The Complexity of the Coverability, the Containment, and the Equivalence Problems for Commutative Semigroups

Ulla Koppenhagen and 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/

Abstract. In this paper, we present optimal decision procedures for the coverability, 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. 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 *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 $\mathcal{P}$ over X and two words u, $v_1 \in X^*$, the (ordinary) coverability problem is the problem of deciding whether there is a derivation of some $v_2 \in X^*$ from v_1 in $\mathcal{P}$ such that u divides v_2. By the results in [MM82], which exhibit the exponential space completeness of the uniform word problem for commutative semigroups, deciding the coverability problem requires at least space $2^{d \cdot \text{size}(u,\mathcal{P})}$ for some constant $d > 0$ independent of u and $\mathcal{P}$. In [Rac78], Rackoff [Rac78] obtained a $2^{c \cdot \text{size}(u,\mathcal{P}) \cdot \log(\text{size}(u,\mathcal{P}))}$ space upper bound for these problems, where again $c > 0$ is some constant independent of u and $\mathcal{P}$. Until now it has been an open problem whether the gap between the $2^{c \cdot \text{size}(u,\mathcal{P}) \cdot \log(\text{size}(u,\mathcal{P}))}$ upper and the $2^{d \cdot \text{size}(u,\mathcal{P})}$ 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 for 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.

Given two commutative semi-Thue systems $\mathcal{P}$, $\mathcal{Q}$ 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 $\mathcal{P}$ is contained in (is equal to) the reachability set of v in $\mathcal{Q}$. In [Hac76], these two problems were shown to be undecidable. The situation changes, however, when one considers commutative Thue systems, or commutative semigroups [Bir67, Tai68]. In [Huy85], Huynh exhibited decision algorithms for the containment and the equivalence problems for commutative semigroups, which operate in space $2^{d \cdot \text{size}(u,v,\mathcal{P},\mathcal{Q}) \cdot \log(\text{size}(u,v,\mathcal{P},\mathcal{Q}))}$, where $d > 0$ is some constant independent of u, v, $\mathcal{P}$ and $\mathcal{Q}$. We are able to show a $2^{c \cdot \text{size}(u,v,\mathcal{P},\mathcal{Q})}$ space upper bound for deciding the containment and the equivalence problems for commutative semigroups, with $c > 0$ some constant independent of u, v, $\mathcal{P}$ and $\mathcal{Q}$. We prove that there is an algorithm which generates a uniformly semilinear representation of any congruence class $[u]_{\mathcal{P}}$ using at most space $2^{c' \cdot \text{size}(u,\mathcal{P})}$. To decide whether $[u]_{\mathcal{P}} \subseteq [v]_{\mathcal{Q}}$ ($[u]_{\mathcal{P}} = [v]_{\mathcal{Q}}$), it has to be checked whether each minimal element a of $[u]_{\mathcal{P}}$ w.r.t. divisibility is contained in $[v]_{\mathcal{Q}}$ (and vice versa) and whether each minimal period b of $[u]_{\mathcal{P}}$ is a period of $[v]_{\mathcal{Q}}$ (and vice versa). We shall see that this can be done in space $2^{c \cdot \text{size}(u,v,\mathcal{P},\mathcal{Q})}$. Thus, the gap between the upper space bound of Huynh and the exponential space lower bound resulting from [MM82] is closed

2 Basic Concepts

2.1 Definitions

Let X denote the finite set $\{x_1, \ldots, x_k\}$, and[1] $\mathbb{Q}[X]$ the (commutative) ring of polynomials with indeterminates $x_1, \ldots, x_k$ and rational coefficients. A *term* t in $x_1, \ldots, x_k$ is a product of the form $t = x_1^{e_1} \cdot x_2^{e_2} \cdots x_k^{e_k}$, with $(e_1, e_2, \ldots, e_k) \in \mathbb{N}^k$ the *degree vector* of t. By the *degree* $\deg(t)$ of a term t we shall mean the integer $e_1 + e_2 + \ldots + e_k$. Each *polynomial* $f(x_1, \ldots, x_k) \in \mathbb{Q}[X]$ is a finite sum $f(x_1, \ldots, x_k) = \sum_{i=1}^{n} a_i \cdot t_i$, with $a_i \in \mathbb{Q} \setminus \{0\}$ the coefficient of the ith term t_i of f. The product $m_i = a_i \cdot t_i$ is called the ith *monomial* of the polynomial f. The degree of a polynomial is the maximum of the degrees of its terms. For $f_1, \ldots, f_h \in \mathbb{Q}[X]$, $\langle f_1, \ldots, f_h \rangle \subseteq \mathbb{Q}[X]$ denotes the ideal generated by $\{f_1, \ldots, f_h\}$ that is[2] $\langle f_1, \ldots, f_h \rangle := \left\{ \sum_{i=1}^{h} p_i f_i;\ p_i \in \mathbb{Q}[X] \text{ for } i \in I_h \right\}$. Whenever $I = \langle f_1, \ldots, f_h \rangle$, $\{f_1, \ldots, f_h\}$ is called a *basis* of I.

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

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

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

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

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

If $(d_1,\ldots,d_k) > (e_1,\ldots,e_k)$, we say that the term $x_1^{d_1}\cdots x_k^{d_k}$ is *greater in the term ordering* than the term $x_1^{e_1}\cdots x_k^{e_k}$ (written $x_1^{d_1}\cdots x_k^{d_k} \succ x_1^{e_1}\cdots x_k^{e_k}$).

For a polynomial $f(x_1,\ldots,x_k) = \sum_{i=1}^{n} a_i \cdot t_i$ we always assume that $t_1 \succ t_2 \succ \ldots \succ t_n$. 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 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 $\succeq$ 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. $\succeq$), 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 any other polynomial in the basis.

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

Let $\mathcal{P} = \{l_i \equiv r_i;\ i \in I_h\}$ be some (finite) commutative semigroup presentation with $l_i, r_i \in X^*$ for $i \in I_h$. We say that a word $v \in X^*$ *is derived in one step* from $u \in X^*$ (written $u \to v\ (\mathcal{P})$) by application of the congruence $(l_i \equiv r_i) \in \mathcal{P}$ iff, for some $w \in X^*$, we have $u = wl_i$ and $v = wr_i$, or $u = wr_i$ and $v = wl_i$ (note, since '$\equiv$' is symmetric, '$\to$' is symmetric). The word u *derives* v, written $u \equiv v \bmod \mathcal{P}$, 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 $u \xrightarrow{*} v\ (\mathcal{P})$ and $u \neq v$. A sequence $(u_0,\ldots,u_n)$ of words $u_i \in X^*$ with $u_i \to u_{i+1}\ (\mathcal{P})$ for $i = 0,\ldots,n-1$, is called a *derivation* (of length n) of u_n from u_0 in $\mathcal{P}$. The *congruence class* of $u \in X^*$ modulo $\mathcal{P}$ is the set $[u]_{\mathcal{P}} = \{v \in X^*;\ u \equiv v \bmod \mathcal{P}\}$.

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

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

We call such an ideal, *i.e.*, an ideal that has a basis consisting only of differences of two terms, a *binomial ideal* (see [KM96b]). By looking at Buchberger's algorithm [Buc65] it is not hard to see that the reduced Gröbner basis of a binomial ideal still consists only of binomials.

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

2.2 The Basic Problems and Their Complexity

The Uniform Word Problem, the Polynomial Ideal Membership Problem The *uniform word problem* for commutative semigroups is the problem of deciding for a commutative semigroup presentation $\mathcal{P}$ over some alphabet X, and two words $u, v \in X^*$ whether $u \equiv v \bmod \mathcal{P}$. The *polynomial ideal membership problem* is the problem of deciding for given polynomials $f, f_1, \ldots, f_h \in \mathbb{Q}[X]$ whether $f \in \langle f_1, \ldots, f_h \rangle$.

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

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

Proposition 2. [Her26] *Let $X = \{x_1, \ldots, x_k\}$, $f, f_1, \ldots, f_h \in \mathbb{Q}[X]$, and $d := \max\{\deg(f_i);\ i \in I_h\}$. If $f \in \langle f_1, \ldots, f_h \rangle$, then there exist $p_1, \ldots, p_h \in \mathbb{Q}[X]$ such that (i) $f = \sum_{i=1}^{h} p_i f_i$;*

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

The Reduced Gröbner Basis of Binomial Ideals

Proposition 3. [KM96b] *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ i \in I_h\}$ with $l_i, r_i \in X^*$ for all $i \in I_h$, and let $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ be the reduced Gröbner basis of the ideal $I(\mathcal{P})$ w.r.t. some admissible term ordering $\succeq$ ($h_i \succ m_i$ for all $i \in I_r$). Then*

(i) m_i is the minimal element (w.r.t. $\succ$) of the congruence class $[h_i]_{\mathcal{P}}$, $i \in I_r$.

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

By size$(\cdot)$ we shall denote the size of the representation of the input in any standard encoding.

Proposition 4. [KM96b] *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ i \in I_h\}$ with $l_i, r_i \in X^*$ for all $i \in I_h$, and $\succeq$ some admissible term ordering. Then there is an algorithm which generates the reduced Gröbner basis $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ of the binomial ideal $I(\mathcal{P})$ using at most space $(\text{size}(\mathcal{P}))^2 \cdot 2^{\bar{c} \cdot k} \leq 2^{c \cdot \text{size}(\mathcal{P})}$, where $\bar{c}, c > 0$ are some constants independent of $\mathcal{P}$.*

Proposition 5. [Dub90] *Let $F = \{f_1, \ldots, f_h\} \subset \mathbb{Q}[X] = \mathbb{Q}[x_1, \ldots, x_k]$, $I = \langle f_1, \ldots, f_h \rangle$ the ideal of $\mathbb{Q}[X]$ generated by F, and let d be the maximum degree of any $f \in F$. Then for any admissible term ordering $\succeq$, the degree of polynomials required in a Gröbner basis for I w.r.t. $\succeq$ is bounded by $2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$*

The Subword Problem Let $X = \{x_1, \ldots, x_k\}$ be some finite alphabet, $\mathcal{P} = \{l_i \equiv r_i;\ i \in I_h\}$ a finite commutative semigroup presentation over X, and u, v_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 $X_{\overline{v_1}} = X \setminus X_{v_1}$. Furthermore, let Y, Z be subsets of X with $Y \cap Z = \emptyset$. W.l.o.g. the variables can be renamed such that this partition of X is determined by some $l, l_0, l_1, l_2, l_3 \in I_k$ providing, for the case $1 < l_0 < l_1 < l < l_2 < l_3 < k$, the following picture:

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

The *Subword Problem* for commutative semigroups is: 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 $l_1 \leq l_2$ resp., $v_2 = v_1 \cdot w$ for some $w \in Z^*$ if $l_1 > l_2$.

Theorem 6. [KM96a] *Let $X = \{x_1, \ldots, x_k\}$ and $\mathcal{P} = \{l_i \equiv r_i;\ i \in I_h\}$ 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 $v_2 \in [u]_{\mathcal{P}}$ 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 $Y = \{x_{l_1}, x_{l_1+1}, \ldots, x_{l_2}\}$ 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 $\mathcal{P}$.*

If there is a v_2 as described in the theorem, the provided v_2 is minimal w.r.t. divisibility among all words in $[u]_{\mathcal{P}}$ that are divisible by $v_1 \cdot v$ and its size is bounded by $\mathrm{size}(u, v_1, \mathcal{P}) \cdot 2^{d \cdot k}$ for some constant $d > 0$ independent of u, v_1, and $\mathcal{P}$.

3 The Coverability Problem

Let $\mathcal{P}$ 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 $\mathcal{P}$, *i.e.*, the set

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

is called the *covering set of u in $\mathcal{P}$*. If a word $v \in X^*$ is an element of $C(u, \mathcal{P})$, 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 $C(u, \mathcal{P})$. Thus, for a closed representation of $C(u, \mathcal{P})$, it suffices to determine the set of minimal elements w.r.t divisibility of $C(u, \mathcal{P})$, denoted by $\min(C(u, \mathcal{P}))$.

The *Coverability Problem* for commutative semigroups is: Given a finite commutative semigroup presentation $\mathcal{P}$ over some finite alphabet X and a word $u \in X^*$, generate a closed representation of the covering set of u in $\mathcal{P}$.

Theorem 7. *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ i \in I_h\}$ 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 $C(u, \mathcal{P})$ of u in $\mathcal{P}$ 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 $2k+3$ new variables m, s, t, $y_1, \ldots, y_k$, and $z_1, \ldots, z_k$. Let $X' = X \cup \{m, s, t, y_1, \ldots, y_k, z_1, \ldots, z_k\}$. 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

$$\begin{aligned} s \cdot x_j &\equiv s \cdot y_j \cdot z_j, \quad \text{for} \quad j = 1, \ldots, k, && (1)\\ s \cdot y(u) &\equiv t, && (2)\\ s \cdot u &\equiv m, && (3) \end{aligned}$$

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

$$\begin{aligned} s \cdot y(l_i) &\equiv s \cdot y(r_i) \quad \text{and} && (4)\\ t \cdot z(l_i) &\equiv t \cdot z(r_i), && (5) \end{aligned}$$

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

Let $\succeq$ be a lexicographic term ordering satisfying $b \succ s \succ a \succ m$ for all $a \in \{x_1, \ldots, x_k\}$, $b \in \{t, y_1, \ldots, y_k, z_1, \ldots, z_k\}$.

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

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

where $\tilde{u}$ is some word in X^* and G is the reduced Gröbner basis of the ideal $I(\mathcal{P}')$ w.r.t. $\succeq$. Then, by Proposition 4, a complete list of all the elements of $\min(C(u, \mathcal{P}))$ can be generated using at most space $(\text{size}(u, \mathcal{P}))^2 \cdot 2^{d \cdot k}$, and, by Proposition 5, the size of the elements of $\min(C(u, \mathcal{P}))$ is bounded by $\text{size}(u, \mathcal{P}) \cdot 2^{\bar{d} \cdot k}$, where d, $\bar{d} > 0$ are some constants independent of u and $\mathcal{P}$.

First, we establish some technical details.

Lemma 8. *For $v \in X^*$, every word $w \in [s \cdot v]_{\mathcal{P}'}$ satisfies the following conditions:*
(i) $\Phi(w, s) + \Phi(w, t) + \Phi(w, m) = 1$;

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

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

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

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

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

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

Proof. Let w be any word in $[s \cdot v]_{\mathcal{P}'}$. Then there is a repetition-free derivation in $\mathcal{P}'$ leading from $s \cdot v$ to w. For derivations of words $w \in [s \cdot v]_{\mathcal{P}'}$ with $\Phi(w, m) = 0$, see Figure 1. '$\xrightarrow[(.)]{+}$' denotes some repetition-free derivation applying only the congruences given in (.), $v_0, v_1, v_1', v_1'', v_2, v_2', v_2'', \ldots, v_n, v_n', v_n''$, $n \geq 1$, are words in $\{x_1, \ldots, x_k, y_1, \ldots, y_k, z_1, \ldots, z_k\}^*$, and w_X is a word in X^*. We see conditions (i) and (ii) are satisfied. 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 applying congruence (3) a repetition-free derivation starting at $s \cdot v$ terminates with a word w containing m and staisfying conditions (i) and (ii). [Lemma 8]□

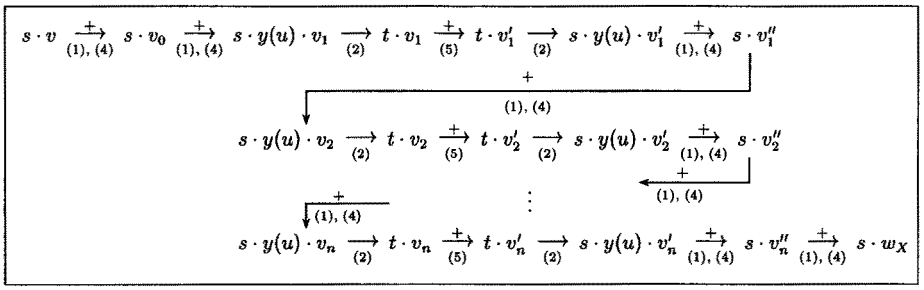

Fig. 1. Repetition-free derivation in $\mathcal{P}'$ starting at $s \cdot v$ without any m.

Lemma 9. *Let v, w be two words in X^* with $v \neq w$. Then $s \cdot w \in [s \cdot v]_{\mathcal{P}'}$ iff $w \in [v]_{\mathcal{P}}$ and there is some $\overline{w} \in [v]_{\mathcal{P}}$ such that u divides $\overline{w}$.*

Lemma 10. *Let v be some word in X^* with $v \notin C(u, \mathcal{P})$. Then $s \cdot v$ is the minimal element (w.r.t. $\succ$) of its congruence class $[s \cdot v]_{\mathcal{P}'}$ modulo $\mathcal{P}'$.*

Proof. If $v \in X^*$ with $v \notin C(u, \mathcal{P})$, then there is no $\bar{v} \in [v]_{\mathcal{P}}$ which is divisible by u. Thus, in any derivation in $\mathcal{P}'$ 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 minimal element of $[s \cdot v]_{\mathcal{P}'}$ w.r.t. $\succ$. [Lemma 10]□

Note that each $v \in X^*$ is the minimal element (w.r.t. $\succ$) of its congruence class $[v]_{\mathcal{P}'}$ modulo $\mathcal{P}'$ because no congruence in $\mathcal{P}'$ is applicable.

If $v \in C(u, \mathcal{P})$, then there is some $w \in X^*$ with $u \cdot w \in [v]_{\mathcal{P}}$, and, by Lemma 9, $s \cdot u \cdot w \in [s \cdot v]_{\mathcal{P}'}$. Since $s \cdot u \equiv m \bmod \mathcal{P}'$, and $b \succ s \succ a \succ m$ for all $a \in \{x_1, \ldots, x_k\}$, $b \in \{t, y_1, \ldots, y_k, z_1, \ldots, z_k\}$, the minimal element w.r.t. $\succ$ of $[s \cdot v]_{\mathcal{P}'}$ with $v \in C(u, \mathcal{P})$ is of the form $m \cdot \tilde{u}$, where $\tilde{u} \in X^*$. Thus, by Proposition 3, each $s \cdot v$ with $v \in C(u, \mathcal{P})$ is an element of $LT(I(\mathcal{P}'))$. In particular, by Lemma 10, each $s \cdot v$ with $v \in \min(C(u, \mathcal{P}))$ is contained in the set of the minimal elements of $LT(I(\mathcal{P}'))$ w.r.t. divisibility. Hence, by Proposition 3, for a word $v \in X^*$, it follows that $v \in \min(C(u, \mathcal{P}))$ iff $s \cdot v - m \cdot \tilde{u} \in G$, where G is the reduced Gröbner basis of the ideal $I(\mathcal{P}')$ w.r.t. $\succeq$. [Theorem 7]□

Since u can be derived in $\mathcal{P}$ from any word in $[u]_{\mathcal{P}}$, we have $[u]_{\mathcal{P}} \subseteq C(u, \mathcal{P})$. Moreover, if the congruence class $[u]_{\mathcal{P}}$ of u is bounded, then $[u]_{\mathcal{P}} \subseteq \min(C(u, \mathcal{P}))$. Consider the commutative semigroup presentation $\mathcal{P}'$ constructed in the proof of Theorem 7. If $[u]_{\mathcal{P}}$ is bounded, then, $[s \cdot u]_{\mathcal{P}'}$ is also bounded. The minimal element (w.r.t. to the lexicographic term ordering $\succeq$ defined in the proof of Theorem 7) of $[s \cdot u]_{\mathcal{P}'}$ is m. Each $s \cdot v$ with $v \in \min(C(u, \mathcal{P}))$ is contained in the set of the minimal elements w.r.t. divisibility of $LT(I(\mathcal{P}'))$, and since $[u]_{\mathcal{P}} \subseteq \min(C(u, \mathcal{P}))$, for a word $v \in X^*$, it follows that

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

where G is the reduced Gröbner basis of the ideal $I(\mathcal{P}')$ w.r.t. $\succeq$. By Proposition 5, the size of the elements of $[u]_{\mathcal{P}}$ is bounded by $\text{size}(u, \mathcal{P}) \cdot 2^{d \cdot k}$, where

$d > 0$ is some constant independent of u and $\mathcal{P}$. Furthermore, by Proposition 4, we obtain for the finite enumeration problem for commutative semigroups:

Corollary 11. *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ i \in I_h\}$ be a finite commutative semigroup presentation over X, and $u \in X^*$ a word such that the congruence class $[u]_\mathcal{P}$ of u modulo $\mathcal{P}$ is bounded. Then there is an algorithm which generates the elements of $[u]_\mathcal{P}$ using at most space $(\text{size}(u,\mathcal{P}))^2 \cdot 2^{\bar{c}\cdot k} \leq 2^{c\cdot \text{size}(u,\mathcal{P})}$, where $\bar{c}$, $c > 0$ are some constants independent of u and $\mathcal{P}$.*

Theorem 12. *The coverability problem and the finite enumeration problem for commutative semigroups are 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 (the input consisting of u, v and $\mathcal{P}$). Actually, the construction in [MM82] proves the following, slightly stronger statement, which we will use for the proof of Theorem 12:

Proposition 13. [MM82] *Let $\mathcal{P}$ be a finite commutative semigroup presentation over some alphabet X, v a word in X^*, and $u \in X^*$ a word such that $[u]_\mathcal{P}$ 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 12. Let $\mathcal{P}$ be the commutative semigroup presentation and u, $v \in X^*$ the two words of Proposition 13. 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 Corollary 11. 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 7 and Corollary 11 establishes the exponential space completeness of the coverability problem and the finite enumeration problem for commutative semigroups. [Theorem 12]□

4 The Containment and the Equivalence Problems

The *Containment Problem* (resp., the *Equivalence Problem*) for commutative semigroups is: Given two finite commutative semigroup presentations $\mathcal{P}$, $\mathcal{Q}$ over some finite alphabet X, and two words u, $v \in X^*$, decide whether $[u]_\mathcal{P} \subseteq [v]_\mathcal{Q}$ (resp., $[u]_\mathcal{P} = [v]_\mathcal{Q}$).

Let $\mathcal{P}$ be a finite commutative semigroup presentation over some finite alphabet $X=\{x_1, \ldots, x_k\}$ 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

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

where $\{a_1,\ldots,a_n\} = \min([u]_{\mathcal{P}})$ and $\{b_1,\ldots,b_t\} = \min(P_{[u]_{\mathcal{P}}} \setminus \{0^k\})$ ($\min(.)$ denotes the minimal elements of the argument w.r.t. divisibility and $P_{[u]_{\mathcal{P}}}$ the set of periods of $[u]_{\mathcal{P}}$, *i.e.*, $P_{[u]_{\mathcal{P}}} = \{x \in \mathbb{N}^k\,;\, u+x \in [u]_{\mathcal{P}}\}$). This shows that the congruence class $[u]_{\mathcal{P}}$ is completely determined by its minimal (w.r.t. divisibility) elements a_j and its minimal periods b_i.

Theorem 14. *Let $X = \{x_1,\ldots,x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ i \in I_h\}$ be a finite commutative semigroup presentation over X, and $u \in X^*$. Then there is an algorithm which generates a closed representation of $[u]_{\mathcal{P}}$ 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. If $[u]_{\mathcal{P}}$ is bounded, then, by Corollary 11, there is an algorithm which generates the elements of $[u]_{\mathcal{P}}$ using at most space $(\mathrm{size}(u,\mathcal{P}))^2 \cdot 2^{\bar{c}\cdot k}$. The size of the elements of $[u]_{\mathcal{P}}$ is bounded by $\mathrm{size}(u,\mathcal{P}) \cdot 2^{d\cdot k}$ for some constant $d > 0$ independent of u and $\mathcal{P}$. In the sequel, we assume that $[u]_{\mathcal{P}}$ is unbounded.

Lemma 15. *Every minimal period b_i of $[u]_{\mathcal{P}}$ has size bounded by $\mathrm{size}(u,\mathcal{P})\cdot 2^{c_b\cdot k}$, where $c_b > 0$ is some constant independent of u and $\mathcal{P}$.*

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

Proposition 16. [Huy85] *Let $P \subseteq \mathbb{N}^k$ be a subtractive submonoid, and let $\mathcal{I}$ be the set of all minimal subsets $I \subseteq I_k$ such that*

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

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

$$p = \sum_{p^I \in U} \varrho_I \cdot p^I, \quad \varrho_I \in \mathbb{Q}^+,\ 0 \leq \varrho_I < 1.$$

The set of periods $P_{[u]_{\mathcal{P}}}$ of a congruence class $[u]_{\mathcal{P}}$ is a subtractive submonoid, and thus, Proposition 16 can be applied to it. In this context, *i.e.*, if $P = P_{[u]_{\mathcal{P}}}$, we call the elements p^I of U the *extreme minimal periods* of $[u]_{\mathcal{P}}$. We shall show that they can be determined by the algorithm of Theorem 6.

Let I_Y be a minimal subset of I_k such that $\min((P_{[u]_{\mathcal{P}}} \setminus \{0^k\}) \cap \{(p_1,\ldots,p_k) \in \mathbb{N}^k\,;\, p_i > 0 \text{ for } i \in I_Y,\ p_i = 0 \text{ for } i \notin I_Y\})$ contains exactly one element p^{I_Y}. By setting $Y = \{x_i\,;\, i \in I_Y\}$, $Z = \emptyset$, and $v_1 = u$, the algorithm of Theorem 6 provides p^{I_Y} whose size is bounded by $\mathrm{size}(u,\mathcal{P}) \cdot 2^{d_1\cdot k}$ for some constant $d_1 > 0$ independent of u and $\mathcal{P}$. Thus, by Proposition 16, the size of every minimal period b_i of $[u]_{\mathcal{P}}$ is bounded by $k \cdot \max\{\mathrm{size}(p)\,;\, p \in U\}$, where U is the set of the extreme minimal periods of $[u]_{\mathcal{P}}$. This implies, for every minimal period b_i of $[u]_{\mathcal{P}}$, $\mathrm{size}(b_i) \leq \mathrm{size}(u,\mathcal{P}) \cdot 2^{c_b\cdot k}$. [Lemma 15]□

The sets I_Y which belong to the extreme minimal periods of $[u]_{\mathcal{P}}$ can be determined by choosing a subset Y of X, deciding by the algorithm of Theorem 6 whether $[u]_{\mathcal{P}}$ has a period b with $b \in Y^*$, and checking that there is no proper

subset Y_s of Y such that $[u]_{\mathcal{P}}$ has also a period b_s with $b_s \in Y_s^*$. Hence, by the above considerations, the extreme minimal periods of $[u]_{\mathcal{P}}$ can be determined using at most space $(\text{size}(u,\mathcal{P}))^2 \cdot 2^{c_1 \cdot k}$ for some constant $c_1 > 0$ independent of u and $\mathcal{P}$.

Recall that $p \in X^*$ is a period of $[u]_{\mathcal{P}}$ if $u \cdot p \equiv u \bmod \mathcal{P}$. Hence, by Propositions 1 and 2, checking a $p \in X^*$ for being a period of $[u]_{\mathcal{P}}$ can be done in space $(\text{size}(u,\mathcal{P}))^2 \cdot 2^{c_b' \cdot k}$, where $c_b' > 0$ is some constant independent of u and $\mathcal{P}$. Thus, we get a closed representation of the set of periods $P_{[u]_{\mathcal{P}}}$ of $[u]_{\mathcal{P}}$ in form of a set B with $B \subseteq P_{[u]_{\mathcal{P}}}$ and $B \supseteq \{b_1, \ldots, b_t\}$ using at most space $(\text{size}(u,\mathcal{P}))^2 \cdot 2^{c_b' \cdot k}$.

Lemma 17. *Every minimal element a_j of $[u]_{\mathcal{P}}$ has size bounded by* $\text{size}(u,\mathcal{P}) \cdot 2^{c_a \cdot k}$, *where $c_a > 0$ is some constant independent of u and $\mathcal{P}$.*

Proof. For determining the upper bound for the size of the minimal elements a_j of $[u]_{\mathcal{P}}$, we project $[u]_{\mathcal{P}}$ onto the bounded coordinates. The ith coordinate, $i \in I_k$, is bounded in $[u]_{\mathcal{P}} \subseteq \mathbb{N}^k$ if the variable x_i is bounded w.r.t. $[u]_{\mathcal{P}}$ in X^*, *i.e.*, $u \notin C(u \cdot x_i, \mathcal{P})$. The set $X_b \subseteq X$ of the bounded variables can be determined by the algorithm of Theorem 6 (or Theorem 7) using at most space $(\text{size}(u,\mathcal{P}))^2 \cdot 2^{c_v \cdot k}$ for some constant $c_v > 0$ independent of u and $\mathcal{P}$. Note that the periods of $[u]_{\mathcal{P}}$ do not contain any bounded variable, *i.e.*, $\Phi(p,x) = 0$ for all $p \in P_{[u]_{\mathcal{P}}}$, $x \in X_b$.

Let w_b denote the projection of any word $w \in X^*$ and $\mathcal{P}_b$ the projection of $\mathcal{P}$ onto the bounded coordinates in X_b. Then the congruence class $[u_b]_{\mathcal{P}_b}$ is bounded, and, by Corollary 11, there is an algorithm which generates the elements of $[u_b]_{\mathcal{P}_b}$ using at most space $(\text{size}(u_b,\mathcal{P}_b))^2 \cdot 2^{c_2' \cdot k} \leq (\text{size}(u,\mathcal{P}))^2 \cdot 2^{c_2' \cdot k}$, where $c_2' > 0$ is some constant independent of u and $\mathcal{P}$. The size of the elements of $[u_b]_{\mathcal{P}_b}$ is bounded by $\text{size}(u,\mathcal{P}) \cdot 2^{d_2' \cdot k}$ for some constant $d_2' > 0$ independent of u and $\mathcal{P}$.

Let $([u]_{\mathcal{P}})_b$ denote the projection of $[u]_{\mathcal{P}}$ onto the bounded coordinates in X_b. Then $([u]_{\mathcal{P}})_b = [u_b]_{\mathcal{P}_b}$. In particular, the projection $(a_j)_b$ of each of the minimal elements a_j of $[u]_{\mathcal{P}}$ onto the bounded coordinates is an element of $[u_b]_{\mathcal{P}_b}$, and each element of $[u_b]_{\mathcal{P}_b}$ is the projection of at least one minimal element a_j. For each word $\overline{u}_b \in [u_b]_{\mathcal{P}_b}$, we determine some $\overline{u} = \overline{u}_b \cdot t \in [u]_{\mathcal{P}}$, $t \in (X - X_b)^*$, as 'representative' of the elements v of $[u]_{\mathcal{P}}$ with $v_b = \overline{u}_b$. By Theorem 6, this computation requires at most space $(\text{size}(u,\mathcal{P}))^2 \cdot 2^{c_2'' \cdot k}$, and the size of $\overline{u}$ is bounded by $\text{size}(u,\mathcal{P}) \cdot 2^{d_2'' \cdot k}$ for some constants c_2'', $d_2'' > 0$ independent of u and $\mathcal{P}$.

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

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

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

such that h_a divides a. Because $h_a \in C(u, \mathcal{P})$, we obtain $P_{[u]_\mathcal{P}} \subseteq P_{[h_a]_\mathcal{P}}$ implying $h_a + P_{[u]_\mathcal{P}} \subseteq [h_a]_\mathcal{P}$.

In the proof of Theorem 7, we have presented an algorithm that generates the elements of $\min(C(u, \mathcal{P}))$ using at most space $(\text{size}(u, \mathcal{P}))^2 \cdot 2^{c_2''' \cdot k}$, where $c_2''' > 0$ is some constant independent of u and $\mathcal{P}$. The size of the elements of $\min(C(u, \mathcal{P}))$ is bounded by $\text{size}(u, \mathcal{P}) \cdot 2^{d_2''' \cdot k}$ for some constant $d_2''' > 0$ independent of u and $\mathcal{P}$.

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

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

Hence, the size of the minimal elements a_j of the uniformly semilinear set $[u]_\mathcal{P}$ is bounded by $\text{size}(u, \mathcal{P}) \cdot 2^{c_a \cdot k}$. [Lemma 17]□

By Propositions 1 and 2, deciding for some word a whose size is bounded by $\text{size}(u, \mathcal{P}) \cdot 2^{c_a \cdot k}$ whether it is an element of $[u]_\mathcal{P}$, *i.e.*, $a \equiv u \bmod \mathcal{P}$, uses at most space $(\text{size}(u, \mathcal{P}))^2 \cdot 2^{c_a' \cdot k}$, where $c_a' > 0$ is some constant independent of u and $\mathcal{P}$. Thus, we get a set A of elements of $[u]_\mathcal{P}$ containing all minimal elements a_j of $[u]_\mathcal{P}$ using at most space $(\text{size}(u, \mathcal{P}))^2 \cdot 2^{c_a' \cdot k}$. [Theorem 14]□

Theorem 18. *Let $\mathcal{P}$, $\mathcal{Q}$ be two finite commutative semigroup presentations over some finite alphabet $X = \{x_1, \ldots, x_k\}$, and u, v two words in X^*. Then there is an algorithm which decides whether $[u]_\mathcal{P}$ is contained in (is equal to) $[v]_\mathcal{Q}$ using at most space $(\max\{\text{size}(u, \mathcal{P}), \text{size}(v, \mathcal{Q})\})^2 \cdot 2^{\bar{c} \cdot k} \leq 2^{c \cdot \text{size}(u,v,\mathcal{P},\mathcal{Q})}$, where $\bar{c}$, $c > 0$ are some constants independent of u, v, $\mathcal{P}$, and $\mathcal{Q}$.*

Proof. Containment of $[u]_\mathcal{P}$ in $[v]_\mathcal{Q}$ can be decided by the exponential space algorithm (for suitable constants c and c') given in Figure 2. Since the word problems occurring in this algorithm can, by Propositions 1 and 2, be decided using at most space $(\max\{\text{size}(u, \mathcal{P}), \text{size}(v, \mathcal{Q})\})^2 \cdot 2^{\bar{c} \cdot k}$, this algorithm can be implemented on a Turing machine whose space is bounded by $(\max\{\text{size}(u, \mathcal{P}), \text{size}(v, \mathcal{Q})\})^2 \cdot 2^{\bar{c} \cdot k}$. Because $[u]_\mathcal{P} = [v]_\mathcal{Q}$ iff $[u]_\mathcal{P} \subseteq [v]_\mathcal{Q}$ and $[u]_\mathcal{P} \supseteq [v]_\mathcal{Q}$, this space bound also holds for the equivalence problem. □

Theorem 19. *The containment and the equivalence problems for commutative semigroups are exponential space complete with respect to log-lin reducibility.*

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

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 $u \equiv v \bmod \mathcal{Q}$ **then**
  for each $a \in X^*$ with degree $\leq 2^{(\max\{\text{size}(u,\mathcal{P}),\, \text{size}(v,\mathcal{Q})\})^2 \cdot 2^{c \cdot k}}$ **do**
    if $(a \equiv u \bmod \mathcal{P}$ **and** $a \not\equiv v \bmod \mathcal{Q})$ **then reject end_if**
  end_for
  for each $b \in X^*$ with degree $\leq 2^{(\max\{\text{size}(u,\mathcal{P}),\, \text{size}(v,\mathcal{Q})\})^2 \cdot 2^{c' \cdot k}}$ **do**
    if $(u \equiv u \cdot b \bmod \mathcal{P}$ **and** $v \not\equiv v \cdot b \bmod \mathcal{Q})$ **then reject end_if**
  end_for
  accept
else reject
end_if

Fig. 2. Algorithm for deciding the containment problem for commutative semigroups

References

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

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

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

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

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

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

[Huy85] D.T. Huynh. The complexity of the equivalence problem for commutative semigroups and symmetric vector addition systems. In *Proceedings of STOC '85*, 405–412, New York, 1985. ACM Press.

[KM96a] U. Koppenhagen and E.W. Mayr. Optimal Gröbner base algorithms for binomial ideals. In *Proceedings of ICALP '96*, *LNCS* 1099, 244–255, Heidelberg, 1996. Springer Verlag.

[KM96b] U. Koppenhagen and E.W. Mayr. An optimal algorithm for constructing the reduced Gröbner basis of binomial ideals. In *Proceedings of ISSAC '96*, 55–62, New York, 1996. ACM Press.

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

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

[Rob85] L. Robbiano. Term orderings on the polynomial ring. In *Proceedings of EUROCAL '85, Vol. 2*, *LNCS* 204, 513–517, Berlin-Heidelberg-New York-Tokyo, 1985. Springer Verlag.

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

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