Testing Simultaneous Similarity of Matrices and Related Problems for Matrix Semigroups

Mitsunori Ogihara*  Yechezkel Zalcstein†
Department of Computer Science  College of Computing
University of Rochester  Georgia Institute of Technology

Abstract

This paper studies the problem of testing simultaneous similarity of matrices and related problems about matrix semigroups. Along with Simultaneous Similarity this paper studies two problems: Nonsingular Nullspace and Nonsingular Basis Combination. These two problems are very similar to Simultaneous Similarity and Simultaneous Similarity is reducible to each of these two.

This paper also studies problems about matrix semigroups. Among other results, it shows that (i) for any field Matrix Semigroup Intersection is PSPACE-complete, (ii) for any finite field Matrix Semigroup Membership, Matrix Semigroup Equality, and Matrix Semigroup Isomorphism are all PSPACE-complete, (iii) for each inverse matrix semigroup over a field of characteristics zero, Matrix Semigroup Membership is PSPACE-complete, and (iv) for any field, Matrix Aperiodicity for inverse semigroups is PSPACE-complete.

Keywords: Simultaneous Similarity, Matrix Semigroups, Complexity, RNC, Algebra

1 Introduction

Square matrices $A$ and $B$ of the same dimension are said to be similar if there exists an invertible matrix $Q$ such that $AQ = QB$. Similarity—the problem of testing matrix similarity—is fundamental in linear algebra and has been settled in the 19th century via the rational and Jordan canonical forms. Byrnes and Gauger [BG77] found a simpler, direct test for Similarity based on the rank of matrices and Zalcstein and Garzon [ZG89] observed that the Byrnes–Gauger Test leads to an $NC^2$ algorithm. The algorithm of Zalcstein and Garzon uses the fact that matrix rank

---

*Address: BOX 270226, Department of Computer Science, University of Rochester, Rochester, NY 14627-0226. email: ogihara@cs.rochester.edu. Supported in part by NSF grants CCR-9701911, CCR-9725021, DUE-9980943, INT-9726724, NIH grants RO1-AG18231 and P30-AG18254, an Alzheimer's Association Grant PIO-1999-1519, and a DARPA grant F30602-98-2-0133

†Address: College of Computing, Georgia Institute of Technology, Atlanta, GA 30332. email: zzalcste@cc.gatech.edu. 
is in NC² [Mul87]. There is more recent development in the study of the complexity of matrix similarity testing. Santha and Tan [ST98] show that Similarity over the field of rational numbers is in AC⁰(C=L), i.e. the closure of C=L under the logspace-uniform AC⁰-reducibility. The class C=L is the logspace “exact counting” class defined by Allender and Ogihara [AO96]. Allender and Ogihara [AO96] show that C=L ⊆ TC¹ and it is well-known that TC¹ ⊆ NC². So, the Santha–Tan result in light of the observation of Allender and Ogihara offers an alternative proof of the Zalestein–Garzon Theorem. Actually, the exact complexity-theoretic characterization of the problem has been known. Allender, Beals, and Ogihara [ABO099] show that verifying the rank of a matrix is complete for the second level of the boolean hierarchy [CGH⁺88] over C=L, both over the integers and over the field of rational numbers. They also show that the class AC⁰(C=L) is equal to the logspace disjunctive truth-table reducibility closure of the second level of the boolean hierarchy over C=L. Based on this characterization, Hoang and Thierauf [HT00] show that Similarity is logspace many-one complete for the class AC⁰(C=L) both over the ring of integers and the field the rational numbers.

A problem closely related to Similarity is Simultaneous Similarity, where the question is to test, given pairs of matrices, (A₁, B₁), . . . , (Aₘ, Bₘ) of the same dimension, whether there is an invertible matrix Q such that for all i, 1 ≤ i ≤ m, it holds that AᵢQ = QBᵢ. In sharp contrast with Similarity, not much is known about the complexity of this problem. The mathematical problem of simultaneous similarity has remained open for many decades. The first solution to the problem was given by Friedland [Fri83] in 1983. Friedland’s paper is very complicated and uses sophisticated mathematical tools. A simpler solution of Friedland’s algorithm has been published in 1999 by Dias da Silva and Laffey [DL99]. However, none of these papers yield an efficient algorithm. A 1981 paper of Grigoriev [Gri81] observes that the problem is in NP and asked whether there is a polynomial-time algorithm.

A goal of this paper is to study the complexity of Simultaneous Similarity. Although we are unable to obtain the exact characterization of the problem, we observe that the problem is solvable in logspace-uniform randomized-TC¹, and thus, in the nonuniform-TC¹ over the field of rational numbers. It is unknown whether such a result hold for finite fields. This motivates us to study problems related to Simultaneous Similarity. To prove that Simultaneous Similarity over the field of rational numbers is in the nonuniform-TC¹, we observe that for every field F simultaneous similarity over F is NC¹₀,F-reducible to Nonsingular Nullspace—the problem of testing, given an m × d² matrix S for some integers d and m, whether the nullspace defined by S contains a vector such that the rearrangement of the vector elements into a d × d matrix is a nonsingular matrix—and that Nonsingular Nullspace is in nonuniform-TC¹ both over the field of rational numbers. Interestingly, over any finite field Nonsingular Nullspace is an NP-complete problem.

We also study complexity of semigroup problems. Most basic questions about matrix semigroups turn out to be PSPACE-hard. Over a finite field we can show that those problems are in PSPACE,
but over a field of characteristic zero, it is still open whether the membership problem for finite semigroups is in \( \text{PSPACE} \). We show that the membership problem for inverse semigroups over the rational numbers is in \( \text{PSPACE} \), where a semigroup \( S \) is an inverse semigroup if every element \( x \) in \( S \) has a pseudo-inverse \( x' \) such that \( xx'x = x \) and \( x'xx' = x' \). Birget et al. [BMMW00] have shown that the membership problem for inverse semigroups is \( \text{PSPACE} \)-hard and hence it follows that it is \( \text{PSPACE} \)-complete. We show several other problems about inverse matrix semigroups are \( \text{PSPACE} \)-complete. An exception is the finiteness problem. For groups, the problem has been shown recently to be in \( \text{P} \) [BBR]. Ivanyos [Iva00] has developed a polynomial-time algorithm for matrix semigroups over fields that are finite transcendental extensions of finite fields. Over a field of characteristic zero, the problem is much harder. We can show that for inverse semigroups over the rational numbers the problem is in \( \text{PSPACE} \), but there is no known lower bound.

### 2 Preliminaries

\( \mathbb{Z}, \mathbb{N}, \) and \( \mathbb{Q} \) respectively denote the set of all integers, the set of all nonnegative integers, and the field of all rational numbers. Let \( F \) be a field. Let \( n \) and \( m \) be positive integers. \( F^{n \times m} \) denotes the set of all \( n \times m \) matrices over \( F \).

Let \( m \geq 1 \) be an integer. Let \( d_1, \ldots, d_m \) be a sequence of positive integers. Let \( A_1, \ldots, A_m \) be a sequence of square matrices such that for all \( i, 1 \leq i \leq m, A_i \) is of dimension \( d_i \). Then \( \text{DIAG}(A_1, \ldots, A_m) \) denotes the block-diagonal matrix of dimension \( d_1 + \cdots + d_m \) constructed by putting \( A_1, \ldots, A_m \) diagonally from upper left corner to the bottom right corner in this order.

Let \( m \) and \( d \) be positive integers. Let \( A_1, \ldots, A_m \) be square matrices, each of dimension \( d \). Then, the semigroup generated by \( A_1, \ldots, A_m \), denoted by \( S(A_1, \ldots, A_m) \), is the set of all matrices \( M \) of dimension \( d \) that are products of finitely many matrices (with multiplicity) chosen from \( A_1, \ldots, A_m \).

We are interested in two computational models: the multi-tape Turing machine and the arithmetic circuit. For the arithmetic circuit model, we use the logspace uniformity as our uniformity condition. We assume that the reader is familiar with standard complexity classes in these models. We are particularly interested in such classes as \( \text{NP} \), \( \text{PSPACE} \), \( \text{NC} \), and \( \text{TC} \). For each \( k \geq 0 \), \( \text{NC}^k \) is the class of functions computed by a family of polynomial-size, \( O(\log^k n) \)-depth bounded-fan-in circuits and \( \text{TC}^k \) is the class of functions computed by a family of polynomial-size, \( O(\log^k n) \)-depth unbounded-fan-in circuits with majority gates, where a majority gate takes \( \{0,1\} \) inputs and checks whether at least a half of its inputs is a 1. Then \( \text{NC} = \bigcup_{k \geq 0} \text{NC}^k \) and \( \text{TC} = \bigcup_{k \geq 0} \text{TC}^k \). The reader unfamiliar with these complexity classes may consult [Pap94]. These models may or may not be augmented by a unit-cost subroutine for the field operations. For a field \( F \) and a complexity class \( \mathcal{C} \), by \( \mathcal{C}_F \) we denote the class \( \mathcal{C} \) augmented by such a unit-cost subroutine. Augmentation by such a subroutine does not create an issue so long as the field is finite. In the case when the field is infinite, in particular, when the field is \( \mathbb{Q} \), it may make sense to assume that the field elements are
encoded in binary and there is no unit-cost subroutine for the field operation. So, we will state some of our results in a generic form without distinguishing between finite fields and infinite fields and clarify what the implications of the results are in the case when the fields are infinite.

Now we define the problems of our interest. **Simultaneous Similarity** over a field $F$ is the problem of deciding, given integers $n, r \geq 1$ and matrices $A_1, \ldots, A_r, B_1, \ldots, B_r \in R^{n \times n}$, whether a nonsingular matrix $Q \in R^{n \times n}$ exists such that for all $i, 1 \leq i \leq r$, it holds that $A_i Q = Q B_i$. **Nonsingular Nullspace** over a field $F$ is the problem of deciding, given integers $m, n \geq 1$ and $T \in T^{m \times n}$, whether an $n^2$-dimensional vector $Q$ over $F$ exists such that $T Q = 0$ holds when $Q$ is viewed as a vector and $\det(Q) \neq 0$ when $Q$ is viewed as an $n \times n$ matrix. **Nonsingular Basis Combination** over a field $F$ is the problem of deciding, given integers $m, n \geq 1$ and $Q_1, \ldots, Q_m \in R^{n \times n}$, whether some $x_1, \ldots, x_m \in R$ exist such that $\det(x_1 Q_1 + \cdots + x_m Q_m) \neq 0$. **Matrix Semigroup Membership** over a field $F$ is the problem of testing membership in a finitely generated semigroup over $F$. **Matrix Semigroup Equality** is the problem of testing equality between two finitely generated semigroups over $F$. **Matrix Semigroup Intersection** over a field $F$ is the problem of testing whether two finitely generated semigroups over $F$ have a common element that is not totally zero. **Matrix Semigroup Isomorphism** over a field $F$ is the problem of testing whether two finitely generated semigroups over $F$ are isomorphic. A finite semigroup $S$ is called **aperiodic** if, for every element $s \in S$, there is a nonnegative integer $n(s)$ such that $s^{n(s)} = s^n$. **Matrix Semigroup Aperiodicity** over a field $F$ is the problem of testing whether a finitely generated semigroup over $F$ is aperiodic. **Matrix Semigroup Finiteness** over a field $F$ is the problem of testing whether a finitely generated semigroup over $F$ is finite.

## 3 Complexity of Simultaneous Similarity

In this section we study the complexity of **Simultaneous Similarity** and related problems.

**Theorem 3.1** Let $F$ be a field. Simultaneous Similarity over $F$ is many-one reducible to Nonsingular Nullspace over $F$ via a function that is computable in $\text{NC}^0_F$. Nonsingular Nullspace over $F$ is many-one reducible to Nonsingular Basis Combination over $F$ via a function that is computable in $\text{AC}^0_F$, with parallel access to both $\text{rank}_F$ and $\text{det}_F$.

**Proof.** Let $n, k \geq 1$ be integers. Let $F$ be a field. Let $I = (n, k, A_1, \ldots, A_k, B_1, \ldots, B_r)$ be an input to Simultaneous Similarity, where $A_1, \ldots, A_k, B_1, \ldots, B_r \in F^{n \times n}$. We need to test whether there is a nonsingular $Q \in F^{n \times n}$ such that for all $i, 1 \leq i \leq k$, it holds that $A_i Q - Q B_i = 0$. By viewing $Q$ as a vector of $n^2$ unknowns, the condition

$$(\forall i \in \{1, \ldots, j\})[A_i Q - Q B_i = 0]$$

can be viewed as a system of linear equations $\Xi$

$$\Xi : T Q = 0,$$

4
where $T$ is a $kn^2 \times n^2$ matrix. For all integers $t$, $i$, and $j$, such that $1 \leq t \leq k$ and $1 \leq i, j \leq n$, let $a_{ij}^{(t)}$ denote the $(ij)$-th entry of $A_t$ and $b_{ij}^{(t)}$ denote the $(ij)$-th entry of $B_t$. The system $\Xi$ consists of the equations, $E(t, j, j), 1 \leq t \leq k$ and $1 \leq i, j \leq n$, defined as follows:

$$(a_{ij}^{(t)} q_{ij} + \cdots a_{in}^{(t)} q_{nj}) - (b_{ij}^{(t)} q_{ii} + \cdots b_{nj}^{(t)} q_{in}) = 0$$

The unknowns in the first term and those in the second have only one term in common, namely $q_{ii}$, so the coefficients of $E(t, i, j)$ can be calculated by one subtraction. This implies that **Simultaneous Similarity** is $\text{NC}^0_F$-reducible to **Nonsingular Nullspace**.

Let $\Xi = (k, n, T)$ be an input to **Nonsingular Nullspace**, where $T$ is of dimension $k \times n^2$. Let $\Xi$ be the system of linear equations given by $T$, namely the collection of all $n^2$-dimensional vectors $Q$ such that $TQ = 0$. Let $Q_1, \ldots, Q_m$ be the basis of $T$. Then each solution $Q$ of $\Xi$ is a linear combination of the basis elements. So there exists a solution $Q$ of $\Xi$ that is a nonsingular matrix if and only if there exist $x_1, \ldots, x_m \in F$ such that $\text{det}(x_1 Q_1 + \cdots + x_m Q_m) \neq 0$.

It is known that the basis can be computed in $\text{NC}^1$ with a constant number of rounds of parallel access to the rank function (see [Gat93, Theorem 13.9]). Let $\rho$ denote the rank of $T$. Then the cardinality $m$ of the basis is $n^2 - \rho$. For each $i$, $1 \leq i \leq k$, let $r_i$ be the rank of the submatrix of $T$ consisting of the first $i$ rows. Also, for each $j$, $1 \leq j \leq n^2$, let $s_j$ be the rank of the submatrix of $T$ consisting of the first $j$ columns. Let $r_0 = 0$ and let $I = \{i \mid 1 \leq i \leq k \land r_i = r_{i-1} + 1\}$. Also, let $s_0 = 0$ and let $J = \{j \mid 1 \leq j \leq n^2 \land s_j = s_{j-1} + 1\}$. Then $\|I\| = \|J\| = \rho$. Let $T_0$ be the $\rho \times n^2$ submatrix of $T$ consisting of the rows $I$ and $\hat{T}$ be the $\rho \times \rho$ submatrix of $T$ consisting of the rows $I$ and the columns $J$. Let $j_1, \ldots, j_p$ be the enumeration of all members of $J$ in increasing order and let $p_1, \ldots, p_m$ be the enumeration of all members of $\{1, \ldots, n^2\} - J$ in increasing order. For each $\ell$, $1 \leq \ell \leq m$, let $y_\ell$ be the $p_\ell$-th column of $T_0$. For each $\ell$, $1 \leq \ell \leq m$, let $w_\ell$ be the $n^2$-dimensional vector defined as follows:

- For each $h$, $1 \leq h \leq \rho$, the $j_h$-th entry of $w_\ell$ is the $h$-th entry of $\hat{T}^{-1}y_\ell$.
- The $p_\ell$-th entry of $w_\ell$ is $-1$.
- All the other entries of $w_\ell$ is 0.

Then $w_1, \ldots, w_m$ form a basis.

The above construction gives a many-one reduction from **Nonsingular Nullspace** to **Nonsingular Basis Combination**. To compute the reduction, the rank of each submatrix of $T$ needs to be calculated, which can be carried out by one-round parallel queries to $\text{rank}_F$. Then the sets of indices, $I$ and $J$, need to be calculate, but this requires only $\text{AC}^1$ computation since all the rank values have been computed. Then inverting $\hat{T}$ can be done by one parallel queries to $\text{det}_F$ and parallel field division. Finally, the basis elements can be computed by matrix multiplication, which is in $\text{AC}^0_F$. Thus, the reduction is computable in $\text{AC}^0_F$ with parallel access to $\text{rank}_F$ and $\text{det}_F$. □
Theorem 3.2 Over the field of rational numbers, \( Q \), SIMULTANEOUS SIMILARITY, NONSINGULAR NULLSPACE, and NONSINGULAR BASIS COMBINATION belong to logspace-uniform randomized-TC\(^1\), and thus, belong to nonuniform-TC\(^1\).

Proof. Let \( \ell \geq 1 \) be an integer. Let \( \mathcal{I} = (m, n, Q_1, \ldots, Q_m) \) be an input to NONSINGULAR BASIS COMBINATION over \( Q \) such that \( |\mathcal{I}| = \ell \), where where \( Q_1, \ldots, Q_m \in F^{n \times n} \). Obviously, \( m, n \leq \ell \). Consider the following algorithm \( \mathcal{A} \):

- Sample \( m \) integers \( c_1, \ldots, c_m \) from the set \( S = \{1, 2, \ldots, 2^{\lceil \log n \rceil + 1}\} \) independently and uniformly at random.
- Compute as \( D \) the determinant of \( c_1 Q_1 + \cdots + c_m Q_m \).
- Accept if \( D \neq 0 \) and reject otherwise.

Let \( x_1, \ldots, x_m \) be indeterminates. Then the determinant of \( x_1 Q_1 + \cdots + x_m Q_m \) is a polynomial in \( x_1, \ldots, x_m \) of degree \( n \). Let \( g \) be that polynomial. If \( g \) is the zero polynomial, then \( \mathcal{A} \) never accepts. If \( g \) is not the zero polynomial, then the number of roots of \( g \) that belong to \( S^m \) is at most \( n\|S\|^{m-1} \) (see [DL78]). Since \( \|S\| \geq 2n \), the probability that \( D \neq 0 \) is at least \( 1/2 \) if \( g \) is not the zero polynomial. So, \( \mathcal{A} \) errs on only positive inputs and has error probability at most \( 1/2 \). The determinant over \( Q \) is known to be in \( \text{C}_\text{=} \text{L} \) [AO96], and \( \text{C}_\text{=} \text{L} \) is a subclass of logspace-uniform TC\(^1\), so NONSINGULAR BASIS COMBINATION is in logspace-uniform randomized-TC\(^1\).

Let \( \mathcal{A}' \) be an algorithm that takes the OR of independent \( n + 1 \) runs of \( \mathcal{A} \). Then the error probability of \( \mathcal{A}' \) is less than \( 2^{-n-1} \). Since there are at most \( 2^n \) instances of length \( n \), there is one assignment to the random bits that leads the circuit to the correct answer for all inputs of length \( n \). This implies that NONSINGULAR BASIS COMBINATION is in nonuniform-TC\(^1\). Note that the reduction in the proof of Theorem 3.1 uses a constant round of parallel access both to the determinant and to the rank over \( Q \). The rank of a matrix over \( Q \) is in \( \text{AC}^0(\text{C}_\text{=} \text{L}) \subseteq \text{TC}^1 \). So, both SIMULTANEOUS SIMILARITY and NONSINGULAR NULLSPACE are in logspace-uniform randomized-TC\(^1\) and nonuniform-TC\(^1\).

Theorem 3.2 raises the question of whether SIMULTANEOUS SIMILARITY, NONSINGULAR NULLSPACE, and NONSINGULAR BASIS COMBINATION have small nonuniform boolean circuit complexity over a finite field. We provide a negative answer to the question for NONSINGULAR NULLSPACE and NONSINGULAR BASIS COMBINATION. These problems are each NP-complete for any finite field.

Theorem 3.3 For any finite field \( F \), NONSINGULAR NULLSPACE is NP-complete.

Proof. It is easy to prove that NONSINGULAR NULLSPACE is in NP. Let \( N \) be a Turing machine that, on input \( \mathcal{I} = (m, n, T) \) such that \( m, n \geq 1 \) and \( T \in F^{m \times n^2} \), nondeterministically selects a matrix \( Q \in F^{n \times n} \) and then accepts if the conditions \( TQ = 0 \) and \( \text{det}_F(Q) = 0 \) both hold.
and rejects otherwise. It is obvious that $N$ is a nondeterministic machine that decides NONSINGULAR NULLSPACE correctly. Since the determinant function over $F$ is in logspace-uniform NC$^2$ (see [Csa76]) and the matrix multiplication is polynomial-time computable, $N$ can be made to run in polynomial time. Thus, NONSINGULAR NULLSPACE is in NP.

To prove that NONSINGULAR NULLSPACE is NP-hard, we reduce NAE-3SAT to this problem, where NAE-3SAT is the problem of deciding whether a given 3CNF formula is satisfiable by a truth-assignment that satisfies at most two literals per clause. This problem is known to be NP-complete [Sch78] (see also [Pap94]). We first present the reduction in the case when the characteristic of $F$ is greater than equal to three.

Let $\varphi(x_1, \ldots, x_n) = C_1 \land \ldots \land C_m$ be a 3CNF formula whose membership in NAE-3SAT we are testing. Let $f = \|F\| - 3$. Let $g_1, \ldots, g_f$ be an enumeration of the elements in $F \setminus \{0,1,-1\}$ in the case when $f \geq 3$. If $f = 3$, then this list is undefined. Let $N = (n + 1) + 2nf + 3m$ and $M = N^2 - 1$. The matrix $T$ is $M \times N^2$ and we need to determine the entries of $T$ so that $\varphi \in$ NAE-3SAT if and only if the nullspace $\Xi : TQ = 0$ contains an element that is nonsingular viewed as an $N \times N$ matrix. For simplicity, for each $i,j$, $1 \leq i,j \leq n$, let $\pi(i,j) = (i - 1)N + j$. For each $i,j$, $1 \leq i,j \leq n$, let $q_{ij}$ denote the $(i,j)$th entry of $Q$ and let $e_{ij}$ denote the $\pi(i,j)$th unit vector of dimension $N^2$.

First we introduce constraints to force every member of the nullspace to be a block diagonal of the form

$$\text{DIAG}(U_0, \ldots, U_n, A_{11}, \ldots, A_{nf}, B_1, \ldots, B_m),$$

where $U_0, \ldots, U_n$ are all scalar, $A_{11}, \ldots, A_{nf} \in F^{2 \times 2}$, and $B_1, \ldots, B_m \in F^{3 \times 3}$. For each $i,j$, $1 \leq i,j \leq N$, such that $(i,j)$ is either above or below this block diagonal, we add the constraint $q_{ij} = 0$ (i.e., as the row vector $e_{ij}$ in $T$).

Now for every solution $Q$ of $\Xi$, $det(Q)$ is the product of the determinant of the diagonal blocks. Since $U_1, \ldots, U_n$ are scalar, every nonsingular solution $Q$ of $\Xi$ needs to satisfy the condition

$$U_0, \ldots, U_n \neq 0. \quad (1)$$

We first define the $A$-matrices. Let $i$, $1 \leq i \leq n$, and $j$, $1 \leq j \leq f$, be fixed. Let $k = n + 1 + 2((i-1)f + (j-1)) + 1$. Then for all $i$, $1 \leq i \leq n$, and for all $j$, $1 \leq j \leq f$, the entries of $A_{ij}$ are on rows $k$ and $k + 1$ and on columns $k$ and $k + 1$. We add constraints:

$$q_{kk} = U_0, q_{k+1,k+1} = U_0, q_{kk+1} = gjU_i, \text{ and } q_{k+1,k} = g_jU_i.$$ 

There constraints are enforced by the row vectors

$$e_{kk} - e_{11}, e_{k+1,k+1} - e_{11}, e_{kk+1} - gje_{i+1,i+1}, \text{ and } e_{k+1,k} - gj e_{i+1,i+1},$$

respectively. These constraints force the determinant of the block $A_{ij}$ to be $(g_jU_i)^2 - U_0^2$. Since $\{g_1, \ldots, g_f\} = F \setminus \{0,1,-1\}$, assuming that $U_0, U_i \neq 0$, for every $i$, $1 \leq i \leq n$,

$$(\forall j, 1 \leq j \leq f)[det(A_{ij}) \neq 0] \iff U_i = \pm U_0.$$
Thus, for every solution $Q$ of $\Xi$ satisfying (1),

$$\forall i, 1 \leq i \leq n) \forall j, 1 \leq j \leq f [\det(A_{ij}) \neq 0] \iff \forall i, 1 \leq i \leq n) [U_i \in \{U_0, -U_0\}]$$

So, assuming (1), for each $i$, $1 \leq i \leq n$, let $\alpha_i = +1$ if $U_i = U_0$ and $-1$ otherwise.

Next we define the $B$-matrices. Let $i$, $1 \leq i \leq m$, be fixed. Let $k = n + 1 + 2fn + 3(i - 1) + 1$. Then the entries of $B_i$ are on rows $k, k + 1, k + 2$ and on columns $k, k + 1, k + 2$. Let $x_{j_1}, x_{j_2}, x_{j_3}$ be the variables in $C_i$ and for each $s$, $1 \leq s \leq 3$, let $b_s = +1$ if the $s$th literal in $C_i$ is the positive form of $x_{j_3}$ and $-1$ otherwise. Then we add the following constraints:

$$q_{kk} = q_{k+1,k+1} = q_{k+2,k+2} = b_1U_{j_1}, \quad q_{k,k+1} = q_{k+1,k+2} = q_{k+2,k} = b_2U_{j_2}, \quad \text{and} \quad q_{k,k+2} = q_{k+1,k} = q_{k+2,k+1} = b_2U_{j_3}.$$ 

by adding the row vectors

$$e_{kk} - e_{k+1,k+1}, e_{kk} - e_{k+2,k+2}, e_{kk} - b_1e_{j_3,j_1}, e_{k,k+1} - e_{k+1,k+2}, e_{k,k+1} - e_{k+2,k}, e_{k,k+1} - b_2e_{j_2,j_2},$$

$$e_{k+1,k} - b_3e_{j_3,j_3}.$$ 

These constraints force the block $B_i$ to be of the form

$$\begin{pmatrix} 
    b_1U_{j_1} & b_2U_{j_2} & b_3U_{j_3} \\
    b_2U_{j_2} & b_3U_{j_3} & b_1U_{j_1} \\
    b_3U_{j_3} & b_1U_{j_1} & b_2U_{j_2} 
\end{pmatrix}.$$ 

This is equal to

$$U_0 \begin{pmatrix} 
    b_1\alpha_{j_1} & b_2\alpha_{j_2} & b_3\alpha_{j_3} \\
    b_2\alpha_{j_2} & b_3\alpha_{j_3} & b_1\alpha_{j_1} \\
    b_3\alpha_{j_3} & b_1\alpha_{j_1} & b_2\alpha_{j_2} 
\end{pmatrix}.$$ 

If $b_1\alpha_{j_1} = b_2\alpha_{j_2} = b_3\alpha_{j_3}$, then the determinant of this matrix is 0; otherwise, the determinant is either $4(U_0)^3$ or $-4(U_0)^3$. Since the characteristic of $F$ is not 2, we have:

- if $U_0 = 1$ and if $b_1\alpha_{j_1}, b_2\alpha_{j_2},$ and $b_3\alpha_{j_3}$ are not all equal, then the determinant is not 0; and

- if $b_1\alpha_{j_1}, b_2\alpha_{j_2},$ and $b_3\alpha_{j_3}$ are all equal, then the determinant is 0.

Now for each $i$, $1 \leq i \leq n$, view $\alpha_i = +1$ as $x_i = true$ and $\alpha_i = -1$ as $x_i = false$. Then there is a solution $Q$ of $\Xi$ that is a nonsingular matrix if and only if there is an assignment $\alpha_1 \cdots \alpha_n$ that satisfies $\varphi$ by satisfying at most two literals per clause. Thus, NAE-3SAT is polynomial-time many-one reducible to NONSINGULAR NULLSPACE in the case when the characteristic of $F$ is greater than or equal to three.

In the case when the characteristic of $F$ is two, for each $i$, $1 \leq i \leq n$, we use $V_i$, which is a $2 \times 2$ matrix, to express an assignment to $x_i$. For each $i$, $1 \leq i \leq n$, let $a_{i,11}, a_{i,12}, a_{i,21}, a_{i,22}$
be the entries of the matrix $V_i$. As in the previous case, for all $i$, $1 \leq i \leq n$, we enforce that $a_{i,11}, a_{i,12} \in \{U_0, 0, -U_0\}$ and that $a_{i,11} = a_{i,22}$ and $a_{i,12} = a_{i,21}$. Noting that the characteristic of the field is 2, the former condition is actually equivalent to $a_{i,11}, a_{i,12} \in \{U_0, 0\}$. If we put $U_0$ and $V_1, \ldots, V_n$ in the diagonal as in the previous case and make the other entries all 0, then that all the other entries are 0, then for each $i$, $1 \leq i \leq n$, there are only two possibilities for $V_i$:

$$
\begin{pmatrix}
U_0 & 0 \\
0 & U_0
\end{pmatrix}
\text{ or }
\begin{pmatrix}
0 & U_0 \\
U_0 & 0
\end{pmatrix}
$$

The $B$-part of the previous case is modified as follows. Let $i$, $1 \leq i \leq m$, be fixed. Let $x_{j_1}, x_{j_2}, x_{j_3}$ be the variables in $C_i$ and for each $s$, $1 \leq s \leq 3$, let $z_s = a_{j_s,11}$ if the $s$th literal in $C_i$ is the positive form of $x_{j_s}$ and $a_{j_s,12}$ otherwise. Let $y_{i,pq}$, $1 \leq p, q \leq 3$, be the entries of $B_i$. We enforce that $y_{i,11} = y_{i,12} = y_{i,13} = U_0$. Also, for each $s$, $1 \leq s \leq 3$, $y_{i,2s} = z_s$ and $y_{i,3s} = z_s + z_{s'}$, where $s' = s + 1$ if $s \leq 2$ and 1 otherwise. By inspection, the determinant of $B_i$ is $U_0^3$ if either exactly one of $z_1, z_2, z_3$ is equal to $U_0$ or exactly two of $z_1, z_2, z_3$ are equal to $U_0$. Otherwise, the determinant of $B_i$ is 0. Thus, the resulting system has a solution that is a nonsingular matrix if and only if the formula has a "not-all-equal" satisfying assignment. Hence, the problem is NP-complete. This proves the theorem.

It is obvious that Nonsingular Basis Combination is in NP for any finite field $F$. By Theorem 3.1 Nonsingular Nullspace is NC$^2$-reducible to Nonsingular Basis Combination, so we have the following corollary.

**Corollary 3.4** For any finite field $F$, Nonsingular Basis Combination is NP-complete.

We do not know the complexity of Simultaneous Similarity over a finite field, other than its reducibility to Nonsingular Nullspace.

### 4 The Complexity of Matrix Semigroup Problems

A related problem to simultaneous similarity is simultaneous triangularizability. While we did not find a reasonable algorithm for this problem, it did focus our attention on the semigroups generated by the matrices. There is a known test for simultaneous triangularizability [Rad86] but it is nonconstructive, involving examination of all elements of the semigroup generated which could be infinite. Even in the finite case, the cardinality of the semigroup may possibly be multiply exponential. Simultaneous similarity becomes the problem of testing similarity of matrix representations of semigroups, and is the only problem studied that admits an efficient algorithm (at least for fields of characteristic zero). We studied several other semigroup problems that turn out to be PSPACE-hard, in sharp contrast to the situation for groups, where the analogous problems either have randomized polynomial-time algorithms or at worst (matrix group intersection) are known to be in NP.
We first show that the matrix semigroup problems that we defined in Section 2 are all PSPACE-complete if the field is finite. We then show that if we restrict the semigroups to be inverse then the membership problem is still in PSPACE even for fields of characteristic zero. Birget et al. [BMMW00] have shown that membership stays PSPACE-hard even for inverse semigroups, thus the problem is PSPACE-complete. We note that the simultaneous triangularizability problem is uninteresting for finite inverse semigroups since for such semigroups triangularizability can be shown to be equivalent to commutativity, a condition that can be checked in linear time.

**Lemma 4.1** For any finite field $F$, Matrix Semigroup Intersection, Matrix Semigroup Isomorphism, Matrix Semigroup Membership, and Matrix Semigroup Equality are all solvable in PSPACE.

**Proof.** Let $F$ be a finite field. Let $A_1, \ldots, A_g \in F^{n \times n}$ be a set of generators. Let $S = S(A_1, \ldots, A_g)$. Define $\mu(n) = \|F\|^n$. Then $\|S\| \leq \mu(n)$. So, for every $M \in S$, there exists a sequence $i_1, \ldots, i_s \in \{1, \ldots, g\}$, $s \leq \mu(n)$, such that $M = A_{i_1} \cdots A_{i_s}$. Define GEN to be the procedure that, on input $A_1, \ldots, A_g$, nondeterministically selects a natural number $s \leq \mu(n)$ and then nondeterministically selects a sequence of indices, $i_1, \ldots, i_s \in \{1, \ldots, g\}$, one after another, to compute the product $M = A_{i_1} \cdots A_{i_s}$ on the fly. This procedure requires $O(n^2)$ space. Also, for every $M \in F^{n \times n}$, $M$ belongs to $S$ if and only if the procedure generates $M$ for some computation path.

To test membership of $X \in S$, simply run GEN and accept if and only if GEN generates $X$. This is a nondeterministic polynomial space algorithm. By Savitch’s Theorem [Sav70], NPSPACE = PSPACE. Thus, Matrix Semigroup Membership is in PSPACE.

To test whether $S(A_1, \ldots, A_g) \cap S(B_1, \ldots, B_h)$ contains a nonzero matrix, run GEN on the two sets of generators independently, and then, accept if and only if both runs generated an identical nonzero matrix. This is a nondeterministic polynomial space procedure. So, Matrix Semigroup Intersection is in PSPACE.

Since Matrix Semigroup Membership is in PSPACE, there is a deterministic polynomial-space procedure for the membership. Given $A_1, \ldots, A_g$ and $B_1, \ldots, B_h$, test whether for all $M \in F^{n \times n}$ it holds that $M \in S(A_1, \ldots, A_g) \iff M \in S(B_1, \ldots, B_h)$ using the deterministic membership procedure. This yields a deterministic polynomial space procedure for Matrix Semigroup Equality.

Finally, suppose we want to test whether $S_1 = S(A_1, \ldots, A_p)$ and $S_2 = S(B_1, \ldots, B_q)$ are isomorphic. These two semigroups are isomorphic if and only if there exist two homomorphisms $f : S_1 \rightarrow S_2$ and $f' : S_2 \rightarrow S_1$ such that $f \circ f'$ is the identity mapping. The latter condition can be tested by the following procedure: Guess matrices $C_1, \ldots, C_p \in F^{n \times n}$. Test if $S_2 = S(C_1, \ldots, C_p)$. If the test fails, reject. Define $f : \{A_1, \ldots, A_p\}^* \rightarrow S_2$ by $f(A_{i_1} \cdots A_{i_k}) = C_{i_1} \cdots C_{i_k}$ and $f' : \{C_1, \ldots, C_p\}^* \rightarrow S_1$ by $f(C_{i_1} \cdots C_{i_k}) = A_{i_1} \cdots A_{i_k}$. Then test whether $f$ and $f'$ are
homomorphisms. Testing whether \( f \) is a homomorphism from \( S_1 \) to \( S_2 \) can be done by examining the condition:

\[(*) \text{ for all sequences } I = [i_1, \ldots, i_k], J = [j_1, \ldots, j_l] \text{ in } \{1, \ldots, p\} \text{ such that } k, l \leq \mu(n), \text{ if } u = A_{i_1} \cdots A_{i_k} \text{ and } v = A_{j_1} \cdots A_{j_l} \text{ are equal matrix products, then } f(u) = f(v).\]

Consider the following procedure: Guess \( k, l \), then guess the elements of \( I \) and \( J \) one after another and compute the products \( u \) and \( v \) as well as their images with respect to \( f \) (note that \( f \) is associative). Accept (since we are testing the negation) if and only if \( u = v \) and \( f(u) \neq f(v) \). This tests the negation of \((*)\). So, testing whether \( f \) is a homomorphism can be done in \( \text{coNPSPACE} \). Since \( \text{coNPSPACE} = \text{PSPACE} \), testing whether \( f \) is a homomorphism can be done in \( \text{PSPACE} \). Similarly, \( f' \) is a homomorphism can be done in \( \text{PSPACE} \). Thus, isomorphism can be tested in \( \text{NP}^{\text{PSPACE}} = \text{NPSPACE} = \text{PSPACE} \). \( \square \)

**Theorem 4.2** Matrix Semigroup Intersection is \( \text{PSPACE}-\text{complete} \) for any field \( F \).

**Proof.** By Lemma 4.1, we have only to show the \( \text{PSPACE} \)-hardness. Kozen [Koz77] proves \( \text{PSPACE} \)-hardness for transformation semigroups. A transformation semigroup is a subset of the semigroup consisting of all mappings from a set of objects to itself. So, it has a representation by matrices over \( \{0, 1\} \) that have at most one 1 in each row. Thus they can be considered as matrices over a field of any characteristic. \( \square \)

Kozen also proves that \( \text{Matrix Semigroup Membership} \) is \( \text{PSPACE} \)-hard. By Lemma 4.1, the problem is already in \( \text{PSPACE} \) for any finite field \( F \). Let \( A_1, \ldots, A_k, \Gamma \) be an instance of \( \text{Matrix Semigroup Membership} \), that is, it is asked whether \( \Gamma \in S(A_1, \ldots, A_k) \). Let \( T \) be this semigroup. Let \( T' = S(A_1, \ldots, A_k, \Gamma) \). Then the following holds: if \( \Gamma \in T \), then \( T = T' \), and thus, \( T \) and \( T' \) are isomorphic; if \( \Gamma \notin T \), then \( T' \) is a finite semigroup that properly contains \( T \), and thus, \( T \) and \( T' \) are not isomorphic. Thus, the membership question can be tested by an isomorphism question as well as by an equality question. Thus, we have the following corollary.

**Corollary 4.3** Matrix Semigroup Membership, Matrix Semigroup Equality, and Matrix Semigroup Isomorphism are all \( \text{PSPACE}-\text{complete} \) for any finite field \( F \).

What is the complexity of these semigroup problems when the field \( F \) is infinite, for example, the field of the rationals? The best upper bound on the size of a finite matrix semigroup over the rational numbers is multiply exponential [Jac78, MS77, Zal77]. For a finite semigroup generated by \( k n \times n \) matrices over the nonnegative integers, Mandel and Simon [MS77] prove a bound of \( k^{3n^2} \), the triple exponential of a \( \Theta(n^2 \log \log \log k) \) function. We do not know whether those semigroup problems are in \( \text{PSPACE} \). As noted above, they are \( \text{PSPACE} \)-hard. However, Birget et al. [BMMW00] have strengthened Kozen’s proof to apply to inverse semigroups. We show that membership for inverse semigroups over a field of characteristic zero is in \( \text{PSPACE} \) and thus
PSPACE-complete. Recall that a semigroup is inverse if every element $x$ in $S$ has a pseudo-inverse $x'$ such that $xx' = x$ and $x'xx' = x'$. A representation of a finite semigroup $S$ is a homomorphism $\phi : S \to F^{n \times n}$. A representation $\phi$ is called reducible if and only if for some $m, m' > 0$ with $m + m' = n$ and homomorphisms $\psi : S \to F^{m \times m}$ and $\chi : S \to F^{m' \times m'}$, it holds that: for all $s \in S$, there exists an $m' \times m$ matrix $f(s)$ over $F$ such that

$$\phi(s) = \begin{pmatrix} \psi(s) & 0 \\ f(s) & \chi(s) \end{pmatrix}.$$ 

A representation is irreducible if it is non-zero and not reducible. A representation is called completely reducible if and only if it is a direct sum of irreducible representations. We will call a matrix semigroup irreducible, completely reducible if the identity mapping is irreducible or completely reducible, respectively. Every representation of a finite group over a field of characteristic zero is completely reducible, but this is not true for semigroups. However, it is true that every representation of a finite inverse semigroup is completely reducible over a field of characteristic zero [Okn91, Corollary 2]. Let $A$ be a finite dimensional algebra over a field. An element $a \in A$ is called properly nilpotent iff for all $x \in A$, $ax$ and $xa$ are nilpotent, i.e. some power of each is zero. The radical $R(A)$ of $A$ is the set of all properly nilpotent elements. $A$ is called semisimple iff $R(A) = \{0\}$.

Let $S$ be a finitely generated semigroup of matrices over $Q$. The enveloping algebra $E[S]$ of $S$ is the algebra generated by the matrices in $S$. Then all representations of $S$ are completely reducible if and only if $E[S]$ is semisimple. There is no easy direct reference to this result since the result is ordinarily phrased in terms of the semigroup algebra rather than the enveloping algebra ([CR62, RZ91]). However, the present formulation can be derived via the Burnside–Steinberg theorem on tensor powers of representations ([RZ91, Proposition 3.22]).

We show that the membership problem for inverse matrix semigroups over a field of characteristic zero is PSPACE-complete. To do this, we need the following lemma that bounds the norm of an element of a semigroup.

**Lemma 4.4** Let $S \subseteq Z^{n \times n}$ be a finite inverse semigroup with generating set $X$. Let $M = \max\{\|x\| \mid x \in X\}$. Then for any $A \in S \|A\| \leq M^2 n^{2n^2+3}$.

**Proof.** This lemma was proven for groups by Babai, Beals, and Rockmore [BBR, Theorem 1.1]. Their proof is for groups, but essentially the same proof will do for inverse semigroups. First, a finite semigroup of rational matrices is similar to a semigroup of integer matrices. This is classical for groups [Fei67]. The proof generalizes trivially to all finite semigroups, since it does not depend on the existence of inverses.

The proof of [BBR] goes through for inverse semigroups since it does not depend on the existence of (group) inverses, but only on properties of the enveloping algebra $E[S]$. Let $d \leq n^2$ be the dimension of $E[S]$ as a vector space over $Q$. Let $A_1, \ldots, A_d$ be a set of generators for $E[S]$. Let $T$ be the $d \times d$ matrix (trace($A_iA_j$)). The only property needed in the proof is the invertibility of
$T$, which, as shown in [BBR], is equivalent to the semisimplicity of $E[S]$, which in turn, as noted above, is equivalent to the complete reducibility of all representations of $S$. \hfill \Box

**Theorem 4.5** The membership problem for inverse matrix semigroups over a field of characteristic zero is PSPACE-complete.

**Proof.** As noted above, PSPACE-hardness has been proven in [BMMW00]. To prove that membership testing is in PSPACE we will bound both the cardinality of the semigroup $S$ and the norms of the elements of $S$. Assume first that $S$ is irreducible. The bound on the cardinality is classical, due to Burnside and Schur [CR62, Section 36] and refined by Mandel and Simon [MS77] (see also Jacob [Jac78]). We have to add a slight further refinement. Let $r(n)$ be the least common multiple of $D = \{d \mid \phi(d) \leq n\}$, where $\phi(d)$ is the number integers in $\{1, \ldots, d - 1\}$ that are not divisible by $d$. Then the cardinality of $S$ is bounded by $(r(n) + 1)^n$. Rosser and Schoenfeld [RS62] show that $n/\phi(n) = \mathcal{O}(\log \log n)$ and the least common multiple of all natural numbers at most $n$ to be $2^\mathcal{O}(n)$. Then the largest element in $D$ is $\mathcal{O}(n \log n)$, and thus, $r(n) = \mathcal{O}(2^\mathcal{O}(n \log n)) = \mathcal{O}(2^n)$. Thus, the cardinality of $S$ is bounded by an exponential function. Now by Lemma 4.4, the norm is bounded.

Hence the elements of the semigroup have encodings of size polynomial in the size of the generators. Since the number of elements is $O(2^{p(n)})$ for some polynomial $p$, one can systematically generate and test all products of the generators, and hence all elements of the semigroup, in polynomial space. \hfill \Box

Recall that a semigroup $S$ is aperiodic if, for every element $s \in S$, there is a nonnegative integer $n(s)$ such that $s^{n(s)+1} = s^{n(s)}$. It is easy to see that if $s$ is an $n \times n$ matrix then $n(s) \leq n$.

**Theorem 4.6** The matrix semigroup aperiodicity for inverse semigroups is complete for PSPACE, over any field.

**Proof.** PSPACE-hardness is proven in [BMMW00]. Over a finite field, we argue as in the proof of Lemma 4.1. Over the rationals, it follows from [MZ75] that a finitely generated aperiodic matrix semigroup must be finite. Thus we first test for finiteness. If the semigroup is finite, we argue as in the proof of Theorem 4.5 that one can systematically enumerate all elements in polynomial space and each element can be tested for aperiodicity in polynomial time. \hfill \Box

**Theorem 4.7** The finiteness problem for inverse semigroups over the field of rational numbers is in PSPACE.

**Proof.** The polynomial-time algorithm of [BBR] for deciding whether a rational matrix group is equivalent to an integer matrix groups generalizes to semigroups. We run the algorithm. If the answer is ‘no’, the semigroup is infinite. Otherwise, we have a semigroup over the integers. From the proof of Theorem 4.5 we have a bound of $t(n) = 2^{cn^5}$ on the cardinality of $S$, if $S$ is
finite. It is easy to see that $S$ is finite if and only if $(\ast)$ for every sequence $I = [i_1, \ldots, i_{t(n)+1}]$ of indices in $\{1, \ldots, g\}$, there exists $k, 1 \leq k \leq t(n)$, a sequence $J = [j_1, \ldots, j_k]$ of indices in $\{1, \ldots, g\}$, such that $A_{i_1} \cdots A_{i_{t(n)+1}} = A_{j_1} \cdots A_{j_k}$. Given $A_1, \ldots, A_g$ and a matrix $B$, by the proof of Theorem 4.5, whether $B$ is the product of an index sequence of length at most $t(n)$ can be tested in nondeterministic polynomial space, and thus also in deterministic polynomial space. Thus the negation of $(\ast)$ can be tested by guessing the sequence $I$ and comparing the product with all products of length at most $t(n)$. We cannot use Lemma 4.4 to bound the norms of the products. However, if the bound is exceeded, we again know that the semigroup is infinite. Thus finiteness is in $\text{coNPSPACE}$ and since $\text{PSPACE}$ is closed under complement, also in $\text{PSPACE}$. \hfill \Box

Acknowledgments

Zeke Zalcstein would like to thank Amin Shokrollahi for an important discussion in the early stage of this research. The authors would like to thank Jin-Yi Cai and Dick Lipton for helpful discussions.
References


