Information and Computation **158**, 98–124 (2000)
doi:10.1006/inco.1999.2812, available online at http://www.idealibrary.com on IDEAL®

Optimal Algorithms for the Coverability, the Subword, the Containment, and the Equivalence Problems for Commutative Semigroups

Ulla Koppenhagen and Ernst W. Mayr[1]

Institut für Informatik, Technische Universität München, D-80290 Munich, Germany
E-mail: koppenha@informatik.tu-muenchen.de, mayr@informatik.tu-muenchen.de

In this paper, we present decision procedures for the coverability, the subword, the containment, and the equivalence problems for commutative semigroups. These procedures require at most space $2^{c \cdot n}$, where n is the size of the problem instance, and c is some problem independent constant. Furthermore, we show that the exponential space hardness of the above problems follows from the work of Mayr and Meyer. Thus, the presented algorithms are space optimal. Our results close the gap between the $2^{c' \cdot n \cdot \log n}$ space upper bound, shown by Rackoff for the coverability problem and shown by Huynh for the containment and the equivalence problems, and the exponential space lower bound resulting from the corresponding bound for the uniform word problem established by Mayr and Meyer.

1. INTRODUCTION

Commutative semi-Thue systems, or, equivalently, vector addition systems, or Petri nets, their equivalent graphical representation, are well-known models for parallel processes. Much effort has been devoted to the study of the mathematical properties of these models. In particular, decidability and complexity questions for these models have received wide attention. In this paper, we focus on the *coverability problem*, the *subword problem*, the *containment problem*, and the *equivalence problem*.

Let X be some finite alphabet and X^* the free commutative monoid generated by X. Given a commutative semi-Thue system $\mathscr{P}$ over X and two words $u, v_1 \in X^*$, the (ordinary) coverability problem is the problem of deciding whether it is possible to derive from v_1 some $v_2 \in X^*$ in $\mathscr{P}$ such that u divides v_2. Lipton [Lip76] showed that deciding the coverability problem requires at least space $2^{d' \cdot \sqrt{\text{size}(u, \mathscr{P})}}$ for some constant $d' > 0$ independent of u and $\mathscr{P}$. By the results in [MM82], which exhibit

[1] Corresponding author.

0890-5401/00 $35.00

the exponential space completeness of the uniform word problem for commutative semigroups, this lower complexity bound by Lipton has been strengthened to $2^{d \cdot \text{size}(u, \mathscr{P})}$ for some constant $d > 0$ independent of u and $\mathscr{P}$. Finally, Rackoff [Rac78] obtained a $2^{c \cdot \text{size}(u, \mathscr{P}) \cdot \log(\text{size}(u, \mathscr{P}))}$ space upper bound for these problems, where $c > 0$ is again some constant independent of u and $\mathscr{P}$. Until now it has been an open problem whether the gap between the $2^{c \cdot \text{size}(u, \mathscr{P}) \cdot \log(\text{size}(u, \mathscr{P}))}$ upper and the $2^{d \cdot \text{size}(u, \mathscr{P})}$ lower space bounds can be reduced.

We shall close this gap for an important subclass of commutative semi-Thue systems, the class of commutative Thue systems, or, equivalently, commutative semigroups (or, equivalently, reversible vector addition systems or reversible Petri nets). We present an exponential space algorithm for an extended version of the ordinary coverability problem, which also provides an exponential space algorithm enumerating the elements of finite congruence classes. The main idea of our algorithm is to construct a basis of a binomial ideal such that the reduced Gröbner basis of this ideal contains the solution.

Let $\mathscr{P}$ be a commutative semi-Thue system over some alphabet $X = \{x_1, ..., x_k\}$, and u, v_1 two words in X^*. Given $\mathscr{P}$, u, and v_1, the (ordinary) *subword problem* is the problem of deciding whether there is a v_2 in the reachability set of u in $\mathscr{P}$ such that $v_2 = v_1 \cdot w$ for some $w \in X^*$ which contains no variable occurring in v_1. I.e., if such a word v_2 exists, then without loss of generality the variables can be renamed such that

strengthening of coverability: must preserve the support

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

i.e., $v_1 \in \{x_1, ..., x_l\}^*$ and $w \in \{x_{l+1}, ..., x_k\}^*$. In the case of commutative semi-Thue systems, or equivalently, general (not necessarily reversible) Petri nets, the subword problem (resp., the submarking reachability problem) easily reduces to the word problem since, in a semi-Thue system, we can arrange irreversible productions from one phase to another. This technique, however, can no longer be applied in the case of Thue systems like commutative semigroups or reversible Petri nets since all productions can, by definition, be undone.

For commutative semi-Thue systems the decidability of the uniform word problem (in the context of Petri nets and vector addition systems also called *reachability problems*) was an open problem for a long time. Lipton [Lip76] showed that it requires at least space $2^{d \cdot \sqrt{n}}$, where n is the size of the problem instance and $d > 0$ some constant independent of n. Finally, Mayr [May81] presented an algorithm for the general word problem for commutative semi-Thue systems. The exact computational complexity of this algorithm is an open problem.

The effective decidability of the uniform word problem for commutative semigroups was first explicitly noted by Malcev [Mal58] and Emiličev [Emi63], though in retrospect this result can be seen to be a special case of results by Hentzelt [Hen22], Hermann [Her26], Hilbert [Hil90], and König [Kön03] on testing membership in polynomial ideals. In [MM82], Mayr and Meyer exhibited the exponential space completeness of the uniform word problem for commutative semigroups.

Our investigation of the complexity of an extended version of the ordinary subword problem for commutative semigroups benefits a lot from the close relationship of commutative semigroups and binomial ideals. As in the case of the coverability problem the proof is an application of the Gröbner basis construction algorithm for binomial ideals.

Given two commutative semi-Thue systems $\mathscr{P}$, $\mathscr{Q}$ over X and two words u, $v \in X^*$, the containment (equivalence) problem is the problem of determining whether the reachability set of u in $\mathscr{P}$ is contained in (is equal to) the reachability set of v in $\mathscr{Q}$. In [Hac76], these two problems were shown to be undecidable. The situation changes, however, when one considers commutative Thue systems, or commutative semigroups [Bir67, Emi63, Mar47, Tai68]. In [Huy85], Huynh exhibited decision algorithms for the containment and the equivalence problems for commutative semigroups which operate in space $2^{d \cdot \text{size}(u, v, \mathscr{P}, \mathscr{Q}) \cdot \log(\text{size}(u, v, \mathscr{P}, \mathscr{Q}))}$, where $d > 0$ is some constant independent of u, v, $\mathscr{P}$, and $\mathscr{Q}$.

We are able to show a $2^{c \cdot \text{size}(u, v, \mathscr{P}, \mathscr{Q})}$ space upper bound for deciding the containment and the equivalence problems for commutative semigroups, with $c > 0$ some constant independent of u, v, $\mathscr{P}$, and $\mathscr{Q}$. We prove that there is an algorithm which generates a uniformly semilinear representation of any congruence class $[u]_{\mathscr{P}}$ using at most space $2^{c' \cdot \text{size}(u, \mathscr{P})}$. To decide whether $[u]_{\mathscr{P}} \subseteq [v]_{\mathscr{Q}}$ ($[u]_{\mathscr{P}} = [v]_{\mathscr{Q}}$), it has to be checked whether each minimal element a of $[u]_{\mathscr{P}}$ with respect to divisibility is contained in $[v]_{\mathscr{Q}}$ (and vice versa) and whether each minimal period b of $[u]_{\mathscr{P}}$ is a period of $[v]_{\mathscr{Q}}$ (and vice versa). We shall see that this can be done in space $2^{c \cdot \text{size}(u, v, \mathscr{P}, \mathscr{Q})}$.

We establish the exponential space completeness of the coverability problem (in a generalized form), the subword problem (in a generalized form), the containment and the equivalence problems for commutative semigroups.

2. BASIC CONCEPTS

2.1. Definitions and Notations

Let $\mathbb{Q}$ be the set of rationals, $\mathbb{N}$ the set of nonnegative integers, and $\mathbb{Z}$ the set of integers. Denote by X the finite set $\{x_1, ..., x_k\}$, and by $\mathbb{Q}[X]$ the (commutative) ring of polynomials with indeterminates $x_1, ..., x_k$ and rational coefficients.

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

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

with $(e_1, e_2, ..., e_k) \in \mathbb{N}^k$ 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 $\geqslant 0$).

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

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

with $a_i \in \mathbb{Q}\backslash\{0\}$ 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 $f_1, ..., f_h \in \mathbb{Q}[X]$, $\langle f_1, ..., f_h \rangle \subseteq \mathbb{Q}[X]$ denotes the ideal generated by $\{f_1, ..., f_h\}$, that is

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

where, for $h \in \mathbb{N}$, I_h denotes the set $\{1, ..., h\}$. Whenever $I = \langle f_1, ..., f_h \rangle$, $\{f_1, ..., f_h\}$ is called a *basis* of I.

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

(T1) $e \geqslant (0, ..., 0)$ for all $e \in \mathbb{N}^k$,

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

If $(d_1, ..., d_k) > (e_1, ..., e_k)$, 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 $f(x_1, ..., x_k) = \sum_{i=1}^{n} a_i \cdot t_i$ we always assume that $t_1 \succ t_2 \succ \cdots \succ t_n$. For any such 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 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 [Rob85, Wei87]).

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

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

(G2) $\{LT(g_1), ..., LT(g_r)\}$ 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 $LT(f) \in \langle LT(g_1), ..., LT(g_r) \rangle$.

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 $X = \{x_1, ..., x_k\}$, let X^* denote the free commutative monoid generated by X. An element u of X^* is called a (*commutative*) *word*. The unit element of X^*, i.e., the empty word, is denoted by ε. Let Φ be the Parikh mapping, i.e., $\Phi(u, x_i)$ (also written $(\Phi(u))_i$) indicates, for every $u \in X^*$ and $i \in \{1, ..., k\}$, the number of occurrences of $x_i \in X$ in u. For a word, the order of the symbols is immaterial, and we shall use exponential notation: $u = x_1^{e_1} \cdots x_k^{e_k}$, where $e_i = \Phi(u, x_i) \in \mathbb{N}$ for $i = 1, ..., k$. We identify any $u \in X^*$ (resp., the corresponding vector $u = (\Phi(u, x_1), ..., \Phi(u, x_k)) \in \mathbb{N}^k$) 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 $\mathscr{P} = \{l_i \equiv r_i; i \in I_h\}$ 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 $u \to v$ $(\mathscr{P})$) by application of the congruence $(l_i \equiv r_i) \in \mathscr{P}$ 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., $u \to v$ $(\mathscr{P}) \Leftrightarrow v \to u$ $(\mathscr{P})$). The word u *derives* v, written $u \equiv v \bmod \mathscr{P}$, iff $u \xrightarrow{*} v$ $(\mathscr{P})$, where $\xrightarrow{*}$ is the reflexive transitive closure of $\to$. More precisely, we write $u \xrightarrow{+} v$ $(\mathscr{P})$, where $\xrightarrow{+}$ is the transitive closure of $\to$, if $u \xrightarrow{*} v$ $(\mathscr{P})$ and $u \neq v$. A sequence $(u_0, ..., u_n)$ of words $u_i \in X^*$ with $u_i \to u_{i+1}$ $(\mathscr{P})$ for $i = 0, ..., n-1$, is called a *derivation* (of length n) of u_n from u_0 in $\mathscr{P}$. The *congruence class* of $u \in X^*$ modulo $\mathscr{P}$ is the set $[u]_{\mathscr{P}} = \{v \in X^* ; u \equiv v \bmod \mathscr{P}\}$.

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

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

We call such an ideal, i.e., an ideal that has a basis consisting only of differences of two terms, a (pure difference) *binomial ideal* (see [KM96]). By looking at Buchberger's algorithm [Buc65] it is not hard to see that the reduced Gröbner basis of a (pure difference) binomial ideal still consists only of (pure difference) binomials.

2.2. The Basic Problems and Their Complexity

The uniform word problem and the polynomial ideal membership problem. The following proposition shows the connection between the uniform word problem for commutative semigroups and the membership problem for ideals in $\mathbb{Q}[X]$. The *uniform word problem* for commutative semigroups is the problem of deciding for a commutative semigroup presentation $\mathscr{P}$ over some alphabet X, and two words $u, v \in X^*$ whether $u \equiv v \bmod \mathscr{P}$. The *polynomial ideal membership problem* is the problem of deciding for given polynomials $f, f_1, ..., f_h \in \mathbb{Q}[X]$ whether $f \in \langle f_1, ..., f_h \rangle$. In [MM82], Mayr and Meyer proved

PROPOSITION 1 [MM82]. *Let $X = \{x_1, ..., x_k\}$ be some finite alphabet, $\mathscr{P} = \{l_i \equiv r_i;\ i \in I_h\}$ a finite commutative semigroup presentation over X, and u, v two words in X^* with $u \neq v$. Then, from $u \equiv v \bmod \mathscr{P}$, it follows that $u - v \in I(\mathscr{P})$, and vice versa, i.e., if there exist $p_1, ..., p_h \in \mathbb{Q}[X]$ such that $u - v = \sum_{i=1}^{h} p_i(l_i - r_i)$, then there is a derivation $u = \gamma_0 \to \gamma_1 \to \cdots \to \gamma_n = v$ $(\mathscr{P})$ of v from u in $\mathscr{P}$ such that, for $j \in \{0, 1, ..., n\}$,*

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

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

PROPOSITION 2 [Her26]. *Let $X = \{x_1, ..., x_k\}$, $f, f_1, ..., f_h \in \mathbb{Q}[X]$, and $d := \max\{\deg(f_i);\ i \in I_h\}$. If $f \in \langle f_1, ..., f_h \rangle$, then there exist $p_1, ..., p_h \in \mathbb{Q}[X]$ such that*

(i) $f = \sum_{i=1}^{h} p_i f_i$;

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

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

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

The reduced Gröbner basis of binomial ideals. The following proposition characterizes the binomials of the reduced Gröbner basis of a binomial ideal.

PROPOSITION 4 [KM96]. *Let* $X = \{x_1, ..., x_k\}$, $\mathscr{P} = \{l_i \equiv r_i;\ i \in I_h\}$ *with* $l_i, r_i \in X^*$ *for all* $i \in I_h$, *and let* $G = \{h_1 - m_1, ..., h_r - m_r\}$ *be the reduced Gröbner basis of the ideal* $I(\mathscr{P})$ *with respect to some admissible term ordering* $\geqslant$ *on* X^* ($h_i \succ m_i$ *for all* $i \in I_r$). *Then*

(i) m_i *is the* $\succ$*-minimal element of the congruence class* $[h_i]_{\mathscr{P}}$, $i \in I_r$.

(ii) $LT(I(\mathscr{P}))$ (*the set of the leading terms of* $I(\mathscr{P})$) *is the set of all terms with non-trivial congruence class which are* not *the* $\succ$*-minimal element in their congruence class.* $H = \{h_1, ..., h_r\}$ *is the set of the minimal elements of* $LT(I(\mathscr{P}))$ *with respect to divisibility.*

The reduced Gröbner basis of binomial ideals can be generated using at most exponential space. We use size$(\cdot)$ to denote the size of the representation of the input in any standard encoding.

PROPOSITION 5 [KM96]. *Let* $X = \{x_1, ..., x_k\}$, $\mathscr{P} = \{l_i \equiv r_i;\ i \in I_h\}$ *with* $l_i, r_i \in X^*$ *for all* $i \in I_h$, *and* $\geqslant$ *some admissible term ordering. Then there is an algorithm which generates the reduced Gröbner basis* $G = \{h_1 - m_1, ..., h_r - m_r\}$ *of the binomial ideal* $I(\mathscr{P})$ *with respect to* $\geqslant$ *using at most space* $(\text{size}(\mathscr{P}))^2 \cdot 2^{\bar{c} \cdot k} \leqslant 2^{c \cdot \text{size}(\mathscr{P})}$, *where* $\bar{c}, c > 0$ *are some constants independent of* $\mathscr{P}$.

For proofs of Propositions 4 and 5 see [KM96].

The following proposition obtained by Dubé [Dub90] provides an upper bound for the total degree of polynomials required in a Gröbner basis.

PROPOSITION 6 [Dub90]. *Let* $F = \{f_1, ..., f_h\} \subset \mathbb{Q}[X] = \mathbb{Q}[x_1, ..., x_k]$, $I = \langle f_1, ..., f_h \rangle$ *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* $\geqslant$, *the degree of polynomials required in a Gröbner basis for* I *with respect to* $\geqslant$ *is bounded by*

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

3. THE COVERABILITY PROBLEM

In this section, we present an optimal decision procedure for an extended version of the ordinary coverability problem for commutative semigroups.

Let $\mathscr{P}$ be a finite commutative semigroup presentation over some finite alphabet X and u a word in X^*. Then the set of words in X^* from which u can be covered in $\mathscr{P}$, i.e., the set

$$C(u, \mathscr{P}) = \{v_1 \in X^*; \exists v_2 \in [v_1]_{\mathscr{P}} \text{ with } v_2 = u \cdot w, w \in X^*\}$$

is called the *covering set of u in* $\mathscr{P}$. If a word $v \in X^*$ is an element of $C(u, \mathscr{P})$, then obviously any v' which is divisible by v, i.e., $v' = v \cdot w_{v'}$ for some $w_{v'} \in X^*$, is also an element of $C(u, \mathscr{P})$. Thus, for a closed representation of $C(u, \mathscr{P})$, it suffices to determine the set of minimal elements with respect to divisibility of $C(u, \mathscr{P})$, denoted by $\min(C(u, \mathscr{P}))$. Note that, by Dickson's lemma (see [Dic13]), there are only finitely many elements in $\min(C(u, \mathscr{P}))$. We formally define the coverability problem for commutative semigroups as follows.

The *Coverability Problem* for commutative semigroups is:

Given a finite commutative semigroup presentation $\mathscr{P}$ over some finite alphabet X and a word $u \in X^*$, generate a closed representation of the covering set of u in $\mathscr{P}$.

THEOREM 1. *Let* $X = \{x_1, ..., x_k\}$, $\mathscr{P} = \{l_i \equiv r_i; i \in I_h\}$ *be a finite commutative semigroup presentation over X, and u a word in* X^*. *Then there is an algorithm which generates a closed representation of the covering set* $C(u, \mathscr{P})$ *of u in* $\mathscr{P}$ *using at most space* $(\text{size}(u, \mathscr{P}))^2 \cdot 2^{\bar{c} \cdot k} \leqslant 2^{c \cdot \text{size}(u, \mathscr{P})}$, *where* $\bar{c}$, $c > 0$ *are some constants independent of u and* $\mathscr{P}$.

Proof. In addition to $x_1, ..., x_k$ we introduce $2k + 3$ new variables m, s, t, $y_1, ..., y_k$, and $z_1, ..., z_k$. Let $X' = X \cup \{m, s, t, y_1, ..., y_k, z_1, ..., z_k\}$. Given $\mathscr{P}$ and the word $u \in X^*$, we construct a new commutative semigroup presentation $\mathscr{P}'$ over X': $\mathscr{P}'$ contains the congruences

$$s \cdot x_j \equiv s \cdot y_j \cdot z_j, \qquad \text{for} \quad j = 1, ..., k, \tag{1}$$

$$s \cdot y(u) \equiv t, \tag{2}$$

$$s \cdot u \equiv m, \tag{3}$$

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

$$s \cdot y(l_i) \equiv s \cdot y(r_i), \tag{4}$$

$$t \cdot z(l_i) \equiv t \cdot z(r_i), \tag{5}$$

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

Let $\succcurlyeq$ be a lexicographic term ordering satisfying

$$b \succ s \succ a \succ m$$

for all $a \in \{x_1, ..., x_k\}$, $b \in \{t, y_1, ..., y_k, z_1, ..., z_k\}$.

In the following, we prove that, for a word $v \in X^*$,

$$v \in \min(C(u, \mathscr{P})) \qquad \text{iff} \quad s \cdot v - m \cdot \tilde{u} \in G,$$

where $\tilde{u}$ is some word in X^* and G is the reduced Gröbner basis of the ideal $I(\mathscr{P}')$ with respect to $\succcurlyeq$. Then, by Proposition 5, a complete list of all the elements of $\min(C(u, \mathscr{P}))$ can be generated using at most space $(\text{size}(u, \mathscr{P}'))^2 \cdot 2^{d' \cdot k} \leqslant (\text{size}(u, \mathscr{P}))^2 \cdot 2^{d \cdot k}$, and, by Proposition 6, the size of the elements of $\min(C(u, \mathscr{P}))$ is bounded by $\text{size}(u, \mathscr{P}) \cdot 2^{\bar{d} \cdot k}$, where d', d, $\bar{d} > 0$ are some constants independent of u and $\mathscr{P}'$ (resp., $\mathscr{P}$).

First, we illuminate the roles of the new variables s, t, m, and y_i, z_i, $i \in \{1, ..., k\}$.

In $\mathscr{P}'$, a word $w \in [v]_{\mathscr{P}}$ cannot be derived directly from v, as in $\mathscr{P}$. For the derivation of $s \cdot w$ from $s \cdot v$ in $\mathscr{P}'$ each x_i which is contained in v and involved in the derivation of w from v in $\mathscr{P}$ has to be split into $y_i \cdot z_i$ by the corresponding congruence in (1). Then the derivation of w has to be performed separately on the y_i's and z_i's by the congruences in (3) and (4). The variables s and t are responsible for the separation of the derivations concerning the y_i's from those concerning the z_i's. A change between the two modes is only possible by congruence (2), which can only be applied if $y(u)$ is covered, i.e., u can be covered from v in $\mathscr{P}$. Finally, the y_i's and z_i's are recombined to x_i's by the congruences in (1).

The variable m is used to ensure that every $v \in \min(C(u, \mathscr{P}))$ appears in the reduced Gröbner basis G of the ideal $I(\mathscr{P}')$ with respect to $\succcurlyeq$.

LEMMA 1. *For $v \in X^*$, every word $w \in [s \cdot v]_{\mathscr{P}'}$ satisfies the conditions*:

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

(ii) *if* $\Phi(w, s) = 1$, *then*

$$x_1^{\Phi(w, x_1) + \Phi(w, y_1)} \cdot x_2^{\Phi(w, x_2) + \Phi(w, y_2)} \cdots x_k^{\Phi(w, x_k) + \Phi(w, y_k)} \in [v]_{\mathscr{P}},$$
$$x_1^{\Phi(w, x_1) + \Phi(w, z_1)} \cdot x_2^{\Phi(w, x_2) + \Phi(w, z_2)} \cdots x_k^{\Phi(w, x_k) + \Phi(w, z_k)} \in [v]_{\mathscr{P}};$$

if $\Phi(w, t) = 1$, *then*

$$x_1^{\Phi(w, x_1) + \Phi(w, y_1)} \cdot x_2^{\Phi(w, x_2) + \Phi(w, y_2)} \cdots x_k^{\Phi(w, x_k) + \Phi(w, y_k)} \cdot u \in [v]_{\mathscr{P}},$$
$$x_1^{\Phi(w, x_1) + \Phi(w, z_1)} \cdot x_2^{\Phi(w, x_2) + \Phi(w, z_2)} \cdots x_k^{\Phi(w, x_k) + \Phi(w, z_k)} \in [v]_{\mathscr{P}};$$

if $\Phi(w, m) = 1$, *then*

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

Proof. Let w be any word in $[s \cdot v]_{\mathscr{P}'}$. Then there is a repetition-free derivation in $\mathscr{P}'$ leading from $s \cdot v$ to w. If w contains m and w can be derived in one step from $s \cdot v$ by congruence (3), then w trivially satisfies conditions (i) and (ii). If in a derivation in $\mathscr{P}'$ congruence (3) is applied to a word of the form $s \cdot v'$ with $v' \in \{x_1, ..., x_k, y_1, ..., y_k, z_1, ..., z_k\}^*$, then this derivation can only be continued by again using

congruence (3), causing a repetition. If w does not contain m, or w cannot be derived in one step from $s \cdot v$ by congruence (3), then in any repetition-free derivation in $\mathscr{P}'$ starting at $s \cdot v$, leading to w, only the congruences in (1) and (4) can be applied until a word $s \cdot y(u) \cdot v_1$, $v_1 \in \{x_1, ..., x_k, y_1, ..., y_k, z_1, ..., z_k\}^*$ is reached and changed to $t \cdot v_1$ by congruence (2). Any word w occurring in this derivation of $s \cdot y(u) \cdot v_1$ from $s \cdot v$ satisfies conditions (i′) and (ii′):

(i′) $\Phi(w, s) = 1$, $\Phi(w, t) = 0$, $\Phi(w, m) = 0$;

$$x_1^{\Phi(w, x_1) + \Phi(w, y_1)} \cdot x_2^{\Phi(w, x_2) + \Phi(w, y_2)} \cdots x_k^{\Phi(w, x_k) + \Phi(w, y_k)} \in [v]_{\mathscr{P}}, \qquad \text{and}$$

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

Then, as long as congruence (2) is not applied, only the congruences in (5) can be applied. In the resulting subderivation starting at $t \cdot v_1$ any word is of the form $t \cdot v_1'$ with $v_1' \in \{x_1, ..., x_k, y_1, ..., y_k, z_1, ..., z_k\}^*$, $\Phi(v_1', x_i) = \Phi(v_1, x_i)$, $\Phi(v_1', y_i) = \Phi(v_1, y_i)$ for all $i \in I_k$, and

$$x_1^{\Phi(v_1', z_1)} \cdot x_2^{\Phi(v_1', z_2)} \cdots x_k^{\Phi(v_1', z_k)} \in [x_1^{\Phi(v_1, z_1)} \cdot x_2^{\Phi(v_1, z_2)} \cdots x_k^{\Phi(v_1, z_k)}]_{\mathscr{P}}.$$

Hence,

$$x_1^{\Phi(v_1', x_1) + \Phi(v_1', y_1)} \cdot x_2^{\Phi(v_1', x_2) + \Phi(v_1', y_2)} \cdots x_k^{\Phi(v_1', x_k) + \Phi(v_1', y_k)} \cdot u \in [v]_{\mathscr{P}},$$

and

$$x_1^{\Phi(v_1', x_1) + \Phi(v_1', z_1)} \cdot x_2^{\Phi(v_1', x_2) + \Phi(v_1', z_2)} \cdots x_k^{\Phi(v_1', x_k) + \Phi(v_1', z_k)} \in [v]_{\mathscr{P}},$$

i.e., conditions (i) and (ii) are satisfied. Congruence (2) changes $t \cdot v_1'$ to $s \cdot y(u) \cdot v_1'$, and again the congruences in (1) and (4) can be applied. By these congruences, from $s \cdot y(u) \cdot v_1'$ words $s \cdot v_1''$ with $v_1'' \in \{x_1, ..., x_k, y_1, ..., y_k, z_1, ..., z_k\}^*$,

$$x_1^{\Phi(v_1'', x_1) + \Phi(v_1'', y_1)} \cdot x_2^{\Phi(v_1'', x_2) + \Phi(v_1'', y_2)} \cdots x_k^{\Phi(v_1'', x_k) + \Phi(v_1'', y_k)} \in [v]_{\mathscr{P}},$$

and

$$x_1^{\Phi(v_1'', x_1) + \Phi(v_1'', z_1)} \cdot x_2^{\Phi(v_1'', x_2) + \Phi(v_1'', z_2)} \cdots x_k^{\Phi(v_1'', x_k) + \Phi(v_1'', z_k)}$$
$$= x_1^{\Phi(v_1', x_1) + \Phi(v_1', z_1)} \cdot x_2^{\Phi(v_1', x_2) + \Phi(v_1', z_2)} \cdots x_k^{\Phi(v_1', x_k) + \Phi(v_1', z_k)} \in [v]_{\mathscr{P}}$$

can be derived. Congruence (2) can only be applied to a word which is divisible by $s \cdot y(u)$. Then $s \cdot y(u)$ can be replaced by t, and the congruences in (5) can again be applied. This case has been considered above.

Congruence (3) can be applied to words divisible by $s \cdot u$. Then the derivation can only be continued by again using congruence (3), causing a repetition. Hence, after

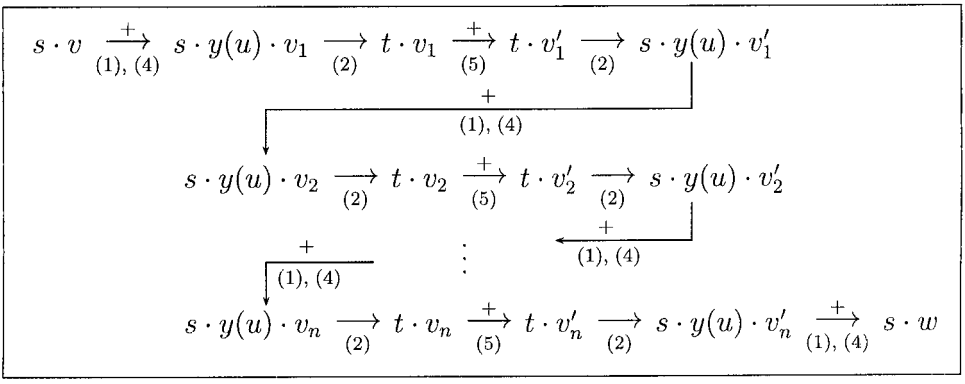

FIG. 1. Arbitrary repetition-free derivation in $\mathscr{P}'$ leading from $s \cdot v$ to $s \cdot w$.

applying congruence (3) a repetition-free derivation terminates. The final word is some $w = m \cdot w'$ with $w' \in \{x_1, ..., x_k, y_1, ..., y_k, z_1, ..., z_k\}^*$, and

$$x_1^{\Phi(w', x_1) + \Phi(w', y_1)} \cdot x_2^{\Phi(w', x_2) + \Phi(w', y_2)} \cdots x_k^{\Phi(w', x_k) + \Phi(w', y_k)} \cdot u \in [v]_{\mathscr{P}},$$

$$x_1^{\Phi(w', x_1) + \Phi(w', z_1)} \cdot x_2^{\Phi(w', x_2) + \Phi(w', z_2)} \cdots x_k^{\Phi(w', x_k) + \Phi(w', z_k)} \cdot u \in [v]_{\mathscr{P}}.$$

Thus, conditions (i) and (ii) are satisfied within the whole derivation leading from $s \cdot v$ to any $w \in [s \cdot v]_{\mathscr{P}'}$. ∎

LEMMA 2. *Let v, w be two words in X^* with $v \neq w$. Then*

- *a repetition-free derivation in $\mathscr{P}'$ leading from $s \cdot v$ to $s \cdot w$ has the form shown in Fig. 1, where "$\xrightarrow[(.)]{+}$" denotes some repetition-free derivation applying only the congruences given in (.), and $v_1, v_1', v_2, v_2', ..., v_n, v_n'$, $n \geqslant 1$, are words in $\{x_1, ..., x_k, y_1, ..., y_k, z_1, ..., z_k\}^*$.*
- *$s \cdot w \in [s \cdot v]_{\mathscr{P}'}$ iff $w \in [v]_{\mathscr{P}}$ and there is some $\bar{w} \in [v]_{\mathscr{P}}$ such that u divides $\bar{w}$.*

Proof. Let $s \cdot v = \gamma_0 \to \gamma_1 \to \cdots \to \gamma_{\bar{n}} = s \cdot w$ be any repetition-free derivation in $\mathscr{P}'$ leading from $s \cdot v$ to $s \cdot w$. Then, by Lemma 1, there must be some $i \in I_{\bar{n}-1}$ with

$$\gamma_i = s \cdot y(u) \cdot v_1 \to \gamma_{i+1} = t \cdot v_1,$$

where

- $v_1 \in \{x_1, ..., x_k, y_1, ..., y_k, z_1, ..., z_k\}^*$,
- $x_1^{\Phi(v_1, x_1) + \Phi(v_1, y_1)} \cdot x_2^{\Phi(v_1, x_2) + \Phi(v_1, y_2)} \cdots x_k^{\Phi(v_1, x_k) + \Phi(v_1, y_k)} \cdot u \in [v]_{\mathscr{P}}$,
- $x_1^{\Phi(v_1, x_1) + \Phi(v_1, z_1)} \cdot x_2^{\Phi(v_1, x_2) + \Phi(v_1, z_2)} \cdots x_k^{\Phi(v_1, x_k) + \Phi(v_1, z_k)} = v$,

and some $j \in I_{\bar{n}-1}$, $j > i$, with

$$\gamma_j = t \cdot v_n' \to \gamma_{j+1} = s \cdot y(u) \cdot v_n',$$

where

- $v'_n \in \{x_1, ..., x_k, y_1, ..., y_k, z_1, ..., z_k\}^*$,
- $x_1^{\Phi(v'_n, x_1)+\Phi(v'_n, y_1)} \cdot x_2^{\Phi(v'_n, x_2)+\Phi(v'_n, y_2)} \cdots x_k^{\Phi(v'_n, x_k)+\Phi(v'_n, y_k)} \cdot u \in [v]_{\mathscr{P}}$,
- $x_1^{\Phi(v'_n, x_1)+\Phi(v'_n, z_1)} \cdot x_2^{\Phi(v'_n, x_2)+\Phi(v'_n, z_2)} \cdots x_k^{\Phi(v'_n, x_k)+\Phi(v'_n, z_k)} = w$

(hence, $w \in [v]_{\mathscr{P}}$).

The words $v_1, v'_1, v_2, v'_2, ..., v_n, v'_n$, $n \geqslant 1$, are elements of $\{x_1, ..., x_k, y_1, ..., y_k, z_1, ..., z_k\}^*$ satisfying ("." denotes any v_i, v'_i for $i \in I_n$)

- $x_1^{\Phi(., x_1)+\Phi(., y_1)} \cdot x_2^{\Phi(., x_2)+\Phi(., y_2)} \cdots x_k^{\Phi(., x_k)+\Phi(., y_k)} \cdot u \in [v]_{\mathscr{P}}$ (hence, there exists $\bar{w} \in [v]_{\mathscr{P}}$ such that u divides $\bar{w}$),
- $x_1^{\Phi(., x_1)+\Phi(., z_1)} \cdot x_2^{\Phi(., x_2)+\Phi(., z_2)} \cdots x_k^{\Phi(., x_k)+\Phi(., z_k)} \in [v]_{\mathscr{P}}$,
- $\Phi(v_i, x_j) = \Phi(v'_i, x_j)$, $\Phi(v_i, y_j) = \Phi(v'_i, y_j)$, $i \in I_n$, $j \in I_k$,
- $x_1^{\Phi(v'_i, x_1)+\Phi(v'_i, z_1)} \cdot x_2^{\Phi(v'_i, x_2)+\Phi(v'_i, z_2)} \cdots x_k^{\Phi(v'_i, x_k)+\Phi(v'_i, z_k)} = x_1^{\Phi(v_{i+1}, x_1)+\Phi(v_{i+1}, z_1)} \cdot x_2^{\Phi(v_{i+1}, x_2)+\Phi(v_{i+1}, z_2)} \cdots x_k^{\Phi(v_{i+1}, x_k)+\Phi(v_{i+1}, z_k)}$, $i \in I_{n-1}$.

Note that in a repetition-free derivation in $\mathscr{P}'$ leading from $s \cdot v$ to $s \cdot w$ congruence (3) does not occur.

Finally, suppose $w \in [v]_{\mathscr{P}}$ and $\bar{w} = u \cdot \bar{w}_u \in [v]_{\mathscr{P}}$, $\bar{w}_u \in X^*$. Then $s \cdot w$ can be derived from $s \cdot v$ by the derivation shown in Fig. 2. ∎

Note that the derivation of Fig. 1 can always be modified such that $n = 1$, i.e., it essentially gets the form of the derivation in Fig. 2.

LEMMA 3. *Let v be some word in X^* with $v \notin C(u, \mathscr{P})$. Then $s \cdot v$ is the $\succ$-minimal element of its congruence class $[s \cdot v]_{\mathscr{P}'}$ modulo $\mathscr{P}'$.*

Proof. If $v \in X^*$ with $v \notin C(u, \mathscr{P})$, then there is no $\bar{v} \in [v]_{\mathscr{P}}$ which is divisible by u. Thus, in any derivation in $\mathscr{P}'$ starting at $s \cdot v$ the congruences (2) and (3) cannot be applied. Only the congruences in (1) and (4) can possibly be used. Since $y_i \succ x_j$ and $z_i \succ x_j$ for all $i, j \in I_k$, $s \cdot v$ is the $\succ$-minimal element of $[s \cdot v]_{\mathscr{P}'}$. ∎

Note that each $v \in X^*$ is the $\succ$-minimal element of its congruence class $[v]_{\mathscr{P}'}$ modulo $\mathscr{P}'$ because no congruence in $\mathscr{P}'$ is applicable.

If $v \in C(u, \mathscr{P})$, then there is some $w \in X^*$ with $u \cdot w \in [v]_{\mathscr{P}}$, and, by Lemma 2, $s \cdot u \cdot w \in [s \cdot v]_{\mathscr{P}'}$. Since $s \cdot u \equiv m \bmod \mathscr{P}'$, and

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

the $\succ$-minimal element of $[s \cdot v]_{\mathscr{P}'}$ with $v \in C(u, \mathscr{P})$ is of the form $m \cdot \tilde{u}$, where $\tilde{u} \in X^*$ and $u \cdot \tilde{u}$ is the $\succ$-minimal element (resp., $\succ_X$-minimal element, where $\succ_X$ is the restriction of $\succ$ to the words in X^*) of $[v]_{\mathscr{P}}$ that covers u. Thus, by Proposition 4, each $s \cdot v$ with $v \in C(u, \mathscr{P})$ is an element of $LT(I(\mathscr{P}'))$. In particular, by Lemma 3, each $s \cdot v$ with $v \in \min(C(u, \mathscr{P}))$ is contained in the set of the minimal elements of $LT(I(\mathscr{P}'))$ with respect to divisibility. Hence, by Proposition 4, for a word $v \in X^*$, it follows that $v \in \min(C(u, \mathscr{P}))$ iff $s \cdot v - m \cdot \tilde{u} \in G$, where G is the reduced Gröbner basis of the ideal $I(\mathscr{P}')$ with respect to $\succcurlyeq$. ∎

$$s \cdot v \xrightarrow[(1)]{+} s \cdot y(v) \cdot z(v) \xrightarrow[(4)]{*} s \cdot y(u) \cdot y(\overline{w}_u) \cdot z(v)$$
$$\xrightarrow[(2)]{} t \cdot y(\overline{w}_u) \cdot z(v) \xrightarrow[(5)]{+} t \cdot y(\overline{w}_u) \cdot z(w) \xrightarrow[(2)]{} s \cdot y(u) \cdot y(\overline{w}_u) \cdot z(w) \xrightarrow[(4)]{*} s \cdot y(w) \cdot z(w) \xrightarrow[(1)]{+} s \cdot w$$

FIG. 2. Repetition-free derivation in $\mathscr{P}'$ leading from $s \cdot v$ to $s \cdot w$.

As an example of Theorem 1, consider the commutative semigroup presentation

$$\mathscr{P} = \{x_1 \equiv x_2 x_3,\ x_2 x_3^3 \equiv x_1,\ x_2 \equiv x_2 x_3^4\}$$

over $X = \{x_1, x_2, x_3\}$. We want to generate a closed representation of the covering set

$$C(x_1, \mathscr{P}).$$

Using the construction of Theorem 1, we compute the reduced Gröbner basis G for the ideal

$$\begin{aligned} I := \langle & sy_1z_1 - sx_1,\ sy_2z_2 - sx_2,\ sy_3z_3 - sx_3,\ t - sy_1,\ sx_1 - m, \\ & sy_1 - sy_2y_3,\ sy_1 - sy_2y_3^3,\ sy_2y_3^4 - sy_2,\ tz_1 - tz_2z_3, \\ & tz_1 - tz_2z_3^3,\ tz_2z_3^4 - tz_2 \rangle \end{aligned}$$

with respect to the lexicographic term ordering $\succcurlyeq$ satisfying

$$t \succ z_1 \succ z_2 \succ z_3 \succ y_1 \succ y_2 \succ y_3 \succ s \succ x_1 \succ x_2 \succ x_3 \succ m.$$

We obtain

$$\begin{aligned} G = \{ & mx_3^2 - m,\ mx_2 - m^2x_3,\ mx_1 - m^2 + ,\ ms - m,\ \boxed{sx_2 - mx_3}, \\ & \boxed{sx_1 - m},\ y_3^2 - m,\ x_2y_2 - mx_3y_2,\ x_1y_2 - my_2,\ sy_2 - y_2, \\ & y_2y_3^2 - y_2,\ my_1 - my_2y_3,\ sy_1 - y_2y_3,\ y_1y_2 - y_2^2y_3,\ mz_3 - mx_3y_3, \\ & sy_3z_3 - sx_3,\ y_2z_3 - x_3y_2y_3,\ y_2z_2 - mx_3,\ mz_1 - mx_3y_3z_2, \\ & y_2z_1 - my_3,\ t - y_2y_3\}. \end{aligned}$$

The binomials $sx_2 - mx_3$ and $sx_1 - m$ provide the solution $\min(C(x_1, \mathscr{P})) = \{x_1, x_2\}$; i.e.,

$$C(x_1, \mathscr{P}) = \{x_1 \cdot w_1,\ x_2 \cdot w_2;\ w_1, w_2 \in X^*\}.$$

Furthermore, the first binomial tells us that x_1x_3 is the $\succ$-minimal word (resp., the $\succ_X$-minimal word, where $\succ_X$ is the strict part of the lexicographic term ordering

$\succcurlyeq_X$ on X^* satisfying $x_1 \succ_X x_2 \succ_X x_3$) in $[x_2]_{\mathscr{P}}$ that covers x_1, i.e., that is divisible by x_1. The second binomial gives us no further new information: x_1 is the minimal word in its congruence class that covers itself.

Let now $\mathscr{P}$ be a finite commutative semigroup presentation over some finite alphabet X and u a word in X^*. Since u can be derived in $\mathscr{P}$ from any word in $[u]_{\mathscr{P}}$, it is obvious that $[u]_{\mathscr{P}} \subseteq C(u, \mathscr{P})$. Moreover, if the congruence class $[u]_{\mathscr{P}}$ of u is bounded, i.e., there are only finitely many elements in $[u]_{\mathscr{P}}$, then we can prove that $[u]_{\mathscr{P}} \subseteq \min(C(u, \mathscr{P}))$. For a contradiction, suppose that $[u]_{\mathscr{P}}$ is bounded and v is some word in X^* with $v \in ([u]_{\mathscr{P}} \backslash \min(C(u, \mathscr{P})))$. Since $v \in (C(u, \mathscr{P}) \backslash \min(C(u, \mathscr{P})))$, there is a $\bar{v} \in \min(C(u, \mathscr{P}))$ such that $v = \bar{v} \cdot w_v$ for some $w_v \in X^* \backslash \{\varepsilon\}$, with $\bar{v} \equiv u \cdot u' \bmod \mathscr{P}$, $u' \in X^*$. Thus, we get $v \equiv u \cdot u' \cdot w_v \bmod \mathscr{P}$, and, since $v \in [u]_{\mathscr{P}}$, it follows that $u \equiv u \cdot u' \cdot w_v \bmod \mathscr{P}$, which contradicts the boundedness of $[u]_{\mathscr{P}}$.

Consider the commutative semigroup presentation $\mathscr{P}'$ constructed in the proof of Theorem 1. If $[u]_{\mathscr{P}}$ is bounded, then, by Lemmas 1 and 2, for a word $v \in X^*$, we have

$$v \in [u]_{\mathscr{P}} \qquad \text{iff} \quad s \cdot v \in [s \cdot u]_{\mathscr{P}'},$$

and from the definition of $\mathscr{P}'$ it follows that $[s \cdot u]_{\mathscr{P}'}$ is also bounded. The minimal element (with respect to the lexicographic term ordering $\succcurlyeq$ defined in the proof of Theorem 1) of $[s \cdot u]_{\mathscr{P}'}$ is m. In the proof of Theorem 1, we have shown that each $s \cdot v$ with $v \in \min(C(u, \mathscr{P}))$ is contained in the set of the minimal elements with respect to divisibility of $LT(I(\mathscr{P}'))$, and since $[u]_{\mathscr{P}} \subseteq \min(C(u, \mathscr{P}))$, for a word $v \in X^*$, it follows that

$$v \in [u]_{\mathscr{P}} \qquad \text{iff} \quad s \cdot v - m \in G,$$

where G is the reduced Gröbner basis of the ideal $I(\mathscr{P}')$ with respect to $\succcurlyeq$.

By Proposition 6, the size of the elements of $[u]_{\mathscr{P}}$ is bounded by $\text{size}(u, \mathscr{P}) \cdot 2^{d \cdot k}$, where $d > 0$ is some constant independent of u and $\mathscr{P}$. Furthermore, by Proposition 5, we obtain for the finite enumeration problem for commutative semigroups.

COROLLARY 1. *Let $X = \{x_1, ..., x_k\}$, $\mathscr{P} = \{l_i \equiv r_i;\ i \in I_h\}$ be a finite commutative semigroup presentation over X, and $u \in X^*$ a word such that the congruence class $[u]_{\mathscr{P}}$ of u modulo $\mathscr{P}$ is bounded. Then there is an algorithm which generates the elements of $[u]_{\mathscr{P}}$ using at most space $(\text{size}(u, \mathscr{P}))^2 \cdot 2^{\bar{c} \cdot k} \leqslant 2^{c \cdot \text{size}(u, \mathscr{P})}$, where $\bar{c}$, $c > 0$ are some constants independent of u and $\mathscr{P}$.*

From the work in [MM82] we know that the uniform word problem for commutative semigroups is exponential space complete (the input consisting of u, v and $\mathscr{P}$). Actually, the construction in [MM82] proves the slightly stronger statement which we will use for the proof of Theorem 2 below.

PROPOSITION 7 [MM82]. *Let $\mathscr{P}$ be a finite commutative semigroup presentation over some alphabet X, v a word in X^*, and $u \in X^*$ a word such that $[u]_{\mathscr{P}}$ is bounded.*

Even with this restriction, the uniform word problem, i.e., the problem of deciding whether $u \equiv v \bmod \mathscr{P}$, *is exponential space complete with respect to log-lin reducibility.*

THEOREM 2. *The coverability problem and the finite enumeration problem for commutative semigroups are exponential space complete with respect to log-lin reducibility.*

Proof. Let $\mathscr{P}$ be the commutative semigroup presentation and $u, v \in X^*$ the two words of Proposition 7. Then $v \equiv u \bmod \mathscr{P}$, i.e., $v \in [u]_{\mathscr{P}}$ iff v is contained in the list of elements of $[u]_{\mathscr{P}}$ generated by the enumeration algorithm of Corollary 1. Thus, an exponential space complete word problem reduces to the finite enumeration problem, and, since the finite enumeration problem is a special case of the coverability problem, it reduces also to the coverability problem. This, together with Theorem 1 and Corollary 1 establishes the exponential space completeness of the coverability problem and the finite enumeration problem for commutative semigroups. ∎

4. THE (GENERALIZED) SUBWORD PROBLEM

Let $X = \{x_1, ..., x_k\}$ be some finite alphabet, $\mathscr{P} = \{l_i \equiv r_i;\ i \in I_h\}$ a finite commutative semigroup presentation over X, and u, v_1 two words in X^*.

By X_{v_1} we denote the set of variables considered for v_1, i.e., $v_1 \in X_{v_1}^*$. If $X_{v_1} \neq X$, then we denote by $X_{\overline{v_1}}$ the set of variables $X_{\overline{v_1}} = X \backslash X_{v_1}$.

Let Y, Z be subsets of X with $Y \cap Z = \varnothing$. Without loss of generality, the variables can be renamed such that $X_{v_1} = \{x_1, ..., x_l\}$, $X_{\overline{v_1}} = \{x_{l+1}, ..., x_k\}$, $Y = \{x_{l_1}, x_{l_1+1}, ..., x_{l_2}\}$, and $Z = \{x_1, ..., x_{l_0}\} \cup \{x_{l_3}, ..., x_k\}$. Then, for the case $1 < l_0 < l_1 < l < l_2 < l_3 < k$ we get the following picture:

$$\overbrace{\underbrace{x_1, ..., x_{l_0}}_{Z}, x_{l_0+1}, ..., x_{l_1-1}, \underbrace{x_{l_1}, ..., x_l}_{Y}}^{X_{v_1}}, \overbrace{\underbrace{x_{l+1}, ..., x_{l_2}}_{Y}, x_{l_2+1}, ..., x_{l_3-1}, \underbrace{x_{l_3}, ..., x_k}_{Z}}^{X_{\overline{v_1}}}.$$

With this notation, we define the (generalized) subword problem for commutative semigroups as follows.

The (*Generalized*) *Subword Problem* for commutative semigroups is:

Given X, $\mathscr{P}$, u, v_1, Y, and Z, decide whether there is a $v_2 \in [u]_{\mathscr{P}}$ such that $v_2 = v_1 \cdot x_{l_1} \cdots x_{l_2} \cdot w$ for some $w \in (Y \cup Z)^*$ if $l_1 \leqslant l_2$ (resp., $v_2 = v_1 \cdot w$ for some $w \in Z^*$ if $l_1 > l_2$).

In this generalized form the subword problem is the problem of deciding whether there is a word $v_2 \in [u]_{\mathscr{P}}$ which can be divided into three parts, where the first consists of v_1, the second ensures that the number of occurrences of each variable in Y is strictly greater in v_2 than in v_1, and the third part is an arbitrary word only consisting of variables contained in Y or Z.

We observe that the uniform word problem and the ordinary coverability problem are special cases of the (generalized) subword problem. If Y and Z are both empty, then $v_2 = v_1$ and the (generalized) subword problem is the problem of deciding whether $v_1 \equiv u \bmod \mathscr{P}$; i.e., it is equivalent to the word problem. If Y is empty and $Z = X$, then v_2 is of the form $v_1 \cdot w$, $w \in X^*$, and the (generalized) subword problem is equivalent to the ordinary coverability problem.

If Y is empty and $Z = X_{\overline{v_1}}$, we get the definition of the ordinary subword problem. Then the (generalized) subword problem is the problem of deciding whether there is a $v_2 \in [u]_{\mathscr{P}}$ such that $v_2 = v_1 \cdot w$ for some $w \in X^*_{\overline{v_1}}$.

THEOREM 3. *Let $X = \{x_1, ..., x_k\}$ and $\mathscr{P} = \{l_i \equiv r_i;\ i \in I_h\}$ be a finite commutative semigroup presentation over X. Then there is an algorithm which, for any two words $u, v_1 \in X^*$, and sets $Y \subseteq X$, $Z \subseteq X \setminus Y$, decides whether there is, and if so, also provides a $v_2 \in [u]_{\mathscr{P}}$ such that $v_2 = v_1 \cdot v \cdot w$, where $w \in (Y \cup Z)^*$ and $v = x_{l_1} \cdots x_{l_2}$ if $Y = \{x_{l_1}, x_{l_1+1}, ..., x_{l_2}\}$ (resp., $v = \varepsilon$ if $Y = \varnothing$), using at most space $(\text{size}(u, v_1, \mathscr{P}))^2 \cdot 2^{\bar{c} \cdot k} \leqslant 2^{c \cdot \text{size}(u, v_1, \mathscr{P})}$ for some constants $\bar{c}$, $c > 0$, independent of u, v_1, and $\mathscr{P}$.*

Proof. We give a procedure for deciding whether there is a $v_2 \in [u]_{\mathscr{P}}$ as described in the theorem. If there is such a v_2, this procedure, which operates in space $(\text{size}(u, v_1, \mathscr{P}))^2 \cdot 2^{\bar{c} \cdot k}$, simultaneously provides one that is minimal with respect to divisibility among all such v_2. The size of such a v_2 is bounded by $\text{size}(u, v_1, \mathscr{P}) \cdot 2^{d \cdot k}$ for some constant $d > 0$ independent of u, v_1, and $\mathscr{P}$, and we shall see that it is minimal with respect to divisibility even among all words in $[u]_{\mathscr{P}}$ that are divisible by $v_1 \cdot v$.

In addition to $x_1, ..., x_k$ we introduce three new variables s, $\bar{s}$, and t. Let $X' = X \cup \{s, \bar{s}, t\}$. Given $\mathscr{P}$ and the two words $u, v_1 \in X^*$, we construct a new commutative semigroup presentation $\mathscr{P}'$ over X' as follows: For every congruence $l_i \equiv r_i$ in $\mathscr{P}$, $\mathscr{P}'$ contains the congruence

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

Then we add to $\mathscr{P}'$ the congruences

$$s \equiv t \cdot u$$

and

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

Let $\succcurlyeq$ be any lexicographic term ordering satisfying

$$s \succ t \succ x \succ \bar{s} \succ y$$

for all $x \in X \setminus (Y \cup Z)$, $y \in (Y \cup Z)$.

Since $s \equiv t \cdot u \bmod \mathscr{P}'$ and $s \succ t \cdot u$, by Proposition 4, we have $s \in LT(I(\mathscr{P}'))$. Because s is minimal in $LT(I(\mathscr{P}'))$ with respect to divisibility, by Proposition 4, the binomial $s - m_s$, where m_s is the $\succ$-minimal element of $[s]_{\mathscr{P}'}$, is an element of the reduced Gröbner basis of $I(\mathscr{P}')$ with respect to $\succcurlyeq$.

In $\mathscr{P}'$ the variable s, as well as the variable $\bar{s}$, occurs in exactly one congruence each, namely $s \equiv t \cdot u$ (resp., $t \cdot v_1 \cdot v \equiv \bar{s}$). In the remaining congruences in $\mathscr{P}'$ each side has the form $t \cdot y$ with $y \in X^*$. Thus, the only congruence in $\mathscr{P}'$ that can be applied to s is $s \equiv t \cdot u$, and any derivation in $\mathscr{P}'$ starting at s first leads from s to $t \cdot u$; i.e., $s \to t \cdot u\ (\mathscr{P}')$. Generally, from the structure of $\mathscr{P}'$ Lemma 4 follows.

LEMMA 4. *Every word γ in a derivation in $\mathscr{P}'$ starting at s satisfies*

$$\Phi(\gamma, s) + \Phi(\gamma, \bar{s}) + \Phi(\gamma, t) = 1.$$

In the following, it will be shown that in any repetition-free derivation in $\mathscr{P}'$ leading from s to some word $w_s \in [s]_{\mathscr{P}'}$ with $s \succ w_s$, the variable s exclusively occurs in the "start"-word s and the variable $\bar{s}$, either in the "end"-word w_s or not at all in the derivation. Furthermore, we shall see that, except for s and possibly w_s, any word in a repetition-free derivation of w_s from s in $\mathscr{P}'$ has the form $t \cdot \delta$ with $\delta \in [u]_{\mathscr{P}}$.

If some word γ_i, $i \in \mathbb{N}$, $i \geqslant 1$, in a derivation $s \to t \cdot u = \gamma_0 \to \gamma_1 \to \cdots \to \gamma_{i-1} \to \gamma_i \to \cdots\ (\mathscr{P}')$ contains the variable s, then, by Lemma 4, the variables t and $\bar{s}$ do not occur in γ_i. Because the congruence $s \equiv t \cdot u$ is the only congruence in $\mathscr{P}'$ with at least one side not containing t or $\bar{s}$, the word γ_i must be derived from γ_{i-1} by application of this congruence. For the same reason, the only way to continue from γ_i is to apply the congruence $s \equiv t \cdot u$, which causes a repetition in the resulting derivation.

Similarly, if some word γ in a repetition-free derivation in $\mathscr{P}'$ starting at s contains the variable $\bar{s}$, then there is exactly one applicable congruence, namely $t \cdot v_1 \cdot v \equiv \bar{s}$. Since this congruence is also applied last, an application of it to γ causes a repetition in the derivation. Hence, if $\Phi(\gamma, \bar{s}) = 1$, then the end of the derivation is reached, i.e., $\gamma = w_s$.

It follows that in a repetition-free derivation

$$s \to t \cdot u = \gamma_0 \to \gamma_1 \to \cdots \to \gamma_{n-1} \to \gamma_n \to w_s(\mathscr{P}')$$

the words γ_i, $i \in \{0, ..., n\}$, $n \in \mathbb{N}$, do not contain s or $\bar{s}$. The only congruences applied to γ_i, $i \in \{0, ..., n-1\}$, are the congruences $t \cdot l_i \equiv t \cdot r_i$, $i \in I_h$. Thus, any repetition-free derivation in $\mathscr{P}'$ leading from s to some w_s with $s \succ w_s$ has the form

$$s \to t \cdot u \to t \cdot \delta_1 \to \cdots \to t \cdot \delta_n \to w_s(\mathscr{P}'),$$

where $\delta_i \in [u]_{\mathscr{P}}$, $i \in I_n$, $n \in \mathbb{N}$, and $w_s = t \cdot w_t$ for some $w_t \in [u]_{\mathscr{P}}$ or $w_s = \bar{s} \cdot w$ for some $w \in X^*$ with $v_1 \cdot v \cdot w \in [u]_{\mathscr{P}}$. (Since we suppose that $s \succ w_s$, the word w_s cannot be of the form $s \cdot w$, $w \in X^*$.) In the latter case, i.e., if $\Phi(w_s, \bar{s}) = 1$, the last step of the derivation is

$$t \cdot \delta_n = t \cdot v_1 \cdot v \cdot w \to \bar{s} \cdot w = w_s.$$

In $\mathscr{P}$ we obtain the corresponding derivation

$$u \to \delta_1 \to \cdots \to \delta_n(\mathscr{P}),$$

where $\delta_n = v_1 \cdot v \cdot w$ if $\Phi(w_s, \bar{s}) = 1$.

Moreover, from the above considerations we obtain

LEMMA 5. *Let δ be a word in X^*. Then*

$$t \cdot \delta \in [s]_{\mathscr{P}'} = [t \cdot u]_{\mathscr{P}'} \quad \text{iff} \quad \delta \in [u]_{\mathscr{P}}.$$

If in $[u]_{\mathscr{P}}$ there is no v_2 that is divisible by $v_1 \cdot v$, then in any derivation in $\mathscr{P}'$ starting at s the congruence $t \cdot v_1 \cdot v \equiv \bar{s}$ cannot be applied. Since $s \succ t$, the $\succ$-minimal element m_s of $[s]_{\mathscr{P}'}$ is of the form $t \cdot w_t$, where $w_t \in X^*$ is the $\succ$-minimal element (resp., the $\succ_X$-minimal element, where $\succ_X$ is the restriction of $\succ$ to the words in X^*) of $[u]_{\mathscr{P}}$. In the case that there is a $v_2 \in [u]_{\mathscr{P}}$ divisible by $v_1 \cdot v$, from $s \succ t \succ x'$ for all $x' \in X' \backslash \{s, t\}$ it follows that $m_s = \bar{s} \cdot w$, where w is the $\succ$-minimal (resp., $\succ_X$-minimal) word in X^* such that $v_1 \cdot v \cdot w \in [u]_{\mathscr{P}}$.

Now, assume that there is a $v_2 \in [u]_{\mathscr{P}}$ with $v_2 = v_1 \cdot v \cdot w'$ for some $w' \in (Y \cup Z)^*$. Then, by Lemma 5, we have $t \cdot v_1 \cdot v \cdot w' \in [s]_{\mathscr{P}'}$, and $t \cdot v_1 \cdot v \cdot w' \equiv \bar{s} \cdot w' \bmod \mathscr{P}'$ implies $\bar{s} \cdot w' \in [s]_{\mathscr{P}'}$. Clearly, $\bar{s} \cdot w'$ is greater or equal in the term ordering $\geqslant$ than the $\succ$-minimal element m_s of $[s]_{\mathscr{P}'}$; i.e., $\bar{s} \cdot w' \geqslant m_s$. In particular, besides the variables s and t, also the variables in $X \backslash (Y \cup Z)$ do not occur in m_s, and $\Phi(m_s, \bar{s}) = 1$; i.e., $m_s = \bar{s} \cdot w$ for some $w \in (Y \cup Z)^*$ with $w' \geqslant w$.

Thus, for the $\succ$-minimal element m_s of $[s]_{\mathscr{P}'}$ we obtain $m_s = \bar{s} \cdot w$, $w \in (Y \cup Z)^*$, iff there is a $v_2 \in [u]_{\mathscr{P}}$ such that $v_2 = v_1 \cdot v \cdot w'$ for some $w' \in (Y \cup Z)^*$.

In case $m_s = \bar{s} \cdot w$ with $w \in X^*$ (no matter whether $w \in (Y \cup Z)^*$), because of the definition of m_s, the word $v_1 \cdot v \cdot w$ is $\succ$-minimal (resp., $\succ_X$-minimal) among all words in $[u]_{\mathscr{P}}$ that are of the form $v_1 \cdot v \cdot w'$, $w' \in X^*$. Since $\geqslant$ is an admissible ordering, $v_1 \cdot v \cdot w$ is minimal also with respect to divisibility among all words in $[u]_{\mathscr{P}}$ divisible by $v_1 \cdot v$.

By Proposition 6, the size of m_s is bounded by $\text{size}(u, v_1, \mathscr{P}) \cdot 2^{d \cdot k}$, and, by Proposition 5, m_s can be determined in space $(\text{size}(u, v_1, \mathscr{P}))^2 \cdot 2^{c \cdot k}$. ∎

As we have already seen the uniform word problem is a special case of the (generalized) subword problem. From the results in [MM82] we know that the uniform word problem for commutative semigroups is exponential space complete with respect to log-lin reducibility. This, together with Theorem 3, provides the following theorem.

THEOREM 4. *The (generalized) subword problem for commutative semigroups is exponential space complete with respect to log-lin reducibility.*

As an example of Theorem 3, again consider the commutative semigroup presentation

$$\mathscr{P} = \{x_1 \equiv x_2 x_3,\ x_2 x_3^3 \equiv x_1,\ x_2 \equiv x_2 x_3^4\}$$

over $X=\{x_1, x_2, x_3\}$. Furthermore, consider the words

$$u=x_1, \qquad v_1=x_1,$$

and the sets

$$Y=\{x_3\}, \qquad Z=\varnothing.$$

In this special case, the (generalized) subword problem is to decide whether there is a $v_2 \in [x_1]_{\mathscr{P}}$ such that $v_2=x_1x_3 \cdot w$ for some $w \in \{x_3\}^*$.

Using the construction of Theorem 3, we compute the reduced Gröbner basis G for the ideal

$$I := \langle s-tx_1, tx_1x_3-\bar{s}, tx_1-tx_2x_3, tx_1-tx_2x_3^3, tx_2x_3^4-tx_2\rangle$$

with respect to the lexicographic term ordering $\succcurlyeq$ satisfying

$$s \succ t \succ x_1 \succ x_2 \succ \bar{s} \succ x_3.$$

We obtain

$$G=\{\bar{s}x_3^2-\bar{s}, \bar{s}x_1-\bar{s}x_2x_3, tx_2-\bar{s}, tx_1-\bar{s}x_3, \boxed{s-\bar{s}x_3}\}.$$

The binomial $s-\bar{s}x_3$ provides the solution $w=x_3$ (resp.,

$$v_2=x_1x_3^2),$$

which can be verified by each of the following two derivations in $\mathscr{P}$:

$$u=x_1 \to x_2x_3 \to x_2x_3^5 \to x_1x_3^2=v_2(\mathscr{P}),$$
$$u=x_1 \to x_2x_3^3 \to x_1x_3^2=v_2(\mathscr{P}).$$

Furthermore, we obtain that, with respect to $\succ$ (resp., $\succ_X$) and thus, also with respect to divisibility, $x_1x_3^2$ is the minimal element of $[x_1]_{\mathscr{P}}$ that is divisible by x_1x_3.

5. THE CONTAINMENT PROBLEM AND THE EQUIVALENCE PROBLEM

The *Containment Problem* (resp., the *Equivalence Problem*) for commutative semigroups is:

Given two finite commutative semigroup presentations $\mathscr{P}$, $\mathscr{Q}$ over some finite alphabet X, and two words $u, v \in X^*$, decide whether

$$[u]_{\mathscr{P}} \subseteq [v]_{\mathscr{Q}} \qquad (\text{resp., } [u]_{\mathscr{P}}=[v]_{\mathscr{Q}}).$$

Let $\mathscr{P}$ be a finite commutative semigroup presentation over some finite alphabet $X=\{x_1, ..., x_k\}$ and u a word in X^*. Note that X^* is isomorphic to $\mathbb{N}^k$ and that

the congruence classes in $\mathbb{N}^k$ are uniformly semilinear subsets of $\mathbb{N}^k$ (see [ES69]), i.e., we can write

$$[u]_{\mathscr{P}} = \bigcup_{j=1}^{n} \left\{ a_j + \sum_{i=1}^{t} n_i b_i;\ n_i \in \mathbb{N} \text{ for } i = 1, ..., t \right\},$$

where $\{a_1, ..., a_n\} = \min([u]_{\mathscr{P}})$ and $\{b_1, ..., b_t\} = \min(P_{[u]_{\mathscr{P}}} \backslash \{0^k\})$ with

$$P_{[u]_{\mathscr{P}}} = \{x \in \mathbb{N}^k;\ u + x \in [u]_{\mathscr{P}}\};$$

the set of periods of $[u]_{\mathscr{P}}$ (min(.) denotes the minimal elements of the argument with respect to divisibility). If $\min(P_{[u]_{\mathscr{P}}} \backslash \{0^k\}) \neq \varnothing$, then we call $b_1, ..., b_t$ the minimal periods of $[u]_{\mathscr{P}}$. It follows that the congruence class $[u]_{\mathscr{P}}$ is completely determined by its minimal (with respect to divisibility) elements a_j and its minimal periods b_i. Note that, by Dickson's lemma [Dic13], the sets $\min([u]_{\mathscr{P}})$ and $\min(P_{[u]_{\mathscr{P}}} \backslash \{0^k\})$ contain only finitely many elements.

To decide whether $[u]_{\mathscr{P}} \subseteq [v]_{\mathscr{Q}}$ ($[u]_{\mathscr{P}} = [v]_{\mathscr{Q}}$), it suffices to check whether each minimal element a of $[u]_{\mathscr{P}}$ with respect to divisibility is contained in $[v]_{\mathscr{Q}}$ (and vice versa) and whether each minimal period b of $[u]_{\mathscr{P}}$ is a period of $[v]_{\mathscr{Q}}$ (and vice versa). We shall see that this can be done in space $2^{c \cdot \text{size}(u, v, \mathscr{P}, \mathscr{Q})}$.

THEOREM 5. *Let $X = \{x_1, ..., x_k\}$, $\mathscr{P} = \{l_i \equiv r_i;\ i \in I_h\}$ be a finite commutative semigroup presentation over X, and $u \in X^*$. Then there is an algorithm which generates a closed representation of $[u]_{\mathscr{P}}$ using at most space $(\text{size}(u, \mathscr{P}))^2 \cdot 2^{\bar{c} \cdot k} \leqslant 2^{c \cdot \text{size}(u, \mathscr{P})}$, where $\bar{c}$, $c > 0$ are some constants independent of u and $\mathscr{P}$.*

Proof. If $[u]_{\mathscr{P}}$ is bounded, then, by Corollary 1, there is an algorithm which generates the elements of $[u]_{\mathscr{P}}$ using at most space $(\text{size}(u, \mathscr{P}))^2 \cdot 2^{\bar{c} \cdot k}$. The size of the elements of $[u]_{\mathscr{P}}$ is bounded by $\text{size}(u, \mathscr{P}) \cdot 2^{d \cdot k}$ for some constant $d > 0$ independent of u and $\mathscr{P}$.

In the sequel, we assume that $[u]_{\mathscr{P}}$ is unbounded; i.e., the set of periods of the congruence class $[u]_{\mathscr{P}}$ consists not only of $\{0^k\}$.

In the following, we first derive an exponential space upper bound on the size of the minimal periods b_i of the uniformly semilinear set $[u]_{\mathscr{P}}$. With this upper bound, we then derive an analogous upper bound for the size of the minimal elements a_j of $[u]_{\mathscr{P}}$.

LEMMA 6. *Every minimal period b_i of $[u]_{\mathscr{P}}$ has size bounded by $\text{size}(u, \mathscr{P}) \cdot 2^{c_b \cdot k}$, where $c_b > 0$ is some constant independent of u and $\mathscr{P}$.*

Proof. The following proposition from the work in [Huy85] shows that, for any congruence class $[u]_{\mathscr{P}}$ in $\mathbb{N}^k$, in order to get an upper bound on the size of all minimal periods in $\min(P_{[u]_{\mathscr{P}}} \backslash \{0^k\})$, it suffices to look at certain minimal periods.

PROPOSITION 8 [Huy85]. *Let $P \subseteq \mathbb{N}^k$ be a subtractive submonoid, and let $\mathscr{I}$ be the set of all minimal subsets $I \subseteq I_k$ such that*

$$\min((P \backslash \{0^k\}) \cap \{(p_1, ..., p_k) \in \mathbb{N}^k;\ p_j > 0 \text{ for } j \in I,\ p_j = 0 \text{ for } j \notin I\})$$

contains exactly one element p^I. *Let* $U = \{p^I; I \in \mathscr{I}\}$. (*Note that* U *consists of at most* k *elements.*) *Then every* $p \in \min(P \backslash \{0^k\}) \backslash U$ *can be written as*

$$p = \sum_{u \in U} \varrho_u u, \qquad \varrho_u \in \mathbb{Q}^+, \quad 0 \leqslant \varrho_u < 1.$$

The set of periods $P_{[u]_{\mathscr{P}}}$ of a congruence class $[u]_{\mathscr{P}}$ is a subtractive submonoid, and thus, Proposition 8 can be applied to it. The minimal periods b_i can be written as

$$b_i = \sum_{p^I \in U} \varrho_I \cdot p^I, \qquad \varrho_I \in \mathbb{Q}^+, \quad 0 \leqslant \varrho_I \leqslant 1,$$

where U is defined as in Proposition 8. We call the elements p^I of U the *extreme minimal periods* of $[u]_{\mathscr{P}}$ and we shall show that they can be determined by the algorithm of Theorem 3.

Let I_Y be a minimal subset of I_k such that $\min((P_{[u]_{\mathscr{P}}} \backslash \{0^k\}) \cap \{(p_1, ..., p_k) \in \mathbb{N}^k; p_i > 0 \text{ for } i \in I_Y,\ p_i = 0 \text{ for } i \notin I_Y\})$ contains exactly one element p^{I_Y}. By setting $Y = \{x_i; i \in I_Y\}$, $Z = \varnothing$, and $v_1 = u$, the algorithm of Theorem 3 provides a period $p \in P_{[u]_{\mathscr{P}}}$ which is an element of $\min(P_{[u]_{\mathscr{P}}} \cap \{(p_1, ..., p_k) \in \mathbb{N}^k;\ p_i > 0 \text{ for } i \in I_Y,\ p_i = 0 \text{ for } i \notin I_Y\})$ and whose size is bounded by $\text{size}(u, \mathscr{P}) \cdot 2^{d_1 \cdot k}$ for some constant $d_1 > 0$ independent of u and $\mathscr{P}$. Because of the definition of p^{I_Y}, we get $p = p^{I_Y}$, and thus, the exponential space bound for the extreme minimal periods of $[u]_{\mathscr{P}}$ is established. Since $[u]_{\mathscr{P}}$ has at most k extreme minimal periods, by Proposition 8, the size of every minimal period b_i of $[u]_{\mathscr{P}}$ is bounded by $k \cdot \max\{\text{size}(p); p \in U\}$, where U is the set of the extreme minimal periods of $[u]_{\mathscr{P}}$. This implies, for every minimal period b_i of $[u]_{\mathscr{P}}$, $\text{size}(b_i) \leqslant \text{size}(u, \mathscr{P}) \cdot 2^{c_b \cdot k}$. ∎

The sets I_Y which belong to the extreme minimal periods of $[u]_{\mathscr{P}}$ can be determined by choosing a subset Y of X, deciding by the algorithm of Theorem 3 whether $[u]_{\mathscr{P}}$ has a period b with $b \in Y^*$, and checking that there is no proper subset Y_s of Y such that $[u]_{\mathscr{P}}$ has also a period b_s with $b_s \in Y_s^*$. Hence, by the above considerations, the extreme minimal periods of $[u]_{\mathscr{P}}$ can be determined using at most space $(\text{size}(u, \mathscr{P}))^2 \cdot 2^{c_1 \cdot k}$ for some constant $c_1 > 0$ independent of u and $\mathscr{P}$.

By Proposition 8, the set of the extreme minimal periods of $[u]_{\mathscr{P}}$ provides a bounded set of "period candidates" that contains all minimal periods b_i of $[u]_{\mathscr{P}}$. The size of each of these candidates is bounded by $\text{size}(u, \mathscr{P}) \cdot 2^{c_c \cdot k}$ for some constant $c_c > 0$ independent of u and $\mathscr{P}$. Recall that $p \in X^*$ is a period of $[u]_{\mathscr{P}}$ if $u \cdot p \equiv u \bmod \mathscr{P}$. Hence, by Proposition 3, checking the candidates for being periods of $[u]_{\mathscr{P}}$ can be done in space $(\text{size}(u, \mathscr{P}))^2 \cdot 2^{c_b' \cdot k}$, where $c_b' > 0$ is again some constant independent of u and $\mathscr{P}$. Thus, we get a closed representation of the set of periods $P_{[u]_{\mathscr{P}}}$ of $[u]_{\mathscr{P}}$ in form of a set B with $B \subseteq P_{[u]_{\mathscr{P}}}$ and $B \supseteq \{b_1, ..., b_t\}$ using at most space $(\text{size}(u, \mathscr{P}))^2 \cdot 2^{c_b' \cdot k}$.

LEMMA 7. *Every minimal element* a_j *of* $[u]_{\mathscr{P}}$ *has size bounded by* $\text{size}(u, \mathscr{P}) \cdot 2^{c_a \cdot k}$, *where* $c_a > 0$ *is some constant independent of* u *and* $\mathscr{P}$.

Proof. Given a finite commutative semigroup presentation $\mathscr{P}$ over some finite alphabet X and u a word in X^*, we call a variable $x_i \in X$ *unbounded with respect to the congruence class* $[u]_{\mathscr{P}}$ iff $u \in C(u \cdot x_i, \mathscr{P})$. Accordingly, we call $x_i \in X$ *bounded with respect to* $[u]_{\mathscr{P}}$ iff $u \notin C(u \cdot x_i, \mathscr{P})$. Note that the congruence class $[u]_{\mathscr{P}}$ is unbounded iff at least one $x_i \in X$ is unbounded with respect to $[u]_{\mathscr{P}}$.

For determining the upper bound for the size of the minimal elements a_j of $[u]_{\mathscr{P}}$, we project $[u]_{\mathscr{P}}$ onto the bounded coordinates. The ith coordinate, $i \in I_k$, is bounded in $[u]_{\mathscr{P}} \subseteq \mathbb{N}^k$ if the variable x_i is bounded with respect to $[u]_{\mathscr{P}}$ in X^*. The set $X_b \subseteq X$ of the bounded variables can be determined by the algorithm of Theorem 3 (or Theorem 1) using at most space $(\text{size}(u, \mathscr{P}))^2 \cdot 2^{c_v \cdot k}$ for some constant $c_v > 0$ independent of u and $\mathscr{P}$. Note that the periods of $[u]_{\mathscr{P}}$ do not contain any bounded variable, i.e., $\Phi(p, x) = 0$ for all $p \in P_{[u]_{\mathscr{P}}}$, $x \in X_b$.

Let w_b denote the projection of any word $w \in X^*$ and $\mathscr{P}_b$ the projection of $\mathscr{P}$ onto the bounded coordinates in X_b. Then the congruence class $[u_b]_{\mathscr{P}_b}$ is bounded, and, by Corollary 1, there is an algorithm which generates the elements of $[u_b]_{\mathscr{P}_b}$ using at most space $(\text{size}(u_b, \mathscr{P}_b))^2 \cdot 2^{c_2' \cdot k} \leqslant (\text{size}(u, \mathscr{P}))^2 \cdot 2^{c_2' \cdot k}$, where $c_2' > 0$ is some constant independent of u and $\mathscr{P}$. The size of the elements of $[u_b]_{\mathscr{P}_b}$ is bounded by $\text{size}(u, \mathscr{P}) \cdot 2^{d_2' \cdot k}$ for some constant $d_2' > 0$ independent of u and $\mathscr{P}$.

Let $([u]_{\mathscr{P}})_b$ denote the projection of $[u]_{\mathscr{P}}$ onto the bounded coordinates in X_b. Then $([u]_{\mathscr{P}})_b = [u_b]_{\mathscr{P}_b}$. In particular, the projection $(a_j)_b$ of each of the minimal elements a_j of $[u]_{\mathscr{P}}$ onto the bounded coordinates is an element of $[u_b]_{\mathscr{P}_b}$, and each element of $[u_b]_{\mathscr{P}_b}$ is the projection of at least one minimal element a_j. For each word $\bar{u}_b \in [u_b]_{\mathscr{P}_b}$, we determine some $\bar{u} = \bar{u}_b \cdot t \in [u]_{\mathscr{P}}$, $t \in (X - X_b)^*$, as "representative" of the elements v of $[u]_{\mathscr{P}}$ with $v_b = \bar{u}_b$. By Theorem 3, this computation requires at most space $(\text{size}(u, \mathscr{P}))^2 \cdot 2^{c_2'' \cdot k}$, and the size of $\bar{u}$ is bounded by $\text{size}(u, \mathscr{P}) \cdot 2^{d_2'' \cdot k}$ for some constants c_2'', $d_2'' > 0$ independent of u and $\mathscr{P}$.

In the following, we show that for each $\bar{u}$ all minimal elements a_j in $[u]_{\mathscr{P}}$ with $(a_j)_b = \bar{u}_b$ have size bounded by $\text{size}(u, \mathscr{P}) \cdot 2^{c_a \cdot k}$. We look at the words in X^* as vectors in $\mathbb{N}^k$. Let $Z(\bar{u}) \subseteq \mathbb{Z}^k$ denote the set

$$Z(\bar{u}) = \left\{ \bar{u} + \sum_{i=1}^{t} z_i b_i;\ z_i \in \mathbb{Z} \text{ for } i = 1, ..., t \right\}$$

with b_i, $i \in I_t$, the minimal periods of the congruence class $[u]_{\mathscr{P}}$. Because $[u]_{\mathscr{P}} = [\bar{u}]_{\mathscr{P}}$ is a uniformly semilinear set, for all minimal elements a_j of $[u]_{\mathscr{P}}$ with $(a_j)_b = \bar{u}_b$, we have $a_j \in Z(\bar{u})$. Let $a \in \mathbb{N}^k$ be some minimal element of $[u]_{\mathscr{P}}$ with respect to divisibility such that $a_b = \bar{u}_b$ and assume that some of its coordinates are greater than $2^{\text{size}(u, \mathscr{P}) \cdot 2^{c_2} \cdot k}$, where $c_2 > 0$ is some constant specified below. Since $[u]_{\mathscr{P}} \subseteq C(u, \mathscr{P})$, in particular, $a \in C(u, \mathscr{P})$, there is some $h_a \in \min(C(u, \mathscr{P}))$ such that h_a divides a. Because $h_a \in C(u, \mathscr{P})$, we obtain $P_{[u]_{\mathscr{P}}} \subseteq P_{[h_a]_{\mathscr{P}}}$ implying $h_a + P_{[u]_{\mathscr{P}}} \subseteq [h_a]_{\mathscr{P}}$ and, moreover,

$$v + P_{[u]_{\mathscr{P}}} = \left\{ v + \sum_{i=1}^{t} n_i b_i;\ n_i \in \mathbb{N} \text{ for } i = 1, ..., t \right\} \subseteq [v]_{\mathscr{P}} \qquad \text{for all } v \in h_a + \mathbb{N}^k.$$

In the proof of Theorem 1, we have presented an algorithm that generates the elements of $\min(C(u, \mathscr{P}))$ using at most space $(\text{size}(u, \mathscr{P}))^2 \cdot 2^{c_2''' \cdot k}$, where $c_2''' > 0$ is some constant independent of u and $\mathscr{P}$. The size of the elements of $\min(C(u, \mathscr{P}))$ is bounded by $\text{size}(u, \mathscr{P}) \cdot 2^{d_2''' \cdot k}$ for some constant $d_2''' > 0$ independent of u and $\mathscr{P}$.

Consider the intersection $(h_a + \mathbb{N}^k) \cap Z(\bar{u})$, which is nonempty (since it contains a). This intersection is a set of the form $M + P_{[u]_{\mathscr{P}}}$, where M is the set of all its minimal elements with respect to divisibility. Because of the exponential space upper bounds for h_a, $\bar{u}$, and for the minimal periods b_i of $[u]_{\mathscr{P}}$, every element of M has coordinates bounded by $2^{\text{size}(u, \mathscr{P}) \cdot 2^{c_2} \cdot k}$, where $c_2 > 0$ is some constant independent of u and $\mathscr{P}$.

There exists an element a' in M such that $a' + P_{[u]_{\mathscr{P}}}$ contains a. Then $a = a' + t$ for some $t \in \mathbb{N}^k \backslash \{0^k\}$. Since $a \in [u]_{\mathscr{P}}$ and by construction $a' \equiv a \bmod \mathscr{P}$, we have $a' \in [u]_{\mathscr{P}}$, which provides a contradiction to the minimality of a.

Hence, the size of the minimal elements a_j of the uniformly semilinear set $[u]_{\mathscr{P}}$ is bounded by $\text{size}(u, \mathscr{P}) \cdot 2^{c_a \cdot k}$.

By Proposition 3, deciding for some word a whose size is bounded by $\text{size}(u, \mathscr{P}) \cdot 2^{c_a \cdot k}$ whether it is an element of $[u]_{\mathscr{P}}$, i.e., $a \equiv u \bmod \mathscr{P}$, uses at most space $(\text{size}(u, \mathscr{P}))^2 \cdot 2^{c_a' \cdot k}$, where $c_a' > 0$ is some constant independent of u and $\mathscr{P}$.

Putting everything together, we have shown that a closed representation of $[u]_{\mathscr{P}}$ as a uniformly semilinear set can be generated using at most space $(\text{size}(u, \mathscr{P}))^2 \cdot 2^{\bar{c} \cdot k}$. ▌

We are now able to prove an exponential space upper bound for the containment and the equivalence problems for commutative semigroups.

THEOREM 6. *Let $\mathscr{P}$, $\mathscr{Q}$ be two finite commutative semigroup presentations over some finite alphabet $X = \{x_1, ..., x_k\}$, and u, v two words in X^*. Then there is an algorithm which decides whether $[u]_{\mathscr{P}}$ is contained in (is equal to) $[v]_{\mathscr{Q}}$ using at most space $(\max\{\text{size}(u, \mathscr{P}), \text{size}(v, \mathscr{Q})\})^2 \cdot 2^{\bar{c} \cdot k} \leqslant 2^{c \cdot \text{size}(u, v, \mathscr{P}, \mathscr{Q})}$, where $\bar{c}$, $c > 0$ are some constants independent of u, v, $\mathscr{P}$, and $\mathscr{Q}$.*

Proof. Containment of $[u]_{\mathscr{P}}$ in $[v]_{\mathscr{Q}}$ can be decided by the exponential space algorithm (for suitable constants c and c') given in Fig. 3. Since the word problems occurring in this algorithm can, by Proposition 3, be decided using at most space $(\max\{\text{size}(u, \mathscr{P}), \text{size}(v, \mathscr{Q})\})^2 \cdot 2^{\bar{c} \cdot k}$, this algorithm can be implemented on a Turing machine whose space is bounded by $(\max\{\text{size}(u, \mathscr{P}), \text{size}(v, \mathscr{Q})\})^2 \cdot 2^{\bar{c} \cdot k}$. Because $[u]_{\mathscr{P}} = [v]_{\mathscr{Q}}$ iff $[u]_{\mathscr{P}} \subseteq [v]_{\mathscr{Q}}$ and $[u]_{\mathscr{P}} \supseteq [v]_{\mathscr{Q}}$, this space bound also holds for the equivalence problem. ▌

THEOREM 7. *The containment problem and the equivalence problem for commutative semigroups are exponential space complete with respect to log-lin reducibility.*

Proof. Let $\mathscr{P}$, $\mathscr{Q}$ be two finite commutative semigroup presentations over some finite alphabet X and u, v two words in X^*. If $\mathscr{Q} = \varnothing$ is the empty commutative semigroup presentation, then $[v]_{\mathscr{Q}} = \{v\}$, and $[v]_{\mathscr{Q}} \subseteq [u]_{\mathscr{P}}$ iff $v \equiv u \bmod \mathscr{P}$. If $\mathscr{Q} = \mathscr{P}$, then $[v]_{\mathscr{Q}} = [v]_{\mathscr{P}}$, and $[v]_{\mathscr{P}} = [u]_{\mathscr{P}}$ iff $v \equiv u \bmod \mathscr{P}$. Thus, the uniform word problem for commutative semigroups, which is known to be exponential

Deciding the Containment Problem for Commutative Semigroups

Input: $u, v \in X^*$; $\mathcal{P}, \mathcal{Q}$ two commutative semigroup presentations over X

Output: $[u]_{\mathcal{P}} \overset{?}{\subseteq} [v]_{\mathcal{Q}}$

```
if u ≡ v mod Q then
  for each a ∈ X* with degree ≤ 2^(max{size(u,P), size(v,Q)})^2·2^(c·k) do
    if (a ≡ u mod P and a ≢ v mod Q) then reject end_if
  end_for
  for each b ∈ X* with degree ≤ 2^(max{size(u,P), size(v,Q)})^2·2^(c'·k) do
    if (u ≡ u·b mod P and v ≢ v·b mod Q) then reject end_if
  end_for
  accept
else
  reject
end_if
```

FIG. 3. Algorithm for deciding the containment problem for commutative semi-groups

space complete (see [MM82]) reduces to the containment problem and the equivalence problem for commutative semigroups. Together with Theorem 22 this fact establishes the exponential space completeness of the containment problem and the equivalence problem for commutative semigroups. ▮

As an example for Theorem 5, again consider the commutative semigroup presentation

$$\mathcal{P} = \{x_1 \equiv x_2x_3,\ x_2x_3^3 \equiv x_1,\ x_2 \equiv x_2x_3^4\}$$

over $X = \{x_1, x_2, x_3\}$. We want to generate a closed representation of the congruence class

$$[x_1]_{\mathcal{P}}$$

as a uniformly semilinear set.

From Section 4 we already know that $x_1 \in C(x_1x_3, \mathcal{P})$, i.e., the variable x_3 is unbounded with respect to $[x_1]_{\mathcal{P}}$, and, hence, $[x_1]_{\mathcal{P}}$ is unbounded. Now, we examine the variables x_1 and x_2.

In order to decide whether x_1 is bounded with respect to $[x_1]_{\mathcal{P}}$, we set $v_1 = u = x_1$, $Y = \{x_1\}$, $Z = X \setminus Y = \{x_2, x_3\}$ and compute the reduced Gröbner basis G for the ideal

$$I := \langle s - tx_1,\ tx_1^2 - \bar{s},\ tx_2x_3 - tx_1,\ tx_2x_3^3 - tx_1,\ tx_2x_3^4 - tx_2 \rangle$$

with respect to the lexicographic term ordering $\succcurlyeq$ satisfying

$$s \succ t \succ \bar{s} \succ x_2 \succ x_3 \succ x_1.$$

We obtain

$$G = \{\bar{s}x_3^2 - \bar{s},\ \bar{s}x_2 - \bar{s}x_1x_3,\ tx_1^2 - \bar{s},\ tx_1x_3^2 - tx_1,\ tx_2 - tx_1x_3,\ \boxed{s - tx_1}\}.$$

The second term of the binomial $s - tx_1$ tells us, since it contains the variable t and no $\bar{s}$, that there is no word in $[x_1]_{\mathscr{P}}$ divisible by x_1^2; i.e., x_1^2 cannot be covered in $[x_1]_{\mathscr{P}}$. Thus, x_1 is bounded with respect to $[x_1]_{\mathscr{P}}$. Furthermore, we obtain that x_1 is the $\succ$-minimal element (resp., the $\succ_X$-minimal element, where $\succ_X$ is the restriction of $\succ$ to the words in X^*) of $[x_1]_{\mathscr{P}}$.

For the examination of x_2, we set $v_1 = u = x_1$, $Y = \{x_2\}$, $Z = X \setminus Y = \{x_1, x_3\}$ and compute the reduced Gröbner basis G for the ideal

$$I := \langle s - tx_1,\ tx_1x_2 - \bar{s},\ tx_1 - tx_2x_3,\ tx_1 - tx_2x_3^3,\ tx_2x_3^4 - tx_2\rangle$$

with respect to the lexicographic term ordering $\succcurlyeq$ satisfying

$$s \succ t \succ \bar{s} \succ x_1 \succ x_3 \succ x_2.$$

We obtain

$$G = \{\bar{s}x_3^2 - \bar{s},\ \bar{s}x_1 - \bar{s}x_2x_3,\ tx_2^2 - \bar{s}x_3,\ tx_2x_3^2 - tx_2,\ tx_1 - tx_2x_3,\ \boxed{s - tx_2x_3}\}.$$

The binomial $s - tx_2x_3$ tells us that there is no word in $[x_1]_{\mathscr{P}}$ divisible by x_1x_2. Thus, x_2 is bounded with respect to $[x_1]_{\mathscr{P}}$. Furthermore, from the binomial $s - tx_2x_3$ we obtain that x_2x_3 is the $\succ$-minimal (resp., $\succ_X$-minimal) element of $[x_1]_{\mathscr{P}}$.

Since the variables x_1 and x_2 are bounded with respect to $[x_1]_{\mathscr{P}}$, whereas x_3 is unbounded with respect to $[x_1]_{\mathscr{P}}$, any period ($\neq 1_{X^*}$) of $[x_1]_{\mathscr{P}}$ is a power of x_3. At the end of Section 4, we obtained that x_3^2 is a period of $[x_1]_{\mathscr{P}}$. It is minimal with respect to divisibility among all periods of $[x_1]_{\mathscr{P}}$ divisible by x_3. Hence, we conclude that $[x_1]_{\mathscr{P}}$ has exactly one minimal period: x_3^2.

It remains to determine the minimal (with respect to divisibility) elements of $[x_1]_{\mathscr{P}}$. According to the construction of Theorem 5, we project $[x_1]_{\mathscr{P}}$ onto the bounded variables x_1 and x_2, getting the bounded congruence class $[x_1]_{\mathscr{P}_b}$ with $\mathscr{P}_b = \{x_1 \equiv x_2\}$. Using the construction of Corollary 1 (resp., Theorem 1), we generate the elements of $[x_1]_{\mathscr{P}_b}$. We compute the reduced Gröbner basis G_b for the ideal

$$\begin{aligned} I_b := \langle & sy_1z_1 - sx_1,\ sy_2z_2 - sx_2,\\ & sy_1 - t,\ sx_1 - m,\\ & sy_1 - sy_2,\\ & tz_1 - tz_2\rangle \end{aligned}$$

with respect to the lexicographic term ordering $\succcurlyeq$ satisfying

$$t \succ z_1 \succ z_2 \succ y_1 \succ y_2 \succ s \succ x_1 \succ x_2 \succ m.$$

We obtain

$$G_b = \{mx_1 - mx_2,\ \boxed{sx_2 - m},\ \boxed{sx_1 - m},\ my_1 - my_2,\ sy_1 - sy_2,$$
$$my_2z_2 - mx_2,\ sy_2z_2 - m,\ mz_1 - mz_2,\ sy_2z_1 - m,\ t - sy_2\}.$$

The binomials in the boxes provide the result $[x_1]_{\mathscr{P}_b} = \{x_1, x_2\}$.

Now, we have to compute all minimal (with respect to divisibility) elements a_j in $[x_1]_{\mathscr{P}}$ with $(a_j)_b = x_1$ and with $(a_j)_b = x_2$; i.e., we have to determine the minimal exponents $e_1, e_2 \in \mathbb{N}$ such that $x_1x_3^{e_1} \in [x_1]_{\mathscr{P}}$ and $x_2x_3^{e_2} \in [x_1]_{\mathscr{P}}$. Since $x_1 \in [x_1]_{\mathscr{P}}$, we trivially get $e_1 = 0$. To determine e_2, we use the algorithm of Theorem 3 with $u = x_1$, $v_1 = x_2$, $Y = \varnothing$, and $Z = \{x_3\}$. With this setting of v_1, Y, and Z the (generalized) subword problem is to decide whether there is a $v_2 \in [x_1]_{\mathscr{P}}$ such that $v_2 = x_2 \cdot w$ for some $w \in \{x_3\}^*$. We compute the reduced Gröbner basis G for the ideal

$$I := \langle s - tx_1,\ tx_2 - \bar{s},\ tx_1 - tx_2x_3,\ tx_1 - tx_2x_3^3,\ tx_2x_3^4 - tx_2 \rangle$$

with respect to the lexicographic term ordering $\succcurlyeq$ satisfying

$$s \succ t \succ x_1 \succ x_2 \succ \bar{s} \succ x_3.$$

We obtain

$$G = \{\bar{s}x_3^2 - \bar{s},\ \bar{s}x_1 - \bar{s}x_2x_3,\ tx_2 - \bar{s},\ tx_1 - \bar{s}x_3,\ \boxed{s - \bar{s}x_3}\}.$$

The binomial $s - \bar{s}x_3$ tells us that x_2x_3 is among all words in $[x_1]_{\mathscr{P}}$ of the form $x_2x_3^e$, $e \in \mathbb{N}$, the one with the smallest exponent e. Hence, we have $e_2 = 1$.

Putting everything together, we get

$$[x_1]_{\mathscr{P}} = \{x_1x_3^{2n_1},\ x_2x_3^{2n_2+1};\ n_1, n_2 \in \mathbb{N}\}.$$

6. CONCLUSION

The results obtained in this paper provide a $2^{c \cdot n}$ space upper bound on the coverability (in a generalized form), the subword (in a generalized form), the containment and the equivalence problems for commutative semigroups, where n is the size of the problem instance, and c is some problem independent constant. This space bound is optimal up to the size of the constant c.

Concerning the equivalence problem we closed the gap between the $2^{c' \cdot n \cdot \log n}$ space upper bound shown in [Huy85] and the exponential space lower bound resulting from the exponential space completeness of the uniform word problem established in [MM82].

An immediate consequence of the complexity bound for our variant of the coverability problem is an analogous upper bound for the finite enumeration problem and also for the finite containment and the finite equivalence problems for commutative semigroups. For an investigation of the finite containment problem for commutative semi-Thue systems, or equivalently, general (not necessarily reversible) Petri nets, (see [MM81]).

Commutative Thue systems permit closed representations of their state space (even if infinite) as semilinear sets. Thus, our algorithms can also be applied in algorithms investigating the behavior of such systems, like bisimulation problems [Par81].

Received February 26, 1998

REFERENCES

[Bir67] Biryukov, A. P. (1967), Some algorithmic problems for finitely defined commutative semigroups, *Siberian Math. J.* **8**, 384–391.

[Buc65] Buchberger, B. (1965), "Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal," Ph.D. thesis, University of Innsbruck.

[Dic13] Dickson, L. E. (1913), Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors, *Amer. J. Math.* **35**, 413–422.

[Dub90] Dubé, T. W. (1990), The structure of polynomial ideals and Gröbner bases, *SIAM J. Comput.* **19**(4), 750–773.

[ES69] Eilenberg, S. and Schützenberger, M. P. (1969), Rational sets in commutative monoids, *J. Algebra* **13**, 173–191.

[Emi63] Emiličev, V. A. (1963), On algorithmic decidability of certain mass problems in the theory of commutative semigroups, *Sibirsk. Mat. Ž.* **4**, 788–798. [Russian]

[Hac76] Hack, M. (1976), The equality problem for vector addition systems is undecidable, *Theoret. Comput. Sci.* **2**, 77–95.

[Hen22] Hentzelt, K. (1922), Zur Theorie der Polynomideale und Resultanten, *Math. Ann.* **88**, 53–79.

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

[Hil90] Hilbert, D. (1890), Über die Theorie der algebraischen Formen, *Math. Ann.* **36**, 473–534.

[Huy85] Huynh, D. T. (1985), The complexity of the equivalence problem for commutative semigroups and symmetric vector addition systems, *in* "Proceedings of the 17th Ann. ACM Symposium on Theory of Computing, Providence, RI," pp. 405–412, ACM Press, New York.

[Kön03] König, J. (1903), "Einleitung in die allgemeine Theorie der algebraischen Größen," Teubner, Leipzig.

[KM96] Koppenhagen, U. and Mayr, E. W. (1996), An optimal algorithm for constructing the reduced Gröbner basis of binomial ideals, *in* "Proceedings of the International Symposium on Symbolic and Algebraic Computation, ISSAC'96," pp. 55–62, ACM Press, New York.

[Lip76] Lipton, R. J. (1976), "The Reachability Problem Requires Exponential Space," Research Report 62, Computer Science Dept., Yale University.

[Mal58] Malcev, A. I. (1958), On homomorphisms of finite groups, *Ivanov. Gos. Ped. Inst. Učen. Zap.* **18**, 49–60. [Russian]

[Mar47] Markov, A. (1947), The impossibility of certain algorithms in the theory of associative systems, *Dokl. Akad. Nauk SSSR* **5**, 587–590.

[May81] Mayr, E. W. (1981), An algorithm for the general Petri net reachability problem, *in* "Proceedings of the 13th Ann. ACM Symposium on Theory of Computing, STOC '81, Milwaukee, WI, May 11–13, 1981," pp. 238–246, ACM Press, New York.

[MM81] Mayr, E. W. and Meyer, A. (1981), The complexity of the finite containment problem for Petri nets, *J. Assoc. Comput. Mach.* **28**(3), 561–576.

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

[Par81] Park, D. (1981), Concurrency and automata on infinite sequences, *in* "Proceedings of the 5th GI Conference on Theoretical Computer Science," Lect. Notes in Comput. Sci., Vol. 104, pp. 167–183, Springer-Verlag, New York.

[Rac78] Rackoff, C. (1978), The covering and boundedness problems for vector addition systems, *Theor. Comput. Sci.* **6**(2), 223–231.

[Rob85] Robbiano, L. (1985), Term orderings on the polynomial ring, *in* "Proceedings of the 10th European Conference on Computer Algebra, EUROCAL'85, Vol. 2," Lect. Notes in Comput. Sci., Vol. 204, pp. 513–517, Springer-Verlag, Berlin/Heidelberg/New York/Tokyo.

[Tai68] Taiclin, M. A. (1968), Algorithmic problems for commutative semigroups, *Soviet Math. Dokl.* **9**, 201–204.

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