T U M

I N S T I T U T   F Ü R   I N F O R M A T I K

Optimal Gröbner Base Algorithms for Binomial Ideals

Ulla Koppenhagen
Ernst W. Mayr

TUM-I9604
Januar 1996

T E C H N I S C H E   U N I V E R S I T Ä T   M Ü N C H E N

TUM-INFO-01-1996-I9604-350/1.-FI

Typescript: ---

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

Optimal Gröbner Base Algorithms for 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/

November 14, 1995

Abstract

Little is known about upper complexity bounds for the normal form algorithms which transform a given polynomial ideal basis into a Gröbner basis. In this paper, we exhibit an optimal, exponential space algorithm for generating the reduced Gröbner basis of binomial ideals. This result is then applied to derive space optimal decision procedures for the finite enumeration and subword problems for commutative semigroups.

1 Introduction

Problems connected with polynomial ideals generated by finite sets of multivariate polynomials occur, as mathematical subproblems, in a number of different areas of computer science, like language generating and term rewriting systems, tiling problems, algebraic manifolds, motion planing, and several models for parallel systems.

However, most ideal theoretic problems in multivariate polynomial rings are very hard to solve. B. Buchberger, in 1965, was the first to show that for polynomials over a field it is possible to construct, from an arbitrary given basis, a "detaching" basis, the so-called Gröbner basis, such that many of the problems mentioned above become easily expressible and algorithmicly solvable (see [Buc65], also [Hi64]).

Although versions of Buchberger's algorithm have been somewhat successful in practice, the complexity of the algorithm is not well understood. First steps towards an upper bound were obtained in [Bay82] and [MoMo84] where upper bounds for the degrees in a minimal Gröbner basis were derived.

However, these results did not, or only under very restrictive assumptions, imply bounds for the degree of the polynomials arising during the intermediate computations of the Gröbner basis algorithms.

Using a novel partitioning method for polynomial ideals, Dubé obtained in [Dub90] 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.

Applying a result of Mayr and Meyer in [MM82] showing that commutative Thue systems can count up to double-exponentially large integers, Huynh derived in [Huy86] 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.

In this paper, we make use of the close relationship between commutative semigroups and binomial ideals. 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 binomial ideal. By the results in [MM82] and [Huy86], this algorithm is space optimal.

This paper is organized as follows. In Section 2 we briefly introduce the basic notations and formalisms. In Section 3 we exhibit the close relationship between commutative semigroups and binomial ideals and give a characterization of the reduced Gröbner basis for binomial ideals. In the following section we describe the exponential space Gröbner basis algorithm and, in Section 5, show two applications of this algorithm: we derive a procedure enumerating the elements of finite congruence classes in commutative semigroups and an algorithm for the general subword problem in commutative semigroups. Both algorithms use exponential space and are thus optimal.

2 Basic Concepts and Notations

In this section we review some definitions and notations used in the sequel.

2.1 Semigroups, Thue Systems, and Semigroup Presentations

A *semigroup* $(H, \circ)$ is a set H with a binary operation $\circ$ which is associative. If additionally $\circ$ is commutative we have a *commutative semigroup*, and a semigroup with a unit element is called a *monoid*. For simplicity, we write ab instead of $a \circ b$.

A commutative monoid M is said to be *finitely generated* by a finite subset $X = \{x_1, \ldots, x_k\} \subseteq M$ if[1]

$$M = \{u | u = \underbrace{x_1 \ldots x_1}_{e_1} \underbrace{x_2 \ldots x_2}_{e_2} \ldots \underbrace{x_k \ldots x_k}_{e_k}, e_i \in \mathbb{N}, x_i \in X\}.$$

Each element of M can then be represented as a k-dimensional vector in $\mathbb{N}^k$, *i.e.*,

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

there is a surjection $\varphi : \mathbb{N}^k \to M$ such that

$$u = \underbrace{x_1 \dots x_1}_{e_1} \underbrace{x_2 \dots x_2}_{e_2} \dots \underbrace{x_k \dots x_k}_{e_k} \quad \Longleftrightarrow \quad \varphi(e_1, \dots, e_k) = u.$$

If φ is also injective, and hence bijective, then every element of M has a unique representation in $\mathbb{N}^k$, and M is said to be *free*.

For a finite alphabet $X = \{x_1, \dots, x_k\}$, X^* denotes the free commutative monoid generated by X.

Let $\Phi =_{\text{def}} \varphi^{-1} : X^* \to \mathbb{N}^k$ be the inverse of φ, the so-called Parikh mapping, *i.e.,* $(\Phi(u))_i$ (also written $\Phi(u, x_i)$) indicates, for every $u \in X^*$ and $i \in \{1, \dots, k\}$, the number of occurrences of $x_i \in X$ in u.

For an element u of X^*, called a (commutative) word, the order of the symbols is immaterial, and we shall in the sequel use an exponent notation: $u = x_1^{e_1} \dots x_k^{e_k}$, where $e_i = \Phi(u, x_i) \in \mathbb{N}$ for $i = 1, \dots, k$.

A *commutative semi-Thue system* over X is given by a finite set $\mathcal{P}$ of productions $l_i \to r_i$, where l_i, $r_i \in X^*$. A word $v \in X^*$ *is derived in one step* from $u \in X^*$ (written $u \to v(\mathcal{P})$) by application of the production $(l_i \to r_i) \in \mathcal{P}$ iff, for some $w \in X^*$, we have $u = wl_i$ and $v = wr_i$. The word u *derives* v iff $u \xrightarrow{*} v(\mathcal{P})$, where $\xrightarrow{*}$ is the reflexive transitive closure of $\to$. More precisely we write $u \xrightarrow{+} v(\mathcal{P})$, where $\xrightarrow{+}$ is the transitive closure of $\to$, if $u \xrightarrow{*} v(\mathcal{P})$ with $u \neq v$. A sequence $(u_0, \dots, u_n)$ of words $u_i \in X^*$ with $u_i \to u_{i+1}(\mathcal{P})$ for $i = 0, \dots, n-1$ is called a *derivation* (of length n) of u_n from u_0 in $\mathcal{P}$.

A *commutative Thue system* is a symmetric commutative semi-Thue system $\mathcal{P}$, *i.e.,*

$$(l \to r) \in \mathcal{P} \Rightarrow (r \to l) \in \mathcal{P}.$$

Derivability in a semigroup establishes a congruence $\equiv_{\mathcal{P}}$ on X^* by the rule

$$u \equiv v \bmod \mathcal{P} \Leftrightarrow_{\text{def}} \ u \xrightarrow{*} v(\mathcal{P}).$$

For semigroups, we also use the notation $l \equiv r \bmod \mathcal{P}$ to denote the pair of productions $(l \to r)$ and $(r \to l)$ in $\mathcal{P}$.

If it is understood that $\mathcal{P}$ is a commutative Thue system the commutativity productions are not explicitly mentioned in $\mathcal{P}$ nor is their application within a derivation in $\mathcal{P}$ counted as a step.

A commutative Thue system $\mathcal{P}$ is also called a *presentation of the quotient semigroup* $X^*/\equiv_{\mathcal{P}}$.

We note that commutative semi-Thue systems appear in other, equivalent formulations in the literature, like *vector addition systems* and *Petri nets*. Finitely presented commutative semigroups are equivalent to *reversible* vector addition systems or Petri nets. A reader more familiar with reversible Petri nets may want to think of a vector in $\mathbb{N}^k$ as a marking.

2.2 Polynomials and Ideals

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. An *ideal* in $\mathbb{Q}[X]$ is any subset I of $\mathbb{Q}[X]$ satisfying the following conditions:

(I1) $\quad p, q \in I \quad \Rightarrow \quad p + q \in I;$

(I2) $\quad r \in \mathbb{Q}[X],\, p \in I \quad \Rightarrow \quad r \cdot p \in I.$

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.

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 $e = (e_1, e_2, \ldots, e_k) \in \mathbb{N}^k$ 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.

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 $a_1 \cdot x_1^{d_1} \cdots x_k^{d_k} \succ a_2 \cdot x_1^{e_1} \cdots x_k^{e_k}$

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

iff, for the corresponding degree vectors d and e, Td is *lexicographically greater* than Te [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) $\{g_1, \ldots, g_r\}$ is a basis of I;

(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

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

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

3 The Connection between Commutative Semigroups and Binomial Ideals

3.1 The Basic Problems and Their Connection

In this section, we consider the *uniform word problem* for commutative semigroups and the *polynomial ideal membership problem*. We will show the connection between these two very basic and fundamental algorithmic problems for commutative semigroups and polynomial ideals.

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 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

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

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

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

We call such an ideal a *binomial ideal*, *i.e.,* each polynomial in the basis is the difference of two terms. By looking at Buchberger's algorithm [Buc65] it is not hard to see that the reduced Gröbner bases of binomial ideals still consist only of binomials.

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 $f, f_1, \ldots, f_h \in Q[X]$ 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 easily 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* $c > 0$, *such that* M *decides for any two words* u, $v \in X^*$ *whether* $u \equiv v \bmod \mathcal{P}$ *using at most space* $(\text{size}(u, v, \mathcal{P}))^2 \cdot 2^{c \cdot k}$, *where* $c > 0$ *is some constant independent of* $\mathcal{P}$.

3.2 A Characterization of the Reduced Gröbner Basis for Binomial Ideals

Let $\mathcal{P}$ be a commutative semigroup presentation over an alphabet X. The following two theorems characterize the binomials of the reduced Gröbner basis of $I(\mathcal{P})$.

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* $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ *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 $m_i - w \in I(\mathcal{P})$, 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 $I(\mathcal{P})$. □

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 $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ 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 and which 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 $s \notin H$. □

4 An Optimal Algorithm for the Reduced Gröbner Basis

In this section we give an exponential space algorithm for generating the reduced Gröbner basis of a binomial ideal. To show the complexity of the algorithm we need the results of Section 3 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 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 $I(\mathcal{P})$.

We have to determine the elements of the set H, 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 $l_i - r_i$, $i \in I_h$.

First we establish some technical details. For detailed proofs see [KM96].

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. $\prec$.*

Proof: Follows immediately from Theorem 2. □

In 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 [KM96] *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 $t \cdot r_i \prec u$, $r_i \in \{r_1, \ldots, r_h\}$, $t \in X^*$, and $\deg(t \cdot r_i) \leq D + 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ such that $u \xrightarrow{+} t \cdot r_i(\mathcal{P})$.*

Given some term $h \in X^*$ 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 $t \cdot r_i \prec h$, $r_i \in \{r_1, \ldots, r_h\}$, $t \in X^*$, $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ such that $h \xrightarrow{+} t \cdot r_i(\mathcal{P})$. For h and $t \cdot r_i$ with $\deg(h)$ and $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$, 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 $\mathcal{P}$. So we decide for the words $t \cdot r_i$ with $t \cdot r_i \prec h$, $r_i \in \{r_1, \ldots, r_h\}$, $t \in X^*$, $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ 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 $t \cdot r_i \prec h$, $r_i \in \{r_1, \ldots, r_h\}$, $t \in X^*$, $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$. In the latter case it is $h \notin H$, and we have to consider the next $h \in X^*$ 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 3 *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 2, 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 $h_{new} \in X^*$ with degree $\leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$, and h does not divide h_{new} because any multiple $t \cdot h$ of h, $t \in X^*$, is not in H if $h \in LT(I(\mathcal{P}))$.

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

The Algorithm

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 $I(\mathcal{P})$

$G := \emptyset$
for each $h \in X^*$ with degree $\leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ **do** **co** $h = x_1^{e_1} \cdots x_k^{e_k}$ **co**
  $D := \deg(h)$
  $m := 1$
  repeat
    $m :=$ the term $t \cdot r_i$ with $t \cdot r_i \prec h$, $r_i \in \{r_1, \ldots, r_h\}$, $t \in X^*$, $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$
      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 $t \cdot r_i \prec h$, $r_i \in \{r_1, \ldots, r_h\}$, $t \in X^*$,
      $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$)
  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**
      $h' := x_1^{e_1} \cdots x_i^{e_i - 1} \cdots x_k^{e_k}$
      $m' := 1$
      repeat
        $m' :=$ the term $t \cdot r_i$ with $t \cdot r_i \prec h'$, $r_i \in \{r_1, \ldots, r_h\}$, $t \in X^*$, $\deg(t \cdot r_i) \leq$
          $(D-1) + 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ 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 $t \cdot r_i \prec h'$, $r_i \in \{r_1, \ldots, r_h\}1$,
          $t \in X^*$, $\deg(t \cdot r_i) \leq (D-1) + 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$)
      if $m' \equiv h' \bmod \mathcal{P}$ **then** **co** $h' \in LT(I(\mathcal{P})) \Rightarrow h \notin H$ **co**
        next h with h_{old} does not divide h_{new}
      end_if
    end_for
    $G := G \cup \{h - m\}$
    next h with h_{old} does not divide h_{new}
  end_if
end_for

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

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 binomial ideal $I(\mathcal{P})$ using at most space $(\mathrm{size}(\mathcal{P}))^2 \cdot 2^{\bar{c} \cdot k} \leq 2^{c \cdot \mathrm{size}(\mathcal{P})}$, where $\bar{c}, c > 0$ are some constants independent of $\mathcal{P}$.

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

5 Applications

We now consider two applications of the exponential space algorithm obtained in Section 4. We present space optimal decision procedures for the finite enumeration and subword problems for commutative semigroups.

5.1 The Finite Enumeration Problem for Commutative Semigroups is Exponential Space Complete

Let $\mathcal{P}$ be a commutative semigroup presentation over an alphabet X, and $u \in X^*$ a word such that the congruence class of u is bounded. Then the finite enumeration problem for commutative semigroups, or equivalently, reversible Petri nets is the problem of generating a complete list of all the elements of $[u]_{\mathcal{P}}$. We give a procedure for the solution of this problem which needs at most exponential work space. From the results in [MM82] we know that the problem of deciding whether some word $v \in X^*$ is in $[u]_{\mathcal{P}}$ is exponential space complete (the input consisting of u, v and $\mathcal{P}$).

Theorem 4 *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$ be a finite commutative semigroup presentation over X, and $u \in X^*$ a word such that the congruence class of u is bounded. Then there is an algorithm which generates the elements of $[u]_{\mathcal{P}}$ 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 $2k + 2$ new variables s, t, $y_1, \ldots, y_k$, and $z_1, \ldots, z_k$. Let $X' = X \cup \{s, t, y_1, \ldots, y_k, z_1, \ldots, z_k\}$. Given $\mathcal{P}$ and the word $u \in X^*$, we construct a new commutative semigroup presentation $\mathcal{P}'$ over X' as follows: $\mathcal{P}'$ contains the congruences

$$\begin{aligned} s \cdot x_j &\equiv s \cdot y_j \cdot z_j, \quad \text{for} \quad j = 1, \ldots, k, && (1) \\ s \cdot y(u) &\equiv t, && (2) \end{aligned}$$

and for every congruence $l_i \equiv r_i$ in $\mathcal{P}$, $\mathcal{P}'$ contains the congruences

$$\begin{aligned} s \cdot y(l_i) &\equiv s \cdot y(r_i), \quad \text{and} && (3) \\ t \cdot z(l_i) &\equiv t \cdot z(r_i), && (4) \end{aligned}$$

where y resp., z are the homomorphisms replacing x_j by y_j resp., z_j for $j \in I_k$.

In the following we prove that $v \in [u]_{\mathcal{P}}$, iff the term $s \cdot v$ occurs in a binomial of G, where G is the reduced Gröbner basis of the ideal $I(\mathcal{P}')$ w.r.t. a lexicographic term order $\prec$, which satisfies

$$a \prec b \quad \text{for all} \quad a \in \{x_1, \ldots, x_k\},\ b \in \{s, t, y_1, \ldots, y_k, z_1, \ldots, z_k\}.$$

Then, by Theorem 3, the elements of $[u]_{\mathcal{P}}$ can be generated using at most space $(\text{size}(u, \mathcal{P}'))^2 \cdot 2^{d' \cdot k} \leq (\text{size}(u, \mathcal{P}))^2 \cdot 2^{d \cdot k}$, where d', $d > 0$ are some constants independent of u and $\mathcal{P}'$ resp., $\mathcal{P}$.

First we establish some technical details.

Lemma 4 *Every word $w \in [s \cdot u]_{\mathcal{P}'}$ satisfies the following conditions:*

(i) $\Phi(w, s),\ \Phi(w, t) \in \{0, 1\}$;

(ii) $\Phi(w, s) + \Phi(w, t) = 1$;

(iii) *if* $\Phi(w, s) = 1$, *then*
$$x_1^{\Phi(w,x_1)+\Phi(w,y_1)} \cdot x_2^{\Phi(w,x_2)+\Phi(w,y_2)} \cdots x_k^{\Phi(w,x_k)+\Phi(w,y_k)} \in [u]_{\mathcal{P}},$$
$$x_1^{\Phi(w,x_1)+\Phi(w,z_1)} \cdot x_2^{\Phi(w,x_2)+\Phi(w,z_2)} \cdots x_k^{\Phi(w,x_k)+\Phi(w,z_k)} \in [u]_{\mathcal{P}};$$

if $\Phi(w, t) = 1$, *then*
$$\Phi(w, x_1) = \Phi(w, x_2) = \ldots = \Phi(w, x_k) = 0,$$
$$\Phi(w, y_1) = \Phi(w, y_2) = \ldots = \Phi(w, y_k) = 0,$$
$$x_1^{\Phi(w,z_1)} \cdot x_2^{\Phi(w,z_2)} \cdots x_k^{\Phi(w,z_k)} \in [u]_{\mathcal{P}}.$$

Proof: Let w be any word in $[s \cdot u]_{\mathcal{P}'}$, then there is a repetition-free derivation in $\mathcal{P}'$ leading from $s \cdot u$ to w. In any repetition-free derivation starting at $s \cdot u$ only the congruences in (1) and (3) can be applied until the word $s \cdot y(u) \cdot z(u)$ is reached and changed to $t \cdot z(u)$ by congruence (2). Since $[u]_{\mathcal{P}}$ is bounded, there is no $u' \in \{y_1, \ldots, y_k\}^*$ with $s \cdot u' \cdot z(u) \in [s \cdot u]_{\mathcal{P}'}$, $u' \neq y(u)$, and $y(u)$ divides u'. Therefore, any word w occuring in this derivation of $s \cdot y(u) \cdot z(u)$ from $s \cdot u$ satisfies the conditions (i) - (iii):

(i) & (ii): $\Phi(w, s) = 1,\ \Phi(w, t) = 0,$

(iii): $x_1^{\Phi(w,x_1)+\Phi(w,y_1)} \cdot x_2^{\Phi(w,x_2)+\Phi(w,y_2)} \cdots x_k^{\Phi(w,x_k)+\Phi(w,y_k)} \in [u]_{\mathcal{P}}$, and
$x_1^{\Phi(w,x_1)+\Phi(w,z_1)} \cdot x_2^{\Phi(w,x_2)+\Phi(w,z_2)} \cdots x_k^{\Phi(w,x_k)+\Phi(w,z_k)} = u.$

Then, as long as congruence (2) is not applied, by the congruences in (4) words $t \cdot z(v)$ with $v \in [u]_{\mathcal{P}}$ can be derived from $t \cdot z(u)$. Note, that for all such words $t \cdot z(v)$ with $v \in [u]_{\mathcal{P}}$ $\Phi(t \cdot z(v), s) = 0$, $\Phi(t \cdot z(v), t) = 1$, and condition (iii) is satisfied. Congruence (2) changes $t \cdot z(v)$ to $s \cdot y(u) \cdot z(v)$ and again the congruences in (1) and (3) can be applied. As above the words w in the resulting sub-derivation starting at $s \cdot y(u) \cdot z(v)$ satisfy (i), (ii), and (iii) with

$$x_1^{\Phi(w,x_1)+\Phi(w,z_1)} \cdot x_2^{\Phi(w,x_2)+\Phi(w,z_2)} \cdots x_k^{\Phi(w,x_k)+\Phi(w,z_k)} = v.$$

By the congruences in (3) from $s \cdot y(u) \cdot z(v)$ any word $s \cdot y(v') \cdot z(v)$ with $v' \in [u]_{\mathcal{P}}$ can be derived. Congruence (2) can only be applied to the word $s \cdot y(u) \cdot z(v)$ causing a repetition. Thus, the conditions (i) - (iii) are satisfied within the whole derivation. $\Box_{\text{Lemma 4}}$

For the derivation of some word $s \cdot v \in [s \cdot u]_{\mathcal{P}'}$ with $v \in X^*$ from $s \cdot u$ in $\mathcal{P}'$ we conclude from Lemma 4 and its proof:

Lemma 5 *Let $s \cdot v \in [s \cdot u]_{\mathcal{P}'}$ with $v \in X^*$, $v \neq u$, and let $s \cdot u = \gamma_0 \to \gamma_1 \to \ldots \to \gamma_n = s \cdot v$ be any repetition-free derivation in $\mathcal{P}'$ leading from $s \cdot u$ to $s \cdot v$. Then, there is exactly one $i \in I_{n-1}$ with $\gamma_i = s \cdot y(u) \cdot z(u)$, $\gamma_{i+1} = t \cdot z(u)$, and exactly one $j \in I_{n-1}$, $j > i$, with $\gamma_j = t \cdot z(v)$, $\gamma_{j+1} = s \cdot y(u) \cdot z(v)$.*

Now we can prove the following:

Lemma 6 *Let v be some word in X^*, then* $\quad v \in [u]_{\mathcal{P}} \quad \Longleftrightarrow \quad s \cdot v \in [s \cdot u]_{\mathcal{P}'}$

Proof: By Lemma 4 and Lemma 5 a repetition-free derivation in $\mathcal{P}'$ leading from $s \cdot u$ to $s \cdot v$ with $v \in X^*$ has the following form:

$$s \cdot u \xrightarrow[(1),\,(3)]{+} s \cdot y(u) \cdot z(u) \xrightarrow[(2)]{} t \cdot z(u) \xrightarrow[(4)]{+} t \cdot z(v) \xrightarrow[(2)]{} s \cdot y(u) \cdot z(v) \xrightarrow[(1),\,(3)]{+} s \cdot v,$$

where $\xrightarrow[(.)]{+}$ denotes some repetition-free derivation only applying the congruences given in (.) . Within the sub-derivations $\xrightarrow[(1),\,(3)]{+}$ the values $\Phi(w, x_i) + \Phi(w, z_i)$ are constant for all $i \in I_k$, *i.e.*, the word $x_1^{\Phi(w,x_1)+\Phi(w,z_1)} \cdot x_2^{\Phi(w,x_2)+\Phi(w,z_2)} \cdots x_k^{\Phi(w,x_k)+\Phi(w,z_k)}$ remains the same within $\xrightarrow[(1),\,(3)]{+}$. Furthermore, all the words occuring in the above derivation satisfy Lemma 4. $\Box_{\text{Lemma 6}}$

Lemma 7 *$[s \cdot u]_{\mathcal{P}'}$ is bounded.*

Proof: Since $[u]_{\mathcal{P}}$ is bounded, it follows from the definition of $\mathcal{P}'$ and Lemma 4 that $[s \cdot u]_{\mathcal{P}'}$ is also bounded. $\Box_{\text{Lemma 7}}$

Lemma 8 *Let v be some word in X^*, with $v \notin [u]_{\mathcal{P}}$, and v divides some $u' \in [u]_{\mathcal{P}}$. Then $s \cdot v$ is the minimal element of $[s \cdot v]_{\mathcal{P}'}$ w.r.t. $\prec$.*

Proof: If $v \in X^*$ with $v \notin [u]_{\mathcal{P}}$, and v divides some $u' \in [u]_{\mathcal{P}}$, then there is some $v' \in X^* - \{\varepsilon\}$ with $u' = v \cdot v' \in [u]_{\mathcal{P}}$. The boundedness of $[u]_{\mathcal{P}}$ implies that there is no $\bar{v} \in [v]_{\mathcal{P}}$ with $\bar{v} = u \cdot \bar{u}$ for some $\bar{u} \in X^*$, because if there would be such a $\bar{v} \in [v]_{\mathcal{P}}$, then $u' = v \cdot v' \equiv \bar{v} \cdot v' \bmod \mathcal{P}$, $\bar{v} \cdot v' = u \cdot \bar{u} \cdot v' \in [u]_{\mathcal{P}}$, *i.e.*, $[u]_{\mathcal{P}}$ is not bounded. Thus, in any derivation starting at $s \cdot v$ congruence (2) can not be applied. Only the congruences in (1) and (3) can be applied. Since $y_i \succ x_i$ resp., $z_i \succ x_i$ for all $i \in I_k$, $s \cdot v$ is the minimal element of $[s \cdot v]_{\mathcal{P}'}$ w.r.t. to the lexicographic term order $\prec$. $\Box_{\text{Lemma 8}}$

Since $[s \cdot u]_{\mathcal{P}'}$ is bounded, it follows from Dickson's Lemma that each $w \in [s \cdot u]_{\mathcal{P}'}$ is minimal in $[s \cdot u]_{\mathcal{P}'}$ w.r.t. divisibility, *i.e.*, if $w \in [s \cdot u]_{\mathcal{P}'}$ there is no $w' \in [s \cdot u]_{\mathcal{P}'}$, $w' \neq w$ with w' divides w. Thus, by Lemma 8, if $w \in [s \cdot u]_{\mathcal{P}'}$, and w is not the minimal element $m_{s\cdot u}$ of $[s\cdot u]_{\mathcal{P}'}$ w.r.t. $\prec$, then $w \in H$, where H denotes the set of the minimal elements of $LT(I(\mathcal{P}'))$ w.r.t. divisibility, and hence $G \supset \{w - m_{s\cdot u} \mid w \in [s \cdot u]_{\mathcal{P}'},\ w \neq m_{s\cdot u}\}$ (see Theorem 1 and Theorem 2). By introducing in $\mathcal{P}'$ a new variable m with $m \equiv s \cdot u \bmod \mathcal{P}'$, and $m \prec a \prec b$ for all $a \in \{x_1, \ldots, x_k\}$, $b \in \{s, t, y_1, \ldots, y_k, z_1, \ldots, z_k\}$, we get $m_{s\cdot u} = m$ and thus $G \supset \{w - m \mid w \in [s \cdot u]_{\mathcal{P}'},\ w \neq m\}$. Therefore, Lemma 6 yields that $v \in [u]_{\mathcal{P}}$, iff the term $s \cdot v$ occurs in a binomial of the reduced Gröbner basis of $I(\mathcal{P}')$ concluding the proof of Theorem 4. $\square$

Theorem 5 *The finite enumeration problem for commutative semigroups is exponential space complete with respect to log-lin reducibility.*

From the work in [MM82] we know that the uniform word problem for commutative semigroups is exponential space complete. Actually, the construction in [MM82] proves the following, slightly stronger statement, which we will use for the proof of Theorem 5:

Proposition 5 [MM82] *Let $\mathcal{P}$ be a finite commutative semigroup presentation over X, v a word in X^*, and $u \in X^*$ a word such that $[u]_{\mathcal{P}}$ is bounded. Even with this restriction, the uniform word problem,* i.e., *the problem of deciding whether $u \equiv v \bmod \mathcal{P}$, is exponential space complete with respect to log-lin reducibility.*

Proof of Theorem 5: Let $\mathcal{P}$ be the commutative semigroup presentation, and u, $v \in X^*$ the two words of Proposition 5. Then, $v \equiv u \bmod \mathcal{P}$, *i.e.,* $v \in [u]_{\mathcal{P}}$, iff v is contained in the list of elements of $[u]_{\mathcal{P}}$ generated by the enumeration algorithm of Theorem 4. Thus, an exponential space complete word problem reduces to the enumeration problem for commutative semigroups, which together with Theorem 4 establishes the exponential space completeness of the enumeration problem for commutative semigroups. $\square$

5.2 The Subword Problem for Commutative Semigroups

Let $X = \{x_1, \ldots, x_k\}$ be a finite alphabet, and $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$ a finite commutative semigroup presentation. The subword problem for commutative semigroups is to decide for any two words u, $v_1 \in X^*$ whether there is a $v_2 \in [u]_{\mathcal{P}}$ such that $v_2 = v_1 \cdot w$ for some $w \in X^*$ which contains no variable occuring in v_1. *I.e.,* if such a word v_2 exists, then w.l.o.g. the variables can be renamed such that

$$v_2 = \underbrace{x_1^{e_1} \cdots x_l^{e_l}}_{v_1} \cdot \underbrace{x_{l+1}^{e_{l+1}} \cdots x_k^{e_k}}_{w},$$

for some $e_1, \ldots, e_l \in \mathbb{N} - \{0\}$ and $e_{l+1}, \ldots, e_k \in \mathbb{N}$.

We denote by $X_{v_1} = \{x_1, \ldots, x_l\}$ $(l \leq k)$ the set of variables occuring in v_1, and if $l < k$ by $X_{\overline{v_1}} = \{x_{l+1}, \ldots, x_k\}$ the set of variables not occuring in v_1.

By Y we denote either the empty set, or a subset $\{x_{l_1}, \ldots, x_{l_2}\}$ of X with the following properties:

- If $X_{v_1} \cap Y$ is not the empty set, then $X_{v_1} \cap Y = \{x_{l_1}, \ldots, x_l\}$, *i.e.*, $l_1 \leq l \leq l_2$.
- If $X_{v_1} \cap Y$ is the empty set, then $l < l_1 \leq l_2$.

By Z we denote either the empty set, or a subset $\{x_{l_3}, \ldots, x_k\}$ of X with $Z \cap Y = \emptyset$, *i.e.*, $l_2 < l_3$ if Y is not the empty set.

Then, for the case $l_1 < l < l_2 < l_3$ we get the following picture:

$$\overbrace{x_1, \ldots, x_{l_1-1}, \underbrace{x_{l_1}, \ldots, x_l, \quad}_{}}^{X_{v_1}} \overbrace{\underbrace{x_{l+1}, \ldots, x_{l_2}}_{Y}, x_{l_2+1}, \ldots, x_{l_3-1}, \underbrace{x_{l_3}, \ldots, x_k}_{Z}}^{X_{\overline{v_1}}}$$

With this notation we define the subword problem for commutative semigroups as follows. Note that this definition extends the definition given at the beginning of this section.

The Subword Problem: Given X, $\mathcal{P}$, u, v_1, Y, and Z, decide whether there is a $v_2 \in [u]_{\mathcal{P}}$ such that $v_2 = v_1 \cdot x_{l_1} \cdots x_{l_2} \cdot w$ for some $w \in (Y \cup Z)^*$ if Y is not the empty set resp., $v_2 = v_1 \cdot w$ for some $w \in Z^*$ if Y is the empty set.

Theorem 6 *Let $X = \{x_1, \ldots, x_k\}$, and $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$ be a commutative semigroup presentation over X. Then there is an algorithm which decides for any two words u, $v_1 \in X^*$, and sets Y, Z defined as above whether there is a $v_2 \in [u]_{\mathcal{P}}$ such that $v_2 = v_1 \cdot v \cdot w$, where $v = x_{l_1} \cdots x_{l_2}$ if $Y = \{x_{l_1}, \ldots, x_{l_2}\}$ resp., $v = \varepsilon$ if $Y = \emptyset$, using at most space $(\mathrm{size}(u, v_1, \mathcal{P}))^2 \cdot 2^{\bar{c} \cdot k} \leq 2^{c \cdot \mathrm{size}(u, v_1, \mathcal{P})}$ for some constants $\bar{c}$, $c > 0$ independent of u, v_1 and $\mathcal{P}$.*

Proof: We show that if there is a $v_2' \in [u]_{\mathcal{P}}$ as described in the Theorem, then there is a $v_2 \in [u]_{\mathcal{P}}$ with the same properties as v_2' and v_2 can be determined in space $(\mathrm{size}(u, v_1, \mathcal{P}))^2 \cdot 2^{\bar{c} \cdot k}$.

In addition to $x_1, \ldots, x_k$ we introduce three new variables s, $\bar{s}$, and t. Let $X_t = X \cup \{s, \bar{s}, t\}$. Given $\mathcal{P}$ and the two words u, $v_1 \in X^*$, we construct a new commutative semigroup presentation $\mathcal{P}_t$ over X_t as follows: For every congruence $l_i \equiv r_i$ in $\mathcal{P}$, $\mathcal{P}_t$ contains the congruence

$$t \cdot l_i \equiv t \cdot r_i.$$

Then we add to $\mathcal{P}_t$ the identities $\quad s \equiv t \cdot u,$

and $\quad t \cdot v_1 \cdot v \equiv \bar{s}.$

To be able to argue by the degree bounds in Gröbner bases we need an admissible term ordering $\prec$. We use a lexicographic order which is defined by the following order on the variables:

$$s \succ t \succ X_{v_1} - (Y \cup Z) \succ X_{\overline{v_1}} - (Y \cup Z) \succ \bar{s} \succ Y \succ Z\,,$$

where the variables in the sets are ordered arbitrarily.

By Theorem 2, $s \in LT(I(\mathcal{P}_t))$, and, since s is minimal in $LT(I(\mathcal{P}_t))$ w.r.t. divisibility, $s \in H_t$, where H_t is the set of the minimal elements of $LT(I(\mathcal{P}_t))$ w.r.t. divisibility. By Theorem 1 and Theorem 2, $s - m_s \in G$, where G is the reduced Gröbner basis of $I(\mathcal{P}_t)$, and m_s is the minimal element of $[s]_{\mathcal{P}_t}$ w.r.t. $\prec$.

Because we assume that there is a $v_2' \in [u]_{\mathcal{P}}$ such that $v_2' = v_1 \cdot v \cdot w'$ for some $w' \in (Y \cup Z)^*$, it follows that $t \cdot v_1 \cdot v \cdot w' \in [t \cdot u]_{\mathcal{P}_t}$. Since $t \cdot v_1 \cdot v \cdot w' \equiv \bar{s} \cdot w' \bmod \mathcal{P}_t$, it is $\bar{s} \cdot w' \in [t \cdot u]_{\mathcal{P}_t}$. For m_s is the minimal element of $[s]_{\mathcal{P}_t} = [t \cdot u]_{\mathcal{P}_t}$ it must be $m_s \prec \bar{s} \cdot w'$, or $m_s = \bar{s} \cdot w'$. In particular, the variables s, t, and the variables in $X_{v_1} - (Y \cup Z)$, $X_{\overline{v_1}} - (Y \cup Z)$ do not occur in m_s. In Lemma 9 we will see that $\Phi(m_s, \bar{s}) = 1$, *i.e.*, $m_s = \bar{s} \cdot w$ for some $w \in (Y \cup Z)^*$ with $w \prec w'$, or $w = w'$. Since $s - m_s \in G$, by Theorem 3, $m_s = \bar{s} \cdot w$ can be determined in space $(\text{size}(u, v_1, \mathcal{P}_t))^2 \cdot 2^{d \cdot k}$ for some constant $d > 0$ independent of u, v_1 and $\mathcal{P}_t$.

In the following it will be shown that in a repetition-free derivation in $\mathcal{P}_t$ leading from s to m_s the variables s and $\bar{s}$ only occur in the words s and m_s. Furthermore, we will see that any word except of s and m_s in a repetition-free derivation of m_s from s in $\mathcal{P}_t$ has the form $t \cdot x$ with $x \in X^*$. So there is a derivation of $v_1 \cdot v \cdot w$ from u in $\mathcal{P}$.

In $\mathcal{P}_t$ the variable s as well as the variable $\bar{s}$ occurs in exactly one congruence, namely $s \equiv t \cdot u$ resp., $t \cdot v_1 \cdot v \equiv \bar{s}$. In the remaining congruences in $\mathcal{P}_t$ each side has the form $t \cdot y$ with $y \in X^*$. Thus the only congruence in $\mathcal{P}_t$ that can be applied to s is $s \equiv t \cdot u$, and any derivation in $\mathcal{P}_t$ starting at s first leads from s to $t \cdot u$, *i.e.*, $s \rightarrow t \cdot u\,(\mathcal{P}_t)$. Generally from the structure of $\mathcal{P}_t$ it follows:

Lemma 9 *Every word γ in a derivation in $\mathcal{P}_t$ starting at s satisfies:*

(i) $\Phi(\gamma, s)$, $\Phi(\gamma, \bar{s})$, $\Phi(\gamma, t) \in \{0, 1\}$, *and*

(ii) $\Phi(\gamma, s) + \Phi(\gamma, \bar{s}) + \Phi(\gamma, t) = 1$, i.e., *exactly one of the variables s, $\bar{s}$, and t occurs exactly once in every word γ of any derivation in $\mathcal{P}_t$ starting at s.*

If some word γ_i, $i \in \mathbb{N}$, $i > 1$, in a derivation $s \rightarrow t \cdot u \rightarrow \gamma_1 \rightarrow \ldots \rightarrow \gamma_{i-1} \rightarrow \gamma_i$ $(\mathcal{P}_t)$ contains the variable s, then the only way to continue is to apply the congruence $s \equiv t \cdot u$. Since this is the only congruence of $\mathcal{P}_t$ in which s occurs, this congruence must be the congruence that derived γ_i from γ_{i-1}. Thus the resulting derivation is not repetition free.

Similarly, if some word γ in a derivation of m_s from s in $\mathcal{P}_t$ contains the variable $\bar{s}$, then either $\gamma = m_s$ and we are finished, or there is exactly one applicable congruence, namely the congruence applied last, which causes a repetition in the derivation.

Hence, the words γ_i in a repetition-free derivation

$$s \rightarrow t \cdot u = \gamma_0 \rightarrow \gamma_1 \rightarrow \ldots \rightarrow \gamma_{n-1} \rightarrow \gamma_n \rightarrow m_s\,(\mathcal{P}_t),$$

$n \in \mathbb{N}$, do not contain s or $\bar{s}$. So the only congruences applied to γ_i, $i \in \{0, \ldots, n-1\}$ are the congruences $t \cdot l_i \equiv t \cdot r_i$ and thus any repetition-free derivation of m_s from s in $\mathcal{P}_t$ has the form

$$s \rightarrow t \cdot u \rightarrow t \cdot \delta_1 \rightarrow \ldots \rightarrow t \cdot \delta_n = t \cdot v_1 \cdot v \cdot w \rightarrow \bar{s} \cdot w = m_s\,(\mathcal{P}_t)$$

with $n \in \mathbb{N}$, and $t \cdot \delta_i = \gamma_i$, $i \in I_n$.

We obtain the following derivation in $\mathcal{P}$ leading from u to $v_2 = v_1 \cdot v \cdot w$:

$$u \rightarrow \delta_1 \rightarrow \ldots \rightarrow \delta_n = v_1 \cdot v \cdot w = v_2\,(\mathcal{P}).$$

By Theorem 3 $m_s = \bar{s} \cdot w$ can be determined in space $(\text{size}(u, v_1, \mathcal{P}_t))^2 \cdot 2^{d \cdot k}$, and thus v_2 can be determined using at most space $(\text{size}(u, v_1, \mathcal{P}))^2 \cdot 2^{\bar{c} \cdot k}$. □

Theorem 7 *The subword problem for commutative semigroups is exponential space complete with respect to log-lin reducibility.*

Proof: From the work in [MM82] we know that the word problem for commutative semigroups is exponential space complete with respect to log-lin reducibility. If Y and Z are the empty set, then the subword problem is equivalent to the word problem. Thus the word problem is a special case of the subword problem, and because of Theorem 6 we conclude the assertion. □

6 Conclusion

For the special case of binomial ideals, we have presented an algorithm for transforming any given basis into the reduced Gröbner basis using at most space $2^{c \cdot n}$, where n is the size 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]).

As an application of our basis construction algorithm, we have also presented space optimal decision procedures for the finite enumeration and subword problems for commutative semigroups. These procedures also require at most space $2^{d \cdot n}$ for some constant d independent of the size n of the problem instance. This complexity bound for the finite enumeration problem also implies an analogous bound for the finite containment problem (FCP) (and the finite equality problem (FEP)) for commutative semigroups and, equivalently, for reversible Petri nets.

The finite containment problem (the finite equality problem) for general (not necessarily reversible) Petri nets is the problem of determining for any two given Petri nets with finite reachability sets whether the reachability set of the first is contained in (is equal to) that of the second. As shown in [KaMi69], FCP (FEP) for Petri nets is decidable, but the complexity of any decision procedure for FCP (FEP) for general Petri nets is non-primitive recursive [MM81], in stark contrast to the situation for reversible Petri nets investigated in this paper.

It is also interesting to note that in the case of general Petri nets, the subword problem (*i.e.,* the submarking reachability problem) easily reduces to the word problem since, in a semi-Thue system, we can arrange irreversible transitions from one phase to another. This technique can no longer be applied in the case of Thue systems like commutative semigroups or reversible Petri nets since all transitions can, by definition, be undone.

Our investigation of the complexity of Gröbner basis algorithms for binomial ideals has benefited a lot from the close relationship to commutative semigroups. It is an interesting open problem, whether this relationship can be extended, in one way or another, to the general case of polynomial ideals over fields or (Noetherian) rings. Another open problem is finding algorithms to construct a representation of the (infinite) state space for process systems other than those defined by symmetric commutative context-free process algebras (corresponding to reversible Petri nets) and determining the complexity of various fundamental problems for process algebras in this context, like bisimulation equivalence.

References

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

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

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

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

[Hi64] Heisuke 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.

[KaMi69] R. Karp and R. Miller. Parallel program schemata. *J. Comput. Syst. Sci.*, 3:147–195, 1969.

[KM95] Ulla Koppenhagen and Ernst W. Mayr. The complexity of the boundedness, coverability, and selfcoverability problems for commutative semigroups. Technical Report TUM-I9518, Institut für Informatik, Technische Universität München, May 1995.

[KM96] Ulla Koppenhagen and Ernst W. Mayr. An Optimal Algorithm for Constructing the Reduced Gröbner Basis of Binomial Ideals. Technical Report TUM-I9605, Institut für Informatik, Technische Universität München, January 1996.

[MM81] Ernst W. Mayr and Albert Meyer. The complexity of the finite containment problem for Petri nets. In *J. ACM*, 28(3):561–576, 1981.

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

[MoMo84] H. Michael Möller and Ferdinando 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.