J. Symbolic Computation (1999) **28**, 317–338
Article No. jsco.1999.0285
Available online at http://www.idealibrary.com on IDEAL®

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

ULLA KOPPENHAGEN† AND ERNST W. MAYR

Institut für Informatik, Technische Universität München, D-80290 München, Germany

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 an optimal algorithm for the uniform word problem in commutative semigroups, we first derive an exponential space algorithm for constructing the reduced Gröbner basis of pure difference binomial ideals. 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 over $\mathbb{Q}$ 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, such as language generating and term rewriting systems, tiling problems, algebraic manifolds, motion planning, and several models for parallel systems.

Using Gröbner bases (see Buchberger, 1965, 1976, 1985; also Hironaka, 1964) many of these 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 David and Bayer (1982) and Möller and Mora (1984) where upper bounds for the degrees in a minimal Gröbner basis were derived. In Dubé (1990), Dubé obtained an improved degree bound of $2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ (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 (1996) exhibited an exponential space computation of Gröbner bases. Their algorithm, however, is based on rather complex parallel computations like parallel rank computations of matrices, and, above that, makes extensive use of the parallel computation thesis of Fortune and Wyllie (1978).

†E-mail: {`koppenha`|`mayr`}`@in.tum.de`

0747–7171/99/090317 + 22 $30.00/0

In this paper, we exploit the close relationship between commutative semigroups and pure difference binomial ideals (for an investigation of the algebraic structure of general binomial ideals see Eisenbud and Sturmfels (1996); concerning toric ideals, a special subset of pure difference binomial ideals, some results based on the connections between toric ideals and integer programming can be found in e.g. Di Biase and Urbanke (1995); Hoşten and Sturmfels (1995); Thomas (1998); Hoşten and Thomas (1998)). Based on the algorithm in Mayr and Meyer (1982) 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 over $\mathbb{Q}$. This algorithm can be implemented, in the case of pure difference binomial ideals, without any difficult parallel rank computations of matrices, or any other complex parallel computations. By the results in Mayr and Meyer (1982) and Huynh (1986), which give a doubly exponential lower bound (in the size of the problem instance) for the maximal degree of the elements of Gröbner bases of pure difference binomial ideals as well as for the cardinality of such bases, our algorithm is space optimal.

Thus, our algorithm and the complexity bounds reported in this paper completely characterize the (asymptotic) computational complexity of Gröbner basis computations for general binomial ideals by basically making use of the close relationship between commutative semigroups and binomial ideals. We do not consider other techniques commonly used for computing Gröbner bases of ideals and modules, such as critical pairs and completion, because their actual computational complexity is much more complex to investigate. And, for most of these algorithms, the space complexity is doubly exponential, one exponential worse than our algorithm.

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 pure difference binomial ideals, and we 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

2.1. Basic definitions and notations

The polynomial ideals which we obtain by using the relationship of finitely presented commutative semigroups and polynomial ideals are *pure difference binomial ideals*, i.e. ideals that have a basis consisting only of differences of two terms. By looking at Buchberger's algorithm (Buchberger, 1965), 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[†] $\mathbb{Q}[X]$ the (commutative) ring of polynomials with indeterminates $x_1, \ldots, x_k$ and rational coefficients. 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 $e_1 + e_2 + \cdots + e_k$ (which is ≥ 0).

[†]$\mathbb{Q}$ denotes the set of rationals, $\mathbb{N}$ the set of non-negative integers, and $\mathbb{Z}$ the set of integers.

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

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

with $a_i \in \mathbb{Q} \setminus \{0\}$ 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[†]

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

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

An *admissible term ordering* $\succeq$ is given by any admissible ordering on $\mathbb{N}^k$, i.e. any total ordering $\geq$ on $\mathbb{N}^k$ satisfying the following two conditions:

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

(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 the term $x_1^{d_1} \cdots x_k^{d_k}$ is *greater in the term ordering* than the term $x_1^{e_1} \cdots x_k^{e_k}$ (written $x_1^{d_1} \cdots x_k^{d_k} \succ x_1^{e_1} \cdots x_k^{e_k}$).

For a polynomial $f(x_1, \ldots, x_k) = \sum_{i=1}^{n} a_i \cdot t_i$ we always assume that $t_1 \succ t_2 \succ \cdots \succ t_n$. For any such non-zero 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 ordering is given as part of the input by a $k \times k$ integer matrix T such that $x_1^{d_1} \cdots x_k^{d_k} \succ x_1^{e_1} \cdots x_k^{e_k}$ iff, for the corresponding degree vectors d and e, Td is *lexicographically greater* than Te (see Robbiano, 1985; Weispfenning, 1987).

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

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

A Gröbner basis is called *reduced* if no monomial in any one of its polynomials is divisible by the leading term of any other polynomial in the basis.

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[‡] $e_i = \Phi(u, x_i) \in \mathbb{N}$ 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*.

Let $\mathcal{P} = \{l_i \equiv r_i;\ i \in I_h\}$ be some (finite) commutative semigroup presentation with $l_i, r_i \in X^*$ for $i \in I_h$. We say that 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, written $u \equiv v \bmod \mathcal{P}$,

[†]For $n \in \mathbb{N}$, I_n denotes the set $\{1, \ldots, n\}$.

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

iff $u \xrightarrow{*} v(\mathcal{P})$, where $\xrightarrow{*}$ is the reflexive transitive closure of $\rightarrow$. More precisely, we write $u \xrightarrow{+} v(\mathcal{P})$, where $\xrightarrow{+}$ is the transitive closure of $\rightarrow$, if $u \xrightarrow{*} v(\mathcal{P})$ and $u \neq v$. A sequence $(u_0, \ldots, u_n)$ of words $u_i \in X^*$ with $u_i \rightarrow u_{i+1}(\mathcal{P})$ for $i = 0, \ldots, n-1$, is called a *derivation* (of length n) of u_n from u_0 in $\mathcal{P}$. The *congruence class* of $u \in X^*$ modulo $\mathcal{P}$ is the set $[u]_{\mathcal{P}} = \{v \in X^*; u \equiv v \bmod \mathcal{P}\}$.

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

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

2.2. The uniform word problem and the corresponding pure difference binomial ideal membership problem

The *uniform word problem* for commutative semigroups is the problem of deciding for a commutative semigroup presentation $\mathcal{P}$ over some alphabet X and two words $u, v \in X^*$ whether $u \equiv v \bmod \mathcal{P}$. The *polynomial ideal membership problem* 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 2.1. (Mayr and Meyer, 1982) *Let $X = \{x_1, \ldots, x_k\}$ be some finite alphabet, $\mathcal{P} = \{l_i \equiv r_i; i \in I_h\}$ a finite commutative semigroup presentation over X, and u, v two words in X^* with $u \neq v$. Then from $u \equiv v \bmod \mathcal{P}$ it follows that $u - v \in I(\mathcal{P})$, and vice versa, i.e. if there exist $p_1, \ldots, p_h \in \mathbb{Q}[X]$ such that $u - v = \sum_{i=1}^{h} p_i(l_i - r_i)$, then there is a derivation $u = \gamma_0 \rightarrow \gamma_1 \rightarrow \cdots \rightarrow \gamma_n = v(\mathcal{P})$ of v from u in $\mathcal{P}$ such that, for $j \in \{0, 1, \ldots, n\}$,*

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

In the fundamental paper (Hermann, 1926), Hermann gave a doubly exponential degree bound for the polynomial ideal membership problem:

Proposition 2.2. (Hermann, 1926) *Let $X = \{x_1, \ldots, x_k\}$, f, $f_1, \ldots, f_h \in \mathbb{Q}[X]$, and $d = \max\{\deg(f_i); i \in I_h\}$. If $f \in \langle f_1, \ldots, f_h \rangle$, then there exist $p_1, \ldots, p_h \in \mathbb{Q}[X]$ such that:*

(i) $f = \sum_{i=1}^{h} p_i f_i$, *and*
(ii) $\deg(p_i) \leq \deg(f) + (hd)^{2^k}]$ *for all* $i \in I_h$.

By size$(\cdot)$ we shall denote the number of bits needed to encode the argument in some standard way (using radix representation for numbers).

Then the two propositions yield an exponential space upper bound for the uniform word problem for commutative semigroups:

Proposition 2.3. (Mayr and Meyer, 1982) *Let $X = \{x_1, \ldots, x_k\}$ be some finite alphabet, and $\mathcal{P} = \{l_i \equiv r_i; i \in I_h\}$ a finite commutative semigroup presentation over X. 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 $(\mathrm{size}(u, v, \mathcal{P}))^2 \cdot 2^{c \cdot k}$.*

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 is a Gröbner basis of the pure difference binomial ideal $I(\mathcal{P})$ w.r.t. some admissible term ordering $\succeq$, then the minimal element m_C of C w.r.t. $\succ$ is not reducible modulo G.

Proposition 3.1. (Huynh, 1986) *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i; i \in I_h\}$ with $l_i, r_i \in X^*$ for all $i \in I_h$, and let $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ be the reduced Gröbner basis of the ideal $I(\mathcal{P})$ w.r.t. some admissible term ordering $\succeq$ ($h_i \succ m_i$ for all $i \in I_r$). Then:*

(i) *m_i is the minimal element (w.r.t. $\succ$) of the congruence class $[h_i]_{\mathcal{P}}$, $i \in I_r$.*
(ii) *$LT(I(\mathcal{P}))$ (the set of the leading terms of $I(\mathcal{P})$) is the set of all terms with nontrivial congruence class which are* not *the minimal element in their congruence class w.r.t. $\succ$. $H = \{h_1, \ldots, h_r\}$ is the set of the minimal elements of $LT(I(\mathcal{P}))$ w.r.t. divisibility.*

If $s \in X^*$ is the minimal element of its congruence class $[s]_{\mathcal{P}}$ w.r.t. $\succ$, then every subword s' of s is also the minimal element of its congruence class $[s']_{\mathcal{P}}$ w.r.t. $\succ$.

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 (1990). Note that we use exponential notation in representing words over X.

Proposition 3.2. (Dubé, 1990) *Let $F = \{f_1, \ldots, f_h\} \subset \mathbb{Q}[X] = \mathbb{Q}[x_1, \ldots, x_k]$, $I = \langle f_1, \ldots, f_h \rangle$ the ideal of $\mathbb{Q}[X]$ generated by F, and let d be the maximum degree of any $f \in F$. Then for any admissible term ordering $\succeq$, the degree of polynomials required in a Gröbner basis for I w.r.t. $\succeq$ is bounded by*

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

Let $X = \{x_1, \ldots, x_k\}$, $\succeq$ an admissible term ordering on X^*, and $\mathcal{P} = \{l_i \equiv r_i; i \in I_h\}$ where, for all $i \in I_h$, $l_i, r_i \in X^*$ and w.l.o.g. $l_i \succ r_i$. We shall give an exponential space algorithm for generating the reduced Gröbner basis of the pure difference binomial ideal $I(\mathcal{P})$ w.r.t. $\succeq$. 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 $[h_i]_\mathcal{P}$ w.r.t. $\succ$, for $i \in I_r$. From Proposition 3.1, we know that the set $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ is the reduced Gröbner basis of $I(\mathcal{P})$ w.r.t. $\succeq$.

Proposition 3.1 shows that $LT(I(\mathcal{P})) \supseteq \{l_1, \ldots, l_h\}$ and that $LT(I(\mathcal{P})) \subseteq \langle l_1, \ldots, l_h, r_1, \ldots, r_h \rangle$. Let L (resp., R) be the subset of $\{l_1, \ldots, l_h\}$ (resp., $\{r_1, \ldots, r_h\}$) containing all those elements which are also minimal (w.r.t. divisibility) in $\{l_1, \ldots, l_h, r_1, \ldots, r_h\}$.

Then $H \supseteq L$, and we still have to determine the elements in $H \backslash L$, as well as the minimal element m_i (w.r.t. $\succ$) of the congruence class of each $h_i \in H$. From Proposition 3.2, 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 the $l_i - r_i$, $(l_i \equiv r_i) \in \mathcal{P}$. Since $H \setminus L \subseteq LT(\langle L, R \rangle) \setminus L$, we consider the terms in $LT(\langle L, R \rangle) \setminus L$ with degree $\leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$.

Lemma 3.1. *For a term $u \in X^*$ with non-trivial congruence class, the minimal element w.r.t. $\succ$ of $[u]_\mathcal{P}$ is of the form $t \cdot r_i$ with $r_i \in R$, $t \in X^*$.*

Proof. W.l.o.g. assume that u is not the minimal element m_u of $[u]_\mathcal{P}$ w.r.t. $\succ$. Then there is a derivation in $\mathcal{P}$ leading from u to $m_u \prec u$, i.e. $u \xrightarrow{+} m_u(\mathcal{P})$, where $m_u = t \cdot r_i$ for some $r_i \in R$, $t \in X^*$ (note that $l_j \succ r_j$ for all $j \in I_h$). □

For $h = x_1^{e_1} \cdots x_k^{e_k} \in X^*$ and $i \in I_k$ such that $e_i \geq 1$, define $h^{(i)} := x_1^{e_1} \cdots x_i^{e_i - 1} \cdots x_k^{e_k}$. Then $h \in H$ iff, for all $i \in I_k$ with $e_i \geq 1$, $h^{(i)} \notin LT(I(\mathcal{P}))$, i.e. $h^{(i)}$ is the minimal element of $[h^{(i)}]_\mathcal{P}$ w.r.t. $\succ$. Thus, H consists exactly of those terms $h \in X^*$ which have degree $\leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$, which are congruent to some term $t \cdot r_i \prec h$ with $r_i \in R$, $t \in X^*$, and $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$, and for which, for all applicable i, $[h^{(i)}]_\mathcal{P}$ is trivial.

For terms h and $t \cdot r_i$ with $\deg(h)$ and $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$, by Proposition 2.3, the decision whether $h \equiv t \cdot r_i \bmod \mathcal{P}$ uses at most space $(\mathrm{size}(\mathcal{P}))^2 \cdot 2^{c \cdot k}$ for some constant $c > 0$ independent of $\mathcal{P}$. Hence, the condition regarding the reducibility of h can also be checked in space $(\mathrm{size}(\mathcal{P}))^2 \cdot 2^{c \cdot k}$. We decide for the words $t \cdot r_i$ with $h \succ t \cdot r_i$, $r_i \in R$, $t \in X^*$, $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ in ascending order w.r.t. $\succ$ whether $t \cdot r_i \equiv h \bmod \mathcal{P}$ until we find the minimal element m_h of $[h]_\mathcal{P}$, or there is no more $t \cdot r_i$ with $h \succ t \cdot r_i$, $r_i \in R$, $t \in X^*$, $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$. In the latter case, $h \notin H$ and we have to consider the next element of $LT(\langle L, R \rangle) \setminus L$ 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 determine whether $h \in H$.

Testing non-reducibility of the $h^{(i)}$ can also be done in exponential space because of Proposition 2.3 and

Lemma 3.2. *A term $u \in X^*$ with $\deg(u) \leq \overline{d}$ is an element of $LT(I(\mathcal{P}))$ iff there is some $t \cdot r_i$ with $u \succ t \cdot r_i$, $r_i \in R$, $t \in X^*$, and $\deg(t \cdot r_i) \leq \overline{d} + 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ such that $u \xrightarrow{+} t \cdot r_i(\mathcal{P})$.*

Proof. We only have to prove the degree bound. Note that $u \in LT(I(\mathcal{P}))$ iff either $u \in H$, and thus, $\deg(m_u) \leq 2\cdot\left(\frac{d^2}{2}+d\right)^{2^{k-1}}$, where m_u is the minimal (w.r.t. $\succ$) element of $[u]_{\mathcal{P}}$, or there is some $h \in H$ with $u = t_u \cdot h$ for some $t_u \in X^*$. The degree of the minimal (w.r.t. $\succ$) element m_h of $[h]_{\mathcal{P}}$ is bounded by $2\cdot\left(\frac{d^2}{2}+d\right)^{2^{k-1}}$. Since $\succeq$ is an admissible term ordering, from $h \succ m_h$ we obtain $u \succ t_u\cdot m_h$ with $\deg(t_u\cdot m_h) \leq \overline{d}+2\cdot\left(\frac{d^2}{2}+d\right)^{2^{k-1}}$.
□

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

Putting everything together, we proved the theorem:

Theorem 3.1. *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i; i \in I_h\}$ with $l_i, r_i \in X^*$ for all $i \in I_h$, and $\succeq$ 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 $I(\mathcal{P})$ w.r.t. $\succeq$ 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 Huynh (1986), we know that, in the worst case, any Gröbner basis of $I(\mathcal{P})$ has maximal degree at least $2^{2^{c'\cdot\text{size}(\mathcal{P})}}$ for some constant $c' > 0$ independent of $\mathcal{P}$. Hence, any algorithm that computes Gröbner bases of pure difference binomial ideals requires at least exponential space in the worst case.

3.3. applications

testing for reducibility

Let $\mathcal{P}$ be a finite commutative semigroup presentation over some finite alphabet X, $u \in X^*$, and $\succeq$ some admissible term ordering. Then u is the minimal element of $[u]_{\mathcal{P}}$ w.r.t. $\succ$ iff u is in normal form modulo a Gröbner basis G of $I(\mathcal{P})$ w.r.t. $\succeq$, i.e. u is not reducible modulo G. Thus, by Proposition 3.1, u is in normal form modulo G iff $u \notin LT(I(\mathcal{P}))$.

Corollary 3.1. *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i; i \in I_h\}$ with $l_i, r_i \in X^*$ for all $i \in I_h$, and $\succeq$ some admissible term ordering. Then for any $u \in X^*$ there is an algorithm which decides whether $u \in LT(I(\mathcal{P}))$, as well as whether u is the minimal element of its congruence class (w.r.t. $\succ$), i.e. u is in normal form modulo a Gröbner basis of $I(\mathcal{P})$ w.r.t. $\succeq$, using at most space $\text{size}(u) + (\text{size}(\mathcal{P}))^2 \cdot 2^{\bar{c}\cdot k} \leq \text{size}(u) + 2^{c\cdot\text{size}(\mathcal{P})}$, 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 $\{h_1, \ldots, h_r\}$, and $u \in LT(I(\mathcal{P}))$ iff there is some h_i, $i \in I_r$, which divides u. Hence, Corollary 3.1 is a direct consequence of Theorem 3.1. □

Constructing the Reduced Gröbner Basis of a Pure Difference Binomial Ideal

Input: admissible term ordering $\succeq$,
$\mathcal{P} = \{l_1 - r_1, \ldots, l_h - r_h\}$ with $l_i, r_i \in X^*$, $l_i \succ r_i\ \forall i \in I_h$
Output: the reduced Gröbner basis $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ of $I(\mathcal{P})$

L := the subset of elements of $\{l_1, \ldots, l_h\}$ that are minimal in $\{l_1, \ldots, l_h, r_1, \ldots, r_h\}$ w.r.t. divisibility
R := the subset of elements of $\{r_1, \ldots, r_h\}$ that are minimal in $\{l_1, \ldots, l_h, r_1, \ldots, r_h\}$ w.r.t. divisibility
k := number of indeterminates; $d := \max\{\deg(l_i),\ \deg(r_i);\ i \in I_h\}$; $G := \emptyset$

for each $h = x_1^{e_1} \cdots x_k^{e_k} \in LT(\langle L, R\rangle) \setminus L$ with degree $\leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ **do**
  $gb :=$ **false**
  if there exists $t \cdot r_i$ with $h \succ t \cdot r_i$, $r_i \in R$, $t \in X^*$, $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$
    which is $\equiv h \bmod \mathcal{P}$ **then** /* $h \in LT(I(\mathcal{P}))$ */
    $m :=$ the minimal (w.r.t. $\succ$) among these terms
    $gb :=$ **true**
  end_if
  if gb **then** /* $h \in LT(I(\mathcal{P}))$ */
    $\overline{d} := \deg(h)$
    for each $i \in I_k$ with $e_i \geq 1$ **while** gb **do**
      $h' := x_1^{e_1} \cdots x_i^{e_i - 1} \cdots x_k^{e_k}$
      if there exists $t \cdot r_j$ with $h' \succ t \cdot r_j$, $r_j \in R$, $t \in X^*$, $\deg(t \cdot r_j) \leq (\overline{d} - 1) + 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$
        which is $\equiv h' \bmod \mathcal{P}$ **then** /* $h' \in LT(I(\mathcal{P})) \Rightarrow h \notin H$ */
        $gb :=$ **false**
      end_if
    end_for
  end_if
  if gb **then** /* $h \in H$ */
    $G := G \cup \{h - m\}$
  end_if
end_for
for each $l_i \in L$ **do**
  $m :=$ the minimal (w.r.t. $\succ$) among the terms $t \cdot r_j$ with $l_i \succ t \cdot r_j$, $r_j \in R$, $t \in X^*$,
    $\deg(t \cdot r_j) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ which are $\equiv l_i \bmod \mathcal{P}$
  $G := G \cup \{l_i - m\}$
end_for

Figure 1. Algorithm for constructing the reduced Gröbner basis of a pure difference binomial ideal.

FINDING THE MINIMAL ELEMENT AND THE NORMAL FORM

The next corollary shows that the minimal element of a congruence class, or equivalently, the normal form of a term can be found in exponential space.

COROLLARY 3.2. *Let* $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i; i \in I_h\}$ *with* $l_i, r_i \in X^*$ *for all* $i \in I_h$, *and* $\succeq$ *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.* $\succ$*), or equivalently, which determines for any term* $u \in X^*$ *the normal form of* u *modulo* *a Gröbner basis of* $I(\mathcal{P})$ *w.r.t.* $\succeq$*, using at most space* $(\mathrm{size}(u,\mathcal{P}))^2 \cdot 2^{\bar{c}\cdot k} \leq 2^{c\cdot \mathrm{size}(u,\mathcal{P})}$*, 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 we add to $\mathcal{P}$ the congruence $s \equiv u$, where u is the word in X^* for whose congruence class we like to determine the minimal element m_u (w.r.t. $\succ$). Let $X_s = X \cup \{s\}$, $\mathcal{P}_s = \mathcal{P} \cup \{s \equiv u\}$, and let $\succeq_s$ be the admissible term ordering on X_s^* which results from $\succeq$ by adding $s \succ w$ for all $w \in X^*$. Then, by Proposition 3.1, $LT(I(\mathcal{P}_s)) = LT(I(\mathcal{P})) \cup \{s \cdot t; t \in X_s^*\}$, in particular, $s \in LT(I(\mathcal{P}_s))$, and, since s is minimal in $LT(I(\mathcal{P}_s))$ w.r.t. divisibility, $H_s = H \cup \{s\}$, 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. $\succ_s$ is the same as the minimal element of $[v]_{\mathcal{P}}$ w.r.t. $\succ$. Thus, because of Proposition 3.1, $s - m_u$ is an element of the reduced Gröbner basis of $I(\mathcal{P})$ w.r.t. $\succeq$, and, by Theorem 3.1, we can determine the minimal element m_u of $[u]_{\mathcal{P}}$ (w.r.t. $\succ$) in space $(\mathrm{size}(u,\mathcal{P}))^2 \cdot 2^{\bar{c}\cdot k}$ for some constant $\bar{c} > 0$ independent of u and $\mathcal{P}$. □

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

The algorithm of Theorem 3.1 generates the reduced Gröbner basis of pure difference binomial ideals. In this section, we will be concerned with constructing the reduced Gröbner basis of 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 denote the set of all monomials in $\mathbb{Q}[X]$, including 0.

By a *binomial* in $\mathbb{Q}[X]$ we mean a polynomial with at most two monomials, say $l - r$. For a finite set $\mathcal{B} = \{l_i - r_i; i \in I_h\}$ with $l_i, r_i \in M[X]$ for all $i \in I_h$, $I(\mathcal{B})$ 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 $c \in \mathbb{Q} \setminus \{0\}$. (Otherwise we could 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 3.1 from pure difference binomial ideals to binomial ideals. First, we establish some technical details.

For $X = \{x_1, \ldots, x_k\}$, and $\mathcal{B} = \{l_i - r_i; i \in I_h\}$ a set of binomials in $\mathbb{Q}[X]$ with $l_i \in X^*$, i.e. $C(l_i) = 1$, $T(l_i) = l_i$, and $r_i \in M[X]$ for all $i \in I_h$, we define the corresponding commutative semigroup presentation

$$\mathcal{P}(\mathcal{B}) = \{l_i \equiv T(r_i); (l_i - r_i) \in \mathcal{B}\},$$

where we set

$$T(0) = x_1^{-\infty} \cdot x_2^{-\infty} \cdots x_k^{-\infty}.$$

Let $\succeq$ be some admissible term ordering on X^*. Then we extend $\succeq$ to an admissible term ordering on $X_0^* = X^* \cup \{x_1^{-\infty} \cdots x_k^{-\infty}\}$ by setting, for all $t \in X^*$,

$$t \succ x_1^{-\infty} \cdot x_2^{-\infty} \cdots x_k^{-\infty}.$$

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 works 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, $v \in X_0^*$,

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

W.l.o.g. we assume that, for all $i \in I_h$,

$$l_i \succ r_i,$$

and that there are no i, $j \in I_h$, $i \neq j$, with $(l_i = l_j) \wedge (T(r_i) = T(r_j))$. (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 l_i and $T(r_i)$.)

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

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

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

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

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

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

Thus, we define the multiplicative factor $\mathcal{C}(D)$ 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 $u = l_{j_1} \cdot w_1$ 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 ith step of D uses $l_i \to T(r_i)(\mathcal{P}(\mathcal{B}))$ resp., $d_i = -c_1 \cdots c_i$ if the ith step of D uses $T(r_i) \to l_i(\mathcal{P}(\mathcal{B}))$. Therefore, $u - \mathcal{C}(D) \cdot v \in I(\mathcal{B})$. Note that u and v are elements of $I(\mathcal{B})$ if $x_1^{-\infty} \cdots x_k^{-\infty}$ occurs in D.

By Propositions 2.1 and 2.2, we conclude the following:

Theorem 4.1. *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{B} = \{l_i - r_i; i \in I_h\}$ with $l_i \in X^*$, $r_i \in M[X]$ for all $i \in I_h$, and let u, v be two monomials in $M[X] \setminus \{0\}$ with $T(u) \neq T(v)$. Then the following are equivalent.*

(i) *There exists* $d \in \mathbb{Q} \setminus \{0\}$ *such that* $u - d \cdot v \in I(\mathcal{B})$.
(ii) *There is a repetition-free derivation* D: $T(u) = \gamma_0 \to \gamma_1 \to \cdots \to \gamma_n = T(v)$ *in* $\mathcal{P}(\mathcal{B})$ *leading from* $T(u)$ *to* $T(v)$ *such that, for* $j \in \{0, 1, \ldots, n\}$,

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

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

By Proposition 2.3, we have:

Corollary 4.1. *Let* $X = \{x_1, \ldots, x_k\}$, *and* $\mathcal{B} = \{l_i - r_i; i \in I_h\}$ *with* $l_i \in X^*$, $r_i \in M[X]$ *for all* $i \in I_h$. *Then there is a (deterministic) Turing machine TM and some constant* $c > 0$ *independent of* $\mathcal{B}$ *such that TM decides for any two monomials* $u, v \in M[X] \setminus \{0\}$, $T(u) \neq T(v)$, *whether there exists* $d \in \mathbb{Q} \setminus \{0\}$ *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 obtain similar results concerning the membership of a single monomial in $I(\mathcal{B})$, we need a further detail.

Theorem 4.2. *Let* $X = \{x_1, \ldots, x_k\}$, $\mathcal{B} = \{l_i - r_i; i \in I_h\}$ *with* $l_i \in X^*$, $r_i \in M[X]$ *for all* $i \in I_h$, *and* $u \neq 0$ *a monomial in* $M[X]$. *Then the following are equivalent.*

(i) $u \in I(\mathcal{B})$.
(ii) *There is a derivation* D: $T(u) = \gamma_0 \to \gamma_1 \to \cdots \to \gamma_n$ *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* $j \in \{0, 1, \ldots, n\}$,

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

and

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

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

Proof. By the above considerations, we already know that if there is a derivation D in $\mathcal{P}(\mathcal{B})$ leading from $T(u)$ to $x_1^{-\infty} \cdots x_k^{-\infty}$, then $C(u) \cdot (T(u) - \mathcal{C}(D) \cdot x_1^{-\infty} \cdots x_k^{-\infty}) = u \in I(\mathcal{B})$. Furthermore, we know that if there is a derivation D in $\mathcal{P}(\mathcal{B})$ leading from $T(u)$ to $T(u)$ with $\mathcal{C}(D) \neq 1$, then $T(u) - \mathcal{C}(D) \cdot T(u) = (1 - \mathcal{C}(D)) \cdot T(u) \in I(\mathcal{B})$, and thus, $u \in I(\mathcal{B})$. Hence, it suffices to show that (i) implies (ii).

W.l.o.g. we assume that $C(u) = 1$. If $u \in I(\mathcal{B})$. Then, by Proposition 2.2, there exist $p'_1, \ldots, p'_h \in \mathbb{Q}[X]$ such that

$$u = \sum_{i=1}^{h} p'_i (l_i - r_i),$$

and $\mathrm{size}(p'_i) \leq \mathrm{size}(u, \mathcal{B}) \cdot 2^{c_1 \cdot k}$, where $c_1 > 0$ is some constant independent of u and $\mathcal{B}$. We may assume that $u = \sum_{j=1}^{m} p_j (l_{i_j} - r_{i_j})$, for some $m \geq 1$, where $p_j \in M[X] \setminus \{0\}$, $\deg(p_j) \leq \deg(p'_{i_j})$, $j \in I_m$, $i_j \in I_h$, and there are no $j_1, j_2 \in I_m$, $j_1 \neq j_2$, with $(T(p_{j_1}) = T(p_{j_2})) \wedge (l_{i_{j_1}} = l_{i_{j_2}}) \wedge (T(r_{i_{j_1}}) = T(r_{i_{j_2}}))$. In the following, we construct from this polynomial identity a replacement tree from which we then extract a derivation D either leading from u to $x_1^{-\infty} \cdots x_k^{-\infty}$, or from u to u with $\mathcal{C}(D) \neq 1$. First, the notion of a replacement tree is defined.

A *replacement tree w.r.t.* $/\mathcal{B}$ is a pair (V, E), where V is a subset of the set of terms X_0^*, and E is a subset of the set of ordered 4-tuples $(V \times V \times \mathbb{Q}\setminus\{0\} \times \mathbb{Q})$. The elements of E are called *arcs*. An arc $(v_1, v_2, c, d) \in E$ is *directed* from the term v_1 to the term v_2. Its meaning is that v_2 is derived in one step from v_1 by application of a congruence in $\mathcal{P}(\mathcal{B})$. The third and fourth components c, d of the arc are called the *coefficients* of the arc. The rational number $c \neq 0$ is the multiplicative factor of the production $l_i \to T(r_i)(\mathcal{P}(\mathcal{B}))$ resp., $T(r_i) \to l_i(\mathcal{P}(\mathcal{B}))$, $i \in I_h$, by which v_2 is derived from v_1, and the rational number d shows "how much v_2" is derived from "how much v_1", i.e. $\frac{d}{c} \cdot v_1 \to d \cdot v_2$.

The *in-degree* of a term $v \in V$, $\deg_{\text{in}}(v)$, is the number of arcs directed into v, and the *out-degree* $\deg_{\text{out}}(v)$ of v is the number of arcs directed out of v. In a replacement tree, exactly one term in V has in-degree zero. This term is the *root* of the replacement tree. The terms in V with out-degree zero are called *leaves*.

A replacement tree is divided up into *levels*. A term of a replacement tree belongs to level i, $i \in \mathbb{N}$, if the length of the shortest derivation contained in the replacement tree leading from the root to that term is i. A replacement tree has the form shown in Figure 2. (The coefficients of the arcs do not appear in the picture.)

For each term $v \in V$ in the replacement tree which is not the root, the sum of the coefficients d_i^{in} of the incoming arcs $(., v, ., d_i^{\text{in}}) \in E$, $i \in I_{\deg_{\text{in}}(v)}$, equals the sum of the quotients $\frac{d_j^{\text{out}}}{c_j^{\text{out}}}$ of the coefficients d_j^{out}, c_j^{out} of the outgoing arcs $(v, ., c_j^{\text{out}}, d_j^{\text{out}}) \in E$, $j \in I_{\deg_{\text{out}}(v)}$, i.e.

$$d_1^{\text{in}} + \cdots + d_{\deg_{\text{in}}(v)}^{\text{in}} = \frac{d_1^{\text{out}}}{c_1^{\text{out}}} + \cdots + \frac{d_{\deg_{\text{out}}(v)}^{\text{out}}}{c_{\deg_{\text{out}}(v)}^{\text{out}}}. \tag{4.1}$$

Note that the leaves in a replacement tree have out-degree zero and thus, for leaves, the right-hand side of this equation is zero. The quotients $\frac{d_j^{\text{out}}}{c_j^{\text{out}}}$ of the coefficients d_j^{out}, c_j^{out} of the arcs $(u, ., c_j^{\text{out}}, d_j^{\text{out}}) \in E$, $j \in I_{\deg_{\text{out}}(u)}$, directed out of the root u satisfy

$$1 = \frac{d_1^{\text{out}}}{c_1^{\text{out}}} + \cdots + \frac{d_{\deg_{\text{out}}(u)}^{\text{out}}}{c_{\deg_{\text{out}}(u)}^{\text{out}}}. \tag{4.2}$$

The root of the replacement tree (V, E) to be constructed from the polynomial identity

$$u = \sum_{j=1}^{m} p_j(l_{i_j} - r_{i_j}) \tag{4.3}$$

is the term u. We start with $V = \{u\}$ and $E = \emptyset$. As u appears as a term on the left-hand side of (4.3), the sum of the monomials $p_j a_j$, $j \in I_m$, on the right-hand side of (4.3) with $T(p_j a_j) = u$, $a_j = l_{i_j}$, or $a_j = -r_{i_j}$ yields u, i.e. for $J_u = \{j \in I_m; T(p_j a_j) = u, a_j = l_{i_j}, \text{ or } a_j = -r_{i_j}\}$, we have

$$\sum_{j \in J_u} p_j a_j = u$$

implying

$$\sum_{j \in J_u} p_j b_j = \sum_{j \in I_m \setminus J_u} p_j(l_{i_j} - r_{i_j}),$$

where $b_j = r_{i_j}$ if $a_j = l_{i_j}$ resp., $b_j = -l_{j_i}$ if $a_j = -r_{i_j}$.

This elimination of all the monomials in (4.3) with power product part u can be inter-

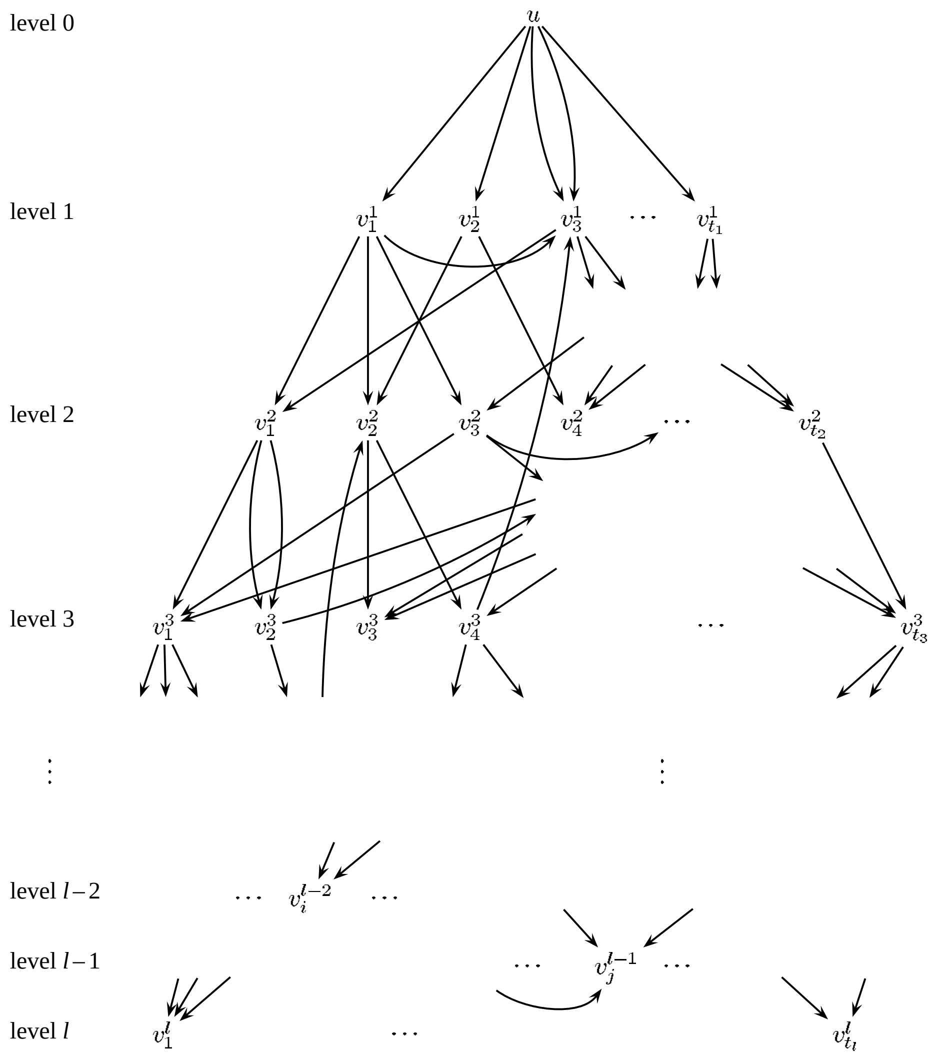

Figure 2. Replacement tree.

preted as one-step derivations $C(p_ja_j)\cdot u \to C(p_jb_j)\cdot T(p_jb_j)$, $j \in J_u$. Add $\{T(p_jb_j); j \in J_u\}$ to V. Then these one-step derivations correspond to the arcs

$$(u, T(p_jb_j), c_j, C(p_jb_j)), j \in J_u,$$

where the c_j are the multiplicative factors of the productions $T(a_j) \to T(b_j)(\mathcal{P}(\mathcal{B}))$, i.e. $V := V \cup \{T(p_jb_j); j \in J_u\}$, $E := E \cup \{(u, T(p_jb_j), c_j, C(p_jb_j)); j \in J_u\}$.

The polynomial identity (4.3) can now be written as

$$\sum_{i=1}^{t} e_iv_i = \sum_{j \in I_m \setminus J_u} p_j(l_{i_j} - r_{i_j}), \tag{4.4}$$

with $v_i \in V \setminus \{x_1^{-\infty}\cdots x_k^{-\infty}\}$ (if $x_1^{-\infty}\cdots x_k^{-\infty} \in V$, then we remember that $x_1^{-\infty}\cdots x_k^{-\infty}$

corresponds to 0) and $e_i \in \mathbb{Q} \setminus \{0\}$, $i \in I_t$. The terms in $\{v_1, \ldots, v_t\}$ are assumed to be pairwise different, and, for each $i \in I_t$, e_i is the resulting coefficient when summing up all coefficients $C(p_j b_j)$, $j \in J_u$, with $T(p_j b_j) = v_i$, i.e.

$$e_i = \sum_{j \in J_u; T(p_j b_j) = v_i} C(p_j b_j).$$

The next step in the construction of the replacement tree is to repeat the described procedure for $e_1 v_1$ on the left-hand side of (4.4). In general, such an elimination step works as follows. At the beginning, we have a polynomial identity

$$\sum_{i=1}^{t} e_i v_i = \sum_{j \in I_m \setminus J_{\mathrm{el}}} p_j (l_{i_j} - r_{i_j}), \tag{4.5}$$

where, for $i \in I_t$, $v_i \in V \setminus \{x_1^{-\infty} \cdots x_k^{-\infty}\}$, $v_i \neq v_{i'}$ for all $i' \in I_t \setminus \{i\}$, $e_i \in \mathbb{Q} \setminus \{0\}$, and $J_{\mathrm{el}} \subset I_m$ contains the indices of already eliminated monomials. Choose a term v_l, $l \in I_t$, which, for instance, belongs to the lowest level among all v_i, $i \in I_t$. The monomial $e_l v_l$ on the left-hand side of (4.5) equals the sum of the monomials $p_j a_j$, $j \in I_m \setminus J_{\mathrm{el}}$, on the right-hand side of (4.5) with $T(p_j a_j) = v_l$, $a_j = l_{i_j}$, or $a_j = -r_{i_j}$, i.e. for $J_{v_l} = \{j \in I_m \setminus J_{\mathrm{el}}; T(p_j a_j) = v_l, a_j = l_{i_j}, \text{ or } a_j = -r_{i_j}\}$, we have

$$\sum_{j \in J_{v_l}} p_j a_j = e_l v_l$$

which implies

$$\sum_{j \in J_{v_l}} p_j b_j + \sum_{i \in I_t \setminus \{l\}} e_i v_i = \sum_{j \in (I_m \setminus J_{\mathrm{el}}) \setminus J_{v_l}} p_j (l_{i_j} - r_{i_j}),$$

where $b_j = r_{i_j}$ if $a_j = l_{i_j}$ resp., $b_j = -l_{j_i}$ if $a_j = -r_{i_j}$.

Let $V := V \cup \{T(p_j b_j); j \in J_{v_l}\}$, and $E := E \cup \{(v_l, T(p_j b_j), c_j, C(p_j b_j)); j \in J_{v_l}\}$, where c_j is the multiplicative factor of $T(a_j) \to T(b_j)$ $(\mathcal{P}(\mathcal{B}))$. From (4.5) we obtain as a new polynomial identity

$$\sum_{i=1}^{\bar{t}} \bar{e}_i \bar{v}_i = \sum_{j \in (I_m \setminus J_{\mathrm{el}}) \setminus J_{v_l}} p_j (l_{i_j} - r_{i_j}),$$

where, for $i \in I_{\bar{t}}$, $\bar{v}_i \in V \setminus \{x_1^{-\infty} \cdots x_k^{-\infty}\}$, $\bar{v}_i \neq \bar{v}_{i'}$ for all $i' \in I_{\bar{t}} \setminus \{i\}$, and, if in (4.5) there is some $i_1 \in I_t$ with $v_{i_1} = \bar{v}_i$, then

$$\bar{e}_i = e_{i_1} + \sum_{j \in J_{v_l}; T(p_j b_j) = \bar{v}_i} C(p_j b_j),$$

else

$$\bar{e}_i = \sum_{j \in J_{v_l}; T(p_j b_j) = \bar{v}_i} C(p_j b_j).$$

The construction is finished if $\bar{e}_i = 0$ for all $i \in I_{\bar{t}}$. Then the pair (V, E) is a replacement tree, because, by construction, for all $v \in V \setminus \{u\}$, the coefficients of the incoming and outgoing arcs satisfy equation (4.1), and the coefficients of the arcs directed out of the root u satisfy equation (4.2).

If in the replacement tree $x_1^{-\infty} \cdots x_k^{-\infty} \in V$, then there is a derivation $u = \gamma_0 \to$

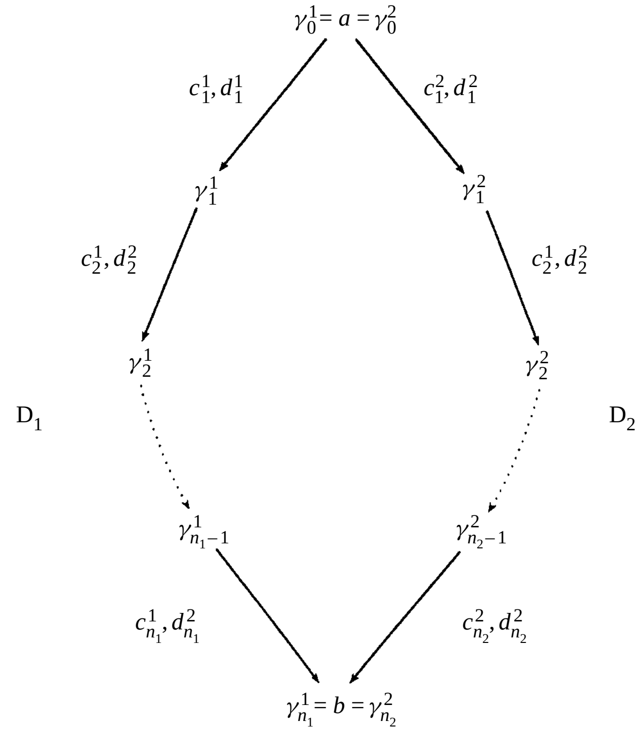

Figure 3. D_1, D_2: two disjoint repetition-free derivations leading from a to b.

$\gamma_1 \to \cdots \to \gamma_n = x_1^{-\infty} \cdots x_k^{-\infty}$ in $\mathcal{P}(\mathcal{B})$ such that, for $j \in \{0, 1, \ldots, n\}$, $\text{size}(\gamma_j) \leq \text{size}(u, \mathcal{B}) \cdot 2^{c_1 \cdot k}$, and $n \leq 2^{\text{size}(u,\mathcal{B}) \cdot 2^{c_2 \cdot k}}$, where $c_1, c_2 > 0$ are some constants independent of u and $\mathcal{B}$, and there is nothing left to prove.

In the following, we assume that $x_1^{-\infty} \cdots x_k^{-\infty} \notin V$. We show how to extract from the constructed replacement tree (V, E) a derivation D in $\mathcal{P}(\mathcal{B})$ leading from u to u with $\mathcal{C}(D) \neq 1$.

Since the leaves of a replacement tree have out-degree zero, the coefficients d_i of the arcs $(., b, ., d_i) \in E$, $i \in I_{\deg_{\text{in}}(b)}$, directed into a leaf $b \in V$ satisfy $d_1 + \cdots + d_{\deg_{\text{in}}(b)} = 0$. Because $b \neq x_1^{-\infty} \cdots x_k^{-\infty}$, it follows from the construction of the replacement tree (V, E) that, for all $i \in I_{\deg_{\text{in}}(b)}$, $d_i \neq 0$, and thus $\deg_{\text{in}}(b) \geq 2$.

Take an arbitrary leaf $b \in V$, and select in the replacement tree (V, E) two repetition-free derivations

$$D_1 : a = \gamma_0^1 \to \gamma_1^1 \to \cdots \to \gamma_{n_1}^1 = b$$

and

$$D_2 : a = \gamma_0^2 \to \gamma_1^2 \to \cdots \to \gamma_{n_2}^2 = b$$

leading from some term $a \in V$ to b with $\gamma_i^1 \notin \{\gamma_1^2, \ldots, \gamma_{n_2-1}^2\}$, $i \in I_{n_1-1}$, and $\gamma_j^2 \notin \{\gamma_1^1, \ldots, \gamma_{n_1-1}^1\}$, $j \in I_{n_2-1}$. Let $(\gamma_i^1, \gamma_{i+1}^1, c_{i+1}^1, d_{i+1}^1)$, $i \in \{0, \ldots, n_1 - 1\}$ resp., $(\gamma_j^2, \gamma_{j+1}^2, c_{j+1}^2, d_{j+1}^2)$, $j \in \{0, \ldots, n_2 - 1\}$ denote the corresponding arcs in E (see Figure 3). Then the multiplicative factors of the derivations D_1, D_2 are $\mathcal{C}(D_1) = c_1^1 \cdots c_{n_1}^1$ and $\mathcal{C}(D_2) = c_1^2 \cdots c_{n_2}^2$.

If $\mathcal{C}(D_1) \neq \mathcal{C}(D_2)$, we are finished because, by reversing the direction of each step in some derivation D: $v_1 = \gamma_0 \to \gamma_1 \to \cdots \to \gamma_n = v_2$ in $\mathcal{P}(\mathcal{B})$, we obtain the reverse derivation D_{r}: $v_2 = \gamma_n \to \gamma_{n-1} \to \cdots \to \gamma_0 = v_1(\mathcal{P}(\mathcal{B}))$ with $\mathcal{C}(D_{\mathrm{r}}) = \frac{1}{\mathcal{C}(D)}$. Furthermore, from (V, E) we obtain a derivation D_u: $u \xrightarrow{*} a(\mathcal{P}(\mathcal{B}))$. Thus, we have a derivation

$$D : u \xrightarrow{*} a \xrightarrow{+} b \xrightarrow{+} a \xrightarrow{*} u$$

in $\mathcal{P}(\mathcal{B})$ with

$$\mathcal{C}(D) = \mathcal{C}(D_u) \cdot \mathcal{C}(D_1) \cdot \frac{1}{\mathcal{C}(D_2)} \cdot \frac{1}{\mathcal{C}(D_u)} \neq 1.$$

In the case $\mathcal{C}(D_1) = \mathcal{C}(D_2)$, we eliminate the arc

$$(\gamma^1_{n_1-1}, b, c^1_{n_1}, d^1_{n_1})$$

from the replacement tree (V, E). Since $\mathcal{C}(D_1) = \mathcal{C}(D_2)$, $d^1_{n_1} b$ can be derived from $\frac{d^1_{n_1}}{\mathcal{C}(D_1)}\, a = \frac{d^1_{n_1}}{\mathcal{C}(D_2)}\, a$ not only by derivation D_1, but also by derivation D_2. The goal is to derive $(d^1_{n_1} + d^2_{n_2})\, b$ from $\frac{d^1_{n_1}+d^2_{n_2}}{\mathcal{C}(D_2)}\, a$ by D_2, and to derive no b from no a by D_1.

To obtain this result, we replace in E

$(\gamma^1_{i-1}, \gamma^1_i, c^1_i, d^1_i)$ by $\left(\gamma^1_{i-1}, \gamma^1_i, c^1_i, d^1_i - \frac{d^1_{n_1}}{c^1_{i+1}\cdots c^1_{n_1}}\right)$, for each $i \in \{1, \ldots, n_1 - 1\}$,
$(\gamma^2_{j-1}, \gamma^2_j, c^2_j, d^2_j)$ by $\left(\gamma^2_{j-1}, \gamma^2_j, c^2_j, d^2_j + \frac{d^1_{n_1}}{c^2_{j+1}\cdots c^2_{n_2}}\right)$, for each $j \in \{1, \ldots, n_2 - 1\}$,
$(\gamma^2_{n_2-1}, \gamma^2_{n_2}, c^2_{n_2}, d^2_{n_2})$ by $(\gamma^2_{n_2-1}, \gamma^2_{n_2}, c^2_{n_2}, d^1_{n_1} + d^2_{n_2})$, and we remove $(\gamma^1_{n_1-1}, \gamma^1_{n_1}, c^1_{n_1}, d^1_{n_1})$.

Since

$$\begin{aligned}
\frac{d^1_1 - \frac{d^1_{n_1}}{c^1_2\cdots c^1_{n_1}}}{c^1_1} + \frac{d^2_1 + \frac{d^1_{n_1}}{c^2_2\cdots c^2_{n_2}}}{c^2_1} &= \frac{d^1_1}{c^1_1} - \frac{d^1_{n_1}}{\mathcal{C}(D_1)} + \frac{d^2_1}{c^2_1} + \frac{d^1_{n_1}}{\mathcal{C}(D_2)} = \frac{d^1_1}{c^1_1} + \frac{d^2_1}{c^2_1},\\
d^1_i - \left(d^1_i - \frac{d^1_{n_1}}{c^1_{i+1}\cdots c^1_{n_1}}\right) &= \frac{d^1_{n_1}}{c^1_{i+1}\cdots c^1_{n_1}} = \frac{d^1_{i+1}}{c^1_{i+1}} - \frac{d^1_{i+1} - \frac{d^1_{n_1}}{c^1_{i+2}\cdots c^1_{n_1}}}{c^1_{i+1}}, i \in I_{n_1-2},\\
d^1_{n_1-1} - \left(d^1_{n_1-1} - \frac{d^1_{n_1}}{c^1_{n_1}}\right) &= \frac{d^1_{n_1}}{c^1_{n_1}} = \frac{d^1_{n_1}}{c^1_{n_1}} - 0,\\
d^2_j - \left(d^2_j + \frac{d^1_{n_1}}{c^2_{j+1}\cdots c^2_{n_2}}\right) &= -\frac{d^1_{n_1}}{c^2_{j+1}\cdots c^2_{n_2}} = \frac{d^2_{j+1}}{c^2_{j+1}} - \frac{d^2_{j+1} + \frac{d^1_{n_1}}{c^2_{j+2}\cdots c^2_{n_2}}}{c^2_{j+1}}, j \in I_{n_2-2},\\
d^2_{n_2-1} - \left(d^2_{n_2-1} + \frac{d^1_{n_1}}{c^2_{n_2}}\right) &= -\frac{d^1_{n_1}}{c^2_{n_2}} = \frac{d^2_{n_2}}{c^2_{n_2}} - \frac{d^1_{n_1} + d^2_{n_2}}{c^2_{n_2}},
\end{aligned}$$

for each $v \in V$, the coefficients of the incoming and outgoing arcs still satisfy equation (4.1) (resp., equation (4.2)). Also, a subsequent removal of all new arcs $(v_1, v_2, c, d) \in E$ with $d = 0$ from E does not change this fact. Hence, after removing all terms $v \in V \backslash \{u\}$ with $\deg_{\mathrm{in}}(v) = 0 (= \deg_{\mathrm{out}}(v))$ from V, the pair (V, E) is still a replacement tree.

In the polynomial identity (4.3), the procedure just described corresponds to a reduction of the number m of products $p_j(l_{i_j} - r_{i_j})$ in the sum on the right-hand side of (4.3) by at least one. Each arc in the replacement tree constructed from the polynomial identity (4.3) corresponds to such a product $p_j(l_{i_j} - r_{i_j})$, $i \in I_m$. Thus, the above elimination of an arc in the replacement tree corresponds to an elimination of some $p_j(l_{i_j} - r_{i_j})$ in (4.3). The resulting modifications of the coefficients of the arcs in the two derivations correspond to appropriate modifications of the coefficients $C(p_j)$ in the respective products $p_j(l_{i_j} - r_{i_j})$.

We may repeat the above argument for any leaf in V, and by induction obtain a derivation D: $u \xrightarrow{+} u$ with $\mathcal{C}(D) \neq 1$. If, during the induction, no such derivation is found until the replacement tree (V, E) only consists of the root u, one leaf b, and two disjoint repetition-free derivations D_1 and D_2 leading from u to b, then, at least now, we have $\mathcal{C}(D_1) \neq \mathcal{C}(D_2)$. Let D_1, D_2, and the corresponding arcs in E be as above. Assume that $\mathcal{C}(D_1) = \mathcal{C}(D_2)$, then from equation (4.1), we obtain

$$d^1_{n_1} = -d^2_{n_2},$$

$$d^1_{n_1-1} = \frac{d^1_{n_1}}{c^1_{n_1}}, \qquad d^1_{n_1-2} = \frac{d^1_{n_1-1}}{c^1_{n_1-1}} = \frac{d^1_{n_1}}{c^1_{n_1-1}\cdot c^1_{n_1}}, \quad \ldots, \quad d^1_1 = \frac{d^1_{n_1}}{c^1_2 \cdots c^1_{n_1}},$$

and

$$d^2_{n_2-1} = \frac{d^2_{n_2}}{c^2_{n_2}}, \qquad d^2_{n_2-2} = \frac{d^2_{n_2-1}}{c^2_{n_2-1}} = \frac{d^2_{n_2}}{c^2_{n_2-1}\cdot c^2_{n_2}}, \quad \ldots, \quad d^2_1 = \frac{d^2_{n_2}}{c^2_2 \cdots c^2_{n_2}}.$$

From equation (4.2), concerning the root we obtain

$$1 = \frac{d^1_1}{c^1_1} + \frac{d^2_1}{c^2_1} = \frac{d^1_{n_1}}{c^1_1 \cdots c^1_{n_1}} + \frac{d^2_{n_2}}{c^2_1 \cdots c^2_{n_2}} = \frac{d^1_{n_1}}{\mathcal{C}(D_1)} + \frac{d^2_{n_2}}{\mathcal{C}(D_2)} = \frac{d^1_{n_1}}{\mathcal{C}(D_1)} - \frac{d^1_{n_1}}{\mathcal{C}(D_2)}$$

which contradicts the assumption. Thus, there is a derivation D: $u = \gamma_0 \to \gamma_1 \to \cdots \to \gamma_n = u$ of length n in $\mathcal{P}(\mathcal{B})$ with $\mathcal{C}(D) \neq 1$ such that, for $j \in \{0, 1, \ldots, n\}$, $\text{size}(\gamma_j) \leq \text{size}(u, \mathcal{B}) \cdot 2^{c_1 \cdot k}$, and $n \leq 2^{\text{size}(u,\mathcal{B})\cdot 2^{c_2 \cdot k}}$, where $c_1, c_2 > 0$ are some constants independent of u and $\mathcal{B}$. □

Furthermore, we can show the following:

THEOREM 4.3. *Let* $X = \{x_1, \ldots, x_k\}$, *and* $\mathcal{B} = \{l_i - r_i; i \in I_h\}$ *with* $l_i \in X^*$, $r_i \in M[X]$ *for all* $i \in I_h$. *Then there is a (deterministic) Turing machine TM and some constant* $c > 0$ *independent of* $\mathcal{B}$ *such that TM decides, for any monomial* $u \neq 0$ *in* $M[X]$, *whether* $u \in I(\mathcal{B})$ *uses at most space* $(\text{size}(u, \mathcal{B}))^2 \cdot 2^{c \cdot k}$.

PROOF. By Theorem 4.2, a non-deterministic Turing machine can determine whether $u \in I(\mathcal{B})$ by generating a derivation D: $T(u) = \gamma_0 \to \gamma_1 \to \cdots \to \gamma_n$ of length n (with n doubly exponentially bounded in the size of the problem instance) in $\mathcal{P}(\mathcal{B})$ leading either 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 such a derivation. If $x_1^{-\infty} \cdots x_k^{-\infty} \in [T(u)]_{\mathcal{P}(\mathcal{B})}$, then $u \in I(\mathcal{B})$, and, by Proposition 2.3, we are done. In the other case, we may assume w.l.o.g. that the derivation D uses no congruence whose right-hand side is $x_1^{-\infty} \cdots x_k^{-\infty}$ (note that $l_i \succ r_i$ for all $i \in I_h$). The Turing machine guesses n and $2h$ counters $z_1, \ldots, z_{2h}$—two for each congruence $l_i \equiv T(r_i)$ in $\mathcal{P}(\mathcal{B})$—representing how often, and in which direction (i.e. $l_i \to T(r_i)$, or $T(r_i) \to l_i$) each of the congruences is applied in D. These counters have to satisfy $z_1 + z_2 + \cdots + z_{2h} = n$, and we obtain

$$\mathcal{C}(D) = \prod_{i \in I_h; r_i \neq 0} \left(\frac{a_i}{b_i}\right)^{z_{2i-1}} \cdot \left(\frac{b_i}{a_i}\right)^{z_{2i}},$$

with $a_i \in \mathbb{Z} \setminus \{0\}$ the numerator, and $b_i \in \mathbb{N} \setminus \{0\}$ the denominator of $C(r_i)$, $i \in I_h$, $r_i \neq 0$.
Let

$$Z = \prod_{i \in I_h; r_i \neq 0} a_i^{z_{2i-1}} \cdot b_i^{z_{2i}}$$

and

$$N = \prod_{i \in I_h; r_i \neq 0} b_i^{z_{2i-1}} \cdot a_i^{z_{2i}},$$

then $\max\{|Z|, |N|\} \leq (2^{\mathrm{size}(u,\mathcal{B})})^{2^{\mathrm{size}(u,\mathcal{B}) \cdot 2^{d_1 \cdot k}}}$ 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. Hardy and Wright, 1985), we know

$$\begin{aligned} \mathcal{C}(D) = 1 &\Longleftrightarrow Z = N \\ &\Longleftrightarrow Z \equiv N \bmod p_j \qquad \text{for all } 1 \leq j \leq m, \end{aligned}$$

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 the decision whether $Z = N$ uses at most space $\mathrm{size}(u, \mathcal{B}) \cdot 2^{d \cdot k}$, with $d > 0$ some constant independent of u and $\mathcal{B}$.

The non-deterministic Turing machine can verify that $\mathcal{C}(D) \neq 1$ by guessing a prime p_j with $j \in I_m$ and computing Z and N modulo this prime. A deterministic Turing machine has to loop through the primes p_j, $j \in I_m$.

For generating the derivation D in $\mathcal{P}(\mathcal{B})$, the non-deterministic 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 $\gamma_{i-1} \to \gamma_i(\mathcal{P}(\mathcal{B}))$. Therefore, by Theorem 4.2 and the above considerations, there is some constant $\bar{c} > 0$ independent of u and $\mathcal{B}$ such that the non-deterministic Turing machine needs at most $\mathrm{size}(u, \mathcal{B}) \cdot 2^{\bar{c} \cdot k}$ tape cells to determine whether $u \in I(\mathcal{B})$.

When simulating the non-deterministic Turing machine by a deterministic one, the standard construction of Savitch (1969) has to be slightly modified, halving the length of the derivation being looked for at every level of the recursion and also guessing (by looping through all possibilities) appropriate values for the tuples of counters.

The deterministic Turing machine calls a recursive Boolean function

$$\mathrm{reachable}(\gamma_1, \gamma_2, (z_1, \ldots, z_{2h})),$$

which returns the Boolean value *true* if there exists a derivation from γ_1 to γ_2 in $\mathcal{P}(\mathcal{B})$ consisting of at most $z_1 + z_2 + \cdots + z_{2h}$ steps, and applying $l_i \to T(r_i)\,(\mathcal{P}(\mathcal{B}))$ resp., $T(r_i) \to l_i\,(\mathcal{P}(\mathcal{B}))$ 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, and the current values of the counters $z_1, \ldots, z_{2h}$. These counters always have to add up to the length of the subderivation, and this length is halved at every level of the recursion. Thus, the depth of the recursion is the logarithm of the initial value n of $z_1 + z_2 + \cdots + z_{2h}$, and, by Theorem 4.2, there are at most size$(u, \mathcal{B}) \cdot 2^{c_1 \cdot k}$ many levels of recursion, each requiring at most size$(u, \mathcal{B}) \cdot 2^{c_2 \cdot k}$ space, where c_1, $c_2 > 0$ are some constants independent of u and $\mathcal{B}$. Hence, $(\text{size}(u, \mathcal{B}))^2 \cdot 2^{c \cdot k}$ space suffices for a deterministic Turing machine to decide whether $u \in I(\mathcal{B})$. □

4.2. THE ALGORITHM

Together with the results of Section 3.2, we are now able to derive an exponential space algorithm for generating the reduced Gröbner basis of the binomial ideal $I(\mathcal{B})$ w.r.t. some admissible term ordering $\succeq$, where $X = \{x_1, \ldots, x_k\}$ and $\mathcal{B} = \{l_i - r_i; i \in I_h\}$ with $l_i \in X^*$, $r_i \in M[X]$, and w.l.o.g. $l_i \succ r_i$ for all $i \in I_h$. 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 4.1. *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{B} = \{l_i - r_i; i \in I_h\}$ with $l_i \in X^*$, $r_i \in M[X]$ for all $i \in I_h$, and let $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ be the reduced Gröbner basis of the ideal $I(\mathcal{B})$ w.r.t. some admissible term ordering $\succeq$ ($h_i \succ m_i$, $C(h_i) = 1$ for all $i \in I_r$). Then $T(m_i)$ is the minimal element (w.r.t. $\succ$) of the congruence class $[h_i]_{\mathcal{P}(\mathcal{B})}$, $i \in I_r$.*

PROOF. With Theorems 4.1 and 4.2, this proof follows immediately from the proof of Proposition 3.1. □

LEMMA 4.2. *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{B} = \{l_i - r_i; i \in I_h\}$ with $l_i \in X^*$, $r_i \in M[X]$ for all $i \in I_h$, and let $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ be the reduced Gröbner basis of the ideal $I(\mathcal{B})$ w.r.t. some admissible term ordering $\succeq$ ($h_i \succ m_i$, $C(h_i) = 1$ for all $i \in I_r$). 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 non-trivial congruence class in $\mathcal{P}(\mathcal{B})$ such that t is* not *the minimal (w.r.t. $\succ$) element m_t of its congruence class (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 Theorems 4.1 and 4.2, this proof follows immediately from the proof of Proposition 3.1. □

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 that $t_1 - \mathcal{C}(D) \cdot t_2 \in I(\mathcal{B})$, 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 $l_i \to T(r_i)\,(\mathcal{P}(\mathcal{B}))$, and z_{2i} the number of applications of $T(r_i) \to l_i\,(\mathcal{P}(\mathcal{B}))$ in D, $i \in I_h$, $r_i \neq 0$. Since each z_i, $i \in I_{2h}$, is bounded by $2^{\text{size}(t_1, t_2, \mathcal{B}) \cdot 2^{c \cdot k}}$ for some constant $c > 0$ independent of t_1, t_2, and $\mathcal{B}$, the multiplicative factor $\mathcal{C}(D)$ of D can be triply exponentially large. Its doubly exponentially long representation can be computed in *exponential space* using $\mathcal{NC}$-circuits for multiplication (Karp and Ramachandran, 1990) and appealing to the parallel computation thesis

Constructing the Reduced Gröbner Basis of a Binomial Ideal

```
Input:   admissible term ordering ⪰,
         B = {l_1 − r_1, ..., l_h − r_h} with l_i ∈ X*, r_i ∈ M[X], l_i ≻ r_i ∀i ∈ I_h
Output:  the reduced Gröbner basis G = {h_1 − m_1, ..., h_r − m_r} of I(B)

 L := {l_1, ..., l_h} ∩ min({l_1, ..., l_h, T(r_1), ..., T(r_h)})
      /* min(.) denotes the minimal elements of the argument w.r.t. divisibility */
 R := {T(r_1), ..., T(r_h)} ∩ min({l_1, ..., l_h, T(r_1), ..., T(r_h)})
 k := number of indeterminates; d := max{deg(l_i), deg(r_i); i ∈ I_h}; G := ∅

for each h = x_1^{e_1} ··· x_k^{e_k} ∈ LT(⟨L, R⟩) \ L with degree ≤ 2·(d²/2+d)^{2^{k−1}} do
  gb := false
  if h ∈ I(B) then gb := true
  else
    if there exists t·T(r_i) with h ≻ t·T(r_i), T(r_i) ∈ R, t ∈ X*, deg(t·r_i) ≤ 2·(d²/2+d)^{2^{k−1}}
       which is ≡ h mod P(B)
      then m := the minimal (w.r.t. ≻) among these terms; gb := true
    end_if
  end_if
  if gb then /* h ∈ LT(I(B)) */ d̄ := deg(h)
    for each i ∈ I_k with e_i ≥ 1 while gb do h' := x_1^{e_1} ··· x_i^{e_i−1} ··· x_k^{e_k}
      if ( h' ∈ I(B) or there exists t · T(r_j) with h' ≻ t · T(r_j), T(r_j) ∈ R, t ∈ X*,
                 deg(t·r_j) ≤ (d̄−1)+2·(d²/2+d)^{2^{k−1}} which is ≡ h' mod P(B) )
        then /* h' ∈ LT(I(B)) ⇒ h ∉ H */ gb := false
      end_if
    end_for
  end_if
  if gb then /* h ∈ H */
    if h ∈ I(B) then G := G ∪ {h}
    else
      C(D) := the multiplicative factor of a derivation D in P(B) leading from h to m
      G := G ∪ {h − C(D) · m}
    end_if
  end_if
end_for
for each l_i ∈ L do
  if l_i ∈ I(B) then G := G ∪ {l_i}
  else
    m := the minimal (w.r.t. ≻) among the terms t · T(r_j) with l_i ≻ t · T(r_j), T(r_j) ∈ R,
t ∈ X*,
         deg(t · r_j) ≤ 2·(d²/2+d)^{2^{k−1}} which are ≡ l_i mod P(B)
    C(D) := the multiplicative factor of a derivation D in P(B) leading from l_i to m
    G := G ∪ {l_i − C(D) · m}
  end_if
end_for
```

Figure 4. Algorithm for constructing the reduced Gröbner basis of a general binomial ideal.

of Fortune and Wyllie (1978). If it suffices to compute a representation of the reduced Gröbner basis of $I(\mathcal{B})$ with the coefficients given as products of negative and positive powers of prime numbers, then an appropriate representation of $\mathcal{C}(D)$ can be computed from the representations of the $C(r_i)$ used in D directly without any $\mathcal{NC}$-circuits and the parallel computation thesis.

From the algorithm for constructing the reduced Gröbner basis of pure difference binomial ideals in Figure 1, we obtain the rather similar exponential space algorithm for constructing the reduced Gröbner basis of general binomial ideals given in Figure 4. Putting everything together, we have proved the following theorem:

Theorem 4.4. *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{B} = \{l_i - r_i; i \in I_h\}$ with $l_i \in X^*$, $r_i \in M[X]$ for all $i \in I_h$, and $\succeq$ 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 binomial ideal $I(\mathcal{B})$ w.r.t. $\succeq$ using at most space $(\mathrm{size}(\mathcal{B}))^2 \cdot 2^{\bar{c}\cdot k} \leq 2^{c\cdot \mathrm{size}(\mathcal{B})}$, 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 Mayr and Meyer (1982) 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 coverability, the subword, the finite enumeration, the containment, and the equivalence problems for commutative semigroups (see Koppenhagen and Mayr, 1996a, 1997).

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, also requiring at most space $2^{d\cdot n}$ for some constant $d > 0$ independent of the size n of the problem instance. Since, in the worst case, any Gröbner basis of pure difference binomial ideals can have maximal degree doubly exponential in n, any algorithm for computing Gröbner bases of binomial ideals requires at least exponential space (see Mayr and Meyer, 1982; Huynh, 1986).

References

Bayer, D. A. (1982). The division algorithm and the Hilbert scheme. Ph.D. Thesis, Harvard University, Cambridge, MA.

Buchberger, B. (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Ph.D. Thesis, Universität Innsbruck.

Buchberger, B. (1976). Some properties of Gröbner-bases for polynomial ideals. *ACM SIGSAM Bull.*, **10**, 19–24.

Buchberger, B. (1985). Gröbner bases: an algorithmic method in polynomial ideal theory. In Bose, N. K., ed., *Multidimensional Systems Theory*, pp. 184–232. Dordrecht-Boston-London, Reidel Publishing Company.

Di Biase, F., Urbanke, R. (1995). An algorithm to calculate the kernel of certain polynomial ring homomorphisms. *Exp. Math.*, **4**, 227–234.

Dubé, T. W. (1990). The structure of polynomial ideals and Gröbner bases. *SIAM J. Comput.*, **19**, 750–773.

Eisenbud, D., Sturmfels, B. (1996). Binomial ideals. *Duke Math. J.*, **84**, 84–145.

Fortune, S., Wyllie, J. (1978). Parallelism in random access machines. In *Proc. 10th Ann. ACM Symp. on the Theory of Computing, STOC '78, San Diego, CA, May 1–3, 1978*, pp. 114–118. New York, ACM Press.

Hardy, G. H., Wright, E. M. (1985). *An Introduction to the Theory of Numbers,* 5th edn. Clarendon Press.

Hermann, G. (1926). Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Math. Ann.*, **95**, 736–788.

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

Hoşten, S., Sturmfels, B. (1995). GRIN: an implementation of Gröbner bases for integer programming. In Balas, E. and Clausen, J., eds, *Proc. Fourth Int. Integer Programming and Combinatorial Optimization Conference, IPCO '95, Copenhagen, Denmark, May 29–31, 1995*, LNCS **920**, pp. 267–276. Berlin–Heidelberg–New York–London–Paris–Tokyo–Hong Kong–Barcelona–Budapest, Springer-Verlag.

Hoşten, S., Thomas, R. R. (1998). Binomial ideals standard pairs and group relaxations in integer programming. Preprint (availiable from `http://www.math.tamu.edu/rekha.thomas`).

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

Karp, R. M., Ramachandran, V. (1990). Parallel algorithms for shared-memory machines. In van Leeuwen, J., ed., *Handbook of Theoretical Computer Science*, volume A: algorithms and complexity, pp. 869–941. Elsevier North–Holland, Amsterdam–New York–Oxford, The MIT Press: Cambridge, MA - London.

Koppenhagen, U., Mayr, E. W. (1996). Optimal Gröbner base algorithms for binomial ideals. In Meyer, F., auf der Heide, and Monien, B., eds, *Proc. 23rd Int. Colloquium on Automata, Languages and Programming, ICALP '96, Paderborn, Germany, July 8–12, 1996*, LNCS **1099**, pp. 244–255. New York–Berlin–Heidelberg–London–Paris–Tokyo–Hong Kong–Barcelona–Budapest, EATCS, Springer-Verlag.

Koppenhagen, U., Mayr, E. W. (1997). The complexity of the coverability, the containment, and the equivalence problems for commutative semigroups. In Chlebus, B. S. and Czaja, L., eds, *Proc. 11th Int. Conf. on the Fundamentals of Computation Theory, FCT '97, Kraków, Poland, September 1–3, 1997*, LNCS **1279**, pp. 257–268. Berlin–Heidelberg–New York–London–Paris–Tokyo–Hong Kong, Springer-Verlag.

Kühnle, K., Mayr, E. W. (1996). Exponential space computation of Gröbner bases. In Lakshman, Y. N., ed., *Proc. 1996 Int. Symp. on Symbolic and Algebraic Computation, ISSAC '96, Zürich, Switzerland, July 24–26, 1996*, pp. 63–71. New York, ACM Press.

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

Möller, H. M., Mora, F. (1984). Upper and lower bounds for the degree of Gröbner bases. In Fitch, J., ed., *Proc. 1984 Int. Symp. on Symbolic and Algebraic Computation EUROSAM '84, Cambridge, England, July 9–11, 1984*, LNCS **174**, pp. 172–183. Berlin–Heidelberg–New York–London–Paris–Tokyo–Hong Kong, M SIGSAM, SAME, Springer-Verlag.

Robbiano, L. (1985). Term orderings on the polynomial ring. In Caviness, B. F., ed., *Proc. 1985 European Conf. on Computer Algebra, EUROCAL '85, volume 2: Research contributions, Linz, Austria, April 1–3,1985*, LNCS **204**, pp. 513–517. Berlin–Heidelberg–New York–London–Paris–Tokyo–Hong Kong, ACM SIGSAM, SAME, Springer-Verlag.

Savitch, W. J. (1969). Deterministic simulation of non-deterministic Turing machines. In *Proc. First Ann. ACM Symp. on the Theory of Computing, STOC '69, Marina del Rey, CA, May 1969*, pp. 247–248. New York, ACM Press.

Thomas, R. R. (1998). Gröbner Bases in integer programming. In Du, D.-Z. and Pardalos, P. M., eds, *Handbook of Combinatorial Optimazation*. Kluwer Academic Publishers.

Weispfenning, V. (1987). Admissible orders and linear forms. *ACM SIGSAM Bull.*, **21**, 16–18.

Originally Received 28 September 1997
Accepted 03 June 1999