# Mortality for $2 \times 2$ Matrices Is NP-Hard

Paul C. Bell[1], Mika Hirvensalo[2], and Igor Potapov[3]

[1] Department of Computer Science, Loughborough University, Loughborough,
LE11 3TU, UK
p.bell@lboro.ac.uk

[2] Department of Mathematics, University of Turku, FIN-20014 Turku, Finland
mikhirve@utu.fi

[3] Department of Computer Science, University of Liverpool, Ashton Building,
Ashton St, Liverpool, L69 3BX, UK
potapov@liverpool.ac.uk

**Abstract.** We study the computational complexity of determining whether the zero matrix belongs to a finitely generated semigroup of two dimensional integer matrices (the mortality problem). We show that this problem is NP-hard to decide in the two-dimensional case by using a new encoding and properties of the projective special linear group. The decidability of the mortality problem in two dimensions remains a long standing open problem although in dimension three is known to be undecidable as was shown by Paterson in 1970.

We also show a lower bound on the minimum length solution to the Mortality Problem, which is exponential in the number of matrices of the generator set and the maximal element of the matrices.

## 1 Introduction

In this paper we study the computational complexity of the problem of determining whether the zero matrix belongs to a matrix semigroup (the Mortality Problem) generated by a finite set of $2 \times 2$ integral matrices. The Mortality Problem of $3 \times 3$ integer matrices was shown to be undecidable in 1970 [13] and the question about $2 \times 2$ matrices is currently open.

In the past there has been much interest in decidability questions for problems concerning matrix semigroups and in particular the Mortality Problem [10,11], which have a number of connections with linear algebra, geometry and controllability of switched linear systems [7,6]. The mortality problem was shown to be decidable for a pair of rational $2 \times 2$ matrices in [7]. Also, it was recently shown in [12] that the Mortality Problem is decidable for any set of $2 \times 2$ integer matrices whose determinants assume the values $0, \pm 1$, by adapting a technique from [9]. The main goal of this paper is to show that the Mortality Problem for the same set of $2 \times 2$ integer matrices (whose determinants assume the values $0, \pm 1$) is NP-hard.

Another set of hardness results is known about bounded membership. A set of matrices over the integers is said to be $k$-mortal (with $k$ a positive integer) if the zero matrix can be expressed as a product of length $k$ of matrices in the set. In

B. Rovan, V. Sassone, and P. Widmayer (Eds.): MFCS 2012, LNCS 7464, pp. 148–159, 2012.

[5], it was shown that the bounded membership problem for the zero matrix (the $k$-mortality problem) is NP-hard for semigroups generated by a pair of matrices (where the dimension is variable). Also a straightforward encoding of the Subset Sum Problem can be used to show NP-hardeness of the bounded membership problem for $2 \times 2$ matrices including the case of commutative matrices [8].

In this paper we prove that the *unbounded* mortality problem for $2 \times 2$ matrices is NP-hard by a more sophisticated construction that requires detailed analysis of the semigroup generator as well as the use of an extended group alphabet and the concept of border letters. We also show a lower bound on the minimum length solution to the Mortality Problem, which is exponential in the number of matrices of the generator set and the maximal element of the matrices.

It is known that many computational problems for matrix semigroups and groups are inherently difficult to solve even for low-dimensions. In contrast to the Mortality($3 \times 3$), which was one of the first matrix problems, shown to be undecidable several decades ago, the *Identity Problem* [1] was shown to be undecidable for dimension 4 only a few years ago [2]. Moreover it has been recently proven in [9] that the Identity Problem for integral matrices of dimension 2 is decidable and later in [3] that the problem for $\mathrm{SL}_2(\mathbb{Z})$ is NP-hard. The NP-hardness result of this paper about the Mortality($2 \times 2$) corresponds very well with the Identity situation. Unfortunately, the same proof technique as in [3] cannot be directly applied for the Mortality Problem and therefore we must use new encoding and properties of the projective special linear group in this paper to derive the result.

## 2 Notations and the Structure of $\mathbf{SL_2}(\mathbb{Z})$

By an alphabet we understand (usually) a finite set $\Gamma$, and call its elements letters. Any alphabet can be furnished with algebraic structure, defining the product by letter juxtaposition (concatenation). Assumption that there are no nontrivial relations between the letters is another way to say that the alphabet generates a free monoid, denoted as $\Gamma^*$ or $\langle \Gamma \rangle$. An element of the monoid $\Gamma^*$ is called word, and the identity element is called *empty word* and denoted by $\varepsilon$ or 1. A *group alphabet* is an alphabet augmented with inverse elements: $\Sigma = \{z_1, z_2, \ldots, z_k, \overline{z_1}, \overline{z_2}, \ldots, \overline{z_k}\}$, where $z_i$ and $\overline{z_i}$ (notation $\overline{z_i} = z_i^{-1}$ is also used) are assumed to satisfy $z_i\overline{z_i} = \overline{z_i}z_i = \varepsilon$. The relation between a letter and its inverse is the only nontrivial relation in a group alphabet. We denote $\Sigma^+ = \{a_1 \ldots a_n \mid a_i \in \Sigma, n \geq 1\}$. For a word $w = w_1 w_2 \cdots w_n$, we denote $\overline{w} = w^{-1} = \overline{w_n} \cdots \overline{w_2}\,\overline{w_1}$.

Let $\Sigma$ be a group alphabet. Using the notation of [1], we shall also introduce a reduction mapping which removes factors of the form $z\overline{z}$ for $z \in \Sigma$. To that end, we define the relation $\vdash \subseteq \Sigma^* \times \Sigma^*$ such that for all $w, w' \in \Sigma^*$, $w \vdash w'$ if and only if there exists $u, v \in \Sigma^*$ and $z \in \Sigma$ where $w = uz\overline{z}v$ and $w' = uv$. We

[1] The Identity Problem for matrix semigroups is a well-known challenging problem which is also equivalent to another fundamental problem in Group Theory: given a finitely generated matrix semigroup S, decide whether a subset of the generator of S generates a nontrivial group (Group Problem).

may then define by $\vdash^*$ the reflexive and transitive closure of $\vdash$. The following Lemma is well-known, see eg. [1] for the proof.

**Lemma 1.** *For each $w \in \Sigma^*$ there exists exactly one word $r(w) \in \Sigma^*$ such that $w \vdash^* r(w)$ does not contain any factor of the form $z\overline{z}$, with $z \in \Sigma$.*

The word $r(w)$ is called the reduced representation of word $w \in \Sigma^*$. As an example, we see that if $w = 132\overline{2}1\overline{1}\,\overline{3}\,\overline{1} \in \Sigma^*$, then $r(w) = \varepsilon$.

A homomorphism $h : \Gamma_1^* \to \Gamma_2^*$, between two monoids $\Gamma_1^*$ and $\Gamma_2^*$ is a mapping satisfying $h(ab) = h(a)h(b)$ for any $a, b \in \Gamma^*$ and $h(1) = 1$ where 1 denotes the identity element of the respective monoid. An injective homomorphism, $h'$, is called a *monomorphism* and is denoted $\Gamma_1^* \hookrightarrow \Gamma_2^*$.

Notation $\mathbb{Z}^{2\times 2}$ stands for the set of all $2 \times 2$ integer matrices. This set has a natural ring structure with respect to ordinary matrix addition and multiplication. A subset of $\mathbb{Z}^{2\times 2}$, $\mathrm{GL}_2(\mathbb{Z})$ (also denoted as $\mathrm{GL}(2,\mathbb{Z})$) stands for the *general linear group* over the ring of integers, meaning all $2 \times 2$ integer matrices having integer matrix inverses:

$$\mathrm{GL}_2(\mathbb{Z}) = \{A \in \mathbb{Z}^{2\times 2} \mid \det(A) \in \{-1, 1\}\}.$$

Group $\mathrm{GL}_2(\mathbb{Z})$ is clearly the largest multiplicative matrix group contained in $\mathbb{Z}^{2\times 2}$, but quite often it is useful to study its subgroup $\mathrm{SL}_2(\mathbb{Z})$ (also denoted as $\mathrm{SL}(2,\mathbb{Z})$), the *special linear group* defined as

$$\mathrm{SL}_2(\mathbb{Z}) = \{A \in \mathrm{GL}_2(\mathbb{Z}) \mid \det(A) = 1\}.$$

Furthermore, it turns out that the quotient group

$$\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\},$$

called the *projective special linear group* has a very useful representation as a free product of two cyclic groups of order 2 and 3.

Group $\mathrm{SL}_2(\mathbb{Z})$ is very important in number theory, and its structure has been studied extensively in various textbooks (see [14], for instance), but for pointing out the algorithmic complexity issues, we reproduce the structural properties most relevant to our study here.

Two structurally important elements of $\mathrm{SL}_2(\mathbb{Z})$ are

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Evidently $S^2 = -I$ (which implies $S^3 = -S$ and $S^4 = I$, so $S$ has order 4), whereas for each $n \in \mathbb{Z}$,

$$T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},$$

implying that $T$ has no finite order.

**Lemma 2.** $\mathrm{SL}_2(\mathbb{Z}) = \langle S, T \rangle$. *Furthermore, any matrix*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

*can be represented as*

$$A = S^{\gamma} T^{q_1} S^3 T^{q_2} S^3 \cdot \ldots S^3 T^{q_k} S^3 T^{q_{k+1}}, \tag{1}$$

*so that* $\gamma \in \{0, 1, 2, 3\}$, $q_i \in \mathbb{Z}$ *for some* $k \geq 0$.

It is worth noticing that even though all matrices $A \in \mathrm{SL}_2(\mathbb{Z})$ can be represented in terms of $S$ and $T$, the representation is by no means unique. A direct computation shows that, for example,

$$TST = ST^{-1}S^3.$$

For a more canonical representation, let

$$R = ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

Direct computation shows that

$$R^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad R^3 = -I,$$

implying that $R^6 = I$, so $R$ is of order 6. Since now $T = S^{-1}R = S^3R$, it follows that $\mathrm{SL}_2(\mathbb{Z}) = \langle S, R \rangle$, and that a representation of $A \in \mathrm{SL}_2(\mathbb{Z})$ in terms of $R$ and $S$ can be obtained by substituting $T = S^3R = -SR$ in (1). It is noteworthy that when substituting $T = -SR$ in (1), one can use $R^3 = -I$ and $S^2 = -I$ to get a representation

$$A = (-1)^{\gamma'} R^{n_0} S R^{n_1} S \cdot \ldots \cdot R^{n_{l-1}} S R^{n_l}, \tag{2}$$

where $\gamma' \in \{0, 1\}$, $n_i \in \{0, 1, 2\}$ and $n_i \in \{1, 2\}$ for $0 < i < l$. It turns out, that representation (2) for a given matrix $A \in \mathrm{SL}_2(\mathbb{Z})$ is unique, but it is very common to present this result ignoring the sign. For that purpose, we let $s = S\{\pm I\}$ and $r = R\{\pm I\}$ be the projections of $S$ and $R$ in $\mathrm{PSL}_2(\mathbb{Z})$.

**Lemma 3.** $\mathrm{PSL}_2(\mathbb{Z})$ *is a free product of* $\langle s \rangle = \{1, s\}$ *and* $\langle r \rangle = \{1, r, r^2\}$. *That is, if*

$$r^{n_0} s r^{n_1} s \cdot \ldots \cdot r^{n_{p-1}} s r^{n_p} = r^{m_0} s r^{m_1} s \cdot \ldots \cdot r^{m_{q-1}} s r^{m_q},$$

*where* $n_i, m_j \in \{0, 1, 2\}$ *and* $n_i$, $m_j \in \{1, 2\}$ *for* $0 < i < p$ *and* $0 < j < q$, *then* $p = q$ *and* $n_k = m_k$ *for each* $0 \leq k \leq p$.

For the proof of the lemma see [14]. We say that a representation in $\mathrm{PSL}_2(\mathbb{Z})$ is *reduced* if it satisfies the conditions of the previous lemma.

Mortality Problem: Decide whether a given finitely generated matrix semigroup contains the zero matrix.

## 3 The Mortality Problem

In this section we show that the mortality problem is NP-hard for a finite set of matrices from $\mathbb{Z}^{2\times 2}$. In order to prove this result, we shall adapt the proof technique used in [3] by showing a monomorphism (injective homomorphism) between an arbitrary sized alphabet and $\mathrm{PSL}_2(\mathbb{Z})$ with certain essential properties.

**Lemma 4.** *Given a group alphabet $\Sigma = \{z_1, z_2, \ldots, z_k, \overline{z_1}, \overline{z_2}, \ldots, \overline{z_k}\}$ and a binary group alphabet $\Sigma_2 = \{c, d, \overline{c}, \overline{d}\}$, then mapping $\alpha : \Sigma \to \Sigma_2^*$ defined by*

$$\alpha(z_i) = c^i d\overline{c}^i, \quad \alpha(\overline{z_i}) = c^i\overline{d}\overline{c}^i$$

*can be extended to a monomorphism $\alpha : \Sigma^* \hookrightarrow \Sigma_2^*$, see [4] for more details.*

**Lemma 5.** *Let $\Sigma_2 = \{c, d, \overline{c}, \overline{d}\}$ be a group alphabet. Then the mapping $\beta : \Sigma_2 \to \mathrm{PSL}_2(\mathbb{Z})$ defined by:*

$$\beta(c) = (rsr)^2, \quad \beta(d) = (rs)^2, \quad \beta(\overline{c}) = (r^2sr^2)^2, \quad \beta(\overline{d}) = (sr^2)^2$$

*can be extended to a monomorphism $\beta : \Sigma_2^* \hookrightarrow \mathrm{PSL}_2(\mathbb{Z})$.*

*Proof.* Recall that $\mathrm{PSL}_2(\mathbb{Z})$ has monoid presentation $\langle s, r | s^2 = r^3 = 1\rangle$, and let $w \in \{c, d, \overline{c}, \overline{d}\}^*$ be a reduced word (i.e., contains no subwords in $\{c\overline{c}, \overline{c}c, d\overline{d}, \overline{d}d\}$). It suffices to show that from $\beta(w)$, we can always deduce the initial symbol of $w \in \Sigma_2^*$.

This follows from a case analysis. The possible initial parts of $w$ can be discovered by computing all products $\beta(cc) = (rsr)^4 = rsr^2sr^2sr^2sr$, $\beta(cd) = (rsr)^2(rs)^2 = rsr^2sr^2srs$, $\beta(c\overline{d}) = rsr^2srsr^2sr^2$, $\beta(dc) = rsrsrsr^2sr$, $\beta(dd) = rsrsrsrs$, $\beta(d\overline{c}) = rsrsr^2srsr^2$, $\beta(\overline{c}d) = r^2sr^2s$, $\beta(\overline{cc}) = r^2srsrsrsr^2$, $\beta(\overline{c}\overline{d}) = r^2srsr^2sr^2sr^2$, $\beta(\overline{d}c) = srsr$, $\beta(\overline{d}\overline{c}) = sr^2srsrsr^2$, and $\beta(\overline{dd}) = sr^2sr^2sr^2sr^2$. The claim follows now from comparing the initial parts of the sequences (no-one is a prefix of another) and from the fact that $\mathrm{PSL}_2(\mathbb{Z}) = \langle s\rangle * \langle r\rangle$. □

*Example 1.* Let $w \in \{c, d, \overline{c}, \overline{d}\}$ and

$$\beta(w) = r^2sr^2srsr^2sr^2sr^2srsrsr^2srsrsrs.$$

As representation in $\mathrm{PSL}_2(\mathbb{Z})$ in this form is unique, we must conclude that $w$ begins with $\overline{c}$ (Only the image of $\overline{c}$ begins with $r^2$). To proceed, we introduce identity $1 = r^2sr^2rsr$ in the representation of $\beta(w)$ to see that

$$\begin{aligned}\beta(w) &= r^2sr^2(r^2sr^2rsr)srsr^2sr^2sr^2srsrsr^2srsrsrs\\ &= (r^2sr^2r^2sr^2)rsrsrsr^2sr^2sr^2srsrsr^2srsrsrs\\ &= \beta(\overline{c})rsrsrsr^2sr^2sr^2srsrsr^2srsrsrs.\end{aligned}$$

writing $w = \overline{c}w_1$ we see that

$$\beta(w_1) = rsrsrsr^2sr^2sr^2srsrsr^2srsrsrs,$$

and now we must have $w_1 = dw_2$, and

$$\beta(w_2) = rsr^2sr^2sr^2srsrsr^2srsrsrs$$

continuing in the same way we see that $w_2 = cw_3$,

$$\beta(w_3) = rsr^2srsrsr^2srsrsrs,$$

$w_3 = cw_4$,

$$\beta(w_4) = srsr^2srsrsrs,$$

and now $w_4$ must begin with $\overline{d}$. Again introducing identity $1 = rsr^2rsr^2$ we see that

$$\beta(w_4) = sr(rsr^2rsr^2)sr^2srsrsrs = (srrsr^2)rsr^2sr^2srsrsrs,$$

and if $w_4 = \overline{d}w_5$, then

$$\beta(w_5) = rsr^2sr^2srsrsrs,$$

and letting $w_5 = cw_6$

$$\beta(w_6) = rsrsrsrs = \beta(dd)$$

combining all letters we see that $w = \overline{c}dcc\overline{d}cdd$.

**Lemma 6.** *For any nonempty reduced word $w \in \Sigma^+$, $\beta \circ \alpha(w)$ has first letter $r$ and last letter $r$ in its reduced representation under* $\mathrm{PSL}_2(\mathbb{Z})$*, where $\beta \circ \alpha : \Sigma^* \to \mathrm{PSL}_2(\mathbb{Z})$.*

*Proof.* For each letter $z_i$ we have

$$\beta(\alpha(z_i)) = \beta(c^i d\overline{c}^i) = \beta(c)^i\beta(d)\beta(\overline{c})^i.$$

Now that $\beta(c)$ begins with $r$, so does $\beta(\alpha(z_i))$, for otherwise $\beta(\alpha(z_i))$ would have two representations, $\beta(\alpha(z_i)) = r\ldots$ and $\beta(\alpha(z_i)) = s\ldots$, contradicting Lemma 5. Similar conclusion can be made for the ending letter and for $\beta(\alpha(\overline{z_i}))$, as well. The result can be directly extended to words $w \in \Sigma^+$, as the failure of it would contradict Lemma 5 as well. □

We see that $\beta\circ\alpha : \Sigma^* \hookrightarrow \mathrm{PSL}_2(\mathbb{Z})$ is a monomorphism since it is the composition of two monomorphisms. We require the following lemma concerning the size of the matrix when $\beta \circ \alpha$ is applied to the power of a letter from $\Sigma$.

**Lemma 7.** *Given $\Sigma = \{z_1, z_2, \ldots, z_k, \overline{z_1}, \overline{z_2}, \ldots, \overline{z_k}\}$, for any letter $z_i \in \Sigma$:*

$$\beta \circ \alpha(z_i^j) = \{\pm I\} \begin{pmatrix} -8i^2j - 4ij - 1 & -8i^2j \\ 8i^2j + 8ij + 2j & 8i^2j + 4ij - 1 \end{pmatrix}$$

*Proof.* Let $\Sigma_2 = \{c, d, \overline{c}, \overline{d}\}$. Since $\alpha$ and $\beta$ are homomorphisms, we have that $\alpha(z_i^j) = \alpha(z_i)^j = c^i d^j \overline{c}^i$ and

$$\begin{aligned}\beta(\alpha(z_i^j)) &= \beta(c)^i\beta(d)^j\beta(\overline{c})^i \\ &= (rsr)^{2i}(rs)^{2j}(r^2sr^2)^{2i}\end{aligned}$$

Elementary matrix multiplication of $\beta \circ \alpha(z_i^j)$ reveals that

$$\begin{aligned}\beta \circ \alpha(z_i^j) &= (rsr)^{2i}(rs)^{2j}r^2(sr)^{2i}r \\ &= \{\pm I\}\begin{pmatrix} -8i^2j-4ij-1 & -8i^2j \\ 8i^2j+8ij+2j & 8i^2j+4ij-1 \end{pmatrix}\end{aligned}$$

We see that the size of the maximal element of the matrices $\beta(\alpha(z_i^j))$ is polynomial in $i$ and $j$ and thus $\text{size}(\beta(\alpha(z_i^j))) = O(i^2j)$. □

We need one final technical lemma concerning mapping $\beta \circ \alpha$.

**Lemma 8.** *For any nonempty reduced word $w \in \Sigma^+$, let $A = \beta \circ \alpha(w)$ where we ignore the sign of the matrix. Then $A_{11} \neq 0$ and $A_{12} \neq 0$.*

*Proof.* By Lemma 6, we have that $\beta \circ \alpha(w)$ has first letter $r$ and last letter $r$ in its reduced representation under $\text{PSL}_2(\mathbb{Z})$. Thus we see that

$$\begin{aligned}A = RXR &= \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} -d & c-d \\ b+d & b+d-a-c \end{pmatrix},\end{aligned}$$

for some matrix $X \in \text{SL}_2(\mathbb{Z})$ (again we are ignoring the sign in this product).

We first prove $A_{12} \neq 0$. By the above formula, $A_{12} = 0$ implies $c - d = 0$. Since $\det(X) = 1$, $ad - bc = 1$ implies $c(a-b) = 1$, thus either $c = d = 1$ and $b = a - 1$, or else $c = d = -1$ and $b = a + 1$. Therefore either:

$$A = R\begin{pmatrix} a & a-1 \\ 1 & 1 \end{pmatrix}R \quad \text{or} \quad A = R\begin{pmatrix} a & a+1 \\ -1 & -1 \end{pmatrix}R.$$

It is not hard to see that matrices $X$ of this form have factorizations $(SR)^xR$ or $(RRS)^xR$ for some $x > 0$. This holds since:

$$(SR)^kR = (-1)^k\begin{pmatrix} k & k-1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad (RRS)^kR = (-1)^k\begin{pmatrix} -k & -(k+1) \\ 1 & 1 \end{pmatrix}$$

and under $\text{PSL}_2(\mathbb{Z})$ we factor out $-I$ and can therefore ignore the sign. Thus, we see that $A = R(SR)^xRR$ or $A = R(RRS)^xRR$ for some $x > 0$. However, these are not reduced representations (since they have $R^3$ on the left or right) and since these reduced factorizations are unique, this contradicts Lemma 6 since under $\text{PSL}_2(\mathbb{Z})$ A would start with $s$.

We now prove $A_{11} \neq 0$. Clearly $A_{11} = 0$ implies $d = 0$. Since $\det(A) = 1$, then $b = \pm 1$ and $c = \mp 1$. Thus $A = \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & x \end{pmatrix}$ for some $x \in \mathbb{Z}$. Now, such $A$ have reduced factorization (up to sign) of $(RS)^aR$ where $a \geq 0$ or $(SRR)^aS$ where $a > 0$ which is easy to check via straight forward matrix calculations. However, Lemma 6 shows that $A$ should end with '$r$' in its reduced representation under

$\mathrm{PSL}_2(\mathbb{Z})$, thus it must be of the form $(RS)^a R$. It is not hard to see however that $(rs)^a r \notin \{\beta(w) \mid w \in \Sigma_2^+\}$ for any $a \geq 0$. This follows because $\beta(w) = (rs)^a r = \beta(d)(rs)^{a-2} r = \ldots = \beta(d)^{a/2} r$ which cannot be further factorized giving a contradiction. □

Combining this information, we now have the following four essential properties:

i) $\beta \circ \alpha : \Sigma^* \hookrightarrow \mathrm{PSL}_2(\mathbb{Z})$ is a monomorphism by Lemma 4 and Lemma 5.

ii) For all nonempty reduced $w \in \Sigma^+$, $\beta \circ \alpha(w)$ has reduced representation $rw'r$ over $\mathrm{PSL}_2(\mathbb{Z}) \cong \langle s, r | s^2 = r^3 = 1\rangle$ for some $w' \in \{s, r\}^*$. This follows from Lemma 6.

iii) For any $z_i \in \Sigma$, the size of matrices in $\beta \circ \alpha(z_i^j)$ in terms of the number of bits to represent it is logarithmic in terms of $i$ and $j$. This follows from Lemma 7.

iv) For any nonempty reduced word $w \in \Sigma^+$, the upper left and upper right entries of matrices $\beta \circ \alpha(w)$ are nonzero by Lemma 8.

We are now ready to prove the main result of this section.

**Theorem 1.** *The mortality problem for matrices in $\mathbb{Z}^{2\times 2}$ is NP-hard.*

*Proof.* We adapt the proof from [3] which shows that the identity problem in $\mathbb{Z}^{2\times 2}$ is NP-hard. The proof in [3] essentially consists of two parts. First, an encoding is shown from the subset sum problem to a problem on words - given a finite set of words, can they be combined in such a way as to reach the identity (or empty) word. The number of letters in these words is exponential in the representation size of the subset sum problem instance however.

Therefore the second half of the proof shows a mapping from this set of words into $\mathbb{Z}^{2\times 2}$ such that the matrix representation of the words has size polynomial in the subset sum problem instance. The set of matrices generate a semigroup containing the identity matrix if and only if the subset sum problem has a solution, thus the identity problem is NP-hard for 2 × 2 matrix semigroups.

For our purposes of the mortality problem, we shall use the identical first part of the proof to give a set of words $W$ encoding a subset sum problem instance. We shall then define a matrix $P$ and use mapping $\beta \circ \alpha : \Sigma^* \hookrightarrow \mathrm{PSL}_2(\mathbb{Z})$ and its properties to encode the set of words $W$ in such a way that the zero matrix is in the semigroup generated by a certain set of matrices if and only if there exists a solution to the subset sum problem.

Let $\Sigma = \{1, 2, \ldots, 2k+2, \overline{1}, \overline{2}, \ldots, \overline{(2k+2)}, a, b, \overline{a}, \overline{b}\}$ be an alphabet. The subset sum instance is given by $S = \{s_1, s_2, \ldots, s_k\}$ and value $x$ - thus the problem is: does there exist a subset of $S$ whose sum is $x$? We now define set of words:

$$W = \begin{array}{ll}
\{1 \cdot a^{s_1} \cdot \overline{2}, & 1 \cdot \varepsilon \cdot \overline{2}, \\
2 \cdot a^{s_2} \cdot \overline{3}, & 2 \cdot \varepsilon \cdot \overline{3}, \\
\vdots & \vdots \\
k \cdot a^{s_k} \cdot \overline{(k+1)}, & k \cdot \varepsilon \cdot \overline{(k+1)}, \\
(k+1) \cdot \overline{a}^x \cdot \overline{(k+2)}, & \\
(k+2) \cdot b^{s_1} \cdot \overline{(k+3)}, & (k+2) \cdot \varepsilon \cdot \overline{(k+3)}, \\
(k+3) \cdot b^{s_2} \cdot \overline{(k+4)}, & (k+3) \cdot \varepsilon \cdot \overline{(k+4)}, \\
\vdots & \vdots \\
(2k+1) \cdot b^{s_k} \cdot \overline{(2k+2)}, & (2k+1) \cdot \varepsilon \cdot \overline{(2k+2)}, \\
(2k+2) \cdot \overline{b}^x \cdot \overline{1}\} \subseteq \Sigma^* &
\end{array}$$

It was proven in [3] that $\varepsilon \in W^+$ if and only if the subset sum instance $S$ has a solution. We shall not repeat the details here, suffice it to say that letters $\{1, \ldots, 2k+2, \overline{1}, \ldots, \overline{2k+2}\}$ act as 'border letters' which enforce a particular ordering on any possible words reducing to give $\varepsilon$. In any such word $w' = w_1 w_2 \cdots w_l \in W^+$ such that $r(w') = \varepsilon$, we can assume by [3] that $w_1$ is from the first row of $W$ (above), $w_2$ is from the second row etc. and that $w_l = (2k+2) \cdot \overline{b}^x \cdot \overline{1}$, thus $l = 2k+2$.

We now use mapping $\beta \circ \alpha : \Sigma^* \hookrightarrow \mathrm{PSL}_2(\mathbb{Z})$ applied to set of words $W$. We earlier defined this function on a different alphabet but the same analysis holds.

Since any element $a$ in $\mathrm{PSL}_2(\mathbb{Z})$ already is a set $\{A, -A\}$ of two matrices in $\mathrm{SL}_2(Z)$ we set $M$ in a way that it will actually contain $2|W|$ matrices. It does not alter this construction, since it does not matter if you select $A$ or $-A$ in the product. Specifically we have

$$M = \{\beta \circ \alpha(w) | w \in W\} \subseteq \mathbb{Z}^{2 \times 2},$$

thus $|M| = 2|W|$. Note that each $w \in W$ contains two border letters and possibly a power of a single letter from $\Sigma$. By Lemma 7, this implies that the size of the matrices in $M$ (i.e. number of bits required to represent them) is polynomial in the number of bits to represent the subset sum problem instance.

Our next steps are to introduce a new matrix $P$ and to modify one of the matrices in $M$ by right multiplying by matrix $S$ which will make it possible to reach the zero matrix if and only if $I \in \langle M \rangle$.

Let $P = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and define $M' = M \cup \{P\}$. For any matrix $X \in \mathbb{Z}^{2 \times 2}$ we have that $(PXP)_{11} = X_{11}$ and $(PXP)_{12} = (PXP)_{21} = (PXP)_{22} = 0$. Since for any reduced word $w \in W^+$, we have that $\beta \circ \alpha(w)_{11} \neq 0$ by Lemma 8, and all matrices in $M$ are unimodular, then the zero matrix is not in $\langle M' \rangle$.

We now modify the matrix set $M'$ one final time. Let $Y$ be the matrix in $M'$ corresponding to word $(2k+2) \cdot \overline{b}^x \cdot \overline{1} \in W$. We now form set $M'' = (M' \setminus \{Y\}) \cup \{YS\}$, i.e. we replace $Y$ in $M'$ by $YS$. Since all other matrices in $M'$ have reduced factorizations of the form $RX'R$ for some $X' \in \{S, R\}^*$, the right multiplication of $Y$ by $S$ in this way does not allow any additional cancelation of elements. More formally, for any non-identity $X_1 Y \in \langle M' \rangle$ and $X_2 \in \langle M' \rangle$ Lemma 6 shows that we have reduced representations $X_1 Y = RX_1'R$ and $X_2 = RX_2'R$ for some $X_1' \in \{S,R\}^*$ and $X_2' \in \{S,R\}^*$. Therefore, under $M''$, since we replace $Y$ by $YS$, then $X_1(YS)X_2 = RX_1'R \cdot S \cdot RX_2'R$ is also a reduced representation and no cancelation has occured by replacing $Y$ with $YS$.

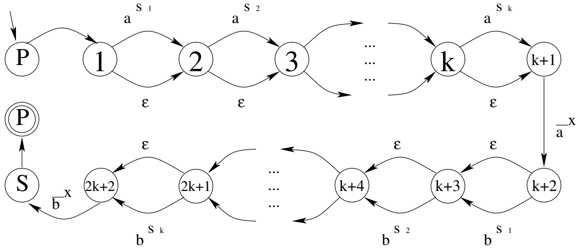

**Fig. 1.** The structure of a solution to the mortality problem

By Lemma 6, all non-identity matrices in $M'$ have reduced (and unique) factorization $RXR$ over $\{R,S\}$ for some $X \in \{S,R\}^*$. The only matrix in $M'$ with a zero upper right corner (up to sign) is the identity matrix by Lemma 8. From the proof of NP-hardness of the identity problem in [3], any reduced word in $W^+$ equal to the empty word must be of the form $w'((2k+2) \cdot \overline{b}^x \cdot \overline{1})$ for some $w' \in W^+$, in other words the last word from $W$ used must be $(2k+2) \cdot \overline{b}^x \cdot \overline{1}$. This word was represented by matrix $Y$ under $M'$, which we replaced with $YS$ in $M''$. Thus, let $VY \in \langle M' \rangle$ be a product equal to the identity matrix. Therefore we see that $S = VYS \in \langle M'' \rangle$ and therefore $PVYSP = PSP$ is the zero matrix as required. This follows since

$$\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} S = \begin{pmatrix} x_{12} & -x_{11} \\ x_{22} & -x_{21} \end{pmatrix} \tag{3}$$

The structure of such a product $PVYSP$ can be seen in Figure 1. To reach the zero matrix, we first use matrix $P$. We follow that by the matrix corresponding to either word $1 \cdot a^{s_1} \cdot \overline{2}$ or word $1 \cdot \varepsilon \cdot \overline{2}$, meaning we move from node 1 to node 2 and choose either $a^{s_1}$ or else $\varepsilon$. This continues iteratively until we reach node $k+1$ at which point we move to $k+2$ with word $\overline{a}^x$. At this point, if the selected nonempty words are such that $a^{s_{j1}} a^{s_{j2}} \cdots a^{s_{jm}} \cdot \overline{a}^x = \varepsilon$ for some $1 \leq s_{j1} < s_{j2} < \ldots < s_{jm} \leq k$, then this corresponds to a correct solution to the subset sum problem instance. The same procedure holds between nodes $k+2$ and $2k+2$ (with $a$'s replaced by $b$'s) at which point we then use matrix $S$ and the final matrix $P$. In the diagram, nodes 1 to $2k+1$ correspond to matrix $V$ and nodes $2k+2$ and $S$ correspond to matrices $Y$ and $S$ respectively. □

Since an upper bound for the decidability result in [12] is unknown, we now consider a lower bound on the minimum length solution to the Mortality Problem. Below we derive a lower bound on the minimum length solution to the Mortality Problem for a constructible set of instances, which is *exponential* in the number of matrices of the generator set and the maximal element of the matrices. This bound shows that the most obvious candidate for an NP algorithm, which is to guess the shortest sequence of matrices which multiply to give the zero matrix, does not work correctly since the certificate would have a length which is exponential in the size of the instance.

**Theorem 2.** *There exists a set of matrices $M = \{M_1, M_2, \ldots, M_n\} \subseteq \mathbb{Z}^{2\times 2}$ where the maximum element of any matrix in $M$ is $O(n^2)$ such that $0 \in \langle M \rangle$ (where $0$ here denote the zero matrix) and the minimal length product over $M$ equal to $0$ is of length $2^n$, which is exponential in the number of matrices in the generator and the maximal element of any matrix in $M$.*

*Proof.* Let $\Sigma = \{1, 2, \ldots, 2n-1, \overline{1}, \overline{2}, \ldots, \overline{2n-1}\}$ be a group alphabet. It is proven in [3] that there exists a set of words $V = \{v_1, v_2, \ldots, v_{2n-2}\} \subseteq \Sigma^3$ such that there exists $w \in V^+$ where $r(w) = \varepsilon$ and $|w| = 2^n - 2$ and for all $w' \in V^+$ such that $|w'| < 2^n - 2$, then $r(w') \neq \varepsilon$. This results from an encoding of a deterministic finite automaton introduced in [1].

First, we encode set of words $V$ into matrices. We apply monomorphism $\beta \circ \alpha : \Sigma^* \hookrightarrow \mathrm{PSL}_2(\mathbb{Z})$ to the set of words $V$ to give

$$V' = \{\beta \circ \alpha(v) | v \in V\} \subseteq \mathrm{PSL}_2(\mathbb{Z})$$

From the encoding of the DFA used in [3], it is shown that for any $w \in V^+$ where $r(w) = \varepsilon$, we may assume that the last letter of $w$ is $v_{2n-2}$. We proceed in a similar manner to that of the proof of Theorem 1. We form the set

$$V'' = (V' \setminus \{\beta \circ \alpha(v_{2n-2})\}) \cup \{\beta \circ \alpha(v_{2n-2})S\},$$

i.e. we right multiply the final matrix of set $V'$ by matrix $S$. Finally, we define matrix $P \in \mathbb{Z}^{2\times 2}$ such that $P_{11} = 1$ and $P_{12} = P_{21} = P_{22}$ and let $V''' = V'' \cup \{P\}$.

For any $w \in V^+$ such that $r(w) = \varepsilon$, then $\beta \circ \alpha(w) = \pm I$ and thus $\beta \circ \alpha(w)S \in V'''$ with $|w| \geq 2^n - 2$. Clearly,

$$P(\beta \circ \alpha(w))SP = \beta \circ \alpha(w)_{12},$$

which equals 0 if and only if $r(w) = \varepsilon$ by Lemma 8 and the number of matrices used is $2^n$. For all $X \in V'''$, then $X_{11} \neq 0$ by Lemma 8 and Equation (3). Thus only matrix $S \in V'''$ is such that $PSP = 0$ where 0 is here the zero matrix.

Finally we need to consider the representation size of $V'''$. Lemma 7 shows that for $|\Sigma| = 4n - 2$, we have that $\mathrm{size}(\beta \circ \alpha(x)) = O(n^2)$ for any $x \in \Sigma$. Since $|V'''| = 2n - 1$, then $\mathrm{size}(V''') = O(n^3)$ where size denotes the number of bits required to represent set $V'''$. □

## References

1. Ang, T., Pighizzini, G., Rampersad, N., Shallit, J.: Automata and reduced words in the free group. arXiv:0910.4555 (2009)
2. Bell, P.C., Potapov, I.: 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)
3. Bell, P.C., Potapov, I.: On the computational complexity of matrix semigroup problems. Fundamenta Informaticae 116(1-4), 1–13 (2012)
4. Birget, J.-C., Margolis, S.: Two-letter group codes that preserve aperiodicity of inverse finite automata. Semigroup Forum 76(1), 159–168 (2008)
5. Blondel, V., Tsitsiklis, J.: When is a pair of matrices mortal? Information Processing Letters 63, 283–286 (1997)
6. Blondel, V., Tsitsiklis, J.: The boundedness of all products of a pair of matrices is undecidable. Systems and Control Letters 41(2), 135–140 (2000)
7. Bournez, O., Branicky, M.: On the mortality problem for matrices of low dimensions. Theory of Computing Systems 35(4), 433–448 (2002)
8. Cai, J.-Y., Liu, Z.: The bounded membership problem of the monoid $\mathrm{SL}_2(N)$. Mathematical Systems Theory 29(6), 573–587 (1996)
9. Choffrut, C., Karhumäki, J.: Some decision problems on integer matrices. Informatics and Applications 39, 125–131 (2005)
10. Krom, M.: An unsolvable problem with products of matrices. Mathematical Systems Theory 14, 335–337 (1981)
11. Miller, M.A.: Mortality for sets of 2x2 matrices. Mathematics Magazine 67(3), 210–213 (1994)
12. Nuccio, C., Rodaro, E.: Mortality Problem for 2 x 2 Integer Matrices. In: Geffert, V., Karhumäki, J., Bertoni, A., Preneel, B., Návrat, P., Bieliková, M. (eds.) SOFSEM 2008. LNCS, vol. 4910, pp. 400–405. Springer, Heidelberg (2008)
13. Paterson, M.S.: Unsolvability in 3 x 3 matrices. Studies in Applied Mathematics 49, 105–107 (1970)
14. Rankin, R.: Modular Forms and Functions. Cambridge University Press, Cambridge (1977)