The Complexity of the Equivalence Problem for Commutative Semigroups and Symmetric Vector Addition Systems

Dung T. Huynh
Computer Science Department
Iowa State University
Ames, Iowa 50011

ABSTRACT

This paper shows that the equivalence problems for commutative semigroups and symmetric vector addition systems are decidable in space $c^{N\log N}$ for some fixed constant c, solving an open question by Cardoza, Lipton, Mayr, and Meyer. From the exponential-space completeness of the word problems, it follows that our upper bound is nearly optimal.

0. Introduction.

Commutative semi-Thue Systems (or equivalently, Petri nets or vector addition systems) are well known models for parallel processes. Considerable effort has gone into the study of mathematical properties of these models. In particular, decidability and complexity questions of decision problems for these models, such as the reachability and equality problems, have received much attention.

It has been shown by Rabin that the containment problem for commutative semi-Thue systems is undecidable. A formal proof for this result together with the result for the equality problem can be found in [Hac-76]. Concerning the reachability problem, a decidability proof has been provided recently by Mayr [May-84].

A natural subclass of commutative semi-Thue systems is the class of commutative Thue systems (or equivalently, reversible Petri nets or symmetric vector addition systems). In this case, the reachability problem and the equality problem may be formulated as the (uniform) word problem and the equivalence problem for commutative semigroups, which have been shown by several researchers, including Malcev, Biryukov, Emilicev and Taiclin, to be decidable.

Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage, the ACM copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Association for Computing Machinery. To copy otherwise, or to republish, requires a fee and or specific permission.

© 1985 ACM 0-89791-151-2/85/005/0405 $00.75

The decidability of the above two decision problems for commutative semigroups raises the natural question about their intrinsic complexity. For the word problem, Cardoza, Lipton and Meyer reported in [CLM-76] a result that this problem is complete for exponential space. A formal proof for this result has been provided by Mayr and Meyer in [MM-82]. For the equivalence problem, no complexity result is known. Indeed, Cardoza, Lipton and Meyer in [CLM-76], and Mayr and Meyer in [MM-82] have stated as an open problem the question whether the equivalence problem is primitive recursive. In this paper, we provide an affirmative answer by showing that this problem can be decided even in space $c^{N\log N}$ for some fixed constant c.

This paper is organized as follows. Basic definitions, notations and statements of the results are contained in Section 1, where a brief sketch of the proof idea of our main result is presented. Section 2 introduces some algebraic notions used for characterizing the structure of congruence classes in commutative semigroups. To make the paper self-contained, we include in Section 3 the result on the coverability problem by Rackoff, which is formulated as a commutative semigroup problem. In Section 4, we slightly extend Rackoff's result for the boundedness problem for vector addition systems so that we obtain efficient procedures for the self-coverability and strict self-coverability problems. The results of Section 4 will then be applied in Section 5 to provide an efficient procedure for testing units in commutative semigroups. Section 6 presents the proof of the main result and the final section (Section 7) contains some concluding remarks.

1. Preliminaries and Results.

In this paper $\mathbb{N}$ denotes the set of nonnegative integers, $\mathbb{Z}$ the set of integers, $\mathbb{Q}$ the set of rationals and $\mathbb{Q}_+$ the set of nonnegative rationals respectively. For a finite alphabet S, $S^\oplus$ denotes the free commutative monoid generated by S.

A presentation of a finitely generated commutative semigroup is a pair (S,P), where S is a finite alphabet and $P \subseteq S^\oplus \times S^\oplus$ is a finite set of defining relations. (S,P) represents the factor semigroup $S^\oplus/P$, that is the factor semigroup of $S^\oplus$

by the congruence on S^o defined by P.

Since S^o is isomorphic to $\mathbb{N}^k$ with k=Card(S), we may, for notational convenience, consider a congruence on S^o as a congruence on $\mathbb{N}^k$. Thus, a presentation (of a finitely generated commutative semigroups) is a pair $(\mathbb{N}^k,P)$, where $P \subseteq \mathbb{N}^k \times \mathbb{N}^k$ is a finite set of pairs of vectors with nonnegative integer entries. The congruence on $\mathbb{N}^k$ generated by P is denoted by $\sim(P)$. If $u, v \in \mathbb{N}^k$ are congruent modulo $\sim(P)$, we write $u \sim v (\mathrm{mod}\ P)$.

Definition 1.1. The word problem (for commutative semigroups) is the following decision problem:

Input. A relation system $P \subseteq \mathbb{N}^k \times \mathbb{N}^k$ and $u, v \in \mathbb{N}^k$.

Question. Is $u \sim v (\mathrm{mod}\ P)$?

The equivalence problem (for commutative semigroups) is the following decision problem:

Input. Two relation systems $P, Q \subseteq \mathbb{N}^k \times \mathbb{N}^k$ and $u, v \in \mathbb{N}^k$.

Question. Is $[u]_P = [v]_Q$?

where $[u]_P, [v]_Q$ denote the congruence classes of u by $\sim(P)$ and v by $\sim(Q)$ repsectively.

Whereas the word problem is complete for exponential-space under log-lin reductions[1], there is no upper bound for the equivalence problem, except the well-known result that it is decidable. The main goal of this paper is to provide an upper bound for the complexity of the equivalence problem. In obtaining this result, we will be considering two other decision problems, namely the coverability and self-coverability problems, which are introduced in the following. We first define some technical notions.

Definition 1.2. Let $k \in \mathbb{N}$, $k \geq 1$, and $P \subseteq \mathbb{N}^k$ be a finite set of relations[2].

Define P^{-1} to be the set $\{(v,u) \mid (u,v) \in P\}$. Define the mapping Δ from $P \cup P^{-1}$ into $\mathbb{Z}^k$ by $\Delta((u,v)) := v - u$. Δ is extended to a homomorphism from $(P \cup P^{-1})^*$ into $\mathbb{Z}^k$ by $\Delta(p_1 \ldots p_m) := \sum_{j=1}^{m} \Delta(p_j)$, and this extension is also denoted by Δ.

A finite sequence ω of vectors in $\mathbb{Z}^k$, $\omega = (w_0,\ldots,w_m)$ is called a path in P if for every $j = 1,\ldots,m$ there is some $p \in P \cup P^{-1}$, $p = (u,v)$, such that $w_j - w_{j-1} = \Delta(p)$. w_0, w_m are the start and final vectors of ω respectively. The yield of ω, denoted by $\tau(\omega)$, is $w_m - w_0$.

Let $1 \leq i \leq k$ be some fixed integer. Let $r \in \mathbb{N}$, $r \geq 1$. A vector $w \in \mathbb{Z}^k$ is said to be (i,r)-bounded if the first i components of w are nonnegative and less than r. The jth component of $w \in \mathbb{Z}^k$ is denoted by w(j), where $1 \leq j \leq k$. $\pi_i : \mathbb{Z}^k \to \mathbb{Z}^i$ denotes the projection on the first i components.

A path $\omega = (w_0,\ldots,w_m)$ is said to be (i,r)-bounded if each of its elements if (i,r)-bounded and for each $j = 0,\ldots,m-1$ there is $(u,v) \in P \cup P^{-1}$ with $\pi_i(u) \leq \pi_i(w_j)$ and $w_{j+1} - w_j = \Delta((u,v))$. An (i,∞)-bounded path is called a derivation in P.

Let $y \in \mathbb{Z}^k$. A path ω in P with final vector v is called an i-covering path for y if for every $j = 1,\ldots,i$, $v(j) \geq y(j)$. A k-covering path for y is simply called a covering path for y.

Let $I \subseteq \{1,\ldots,k\}$. $\mathbb{N}_I^k := \{x \in \mathbb{N}^k \mid x(j) \geq 0$ for $j \in I$, and $x(j) = 0$ for $j \notin I\}$. A path $\omega = (w_0,\ldots,w_m)$ is called I-self-covering if there is some j, $0 \leq j < m$, such that $w_j \neq w_m$ and $w_m - w_j \in \mathbb{N}_I^k$. In case $I = \{1,\ldots,k\}$, ω is simply called a self-covering path.

We now define the coverability and self-coverability problems.

Definition 1.3. The coverability problem is the following decision problem:

Input. A finite set of relations $R \subseteq \mathbb{N}^k \times \mathbb{N}^k$ and $u, v \in \mathbb{N}^k$.

Question. Is there any derivation starting at u that is a covering path for v?

The self-coverability problem is the following decision problem:

Input. A finite set of relations $R \subseteq \mathbb{N}^k \times \mathbb{N}^k$, a subset $I \subseteq \{1,\ldots,k\}$ and $u \in \mathbb{N}^k$.

Question. Is there any derivation starting at u that is an I-self-covering path?

The results of this paper are the following:

Result 1. The self-coverability problem is decidable in space $c^{N \log N}$, where N is the input size and c is some fixed constant.

Result 2. (Main Result) The equivalence problem is decidable in space $c^{N \log N}$, where N is the input size and c is some fixed constant.

Remark. Result 1 is a slight extension of Rackoff's result on the boundedness problem for vector addition systems. (See Section 4.)

We now define the size of input instances. The size of nonnegative integer is the length of its binary representation without leading zeros. In accordance with the size definition in [MM-82], we define the size of 0 to be 0. (Note that in [Rac-78], the size of 0 is defined to be 1.) The size of a vector with integer entries is defined to be the sum of the sizes of its entries. The size of an input instance is the sum of the sizes of those vectors occurring in that instance.

Remark. W.l.o.g. we may assume that the dimension (k) is bounded by the size of the input instance, since if such an input instance is presented in terms of generating symbols and relations, we may

---

[1] Log-lin reductions are log-space computable reductions that have linearly length-bounded outputs. For complexity notions the reader is referred to [HU-79].

[2] We assume w.l.o.g. that if $(u,v) \in P$, then $(v,u) \notin P$.

BIBLIOTHÈQUE
FACULTÉ
des SCIENCES
PARIS
INFORMATIQUE-RECHERCHE

assume that every generating symbol must appear in some word in the input instance. Also note that if N is the size of some input instance, then all integers in that instance are bounded by 2^N.

The proof idea of the main result is as follows. We first show an algebraic characterization of the structure of congruence classes. Essentially, this characterization states that a **congruence class is completely determined by its minimal elements and its minimal "periods".** We then show that an upper bound for certain periods can be obtained, using the result on the self-coverability problem. This upper bound yields a similar upper bound for **all minimal periods.** Applying the result on the coverability problem, an upper bound of the same order of magnitude for **all minimal elements can be obtained.** Using the decision procedures for the coverability and self-coverability problems, we obtain a decision procedure for the equivalence problem that operates within the desired space bound.

2. Congruence Classes and Subtractive Submonoids.

In this section we want to show an algebraic characterization of the structure of congruence classes in $\mathbb{N}^k$. More precisely, we will prove that a congruence class is the 'sum' of its minimal elements with a submonoid in $\mathbb{N}^k$ that is a subtractive submonoid. It turns out that subtractive submonoids enjoy several nice properties. In particular, a subtractive submonoid can be generated by its nonzero minimal elements. We will show that the nonzero minimal elements of a subtractive submonoid can be bounded by those nonzero minimal elements that are extreme points of the cone in $\mathbb{Q}_+^k$ generated by the submonoid itself.

Definition 2.1. Define the partial order $\leq$ on $\mathbb{Z}^k$ as follows. For $x, y \in \mathbb{Z}^k$, $z \leq y$ iff $x(j) \leq y(j)$ for all $j = 1,\ldots,k$. We write $x < y$ if $x \leq y$ and $x \neq y$.

An element $x \in \mathbb{Z}^k$ is nonnegative if $x \in \mathbb{N}^k$. For a subset $I \subseteq \{1,\ldots,k\}$, $x \in \mathbb{Z}^k$ is I-positive if $x \in \mathbb{N}_I^k$ and $x(j) > 0$ for all $j \in I$. X is positive if it is $\{1,\ldots,k\}$-positive.

For two subsets $X, Y \subseteq \mathbb{Z}^k$, $X + Y$ denotes the set $\{x + y \mid x \in X, y \in Y\}$. If $X = \{x\}$, we also write $x + Y$.

For a subset $X \subseteq \mathbb{N}^k$, Min(X) or Min X denotes the set of all elements in X that are minimal w.r.t. $\leq$. For $y \in \mathbb{N}^k$, we write $X - y$ to denote $\{x \in \mathbb{N}^k \mid y + x \in X\}$.

Remark. It is a well-known result that Min(X) is finite for any subset X of $\mathbb{N}^k$. (Cf. e.g. [ES-69].)

Definition 2.2. A submonoid M of $\mathbb{N}^k$ is said to be subtractive ([ES-69]) if $x, x + z \in M$ imply $z \in M$, where $z \in \mathbb{N}^k$. We call a nonzero element of M a period or unit. The set of nonzero minimal elements of M is denoted by Min M. For a subset X of $\mathbb{Z}^k$, $\ll X \gg$ denotes the submodule of $\mathbb{Z}^k$ generated by X. For a subset U of $\mathbb{N}^k$, $\langle U \rangle$ denotes the submonoid of $\mathbb{N}^k$ generated by U.

Proposition 2.3. ([Hu-84]) Let Q be a congruence on $\mathbb{N}^k$. For every $x \in \mathbb{N}^k$, $[x]_Q - x$ is a subtractive submonoid of $\mathbb{N}^k$. Furthermore, if $x \sim y \pmod{Q}$, then $[x]_Q - x = [y]_Q - y$. □

Notation. In view of Proposition 2.3, we denote the subtractive submonoid $[x]_Q - x$ by $M_Q(x)$.

Proposition 2.4. ([Hu-84]) Let Q be a congruence on $\mathbb{N}^k$. Then for every $x \in \mathbb{N}^k$, it holds that $[x]_Q = \mathrm{Min}[x]_Q + M_Q(x)$. □

Remark. From Proposition 2.4 it follows that $[x]_Q$ is determined if $\mathrm{Min}[x]_Q$ and a set of generators for $M_Q(x)$ are determined.

Proposition 2.5. ([Hu-84]) Let $M \subseteq \mathbb{N}^k$ be a submonoid. Then M is subtractive iff M is the intersection of a submodule of $\mathbb{Z}^k$ with $\mathbb{N}^k$. In particular, it holds that $\langle \mathrm{Min}\ M \rangle = M$ and $\ll \mathrm{Min}\ M \gg \cap \mathbb{N}^k = M$. □

In the remainder of this section, we derive some more properties of subtractive submonoids which will be used in the proof of the main result.

Definition 2.6. The rank of a submodule Z of $\mathbb{Z}^k$ is the dimension of the linear subspace of $\mathbb{Q}^k$ generated by Z. The rank of a subtractive submonoid M is the rank of the submodule $\ll M \gg$.

For a subset $U \subseteq \mathbb{N}^k$, the cone generated by U, denoted by K(U), is the following subset of $\mathbb{Q}_+^k$:

$$K(U) = \{ \textstyle\sum_{u \in U} p_u u \mid p_u \in \mathbb{Q}_+ \}.$$

U is a generating system for K(U), $u \in U$ is an extreme point of K(U) if it is not a linear combination with strictly positive coefficients of any two points of K(U). The set of all extreme points of U forms a generating system for K(U).

Proposition 2.7. Let M be a subtractive submonoid of rank $k' \leq k$, $M \subseteq \mathbb{N}^k$. Let $\mathbf{I}$ be the set of all minimal subsets $I \subseteq \{1,\ldots,k\}$ such that $\mathrm{Min}\ M \cap \mathbb{N}_I^k$ contains exactly one element. Let

$$U := \{\mathrm{Min}\ M \cap \mathbb{N}_I^k \mid I \in \mathbf{I}\}.$$

Then it holds that $K(U) = K(M)$.

Proof. The proof is omitted. □

Proposition 2.8. Let $M \subseteq \mathbb{N}^k$ be a subtractive submonoid with rank $k' \leq k$. Further let U be as in Proposition 2.7. Then for every $x \in (\mathrm{Min}\ M) \setminus U$, x can be written as

$$x = \textstyle\sum_{u \in U'} p_u u, \quad p_u \in \mathbb{Q}_+, \ 0 \leq p_u < 1,$$

where $U' \subseteq U$ is a subset of k' linearly independent vectors.

Proof. Let $x \in (\mathrm{Min}\ M) \setminus U$. Then $x \in K(U)$. By Caratheorory's Theorem for cones (Cf. [SW-70], p. 35), there is a subset $U' \subseteq U$ of k' linearly independent vectors such that $x \in K(U')$, i.e.

$$x = \textstyle\sum_{u \in U'} p_u u, \quad p_u \in \mathbb{Q}_+.$$

We claim that $p_u < 1$ for all $u \in U'$. Other-

wise define

$$x' := x - \sum_{u \in U^*} \lfloor p_u \rfloor u ,$$

where $\lfloor p \rfloor$ denotes the greatest integer $\leq p$, $p \in \mathbb{Q}$. Obviously, $x' \in \mathbb{N}^k$. Since M is subtractive, we have $x' \in M$. Now, $x' < x$ and $x' \in M$ imply that x is not minimal, a contradiction! □

3. The Coverability Problem.

In this section we want to show that the coverability problem is decidable in space $c^{N\log N}$, where c is some fixed constant. The proof is essentially similar to that in [Rac-78].

In this section we fix a positive integer k, a vector $v \in \mathbb{N}^k$ and a relation system $P \subseteq \mathbb{N}^k \times \mathbb{N}^k$. Let N denote the sum of the sizes of v and P.

For any $x \in \mathbb{Z}^k$ define f(i,x) to be the length of a shortest i-bounded, i-covering path in P for v starting at x if such a path exist; f(i,x) = 0 otherwise. Define

$$f(i) := \text{Max}\{f(i,x) \mid x \in \mathbb{Z}^k\}.$$

Thus f(k) gives us an upper bound for the length of some minimal length derivation in P starting at any $x \in \mathbb{N}^k$ that is a covering path for v. In the following we derive an upper bound for f(k).

Fact 3.1. $f(0) = 1$. □

Lemma 3.2. $f(i+1) \leq (2^N f(i))^{i+1} + f(i)$ for all $i = 0,\ldots,k-1$.

Proof. The proof is omitted. □

Lemma 3.3. $f(k) \leq 2^{2^{cN\log N}}$, where c is some fixed constant. □

Corollary 3.4. For any $x \in \mathbb{N}^k$, if there is a derivation in P starting at x that is a covering path for v, then there is one of length $\leq 2^{2^{cN\log N}}$, where c is the constant in Lemma 3.3 □

Theorem 3.5. ([Rac-78]) The coverability problem is decidable in space $c^{N\log N}$, where c is some fixed constant. □

4. The Self-Coverability Problem.

In this section we will show that the self-coverability problem is decidable in space $c^{N\log N}$ for some fixed constant c. This slightly extends the result in [Rac-78] on the boundedness problem. The technique of this section will be applied in the next section to show how to test whether a large vector belongs to the subtractive submonoid of a congruence class.

In the following we fix a positive integer k, a relation system $P \subseteq \mathbb{N}^k \times \mathbb{N}^k$ and a subset $I \subseteq \{1,\ldots,k\}$. Let $0 \leq i \leq k$. For any $x \in \mathbb{Z}^k$ define g(i,x) to be the length of a shortest i-bounded, I-self-covering path in P starting at x if such a path exists, otherwise g(i,x) := 0. Define

$$g(i) := \text{Max}\{g(i,x) \mid x \in \mathbb{Z}^k\}.$$

We are interested in obtaining an upper bound for g(k). The following lemma will be needed.

Lemma 4.1. ([GS-78]) Let $A \in \mathbb{Z}^{m\times n}$, $B \in \mathbb{Z}^{q\times n}$, $a \in \mathbb{Z}^{m\times 1}$, $b \in \mathbb{Z}^{q\times 1}$, be $(m \times n)$-, $(q \times n)$-, $(m \times 1)$-, $(q \times 1)$- matrices respectively. Let s be the rank of the $((m+q) \times n)$- matrix $\begin{bmatrix} A \\ B \end{bmatrix}$. Let r be the maximum of the absolute values of all entries of A, B, a, b.

If the system of equalities $A.x = a$ and inequalities $B.x \geq b$ has a nonnegative integer solution, then it has one with entries bounded by $(n+1)(sr^2)^{s/2}$. □

Let $0 \leq i \leq k$ and $r \in \mathbb{N}$, $r > 1$. In order to obtain an upper bound for g(k), we have to derive an upper bound for the length of a shortest (i,r)-bounded, I-self-covering path in P starting at any $x \in \mathbb{Z}^k$ if such a path exists (Lemma 4.6).

We first introduce some technical notions and make some observations.

Consider a minimal length (i,r)-bounded, I-self-covering path in P starting at $x \in \mathbb{Z}^k$. Let ω be this path:

$$\omega = (x=v_1, v_2, \ldots, v_{m_1}, w_1, w_2, \ldots, w_{m_2}),$$

where $w_1 < w_{m_2}$ and $w_{m_2} - w_1 \in \mathbb{N}_I^k$.

Let $\omega_1 := (v_1,\ldots,v_{m_1})$ and $\omega_2 := (w_1,\ldots,w_{m_2})$. Let $\pi_i : \mathbb{Z}^k \to \mathbb{Z}^i$ be the projection on the first i components. (If i=0, then $\mathbb{Z}^0 := \emptyset$.) Consider the projection of ω on the first i components:

$$\pi_i(\omega) = (\pi_i(v_1),\ldots,\pi_i(v_{m_1}),\pi(w_1),\ldots,\pi_i(w_{m_2})).$$

Observe that all elements on $\pi_i(\omega_1)$ are pairwise distinct, since otherwise ω_1 can be shortened and ω is not of minimal length. Thus, $m_1 \leq r^i \leq r^k$. Consider $\pi_i(\omega_2)$. We will show that if m_2 is too large, then ω_2 consists of "loops" so that certain "loops" can be eliminated to yield a new path w'_2 starting at w_1. Then the concatenation of ω_1 and ω'_2 is an (i,r)-bounded, I-self-covering path starting at x that has a bounded length.

Definition 4.2. For two paths ω, ω' in P with the property that the final vector of ω is equal to the start vector of ω', ωω' denotes the concatenation of ω with ω'.

Let $\alpha = p_1 \ldots p_k \in (P \cup P^{-1})'$ and $v \in \mathbb{Z}^k$. Then path (v,α) denotes the path

$$(v, v+\Delta(p_1), \ldots, v + \sum_{j=1}^{k} \Delta(p_j)).$$

If path(v,α) is (i,r)-bounded, then α is said to be i-valid (or simply valid) for v. If path(v,α) is valid for v and the projections of its start and final vectors on the first i components are identical, then path(α) is called a loop at v. If all elements of a loop except the final vector are pairwise distinct, then it is called a simple loop.

The following facts will be useful. We use

the above notations, ω is an (i,r)-bounded, I-self-covering path and $\omega = \omega_1\omega_2$, where ω_1 has length $\leq r^k$. Let $\omega_2 = (w_1, w_2, \ldots, w_{m_2})$ and $\omega_2 = \text{path}(w_1, p_1 p_2 \cdots p_{m_2-1})$, where $p_1, \ldots, p_{m_2-1} \in (P \cup P^{-1})$.

Fact 4.3. Let $\lambda = w_{j_1} \ldots w_{j_2}$, $1 \leq j_1 \leq j_2 \leq m_2$, be a subpath of ω_2 that is a loop. Then the path $(w_1 \ldots w_{j_1})$ path $(w_{j_2}, p_{j_2}, \ldots p_{m_2-1})$ remains (i,r)-bounded. □

Fact 4.4. If $m_2 \geq r^k + 1$, then ω_2 contains loops.

Proof. ω_2 is (i,r)-bounded. Therefore, if $m_2 \geq r^k + 1$, then ω_2 has at least one pair of elements whose projections on the first i components are identical. The subpath with such a pair of elements as start and final vectors is certainly a loop. □

Fact 4.5. Let w_j be an element on ω_2, $1 \leq j \leq m_2$. If $\lambda = \text{path}(w, t_1 \ldots t_m)$ is a loop at w and $\pi_i(w_j) = \pi_i(w)$, then the path $(w_1 \ldots w_j)$ path $(w_j m t_1 \ldots t_m p_j \ldots p_{m_2-1})$ is (i,r)-bounded. □

Lemma 4.6. Let $0 \leq i \leq k$, $x \in \mathbf{Z}^k$, $r \in \mathbf{N}$, $r > 1$. If there is an (i,r)-bounded, I-self-covering path in P starting at x, then there is one of length $\leq r^{N^c}$, where c is some fixed constant independent of N, x, r.

Proof. As in the preceding discussion, let ω be an (i,r)-bounded, I-self-covering path in P starting at x. Let $\omega = \omega_2\omega_2$, where $\omega_2 = (w_1, \ldots, w_{m_2})$ with $w_{m_2} \neq w_1$ and $w_{m_2} - w_1 \in \mathbf{N}_I{}^k$. Further, let length of $\omega_1 \leq r^k$.

The proof idea is as follows. We show that if m_2 is too large, then ω_2 consists of a large number of simple loops so that many of them can be eliminated to yield a new path ω'_2. The path $\omega_1\omega'_2$ is then an (i,r) bounded I-self-covering path in P starting at x of length $\leq r^{N^c}$, where c is some fixed constant.

If $m_2 < (r^k + 1)^2$, then let ω'_2 be ω_2. Otherwise, assume that $m_2 \geq (r^k + 1)^2$. We first show that ω_2 is the "sum" of a short path of length $< (r^k + 1)^2$, say ω'_2, with simple loops.

Divide ω_2 into blocks of length $r^k + 1$, starting from the left. Since $m_2 \geq (r^k + 1)^2$, there are at least $(r^k + 1)$ blocks. On each block there is at least one element that occurs at least twice. Further, in some block, none of the elements occurs for the first time. This block contains a simple loop that can be removed so that the remaining path is, by Fact 4.3, still (i,r)-bounded. Repeat this procedure until a path of length $< (r^k + 1)^2$ results. Let ω'_2 be this path and L be the multiset[3] of simple loops obtained by the above process.

Claim. (1) ω'_2 is an (i,r)-bounded path starting at x.

(2) Let $\lambda \in L$ be a loop at v. Then there is some element w on ω'_2 such that $\pi_i(w) = \pi_i(v)$.

(3) There are at most $(2(2^N r^k) + 1)^k$ distinct loop yields. □

In the following we show how to obtain ω'_2 from ω''_2 by inserting simple loops into ω''_2. Let $\omega''_2 = \text{path}(w_1, t_1 \ldots t_m)$ and $\beta = t_1 \ldots t_m$. Let A be the k x n- matrix obtained from loop yield vectors written as column vectors.

Obviously, the following equality holds

$$(\S) \qquad \Delta(\beta) + \sum_{\lambda \in L} \Gamma(\lambda) = w_{m_2} - w_1 \ .$$

Let A_j, $j=1,\ldots,k$, denote the jth row of A. Further let $I' = \{j \mid (w_{m_2} - w_1)(j) \geq 1\}$. (Notice that $I' \subseteq I$.) Then the above equality implies that the system of euqalities

$$A_j z = -(\Delta(\beta))_j \ , \ j \notin I'$$

and inequalities

$$A_j z \geq 1 - (\Delta(\beta))_j \ , \ j \in I'$$

has a nonnegative integer solution, where z is a column vector of n unknowns.

Since the entries of A and $\Delta(\beta)$ are bounded by $2^N(r^k + 1)^2$ in absolute values, the above system of equalities and inequalities has, by Lemma 4.1, a nonnegative integer solution z_0 with entries bounded by

$$(n + 1)(k(2^N(r^k + 1)^2)2)^{k/2} \leq r^{N^d} \ ,$$

where d is some fixed constant. Furthermore, z_0 can be so chosen that z_0 is $\leq$ the solution obtained from (§). This implies that there are $\sum_{\ell=1}^{n} z_0(\ell)$ loops in L which provide a yield equal to $A\, z_0$. These loops can, by Fact 4.5, be inserted back into ω''_2 successively so that the resulting path ω'_2 is (i,r)-bounded.

Consider $\omega_1\omega'_2$. $\omega_1\omega'_2$ is obviously I-self-covering:

$$\Gamma(\omega'_2) = \Gamma(\omega''_2) + A\, z_0 = \Delta(\beta) + A\, z_0 \ (\neq 0) \in \mathbf{N}_I{}^k$$

The length of $\omega_1\omega'_2$ is bounded by

$$(r^k + 1)^2 + (r^k + 1)r^{N^d} \leq r^{N^c} \ ,$$

where c is some fixed constant. This completes the proof of Lemma 4.6. □ □

We are now in position to obtain an upper bound for g(k).

Lemma 4.7. $g(0) \leq 2^{N^c}$, where c is the constant in Lemma 4.6. □

Lemma 4.8. $g(i + 1) \leq (2^N g(i))^{N^c}$ for all $i = 0, \ldots, k-1$, where c is the constant in Lemma 4.6.

Proof. Let $x \in \mathbf{Z}^k$ such that there is an (i + 1)-bounded, I-self-covering path in P starting at x. Let this path be ω.

Case 1. ω is $(i + 1, 2^N g(i))$-bounded. By Lemma 4.6, there is an (i + 1)-bounded, I-self-covering path in P starting at x that has length

[3] That is an element may occur with multiplicity.

$\leq 2^N g(i))^{N^c}$.

Case 2. ω is not $(I + 1, 2^N g(i))$-bounded. Let

$\omega = (x = w_1,\ldots,w_1,w_{1+1},\ldots,w_m)$

so that $w_m - w_1 \in \mathbb{N}_I^k$ and $w_m \neq w_1$. Further let $\omega = \text{path}(x,p_1\ldots p_{m-1})$, where $p_1,\ldots,p_{m-1} \in P \cup P^{-1}$.

Let w_{m_0+1} be the first element of ω that is not $(i + 1, 2^N g(i))$-bounded. Then the subpath $(w_1,\ldots,w_{m_0})$ can be shortened so that no two elements agree on the first $(i + 1)$ components. We have $m_0 \leq (2^N g(i))^{i+1}$.

Now consider $(w_{m_0+1},\ldots,w_m)$. w.l.o.g. we may assume that $w_{m_0+1}(j + 1) \geq 2^N g(i)$. Since $(w_1,\ldots,w_m)$ is $(i + 1)$-bounded, the path $\text{path}(w_m,p_1\ldots p_{m-1})$ is also $(i + 1)$-bounded. Therefore

$\omega' := (w_1,\ldots,w_{m_0},w_{m_0+1},\ldots,w_m)\text{path}(w_m,p_1\ldots p_{m-1})$

is $(i + 1)$-bounded. In particular, the subpath $\text{path}(w_{m_0+1},p_{m_0+1}\ldots p_{m-1}p_1\ldots p_{m-1})$ of ω' is an $(i + 1)$-bounded, I-self-covering path in P that is also i-bounded and I-self-covering. By induction hypothesis, there is an i-bounded, I-self-covering path ω'' starting at w_{m_0+1} of length $\leq g(i)$.

Consider $(w_1,\ldots,w_{m_0},w_{m_0+1})\omega''$. This is an $(i + 1)$-bounded, I-self-covering path in P starting at w_1, since $w_{m_0+1}(i + 1) \geq 2^N g(i)$. The length of this path is bounded by $(2^N g(i))^{i+1} + g(i) \leq (2^N g(i))^{N^c}$, where c (assumed > 1) is the constant in Lemma 4.6. This completes the proof of Lemma 4.8. □

Lemma 4.9. $g(k) \leq 2^{2^{cN\log N}}$, where c is some fixed constant. □

Theorem 4.10. The self-coverability problem is decidable in space $c^{N\log N}$, where c is some fixed constant. □

The results obtained above can be strengthened slightly as follows.

Definition 4.11. A path $\omega = (w_1,\ldots,w_m)$ is said to be I-strictly-self-covering if $w_m - w_l$ is I-positive for some l, $1 \leq l < m$.

The strict self-coverability problem is defined as follows.

Input. A relation system $P \subseteq \mathbb{N}^k \times \mathbb{N}^k$, $x \in \mathbb{N}^k$ and $I \subseteq \{1,\ldots,k\}$.

Question. Is there any derivation in P starting at x that is an I-strictly-self-covering path?

Let $g_s(i)$ be defined as $g(i)$, where the phrase "I-self-covering" is replaced by "I-strictly-self-covering". Then a closer look at the proofs of Lemmas 4.6 - 4.8 yields the following.

Lemma 4.12. $g(k) \leq 2^{2^{cN\log N}}$, where c is some fixed constant. □

Theorem 4.13. The strict self-coverability problem is decidable in space $c^{N\log N}$, where c is some fixed constant. □

5. Testing for Units in Commutative Semigroups.

In Section 2, we proved that every congruence class is the "sum" of its minimal elements with its subtractive submonoid. Further, every subtractive submonoid is completely determined by its nonzero minimal elements. To test whether two subtractive submonoids are identical, we need only to check whether each nonzero minimal element of one subtractive submonoid belongs to the other and vice versa. The purpose of this section is to show that the test whether $u \in \mathbb{N}^k$ belongs to the subtractive submonoid of some congruence class in $\mathbb{N}^k$ can be performed efficiently, even when u is much larger than the size of the relation system. (Note that a direct application of the procedure for the word problem yields a much worse upper bound.)

In the following we fix a positive integer k, a relation system $P \subseteq \mathbb{N}^k \times \mathbb{N}^k$ and some $x \in \mathbb{N}^k$ so that the size of P is bounded by N. Let $u \in \mathbb{N}^k$, $u \neq 0$, so that its entries are bounded by $2^{e(N)}$, where $e:\mathbb{N}\to\mathbb{N}$ satisfies $e(n) \geq n$.

Definition 5.1. A path $\omega = (w_1,\ldots,w_m)$ is said to be u-self-covering if there is some l, $1 \leq l < m$, such that $w_m - w_l = u$.

Obviously, $u \in M_p(x)$ iff there is a derivation in P starting at x that is a u-self-covering path. We want to obtain, in terms of N and e(N), an upper bound for the length of such a path that is a shortest one.

Let $0 \leq i \leq k$. For $x \in \mathbb{Z}^k$ define $h(i,x)$ to be the length of a shortest i-bounded, u-self-covering path in P starting at x if such a path exists; otherwise $h(i,x) := 0$. Define

$h(i) := \text{Max}\{h(i,x) \mid x \in \mathbb{Z}^k\}$.

We want to obtain an upper bound for $h(k)$ in terms of N and e(N). In the following we fix a positive integer $r \geq 2^{e(N)}$.

Lemma 5.2. Let $0 \leq i \leq k$. If there exists some (i,r)-bounded, u-self-covering path in P starting at x, then there is one of length $\leq r^{N^c}$, where c is some fixed constant independent of N, x, u, r.

Proof. The proof of this lemma is similar to that of Lemma 4.6 and is omitted. □

Lemma 5.3. $h(0) \leq 2^{e(N)^c}$, where c-1 is the constant in Lemma 5.2. □

Lemma 5.4. $h(i + 1) \leq (2^N h(i))^{N^c}$ for all $i = 0,\ldots,k-1$, where c is the constant in Lemma 5.2. □

Lemma 5.5. $h(k) \leq 2^{e(N)c_2 dN\log N}$, where c, d are some fixed constants. □

Corollary 5.6. If $e(N) \leq 2^{c'N\log N}$ for some constand c', then $h(k) \leq 2^{2^{cN\log N}}$, where c is some fixed constant. □

Remark. Corollary 5.6 provides us an efficient procedure for testing whether $u \in M_p(x)$: search for a derivation in P starting at x that is a u-self-covering path of length $\leq 2^{2^{cN\log N}}$. The elements on such a path have sizes bounded by $c''^{N\log N}$ for some fixed constant c".

6. The Complexity of the Equivalence Problem.

In this section we will prove our main result. We first derive an upper bound for the entries of the nonzero minimal elements of the subtractive submonoid of a congruence class, using the results of the preceding sections. With this upper bound we then derive an upper bound for the entries of the minimal elements of a congruence class. This will be shown using the result on the coverability problem.

In the following we fix a positive integer k, a relation system $P \subseteq \mathbb{N}^k \times \mathbb{N}^k$ and a vector $x \in \mathbb{N}^k$. Let N be an upper bound for the sizes of P and x. Let M denote the subtractive submonoid $M_p(x)$. Further let U be the set of all nonzero extreme minimal elements defined in Proposition 2.7.

Lemma 6.1. Every nonzero extreme minimal element of M has size bounded by $c^{N\log N}$, where c is some fixed constant.

Proof. We apply the result on the strict self-coverability problem. As in Proposition 2.7, let $\mathbf{I}$ denote the set of all minimal subsets $I \subseteq \{1,\ldots,k\}$ such that $\mathrm{Min}\, M \cap \mathbb{N}_I^k$ has exactly one element. Let u_I denote $\mathrm{Min}\, M \cap \mathbb{N}_I^k$, $I \in \mathbf{I}$. Then u_I is I-positive.

By Lemma 4.12, there is for $I \in \mathbf{I}$ a derivation in P starting at x that is an I-strict-self-covering path ω of the form $\omega = (w_1,\ldots,w_1,\ldots,w_m)$ such that $w_m - w_1$ is I-positive and the length of ω is bounded by $2^{2^{c'N\log N}}$, where c' is some fixed constant. Since u_I is a minimal I-positive element in M, it follows that the size of u_I is bounded by $c^{N\log N}$, where c is some fixed constant. □

Corollary 6.2. Every nonzero minimal element of M has size bounded by $c^{N\log N}$, where c is some fixed constant.

Proof. This follows easily from Lemma 6.1 and Proposition 2.8. □

We next show an upper bound of the same order of magnitude for the minimal elements of $[x]_p$.

Lemma 6.3. Every minimal element of $[x]_p$ has size bounded by $c^{N\log N}$, where c is some fixed constant.

Proof. Let $m := 2^{2^{c_1 N\log N}}$, where c_1 is the constant in Lemma 3.3. Let $m' := 2^N(m+1)$. We first consider the case $M = \{0\}$. Let $y \in \mathrm{Min}[x]_p$ such that some of its entries are $> m'$. Since $y \sim x \pmod P$, there is a derivation in P starting at y that is a covering path for x. From Corollary 3.4, such a derivation can be chosen so that its length is bounded by m. It follows that the final vector of this path is $> x$, a contradiction!

Next consider the case $M \neq \{0\}$. Let $y \in \mathrm{Min}[x]_p$ so that some of its entries are $> 2^{2^{c_2 N\log N}}$, where c_2 is specified below. Then there is a derivation ω of length $\leq m$ that starts at y and has $v \in x + M$ as final vector. Let $\omega = \mathrm{path}(y, p_1 \cdots p_\ell)$, $\ell \leq m$.

Consider the path $\mathrm{path}(x, p_\ell p_{\ell-1} \cdots p_1)$. Let z be the final vector of this path. Then $y \in z + M$. We show that in $z + M$ there is some $y' < y$ such that $y' \sim x \pmod P$.

Fact 1. Define $E = \{w \in \mathbb{N}^k \mid \mathrm{path}(w, p_1 \cdots p_\ell)$ is a derivation in P$\}$. Then E is of the form $\mathrm{Min}\, E + \mathbb{N}^k$ and each element in Min E has entries bounded by m'.

Proof of Fact 1. Since $w \in E$ implies $w + w' \in E$ for every $w' \in \mathbb{N}^k$, it is obvious that E has the form $\mathrm{Min}\, E + \mathbb{N}^k$. The bound for elements in Min E obviously holds. □

We are now in position to define y'. Consider the intersection $(z + M) \cap E$, which is nonempty (since it contains y). This intersection is a set of the form $G + M$, where G is the set of all minimal elements. It can easily be shown that every element of G has entries bounded by $2^{2^{c_2 N\log N}}$, where c_2 is some fixed constant.

Let y' be an element in G such that $y' + M$ contains y. Then $y' < y$. We claim that $y' \sim x \pmod P$, which provides a contradiction to the minimality of y. To this end, consider the path $\mathrm{path}(y', p_1 \cdots p_\ell)$ with final vector denoted by v'. Since $y' \in z + M$, we have, by the definition of z, $v' \in x + K(M)$. Since $y - y' = v - v'$ and since M is subtractive, it follows that $v' - x \in M$. Thus $v' \sim x \pmod P$, and hence $y' \sim x \pmod P$. This completes the proof of Lemma 6.3. □ □

We are now in position to obtain our main result.

Theorem 6.4. (Main Theorem) The equivalence problem is decidable is space $c^{N\log N}$, where c is some fixed constant.

Proof. The proof is omitted. □

7. Concluding Remarks.

In this paper we have shown that the equivalence problem for commutative semigroups is decidable in space $c^{N\log N}$ for some fixed constant c. Since this problem is at least as hard as the

word problem (i.e. the word problem can trivially be reduced to the equivalence problem), which is known to be complete for exponential space ([MM-82]), our result is nearly optimal. There is, however, still a gap. The reader should have noticed that some of our arguments are based on the results of Sections 3 and 4 on the coverability and self-coverability problems, where we did not exploit the symmetry property in commutative semigroups. It remains an open question whether these results can be improved so that a tight upper bound for the equivalence problem follows.

REFERENCES.

[Bir-67] Biryukov, A.P.: "Some Algorithmic Problems for Finitely Defined Commutative Semigroups", Siberian Mathematics Journal 8, 1967, pp. 384-391.

[Car-75] Cardoza, E.W.: "Computational Complexity of the Word Problems for Commutative Semigroups", M.I.T. TM 67, 1975.

[CLM-76] Cardoza, E., Lipton, R., Meyer, A.R.: "Exponential Space Complete Problems for Petri Nets and Commutative Semigroups: Preliminary Report", Proc. 8th STOC, 1976, pp. 50-54.

[ES-69] Eilenberg, S., Schützenberger M.P.: "Rational Sets in Commutative Monoids", J. Algebra 13, 1969, pp. 173-191.

[GS-78] v.z. Gathen, J., Sieveking, M.: "A Bound on Solutions of Linear Integer Equalities and Inequalities", Proc. A.M.S. 72, 1978, pp. 155-158.

[Hac-76] Hack, M.: "The Equality Problem for Vector Addition Systems is Undecidable", Theor. Comp. Sci. 2, 1976, pp. 77-95.

[HU-79] Hopcroft, J., Ullman, J.: "Introduction to Automata Theory, Languages and Computation" Addison-Wesley, 1979.

[Hu-84] Huynh, D.T.: "Properties of Congruences on Commutative Monoids", Semigroup Forum. 30, 1984, pp. 351-364.

[May-84] Mayr, E.W.: "An Algorithm for the General Petri Net Reachability Problem", SIAM J. Comput. 13, 1984, pp. 441-460.

[MM-82] Mayr, E.W., Meyer, A.R.: "The Complexity of the Word Problems for Commutative Semigroups and Polynomial Ideals", Advances in Mathematics 45, 1982, pp. 305-329.

[Rac-78] Rackoff, C.: "The Covering and Boundedness Problems for Vector Addition Systems", Theor. Comp. Sci. 6, 1978, pp. 223-231.

[SW-70] Stoer, J., Witzgall, C.: "Convexity and Optimization in Finite Dimensions, I", Springer Verlag, 1970.

[Tai-68] Taiclin, M.A.: "Algorithmic Problems for Commutative Semigroups", Soviet Math. Dokl. 9, 1968, pp. 201-204.