T U M

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

The Complexity of the Equivalence Problem for Commutative Semigroups

Ulla Koppenhagen
Ernst W. Mayr

TUM-I9603
Januar 1996

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

TUM-INFO-01-1996-I9603-350/1.-FI

Typescript: ---

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

The Complexity of the Equivalence Problem for Commutative Semigroups

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

November 7, 1995

Abstract

In this paper, optimal decision procedures for the equivalence, subword, and finite enumeration problems for commutative semigroups are obtained. 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 this space requirement is inevitable: *any* decision procedure for these problems requires at least exponential space in the worst case, the equivalence, subword, and finite enumeration problems for commutative semigroups are exponential space complete.

For the equivalence problem, our results close the gap between the $2^{c' \cdot n \cdot \log n}$ space upper bound shown by Huynh 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 (VAS), and 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 of decision problems for these models have received much attention.

In this paper we focus on the *equivalence problem*. This is the problem of determining for any two given commutative semi-Thue systems, or equivalently, VAS, or Petri nets whether the reachability set of the first is equal to the other. In [Hac76] this problem was shown to be undecidable. The situation changes, however, when one considers an important subclass of commutative semi-Thue systems, the class of commutative Thue systems, or commutative semigroups (or equivalently, reversible VAS, or reversible Petri nets) [Bir67, Emi63, Mar47, Tai68].

The equivalence (containment) problem for commutative semigroups, or equivalently, reversible Petri nets is the problem of deciding for any two given congruence classes $[u]_{\mathcal{P}}$, $[v]_{\mathcal{Q}}$, where $\mathcal{P}$, $\mathcal{Q}$ are two commutative semigroup presentations over some alphabet X, and u, v are two words in X^*, whether $[u]_{\mathcal{P}}$ is equal to (is contained in) $[v]_{\mathcal{Q}}$. In [Huy85] Huynh exhibited a decision algorithm for the equivalence problem for commutative semigroups which operates in space $2^{d\cdot \mathrm{size}(u,v,\mathcal{P},\mathcal{Q})\cdot\log(\mathrm{size}(u,v,\mathcal{P},\mathcal{Q}))}$, where $d > 0$ is some constant independent of u, v, $\mathcal{P}$ and $\mathcal{Q}$. The arguments for this upper bound are based on the $2^{d'\cdot s\cdot\log s}$ space upper bound for the coverability and selfcoverability problems for general Petri nets obtained by Rackoff in [Rac78], where s is the size of the problem instance.

We are able to show a $2^{c\cdot\mathrm{size}(u,v,\mathcal{P},\mathcal{Q})}$ space upper bound for deciding the equivalence problem for commutative semigroups, with $c > 0$ some constant independent of u, v, $\mathcal{P}$ and $\mathcal{Q}$.

In Section 3 we present efficient decision procedures for the subword and finite enumeration problems which operate in exponential space. The proofs are based on an algorithm for generating the reduced Gröbner basis of a binomial ideal using at most exponential space. Furthermore, we show that the exponential space requirement is inevitable: *any* decision procedure for the subword and finite enumeration problems requires at least exponential space. The proof of this lower bound on the complexity of the problems is based on reducing the uniform word problem resp., a special form of the uniform word problem, which is exponential space complete (see [MM82]), to the subword resp., finite enumeration problem.

In Section 4, these complexity results are applied to obtain the exponential space upper bound for the equivalence problem for commutative semigroups. Thus, the gap between the $2^{c\cdot\mathrm{size}(u,v,\mathcal{P},\mathcal{Q})\cdot\log(\mathrm{size}(u,v,\mathcal{P},\mathcal{Q}))}$ space upper bound and the exponential space lower bound resulting from the exponential space completeness of the uniform word problem is closed, and the exponential space completeness of the equivalence problem for commutative semigroups is established.

2 Basic Definitions and Notations

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

2.1 Semigroups, Thue Systems, and Semigroup Presentations

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

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

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

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

Each element of M can then be represented as a k-dimensional vector in $\mathbb{N}^k$, *i.e.,* there is a surjection $\varphi : \mathbb{N}^k \to M$ such that

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

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

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

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

For an element u of X^*, called a (commutative) word, the order of the symbols is immaterial, and we shall in the sequel use an exponent notation: $u = x_1^{e_1} \dots x_k^{e_k}$, where $e_i = \Phi(u, x_i) \in \mathbb{N}$ for $i = 1, \dots, k$. For instance, we may denote $x_1x_2x_1x_1x_3x_3x_2$ by $x_1^3x_2^2x_3^2$, interchangeably with, say, $x_1^2x_3x_1x_2^2x_3$.

Notice that power products in $\mathbb{Q}[x_1, \dots, x_k]$ (monomials with coefficient 1) may be regarded as elements of $\{x_1, \dots, x_k\}^*$.

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

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

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

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

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

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

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

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

We remark that commutative semi-Thue systems appear in the literature in two additional equivalent formulations: *vector addition systems* (see next section) and *Petri nets*. Finitely presented commutative semigroups are equivalent to *reversible* vector addition systems or Petri nets. A reader more familiar with reversible Petri nets may want to think of a vector in $\mathbb{N}^k$ as a marking.

2.2 Exponential Space

In this section we briefly review the few necessary technical definitions from complexity theory.

Complexity is usually measured relative to the size of a problem instance. Note that we use exponential notation in representing words over X. For example, a word consisting of 805 x's has size 4 because it has a representation in exponential notation of 4 symbols, namely, x^{805}. Thus, a word, or equivalently, a term $u \in X^*$ with $\text{size}(u) = n$ has degree $O(2^n)$ resp., a term $u \in X^*$ with $\deg(u) = d$ has size $O(\log d)$.

Let X_1, X_2 be finite alphabets. A function $f : X_1^* \to X_2^*$ *reduces* a set $A \subseteq X_1^*$ to a set $B \subseteq X_2^*$ in case

$$\alpha \in A \iff f(\alpha) \in B$$

for all $\alpha \in X_1^*$. If f is computable by a Turing machine which visits at most $\log_2 n$ work tape squares during its computation on any word $\alpha \in X_1^*$ of length $n > 1$, then A is said to be *log-space reducible* to B. (We assume the Turing machine has a read-only input tape and a write-only output tape separate from its work tape.) If in addition the length of $f(\alpha)$ is $\mathcal{O}(length(\alpha))$, then A is *log-lin reducible* to B.

The set $B \subseteq X_2^*$ is said to be *decidable in space* $g : \mathbb{N} \to \mathbb{N}$ if there is a Turing machine which accepts B and visits at most $g(n)$ work tape squares during its computation on any word $\beta \in X_2^*$ of length n.

B is decidable in *exponential space* if it is decidable in space g, where $g(n) \leq c^n$ for some $c > 1$.

B is *exponential space complete with respect to log-lin reducibility* if

(i) it is decidable in exponential space, and

(ii) every set which is decidable in exponential space is log-lin reducible to B.

If B satisfies condition (ii) only, it is said to be *exponential space hard.*

2.3 Polynomials and Ideals

Let X denote the finite set $\{x_1, \ldots, x_k\}$, and $\mathbb{Q}[X]$ the (commutative) ring of polynomials with indeterminates $x_1, \ldots, x_k$ and rational coefficients. An *ideal* in $\mathbb{Q}[X]$ is any subset I of $\mathbb{Q}[X]$ satisfying the following conditions:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Gröbner bases have been introduced in [Hi64, Hi64a] and [Buc65].

A basis is called *minimal* if it does not strictly contain some other basis of the same ideal. A Gröbner basis is called *reduced* if no monomial in any one of its polynomials is divisible by the leading term of some other polynomial in the basis.

Now let $\mathcal{P} = \{l_i \equiv r_i;\ i \in I_h\}$ be any (finite) commutative semigroup presentation with $l_i, r_i \in X^*$ for $i \in I_h$. We identify any $u \in X^*$ (resp., the corresponding vector $u = (\Phi(u, x_1), \ldots, \Phi(u, x_k)) \in \mathbb{N}^k$) with the term $u = x_1^{\Phi(u,x_1)} \cdot x_2^{\Phi(u,x_2)} \cdots x_k^{\Phi(u,x_k)}$ and vice versa any term $u = x_1^{e_1} \cdot x_2^{e_2} \cdots x_k^{e_k} \in \mathbb{Q}[X]$ with the word

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

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

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

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

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

In [MM82], Mayr and Meyer proved:

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

(i) There exist $p_1, \ldots, p_h \in \mathbb{Q}[X]$ such that

$$v - u = \sum_{i=1}^{h} p_i(l_i - r_i).$$

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

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

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

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

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

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

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

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

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

For the proofs in Sections 3 and 4 we need the following three theorems. The first shows that in each binomial of the reduced Gröbner basis G of $I(\mathcal{P})$ the smaller term (w.r.t. $\prec$) is the minimal element of the congruence class of the leading term.

Theorem 1 [KM96] *Let* $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$, *and* $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ *the reduced Gröbner basis of the ideal* $I(\mathcal{P})$ *w.r.t. some admissible term ordering* $\prec$ $(m_i \prec h_i)$. *Then* m_i *is the minimal element (w.r.t.* $\prec$*) of the congruence class* $[h_i]_{\mathcal{P}}$, $i \in I_r$.

The next theorem gives a characterization of the leading terms of the polynomials in $I(\mathcal{P})$.

Theorem 2 [KM96] *Let* $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$, *and* $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ *the reduced Gröbner basis of the ideal* $I(\mathcal{P})$ *w.r.t. some admissible term ordering* $\prec$ $(m_i \prec h_i)$. *Then* $LT(I(\mathcal{P}))$ *(the set of the leading terms of* $I(\mathcal{P})$*) is the set of all terms with nontrivial congruence class and which are NOT the minimal element in their congruence class w.r.t.* $\prec$. $H = \{h_1, \ldots, h_r\}$ *is the set of the minimal elements of* $LT(I(\mathcal{P}))$ *w.r.t. divisibility.*

Finally, we need the following complexity result.

Theorem 3 [KM96] *Let* $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$, *and* $\prec$ *be some admissible term ordering. Then there is an algorithm which generates the reduced Gröbner basis* $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ *of the binomial ideal* $I(\mathcal{P})$ *using at most space* $(\mathrm{size}(\mathcal{P}))^2 \cdot 2^{\bar{c} \cdot k} \leq 2^{c \cdot \mathrm{size}(\mathcal{P})}$, *where* $\bar{c}, c > 0$ *are some constants independent of* $\mathcal{P}$.

For a proof of these Theorems see [KM96].

3 The Basic Problems and Their Complexity

In this section we are going to prove the exponential space completeness of the subword and finite enumeration problems for commutative semigroups. These results will then be applied in Section 4 to provide a space optimal decision procedure for the equivalence problem for commutative semigroups.

3.1 The Subword Problem for Commutative Semigroups

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

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

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

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

Let Y be the subset $\{x_{l_1}, \ldots, x_{l_2}\}$ of X with $l_2 \geq l$ (if $l_1 > l_2$ then $Y = \emptyset$).
Similarly, Z is the subset $\{x_{l_3}, \ldots, x_k\}$ of X with $l_2 < l_3$, and $Z = \emptyset$ if $l_3 > k$.
Then, for the case $l_1 < l < l_2 < l_3$ we get the following picture:

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

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

- The Subword Problem: Given X, $\mathcal{P}$, u, v_1, Y, and Z, decide whether there is a $v_2 \in [u]_{\mathcal{P}}$ such that $v_2 = v_1 \cdot x_{l_1} \cdots x_{l_2} \cdot w$ for some $w \in (Y \cup Z)^*$.
- The Word Problem: Given X, $\mathcal{P}$, u, v_1, decide whether $v_1 \in [u]_{\mathcal{P}}$. In [MM82] this problem is shown to be exponential space complete.
- The Coverability Problem: Given X, $\mathcal{P}$, u, v_1, decide whether there is a $v_2 \in [u]_{\mathcal{P}}$ such that v_1 is a subword of v_2, *i.e.,* $v_2 = v_1 \cdot w$ for some $w \in X^*$. In [KM95] we showed that this problem is exponential space complete.

We see that the word problem and the coverability problem are special cases of the subword problem. If Y and Z are the empty set, then the subword problem is equivalent to the word problem. If Y is the empty set and $Z = X$, then the subword problem is equivalent to the coverability problem.

If Y is the empty set and $Z = X_{\overline{v_1}}$, *i.e.,* $l_3 = l + 1$, we get the former definition. Then the subword problem is to decide whether there is a $v_2 \in [u]_{\mathcal{P}}$ such that $v_2 = v_1 \cdot w$ for some $w \in X^*_{\overline{v_1}}$.

Theorem 4 *Let $X = \{x_1, \ldots, x_k\}$, and $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$ be a commutative semigroup presentation over X. Then there is an algorithm which decides for any two words u, $v_1 \in X^*$, and sets Y, $Z \subseteq X$ defined as above whether there is 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*

$Y = \{x_{l_1}, \ldots, x_{l_2}\}$ *resp.,* $v = \varepsilon$ [3] *if* $Y = \emptyset$, *using at most space* $(\mathrm{size}(u, v_1, \mathcal{P}))^2 \cdot 2^{\bar{c} \cdot k} \leq 2^{c \cdot \mathrm{size}(u, v_1, \mathcal{P})}$ *for some constants* $\bar{c}$, $c > 0$ *independent of* u, v_1 *and* $\mathcal{P}$.

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

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

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

Then we add to $\mathcal{P}_t$ the congruences

$$s \equiv t \cdot u,$$

and

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

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

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

where the variables in the sets are ordered arbitrarily.

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

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

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

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

[3] ε denotes the empty word

Lemma 1 *Every word γ in a derivation in $\mathcal{P}_t$ starting at s satisfies:*

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

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

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

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

Hence, the words γ_i in a repetition-free derivation

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

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

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

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

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

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

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

Theorem 5 *The subword problem for reversible Petri nets and commutative semigroups is exponential space complete with respect to log-lin reducibility.*

Proof: From the results in [MM82] we know that the word problem for commutative semigroups is exponential space complete with respect to log-lin reducibility. Since the word problem is a special case of the subword problem, and because of Theorem 4 we conclude the assertion. □

3.2 The Finite Enumeration Problem for Commutative Semigroups

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

Theorem 6 *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$ be a finite commutative semigroup presentation over X, and $u \in X^*$ a word such that the congruence class of u is bounded. Then there is an algorithm which generates the elements of $[u]_\mathcal{P}$ using at most space $(\mathrm{size}(u,\mathcal{P}))^2 \cdot 2^{\bar{c}\cdot k} \leq 2^{c\cdot \mathrm{size}(u,\mathcal{P})}$, where $\bar{c}$, $c > 0$ are some constants independent of u and $\mathcal{P}$.*

Proof: In addition to $x_1, \ldots, x_k$ we introduce $2k+3$ 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) for $j \in I_k$.

Let $\prec$ be a lexicographic term ordering satisfying

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

In the following we prove that $v \in [u]_\mathcal{P}$ iff the term $s \cdot v$ occurs in a binomial of G, where G is the reduced Gröbner basis of the ideal $I(\mathcal{P}')$ w.r.t. $\prec$. Then, by Theorem 3, the elements of $[u]_\mathcal{P}$ can be generated using at most space $(\mathrm{size}(u,\mathcal{P}'))^2 \cdot 2^{d'\cdot k} \leq (\mathrm{size}(u,\mathcal{P}))^2 \cdot 2^{d\cdot k}$, where d', $d > 0$ are some constants independent of u and $\mathcal{P}'$ (resp., $\mathcal{P}$).

First we establish some technical details.

Lemma 2 *Every word $w \in [s \cdot u]_{\mathcal{P}'}$ satisfies the following conditions:*

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

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

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

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

if $\Phi(w,t) = 1$, *then* $\Phi(w,x_1) = \Phi(w,x_2) = \ldots = \Phi(w,x_k) = 0$,

$$\Phi(w,y_1) = \Phi(w,y_2) = \ldots = \Phi(w,y_k) = 0,$$

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

Proof: Let w be any word in $[s \cdot u]_{\mathcal{P}'}$, then there is a repetition-free derivation in $\mathcal{P}'$ leading from $s \cdot u$ to w. If $w = m$, then w is derived in one step from $s \cdot u$ by

congruence (3) and w trivially satisfies the conditions (i) - (iii). Note that if in a derivation starting at $s \cdot u$ congruence (3) is applied, then this derivation can only be continued by again using congruence (3) what causes a repetition. If $w \neq m$, then in any repetition-free derivation starting at $s \cdot u$ leading to w only the congruences in (1) and (4) can be applied until the word $s \cdot y(u) \cdot z(u)$ is reached and changed to $t \cdot z(u)$ by congruence (2). Since $[u]_{\mathcal{P}}$ is bounded, there is no $u' \in \{y_1, \ldots, y_k\}^*$ with $s \cdot u' \cdot z(u) \in [s \cdot u]_{\mathcal{P}'}$, $u' \neq y(u)$, and $y(u)$ divides u'. Therefore, any word w occuring in this derivation of $s \cdot y(u) \cdot z(u)$ from $s \cdot u$ satisfies the conditions (i) - (iii):

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

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

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

Then, as long as congruence (2) is not applied, by the congruences in (5) words $t \cdot z(v)$ with $v \in [u]_{\mathcal{P}}$ can be derived from $t \cdot z(u)$. Note, that for all such words $t \cdot z(v)$ with $v \in [u]_{\mathcal{P}}$ $\Phi(t \cdot z(v), s) = 0$, $\Phi(t \cdot z(v), t) = 1$, and condition (iii) is satisfied. Congruence (2) changes $t \cdot z(v)$ to $s \cdot y(u) \cdot z(v)$ and again the congruences in (1) and (4) can be applied. As above the words w in the resulting sub-derivation starting at $s \cdot y(u) \cdot z(v)$ satisfy (i), (ii), and (iii) with

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

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

$\square_{\text{Lemma 2}}$

For the derivation of some word $s \cdot v \in [s \cdot u]_{\mathcal{P}'}$ with $v \in X^*$ from $s \cdot u$ in $\mathcal{P}'$ we conclude from Lemma 2 and its proof:

Lemma 3 *Let $s \cdot v \in [s \cdot u]_{\mathcal{P}'}$ with $v \in X^*$, $v \neq u$, and let $s \cdot u = \gamma_0 \to \gamma_1 \to \ldots \to \gamma_n = s \cdot v$ be any repetition-free derivation in $\mathcal{P}'$ leading from $s \cdot u$ to $s \cdot v$. Then, there is exactly one $i \in I_{n-1}$ with $\gamma_i = s \cdot y(u) \cdot z(u)$, $\gamma_{i+1} = t \cdot z(u)$, and exactly one $j \in I_{n-1}$, $j > i$, with $\gamma_j = t \cdot z(v)$, $\gamma_{j+1} = s \cdot y(u) \cdot z(v)$.*

Thus, we have:

Lemma 4 *Let v be some word in X^*, then*

$$v \in [u]_{\mathcal{P}} \quad \Longleftrightarrow \quad s \cdot v \in [s \cdot u]_{\mathcal{P}'}$$

Proof: By Lemma 2 and Lemma 3 a repetition-free derivation in $\mathcal{P}'$ leading from $s \cdot u$ to $s \cdot v$ with $v \in X^*$ has the following form:

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

where $\xrightarrow[(.)]{+}$ denotes some repetition-free derivation only applying the congruences given in (.) . Within the sub-derivations $\xrightarrow[(1),\,(4)]{+}$ the values $\Phi(w, x_i) + \Phi(w, z_i)$ are

constant for all $i \in I_k$, *i.e.,* the word $x_1^{\Phi(w,x_1)+\Phi(w,z_1)} \cdot x_2^{\Phi(w,x_2)+\Phi(w,z_2)} \cdots x_k^{\Phi(w,x_k)+\Phi(w,z_k)}$ remains the same within $\xrightarrow[(1),\,(4)]{+}$. Furthermore, all the words occuring in the above derivation satisfy Lemma 2. $\square_{\text{Lemma 4}}$

Lemma 5 *$[s \cdot u]_{\mathcal{P}'}$ is bounded.*

Proof: Since $[u]_{\mathcal{P}}$ is bounded, it follows from the definition of $\mathcal{P}'$ and Lemma 2 that $[s \cdot u]_{\mathcal{P}'}$ is also bounded. $\square_{\text{Lemma 5}}$

Lemma 6 *Let v be some word in X^* with $v \notin [u]_{\mathcal{P}}$, and v divides some $u' \in [u]_{\mathcal{P}}$. Then $s \cdot v$ is the minimal element of its congruence class $[s \cdot v]_{\mathcal{P}'}$ w.r.t. $\prec$.*

Proof: If $v \in X^*$ with $v \notin [u]_{\mathcal{P}}$, and v divides some $u' \in [u]_{\mathcal{P}}$, then there is some $v' \in X^* - \{\varepsilon\}$ with $u' = v \cdot v' \in [u]_{\mathcal{P}}$. Because of the boundedness of $[u]_{\mathcal{P}}$ there is no $\bar{v} \in [v]_{\mathcal{P}}$ with $\bar{v} = u \cdot \bar{u}$ for $\bar{u} \in X^*$. If there would be such a $\bar{v} \in [v]_{\mathcal{P}}$, then $u' = v \cdot v' \equiv \bar{v} \cdot v' \bmod \mathcal{P}$, $\bar{v} \cdot v' = u \cdot \bar{u} \cdot v' \in [u]_{\mathcal{P}}$, *i.e.,* $[u]_{\mathcal{P}}$ is not bounded. Thus, in any derivation starting at $s \cdot v$ the congruences (2) and (3) can not be applied. Only the congruences in (1) and (4) can possibly be used. Since $y_i \succ x_i$ (resp., $z_i \succ x_i$) for all $i \in I_k$, $s \cdot v$ is the minimal element of $[s \cdot v]_{\mathcal{P}'}$ w.r.t. $\prec$. $\square_{\text{Lemma 6}}$

Since $[s \cdot u]_{\mathcal{P}'}$ is bounded, it follows from Dickson's Lemma that each $w \in [s \cdot u]_{\mathcal{P}'}$ is minimal in $[s \cdot u]_{\mathcal{P}'}$ w.r.t. divisibility, *i.e.,* if $w \in [s \cdot u]_{\mathcal{P}'}$ there is no $w' \in [s \cdot u]_{\mathcal{P}'}$, $w' \neq w$ such that w' divides w. Thus, by Lemma 6, if $w \in [s \cdot u]_{\mathcal{P}'}$, and w is not the minimal element $m_{s \cdot u} = m$ of $[s \cdot u]_{\mathcal{P}'}$ w.r.t. $\prec$, then $w \in H$, where H denotes the set of the minimal elements of $LT(I(\mathcal{P}'))$ w.r.t. divisibility, and hence $G \supset \{w - m \mid w \in [s \cdot u]_{\mathcal{P}'},\ w \neq m\}$ (see Theorems 1 and 2). $\square$

Theorem 7 *The finite enumeration problem for reversible Petri nets and commutative semigroups is exponential space complete with respect to log-lin reducibility.*

From the work in [MM82] we know that the uniform word problem for commutative semigroups is exponential space complete. Actually, the construction in [MM82] proves the following, slightly stronger statement, which we will use for the proof of Theorem 7:

Proposition 4 [MM82] *Let $\mathcal{P}$ be a finite commutative semigroup presentation over X, v a word in X^*, and $u \in X^*$ a word such that $[u]_{\mathcal{P}}$ is bounded. Even with this restriction, the uniform word problem,* i.e., *the problem of deciding whether $u \equiv v \bmod \mathcal{P}$, is exponential space complete with respect to log-lin reducibility.*

Proof of Theorem 7: Let $\mathcal{P}$ be the commutative semigroup presentation, and $u, v \in X^*$ the two words of Proposition 4. Then, $v \equiv u \bmod \mathcal{P}$, *i.e.,* $v \in [u]_{\mathcal{P}}$ iff v is contained in the list of elements of $[u]_{\mathcal{P}}$ generated by the enumeration algorithm of Theorem 6. Thus, an exponential space complete word problem reduces to the enumeration problem for commutative semigroups, which together with Theorem 6 establishes the exponential space completeness of the enumeration problem for reversible Petri nets and commutative semigroups. $\square$

In the following we are going to show that Theorem 6 also provides an exponential space upper bound for the finite containment problem (FCP) (and the finite equality problem (FEP)) for reversible Petri nets and commutative semigroups.

The finite containment problem (the finite equality problem) for general (not necessary reversible) Petri nets is the problem of determining for any two given Petri nets with finite reachability sets whether the reachability set of the first is contained in (is equal to) the other. A result by Karp and Miller in [KaMi69] shows that FCP (FEP) for Petri nets is decidable, but in [MM81] Mayr and Meyer proved that the complexity of each decision procedure for FCP (FEP) for general Petri nets exceeds any primitive recursive function infinitely often. For reversible Petri nets, or equivalently, commutative semigroups the situation changes.

Corollary 1 *Let $X = \{x_1, \ldots, x_k\}$, and $\mathcal{P}$, $\mathcal{Q}$ be two finite commutative semigroup presentations over X. Then there is an algorithm which decides for any two words u, $v \in X^*$ with bounded congruence classes $[u]_\mathcal{P}$, $[v]_\mathcal{Q}$ whether $[u]_\mathcal{P} \subseteq [v]_\mathcal{Q}$ 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: By Theorem 6 a complete list of all the elements of $[u]_\mathcal{P}$ can be generated using at most space $(\text{size}(u,\mathcal{P}))^2 \cdot 2^{c'\cdot k}$ for some constant $c' > 0$ independent of u and $\mathcal{P}$. For every $w \in [u]_\mathcal{P}$, by Proposition 1 and Proposition 2, it can be decided whether $w \equiv v \bmod \mathcal{Q}$, *i.e.*, $w \in [v]_\mathcal{Q}$, using at most space $(\max\{\text{size}(u,\mathcal{P}), \text{size}(v,\mathcal{Q})\})^2 \cdot 2^{\bar{c}\cdot k}$. □

From Proposition 4 we can derive that FCP for commutative semigroups, or equivalently, reversible Petri nets is exponential space hard. Thus, we establish the exponential space completeness of the finite containment problem (the finite equality problem) for reversible Petri nets and commutative semigroups.

Theorem 8 *The finite containment problem (the finite equality problem) for reversible Petri nets and commutative semigroups is exponential space complete with respect to log-lin reducibility.*

Proof: Let $\mathcal{P}$ be the commutative semigroup presentation, and u, $v \in X^*$ the two words of Proposition 4, and $\mathcal{Q} = \emptyset$ the empty commutative semigroup presentation. Then

$$[v]_\mathcal{Q} = \{v\} \subseteq [u]_\mathcal{P} \quad \Longleftrightarrow \quad v \equiv u \bmod \mathcal{P}.$$

Thus, an exponential space complete word problem reduces to FCP for commutative semigroups, which together with Corollary 1 establishes the exponential space completeness of FCP (FEP) for reversible Petri nets and commutative semigroups. □

4 The Equivalence Problem for Commutative Semigroups

The equivalence problem for commutative semigroups, or equivalently, reversible Petri nets is the problem of deciding for any two given congruence classes $[u]_\mathcal{P}$, $[v]_\mathcal{Q}$,

where $\mathcal{P}$, $\mathcal{Q}$ are two commutative semigroup presentations over some alphabet X, and u, v are two words in X^*, whether $[u]_{\mathcal{P}}$ is equal to $[v]_{\mathcal{Q}}$.

Using the results of the previous section we are able to prove an exponential work space upper bound for the equivalence problem.

Theorem 9 *Let $\mathcal{P}$, $\mathcal{Q}$ be two finite commutative semigroup presentations over $X = \{x_1, \ldots, x_k\}$, and u, v two words in X^*. Then there is an algorithm which decides whether $[u]_{\mathcal{P}}$ is equal to $[v]_{\mathcal{Q}}$ using at most space $2^{c \cdot \max\{\text{size}(u,\mathcal{P}),\text{size}(v,\mathcal{Q})\}} \leq 2^{c \cdot \text{size}(u,v,\mathcal{P},\mathcal{Q})}$, where c is some constant independent of u, v, $\mathcal{P}$ and $\mathcal{Q}$.*

For the proof of this Theorem we note that X^* is isomorphic to $\mathbb{N}^k$ and that the congruence classes in $\mathbb{N}^k$ are uniformly semilinear sets (see [ES69]), *i.e.,*

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

for some vectors $a_j, b^{(1)}, \ldots, b^{(t)} \in \mathbb{N}^k$, $j = 1, \ldots, n$. Thus, the congruence class $[u]_{\mathcal{P}}$ is completely determined by its minimal elements (w.r.t. divisibility) a_j and its minimal periods (w.r.t. divisibility) $b^{(i)}$. The proof of Theorem 9 follows from the next theorem.

Theorem 10 *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$ be a finite commutative semigroup presentation over X, and $u \in X^*$. Then there is an algorithm which generates a closed representation of $[u]_{\mathcal{P}}$ using at most space $2^{c \cdot \text{size}(u,\mathcal{P})}$, where $c > 0$ is some constant independent of u and $\mathcal{P}$.*

Proof: If $[u]_{\mathcal{P}}$ is bounded, then, by Theorem 6, there is an algorithm which generates the elements of $[u]_{\mathcal{P}}$ using at most space $(\text{size}(u, \mathcal{P}))^2 \cdot 2^{\bar{c} \cdot k}$, where $\bar{c} > 0$ is some constant independent of u and $\mathcal{P}$. In the following we assume that $[u]_{\mathcal{P}}$ is unbounded, *i.e.* the set of periods $P_{[u]_{\mathcal{P}}} = \{\sum_{i=1}^{t} n_i b^{(i)}; n_i \in \mathbb{N}\}$ of the congruence class $[u]_{\mathcal{P}}$ is not the empty set.

First we show that the minimal periods $b^{(i)}$ of the uniformly semilinear set $[u]_{\mathcal{P}}$ can be determined using at most space $2^{c_1 \cdot \text{size}(u,\mathcal{P})}$, where $c_1 > 0$ is some constant independent of u and $\mathcal{P}$. Then we show a $2^{c_2 \cdot \text{size}(u,\mathcal{P})}$ space bound for the minimal elements a_j of $[u]_{\mathcal{P}}$, where $c_2 > 0$ is some constant independent of u and $\mathcal{P}$.

The bound for the minimal periods $b^{(i)}$ of $[u]_{\mathcal{P}}$ can be derived from the bound for the subword problem in Theorem 4. To see this we briefly review a useful property of subtractive submonoids in $\mathbb{N}^k$.

A submonoid P of $\mathbb{N}^k$ is said to be *subtractive* (see [ES69]), if p, $p + q \in P$ with $q \in \mathbb{N}^k$ implies $q \in P$. Note that the set of periods $P_{[u]_{\mathcal{P}}}$ of $[u]_{\mathcal{P}}$ in $\mathbb{N}^k$ is a subtractive submonoid of $\mathbb{N}^k$. The set of the nonzero minimal elements of P w.r.t. the canonical partial ordering of $\mathbb{N}^k$ is denoted by $\text{Min}(P)$. From the work in [Huy85] and [SW70] we know the following:

Proposition 5 [Huy85], [SW70] *Let $P \subset \mathbb{N}^k$ be a subtractive submonoid, and let $\mathcal{I}$ be the set of all minimal subsets $I \subseteq I_k$ such that* $\text{Min}(P) \cap \{p = (p_1, \ldots, p_k) \in$

$\mathbb{N}^k \mid p_j > 0$ *for* $j \in I$, $p_j = 0$ *for* $j \notin I\}$ *contains exactly one element* p^I. *Let* $U = \{p^I \mid I \in \mathcal{I}\}$. *Then every* $p \in \mathrm{Min}(P) - U$ *can be written as*

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

We call the elements p^I of U *extreme minimal periods.*

Let $p^I = (p_1^I, \ldots, p_k^I)$ be some extreme minimal period of $P_{[u]_\mathcal{P}}$. Since $[u]_\mathcal{P}$ is a uniformly semilinear set and p^I is a period of $[u]_\mathcal{P}$, *i.e.*, $p^I \in P_{[u]_\mathcal{P}}$, the word $v = u \cdot x_1^{p_1^I} \cdots x_k^{p_k^I}$ is an element of $[u]_\mathcal{P}$. From Theorem 4 it follows that v, and thus p^I, can be determined in space $(\mathrm{size}(u,\mathcal{P}))^2 \cdot 2^{c_1' \cdot k}$ for some constant $c_1' > 0$ independent of u and $\mathcal{P}$. By Proposition 5, the minimal periods $b^{(i)}$ can be written as

$$b^{(i)} = \sum_{p^I \in U} \varrho_I \cdot p^I\,, \quad \varrho_I \in \mathbb{Q}^+,\ 0 \le \varrho_I < 1,$$

where U is the set of the extreme minimal periods p^I of $P_{[u]_\mathcal{P}}$, and hence can be determined in space $(\mathrm{size}(u,\mathcal{P}))^2 \cdot 2^{c_1'' \cdot k}$ for some constant $c_1'' > 0$ independent of u and $\mathcal{P}$.

For determining the minimal elements of $[u]_\mathcal{P}$, we first consider the commutative semigroup presentation $\mathcal{P}'$ obtained from $\mathcal{P}$ by the same way as in Section 3.2. Since $[u]_\mathcal{P}$ is unbounded, Lemma 2, 3, and 4 have to be modified slightly. The proofs of the resulting lemmata are analogous to the proofs of the corresponding lemmata in Section 3.2.

Lemma 7 *For some* $v \in X^*$, *every word* $w \in [s \cdot v]_{\mathcal{P}'}$ *satisfies the following conditions:*

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

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

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

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

if $\Phi(w,t)=1$, *then* $x_1^{\Phi(w,x_1)+\Phi(w,y_1)} \cdot x_2^{\Phi(w,x_2)+\Phi(w,y_2)} \cdots x_k^{\Phi(w,x_k)+\Phi(w,y_k)} \cdot u \in [v]_\mathcal{P}$,

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

Lemma 8 *For some* $v \in X^*$ *let* $s \cdot w \in [s \cdot v]_{\mathcal{P}'}$ *with* $w \in X^*$, $w \neq v$, *and let* $s \cdot v = \gamma_0 \to \gamma_1 \to \ldots \to \gamma_n = s \cdot w$ *be any repetition-free derivation in* $\mathcal{P}'$ *leading from* $s \cdot v$ *to* $s \cdot w$. *Then there must be some* $i \in I_{n-1}$ *with* $\gamma_i = s \cdot y(u) \cdot \overline{v}$, $\gamma_{i+1} = t \cdot \overline{v}$, $\overline{v} \in \{x_1, \ldots x_k, y_1, \ldots y_k, z_1, \ldots z_k\}^*$, $x_1^{\Phi(\overline{v},x_1)+\Phi(\overline{v},z_1)} \cdot x_2^{\Phi(\overline{v},x_2)+\Phi(\overline{v},z_2)} \cdots x_k^{\Phi(\overline{v},x_k)+\Phi(\overline{v},z_k)} = v$, *and some* $j \in I_{n-1}$, $j > i$, *with* $\gamma_j = t \cdot \overline{w}$, $\gamma_{j+1} = s \cdot y(u) \cdot \overline{w}$, $\overline{w} \in \{x_1, \ldots x_k, y_1, \ldots y_k, z_1, \ldots z_k\}^*$, $x_1^{\Phi(\overline{w},x_1)+\Phi(\overline{w},z_1)} \cdot x_2^{\Phi(\overline{w},x_2)+\Phi(\overline{w},z_2)} \cdots x_k^{\Phi(\overline{w},x_k)+\Phi(\overline{w},z_k)} = w$.

Lemma 9 *Let* v, w *be two words in* X^*, *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* $\overline{w}$.

Thus, for all minimal elements a_j of $[u]_{\mathcal{P}}$ w.r.t. divisibility, from Theorem 2 it follows that $s \cdot a_j \in LT(I(\mathcal{P}'))$. Furthermore, if $s \cdot v \in LT(I(\mathcal{P}'))$ for some $v \in X^*$, then there is some $w \in [v]_{\mathcal{P}}$ such that u divides w. Hence, for all words $v \in X^*$ with $s \cdot v \in LT(I(\mathcal{P}'))$, and all periods $p = (p_1, \ldots, p_k) \in P_{[u]_{\mathcal{P}}}$, we have that $v \cdot x_1^{p_1} \cdots x_k^{p_k}$ is an element of $[v]_{\mathcal{P}}$. Especially, this is true for the minimal (w.r.t. divisibility) elements H' of $LT(I(\mathcal{P}'))$, which, by Theorem 3, can be determined in space $2^{\overline{c} \cdot \mathrm{size}(u,\mathcal{P})}$ for some constant $\overline{c} > 0$ independent of u and $\mathcal{P}$.

Now we project $[u]_{\mathcal{P}}$ onto the bounded coordinates. The set $X_b \subseteq X$ of the bounded coordinates can be found using the exponential space algorithm for the selfcoverability problem for commutative semigroups described in [KM95]. This algorithm is based on the following proposition:

Proposition 6 [KM95] *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$, and $u \in X^*$. Then for $j \in I_k$ the following are equivalent:*

(i) There exist $p_1, \ldots, p_h, q_j \in \mathbb{Q}[X]$ such that

$$\sum_{i=1}^{h} p_i(l_i - r_i) = u \cdot x_j \cdot q_j - u$$

(ii) There is a derivation $u = \gamma_0 \to \gamma_1 \to \ldots \to \gamma_n = v(\mathcal{P})$ leading from u to some $v \in [u]_{\mathcal{P}}$ such that u is a proper subword of v, $\Phi(v, x_j) > \Phi(u, x_j)$, and for $\tilde{n} \in I_n$

$$\mathrm{length}(\gamma_{\tilde{n}}) \leq \max\{\deg(l_i p_i),\ \deg(r_i p_i);\ i \in I_h\}.$$

From Dickson's Lemma we can derive that an element x_j of X is in X_b iff there is no $v \in [u]_{\mathcal{P}}$ such that u is a proper subword of v, and $\Phi(v, x_j) > \Phi(u, x_j)$. Thus, by Proposition 6 and Proposition 2, for every $j \in I_k$ it can be decided whether $x_j \in X_b$ using at most space $2^{d \cdot \mathrm{size}(u,\mathcal{P})}$ for some constant $d > 0$ independent of u and $\mathcal{P}$.

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 Theorem 6, there is an algorithm which generates the elements of $[u_b]_{\mathcal{P}_b}$ using at most space $(\mathrm{size}(u_b, \mathcal{P}_b))^2 \cdot 2^{c_2' \cdot k} \leq (\mathrm{size}(u, \mathcal{P}))^2 \cdot 2^{c_2' \cdot k}$, where $c_2' > 0$ is some constant 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 4, this computation requires at most space $(\mathrm{size}(u, \mathcal{P}))^2 \cdot 2^{c_2'' \cdot k}$ for some constant $c_2'' > 0$ independent of u and $\mathcal{P}$.

In the following we show that the representative $\overline{u}$ together with the minimal periods of $[u]_{\mathcal{P}}$ provides all minimal elements a_j of $[u]_{\mathcal{P}}$ with $(a_j)_b = \overline{u}_b$. We consider the words in X^* as vectors in $\mathbb{N}^k$. Let $Z(\overline{u}) \subseteq \mathbb{Z}^k$ denote the set $\left\{\overline{u} + \sum_{i=1}^{t} z_i b^{(i)}; z_i \in \mathbb{Z} \text{ for } i = 1, \ldots, t\right\}$ 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 $a_j \in Z(\overline{u})$. Assume that $a \in \mathbb{N}^k$

is a minimal element of $[u]_{\mathcal{P}}$ w.r.t. divisibility such that $a_b = \overline{u}_b$, and some of its entries are greater than $2^{2^{c_2 \cdot \text{size}(u,\mathcal{P})}}$, where $c_2 > 0$ is some constant specified below. Since $s \cdot a \in LT(I(\mathcal{P}'))$, there is some $s \cdot h_a \in H'$ such that h_a divides a. We know that $h_a + P_{[u]_{\mathcal{P}}} \subseteq [h_a]_{\mathcal{P}}$, and moreover, $v + P_{[u]_{\mathcal{P}}} \subseteq [v]_{\mathcal{P}}$ for all $v \in \mathbb{N}^k$ such that h_a divides v.

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

Let a' be an element in M such that $a' + P_{[u]_{\mathcal{P}}}$ contains a. Then $a = a' + t$ for some $t \in \mathbb{N}^k - \{0\}$. 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 minimal elements a_j of the uniformly semilinear set $[u]_{\mathcal{P}}$ can be determined using at most space $2^{c_2 \cdot \text{size}(u,\mathcal{P})}$. □

Now we are able to prove the main result, Theorem 9.

Proof of Theorem 9: Equality of $[u]_{\mathcal{P}}$ and $[v]_{\mathcal{Q}}$ can be tested by the exponential space algorithm given in Figure 1.

Since the word problems occuring in this algorithm, by Proposition 3, can be decided using at most space $2^{\bar{c} \cdot \max\{\text{size}(u,\mathcal{P}),\text{size}(v,\mathcal{Q})\}}$ for some constant $\bar{c} > 0$ independent of u, v, $\mathcal{P}$ and $\mathcal{Q}$, this algorithm can be implemented on a Turing machine with space bound $2^{c \cdot \max\{\text{size}(u,\mathcal{P}),\text{size}(v,\mathcal{Q})\}} \leq 2^{c \cdot \text{size}(u,v,\mathcal{P},\mathcal{Q})}$ for some constant $c > 0$ independent of u, v, $\mathcal{P}$ and $\mathcal{Q}$. □

Corollary 2 *The equivalence problem for reversible Petri nets and commutative semigroups is exponential space complete with respect to log-lin reducibility.*

Proof: Since FEP for reversible Petri nets, or equivalently, commutative semigroups is a special case of the equivalence problem, and because of Theorem 8 and Theorem 9 we conclude the assertion. Together with Theorem 9 this fact establishes the exponential space completeness of the equivalence problem for reversible Petri nets and commutative semigroups. □

5 Conclusion

The results obtained in this paper show that the equivalence problem for commutative semigroups is decidable in space $2^{c \cdot n}$, where n is the size of the problem instance, and c is some constant independent of n. This space bound is optimal up to the size of the constant c. 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].

Furthermore, we provide asymptotically optimal decision procedures for the subword and finite enumeration problems for commutative semigroups. These procedures also require at most space $2^{d \cdot n}$. An immediate consequence of this complexity

The Algorithm

Input: $u, v \in X^*$
$\mathcal{P}$, $\mathcal{Q}$ two commutative semigroup presentations over X
Output: $[u]_{\mathcal{P}} \stackrel{?}{=} [v]_{\mathcal{Q}}$

if ($u \equiv v \bmod \mathcal{P}$ **and** $u \equiv v \bmod \mathcal{Q}$) **then**
  for each $a \in X^*$ with degree $\leq 2^{2^{c_1 \cdot \min\{\mathrm{size}(u,\mathcal{P}),\mathrm{size}(v,\mathcal{Q})\}}}$ **do**
    if (($a \equiv u \bmod \mathcal{P}$ **and** $a \not\equiv v \bmod \mathcal{Q}$) **or**
        ($a \not\equiv u \bmod \mathcal{P}$ **and** $a \equiv v \bmod \mathcal{Q}$)) **then**
      reject
    end_if
  end_for
  for each $b \in X^*$ with degree $\leq 2^{2^{c_2 \cdot \min\{\mathrm{size}(u,\mathcal{P}),\mathrm{size}(v,\mathcal{Q})\}}}$ **do**
    if (($u \equiv u \cdot b \bmod \mathcal{P}$ **and** $v \not\equiv v \cdot b \bmod \mathcal{Q}$) **or**
        ($u \not\equiv u \cdot b \bmod \mathcal{P}$ **and** $v \equiv v \cdot b \bmod \mathcal{Q}$)) **then**
      reject
    end_if
  end_for
  accept
  else reject
end_if

Figure 1: The exponential space algorithm for deciding the equivalence problem for commutative semigroups (for suitable constants c_1 and c_2)

bound for the finite enumeration problem is an analogous bound for the finite containment problem for commutative semigroups. Again, these results are asymptotically optimal, and we establish the exponential space completeness of the subword, finite enumeration and finite containment problems for commutative semigroups.

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

References

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

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

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

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

[Hac76] Michel Hack. Decidability questions for Petri nets. Technical Report 161, Laboratory for Computer Science, M.I.T., June 1976.

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

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

[Hi64a] Heisuke Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero: II. *Ann. of Math.*, 79(2):205–326, 1964.

[Huy85] D.T. Huynh. 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)*, pages 405–412, New York, 1985. ACM, ACM Press.

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

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

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

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

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

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

[Par81] D. Park. Concurrency and automata on infinite sequences. In *Proceedings of the 5th GI Conference on Theoretical Computer Science*, volume 104 of *LNCS*, pages 167–183, New York, 1981. Springer Verlag.

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

[SW70] J. Stoer and C. Witzgall. Convexity and optimization in finite dimensions I. 1970. 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.