On the Identity and Group Problems for Complex Heisenberg Matrices

Paul C. Bell[1], Reino Niskanen[2], Igor Potapov[3], and Pavel Semukhin[2]

[1] Keele University, UK
p.c.bell@keele.ac.uk
[2] Liverpool John Moores University, UK
{r.niskanen,p.semukhin}@ljmu.ac.uk
[3] University of Liverpool, UK
potapov@liverpool.ac.uk

Abstract. We study the Identity Problem, the problem of determining if a finitely generated semigroup of matrices contains the identity matrix; see Problem 3 (Chapter 10.3) in "Unsolved Problems in Mathematical Systems and Control Theory" by Blondel and Megretski (2004). This fundamental problem is known to be undecidable for $\mathbb{Z}^{4\times4}$ and decidable for $\mathbb{Z}^{2\times2}$. The Identity Problem has been recently shown to be in polynomial time by Dong for the Heisenberg group over complex numbers in any fixed dimension with the use of Lie algebra and the Baker-Campbell-Hausdorff formula. We develop alternative proof techniques for the problem making a step forward towards more general problems such as the Membership Problem. We extend our techniques to show that the fundamental problem of determining if a given set of Heisenberg matrices generates a group, can also be decided in polynomial time.

1 Introduction

Matrices and matrix products can represent dynamics in many systems, from computational applications in linear algebra and engineering to natural science applications in quantum mechanics, population dynamics and statistics, among others [4, 5, 10, 11, 15, 19, 24, 28, 29]. The analysis of various evolving systems requires solutions of reachability questions in linear systems, which form the essential part of verification procedures, control theory questions, biological systems predictability, security analysis etc.

Reachability problems for matrix products are challenging due to the complexity of this mathematical object and a lack of effective algorithmic techniques. The significant challenge in the analysis of matrix semigroups was initially illustrated by Markov(1947), [27] and later highlighted by Paterson (1970) [30], Blondel and Megretski (2004) [5], and Harju (2009) [21]. The central reachability question is the **Membership Problem**: *Decide whether or not a given matrix M belongs to the matrix semigroup S generated by a set of square matrices G.* By restricting M to be the identity matrix, the problem is known as the *Identity Problem*.

Problem 1 (Identity Problem). Let S be a matrix semigroup generated by a finite set of $n \times n$ matrices over $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{A}, \mathbb{Q}(\mathrm{i}), \ldots$ Is the identity matrix $\boldsymbol{I}$ in the semigroup, i.e., does $\boldsymbol{I} \in S$ hold?

The Membership Problem is known to be undecidable for integer matrices from dimension three, but the decidability status of the Identity Problem was unknown for a long time for matrix semigroups of any dimension, see Problem 10.3 in "Unsolved Problems in Mathematical Systems and Control Theory" [5]. The Identity Problem was shown to be undecidable for 48 matrices from $\mathbb{Z}^{4\times4}$ in [3] and for a generator of eight matrices in [23]. This implies that the *Group Problem* (decide whether a finitely generated semigroup is a group) is also undecidable. The Identity Problem and the Group Problem are open for $\mathbb{Z}^{3\times3}$.

The Identity Problem for a semigroup generated by 2×2 matrices was shown to be EXPSPACE decidable in [9] and later improved by showing to be NP-complete in [2]. The only decidability beyond integer 2×2 matrices were shown in [14] for flat rational subsets of $\mathrm{GL}(2, \mathbb{Q})$.

Similarly to [8], the work [23] initiated consideration of matrix decision problems in the Special Linear Group $\mathrm{SL}(3, \mathbb{Z})$, by showing that there is no embedding from pairs of words into matrices from $\mathrm{SL}(3, \mathbb{Z})$. Beyond the 2×2 case, the Identity Problem was shown to be decidable for the discrete Heisenberg group $\mathrm{H}(3, \mathbb{Z})$ which is a subgroup of $\mathrm{SL}(3, \mathbb{Z})$.

The Heisenberg group is widely used in mathematics and physics. This is in some sense the simplest non-commutative group, and has close connections to quantum mechanical systems [6, 20, 25], harmonic analysis, and number theory [7, 13]. It also makes appearances in complexity theory, e.g., the analysis and geometry of the Heiseberg group have been used to disprove the Goemans-Linial conjecture in complexity theory [26]. Matrices in physics and engineering are ordinarily defined with values over $\mathbb{R}$ or $\mathbb{C}$. In this context, we formulate our decision problems and algorithmic solutions over the field of complex numbers with a finite representation, Gaussian rationals $\mathbb{Q}(\mathrm{i})$.

The Identity Problem was recently shown to be decidable in polynomial time for complex Heisenberg matrices in a paper by Dong [18]. They first prove the result for upper-triangular matrices with rational entries and ones on the main diagonal, $\mathrm{UT}(\mathbb{Q})$ and then use a known embedding of the Heisenberg group over algebraic numbers into $\mathrm{UT}(\mathbb{Q})$. Their approach is different from our techniques; the main difference being that [18] uses tools from Lie algebra, and in particular, matrix logarithms and the Baker-Campbell-Hausdorff formula, to reason about matrix products and their properties. In contrast, our approach first characterises matrices which are 'close to' the identity matrix, which we denote Ω-matrices. Such matrices are close to the identity matrix in that they differ only in a single position in the top-right corner. We then argue about the commutator angle of matrices within this set in order to determine whether zero can be reached, in which case the identity matrix is reachable. We believe that these techniques take a step towards proving the decidability of the more general *membership problem*, which we discuss towards the end of the paper. A careful analysis then follows to ensure that all steps require only Polynomial time, and we extend our

techniques to show that determining if a given set of matrices forms a group (the *group problem*) is also decidable in P (this result is shown in [16] using different techniques). We thus present polynomial time algorithms for both these problems for Heisenberg matrices over $\mathbb{Q}(\mathrm{i})$ in any dimension n.

These new techniques allow us to extend previous results for the discrete Heisenberg group $\mathrm{H}(n,\mathbb{Z})$ and $\mathrm{H}(n,\mathbb{Q})$ [12,17,23,24] and make a step forward towards proving the decidability of the membership problem for complex Heisenberg matrices.

2 Roadmap

We will give a brief overview of our approach here. Given a Heisenberg matrix $M = \begin{pmatrix} 1 & \boldsymbol{m}_1^T & m_3 \\ \mathbf{0} & \boldsymbol{I}_{n-2} & \boldsymbol{m}_2 \\ 0 & \mathbf{0}^T & 1 \end{pmatrix} \in \mathrm{H}(n,\mathbb{Q}(\mathrm{i}))$, denote by $\psi(M)$ the triple $(\boldsymbol{m}_1, \boldsymbol{m}_2, m_3) \in \mathbb{Q}(\mathrm{i})^{2n-3}$. We define the set $\Omega \subseteq \mathrm{H}(n,\mathbb{Q}(\mathrm{i}))$ as those matrices where $\boldsymbol{m}_1$ and $\boldsymbol{m}_2$ are zero vectors, i.e., matrices in Ω look like $\boldsymbol{I}_n$ except allowing any element of $\mathbb{Q}(\mathrm{i})$ in the top right element. Such matrices play a crucial role in our analysis.

In particular, given a set of matrices $G = \{G_1, \ldots, G_t\} \subseteq \mathrm{H}(n,\mathbb{Q}(\mathrm{i}))$ generating a semigroup $\langle G \rangle$, we can find a description of $\Omega_{\langle G \rangle} = \langle G \rangle \cap \Omega$. Since $\boldsymbol{I} \in \Omega$, the Identity Problem reduces to determining if $\boldsymbol{I} \in \Omega_{\langle G \rangle}$.

Several problems present themselves, particularly if we wish to solve the problem in Polynomial time (P). The set $\Omega_{\langle G \rangle}$ is described by a linear set $\mathcal{S} \subseteq \mathbb{N}^t$, which is the solution set of a homogeneous system of linear Diophantine equations induced by matrices in G. This is due to the observation that the elements $(\boldsymbol{m}_1, \boldsymbol{m}_2) \in \mathbb{Q}(\mathrm{i})^{2n-4}$ behave in an additive fashion under multiplication of Heisenberg matrices. The main issue is that the size of the basis of $\mathcal{S}$ is exponential in the description size of G. Nevertheless, we can determine *if a solution exists* to such a system in P (Lemma 1), and this proves sufficient.

The second issue is that reasoning about the element $m_3 \in \mathbb{Q}(\mathrm{i})$ (i.e., the top right element) in a product of Heisenberg matrices is much more involved than for elements $(\boldsymbol{m}_1, \boldsymbol{m}_2) \in \mathbb{Q}(\mathrm{i})^{2n-4}$. Techniques to determine if $m_3 = 0$ for an Ω-matrix within $\Omega_{\langle G \rangle}$ take up the bulk of this paper.

The key to our approach is to consider *commutators* of pairs of matrices within G, which in our case can be described by a single complex number. That is, for $M_1, M_2 \in G$, the commutator is $[M_1, M_2] \in \mathbb{Q}(\mathrm{i})$. After removing all *redundant matrices* (those never reaching an Ω-matrix), we have two cases to consider. Either every pair of matrices from G has the same *angle* in the polar form of the commutator or else there are at least two commutators with different angles.

The latter case is used in Lemma 5. It states that the identity matrix can always be constructed using a solution that contains four particular matrices. Let M_1, M_2, M_3 and M_4 be such that $[M_1, M_2] = r\exp(\mathrm{i}\gamma)$ and $[M_3, M_4] = r'\exp(\mathrm{i}\gamma')$, where $\gamma \neq \gamma'$ so that pairs M_1, M_2 and M_3, M_4 have different commutator angles. We may then define four matrix products using the same generators but matrices M_1, M_2, M_3 and M_4 are in a different order. This difference in

order and the commutator angles being different, ensures that we can control the top right corner elements in order to construct the identity matrix. Lemma 3 provides details on how to calculate the top right element in these products. We then prove that these top right elements in the four matrices are not contained in an open half-plane and this is sufficient for us to construct the identity matrix.

The above construction does not work when all commutators have the same angle, and indeed in this case the identity may or may not be present. Hence, we need to consider various possible shuffles of matrices in these products. To this end, we extend the result of Lemma 3 to derive a formula for the top right element for any shuffle and prove it as Lemma 4. We observe that there is a *shuffle invariant* part of the product that does not depend on the shuffle, and that shuffles add or subtract commutators. Furthermore, this shuffle invariant component can be calculated from the generators used in the product. As we assume that all commutators have the same angle, γ, different shuffles move the value along the line in the complex plane defined by the common commutator angle which we call the γ-*line*.

It is straightforward to see that if it is not possible to reach the γ-line using the additive semigroup of shuffle invariants, then the identity cannot be generated. Indeed, since different shuffles move the value along the γ-line but the shuffle invariant part never reaches it, then the possible values are never on the γ-line, which includes the origin.

We show that if it *is* possible to reach the γ-line using shuffle invariants and there are at least two non-commuting matrices in the used solution, then the identity matrix is in the semigroup (Lemma 6). Testing this property requires determining the solvability of a polynomially-sized set of non-homogeneous systems of linear Diophantine equations, which can be done in polynomial time by Lemma 1.

If the γ-line can be reached only using commuting matrices, we can construct another system of linear Diophantine equations since the top right element has an explicit formula in terms of generators used (see Lemma 6).

3 Preliminaries

The sets of rational numbers, real numbers and complex numbers are denoted by $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. The set of rational complex numbers is denoted by $\mathbb{Q}(\mathrm{i}) = \{a + b\mathrm{i} \mid a, b \in \mathbb{Q}\}$. The set $\mathbb{Q}(\mathrm{i})$ is often called the Gaussian rationals in the literature. A complex number can be written in polar form $a + b\mathrm{i} = r\exp(\mathrm{i}\varphi)$, where $r \in \mathbb{R}$ and $\varphi \in [0, \pi)$. We denote the *angle* of the polar form φ by $\arg(a + b\mathrm{i})$. We also denote $\mathrm{Re}(a + b\mathrm{i}) = a$ and $\mathrm{Im}(a + b\mathrm{i}) = b$. It is worth highlighting that commonly the polar form is defined for a positive real r and an angle between $[0, 2\pi)$. These two definitions are obviously equivalent.

The *identity matrix* is denoted by $\boldsymbol{I}_n$ or, if the dimension n is clear from the context, by $\boldsymbol{I}$. The *Heisenberg group* $\mathrm{H}(n, \mathbb{K})$ is formed by $n \times n$ matrices of the form $M = \begin{pmatrix} 1 & \boldsymbol{m}_1^T & m_3 \\ \mathbf{0} & \boldsymbol{I}_{n-2} & \boldsymbol{m_2} \\ 0 & \mathbf{0}^T & 1 \end{pmatrix}$, where $\boldsymbol{m}_1, \boldsymbol{m}_2 \in \mathbb{K}^{n-2}$, $m_3 \in \mathbb{K}$ and $\mathbf{0} =$

$(0,0,\ldots,0)^T \in \mathbb{K}^{n-2}$ is the zero vector. It is easy to see that the Heisenberg group is a non-commutative subgroup of $\mathrm{SL}(n,\mathbb{K}) = \{M \in \mathbb{K}^{n\times n} \mid \det(M) = 1\}$.

We will be interested in subsemigroups of $\mathrm{H}(n,\mathbb{Q}(\mathrm{i}))$ which are finitely generated. Given a set of matrices $G = \{G_1,\ldots,G_t\} \subseteq \mathrm{H}(n,\mathbb{Q}(\mathrm{i}))$, we denote the matrix semigroup generated by G as $\langle G\rangle$.

Let $M = \begin{pmatrix} 1 & \boldsymbol{m}_1^T & m_3 \\ \mathbf{0} & \boldsymbol{I}_{n-2} & \boldsymbol{m}_2 \\ 0 & \mathbf{0}^T & 1 \end{pmatrix}$, then $(M)_{1,n} = m_3$ is the top right element. To improve readability, by $\psi(M)$ we denote the triple $(\boldsymbol{m}_1, \boldsymbol{m}_2, m_3) \in \mathbb{Q}(\mathrm{i})^{2n-3}$.

The vectors $\boldsymbol{m}_1, \boldsymbol{m}_2$ play a crucial role in our considerations. We define the set $\Omega \subseteq \mathrm{H}(n,\mathbb{Q}(\mathrm{i}))$ as those matrices where $\boldsymbol{m}_1$ and $\boldsymbol{m}_2$ are zero vectors, i.e., matrices in Ω look like $\boldsymbol{I}_n$ except allowing any element of $\mathbb{Q}(\mathrm{i})$ in the top right element. That is, $\Omega = \left\{ \begin{pmatrix} 1 & \mathbf{0}^T & m_3 \\ \mathbf{0} & \boldsymbol{I}_{n-2} & \mathbf{0} \\ 0 & \mathbf{0}^T & 1 \end{pmatrix} \mid m_3 \in \mathbb{Q}(\mathrm{i}) \right\}$, where $\mathbf{0} = (0,0,\ldots,0)^T \in \mathbb{Q}(\mathrm{i})^{n-2}$ is the zero vector.

Let us define a shuffling of a product of matrices. Let $M_1,\ldots,M_k \in G$. The set of permutations of a product of these matrices is denoted by $\mathsf{shuffle}(M_1,\ldots,M_k) = \{M_{\sigma(1)}\cdots M_{\sigma(k)} \mid \sigma \in \mathcal{S}_k\}$, where $\mathcal{S}_k$ is the set of permutations on k elements. If some matrix appears multiple times in the list, say M_1 appears x times, we write $\mathsf{shuffle}(M_1^x, M_2,\ldots,M_k)$ instead of $\mathsf{shuffle}(\underbrace{M_1,\ldots,M_1}_{x \text{ times}}, M_2,\ldots,M_k)$.

Let $M_1 = \begin{pmatrix} 1 & \boldsymbol{a}_1^T & c_1 \\ \mathbf{0} & \boldsymbol{I}_{n-2} & \boldsymbol{b}_1 \\ 0 & \mathbf{0}^T & 1 \end{pmatrix}$ and $M_2 = \begin{pmatrix} 1 & \boldsymbol{a}_2^T & c_2 \\ \mathbf{0} & \boldsymbol{I}_{n-2} & \boldsymbol{b}_2 \\ 0 & \mathbf{0}^T & 1 \end{pmatrix}$. By an abuse of notation, we define the *commutator* $[M_1, M_2]$ of M_1 and M_2 by $[M_1, M_2] = \boldsymbol{a}_1^T\boldsymbol{b}_2 - \boldsymbol{a}_2^T\boldsymbol{b}_1 \in \mathbb{Q}(\mathrm{i})$. Note that the commutator of two arbitrary matrices A, B is ordinarily defined as $[A,B] = AB - BA$, i.e., a matrix. However, for matrices $M_1, M_2 \in \mathrm{H}(n,\mathbb{Q}(\mathrm{i}))$, it is clear that $M_1M_2 - M_2M_1 = \begin{pmatrix} 0 & \mathbf{0}^T & \boldsymbol{a}_1^T\boldsymbol{b}_2 - \boldsymbol{a}_2^T\boldsymbol{b}_1 \\ \mathbf{0} & O & \mathbf{0} \\ 0 & \mathbf{0}^T & 0 \end{pmatrix}$, where O is the $(n-2)\times(n-2)$ zero matrix, thus justifying our notation which will be used extensively. Observe that the matrices M_1, M_2 commute if and only if $[M_1, M_2] = 0$.

Note that the commutator is antisymmetric, i.e., $[M_1, M_2] = -[M_2, M_1]$. We further say that γ is the *angle of the commutator* if $[M_1, M_2] = r\exp(\mathrm{i}\gamma)$ for some $r \in \mathbb{R}$ and $\gamma \in [0,\pi)$. If two commutators $[M_1, M_2]$, $[M_3, M_4]$ have the same angles, that is, $[M_1, M_2] = r\exp(\mathrm{i}\gamma)$ and $[M_3, M_4] = r'\exp(\mathrm{i}\gamma)$ for some $r, r' \in \mathbb{R}$, then we denote this property by $[M_1, M_2] \overset{\gamma}{=} [M_3, M_4]$. If they have different angles, then we write $[M_1, M_2] \overset{\gamma}{\neq} [M_3, M_4]$. By convention, if $[M_1, M_2] = 0$, then $[M_1, M_2] \overset{\gamma}{=} [M_3, M_4]$ for every $M_3, M_4 \in \mathrm{H}(n,\mathbb{Q}(\mathrm{i}))$.

To show that our algorithms run in polynomial time, we will need the following lemma.

Lemma 1. *(i) Let $A \in \mathbb{Q}^{n\times m}$ be a rational matrix, and $\boldsymbol{b} \in \mathbb{Q}^n$ be an n-dimensional rational vector with non-negative coefficients. Then we can decide in polynomial time whether the system of inequalities $A\boldsymbol{x} \geq \boldsymbol{b}$ has an integer solution $\boldsymbol{x} \in \mathbb{Z}^m$.*

(ii) Let $A_1 \in \mathbb{Q}^{n_1\times m}$ and $A_2 \in \mathbb{Q}^{n_2\times m}$ be a rational matrices. Then we can decide in polynomial time whether the system of inequalities $A_1\boldsymbol{x} \geq \mathbf{0}^{n_1}$ and $A_2\boldsymbol{x} > \mathbf{0}^{n_2}$ has an integer solution $\boldsymbol{x} \in \mathbb{Z}^m$.

4 Properties of Ω-matrices

To solve the Identity Problem for subsemigroups of $\mathrm{H}(n, \mathbb{Q}(\mathrm{i}))$ (Problem 1), we will be analysing matrices in Ω (matrices with all zero elements, except possibly the top-right corner value). Let us first discuss how to construct Ω-matrices from a given set of generators $G \subseteq \mathrm{H}(n, \mathbb{Q}(\mathrm{i}))$.

As observed earlier, when multiplying Heisenberg matrices of the form $\begin{pmatrix} 1 & \boldsymbol{m}_1^T & m_3 \\ \mathbf{0} & \boldsymbol{I}_{n-2} & \boldsymbol{m}_2 \\ 0 & \mathbf{0}^T & 1 \end{pmatrix}$, elements $\boldsymbol{m}_1$ and $\boldsymbol{m}_2$ are *additive*. We can thus construct a homogeneous system of linear Diophantine equations (SLDEs) induced by matrices in G. Each Ω-matrix then corresponds to a solution to this system.

Let $G = \{G_1, \ldots, G_t\}$, where $\psi(G_i) = (\boldsymbol{a}_i, \boldsymbol{b}_i, c_i)$. For a vector $\boldsymbol{a} \in \mathbb{Q}(\mathrm{i})^{n-2}$, define $\mathrm{Re}(\boldsymbol{a}) = (\mathrm{Re}(\boldsymbol{a}(1)), \ldots, \mathrm{Re}(\boldsymbol{a}(n-2)))$ (similarly for $\mathrm{Im}(\boldsymbol{a})$). We consider system $A\boldsymbol{x} = \mathbf{0}$, where

$$A = \begin{pmatrix} \mathrm{Re}(\boldsymbol{a}_1) & \mathrm{Re}(\boldsymbol{a}_2) & \cdots & \mathrm{Re}(\boldsymbol{a}_t) \\ \mathrm{Im}(\boldsymbol{a}_1) & \mathrm{Im}(\boldsymbol{a}_2) & \cdots & \mathrm{Im}(\boldsymbol{a}_t) \\ \mathrm{Re}(\boldsymbol{b}_1) & \mathrm{Re}(\boldsymbol{b}_2) & \cdots & \mathrm{Re}(\boldsymbol{b}_t) \\ \mathrm{Im}(\boldsymbol{b}_1) & \mathrm{Im}(\boldsymbol{b}_2) & \cdots & \mathrm{Im}(\boldsymbol{b}_t) \end{pmatrix}, \tag{1}$$

$\boldsymbol{x} \in \mathbb{N}^t$ and $\mathbf{0}$ is the $4(n-2)$-dimensional zero vector; noting that $A \in \mathbb{Q}^{4(n-2)\times t}$. Let $\mathcal{S} = \{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_p\}$ be the set of minimal solutions to the system. Recall that elements of $\mathcal{S}$ are irreducible. That is, a minimal solution cannot be written as a sum of two nonzero solutions. The set $\mathcal{S}$ is always finite and constructable [31].

A matrix $M_i \in G$ is *redundant* if the ith component is 0 in every minimal solution $\boldsymbol{s} \in \mathcal{S}$. Non-redundant matrices can be recognized by checking whether a non-homogeneous SLDE has a solution. More precisely, to check whether M_i is non-redundant, we consider the system $A\boldsymbol{x} = \mathbf{0}$ together with the constraint that $\boldsymbol{x}(i) \geq 1$, where $\boldsymbol{x}(i)$ is the ith component of $\boldsymbol{x}$. Using Lemma 1, we can determine in polynomial time whether such a system has an integer solution.

For the remainder of the paper, we assume that G is the set of non-redundant matrices. This implicitly assumes that for this G, the set $\mathcal{S} \neq \emptyset$. Indeed, if there are no solutions to the corresponding SLDEs, then all matrices are redundant. Hence $G = \emptyset$ and $\boldsymbol{I} \notin \langle G \rangle$ holds trivially.

Let $M_1, \ldots, M_k \in G$ be such that $X = M_1 \cdots M_k \in \Omega$. The Parikh vector of occurrences of each matrix from G in product X may be written as $\boldsymbol{x} = (m_1, \ldots, m_t) \in \mathbb{N}^t$. This Parikh vector $\boldsymbol{x}$ is a linear combination of elements of $\mathcal{S}$, i.e., $\boldsymbol{x} = \sum_{j=1}^{p} y_j \boldsymbol{s}_j$, with $y_j \in \mathbb{N}$, because $\boldsymbol{x}$ is a solution to the SLDEs. Each element of $\mathsf{shuffle}(M_1, \ldots, M_k)$ has the same Parikh vector, but their product is not necessarily the same matrix; potentially differing in the top right element.

Let us state some properties of Ω-matrices.

Lemma 2. *The Ω-matrices are closed under matrix product; the top right element is additive under the product of two matrices; and Ω-matrices commute with Heisenberg matrices. In other words, let $A, B \in \Omega$ and $M \in \mathrm{H}(n, \mathbb{Q}(\mathrm{i}))$, then*

$$(i) \quad AB \in \Omega; \qquad (ii) \quad (AB)_{1,n} = A_{1,n} + B_{1,n}; \qquad (iii) \quad AM = MA.$$

Furthermore, if $N = M_1M_2\cdots M_{k-1}M_k \in \Omega$ *for some* $M_1,\ldots,M_k \in \mathrm{H}(n,\mathbb{Q}(\mathrm{i}))$, *then every cyclic permutation of matrices results in the same matrix,* N. *That is,* $N = M_2M_3\cdots M_kM_1 = \cdots = M_kM_1\cdots M_{k-2}M_{k-1}$.

We require the following technical lemma that allows us to calculate the value in top right corner for particular products. The claim is proven by a direct computation.

Lemma 3. *Let* $M_1, M_2, \ldots, M_k \in \mathrm{H}(n,\mathbb{Q}(\mathrm{i}))$ *such that* $M_1M_2\cdots\ M_k \in \Omega$ *and let* $\ell \geq 1$. *Then,*

$$(M_1^\ell M_2^\ell \cdots\ M_k^\ell)_{1,n} = \ell\sum_{i=1}^{k}\left(c_i - \frac{1}{2}\boldsymbol{a}_i^T\boldsymbol{b}_i\right) + \frac{\ell^2}{2}\sum_{1\leq i<j\leq k-1}[M_i,M_j],$$

where $\psi(M_i) = (\boldsymbol{a}_i, \boldsymbol{b}_i, c_i)$ *for each* $i = 1,\ldots,k$.

If we further assume that the matrices from the previous lemma commute, then for every $M \in \mathsf{shuffle}(M_1^\ell, M_2^\ell, \ldots, M_k^\ell)$:

$$M_{1,n} = \ell\sum_{i=1}^{k}\left(c_i - \frac{1}{2}\boldsymbol{a}_i^T\boldsymbol{b}_i\right) + \frac{\ell^2}{2}\sum_{1\leq i<j\leq k-1}[M_i,M_j] = \ell\sum_{i=1}^{k}\left(c_i - \frac{1}{2}\boldsymbol{a}_i^T\boldsymbol{b}_i\right), \quad (2)$$

noting that $[M_i, M_j] = 0$ when matrices M_i and M_j commute.

In Lemma 3, the matrix product has an ordering which yielded a simple presentation of the value in the top right corner. In the next lemma, we consider an arbitrary shuffle of the product and show that the commutators are important when expressing the top right corner element.

Lemma 4. *Let* $M_1, M_2, \ldots, M_k \in \mathrm{H}(n,\mathbb{Q}(\mathrm{i}))$ *such that* $M_1M_2\cdots\ M_k \in \Omega$ *and let* $\ell \geq 1$. *Let* M *be a shuffle of the product* $M_1^\ell M_2^\ell \cdots M_k^\ell$ *by a permutation* σ *that acts on* $k\ell$ *elements. Then*

$$(M)_{1,n} = \ell\sum_{i=1}^{k}\left(c_i - \frac{1}{2}\boldsymbol{a}_i^T\boldsymbol{b}_i\right) + \frac{\ell^2}{2}\sum_{1\leq i<j\leq k-1}[M_i,M_j] - \sum_{1\leq i<j\leq k} z_{ji}[M_i,M_j],$$

where $\psi(M_i) = (\boldsymbol{a}_i, \boldsymbol{b}_i, c_i)$ *for* $i = 1,\ldots,k$, *and* z_{ji} *is the number of times* M_j *appears before* M_i *in the product; so* z_{ji} *is the number of inversions of* i, j *in* σ.

The crucial observation is that regardless of the shuffle, the top right corner element has a common term, namely $\sum_{i=1}^{k}(c_i - \frac{1}{2}\boldsymbol{a}_i^T\boldsymbol{b}_i)$, plus some linear combination of commutators. We call the common term the *shuffle invariant*. Note that the previous lemmas apply to any Heisenberg matrices, even those in $\mathrm{H}(n,\mathbb{C})$. For the remainder of the section, we restrict considerations to matrices in G.

Definition 1 (Shuffle Invariant). *Let* $M_1,\ldots,M_k \in G$ *be such that* $X = M_1\cdots\ M_k \in \Omega$. *The Parikh vector of occurrences of each matrix from* G *in product* X *may be written as* $\boldsymbol{x} = (m_1,\ldots,m_t) \in \mathbb{N}^t$ *where* $t = |G|$ *as before. Define* $\Lambda_{\boldsymbol{x}} = \sum_{i=1}^{t} m_i(c_i - \frac{1}{2}\boldsymbol{a}_i^T\boldsymbol{b}_i)$ *as the shuffle invariant of Parikh vector* $\boldsymbol{x}$.

Note that the shuffle invariant is dependant only on the generators used in the product and the Parikh vector $\boldsymbol{x}$.

Let $\mathcal{S} = \{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_p\} \subseteq \mathbb{N}^k$ be the set of minimal solutions to the system of linear Diophantine equations for G giving an Ω-matrix, as described in the beginning of the section. Each $\boldsymbol{s}_j$ thus induces a shuffle invariant that we denote $\Lambda_{\boldsymbol{s}_j} \in \mathbb{Q}(\mathrm{i})$ as shown in Definition 1. The Parikh vector of any $X = M_1 M_2 \cdots M_k$ with $X \in \Omega$, denoted $\boldsymbol{x}$, is a linear combination of elements of $\mathcal{S}$, i.e., $\boldsymbol{x} = \sum_{j=1}^{p} y_j \boldsymbol{s}_j$. We then note that the shuffle invariant $\Lambda_{\boldsymbol{x}}$ of $\boldsymbol{x}$ is $\Lambda_{\boldsymbol{x}} = \sum_{j=1}^{p} y_j \Lambda_{\boldsymbol{s}_j}$, i.e., a linear combination of shuffle invariants of $\mathcal{S}$.

Finally, it follows from Lemma 4 that for any $X \in \mathsf{shuffle}(M_1, M_2, \ldots, M_k)$, where as before $M_1 M_2 \cdots M_k \in \Omega$ and whose Parikh vector is $\boldsymbol{x} = \sum_{j=1}^{p} y_j \boldsymbol{s}_j$, the top right entry of X is equal to

$$X_{1,n} = \Lambda_{\boldsymbol{x}} + \sum_{1 \leq i < j \leq k} \alpha_{ij}[M_i, M_j] \; = \; \sum_{j=1}^{p} y_j \Lambda_{\boldsymbol{s}_j} + \sum_{1 \leq i < j \leq k} \alpha_{ij}[M_i, M_j], \quad (3)$$

where each $\alpha_{ij} \in \mathbb{Q}$ depends on the shuffle.

Furthermore, if a product of Heisenberg matrices is an Ω-matrix and all matrix pairs share a common angle γ for their commutators, then shuffling the matrix product only modifies the top right element of the matrix by a real multiple of $\exp(\mathrm{i}\gamma)$. This drastically simplifies our later analysis.

5 The Identity Problem for subsemigroups of $\mathrm{H}(\boldsymbol{n}, \mathbb{Q}(\mathrm{i}))$

In this section, we prove our main result.

Theorem 1. *Let $G \subseteq \mathrm{H}(n, \mathbb{Q}(\mathrm{i}))$ be a finite set of matrices. Then it is decidable in polynomial time if $\boldsymbol{I} \in \langle G \rangle$.*

The proof relies on analysing generators used in a product that results in an Ω-matrix. There are two distinct cases to consider: either there is a pair of commutators with distinct angles, or else all commutators have the same angle. The former case is considered in Lemma 5 and the latter in Lemma 6. More precisely, we will prove that in the former case, the identity matrix is always in the generated semigroup and that the latter case reduces to deciding whether shuffle invariants reach the line defined by the angle of the commutator.

The two cases are illustrated in Figure 1. On the left, is a depiction of the case where there are at least two commutators with different angles, γ_1 and γ_2. We will construct a sequence of products where the top right element tends to $r_1 \exp(\mathrm{i}\gamma_1)$ with positive r_1 and another product that tends to $r_2 \exp(\mathrm{i}\gamma_1)$ with negative r_2. This is achieved by changing the order of matrices whose commutator has angle γ_1. Similarly, we construct two sequences of products where the top right elements tend to $r_3 \exp(\mathrm{i}\gamma_2)$ and $r_4 \exp(\mathrm{i}\gamma_2)$, where r_3 and r_4 have the opposite signs. Together these sequences ensure, that eventually, the top right elements do not lie in the same open half-planes. On the right, is a depiction of the other case, where all commutators lie on γ-line. In this case, the shuffle invariants of products need to be used to reach the line.

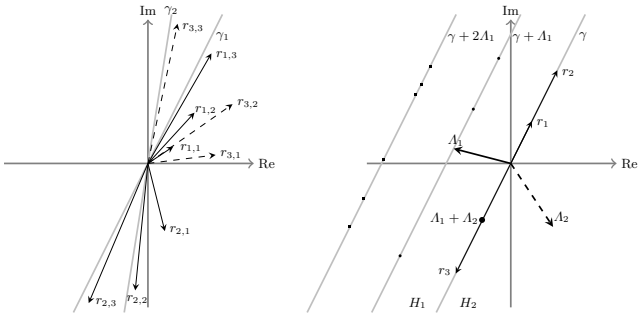

Fig. 1. Illustrations of Lemma 5 and Lemma 6. Left shows two lines defined by two different commutators and how the values $r_{1,\ell}$ and $r_{2,\ell}$ tend to γ_1-line in opposite directions, while $r_{3,\ell}$ tends to γ_2-line ($r_{4,\ell}$ is omitted for clarity). Eventually, they are not all within the same closed half-plane. Right shows that if there is only one shuffle invariant, say Λ_1, then all reachable values are on lines parallel to the γ-line, namely, $\gamma + k\Lambda_1$ for $k > 0$. But if there exists Λ_2 in the opposite half-plane, then the γ-line itself is reachable.

Lemma 5. *Let $G = \{G_1, \ldots, G_t\} \subseteq \mathrm{H}(n, \mathbb{Q}(\mathrm{i}))$, where each G_i is non-redundant. Suppose there exist $M_1, M_2, M_3, M_4 \in G$ such that $[M_1, M_2] \overset{\gamma}{\neq} [M_3, M_4]$. Then $\boldsymbol{I} \in \langle G \rangle$.*

It remains to consider the case when the angles of commutators coincide for each pair of non-redundant matrices. Our aim is to prove that, under this condition, it is decidable whether the identity matrix is in the generated semigroup.

Lemma 6. *Let $G = \{G_1, \ldots, G_t\} \subseteq \mathrm{H}(n, \mathbb{Q}(\mathrm{i}))$ be a set of non-redundant matrices such that the angle of commutator $[G_i, G_{i'}]$ is γ for all $1 \leq i, i' \leq t$, then we can determine in polynomial time if $\boldsymbol{I} \in \langle G \rangle$.*

Proof. Let $\{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_p\} \subseteq \mathbb{N}^t$ be the set of minimal solutions to the SLDEs for G giving zeros in $\boldsymbol{a}$ and $\boldsymbol{b}$ elements. Each $\boldsymbol{s}_j$ induces a shuffle invariant $\Lambda_{\boldsymbol{s}_j} \in \mathbb{Q}(\mathrm{i})$ as explained in Definition 1.

Consider a product $X = M_1 \cdots M_k \in \Omega$, where each $M_i \in G$. Let $\boldsymbol{x} = (m_1, m_2, \ldots, m_t) \in \mathbb{N}^t$ be the Parikh vector of the number of occurrences of each matrix from G in product X. Since $X \in \Omega$, we have $\boldsymbol{x} = \sum_{j=1}^{p} y_j \boldsymbol{s}_j$, where each $y_j \in \mathbb{N}$. Notice that $X \in \mathsf{shuffle}(G_1^{m_1}, \ldots, G_t^{m_t})$. Hence, by Equation (3), we have

$$X_{1,n} = \Lambda_{\boldsymbol{x}} + \sum_{1 \leq i < j \leq k} \alpha_{ij}[M_i, M_j] = \sum_{j=1}^{p} y_j \Lambda_{\boldsymbol{s}_j} + r \exp(\mathrm{i}\gamma), \tag{4}$$

where $\alpha_{ij} \in \mathbb{Q}$ and $r \in \mathbb{R}$ depend on the shuffle. In other words, any shuffle of the product X will change the top right entry $X_{1,n}$ by a real multiple of $\exp(\mathrm{i}\gamma)$.

Let H_1, H_2 be the two *open* half-planes of the complex plane induced by $\exp(\mathrm{i}\gamma)$, that is, the union $H_1 \cup H_2$ is the complement of the γ-line; thus $0 \notin$

$H_1 \cup H_2$. We now prove that if $\{\Lambda_{\boldsymbol{s}_1}, \ldots, \Lambda_{\boldsymbol{s}_p}\} \subseteq H_1$ or $\{\Lambda_{\boldsymbol{s}_1}, \ldots, \Lambda_{\boldsymbol{s}_p}\} \subseteq H_2$ then we cannot reach the identity matrix.

Assume that $\{\Lambda_{\boldsymbol{s}_1}, \ldots, \Lambda_{\boldsymbol{s}_p}\} \subseteq H_1$, renaming H_1, H_2 if necessary. Assume that there exists some product $X = X_1 X_2 \cdots X_k$ equal to the identity matrix, where $k > 0$ and $X_j \in G$. Then since $X \in \Omega$, we see from Equation (4) that $X_{1,n} = \sum_{j=1}^{p} y_j \Lambda_{\boldsymbol{s}_j} + r\exp(\mathrm{i}\gamma)$, where $r \in \mathbb{R}$.

Clearly, $\sum_{j=1}^{p} y_j \Lambda_{\boldsymbol{s}_j} \in H_1$, and since $y_j \neq 0$ for at least one i, we have $\sum_{j=1}^{p} y_j \Lambda_{\boldsymbol{s}_j} \neq 0$. Now, since $r\exp(\mathrm{i}\gamma)$ is on the γ-line, which is the boundary of H_1, the value $X_{1,n}$ belongs to H_1 and cannot equal zero. This contradicts the assumption that X is the identity matrix.

If $\{\Lambda_{\boldsymbol{s}_1}, \ldots, \Lambda_{\boldsymbol{s}_p}\}$ is not fully contained in either H_1 or H_2, then there are two possibilities. Either there exists some $\Lambda_{\boldsymbol{s}_j} \in \mathbb{Q}(\mathrm{i})$ such that the angle of $\Lambda_{\boldsymbol{s}_j}$ is equal to γ (in which case such a $\Lambda_{\boldsymbol{s}_j}$ lies on the line defined by $\exp(\mathrm{i}\gamma)$), or else there exist $\Lambda_{\boldsymbol{s}_i}, \Lambda_{\boldsymbol{s}_j}$ such that $1 \leq i < j \leq p$ and $\Lambda_{\boldsymbol{s}_i}$ and $\Lambda_{\boldsymbol{s}_j}$ lie in different open half-planes, say $\Lambda_{\boldsymbol{s}_i} \in H_1$ and $\Lambda_{\boldsymbol{s}_j} \in H_2$.

In the latter case, note that there exists $x, y \in \mathbb{N}$ such that $x\Lambda_{\boldsymbol{s}_i} + y\Lambda_{\boldsymbol{s}_j} = r\exp(\mathrm{i}\gamma)$ for some $r \in \mathbb{R}$ since $\Lambda_{\boldsymbol{s}_i}, \Lambda_{\boldsymbol{s}_j}$ and the commutators that define the γ-line have rational components. It means that in both cases there exist $z_1, \ldots, z_p \in \mathbb{N}$ such that $\sum_{j=1}^{p} z_j \Lambda_{\boldsymbol{s}_j} = r\exp(\mathrm{i}\gamma)$ for some $r \in \mathbb{R}$.

Consider a product $T = T_1 \cdots T_k \in \Omega$, where each $T_j \in G$ and whose Parikh vector is equal to $\sum_{j=1}^{p} z_j \boldsymbol{s}_j$, where $z_1, \ldots, z_p \in \mathbb{N}$ are as above. It follows from Equation (4) that $T_{1,n} = \sum_{j=1}^{p} z_j \Lambda_{\boldsymbol{s}_j} + r'\exp(\mathrm{i}\gamma) = r\exp(\mathrm{i}\gamma) + r'\exp(\mathrm{i}\gamma)$, where $r, r' \in \mathbb{R}$ and shuffles of such a product change only r'.

We have two possibilities. Either $T = T_1 \cdots T_k$ is a product only consisting of commuting matrices from G, or else two of the matrices in the product of T do not commute. In the latter case, let us write $T' = N_1 N_2 X' \in \mathsf{shuffle}(T_1, \ldots, T_k)$, where $N_1 \in G$ and $N_2 \in G$ do not commute and X' is the product of the remaining matrices in any order. We observe that Lemma 3 implies

$$(N_1^{\ell_1} N_2^{\ell_1} X'^{\ell_1})_{1,n} = \ell_1 r\exp(\mathrm{i}\gamma) + \frac{\ell_1^2}{2}[N_1, N_2] = \ell_1 r\exp(\mathrm{i}\gamma) + \frac{\ell_1^2}{2} r'\exp(\mathrm{i}\gamma) \quad \text{and}$$
$$(N_2^{\ell_2} N_1^{\ell_2} X'^{\ell_2})_{1,n} = \ell_2 r\exp(\mathrm{i}\gamma) + \frac{\ell_2^2}{2}[N_2, N_1] = \ell_2 r\exp(\mathrm{i}\gamma) - \frac{\ell_2^2}{2} r'\exp(\mathrm{i}\gamma),$$

for some $0 \neq r' \in \mathbb{R}$. We then notice that $\left((N_1^{\ell_1} N_2^{\ell_1} X'^{\ell_1})^{d_1} (N_2^{\ell_2} N_1^{\ell_2} X'^{\ell_2})^{d_2}\right)_{1,n} = d_1\left(\ell_1 r\exp(\mathrm{i}\gamma) + \frac{\ell_1^2}{2} r'\exp(\mathrm{i}\gamma)\right) + d_2\left(\ell_2 r\exp(\mathrm{i}\gamma) - \frac{\ell_2^2}{2} r'\exp(\mathrm{i}\gamma)\right)$. Now,

$$\begin{aligned} d_1\left(\ell_1 r\exp(\mathrm{i}\gamma) + \frac{\ell_1^2}{2} r'\exp(\mathrm{i}\gamma)\right) + d_2\left(\ell_2 r\exp(\mathrm{i}\gamma) - \frac{\ell_2^2}{2} r'\exp(\mathrm{i}\gamma)\right) &= 0 \\ \iff d_1(2\ell_1 r + \ell_1^2 r') + d_2(2\ell_2 r - \ell_2^2 r') &= 0 \\ \iff d_1(2\frac{r}{r'}\ell_1 + \ell_1^2) + d_2(2\frac{r}{r'}\ell_2 - \ell_2^2) &= 0. \end{aligned}$$

By our assumption, the vectors $r\exp(\mathrm{i}\gamma)$ and $r'\exp(\mathrm{i}\gamma)$ have rational coordinates and the same angle γ. It follows that $\frac{r}{r'} \in \mathbb{Q}$. Hence we may choose sufficiently

large $\ell_1, \ell_2 > 1$ such that $2\frac{r}{r'}\ell_1 + \ell_1^2$ and $2\frac{r}{r'}\ell_2 - \ell_2^2$ have different signs, and then integers $d_1, d_2 > 1$ can be chosen that satisfy the above equation. This choice of ℓ_1, ℓ_2, d_1, d_2 is then such that $(N_1^{\ell_1} N_2^{\ell_1} X'^{\ell_1})^{d_1} (N_2^{\ell_2} N_1^{\ell_2} X'^{\ell_2})^{d_2} = \boldsymbol{I}$ as required. Thus if such non-commuting matrices are present, we can reach the identity.

Otherwise, our final case is that only commuting matrices can be used to reach the γ-line. In this case we can compute in polynomial time a subset $C \subseteq G$ of these matrices. Then we can check if the identity matrix is in $\langle C \rangle$ in polynomial time as follows.

Since C consists only of commuting matrices, by Equation (2), the top corner value $M_{1,n}$ of any $M \in \langle C \rangle \cap \Omega$ can be expressed as a linear combination of $c_i - \frac{1}{2}\boldsymbol{a}_i^T \boldsymbol{b}_i$, where $G_i \in C$. We now construct a new homogeneous system of linear Diophantine equations. Let $C = \{G_1, \ldots, G_{t'}\}$, and let $A \in \mathbb{Q}^{4(n-2)\times t'}$ be defined as in Equation (1) using only matrices present in C. Also, let $A_2 = (c_1 - \frac{1}{2}\boldsymbol{a}_1^T \boldsymbol{b}_1, \ldots, c_{t'} - \frac{1}{2}\boldsymbol{a}_{t'}^T \boldsymbol{b}_{t'})$. Now construct a system $\binom{A}{A_2}\boldsymbol{x} = \boldsymbol{0}$, where $\boldsymbol{x} \in \mathbb{N}^{t'}$ and $\boldsymbol{0}$ is the $(4(n-2)+1)$-dimensional zero vector. Note that if this system has a solution $\boldsymbol{x}$, then $G_1^{x(1)} G_2^{x(2)} \cdots G_{t'}^{x(t')} = \boldsymbol{I}$. By Lemma 1 (see also [22]), we can decide if such a system has a non-zero solution in polynomial time.[4]

The proof is concluded by showing that the whole procedure is in P. Namely, we first decide if there is a pair G_i, G_j of non-commuting matrices such that the γ-line can be reached using G_i and G_j, in which case $\boldsymbol{I} \in \langle G \rangle$ by the above argument. This requires constructing a polynomially sized set of non-homogeneous systems of linear Diophantine equations and deciding whether they have solutions. This can be done in polynomial time.

If the γ-line can be reached only using commuting matrices, then we can compute the set $C \subseteq G$ of these matrices and check whether $\boldsymbol{I} \in \langle \mathcal{C} \rangle$ in polynomial time. □

Lemmata 5 and 6 allow us to prove the main result, Theorem 1.

The decidability of the Identity Problem implies that the Subgroup Problem is also decidable. That is, whether the semigroup generated by the generators G contains a non-trivial subgroup. However, the decidability of the Group Problem, i.e., whether $\langle G \rangle$ is a group, does not immediately follow. Our result can be extended to show decidability of the Group Problem.

Corollary 1. *It is decidable in polynomial time whether a finite set of matrices $G \subseteq \mathrm{H}(n, \mathbb{Q}(\mathrm{i}))$ forms a group.*

Proof. We give a brief overview of the proof. For $\langle G \rangle$ to be a group, each element of G must have a multiplicative inverse in $\langle G \rangle$. If $\boldsymbol{I} \in \langle G \rangle$, then each element used in a factorization of $\boldsymbol{I}$ has such an inverse. E.g., if $M_1 \cdots M_k = \boldsymbol{I}$, then $M_1^{-1} = M_2 \cdots M_k$ etc. The difficulty is that perhaps $\boldsymbol{I} \in \langle G \rangle$, but this does not imply that every matrix in G has a multiplicative inverse (since not every matrix may be used within a product equal to $\boldsymbol{I}$).

[4] Note by a result of [1], the Membership Problem is decidable in polynomial time for commuting matrices. However, the authors prefer to have a self-contained proof.

We therefore proceed by first ensuring there are no redundant matrices (carried out in P) since a redundant matrix cannot even be used to reach an Ω-matrix. Assuming all matrices are non-redundant, we then adapt the proofs of Lemmata 5 and 6 to ensure that not only can we reach the identity matrix, but we can do so with a product that uses every matrix from G. Both lemmata use Ω-matrices as part of their proofs, and we know there is a product containing all matrices giving an Ω-matrix since all matrices are non-redundant. Lemma 5 can then be adapted to say that if two pairs have different commutator angles, then we can reach the identity matrix using all matrices within the product. If all commutator angles of pairs of matrices in G are identical, then we can adapt the non-homogeneous system of linear Diophantine equations from the proof of Lemma 6 to enforce that all matrices are used at least once. This gives us a polynomial time algorithm for deciding whether $\langle G \rangle$ is a group. □

6 Future research

We believe that the techniques, and the general approach, presented in the previous chapters can act as stepping stones for related problems. In particular, consider the Membership Problem, i.e., where the target matrix can be any matrix rather than the identity matrix. Let $M = \begin{pmatrix} 1 & \boldsymbol{m}_1^T & m_3 \\ \mathbf{0} & \boldsymbol{I}_{n-2} & \boldsymbol{m}_2 \\ 0 & \mathbf{0}^T & 1 \end{pmatrix}$ be the target matrix and let $G = \{G_1, \ldots, G_t\}$, where $\psi(G_i) = (\boldsymbol{a}_i, \boldsymbol{b}_i, c_i)$. Following the idea of Section 4, we can consider system $A\boldsymbol{x} = (\boldsymbol{m}_1, \boldsymbol{m}_2)$, where $\boldsymbol{x} \in \mathbb{N}^t$. This system is a non-homogeneous system of linear Diophantine equations that can be solved in NP. The solution set is a union of two finite solution sets, S_0 and S_1. The set S_0 being the solutions to the corresponding homogeneous system that can be repeated any number of times as they add up to $\mathbf{0}$ on the right-hand side. The other set, S_1, corresponds to reaching the vector $(\boldsymbol{m}_1, \boldsymbol{m}_2)$. The matrices corresponding to the solutions in S_1 have to be used exactly this number of times.

The techniques developed in Section 4 allow us to manipulate matrices corresponding to solutions in S_0 in order to obtain the desired value in the top right corner. However, this is not enough as the main technique relies on repeated use of Ω-matrices. These can be interspersed with matrices corresponding to a solution in S_1 affecting the top right corner in uncontrollable ways.

References

1. László Babai, Robert Beals, Jin-yi Cai, Gábor Ivanyos, and Eugene M. Luks. Multiplicative equations over commuting matrices. In *Proceedings of SODA 1996*, pages 498–507. SIAM, 1996. URL: http://dl.acm.org/citation.cfm?id=313852.314109.
2. Paul C. Bell, Mika Hirvensalo, and Igor Potapov. The identity problem for matrix semigroups in SL(2, $\mathbb{Z}$) is NP-complete. In *Proceedings of SODA 2017*, pages 187–206. SIAM, 2017. doi:10.1137/1.9781611974782.13.

3. Paul C. Bell and Igor Potapov. On the undecidability of the identity correspondence problem and its applications for word and matrix semigroups. *International Journal of Foundations of Computer Science*, 21(6):963–978, 2010. doi:10.1142/S0129054110007660.
4. Kenneth R. Blaney and Andrey Nikolaev. A PTIME solution to the restricted conjugacy problem in generalized Heisenberg groups. *Groups Complexity Cryptology*, 8(1):69–74, 2016. doi:10.1515/gcc-2016-0003.
5. Vincent D. Blondel and Alexandre Megretski, editors. *Unsolved problems in mathematical systems and control theory*. Princeton University Press, 2004.
6. Jean-Luc Brylinski. *Loop spaces, characteristic classes, and geometric quantization*. Birkhäuser, 1993.
7. Daniel Bump, Persi Diaconis, Angela Hicks, Laurent Miclo, and Harold Widom. An exercise(?) in Fourier analysis on the Heisenberg group. *Ann. Fac. Sci. Toulouse Math. (6)*, 26(2):263–288, 2017. doi:10.5802/afst.1533.
8. Julien Cassaigne, Tero Harju, and Juhani Karhumäki. On the undecidability of freeness of matrix semigroups. *International Journal of Algebra and Computation*, 9(03n04):295–305, 1999. doi:10.1142/S0218196799000199.
9. Christian Choffrut and Juhani Karhumäki. Some decision problems on integer matrices. *RAIRO - Theoretical Informatics and Applications*, 39(1):125–131, 2005. doi:10.1051/ita:2005007.
10. Ventsislav Chonev, Joël Ouaknine, and James Worrell. The orbit problem in higher dimensions. In *Proceedings of STOC 2013*, pages 941–950. ACM, 2013. doi:10.1145/2488608.2488728.
11. Ventsislav Chonev, Joël Ouaknine, and James Worrell. On the complexity of the orbit problem. *Journal of the ACM*, 63(3):23:1–23:18, 2016. doi:10.1145/2857050.
12. Thomas Colcombet, Joël Ouaknine, Pavel Semukhin, and James Worrell. On reachability problems for low-dimensional matrix semigroups. In *Proceedings of ICALP 2019*, volume 132 of *LIPIcs*, pages 44:1–44:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. doi:10.4230/LIPIcs.ICALP.2019.44.
13. Persi Diaconis and Maryanthe Malliaris. Complexity and randomness in the heisenberg groups (and beyond), 2021. doi:10.48550/ARXIV.2107.02923.
14. Volker Diekert, Igor Potapov, and Pavel Semukhin. Decidability of membership problems for flat rational subsets of GL(2, $\mathbb{Q}$) and singular matrices. In Ioannis Z. Emiris and Lihong Zhi, editors, *ISSAC '20: International Symposium on Symbolic and Algebraic Computation, Kalamata, Greece, July 20-23, 2020*, pages 122–129. ACM, 2020. doi:10.1145/3373207.3404038.
15. Jintai Ding, Alexei Miasnikov, and Alexander Ushakov. A linear attack on a key exchange protocol using extensions of matrix semigroups. *IACR Cryptology ePrint Archive*, 2015:18, 2015.
16. Ruiwen Dong. On the identity problem and the group problem for subsemigroups of unipotent matrix groups. *CoRR*, abs/2208.02164, 2022. doi:10.48550/arXiv.2208.02164.
17. Ruiwen Dong. On the identity problem for unitriangular matrices of dimension four. In *Proceedings of MFCS 2022*, volume 241 of *LIPIcs*, pages 43:1–43:14, 2022. doi:10.4230/LIPIcs.MFCS.2022.43.
18. Ruiwen Dong. Semigroup Intersection Problems in the Heisenberg Groups. In *In Proceedings of STACS 2023*, volume 254 of *LIPIcs*, pages 25:1–25:18, 2023. doi:10.4230/LIPIcs.STACS.2023.25.
19. Esther Galby, Joël Ouaknine, and James Worrell. On matrix powering in low dimensions. In *Proceedings of STACS 2015*, volume 30 of *LIPIcs*, pages 329–340, 2015. doi:10.4230/LIPIcs.STACS.2015.329.

20. Razvan Gelca and Alejandro Uribe. From classical theta functions to topological quantum field theory. In *The influence of Solomon Lefschetz in geometry and topology*, volume 621 of *Contemprorary Mathematics*, pages 35–68. American Mathematical Society, 2014. doi:10.1090/conm/621.
21. Tero Harju. Post correspondence problem and small dimensional matrices. In *Proceedings of DLT 2009*, volume 5583 of *LNCS*, pages 39–46. Springer, 2009. doi:10.1007/978-3-642-02737-6_3.
22. Leonid G. Khachiyan. Polynomial algorithms in linear programming. *USSR Computational Mathematics and Mathematical Physics*, 20(1):53–72, 1980.
23. Sang-Ki Ko, Reino Niskanen, and Igor Potapov. On the identity problem for the special linear group and the Heisenberg group. In *Proceedings of ICALP 2018*, volume 107 of *LIPIcs*, pages 132:1–132:15, 2018. doi:10.4230/lipics.icalp.2018.132.
24. Daniel König, Markus Lohrey, and Georg Zetzsche. Knapsack and subset sum problems in nilpotent, polycyclic, and co-context-free groups. *Algebra and Computer Science*, 677:138–153, 2016. doi:10.1090/conm/677/13625.
25. Bertram Kostant. Quantization and unitary representations. In *Lectures in Modern Analysis and Applications III*, pages 87–208. Springer, 1970. doi:10.1007/BFb0079068.
26. James R. Lee and Assaf Naor. Lp metrics on the heisenberg group and the Goemans-Linial conjecture. In *2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)*, pages 99–108, 2006. doi:10.1109/FOCS.2006.47.
27. Andrei A. Markov. On certain insoluble problems concerning matrices. *Doklady Akademii Nauk SSSR*, 57(6):539–542, 1947.
28. Alexei Mishchenko and Alexander Treier. Knapsack problem for nilpotent groups. *Groups Complexity Cryptology*, 9(1):87–98, 2017. doi:10.1515/gcc-2017-0006.
29. Joël Ouaknine, João Sousa Pinto, and James Worrell. On termination of integer linear loops. In *Proceedings of SODA 2015*, pages 957–969. SIAM, 2015. doi:10.1137/1.9781611973730.65.
30. Michael S. Paterson. Unsolvability in 3×3 matrices. *Studies in Applied Mathematics*, 49(1):105, 1970. doi:10.1002/sapm1970491105.
31. Alexander Schrijver. *Theory of Linear and Integer Programming*. Wiley, 1998.