UNIVERSITY OF LIVERPOOL

Computational Problems in Matrix Semigroups

Thesis submitted in accordance with the
requirements of the University of Liverpool
for the degree of Doctor in Philosophy by
Paul Charles Bell

Thesis Supervisors: Dr. Igor Potapov
Dr. Paul Dunne

Department of Computer Science
The University of Liverpool
July, 2007

Abstract

This thesis deals with computational problems that are defined on matrix semigroups, which play a pivotal role in Mathematics and Computer Science in such areas as control theory, dynamical systems, hybrid systems, computational geometry and both classical and quantum computing to name but a few. Properties that researchers wish to study in such fields often turn out to be questions regarding the structure of the underlying matrix semigroup and thus the study of computational problems on such algebraic structures in linear algebra is of intrinsic importance.

Many natural problems concerning matrix semigroups can be proven to be intractable or indeed even unsolvable in a formal mathematical sense. Thus, related problems concerning physical, chemical and biological systems modelled by such structures have properties which are not amenable to algorithmic procedures to determine their values.

With such recalcitrant problems we often find that there exists a tight border between decidability and undecidability dependent upon particular parameters of the system. Examining this border allows us to determine which properties we can hope to derive algorithmically and those problems which will forever be out of our reach, regardless of any future advances in computational speed.

There are a plethora of open problems in the field related to dynamical systems, control theory and number theory which we detail throughout this thesis. We examine undecidability in matrix semigroups for a variety of different problems such as membership and vector reachability problems, semigroup intersection emptiness testing and freeness, all of which are well known from the literature. We also formulate and survey decidability questions for several new problems such as vector ambiguity, recurrent matrix problems, the presence of any diagonal matrix and quaternion matrix semigroups, all of which we feel give a broader perspective to the underlying structure of matrix semigroups.

Acknowledgements

I would like to especially thank my main supervisor, Dr. Igor Potapov, for his continued support and guidance throughout both my undergraduate as well as graduate degrees. His enthusiasm, constructive criticism, research ideas and always making time for discussions over the past four years has made the completion of my Ph.D. both possible and highly enjoyable.

I would also like to express my gratitude to my second supervisor, Dr. Paul Dunne, and my thesis advisor, Dr. Alexei Lisitsa, for their assistance and suggestions over the past three years.

The Complexity Theory and Algorithmics Group and the Department of Computer Science in general at Liverpool University has been an excellent place in which to conduct research and all members of staff have been encouraging and helpful whenever needed. I would also like to kindly thank the Department of Computer Science for funding my postgraduate studies.

Very sincere thanks also go to both of my thesis examiners, Prof. Leszek Gąsieniec, who was my internal examiner and Dr. Vesa Halava (Turku University) who was my external examiner, for their careful checking of my thesis and helpful comments and suggestions during my viva.

Last, but by no means least, I am eternally indebted to my family and especially my parents for their invariable support and encouragement, without whom the completion of my Ph.D. would not have been possible.

Contents

Notation Glossary

Basic Notation

$\mathbb{N}$ - The set of natural numbers ($\{0,1,2,\ldots\}$).

$\mathbb{Z}$ - The ring of integers.

$\mathbb{Q}$ - The field of rational numbers.

$\mathbb{C}$ - The field of complex numbers.

$\mathbb{C}(\mathbb{Q})$ - The field of rational complex numbers.

$\mathbb{H}(\mathbb{Q})$ - The division ring of rational quaternions.

$\mathbb{H}(\mathbb{Q})_0$ - The ring of pure rational quaternions.

$\mathbb{F}$ - Arbitrary ring of numbers.

$\Re(z)$ - Real part of complex number $z \in \mathbb{C}$.

$\Im(z)$ - Imaginary part of complex number $z \in \mathbb{C}$.

$\overline{z}$ - Complex conjugate of complex number $z \in \mathbb{C}$.

$|z|$ - Modulus of complex number $z \in \mathbb{C}$, ($|z| = \sqrt{(\Re(z)^2 + \Im(z)^2)}$).

$\delta_{i,j}$ - The Kronecker delta; equal to 1 if $i = j$ else equal to 0.

Matrix Notation

I_n - The $n \times n$ identity matrix.

$\mathbb{F}^{n \times n}$ - The set of $n \times n$ matrices over number system $\mathbb{F}$.

$\det(M)$ - The determinant of matrix M.

M^{-1} - The inverse of matrix M (exists iff $\det(M) \neq 0$).

M^T - The transpose of matrix M.

M^* - The Hermitian transpose of matrix M.

$M_{[i,j]}$ - The element at row i and column j of matrix M.

$\sigma(M)$ - The set of eigenvalues of matrix M.

$\rho(M)$ - The spectral radius of matrix M.

$A \otimes B$ - The Kronecker product of matrices A and B.

$A \oplus B$ - The direct sum of matrices A and B.

Word Notation

Given words $u = u_1u_2 \cdots u_n$ and $v = v_1v_2 \cdots v_m$:

- $u \cdot v = u_1u_2 \ldots u_nv_1v_2 \ldots v_m$ - The concatenation of u and v.
- $u^R = u_n \ldots u_2u_1$ - The reverse of word u.
- ε - The empty word.

Group Theory Notation

$A \cup B$ - The *union* of the sets A and B.
$A \cap B$ - The *intersection* of the sets A and B.
$|A|$ - The *cardinality* (or size) of the set A.
$\langle \mathscr{G} \rangle$ - The semigroup *generated* by set of square matrices $\mathscr{G}$.
$\mathscr{S}$ - A matrix semigroup.

Symbols

PCP - Post's correspondence problem.
n_{PCP} - The minimum instance size for which Post's correspondence problem (PCP) is *known to be* undecidable (currently 7, see [43]).
n_{CLAUS} - The minimum instance size for which Post's correspondence problem (PCP) is *known to be* undecidable using "Claus instances" (currently 7, see [28]).

Chapter 1

Introduction

"Quod est, nullum non problema solvere",
There is no problem which cannot be solved,
Françoise Viète.

1.1 Background

Matrices play a fundamental and central role in a plethora of mathematical disciplines. They describe linear transformations and their use has propagated to such an extent, that to prove a result purely in terms of matrix theory can induce an abundance of related results in a set of diverse fields.

Matrices are central to linear algebra which studies general properties of vector spaces. Our aim is to study a core set of problems which may be defined in terms of linear algebra. We shall detail an amalgamation of disparate computational problems whose decidability status we shall explore using several methods which shall be studied and developed in the early chapters of this thesis. The exact and formal mathematical definitions of these problems will appear in Section 2.3 of Chapter 2 but we shall give a less formal description of them here in order to motivate the reader as to the type of problems considered.

There are many natural and important questions in terms of linear algebra and one such problem is the *membership problem*, which is to determine whether some element (linear transformation) is present within a given set (of linear transformations). As an instance of the problem we are given a finite set of objects $\mathscr{G}$ and a binary operator allowing us to take two elements and create a new element. Thus from the set $\mathscr{G}$, we can create a new set of elements which may be infinite in size called $\mathscr{S}$. The set $\mathscr{S}$ is formally named a *semigroup* and we shall be dealing with *matrix semigroups* where each element of the set is a square matrix. The membership problem on matrix semigroups asks whether a particular matrix is contained within the semigroup.

Another interesting and fundamental problem concerning semigroups is the *vector reachability problem* (VRP). This question asks "given a set of linear transformations and two points x and y, is it possible to find a combination of transformations from the set that maps x to y?". The problem can also be formulated in terms of a matrix semigroup [1], $\mathscr{S}$, and a pair of vectors x, y as input and the problem then becomes whether there exists any matrix $M \in \mathscr{S}$ such that $Mx = y$. A related problem is the *scalar reachability problem* which takes as input a finitely generated matrix semigroup $\mathscr{S}$, two vectors a, b and a scalar k. The problem asks, "does there exist any matrix $M \in \mathscr{S}$ such that $a^T Mb = k$?". The equality can also be replaced by other relations such as $<, >, \leq, \geq$, etc.

Other problems often arise in the study of semigroups such as determining the freeness of a matrix semigroup. In this problem we must determine if a given finitely generated semigroup is free, i.e., if every element of the semigroup has a unique factorisation over elements of the generator. Studying the decidability of such general problems for matrix semigroups can prove the decidability of problems in many other areas. We shall now show several such areas from mathematics and computer science where problems that are

[1] We may define the set of linear transformations as a matrix semigroup since the combination of linear transformations corresponds to matrix multiplication

being researched are strongly related to computational problems on matrix semigroups.

In automata theory, it is a widely known and utilised fact that finite state machines can be simulated via a set of integral matrices. If we allow the finite state machine to be non-deterministic and assign probabilities which sum to 1 on each outgoing edge set for each vertex, this gives us probabilistic finite state automata (PFA). Such automata may be simulated by a set of rational matrices, one for each input letter. A possible question we might ask on a PFA is "Starting from a given state, does there exist a word w, leading to a final state with a probability greater than a certain threshold?". It is possible to define this problem instead as a type of scalar reachability problem on *stochastic matrix semigroups* as is not difficult to show, see [15] for example.

If we instead specify that the sum of squares of the values of outgoing edges from each vertex equals 1 then we obtain the model of *quantum finite state automata*. When studying quantum automata, the matrices in the generator are *unitary matrices*. Thus, if we have general properties for computational problems on stochastic or unitary matrices in different dimensions (such as the decidability status of various problems) then it can aid in the study of problems on probabilistic and quantum automata.

Another field where matrix problems play a central role is dynamical systems in which we often aim to describe some real world system and derive properties of it. For example, we may wish to simulate the trajectory of a billiard ball on a table, the motion of celestial bodies or the dynamics of particles in a fluid. Properties studied include fixed points of the system, convergence and divergence of the system, the onset of chaotic behaviour and various stability criteria. In a linear dynamical system we can describe the evolution of a point via matrix equations and thus the properties of the system we wish to discover can turn out to be specific properties of the matrices used to represent it.

Let us consider an example of one such dynamical system. Given an initial state vector $s_0 = (u_0, u_1, \ldots, u_{n-1})^T \in \mathbb{C}^n$ and a set of matrices, $\mathscr{G} = \{M_0, M_1, \ldots, M_k\} \in \mathbb{C}^{n \times n}$. If we consider a discrete time model, then at each time step we non-deterministically (i.e., randomly) choose a particular matrix M_i and obtain the next state vector, thus $u_{j+1} = M_i u_j$. This process continues iteratively and we can see that it is a type of linear non-deterministic dynamical system.

Typical questions we might ask on such a model are: "Given an instance of the system, is it possible to reach a particular state v?" or another question might be "Given a fixed set of matrices, does every initial vector converge to the zero vector for all possible products?". The former problem seems very natural to ask but in fact we show that it is *undecidable* (which we explain later) even for just 7 rational matrices of dimension-3 in Theorem 4.10. The decidability status of the latter problem is a fundamental but open problem in the field related to the *joint spectral radius* of a set of matrices, see [15, 52].

Matrices and matrix semigroups also play a key role in other areas of Mathematics and Computer Science. In Graph theory we model pair-wise relations between vertices from a given set, often via *adjacency matrices.* There exists a large number of problems on graphs such as colouring problems, the clique problem, the Hamiltonian path problem and the travelling salesman problem to name but a few. Again we may often define these problems in terms of properties of specific classes of matrices.

In the field of computer graphics we are interested in visualising mathematically described objects on a $2D$ computer screen. We can conceptualise the process by having a matrix represent the movement and rotations of objects or the "camera" out of which we view the scene.

The above examples illustrate only a fraction of subjects whereby the structures in question may be modelled via matrices or matrix semigroups. Thus, as previously mentioned, algorithmic solutions to these questions on specific classes of matrix semigroups can aid us in several disciplines.

Complexity and Computability Theory

The discussion can now turn to *complexity* and *computability* issues arising from the study of computational questions on these structures. For many problems we may create a decision problem which will return the correct answer "true" or "false" in a short amount of time whereby we use the standard definition of a short amount of time to mean time which is proportional to a polynomial of the input size of an instance in some "reasonable" representation. [2] The class of all such problems is denoted P for *polynomial time algorithms.*

However, it is well known that certain problems seem to be much more difficult to solve than problems in P. If we allow an algorithm to "guess" the next computational step randomly and allow that the algorithm accepts a given instance if and only if at least one path leads to an accepting state, then we get the class NP of *non-deterministic polynomial time* algorithms. It is a well known and fundamental open problem whether $P = NP$ in computer science but the equality is widely believed to be false and most scientists would conjecture that $P \neq NP$.

Even in the case of NP problems however, there exists an algorithm which will return the correct answer "true" or "false" after some finite amount of time, even if the amount of time turns out to be exponential in the size of the input. Throughout this thesis we shall not study the time complexity of algorithms, we shall instead be interested in whether or not *any algorithm* exists which will solve the problem regardless of any time constraints. This is the area of *computability theory.*

We shall show many decision problems on matrix semigroups for which there does not exist *any* algorithm which is guaranteed to return the correct answer "true" or "false" in a finite amount of time. The problems are

[2] By reasonable we mean storing integers in binary rather than unary encoding etc.

termed *undecidable.* Alan Turing proved the first undecidable problem in computability theory, known as the halting problem. From this result we can use a technique called "reduction", discussed in Chapter 3, to show many other problems are also undecidable.

One of the first results of undecidability in matrix semigroups was by A. Markov [42] in 1947 where he proved results which we may interpret as the emptiness testing of the intersection of matrix semigroups. We study this problem in Section 4.4 and show some variations of the undecidability results. In 1970, M. Paterson showed the *mortality problem* is undecidable. This problem is concerned with determining whether the zero matrix (a matrix with all zero elements) is in a semigroup generated by a given finite set of integer matrices. Since that time there has been much interest in decidability questions for problems concerning matrix semigroups.

One might question the rationale of studying the undecidability of computational problems since an undecidability result inherently means a solution for the problem does not exist. There are two main reasons which may be highlighted. Firstly, once a problem has been shown to be undecidable, it can be considered futile to search further for an algorithmic solution to the problem.

In this case we do have available choices such as simplifying the system to some extent or using approximations of solutions for example which can lead to algorithmic solvability of a problem. Let us illustrate this with an example. Given a finite set of matrices, we may assign a non-negative real number to the set called the *joint spectral radius* which can be thought of as a generalisation of the spectral radius on single matrices. It was shown in [15] that determining if the joint spectral radius, ρ, of a set of matrices Σ is less than or equal to 1, i.e., determining if $\rho(\Sigma) \leq 1$ is undecidable. However, it is known from a result of [11] that we can approximate the joint spectral radius *to any degree of accuracy* greater than 0. Thus, seemingly similar properties can have a different decidability status and if we can tolerate some degree of approximation or probability then algorithmic solutions can be developed.

The second reason to study undecidability is from a purely theoretical perspective; we are truly studying the limits of what is computable. Often with a small change to a parameter, i.e., the dimension of the matrices considered, the number of matrices in the generator or the number system used in the matrices, we can observe a change from decidability to undecidability. Understanding the reasons for this change is fundamental to understanding computability in general.

Hopefully the above reasoning shows that since matrices and matrix semigroups are so ubiquitous in mathematics and computer science, the study of computability of problems on such structures is fundamental and important in determining the computability of problems defined in many diverse fields.

1.2 Currently Known Results

In this section we shall give the current state of known decidability results for a set of problems in several dimensions and over different number fields. Since this is a currently active research area, many of these results may be improved upon relatively quickly but they are correct at the time of writing as far as the author is aware.

Let us now give a list of the problems with a brief and informal description of each. For more details and rigorous definitions, see Section 2.3 of Chapter 2.

Given a finite set of $n \times n$ matrices $\mathcal{G}$ over a semi-ring $\mathbb{F}$, generating a semigroup $\mathcal{S}$ we define the problems:

- MEMBERSHIP - Given a particular matrix $M \in \mathbb{F}^{n \times n}$, is it true that $M \in \mathcal{S}$?

- VECTOR REACHABILITY (VRP) - Given two vectors $x, y \in \mathbb{F}^n$ does there exist a matrix $M \in \mathscr{S}$ such that $Mx = y$?

- MORTALITY - Does the *zero matrix* belong to the semigroup $\mathscr{S}$?
- IDENTITY - Does the *identity matrix* belong to the semigroups $\mathscr{S}$?
- FREENESS - Is the semigroup $\mathscr{S}$ free? I.e. does each element of $\mathscr{S}$ have a unique factorisation over elements of $\mathscr{G}$?
- ANY DIAGONAL (AD) - Does the semigroup $\mathscr{S}$ contain any *diagonal* matrix?
- SCALAR - Does the semigroup $\mathscr{S}$ contain a specific scalar matrix kI (where $k \neq 0, \pm 1$)?
- VECTOR AMBIGUITY - Given a vector $x \in \mathbb{F}^n$, is the set of vectors $\{Mx : M \in \mathscr{S}\}$ free? I.e. is it true that for two matrices $M, N \in \mathscr{S}$, it holds that $Mx = Nx \Rightarrow M = N$?

We shall present a table of known results including some, but not all, of our contributions to the field presented in this thesis (highlighted in bold and underlined). Let us discuss the notation; the top row represents the problem to which we refer and they are listed above, the left column represents the dimension of the matrices. Each element at arbitrary row i and column j is of the form $\{\mathbf{D}, \mathbf{U}\}(\mathbb{F})_n$ or empty. The letters **D** and **U** represent Decidable and Undecidable respectively, $\mathbb{F}$ represents the particular semiring over which the decidability status refers and the subscript n represents the number of matrices in the generator (the symbol k means the result holds over any arbitrary (finite) number k).

Dim	MEMB	VRP	MORT	IDENT	FREE	AD	SCALAR
1	$D(\mathbb{C})_k$	$D(\mathbb{C})_k$	$D(\mathbb{H})_k$	$D(\mathbb{C})_k$	$D(\mathbb{C})_k$	$D(\mathbb{H})_k$	$D(\mathbb{H})_k$
2	$\underline{\boldsymbol{U}(\mathbb{H})_{14}}$	$\underline{\boldsymbol{U}(\mathbb{H})_{14}}$	$D(\mathbb{Q})_2$	$D(\mathbb{Z})_k$	$\underline{\boldsymbol{U}(\mathbb{H})_{18}}$	$\underline{\boldsymbol{U}(\mathbb{H})_{7}}$	$\underline{\boldsymbol{U}(\mathbb{H})_{14}}$
3	$U(\mathbb{Z})_8$	$\underline{\boldsymbol{U}(\mathbb{Q})_{5}}$	$U(\mathbb{Z})_8$	?	$U(\mathbb{N})_{18}$	?	$\underline{\boldsymbol{U}(\mathbb{Q})_{14}}$
4	$U(\mathbb{Z})_8$	$\underline{\boldsymbol{U}(\mathbb{Z})_{5}}$	$U(\mathbb{Z})_8$	?	$U(\mathbb{N})_{18}$	$\underline{\boldsymbol{U}(\mathbb{C})_{14}}$	$\underline{\boldsymbol{U}(\mathbb{Z})_{14}}$

The underlined and bold symbols represent a subset of our results that are presented within this thesis. Note that we have the containment hierarchy: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{C} \subset \mathbb{H}$. This means that if a problem is decidable over $\mathbb{Q}$ for example, then it is also automatically decidable over $\mathbb{N}$ and $\mathbb{Z}$ but it does not follow that the problem is decidable over $\mathbb{C}$ or $\mathbb{H}$. The opposite assertion is also true; if a problem is undecidable over $\mathbb{Q}$ then it follows that it is undecidable over $\mathbb{C}$ and $\mathbb{H}$ but not necessarily over $\mathbb{N}$ or $\mathbb{Z}$. In a similar fashion, if a problem is undecidable when its generator contains j matrices then the problem is also undecidable using any number greater than j of matrices. The number of matrices required is based upon the minimum instance size for which Post's correspondence problem (PCP) or one of its variants is currently known to be undecidable, therefore these numbers may change if smaller instance sizes are found for which the corresponding PCP variant used is still undecidable.

In dimension 1 all problems are straight forwardly decidable over the complex numbers since they are commutative. Some problems are also easy over the quaternions, for example the mortality problem, since the quaternions do not have zero divisors. However, we later state an open problem about the decidability of membership in one-dimensional quaternion semigroups in Open Problem 7.9 and also the decidability of the one-dimensional quaternion semigroup freeness problem in Open Problem 7.10.

All the undecidability results in two-dimensional quaternion matrix semigroups are from our paper [10] but decidability results in two dimensions are very sparse. In fact, only partial results are known for sub cases of many problems, for example a subclass of upper-triangular matrices is known in two dimensions where the freeness is decidable, see [17]. The decidability of the membership problem for the identity matrix in a matrix semigroup in two-dimensional integral matrices was shown in [19].

The mortality problem for three-dimensional integral matrices was shown to be undecidable in [45] and the number of matrices required in the generator for undecidability was reduced to just 8 in [25]. Note that the mortality problem is a special case of the membership problem. We later show, in Theorem 4.10, that the vector reachability problem is undecidable for matrix semigroups generated by 7 rational matrices of dimension 3. This result is from our paper [8]. The mortality problem was shown to be *decidable* for a pair of rational 2×2 matrices in [16]. The decidability status for an arbitrary number of matrices is an important open problem which we state in Open Problem 6.6.

We also mention that the problem of determining whether a finitely generated semigroup over any field is finite or not is a decidable problem, see [24] and [41]. From this result it follows that determining whether the semigroup generated by a single matrix is free or not is a decidable problem. To see this, we simply determine if the semigroup generated is finite, in which case the semigroup is not free; else the semigroup is free. The mortality problem for a single matrix is also thus decidable since we simply determine if the semigroup is finite and if it is, search for zero matrix in the finite number of matrices given. Lastly, the same argument holds to show that the membership problem for the identity matrix is decidable for a matrix semigroup generate by a single matrix (since the presence of the identity matrix means the semigroup must be finite, thus we simply need search the finite set for its presence).

1.3 Overview of the Thesis

We shall now show the general structure of the thesis. Chapter 2, *"Preliminaries"*, gives all the required elementary definitions from matrix theory, group theory and abstract algebra that will be used throughout. We have attempted to make this as self contained as possible and indicated references to books for other material when necessary. We also introduce hypercomplex numbers, specifically *quaternions* in this chapter. Since these are perhaps not as well known to some researchers, we have given a more thorough treatment of them.

Several classes of computational questions such as "membership problems", "vector reachability problems" and "freeness problems" are then given and discussed. The majority of problems studied throughout the thesis will fall into one of these categories and we give a general overview of them from a higher level here. Finally we show the strong connection between words and matrices and present a list of semigroup and group morphisms both from the literature and our work which may be useful as a reference.

In Chapter 3, *"Decision Problems for Words"*, we introduce the formal concept of undecidability and reduction which will be so useful throughout. This allows us to then show the familiar Post's correspondence problem (PCP) with some of its more recent variants. We provide two new versions which we name *Index Coding PCP* and *Fixed Element PCP* for reasons which become clear upon examining their proofs. The usefulness of the undecidability of these two problems becomes apparent later in the thesis when we reduce them to show new undecidability proofs of important matrix semigroup problems.

We then introduce two models of computation, namely, Turing machines and two-counter Minsky machines. A method of encoding these computational devices within two words will be shown and this allows us to obtain results later in the chapter. In fact, the simulation of a Turing machine via two words is exactly the way PCP can be shown to be undecidable. The results of this chapter and some from Chapter 4 were presented in [9]:

- P. Bell and I. Potapov, *Periodic and Infinite Traces in Matrix Semigroups*, Technical Report, The University of Liverpool, 2007.

Chapter 4, *"Integral to Complex Matrix Semigroups"*, begins the discussion of matrix semigroups problems on number fields up to the rational complex numbers [3]. We show that the membership problem for a *scalar matrix* in an integral matrix semigroup is an undecidable problem. A scalar

[3] i.e., integers, rationals, complex rationals but excluding the quaternions

matrix is one with a particular value k on each element of the main diagonal and 0 elsewhere. Such a matrix is important since it scales all matrices or vectors by an equal amount. These types of matrices occur in many applications due to this property. For the proof of this theorem we use the *Index Coding PCP* discussed in Chapter 3. We presented this paper at the Developments in Language Theory conference (DLT05) [5] and subsequently published in the Theoretical Computer Science journal, [7]:

- P. Bell, I. Potapov, *On the Membership of Invertible Diagonal Matrices*, Developments in Language Theory (DLT05), LNCS 3572, 146-157, 2005.
- P. Bell, I. Potapov, *On the Membership of Invertible and Diagonal Scalar Matrices*, Theoretical Computer Science, 372:37-45, 2007.

We then move to a problem which upon initial examination appears somewhat contrived but actually has links to several areas, namely that of determining whether in a particular finitely generated integral matrix semigroup any matrix has a zero in the top right element. The problem is often named the *Zero in the Upper Right Corner Problem* and is related to Skolem's problem on linear recurrences as is shown in Chapter 6 and the related *Zero in the Upper Left Corner Problem* was used in the proof of the mortality problem, see [25]. We reduce the dimensions of the two matrices needed for undecidability with an encoding technique which may be useful in other areas. We also use this technique to reduce the dimensions needed for the undecidability of the vector reachability problem to just 11 for semigroups generated by two rational matrices. These results were presented at the Developments in Language Theory 2006 conference and are currently awaiting publication in a special issue of Theoretical Computer Science, see [6, 8]:

- P. Bell, I. Potapov, *Lowering Undecidability Bounds for Decision Questions in Matrices*, Developments in Language Theory (DLT06), LNCS

4036, 375-385, 2007.

- P. Bell, I. Potapov, *On Undecidability Bounds for Matrix Decision Problems*, Special Issue of Theoretical Computer Science, (accepted for publication), 2007.

Next we move to the problem of determining whether any matrix in a rational complex matrix semigroup is diagonal. Clearly we can see similarities in the problem description to that of the scalar matrix problem mentioned above however the scalar matrix problem looks for a single particular matrix but there may also be other diagonal matrices which are in the semigroups which do not correspond to correct solutions of the PCP instance. Thus we cannot prove undecidability for any diagonal matrix using that particular method. The problem was given in [14] and the decidability status was said to be an open problem in any dimension. We show it is undecidable for four-dimensional rational complex matrix semigroups using the *Fixed Element PCP* of Chapter 3.

We then study several *vector reachability* problems and specifically the *Vector Ambiguity Problem*, the precise definition of which we leave for Section 2.3. At this point we then show how to simulate the previously mentioned computational models within a matrix semigroup in order to derive results on the undecidability of properties of the structure of matrix semigroups such as the *Recurrent Matrix Problem.*

The intersection emptiness problem for two semigroups is then discussed and undecidability results are shown similar to those studied by A. Markov [42]. This problem can roughly be stated as "Given two finitely generated semigroups S, T, is the intersection of these two semigroups empty? I.e. is $|S \cap T| = 0$?". The results on semigroup intersections are from [4]:

- P. Bell, *A note on the emptiness of semigroup intersections*, Fundamenta Informaticae, 79:1-4, 2007.

Chapter 5, "Quaternion Matrix Semigroup Problems", concerns computational problems on quaternion matrices which can be thought of as an extension to complex numbers which retain associativity but lose the commutativity property. Even more exotic number systems exist for any dimension which is a power of 2 however, after the four-dimensional quaternions, these numbers systems (starting from the 8-dimensional octonions) lose the property of associativity with their multiplication. Since semigroups require associativity by their definition, when using multiplication as the binary operator, the quaternions are the most abstract number system we may use.

For this reason we study computational problems on quaternion and quaternion matrix semigroups since in some ways this gives a more complete understanding of these problems. We start the chapter with an introductory discussion on the quaternions and then move to word morphisms. We then show a monomorphism $\gamma : \Sigma^* \mapsto \mathbb{H}(\mathbb{Q})$ between words and quaternions. This result allows us to encode word problems and show undecidability for several results such as membership, vector reachability, freeness, the existence of any diagonal matrix in the semigroup and semigroup intersection emptiness problems. We can also use the result to derive a free group of complex unitary matrices. We presented the majority of the results of this chapter in [10]:

- P. Bell, I. Potapov, *Reachability Problems in Quaternion Matrix and Rotation Semigroups*, Mathematical Foundations of Computer Science (MFCS), accepted for publication, 2007.

In Chapter 6 we consider matrix interpretations of Skolem's problem. We show the well known result that Skolem's problem can be interpreted as the zero in the upper right corner problem but we also show it is equivalent to the zero in the upper left corner problem. This proves useful since we can then show that Skolem's problem can be reduced to an instance of the Mortality problem on a semigroup generated by two matrices.

The results of this thesis were presented at the British Colloquium of Theoretical Computer Science (BCTCS 2005), Developments in Language Theory conference (DLT 2005, DLT 2006), Workshop on Algorithms on Words (WAW 2007), Mathematical Foundations of Computer Science (MFCS 2007) and several internal seminars in the Department of Computer Science at the University of Liverpool.

Chapter 2

Preliminaries

In this chapter we shall outline the introductory material from number theory, matrix theory, group theory and abstract algebra that will be required in this thesis. We try to give full definitions when possible for completeness and refer to the literature for any concepts not fully defined. A rather more complete introduction to *quaternions* is also given since this subject is perhaps not as widely known or studied in the field. We study computational problems on quaternions and quaternion matrices in Chapter 5.

We shall also define a general set of problems on matrix semigroups which will be studied extensively throughout this thesis with different constraints. To a large extent, all the problems studied will fall into one of these general categories.

The well known connection between binary words and matrices will also be shown and a selection of 2 × 2 free matrix semigroups and groups will be given. This will prove invaluable in many of the proofs of this paper and we collect them here for reference. The different homomorphisms between words and matrices have different properties which will aid us in later proofs.

2.1 Definitions

We use the standard notations $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{C}$ for the sets of natural numbers (including 0), integers, rationals and complex numbers respectively. We denote by $\mathbb{C}(\mathbb{Q})$ the field of *rational complex* numbers, i.e., numbers of the form $a + bi$ where $a, b \in \mathbb{Q}$ and $i = \sqrt{-1}$. This avoids the problem of how to input real numbers which do not have a finite representation.

Where we wish to be more general and not restrict ourselves to a specific number system, we shall use the notation $\mathbb{F}$ to refer to an arbitrary ring (defined below).

A *set* is a collection of distinct objects (called elements of the set). Given two finite sets, for example, $A = \{w, x, y\}$ and $B = \{x, y, z\}$, the *union* of A and B is denoted by $A \cup B = \{w, x, y, z\}$ and is the set of objects from either set A or B (discounting multiplicities). The *intersection* of sets A and B is denoted by $A \cap B = \{y, z\}$ and is the set of objects appearing in *both* A and B.

The *cardinality* of a set $A = \{a_1, a_2, \ldots a_n\}$ is denoted by $|A|$ and is defined as the number of objects in the set A, thus $|A| = n$ (note that we do not allow multiple copies of the same element in the set).

2.1.1 Matrix Theory

We denote an $m \times n$ matrix over a ring $\mathbb{F}$ by $\mathbb{F}^{m \times n}$. Actually, we shall almost exclusively be dealing with square matrices where $m = n$. We shall use basic properties of matrices which are outlined below. See [31] for a more thorough treatment. We denote by I_n the $n \times n$ *identity matrix*:

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

For a matrix $M \in \mathbb{F}^{n \times n}$ we denote the element in the i'th row and j'th column by $M_{[i,j]} \in \mathbb{F}$. For a matrix M, we denote the *transpose* of M by M^T. This is obtained by exchanging rows for columns, i.e., setting $M_{[j,i]} = M_{[i,j]}$.

A row vector x is a $1 \times n$ matrix $x = (x_0, x_1, \ldots, x_{n-1})$. A column vector is the transpose of a row vector and of dimension $n \times 1$. Two vectors $x = (x_0, x_1, \ldots, x_k)^T$, $y = (y_0, y_1, \ldots, y_k)^T$ are said to be *orthogonal* if

$$x^T y = (x_0, x_1, \ldots, x_k)(y_0, y_1, \ldots, y_k)^T = \sum_{i=0}^{k} x_i y_i = 0.$$

If the vectors x, y are both of unit length, i.e., $\sum_{i=0}^{k} x_i^2 = \sum_{i=0}^{k} y_i^2 = 1$, and also orthogonal, then they are said to be *orthonormal.*

The determinant of a matrix M is denoted by $\det(M)$. We may define it inductively using the Laplace expansion by minors. Given a matrix $A = [a_{ij}] \in \mathbb{F}^{n \times n}$ where $\mathbb{F}$ is an arbitrary ring, then let $\widetilde{A}_{ij} \in \mathbb{F}^{(n-1)\times(n-1)}$ denote the submatrix of A with row i and column j deleted. Assume that the determinant is already defined on $\mathbb{F}^{(n-1)\times(n-1)}$, then let:

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(\widetilde{A}_{ij})$$

for all $1 \leq i \leq n$ and define that the determinant of a 1×1 matrix is the single value in the matrix. See also [31] for more details. The important property that we shall require is that the determinant is multiplicative:

$$\det(AB) = \det(A) \cdot \det(B); \quad A, B \in \mathbb{F}^{n \times n}$$

A matrix M is *invertible* (i.e., has an inverse, M^{-1}, such that $MM^{-1} = I$) iff $\det(M) \neq 0$. Otherwise M is called *singular* or *non-invertible*. A matrix D is said to be *diagonal* if $D_{[i,j]} = 0$ whenever $i \neq j$, i.e., all off diagonal elements are zero. A matrix T is said to be *upper triangular* if $T_{[i,j]} = 0$ whenever $j < i$, i.e., the lower triangular part of the matrix (excluding the leading diagonal) is zero.

Given a matrix $M \in \mathbb{F}^{n \times n}$, a non-zero vector $x \in \mathbb{F}^n$ such that $Mx = \lambda x$, where $\lambda \in \mathbb{C}$, is called an *eigenvector*. The scalar λ is called an *eigenvalue* of the matrix M. In general, the matrix M may have up to n different eigenvalues but it may have duplicates. We denote by $\sigma(M)$ the set of eigenvalues of M. This is called the spectrum of M. The spectral radius of M is the non-negative value $\rho(M) = \max\{|\lambda| : \lambda \in \sigma(M)\}$.

If $Mx = \lambda x$ then $(\lambda I - M)x = 0$. Since x is not the zero vector, $(\lambda I - M)$ is singular, thus $\det(\lambda I - M) = 0$. This gives a degree n polynomial, named the characteristic polynomial, the roots of which are the eigenvalues of M.

Given two matrices $A \in \mathbb{F}^{i \times j}$ and $B \in \mathbb{F}^{k \times m}$ then the *Kronecker product* of A and B, denoted by $A \otimes B$ is defined by:

$$A \otimes B = \begin{pmatrix} A_{[1,1]}B & \cdots & A_{[1,j]}B \\ \vdots & \ddots & \vdots \\ A_{[i,1]}B & \cdots & A_{[i,j]}B \end{pmatrix} \in \mathbb{F}^{ik \times jm}.$$

We shall require the *mixed-product* property of Kronecker products:

Lemma 2.1. *[32] Let $A \in \mathbb{F}^{m \times n}, B \in \mathbb{F}^{p \times q}, C \in \mathbb{F}^{n \times k}$ and $D \in \mathbb{F}^{q \times r}$. Then $(A \otimes B)(C \otimes D) = AC \otimes BD$.*

Given two matrices $A \in \mathbb{F}^{m \times m}$ and $B \in \mathbb{F}^{n \times n}$, the *direct sum* of A and B, denoted by $A \oplus B$ is given by:

$$A \oplus B = \begin{pmatrix} A_{[1,1]} & \cdots & A_{[1,m]} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ A_{[m,1]} & \cdots & A_{[m,m]} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & B_{[1,1]} & \cdots & B_{[1,n]} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & B_{[n,1]} & \cdots & B_{[n,n]} \end{pmatrix} \in \mathbb{F}^{(m+n) \times (m+n)}.$$

It is easily shown that $\det(A \oplus B) = \det(A) \cdot \det(B)$ by the definition of the determinant.

2.1.2 Group Theory

A *semigroup* is denoted by $(\mathcal{S}, \cdot)$ where $\mathcal{S}$ is a (possibly infinite) set of elements and $\cdot$ is an associative binary operation such that if $a, b \in \mathcal{S}$ then

$a \cdot b \in \mathscr{S}$. We usually omit $\cdot$ and simply write ab. It is also a standard abuse of notation to refer to the semigroup itself by $\mathscr{S}$. We call the minimal set of elements $\mathscr{G}$ such that any element of $\mathscr{S}$ can be expressed as a product of elements of $\mathscr{G}$ the *generator* of the semigroup $\mathscr{S}$. If each such factorisation is unique, we call the semigroup *free*.

If there exists an element $e \in \mathscr{S}$ such that for all $x \in \mathscr{S}$, we have that $xe = ex = x$, then e is called the *identity element* and $\mathscr{S}$ is then called a *monoid* denoted by $(\mathscr{S}, \cdot, e)$. It can be proven that the identity element e is unique. Furthermore, if for all $x \in \mathscr{S}$ there exists a $y \in \mathscr{S}$ such that $xy = yx = e$ then $\mathscr{S}$ is called a *group* (each element has an inverse). If $\cdot$ is also commutative (i.e., $ab = ba$ for all $a, b \in \mathscr{S}$) then the above structures are called a *commutative semigroup, commutative monoid* and an *Abelian group* respectively. If each factorisation of elements of $\mathscr{S}$ is unique with respect to the generator of the group for *reduced products* (where we discount consecutive inverse elements), then the group is said to be *free*.

A *semi-ring* is a set $\mathscr{S}$, with two operations defined on it, denoted $+$ and $\cdot$ and two distinct elements $0, 1$ such that $(\mathscr{S}, +, 0)$ is a commutative monoid and $(\mathscr{S}, \cdot, 1)$ is a monoid. If $(\mathscr{S}, +, 0)$ is an Abelian group then $\mathscr{S}$ is known as a *ring*. If $(\mathscr{S} \setminus \{0\}, \cdot, 1)$ forms an Abelian group as well, then $\mathscr{S}$ is a *field* [1].

A *division ring* is a ring in which each element has a multiplicative inverse. We can see that a division ring is thus similar to a field but without the requirement of multiplicative commutativity. We shall see that the *quaternions* form a division ring but *not* a field since they have a non-commutative multiplication. Division rings are also sometimes known as *skew fields* or *non-commutative fields* in the literature but we shall not use this terminology since it is non standard.

2.1.3 Abstract Algebra

The structures discussed in Section 2.1.2, such as semigroups, groups, fields etc., are known collectively as *algebraic structures* (note that the list of structures given is by no means complete). We shall utilise functions or *mappings* between equivalent algebraic structures which preserve certain properties.

Given two algebraic structures A, B of the same type, we define a function ψ mapping elements of A (called the domain) to elements of B (called the codomain) by $\psi : A \mapsto B$. If each element of A maps to a distinct element of B, i.e., $\psi(x) = \psi(y) \Rightarrow x = y$, then ψ is said to be *injective*. If, for each element $y \in B$, there exists some $x \in A$ such that $\psi(x) = y$, then ψ is said to be *surjective*. A function which is both injective and surjective is called *bijective*.

A *homomorphism* is a mapping ψ between two algebraic structures of the same type A, B such that $\psi(x * y) = \psi(x) \circ \psi(y)$ for all $x, y \in A$ where $*$ is the binary operator of A and $\circ$ is the binary operator of B. A *monomorphism* is an injective homomorphism and an *isomorphism* is a bijective homomorphism.

2.1.4 Finite Words

Given an alphabet $\Gamma = \{a_0, a_1, \ldots, a_k\}$ we define a finite word, w, over the set Γ by $w = w_0 w_1 \cdots w_n \in \Gamma^*$. Given two words, $u = u_0 u_1 \cdots u_m$ and $v = v_0 v_1 \cdots v_n$ over the same alphabet, $u, v \in \Gamma^*$, the *concatenation* of u and v, written $u \cdot v$ (or uv for brevity) is given by:

$$uv = u_0 u_1 \cdots u_m v_0 v_1 \cdots v_n \in \Gamma^*.$$

The reverse of word $w = w_0 w_1 \cdots w_n$ is written w^R and is defined by $w^R = w_n \cdots w_1 w_0$. The *empty word* is denoted by ε and signifies a word with 0 letters. The notation $|w|$ is used for the *length* of word w, thus for the word $w = w_0 w_1 \cdots w_n$, clearly $|w| = n + 1$ and also $|\varepsilon| = 0$.

The inverse of a letter, a is denoted by either a^{-1} or $\overline{a}$ (depending which is clearer in the proof). The inverse of a word $w = w_0 w_1 \cdots w_n$ may be defined as: $\overline{w} = w^{-1} = \overline{w_n} \cdots \overline{w_1} \cdot \overline{w_0}$, which is the reverse of w with each letter replaced by its inverse. This is the inverse of w since clearly:

$$w\overline{w} = w_0 \cdot w_1 \cdots w_n \cdot \overline{w_n} \cdots \overline{w_1} \cdot \overline{w_0} = \varepsilon.$$

2.1.5 Hypercomplex Numbers

Rational complex numbers, which we denote by $\mathbb{C}(\mathbb{Q})$, are of the form $a + b\mathbf{i}$ where $a, b \in \mathbb{Q}$ and $\mathbf{i} = \sqrt{-1}$. There is a natural extension to complex numbers which gives *hypercomplex numbers* where we allow more imaginary parts.

W. R. Hamilton discovered that by using four dimensions, we can extend complex numbers to form a division ring with similar properties to the complex numbers. In fact, using the so called "Cayley-Dickson construction", it is possible to define such an algebra in any dimension which is a power of two.

In a similar style to complex numbers, rational quaternions, which are hypercomplex numbers, can be written $\vartheta = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ where $a, b, c, d \in \mathbb{Q}$. To ease notation let us define the vector: $\mu = (1, \mathbf{i}, \mathbf{j}, \mathbf{k})$ and it is now clear that $\vartheta = (a, b, c, d) \cdot \mu$ where $\cdot$ denotes the inner or 'dot' product. We denote rational quaternions by $\mathbb{H}(\mathbb{Q})$. A quaternion with real part 0 is called a *pure quaternion* and the set of such rational quaternions is denoted $\mathbb{H}(\mathbb{Q})_0$.

Quaternion addition is simply the componentwise addition of elements as in complex numbers, i.e.,

$$(a_1, b_1, c_1, d_1)\mu + (a_2, b_2, c_2, d_2)\mu = (a_1 + a_2, b_1 + b_2, c_1 + c_2, d_1 + d_2)\mu$$

It is well known that quaternion multiplication is not commutative. Multiplication is completely defined by the equations

$$\begin{aligned} \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 &= -1, \\ \mathbf{ij} = \mathbf{k} &= -\mathbf{ji}, \\ \mathbf{jk} = \mathbf{i} &= -\mathbf{kj}, \\ \mathbf{ki} = \mathbf{j} &= -\mathbf{ik} \end{aligned}$$

Thus for two quaternions $\vartheta_1 = (a_1, b_1, c_1, d_1)\mu$ and $\vartheta_2 = (a_2, b_2, c_2, d_2)\mu$, we can define their product as:

$$\begin{aligned} \vartheta_1\vartheta_2 = \quad & (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)\mathbf{i} \\ & +(a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)\mathbf{j} + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)\mathbf{k} \end{aligned}$$

which can be verified by laborious multiplication using the above equations.

In a similar way to complex numbers, we define the conjugate of $\vartheta = (a, b, c, d) \cdot \mu$ by $\overline{\vartheta} = (a, -b, -c, -d) \cdot \mu$. We can now define a norm on the quaternions by $||\vartheta|| = \sqrt{\vartheta\overline{\vartheta}} = \sqrt{a^2 + b^2 + c^2 + d^2}$. The inverse of a quaternion is given by:

$$\vartheta^{-1} = \frac{\overline{\vartheta}}{||\vartheta||^2}$$

since we see that

$$\vartheta\vartheta^{-1} = \frac{\vartheta\overline{\vartheta}}{||\vartheta||^2} = \frac{||\vartheta||^2}{||\vartheta||^2} = 1$$

Any non zero quaternion has a multiplicative (and obviously an additive) inverse [38]. Note also that $\vartheta_I = (1, 0, 0, 0)\mu \in \mathbb{H}(\mathbb{Q})$ is the multiplicative identity quaternion which is clear from the multiplication shown above. The other properties of being a division ring can be easily checked.

A *unit* quaternion has norm 1 and corresponds to a rotation in three-dimensional space. Given a unit vector $\vec{r} = (r_1, r_2, r_3)$ and a rotation angle $0 \le \theta < 2\pi$, we would like to find a quaternion transformation to represent a rotation of θ radians of a point $P' = (x, y, z) \in \mathbb{Q}^3$ about the $\vec{r}$ axis. To facilitate this, we require an encoding of P' as a pure quaternion P, namely $P = (0, x, y, z) \cdot \mu \in \mathbb{H}(\mathbb{Q})_0$.

Let us define a function $\psi_q : \mathbb{H}(\mathbb{Q}) \mapsto \mathbb{H}(\mathbb{Q})$ by $\psi_q(P) = qPq^{-1}\ q, P \in \mathbb{H}(\mathbb{Q})$ and $||q|| = 1$. If q is correctly chosen to represent a rotation of θ about a unit axis r, then this function will return a pure quaternion of the form $(0, x', y', z') \cdot \mu$ where $(x', y', z') \in \mathbb{Q}^3$ is the correctly rotated point.

It is well known (see, for example, [38]) that:

$$\vartheta = \left(\cos\frac{\theta}{2}, \vec{r}\sin\frac{\theta}{2}\right) \cdot \mu$$

represents a rotation of angle θ about the $\vec{r}$ axis. Therefore using $\psi_\vartheta(P)$ as just described rotates P as required. This will be used in the next section.

All possible unit quaternions correspond to points on the three-sphere. Any pair of unit quaternions p, q represent a four-dimensional rotation. Given a point $x \in \mathbb{H}(\mathbb{Q})$, we define a rotation of x, by $px\overline{q}$ [53]. Also we use the notation SU_2 to denote the special unitary group (the set of all 2×2 unitary unimodular matrices), the double cover of SO_3 which is the special orthogonal group (the set of all 3×3 orthogonal unimodular matrices).

2.2 Connections between Words and Matrices

There is a strong connection between word problems and matrix problems. In this section we shall emphasise this connection and show several monomorphisms between words or set of words and low dimensional matrices. Obviously, since the complex numbers are commutative, we cannot hope to store a word within a single complex number when using standard multiplication for concatenation, however we shall show that words *can* be stored in 2-dimensional matrices even over the integers.

We shall only be considering binary words in this section and most of the thesis, since we can usually use a simple homomorphism from arbitrary alphabets to binary alphabets. For example, given two alphabets, $\Gamma = \{x_1, x_2, \dots x_k\}$ and $\Sigma = \{a, b\}$, we may define the homomorphism $\psi : \Gamma^* \mapsto \Sigma^*$ by $\psi(x_i) = a^i b$ for example. This is an injective homomorphism (thus a *monomorphism*) and can usually be used to reduce problems over arbitrary alphabets to problems on binary alphabets.

We shall give examples of both free semigroups and free groups (where we require the presence of inverse letters also). These morphisms will be used in several places throughout this thesis and all but ζ below are well known from the literature. We arrived at the freeness of ζ through studying quaternions, see Chapter 5.

2.2.1 Semigroup Monomorphisms

Given a binary alphabet $\Sigma = \{a, b\}$, let $\gamma_1 : \Sigma^* \mapsto \mathbb{Z}^{2\times 2}$ be defined by:

$$\gamma_1(a) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \gamma_1(b) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

then γ_1 is a monomorphism.

Next we shall give a pair of monomorphisms which will be useful in Section 4.4. Let $\rho, \tau : \Sigma^* \mapsto \mathbb{Z}^{2\times 2}$ be monomorphisms defined as:

$$\rho(a) = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \rho(b) = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix} \tau(a) = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \tau(b) = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}.$$

The interesting properties of ρ and τ are that they are both integral and upper triangular. Furthermore, since element $[2, 2]$ of $\rho(w_1)$ and element $[1, 1]$ of $\tau(w_2)$ are equal to 1 for any $w_1, w_2 \in \Sigma^*$, when we form the direct product $\rho(w_1) \oplus \tau(w_2)$, we can join this element together and map into $\mathbb{N}^{3\times 3}$ (which will also be upper triangular) rather than $\mathbb{N}^{4\times 4}$. See Section 4.4 for further details.

2.2.2 Group Monomorphisms

Given a binary alphabet with its inverses $\Sigma = \{a, b, \overline{a}, \overline{b}\}$ forming a group $\langle \Sigma, \cdot \rangle$. Let $\lambda : \Sigma^* \mapsto \mathbb{N}^{2\times 2}$ be defined by:

$$\lambda(a) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \lambda(b) = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \lambda(\overline{a}) = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}, \lambda(\overline{b}) = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}.$$

It is well known from the literature that λ is an injective homomorphism, i.e., the group generated by $\{\lambda(a), \lambda(b), \lambda(\overline{a}), \lambda(\overline{b})\}$ is free.

In Chapter 5 we shall deal with computational problems on rational quaternions. The theorems developed there allow us to define a mapping $\zeta : \Sigma^* \mapsto \mathbb{C}(\mathbb{Q})^{2\times 2}$ where:

$$\zeta(a) = \begin{pmatrix} \frac{3}{5}+\frac{4}{5}\mathrm{i} & 0 \\ 0 & \frac{3}{5}-\frac{4}{5}\mathrm{i} \end{pmatrix}, \quad \zeta(b) = \begin{pmatrix} \frac{3}{5} & \frac{4}{5} \\ -\frac{4}{5} & \frac{3}{5} \end{pmatrix},$$
$$\zeta(\overline{a}) = \begin{pmatrix} \frac{3}{5}-\frac{4}{5}\mathrm{i} & 0 \\ 0 & \frac{3}{5}+\frac{4}{5}\mathrm{i} \end{pmatrix}, \quad \zeta(\overline{b}) = \begin{pmatrix} \frac{3}{5} & -\frac{4}{5} \\ \frac{4}{5} & \frac{3}{5} \end{pmatrix}.$$

We prove that ζ is an injective homomorphism in Section 5.2.1 and thus the group generated by $\{\zeta(a), \zeta(b), \zeta(\overline{a}), \zeta(\overline{b})\}$ is free. Note that these matrices are unitary.

2.3 Computational Problems in Matrix Semigroups

We shall primarily be dealing with computational problems on matrix semigroups. There are a general set of problems which we can consider on such structures which we shall now outline.

Problem 2.2. MEMBERSHIP PROBLEM - *Given a semigroup $\mathscr{S}$ generated by a finite set $\mathscr{G}$, and some single element X. Is it true that $X \in \mathscr{S}$?*

We ask these computational problems for a class of instances rather than a single specific instance. For example, we might ask "Given a generator of 10 integral matrices of dimension 4 generating a semigroup $\mathscr{S}$, does there exist an algorithm to determine if $X \in \mathscr{S}$ where $X \in \mathbb{Z}^{4\times 4}$?". We wish to either find a single algorithm which can take any instance of this class and return the answer "true" or "false" after some *finite* amount of time or else we wish to prove that no such algorithm exists.

Problem 2.3. VECTOR REACHABILITY PROBLEM - *Given a semigroup of matrices $\mathscr{S}$, generated by a finite set $\mathscr{G} \subset \mathbb{F}^{n \times n}$ and two column vectors $x, y \in \mathbb{F}^n$. Does there exist some matrix $M \in \mathscr{S}$ such that $Mx = y$?*

It should be clear that in the vector reachability problem the matrix M is not unique. For example, we see that:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{3}{2} \\ -1 & 2 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

Problem 2.4. SCALAR REACHABILITY PROBLEM - *Given a semigroup of matrices $\mathscr{S}$, generated by a finite set $\mathscr{G} \subset \mathbb{F}^{n \times n}$ two column vectors $x, y \in \mathbb{F}^n$ and a scalar $r \in \mathbb{F}$. Does there exist some matrix $M \in \mathscr{S}$ such that $x^T M y = r$?*

Again, it is clear that M is not unique in the scalar reachability problem.

Problem 2.5. SEMIGROUP FREENESS PROBLEM - *Given a finite set of matrices $\mathscr{G}$ generating a semigroup $\mathscr{S}$, does every element $M \in \mathscr{S}$ have a* single, unique *factorisation over $\mathscr{G}$?*

As an example of the SEMIGROUP FREENESS PROBLEM, imagine we have a set of two matrices $\mathscr{G} = \{A, B\}$ generating a semigroup $\mathscr{S}$. Consider the binary tree of products of $\mathscr{G}$ in Figure 2.1.

If for example the two elements marked, AAB and BBA, are equal then the matrix they are equal to does not have a unique factorisation over $\mathscr{G}$. If every matrix in the *infinite* binary tree is unique, then the semigroup is free. We study the freeness of quaternion matrix semigroups in Theorem 5.8 of Section 5.3.

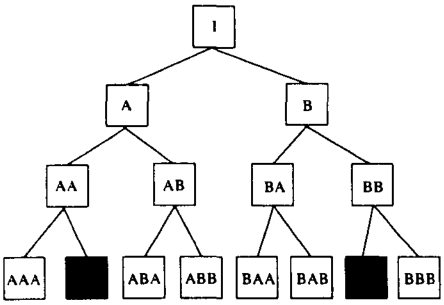

Figure 2.1: Binary Tree of Two Matrices

Problem 2.6. VECTOR AMBIGUITY PROBLEM - *Given a semigroup $\mathcal{S} \subseteq \mathbb{F}^{n \times n}$ and an initial vector $u \in \mathbb{F}^{n \times n}$. Let V be a set of vectors such that $V = \{v : v = Mu; M \in S\}$. Does $\mathcal{S}$ and u generate an ambiguous set of vectors? In other words the question is whether for every vector of set V there is a unique matrix $M \in \mathcal{S}$ such that $Mu = v$?*

This problem can be thought of as the freeness problem for a set of vectors formed by multiplication of each matrix is a finitely generated semigroup. We show that this problem is undecidable in Theorem 4.12 of Section 4.2.

Throughout this thesis we shall study these and related decision problems on algebraic structures. Our main aim is to explore the boundaries of decidability for the problems. This means we would either like to present an algorithm to solve the problems or to prove that no algorithm exists which will always halt and give the correct answer to the decision problem. In the next chapter we shall therefore begin the discussion of undecidability for *word problems* by embedding computational models. This will allow us in later chapters to encode such problems within matrix semigroups.

Chapter 3

Decision Problems for Words

In this chapter we shall begin exploring *computability theory* and introduce the fundamental mathematical concept of *undecidability* which will feature heavily throughout this thesis. The problems we shall encounter will be defined on words. Since we showed the strong correspondence between word problems and matrix problems in the last chapter, we will then be able to interpret the undecidable problems of this chapter in terms of matrix problems in later results.

One of the central problems that we will utilise several times called Post's correspondence problem will be shown and proven to be undecidable via the standard encoding of a Turing machine within it such that the instance has a solution if and only if the corresponding Turing machine halts. This may be familiar and a standard result, however we give a simple proof of the theorem in Section 3.3.2, both for completeness and also since the details of the proof itself will be required for a later result.

Two models of computation will be shown, namely "Turing machines" and "Two-counter Minsky machines". The concept of a universal machine will be introduced and will play a role in a later theorem.

3.1 Algorithmic Undecidability

A decision problem takes an instance of a problem in some representation, performs a calculation on the instance data using a computational device (such as a Turing machine [49]) and returns the answer "true" or "false".

Given a class of instances of a decision problem, then the problem is said to be *decidable* for that class if there exists an algorithm $\mathcal{A}$ that 'halts' after some *finite* amount of time on every input of the class and returns the correct "true" or "false" answer to the decision problem.

If, for some decision problem, we can show that no such algorithm exists, the problem is said to be *undecidable*. The natural question then is "how do we *prove* that no such algorithm can exist for a particular class of problems?".

Alan Turing, building upon previous work by Kurt Gödel, famously proved that the *halting problem* is undecidable. He then reduced this to the "Entscheidungsproblem" (German for "decision problem") posed by David Hilbert. The idea of algorithmic reduction is a key step in showing undecidability and we shall give an informal description of the method (see [49] for more details).

Given two problems A and B, a *reduction* is a way of converting problem A to problem B such that a solution to problem B gives a solution to problem A. We say A is reducible to problem B. Thus, intrinsically problem B is at least as hard as problem A. If we know that problem A is "hard" in some formal sense, then so is problem B.

We shall show an intuitive example of this. Imagine we have a problem "FACTOR" which takes a natural number and returns its full factorisation. We also have a second problem "PRIME" which takes a natural number and returns "true" or "false" (it is a decision problem) depending whether the number is a prime. Obviously "PRIME" is reducible to "FACTOR" since if we can factor a number then it is prime iff the number itself and 1 are its factors.

We shall heavily utilise a well known undecidable problem known as Post's correspondence problem (PCP). By reducing this problem to other problems we consider, we can show that they are also undecidable. In fact, Post's correspondence problem is a reduction from the halting problem discussed above but clearly reduction is transitive.

3.2 Post's Correspondence Problem (PCP) and Variants

We shall use Post's correspondence problem several times throughout this thesis and therefore we shall give two equivalent definitions of the problem. Sometimes one definition may be easier to visualise than the other or may give a simpler proof but it is clear that the two formulations are essentially the same.

Problem 3.1. PCP Version 1 - *Given a binary alphabet $\Sigma = \{a, b\}$ and a finite set of pairs of words:*

$$P = \{(u_1, v_1), (u_2, v_2), \dots, (u_n, v_n)\} \subset \Sigma^* \times \Sigma^*.$$

Does there exist a finite sequence $s = (s_1, s_2, \dots, s_k)$ of indices such that $u_{s_1}u_{s_2} \cdots u_{s_k} = v_{s_1}v_{s_2} \cdots v_{s_k}$?

and the equivalent formulation of the problem:

Problem 3.2. PCP Version 2 - *Given a finite alphabet Γ, a binary alphabet Σ and two homomorphisms $h, g : \Gamma^* \mapsto \Sigma^*$. Does there exist any word $w \in \Gamma^+$ such that $h(w) = g(w)$?*

Once again we state that Problems 3.1 and 3.2 are equivalent as can easily be seen. The instance size of Post's correspondence problem (PCP) is the number of pairs of words n in Problem 3.1 or the cardinality of Γ in Problem 3.2. These two values are also equivalent in each problem regardless of which definition of the problem we use.

Post's correspondence problem was shown to be undecidable in 1946 by Emil Post [46]. In fact it is undecidable even when $|\Gamma| = 7$ as was shown in [43] and it is known to be decidable when $|\Gamma| = 2$ [22]. The decidability status when $3 \leq |\Gamma| \leq 6$ are currently open problems. We denote by n_{PCP} the minimum instance size of PCP which is known to be undecidable, thus n_{PCP} currently equals 7. We show a standard proof of the undecidability of PCP in Section 3.3.2 after we have introduced the mathematical model of a Turing machine.

An example of Post's correspondence problem - Given the set of pairs of words $P = \{P_1, P_2, P_3\}$ such that:

$$P_1 = \left[\frac{aab}{a}\right], P_2 = \left[\frac{ba}{a}\right], P_3 = \left[\frac{ab}{bbaabb}\right],$$

where we have placed the first word on top and the second word on the bottom to make the example clearer. Now take the sequence $P_1P_2P_3P_2$ which gives:

$$\left[\frac{aab}{a}\right]\left[\frac{ba}{a}\right]\left[\frac{ab}{bbaabb}\right]\left[\frac{ba}{a}\right].$$

Reading the top and bottom words we see that they are equal thus this is a correct solution to PCP.

3.2.1 Claus Instances of PCP

We shall now describe a variation of Post's correspondence problem (PCP) which allows us to use a smaller instance size in several problems. We shall state the theorem without proof and refer the interested reader to the original recent paper [28]. The authors of that paper name such instances of PCP as *Claus Instances* of PCP after the author of a paper (V. Claus) who shows how to encode a semi-Thue system within PCP instances of small size

[20]. This result was later used by Y. Matiyasevich and G. Sénizergues to show that PCP(7) is undecidable.

Problem 3.3. CLAUS INSTANCES PCP: *Given a finite set of letters* $\Gamma = \{x_1, x_2, \ldots, x_n\}$, *a binary alphabet* $\Sigma = \{a, b\}$, *and a pair of homomorphisms* $h, g : \Gamma^* \mapsto \Sigma^*$. *Does there exist a solution* $x_1 w x_n$ *where* $w \in \{x_2, x_3, \ldots, x_{n-1}\}^*$? *I.e. does* $h(x_1 w x_n) = g(x_1 w x_n)$?

Note that this means the first and last letters, x_1 and x_n respectively, are used just once and their positions within the solution are known in advance. The following result was studied in [28] and originally shown in the works of [20] and [43]:

Theorem 3.4. *[20, 28, 43] Problem 3.3,* CLAUS INSTANCES PCP *is undecidable with* 7 *letters in the domain, i.e.,* $|\Gamma| = 7$.

In fact, even Post's original proof of the undecidability of PCP used a similar formulation whereby we fix the first and last letters of the domain which are used just once in (respectively) the first and last positions of the solution. It is often possible to use this problem instead of the usual version of PCP in order to derive lower dimensions of undecidability in many cases. Indeed, we use this theorem several times throughout this thesis. Actually, by studying the proof of [43] where the authors prove PCP is undecidable with just 7 words, the authors encode a semi-Thue system exactly in the above way. Thus whenever we use the result of [43] we are in fact using these "Claus instances" already.

3.2.2 Index Coding PCP

A new coding technique for Post's correspondence problem (PCP) which we call INDEX CODING PCP will be of use several times throughout this thesis. We developed this coding in order to show the scalar matrix membership is undecidable in matrix semigroups. It appears to be of separate interest however since it has been useful in other contexts [10] and was recently studied by V. Halava, T. Harju and M. Hirvensalo [28].

Problem 3.5. INDEX CODING PCP: *Given a binary alphabet $\Sigma = \{a, b\}$, inverse alphabet $\overline{\Sigma} = \{\bar{a}, \bar{b}\}$ and a finite set of pairs of words:*

$$\{(u_i, v_i) | 1 \leq i \leq n\} \subset (\Sigma \cup \overline{\Sigma})^* \times (\Sigma \cup \overline{\Sigma})^*.$$

Does there exist a finite sequence $s = (s_1, s_2, \ldots, s_k)$ such that exactly one $s_j = n$ and $u_{s_1} u_{s_2} \cdots u_{s_k} = v_{s_1} v_{s_2} \cdots v_{s_k} = \varepsilon$?

Theorem 3.6. *The* INDEX CODING PCP *(Problem 3.5) is undecidable.*

We shall utilise this theorem several times throughout this thesis. By examining and proving the result purely in terms of words, we can later use the proof in matrix problems with reasonably straight-forward encodings. We use a similar style to that of [28] by proving the result in terms of words rather than just matrices, but we do not use Claus instances and thus the number of matrices in the generator will be somewhat larger than required. See [28] for details.

Proof. We shall first give an outline of the proof followed by the detailed explanation. The proof is somewhat technical in nature but not difficult to follow once the general idea is understood. Given a standard version of PCP, we try to find a sequence $s = (s_1, s_2, \ldots, s_k)$ such that $u_{s_1} u_{s_2} \cdots u_{s_k} = v_{s_1} v_{s_2} \cdots v_{s_k}$ but without using inverse alphabet $\overline{\Sigma}$. If we invert the second word, we see that:

$$u_{s_1} u_{s_2} \cdots u_{s_k} \cdot \overline{v_{s_k}} \cdots \overline{v_{s_2}}\, \overline{v_{s_1}} = \varepsilon.$$

This means we only need store *one* word rather than two, and if some non-empty sequence equals ε, we have a solution to the PCP. However, we need to ensure that the sequence of indices is also in the correct order and for this we require the second word. With the encoding we outline below, the first and second word will both equal ε in the case that we have a correct solution to PCP.

We can think of the indices as being a stack, we push on each index of the u word we use and then pop each once we start using v words. Using our encoding, if there is ever an "error" (the sequence is not in the correct order), then the word produced cannot ever equal ε after that. We shall now give the details of the proof.

Given an instance of Post's correspondence problem (PCP), i.e., a finite set $\{(u_j, v_j) : 1 \leq j \leq n\} \subset \Sigma^* \times \Sigma^*$ where Σ is a binary alphabet. Define the set of pairs of words P by:

$$P = \{(u_i, a^i b), (\overline{v_i}, \overline{a}^i \overline{b}), (\varepsilon, b), (\overline{\star}, \overline{b}) : 1 \leq i \leq n\}.$$

We use the mixed modification PCP where the first pair used is fixed, see Section 3.3.2. For a technical reason, we also append $\star$ to the beginning of u_1 in the instance (which is then mapped into a unique binary sequence as explained in the proof). We then put $\overline{\star}$ under this same binary encoding into the first element of the final pair of words $(\overline{\star}, \overline{b})$. The reason for this will become apparent later.

Let $m = |P| = 2n + 2$ and assume there exists some sequence $s = (s_0, s_1, \ldots, s_k)$ with each $1 \leq s_i \leq m$, exactly one $s_j = m$ and $P_{s_0} P_{s_1} \cdots P_{s_k} = (\varepsilon, \varepsilon)$ using pairwise concatenation. Let us consider the form the second word must take.

Take the set of second words from pairs in P, i.e., $S = \{a^i b, \overline{a}^i \overline{b}, b, \overline{b} : 1 \leq i \leq (n-1)\}$. We shall prove that for all words $w \in S^+$ such that $w = \varepsilon$ and w uses the final word $(\overline{b})$ exactly once, w is a conjugate of the form :

$$w = (a^{i_1} b)(a^{i_2} b) \cdots (a^{i_t} b)(\overline{b})(\overline{a}^{i_t} \overline{b}) \cdots (\overline{a}^{i_2} \overline{b})(\overline{a}^{i_1} \overline{b})(b) = \varepsilon. \qquad (\dagger)$$

Let us assume for now that *both* b and $\overline{b}$ are used only once in the second word.

Clearly w equals ε so we must only prove that any word $w \in S^+$ containing exactly one b and $(\bar{b})$ equalling ε is of the given form.

Notice first that no product from $A = \{a^i b, \bar{a}^i \bar{b} : 1 \leq i \leq n\}$ equals the identity element. Thus if b and $\bar{b}$ are consecutive then the product contains no element from A if it equals ε. Since the first words corresponding to b and $\bar{b}$ are not inverse by the construction of the PCP, we can discount this situation since the first word would not equal ε and we thus require that at least one $a^i b$ and $\bar{a}^i \bar{b}$ type word from S is used. Assume then that the product does contain elements from A and thus b and $\bar{b}$ are *not* consecutive.

Assume we have a product containing exactly one b and $\bar{b}$ in the second word which equals ε. Clearly then we can write the product in the form:

$$x_1 x_2 \cdots x_n \bar{b} y_1 y_2 \cdots y_m b \quad ; x_i, y_i \in A$$

by cyclically permuting the product (since it equals identity). If $x_n = \bar{a}^i \bar{b}$ for some i, then we have $x_n \bar{b} = \bar{a}^i \bar{b}\bar{b}$. No element of A can left or right multiply to reduce this product and we cannot right multiply by the remaining b since b and $\bar{b}$ would then be consecutive. Thus $x_n = a^i b$ for some i. This gives the product $x_n \bar{b} = a^i$. Now consider y_1; if it equals $a^j b$ for some j, then we get $x_n \bar{b} y_1 = a^{i+j} b$. Since $\bar{b}$ has been used however, we cannot reduce this further by right multiplications, thus $y_1 = \bar{a}^j \bar{b}$ for some j.

Assume that $i \neq j$, then $x_n \bar{b} y_1$ equals either $a^{i-j} \bar{b}$ if $i > j$ or $\bar{a}^{j-i} \bar{b}$ if $j > i$. The only way these can be reduced is to right multiply by b giving a^{i-j} or $\bar{a}^{j-i}$ with both b and $\bar{b}$ now used. But now we must right multiply by $\bar{a}^{i-j} \bar{b}$ or $a^{j-i} b$ respectively leaving a single $\bar{b}$ or b. But since we only have one such element, it cannot reduce the product to ε; thus $i = j$.

Finally then we see that $x_n = a^i b$ and $y_1 = \bar{a}^i \bar{b}$ for some i. This gives the central product $x_n \bar{b} y_1 = \bar{b}$. We can continue this argument inductively and see that the product must be a conjugate of the form given on the previous page (†).

This therefore fixes the form of the second word in a sequence where both words equal ε. Now we shall observe the form of the first word when the second word is of the form (†). It clearly must be:

$$\star u_{i_1} u_{i_2} \cdots u_{i_t} \varepsilon \overline{v_{i_t}} \cdots \overline{v_{i_2}}\,\overline{v_{i_1}}\,\overline{\star}$$

From the mixed modification PCP we used, the first pair of words is fixed, thus $i_1 = 1$. Clearly then, this product equals ε if and only if $u_{i_1} u_{i_2} \cdots u_{i_t} = v_{i_1} v_{i_2} \cdots v_{i_t}$ if and only if the mixed modification PCP instance has a solution. Thus the problem is undecidable as required. □

In our proof we required that the last *two* pairs of words were use only once instead of only the last pair, however it was proven in [28] that using a different encoding and Claus instances of PCP, we can in fact fix that only one pair of words must be used once and also reduce the number of pairs of words required.

Corollary 3.7. *[28] The* INDEX CODING PCP *is undecidable for* $2n_{CLAUS}$ *pairs of words were one specific pair is used only once in any product.*

We shall now give an example of INDEX CODING PCP to show how an instance of the standard PCP can be adapted to fit into this problem using the ideas present in the previous proof.

An example of Index Coding PCP - We will use the same initial instance of PCP from the previous example and extend the instance set using the instructions of Theorem 3.6. Let us define:

$$L_1 = \left[\frac{\star aab}{ab}\right], L_2 = \left[\frac{ba}{aab}\right], L_3 = \left[\frac{ab}{aaab}\right] M = \left[\frac{\varepsilon}{b}\right],$$

$$R_1 = \left[\frac{\overline{a}}{\overline{a}\,\overline{b}}\right], R_2 = \left[\frac{\overline{a}}{\overline{a}\,\overline{a}\,\overline{b}}\right], R_3 = \left[\frac{\overline{bbaabb}}{\overline{a}\,\overline{a}\,\overline{a}\,\overline{b}}\right] N = \left[\frac{\overline{\star}}{\overline{b}}\right],$$

where according to the construction, u_1, u_2, u_3 are stored in the first word of L_1, L_2, L_3 and v_1, v_2, v_3 are stored in the first words of R_1, R_2, R_3 respectively. Thus since as in the previous example a correct solution was $P_1P_2P_3P_2$, a correct solution in this example is $L_1L_2L_3L_2MR_2R_3R_2R_1N$.

Note that, as required, N is used once. The first word of this product is given by:

$$\star aab \quad ba \quad ab \quad ba \quad \varepsilon \quad \overline{a} \quad \overline{bbaabb} \quad \overline{a} \quad \overline{a} \quad \overline{\star} = \varepsilon,$$

as we expect. The second word in this product can be seen to be:

$$ab \quad aab \quad aaab \quad aab \quad \overline{b} \quad \overline{a}\overline{a}\overline{b} \quad \overline{a}\overline{a}\overline{a}\overline{b} \quad \overline{a}\overline{a}\overline{b} \quad \overline{a}\overline{b} \quad \overline{b} = \varepsilon,$$

again as expected. Thus if we have such a solution, the top and bottom words will equal ε and correspond to it (so long as a specific element N is used once in the solution).

3.2.3 Fixed Element PCP

We shall now detail another variant of Post's correspondence problem (PCP) which shall later be useful. It is similar to the INDEX CODING PCP but with some interesting differences which allow us to directly show the undecidability of determining if there exists any diagonal matrix in a complex matrix semigroup. The proof is also somewhat simpler than that of INDEX CODING PCP since we avoid conjugates.

Problem 3.8. FIXED ELEMENT PCP - *Given an alphabet* $\Gamma = \{a, b, \overline{a}, \overline{b}, \star\}$ *and a finite set of pairs of words over* Γ,

$$P = \{(u_1, v_1), (u_2, v_2), \ldots, (u_n, v_n)\} \subset \Gamma^* \times \Gamma^*.$$

Does there exist a finite sequence of indices $s = (s_1, s_2, \ldots, s_k)$ *such that* $u_{s_1}u_{s_2}\cdots u_{s_k} = v_{s_1}v_{s_2}\cdots v_{s_k} = \star$*?*

This variant of PCP is interesting since it looks similar to the original PCP however it is over a binary group alphabet and instead of testing for a solution via equality checking for two arbitrary words, the solutions will have a specific form for a fixed letter $\star$. This is useful since we know the specific form of a solution.

Theorem 3.9. *The* FIXED ELEMENT PCP *is undecidable.*

Proof. Given a binary alphabet $\Sigma = \{a, b\}$, let us define a new alphabet, $\Gamma = \Sigma \cup \{\overline{a}, \overline{b}, \star\}$, where $\star, \notin \Sigma$.

The instance set of FIXED ELEMENT PCP will now be defined. Given a standard instance of PCP:

$$P' = \{(u_1, v_1), (u_2, v_2), \ldots, (u_m, v_m)\} \subset \Sigma^* \times \Sigma^*$$

we define the two sets:

$$L = \{(\star u_1, \star bab), (u_i, a^i b)\} \subset \Gamma^* \times \Gamma^* \quad ; 2 \leq i \leq m \tag{3.1}$$

$$R = \{(\overline{v_i}, \overline{a}^i \overline{b}), (\overline{v_m}, \overline{b}\overline{a}^m \overline{b})\} \subset \Gamma^* \times \Gamma^* \quad ; 1 \leq i \leq m - 1 \tag{3.2}$$

Since we are looking for a product of pairs of words equal to $(\star, \star)$ and $\star^{-1} \notin \Gamma$, then the first pair $L_1 = (\star u_1, \star bab)$ must occur exactly once. Let us therefore define any such product (if it exists) as:

$$X = (\star, \star) = X_1 X_2 \cdots X_k \in \langle L \cup R \rangle.$$

It can be seen that $X_1 = L_1$, otherwise if $X_j = L_1$ for some $j > 1$, then:

$$\langle (L \cup R) \setminus \{L_1\} \rangle \supseteq X_1 X_2 \cdots X_{j-1} = (\varepsilon, \varepsilon),$$

but this is impossible since clearly $\varepsilon \notin \langle \{\overline{b}\overline{a}^m \overline{b}, a^i b, \overline{a}^i \overline{b} \; : \; 1 \leq i \leq m\} \rangle$, therefore the second word cannot equal ε. Thus we must have:

$$X = L_1 X_2 \cdots X_k = (\star, \star).$$

Let us consider the second words, in order to determine the sequence they must take to give $\star$. We have the set of elements:

$$A = \{\star bab, \overline{b}\overline{a}^m \overline{b}, a^2 b, \ldots a^m b, \overline{a}\overline{b}, \ldots, \overline{a}^i \overline{b}\}.$$

We know the first element is $\star bab$ which is used only once. We must find the form of any product equal to $\star$.

Clearly, $(\star bab)(\overline{b}\overline{a}\overline{b}) = \star$ is one such solution but since the first words will not be equal (unless we have a trivial PCP solution), we discount such a situation. Since $(\star bab)$ is the first element used, assume that the next element is from R, i.e., of the form $\overline{a}^i\overline{b}$ for some $1 \leq i \leq m-1$. But this gives $(\star bab)(\overline{a}^i\overline{b})$ and this cannot be reduced by further right multiplications since clearly from the set A, there is not any product of elements with a 'b' on the left hand side (even when using products of elements).

Thus, the second element must be of the form a^ib for $2 \leq i \leq m$. Let $j+1$ be the first index at which we do not have an element from L, thus the product $X_1X_2\cdots X_j$ is of the form: $(\star bab)(a^{i_2}b)(a^{i_3}b)\cdots(a^{i_j}b)$ where $2 \leq i_2, i_3, \ldots, i_j \leq m$. To reduce this product, the next element must be $\overline{b}\overline{a}^m\overline{b}$ since this is the only element with a '$\overline{b}$' on the left. The product of $(a^{i_j}b)(\overline{b}\overline{a}^m\overline{b})$ is $\overline{a}^{m-i_j}\overline{b}$. If $m \neq i_j$ then this will not reduce to '$\overline{b}$' and similarly to before, we cannot reduce this product any further since the right hand element is $\overline{b}$. Thus $i_j = m$.

The next element to the right cannot be $\overline{b}\overline{a}^m\overline{b}$ since this will have a $\overline{b}$ on the right hand side which cannot be cancelled, thus using the same argument as before, it must be of the form $\overline{a}^k\overline{b}$ giving:

$$\cdots(a^{i_{j-1}}b)(\overline{b})(\overline{a}^k\overline{b})\cdots$$

which cancels again to give $\overline{b}$ iff $k = i_{j-1}$. This continues inductively for each pair of elements from the centre outwards and we see that we finally reach $\star$ if and only if the product is of the form:

$$L_1L_{i_1}L_{i_2}\cdots L_mR_m\cdots R_{i_2}R_{i_1}R_1$$

The first word corresponding to this is a correctly encoded PCP sequence which equals $\star$ iff it corresponds to a correct solution word completing the proof.

Recall that the original PCP can be encoded into words over just two letters. In a similar way we may encode Σ' into two letters $\{a, b\}$ together with inverses $\{\overline{a}, \overline{b}\}$ and a special symbol $\star$ and thus we get the result of the theorem.

In fact, we could map all letters into just the set $\{a, b, \overline{a}, \overline{b}\}$ by using a homomorphism such that $\overline{\star}$ is not contained in the image of the morphism. For example, given the set $\Gamma = \{a, b, \overline{a}, \overline{b}, \star\}$ we map each element via an injective homomorphism $\gamma : \Gamma \mapsto \{a, b, \overline{a}, \overline{b}\}$ defined as:

$$\gamma(a) = aba, \gamma(b) = bab, \gamma(\overline{a}) = \overline{a}\overline{b}\overline{a}, \gamma(\overline{b}) = \overline{b}\overline{a}\overline{b}, \gamma(\star) = aaa.$$

This idea will be useful later in Theorem 4.1.3. □

3.3 Word Embeddings of Computational Models

The undecidability results for matrix semigroups we shall show will in general use a reduction from Post's correspondence problem (PCP) which simulates a Turing machine and thus deciding whether it has a solution is an undecidable problem. In this section we will show other direct embeddings of classical computational models such as Turing machines and two-counter automata into matrix semigroups. The simulation is done via pairs of words as in PCP, but in such a way that the termination of the computation is not always required for analysis, which is similar to the idea of infinite PCP.

We shall convert these word problems into matrix problems in Section 4.3. We shall then show that the proposed simulations can be used as a new tool for the analysis of matrix semigroup structures. In particular, we reformulate several undecidable questions for the above models into matrix semigroup problems. This is a different approach from standard undecidability results which may have far-reaching consequences and may help with some open problems that are difficult to explore by reduction directly from the undecidability of Post's Correspondence Problem.

3.3.1 Computational Models

Turing Machines - Let $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{accept}}, q_{\text{reject}})$ be a Turing machine, where Q is the finite set of states, Σ is the input alphabet, Γ is the tape alphabet q_0 is the initial state, q_{accept} is the accepting state, q_{reject} is the rejecting state and δ is the transition function. An instantaneous description of the Turing machine is given by $s_1s_2\ldots s_{m_1}q_it_1t_2\ldots t_{m_2}$ where each $s_j, t_j \in \Gamma$ and $q_i \in Q$. This means that M is in state q_i and $s_1s_2\ldots s_{m_1}$ are the symbols to the left of the tape head and $t_1t_2\ldots t_{m_2}$ is to the right of the tape head (or the words may be empty).

The transition function δ defines the next rule to apply depending which state we are in and the next symbol read to the *right* of the tape head. The rule can change the current state, write a new symbol to the right of the tape head and then move left or right one step. If L denotes a left move and R denotes a right move, then $\delta : Q \times \Gamma \mapsto Q \times \Gamma \times \{L, R\}$ is the transition function. For example, let $\delta(q_i, a) = (q_j, b, R)$. This means, if we are in state q_i with symbol 'a' to the right, then we move to state q_j, change the 'a' to a 'b' and move the tape head to the right. In terms of instantaneous descriptions, this means "$\ldots q_ia\ldots$" will map to "$\ldots bq_j\ldots$" under δ for example.

Two-Counter Register Machine - In this section we describe a well known model known as a Minsky machine (or register machine). Informally speaking, a Minsky machine is a two-counter automata that can increment and decrement counters by one and test them for zero. It is known that a two-counter Minsky machine represents a universal model of computation [44]. Being of very simple structure, Minsky machines are very useful for proving undecidability results (see for example [36, 37, 40]).

It is convenient to represent a counter machine as a simple imperative program $\mathcal{M}$ consisting of a sequence of instructions labelled by natural numbers from 1 to some $L \in \mathbb{Z}^+$. Any instruction is one of the following forms:

l: ADD 1 to S_k; GOTO l';

l: IF $S_k \neq 0$ THEN SUBTRACT 1 FROM S_k; GOTO l';

ELSE GOTO l'';

l: STOP;

where $k \in \{1, 2\}$ and $l, l', l'' \in \{1, \dots, L\}$.

The machine $\mathcal{M}$ starts executing with some initial non-negative integer values in counters S_1 and S_2 and the control at instruction labelled 1. We assume the semantics of all above instructions and of entire program is clear. Without loss of generality one can suppose that every machine contains exactly one instruction of the form l: STOP which is the last one ($l = L$). It should be clear that the execution process (run) is deterministic and has no failure. Any such process is either finished by the execution of L: STOP instruction or lasts forever.

As a consequence of the universality of such computational model the halting problem for Minsky machines is undecidable:

Theorem 3.10 ([44]). *It is undecidable whether a two-counter Minsky machine halts when both counters initially contain* 0.

3.3.2 Simulation of Computational Models

Turing Machine Simulation - We shall illustrate the simple encoding of a Turing machine by a set of pairs of words as is standard in the proof of Post's correspondence problem [49].

Given a Turing machine M, our aim is to produce a set of pairs of words $P = \{(u_1, v_1), (u_2, v_2), \dots, (u_n, v_n)\}$ such that there exists a finite sequence of indices $S = (i_1, i_2, \dots, i_k)$ with each $1 \leq i_j \leq n$ where $u_{i_1} u_{i_2} \cdots u_{i_k} = v_{i_1} v_{i_2} \cdots v_{i_k}$ iff M halts on input v which is encoded in v_1. The sequence S we shall call a solution and corresponds to a halting configuration of M.

We may assume without loss of generality that M doesn't attempt to move its tape head to the left of an empty word which is an easy restriction to impose. Furthermore, we currently assume the first pair used for a solution is (u_1, v_1) and we remove this restriction later.

We shall now show a set of pairs of words simulating the Turing machine M. Let $w = w_1 w_2 \cdots w_f \subset \Sigma^*$ be the input word. Then define the pair $(u_1, v_1) = (\#, \# q_0 w_1 w_2 \cdots w_f \#) \in P$. This is the initial configuration of M. Now, for every $a, b \in \Gamma$ and every $q_i, q_j \in Q$, with $q_i \neq q_{\text{reject}}$, if $\delta(q_i, a) = (q_j, b, R)$, add pair $(q_i a, b q_j)$ to the set P.

Also, for every $a, b, c \in \Gamma$ and every $q_i, q_j \in Q$ with $q_i \neq q_{\text{reject}}$, if $\delta(q_i, a) = (q_j, b, L)$, add pair $(c q_i a, q_j c b)$ to set P. Now, for every $a \in \Gamma$, add (a, a) to P. Also add $(\#, \#)$ to P which is used to separate instantaneous descriptions and for all $a \in \Gamma$, add $(a q_{\text{accept}}, q_{\text{accept}}), (q_{\text{accept}} a, q_{\text{accept}})$.

We can now see that the given construction will have a solution iff the Turing machine M halts on input w. We must start with the first pair $(u_1, v_1) = (\#, \# q_0 w_1 w_2 \cdots w_f \#)$ as stated previously. The next pair (u_{i_2}, v_{i_2}) in a solution must have $u_{i_2} = q_0 w_1$ and thus v_{i_2} will be the corresponding pair from the transition function. We must then use pair $(u_{i_3}, v_{i_4}) = (w_2, w_2)$ and this continues for the rest of w until we must use pair $(\#, \#)$. At this point we may have the following pairs:

$$(\# q_0 w_1 w_2 \cdots w_f \#, \# q_0 w_1 w_2 \cdots w_f \# y_1 q_i w_2 w_3 \cdots w_f \#)$$

for example. As can be seen, the first word contains the first instantaneous description $q_0 w$ and the second contains the first description $q_0 w$ followed by δ applied to the first configuration. After the next iteration of applying these pairs of words, the second configuration will be concatenated to the first pair and the *third* configuration will be appended to the second pair. This continues until we reach a state with q_{accept} at which point we use the pairs $(a q_{\text{accept}}, q_{\text{accept}}), (q_{\text{accept}} a, q_{\text{accept}})$ which will increase the size of the first word to be equal to the second word which corresponds to a correct solution.

We can enforce that the first pair used must be (u_1, v_1) by using a word morphism. Let $y = y_1 y_2 \cdots y_n \subset \Gamma^*$ be any word and let '$*, \triangleright$' be new letters not in Γ. Then define the three functions:

$$\begin{aligned} \star y = &\quad *y_1 * y_2 \cdots * y_n \\ y\star = &\quad y_1 * y_2 * \cdots y_n * \\ \star y \star = &\quad *y_1 * y_2 * \cdots * y_n * \end{aligned}$$

We finally add $(u_n, v_n) = (*\triangleright, \triangleright)$ to set P. Now, for each element of $P = \{(u_i, v_i) | 1 \leq i \leq n\} \subset (Q \cup \Gamma \cup \{*, \triangleright\})^* \times (Q \cup \Gamma \cup \{*, \triangleright\})^*$, we apply one of the three above $\star$ functions to each word pair. Let $(u_1, v_1) = (\star u_1, \star v_1 \star)$, $(u_j, v_j) = (\star u_j, v_j \star)$ for each $2 \leq j \leq (n-1)$ and $(u_n, v_n) = (*\triangleright, \triangleright)$ is left as before. Clearly if a match occurs in P it must start with this new (u_1, v_1) since only the first two letters in these two words are equal. Examining the morphism allows us to conclude it must then proceed as before using the new pairs (u_i, v_i) with $2 \leq i \leq n$ and finally finish with the pair (u_n, v_n), see [49] for further details.

Two-Counter Minsky Machine Simulation - Finally we show how to simulate a two-counter Minsky machine using a set of pairs of words P. We use the definitions of a two counter machine from [33]. We require two operations, firstly "from state q, increment counter $\{1, 2\}$ and move to state s". Secondly we require operation "test if counter $\{1, 2\}$ is zero, moving to state r if it is, or state t if it is positive". We shall use the symbol 'z' throughout to denote a zero counter.

We start with the initial pair of words $(u_1, v_1) = (\#, \#za^iq_0a^jz\#)$ where i denotes the value of the first counter C_1 and j denotes the value of the second counter C_2. Note that a^i is simply i copies of the letter 'a', thus $a^i = aa \cdots a$. Let us deal with the first type of operation. To move from state q to s and increment C_1, we add the pair (q, as) to P. To move from state q to s and increment C_2, we add the pair (q, sa) to P. But the counters could be zero (denoted zqC_2 or C_1qz) so we also add pairs (zq, zas) to increment C_1 and (qz, saz) to increment C_2.

For the second operation, we require to move from q to r if C_1 is zero, so we add pair (zq, zr). To move from q to r if C_2 is zero, we add pair (qz, rz). To move from q to t and decrement C_1 if not zero, we add pair (aq, t) and to move from q to t and decrement C_2 if not zero, we add pair (qa, t). Finally, we add pairs (a, a), $(\#, \#)$, (z, z), $(aq_{\text{accept}}, q_{\text{accept}})$, $(q_{\text{accept}}a, q_{\text{accept}})$ and $(\#\triangleright, \triangleright)$ to P.

Once more, we use morphism $\star$ to ensure pair $(u_1, v_1) \in P$ is used first and to avoid trivial PCP solutions and if there exists some sequence $S = (i_1, i_2, \ldots, i_k)$ such that the equation $u_1 u_{i_1} u_{i_2} \cdots u_{i_k} = v_1 v_{i_1} v_{i_2} \cdots v_{i_k}$ holds, then it corresponds to a correct halting computation of a two-counter machine and it is thus undecidable whether such a sequence S exists.

Proposition 3.11. *Turing machines and two-counter machines can be simulated by Post's correspondence problem (*PCP*).*

This is straight-forward from the above descriptions. It is usual to prove PCP undecidability by simulating a Turing machine but we have shown it is also possible to *directly* simulate a two-counter Minsky machine.

3.3.3 Periodicity in Counter Machines

Counter machines are a particularly nice model of computation since they are simple to define whilst retaining universality with just two counters. It was proven in [12] that given a counter machine M which may or may not halt, we can construct a second counter machine, called M', such that M' never halts and has a periodic configuration if and only if M halts. Since the halting problem for arbitrary counter machines is undecidable, this means that checking the periodicity of counter machines is also undecidable.

We shall now give a simpler proof to the above result from [12]:

Theorem 3.12. *Let M' be a counter machine that has no halting configuration. The problem of deciding if M' has a periodic configuration is undecidable. The problem is undecidable even in the case of two-counter machines.*

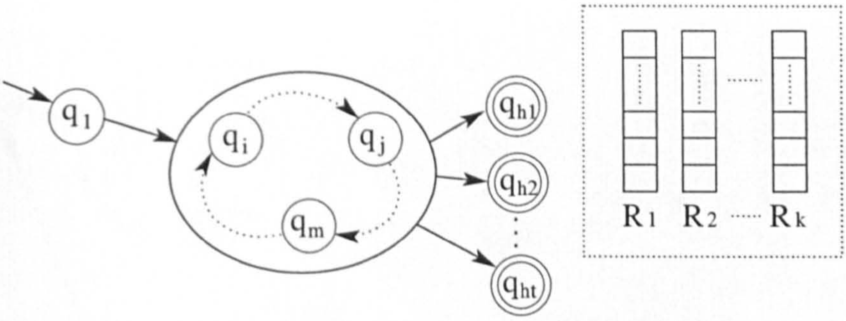

Figure 3.1: Minsky machine with k counters

Proof. Given a specific counter machine M. Let q_0 be the initial state of M and $H = \{q_{h_1}, q_{h_2}, \ldots, q_{h_t}\}$ be the set of halting states. Let $R = \{R_1, R_2, \ldots, R_k\}$ be the set of counters (or registers) of M. See Figure 3.1.

The transition function of M depends upon whether specific registers equal zero. Firstly, it can increase a register R_i and move to a new state. Secondly, if a specific register R_i is non-zero, it can decrease R_i and then move to a new state r. Otherwise, if register R_i is equal to zero, it leaves it unchanged and moves to a new state s. The transition function, δ, will be a set of such rules.

We shall now show how to create a new machine M'. Initially, let M' have the same states Q as M and the same transition function δ. We add a new start state q_I and add the two rules to δ which move from q_I to state q_0 regardless of whether the first register R_1 equals zero and leaves all registers as they are.

We define all halting states $H \subseteq Q$ to be non-halting states and add new states $q_{R_1}, q_{R_2}, \ldots, q_{R_k}$. These new states will be used to zero all counters. We add rules which move us from each $q \in H$ to q_{R_1} regardless of whether R_1 is non-zero and leave all counters at their current values. Then for each state q_{R_i}, $1 \leq i < k$ we add rules which decrease R_i if it is non-zero and remain in the current state. We add a rule to move to state $q_{r_{i+1}}$ if it does equal zero (thus the counter is decremented to zero before going to the next

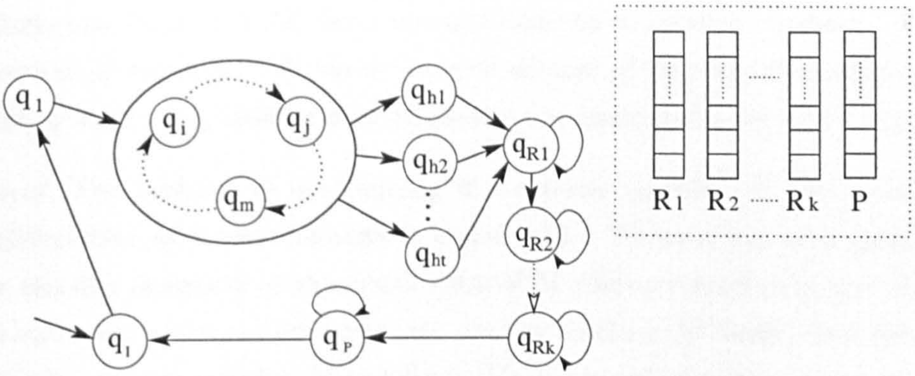

Figure 3.2: Periodic Minsky machine

state. Finally, for state q_{R_k} we add a rule to decrease R_k if it is non-zero and stay in state q_{R_k}, or else move to the initial state q_I if it does equal zero (note that once we go to q_I, all counters are equal to 0 and we are back to the original configuration).

Thus, if M reached a halting state with some values in its counters R, then M' will instead decrement all counters to zero and restart the computation. Clearly the only way to get back to q_I is via some state in H of M, thus the only way M' is periodic (i.e., the only way it goes to q_I and zeros all counters) is if M halts as required.

We may note that there may be some configuration of M which is periodic, thus M' will contain an ultimately periodic configuration (though not periodic since it still wont go to q_I). We can avoid this situation if required by a simple construction. Add a new counter P such that every transition from machine M increments P and then does what it would do normally (we need to add new states and rules to do this). Then add a new state q_P such that q_{R_k} now goes to q_P instead of q_I. Then add rules to decrement q_P to zero as before and then move to state q_I. The only way to decrement counter P is via a halting state thus now the *only* periodic configuration contains q_I with all counters zero in the period. See Figure 3.2. □

Theorem 3.13. *Let M' be a nondeterministic n-counter machine. The problem of deciding if M' has an infinite number of trajectories leading to a halting state s_{final} with zero in all counters is undecidable for any $n \geq 2$.*

Proof. The problem of determining if a counter machine M can reach a halting state with zero counters is undecidable. Without loss of generality we can also assume that the initial state of M will be visited only once. Let us construct a new nondeterministic counter machine M' based on a deterministic counter machine M as follows. First, we add two extra states q_{final} (which is the only halting state of M') and $q_{continue}$. Then add transitions from all halting states of M leading to both q_{final} and $q_{continue}$ which will only be executed if both counters are zero. Secondly, we create copies of all transitions from the initial state of M and add them to the automaton as outgoing transitions from $q_{continue}$.

As a result, we have that the initial state of M' (which is the same as in M) will be visited only once and a state q_{final} with zero counters is reachable in M' if and only if machine M can reach a halting state with zero counters. On the other hand, if q_{final} with zero counters can be reached at least once, we can construct an infinite number of traces that will lead to q_{final} by returning from the halting state of M to $q_{continue}$ and repeating the same looping trace an unbounded number of times before going to state q_{final}. □

3.3.4 The Infinite Post Correspondence Problem

It was shown in [12] that the INFINITE POST CORRESPONDENCE PROBLEM is undecidable for 105 pairs of words. This result was later improved to 9 by V. Halava and T. Harju [27] by encoding semi-Thue systems and utilising Claus's construction for Post's correspondence problem (PCP). The authors of [27] also show a related result that determining if a particular PCP instance has a solution that is non ultimately periodic is undecidable.

Lemma 3.14. *[27] If the termination problem is undecidable for n-rule semi-Thue system, then it is undecidable for instances of the* PCP *size $n+3$ whether or not there exists an infinite solution that is not ultimately periodic.*

We recall that an infinite word is said to be ultimately periodic if it can be written in the form $w = uv^{\infty}$ where u, v are non-empty, finite words. We shall not give the definition of the termination problem for a semi-Thue system, (see [27]), but merely state that it is undecidable for instances of size 3 as was proven in [43]. Thus Lemma 3.14 is undecidable for PCP instances of size 6.

We shall use our encoding of two-counter Minsky machines into pairs of words and thus PCP instances and Theorem 3.12 of [12] to derive a result on a specific set of words (we use the definition of PCP in terms of homomorphisms):

Theorem 3.15. *There exists a class of instances of Post's correspondence problem which have a guaranteed single infinite solution and no finite solution where it is undecidable whether the solution is ultimately periodic.*

Proof. We saw a construction in Section 3.3.2 which allowed us to simulate an arbitrary two-counter machine by a pair of words as is done in PCP. We shall use the idea from Theorem 3.12 in which we start with an initial counter machine M and create a second counter machine M' such that M' *does not halt* and M' has a periodic configuration if and only if M halts on its input in the same way as was originally done in [12]. Since determining if the arbitrary counter machine M halts is undecidable, determining if M' has a periodic configuration is undecidable as explained in Theorem 3.12.

It is well known that a k-counter machine can be simulated by a two-counter machine (with an increase to the number of states and instructions). Let $R_1, R_2, \ldots, R_k$ be the k counters of the machine. We create a new machine with two counters C_1, C_2 such that C_1 stores the prime number encoding of the previous counters, i.e.,

$$C_1 = 2^{R_1} 3^{R_2} 5^{R_3} \cdots \pi(k)^{R_k}; \quad R_i \in \mathbb{N},$$

where $\pi(k)$ is the k'th prime number. We can thus increment register R_j by multiplying C_1 by $\pi(j)$, test counter R_j for zero equality by testing if C_1 is divisible by $\pi(j)$ and decrement C_1 by performing this division. The second counter C_2 allows us to achieve these operations whilst retaining the other values in counter C_1.

Therefore, from machine M', we create a third machine M'' which has only two states using the prime power idea of the previous paragraph. Using the construction in Section 3.3.2, and Proposition 3.11, we can simulate machine M'' via an instance of PCP which we denote P. However, because of the construction of M', we know that it *does not halt*, thus P has no solution.

The counter machine M' is deterministic and has a guaranteed infinite run since it does not halt. Therefore instance P has a single infinite word solution. By the conversion from a two-counter machine to a PCP instance from Section 3.3.2, there is a single letter $\gamma_1 \in \Gamma$ which must be used first and then never again. Therefore, the infinite solution to PCP is of the form:

$$w' = \gamma_1 w; \quad \gamma_1 \in \Gamma, w \in (\Gamma \setminus \{\gamma_1\})^\infty.$$

Since determining if M' is periodic is undecidable, it is also undecidable whether w is a periodic word, or equivalently, whether w' is ultimately periodic, thus completing the proof.

Therefore our steps are as follows. Given any two-counter Minsky machine M, we create a second machine M' such that M' does not halt and it is periodic if and only if M halts (see Theorem 3.12). Then we create a third machine M'' which is equivalent to M' but uses only two states. Next we convert M'' to a PCP instance with a guaranteed single infinite solution and no finite solutions (see Section 3.3.2). This gives us a specific infinite word of the form $\gamma_1 w$ for each initial counter machine M such that w is periodic if and only if M halts. □

Chapter 4

Integral to Complex Matrix Semigroups

In this chapter we shall explore various reachability problems on semigroups of matrices defined over integers, rational numbers and complex rational numbers in small dimensions such as those outlined in Section 2.3. In general, we shall identify which problems are undecidable and attempt to minimise the number of matrices required in the generator of the semigroup as well as the dimension of the matrices used.

Since the integers are a subset of the rationals which in turn are a subset of rational complex numbers, we will also try to prove results on the smallest subset possible, i.e., integers before rationals which in turn we try to use before complex rationals. When the number system used impacts the dimension or number of matrices required however, we may indicate both bounds in corollaries.

We have separated these results on integral, rational and rational complex matrix semigroups from that of Chapter 5 which deals with hypercomplex numbers. There are two main reasons for this. Firstly, number systems up to the complex numbers are more 'traditional' to study for computability problems and there exists a plethora of results in this area. It may be unclear how the results on quaternions matrices should be compared with the current results in the field and thus they are included separately so that we can give a better context for their study. Secondly, the quaternions are non-commutative and thus they have a fundamental difference from numbers up to the complex rationals which we study here.

4.1 Membership Problems

We recall from Section 2.3 the general definition of a membership problem:

MEMBERSHIP PROBLEM - Given a semigroup $\mathscr{S}$ generated by a finite set $\mathscr{G}$, and some single element X. Is it true that $X \in \mathscr{S}$?

We shall evaluate the decidability of this problem for a particular scalar diagonal matrix and then consider a special case of the membership whereby we are only interested in a specific single element of the matrices generated.

One of the first problems in this area shown to be undecidable was THE MORTALITY PROBLEM, which is the membership problem of the *zero matrix* in a finitely generated matrix semigroup. The problem was shown to be undecidable for three-dimensional integral matrix semigroups in 1970 by M. Paterson [45]. It was then shown by V. Halava and T. Harju that the problem is in fact undecidable even when the generator contains only eight matrices, see [25]. See Chapter 6 for a reduction of SKOLEM'S PROBLEM to THE MORTALITY PROBLEM.

The presence of a zero matrix in a semigroup is important since it means any time we multiply by this matrix, all current values are lost; there is no way to recover the previous state. This is indeed the case for any singular matrix (when the determinant equals 0) since we cannot invert the matrix to retrieve the state before applying this matrix.

Another important matrix is the identity matrix I. Multiplication by I leaves the matrix unaffected and the presence of the identity matrix in a semigroup is an important property to determine for many problems, for example it tells us whether the semigroup is a monoid and also whether the semigroup is a group.

It is known that for commuting matrix semigroups, membership is decidable, see [3]. In fact there exists a polynomial time algorithm to solve the membership problem. It was shown in [39] that membership in integral row-monomial matrix semigroups is decidable in any dimension which is one of the very few known decidable cases for non-commuting matrix semigroups.

We shall now consider membership problems for scalar matrices which have interesting geometric properties.

4.1.1 Scalar Matrix Membership Problem

A rational *scalar matrix* is a matrix of the form kI_n where $k \in \mathbb{Q}$ and I_n is the $n \times n$ identity matrix. It is thus of the form:

$$\begin{pmatrix} k & 0 & \cdots & 0 \\ 0 & k & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & k \end{pmatrix} \quad ; k \in \mathbb{Q}.$$

Geometrically, a scalar matrix will *scale* a vector to be of a different length (the length is multiplied by k) but the direction remains unchanged. When multiplied by a matrix a scalar matrix will multiply all elements by k while retaining the general properties of the matrix. The determinant will clearly be multiplied by k^n.

We are now ready for the main result of this section:

Theorem 4.1. *Given a finite set of integer matrices $\mathcal{G}$ in dimension 4 generating a semigroup $\mathcal{S}$, and a scalar $k \in \mathbb{Z}$ such that $|k| > 1$, it is undecidable whether $kI_4 \in \mathcal{S}$.*

Proof. In order to prove this result we shall use the INDEX CODING PCP (see Section 3.2.2). Given a binary alphabet $\Sigma = \{a, b\}$ and inverse alphabet

$\overline{\Sigma} = \{\overline{a}, \overline{b}\}$, an instance of this problem is of the form:

$$P = \{(u_i, v_i) | 1 \leq i \leq n\} \subset (\Sigma \cup \overline{\Sigma})^* \times (\Sigma \cup \overline{\Sigma})^*.$$

and we must determine if there exists a finite sequence $s = (s_1, s_2, \ldots, s_k)$ such that exactly one $s_j = n$ and $u_{s_1} u_{s_2} \cdots u_{s_k} = v_{s_1} v_{s_2} \cdots v_{s_k} = \varepsilon$. We shall reduce this problem to the membership problem for a particular k-scalar matrix in a 4×4 integral matrix semigroup such that the matrix kI is in the semigroup if and only if the instance of Index Coding PCP has a solution thus proving the undecidability of the membership problem.

Let us use the injective homomorphism $\lambda : (\Sigma \cup \overline{\Sigma})^* \mapsto \mathbb{Z}^{2 \times 2}$ from Section 2.2.2 defined by:

$$\lambda(a) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \lambda(b) = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \lambda(\overline{a}) = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}, \lambda(\overline{b}) = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}.$$

Since this is an injective homomorphism, the group $\langle\{\lambda(a), \lambda(b), \lambda(\overline{a}), \lambda(\overline{b})\}\rangle$ is free. Given the instance P above, for each pair $(u_i, v_i) \in P$, where $1 \leq i \leq n$, we define a matrix:

$$X_i = \begin{pmatrix} \lambda(u_i) & \mathbf{0}_2 \\ \mathbf{0}_2 & \lambda(v_i) \end{pmatrix}$$

where $\mathbf{0}_2$ is the 2×2 zero matrix. Note that by the definitions of the monomorphisms used, each X_i is unimodular. We must enforce that in the Index Coding PCP the final pair (u_n, v_n) is used only once. To encode this within the semigroup, we shall multiply the final matrix X_n by a scalar k (say $k = 2$ will do).

Now, let $\mathcal{S}$ be a semigroup generated by $\{X_1, X_2, \ldots, kX_n\}$. If matrix kI_4 (the k-scalar matrix) is in $\mathcal{S}$, it implies that the matrix kX_n is used in its product exactly once since all other matrices in the generator are unimodular (the determinant is multiplicative). Therefore there exists a finite product:

$$X_{s_1} X_{s_2} \cdots X_{s_j} = kI_4.$$

where exactly one $X_{s_i} = X_n$. Examining the top left and bottom right 2×2 matrices of this product, since λ is a monomorphism, we see that if such a product exists, then:

$$u_{s_1} u_{s_2} \cdots u_{s_j} = v_{s_1} v_{s_2} \cdots v_{s_j} = \varepsilon,$$

again with exactly one $s_i = n$. This is a reduction of INDEX CODING PCP to the membership of the matrix kI_4 in a matrix semigroup $\mathscr{S}$. Since INDEX CODING PCP is undecidable with 14 pairs of words [28], the membership problem is undecidable for semigroups generated by 14 matrices. □

We can also extend the generator by a single matrix to gain a more general result for different k:

Corollary 4.2. *Given a finite set of* rational *matrices $\mathscr{G}$ in dimension* 4 *generating a semigroup $\mathscr{S}$, and* any *scalar $k \in \mathbb{Q} \setminus \{0, \pm 1\}$, it is undecidable whether $kI_4 \in \mathscr{S}$.*

Proof. In the last step of Theorem 4.1, we multiplied matrix X_n by 2. Clearly we could multiply by any $k \in \mathbb{Q} \setminus \{0, \pm 1\}$ instead and obtain a more general result. □

We might ask about the excluded cases whereby $k = 0, \pm 1$ in which our construction fails to hold. For $k = 0$ this is simply the mortality problem, "Does the zero matrix belong to a finitely generated semigroup?". This was shown to be undecidable by M. Paterson, see [45].

For the case where $k = 1$, this is also an important open problem which has been studied extensively without avail:

Open Problem 4.3. IDENTITY MATRIX MEMBERSHIP PROBLEM - *Given a finitely generated matrix semigroup $\mathscr{S}$, does the identity matrix I belong to $\mathscr{S}$?*

This seems to be a difficult and long standing open problem whose solution might have many consequences in different settings. Unfortunately our construction above fails to work for the identity matrix. We must ensure that one specific pair of words in INDEX CODING PCP is used exactly once in a correct sequence. We enforce this by making all matrices unimodular except one special matrix X_n whose determinant k is not equal to $0, \pm 1$. This allows us to conclude that if we have a matrix product with determinant k, it must contain X_n exactly once as required. But by using all unimodular matrices we cannot enforce this constraint and we no longer reduce the problem correctly to that of membership.

4.1.2 Zero in Upper Right Corner Problem

In Section 4.1.1, we showed the undecidability of a particular matrix in a matrix semigroup. We shall now consider a slightly different membership type problem where we ask if there is any matrix M in the semigroup such that the top right element is equal to 0.

Problem 4.4. ZERO IN THE UPPER RIGHT CORNER PROBLEM *(ZURC)- Given a finite set of $n \times n$ integral matrices $\mathcal{G}$ generating a semigroup $\mathcal{S}$. Does there exist any matrix $M \in \mathcal{S}$ such that $M_{[1,n]} = 0$?*

This may seem somewhat artificial at first glance, however the problem of whether a zero appears in the upper right corner of a matrix can encode Skolem's problem as we show in Chapter 6. Furthermore, the presence of a zero in the top left corner was a pivotal point in the proof of the undecidability of THE MORTALITY PROBLEM [45].

We shall consider the zero in the upper right corner problem where the generator contains just two integral matrices. This problem was known to be undecidable for dimension $3n_{\text{PCP}} + 3$ (currently 24) in [18] and this was improved to $3n_{\text{PCP}}+2$ (currently 23) in [23]. We shall now prove the problem is undecidable even for dimension $2n_{\text{PCP}} + 4$ (currently 18).

Theorem 4.5. *The* ZERO IN THE UPPER RIGHT CORNER PROBLEM *is undecidable for a semigroup generated by two integral matrices of dimension* $2n_{PCP}+4$ *(currently* 18*).*

Proof. We have already seen that there exists an injective morphism between pairs of words over a binary alphabet $\Sigma = \{a, b\}$ and integral matrices in Section 2.2. In fact, one such morphism, which was originally used by M. Paterson to prove the undecidability of the mortality problem for integral matrix semigroups [45], is $\lambda' : \Sigma^* \times \Sigma^* \mapsto \mathbb{Z}^{3\times 3}$ defined by:

$$\lambda'(s,t) = \begin{pmatrix} 3^{|s|} & 0 & \sigma(s) \\ 0 & 3^{|t|} & \sigma(t) \\ 0 & 0 & 1 \end{pmatrix}$$

for two words $s = s_1 s_2 \cdots s_r$ and $t = t_1 t_2 \cdots t_j$, with $s_i, t_i \in \Sigma$, where $\sigma(w)$ is the 3-adic representation of the binary word w, i.e., let 1,2 correspond to a,b respectively, then

$$\sigma(w) = \sum_{k=1}^{|w|} w_k 3^{|u|-k} \quad ; w_i \in \{1, 2\}.$$

Now consider the following matrix:

$$H = \begin{pmatrix} 1 & -1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

which is self-inverse since $HH = I_3$. We can thus define a similarity transform $H\lambda'(s,t)H$ which gives us the alternate (but still injective) morphism:

$$\lambda(s,t) = H\lambda'(s,t)H = \begin{pmatrix} 3^{|s|} & 3^{|t|} - 3^{|s|} & \sigma(t) - \sigma(s) \\ 0 & 3^{|t|} & \sigma(t) \\ 0 & 0 & 1 \end{pmatrix}$$

Notice that $s = t$ iff $\lambda(s,t)_{[1,3]} = 0$ since the top right element of the matrix is the subtraction of the 3-adic representations of s, t. It is therefore easy from this point to obtain the undecidability of ZRUC for n_{PCP} integral matrices of dimension 3. However, we would like to obtain the result for a semigroup generated by just two matrices.

Given a PCP instance $P = \{(u_1, v_1), (u_2, v_2), \ldots, (u_n, v_n)\}$, we can apply a new encoding technique to embed the n matrices $\lambda(u_i, v_i)$ for $1 \leq i \leq n$ into a single matrix, B, of size $2n + 1$ and use a second matrix T which is a permutation matrix to give all possible products of words in the semigroup. Let us define:

$$B = \begin{pmatrix} 3^{|u_1|} & 3^{|v_1|} - 3^{|u_1|} & 0 & 0 & \cdots & \sigma(v_1) - \sigma(u_1) \\ 0 & 3^{|v_1|} & 0 & 0 & \cdots & \sigma(v_1) \\ 0 & 0 & 3^{|u_2|} & 3^{|v_2|} - 3^{|u_2|} & \cdots & \sigma(v_2) - \sigma(u_2) \\ 0 & 0 & 0 & 3^{|v_2|} & \cdots & \sigma(v_2) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

and define the permutation matrix T by:

$$T = \begin{pmatrix} 0 & I_2 & 0 & 0 \\ I_{2n-3} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

It is clear that $B, T \in \mathbb{Z}^{(2n+1)\times(2n+1)}$. Note that applying T to matrix B alters the ordering of the pairs of rows but preserves the word mapping itself since it is a permutation matrix. We can see that a product containing *both* B and T has a zero in the upper right corner iff there exists a solution to the PCP. This follows since the top right element will simply be the subtraction of two words 3-adic representations. However, T has a zero upper right corner on its own so the required result does not immediately follow. We can apply the encoding technique used in [18] so that the case with a power of only T matrices can be avoided. Define:

$$B' = \begin{pmatrix} 0 & 1 & x & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & B & z \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \quad T' = \begin{pmatrix} 0 & 1 & x & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & T & z \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

where $x = (1, 0, \cdots, 0), z = (0, 0, \cdots, 1)^T$, with $x \in \mathbb{Z}^{1\times k}, z \in \mathbb{Z}^{k\times 1}$ and k is the dimension of matrix B (and T). It is clear that the sub-matrices B, T are multiplied in the same way as before and unaffected by this extension. Notice the element $[2, 2]$ is 0 in B' and 1 in T'. This will be used to avoid the pathological case of a matrix product with only T matrices.

Consider an arbitrary product $Q = Q_1 Q_2 \cdots Q_m$ where $Q_i \in \{B', T'\}$ for $1 \leq i \leq m$. It is easily seen that if $m \leq 2$ then the top right element of Q equals 1 for any Q_1, Q_2. Let us thus assume $m \geq 3$ and write this multiplication as $Q = Q_1 C' Q_m$ where $C' = Q_2 Q_3 \cdots Q_{m-1}$,

$$C' = \begin{pmatrix} 0 & * & * & * \\ 0 & \lambda & 0 & * \\ 0 & 0 & C & * \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

where $*$ denotes unimportant values, $\lambda = \{0, 1\}$ and C is a submatrix equal to some product of B, T matrices.

Now we compute the top right element of Q. Let r denote the dimension of matrix C' (or Q). The first row of $Q_1 C'$ equals $(0, \lambda, C_{1,1}, C_{1,2}, \cdots, C_{1,k}, *)$ where again $*$ is unimportant. Note that this vector contains the top row of the C submatrix. We can now easily see that $Q_{[1,r]} = (Q_1 C' Q_m)_{[1,r]}$ equals $(0, \lambda, C_{1,1}, C_{1,2}, \cdots, C_{1,k}, *) \cdot (1, 1, z^T, 0)^T = \lambda + C_{1,k}$. It is clear that $\lambda = 1$ iff $C' = (T')^{m-2}$, i.e., C' is a power of only T' matrices. In this case, note that $(C'^{m-2})_{[1,k]} = 0$ since this is a power of matrix T. Thus $Q_{[1,r]} = 1 + 0 = 1$ which is non-zero as required (since this is not a solution).

In the second case, $\lambda = 0$ whenever C' contains a factor B'. Therefore $Q_{[1,r]} = 0 + C_{[1,k]} = C_{[1,k]}$ which is exactly the top right element of C as required. This equals 0 iff there exists a solution to the PCP instance.

We must increase the dimension of the matrices by 3 for this encoding therefore the problem is undecidable for dimension $2n_{\text{PCP}}+1+3 = 2n_{\text{PCP}}+4$ (currently 18).

□

4.1.3 Any Diagonal Matrix Problem

A related problem to that of Theorem 4.1 (determining whether any element of a matrix semigroup is equal to a particular scalar matrix) was given as an open problem in [14]:

Problem 4.6. *Given a finite set of matrices $\mathcal{G}$ generating a semigroup $\mathcal{S}$. Does there exist* any *matrix $D \in \mathcal{S}$ such that D is a diagonal matrix?*

We shall now show that Problem 4.6 is undecidable for *rational complex* matrix semigroups by using the FIXED ELEMENT PCP. In our proof we shall exhibit a semigroup that has no diagonal matrices if the instance of PCP has no solution and an infinite number of diagonal matrices (which are powers of a specific, known diagonal matrix) if the PCP instance does have a solution.

Theorem 4.7. *Given a finitely generated matrix semigroup $\mathcal{S} \subseteq \mathbb{C}(\mathbb{Q})^{4\times 4}$, it is algorithmically undecidable to determine whether there exists any matrix $D \in \mathcal{S}$ such that D is a diagonal matrix.*

Proof. We shall utilise the FIXED ELEMENT PCP, the matrix representation ζ of the free group of rational quaternions and some properties of linear algebra. Recall the definition of ζ:

$$\zeta(a) = \begin{pmatrix} \frac{3}{5}+\frac{4}{5}\mathbf{i} & 0 \\ 0 & \frac{3}{5}-\frac{4}{5}\mathbf{i} \end{pmatrix}, \quad \zeta(b) = \begin{pmatrix} \frac{3}{5} & \frac{4}{5} \\ -\frac{4}{5} & \frac{3}{5} \end{pmatrix},$$
$$\zeta(\overline{a}) = \begin{pmatrix} \frac{3}{5}-\frac{4}{5}\mathbf{i} & 0 \\ 0 & \frac{3}{5}+\frac{4}{5}\mathbf{i} \end{pmatrix}, \quad \zeta(\overline{b}) = \begin{pmatrix} \frac{3}{5} & -\frac{4}{5} \\ \frac{4}{5} & \frac{3}{5} \end{pmatrix}.$$

thus, $\zeta(a), \zeta(b), \zeta(a)^{-1}, \zeta(b)^{-1} \in \mathbb{C}(\mathbb{Q})^{2\times 2}$ and they form a free group as we shall prove later in Corollary 5.2 (see Section 5.2.1). Recall also that in Fixed Element PCP we have an alphabet over 5 letters, $\Gamma = \{a, b, \overline{a}, \overline{b}, \star\}$. We shall use a homomorphism, $\gamma : \Gamma^* \mapsto \mathbb{C}(\mathbb{Q})^{2\times 2}$, to encode these letters using elements of ζ. Specifically, let:

$$\begin{array}{lll} \gamma(\star) \mapsto \zeta(aaa), & \gamma(a) \mapsto \zeta(aba), & \gamma(b) \mapsto \zeta(bab) \\ & \gamma(\overline{a}) \mapsto \zeta(\overline{a}\overline{b}\overline{a}), & \gamma(\overline{b}) \mapsto \zeta(\overline{b}\overline{a}\overline{b}) \end{array} .$$

Now, given an instance of Fixed Element PCP:

$$P = \{(u_1, v_1), (u_2, v_2), \ldots, (u_n, v_n)\} \subseteq \Gamma^* \times \Gamma^*,$$

we create the new set of pairs of two-dimensional rational complex matrices:

$$R = \{(\gamma(u_1), \gamma(v_1)), (\gamma(u_2), \gamma(v_2)), \ldots, (\gamma(u_n), \gamma(v_n))\} \subseteq \mathbb{C}(\mathbb{Q})^{2\times 2} \times \mathbb{C}(\mathbb{Q})^{2\times 2}$$

Using the *mixed product* property of Kronecker products that for any four matrices $A, B, C, D \in \mathbb{C}^{j\times j}$:

$$(AB \otimes CD) = (A \otimes C)(B \otimes D),$$

given in Lemma 2.1, we create a final set of four-dimensional rational complex matrices:

$$T = \{\gamma(u_1) \otimes \gamma(v_1), \gamma(u_2) \otimes \gamma(v_2), \ldots, \gamma(u_n) \otimes \gamma(v_n)\} \subseteq \mathbb{C}(\mathbb{Q})^{4\times 4}.$$

From the definition of Fixed Element PCP, we know that a solution $s = (s_1, s_2, \ldots, s_k)$ gives the equation $u_{s_1}u_{s_2}\cdots u_{s_k} = v_{s_1}v_{s_2}\cdots v_{s_k} = \star$

for the special symbol $\star$. Now, using our above encoding, we observe that $\gamma(\star) = \zeta(a)^3$ which is clearly a diagonal matrix. Thus, given a correct solution to FIXED ELEMENT PCP, there exists a matrix $D \in \langle T \rangle$ such that:

$$D = \gamma(u_{s_1}u_{s_2}\cdots u_{s_k}) \otimes \gamma(v_{s_1}v_{s_2}\cdots v_{s_k}) = \gamma(\star) \otimes \gamma(\star) = \zeta(a)^3 \otimes \zeta(a)^3,$$

which is diagonal (since the Kronecker product of two diagonal matrices is diagonal). It can be seen that any word which is not a solution will contain at least one matrix $\zeta(b)$ or $\zeta(\bar{b})$ which can be clearly observed by considering the definition of the morphism γ. Since these two matrices are not diagonal, the Kronecker product will not be diagonal either. □

This shows that Problem 4.6 is undecidable for four-dimensional rational complex matrix semigroups. We can convert all the matrices to rational matrices by using a simple well-known encoding from complex numbers to two-dimensional real matrices by defining a function $\phi : \mathbb{C}(\mathbb{Q}) \mapsto \mathbb{Q}^{2\times 2}$ by:

$$\phi(z) = \begin{pmatrix} \Re(z) & -\Im(z) \\ \Im(z) & \Re(z) \end{pmatrix}; \quad z \in \mathbb{C}(\mathbb{Q}),$$

and clearly we can apply ϕ to each element of the four-dimensional rational complex matrices constructed in Theorem 4.7 to map into eight-dimensional *rational matrices*. However a correct solution will now only give a *block diagonal* matrix (of 2 × 2 blocks). Thus the problem remains open in any dimension for rational and thus integral matrices. We shall therefore state the open problem which is a subcase of that found in [14]:

Open Problem 4.8. ANY DIAGONAL MATRIX - *Given a finite set of* integral *matrices $\mathscr{G}$ generating a semigroup $\mathscr{S}$. Does there exist any matrix $D \in \mathscr{S}$ such that D is a diagonal matrix? I.e. is Problem 4.6 decidable for integral matrices?*

4.2 Vector Reachability Problems

In this section we shall evaluate the decidability of reachability problems on planar points mapped by a semigroup of two-dimensional affine transforms.

We can represent a point on the plane p_0 via a two-dimensional rational vector $(x, y) \in \mathbb{Q}^2$. An affine transformation of point (x, y) is a function $\psi : \mathbb{Q}^2 \mapsto \mathbb{Q}^2$ such that $\psi((x, y)) = (a_1 x + a_2 y + a_3, b_1 x + b_2 y + b_3)$ and $a_i, b_i \in \mathbb{Q}$ for $1 \leq i \leq 3$.

Theorem 4.9. *Given a semigroup of two-dimensional affine transformations $\mathscr{S}$ generated by a finite set of transformations $\mathscr{G}$, determining if a particular point p_0 can be mapped back to itself via some transformation in $\mathscr{S}$ is undecidable.*

Proof. Let $\Sigma = \{a, b\}$ be a binary alphabet and define the monomorphism $\lambda : \Sigma^* \mapsto \mathbb{Q}^{2\times 2}$ by:

$$\lambda(a) = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \quad \lambda(b) = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}.$$

as stated in Section 2.2.1, this pairs of matrices generates a free semigroup. Let us also define a second monomorphism $\gamma : \Sigma^* \mapsto \mathbb{Q}^{2\times 2}$ using the inverse matrices of λ:

$$\gamma(a) = \begin{pmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix}, \quad \gamma(b) = \begin{pmatrix} 1 & -1 \\ 0 & \frac{1}{2} \end{pmatrix}.$$

Assume that we have an instance of Post's correspondence problem (PCP), $h, g : \Gamma^* \mapsto \Sigma^*$. For each element $c \in \Gamma$, we shall create the pair of matrices $\lambda(h(c))$ and $\gamma(g(c))$. Note that if there exists a solution to PCP, then there exists a word $w \in \Gamma^+$ such that $h(w) = g(w)$ and thus $h(w) \cdot (g(w))^{-1} = \varepsilon$.

Thus to encode this problem, we shall begin with the empty word ε and to add the next PCP letter, $c \in \Gamma$, we will add $h(c)$ to the left and $(g(c))^{-1}$

to the right, i.e., $\varepsilon \mapsto h(c)\varepsilon(g(c))^{-1}$. We continue this iteratively for a word $w \in \Gamma^+$ and clearly we return to the empty word ε iff $h(w) = g(w)$.

In terms of matrices, we associate a matrix $C_w \in \mathbb{Q}^{2\times 2}$ where $w \in \Gamma^*$ with $h(w)(g(w))^{-1}$ and clearly C_w is of the form:

$$C_w = \begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix}; \quad x, y \in \mathbb{Q}$$

To extend this configuration by the next letter $c \in \Gamma$, we multiply C_w to the left by $\lambda(h(c))$ and to the right by $\gamma(g(c))$ giving:

$$C_{wc} = \lambda(h(c))C_w\gamma(g(c))$$

This will give us a matrix product of the form:

$$\begin{pmatrix} 1 & x' \\ 0 & y' \end{pmatrix} = \begin{pmatrix} 1 & p_1 \\ 0 & p_2 \end{pmatrix} \cdot \begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} \cdot \begin{pmatrix} 1 & q_1 \\ 0 & q_2 \end{pmatrix}$$

Performing the matrix multiplication, we find that:

$$\begin{pmatrix} 1 & x' \\ 0 & y' \end{pmatrix} = \begin{pmatrix} 1 & q_2x + q_2p_1y + q_1 \\ 0 & q_2p_2y \end{pmatrix}$$

But in fact we see that this is a two-dimensional affine transformation of the point (x, y). It can be written as:

$$\begin{cases} x' = & q_2x + q_2p_1y + q_1 \\ y' = & p_2q_2y \end{cases}$$

Since the starting configuration is ε, we start with the matrix $C_\varepsilon = I_2$, the 2×2 identity matrix which corresponds to the point $x = 0, y = 1$ and a correct solution to PCP maps I_2 to I_2 which also corresponds to the point $(0, 1)$. Therefore, the problem of mapping point $(0, 1)$ back to itself by using a set of two-dimensional affine transformations is undecidable as required. Note that we require n_{PCP} (currently 7) transforms in the generator $\mathcal{G}$. □

We recall the general definition of a vector reachability problem for a matrix semigroup from Section 2.3:

VECTOR REACHABILITY PROBLEM : Given a semigroup of matrices $\mathscr{S}$, generated by a finite set $\mathscr{G} \subset \mathbb{F}^{n \times n}$ and two column vectors $x, y \in \mathbb{F}^n$. Does there exist some matrix $M \in \mathscr{S}$ such that $Mx = y$?

Utilising the undecidability results on two-dimensional affine transformations from Theorem 4.9 allows us to easily gain an undecidability result on three-dimensional integral matrices:

Theorem 4.10. *The vector reachability problem is undecidable for three-dimensional rational matrix semigroups.*

Proof. We proved in Theorem 4.9 that there is a set of two-dimensional affine transformations generating a semigroup for which it is undecidable if there exists an element of the semigroup mapping point $(0,1)$ to $(0,1)$. We shall convert each two-dimensional affine transformation into an equivalent three-dimensional linear transformation as follows:

$$\begin{pmatrix} x' = & q_2x + q_2p_1y + q_1 \\ y' = & p_2q_2y \end{pmatrix} \Rightarrow \begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = \begin{pmatrix} q_2 & q_2p_1 & q_1 \\ 0 & p_2q_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$$

Thus for a set of n affine functions, this conversion gives us a set of matrices $\{M_1, M_2, \ldots, M_n\} \subset \mathbb{Q}^{3\times 3}$.

From the proof of Theorem 4.9 follows that the problem to decide whether there exists a product $M = M_{i_1}M_{i_2}\cdots M_{i_k}$ where $1 \leq i_j \leq n$ for $1 \leq j \leq k$ such that $Mv = v$ where $v = (0,1,1)^T$ is undecidable. Theorem 4.9 was shown undecidable for semigroups generated by n_{PCP} transforms thus the vector reachability problem is undecidable for three-dimensional rational matrix semigroups generated by n_{PCP} matrices. □

We shall now show that the vector reachability problem is also undecidable for semigroups that are generated by just 2 rational matrices of dimension $2(n_{\mathrm{PCP}} - 2) + 1$.

Theorem 4.11. *The vector reachability problem is undecidable for semigroups generated by two rational matrices of dimension* $2(n_{PCP} - 2) + 1$ *(currently* 11*).*

Proof. We shall perform three steps and reduce the dimensions of the two matrices in each of these steps. Given a set of matrices $\{M_1, M_2, \ldots, M_n\}$ where $M_i \in \mathbb{Q}^{m \times m}$. Let us define two block diagonal matrices A_1 and T_1 by:

$$A_1 = M_1 \oplus \cdots \oplus M_n = \begin{pmatrix} M_1 & 0 & \cdots & 0 \\ 0 & M_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M_n \end{pmatrix}, \quad T_1 = \begin{pmatrix} 0 & I_m \\ I_{n(m-1)} & 0 \end{pmatrix}$$

where 0 denotes a submatrix with zero elements. The dimension of both of A_1 and T_1 is nm. Furthermore, it can be seen that for any $1 \leq j \leq n$ then $T_1^{n-j+1} A_1 T_1^{j-1}$ permutes the blocks of A_1 in a cyclic way, so that the direct sum of $T_1^{n-j+1} A_1 T_1^{j-1}$ is $M_j \oplus M_{j+1} \oplus \cdots \oplus M_n \oplus M_1 \oplus \cdots \oplus M_{j-1}$. We can also note that $A_1 \sim T_1^{n-j+1} A_1 T_1^{j-1}$ (therefore this is a similarity transform) since $T_1^{n-j+1} \cdot T_1^{j-1} = T_1^n = I_n$. It is therefore apparent that any product of the matrices can thus occur and in fact can appear in the first block of the nm matrix product.

Let us define a vector $x = (v, 0, \cdots, 0)^T \in \mathbb{Q}^{nm}$ where $v = (0, 1, 1)$. It is easily observed that there exists a matrix product $M = M_{i_1} M_{i_2} \cdots M_{i_t}$ satisfying $Mv = v$ as in Theorem 4.10 iff there exists a matrix $R \in \langle A_1, T_1 \rangle$ satisfying $Rx = x$ *unless* $R = T_1^n = I$ which is a pathological case we must avoid. This can easily be achieved by increasing all dimensions by one but we shall not detail this since we are going to reduce the dimensions two times further. From Theorem 4.10 then, this establishes the undecidability of the vector reachability problem for 2 rational matrices of dimension $3n_{\text{PCP}} + 1$ (currently 22).

The first step is now complete, however we can reduce the dimensions of the two matrices A_1, T_1. We observe that $(M_i)_{[3,3]} = 1$ and M_i is upper triangular for all $1 \leq i \leq n$. Let us now construct two new matrices $A_2, T_2 \in \mathbb{Q}^{(2n+2)\times(2n+2)}$ directly using the elements from the matrices in Theorem 4.10:

$$A_2 = \begin{pmatrix} (q_2)_1 & (q_2p_1)_1 & 0 & 0 & \cdots & (q_1)_1 \\ 0 & (p_2q_2)_1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & (q_2)_2 & (q_2p_1)_2 & \cdot & (q_1)_2 \\ 0 & 0 & 0 & (p_2q_2)_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, T_2 = \begin{pmatrix} 0 & I_2 & 0 \\ I_{2n-2} & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where 0 denotes either the number zero or a submatrix with zero elements, I_k is the k dimensional identity matrix and $(x)_i$ denotes the element x from matrix M_i used in Theorem 4.10. Straight-forward calculation shows that $T_2^{n-j+1} A_2 T_2^{j-1}$ permutes the pairs of *rows* in A_2 and using a similar argument as before, we thus can form any product of matrices in the first two rows of this matrix. We define a $2n+2$-dimensional vector $w = (0, 1, 0, \cdots, 0, 1)^T$.

Finally we see that there exists a solution $Mv = v$ to PCP as in Theorem 4.10 iff there exists a matrix $R \in \langle A_2, T_2 \rangle$ satisfying $Rw = w$ *unless* $R = T_2^k = I$ for some $k \in \mathbb{N}$ which again is a pathological case we can avoid by increasing the dimensions by one. This completes the second step and gives the undecidability of the vector reachability problem for semigroups generated by two rational matrices of dimension $2n_{\text{PCP}} + 2$ (currently 16).

We now perform the final reduction to create two rational matrices A_3, T_3. We shall use Claus instances of PCP (see Section 3.2.1) which allow our previous encoding to use smaller dimensions. Recall that in the Claus construction of PCP we fix an initial and final pair $(u_1, v_1), (u_n, v_n)$ and must find a sequence $s = (s_1, s_2, \ldots, s_k)$ such that:

$$u_1 u_{s_1} u_{s_2} \cdots u_{s_k} u_n = v_1 v_{s_1} v_{s_2} \cdots v_{s_k} v_n,$$

where $2 \leq s_i \leq (n-1)$.

In terms of matrices, this means if $\mathscr{G} = \{M_1, M_2, \ldots, M_n\}$ encode each pair of words, then we may fix the first and last matrices M_1, M_n and then take the semigroup $\mathscr{S}$ generated by $\mathscr{G} \backslash \{M_1, M_n\}$. This set is of size $n_{\text{CLAUS}} - 2$ and using the construction for the second reduction above, this reduces the matrix dimension in the generator to $2(n_{\text{CLAUS}} - 2) + 1$ (we ignore the pathological case of T^k for the moment).

Since M_1 is the first matrix of the product and M_n is the last, given a product of the form:

$$M_1 M_{s_1} M_{s_2} \cdots M_{s_k} M_n v = v$$

as in Theorem 4.10, we can instead write this product as:

$$M_{s_1} M_{s_2} \cdots M_{s_k} x = y$$

where $x = M_n v$ and $y = M_1^{-1} v$ (clearly M_1 is invertible by the construction). Applying this idea to the second step above also avoids the pathological case of a matrix in the semigroup containing $T^k = I$ giving an incorrect result, since now $x \neq y$ as can be seen by examining the Claus construction. This completes the proof giving the undecidability of the Vector Reachability Problem for semigroups generated by two rational matrices of dimension $2(n_{\text{CLAUS}} - 2) + 1$ (currently 11). □

We shall now show that the related Vector Ambiguity Problem is undecidable. We recall the previous definition:

Problem 2.6. Vector Ambiguity Problem - Given a semigroup $\mathscr{S} \subseteq \mathbb{F}^{n \times n}$ and an initial vector $u \in \mathbb{F}^{n \times n}$. Let V be a set of vectors such that $V = \{v : v = Mu; M \in S\}$. Does $\mathscr{S}$ and u generate an ambiguous set of vectors? In other words the question is whether for every vector of set V there is a unique matrix $M \in \mathscr{S}$ such that $Mu = v$?

Theorem 4.12. *The* VECTOR AMBIGUITY PROBLEM *is undecidable for matrix semigroups over integers in dimension* 4 *and over rational matrices in dimension* 3.

Proof. It was proven in [12] that distinguishing between counter machines that have a periodic configuration from those that do not, is an algorithmically undecidable problem. We gave a simpler proof which used a fewer number of rules in Theorem 3.12 from Section 3.3.3.

The proof of Theorem 3.12 was achieved via a reduction of the classical counter halting problem for counter machines. In the proof, we started with a machine M and described how to construct a counter machine M' that has no halting configuration and that has a periodic configuration if and only if M halts on its initial configuration in a similar way to that of [12].

Let us use a construction proposed in Section 3.3.2, which simulates any two-counter machine by a set of pairs of words. Note that our method does not require defining a halting state of the machine and in this case we can only predefine an initial configuration of a counter machine M.

Assume that a set of pairs of word that are used for a counter machine simulation is $P = \{(u_i, v_i) | 1 \leq i \leq n\}$. Let us construct a set of pairs of 2×2 matrices using the homomorphism λ:

$$\{(\lambda(\overline{u_1}), \lambda(v_1)), \ldots, (\lambda(\overline{u_n}), \lambda(v_n))\}.$$

Instead of equation $u = v$ we consider a concatenation of two words $\overline{u} \cdot v$ which equals ε only in the case where $u = v$. We associate 2×2 matrix C with a word w of the form $\overline{u} \cdot v$. Initially C is a matrix that corresponds to the initial configuration of the machine which is stored in the first pair (u_1, v_1), so $C = \overline{u_1} \cdot v_1$.

The extension of a word w by a new pair of words (u_r, v_r) (i.e., that gives us $w' = \overline{u_r} \cdot w \cdot v_r$) corresponds to the following matrix multiplication

$$C_{w'} = \lambda(\overline{u_r}) \times C_w \times \lambda(v_r) \qquad (1)$$

Let us rewrite operation (1) in more detail.

$$\begin{pmatrix} c_{w'}^{11} & c_{w'}^{12} \\ c_{w'}^{21} & c_{w'}^{22} \end{pmatrix} = \begin{pmatrix} u^{11} & u^{12} \\ u^{21} & u^{22} \end{pmatrix} \cdot \begin{pmatrix} c_{w}^{11} & c_{w}^{12} \\ c_{w}^{21} & c_{w}^{22} \end{pmatrix} \cdot \begin{pmatrix} v^{11} & v^{12} \\ v^{21} & v^{22} \end{pmatrix} \qquad (2)$$

In this case, pairwise multiplication will correspond to an update of the current state according to the operation of the two-counter machine M.

Let us consider the dynamics of changes for the matrix C. It is easy to see that in the case of an incorrectly applied command for a machine M, the pairwise concatenation (multiplication) will lead to an increase of the length for a word w and will never end up in a repeated word after that. Therefore after an incorrect application of a command of M, a matrix C will never have the same value again. The correct application of pairwise concatenation of words or multiplication of matrices covers the set of correct configurations of a two-counter machine M. In the case of a periodic two-counter machine, the finiteness of the configuration space will lead to the finiteness of the set X of possible C matrices that can be generated during the correct application of rules for M, since every matrix $C \in X$ corresponds to a unique reachable configuration of M. Thus the set of matrices that can be generated by pairwise multiplication may contain repetitions if and only if a two-counter machine has periodic behaviour.

In order to finish the proof of undecidability for the case of an integer matrix semigroup, we represent matrix C as a vector $x = ({c_w}^{11}, {c_w}^{12}, {c_w}^{21}, {c_w}^{22})^T$ increasing the dimension to 4 and rewriting pairwise multiplication as a four-dimensional linear transformation of a vector x.

$$\begin{pmatrix} c_{w'}^{11} \\ c_{w'}^{12} \\ c_{w'}^{21} \\ c_{w'}^{22} \end{pmatrix} = \begin{pmatrix} u^{11} & u^{12} \\ u^{21} & u^{22} \end{pmatrix} \otimes \begin{pmatrix} v^{11} & v^{12} \\ v^{21} & v^{22} \end{pmatrix} \cdot \begin{pmatrix} c_{w}^{11} \\ c_{w}^{12} \\ c_{w}^{21} \\ c_{w}^{22} \end{pmatrix}$$

The same method can be used to prove the undecidability of the vector freeness problem in dimension three for rational matrices by using another homomorphism τ based on a free semigroup:

$$\tau(a) = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \quad \tau(b) = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix},$$

$$\tau(\overline{a}) = \begin{pmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix}, \quad \tau(\overline{b}) = \begin{pmatrix} 1 & -1 \\ 0 & \frac{1}{2} \end{pmatrix}.$$

The rest of the proof repeats the above arguments along the lines of the proof of undecidability for the vector reachability problem for rational matrices in dimension 3 shown in [8]. □

Note that from the above result it follows that it is undecidable whether there exists a periodic trace of configurations in a one-state blind nondeterministic four-counter machine with counter updates in terms of linear transformations.

We can also see that it follows from the above proof that any periodic orbit of the given two-counter Minsky machine will correspond to a unique solution of the INDEX CODING PCP.

4.3 Matrix Embeddings of Computational Models

We shall now show how a Turing machine or two-counter Minsky machine can be encoded within a finitely generated integral matrix semigroup. We use the simulation of a computational device via a set of pairs of words as in Section 3.3.2.

We gave a construction in Proposition 3.11 showing that a Turing machine and a two-counter Minsky machine can be stored within an instance of Post's correspondence problem (PCP) such that the instance has a solution if and only if the computational model halts and accepts. In Theorem 3.6 we showed how to convert an instance of PCP into an instance of INDEX CODING PCP which is Problem 3.5.

Let us therefore consider an instance of INDEX CODING PCP corresponding to the simulation of a Turing machine or a two-counter Minsky machine given by:

$$P = \{(u_i, v_i) : 1 \leq i \leq n\} \subset \Gamma^* \times \Gamma^*,$$

where $\Gamma = \{a, b, \bar{a}, \bar{b}\}$ is a binary alphabet with inverses. We shall use the homomorphism $\lambda : \Gamma^* \mapsto \mathbb{Z}^{2\times 2}$ defined by:

$$\lambda(a) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \lambda(b) = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \lambda(\bar{a}) = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}, \lambda(\bar{b}) = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix},$$

which, as stated in Section 2.2.2, is an injective homomorphism. Let us now create a set of matrices $\mathscr{G}$ defined by:

$$\mathscr{G} = \left\{ \begin{pmatrix} \lambda(u_i) & \mathbf{0}_2 \\ \mathbf{0}_2 & \lambda(v_i) \end{pmatrix} : 1 \leq i \leq n \right\} \subset \mathbb{Z}^{4\times 4},$$

where $\mathbf{0}_2$ is the 2×2 *zero matrix*. This is now exactly an instance of INDEX CODING PCP as defined in Problem 3.5 which directly simulates a Turing Machine or two-counter Minsky machine. We shall use this construction in the next theorem.

Theorem 4.13. *There is a fixed matrix semigroup $\mathscr{S}$ with an undecidable membership problem. There is a fixed semigroup T with undecidable vector reachability problem.*

Proof. It is well known that there exists universal Turing machines which can simulate another Turing machine input in a pre-defined way which halts iff the machine it is simulating halts. Thus, we can define semigroup $\mathscr{S}$ to be a *fixed* encoding of a universal Turing machine generated by a finite set of integral matrices. From the proof of Theorem 3.6, it can be seen that the first pair (u_1, v_1) in such an instance is used only once.

Since u_1 stores the input word to the problem, we may remove the corresponding matrix $X = \lambda(u_1) \oplus \lambda(v_1)$ from the generator set $\mathscr{G}$. Now, a correct solution to INDEX CODING PCP corresponds to the identity matrix and uses X exactly once, thus we see that $X^{-1} \in \mathscr{S}$ if and only if there exists a solution to INDEX CODING PCP.

Finally then, we see that the semigroup generated by $\mathscr{G}' = \mathscr{G} \setminus \{X\}$ stores a universal Turing machine and the input to this Turing machine is contained within matrix $X = \lambda(u_1) \oplus \lambda(v_1)$. Thus, we have a fixed matrix semigroup $\mathscr{S}$ generated by $\mathscr{G}'$, and determining if $X^{-1} \in \mathscr{S}$ for varying X is algorithmically undecidable as required.

The existence of a semigroup with an undecidable vector reachability problem follows from the same arguments and the construction of an undecidable vector reachability problem for 3×3 matrix semigroups over rationals and 4×4 matrix semigroup over integers (due to the invertibility of the matrices). For more details see Theorem 4.10 and [47]. □

The next problem that we consider here is the problem of whether an element of a matrix semigroup has an infinite number of factorisations over elements of the generator. This question is trivially undecidable in the case of singular matrices since it can be reduced to the mortality problem (whether a zero matrix belongs to a semigroup). Here we show that this problem is also undecidable for invertible matrix semigroups.

Problem 4.14. RECURRENT MATRIX PROBLEM - *Given a matrix semigroup $\mathscr{S}$ generated by a finite set of matrices $\mathscr{G}$ and a matrix M. Does M have an infinite number of factorisations over elements of $\mathscr{G}$?*

Theorem 4.15. *The* RECURRENT MATRIX PROBLEM *is undecidable for integral 4×4 matrix semigroups.*

Proof. The proof is achieved via a simulation of a nondeterministic two-counter machine, where the problem of deciding if M' has an infinite number of trajectories leading to a final state s_{final} with zero counters is undecidable, see Theorem 3.13.

Note that in Section 3.3.2 we showed how to simulate a Turing machine via a PCP instance but as mentioned in the comments, the proof is essentially the same for a two-counter machine.

Given an instance of PCP, P', which simulates the two-counter machine M' above, we create an instance of INDEX CODING PCP, P as explained in Theorem 3.6 and embed the instance into a four dimensional integral matrix generator set $\mathcal{G}$ as is done in Theorem 4.1. Since a particular matrix, N, must appear exactly once in a product equalling the identity matrix for a correct solution, we shall consider the semigroup generated by $\mathcal{G} \setminus \{N\}$ (N is invertible by the construction).

If $N^{-1} \in \langle \mathcal{G} \setminus \{N\} \rangle$, then it corresponds to a correct computational path of the counter machine M'. Let us assume that we have an algorithm to check if matrix N^{-1} has infinitely many factorisations. This means that M' has an infinite number of trajectories leading to a configuration s_{final} with zero counters. Since the last problem is undecidable the problem whether M' has an infinite number of factorisations is undecidable. □

4.4 Semigroup Intersection Problems

In this section we shall study the decidability of the intersection of a pair of matrix semigroups. Such problems were studied by A. Markov [42] and more recently by V. Halava and T. Harju [26]. We shall use a different encoding to that of V. Halava and T. Harju to obtain a similar result which more closely mirrors that of A. Markov but in reduced dimensions.

Our primary aim shall be to determine if the intersection of two semigroups generated by a finite set of matrices is empty or not. In other words, is there some matrix in one semigroup that is also in the other semigroup? The emptiness problem for matrix semigroup intersection was shown to be undecidable by A. Markov, although we have written the theorem in a different but equivalent form, [42]:

Theorem 4.16. *[42] Given two finite sets $X = \{X_1, X_2, \ldots, X_n\}$ and $Y = \{Y_1, Y_2\}$ of 4×4 non-negative integer uni-modular square matrices. It is undecidable if $|\langle X\rangle \cap \langle Y\rangle| = 0$. We may assume that all matrices in X, Y except for X_1 are fixed* [1].

Note that Markov's result was recently improved by the following theorem:

Theorem 4.17. *[26] Given two sets $X = \{X_1, X_2, \ldots, X_n\}$ and $Y = \{Y_1, Y_2\}$ of 3×3 integer non-singular matrices. It is algorithmically undecidable if $|\langle X\rangle \cap \langle Y\rangle| = 0$.*

Note that the authors in [26] used semigroups over $\mathbb{Z}^{3\times 3}$ rather than $\mathbb{N}^{4\times 4}$ as was used by A. Markov. We use a new encoding to show that it is in fact possible to obtain a similar theorem over $\mathbb{N}^{3\times 3}$ even with upper triangular matrices. We shall also show that we may prove a similar result on unimodular matrices as Markov did, but we require matrices over $\mathbb{Q}^{3\times 3}$ instead. It was shown that an embedding of two words is not possible into 2×2 complex matrices using matrix multiplication as the binary operator in [17].

Theorem 4.18. *Given two sets $X = \{X_1, X_2, \ldots, X_n\}$ and $Y = \{Y_1, Y_2\}$ of 3×3 non-negative upper-triangular integral non-singular matrices. It is undecidable if $|\langle X\rangle \cap \langle Y\rangle| = 0$.*

Proof. Let $\Gamma = \{a, b\}$ to be a binary alphabet. Let:

$$P = \{(u_j, v_j) | 1 \leq j \leq n\} \subset \Gamma^* \times \Gamma^*$$

be an instance of Post's correspondence problem (PCP). Define two morphisms $\sigma, \tau : \Gamma^* \mapsto \mathbb{N}^{2\times 2}$ by:

$$\sigma(a) = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \sigma(b) = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}, \tau(a) = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \tau(b) = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}.$$

[1] The statement that all matrices except X_1 can be fixed is not difficult, see [26].

We stated in Section 2.2.1 that σ, τ are injective homomorphisms. Note that for all pairs of words $w_1, w_2 \in \Gamma^*, \sigma(w_1)_{[2,2]} = \tau(w_2)_{[1,1]} = 1$ thus the pair of 2×2 matrices, $\sigma(w_1), \tau(w_2)$, can be embedded into $\mathbb{N}^{3\times 3}$ by using the direct sum $\sigma(w_1) \oplus \tau(w_2)$ and joining the common element 1. Let us define the morphism $\lambda : \Gamma^* \times \Gamma^* \mapsto \mathbb{N}^{3\times 3}$ by:

$$\lambda(w_1, w_2) = \sigma(w_1) \oplus \tau(w_2) = \begin{pmatrix} 2^{|w_1|} & x & 0 \\ 0 & 1 & y \\ 0 & 0 & 2^{|w_2|} \end{pmatrix},$$

where $w_1, w_2 \in \Gamma^*$ and $x, y \in \mathbb{N}$. This is still a monomorphism. Define $X_i = \lambda(u_i, v_i)$ for each $1 \leq i \leq n$, $Y_1 = \lambda(a, a)$ and $Y_2 = \lambda(b, b)$. If there exists a solution to the PCP $(i_1, i_2, \ldots, i_k)$ then $X_{i_1} X_{i_2} \cdots X_{i_k} \in \langle X \rangle$ is of the form $\lambda(u_{i_1} u_{i_2} \cdots u_{i_k}, v_{i_1} v_{i_2} \cdots v_{i_k}) = \lambda(w, w) \in \langle Y \rangle$ for some $w \in \Gamma^*$ thus their intersection is non-empty. Clearly $\langle Y \rangle$ contains only matrices embedding the same two words which corresponds to a correct solution to the PCP. Thus the intersection is not empty iff there exists a solution to the PCP. Since PCP is undecidable with 7 pairs of words[43], X is generated by 7 matrices and Y is generated by 2 matrices. □

Corollary 4.19. *Given two sets $X = \{X_1, X_2, \ldots, X_n\}$ and $Y = \{Y_1, Y_2\}$ of 3×3 non-negative upper-triangular rational unimodular matrices. It is undecidable if $|\langle X \rangle \cap \langle Y \rangle| = 0$.*

Proof. Since each matrix in X, Y is invertible we can divide through by the cubic root of the determinant $(\sqrt[3]{\det(\lambda(w_1, w_2))} = \sqrt[3]{2^{|w_1|+|w_2|}})$ to make each unimodular (but mapping instead into $\mathbb{R}^{3\times 3}$) and obtain the same result since the determinant is multiplicative, however the resulting matrices are now real. Using a similar idea as in [26] suggested by M. Soittola, we can replace the 2 on the main diagonal in the definitions of σ, τ and λ with 8. This will give 8-adic numbers on the off diagonal elements rather than 2-adic numbers and they retain their freeness. The determinant of λ will now be a power of 8, thus the cubic root of the determinant will be a power of 2. Therefore we can map into $\mathbb{Q}^{3\times 3}$ as required. □

Using the idea of PCP and "Claus instances" as in [26], we can reduce the required number of matrices after slight modification of the problem. Given two matrices A, B and two semigroups $X = \langle\{X_1, X_2, \ldots, X_5\}\rangle$, $Y = \langle\{Y_1, Y_2\}\rangle$ it is undecidable if there exists $M \in X$ such that $AMB \in Y$. See [26] for a more detailed discussion.

Chapter 5

Quaternion Matrix Semigroup Problems

5.1 Hypercomplex Numbers Introduction

Quaternions have long been used in many fields including computer graphics, robotics, global navigation and quantum physics as a useful mathematical tool for formulating the composition of arbitrary spatial rotations and establishing the correctness of algorithms founded upon such compositions.

Many natural questions about quaternions are quite difficult and correspond to fundamental theoretical problems in mathematics, physics and computational theory. Unit quaternions actually form a *double cover* of the rotation group SO_3, meaning each element of SO_3 corresponds to two unit quaternions. This makes them expedient for studying rotation and angular momentum and they are particularly useful in quantum mechanics. The group of unit quaternions form the group SU_2 which is the special unitary group. The large number of applications has renewed interest in quaternions and quaternion matrices ([2], [21], [50], [54], [55]).

Quaternions do not commute and this leads to many problems with their analysis. In particular, defining the determinant and finding the eigenvalues and the inverse of a quaternion matrix are unexpectedly difficult problems [55]. In this chapter, we shall study decision questions about semigroups of quaternions, quaternion matrices and rotations, such as several reachability questions, membership problems, freeness problems, etc.

It appears that there has not so far been much research on *computational problems* for quaternions and quaternion matrices. This is partially because the results for matrices over $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ are not easily transferable to the case of quaternions. We shall investigate most of the open problems for 2×2 matrix semigroups showing undecidability of them in the case of matrices over quaternions. After the quaternions, the hypercomplex numbers lose the associativity property and thus no longer form a semigroup. Due to this fact it could be concluded that research on quaternion matrices gives a more complete picture of decision problems for matrix semigroups. We shall also study several problems for the case of Lipschitz integers and state several new open problems which arose from our research.

We shall also establish connections between classical matrix semigroup problems and reachability problems for semigroups of rotations. In fact, using unit quaternions for encoding computational problems gives us an opportunity to formulate and prove several interesting results in terms of 3 and 4-dimensional rotations defined by quaternions. In particular, we will show that the point-to-point rotation problem for the 3-sphere is undecidable. The same problem for the 2-sphere is open and can be formulated as a special case of the scalar reachability problem for matrix semigroups that we show is undecidable in general. As an additional benefit, the results on rotation semigroups give immediate corollaries for a class of orthogonal matrix semigroups.

These type of geometric interpretations of quaternions and quaternion matrices will be studied later in Chapter 7. We show that studying such matrix problems is of interest since they do arise in many situations in the real world.

5.2 Quaternion Word Morphisms

Let $\Sigma = \{a, b\}$ be a binary alphabet and $\overline{\Sigma} = \{\overline{a}, \overline{b}\}$ be the inverse alphabet, thus $\overline{a} = a^{-1}$ and $\overline{b} = b^{-1}$. Let $\overline{u} = (1,0,0)$ and $\overline{v} = (0,1,0)$ with $\overline{u}, \overline{v} \in \mathbb{Q}^3$. Define $\varphi : (\Sigma \cup \overline{\Sigma})^* \times \mathbb{Q} \mapsto \mathbb{H}(\mathbb{Q})$ to be the following homomorphism:

$$\begin{aligned}
\varphi(a, \theta) &= (\cos(\tfrac{\theta}{2}), \overline{u}\sin(\tfrac{\theta}{2})) \cdot \mu,\\
\varphi(b, \theta) &= (\cos(\tfrac{\theta}{2}), \overline{v}\sin(\tfrac{\theta}{2})) \cdot \mu,\\
\varphi(\overline{a}, \theta) &= (\cos(\tfrac{\theta}{2}), -\overline{u}\sin(\tfrac{\theta}{2})) \cdot \mu,\\
\varphi(\overline{b}, \theta) &= (\cos(\tfrac{\theta}{2}), -\overline{v}\sin(\tfrac{\theta}{2})) \cdot \mu,
\end{aligned}$$

where $\theta \in \mathbb{Q} \in [0, 2\pi)$, i.e., $\varphi(a, \theta)$ is a quaternion corresponding to a rotation of angle θ about the $\overline{u}$ axis and $\varphi(b, \theta)$ corresponds to a rotation of angle θ about the $\overline{v}$ axis, with the inverse elements being the opposite rotations. $\varphi(\varepsilon, \theta) = \vartheta_I$ is the multiplicative identity element of the division ring of rational quaternions. Note that $\overline{u} \cdot \overline{v} = 0$ and $||\overline{u}|| = ||\overline{v}|| = 1$, thus these two vectors are orthonormal.

Let us define a specific instance of this morphism. Let $\alpha = 2\arccos(\frac{3}{5}) \in \mathbb{R}$. Now we define $\gamma : (\Sigma \cup \overline{\Sigma})^* \mapsto \mathbb{H}(\mathbb{Q})$ where $\gamma(a) = \varphi(a, \alpha)$, $\gamma(\overline{a}) = \varphi(\overline{a}, \alpha)$, $\gamma(b) = \varphi(b, \alpha)$ and $\gamma(\overline{b}) = \varphi(\overline{b}, \alpha)$. This gives the homomorphism:

$$\begin{aligned}
\gamma(a) = &\ (\cos(\arccos(\tfrac{3}{5})), \vec{u}\sin(\arccos(\tfrac{3}{5}))) \cdot \mu &= (\tfrac{3}{5}, \ \tfrac{2}{5}, 0, 0) \cdot \mu\\
\gamma(\overline{a}) = &\ \gamma(a)^{-1} = \gamma(a)^* &= (\tfrac{3}{5}, -\tfrac{2}{5}, 0, 0) \cdot \mu\\
\gamma(b) = &\ (\cos(\arccos(\tfrac{3}{5})), \vec{v}\sin(\arccos(\tfrac{3}{5}))) \cdot \mu &= (\tfrac{3}{5}, 0, \ \tfrac{2}{5}, 0) \cdot \mu\\
\gamma(\overline{b}) = &\ \gamma(b)^{-1} = \gamma(b)^* &= (\tfrac{3}{5}, 0, -\tfrac{2}{5}, 0) \cdot \mu
\end{aligned}$$

which follows from the identity $\cos^2\theta + \sin^2\theta = 1$ since $\sqrt{1 - (\frac{3}{5})^2} = \frac{2}{5}$. It can be seen that the rational quaternions in the image of γ are unit, i.e., $\forall w \in \Sigma^*, ||\gamma(w)|| = 1$ since quaternion length is multiplicative ($||q_1 q_2|| = ||q_1|| \cdot ||q_2||$, which we prove later in Lemma 5.12) and $\gamma(a), \gamma(b)$ have unit length.

Lemma 5.1. *The mapping $\gamma : \Sigma^* \mapsto \mathbb{H}(\mathbb{Q})$ is a monomorphism.*

Proof. It was proven in [51] that if $\cos(\theta) \in \mathbb{Q}$ then the subgroup of $SO_3(\mathbb{R})$ generated by rotations of angle θ about two perpendicular axes is free iff $\cos(\theta) \neq 0, \pm\frac{1}{2}, \pm 1$. We note that in the definition of γ we use a rotation about two orthonormal axes $\overline{u}, \overline{v}$. We use a rotation of $\alpha = 2\arccos\frac{3}{5}$. From basic trigonometry, $\cos(2\arccos(\frac{3}{5})) = -2\sin^2(\arccos(\frac{3}{5})) = 1-2(\frac{4}{5})^2 = -\frac{7}{25}$ and $\sin(2\arccos(\frac{3}{5})) = (\cos(\arccos(\frac{3}{5}))\sin(\arccos(\frac{3}{5}))) = \frac{24}{25}$, thus the cosine and sine of both angles are rational and not equal to $0, \pm\frac{1}{2}, \pm 1$ (we only require this of the cosine) as required. We showed that all elements of the quaternions are rational, thus we have a free subgroup of $SO_3(\mathbb{Q})$ generated by $\gamma(a), \gamma(\overline{a}), \gamma(b), \gamma(\overline{b}) \in \mathbb{H}(\mathbb{Q})$. □

Note that the conditions mentioned are guaranteed to give a free group but are not necessary for freeness. See [21].

5.2.1 Matrix Representation of Quaternions

It is possible to represent a quaternion $q \in \mathbb{H}(\mathbb{Q})$ by a matrix $M \in \mathbb{C}(\mathbb{Q})^{2\times 2}$. For a general quaternion $\vartheta = (a, b, c, d) \cdot \mu$ we define the matrix:

$$M = \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}.$$

The correctness of multiplication and addition under this encoding can be checked by verifying the result of the operation in terms of quaternions and matrices separately.

Corollary 5.2. *There exists a class of two-dimensional complex unitary matrices forming a free group.*

Proof. We can define a morphism similar to γ which instead maps to two-dimensional complex matrices: Formally, $\zeta : \Sigma^* \mapsto \mathbb{C}(\mathbb{Q})^{2\times 2}$ where:

$$\zeta(a) = \begin{pmatrix} \frac{3}{5}+\frac{4}{5}i & 0 \\ 0 & \frac{3}{5}-\frac{4}{5}i \end{pmatrix}, \zeta(b) = \begin{pmatrix} \frac{3}{5} & \frac{4}{5} \\ -\frac{4}{5} & \frac{3}{5} \end{pmatrix},$$

Note that matrices $\zeta(a)$ and $\zeta(b)$ are unitary, therefore let $\zeta(\overline{a}) = \zeta(a)^{-1} = \zeta(a)^*$ and $\zeta(\overline{b}) = \zeta(b)^{-1} = \zeta(b)^*$ where $*$ denotes the Hermitian transpose, thus:

$$\zeta(\overline{a}) = \begin{pmatrix} \frac{3}{5} - \frac{4}{5}\mathbf{i} & 0 \\ 0 & \frac{3}{5} + \frac{4}{5}\mathbf{i} \end{pmatrix}, \zeta(\overline{b}) = \begin{pmatrix} \frac{3}{5} & -\frac{4}{5} \\ \frac{4}{5} & \frac{3}{5} \end{pmatrix},$$

Therefore we have the injective morphism $\zeta : (\Sigma \cup \overline{\Sigma})^* \mapsto \mathbb{C}(\mathbb{Q})^{2\times 2}$. Since γ is an injective homomorphism, ζ is also clearly injective and therefore the set $\mathscr{G} = \{\zeta(a), \zeta(\overline{a}), \zeta(b), \zeta(\overline{b})\} \subset \mathbb{C}(\mathbb{Q})^{2\times 2}$ generates a free group of two-dimensional complex rational matrices. □

Also note that we can define such matrices for any two orthonormal vectors where the rotation angle θ satisfies $\cos(\theta) \in \mathbb{Q}$ and $\cos(\theta) \neq 0, \pm\frac{1}{2}, \pm 1$. Thus we can find an infinite number of such matrices which will obviously be unitary by the definition of ζ and unit quaternions.

Notice that we can multiply both matrices by the scalar matrix with element 5 to give a Gaussian integral matrix (at the expense of losing unimodularity).

5.3 Low Dimension Quaternion Matrix Semigroups

We shall now show an undecidability result similar to the one considered in Section 4.4 concerning semigroup intersections as studied by A. Markov [42].

Theorem 5.3. *Given two sets $A = \{a_1, a_2, \ldots, a_n\}$ and $B = \{b_1, b_2, \ldots, b_n\}$, where $A, B \subset \mathbb{H}(\mathbb{Q})$, it is undecidable whether there exists a non-empty sequence of indices $r = (r_1, r_2, \ldots, r_m)$ such that $a_{r_1} a_{r_2} \cdots a_{r_m} = b_{r_1} b_{r_2} \cdots b_{r_m}$. Moreover, this holds for $n = n_{PCP}$.*

Proof. We use a reduction of Post's correspondence problem (PCP) (see Section 3.2) and the morphism γ defined in Section 5.1. Given two alphabets Γ, Σ, such that Σ is binary, and an instance of the PCP, $(h, g) : \Gamma^* \mapsto \Sigma^*$.

We proved in Lemma 5.1 that $\gamma : (\Sigma \cup \overline{\Sigma})^* \mapsto \mathbb{H}(\mathbb{Q})$ is a monomorphism. Thus let us define a new pair of morphisms (ρ, τ) to map $\Gamma^+ \times \Gamma^+$ directly into $\mathbb{H}(\mathbb{Q}) \times \mathbb{H}(\mathbb{Q})$ (we can think of this as $\mathrm{SU}_2 \times \mathrm{SU}_2$ since each of these unit quaternions represents an element of S^3 (the 3-sphere)). Formally, $\rho : \Gamma^* \mapsto \mathbb{H}(\mathbb{Q})$, $\tau : \Gamma^* \mapsto \mathbb{H}(\mathbb{Q})$ where for any $w \in \Gamma^+$, we define $\rho(w) = \gamma(h(w))$ and $\tau(w) = \gamma(g(w))$. This is clearly injective since it is the composition of two injective homomorphisms.

Thus for an instance of PCP, $\Gamma = \{a_1, a_2, \dots, a_m\}$, (h, g), we instead use the pair of morphisms (ρ, τ). Define two semigroups S_1, S_2 generated respectively by $\{\rho(a_1), \rho(a_2), \dots, \rho(a_m)\}$ and $\{\tau(a_1), \tau(a_2), \dots, \tau(a_m)\}$. We see there exists a solution to the given instance of PCP iff $\exists w \in \Gamma^+$ such that $\rho(w) = \tau(w)$. □

We now move to an extension of the previous theorem where it is no longer necessary to consider the index sequence. Markov obtained a similar result by extending the dimension of the integral matrices to 4 × 4.

Theorem 5.4. *Given two sets of matrices $A = \{A_1, A_2, \dots, A_n\}$ and $B = \{B_1, B_2\}$ where $A, B \subset \mathbb{H}(\mathbb{Q})^{2\times 2}$ generating two semigroups S, T respectively. It is undecidable if $|S \cap T| = 0$. Furthermore, all matrices in S, T are diagonal.*

Proof. Given an instance of PCP, (h, g) where $h, g : \Gamma^* \mapsto \Sigma^*$. We again use the injective morphisms $\rho, \tau : \Gamma^* \mapsto \mathbb{H}(\mathbb{Q})$ introduced in Theorem 5.3. Now, for each $a \in \Gamma$ we define:

$$A_a = \begin{pmatrix} \rho(a) & 0 \\ 0 & \tau(a) \end{pmatrix}$$

and these matrices form the generator for the semigroup S. For the second semigroup, T, we simply wish to encode each symbol from Σ in the $[1, 1]$ and $[2, 2]$ elements using the morphism $\gamma : \Sigma^* \mapsto \mathbb{H}(\mathbb{Q})$ which was shown to be injective in Lemma 5.1:

$$B_1 = \begin{pmatrix} \gamma(a) & 0 \\ 0 & \gamma(a) \end{pmatrix}, \qquad B_2 = \begin{pmatrix} \gamma(b) & 0 \\ 0 & \gamma(b) \end{pmatrix}.$$

Now we can prove the theorem. We see that for some $M \in A$, $M_{[1,1]} = M_{[2,2]}$ iff there exists a solution $w \in \Gamma^+$ to the instance of PCP. This follows since element $[1,1]$ of M stores an encoding of $h(w)$ and element $[2,2]$ of M stores an encoding of $g(w)$. Clearly any such matrix M will also be in B since every matrix in B corresponds to an encoding of a word over Σ^+. Matrices in B clearly store an encoding of the same word in elements $[1,1]$ and $[2,2]$. Note that all matrices are diagonal and each element on the leading diagonal is a unit quaternion by the definitions of the morphisms used. □

The previous two theorems used two separate semigroups. It is more natural to ask whether a particular element is contained within a *single* semigroup. We shall show an undecidable membership result for a class of two-dimensional quaternion matrices.

Theorem 5.5. *Given a matrix semigroup $\mathcal{S}$ generated by the (finite) set $\mathcal{G} = \{X_1, X_2, \ldots, X_n\} \subset \mathbb{H}(\mathbb{Q})^{2\times 2}$ where X_i is diagonal for each $1 \leq i \leq n$. It is undecidable for a fixed matrix Y whether $Y \in \mathcal{S}$. Moreover, Y can be chosen such that each diagonal element of Y has the form $(a, 0, 0, 0) \cdot \mu$ with $a \in \mathbb{Q} \setminus \{0, \pm 1\}$.*

Proof. This theorem can be proved essentially in the same way as Theorem 4.1 using an instance of INDEX CODING PCP. We shall however use a different injective homomorphism in order to map into the rational quaternions rather than 2×2 integral matrices.

We shall use the version of INDEX CODING PCP which is defined using the pair of homomorphisms $h, g : \Gamma^* \mapsto (\Sigma \cup \overline{\Sigma})^*$ where $\Sigma = \{a, b\}$ is a binary alphabet and $\Gamma = \{a_1, a_2, \ldots, a_n\}$. We thus require a solution to

Index Coding PCP:

$$w = w_1 w_2 \cdots w_k \in \Gamma^*,$$

such that exactly one $w_i = n$ and $h(w) = g(w) = \varepsilon$.

Recall the injective homomorphism $\gamma : (\Sigma \cup \overline{\Sigma})^* \mapsto \mathbb{H}(\mathbb{Q})$ defined by:

$$\begin{array}{ll} \gamma(a) = (\frac{3}{5}, \ \ \frac{2}{5}, 0, 0) \cdot \mu, & \gamma(b) = (\frac{3}{5}, 0, \ \ \frac{2}{5}, 0) \cdot \mu, \\ \gamma(\overline{a}) = (\frac{3}{5}, -\frac{2}{5}, 0, 0) \cdot \mu, & \gamma(\overline{b}) = (\frac{3}{5}, 0, -\frac{2}{5}, 0) \cdot \mu, \end{array}$$

from above.

We define the matrices $\mathscr{G} = \{X_1, X_2, \ldots, X_n\} \subset \mathbb{H}(\mathbb{Q})^{2\times 2}$ where:

$$X_i = \begin{pmatrix} \gamma(h(a_i)) & 0 \\ 0 & \gamma(g(a_i)) \end{pmatrix}, 1 \leq i \leq n$$

which is analogous to the mapping into matrices we used in Theorem 4.1. If there exists a solution to Index Coding PCP, say $w = w_1 w_2 \cdots w_k \in \Gamma^*$ with exactly one $w_i = n$, then:

$$X_{w_1} X_{w_2} \cdots X_{w_k} = \begin{pmatrix} \gamma(\varepsilon) & 0 \\ 0 & \gamma(\varepsilon) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.$$

We need to enforce the constraint that only one element of this product equals X_n however. We achieve this in a similar way to that in Theorem 4.1. We multiply matrix X_n by a scalar such as 2, giving $X_n' = 2X_n$ and we can therefore see by the construction that $2I_2 \in \langle \mathscr{G} \rangle$ iff the instance of Index Coding PCP has a solution.

We again require 14 matrices since Index Coding PCP is undecidable for an instance of size 14. □

Note that in Theorem 5.5 we use diagonal quaternion matrices which are equivalent to *double quaternions*.

Corollary 5.6. *The vector reachability problem for a semigroup of* 2×2 *quaternion matrices is undecidable.*

Proof. The vector reachability question for quaternions is defined as: "Given two vectors $a, b \in \mathbb{H}(\mathbb{Q})^n$ and a finitely generated semigroup of matrices $\mathcal{S} \subset \mathbb{H}(\mathbb{Q})^{n \times n}$, does there exist some $M \in \mathcal{S}$ such that $Ma = b$?".

The undecidability of this problem is straightforward from Theorem 5.5. Let $x, y \in \mathbb{H}(\mathbb{Q})^2$ and $x = (1,1)^T, y = (2,2)^T$. Then, for some $M \in \mathcal{S}$, it is clear that $Mx = y$ iff $M = 2I_2$ since all matrices in $\mathcal{S}$ are diagonal. Since determining if $2I_2 \in \mathcal{S}$ was shown to be undecidable, the vector reachability problem is also undecidable. □

The next problem was given as an open problem over matrices of natural numbers $\mathbb{N}$ in any dimension [14]. We show it is undecidable over $\mathbb{H}(\mathbb{Q})^{2\times2}$.

Theorem 5.7. *It is undecidable for a two-dimensional rational quaternion matrix semigroup $\mathcal{S}$ whether there exists* any *diagonal matrix $D \in \mathcal{S}$. This holds for a semigroup generated by n_{PCP} matrices.*

Proof. Given a pair of homomorphisms $h, g : \Gamma^* \mapsto \Sigma^*$ which are an instance of Post's correspondence problem (PCP) where $\Sigma = \{a, b\}$ is a binary alphabet. We use the injective homomorphism $\gamma : \Sigma^* \mapsto \mathbb{H}(\mathbb{Q})$ defined and proven injective in Section 5.2.

Let us define a homomorphism $\Psi : \mathbb{H}(\mathbb{Q}) \times \mathbb{H}(\mathbb{Q}) \mapsto \mathbb{H}(\mathbb{Q})^{2\times2}$, where for any two quaternions $q, r \in \mathbb{H}(\mathbb{Q})$:

$$\Psi(q,r) = \frac{1}{2}\begin{pmatrix} q+r & q-r \\ q-r & q+r \end{pmatrix}$$

It is clear that Ψ is a homomorphism, as shown in [13], since clearly $\Psi(q_1, r_1) \cdot \Psi(q_2, r_2) = \Psi(q_1q_2, r_1r_2)$ which is verified easily via:

$$\frac{1}{2}\begin{pmatrix} q_1+r_1 & q_1-r_1 \\ q_1-r_1 & q_1+r_1 \end{pmatrix} \cdot \frac{1}{2}\begin{pmatrix} q_2+r_2 & q_2-r_2 \\ q_2-r_2 & q_2+r_2 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} q_1q_2+r_1r_2 & q_1q_2-r_1r_2 \\ q_1q_2-r_1r_2 & q_1q_2+r_1r_2 \end{pmatrix}.$$

It is now obvious that $\Psi(q, r)$ is diagonal iff $q = r$ since the top right and bottom left elements of the matrix equal 0 only if the two quaternions are equal.

Therefore, given an instance of Post's correspondence problem (PCP), $h, g : \Gamma^* \mapsto \Sigma^*$, where $\Gamma = \{a_1, a_2, \dots a_n\}$, we define the set of matrices $\mathscr{G} = \{X_1, X_2, \dots, X_n\} \subset \mathbb{H}(\mathbb{Q})^{2\times 2}$ where:

$$X_i = \begin{pmatrix} \gamma(h(a_i)) + \gamma(g(a_i)) & \gamma(h(a_i)) - \gamma(g(a_i)) \\ \gamma(h(a_i)) - \gamma(g(a_i)) & \gamma(h(a_i)) + \gamma(g(a_i)) \end{pmatrix}, a_i \in \Gamma$$

If there exists a solution $w_1 w_2 \cdots w_k \in \Gamma^*$ to the given instance of PCP, then $h(w) = g(w)$ and therefore:

$$X_{w_1} X_{w_2} \cdots X_{w_k} = \begin{pmatrix} 2\gamma(h(w)) & 0 \\ 0 & 2\gamma(h(w)) \end{pmatrix}$$

which is diagonal, and as previously stated, this is the only case in which such a diagonal matrix will occur in the semigroup $\mathscr{S} = \langle \mathscr{G} \rangle$. Since we know that PCP is undecidable for $|\Gamma| = 7$, this problem is undecidable for semigroups generated by 7 quaternion matrices of dimension 2. □

Unfortunately this does not hold when we convert the matrices to four-dimensional rational matrices since we only get a *block diagonal* matrix. We showed previously in Theorem 4.7 that the problem is also undecidable for 4×4 complex rational matrix semigroups.

Another problem which can be stated is that of *freeness* of quaternion matrix semigroups. We shall use an almost identical proof to that in [17] to show the undecidability of the problem, and we obtain the result for matrices over $\mathbb{H}(\mathbb{Q})^{2\times 2}$ rather than $(\mathbb{Z}^+)^{3\times 3}$:

Theorem 5.8. *Given a semigroup $\mathscr{S}$ generated by a finite set of matrices $\mathscr{G} = \{M_1, \dots, M_n\}$ where $M_i \in \mathbb{H}(\mathbb{Q})^{2\times 2}$, deciding whether $\mathscr{S}$ is free is algorithmically undecidable.*

Proof. Since we can store two words within a matrix $M_i \in \mathbb{H}(\mathbb{Q})^{2\times 2}$ we can use an almost identical proof that was used in [17]. We will give a brief sketch of the proof and refer to [17] for a more rigorous version.

The mixed modification PCP (or MMPCP) is a variant of the standard Post's correspondence problem (PCP). As in the original PCP, we are given two (finite) alphabets Γ, Σ and two morphisms $h, g : \Gamma^* \to \Sigma^*$. The MMPCP asks whether there exists a word $w = w_1 w_2 \cdots w_m \in \Sigma^+$ such that:

$$h_1(w_1)h_2(w_2)\cdots h_m(w_m) = g_1(w_1)g_2(w_2)\cdots g_m(w_m)$$

where each $h_i, g_i \in \{h, g\}$ and $h_j \neq g_j$ for some $1 \leq j \leq m$. We shall use a reduction of this problem to the freeness of quaternion matrix semigroups.

Define the set of 2 × 2 quaternion matrices:

$$\mathscr{G} = \left\{ \begin{pmatrix} \gamma(a) & 0 \\ 0 & h(a) \end{pmatrix}, \begin{pmatrix} \gamma(a) & 0 \\ 0 & g(a) \end{pmatrix} ; \quad a \in \Gamma \right\}.$$

If $\mathscr{S}$ is not free then there is a word $w = w_1 w_2 \cdots w_n \in \Sigma^+$ such that $h_1(w_1)h_2(w_2)\cdots h_m(w_m) = g_1(w_1)g_2(w_2)\cdots g_m(w_m)$ since any equal matrix product in $\mathscr{S}$ must have the same word w in the top left element and the same element in the bottom right which was generated by *different* matrices. Thus the problem of freeness for 2×2 rational quaternion matrix semigroups is undecidable. See [17] for more details of the proof method.

Note that an alphabet size of $|\Gamma| = 7$ was required for the undecidability of MMPCP (see [28]), thus the problem is undecidable for a semigroup generated by 7 matrices. □

We now consider a problem which is *decidable* over complex numbers, but *undecidable* over rational quaternions. This gives a bound between the computational power of complex numbers and quaternions. We first require a lemma.

Lemma 5.9. *[3] Given a semigroup $\mathscr{S}$ of commutative matrices of any dimension, then the membership problem for $\mathscr{S}$ is decidable.*

Corollary 5.10. *The problems for diagonal matrices stated in Theorems 5.3, 5.4 and 5.5 are decidable when taken instead over any field up to the complex numbers.*

Proof. In Theorem 5.3 we can change the problem to one over two-dimensional matrices which will be equivalent. For each $1 \leq k \leq n$ we define

$$M_k = \begin{pmatrix} q_{ik} & 0 \\ 0 & q_{jk} \end{pmatrix} \in \mathbb{C}^{2\times 2}.$$

Now define a semigroup $\mathscr{S}$ generated by $\mathscr{G} = \{M_1, M_2, \ldots, M_n\}$. Clearly then the problem becomes "Does there exist a matrix X in $\mathscr{S}$ such that $X_{[1,1]} = X_{[2,2]}$?". This is decidable if the matrices commute (in the case of complex diagonal matrices) and we have shown it to be undecidable for diagonal matrices over the quaternions.

Theorem 5.4 concerns the emptiness testing of the intersection of two semigroups A, B. However, B is just the set of matrices with equal elements on the diagonal generated by $\gamma(a)$ and $\gamma(b)$. Thus the problem when taken for complex numbers is simply: "Does there exist some matrix, $X \in A$ with $X_{[1,1]} = X_{[2,2]}$" as in the previous paragraph. Again, since the matrices are diagonal and complex, they commute and the problem is clearly decidable.

For Theorem 5.5, all matrices in the semigroup commute since they are diagonal with complex entries. By Lemma 5.9 this means we can decide if any M is in semigroup $\mathscr{S}$ (in polynomial time) thus concluding the proof. □

5.4 Computational Problems in Lipschitz Integers

We shall now consider decision questions on matrices over *Lipschitz integers*, denoted by $\mathbb{H}(\mathbb{Z})$ which are quaternions with integral parts.

Corollary 5.11. *The problems stated in Theorems 5.3 and 5.4 are undecidable for matrix semigroups when taken instead over the Lipschitz integers* $\mathbb{H}(\mathbb{Z})$.

Proof. Note that in Lemma 5.1 we showed γ is injective and in Section 5.2.1 we showed an isomorphism between quaternions and a subgroup of the two-dimensional complex matrices, $\mathbb{H}(\mathbb{Q}) \cong \mathbb{C}^{2\times 2}$. If we examine the definition of ζ in 5.2.1 we see that all elements have 5 as their denominator thus we can multiply $\zeta(a), \zeta(b)$ by the scalar matrix $5I_2$ thus giving two-dimensional matrices over the Gaussian integers. This will still be free and is equivalent to the (non-unit) quaternions $q_1 = 5(\frac{3}{5}, \frac{4}{5}, 0, 0) \cdot \mu = (3, 4, 0, 0) \cdot \mu$ and $q_2 = 5(\frac{3}{5}, 0, \frac{4}{5}, 0) \cdot \mu = (3, 0, 4, 0) \cdot \mu$ which still form a free semigroup. We therefore define $\lambda : \Sigma^* \mapsto \mathbb{H}(\mathbb{Q})$ by

$$\lambda(x) = \begin{pmatrix} 5 \cdot \gamma(x) & \text{if } x \neq \varepsilon \\ \gamma(x) & \text{if } x = \varepsilon \end{pmatrix}.$$

Thus in Theorems 5.3 and 5.4 we can replace the definitions of ρ, τ to use λ instead and this will give an injective morphism over the Lipschitz integers $\mathbb{H}(\mathbb{Z})$. This cannot be extended to Theorem 5.5 however since the inverse of a non-identity Lipschitz integer is not itself a Lipschitz integer (obviously it must have rational coefficients). □

Lemma 5.12. *The modulus of quaternions is multiplicative and the ring of Lipschitz integers with multiplication and addition is closed.*

Proof. These simple results are needed in Theorem 5.13 below. For the first statement we wish to prove $||q_1 q_2|| = ||q_1|| \cdot ||q_2||$. Fortunately we do not need to use a laborious proof of this since the determinant of the matrix representation of a quaternion shown in 5.2.1 corresponds to the modulus. It is well known that the determinant of complex matrices is multiplicative, see [31].

The second part is easy to see by examining the product of two quaternions. We only multiply and sum entries in the product therefore if both quaternions have integral components, so does their product. Thus the product of two Lipschitz integers is a Lipschitz integer and obviously the sum is also closed since it is simply the component-wise addition of integers. □

Theorem 5.13. *Given a set of Lipschitz integers $\mathscr{G} \in \mathbb{H}(\mathbb{Z})$ generating a semigroup $\mathscr{S} = \langle \mathscr{G} \rangle$, the problem of deciding for an arbitrary $L \in \mathbb{H}(\mathbb{Z})$ if $L \in \mathscr{S}$ is decidable.*

Proof. Note that all non-zero quaternions have modulus $d \in \mathbb{R}^+$. Furthermore, it is obvious that for any non-zero Lipschitz integer $L \in \mathbb{H}(\mathbb{Z})$, that $d \geq 1$, with equality iff

$$L \in \Phi = \{(\pm1,0,0,0)\cdot\mu, (0,\pm1,0,0)\cdot\mu, (0,0,\pm1,0)\cdot\mu, (0,0,0,\pm1)\cdot\mu\}.$$

We have named this set Φ for later explanation. It is easily seen $\forall q \in \Phi$ that q is of unit length, i.e.,

$$||q|| = q\bar{q} = \sqrt{a^2+b^2+c^2+d^2} = 1.$$

Also note that their fourth powers are all equal to the identity element, i.e., $\forall q \in \Phi, q^4 = \vartheta_I = (1,0,0,0)\cdot\mu$ which is easily checked.

For a given $L \in \mathbb{H}(\mathbb{Z})$ whose membership in $\mathscr{S}$ we wish to determine, it will have a magnitude $||L|| = m \in \mathbb{R}$. If $m < 1$ then L cannot be a product a Lipschitz integers since the magnitude must be at least 1 by definition of the quaternion magnitude. If $m = 1$ then L can only be a product of elements from Φ and membership is trivial by examining the generator $\mathscr{G}$. Otherwise, $m > 1$. Let $\mathscr{G}' = \mathscr{G} \setminus \Phi$ (which is the generator set $\mathscr{G}$ minus any elements of Φ). We can see that there exists only a finite number of products to check since $m > 1$ and $\forall x \in \langle\mathscr{G}'\rangle$ we have that $||x|| > 1$. Again, this is easy to see from the definition of the magnitude when considering integral components.

Thus, excluding Φ we have a *finite* set of products of *finite* length to check. However if a (non-identity) element of Φ is in the generator, we must include these in the products. Let $\mathscr{S}' = \langle\mathscr{G}'\rangle$. For each product from $\mathscr{S}'$ whose magnitude equals L:

$$P = p_1p_2\cdots p_n \qquad |(p_t \in S') \wedge (||P|| = m)$$

we define the (finite) set of products:

$$\left\{P = \left(\prod_{t=1}^{n} r_t p_t\right) r_{n+1} \,|r_t, p_t \in \mathbb{H}(\mathbb{Z})\right\},$$

where each r_t varies over all elements of $[(\Phi\cap\mathscr{G})\cup\vartheta_I]$ for $1 \leq t \leq n+1$. I.e. r_t varies over all possible products of elements of Φ that are in $\mathscr{G}$ or the identity quaternion in all possible places in the product (since elements of $\langle \Phi \rangle$ are unimodular). We must simply prove that $\langle \Phi \rangle$ (the semigroup over elements of Φ) is finite. This is easily seen however from the following three facts; the only Lipschitz integers with moduli 1 are in Φ, the quaternion moduli is closed under multiplication and the product of two Lipschitz integers is a Lipschitz integer.

The first fact is obvious since the square root of a sum of four squares is equal to 1 iff exactly one component is 1. The second and third facts were proven in Lemma 5.12. Thus $\langle \Phi \rangle$ is a finite semigroup and there exists a finite set of products to check for equality to $L \in \mathbb{H}(\mathbb{Z})$ and thus this is a decidable problem. □

Chapter 6

Reductions of Skolem's Problem

In this chapter we shall study some encodings of a well known problem known as SKOLEM'S PROBLEM. It is also sometimes called Pisot's problem. The problem itself is concerns the decidability of determining zeros in *linear recurrent sequences* which we shall soon detail. We shall show how the problem is related to THE MORTALITY PROBLEM and exponential Diophantine equations.

We are often interested in systems whereby future states depend on some finite history. Given such a system we would then like to characterise its properties. For example, is the set of possible future states bounded? Is it periodic? Can we reach a particular state? Such problems are related to dynamical systems but it is frustrating that for even simply defined systems we often cannot develop algorithms to determine the types of properties listed. We shall now define a very simple example of this type of system.

A sequence $\mathbf{u} = (u_0, u_1, \cdots) = (u_i)_{i=0}^{\infty}$ is called a *linear recurrent sequence* if it satisfies the condition that:

$$u_k = r_{n-1}u_{k-1} + r_{n-2}u_{k-2} + \cdots + r_0u_{k-n},$$

for all $k \geq n$ where $(r_0, r_1, \ldots, r_{n-1}) \in \mathbb{Z}^n$ is a fixed integral vector we shall call the *coefficient vector*. We can see that the next value u_k depends upon this fixed coefficient vector and the n previous values $u_{k-1}, u_{k-2}, \ldots u_{k-n}$.

Let us consider an example. Take $u_0 = 0, u_1 = 1$ and the coefficient vector $(2, 1)$. Thus, $u_2 = 2u_1+u_0 = 2$, $u_3 = 2u_2+u_1 = 5$ and $u_4 = 2u_3+u_2 = 12$ etc. This gives us the sequence $(0, 1, 2, 5, 12, 25, 70, 169, 408, \ldots)$ which are the so called *Pell numbers* which can be used to approximate $\sqrt{2}$ by the formula

$$\sqrt{2} \approx \frac{u_{k-1} + u_k}{u_k}.$$

Another more famous example is given by $u_0 = 0, u_1 = 1$ and the coefficient vector $(1, 1)$ which generates the Fibonacci sequence of natural numbers $(0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots)$.

We are now ready to state SKOLEM'S PROBLEM:

Open Problem 6.1. SKOLEM'S PROBLEM - *Given a linear recurrent sequence $(u_0, u_1, u_2, \ldots) \in \mathbb{Z}^{\mathbb{N}}$, does there exist some value $k \geq 0$ such that $u_k = 0$?*

We can represent linear recurrent sequences using matrix notation and properties of the sequence can then be formulated as a property of the underlying matrix and vector equations. We shall show this representation in the next section. This will allow us to express SKOLEM'S PROBLEM in terms of a matrix property.

The decidability status of SKOLEM'S PROBLEM is a long standing open problem. It is known to be decidable for $n = 5$ which is a highly non-trivial result requiring algebraic number theory, see [29]. A related problem, that of determining whether all elements of a linear recurrent sequence of depth 2 are all positive, is known to be decidable [30].

We can represent linear recurrent sequences using matrix notation and properties of the sequence can then be formulated as a property of the underlying matrix and vector equations. We shall show this standard representation in the next theorem.

6.1 Zero in the Upper Right Corner

There is a well known construction whereby we can convert an instance of Skolem's Problem to an instance of the zero in the upper right corner problem for a single integral matrix. Let $(r_0, r_1, \ldots, r_{n-1})$ be the coefficient vector and $u = (u_n, u_{n-1}, \ldots u_0)$ be the initial values. We construct the matrix:

$$A' = \begin{pmatrix} r_{n-1} & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ r_2 & 0 & \cdots & 1 & 0 \\ r_1 & 0 & \cdots & 0 & 1 \\ r_0 & 0 & \cdots & 0 & 0 \end{pmatrix} \in \mathbb{Z}^{n \times n}.$$

Let $\mathbf{0} = (0, 0, \ldots, 0)^T \in \mathbb{Z}^n$ be a zero vector. We may now extend matrix A' by 1 dimension to give the matrix:

$$A = \begin{pmatrix} 0 & uA' \\ \mathbf{0} & A' \end{pmatrix} \in \mathbb{Z}^{(n+1)\times(n+1)},$$

and clearly by studying the form of the matrix we can see that:

$$A^j = \begin{pmatrix} 0 & uA'^j \\ \mathbf{0} & A'^j \end{pmatrix} \in \mathbb{Z}^{(n+1)\times(n+1)}.$$

Thus the top right element of this matrix, $A^j_{[1,n+1]} = u_{j+n}$ for any $j \geq 1$ as required. Therefore it follows that Skolem's Problem has a solution if an only if some power of matrix A has a zero in its upper right corner as required.

This construction is well known from the literature and for a depth n linear recurrence it requires a matrix of dimension $n + 1$. We shall next show that instances of Skolem's Problem can be converted to instances of the zero in the upper *left* corner problem on a single matrix of dimension n. The resulting matrices are rational however rather than integral. The reason for us showing such a construction is to reduce any instance of SKOLEM'S PROBLEM to the mortality problem for a pair of integral matrices later in the chapter.

6.2 Zero in the Upper Left Corner

In this section we shall show a new formulation in terms of rational matrices where SKOLEM'S PROBLEM instances can be converted into instances of the ZERO IN THE UPPER LEFT CORNER PROBLEM (which we now define), and also into the THE MORTALITY PROBLEM for integral matrix semigroups which we define in the next section.

Problem 6.2. ZERO IN THE UPPER LEFT CORNER PROBLEM - *Given a finite set of matrices* $\mathcal{G} = \{M_1, M_2, \ldots, M_n\} \subseteq \mathbb{Z}^{k \times k}$ *generating a semigroup* $\mathcal{S}$, *does there exist some* $M \in \mathcal{S}$ *such that* $M_{[1,1]} = 0$*? I.e. does there exist some matrix in the semigroup with a zero in the top left element?*

In the next theorem we convert instances of SKOLEM'S PROBLEM to an instance of ZERO IN THE UPPER LEFT CORNER PROBLEM with just a single matrix in the generator. Then we shall show that we can also convert into instances of THE MORTALITY PROBLEM which we define in the next section with just two matrices in the generator.

Theorem 6.3. SKOLEM'S PROBLEM *of depth n is equivalent to an instance of the* ZERO IN THE UPPER LEFT CORNER PROBLEM *for a semigroup generated by a single matrix* $M \in \mathbb{Q}^{n \times n}$.

Proof. Let $u = (u_0, u_1, \ldots, u_{n-1})^T \in \mathbb{Z}^n$ be the initial vector of values for a depth n linear recurrence and $r = (r_0, r_1, \ldots, r_{n-1}) \in \mathbb{Z}^n$ be the coefficient vector.

We may write the updating procedure using matrices in the following way:

$$R = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ r_0 & r_1 & r_2 & \cdots & r_{n-1} \end{pmatrix}, u = \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ \vdots \\ u_{n-1} \end{pmatrix}$$

where $R \in \mathbb{Z}^{n \times n}$ and we see that $R \cdot u = (u_1, u_2, \ldots, u_{n-1}, u_n)^T$, and more generally:

$$R^k \cdot u = (u_k, u_{k+1}, \ldots, u_{n+k-2}, u_{n+k-1}) \tag{6.1}$$

We can then define a vector $x = (0, 0, \ldots, 1)^T \in \mathbb{Z}^n$ and individual values of the sequence can be obtained:

$$u_{n+k} = x^T R^{k+1} u; \quad k \geq 0$$

Now let us define two new matrices $S, S^{-1} \in \mathbb{Z}^{n \times n}$ by:

$$S = \begin{pmatrix} u_0 & 1 & 0 & \cdots & 0 \\ u_1 & 0 & 1 & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ u_{n-2} & 0 & 0 & \cdots & 1 \\ u_{n-1} & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad S^{-1} = \begin{pmatrix} 0 & 0 & 0 & \cdots & \frac{1}{u_{n-1}} \\ 1 & 0 & 0 & \cdots & -\frac{u_0}{u_{n-1}} \\ 0 & 1 & 0 & \ddots & -\frac{u_1}{u_{n-1}} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -\frac{u_{n-2}}{u_{n-1}} \end{pmatrix}$$

Clearly, $\det(S) = (-1)^{n-1} \cdot u_{n-1}$, and S is thus invertible (since if $u_i = 0$ for $1 \leq i < n$, we have a trivial solution to Skolem's problem). Let us now examine element $(RS)_{[n,1]}$ (the bottom left element of this product). It is equal to $\sum_{i=0}^{n-1} r_i u_i$ which is exactly u_n. Now consider element $(S^{-1}RS)_{[1,1]}$:

$$(S^{-1}RS)_{[1,1]} = -\frac{1}{u_{n-1}} \cdot \sum_{i=0}^{n-1} r_i u_i,$$

and we know $u_{n-1} \neq 0$ as stated previously. Let us define $X = S^{-1}RS$ and consider powers of this matrix. We see that:

$$X^k = S^{-1}R^kS \tag{6.2}$$

We see that $(R^k \cdot S)_{[n,1]} = \sum_{i=k}^{n+k-1} r_i u_i = u_{n+k}$ which follows from (6.1) since the first column of S equals the vector u. Finally then we see as before that:

$$X^k_{[1,1]} = (S^{-1}R^kS)_{[1,1]} = \frac{1}{u_n}\sum_{i=0}^{n-1} r_i u_{k+i} = \frac{1}{u_n} \cdot u_{n+k} \tag{6.3}$$

Since $\frac{1}{u_n} \neq 0$, then $(X^k)_{[1,1]} = 0$ iff $\sum_{i=0}^{n-1} r_i u_{k+i} = 0$ iff there exists a solution to the instance of Skolem's problem.

The characteristic polynomial of R equals $t^n - r_{n-1}t^{n-1} - \ldots - r_0$ and therefore by the Cayley-Hamilton theorem:

$$X^n = r_{n-1}X^{n-1} + r_{n-2}X^{n-2} + \cdots + r_0 I.$$

Thus, $X^{k+n} = r_{n-1}X^{k+n-1} + r_{n-2}X^{k+n-2} + \cdots + r_0 X^k$ for any $k \in \mathbb{Z}^+$ validating the correctness of the encoding. □

We now state a simple result we shall require later on:

Lemma 6.4. *The characteristic polynomial of a depth n minimal linear recurrent sequence does not have* 0 *as a solution.*

Proof. The characteristic polynomial is $t^n - r_{n-1}t^{n-1} - \ldots - r_0$. If $r_0 = 0$ then the linear recurrent sequence is not minimal, we can replace it by an equivalent recurrence of depth $(n-1)$. □

Therefore, we initially have an integral matrix $R \in \mathbb{Z}^{n \times n}$ and then define $X = S^{-1}RS$ for $S, S^{-1} \in \mathrm{GL}_n(\mathbb{Q})$, such that the given instance of SKOLEM'S PROBLEM has a solution iff there exists $k > 0$ such that $X^k_{[1,1]} = 0$.

6.3 The Mortality Problem

We have shown that SKOLEM'S PROBLEM can be converted to an instance of the ZERO IN THE UPPER LEFT CORNER PROBLEM. We shall now show that it can also be converted to THE MORTALITY PROBLEM which we now define:

Problem 6.5. THE MORTALITY PROBLEM - *Given a finite set of integral matrices* $\mathcal{G} = \{M_1, M_2, \ldots, M_n\} \subseteq \mathbb{Z}^{k \times k}$ *generating a semigroup* $\mathcal{S}$, *does there exist* $Z \in \mathcal{S}$ *where* Z *is the* zero matrix*?*

It is known that THE MORTALITY PROBLEM is undecidable for semigroups generated by 8 integral matrices of dimension 3, see [25]. Conversely, it is known that the problem is decidable for a pair of 2×2 rational matrices, see [16]. The problem is currently open for an arbitrary number of matrices in dimension 2:

Open Problem 6.6. *Is* THE MORTALITY PROBLEM *decidable for a semigroup generated by a finite set of* 2×2 *rational matrices?*

Theorem 6.7. SKOLEM'S PROBLEM *for linear recurrences of depth* n *can be converted to* THE MORTALITY PROBLEM *for a 2-generator integral matrix semigroup of dimension* n.

Proof. This can be shown in a similar way to THE MORTALITY PROBLEM was proven undecidable in [25]. Let $X = S^{-1}RS$ as in the previous theorem. Define

$$P = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

Now define a semigroup $\mathscr{S} = \langle X, P \rangle$. Notice that PX^rP has zero's everywhere except the top left element which is 0 iff $X^r_{[1,1]} = 0$ iff $u_{r+k} = 0$.

Now, assume that some matrix $M \in \mathscr{S}$ is equal to the zero matrix: $M = M_1M_2 \cdots M_t = 0$. Since P is idempotent (i.e., $P^2 = P$), clearly we can equivalently write this in the form:

$$M = (X^i \cdot P) \cdot (P \cdot X^{j_1} \cdot P) \cdots (P \cdot X^{j_k} \cdot P) \cdot (P \cdot X^m),$$

where $i, m, k \geq 0$ and $j_l > 0$ for each $1 \leq l \leq k$, since it either starts/ends with a power of X matrices or with P. If $(X^i \cdot P)_{[1,1]} = 0$ or $(P \cdot X^m)_{[1,1]} = 0$ then we are done (since this is a solution), otherwise assume they do not.

Now consider each central product $(P \cdot X^{j_l} \cdot P)$. Clearly from the form of P this equals $X^{j_l}_{[1,1]} \cdot P$, which is a matrix with all zeros except the top left element which equals the top left element of X^{j_l}.

Thus if $(P \cdot X^{j_1} \cdot P)(P \cdot X^{j_2} \cdot P) \cdots (P \cdot X^{j_k} \cdot P)_{[1,1]} = 0$ then one of the bracketed subproducts equals 0 which corresponds to a correct solution. Thus, again assume no such product equals the zero matrix.

Finally then we have a product $M = (X^i \cdot P)(\lambda P)(P \cdot X^m) = 0$ where $\lambda \in \mathbb{Q} \setminus \{0\}$. But $(X^i \cdot P)(\lambda \cdot P) = X^i \cdot \lambda P$. This has zero's everywhere except the leftmost column and $(P \cdot X^m)$ has zeros everywhere except the uppermost row. Thus element $M_{[1,1]} = (X^i \cdot \lambda P)_{[1,1]} \cdot (P \cdot X^m)_{[1,1]} = 0$ but this is a contradiction since if the upper left corner is zero it corresponds to a correct solution. □

6.4 Exponential Diophantine Equations

It is also interesting to note that from this matrix representation we may derive a related problem in terms of exponential Diophantine equations. This may also be derived more directly from the Cayley-Hamilton theorem but we include it here for completeness and to show the connection between these three problems.

Problem 6.8. *Given two vectors $x = (x_0, x_1, \dots, x_{n-1}), z = (z_0, z_1, \dots, z_{n-1})$ where $x, z \in \mathbb{C}^n$ and each x_i, z_i are algebraic integers. Does there exist some $k \in \mathbb{N}$ such that:*

$$\sum_{i=0}^{n-1} z_i x_i^k = 0\,?$$

Or equivalently:

Problem 6.9. *Given two vectors of algebraic integers $x, z \in \mathbb{C}^n$, we can define the decision question,*

$$\text{Does } \prod_{k=1}^{\infty} \sum_{i=0}^{n-1} z_i x_i^k = 0? \qquad ;\ z_i, x_i \in \mathbb{C}$$

We shall now show a case where SKOLEM'S PROBLEM can be reduced to Problem 6.8, or equivalently to Problem 6.9. In other words we show a subset of instances of SKOLEM'S PROBLEM that have a solution if either Problems 6.8 or 6.9 have an algorithmic solution.

Theorem 6.10. *Given an instance of* SKOLEM'S PROBLEM *with linear recurrent sequence $u = (u_0, u_1, \dots, u_n)$, if the companion matrix of u has a characteristic polynomial with distinct roots then the instance can be reduced to Problem 6.8.*

Proof. Since the characteristic polynomial of R has distinct non-zero roots (by the statement of the theorem and Lemma 6.4), R is diagonalizable, thus $R = T^{-1}DT$ where $T \in \mathrm{GL}_n(\mathbb{C})$ and $D \in \mathbb{C}^{n \times n}$ is a diagonal matrix. Now, as before, we let $X = S^{-1}R^kS$. Therefore we see that:

$$X^k = (S^{-1}T^{-1}DTS)^k = S^{-1}T^{-1}D^kTS; \qquad S, T \in \mathrm{GL}_n(\mathbb{C}), D \in \mathbb{C}^{n \times n}$$

It is now apparent that we have fixed matrices $S^{-1}T^{-1}$, TS and a diagonal matrix D whose powers are easy to compute. We are interested in the upper left corner of X. Let u be the top row of $S^{-1}T^{-1}$ and v be the leftmost column of TS. Obviously $u^Tv = 1$ since these matrices are inverse to each other.

Let $D = d_1 \oplus d_2 \oplus \ldots \oplus d_n$ where $d_i \in \mathbb{C}$ be the diagonal matrix. Thus $D^k = d_1^k \oplus d_2^k \oplus \ldots \oplus d_n^k$. Now we see that:

$$X^k_{[1,1]} = (u_1 d_1^k, u_2 d_2^k, \ldots, u_n d_n^k) \cdot v^T = \sum_{i=1}^{n} u_i v_i d_i^k$$

Clearly $u_i v_i$ is constant for each instance and we simply take the initial vector x in the statement of Problem 6.8 to be $x = (u_1 v_1, u_2 v_2, \ldots, u_n v_n) \in \mathbb{C}^n$. We take the second vector z to be $z = (d_1, d_2, \ldots, d_n)$. And now we see that the two problems are indeed equivalent. Note that we still have the factor $\frac{1}{u_n}$ which changes the result but since this is non-zero, the summand equals zero iff the instance of Skolem's problem has a solution. □

What form will the diagonalizing matrix for R (a companion matrix) take? The next proposition will show this.

Proposition 6.11. *If the characteristic polynomial of a companion matrix $R \in \mathbb{C}^{n \times n}$ has n distinct roots $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$, then it is diagonalized by the Vandermonde matrix V of these values.*

Proof. Let us define the Vandermonde matrix V of $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ by:

$$V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_{n-1} \\ \alpha_0^2 & \alpha_1^2 & \cdots & \alpha_{n-1}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{n-1} & \alpha_1^{n-1} & \cdots & \alpha_{n-1}^{n-1} \end{pmatrix}$$

Let $\{x_0, x_1, \ldots, x_{n-1}\}$ be the set of row vectors of V^{-1}. Thus:

$$x_i \cdot (1, \alpha_j, \alpha_j^2, \ldots, \alpha_j^n)^T = \delta_{ij} \qquad (\dagger\dagger)$$

where δ_{ij} is the Kronecker delta. Recall the companion matrix R defined as:

$$R = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ r_0 & r_1 & r_2 & \cdots & r_{n-1} \end{pmatrix}$$

Consider the product $R \cdot V$. Since the characteristic polynomial $p(\lambda)$ of R is defined by $p(\lambda) = \det(\lambda I - R) = \lambda^n - r_{n-1}\lambda^{n-1} - \ldots - r_0$ then $r_0\alpha_j + r_1\alpha_j^2 + \cdots + r_{n-1}\alpha_j^{n-1} = \alpha_j^n$ iff $p(\alpha_j) = 0$. Thus if $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ are indeed latent roots of R, then:

$$RV = \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{n-1} \\ \alpha_0^2 & \alpha_1^2 & \cdots & \alpha_{n-1}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^n & \alpha_1^n & \cdots & \alpha_{n-1}^n \end{pmatrix}$$

Finally we must compute $V^{-1}R = [b_{ij}] \in \mathbb{C}^{n \times n}$. Element b_{ij} of $V^{-1}RV$ is given by $x_i \cdot y_j$ where x_i is the i'th row vector of V^{-1} and y_j is the j'th column vector of RV (i.e, $y_j = (\alpha_j, \alpha_j^2, \ldots, \alpha_j^n)^T$). From (††) on the previous page, we know that $x_i \cdot (1, \alpha_j, \alpha_j^2, \ldots, \alpha_j^n)^T = \delta_{ij}$ thus:

$$b_{ij} = x_i y_j = \sum_{k=0}^{n-1} (x_i)_k \alpha_j^{k+1} = \alpha_j \cdot \sum_{k=0}^{n-1} (x_i)_k \alpha_j^k = \alpha_j \cdot \delta_{ij},$$

and $[b_{ij}]$ is a diagonal matrix (due to the Kronecker delta) which is equal to $\alpha_0 \oplus \alpha_1 \oplus \cdots \oplus \alpha_{n-1}$ as required. □

It is now clear that in Theorem 6.10, T can be taken to be the Vandermonde matrix of the eigenvalues of R. Let $D = [b_{ij}] = \alpha_0 \oplus \alpha_1 \oplus \cdots \oplus \alpha_{n-1}$ be the diagonal matrix from the last theorem. Then $V^{-1}RV = D$ and thus $R = VDV^{-1}$.

In Theorem 6.3, we defined a matrix $X = S^{-1}RS$ and noted that the linear recurrent sequence had a zero iff there exists a particular $k > 0$ such that $X^k_{[1,1]} = 0$ with k a positive integer. Since $R = VDV^{-1}$ we can see that $X = S^{-1}VDV^{-1}S$ and that a zero in the linear recurrent sequence is present iff there exists a $k > 0$ such that $(S^{-1}VD^kV^{-1}S)_{[1,1]} = 0$.

In conclusion, we have shown that any instance of SKOLEM'S PROBLEM with a linear recurrent sequence of depth n can be reduced to an instance of THE MORTALITY PROBLEM with a pair of integral matrices of dimension $n \times n$. We have also shown a subclass of instances of SKOLEM'S PROBLEM which can be reduced to a form of exponential Diophantine equation problems where the coefficients are algebraic integers.

Chapter 7

Geometric Interpretations and Applications

In this section, we will move from an algebraic point of view to geometric interpretations of previously considered problems and in particular, new theorems concerning quaternion matrix semigroup problems. This leads to an interesting set of problems which we shall now outline.

Problem 7.1. POINT ROTATION PROBLEM *(PRP(n)) - Given points $x, y \in \mathbb{Q}^n$ on the unit $(n-1)$-sphere and a semigroup $\mathscr{S}$ of n-dimensional rotations. Does there exist $M \in \mathscr{S}$ such that M rotates x to y?*

In general, we can consider PRP(n) with a semigroup of n-dimensional rotation matrices (i.e., orthogonal matrices with determinant 1). In 3-dimensions, we may take $\mathscr{S}$ to be a semigroup of quaternions and define the rotation problem to be "Does there exist $q \in \mathscr{S}$ such that $qx'q^{-1} = y'$ where $x', y' \in \mathbb{H}(\mathbb{Q})_0$ are pure quaternions with imaginary components corresponding to the vectors x, y.

We shall show that the POINT ROTATION PROBLEM is *decidable* for 2-dimensions. Further, it is *undecidable* in 4-dimensions, and its decidability status is open in 3-dimensions.

Theorem 7.2. *The* POINT ROTATION PROBLEM, *PRP(2) is decidable.*

Proof. Points $x, y \in \mathbb{Q}^2$ where $x = (x_0, x_1), y = (y_0, y_1)$, can be represented instead as complex numbers $x', y' \in \mathbb{C}$. Using the exponential representation, let $x' = r_1 e^{i\theta_1}$ and $y' = r_2 e^{i\theta_2}$ where $r_1 = |x|$, $r_2 = |y|$, $\theta_1 = \arccos(\frac{x_1}{x_0})$ and $\theta_1 = \arccos(\frac{y_1}{y_0})$. We can convert all rotations of the semigroup in the same way to give a complex semigroup S^C. Now the problem becomes: "Does there exist $M \in S^C$ such that $Mx' = y'$?", but clearly $M = \frac{y'}{x'}$ and since S^C is commutative, membership is decidable [3], proving the result. □

We can define a standard scalar reachability problem in terms of quaternions:

Problem 7.3. QUATERNION SCALAR REACHABILITY PROBLEM *(QSRP(n)) - Given vectors $u, v \in \mathbb{H}(\mathbb{Q})^n$ a scalar $r \in \mathbb{H}(\mathbb{Q})$ and a semigroup of matrices $\mathcal{S} \subset \mathbb{H}(\mathbb{Q})^{n \times n}$. Does there exist $M \in \mathcal{S}$ such that $u^T M v = r$?*

Now we can prove that:

Theorem 7.4. *The* POINT ROTATION PROBLEM *PRP(3) is reducible to the* QUATERNION SCALAR REACHABILITY PROBLEM *QSRP(2).*

Proof. Since we are dealing with three-dimensional rotations, we can convert all elements of the PRP(3) instance to quaternions. Specifically, we define $x', y' \in \mathbb{H}(\mathbb{Q})_0$ to be pure quaternions with imaginary parts corresponding to x, y vectors respectively. We convert each three-dimensional rotation, R in $\mathcal{S}$ to an equivalent unit quaternion q such that the imaginary vector in $qx'q^{-1}$ is equivalent to Rx for example.

Each quaternion q in the PRP(3) is of unit length, therefore it is invertible and thus if $qxq^{-1} = y$ we may write $qx = yq$. Let $\mathcal{G} = \{q_0, q_1, \ldots, q_m\} =$

$\mathscr{S} \setminus \mathscr{S}^2$ be the generator of $\mathscr{S}$. Define $\alpha = (y, 1)$ and $\beta = (-1, x)^T$ and let $\mathscr{G}' = \{M_0, M_1, \ldots, M_m\}$ where

$$\mathscr{G}' = \left\{ M_i = \begin{pmatrix} q_i & 0 \\ 0 & q_i \end{pmatrix}; \quad 1 \leq i \leq m \right\}$$

and let $\mathscr{S}' = \langle \mathscr{G}' \rangle$ be a new semigroup.

Then $\exists M \in \mathscr{S}'$ such that $\alpha M \beta = 0$ iff $\exists q \in \mathscr{S}$ such that $qxq^{-1} = y$. To see this, note that $\alpha M \beta = qx - qy$ where $M = \begin{pmatrix} q & 0 \\ 0 & q \end{pmatrix}$ and

$$\begin{aligned} & qx - yq = 0 \\ \Rightarrow \quad & qx = yq \\ \Rightarrow \quad & qxq^{-1} = y \end{aligned}$$

as required. □

In fact we know that QSRP(2) is undecidable in general:

Theorem 7.5. *The* QUATERNION SCALAR REACHABILITY PROBLEM *is undecidable for a semigroup $\mathscr{S}$ generated by* 5 *two-dimensional diagonal quaternion matrices.*

Proof. Let $\gamma : \Sigma^* \mapsto \mathbb{H}(\mathbb{Q})$ be an injective homomorphism as defined previously. Let

$$\{(u_1, v_1), (u_2, v_2), \ldots, (u_n, v_n)\} \subset \Sigma^* \times \Sigma^*$$

be a Claus instance of PCP. Then we see that if

$$M_i = \begin{pmatrix} \gamma(u_i) & 0 \\ 0 & \gamma(v_i) \end{pmatrix} \quad ; 2 \leq i \leq n-1,$$

and $\alpha = (\gamma(u_1), \gamma(v_1))$, $\beta = (\gamma(u_n), -\gamma(v_n))^T$ and $r = 0$ then:

$$\alpha M_w \beta = \gamma(u_1 u_w u_n) - \gamma(v_1 v_w v_n) = 0 \Leftrightarrow u_1 u_w u_n = v_1 v_w v_n$$

where $M_w = M_{w_1} M_{w_2} \cdots M_{w_k}$ and $1 \leq w_i \leq n-1$ for each $1 \leq i \leq k$. Since there exists a Claus instance of PCP which is undecidable for $n = 7$ [28], the problem is undecidable for 5 matrices (since we have put the first and last elements inside the vectors α, β). □

But the decidability status of PRP(3) remains open (since the reduction is one way):

Open Problem 7.6. 3D Point Rotation Problem (PRP(3)) - *Given two points on the 2-sphere, $x, y \in \mathbb{Q}^3$, and a semigroup of rotations $\mathscr{S}$ generated by a finite set $\mathscr{G}$. Does there exist some rotation $R \in \mathscr{S}$ such that R rotates x to y?*

The rotation problem $PRP(3)$ is not only related to problems on quaternions but can also be reformulated as a 1-dimensional vector reachability problem for a semigroup or a group of rational linear functions over the complex field also known as Möbius transformations. In geometry, a Möbius transformation is a function, $f : \mathbb{C} \mapsto \mathbb{C}$ defined by:

$$f(z) = \frac{az+b}{cz+d},$$

where $z, a, b, c, d \in \mathbb{C}$ are complex numbers satisfying $ad - bc \neq 0$. Möbius transformations may be performed by taking a stereographic projection from a plane to a sphere, rotating and moving the sphere to a new arbitrary location and orientation, and making a stereographic projection back to the plane. Since there is a unique mapping between rotations of the 2-sphere and Möbius transformations, problem $PRP(3)$ is equivalent to the reachability problem of nondeterministic iterative maps: "Given a finite set M of one-dimensional linear rational functions over the complex field and two points x and y on the complex plane. Does there exist an algorithm to determine whether it is possible to map x to y by a finite sequence of linear rational functions from the set M?".

We next show that PRP(4) is undecidable.

Theorem 7.7. *The four-dimensional Point Rotation Problem (PRP(4)) is undecidable.*

Proof. The set of all unit quaternions forms a 3-dimensional sphere (3-sphere) and any pair of unit quaternions a and b can represent a rotation in 4D space. We can rotate a point $x = (x_1, x_2, x_3, x_4)$ on the 3-sphere, represented by a quaternion $q_x = (x_1, x_2, x_3, x_4)$, in the following way: aq_xb^{-1}.

Given a finite set of rotations, $\{(a_1, b_1), \ldots, (a_n, b_n)\}$, represented by pairs of quaternions. The question of whether a point x on the 3-sphere can be mapped to itself by the above set of rotations is equivalent to the problem whether there exists a non-empty sequence of indices $(r_1, \ldots, r_m)$ such that $a_{r_1} \cdots a_{r_m} q_x b_{r_m}^{-1} \cdots b_{r_1}^{-1} = q_x$.

If x is a point represented by quaternion $(1, 0, 0, 0)\mu$ the above equation only holds when $a_{r_1} a_{r_2} \cdots a_{r_m} = b_{r_1} b_{r_2} \cdots b_{r_m}$. According to Theorem 5.3 we have that the four-dimensional Point Rotation Problem is undecidable for 7 rotations. Moreover it is easy to see that PRP(4) is undecidable even for 5 rotations using the idea of Claus instances of PCP, see Section 3.2.1 and [28], where two of the rotations (the first and the last one) can be fixed and used only once. □

Corollary 7.8. *The vector reachability problem for* $n \times n$ *rational orthogonal matrix semigroups is decidable when* $n \leq 2$ *and undecidable for* $n \geq 4$ *with at least* 5 *matrices in the semigroup generator.*

It is not clear whether or not the membership for semigroups of rational quaternions is decidable and thus we pose the open problem:

Open Problem 7.9. QUATERNION MEMBERSHIP PROBLEM - *Given a semigroup of rational quaternions,* $\mathscr{S}$*, generated by a finite set* $\mathscr{G} \subset \mathbb{H}(\mathbb{Q})$*, is membership decidable for* $\mathscr{S}$*? I.e. can we decide if* $x \in \mathscr{S}$ *for any* $x \in \mathbb{H}(\mathbb{Q})$*?*

Another natural question to ask on finitely generated semigroups of rational quaternions concerns the decidability of the freeness of the semigroup:

Open Problem 7.10. QUATERNION FREENESS PROBLEM - *Given a semigroup of rational quaternions,* $\mathscr{S}$*, generated by a finite set* $\mathscr{G} \subset \mathbb{H}(\mathbb{Q})$*, is* $\mathscr{S}$

free? I.e., is it decidable to determine whether each element of $\mathscr{S}$ has a unique factorisation in terms of elements of $\mathscr{G}$?

Note that the Problem 7.10 can be formulated instead as a freeness problem on two-dimensional rational complex matrices since there exists an injective homomorphism between the two structures. Some decidable conditions on freeness for two-dimensional rational matrix semigroups were given in [17] but the case of complex matrices would appear to be more difficult.

It seems unlikely that the above two open problems would be undecidable since it would almost certainly imply we could simulate universal computation within a two-dimensional complex matrix semigroup. Since we know that two separate words cannot be stored and updated by standard multiplication in two-dimensional complex matrices by the results of [17], this makes it improbable that universality can be achieved; this is of course only a conjecture however.

Chapter 8

Conclusion

New Results

In this thesis we explored a wide range of computational decision problems on matrix semigroups. We were primarily concerned with the *computability* of such problems, i.e., we attempted to derive algorithms which solved the decision problems for a set of instances or prove that no such general algorithm could exist. In the introductory chapter we showed how matrices and matrix semigroups underlie many fields of mathematics and computer science and thus the decidability of problems on these structures can have wide ranging consequences in other fields. We do not simply show a set of undecidable membership problems, but instead try to study fundamental problems on semigroup structures themselves as we shall outline below.

We presented four distinct variants of "Post's correspondence problem (PCP)", two of which were our own and these allowed us to prove several undecidability results throughout the thesis. Specifically, we formulated and proved the undecidability of "Index Coding PCP" and "Fixed Element PCP". The definitions and proofs of these two variants are similar, however the different formulations were essential is the proofs of a set of results discussed below. We also presented the so called "Claus Instances" of PCP since they are perhaps not yet widely known, however we did not prove their undecidability within this thesis, see [20] and [28] for these proofs. We also gave a standard proof that PCP is undecidable.

The first undecidability proof given was that of membership for a scalar matrix in a finitely generated 4×4 integral matrix semigroup. We presented the results of this theorem in [5, 7] and showed the undecidability of the problem via an embedding of the Index Coding PCP. The problem seems both natural and fundamental since a scalar matrix has an obvious geometric meaning, that of scaling an object represented by a set of vectors, by a fixed amount. The problem would also appear to be connected to the long standing open problem called the identity matrix membership problem, see Open Problem 4.3. This problem asks whether the *identity matrix* is present in a finitely generated semigroup. The connection between the two problems seems strong but our technique unfortunately does not work in this specific case.

We then proved that the "Zero in the Upper Right Corner Problem" is undecidable for a semigroup generated by a pair of 18-dimensional integral matrices. This problem has appeared several times in the literature and we reduced the dimensions needed for undecidability using a new encoding technique. We presented this result in [6, 8].

Next we considered the problem of determining whether *any* matrix in a semigroup is diagonal. This appeared as an open problem in a recent book *"Unsolved Problems in Mathematical Systems and Control Theory"* [14] and we showed it's undecidability for 4×4 complex matrix semigroups by utilising the Fixed Element PCP in [9]. Diagonal matrices are extensively used in linear algebra and thus determining if any matrix in a semigroup is diagonal appears to be an important question, see also Open Problem 4.8.

We then study "Vector Reachability Problems" (VRP) on matrix semigroups. We show that the VRP on a semigroup generated by five rational 3×3 matrices is undecidable. Using the above mentioned Claus instances of PCP, we then show how this problem is in fact undecidable even for semigroups generated by just two rational matrices of dimension 11 in [6, 7]. The next result in this section concerns the "Vector Ambiguity Problem". This problem asks whether a set of vectors generated by left multiplication of a specific vector by elements of a semigroup is free. We show that the problem is undecidable for a finitely generated semigroup of three-dimensional rational, or four-dimensional integral, matrices in our paper [9].

Next we showed that there exists a specific *fixed* matrix semigroup such that determining whether a matrix is present in the semigroup is undecidable. This is an interesting result since usually the instance of the membership problem is both a specific matrix M and a set of matrices $\mathscr{G}$ comprising the generator of the semigroup. We show that even if the generator is fixed, we can still have an undecidable membership problem for varying single matrix M. This proof is achieved via an encoding of a universal Turing machine within a set of matrices.

We also study the so called "Recurrent Matrix Problem" which asks whether a specific matrix M has an infinite number of factorisations over elements of a generator $\mathscr{G}$. We ask the problem for an invertible matrix M, since the problem is not so interesting for a singular matrix (the problem is trivially undecidable from the proof of undecidability of the mortality problem). These results were also from our recent paper [9].

The testing for emptiness of the intersection of two semigroups of matrices of the same size was studied by A. Markov in 1947 where he showed the problem is undecidable for four-dimensional unimodular non-negative matrices [42]. This result was improved by V. Halava and T. Harju to semigroups in three-dimensional integral non-singular matrix semigroups. We prove a slight improvement of this result where we obtain the result for three-dimensional integral non-singular upper-triangular non-negative matrices by using a different embedding of words into matrices. We also show that the problem remains undecidable for three dimensions when the matrices of the generator are unimodular, non-negative and upper-triangular although this result is over rational numbers rather than integers [4].

The next chapter of the thesis deals with computational decision problems on quaternion and quaternion matrix semigroups. This is a relatively unexplored area and we gave a solid justification as to its study in the introduction. This mainly stems from the fact that the quaternions are a superset of the complex numbers (they are so called hypercomplex numbers) which still retain the property of associativity (although they lose commutativity). The next number system in the Cayley-Dickson construction are the 8-dimensional octonions which in fact lose the associativity property. Since associativity is required by definition in semigroups, the quaternions are the most abstract number system we may reasonably use in such computational problems. Furthermore, the quaternions have a natural geometrical interpretation and thus we can derive many corollaries from the algebraic results we obtain on quaternion semigroup problems.

We prove that most problems are undecidable for quaternion matrix semigroups in dimension two. Specifically we show that membership, vector reachability and freeness are all undecidable. We also show semigroup intersection problems are undecidable for dimension 1 and 2 depending upon the definition. Determining whether any matrix in a finitely generated two-dimensional quaternion matrix semigroup is diagonal is also shown to be undecidable. This is in contrast to the same problem being shown to be undecidable over four-dimensional complex matrix semigroups. It should be noted that we are required to use completely different proofs for these two results, one does not follow as a corollary of the other result. We leave Open Problem 4.8 unresolved, which is the determination as to whether any matrix in an *integral* matrix semigroup is diagonal.

We show that membership is decidable for a semigroup of *Lipschitz integers* (quaternions with integral components) although we also show semigroup intersection emptiness problems over Lipschitz integers is undecidable.

All of the quaternion matrix semigroup results were presented in [10].

Skolem's problem (or Pisot's problem) is the decidability status of the algorithmic determination as to whether or not a given linear recurrent sequence has a zero. We showed a reduction of this problem to the mortality problem for a pair of integral matrices and an equivalence with exponential Diophantine equations in a restricted subclass of instances of the problem.

Finally we examined computational problems from a geometric perspective. Since quaternions have a geometric meaning, the study of computational problems on them gives rise to many naturally defined questions from a real world physical perspective which could have a wide range of applicability in different fields. We mainly study *rotation problems*; given two specific points x, y and a finitely generated semigroup of rotations, is it possible to find a rotation mapping x to y? In three dimensions this problem can be defined on a robotic arm for example. If the arm can only rotate in a certain number of ways, can we move the arm to a specific point? The problems are also interesting from a purely theoretical point of view since they are reachability problems on algebraic structures as we examine throughout the thesis.

Open Problems

There is much more work to be carried out in this area, and indeed there exists a number of open problems within the field, some of which we have highlighted throughout the thesis. Clearly defining the boundary between decidable and undecidable problems is worthwhile since it can indicate the necessary conditions for undecidability to be present and help us to understand computability theory to a greater extent.

Some problems appear to be of a more fundamental nature, such as determining whether the identity element is present within a semigroup. This is because the presence of the identity matrix has many implications for other problems. If a product of elements equals the identity element, then each element of the product has a multiplicative inverse and it allows us to determine if a given generator set forms a group rather than just a semigroup; therefore if the membership problem for the identity matrix is decidable, so is determining if the semigroup is a group for example.

We shall now collect together and discuss the complete list of open problems present within this thesis which are all concerned with the decidability status of decision problems.

Open Problem 4.3 IDENTITY MATRIX MEMBERSHIP PROBLEM - Given a finitely generated matrix semigroup $\mathscr{S}$, does the identity matrix I belong to $\mathscr{S}$?

This seems to be a very important problem and despite extensive study by several researchers, it remains unsolved. The problem seems superficially related to the scalar matrix reachability problem which was shown to be undecidable in Theorem 4.1 which is concerned with the membership problem for a scalar matrix of the form kI where $|k| > 1$ and I is the multiplicative identity matrix. However, the property that k must be non-unit appears intrinsic to the use of the "Index Coding PCP", since we must ensure a specific matrix in the semigroup is used only once when we obtain a product corresponding to a correct PCP solution. Despite many attempts we cannot use this technique for proving a similar result on the identity matrix.

Open Problem 4.8 ANY DIAGONAL MATRIX - Given a finite set of *integral* matrices $\mathscr{G}$ generating a semigroup $\mathscr{S}$. Does there exist any matrix $D \in \mathscr{S}$ such that D is a diagonal matrix?

The problem was posed in [14] and the authors there considered a case for three-dimensional integral matrices which does not quite work. We showed the problem to be undecidable in two-dimensions over quaternions matrices in Theorem 5.7 and over four-dimensional rational complex matrix semigroups in Theorem 4.7. Thus the problem remains open for integral matrices over any dimension.

Open Problem 6.1 SKOLEM'S PROBLEM - Given a linear recurrent sequence $(u_0, u_1, u_2, \ldots) \in \mathbb{Z}^{\mathbb{N}}$, does there exist some value $k \geq 0$ such that $u_k = 0$?

This is a very famous open problem and has been extensively studied. We showed a reduction of the problem to the mortality problem for a pair of integral matrices and a subcase where the problem is reducible to an exponential Diophantine equation but the decidability of the problem itself, of course, remains open. The problem is decidable for linear recurrences of size 5 [29].

Open Problem 6.6 The 2×2 MORTALITY PROBLEM - Is the mortality problem decidable for a semigroup generated by a finite set of 2×2 rational matrices?

This open problem first appeared in [48] in a slightly different form. The problem is known to be decidable when we have a semigroup generated by a *pair* of 2×2 rational matrices, see [16], but the decidability for an arbitrary number of matrices in the generator is unknown. It is an important open problem since it is related to the controllability of a switched linear system and has been studied several times, see also [34] and [35].

Open Problem 7.6 3D POINT ROTATION PROBLEM (PRP(3)) - Given two points on the 2-sphere, $x, y \in \mathbb{Q}^3$, and a semigroup of rotations $\mathcal{S}$ generated by a finite set $\mathcal{G}$. Does there exist some rotation $R \in \mathcal{S}$ such that R rotates x to y?

This problem is similar to Problem 7.9 below, but the two problems are not exactly the same and since this problem is of a strictly geometric nature, its solvability might have an impact in the real world since it deals with 3-dimensional space. The decidability status of the problem might also have an impact on more general algebraic questions on quaternion semigroups.

Open Problem 7.9 QUATERNION MEMBERSHIP PROBLEM - Given a semigroup of rational quaternions, $\mathscr{S}$, generated by a finite set $\mathscr{G} \subset \mathbb{H}(\mathbb{Q})$, is membership decidable for $\mathscr{S}$? I.e. can we decide if $x \in \mathscr{S}$ for any $x \in \mathbb{H}(\mathbb{Q})$?

Since a single rational quaternion may be represented by a two-dimensional rational quaternion matrix, this problem is a restricted form of the decidability of membership for 2×2 complex matrix semigroups. It is known that a pair of words cannot be stored in such a semigroup where standard matrix multiplication is the binary operator, see [17]. The problem posed has additional constraints, thus is would seem unlikely that it would be undecidable but we do not know of a decision procedure for it.

Open Problem 7.10 QUATERNION FREENESS PROBLEM - Given a semigroup of rational quaternions, $\mathscr{S}$, generated by a finite set $\mathscr{G} \subset \mathbb{H}(\mathbb{Q})$, is it algorithmically decidable whether $\mathscr{S}$ is free? I.e. is it decidable whether each element of $\mathscr{S}$ has a unique factorisation in terms of elements of $\mathscr{G}$?

This is another problem which naturally arose from our study of quaternion matrix semigroup problems. Freeness problems for 2×2 matrix semigroups were recently studied in [17] but even for upper triangular integral matrices the problem appears difficult and only some restricted subclasses are known which are decidable. However, since the quaternions have a different form, perhaps the problem can be tackled with a new technique.

Bibliography

[1] J.P. Allouche and J. Shallit. *Automatic Sequences: Theory, Applications, Generalizations.* Cambridge University Press, 2003.

[2] Y. H. Au-Yeung. On the eigenvalues and numerical range of a quaternionic matrix. Preprint, 1994.

[3] L. Babai, R. Beals, J. Cai, G. Ivanyos, and E. M. Luks. Multiplicative equations over commuting matrices. In *Proc. 7th ACM-SIAM Symp. on Discrete Algorithms (SODA '96)*, 1996.

[4] P. Bell. A note on the emptiness of semigroup intersections. *Fundamenta Informaticae*, 79:1–4, 2007.

[5] P. Bell and I. Potapov. On the membership of invertible diagonal matrices. In *Developments in Language Theory*, volume LNCS 3572, pages 146–157, 2005.

[6] P. Bell and I. Potapov. Lowering undecidability bounds for decision questions in matrices. In *Developments in Language Theory*, volume LNCS 4036, pages 375–385, 2006.

[7] P. Bell and I. Potapov. On the membership of invertible diagonal and scalar matrices. *Theoretical Computer Science*, 372:37–45, 2007.

[8] P. Bell and I. Potapov. On undecidability bounds for matrix decision problems. *Special Issue of Theoretical Computer Science*, (accepted for publication), 2007.

[9] P. Bell and I. Potapov. Periodic and infinite traces in matrix semigroups. Technical report, The University of Liverpool, 2007.

[10] P. Bell and I. Potapov. Reachability problems in quaternion matrix and rotation semigroups. In *Mathematical Foundations of Computer Science (MFCS 2007) (accepted)*, 2007.

[11] M. Berger and Y. Wang. Bounded semigroups of matrices. *Linear Algebra and its Applications*, 166:21–27, 1992.

[12] V. Blondel, J. Cassaigne, and C. Nichitiu. On the presence of periodic configurations in Turing machines and in counter machines. *Theoretical Computer Science*, 289:573–590, 2002.

[13] V. Blondel, E. Jeandel, P. Koiran, and N. Portier. Decidable and undecidable problems about quantum automata. *SIAM Journal on Computing*, 36:4:1464–1473, 2005.

[14] V. Blondel and A. Megretski. *Unsolved Problems in Mathematical Systems and Control Theory.* Princeton University Press, 2004.

[15] V. Blondel and J. Tsitsiklis. The boundedness of all products of a pair of matrices is undecidable. *Systems and Control Letters*, 41:2:135–140, 2000.

[16] O. Bournez and M. Branicky. The mortality problem for matrices of low dimensions. *Theory of Computing Systems*, 35:433–448, 2002.

[17] J. Cassaigne, T. Harju, and J. Karhumäki. On the undecidability of freeness of matrix semigroups. *International Journal of Algebra and Computation*, 9(3-4):295–305, 1999.

[18] J. Cassaigne and J. Karhumäki. Examples of undecidable problems for 2-generator matrix semigroups. *Theoretical Computer Science*, 204(1-2):29–34, 1998.

[19] C. Choffrut and J. Karhumäki. Some decision problems on integer matrices. *Theoretical Informatics and Applications*, 39:125–131, 2005.

[20] V. Claus. Some remarks on PCP(k) and related problems. *Bulletin of the EATCS*, 12:54–61, 1980.

[21] F. D'Allesandro. Free groups of quaternions. *International Journal of Algebra & Computation (IJAC)*, 14(1):69–86, 2004.

[22] A. Ehrenfeucht, J. Karhumäki, and G. Rozenberg. The (generalized) Post correspondence problem with lists consisting of two words is undecidable. *Theoretical Computer Science*, 21(2):119–144, 1982.

[23] S. Gaubert and R. Katz. Reachability problems for products of matrices in semirings. *International Journal of Algebra & Computation (IJAC)*, 16(3):603–627, 2006.

[24] V. Halava. Decidable and undecidable problems in matrix theory. Technical Report 127, Turku University, 1997.

[25] V. Halava and T. Harju. Mortality in matrix semigroups. *Amer. Math. Monthly*, 108:649–653, 2001.

[26] V. Halava and T. Harju. On Markov's undecidability theorem for integer matrices. Technical Report 758, Turku University, 2006.

[27] V. Halava and T. Harju. Undecidability of infinite Post correspondence problem for instances of size 9. *Theoretical Informatics and Applications*, 40:551–557, 2006.

[28] V. Halava, T. Harju, and M. Hirvensalo. Undecidability bounds for integer matrices using Claus instances. Technical Report 766, Turku University, 2006.

[29] V. Halava, T. Harju, M. Hirvensalo, and J. Karhumäki. Skolem's problem - on the border between decidability and undecidability. Technical Report 683, Turku University, 2005.

[30] V. Halava, T.Harju, and M. Hirvensalo. Positivity of second order linear recurrent sequences. *Discrete Applied Mathematics*, 154:447–451, 2006.

[31] R. A. Horn and C. R. Johnson. *Matrix Analysis*. Cambridge University Press, 1985.

[32] R. A. Horn and C. R. Johnson. *Topics in Matrix Analysis*. Cambridge University Press, 1991.

[33] I. Korec. Small universal register machines. *Theoretical Computer Science*, 168:267–301, 1996.

[34] M. Krom and M. Krom. Recursive solvability of problems with matrices. *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, 35(5):437–442, 1989.

[35] M. Krom and M. Krom. More on mortality. *American Mathematical Monthly*, 97(1):37–38, 1990.

[36] G. Kucherov and M. Rusinowitch. Undecidability of ground reducibility for word rewriting systems with variables. *Information Processing Letters (IPL)*, 53:209–215, 1995.

[37] O. Kurganskyy and I. Potapov. Computation in one-dimensional piecewise maps and planar pseudo-billiard systems. In *Unconventional Computation*, pages 169–175, 2005.

[38] E. Lengyel. *Mathematics for 3D Game Programming & Computer Graphics*. Charles River Media, 2004.

[39] A. Lisitsa and I. Potapov. Membership and reachability problems for row-monomial transformations. In *Mathematical Foundations of Computer Science*, 2004.

[40] A. Lisitsa and I. Potapov. In time alone: On the computational power of querying the history. In *TIME 06*, pages 42–49, 2006.

[41] A. Mandel and I. Simon. On finite semigroups of matrices. *Theoretical Computer Science*, 5:101–111, 1977.

[42] A. Markov. On certain insoluble problems concerning matrices. *Doklady Akad. Nauk SSSR*, 57:539–542, 1947.

[43] Y. Matiyasevich and G. Sénizergues. Decision problems for semi-Thue systems with a few rules. *Theoretical Computer Science*, 330:145–169, 2005.

[44] M. Minsky. *Computation: Finite and Infinite Machines.* Prentice Hall International, 1967.

[45] M. Paterson. Unsolvability in 3 × 3 matrices. *Studies in Applied Mathematics*, 49:105–107, 1970.

[46] E. Post. A variant of a recursively unsolvable problem. *Bulletin of the American Mathematical Society*, 52:264–268, 1946.

[47] I. Potapov. From Post systems to the reachability problems for matrix semigroups and multicounter automata. In *Developments in Language Theory*, volume LNCS 3340, pages 345–356, 2004.

[48] P. Schultz. Mortality of 2×2 matrices. *American Mathematical Monthly*, 84(2):463–464, 1977.

[49] M. Sipser. *Introduction to the Theory of Computation.* PWS Publishing Company, 1997.

[50] W. So, R. C. Thomson, and F. Zhang. Numerical ranges of matrices with quaternion entries. *Linear and Multilinear Algebra*, 37:175–195, 1994.

[51] S. Swierczkowski. A class of free rotation groups. *Indagationes Mathematicae*, 5(2):221–226, 1994.

[52] J. Theys. *Joint Spectral Radius: Theory and Approximations.* PhD thesis, Universitè catholique de Louvain, May 2005.

[53] D. Velichova and S. Zacharias. Projection from 4D to 3D. *Journal for Geometry and Graphics*, 4(1):55–69, 2000.

[54] N. A. Wiegmann. Some theorems on matrices with real quaternion elements. *Canadian Journal of Mathematics*, 7:191–201, 1955.

[55] F. Zhang. Quaternions and matrices of quaternions. *Linear Algebra and its Applications*, 251:21–57, 1997.

Index