac{d^2}{2} + d \right)^{2^{k-1}}.$$

Now we will generate the reduced Gröbner basis of the pure difference binomial ideal $I(\mathcal{P})$ w.r.t. $\prec$, where $X = \{x_1, \ldots, x_k\}$, and $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$ (w.l.o.g. $l_i \succ r_i$). Let H denote the set $\{h_1, \ldots, h_r\}$ of the minimal elements of $LT(I(\mathcal{P}))$ w.r.t. divisibility and m_i the minimal element of $[h_i]_{\mathcal{P}}$, $i \in I_r$, w.r.t. $\prec$. From Theorem 1 and Theorem 2 we know the set $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ is the reduced Gröbner basis of $I(\mathcal{P})$.

Theorem 2 shows that $\langle LT(I(\mathcal{P}))\rangle \supseteq \langle l_1, \ldots, l_h \rangle$ and $\langle LT(I(\mathcal{P}))\rangle \subseteq \langle l_1, \ldots, l_h, r_1, \ldots, r_h \rangle$. Let $L' = \{l_1, \ldots, l_{n'_l}\}$ be the set of the minimal elements of $\{l_1, \ldots, l_h\}$ w.r.t. divisibility. Then the subset of $\{r_1, \ldots, r_h\}$ which contains only minimal elements of $\{l_1, \ldots, l_{n'_l}, r_1, \ldots, r_h\}$ w.r.t. divisibility is denoted by $R = \{r_1, \ldots, r_{n_r}\}$ and the subset of $\{l_1, \ldots, l_{n'_l}\}$ which contains only minimal elements of $\{l_1, \ldots, l_{n'_l}, r_1, \ldots, r_{n_r}\}$ w.r.t. divisibility by $L = \{l_1, \ldots, l_{n_l}\}$. Note that

$$\begin{aligned} H &\supseteq L, \\ \langle LT(I(\mathcal{P}))\rangle &\supseteq \langle L' \rangle \supseteq \langle L \rangle, \\ \langle LT(I(\mathcal{P}))\rangle &\subseteq \langle L, R \rangle = \langle L', R \rangle. \end{aligned}$$

We have to determine the elements of the set $H - L$, and the minimal elements m_i (w.r.t. $\prec$) of the congruence classes of all $h_i \in H$. From Proposition 4 we know that the degrees $\deg(h_i)$, and $\deg(m_i)$ are bounded by $2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$, where d is the maximum degree of any $l_i - r_i$, $i \in I_h$. Since

$$H - L \subset LT(\langle L', R\rangle) - LT(\langle L'\rangle) \cup (L' - L) =: KH,$$

we consider the terms in KH with degree $\leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ in some order, e.g. in ascending lexicographic order with $x_1 \prec_{lex} x_2 \prec_{lex} \ldots \prec_{lex} x_k$. From Theorem 2 follows immediately:

Lemma 1 *A term $u \in X^*$ is an element of $LT(I(\mathcal{P}))$ iff u is not the minimal element of $[u]_{\mathcal{P}}$ w.r.t. $\prec$.*

For the case that the term u is not the minimal element m_u of $[u]_{\mathcal{P}}$ the next lemma gives a characterization of the elements $m \in [u]_{\mathcal{P}}$ with $m \prec u$.

Lemma 2 *A term $u \in X^*$ is the minimal element of $[u]_{\mathcal{P}}$ w.r.t. $\prec$ iff there is no $t \cdot r_i$ with $t \cdot r_i \prec u$, $r_i \in R$, $t \in X^*$ such that $u \xrightarrow{+} t \cdot r_i(\mathcal{P})$.*

Proof: If u is the minimal element of $[u]_{\mathcal{P}}$ w.r.t. $\prec$, then there is no $m \in X^*$ with $m \prec u$, and $u \xrightarrow{+} m(\mathcal{P})$.
Now assume that u is not minimal in $[u]_{\mathcal{P}}$ w.r.t. $\prec$. Then there is a derivation in $\mathcal{P}$ leading from u to the minimal element $m_u \prec u$ of $[u]_{\mathcal{P}}$ w.r.t. $\prec$, *i.e.*, $u \xrightarrow{+} m_u(\mathcal{P})$, where $m_u = t \cdot r_i$ for some $r_i \in \{r_1, \ldots, r_h\}$ (note $l_j \succ r_j$ $\forall j \in I_h$), $t \in X^*$. Since $\{r_1, \ldots, r_h\} - R \subset LT(I(\mathcal{P}))$, we can even say $r_i \in R$. □

Considering degree bounds this Lemma has the following form.

Lemma 3 *A term $u \in X^*$ with* $\deg(u) \leq D$ *is the minimal element of $[u]_{\mathcal{P}}$ w.r.t. $\prec$ iff there is no $t \cdot r_i$ with $t \cdot r_i \prec u$, $r_i \in R$, $t \in X^*$, and* $\deg(t \cdot r_i) \leq D + 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ *such that $u \xrightarrow{+} t \cdot r_i(\mathcal{P})$.*

Proof: If u is not the minimal element m_u of $[u]_{\mathcal{P}}$ w.r.t. $\prec$, *i.e.*, $u \in LT(I(\mathcal{P}))$, then either $u \in H$ and $\deg(m_u) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$, or there is some $h \in H$ with $u = t_u \cdot h$ for some $t_u \in X^*$. The degree of the minimal element m_h of $[h]_{\mathcal{P}}$ w.r.t. $\prec$ is bounded by $2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$. From $m_h \prec h$ we get $t_u \cdot m_h \prec u$ with $\deg(t_u \cdot m_h) \leq D + 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$. □

Given some term $h \in KH$ with $\deg(h) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$, we have to decide whether $h \in H$, and if $h \in H$ we have to determine the minimal element m_h of $[h]_{\mathcal{P}}$ w.r.t. $\prec$. If $h \in H$, then, by Lemma 2 and Proposition 4, there is a term $t \cdot r_i$ with $t \cdot r_i \prec h$, $r_i \in R$, $t \in X^*$, $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ such that $h \xrightarrow{+} t \cdot r_i(\mathcal{P})$. For h and $t \cdot r_i$ with $\deg(h)$, $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$, by Proposition 3, the decision whether $h \equiv t \cdot r_i \bmod \mathcal{P}$ uses at most space $(\text{size}(\mathcal{P}))^2 \cdot 2^{c \cdot k}$ for some constant $c > 0$ independent of $\mathcal{P}$. Thus we decide for the words $t \cdot r_i$ with $t \cdot r_i \prec h$, $r_i \in R$, $t \in X^*$, $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ in ascending term order whether $h \equiv t \cdot r_i \bmod \mathcal{P}$ until we find the minimal element m_h of $[h]_\mathcal{P}$, or there is no more $t \cdot r_i$ with $t \cdot r_i \prec h$, $r_i \in R$, $t \in X^*$, $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$. In the latter case $h \notin H$, and we have to consider the next element of KH with degree $\leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$. Otherwise $h \in LT(I(\mathcal{P}))$ and we have to decide whether $h \in H$.

Lemma 4 *Let $h = x_1^{e_1} \cdots x_k^{e_k}$ with $h \in LT(I(\mathcal{P}))$, then $h \in H$ iff for all $i \in I_k$ with $e_i \geq 1$ $h^{(i)} := x_1^{e_1} \cdots x_i^{e_i - 1} \cdots x_k^{e_k} \notin LT(I(\mathcal{P}))$,* i.e., *$h^{(i)}$ is the minimal element of $[h^{(i)}]_\mathcal{P}$ w.r.t. $\prec$.*

Proof: Follows immediately from the definition of H. □

Since $\deg(h) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ and because of Lemma 3, and Proposition 3 the decision whether $h^{(i)} \in LT(I(\mathcal{P}))$ $(i \in I_k,\ e_i \geq 1)$ uses at most space $(\text{size}(\mathcal{P}))^2 \cdot 2^{c \cdot k}$ for some constant $c > 0$ independent of $\mathcal{P}$. If $h \in H$, then $h - m_h$ is an element of the reduced Gröbner basis G of $I(\mathcal{P})$. The algorithm continues by considering the next element h_{new} of KH with $\deg(h_{new}) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$, and h does not divide h_{new} because any multiple $t \cdot h$ of h, $t \in X^*$, is not in H if $h \in LT(I(\mathcal{P}))$.

When all the elements in KH with degree $\leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ are examined it remains to determine the minimal elements (w.r.t. $\prec$) of the congruence classes of the terms $l_i \in L$. Again from Proposition 4 we know that the degree of the minimal element m_{l_i} of $[l_i]_\mathcal{P}$ (w.r.t. $\prec$) is bounded by $2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$. As above we determine m_{l_i} by deciding for the words $t \cdot r_i$ with $t \cdot r_i \prec l_i$, $r_i \in R$, $t \in X^*$, $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ in ascending term order whether $l_i \equiv t \cdot r_i \bmod \mathcal{P}$.

From this, we derive the exponential space algorithm given in Figure 1.

Putting everything together, we proved the theorem:

Theorem 3 *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$, and $\prec$ be some admissible term ordering. Then there is an algorithm which generates the reduced Gröbner basis $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ of the pure difference binomial ideal $I(\mathcal{P})$ using at most space $(\text{size}(\mathcal{P}))^2 \cdot 2^{\bar{c} \cdot k} \leq 2^{c \cdot \text{size}(\mathcal{P})}$, where $\bar{c}, c > 0$ are some constants independent of $\mathcal{P}$.*

From the results in [Huy86] we know that, in the worst case, any Gröbner basis of $I(\mathcal{P})$ has maximal degree at least $2^{2^{\text{size}(\mathcal{P})}}$. Hence any algorithm that computes Gröbner bases requires at least exponential space in the worst case.

3.3 Applications

We now consider some applications of the algorithm of Theorem 3.

```
Algorithm 1
 Input:   $\{l_1 - r_1, \ldots, l_h - r_h\}$, admissible term ordering $\prec$
 Output:  the reduced Gröbner basis $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ of $I(\mathcal{P})$
 $L' := \{l_1, \ldots, l_{n_l'}\}$      the set of the minimal elements of $\{l_1, \ldots, l_h\}$ w.r.t. divisibility
 $R := \{r_1, \ldots, r_{n_r}\}$      the subset of $\{r_1, \ldots, r_h\}$ which contains only minimal elements of
                                $\{l_1, \ldots, l_{n_l'}, r_1, \ldots, r_h\}$ w.r.t. divisibility
 $L := \{l_1, \ldots, l_{n_l}\}$      the subset of $\{l_1, \ldots, l_{n_l'}\}$ which contains only minimal elements of
                                $\{l_1, \ldots, l_{n_l'}, r_1, \ldots, r_{n_r}\}$ w.r.t. divisibility
 $d := \max\{\deg(l_i),\ \deg(r_i);\ i \in I_h\}\,;\quad G := \emptyset\,;\quad h := 1$
repeat
  $h :=$ the term of $LT(\langle L', R\rangle) - LT(\langle L'\rangle) \cup (L' - L)$ with degree $\leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ which
       follows $h$ in the lexicographic order defined by $x_1 \prec_{lex} x_2 \prec_{lex} \ldots \prec_{lex} x_k$
       co $h = x_1^{e_1} \cdots x_k^{e_k}$ co
  $D := \deg(h)\,;\quad m := 1$
  repeat
    $m :=$ the term $t \cdot r_i$ with $t \cdot r_i \prec h$, $r_i \in R, t \in X^*$, $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ which
         follows $m$ in the term ordering $\prec$
  until ( $m \equiv h \bmod \mathcal{P}$ or there is no more $t \cdot r_i$ with $t \cdot r_i \prec h$, $r_i \in R, t \in X^*$,
                        $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ )
  if $m \equiv h \bmod \mathcal{P}$ then   co $h \in LT(I(\mathcal{P}))$ co
    for each $i \in I_k$ with $e_i \geq 1$ do $h' := x_1^{e_1} \cdots x_i^{e_i - 1} \cdots x_k^{e_k}\,;\quad m' := 1$
      repeat
        $m' :=$ the term $t \cdot r_i$ with $t \cdot r_i \prec h'$, $r_i \in R$, $t \in X^*$, $\deg(t \cdot r_i) \leq$
              $(D - 1) + 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ which follows $m'$ in the term ordering $\prec$
      until ( $m' \equiv h' \bmod \mathcal{P}$ or there is no more $t \cdot r_i$ with $t \cdot r_i \prec h'$, $r_i \in R, t \in X^*$,
                        $\deg(t \cdot r_i) \leq (D - 1) + 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ )
      if $m' \equiv h' \bmod \mathcal{P}$ then next $h$ with $h_{old}$ does not divide $h_{new}$ end_if
        co $h' \in LT(I(\mathcal{P})) \Rightarrow h \notin H$ co
    end_for
    $G := G \cup \{h - m\}$
    next $h$ with $h_{old}$ does not divide $h_{new}$
  end_if
until there is no more $h \in LT(\langle L', R\rangle) - LT(\langle L'\rangle) \cup (L' - L)$ with degree $\leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$
for each $l_i \in L$ do $m := 1$
  repeat
    $m :=$ the term $t \cdot r_i$ with $t \cdot r_i \prec l_i$, $r_i \in R$, $t \in X^*$, $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ which
         follows $m$ in the term ordering $\prec$
  until $m \equiv l_i \bmod \mathcal{P}$
  $G := G \cup \{l_i - m\}$
end_for
```

Figure 1: Algorithm for the Reduced Gröbner Basis of a Pure Difference Binomial Ideal

3.3.1 Testing for Reducibility

Let $\mathcal{P}$ be a finite commutative semigroup presentation over some alphabet X, $u \in X^*$, and $\prec$ some admissible term ordering on $\mathbb{Q}[X]$. Then, u is the minimal element of $[u]_{\mathcal{P}}$ w.r.t. $\prec$ iff u is in normal form modulo a Gröbner basis G of $I(\mathcal{P})$ w.r.t. $\prec$, *i.e.* u is not reducible modulo G. Thus, by Lemma 1, u is in normal form modulo G iff $u \notin LT(I(\mathcal{P}))$.

Corollary 1 *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$, and $\prec$ be some admissible term ordering. Then for any $u \in X^*$*

(i) there is an algorithm which decides whether $u \in LT(I(\mathcal{P}))$ using at most space $\mathrm{size}(u) + (\mathrm{size}(\mathcal{P}))^2 \cdot 2^{\bar{c}\cdot k} \leq \mathrm{size}(u) + 2^{c\cdot\mathrm{size}(\mathcal{P})}$, where $\bar{c}$, $c > 0$ are some constants independent of u and $\mathcal{P}$.

(ii) there is an algorithm which decides whether u is the minimal element of its congruence class (w.r.t. $\prec$), or equivalently, whether u is in normal form modulo the Gröbner basis of $I(\mathcal{P})$ using at most space $\mathrm{size}(u)$ $+(\mathrm{size}(\mathcal{P}))^2 \cdot 2^{\bar{c}\cdot k} \leq \mathrm{size}(u) + 2^{c\cdot\mathrm{size}(\mathcal{P})}$, where $\bar{c}$, $c > 0$ are some constants independent of u and $\mathcal{P}$.

Proof: Let $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ be the reduced Gröbner basis of $I(\mathcal{P})$. Then $LT(I(\mathcal{P}))$ is generated by $\{h_1, \ldots, h_r\}$. Thus, $u \in LT(I(\mathcal{P}))$ iff there is some h_i, $i \in I_r$, which divides u. □

3.3.2 Finding the Minimal Element, and the Normal Form

The next corollary shows that the minimal element of a congruence class w.r.t. $\prec$, and the normal form of a word modulo G can be found in exponential space.

Corollary 2 *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$, and $\prec$ be some admissible term ordering. Then there is an algorithm, which determines for any word $u \in X^*$ the minimal element of its congruence class (w.r.t. $\prec$), or equivalently, which determines for any term $u \in X^*$ the normal form of u modulo the Gröbner basis of $I(\mathcal{P})$ using at most space $(\mathrm{size}(u)+\mathrm{size}(\mathcal{P}))^2 \cdot 2^{\bar{c}\cdot k} \leq 2^{c\cdot(\mathrm{size}(u)+\mathrm{size}(\mathcal{P}))}$, where $\bar{c}$, $c > 0$ are some constants independent of u and $\mathcal{P}$.*

Proof: In addition to $x_1, \ldots, x_k$ we introduce a new variable s, and to $\mathcal{P}$ we add the identity $s \equiv u$, where u is the word in X^* for whose congruence class we like to determine the minimal element (w.r.t. $\prec$). Let $X_s = X \cup \{s\}$, $\mathcal{P}_s = \mathcal{P} \cup \{s \equiv u\}$, and $\prec_s$ be the admissible term ordering which results from $\prec$ by adding $w \prec s$ for all $w \in X^*$. Then, by Theorem 2, $LT(I(\mathcal{P}_s)) = LT(I(\mathcal{P})) \cup \{s \cdot t;\ t \in X_s^*\}$, in particular $s \in LT(I(\mathcal{P}_s))$, and, since s is minimal in $LT(I(\mathcal{P}_s))$ w.r.t. divisibility, $H_s = H \cup \{s\}$, in particular $s \in H_s$, where H resp., H_s is the set of the minimal elements of $LT(I(\mathcal{P}))$ resp., $LT(I(\mathcal{P}_s))$ w.r.t. divisibility. Because $s \succ w$ for all $w \in X^*$, the minimal element of some congruence class $[v]_{\mathcal{P}_s}$, $v \in X^*$, w.r.t. $\prec_s$ is the same as the minimal element of $[v]_{\mathcal{P}}$ w.r.t. $\prec$. So, because of Theorem 1, and Theorem 3, we can determine the minimal element of $[u]_{\mathcal{P}}$ (w.r.t. $\prec$) in space $(\mathrm{size}(u) + \mathrm{size}(\mathcal{P}))^2 \cdot 2^{\bar{c}\cdot k}$ for some constant $\bar{c} > 0$ independent of u and $\mathcal{P}$. □

So far, we only considered terms. Since a polynomial $f = \sum_{i=1}^{n} a_i \cdot t_i$ is in normal form iff all its terms t_i are in normal form, the results obtained for terms can easily be extended to polynomials.

Corollary 3 *Let* $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$, *and* $\prec$ *be some admissible term ordering. Then for any polynomial* $f = \sum_{i=1}^{n} a_i \cdot t_i$ *in* $Q[X]$,

(i) there is an algorithm, which decides whether f *is in normal form modulo the Gröbner basis of* $I(\mathcal{P})$ *using at most space* $\max_{i\in I_n}\{\mathrm{size}(t_i)\}+(\mathrm{size}(\mathcal{P}))^2\cdot 2^{\bar{c}\cdot k} \leq \max_{i\in I_n}\{\mathrm{size}(t_i)\} + 2^{c\cdot\mathrm{size}(\mathcal{P})}$, *where* $\bar{c}$, $c > 0$ *are some constants independent of* f *and* $\mathcal{P}$.

(ii) there is an algorithm, which determines the normal form of f *modulo the Gröbner basis of* $I(\mathcal{P})$ *using at most space* $(\max_{i\in I_n}\{\mathrm{size}(t_i)\}+\mathrm{size}(\mathcal{P}))^2\cdot 2^{\bar{c}\cdot k} \leq 2^{c\cdot(\max_{i\in I_n}\{\mathrm{size}(t_i)\}+\mathrm{size}(\mathcal{P}))}$, *where* $\bar{c}$, $c > 0$ *are some constants independent of* f *and* $\mathcal{P}$.

Proof: Follows immediately from Corollary 1 and Corollary 2. □

4 Constructing the Reduced Gröbner Basis of a Binomial Ideal in Exponential Space

The algorithm of Theorem 3 generates the reduced Gröbner basis for pure difference binomial ideals. In this section we will be concerned with constructing the reduced Gröbner basis of a larger class of ideals: binomial ideals, in general.

4.1 Basics

Let $m = a \cdot t$ be a monomial in $\mathbb{Q}[X]$ with $a \in \mathbb{Q}$, and t a term in X. Then we write $C(m)$ for the coefficient a, and $T(m)$ for the term t of the monomial m. By $M[X]$ we mean the set of all monomials in $\mathbb{Q}[X]$.

By a binomial in $\mathbb{Q}[X]$ we mean a polynomial with at most two monomials, say $l - r$ $(l \succ r)$. For a finite set $\mathcal{B} = \{l_i - r_i;\ l_i, r_i \in M[X], C(l_i) = 1, i \in I_h\}$, $I(\mathcal{B})$ denotes the binomial $\mathbb{Q}[X]$-ideal generated by $\mathcal{B}$, *i.e.*,

$$I(\mathcal{B}) := \left\{ \sum_{i=1}^{h} p_i(l_i - r_i);\ p_i \in \mathbb{Q}[X] \ \text{ for } \ i \in I_h \right\}.$$

W.l.o.g. we assume that there are no i, $j \in I_h$, $i \neq j$, with $l_i - r_i = c \cdot (l_j - r_j)$ for some $c \in \mathbb{Q} - \{0\}$. (Otherwise we remove one of the two binomials).

As in the case of pure difference binomial ideals we see from Buchberger's algorithm that the reduced Gröbner basis of a binomial ideal still consists only of binomials.

In the following we generalize the algorithm of Theorem 3 from pure difference binomial ideals to binomial ideals.

First we establish some technical details.

For $X = \{x_1, \ldots, x_k\}$, and $\mathcal{B} = \{l_i - r_i;\ l_i, r_i \in M[X],\ C(l_i) = 1, i \in I_h\}$ a set of binomials in $\mathbb{Q}[X]$, we define the corresponding commutative semigroup presentation $\mathcal{P}(\mathcal{B}) := \{T(l_i) \equiv T(r_i);\ l_i - r_i \in \mathcal{B}\}$, where we set $T(0) := x_1^{-\infty} \cdot x_2^{-\infty} \cdots x_k^{-\infty}$. If we agree that $-\infty + n = n + (-\infty) = -\infty$ for any integer n, and $-\infty + (-\infty) = -\infty$, then the whole formalism for commutative semigroups introduced in Section 2 still holds for $\mathcal{P}(\mathcal{B})$. The only difference is that, in addition to the words in X^*, we have the word $x_1^{-\infty} \cdot x_2^{-\infty} \cdots x_k^{-\infty}$ which corresponds to 0 when we consider polynomials. In particular, we still have for u, $v \in X_0^* := X^* \cup \{x_1^{-\infty} \cdots x_k^{-\infty}\}$

$$u - v \in I(\mathcal{P}(\mathcal{B})) \quad \Longleftrightarrow \quad u \equiv v \bmod \mathcal{P}(\mathcal{B})\,.$$

W.l.o.g. we assume that there are no i, $j \in I_h$, $i \neq j$, with $(T(l_i) = T(l_j)) \wedge (T(r_i) = T(r_j))$. (Otherwise, since there is no $c \in \mathbb{Q}$ with $l_i - r_i = c \cdot (l_j - r_j)$, we know that $l_i \in I(\mathcal{B})$ and $r_i \in I(\mathcal{B})$, and we replace the two binomials in $\mathcal{B}$ by $T(l_i)$, and $T(r_i)$ if $T(r_i) \neq 0$.)

Let u, $v \in X_0^*$, and D be a derivation in $\mathcal{P}(\mathcal{B})$ leading from u to v. Then there are terms w_i such that $u = T(a_1) \cdot w_1 \to T(b_1) \cdot w_1 = T(a_2) \cdot w_2 \to T(b_2) \cdot w_2 \to \ldots \to T(b_n) \cdot w_n = v$, where $a_i = l_{j_i}$ and $b_i = r_{j_i}$, or $a_i = r_{j_i}$ and $b_i = l_{j_i}$, $j_i \in I_h$, $i \in I_n$.

Now attach to each $T(l_i) \to T(r_i)(\mathcal{P}(\mathcal{B}))$, $i \in I_h$, the multiplicative factor $C(r_i)$ if $C(r_i) \neq 0$ resp., 1 if $C(r_i) = 0$, and to each $T(r_i) \to T(l_i)(\mathcal{P}(\mathcal{B}))$, $i \in I_h$, the multiplicative factor $\frac{1}{C(r_i)}$ if $C(r_i) \neq 0$ resp., 1 if $C(r_i) = 0$. Taking into account these factors, we obtain from D a derivation in which the i-th step has the form

$$c \cdot T(l_{j_i}) \cdot w_i \to c \cdot c_i \cdot T(r_{j_i}) \cdot w_i$$

with $c_i = C(r_{j_i})$ resp., $c_i = 1$, or

$$c \cdot T(r_{j_i}) \cdot w_i \to c \cdot c_i \cdot T(l_{j_i}) \cdot w_i$$

with $c_i = \frac{1}{C(r_{j_i})}$ resp., $c_i = 1$ for some constant $c \in \mathbb{Q} - \{0\}$ resulting from the first $(i-1)$ steps of D.

Thus, we define the multiplicative factor of D as

$$\mathcal{C}(D) := c_1 \cdot c_2 \cdots c_n\,.$$

Then, for any derivation D in $\mathcal{P}(\mathcal{B})$ leading from u to v, u, $v \in X_0^*$ we have

$$\sum_{i=1}^{n} d_i \cdot (l_{j_i} - r_{j_i}) \cdot w_i = u - \mathcal{C}(D) \cdot v\,,$$

where $d_1 = 1$ if $u = T(l_{j_1}) \cdot w_1$, resp., $d_1 = -c_1$ if $u = T(r_{j_1}) \cdot w_1$, and for $i > 1$ $d_i = c_1 \cdots c_{i-1}$ if the i-th step of D uses $T(l_i) \to T(r_i)$, resp., $d_i = -c_1 \cdots c_i$ if the i-th step of D uses $T(r_i) \to T(l_i)$. Therefore, $u - \mathcal{C}(D) \cdot v \in I(\mathcal{B})$. Note that $u \in I(\mathcal{B})$, and $v \in I(\mathcal{B})$ if $x_1^{-\infty} \cdots x_k^{-\infty}$ occurs in D.

Hence, by Proposition 2, we conclude the following

Theorem 4 *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{B} = \{l_i - r_i;\ l_i, r_i \in M[X], C(l_i) = 1, i \in I_h\}$, and u, v, $T(u) \neq T(v)$, be monomials in $M[X]$. Then the following are equivalent:*

(i) There exists $d \in \mathbb{Q} - \{0\}$ such that $u - d \cdot v \in I(\mathcal{B})$.

(ii) There is a repetition-free derivation D: $T(u) = \gamma_0 \rightarrow \gamma_1 \rightarrow \ldots \rightarrow \gamma_n = T(v)$ in $\mathcal{P}(\mathcal{B})$ leading from $T(u)$ to $T(v)$ and such that, for $j \in I_n$,

$$\mathrm{size}(\gamma_j) \leq \mathrm{size}(u, v, \mathcal{B}) \cdot 2^{c \cdot k},$$

where $c > 0$ is some constant independent of $\mathcal{B}$, u, and v.

Then, by Proposition 3, we have:

Theorem 5 *Let $X = \{x_1, \ldots, x_k\}$, and $\mathcal{B} = \{l_i - r_i;\ l_i, r_i \in M[X], C(l_i) = 1, i \in I_h\}$. Then there is a (deterministic) Turing machine M and some constant $c > 0$ independent of $\mathcal{B}$, such that M decides for any two monomials u, $v \in M[X]$, $T(u) \neq T(v)$, whether there exists $d \in \mathbb{Q} - \{0\}$ such that $u - d \cdot v \in I(\mathcal{B})$ using at most space $(\mathrm{size}(u, v, \mathcal{B}))^2 \cdot 2^{c \cdot k}$.*

To get similar results concerning the membership of a single monomial in $I(\mathcal{B})$, we need a further detail.

Lemma 5 *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{B} = \{l_i - r_i;\ l_i, r_i \in M[X], C(l_i) = 1, i \in I_h\}$, and $u \neq 0$ be a monomial in $M[X]$. Then $u \in I(\mathcal{B})$ iff there is some $t \in [T(u)]_{\mathcal{P}(\mathcal{B})}$ such that there is a repetition-free derivation D in $\mathcal{P}(\mathcal{B})$ leading from t to $x_1^{-\infty} \cdots x_k^{-\infty}$, or from t to t with $\mathcal{C}(D) \neq 1$.*

Proof: By the above considerations, we already know that $u \in I(\mathcal{B})$ iff there is a derivation D: $T(u) = \gamma_0 \rightarrow \gamma_1 \rightarrow \ldots \rightarrow \gamma_n$ in $\mathcal{P}(\mathcal{B})$ with $\gamma_n = x_1^{-\infty} \cdots x_k^{-\infty}$, or $\gamma_n = T(u)$, and $\mathcal{C}(D) \neq 1$. If $\gamma_n = x_1^{-\infty} \cdots x_k^{-\infty}$, then there is nothing left to prove. In the following we assume that $x_1^{-\infty} \cdots x_k^{-\infty} \notin [T(u)]_{\mathcal{P}(\mathcal{B})}$. We derive from $u \in I(\mathcal{B})$, $\gamma_n = T(u)$, and $\gamma_i \neq x_1^{-\infty} \cdots x_k^{-\infty}$, $i \in I_n$, that there is a repetition-free derivation $\overline{D}$ in $\mathcal{P}(\mathcal{B})$ leading from some $t \in [T(u)]_{\mathcal{P}(\mathcal{B})}$ to t with $\mathcal{C}(\overline{D}) \neq 1$. We have $\mathcal{C}(D) = c_1 \cdots c_n \neq 1$. If $\gamma_1 = \gamma_{n-1}$, then $c_1 = \frac{1}{c_n}$, and $\mathcal{C}(D) = c_2 \cdots c_{n-1}$. Generally, if $\gamma_i = \gamma_{n-i}$ for $i = 1, \ldots, j$, $j \leq \left\lfloor \frac{n}{2} \right\rfloor - 1$, then $\mathcal{C}(D) = c_{j+1} \cdots c_{n-j} \neq 1$. Thus, D': $\gamma_j \rightarrow \gamma_{j+1} \rightarrow \ldots \rightarrow \gamma_{n-j}$ is a subderivation of D with $\mathcal{C}(D') = \mathcal{C}(D) \neq 1$, $\gamma_j = \gamma_{n-j}$, and $\gamma_{j+1} \neq \gamma_{n-j-1}$. If D' is repetition-free, then we are finished. Otherwise, define m_1 as the largest, and m_2 as the smallest index such that $j+1 < m_1 < m_2 < n-j-1$, and $\gamma_{m_1-1} = \gamma_{m_2}$. Let D'' be the repetition-free derivation $\gamma_{m_1-1} \rightarrow \ldots \rightarrow \gamma_{m_2}$. If $\mathcal{C}(D'') = c_{m_1} \cdots c_{m_2} \neq 1$, then we are finished. Otherwise, *i.e.,* if $\mathcal{C}(D'') = 1$, we consider the derivation D''': $\gamma_j \rightarrow \ldots \rightarrow \gamma_{m_1-1} = \gamma_{m_2} \rightarrow \ldots \rightarrow \gamma_{n-j}$ with $\mathcal{C}(D''') = \mathcal{C}(D) = c_j \cdots c_{m_1-1} \cdot c_{m_2+1} \cdots c_{n-j} \neq 1$, and by induction obtain a repetition-free derivation $\overline{D}$ in $\mathcal{P}(\mathcal{B})$ leading from some $t \in [T(u)]_{\mathcal{P}(\mathcal{B})}$ to t with $\mathcal{C}(\overline{D}) \neq 1$.

For the converse implication assume that there is some $t \in [T(u)]_{\mathcal{P}(\mathcal{B})}$ such that there is a derivation D: $t = \gamma_0 \rightarrow \gamma_1 \rightarrow \ldots \rightarrow \gamma_n$ in $\mathcal{P}(\mathcal{B})$ with $\gamma_n = x_1^{-\infty} \cdots x_k^{-\infty}$, or $\gamma_n = t$, and $\mathcal{C}(D) \neq 1$. Then, there is also a derivation D': $T(u) = \overline{\gamma}_0 \rightarrow \ldots \rightarrow$

$\overline{\gamma}_m = t = \gamma_0 \to \gamma_1 \to \ldots \to \gamma_n$ in $\mathcal{P}(\mathcal{B})$ for some $m \in \mathbb{N}$. If $\gamma_n = x_1^{-\infty} \cdots x_k^{-\infty}$, then it is clear that $u \in I(\mathcal{B})$. If $\gamma_n = t$, and $\mathcal{C}(D) \neq 1$, then the multiplicative factor of the derivation D'': $T(u) = \overline{\gamma}_0 \to \ldots \to \overline{\gamma}_m = t = \gamma_0 \to \gamma_1 \to \ldots \to \gamma_n = t = \overline{\gamma}_m \to \ldots \to \overline{\gamma}_0 = T(u)$ satisfies $\mathcal{C}(D'') = \mathcal{C}(D) \neq 1$, and hence $u \in I(\mathcal{B})$. □

In the last part of the above proof we already showed the following lemma.

Lemma 6 *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{B} = \{l_i - r_i;\ l_i, r_i \in M[X], C(l_i) = 1, i \in I_h\}$, and $u \neq 0$ be a monomial in $M[X]$. Then for all $t \in [T(u)]_{\mathcal{P}(\mathcal{B})}$*

$$u \in I(\mathcal{B}) \quad \Longleftrightarrow \quad t \in I(\mathcal{B})\,.$$

Putting the above results, and Proposition 2 together, we proved the following.

Theorem 6 *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{B} = \{l_i - r_i;\ l_i, r_i \in M[X], C(l_i) = 1, i \in I_h\}$, and $u \neq 0$ be a monomial in $M[X]$. Then the following are equivalent:*

(i) $u \in I(\mathcal{B})$.

(ii) There is a derivation D: $T(u) = \gamma_0 \to \gamma_1 \to \ldots \to \gamma_n$ of length n in $\mathcal{P}(\mathcal{B})$ leading from $T(u)$ to $x_1^{-\infty} \cdots x_k^{-\infty}$, or from $T(u)$ to $T(u)$ with $\mathcal{C}(D) \neq 1$ such that, for $j \in I_n$,

$$\text{size}(\gamma_j) \leq \text{size}(u, \mathcal{B}) \cdot 2^{c_1 \cdot k},$$

and

$$\text{size}(n) \leq \text{size}(u, \mathcal{B}) \cdot 2^{c_2 \cdot k},$$

where $c_1, c_2 > 0$ are some constants independent of $\mathcal{B}$, and u.

Furthermore, we can show the following:

Theorem 7 *Let $X = \{x_1, \ldots, x_k\}$, and $\mathcal{B} = \{l_i - r_i;\ l_i, r_i \in M[X], C(l_i) = 1, i \in I_h\}$. Then there is a (deterministic) Turing machine M and some constant $c > 0$ independent of $\mathcal{B}$, such that M decides for any monomial $u \neq 0$ in $M[X]$ whether $u \in I(\mathcal{B})$ using at most space $(\text{size}(u, \mathcal{B}))^2 \cdot 2^{c \cdot k}$.*

Proof: By Theorem 6, a nondeterministic Turing machine may determine whether $u \in I(\mathcal{B})$ by generating a derivation D: $T(u) = \gamma_0 \to \gamma_1 \to \ldots \to \gamma_n$ of length n in $\mathcal{P}(\mathcal{B})$ leading from $T(u)$ to $x_1^{-\infty} \cdots x_k^{-\infty}$, or from $T(u)$ to $T(u)$ with $\mathcal{C}(D) \neq 1$ iff there is one. If $x_1^{-\infty} \cdots x_k^{-\infty} \in [T(u)]_{\mathcal{P}(\mathcal{B})}$, then, by Proposition 3, we can conclude the assertion. In the following we assume that $x_1^{-\infty} \cdots x_k^{-\infty} \notin [T(u)]_{\mathcal{P}(\mathcal{B})}$. Then the Turing machine has to decide whether there is a derivation D from $T(u)$ to $T(u)$ with $\mathcal{C}(D) \neq 1$. For this purpose, the Turing machine needs $2h$ counters $z_1, \ldots, z_{2h}$ - two for each congruence $T(l_i) \equiv T(r_i)$ in $\mathcal{P}(\mathcal{B})$ - to know how often, and in which direction (*i.e.* $T(l_i) \to T(r_i)$, or $T(r_i) \to T(l_i)$) each of the congruences has been applied in D. (Note that, since $x_1^{-\infty} \cdots x_k^{-\infty} \notin [T(u)]_{\mathcal{P}(\mathcal{B})}$, in any derivation starting at $T(u)$ no congruence with $r_i = 0$ (by definition $l_i \neq 0$ for all $i \in I_h$) can be applied (*i.e.*, $z_i = 0$ iff $r_i = 0$), and hence at the end of D $z_1 + z_2 + \ldots + z_{2h} =$

n.) Then $\mathcal{C}(D) = \prod_{i \in I_h; r_i \neq 0} \left(\frac{a_i}{b_i}\right)^{z_{2i-1}} \cdot \left(\frac{b_i}{a_i}\right)^{z_{2i}}$, with $a_i \in \mathbb{Z} - \{0\}$ the numerator, and $b_i \in \mathbb{N} - \{0\}$ the denominator of $C(r_i) \in \mathbb{Q} - \{0\}$, $i \in I_h$, $r_i \neq 0$. Let $Z := \prod_{i \in I_h; r_i \neq 0} a_i^{\max\{0, z_{2i-1} - z_{2i}\}} \cdot b_i^{\max\{0, z_{2i-1} - z_{2i}\}}$ and $N := \prod_{i \in I_h; r_i \neq 0} b_i^{\max\{0, z_{2i} - z_{2i-1}\}} \cdot a_i^{\max\{0, z_{2i} - z_{2i-1}\}}$, then $\max\{Z, N\} \leq \left(2^{\mathrm{size}(u,\mathcal{B})}\right)^{2^{\mathrm{size}(u,\mathcal{B}) \cdot 2^{d_1 \cdot k}}}$ for some constant $d_1 > 0$ independent of u, and $\mathcal{B}$. By the Chinese Remainder Theorem and the Prime Number Theorem (see *e.g.* [HW85]), we know

$$\begin{aligned} \mathcal{C}(D) = 1 &\iff Z = N \\ &\iff Z \equiv N \bmod p_j \quad \forall\, 1 \leq j \leq m\,, \end{aligned}$$

where p_j, $j \in I_m$, are the prime numbers satisfying $2 \leq p_j \leq d_2 \cdot \log M$ for any integer $M > 2 \cdot \max\{|Z|, |N|\}$ with $d_2 > 0$ some constant independent of u, and $\mathcal{B}$. Thus, the products Z, and N only have to be computed modulo the prime numbers p_j, $j \in I_m$, and hence the decision whether $Z = N$ uses at most space $\mathrm{size}(u, \mathcal{B}) \cdot 2^{d \cdot k}$, where $d > 0$ is some constant independent of u, and $\mathcal{B}$.

Moreover, for generating the derivation D, the nondeterministic Turing machine has to keep in storage at any time two consecutive words γ_{i-1} and γ_i of D in order to check whether $\gamma_{i-1} \rightarrow \gamma_i$ $(\mathcal{P}(\mathcal{B}))$. Therefore, by Theorem 6 and the above considerations, there is some constant $\bar{c} > 0$ independent of u, and $\mathcal{B}$ such that the nondeterministic Turing machine needs at most $\mathrm{size}(u, \mathcal{B}) \cdot 2^{\bar{c} \cdot k}$ tape cells to determine whether $u \in I(\mathcal{B})$.

By Savitch's Theorem, this nondeterministic Turing machine can be simulated by a deterministic one that calls a recursive boolean function *reachable*$(\gamma_1, \gamma_2, (z_1, \ldots, z_{2h}))$, which returns the boolean value *true* if there exists a derivation from γ_1 to γ_2 consisting of at most $z_1 + z_2 + \ldots + z_{2h}$ steps, and applying $T(l_i) \rightarrow T(r_i)(\mathcal{P}(\mathcal{B}))$ resp., $T(r_i) \rightarrow T(l_i)(\mathcal{P}(\mathcal{B}))$ z_{2i-1} resp., z_{2i} times, $i \in I_h$. The function *reachable* works by looking for the word γ in the middle of the derivation from γ_1 to γ_2, and checking recursively that it is indeed the middle word. For each call we must store the current values of γ, γ_1, and γ_2, of size at most $\mathrm{size}(u, \mathcal{B}) \cdot 2^{c_1 \cdot k}$ each, and the current value of $(z_1, \ldots, z_{2h})$, of size at most $\mathrm{size}(u, \mathcal{B}) \cdot 2^{c_2 \cdot k}$ for some constants $c_1, c_2 > 0$ independent of u, and $\mathcal{B}$. Each call bisects the value of the sum $z_1 + z_2 + \ldots + z_{2h}$, and hence the depth of the recursion is the logarithm of the initial value n of $z_1 + z_2 + \ldots + z_{2h}$. Therefore, by Theorem 6, $(\mathrm{size}(u, \mathcal{B}))^2 \cdot 2^{c \cdot k}$ space suffices for a deterministic Turing machine to decide whether $u \in I(\mathcal{B})$, where $c > 0$ is some constant independent of u, and $\mathcal{B}$. □

4.2 The Algorithm

Now we derive from the algorithm of Section 3 an exponential space algorithm for generating the reduced Gröbner basis of the binomial ideal $I(\mathcal{B})$ w.r.t. some admissible term ordering $\prec$, where $X = \{x_1, \ldots, x_k\}$, and $\mathcal{B} = \{l_i - r_i;\ l_i, r_i \in M[X], C(l_i) = 1, i \in I_h\}$. Because this algorithm works with words in $X_0^* = X^* \cup \{x_1^{-\infty} \cdots x_k^{-\infty}\}$, we define $\prec_0$ to be the term ordering which results from $\prec$ by adding $x_1^{-\infty} \cdots x_k^{-\infty} \prec_0 t$ for all $t \in X^*$. W.l.o.g. we assume $r_i \prec_0 l_i$, $i \in I_h$. As in

Section 3.1, we first analyze the elements of the reduced Gröbner basis of a binomial ideal. Note that $t \in I(\mathcal{B})$ for all $t \in [x_1^{-\infty} \cdots x_k^{-\infty}]_{\mathcal{P}(\mathcal{B})}$.

Lemma 7 *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{B} = \{l_i - r_i;\ l_i, r_i \in M[X], C(l_i) = 1, i \in I_h\}$, and $G = \{h_1 - m_1, \ldots, h_r - m_r;\ C(h_i) = 1, i \in I_r\}$ be the reduced Gröbner basis of the ideal $I(\mathcal{B})$ w.r.t. some admissible term ordering $\prec$ ($m_i \prec_0 h_i$). Then, if $m_i \neq 0$, m_i is the minimal element (w.r.t. $\prec_0$) of the congruence class $[h_i]_{\mathcal{P}(\mathcal{B})}$, $i \in I_r$.*

Proof: With Theorem 4 and Theorem 6, this proof follows immediately from the proof of Theorem 1. □

Lemma 8 *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{B} = \{l_i - r_i;\ l_i, r_i \in M[X], C(l_i) = 1, i \in I_h\}$, and $G = \{h_1 - m_1, \ldots, h_r - m_r;\ C(h_i) = 1, i \in I_r\}$ be the reduced Gröbner basis of the ideal $I(\mathcal{B})$ w.r.t. some admissible term ordering $\prec$ ($m_i \prec_0 h_i$). Then $LT(I(\mathcal{B}))$ (the set of the leading terms of $I(\mathcal{B})$) is the set of all terms $t \neq 0$ with either $t \in I(\mathcal{B})$, or, if $t \notin I(\mathcal{B})$, with nontrivial congruence class in $\mathcal{P}(\mathcal{B})$, and t is* not *the minimal element m_t of its congruence class w.r.t. $\prec_0$ (note, if $t \notin I(\mathcal{B})$, then $m_t \neq x_1^{-\infty} \cdots x_k^{-\infty}$). $H = \{h_1, \ldots, h_r\}$ is the set of the minimal elements of $LT(I(\mathcal{B}))$ w.r.t. divisibility.*

Proof: With Theorem 4 and Theorem 6, this proof follows immediately from the proof of Theorem 2. □

For any two terms t_1, $t_2 \in X_0^*$, $t_1 \neq t_2$, with $t_1 \equiv t_2 \bmod \mathcal{P}(\mathcal{B})$, it follows $t_1 - \mathcal{C}(D) \cdot t_2 \in I(\mathcal{B})$, where D is a derivation from t_1 to t_2 in $\mathcal{P}(\mathcal{B})$. By definition $\mathcal{C}(D) = \prod_{i \in I_h; r_i \neq 0} C(r_i)^{z_{2i-1}} \cdot \left(\frac{1}{C(r_i)}\right)^{z_{2i}}$, where z_{2i-1} is the number of applications of $T(l_i) \to T(r_i)(\mathcal{P}(\mathcal{B}))$, and z_{2i} the number of applications of $T(r_i) \to T(l_i)(\mathcal{P}(\mathcal{B}))$ in D, $i \in I_h$, $r_i \neq 0$. Since, by Theorem 4, the size of each z_i, $i \in I_{2h}$, is bounded by size$(t_1, t_2, \mathcal{B}) \cdot 2^{c \cdot k}$, $\mathcal{C}(D)$ can be represented in space size$(t_1, t_2, \mathcal{B}) \cdot 2^{d \cdot k}$, where c, $d > 0$ are some constants independent of $\mathcal{B}$, t_1, and t_2.

Thus, we get an exponential space algorithm for constructing the reduced Gröbner basis of general binomial ideals which is rather similar to Algorithm 1 for pure difference binomial ideals. A listing of this Algorithm 2 is given in the Appendix.

Putting everything together, we proved the theorem:

Theorem 8 *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{B} = \{l_i - r_i;\ l_i, r_i \in M[X], C(l_i) = 1, i \in I_h\}$, and $\prec$ be some admissible term ordering. Then there is an algorithm which generates the reduced Gröbner basis $G = \{h_1 - m_1, \ldots, h_r - m_r;\ C(h_i) = 1, i \in I_r\}$ of the binomial ideal $I(\mathcal{B})$ using at most space $(\text{size}(\mathcal{B}))^2 \cdot 2^{\bar{c} \cdot k} \leq 2^{c \cdot \text{size}(\mathcal{B})}$, where $\bar{c}, c > 0$ are some constants independent of $\mathcal{B}$.*

5 Conclusion

The results obtained in this paper first give an algorithm for generating the reduced Gröbner basis of a pure difference binomial ideal using at most space $2^{c \cdot n}$, where n is the size of the problem instance, and $c > 0$ some constant independent of n. The fundamental concept is the algorithm in [MM82] for the uniform word problem in commutative semigroups.

Because of the close relationship between commutative semigroups and pure difference binomial ideals, our basis construction algorithm has a number of applications to finitely presented commutative semigroups. Besides those mentioned in Section 3.3, we are able to derive exponential space complete decision procedures for the subword, finite enumeration, finite containment, and equivalence problems for commutative semigroups (see [KM96]).

Furthermore, as shown in Section 4, we obtain an algorithm for transforming any given basis into the reduced Gröbner basis for binomial ideals in general, which also requires at most space $2^{c \cdot n}$ for some constant $d > 0$ independent of the the size n of the problem instance. Since, in the worst case, any Gröbner basis can have maximal degree at least 2^{2^n}, any algorithm for computing Gröbner bases requires at least exponential space (see [MM82], [Huy86]).

References

[Bay82] D. Bayer. The division algorithm and the Hilbert scheme. Ph.d. thesis, Harvard University, Cambridge, MA, 1982.

[Buc65] B. Buchberger. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal. Ph.d. thesis, Department of Mathematics, University of Innsbruck, 1965.

[Dub90] T.W. Dubé. The structure of polynomial ideals and Gröbner bases. *SIAM J. Comput.*, 19:750–773, 1990.

[EiSt94] D. Eisenbud and B. Sturmfels. Binomial Ideals. Preprint, June 1994.

[FW78] S. Fortune and J. Wyllie. Parallelism in random access machines. In *Proceedings of the 10th Ann. ACM Symposium on Theory of Computing (San Diego, CA)*, pages 114–118, New York, 1978. ACM, ACM Press.

[HW85] G.H. Hardy and E.M. Wright. An Introduction to the Theory of Numbers. Oxford, 5*th* Edition 1985. Clarendon Press.

[Her26] G. Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Math. Ann.*, 95:736–788, 1926.

[Hi64] H. Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero: I. *Ann. of Math.*, 79(1):109–203, 1964.

[Huy86] D.T. Huynh. A superexponential lower bound for Gröbner bases and Church-Rosser commutative Thue systems. *Inf. Control*, 68(1-3):196–206, 1986.

[KM96] U. Koppenhagen and E.W. Mayr. The Complexity of the Equivalence Problem for Commutative Semigroups. Technical Report TUM-I9603, Institut für Informatik, Technische Universität München, January 1996.

[KuMa96] K. Kühnle and E.W. Mayr. Exponential space computation of Gröbner bases. Technical Report TUM-I9606, Institut für Informatik, Technische Universität München, January 1996.

[MM82] E.W. Mayr and A. Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Adv. Math.*, 46(3):305–329, December 1982.

[MoMo84] H.M. Möller and F. Mora. Upper and lower bounds for the degree of Gröbner bases. In *Proceedings of the 3rd International Symposium on Symbolic and Algebraic Computation, EUROSAM 84*, volume 174 of *LNCS*, pages 172–183, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong, 1984. Springer Verlag.

[Rob85] L. Robbiano. Term orderings on the polynomial ring. In *Proceedings of the 10th European Conference on Computer Algebra, EUROCAL '85. Vol. 2: Research contributions (Linz, Austria, April 1-3, 1985)*, volume 204 of *LNCS*, pages 513–517, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong, 1985. Springer Verlag.

[Wei87] V. Weispfenning. Admissible orders and linear forms. *ACM SIGSAM Bulletin*, 21(2):16–18, 1987.

6 Appendix

The listing of the exponential space algorithm for constructing the reduced Gröbner basis of a general binomial ideal:

Algorithm 2

```
Input:    $\mathcal{B} = \{l_1 - r_1, \ldots, l_h - r_h;\ C(l_i) = 1,\ i \in I_h\}$, admissible term ordering $\prec$
Output:   the reduced Gröbner basis $G = \{h_1 - m_1, \ldots, h_r - m_r;\ C(h_i) = 1,\ i \in I_r\}$ of $I(\mathcal{B})$
$L' := \{T(l_1), \ldots, T(l_{n'_l})\}$     the set of the minimal elements $\neq 0$ of $\{T(l_1), \ldots, T(l_h)\}$ w.r.t.
                                          divisibility
$R := \{T(r_1), \ldots, T(r_{n_r})\}$      the subset of $\{T(r_1), \ldots, T(r_h)\}$ which contains only minimal
                                          elements $\neq 0$ of $\{T(l_1), \ldots, T(l_{n'_l}),\ T(r_1), \ldots, T(r_h)\}$ w.r.t.
                                          divisibility
$L := \{T(l_1), \ldots, T(l_{n_l})\}$      the subset of $\{T(l_1), \ldots, T(l_{n'_l})\}$ which contains only minimal ele-
                                          ments of $\{T(l_1), \ldots, T(l_{n'_l}), T(r_1), \ldots, T(r_{n_r})\}$ w.r.t. divisibility
$d_m := \max\{\deg(l_i),\ \deg(r_i);\ i \in I_h\}$ ;   $d := 2 \cdot \left(\frac{d_m^2}{2} + d_m\right)^{2^{k-1}}$ ;   $G := \emptyset$ ;   $h := 1$
repeat
  $h :=$ the term of $LT(\langle L', R\rangle) - LT(\langle L'\rangle) \cup (L' - L)$ with degree $\leq d$ which follows $h$ in the
        lexicographic order defined by $x_1 \prec_{lex} x_2 \prec_{lex} \ldots \prec_{lex} x_k$   co $h = x_1^{e_1} \cdots x_k^{e_k}$ co
  if $h \notin I(\mathcal{B})$ then $\overline{d} := \deg(h)$ ;  $m := 1$
    repeat
      $m :=$ the term $t \cdot T(r_i)$ with $t \cdot T(r_i) \prec h, T(r_i) \in R, t \in X^*, \deg(t \cdot T(r_i)) \leq d$ which
            follows $m$ in the term ordering $\prec$
    until ( $m \equiv h \bmod \mathcal{P}(\mathcal{B})$ or there is no more $t \cdot T(r_i)$ with $t \cdot T(r_i) \prec h, T(r_i) \in R$,
                                          $t \in X^*, \deg(t \cdot T(r_i)) \leq d$ )
  end_if
  if $h \in I(\mathcal{B})$ or $m \equiv h \bmod \mathcal{P}(\mathcal{B})$, $i.e.$ there is a derivation $D$ from $h$ to $m$ in $\mathcal{P}(\mathcal{B})$ then
    co $h \in LT(I(\mathcal{B}))$ co
    for each $i \in I_k$ with $e_i \geq 1$ do $h' := x_1^{e_1} \cdots x_i^{e_i - 1} \cdots x_k^{e_k}$
      if $h' \in I(\mathcal{B})$ then next $h$ with $h_{old}$ does not divide $h_{new}$ end_if
        co $h' \in LT(I(\mathcal{B})) \Rightarrow h \notin H$ co
      $m' := 1$
      repeat
        $m' :=$ the term $t \cdot T(r_i)$ with $t \cdot T(r_i) \prec h'$, $T(r_i) \in R$, $t \in X^*$, $\deg(t \cdot T(r_i)) \leq$
              $(\overline{d} - 1) + d$ which follows $m'$ in the term ordering $\prec$
      until ( $m' \equiv h' \bmod \mathcal{P}(\mathcal{B})$ or there is no more $t \cdot T(r_i)$ with $t \cdot T(r_i) \prec h'$, $T(r_i) \in R$,
                                          $t \in X^*, \deg(t \cdot T(r_i)) \leq (\overline{d} - 1) + d$ )
      if $m' \equiv h' \bmod \mathcal{P}(\mathcal{B})$ then next $h$ with $h_{old}$ does not divide $h_{new}$ end_if
        co $h' \in LT(I(\mathcal{B})) \Rightarrow h \notin H$ co
    end_for
    if $h \in I(\mathcal{B})$ then $G := G \cup \{h\}$ else $G := G \cup \{h - \mathcal{C}(D) \cdot m\}$ end_if
    next $h$ with $h_{old}$ does not divide $h_{new}$
  end_if
until there is no more $h \in LT(\langle L', R\rangle) - LT(\langle L'\rangle) \cup (L' - L)$ with degree $\leq d$
for each $T(l_i) \in L$ do
  if $T(l_i) \notin I(\mathcal{B})$ then $m := 1$
    repeat
      $m :=$ the term $t \cdot T(r_i)$ with $t \cdot T(r_i) \prec l_i, T(r_i) \in R, t \in X^*, \deg(t \cdot T(r_i)) \leq d$ which
            follows $m$ in the term ordering $\prec$
    until $m \equiv T(l_i) \bmod \mathcal{P}(\mathcal{B})$, $i.e.$ there is a derivation $D$ from $T(l_i)$ to $m$ in $\mathcal{P}(\mathcal{B})$
  end_if
  if $T(l_i) \in I(\mathcal{B})$ then $G := G \cup \{T(l_i)\}$ else $G := G \cup \{T(l_i) - \mathcal{C}(D) \cdot m\}$ end_if
end_for
```