

Solving Commutative Relaxations of Word Problems

Danielle C. Tarraf and Pablo A. Parrilo

Abstract—We present an algebraic characterization of the standard commutative relaxation of the word problem in terms of a polynomial equality. We then consider a variant of the commutative word problem, referred to as the “Zero-to-All reachability” problem. We show that this problem is equivalent to a finite number of commutative word problems, and we use this insight to derive necessary conditions for Zero-to-All reachability. We conclude with a set of illustrative examples.

I. INTRODUCTION

A. Motivation and Background

The paper focuses on solving commutative relaxations of the word problem for finite Semi-Thue systems, referred to simply as the “word problem” for brevity. While this problem has long been studied by the computer science community [3], our interest in it stems from its relevance to a number of verification and analysis problems in emerging engineering applications, ranging from multi-agent systems described by graph grammars [6] to biochemical processes in cells [10].

Let Σ be a finite set and let Σ^* denote the set of all sequences over Σ , including the empty sequence denoted by $\#$. A *grammar rule* or *production* is an ordered pair in $\Sigma^* \times \Sigma^*$. A (finite) Semi-Thue system is a finite alphabet set Σ and a (finite) set of productions $\mathcal{P} \subset \Sigma^* \times \Sigma^*$. The word problem for Semi-Thue systems can be stated as follows: Given a Semi-Thue system (Σ, \mathcal{P}) and two words u and v in Σ^* , is it possible to transform u into v by applying rules from \mathcal{P} ? This problem is known to be undecidable even when \mathcal{P} is finite [11].

A relaxation of the word problem can be obtained by considering a commutative version in which $(ab, ba) \in \mathcal{P}$ for all a and b in Σ . The word problem in finite commutative Semi-Thue systems is known to be equivalent to several other problems, including the reachability problem for vector addition systems (also referred to as vector replacement systems) and the Petri net reachability problem, all of which have been shown to be decidable [12], [9], [7].

A further relaxation of the word problem can be obtained by considering a symmetric version of the commutative relaxation, namely one in which the set of productions \mathcal{P} has the property that if $(u, v) \in \mathcal{P}$, then $(v, u) \in \mathcal{P}$. The word problem for the corresponding finite commutative Thue system (Σ, \mathcal{P}) has been extensively studied over the past century, leading to a recognition of its connection to algebraic problems. In particular, the relation between finitely presented commutative monoids and polynomial rings was

first noted in [5], where it was also proved that the ideal membership problem for a polynomial ring is decidable (see [13] for a more accessible reference). The word problem for finite commutative Thue systems and the corresponding ideal membership problem were subsequently shown to be NP-hard [8]. Various computational techniques for verifying ideal membership exist, beginning with Buchberger’s work on Gröbner basis [1], [2], and continuing with more recent developments including the approach in [4] based on primary decompositions of the ideal.

B. Overview of the Paper

The contributions of the paper are as follows: First, we present an algebraic characterization of the standard commutative relaxation of the word problem in terms of a polynomial equality where the coefficients of certain polynomials are restricted to be non-negative. Next, we consider a variant of the commutative word problem, referred to as the “Zero-to-All reachability” problem, stated as follows: Is it possible to transform the empty string into any word in Σ^* using the rules in \mathcal{P} ? We show that this problem is equivalent to a finite number of commutative word problems, and we use this insight to derive necessary conditions for Zero-to-All reachability.

The paper is organized as follows: A formal statement of the word problem and a precise description of its standard commutative relaxation, expressed as a point-to-point reachability problem in an infinite directed graph, is presented in Section II. The algebraic characterization and computational tools proposed for solving the commutative word problem (or equivalently, the point-to-point reachability problem) are presented in Section III. It is shown in Section IV that the Zero-to-All reachability problem is equivalent to finitely many point-to-point reachability problems, and a necessary condition for reachability is derived. A set of simple illustrative examples follows in Section V, and the paper concludes in Section VI where directions for future work are given.

II. COMMUTATIVE RELAXATIONS

Consider a finite alphabet set Σ and a finite set of productions $\mathcal{P} \subset \Sigma^* \times \Sigma^*$ defining a finite Semi-Thue system (Σ, \mathcal{P}) . The application of rule $(r, w) \in \mathcal{P}$ to a word $u = \alpha r \beta$, where $\alpha, \beta \in \Sigma^*$, yields another word $u' = \alpha w \beta$. The word problem can be stated as follows:

Given a finite Semi-Thue system (Σ, \mathcal{P}) and two words $u, v \in \Sigma^$, is it possible to transform u into v by sequentially applying rules in \mathcal{P} ?*

D. C. Tarraf is with the Division of Control and Dynamical Systems, Caltech, Pasadena, CA 91125, USA (dtarraf@cds.caltech.edu).

P. A. Parrilo is with the Electrical Engineering and Computer Science Department, MIT, Cambridge, MA 02139, USA (parrilo@mit.edu).

A finite *commutative* Semi-Thue system is a finite Semi-Thue system (Σ, \mathcal{P}) such that:

$$\{(ab, ba) | a, b \in \Sigma\} \subset \mathcal{P}$$

The word problem for finite commutative Semi-Thue systems will be referred to throughout the paper as the “commutative word problem”.

A. Commutative Relaxation for the Word Problem

A relaxation of the word problem for a given finite Semi-Thue system (Σ, \mathcal{P}) can be obtained by considering the word problem for a new system (Σ, \mathcal{P}') such that $\mathcal{P} \subset \mathcal{P}'$. In this case, it is clear that if there exists a transformation of u into v using rules in \mathcal{P} , there also exists such a transformation using rules in \mathcal{P}' . Equivalently, the non-existence of a transformation using rules in \mathcal{P}' implies the non-existence of a transformation using rules in \mathcal{P} .

In particular, a commutative relaxation of the word problem for a given system (Σ, \mathcal{P}) can be obtained by defining:

$$\mathcal{P}' = \mathcal{P} \cup \{(ab, ba) | a, b \in \Sigma\}$$

B. Graph Theoretic Formulation of the Commutative Word Problem

Consider an alphabet set $\Sigma = \{a_1, \dots, a_n\}$ and let (Σ, \mathcal{P}) be a finite commutative Semi-Thue system. Consider the Parikh mapping $\Phi : \Sigma^* \rightarrow \mathbb{N}^n$, in which the i^{th} coordinate of $\Phi(u)$ is the number of occurrences of the symbol a_i in word u . In this setting, words u and v are equivalent, denoted $u \mathcal{R} v$, if their images by the Parikh mapping are identical¹. For any two words u and v in the same equivalence class, there always exists a transformation of u into v and one of v into u using the rules in \mathcal{P} . Now consider two words u and v with $\Phi(u) \neq \Phi(v)$. Note that it is possible to transform u into v using the rules in \mathcal{P} iff it is possible to transform a representative element of the equivalence class of u into a representative element of the equivalence class of v . It follows from this simple observation that the commutative word problem can be formulated as a point-to-point reachability problem in an infinite directed graph.

Indeed, consider a finite commutative Semi-Thue system (Σ, \mathcal{P}) , where $\Sigma = \{a_1, \dots, a_n\}$. Define a set $\mathcal{B} \subset \mathbb{N}^n \times \mathbb{N}^n$ as follows:

$$\mathcal{B} = \{(\Phi(r), \Phi(w)) | (r, w) \in \mathcal{P}\}$$

We can construct an infinite directed graph $G_{\mathcal{B}} = (\mathcal{N}, \mathcal{E})$ with nodes $\mathcal{N} = \mathbb{N}^n$ and directed edges defined by (see Figure 1):

$$\mathcal{E} = \{(s + \delta, t + \delta) | (s, t) \in \mathcal{B}, \delta \in \mathbb{N}^n\}$$

A directed path from node u to node v is understood to be a sequence of directed edges $(u_1, v_1), \dots, (u_k, v_k)$ of $G_{\mathcal{B}}$ satisfying $u_1 = u$, $u_{i+1} = v_i$ for $i \in \{1, \dots, k-1\}$, and $v_k = v$. The point-to-point reachability problem can be stated as follows:

¹ \mathcal{R} clearly defines an equivalence relation on Σ^* , being reflexive, symmetric and transitive.

Given an infinite directed graph $G_{\mathcal{B}}$ and two nodes u and v , does there exist a directed path from u to v in $G_{\mathcal{B}}$?

The commutative word problem for system (Σ, \mathcal{P}) and the point-to-point reachability problem for the corresponding graph $G_{\mathcal{B}}$ are equivalent. Indeed, the nodes of $G_{\mathcal{B}}$ in this case are understood to be the representative elements of the equivalence classes in Σ^* .

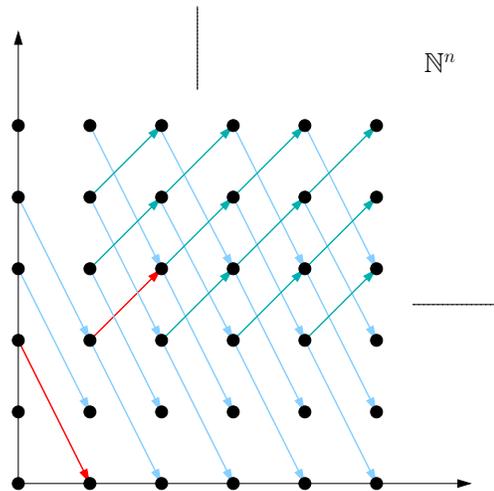


Fig. 1. Construction of infinite digraph $G_{\mathcal{B}}$ for a case where the alphabet set Σ is binary and where $\mathcal{B} = \{(\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}), (\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix}), (\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}), (\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}), (\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}), (\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix})\}$.

III. THE POINT-TO-POINT REACHABILITY PROBLEM

In this section, we present an algebraic characterization of the point-to-point reachability problem. In particular, we show that existence of a directed path from one given node to another is equivalent to the existence of a “non-negative” polynomial solution to a particular polynomial equation.

A. Algebraic Characterization of Point-to-Point Reachability

Consider a set $\mathcal{B} \subset \mathbb{N}^n \times \mathbb{N}^n$ with cardinality p and a corresponding digraph $G_{\mathcal{B}}$ as described in Section II-B. We can uniquely associate with every node $u = (u_1, \dots, u_n)$ a monomial $x^u \in \mathbb{Q}[x_1, \dots, x_n]$, where \mathbb{Q} denotes the field of rationals, as follows:

$$x^u = x_1^{u_1} \dots x_n^{u_n}$$

We can also uniquely associate with every element $(s, t) \in \mathcal{B}$ a binomial $x^t - x^s \in \mathbb{Q}[x_1, \dots, x_n]$.

Theorem 1: There exists a directed path from node u to node v in $G_{\mathcal{B}}$ iff there exists polynomials $g_1, \dots, g_p \in \mathbb{Q}[x_1, \dots, x_n]$, with *non-negative* coefficients, such that:

$$x^v - x^u = \sum_{i=1}^p (x^{t_i} - x^{s_i}) g_i(x) \quad (1)$$

with $(s_i, t_i) \in \mathcal{B}$ for all i .

Proof: Note that when $u = v$, the Theorem holds vacuously. We will thus assume that $u \neq v$ in the following proof.

To prove necessity, let $(u_0, v_0), (u_1, v_1), \dots, (u_N, v_N)$ be a directed path from $u = u_0$ to $v = v_N$ in G_B . For each $i \in \{0, 1, \dots, N\}$, we have:

$$(u_i, v_i) = (s_{k_i} + \delta_i, t_{k_i} + \delta_i)$$

for some $(s_{k_i}, t_{k_i}) \in \mathcal{B}$ and some $\delta_i \in \mathbb{N}^n$. Hence we have $x^{u_i} = x^{s_{k_i} + \delta_i} = x^{s_{k_i}} x^{\delta_i}$ and $x^{v_i} = x^{t_{k_i} + \delta_i} = x^{t_{k_i}} x^{\delta_i}$. It follows that:

$$x^v - x^u = \sum_{i=0}^N (x^{v_i} - x^{u_i}) = \sum_{i=0}^N (x^{t_{k_i}} - x^{s_{k_i}}) x^{\delta_i}$$

Collecting terms, we get the expression in (1) with each polynomial $g_i(x)$ having non-negative integer coefficients.

To prove sufficiency, suppose there exists polynomials g_1, \dots, g_p with non-negative rational coefficients such that (1) holds, and let d be the least common denominator of the coefficients. Equation (1) can be re-written as:

$$dx^v - dx^u = \sum_{i=1}^p (x^{t_i} - x^{s_i}) h_i(x)$$

where polynomials h_1, \dots, h_p have non-negative integer coefficients. We can then write:

$$(d-1)(x^v - x^u) + x^v - x^u = \sum_{i=1}^m (x^{t_i} - x^{s_i}) h'_i(x) \quad (2)$$

where h'_1, \dots, h'_m are *monomials* with *unity* coefficients (obtained by simply expanding polynomials h_1, \dots, h_p) and with $m \geq p$. Note that there must exist a $j \in \{1, \dots, m\}$ such that $x^u = x^{s_j} h'_j(x)$. Let $x^{u_1} = x^{t_j} h'_j(x)$. We can write:

$$(d-1)(x^v - x^u) + x^v - x^{u_1} = \sum_{i \in \{1, \dots, m\} \setminus \{j\}} (x^{t_i} - x^{s_i}) h'_i(x)$$

Pair (u, u_1) is a directed edge in G_B , since $(u, u_1) = (s_j + \delta_j, t_j + \delta_j)$, with $h'_j(x) = x^{\delta_j}$ and hence $\delta_j \in \mathbb{N}^n$. If $u_1 = v$ we are done, having found a directed path $(u, u_1) = (u, v)$ from u to v . Otherwise, by repeating the same argument k times for x^{u_i} , with $k \leq m - d$ (see comment²), we can construct a sequence of edges $(u, u_1), (u_1, u_2), \dots, (u_k, v)$. For if such a sequence does not exist, we would have:

$$(d-1)(x^v - x^u) + x^v - x^{u_{m-d+1}} = \sum_{i \in I} (x^{t_i} - x^{s_i}) h'_i(x) \quad (3)$$

where index set $I \subset \{1, \dots, m\}$ has cardinality $d - 1$. The left and right hand sides of (3) would thus include d (identical) monomials with unity coefficients and $d - 1$ monomials with unity coefficients, respectively, implying that the equality cannot hold and thus leading to a contradiction. \square

²It should be clear that $m \geq d$ otherwise (2) cannot hold unless $x^v = x^u$, which is excluded here.

B. Verifying the Polynomial Equation

Having thus derived an algebraic characterization of point-to-point reachability, the question becomes: How can we verify the condition in (1)?

A naive way consists of solving a sequence of increasingly large linear programs until a feasible solution is found. Consider p candidate polynomials of fixed total degree r :

$$g_i(x) = \sum_{|\alpha| \leq r} c_{i,\alpha} x^\alpha, \quad i \in \{1, \dots, p\}$$

where $|\alpha|$ refers to the total degree of monomial x^α . Verifying (1) for this choice of candidate polynomials reduces to verifying feasibility of a linear program of the form:

$$\begin{aligned} Ax &= 0 \\ x &\geq 0 \end{aligned}$$

Decision variable x here is the vector of coefficients of g_1, \dots, g_p . The equality constraints are obtained by collecting terms in:

$$x^v - x^u - \sum_{i=1}^p (x^{t_i} - x^{s_i}) g_i(x) = 0$$

and setting the coefficient of each monomial term equal to 0. The inequality constraints impose the restriction that the coefficients of g_1, \dots, g_p are non-negative.

The solution procedure is then as follows: Initialize r to $\max\{1, |v| - \max_i |t_i|, |u| - \max_i |s_i|\}$, and consider the corresponding linear program. If a feasible solution exists, the existence of a directed path from u to v is verified, and at least one such directed path can be explicitly constructed from the verified polynomial equality (see Example 1 in Section V). On the other hand, if the linear program is found to be infeasible, increase r by 1 and repeat the process.

This approach, while conceptually simple, is not particularly efficient. One major direction of future research will focus on developing more computationally efficient verification tools. Note that dropping the requirement of non-negative coefficients reduces the problem to an ideal membership problem, which has been extensively studied in algebraic-geometry and for which more efficient approaches, based on ideal primary decompositions, have been developed [2], [4]. One direction that will thus be explored is the possibility of developing similar reduction techniques for the class of problems of interest.

IV. VARIANTS OF THE COMMUTATIVE WORD PROBLEM

In this section, we consider another graph reachability problem corresponding to a variant of the commutative word problem. We show how it can be equivalently re-formulated as a finite number of point-to-point reachability problems, and we derive necessary conditions for reachability.

A. Zero-to-All Reachability

Given an infinite directed graph $G_{\mathcal{B}}$ constructed as in Section II-B, let 0 denote the node $0^n \in \mathbb{N}^n$. The Zero-to-All reachability problem can be stated as:

Is there a directed path in $G_{\mathcal{B}}$ from node 0 to every node in $\mathcal{N} \setminus \{0\}$?

This problem is equivalent to the following problem for the corresponding finite commutative Semi-Thue system (Σ, \mathcal{P}) :

Is it possible to transform the empty string $\#$ into any word in Σ^ by applying rules from \mathcal{P} ?*

Remark 1: The All-to-Zero reachability problem can be stated as follows: Is there a directed path in $G_{\mathcal{B}}$ from every node to 0? While this Section focuses on the Zero-to-All reachability problem, the All-to-Zero reachability problem can be similarly treated: It suffices to note that All-to-Zero reachability of $G_{\mathcal{B}}$ is equivalent to Zero-to-All reachability of $G_{\mathcal{B}'}$, where $\mathcal{B}' = \{(t, s) | (s, t) \in \mathcal{B}\}$.

B. Reduction to Point-to-Point Reachability

We begin by noting that the Zero-to-All reachability problem can be reduced to solving n point-to-point reachability problems. Given a set \mathcal{B} and an associated infinite digraph $G_{\mathcal{B}}$ as described in Section II-B, let e_i be the node corresponding to the coordinates of the i^{th} basis vector (i.e. the unit vector whose i^{th} entry is 1).

Theorem 2: $G_{\mathcal{B}}$ is Zero-to-All reachable iff there exists a directed path from 0 to each of the nodes e_1, \dots, e_n .

Proof: Necessity is trivial: If the digraph is Zero-to-All reachable, there exists a directed path from 0 to every node in \mathcal{N} , in particular to e_1, \dots, e_n .

To prove sufficiency, we begin by noting that if there exists a directed path from 0 to e_i , there also exists a directed path from any node $v = (v_1, \dots, v_n)'$ to $w = (v_1, \dots, v_i + 1, \dots, v_n)'$. Indeed, let $(0, u_1), (u_1, u_2), \dots, (u_k, e_i)$ be a directed path from 0 to e_i . Then the path $(v, u_1 + v), (u_1 + v, u_2 + v), \dots, (u_k + v, e_i + v)$ is a directed path from v to w . It follows that it is always possible to construct a directed path from 0 to any node $v = (v_1, \dots, v_n)'$ passing through nodes $e_1,$

$2e_1, \dots, v_1e_1, v_1e_1 + e_2, \dots, v_1e_1 + v_2e_2, \dots, \sum_{i=1}^n v_i e_i$. \square

C. A Necessary Condition for Zero-to-All Reachability

We next show that feasibility of n decoupled integer linear programs is a necessary condition for Zero-to-All reachability. Associate with every $(s, t) \in \mathcal{B}$ a vector $b = t - s$ in \mathbb{N}^n .

Theorem 3: If $G_{\mathcal{B}}$ is Zero-to-All reachable, then there exists non-negative integers $\alpha_1^i, \dots, \alpha_p^i, i \in \{1, \dots, n\}$ satisfying the following set of decoupled linear equations:

$$\begin{aligned} \alpha_1^1 b_1 + \dots + \alpha_p^1 b_p &= e_1 \\ &\vdots \\ \alpha_1^n b_1 + \dots + \alpha_p^n b_p &= e_n \end{aligned} \quad (4)$$

where e_i is the i^{th} basis vector.

Note that Theorem 3 is only a necessary condition. Thus, while it does not allow us to directly verify Zero-to-All reachability, it can be used to certify that a given graph $G_{\mathcal{B}}$ is *not* Zero-to-All reachable when at least one of the n integer linear programs defined by (4) does not admit a feasible (non-negative, integer) solution. The following intermediate statements will be used in the proof.

Lemma 1: If there exists a directed path in $G_{\mathcal{B}}$ from 0 to x , then $x = \sum_{i=0}^p \alpha_i b_i$ for some $\alpha_i \in \mathbb{N}$.

Proof: Let $(u_0, u_1), (u_1, u_2), \dots, (u_{k-1}, u_k)$ be such a directed path, and let $\beta_i = u_{i+1} - u_i$. We have:

$$\begin{aligned} x &= u_k - u_0 \\ &= \sum_{i=0}^{k-1} (u_{i+1} - u_i) \\ &= \sum_{i=0}^{k-1} \beta_i \\ &= \sum_{i=0}^p \alpha_i b_i, \text{ for some } \alpha_i \in \mathbb{N}. \end{aligned}$$

\square

Lemma 2: Let $R = \left\{ \sum_{i=1}^p \alpha_i b_i \mid \alpha_i \in \mathbb{N} \right\}$. If $G_{\mathcal{B}}$ is Zero-to-All reachable, then $\mathbb{N}^n \subseteq R$.

Proof: Suppose there exists an $x \in \mathbb{N}^n$ such that $s \notin R$: thus, $x \neq \sum_{i=1}^p \alpha_i b_i$ for any choice of $\alpha_1, \dots, \alpha_p$ in \mathbb{N} , there exists no directed path from 0 to x , and hence $G_{\mathcal{B}}$ is not Zero-to-All reachable. \square

Lemma 3: $\mathbb{N}^n \subseteq R$ iff each of the integer linear programs in (4) has a feasible non-negative integer solution.

Proof: Necessity is straightforward: Suppose that the i^{th} linear equation in (4) does not have a feasible non-negative integer solution. Then there exists at least one element of \mathbb{N}^n that is not in R , namely e_i .

To prove sufficiency, note that if each of the linear programs in (4) has a feasible non-negative integer solution, then the linear program:

$$\sum_{i=1}^p \left(\sum_{j=1}^n a_j \alpha_i^j \right) b_i = \sum_{j=1}^n a_j e_j$$

has a non-negative integer solution for any choice of values a_1, \dots, a_n in \mathbb{N} . Thus, every $x \in \mathbb{N}^n$ also belongs to R . \square

Proof of Theorem 3: Follows as a direct consequence of Lemmas 1, 2 and 3. \square

V. ILLUSTRATIVE EXAMPLES

Example 1 uses a toy problem to give insight into Theorem 1. Examples 2-4 present simple variations of the toy problem to illustrate the results derived in Sections III and IV.

Example 1: Consider a knight playing on an infinite chessboard. The squares of the chessboard can be associated with \mathbb{N}^2 , as shown in Figure 2. Let $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $e_2 =$

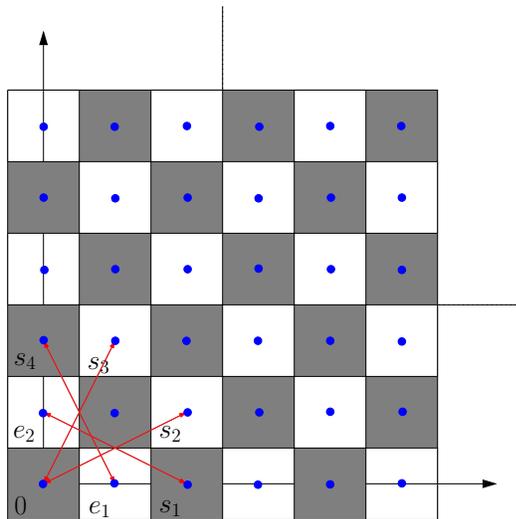


Fig. 2. Knight on an infinite chessboard.

$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $s_1 = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$, $s_2 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$, $s_3 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$, $s_4 = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$. The basic moves of the knight are given by:

$$\mathcal{B} = \{(0, s_2), (0, s_3), (s_1, e_2), (s_4, e_1), (s_2, 0), (s_3, 0), (e_2, s_1), (e_1, s_4)\}$$

and the binomials associated with the elements of \mathcal{B} are:

$$\begin{aligned} (0, s_2) &\rightarrow x^2y - 1 \\ (0, s_3) &\rightarrow xy^2 - 1 \\ (s_1, e_2) &\rightarrow y - x^2 \\ (s_4, e_1) &\rightarrow x - y^2 \\ (s_2, 0) &\rightarrow 1 - x^2y \\ (s_3, 0) &\rightarrow 1 - xy^2 \\ (e_2, s_1) &\rightarrow x^2 - y \\ (e_1, s_4) &\rightarrow y^2 - x \end{aligned}$$

By Theorem 1, the following (readily verifiable) polynomial equality, being of the form (1), allows us to prove the existence of a feasible directed path for the chess knight from node $u = \begin{pmatrix} 4 \\ 4 \end{pmatrix}$ to node $v = \begin{pmatrix} 3 \\ 3 \end{pmatrix}$:

$$\begin{aligned} x^3y^3 - x^4y^4 &= (xy^2 - 1)x^4y^4 \\ &+ (y - x^2)\left(\frac{1}{2}x^3y^2 + \frac{1}{2}x^4y^4\right) \\ &+ (x - y^2)x^5y^4 \\ &+ (1 - xy^2)\left(\frac{1}{2}x^3y^3 + \frac{1}{2}x^5y^2\right) \end{aligned} \tag{5}$$

Indeed, following the steps in the sufficiency proof of Theorem 1, we can construct a sequence of directed edges starting at u , passing through nodes $u_1 = \begin{pmatrix} 5 \\ 6 \end{pmatrix}$, $u_2 = \begin{pmatrix} 6 \\ 4 \end{pmatrix}$, $u_3 = \begin{pmatrix} 4 \\ 5 \end{pmatrix}$ and ending at $u_4 = v$. Using the same

procedure, we can alternatively construct another sequence of directed edges, also starting at u , but passing through $u_1 = \begin{pmatrix} 5 \\ 6 \end{pmatrix}$, $u_2 = \begin{pmatrix} 6 \\ 4 \end{pmatrix}$, $u_3 = \begin{pmatrix} 5 \\ 2 \end{pmatrix}$ and ending at $u_4 = v$. This simple example illustrates the intuition behind the algebraic characterization of point-to-point reachability given by (1), namely that the right hand side describes an ‘‘average’’ of d different directed paths from u to v .

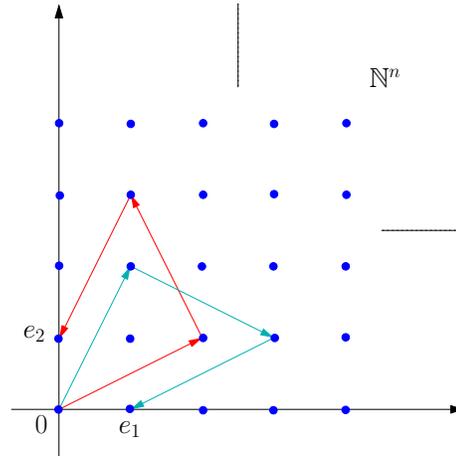


Fig. 3. Directed paths of the knight from 0 to e_1 and e_2 .

Example 2: Assume that the knight begins the game at the corner of the infinite chessboard, associated with the 0 node in this setup (see Figure 2). An interesting question is this: Can she can reach all the squares of the chessboard? Equivalently, we need to check whether the infinite directed graph $G_{\mathcal{B}}$ constructed as described in Section II-B for \mathcal{B} given in Example 1 is Zero-to-All reachable. By Theorem 2, we need to verify existence of directed paths from 0 to e_1 and e_2 , which can be easily done by inspection (see Figure 3).

Example 3: Variants of the problem in Example 2 can be posed by restricting the knight’s allowable moves. For instance, consider the case where the knight’s moves are restricted to a subset of \mathcal{B} given by:

$$\mathcal{B}_2 = \{(0, s_2), (s_4, e_1), (s_3, 0)\}$$

Can the knight still reach all the squares of the chessboard starting from 0? According to Theorem 3, the answer is no whenever the integer linear program in (4) has no feasible non-negative solution. In this particular example, this reduces to checking the feasibility of two integer linear programs (corresponding to $i = 1, 2$):

$$\begin{aligned} Ax &= e_i \\ x &\geq 0 \end{aligned}$$

with A given by:

$$A = \begin{bmatrix} 2 & 1 & -1 \\ 1 & -2 & -2 \end{bmatrix}$$

Both ILPs turn out to be infeasible here, hence we conclude that the knight cannot reach all the squares on the playing board (in fact, she cannot even reach e_1 and e_2 with the allowable moves).

Example 4: Finally, consider the case where the knight's basic moves are restricted to:

$$\mathcal{B}_3 = \{(0, s_2), (s_3, 0), (e_2, s_1), (e_1, s_4)\}$$

The corresponding linear programs described in (4) are both feasible in this case, which gives us hope that there could exist directed paths from 0 to e_1 and e_2 . We will attempt to construct these paths using Theorem 1 in conjunction with the naive LP-based procedure proposed in Section III-B. We begin by considering candidate polynomials g_1, g_2, g_3 and g_4 of total degree 1 (i.e. $g_i(x, y) = a_i + b_i x + c_i y$). The corresponding linear programs are both found to be infeasible. We then increase the total degree of the candidate polynomials to 2 (i.e. $g_i(x, y) = a_i + b_i x + c_i y + d_i x^2 + f_i xy + l_i y^2$) and repeat the procedure. In this case, a solution to both LPs is found, and the corresponding verified polynomial equalities are:

$$x - 1 = (x^2 y - 1)(1 + y) + (1 - xy^2)(x + y) + (y^2 - x)xy$$

and:

$$y - 1 = (x^2 y - 1) + (1 - xy^2)y + (y^2 - x)xy$$

The corresponding directed paths from 0 to e_1 and e_2 , which can be reconstructed (see Example 1), are shown in Figure 4. It is interesting to note that the knight can reach all squares of the chessboard using only 3 basic moves, namely $(0, s_2)$, $(s_3, 0)$ and (e_1, s_4) .

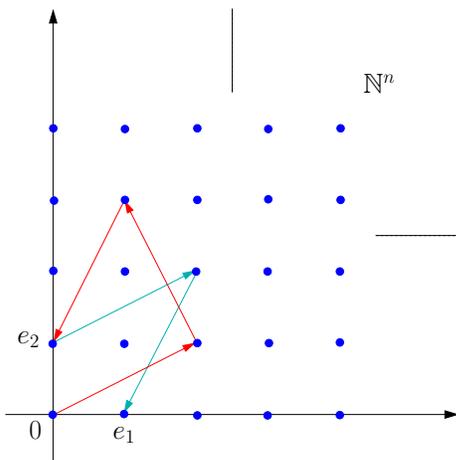


Fig. 4. Directed paths of the knight from 0 to e_1 and e_2 in Example 4.

VI. CONCLUSIONS AND FUTURE WORK

A. Conclusions

We presented an algebraic characterization of commutative word problems in terms of a polynomial equality, thus generalizing existing results for the symmetric case. We also considered a “Zero-to-All reachability” question for

commutative Semi-Thue systems: We showed that solving this problem is equivalent to solving a finite number of commutative word problem, and we used this insight to derive necessary conditions for Zero-to-All reachability.

B. Future Work

Research will be pursued in two broad directions. The first direction will aim at addressing the following questions: Is it possible to construct a hierarchy of commutative relaxations for a given Semi-Thue system? And if so, can anything be said about the solution of the word problem for the original system based on the properties of the solutions of the word problem for a number of the commutative relaxations? The second direction is computational, and will aim at (i) understanding the relation between the algebraic characterization of the commutative word problem and the standard LP solution of shortest path problems in appropriately defined finite subgraphs and (ii) finding more efficient computational procedures for verifying the polynomial equation, possibly via appropriate reduction procedures.

VII. ACKNOWLEDGMENTS

This research was supported by AFOSR MURI grant #102-108-0673.

REFERENCES

- [1] B. Buchberger. *An Algorithm for Finding the Bases Elements of the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal (in German)*. PhD dissertation, University of Innsbruck, Innsbruck, Austria, 1965.
- [2] B. Buchberger. Grobner bases: An algorithmic method in polynomial ideal theory. In N. K. Bose, editor, *Multidimensional Systems Theory*, pages 184–232. Dordrecht: Reidel, 1985.
- [3] N. Dershowitz and J. Jouannaud. Rewrite systems. In *Handbook of Theoretical Computer Science*, volume B, pages 243–320. Elsevier, 1991.
- [4] P. Diaconis, D. Eisenbud, and B. Sturmfels. Lattice walks and primary decompositions. In B. Sagan and R. P. Stanley, editors, *Mathematical Essays in Honor of Gian-Carlo Rota*, volume 161 of *Progress in Mathematics*, pages 173–194. Birkhauser, Boston; Basel; Berlin, 1998.
- [5] V. A. Emelichev. Commutative semigroups with one defining relation. *Uchenye zap. Shuiskogo ped. in-ta*, 6:227–242, 1958.
- [6] E. Klavins, R. Ghrist, and D. Lipsky. A grammatical approach to self-organizing robotic systems. *IEEE Transactions on Automatic Control*, 51(6):949–962, 2006.
- [7] S. R. Kosaraju. Decidability of reachability in vector addition systems. In *Proceedings of the 14th Annual ACM Symposium on Theory of Computing*, pages 267–281, 1982.
- [8] E. Mayr and A. Meyer. The complexity of the word problem for commutative semigroups and polynomial ideals. *Advances in Mathematics*, 46:305–329, 1982.
- [9] E. W. Mayr. An algorithm for the general Petri net reachability problem. In *Proceedings of the 13th Annual ACM Symposium on Theory of Computing*, pages 238–246, 1981.
- [10] B. Munsky and M. Khammash. The finite state projection algorithm for the solution of the chemical master equation. *The Journal of Chemical Physics*, 124(044104), 2006.
- [11] E. Post. Recursive unsolvability of a problem of Thue. *Journal of Symbolic Logic*, 12(1):1–11, 1947.
- [12] G. S. Sacerdote and R. L. Tenney. The decidability of the reachability problem for vector addition systems. In *Proceedings of the 9th Annual ACM Symposium on Theory of Computing*, pages 61–76, 1977.
- [13] A. Seidenberg. Constructions in algebra. *Transactions of the American Mathematical Society*, 197:273–313, 1974.