# 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 Boundedness, Coverability, and Selfcoverability Problems for Commutative Semigroups


Ulla Koppenhagen
Ernst W. Mayr



TUM-I9518
Mai 1995


TECHNISCHE UNIVERSITÄT MÜNCHEN

TUM-INFO-05-1995-I9518-350/1.-FI


Typescript: ---

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

# The Complexity of the Boundedness, Coverability, and Selfcoverability Problems for Commutative Semigroups

Ulla Koppenhagen, Ernst W. Mayr

May 22, 1995

**Abstract**

In this paper, efficient decision procedures for the boundedness, coverability and selfcoverability 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 constant independent of $n$. Furthermore, we show that this space requirement is inevitable: *any* decision procedure for these problems requires at least exponential space. Thus, we establish the exponential space completeness of the boundedness, coverability and selfcoverability problems for commutative semigroups.

## 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 *boundedness, coverability* and *selfcoverability* problems. These were first shown to be decidable by Karp and Miller [KM69], but their algorithm, which constructs what was later called the *coverability tree*, requires non-primitive recursive space. Subsequently Lipton [Lip76] proved that deciding the boundedness and the covering problems require at least space $2^{c \cdot \sqrt{n}}$, where $n$ is the size of the problem instance, and $c$ is some constant independent of $n$. Finally, Rackoff [Rac78] obtained a $2^{c \cdot n \log n}$ space upper bound for the boundedness, coverability and selfcoverability problems. Until now it is an open problem whether the gap between the upper and the lower bounds can be reduced.

For an important subclass of commutative semi-Thue systems, the class of commutative Thue-systems (or equivalently, reversible vector addition systems or Petri nets), we present here efficient decision procedures for the boundedness, coverability and selfcoverability problems which operate in space $2^{c \cdot n}$. We show in Sections 4 and 5 below that the three problems are straightforwardly reducible to the polynomial ideal membership problem, which is known to be exponential space complete (see [May89]). Furthermore, we show that the exponential space requirement is inevitable: *any* decision procedure for these problems requires at least exponential space. The proof in Section 6 of this lower bound on the complexity of the problems is based on reducing a special form of the uniform word problem, which is exponential space complete (see [MM82]), to the boundedness problem. Thus, we establish the exponential space completeness of the boundedness, coverability, and selfcoverability problems.

The remainder of the paper is organized as follows. Basic definitions and notations concerning exponential space complexity, Thue systems and vector addition systems are contained in Section 2. In Section 3 we briefly introduce the boundedness, coverability and selfcoverability problems for commutative semigroups. As mentioned above, in Sections 4, 5, and 6 we prove the exponential space completeness of these three problems. Finally, Section 7 contains some concluding remarks.

# 2 Basic Definitions and Notations

## 2.1 Exponential Space

We first briefly review the few necessary technical definitions from complexity theory.

Let $S_1, S_2$ be finite alphabets. A function $f : S_1^* \to S_2^*$ *reduces* a set $A \subseteq S_1^*$ to a set $B \subseteq S_2^*$ in case

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

for all $\alpha \in S_1^*$. If $f$ can be evaluated in logarithmic space, then $A$ is said to be *log-space reducible* to $B$. If in addition the length of $f(\alpha)$ is $\mathcal{O}(length(\alpha))$, then $A$ is *log-lin reducible* to $B$.

The set $B \subseteq S_2^*$ is said to be *decidable in space*[1] $g : \mathbb{N} \to \mathbb{N}$ if there is a Turing machine which accepts $B$ and visits at most $g(n)$ work tape squares during its computation on any word $\beta \in S_2^*$ of length $n$. (We assume the Turing machine has a read-only input tape and a write-only output tape separate from its work tape.)

$B$ 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*.

## 2.2 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 $S = \{s_1, \ldots, s_k\} \subseteq M$ if

$$M = \{u | u = \underbrace{s_1 \ldots s_1}_{e_1} \underbrace{s_2 \ldots s_2}_{e_2} \ldots \underbrace{s_k \ldots s_k}_{e_k}, e_i \in \mathbb{N}, s_i \in S\}.$$

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

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

$$u = \underbrace{s_1 \ldots s_1}_{e_1} \underbrace{s_2 \ldots s_2}_{e_2} \cdots \underbrace{s_k \ldots s_k}_{e_k} \quad \Longleftrightarrow \quad \varphi(e_1, \ldots, e_k) = u.$$

If $\varphi$ 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 $S = \{s_1, \ldots, s_k\}$, $S^*$ denotes the free commutative monoid generated by $S$.

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

For an element $u$ of $S^*$, called a (commutative) word, the order of the symbols is immaterial, and we shall in the sequel use an exponent notation: $u = s_1^{e_1} \cdots s_k^{e_k}$, where $e_i = \Phi(u, s_i) \in \mathbb{N}$ for $i = 1, \ldots, k$. For instance, we may denote $s_1 s_2 s_1 s_1 s_3 s_3 s_2$ by $s_1^3 s_2^2 s_3^2$, interchangeably with, say, $s_1^2 s_3 s_1 s_2^2 s_3$.

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

A *commutative semi-Thue system* over $S$ is given by a finite set $\mathcal{P}$ of productions $l_i \to r_i$, where $l_i$, $r_i \in S^*$. A word $v \in S^*$ *is derived in one step* from $u \in S^*$ (written $u \to v(\mathcal{P})$) by application of the production $(l_i \to r_i) \in \mathcal{P}$ iff, for some $w \in S^*$, 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 $\to$. A sequence $(u_0, \ldots, u_n)$ of words $u_i \in S^*$ 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 $\mathcal{P}$.

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 $S^*$ 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* $S^*/\equiv_{\mathcal{P}}$.

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.

## 2.3 Vector Addition Systems and Uniformly Semilinear Sets

Since $S^*$ is isomorphic to $\mathbb{N}^k$ with $k = \mathrm{Card}(S)$, we may, for notational convenience, consider a congruence on $S^*$ as a congruence on $\mathbb{N}^k$. Thus, a presentation of the quotient semigroup $S^*/\equiv_{\mathcal{P}}$ is a presentation of the quotient semigroup $\mathbb{N}^k/\equiv_{\mathcal{P}}$, where $\mathcal{P} \subset \mathbb{N}^k \times \mathbb{N}^k$ is a finite set of pairs of vectors with nonnegative integer entries and $\equiv_{\mathcal{P}}$ is the congruence on $\mathbb{N}^k$ generated by $\mathcal{P}$. Define the mapping $\Delta$ from $\mathbb{N}^k \times \mathbb{N}^k$ into $\mathbb{Z}^k$ by $\Delta((u,v)) := v - u$. Thus we get a *vector addition system* or *VAS*, which is a pair $(x, V)$. The vector $x \in \mathbb{N}^k$ is called the *start vector*, the integer $k$ is the *dimension* of the VAS, and $V = \Delta(\mathcal{P}) \subset \mathbb{Z}^k$ is a finite set of *transition vectors*. Define $\mathcal{P}^{-1}$ to be the set $\{(v,u) | (u,v) \in \mathcal{P}\}$, and let $V = \Delta(\mathcal{P}) \cup \Delta(\mathcal{P}^{-1})$. Then $(x, V)$ is a *reversible* VAS. The *reachability set* of a VAS $(x, V)$ is the smallest set $R(x, V)$ satisfying the following two properties:

(i) $x \in R(x, V)$

(ii) whenever $z \in R(x, V)$, $v \in V$, and $z + v \in \mathbb{N}^k$ then $z + v \in R(x, V)$; i.e., $R(x, V)$ is closed under addition of transition vectors as long as the sum has only nonnegative components.

A *transition sequence* $\left(v^{(i)}\right)_{1 \le i \le t}$ of transition vectors $v^{(i)}$ is *applicable* to some vector $y \in \mathbb{N}^k$ if $y + \sum_{j=1}^{i} v^{(j)} \in \mathbb{N}^k$ for all $i = 1, \ldots, t$. In this case, the vector $z = y + \sum_{j=1}^{t} v^{(j)}$ is called *reachable from $y$ in $(x, V)$*, and the transition sequence is called a *derivation* (of length $t$) of $z$ from $y$. To denote this, we also use (see above) $y \xrightarrow{*} z \ (\mathcal{P})$. Thus, $R(x, \Delta(\mathcal{P})) = \{z | \ x \xrightarrow{*} z \ (\mathcal{P})\}$.

**Definition 1** *A* linear *subset $L$ of $\mathbb{N}^k$ is a set of the form*

$$L = \left\{ a + \sum_{i=1}^{t} n_i b^{(i)}; \ n_i \in \mathbb{N} \text{ for } i = 1, \ldots, t \right\}$$

*for some vectors $a, b^{(1)}, \ldots, b^{(t)} \in \mathbb{N}^k$.*

*A* semilinear *set $SL$ is a finite union of linear sets:*

$$SL = \bigcup_{j=1}^{n} \left\{ a_j + \sum_{i=1}^{t_j} n_i b_j^{(i)}; n_i \in \mathbb{N} \text{ for } i = 1, \ldots, t_j \right\}$$

*for some vectors $a_j, b_j^{(1)}, \ldots, b_j^{(t_j)} \in \mathbb{N}^k$, $j = 1, \ldots, n$.*

*A* uniformly semilinear *subset $UL$ of $\mathbb{N}^k$ is a set of the form*

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

*for some vectors $a_j, b^{(1)}, \ldots, b^{(t)} \in \mathbb{N}^k$, $j = 1, \ldots, n$.*

From the work in [ES69], we can derive the following:

**Proposition 1** *Let $\equiv$ be any congruence relation on $\mathbb{N}^k$. Then the congruence class $[u]$ of any element $u \in \mathbb{N}^k$ with respect to $\equiv$ is a uniformly semilinear set in $\mathbb{N}^k$.*

If we have a reversible VAS $(x, V)$ the above proposition says that the reachability set $R(x, V)$ is a uniformly semilinear set.

## 3 The Boundedness, Coverability, and Selfcoverability Problems for Commutative Semigroups

We know that the congruence classes of commutative semigroups (resp., the reachability sets of reversible VAS's) are uniformly semilinear. In the following sections we shall see that the decision procedures for the boundedness, coverability, and selfcoverability problems are exponential space complete with respect to log-lin reducibility.

Let $\leq$ be the canonical partial order on $\mathbb{N}^k$, i.e., $\forall v, w \in \mathbb{N}^k$: $v \leq w \iff \exists x \in \mathbb{N}^k$ : $x + v = w$. If $v \leq w$ but $v \neq w$, i.e., $\exists x \in \mathbb{N}^k$, $x \neq 0$ : $x + v = w$, then we write $v < w$. We will use the same order on $S^*$ ($S = \{s_1, \ldots s_k\}$), i.e., $\forall u, v \in S^*$:

$$u \leq v \iff (\Phi(u, s_1), \ldots, \Phi(u, s_k)) = (d_1, \ldots, d_k) \leq (e_1, \ldots, e_k) = (\Phi(v, s_1), \ldots, \Phi(v, s_k)),$$

resp.,

$$u < v \iff (\Phi(u, s_1), \ldots, \Phi(u, s_k)) = (d_1, \ldots, d_k) < (e_1, \ldots, e_k) = (\Phi(v, s_1), \ldots, \Phi(v, s_k))$$

where $u = s_1^{d_1} \cdots s_k^{d_k}$, $v = s_1^{e_1} \cdots s_k^{e_k}$.

The *boundedness problem* for commutative semigroups (resp., reversible VAS's) is to determine for $S^*/\equiv_{\mathcal{P}}$ (resp., $\mathbb{N}^k/\equiv_{\mathcal{P}}$) and a word $u \in S^*$ (resp., a vector $u \in \mathbb{N}^k$), if the congruence class $[u]$ of $u$ (resp., $R(u, \Delta(\mathcal{P}))$ is finite. Such a *boundedness problem instance* is denoted by a tuple $(u, \mathcal{P})$.

The *coverability problem* is to determine for $S^*/\equiv_{\mathcal{P}}$ (resp., $\mathbb{N}^k/\equiv_{\mathcal{P}}$) and two words $u, v_1 \in S^*$ (resp., two vectors $u, v_1 \in \mathbb{N}^k$), if there is a derivation of some $v_2 \in [u]$ (resp., $v_2 \in R(u, \Delta(\mathcal{P}))$ from $u$ such that $v_2 \geq v_1$. Such a *coverability problem instance* is denoted by a triple $(u, v_1, \mathcal{P})$.

The *selfcoverability problem* is to determine for a word $u \in S^*$ (resp., a vector $u \in \mathbb{N}^k$), if there is a derivation of some $v \in [u]$ (resp., $v \in R(u, \Delta(\mathcal{P}))$ from $u$ such that $v > u$. Such a *selfcoverability problem instance* is denoted by a tuple $(u, \mathcal{P})$.

**Lemma 1** *Let $\equiv$ be any congruence relation on $\mathbb{N}^k$. Then the congruence class $[u]$ of any element $u \in \mathbb{N}^k$ with respect to $\equiv$ is unbounded iff there are $v_1$, $v_2 \in [u]$ with $v_1 > v_2$.*

**Proof:**

$\Longrightarrow$: Follows immediately from Dickson's Lemma.

$\Longleftarrow$: $v_1 > v_2$ means that there is an $x \in \mathbb{N}^k$, $x \neq 0$, with $v_1 = v_2 + x \in [u]$. Since $\equiv$ is a congruence relation, and $v_2 \in [u]$ and $v_2 + x \in [u]$ we know that $v_2 + x + x \in [u]$, $v_2 + x + x + x \in [u], \ldots$, i.e., we can add $x$ infinitely often to $v_2$ without leaving the congruence class $[u]$. So $[u]$ is unbounded.

$\square$

**Lemma 2** *Let $\equiv$ be any congruence relation on $\mathbb{N}^k$. Then the congruence class $[u]$ of any element $u \in \mathbb{N}^k$ with respect to $\equiv$ is unbounded iff there is a $v \in [u]$ with $v > u$.*

**Proof:**

$\Longrightarrow$: With the above Lemma we have $v_1,\ v_2 \in [u]$ with $v_1 = v_2 + x,\ x \in \mathbb{N}^k,\ x \neq 0$. Since $\equiv$ is a congruence relation, and $v_2 \in [u]$ and $v_2 + x \in [u]$ we get $v := u + x \in [u]$, $v > u$.

$\Longleftarrow$: See proof of the above Lemma.

□

# 4 Polynomial Ideals

Let $X$ denote the finite set $\{x_1, \ldots, x_k\}$, and $\mathbb{Q}[X]$ (resp., $\mathbb{Z}[X]$) the (commutative) ring of polynomials with indeterminates $x_1, \ldots, x_k$ and rational (resp., integer) coefficients. For $g_1, \ldots, g_h \in \mathbb{Q}[X]$, let $\langle g_1, \ldots, g_h \rangle \subseteq \mathbb{Q}[X]$ denote the ideal generated by $\{g_1, \ldots, g_h\}$, that is[2]

$$\langle g_1, \ldots, g_h \rangle := \left\{ \sum_{i=1}^{h} p_i g_i;\ p_i \in \mathbb{Q}[X] \ \text{ for } \ i \in I_h \right\}.$$

The *polynomial ideal membership problem PI* is defined to be

$$\{(g_0, g_1, \ldots, g_h)\,; g_0 \text{ is in the ideal } \langle g_1, \ldots, g_h \rangle\}$$

Then a *PI problem instance* is denoted by a tuple $(g_0, g_1, \ldots, g_h)$.

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 unary monomial $u = x_1^{\Phi(u,x_1)} \cdots x_k^{\Phi(u,x_k)}$. For a monomial $v$ we let $I_{\mathbb{Q}}(\mathcal{P}, v)$ (resp., $I_{\mathbb{Z}}(\mathcal{P}, v)$) be the $\mathbb{Q}[X]$-ideal (resp., $\mathbb{Z}[X]$-ideal) generated by $\{l_1 - r_1, \ldots, l_h - r_h, vx_1, \ldots, vx_k\}$, i.e.,

$$I_R(\mathcal{P}, v) := \left\{ \sum_{i=1}^{h} p_i (l_i - r_i) + \sum_{j=1}^{k} v x_j q_j;\ p_i, q_j \in R[X] \ \text{ for } \ i \in I_h, j \in I_k \right\}$$

for $R = \mathbb{Q}, \mathbb{Z}$.

Let $<$ be the partial order on the set of monomials in $X$ which results from the partial order on the Parikh mappings of the monomials, i.e.,

$$u < v \Longleftrightarrow (\Phi(u, x_1), \ldots, \Phi(u, x_k)) = (d_1, \ldots, d_k) < (e_1, \ldots, e_k) = (\Phi(v, x_1), \ldots, \Phi(v, x_k)),$$

where $u = x_1^{d_1} \cdots x_k^{d_k}, v = x_1^{e_1} \cdots x_k^{e_k}$.

The following lemma shows the connection between the membership problem for ideals in $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$ and the boundedness, coverability, and selfcoverability problems for commutative semigroups.

**Lemma 3** *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$, and $u,\ v_1 \in X^*$. Then the following are equivalent:*

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

*(i) There exist* $p_1, \ldots, p_h, q_1, \ldots, q_k \in \mathbb{Q}[X]$ *such that*

$$\sum_{i=1}^{h} p_i(l_i - r_i) = v_1 \sum_{j=1}^{k} x_j q_j - u$$

*(ii)* $\exists\, v_2 \in X^*,\ v_2 > v_1,\ v_2 \equiv u \bmod \mathcal{P}$.

**Proof:**
(i) $\Longrightarrow$ (ii):
We show that if

$$\sum_{i=1}^{h} p_{1i}(l_i - r_i) + \sum_{i=1}^{h} p_{2i}(r_i - l_i) = v_1 \sum_{j=1}^{k} x_j q_j - u$$

for $p_{1i},\ p_{2i} \in \mathbb{Q}^+[X]$, $q_j \in \mathbb{Q}[X]$, then there is a derivation of $v_2$, $v_2 > v_1$, $v_2 \equiv u$ in $\mathcal{P}$. Let $d \in \mathbb{N}$ be a common denominator for all the rational coefficients in the $p_{1i}$, $p_{2i}$, $i \in I_h$, and $q_j$, $j \in I_k$. Then we may assume

$$\sum_{m_1=1}^{n_1} p'_{1m_1}(l_{i_{m_1}} - r_{i_{m_1}}) + \sum_{m_2=1}^{n_2} p'_{2m_2}(r_{i_{m_2}} - l_{i_{m_2}}) - v_1 \sum_{l=1}^{n_3} x_{j_l} q'_l = -du$$

for some $n_1,\ n_2,\ n_3 \geq 1$, where $p'_{1m_1}, p'_{2m_2} \in \mathbb{N}[X]$, $m_1 \in I_{n_1}$, $m_2 \in I_{n_2}$, are monomials with coefficient $+1$, $q'_l \in \mathbb{Z}[X]$, $l \in I_{n_3}$, are monomials with coefficient $\pm 1$, and $\deg(p'_{1m_1}) \leq \deg(p_{1i_{m_1}})$, $\deg(p'_{2m_2}) \leq \deg(p_{2i_{m_2}})$, and $\deg(q'_l) \leq \deg(q_{j_l})$ for $m_1 \in I_{n_1}$, $m_2 \in I_{n_2}$, $l \in I_{n_3}$. As $u$ appears as a term on the right hand side of this polynomial identity there must be some $s \in I_{n_1}$ such that $u = r_{i_s} p'_{1s}$, or some $s \in I_{n_2}$ such that $u = l_{i_s} p'_{2s}$, implying

(i) $\displaystyle\sum_{m_1 \in I_{n_1} - \{s\}} p'_{1m_1}(l_{i_{m_1}} - r_{i_{m_1}}) + \sum_{m_2 \in I_{n_2}} p'_{2m_2}(r_{i_{m_2}} - l_{i_{m_2}}) - v_1 \sum_{l=1}^{n_3} x_{j_l} q'_l$
$\displaystyle\qquad = -(d-1)u - l_{i_s} p'_{1s}$

(ii) $u \longrightarrow l_{i_s} p'_{1s} =: w_1$

or

(i) $\displaystyle\sum_{m_1 \in I_{n_1}} p'_{1m_1}(l_{i_{m_1}} - r_{i_{m_1}}) + \sum_{m_2 \in I_{n_2} - \{s\}} p'_{2m_2}(r_{i_{m_2}} - l_{i_{m_2}}) - v_1 \sum_{l=1}^{n_3} x_{j_l} q'_l$
$\displaystyle\qquad = -(d-1)u - r_{i_s} p'_{2s}$

(ii) $u \longrightarrow r_{i_s} p'_{2s} =: w_1$,

or there must be some $t \in I_{n_3}$ such that $u = v_1 x_{j_t} q'_t$. In the case $u = v_1 x_{j_t} q'_t$ we are finished. Otherwise we may repeat the above argument for $l_{i_s} p'_{1s}$ resp., $r_{i_s} p'_{2s}$ in place of $u$, and by induction obtain a derivation

$$u \longrightarrow w_1 \longrightarrow \ldots \longrightarrow w_{n'} = v_1 x_{j_t} q'_t = v_2 > v_1$$

with $n' \leq n_1 + n_2$, where each $w_g$, $g < n'$, is of the form $l_{i_s} p'_{1s}$ or $r_{i_s} p'_{2s}$ for some $s = s(g) \in I_{n_1},\ I_{n_2}$.

(ii) $\Longleftarrow$ (i):

We show that if $v_2 \equiv u \bmod \mathcal{P}$, $v_2 > v_1$, then $v_1 x_t q_t - u \in I_{\mathbb{Z}}(\mathcal{P}, v)$ for some $t \in I_k$ and some term $q_t \in \mathbb{Z}[X]$.

Suppose $u = w_0 \longrightarrow \ldots \longrightarrow w_n = v_1 x_t q_t = v_2$. Then, for $m \in I_n$, there are $z_m \in X^*$ such that

$$w_{m-1} = l_{i_m} z_m \quad \text{and} \quad w_m = r_{i_m} z_m$$

and hence

$$v_2 - u = \sum_{m=1}^{n} (r_{i_m} - l_{i_m}) z_m \in I_{\mathbb{Z}}(\mathcal{P}).$$

□

If, in Lemma 3, $v_1 \neq u$, we have a mapping from the coverability problem instance $(u, v_1, \mathcal{P})$ to the PI problem instance $(u, v_1 x_1, \ldots, v_1 x_k, l_1 - r_1, \ldots, l_h - r_h)$. If $v_1 = u$, we have a mapping from the selfcoverability problem instance $(u, \mathcal{P})$ and, with Lemma 2, also from the boundedness problem instance $(u, \mathcal{P})$ to the PI problem instance $(u, v_1 x_1, \ldots, v_1 x_k, l_1 - r_1, \ldots, l_h - r_h)$. The mappings are computationally trivial and size preserving, so that the boundedness, coverability, and selfcoverability problems are log-lin reducible to PI.

# 5 An Exponential Space Upper Bound

From the work in [MM82] and [May89], we know that the polynomial ideal membership problem is exponential space complete. This fact and Lemma 3 of the previous section easily yield:

**Theorem 1** *Let $S = \{s_1, \ldots, s_k\}$ and $\mathcal{P} = \{l_i \equiv r_i;\ i \in I_h\}$ be a commutative semigroup presentation over $S$. Then, for $u, v_1 \in S^*$, there is an algorithm which decides for any instance $(u, v_1, \mathcal{P})$ whether there is $v_2 \in S^*$, $v_2 > v_1$, $v_2 \equiv u \bmod \mathcal{P}$ using at most space $2^{c \cdot \mathrm{size}(u, v_1, \mathcal{P})}$, where $c > 0$ is some universal constant independent of $(u, v_1, \mathcal{P})$.*

**Proof:**
From Lemma 3 we know that the coverability problem instance $(u, v_1, \mathcal{P})$ is log-lin reducible to the PI problem instance $(u, v_1 s_1, \ldots, v_1 s_k, l_1 - r_1, \ldots, l_h - r_h)$. Furthermore, the PI problem is solvable in exponential space (see [May89]).

□

**Corollary 1** *Let $S = \{s_1, \ldots, s_k\}$ and $\mathcal{P} = \{l_i \equiv r_i;\ i \in I_h\}$ be a commutative semigroup presentation over $S$. Then, for $u \in S^*$, there is an algorithm which decides for any instance $(u, \mathcal{P})$ whether there is $v \in S^*$, $v > u$, $v \equiv u \bmod \mathcal{P}$ using at most space $2^{c \cdot \mathrm{size}(u, \mathcal{P})}$, where $c > 0$ is some universal constant independent of $(u, \mathcal{P})$.*

**Proof:**
Follows immediately from Theorem 1 with $v_1 = u$.

□

**Corollary 2** *Let $S = \{s_1, \ldots, s_k\}$ and $\mathcal{P} = \{l_i \equiv r_i;\ i \in I_h\}$ be a commutative semigroup presentation over $S$. Then, for $u \in S^*$, there is an algorithm which decides for any instance $(u, \mathcal{P})$ whether the congruence class $[u]$ is finite using at most space $2^{c \cdot \mathrm{size}(u, \mathcal{P})}$, where $c > 0$ is some universal constant independent of $(u, \mathcal{P})$.*

**Proof:**
With Lemma 2 this corollary follows immediately from Corollary 1.

$\square$

# 6 An Exponential Space Lower Bound

This section provides a proof for the exponential space hardness of the boundedness, coverability, and selfcoverability problems. The proof is based on reducing a special form of the uniform word problem for commutative semigroups, which in the common form is the problem of deciding for a commutative Thue system $\mathcal{P}$ over $S$ and two words $u, v \in S^*$ whether $u \equiv v \bmod \mathcal{P}$, to the boundedness problem. 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:

**Proposition 2** *Let $\mathcal{P}'$ be a finite commutative semigroup presentation over $S$ and $u, v \in S^*$ two words such that (i) $[u]$ is bounded and (ii) $v$ is not a proper subword of any word in $[u]$. Even with these restrictions, 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.*

If we add to $\mathcal{P}'$ of the above Proposition the equivalence $v \equiv vt$, where $t$ is a new symbol $\notin S$ and $v$ is not a proper subword of any word in $[u]$, then the uniform word problem, i.e. the problem of deciding whether $u \equiv v \bmod \mathcal{P}$, with $\mathcal{P} = \mathcal{P}' \cup \{v \equiv vt\}$ and $[u]$ bounded in $\mathcal{P}'$, remains exponential space complete.

**Lemma 4** *Let $u, v \in S^*$ be the two words and $\mathcal{P}$ the finite commutative semigroup presentation from above. Then we have:*

$$u \equiv v \bmod \mathcal{P} \Longleftrightarrow [u] \textit{ is unbounded.}$$

**Proof:**
$[u]$ is bounded in $\mathcal{P} - \{v \equiv vt\}$. Therefore the only way for $[u]$ to be unbounded in $\mathcal{P}$ is that the number of occurences of $t$ in the words congruent to $u$ get infinite by means of the equivalence $v \equiv vt$. Since $v$ is not a proper subword of any word in $[u]$, we have $u \equiv v \bmod \mathcal{P}$, iff $[u]$ is unbounded.

$\square$

Now we can prove the following:

**Theorem 2** *The boundedness, coverability, and selfcoverability problems for commutative semigroups are exponential space complete with respect to log-lin reducibility.*

**Proof:**
Lemma 4 shows that an exponential space complete word problem reduces to the unboundedness resp. boundedness problem (the class of exponential space complete problems is closed under complement) and, with Lemma 2, also to the selfcoverability (resp., coverability) problem. The reduction is computationally trivial and size preserving, hence log-lin.

$\square$

# 7 Conclusion

By reducing the boundedness, coverability, and selfcoverability problems for commutative semigroups to the polynomial ideal membership problem we have shown that they are decidable in space $2^{c \cdot n}$, where $n$ is the size of the problem instance, and $c$ is some constant independent of $n$. Furthermore, we established the exponential space completeness of the three problems by reducing a special form of the uniform word problem to the boundedness problem.

In [Huy85] Huynh exhibited a decision algorithm for the equivalence problem for commutative semigroups, which is the problem of deciding for two commutative Thue systems $\mathcal{P}$, $\mathcal{Q}$ over $S$ and two words $u, v \in S^*$, whether $[u]_{\mathcal{P}} = [v]_{\mathcal{Q}}$. This algorithm operates in space $2^{c \cdot N \log N}$, where $N$ is the size of the problem instance, and $c$ is some constant independent of $N$. The arguments for this upper bound are based on the $2^{c' \cdot N' \log N'}$ space upper bound for the coverability and selfcoverability problems obtained by Rackoff [Rac78]. But notice that Rackoff's size $N'$ of the coverability problem instance does *not* contain the size of the word at the beginning of the covering derivation, whereas our size $n$ of the coverability problem instance contains it. Because of this difference it remains an open question to improve the upper bound for the equivalence problem for commutative semigroups.

# References


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

[Hac74] Michel Hack. Petri nets and commutative semigroups. Computation Structures Note 18, Project MAC, MIT, July 1974.

[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.

[Huy86] D.T. Huynh. A superexponential lower bound for Gröbner bases and Church-Rosser commutative Thue systems. *Inf. Control*, 68(1-3):196–206, 1986.

[KBLM89] Hans Kleine Büning, Theodor Lettmann, and Ernst W. Mayr. Projections of vector addition system reachability sets are semilinear. *Theor. Comput. Sci.*, 64:343–350, 1989.

[KM69] R.M. Karp and R.E. Miller. Parallel program schemata. *J. Comput. Syst. Sci.*, 3:147–195, 1969.

[Lip76] Richard Lipton. The reachability problem requires exponential space. Research Report 62, Computer Science Dept., Yale University, January 1976.

[May89] Ernst W. Mayr. Membership in polynomial ideals over $\mathbb{Q}$ is exponential space complete. In B. Monien and R. Cori, editors, *Proceedings of the 6th Annual Symposium on Theoretical Aspects of Computer Science (Paderborn, FRG,* *February 1989)*, LNCS 349, pages 400–406, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong, 1989. GI, afcet, Springer-Verlag.

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

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