RAIRO-Theor. Inf. Appl. 46 (2012) 355–399
DOI: 10.1051/ita/2012010

Available online at:
www.rairo-ita.org

ON THE DECIDABILITY OF SEMIGROUP FREENESS *

Julien Cassaigne[1] and Francois Nicolas[2]

Abstract. This paper deals with the decidability of semigroup freeness. More precisely, the freeness problem over a semigroup S is defined as: given a finite subset $X \subseteq S$, decide whether each element of S has at most one factorization over X. To date, the decidabilities of the following two freeness problems have been closely examined. In 1953, Sardinas and Patterson proposed a now famous algorithm for the freeness problem over the free monoids. In 1991, Klarner, Birget and Satterfield proved the undecidability of the freeness problem over three-by-three integer matrices. Both results led to the publication of many subsequent papers. The aim of the present paper is (*i*) to present general results about freeness problems, (*ii*) to study the decidability of freeness problems over various particular semigroups (special attention is devoted to multiplicative matrix semigroups), and (*iii*) to propose precise, challenging open questions in order to promote the study of the topic.

Mathematics Subject Classification. 20M05, 03B25, 15A30.

1. Introduction

We first introduce basic notation and definitions; the organization of the paper is more precisely described in Section 1.3.

Keywords and phrases. Decidability, semigroup freeness, matrix semigroups, Post correspondence problem.

* *Most of the research was achieved while the authors were visiting the University of Turku. The Academy of Finland supported the work under grants 203354 and 7523004.*

[1] Institut de mathématiques de Luminy, case 907, 163 avenue de Luminy, 13288 Marseille Cedex 9, France. cassaigne@iml.univ-mrs.fr

[2] Lehrstuhl für Bioinformatik, Friedrich-Schiller-Universität Jena, Ernst-Abbe-Platz 2, 07743 Jena, Germany. francois.nicolas@uni-jena.de

Article published by EDP Sciences

As usual, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote the semiring of naturals, the ring of integers, the field of rational numbers, the field of real numbers, and the field of complex numbers, respectively. For all m, $n \in \mathbb{Z}$, $[\![m, n]\!]$ denotes the set of all $k \in \mathbb{N}$ such that $m \leq k \leq n$. Unless otherwise stated, the additive and multiplicative identity elements of any semiring are simply denoted 0 and 1, respectively. The letter O denotes any matrix whose entries are all 0.

A *word* is a finite sequence of symbols called its letters. The *empty word* is denoted ε. For every word w, the *length* of w is denoted $|w|$; for every symbol a, $|w|_a$ denotes the number of occurrences of a in w. An *alphabet* is a (finite or infinite) set of symbols. The canonical alphabet is the binary alphabet $\{\mathtt{0}, \mathtt{1}\}$.

1.1. Free semigroups and codes

1.1.1. *Definitions*

A *semigroup* is a set equipped with an associative binary operation. Unless otherwise stated, semigroup operations are denoted multiplicatively.

Definition 1.1 (code)**.** Let S be a semigroup and let X be a subset of S. We say that X is a *code* if the property

$$x_1 x_2 \dots x_m = y_1 y_2 \dots y_n \iff (x_1, x_2, \dots, x_m) = (y_1, y_2, \dots, y_n)$$

holds for any integers m, $n \geq 1$ and any elements x_1, x_2, $\dots$, x_m, y_1, y_2, $\dots$, $y_n \in X$.

Note that $(x_1, x_2, \dots, x_m) = (y_1, y_2, \dots, y_n)$ means that both $m = n$ and $x_i = y_i$ for every $i \in [\![1, m]\!]$. Informally, a set is not a code iff its elements satisfy a non-trivial equation. Or, in other words, a subset X of a semigroup S is a code iff no element of S has more than one factorization over X.

For every semigroup S and every subset $X \subseteq S$, X^+ denotes the closure of X under the semigroup operation: X^+ is the subsemigroup of S generated by X, and as such, it is equipped with the semigroup operation induced by the operation of S.

Definition 1.2 (free semigroup)**.** A semigroup S is called *free* if there exists a code $X \subseteq S$ such that $S = X^+$.

In other words, a semigroup is free iff it is generated by a code.

A semigroup with an identity element is called a *monoid*. Many semigroups mentioned in the paper are monoids. For every monoid M and every subset $X \subseteq M$, $X^\star$ denotes the set X^+ augmented with the identity element of M. A monoid M is called *free* if there exists a code $X \subseteq M$ such that $M = X^\star$.

Remark 1.3. No monoid is a free semigroup.

1.1.2. Illustration

Let Σ be an alphabet. The set of all words over Σ is a free monoid under concatenation with ε as identity element and Σ as generating code. In accordance with our notation, this monoid is denoted as usual $\Sigma^\star$. In the same way, the set of all non-empty words over Σ equals Σ^+ and is a free semigroup. Both examples of free monoid and free semigroup are canonical (see Sect. 1.4.3).

A subset of $\Sigma^\star$ is called a *language* over Σ. In the context of combinatorics on words, the term "code" was originally introduced to denote those languages that are codes under concatenation. This particular topic has been widely studied [4]. A *prefix code* over Σ is a subset $X \subseteq \Sigma^+$ such that for every $x \in X$ and every $s \in \Sigma^+$, $xs \notin X$. It is clear that any prefix code is a code under concatenation.

Example 1.4. Consider the semigroup $\mathbb{W} := \{\mathtt{0},\mathtt{1}\}^\star$. The three subsets $\{\mathtt{00},\mathtt{01},\mathtt{10},\mathtt{11}\}$, $\{\mathtt{01},\mathtt{011},\mathtt{11}\}$ and $\{\mathtt{0}^n\mathtt{1} : n \in \mathbb{N}\}$ of $\mathbb{W}$ are codes under concatenation, but $\{\mathtt{01},\mathtt{10},\mathtt{0}\}$ is not: $\mathtt{0}(\mathtt{10}) = (\mathtt{01})\mathtt{0}$.

For any two semigroups S_1 and S_2, define the *direct product* of S_1 and S_2 as the Cartesian product $S_1 \times S_2$ equipped with the componentwise semigroup operation derived from the operations of S_1 and S_2: for any two elements (x_1, x_2) and (y_1, y_2) of $S_1 \times S_2$, the product $(x_1, x_2)(y_1, y_2)$ is defined as (x_1y_1, x_2y_2).

Example 1.5. Consider the semigroup $\mathbb{W} \times \mathbb{W}$. Both subsets $\{(\mathtt{0},\mathtt{1}),(\mathtt{1},\mathtt{0})\}$ and $\{(\mathtt{0},\mathtt{0}),(\mathtt{1},\mathtt{01}),(\mathtt{01},\mathtt{10})\}$ of $\mathbb{W} \times \mathbb{W}$ are codes under componentwise concatenation but $\{(\mathtt{0},\mathtt{0}),(\mathtt{1},\mathtt{101}),(\mathtt{01},\mathtt{01})\}$ is not: $(\mathtt{0},\mathtt{0})(\mathtt{1},\mathtt{101})(\mathtt{01},\mathtt{01}) = (\mathtt{01},\mathtt{01})(\mathtt{0},\mathtt{0})(\mathtt{1},\mathtt{101})$.

Let D be a semiring and let $D^{d\times d}$ denote the set of all d-by-d matrices over D: $D^{d\times d}$ is a semiring under the usual matrix operations, so in particular, $D^{d\times d}$ is a multiplicative semigroup.

Example 1.6. Consider the semigroup $\mathbb{N}^{2\times 2}$. Let k be an integer greater than 1. The subsets

$$\left\{ \begin{bmatrix} k & i \\ 0 & 1 \end{bmatrix} : i \in [\![0, k-1]\!] \right\}$$

and

$$\left\{ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\}$$

of $\mathbb{N}^{2\times 2}$ are codes under matrix multiplication [11] but

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} \right\}$$

is not:

$$\begin{bmatrix}1&3\\0&1\end{bmatrix}\begin{bmatrix}1&0\\0&2\end{bmatrix}=\begin{bmatrix}1&0\\0&2\end{bmatrix}\begin{bmatrix}1&3\\0&1\end{bmatrix}\begin{bmatrix}1&3\\0&1\end{bmatrix}.$$

1.2. Freeness problems

Our aim is to study the decidability of freeness problems over various semigroups:

Definition 1.7. Let S be a semigroup with a recursive underlying set. The *freeness problem over* S, denoted $\textsc{Free}\big[S\big]$, is: given a finite subset $X \subseteq S$, decide whether X is a code. For every integer $k \geq 1$, define $\textsc{Free}(k)\big[S\big]$ as the following problem: given a k-element subset $X \subseteq S$, decide whether X is a code.

For every integer $k \geq 1$, $\textsc{Free}(k)\big[S\big]$ is a restriction of $\textsc{Free}\big[S\big]$.

Remark 1.8. Let S be a semigroup with a recursive underlying set. $\textsc{Free}\big[S\big]$ should not be confused with the following problem, which is not the concern of the paper: given a finite subset $X \subseteq S$, decide whether X^+ is a free semigroup. For any a, $b \in S$ such that $\{a, b\}$ is a code, $\{a, b, ab\}$ is not a code but $\{a, b, ab\}^+$ is a free semigroup. In general, for every subset of $X \subseteq S$, the semigroup X^+ is free iff there exists a code $Y \subseteq X$ such that $X \subseteq Y^+$.

Let us now present some relevant examples of freeness problems.

Example 1.9. The decidability of $\textsc{Free}\big[\Sigma^\star\big]$ for any finite alphabet Σ was proven by Sardinas and Patterson in 1953. Efficient polynomial-time algorithms were proposed afterwards [4].

Example 1.10. For any alphabet Σ and any x, $y \in \Sigma^\star$ with $x \neq y$, the following three assertions are equivalent:

(1) $\{x, y\}$ is not a code,
(2) $xy = yx$, and
(3) there exist $s \in \Sigma^\star$ and p, $q \in \mathbb{N}$ such that $x = s^p$ and $y = s^q$ [4, 32, 33].

More generally, let Σ_1, Σ_2, $\ldots$, Σ_d be d alphabets, and let $\mathbf{x} = (x_1, x_2, \ldots, x_d)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_d)$ be two elements of $\Sigma_1^\star \times \Sigma_2^\star \times \cdots \times \Sigma_d^\star$. The 2-element set $\{\mathbf{x}, \mathbf{y}\}$ is not a code iff $x_i y_i = y_i x_i$ for every $i \in [\![1, d]\!]$. Hence, if Σ_i is finite for every $i \in [\![1, d]\!]$ then $\textsc{Free}(2)\big[\Sigma_1^\star \times \Sigma_2^\star \times \cdots \times \Sigma_d^\star\big]$ is decidable. In Section 7, we prove that $\textsc{Free}\big[\mathbb{W} \times \mathbb{W}\big]$ is undecidable.

Example 1.11. For each integer $d \geq 1$, $\textsc{Free}(1)\big[\mathbb{Q}^{d\times d}\big]$ is decidable in polynomial time [35] (see also Sect. 2). However, Klarner, Birget, and Satterfield proved in 1991 that $\textsc{Free}\big[\mathbb{N}^{3\times 3}\big]$ is undecidable. More precisely, $\textsc{Free}(k)\big[\mathbb{N}^{3\times 3}\big]$ is decidable for at most finitely many integers $k \geq 1$ [11, 22] (see also Sect. 7).

1.3. Contribution

The paper is divided into eight sections.

Section 1

In the remainder of this section, we first state some useful, basic facts about semigroup morphisms (Sect. 1.4). Then, a list of previously studied problems related to the combinatorics of semigroups is presented to broaden the discussion (Sect. 1.5).

Section 2

A square matrix X is called torsion if there exist two integers p, $q \geq 1$ such that $X^p = X^{p+q}$; equivalently, X is torsion iff the singleton $\{X\}$ is not a code under matrix multiplication. Problems related with matrix torsion are thoroughly studied.

Section 3

We first prove that for any semigroup S and any subset $X \subseteq S$ with cardinality greater than 1, X is not a code iff the elements of X satisfy a non-trivial *balanced* equation. We then explore the consequences of the latter statement. The most interesting of them is that, for every integer $d \geq 1$, $\textsc{Free}\big[\mathbb{Q}^{d\times d}\big]$ reduces to $\textsc{Free}\big[\mathbb{Z}^{d\times d}\big]$.

Section 4

We show that $\textsc{Free}\big[\mathrm{GL}(2,\mathbb{Z})\big]$ is decidable, and that for every finite alphabet Σ, $\textsc{Free}\big[\,\mathrm{FG}(\Sigma)\big]$ is decidable in polynomial time, where $\mathrm{FG}(\Sigma)$ denotes the free group over Σ. The latter result generalizes Example 1.9. Both proofs rely on automata theory.

Section 5

We first show that the following seemingly obvious statement is wrong: for any semigroup S with a recursive underlying set and any integer $k \geq 1$, the decidability of $\textsc{Free}(k+1)\big[S\big]$ implies the decidability of $\textsc{Free}(k)\big[S\big]$. We then prove that, for any semigroup S with a computable operation, either $\textsc{Free}(k)\big[S\big]$ is decidable for every integer $k \geq 2$, or $\textsc{Free}(k)\big[S\big]$ is undecidable for infinitely many integers $k \geq 2$.

Section 6

The decidability of $\textsc{Free}\big[\mathbb{N}^{2\times 2}\big]$ is a very exciting but difficult open question [8, 11, 15, 30]. New ideas to tackle the problem are proposed.

Section 7

We prove that both $\textsc{Free}(k)\big[\mathbb{W} \times \mathbb{W}\big]$ and $\textsc{Free}(k)\big[\mathbb{N}^{3\times 3}\big]$ are undecidable for every integer $k \geq 13$. The undecidabilities of $\textsc{Free}(13)\big[\mathbb{W} \times \mathbb{W}\big]$ and $\textsc{Free}(13)\big[\mathbb{N}^{3\times 3}\big]$ where previously unknown.

Section 8

We complete the picture of undecidability for freeness problems over matrix semigroups: we prove that $\textsc{Free}(7+h)\big[\mathbb{N}^{6\times 6}\big]$, $\textsc{Free}(5+h)\big[\mathbb{N}^{9\times 9}\big]$, $\textsc{Free}(4+h)\big[\mathbb{N}^{12\times 12}\big]$, $\textsc{Free}(3+h)\big[\mathbb{N}^{18\times 18}\big]$, and $\textsc{Free}(2+h)\big[\mathbb{N}^{36\times 36}\big]$ are undecidable for every $h \in \mathbb{N}$.

Open questions

Relevant open questions are stated all along the paper.

1.4. Semigroup morphisms

1.4.1. Definition

Let S and S' be two semigroups. A function $\sigma\colon S \to S'$ is called a *morphism* if for all x, $y \in S$, $\sigma(xy) = \sigma(x)\sigma(y)$. Note that even if both S and S' are monoids, a morphism from S to S' does not necessarily map the identity element of S to the identity element of S': "morphism" always means "semigroup morphism" but not necessarily "monoid morphism". The following two claims are explicitly or implicitly used many times throughout the paper.

Claim 1.12 (universal property)**.** Let $\varSigma$ be an alphabet and let S be a semigroup. For any function $s\colon \varSigma \to S$, there exists exactly one morphism $\sigma\colon \varSigma^+ \to S$ such that $\sigma(a) = s(a)$ for every $a \in \varSigma$.

Claim 1.13. Let S and S' be two semigroups, let $\sigma\colon S \to S'$ be a morphism, and let X be a subset of S. The following two assertions are equivalent:

(1) σ is injective on X and $\sigma(X)$ is a code;
(2) σ is injective on X^+ and X is a code.

1.4.2. Freeness problems as morphism problems

Let S be a semigroup with a recursive underlying set and let $\varSigma$ be a finite alphabet. Although the set of all functions from $\varSigma^+$ to S has the power of the continuum whenever S is non-trivial, the restriction of σ to $\varSigma$ provides a finite encoding of σ for any morphism $\sigma\colon \varSigma^+ \to S$. From now on such encodings are considered as canonical. Hence, $\textsc{Free}\big[S\big]$ can be restated as follows: given a finite alphabet $\varSigma$ and a morphism $\sigma\colon \varSigma^+ \to S$, decide whether σ is injective. In the same way, for every positive integer k, an alternative formulation of $\textsc{Free}(k)\big[S\big]$ is: given an alphabet $\varSigma$ with cardinality k and a morphism $\sigma\colon \varSigma^+ \to S$, decide whether σ is injective.

1.4.3. The free semigroup and the free monoid structures

A bijective morphism is called an *isomorphism*. The inverse function of any isomorphism is also an isomorphism. A semigroup S is free iff for some alphabet Σ, there exists an isomorphism from Σ^+ onto S. A monoid M is free iff for some alphabet Σ, there exists an isomorphism from $\Sigma^\star$ onto M. Given a monoid M and an alphabet Σ, every morphism from M to $\Sigma^\star$ maps the identity element of M to the empty word. Since $\mathbb{W}$ contains infinite codes, *e.g.*, the prefix code $\{\mathtt{0}^n\mathtt{1} : n \in \mathbb{N}\}$, we may state:

Claim 1.14. For any finite or countable alphabet Σ, there exists an injective morphism from $\Sigma^\star$ to $\mathbb{W}$.

1.5. Other decision problems

The decision problems that are stated in this section are related to the combinatorics of semigroups. Although they do not play any crucial role in the paper, it is interesting to compare their properties with the ones of the freeness problems.

1.5.1. Mortality [40]

Let S be a semigroup. A *zero element* of S is an element $z \in S$ such that $zs = sz = z$ for every $s \in S$. No semigroup has more than one zero element. For every semigroup S with a recursive underlying set and a zero element, let $\textsc{Mortal}\big[S\big]$ denote the following problem: given a finite subset $X \subseteq S$, decide whether the zero element of S belongs to X^+; for every integer $k \geq 1$, $\textsc{Mortal}(k)\big[S\big]$ denotes the restriction of $\textsc{Mortal}\big[S\big]$ to input sets X of cardinality k.

1.5.2. Boundedness [7]

Let d be a positive integer. A subset $X \subseteq \mathbb{C}^{d\times d}$ is called *bounded* if there exists a positive constant M such that the modulus of any entry of any matrix in X is less than M. Let S be a recursive subset of $\mathbb{Q}^{d\times d}$. Let $\textsc{Bounded}\big[S\big]$ denote the following problem: given a finite subset $X \subseteq S$, decide whether X^+ is bounded; for every integer $k \geq 1$, $\textsc{Bounded}(k)\big[S\big]$ denotes the restriction of $\textsc{Bounded}\big[S\big]$ to input sets X of cardinality k.

1.5.3. Semigroup membership

For every semigroup S with a recursive underlying set, let $\textsc{Member}\big[S\big]$ denote the following problem: given a finite subset $X \subseteq S$ and an element $a \in S$, decide whether $a \in X^+$; for every integer $k \geq 1$, $\textsc{Member}(k)\big[S\big]$ denotes the restriction of $\textsc{Member}\big[S\big]$ to those instances (X, a) such that the cardinality of X equals k.

1.5.4. Semigroup finiteness

Let $\textsc{Finite}\big[S\big]$ denote the following problem: given a finite subset $X \subseteq S$, decide whether X^+ is finite; for every integer $k \geq 1$, $\textsc{Finite}(k)\big[S\big]$ denotes the restriction of $\textsc{Finite}\big[S\big]$ to input sets X of cardinality k.

1.5.5. Generalized Post correspondence problem [14]

Let GPCP denote the following problem: given a finite alphabet Σ, two morphisms σ, $\tau\colon \Sigma^\star \to \mathbb{W}$, and s, s', t, $t' \in \mathbb{W}$, decide whether there exists $w \in \Sigma^\star$ such that $s\sigma(w)s' = t\tau(w)t'$; for every integer $k \geq 1$, GPCP(k) denotes the restriction of GPCP to those instances $(\Sigma, \sigma, \tau, s, s', t, t')$ such that the cardinality of Σ equals k.

2. The case of a single generator

Definition 2.1. Let S be a semigroup. An element $s \in S$ is called *torsion* if it satisfies the following four equivalent conditions.

(1) The singleton $\{s\}$ is not a code;
(2) there exist two integers p and q with $0 < p < q$ such that $s^p = s^q$;
(3) the semigroup $\{s, s^2, s^3, s^4, \dots\}$ has finite cardinality;
(4) the sequence $(s, s^2, s^3, s^4, \dots)$ is eventually periodic.

For any semigroup S with a recursive underlying set, Free$(1)\left[S\right]$ is the complementary problem of Finite$(1)\left[S\right]$.

2.1. Matrix torsion over the complex numbers

The next theorem characterizes those complex square matrices that are torsion. The proof uses the following basic fact from linear algebra:

Lemma 2.2 (Theorem 3.3.6 in [25])**.** *Let M be a complex square matrix and let λ be an eigenvalue of M. The multiplicity of λ as a root of the minimal polynomial of M equals the maximum order of a Jordan block of M corresponding to λ.*

Theorem 2.3. *Let d be a positive integer and let $M \in \mathbb{C}^{d\times d}$. The following four assertions are equivalent.*

(*i*) *The matrix M is torsion;*
(*ii*) *there exist $v \in [\![0, d]\!]$ and a finite set U of roots of unity such that the minimal polynomial of M over $\mathbb{C}$ equals*

$$\mathtt{z}^v \prod_{u\in U} (\mathtt{z} - u);$$

(*iii*) *there exist a diagonal matrix D and a nilpotent matrix N such that every eigenvalue of D is a root of unity and*

$$\begin{bmatrix} D & O \\ O & N \end{bmatrix}$$

is a Jordan normal form of M;
(*iv*) *there exists an integer $n \geq 2$ such that $M^d = M^{nd}$.*

Proof. $(i) \implies (ii)$. Assume that assertion (i) holds. Then, there exist two integers p and q with $0 \leq p < q$ such that $M^p = M^q$. Let $\mu(\mathtt{z})$ denote the minimal polynomial of M. Since $M^q - M^p$ is a zero matrix, $\mu(\mathtt{z})$ divides $\mathtt{z}^q - \mathtt{z}^p = \mathtt{z}^{q-p}(\mathtt{z}^p - 1)$. Therefore, $\mu(\mathtt{z})$ can be written in the form $\mu(\mathtt{z}) = \mathtt{z}^v \prod_{u \in U}(\mathtt{z} - u)$ with $v \in [\![0, q-p]\!]$ and $U \subseteq \{u \in \mathbb{C} : u^p = 1\}$. Moreover, the Cayley-Hamilton theorem implies that $\mu(\mathtt{z})$ divides the characteristic polynomial of M which is of degree d, so v is not greater than d. We have thus shown assertion (ii).

$(ii) \implies (iii)$. The equivalence $(ii) \iff (iii)$ follows from Lemma 2.2.

$(iii) \implies (iv)$. Assume that assertion (iii) holds. Then, there exist a non-singular matrix P, a diagonal matrix D, and a nilpotent matrix N such that every eigenvalue of D is a root of unity and

$$M = P \begin{bmatrix} D & O \\ O & N \end{bmatrix} P^{-1}.$$

Let m be a positive integer such that $\lambda^m = 1$ for every eigenvalue λ of D: D^m is an identity matrix, and thus $D^{(m+1)d} = (D^m)^d D^d = D^d$. Moreover, $N^{(m+1)d}$ and N^d are equal to the same zero matrix, and thus

$$M^{(m+1)d} = P \begin{bmatrix} D^{(m+1)d} & O \\ O & N^{(m+1)d} \end{bmatrix} P^{-1} = P \begin{bmatrix} D^d & O \\ O & N^d \end{bmatrix} P^{-1} = M^d.$$

Hence, assertion (iv) holds with $n := m + 1$.

$(iv) \implies (i)$. The implication $(iv) \implies (i)$ is trivial. □

Let us now turn to matrices with rational entries. The next proposition characterizes those two-by-two rational matrices that are torsion.

Lemma 2.4. *Let ϕ denote Euler's totient function: for every integer $n \geq 1$, $\phi(n)$ equals the number of $k \in [\![1, n]\!]$ such that k and n are coprime. For every integer $n \geq 1$, $\phi(n) = 2$ is equivalent to $n \in \{3, 4, 6\}$.*

Proof. Let n be an integer greater than 6. Let T denote the set of all $k \in [\![1, n]\!]$ such that k and n are coprime. Let $r, m \in \mathbb{N}$ be such that $n = 2^r m$ and m is odd. If $m \in \{1, 3\}$ then $\{1, 5, n-1\}$ is 3-element subset of T; if $m \geq 5$ then $\{1, m-2, n-1\}$ is a 3-element subset of T. Hence, $\phi(n)$ is greater than 2 for every integer $n > 6$. Besides, we have $\phi(1) = \phi(2) = 1$, $\phi(3) = \phi(4) = \phi(6) = 2$, and $\phi(5) = 4$, so the lemma holds. □

Recall that for each integer $n \geq 1$, the degree of the nth cyclotomic polynomial, denoted $\Phi_n(\mathtt{z})$, equals $\phi(n)$.

Proposition 2.5. *Let i denote the imaginary unit and let $\zeta := \frac{1}{2} + i\frac{\sqrt{3}}{2}$:*

- *ζ and $\zeta^5 = \frac{1}{2} - i\frac{\sqrt{3}}{2}$ are the primitive sixth roots of unity;*
- *i and $-i$ are the primitive fourth roots of unity; and*
- *$\zeta^2 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ and $\zeta^4 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$ are the primitive cube roots of unity.*

For every $M \in \mathbb{Q}^{2\times 2}$, M is torsion iff one of the following ten matrices is a Jordan normal form of M:

$$\left[\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} -1 & 0 \\ 0 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right], \left[\begin{smallmatrix} \zeta^2 & 0 \\ 0 & \zeta^4 \end{smallmatrix}\right], \left[\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right], \text{ or } \left[\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^5 \end{smallmatrix}\right].$$

Proof. It is easy to check that the ten matrices listed above are torsion, so the "if part" holds true. Let us now prove the "only if part".

Assume that M is torsion. Theorem 2.3 implies that M is nilpotent or diagonalizable (over $\mathbb{C}$). If M is nilpotent then either M equals $\left[\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right]$, or $\left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right]$ is the Jordan normal form of M. Hence, we may assume that M is diagonalizable for the rest of the proof. Let $\chi(\mathtt{z})$ denote the characteristic polynomial of M.

First, assume that $\chi(\mathtt{z})$ is reducible over $\mathbb{Q}$. Since $\chi(\mathtt{z})$ is of degree 2, the eigenvalues of M are rational numbers. Besides, Theorem 2.3 implies that every non-zero eigenvalue of M is a root of unity. Since -1 and $+1$ are the only rational roots of unity, the eigenvalues of M lie in the set $\{-1, 0, +1\}$. Hence, one of the following six matrices is a Jordan normal form of M: $\left[\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} -1 & 0 \\ 0 & 0 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$, or $\left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$.

Second, assume that $\chi(\mathtt{z})$ is irreducible over $\mathbb{Q}$. Then, $\chi(\mathtt{z})$ is a cyclotomic polynomial. Besides, it follows from Lemma 2.4 than the only cyclotomic polynomials of degree 2 are:

(1) $\Phi_3(\mathtt{z}) = \mathtt{z}^2 + \mathtt{z} + 1 = (\mathtt{z} - \zeta^2)(\mathtt{z} - \zeta^4)$;
(2) $\Phi_4(\mathtt{z}) = \mathtt{z}^2 + 1 = (\mathtt{z} - i)(\mathtt{z} + i)$; and
(3) $\Phi_6(\mathtt{z}) = \mathtt{z}^2 - \mathtt{z} + 1 = (\mathtt{z} - \zeta)(\mathtt{z} - \zeta^5)$.

Therefore, one of the following three matrices is a Jordan normal form of M: $\left[\begin{smallmatrix} \zeta^2 & 0 \\ 0 & \zeta^4 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right]$, or $\left[\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^5 \end{smallmatrix}\right]$. □

Note that $\left[\begin{smallmatrix} \zeta^2 & 0 \\ 0 & \zeta^4 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right]$, and $\left[\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^5 \end{smallmatrix}\right]$ are the Jordan normal forms of the integer matrices $\left[\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$, and $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right]$, respectively.

2.2. The matrix torsion problem

Definition 2.6. Define the Matrix Torsion problem as: given an integer $d \geq 1$ and a matrix $M \in \mathbb{Q}^{d\times d}$, decide whether M is torsion.

For every integer $d \geq 1$, the complementary problem of Free(1)$\left[\mathbb{Q}^{d\times d}\right]$ is a restriction of Matrix Torsion.

Theorem 2.7 (Mandel and Simon [35])**.** *There exists a computable function $r\colon \mathbb{N}\setminus\{0\} \to \mathbb{N}\setminus\{0\}$ such that for every integer $d \geq 1$ and every matrix $M \in \mathbb{Q}^{d\times d}$, $M^d = M^{d+r(d)}$ iff M is torsion.*

It follows from Theorem 2.7 that:

(1) Matrix Torsion is decidable and
(2) for each integer $d \geq 1$, Free(1)$\left[\mathbb{Q}^{d\times d}\right]$ is decidable in polynomial time.

However, r is not polynomially bounded so the proof of the following theorem requires other ideas:

Theorem 2.8. *The* Matrix Torsion *problem is decidable in polynomial time.*

Proof. The Matrix Power problem is: given an integer $d \geq 1$ and two matrices A, $B \in \mathbb{Q}^{d\times d}$, decide whether there exists $n \in \mathbb{N}$ such that $A^n = B$. Note that for each integer $d \geq 1$, Member$(1)\left[\mathbb{Q}^{d\times d}\right]$ is a restriction of Matrix Power. Kannan and Lipton showed that Matrix Power is decidable in polynomial time [29], so it suffices to show that there exists a polynomial-time many-one reduction from Matrix Torsion to Matrix Power.

Let (d, M) be an instance of Matrix Torsion. Define two matrices A, $B \in \mathbb{Q}^{(d+2)\times(d+2)}$ by:

$$A := \begin{bmatrix} M^d & O \\ O & N_2 \end{bmatrix} \qquad \text{where} \qquad N_2 := \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

and

$$B := \begin{bmatrix} M^d & O \\ O & O_2 \end{bmatrix} \qquad \text{where} \qquad O_2 := \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Clearly, $(d + 2, A, B)$ is an instance of Matrix Power and $(d + 2, A, B)$ is computable from (d, M) in polynomial time. Let $n \in \mathbb{N}$. Since $N_2^n = O_2$ is equivalent to $n \geq 2$, $A^n = B$ is equivalent to the conjunction of $M^{nd} = M^d$ and $n \geq 2$. It thus follows from Theorem 2.3 that: $(d + 2, A, B)$ is a yes-instance of Matrix Power iff (d, M) is a yes-instance of Matrix Torsion. □

At this point, it is interesting to briefly discuss about power boundedness.

Definition 2.9. A complex square matrix M is called *power bounded* if the semigroup $\left\{M, M^2, M^3, M^4, \dots\right\}$ is bounded. Define the Matrix Power Boundedness problem as: given an integer $d \geq 1$ and a matrix $M \in \mathbb{Q}^{d\times d}$, decide whether M is power bounded.

For every integer $d \geq 1$, Bounded$(1)\left[\mathbb{Q}^{d\times d}\right]$ is a restriction of Matrix Power Boundedness.

Proposition 2.10. *The* Matrix Power Boundedness *problem is decidable.*

Proof. Let M be a complex square matrix. Let $\mu(\mathtt{z})$ denote the minimal polynomial of M: the roots of $\mu(\mathtt{z})$ are the eigenvalues of M. Put $\nu(\mathtt{z}) := \gcd(\mu(\mathtt{z}), \mu'(\mathtt{z}))$: the roots of $\nu(\mathtt{z})$ are the multiple roots of $\mu(\mathtt{z})$. It is easy to see that M is power bounded iff the following two conditions are met:

(i) every root of $\mu(\mathtt{z})$ has modulus at most 1 and
(ii) every root of $\nu(\mathtt{z})$ has modulus less than 1.

Now, consider the case where every entry of M is in $\mathbb{Q}$. Then, $\mu(\mathtt{z})$ and $\nu(\mathtt{z})$ are computable from M in polynomial time [29]. Therefore, deciding whether M is power bounded reduces to checking conditions (i) and (ii). This can be achieved using Tarski's decision procedure [46]. □

We conjecture that Matrix Power Boundedness is decidable in polynomial time.

2.3. The morphism torsion problem

Definition 2.11. For any alphabet Σ, let $\hom(\Sigma^\star)$ denote the set of all morphisms from $\Sigma^\star$ to itself. Define the Morphism Torsion problem as: given a finite alphabet Σ and a morphism $\sigma \in \hom(\Sigma^\star)$, decide whether σ is torsion (under function composition).

The size of an instance (Σ, σ) of Morphism Torsion equals $\sum_{a \in \Sigma} (1 + |\sigma(a)|)$.

Definition 2.12 (incidence matrix)**.** Let Σ be a finite alphabet, let d denote the cardinality of Σ, and let a_1, a_2, ..., a_d be such that $\Sigma = \{a_1, a_2, \ldots, a_d\}$: $a_1 a_2 \cdots a_d$ is a permutation of Σ. The *incidence matrix* of σ relative to $a_1 a_2 \ldots a_d$ is defined as

$$\begin{bmatrix} |\sigma(a_1)|_{a_1} & |\sigma(a_2)|_{a_1} & \cdots & |\sigma(a_d)|_{a_1} \\ |\sigma(a_1)|_{a_2} & |\sigma(a_2)|_{a_2} & \cdots & |\sigma(a_d)|_{a_2} \\ \vdots & \vdots & \ddots & \vdots \\ |\sigma(a_1)|_{a_d} & |\sigma(a_2)|_{a_d} & \cdots & |\sigma(a_d)|_{a_d} \end{bmatrix}.$$

The incidence matrix of σ relative to $a_1 a_2 \ldots a_d$ belongs to $\mathbb{N}^{d \times d}$; for all $i, j \in [\![1, d]\!]$, its $(i, j)^{\text{th}}$ entry equals the number of occurrences of a_i in $\sigma(a_j)$.

Claim 2.13. Let Σ be a finite alphabet. For each $\sigma \in \hom(\Sigma^\star)$, let P_σ denote the incidence matrix of σ relative to some fixed permutation of Σ.

(i) Equality $P_\sigma P_\tau = P_{\sigma\tau}$ holds for all σ, $\tau \in \hom(\Sigma^\star)$;
(ii) for each $P \in \mathbb{N}^{d \times d}$, there exist at most finitely many $\tau \in \hom(\Sigma^\star)$ such that $P_\tau = P$.

Theorem 2.14. *The* Morphism Torsion *problem is decidable in polynomial time.*

Proof. By Theorem 2.8, it suffices to show that there exists a polynomial-time many-one reduction from Morphism Torsion to Matrix Torsion. The idea is to prove that a morphism is torsion iff its incidence matrix is torsion.

Let (Σ, σ) be an instance of Morphism Torsion. Let d denote the cardinality of Σ. For each $\tau \in \hom(\Sigma^\star)$, let P_τ denote the incidence matrix of τ relative to some fixed permutation of Σ. Clearly, (d, P_σ) is an instance of Matrix Torsion and (d, P_σ) is computable from (Σ, σ) in polynomial time.

Let us check that (Σ, σ) is a yes-instance of Morphism Torsion iff (d, P_σ) is a yes-instance of Matrix Torsion. It follows from Claim 2.13 (i) that $P_\sigma^n = P_{\sigma^n}$ for every $n \in \mathbb{N}$. Therefore, if σ is torsion then P_σ is torsion. Conversely, assume that P_σ is torsion. Then, the set of matrices $\mathcal{P} := \{P_\sigma, P_\sigma^2, P_\sigma^3, P_\sigma^4, \dots\}$ is finite, so by Claim 2.13 (ii), there exist at most finitely many $\tau \in \hom(\Sigma^\star)$ such that $P_\tau \in \mathcal{P}$. Since $P_{\sigma^n} \in \mathcal{P}$ for every integer $n \geq 1$, the set $\{\sigma, \sigma^2, \sigma^3, \sigma^4, \dots\}$ is finite, and thus σ is torsion. □

Corollary 2.15. *For any finite alphabet Σ,* Free(1)$\left[\hom(\Sigma^\star)\right]$ *is decidable in polynomial time.*

Open question 1 (Richomme [43])**.** *For any finite alphabet Σ with cardinality greater than* 1 *and any integer $k > 1$, the decidability of* Free(k)$\left[\hom(\Sigma^\star)\right]$ *is open.*

The decidability of Free(2)$\left[\hom(\mathbb{W})\right]$ is tackled in Section 6.3.

3. Balanced equations

This section centers on the consequences of the following lemma:

Lemma 3.1. *Let S be a semigroup and let X be a subset of S with cardinality greater than* 1*. The set X is not a code iff there exist x, $x' \in X$ and z, $z' \in X^+$ such that $x \neq x'$ and $zxzx'z' = zx'z'xz$.*

Proof. The "if part" is clear. Let us prove the "only if part".

Let Σ be an alphabet and let $\sigma\colon \Sigma^+ \to S$ be a morphism such that σ induces a bijection from Σ onto X. Assume that X is not a code. By Claim 1.13, σ is non-injective. Therefore, there exist w, $w' \in \Sigma^+$ such that $w \neq w'$ and $\sigma(w) = \sigma(w')$.

First, assume that w is not a prefix of w' and that w' is not a prefix of w. Then, there exist a, $a' \in \Sigma$ and u, v, $v' \in \Sigma^\star$ such that $a \neq a'$, $w = uav$, and $w' = ua'v'$: u is the longest common prefix of w and w'. Note that u, v, or v' may be the empty word. It is easy to see that $\sigma(a)$, $\sigma(a')$, $\sigma(vau)$, and $\sigma(v'au)$ are suitable choices for x, x', z, and z', respectively.

Second, assume that w is a proper prefix of w'. Then, there exists $a \in \Sigma$ such that wa is a prefix of w'. Since Σ and X are equinumerous, the cardinality of Σ is greater than 1, and thus there exists $b \in \Sigma$ such that $a \neq b$. Clearly, we have $\sigma(wb) = \sigma(w'b)$, wb is not a prefix of $w'b$, and $w'b$ is not a prefix of wb. Therefore, the second case reduces to the first case.

Third, assume that w' is a proper prefix of w. Since w and w' play symmetric roles, the third case reduces to the second case. □

For each $y \in X^+$, the factorizations of y over X are in one-to-one correspondence with the preimages of y under σ. Let $\bar{x}$, $\bar{x}' \in \Sigma$ and $\bar{z}$, $\bar{z}' \in \Sigma^+$ be such that $x = \sigma(\bar{x})$, $x' = \sigma(\bar{x}')$, $z = \sigma(\bar{z})$, and $z' = \sigma(\bar{z}')$. Equation $zxzx'z' = zx'z'xz$ is "balanced" in the sense that the word $\bar{z}\bar{x}\bar{z}\bar{x}'\bar{z}'$, which corresponds to a factorization of the left-hand side, is a permutation of the word $\bar{z}\bar{x}'\bar{z}'\bar{x}\bar{z}$, which corresponds to a factorization of the right-hand side.

3.1. Cancellation

Definition 3.2 (cancellation)**.** Let S be a semigroup and let $s \in S$. We say that s is *left-cancellative* in S if for all u, $v \in S$, $su = sv$ implies $u = v$. In the same way, we say that s is *right-cancellative* in S if for all u, $v \in S$, $us = vs$ implies $u = v$. We say that s is *cancellative* in S if s is both left-cancellative and right-cancellative in S.

Example 3.3. Let X be a (finite or infinite) set and let S denote the set of all functions from X to itself. Clearly, S is a semigroup under function composition. The left-cancellative elements of S are the injections, the right-cancellative elements of S are the surjections, and the cancellative elements of S are the bijections.

The first useful corollary of Lemma 3.1 is:

Lemma 3.4. *Let S be a semigroup and let X be a subset of S such that the cardinality of X is greater than 1 and every element of X is left-cancellative in S. The set X is not a code iff there exist x, $x' \in X$ and z, $z' \in X^+$ such that $x \neq x'$ and $xz = x'z'$.*

Proof. The "if part" is clear. It remains to prove the "only if part".

Assume that X is not a code. By Lemma 3.1, there exist x, $x' \in X$ and t, $t' \in X^+$ such that $txtx't' = tx't'xt$. Since t is left-cancellative, equality $xz = x'z'$ holds with $z := tx't'$ and $z' := t'xt$. $\square$

Lemma 3.4 is extensively used throughout the paper. The following example shows that Lemma 3.4 does not hold without any cancellation property:

Example 3.5. Let

$$X := \begin{bmatrix} 4 & 2 \\ 2 & 1 \end{bmatrix} \qquad \text{and} \qquad X' := \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} .$$

The set $\{X, X'\}$ is not a code under matrix multiplication because $XXX'X = XX'XX$. Besides, the row matrix $L := \begin{bmatrix} -1 & 2 \end{bmatrix}$ satisfies $LX = \begin{bmatrix} 0 & 0 \end{bmatrix}$ and $LX' = \begin{bmatrix} 3 & 6 \end{bmatrix}$. For all Z, $Z' \in \{X, X'\}^+$, we thus have $LXZ = \begin{bmatrix} 0 & 0 \end{bmatrix}$ while the entries of $LX'Z'$ are positive. Therefore, XZ and $X'Z'$ are distinct for all Z, $Z' \in \{X, X'\}^+$,

3.2. Direct products of semigroups

Given two semigroups S and T such that T is commutative, let us characterize those subsets of $S \times T$ that are codes.

Lemma 3.6. *Let S and T be two semigroups and let Z be a subset of $S \times T$ such that T is commutative and the cardinality of Z is greater than 1. Let $\alpha \colon S \times T \to S$ be defined by: $\alpha(s,t) := s$ for every $(s,t) \in S \times T$. The set Z is a code iff the following two conditions are met: α is injective on Z and $\alpha(Z)$ is a code.*

Proof. The "if part" follows from Claim 1.13. It remains to prove the "only if part".

First, assume that α is non-injective on Z. Then, there exist $x \in S$ and $y, y' \in T$ such that $y \neq y'$, $(x, y) \in Z$, and $(x, y') \in Z$. Since (x, y) and (x, y') commute, Z is not a code.

Second, assume that $\alpha(Z)$ is not a code. By Lemma 3.1, there exist (x, y), $(x', y') \in Z$ and (u, v), $(u', v') \in Z^+$ such that $x \neq x'$ and $uxux'u' = ux'u'xu$. Now, remark that $vyvy'v' = vy'v'yv$ because T is commutative. Hence, we have

$$(u, v)(x, y)(u, v)(x', y')(u', v') = (u, v)(x', y')(u', v')(x, y)(u, v),$$

and thus Z is not a code. □

To complete Lemma 3.6, let us characterize those elements of $S \times T$ that are torsion: for every $(s, t) \in S \times T$, (s, t) is torsion iff both s and t are torsion.

Lemma 3.7. *Let S and T be two semigroups and let $y \in Y$. For every subset $X \subseteq S$ such that the cardinality of X is greater than 1, $X \times \{y\}$ is a code iff X is a code.*

Proof. Although T is not necessarily commutative, $T' := \{y, y^2, y^3, y^4, \dots\}$ is a commutative subsemigroup of T such that $X \times \{y\} \subseteq S \times T'$. The desired result can thus be deduced from Lemma 3.6. □

Theorem 3.8. *Let S and T be two non-empty semigroups with recursive underlying sets and let k be an integer greater than 1. If $\text{FREE}(k)[S \times T]$ is decidable then both $\text{FREE}(k)[S]$ and $\text{FREE}(k)[T]$ are decidable.*

Proof. Let y be a fixed element of T. For each k-element subset $X \subseteq S$, $X \times \{y\}$ is a k-element subset of $S \times T$, and according to Lemma 3.7, X is a code iff $X \times \{y\}$ is a code. Hence, there exists a many-one reduction from $\text{FREE}(k)[S]$ to $\text{FREE}(k)[S \times T]$. In the same way, $\text{FREE}(k)[T]$ reduces to $\text{FREE}(k)[S \times T]$. □

The converse of Theorem 3.8 is false in general: for instance, $\text{FREE}[\mathbb{W}]$ is decidable (see Ex. 1.9) while $\text{FREE}(k)[\mathbb{W} \times \mathbb{W}]$ is undecidable for every integer $k \geq 13$ (see Sect. 7). An interesting partial converse is:

Lemma 3.9. *Let S and T be two semigroups with recursive underlying sets and let k be an integer greater than 1. If $\text{FREE}(k)[S]$ is decidable and if T is commutative then $\text{FREE}(k)[S \times T]$ is decidable.*

Proof. It follows from Lemma 3.6 that $\text{FREE}(k)[S \times T]$ reduces to $\text{FREE}(k)[S]$. □

Theorem 3.8 and Lemma 3.9 deserve further comments. By Theorem 5.1 below, there exists a commutative (semi)group T with a recursive underlying set such that $\text{FREE}(1)[T]$ is undecidable. However, $\text{FREE}(1)[\{\mathtt{1}\}^+ \times T]$ is decidable because no element of $\{\mathtt{1}\}^+ \times T$ is torsion. Hence, it is essential to assume $k > 1$ in Theorem 3.8. Moreover, $\text{FREE}(1)[\{\varepsilon\} \times T]$ is undecidable while $\text{FREE}(1)[\{\varepsilon\}]$ is decidable, so it is also essential to assume $k > 1$ in Lemma 3.9.

Definition 3.10. For each $d \in \mathbb{N}$, let $\mathbb{W}^{\times d}$ denote the semigroup obtained as the direct product of d copies of $\mathbb{W}$: $\mathbb{W}^{\times 0} = \{\varepsilon\}$, $\mathbb{W}^{\times 1} = \mathbb{W}$, $\mathbb{W}^{\times 2} = \mathbb{W} \times \mathbb{W}$, $\mathbb{W}^{\times 3} = \mathbb{W} \times \mathbb{W} \times \mathbb{W}$, *etc.*

Theorem 3.11. *Let n be a positive integer and let Σ_1, Σ_2, ..., Σ_n be n finite alphabets. Let d denote the number of $i \in [\![1, n]\!]$ such that the cardinality of Σ_i is greater than 1. For every integer $k \geq 1$, $\text{FREE}(k)\big[\Sigma_1^\star \times \Sigma_2^\star \times \cdots \times \Sigma_n^\star\big]$ is decidable iff $\text{FREE}(k)\big[\mathbb{W}^{\times d}\big]$ is decidable.*

Proof. We only need to consider the case where $k > 1$ because both problems are trivially decidable in the case where $k = 1$. Moreover, for each permutation $(i_1, i_2, \ldots, i_n)$ of $[\![1, n]\!]$, $\Sigma_1^\star \times \Sigma_2^\star \times \cdots \times \Sigma_n^\star$ and $\Sigma_{i_1}^\star \times \Sigma_{i_2}^\star \times \cdots \times \Sigma_{i_n}^\star$ are isomorphic: the function mapping each $(w_1, w_2, \ldots, w_n) \in \Sigma_1^\star \times \Sigma_2^\star \times \cdots \times \Sigma_n^\star$ to $(w_{i_1}, w_{i_2}, \ldots, w_{i_n})$ is an isomorphism. Therefore, we may assume without loss of generality that the cardinality of Σ_i is greater than 1 for every $i \in [\![1, d]\!]$, or equivalently, that $\Sigma_i^\star$ is commutative for every $i \in [\![d+1, n]\!]$. Hence, it follows from Lemma 3.9 that $\text{FREE}(k)\big[\Sigma_1^\star \times \Sigma_2^\star \times \cdots \times \Sigma_n^\star\big]$ is decidable iff $\text{FREE}(k)\big[S\big]$ is decidable, where $S := \Sigma_1^\star \times \Sigma_2^\star \times \cdots \times \Sigma_d^\star$.

For each $i \in [\![1, d]\!]$, let $\phi_i \colon \mathbb{W} \to \Sigma_i^\star$ be an injective morphism, *e.g.*, ϕ_i can be any morphism extending an injection from $\{\mathtt{0}, \mathtt{1}\}$ to Σ_i. The function mapping each $(u_1, u_2, \ldots, u_d) \in \mathbb{W}^{\times d}$ to $(\phi_1(u_1), \phi_2(u_2), \ldots, \phi_d(u_d))$ is an injective morphism from $\mathbb{W}^{\times d}$ to S; it induces a one-one reduction from $\text{FREE}(k)\big[\mathbb{W}^{\times d}\big]$ to $\text{FREE}(k)\big[S\big]$. Hence, the "only if part" of the theorem holds.

For each $i \in [\![1, d]\!]$, let $\psi_i \colon \Sigma_i^\star \to \mathbb{W}$ be an injective morphism (see Claim 1.14). The function mapping each $(v_1, v_2, \ldots, v_d) \in S$ to $(\psi_1(v_1), \psi_2(v_2), \ldots, \psi_d(v_d))$ is an injective morphism from S to $\mathbb{W}^{\times d}$; it induces a one-one reduction from $\text{FREE}(k)\big[S\big]$ to $\text{FREE}(k)\big[\mathbb{W}^{\times d}\big]$. Hence, the "if part" of the theorem holds. $\square$

3.3. Rational matrices versus integer matrices

The following lemma generalizes Lemma 3 in [11]:

Lemma 3.12. *Let d be a positive integer, let $\mathcal{X}$ be a subset of $\mathbb{C}^{d \times d}$ with cardinality greater than 1, and let $\lambda \colon \mathcal{X} \to \mathbb{C} \setminus \{0\}$. The set $\mathcal{X}$ is a code under matrix multiplication iff the following two conditions are met:*

(i) $\{\lambda(X)X : X \in \mathcal{X}\}$ *is a code under matrix multiplication and*
(ii) for all X, $Y \in \mathcal{X}$, $X \neq Y$ implies $\lambda(X)X \neq \lambda(Y)Y$.

Proof. Let $\mathcal{Z} := \{(X, \lambda(X)) : X \in \mathcal{X}\}$. By Lemma 3.6, $\mathcal{Z}$ is a code iff $\mathcal{X}$ is a code. Let $\mathcal{Z}' := \{(\lambda(X)X, \lambda(X)) : X \in \mathcal{X}\}$. By Lemma 3.6, $\mathcal{Z}'$ is a code iff conditions (i) and (ii) are met. Let $\check{\mathbb{C}} := \mathbb{C} \setminus \{0\}$. Let $\sigma \colon \mathbb{C}^{d \times d} \times \check{\mathbb{C}} \to \mathbb{C}^{d \times d} \times \check{\mathbb{C}}$ be defined by: $\sigma(X, a) := (aX, a)$ for every $(X, a) \in \mathbb{C}^{d \times d} \times \check{\mathbb{C}}$. Remark that $\sigma(\mathcal{Z}) = \mathcal{Z}'$, σ is injective, and σ is a morphism: $\sigma(XY, ab) = ((aX)(bY), ab) = \sigma(X, a)\sigma(Y, b)$ for all X, $Y \in \mathbb{C}^{d \times d}$ and all a, $b \in \check{\mathbb{C}}$. Therefore, $\mathcal{Z}$ is code iff $\mathcal{Z}'$ is a code. We have thus proven that the following four assertions are equivalent: $\mathcal{X}$ is a code, $\mathcal{Z}$ is a code, $\mathcal{Z}'$ is a code, and conditions (i) and (ii) are met. $\square$

Let $X := \left[\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right]$, $Y := \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, $\mathcal{X} := \{X, Y\}$, $\lambda(X) := 1$, and $\lambda(Y) := 2$. Note that $\lambda(X)X = \lambda(Y)Y$. Clearly, $\{\lambda(X)X, \lambda(Y)Y\} = \{X\}$ is a code under matrix multiplication but $\mathcal{X}$ is not. Hence, condition (ii) is crucial for the "if part" of Lemma 3.12.

The main result of the section is now easy to prove:

Theorem 3.13. *For all integers k, $d \geq 1$, $\mathrm{F{\scriptsize REE}}(k)\big[\mathbb{Q}^{d\times d}\big]$ is decidable iff $\mathrm{F{\scriptsize REE}}(k)\big[\mathbb{Z}^{d\times d}\big]$ is decidable.*

Proof. The "only if part" holds because $\mathrm{F{\scriptsize REE}}(k)\big[\mathbb{Z}^{d\times d}\big]$ is a restriction of $\mathrm{F{\scriptsize REE}}(k)\big[\mathbb{Q}^{d\times d}\big]$. Moreover, $\mathrm{F{\scriptsize REE}}(1)\big[\mathbb{Q}^{d\times d}\big]$ is decidable by Theorems 2.7 or 2.8. Hence, to conclude the proof of the theorem, it suffices to show that there exists a many-one reduction from $\mathrm{F{\scriptsize REE}}(k)\big[\mathbb{Q}^{d\times d}\big]$ to $\mathrm{F{\scriptsize REE}}(k)\big[\mathbb{Z}^{d\times d}\big]$ in the case where $k > 1$.

For each finite subset $\mathcal{X} \subseteq \mathbb{Q}^{d\times d}$, let $t(\mathcal{X})$ denote the smallest integer $n \geq 1$ such that $nX \in \mathbb{Z}^{d\times d}$ for every $X \in \mathcal{X}$. For each instance $\mathcal{X}$ of $\mathrm{F{\scriptsize REE}}(k)\big[\mathbb{Q}^{d\times d}\big]$, $\mathcal{X}' := \{t(\mathcal{X})X : X \in \mathcal{X}\}$ is an instance of $\mathrm{F{\scriptsize REE}}(k)\big[\mathbb{Z}^{d\times d}\big]$, $\mathcal{X}'$ is computable from $\mathcal{X}$, and by Lemma 3.12, $\mathcal{X}$ is a yes-instance of $\mathrm{F{\scriptsize REE}}(k)\big[\mathbb{Q}^{d\times d}\big]$ iff $\mathcal{X}'$ is a yes-instance of $\mathrm{F{\scriptsize REE}}(k)\big[\mathbb{Z}^{d\times d}\big]$. $\square$

To conclude the section, let us discuss whether analogues of Theorem 3.13 hold for mortality, boundedness, and semigroup membership. First, for all integers k, $d \geq 1$, $\mathrm{M{\scriptsize ORTAL}}(k)\big[\mathbb{Q}^{d\times d}\big]$ is decidable iff $\mathrm{M{\scriptsize ORTAL}}(k)\big[\mathbb{Z}^{d\times d}\big]$ is decidable: the many-one reduction from $\mathrm{F{\scriptsize REE}}(k)\big[\mathbb{Q}^{d\times d}\big]$ to $\mathrm{F{\scriptsize REE}}(k)\big[\mathbb{Z}^{d\times d}\big]$ presented in the proof of Theorem 3.13 is also a many-one reduction from $\mathrm{M{\scriptsize ORTAL}}(k)\big[\mathbb{Q}^{d\times d}\big]$ to $\mathrm{M{\scriptsize ORTAL}}(k)\big[\mathbb{Z}^{d\times d}\big]$. Note in passing that the decidability of $\mathrm{M{\scriptsize ORTAL}}(k)\big[\mathbb{Q}^{d\times d}\big]$ is still open for several pairs (d, k) of positive integers [9, 22]. Second, $\mathrm{B{\scriptsize OUNDED}}(2)\big[\mathbb{Q}^{47\times 47}\big]$ is undecidable [5], but for every integer $d \geq 1$, $\mathrm{B{\scriptsize OUNDED}}\big[\mathbb{Z}^{d\times d}\big]$ is decidable: $\mathrm{B{\scriptsize OUNDED}}\big[\mathbb{Z}^{d\times d}\big]$ is in fact the same problem as $\mathrm{F{\scriptsize INITE}}\big[\mathbb{Z}^{d\times d}\big]$ and the latter is decidable [26,35]. Third, it is still unknown whether there exist positive integers k_0 and d_0 satisfying the following two properties: $\mathrm{M{\scriptsize EMBER}}(k_0)\big[\mathbb{Q}^{d_0\times d_0}\big]$ is undecidable and $\mathrm{M{\scriptsize EMBER}}(k_0)\big[\mathbb{Z}^{d_0\times d_0}\big]$ is decidable.

4. Subsemigroups of groups

Automata over monoids, and in particular automata over the free group, have been widely studied [17, 44]. In this section, we first prove that for any group G with a recursive underlying set, $\mathrm{F{\scriptsize REE}}\big[G\big]$ reduces to an automata theory problem (Thm. 4.8). We then use this reduction to show that both $\mathrm{GL}(2, \mathbb{Z})$ and the free group have decidable freeness problems (Cors. 4.9 and 4.14).

Remark 4.1. Let G be a group with a recursive underlying set. $\mathrm{F{\scriptsize REE}}\big[G\big]$ should not be confused with the following problem, which is not the concern of the paper: given a finite subset $X \subseteq G$, decide whether the subgroup of G generated by X is a free group with basis X.

Definition 4.2 (automaton)**.** Let X be a set. An *automaton* over X is a quadruple $A = (Q, E, I, T)$ where Q is a set, I and T are subsets of Q, and E is a subset of $Q \times X \times Q$. The elements of Q are the *states* of A, the elements of E are the *transitions* of A, the elements of I are the *initial* states of A, and the elements of T are the *terminal* states of A. We say that A is *finite* if Q and E are finite. A transition $(p, s, q) \in E$ is usually denoted $p \xrightarrow{s} q$.

Finite automata over finite alphabets play a central role in theoretical computer science; they are termed "nondeterministic automata" or simply "automata" in most of the literature. According to our definition, an automaton over X is also an automaton over any superset of X. In particular, for any alphabet Σ, an automaton over Σ is also an automaton over the free monoid $\Sigma^\star$.

Definition 4.3 (acceptance)**.** Let M be a monoid, let A be an automaton over M, and let s be an element of M. We say that A *accepts* s if for some integer $n \in \mathbb{N}$, there exist $n+1$ states $q_0, q_1, \ldots, q_n$ and n elements $s_1, s_2, \ldots, s_n \in M$ meeting the following requirements: $s = s_1 s_2 \ldots s_n$, q_0 is an initial state of A, q_n is a terminal state of A, and $q_{i-1} \xrightarrow{s_i} q_i$ is a transition of A for every $i \in [\![1, n]\!]$. Define the *behavior* of A as the set of those elements of M that are accepted by A.

For every automaton $A = (Q, E, I, T)$ over M such that $I \cap T \neq \emptyset$, it follows from Definition 4.3 that A accepts the identity element of M.

Let Σ be a finite alphabet. Every finite automaton over $\Sigma^\star$ can be transformed in polynomial time into a finite automaton over $\Sigma \cup \{\varepsilon\}$ with the same behavior: simply split each transition labeled with a word of length greater than 1. Moreover, every finite automaton over $\Sigma \cup \{\varepsilon\}$ can be transformed in polynomial time into a finite automaton over Σ with the same behavior (Sect. 2.5 in [24]).

Remark 4.4 (Kleene's theorem)**.** Let M be a monoid. A subset of M is called *rational* if it equals the behavior of some finite automaton over M. We claim that the set of all rational subsets of M equals the closure of the set of all finite subsets of M under set union, set product, and star. If $M = \Sigma^\star$ for some finite alphabet Σ then our claim is simply Kleene's theorem (Sect. 3.2 in [24]). The generalization to an arbitrary monoid is straightforward [44].

Definition 4.5. For every monoid M with a recursive underlying set, define Accept$\big[M\big]$ as the following problem: given a finite automaton A over M and an element $s \in M$, decide whether A accepts s.

Note that Accept$\big[M\big]$ is also known as the rational subset problem for M [28] and as the rational membership problem over M [17].

Example 4.6 (Sect. 4.3.3 in [24])**.** For any finite alphabet Σ, Accept$\big[\Sigma^\star\big]$ is decidable in polynomial time.

A *group* is a monoid G in which every element is invertible. The identity element of G is denoted 1_G. The *inversion* in G is the function from G onto itself that maps each element $g \in G$ to its inverse g^{-1}. For every $x \in G$, x is torsion iff there exists an integer $n \geq 1$ such that $x^n = 1_G$.

Lemma 4.7.

(i) *Let M be a monoid with a recursive underlying set. If* $\textsc{Accept}\bigl[M\bigr]$ *is decidable then the operation of M is computable.*
(ii) *Let G be a group with a recursive underlying set. If the operation of G is computable then the inversion in G is computable.*

Proof. Let x, $y \in M$. Let $A_{x,y}$ be the automaton over $\{x, y\}$ defined by:

- $\mathtt{I}$, $\mathtt{Q}$, and $\mathtt{T}$ are the states of $A_{x,y}$;
- $\mathtt{I} \xrightarrow{x} \mathtt{Q}$ and $\mathtt{Q} \xrightarrow{y} \mathtt{T}$ are the transitions of $A_{x,y}$;
- $\mathtt{I}$ is the unique initial state of $A_{x,y}$; and
- $\mathtt{T}$ is the unique terminal state of $A_{x,y}$.

Clearly, the behavior of $A_{x,y}$ equals $\{xy\}$. Now, assume that $\textsc{Accept}\bigl[M\bigr]$ is decidable. To compute the result of the operation xy, first compute $A_{x,y}$, and then examine the elements of M one after another until finding the one that is accepted by $A_{x,y}$. We have thus proven part (i).

Let us now turn to part (ii). Let g, $h \in G$. To decide whether h is the inverse of g, it suffices to compute the operation gh and then check whether the result equals 1_G. Hence, the inverse of any element of G is computable by inspection. □

Theorem 4.8. *Let G be a group with a recursive underlying set.*

(i) *If the inversion in G is computable in polynomial time and if* $\textsc{Accept}\bigl[G\bigr]$ *is decidable in polynomial time then* $\textsc{Free}\bigl[G\bigr]$ *is decidable in polynomial time;*
(ii) *if* $\textsc{Accept}\bigl[G\bigr]$ *is decidable then* $\textsc{Free}\bigl[G\bigr]$ *is decidable.*

Proof. We do *not* show that there exists a many-one reduction from $\textsc{Free}\bigl[G\bigr]$ to $\textsc{Accept}\bigl[G\bigr]$.

First, consider a finite subset $X \subseteq G$ with cardinality greater than 1. For every $x \in G$, let A_x be the automaton over G defined by:

- $\mathtt{I}$, $\mathtt{Q}$, and $\mathtt{T}$ are the states of A_x;
- the transitions of A_x are $\mathtt{I} \xrightarrow{x} \mathtt{Q}$, $\mathtt{Q} \xrightarrow{1_G} \mathtt{T}$, and for each $y \in X$, $\mathtt{Q} \xrightarrow{y} \mathtt{Q}$ and $\mathtt{T} \xrightarrow{y^{-1}} \mathtt{T}$;
- $\mathtt{I}$ is the unique initial state of A_x; and
- $\mathtt{T}$ is the unique terminal state of A_x.

The behavior of A_x equals $\bigl\{xzz'^{-1} : (z, z') \in X^\star \times X^\star\bigr\}$. It thus follows from Lemma 3.4 that X is not a code iff there exist x, $x' \in X$ such that $x \neq x'$ and A_x accepts x'. If the inversion in G is computable in polynomial time then A_x is computable from x and X in polynomial time. If $\textsc{Accept}\bigl[G\bigr]$ is decidable then A_x is computable from x and X by Lemma 4.7.

Second, consider an element $x \in G$. Let B be the automaton over G defined by:

- $\mathtt{I}$ and $\mathtt{T}$ are the states of B;
- $\mathtt{I} \xrightarrow{x} \mathtt{T}$ and $\mathtt{T} \xrightarrow{x} \mathtt{T}$ are the transitions of B;
- $\mathtt{I}$ is the unique initial state of B; and
- $\mathtt{T}$ is the unique terminal state of B.

The behavior of B equals $\left\{x, x^2, x^3, x^4, \dots\right\}$. Therefore, x is torsion iff B accepts 1_G. Moreover, B is clearly computable from x in polynomial time.

The theorem follows from the preceding discussion. □

The proof of Theorem 4.8 deserves two observations. First, the result still holds even if $\text{Accept}\left[G\right]$ is restricted to those instances (A, s) such that the automaton A has at most 3 states. Second, we claim that if the inversion in G is computable (in polynomial time) then there exists a (polynomial-time) many-one reduction from the complementary problem of $\text{Free}\left[G\right]$ to $\text{Accept}\left[G\right]$. The verification is left to the reader.

The general linear group of degree d over $\mathbb{Z}$ is denoted $\mathrm{GL}(d, \mathbb{Z})$:

$$\mathrm{GL}(d, \mathbb{Z}) = \left\{X \in \mathbb{Z}^{d \times d} : \det(X) = \pm 1\right\}.$$

Equivalently, $\mathrm{GL}(d, \mathbb{Z})$ is the set of all matrices $X \in \mathbb{Z}^{d \times d}$ such that X has an inverse in $\mathbb{Z}^{d \times d}$. Choffrut and Karhumäki have shown that $\text{Accept}\left[\mathrm{GL}(2, \mathbb{Z})\right]$ is decidable [12]. Hence, it follows from Theorem 4.8 (*ii*):

Corollary 4.9. $\text{Free}\left[\mathrm{GL}(2, \mathbb{Z})\right]$ *is decidable.*

Let us now turn to the free group. To properly deal with this algebraic structure, we introduce the notion of semi-Thue system. (Semi-Thue systems are also involved in Sect. 7.1).

Definition 4.10 (semi-Thue system)**.** A *semi-Thue system* is a pair $T = (\Sigma, R)$ where Σ is an alphabet and R is a subset of $\Sigma^\star \times \Sigma^\star$. The elements of R are the *rules* of T. The *immediate accessibility under* T is the binary relation over $\Sigma^\star$ defined by: for every x, $y \in \Sigma^\star$, y is immediately accessible from x under T iff there exist $(s, t) \in R$ and z, $z' \in \Sigma^\star$ such that $x = zsz'$ and $y = ztz'$. The reflexive-transitive closure of the immediate accessibility under T is simply called the *accessibility under* T.

For the rest of the section, overlining is construed as a purely formal operation on the symbols. In fact, for each symbol a, $\bar{a}$ is a symbol which is distinct from a; moreover, if a and b are distinct symbols then $\bar{a}$ and $\bar{b}$ are also distinct symbols.

Let Σ be an alphabet. Define $\bar{\Sigma} := \{\bar{a} : a \in \Sigma\}$: the alphabets Σ and $\bar{\Sigma}$ are equinumerous and disjoint. Given two words x and y over $\Sigma \cup \bar{\Sigma}$, we say that x *freely reduces* to y if y is accessible from x under the semi-Thue system

$$\left(\Sigma \cup \bar{\Sigma}, \{(a\bar{a}, \varepsilon) : a \in \Sigma\} \cup \{(\bar{a}a, \varepsilon) : a \in \Sigma\}\right).$$

A word w over $\Sigma \cup \bar{\Sigma}$ is called *freely reduced* if there does not exist any $a \in \Sigma$ such that $a\bar{a}$ or $\bar{a}a$ occurs in w. Let $f\colon \left(\Sigma \cup \bar{\Sigma}\right)^\star \times \left(\Sigma \cup \bar{\Sigma}\right)^\star \to \left(\Sigma \cup \bar{\Sigma}\right)^\star$ be defined by: for all words x and y over $\Sigma \cup \bar{\Sigma}$, $f(x, y)$ is the unique freely reduced word over $\Sigma \cup \bar{\Sigma}$ to which xy freely reduces. The free group over Σ, denoted $\mathrm{FG}(\Sigma)$, can be defined as follows: its underlying set is the set of all freely reduced words over $\Sigma \cup \bar{\Sigma}$ and its operation is induced by f. A more detailed introduction to the free group can be found in [34].

Assume now that Σ is finite. The underlying set of $\mathrm{FG}(\Sigma)$ is then recursive. $\textsc{Accept}\left[\mathrm{FG}(\Sigma)\right]$ can be restated as follows: given a finite automaton A over $\Sigma \cup \bar{\Sigma} \cup \{\varepsilon\}$ and a freely reduced word s over $\Sigma \cup \bar{\Sigma}$, decide whether there exists a word s' over $\Sigma \cup \bar{\Sigma}$ such that A accepts s' and s' freely reduces to s.

Definition 4.11. Let Σ be an alphabet and let $A = (Q, E, I, T)$ be an automaton over $\Sigma \cup \bar{\Sigma} \cup \{\varepsilon\}$.

A *free reducibility* of A is an element $(p, q) \in Q \times Q$ for which there exists $a \in \Sigma$ such that the automaton $(Q, E, \{p\}, \{q\})$ accepts $a\bar{a}$ or $\bar{a}a$. We say that A is *freely reduced* if for every free reducibility (p, q) of A, $p \xrightarrow{\varepsilon} q$ belongs to E.

Let $\mathcal{F}$ denote the set of all subsets $F \subseteq Q \times \{\varepsilon\} \times Q$ such that $(Q, E \cup F, I, T)$ is freely reduced. Note that $\mathcal{F}$ is non-empty because $Q \times \{\varepsilon\} \times Q \in \mathcal{F}$. The automaton $\tilde{A} := (Q, E \cup \bigcap_{F \in \mathcal{F}} F, I, T)$ is called the *free reduction* of A.

Colloquially, $\tilde{A}$ is the smallest freely reduced "super-automaton" of A.

Theorem 4.12 (Algorithm 1.3.7 in [17], see also [3,16])**.** *Let Σ be a finite alphabet. For every finite automaton A over $\Sigma \cup \bar{\Sigma} \cup \{\varepsilon\}$,*

(i) *$\tilde{A}$ is computable from A in polynomial time and*
(ii) *the behavior of $\tilde{A}$ is the closure of the behavior of A under free reduction.*

Theorem 4.12 (ii) could be stated as follows: for every word x over $\Sigma \cup \bar{\Sigma}$, $\tilde{A}$ accepts x iff A accepts a word over $\Sigma \cup \bar{\Sigma}$ that freely reduces to x. From Example 4.6 and Theorem 4.12, we deduce:

Corollary 4.13. *For any finite alphabet Σ,* $\textsc{Accept}\left[\mathrm{FG}(\Sigma)\right]$ *is decidable in polynomial time.*

From Theorem 4.8 (i) and Corollary 4.13 we deduce:

Corollary 4.14. *For any finite alphabet Σ,* $\textsc{Free}\left[\mathrm{FG}(\Sigma)\right]$ *is decidable in polynomial time.*

5. Number of generators

The section begins with two natural questions:

Open question 2. *Does there exist a semigroup S_∞ with a recursive underlying set and satisfying the following two properties:* $\textsc{Free}\left[S_\infty\right]$ *is undecidable and* $\textsc{Free}(k)\left[S_\infty\right]$ *is decidable for every integer $k \geq 1$?*

Open question 3. *Let K denote the set of all integers $k \geq 1$ such that there exists a semigroup S_k with a recursive underlying set and satisfying the following two properties:* $\textsc{Free}(k)\big[S_k\big]$ *is decidable and* $\textsc{Free}(k+1)\big[S_k\big]$ *is undecidable. Is the cardinality of K finite?*

Combining Example 1.11 above and Corollary 8.6 below, we get that $1 \in K$: $\mathbb{N}^{36\times 36}$ is a suitable choice for S_1. Combining Example 1.10 above and Theorem 7.19 below, we get that $K \cap [\![2, 12]\!] \neq \emptyset$: for some $k \in [\![2, 12]\!]$, $\mathbb{W} \times \mathbb{W}$ is a suitable choice for S_k.

The following theorem states the existence of bizarre (semi)groups:

Theorem 5.1. *There exists an abelian group G with a computable operation such that* $\textsc{Free}(1)\big[G\big]$ *is undecidable.*

Proof. Let M be a universal Turing machine [24]; note that the input alphabet of M equals $\{\mathtt{0}, \mathtt{1}\}$. Let $f \colon \mathbb{W} \to \mathbb{N} \cup \{\infty\}$ be defined by: for each $w \in \mathbb{W}$, $f(w)$ equals the running time of M on input w. Note that $f(w)$ is non-zero for every $w \in \mathbb{W}$: any Turing machine that decides a non-trivial language must read at least one letter of each input word before halting. The following problem is decidable: given $w \in \mathbb{W}$ and $n \in \mathbb{N}$, decide whether $f(w) \geq n$.

Let G be the set of all $g \colon \mathbb{W} \to \mathbb{Z}$ such that $\{w \in \mathbb{W} : g(w) \neq 0\}$ is finite and $-f(w) < g(w) < f(w)$ for every $w \in \mathbb{W}$. Remark that G is a recursive set. Let us equip G with the computable abelian group operation $\oplus$ defined by:

$$(g \oplus h)(w) := \begin{cases} g(w) + h(w) - 2f(w) + 1 & \text{if } g(w) + h(w) \geq f(w) \\ g(w) + h(w) + 2f(w) - 1 & \text{if } g(w) + h(w) \leq -f(w) \\ g(w) + h(w) & \text{otherwise} \end{cases}$$

for every g, $h \in G$ and every $w \in \mathbb{W}$.

It remains to prove that $\textsc{Free}(1)\big[G\big]$ is undecidable. Let $w \in \mathbb{W}$. Let $g \in G$ be defined by: $g(w) := 1$ and $g(v) := 0$ for every $v \in \mathbb{W} \setminus \{w\}$. Clearly, g generates a subgroup of G with cardinality $2f(w) - 1$. Therefore, the following three assertions are equivalent: g is torsion, $f(w) \neq \infty$, and M halts on input w. Hence, there exists a many-one reduction from the halting problem to $\textsc{Free}(1)\big[G\big]$. □

For any commutative semigroup S with a recursive underlying set and any integer $k \geq 2$, $\textsc{Free}(k)\big[S\big]$ is trivially decidable. Hence, by Theorem 5.1, there exists a group G with a recursive underlying set satisfying the following two properties: $\textsc{Free}(1)\big[G\big]$ is undecidable and $\textsc{Free}(k)\big[G\big]$ is decidable for every integer $k \geq 2$.

Open question 4. *Does there exist a semigroup S with a recursive underlying set and an integer $k \geq 2$ satisfying the following two properties:* $\textsc{Free}(k)\big[S\big]$ *is undecidable and* $\textsc{Free}(k+1)\big[S\big]$ *is decidable?*

5.1. Regular behaviors

Theorem 5.1 identifies a "misbehavior" of the freeness problems. The next proposition ensures that a large class of problems related to the combinatorics of semigroups are well-behaved.

For any set S, let $\mathcal{P}(S)$ denote the *power set* of S.

Proposition 5.2. *Let S be a semigroup with a recursive underlying set, let A be a recursive set, and let $\mathcal{Y}$ be a subset of $\mathcal{P}(S) \times A$. For every integer $k \geq 1$, let $\mathrm{D}(k)$ denote the following problem: given a k-element subset $X \subseteq S$ and an element $a \in A$, decide whether $(X^+, a) \in \mathcal{Y}$. Let F denote the following problem: given a finite subset $X \subseteq S$ and an element $a \in A$, decide whether $(X, a) \in \mathcal{Y}$. Assume that the operation of S is computable and that F is decidable. One of the following two assertions holds:*

(1) *for every integer $k \geq 1$, $\mathrm{D}(k)$ is decidable;*
(2) *there exists an integer $l \geq 1$ such that*
   - *$\mathrm{D}(k)$ is decidable for every integer k with $1 \leq k < l$ and*
   - *$\mathrm{D}(k)$ is undecidable for every integer $k \geq l$.*

Proof. Let (X, a) be an instance of $\mathrm{D}(k)$. First, assume that X is not a subsemigroup of S. Then, there exist x, $x' \in X$ such that $xx' \notin X$. Remark that $(X \cup \{xx'\}, a)$ is an instance of $\mathrm{D}(k+1)$. Moreover, we have $(X \cup \{xx'\})^+ = X^+$. Therefore, (X, a) is a yes-instance of $\mathrm{D}(k)$ iff $(X \cup \{xx'\}, a)$ is a yes-instance of $\mathrm{D}(k+1)$. Second, assume that X is a subsemigroup of S. Then, (X, a) is a yes-instance of $\mathrm{D}(k)$ iff (X, a) is a yes-instance of F.

It follows from the preceding discussion that $\mathrm{D}(k+1)$ is decidable only if $\mathrm{D}(k)$ is decidable. Therefore, the desired result holds. $\square$

Proposition 5.2 easily applies to semigroup membership problems: if $A = S$ and if $\mathcal{Y}$ equals the set of all $(X, a) \in \mathcal{P}(S) \times S$ such that $a \in X$ then $\mathrm{D}(k)$ equals $\textsc{Member}(k)\big[S\big]$. Let us now show that Proposition 5.2 also applies to mortality, semigroup finiteness, and semigroup boundedness problems by selecting $A := \{\mathtt{a}\}$. Let $\mathcal{Z}$ be the set of all $X \in \mathcal{P}(S)$ such that the zero element of S belongs to X; in the case where $\mathcal{Y} = \mathcal{Z} \times \{\mathtt{a}\}$, $\mathrm{D}(k)$ is equivalent to $\textsc{Mortal}(k)\big[S\big]$. Let $\mathcal{F}$ be the set of all finite subsets of S; in the case where $\mathcal{Y} = \mathcal{F} \times \{\mathtt{a}\}$, $\mathrm{D}(k)$ is equivalent to $\textsc{Finite}(k)\big[S\big]$. Let d be a positive integer and let $\mathcal{B}$ be the set of all bounded subsets of $\mathbb{Q}^{d \times d}$; in the case where $S = \mathbb{Q}^{d \times d}$ and $\mathcal{Y} = \mathcal{B} \times \{\mathtt{a}\}$, $\mathrm{D}(k)$ is equivalent to $\textsc{Bounded}(k)\big[\mathbb{Q}^{d \times d}\big]$. Lastly, consider the case where $S = \mathbb{W} \times \mathbb{W}$, $A = \mathbb{W} \times \mathbb{W} \times \mathbb{W} \times \mathbb{W}$, and $\mathcal{Y}$ equals the set of all $(X, (s, s', t, t')) \in \mathcal{P}(S) \times A$ such that $sxs' = tyt'$ for some $(x, y) \in X \cup \{(\varepsilon, \varepsilon)\}$. Then, $\mathrm{D}(k)$ is equivalent to $\mathrm{GPCP}(k)$.

$\mathrm{GPCP}(2)$ is decidable [21] and $\mathrm{GPCP}(5)$ is undecidable [22], so there exists $l \in [\![3, 5]\!]$ such that for every integer $k \geq 1$, $\mathrm{GPCP}(k)$ is decidable iff $k < l$. Let us illustrate the cases of semigroup finiteness, semigroup boundedness, mortality, and semigroup membership problems with results drawn from the literature. Let

d be a fixed positive integer. $\textsc{Finite}[\mathbb{Q}^{d\times d}]$ is decidable [26, 35], so for every integer $k \geq 1$, $\textsc{Finite}(k)[\mathbb{Q}^{d\times d}]$ is decidable. $\textsc{Bounded}(1)[\mathbb{Q}^{d\times d}]$ is decidable by Proposition 2.10 and $\textsc{Bounded}(2)[\mathbb{Q}^{47\times 47}]$ is undecidable [5], so for every integer $k \geq 1$, $\textsc{Bounded}(k)[\mathbb{Q}^{47\times 47}]$ is decidable iff $k = 1$. $\textsc{Mortal}(1)[\mathbb{Z}^{d\times d}]$ is decidable because for every $M \in \mathbb{Z}^{d\times d}$, $\{M\}$ is a yes-instance of $\textsc{Mortal}(1)[\mathbb{Z}^{d\times d}]$ iff M^d is a zero matrix. On the other hand, $\textsc{Mortal}(7)[\mathbb{Z}^{3\times 3}]$ is undecidable [22]. Therefore, there exists $l_0 \in [\![2, 7]\!]$ such that for every integer $k \geq 1$, $\textsc{Mortal}(k)[\mathbb{Z}^{3\times 3}]$ is decidable iff $k < l_0$. $\textsc{Member}(1)[\mathbb{Q}^{d\times d}]$ is decidable [29] and $\textsc{Member}(k)[S]$ can be seen as a generalization of $\textsc{Mortal}(k)[S]$ for every integer $k \geq 1$ and every semigroup S with a recursive underlying set and a zero element. Therefore, there exists $l_1 \in [\![2, l_0]\!]$ such that $\textsc{Member}(k)[\mathbb{Z}^{3\times 3}]$ is decidable iff $k < l_1$.

5.2. The case of the freeness problem

Although Proposition 5.2 does not apply to freeness problems in any obvious way, the answer to Question 4 might as well be "no". Such an eventuality is supported by the next theorem, whose proof relies on the following gadget:

Definition 5.3. Let S be a semigroup. For every integer $d \geq 1$, every element $x \in S$, and every subset $Y \subseteq S$ define

$$C_d(x, Y) := \{x^d\} \cup \bigcup_{i=0}^{d-1} x^i Y.$$

The simplest non-trivial instance of the gadget is $C_2(x, \{y\}) = \{x^2, y, xy\}$. The following two lemmas establish the main properties of the gadget.

Lemma 5.4. *Let d be a positive integer, let a be a symbol, and let Σ be an alphabet such that $a \notin \Sigma$.*

- (i) *Assume that Σ is finite. Let k denote the cardinality of Σ. The cardinality of $C_d(a, \Sigma)$ equals $kd + 1$.*
- (ii) *The language $C_d(a, \Sigma)$ is a prefix code.*
- (iii) *Every non-empty word over $\{a\} \cup \Sigma$ that does not end with a belongs to $C_d(a, \Sigma)^+$.*

Proof. Parts (i) and (ii) are clear. Let $(n, b) \in \mathbb{N}\times\Sigma$. Write n in the form $n = qd+r$ with $q \in \mathbb{N}$ and $r \in [\![0, d-1]\!]$. Since a^d and $a^r b$ belong to $C_d(a, \Sigma)$, $a^n b = (a^d)^q (a^r b)$ is an element of $C_d(a, \Sigma)^+$. Put $L := \{a^n b : (n, b) \in \mathbb{N} \times \Sigma\}$. We have just proven $L \subseteq C_d(a, \Sigma)^+$. It follows $L^+ \subseteq C_d(a, \Sigma)^+$. Since L^+ equals the set of all non-empty words over $\{a\} \cup \Sigma$ that do not end with a, part (iii) holds. $\square$

In fact, it is easy to see that $C_d(a, \Sigma)^+ = (\{a\} \cup \Sigma)^\star \Sigma \{a^d\}^\star \cup \{a^d\}^+$.

Lemma 5.5. *Let S be a semigroup, let d be a positive integer, let x be an element of S, and let Y be a finite subset of S such that $x \notin Y$. Let k denote the cardinality of Y. The set $\{x\} \cup Y$ is a code iff the following two conditions are met: the cardinality of $C_d(x, Y)$ equals $kd + 1$ and $C_d(x, Y)$ is a code.*

Proof. The "only if part" follows from Lemmas 5.4 (i) and 5.4 (ii): if $\{x\} \cup Y$ is a code then x can be thought as the symbol a and Y as the alphabet Σ. Let us now prove the "if part".

Let Σ be an alphabet with cardinality k, let a be a symbol such that $a \notin \Sigma$, and let $\sigma\colon (\{a\} \cup \Sigma)^+ \to S$ be a morphism such that $\sigma(a) = x$ and $\sigma(\Sigma) = Y$. Clearly, σ maps $C_d(a, \Sigma)$ onto $C_d(x, Y)$. Assume that the cardinality of $C_d(x, Y)$ equals $kd + 1$ and that $C_d(x, Y)$ is a code. Then, by Lemma 5.4 (i), σ induces a bijection from $C_d(a, \Sigma)$ onto $C_d(x, Y)$, and subsequently, it follows from Claim 1.13 that σ is injective on $C_d(a, \Sigma)^+$. Let u, $v \in (\{a\} \cup \Sigma)^+$ be such that $\sigma(u) = \sigma(v)$. Let $b \in \Sigma$. On the one hand, we have $\sigma(ub) = \sigma(vb)$, and on the other hand, both ub and vb belong to $C_d(a, \Sigma)^+$ by Lemma 5.4 (iii). Since σ is injective on the latter set, we get $ub = vb$, which implies $u = v$. We have thus shown that σ is injective. Therefore, $\{x\} \cup Y$ is a code by Claim 1.13. □

Theorem 5.6. *Let S be a semigroup with a computable operation and let k and d be positive integers. If* $\textsc{Free}(kd + 1)\big[S\big]$ *is decidable then* $\textsc{Free}(k + 1)\big[S\big]$ *is decidable.*

Proof. It follows from Lemma 5.5 that there exists a many-one reduction from $\textsc{Free}(k + 1)\big[S\big]$ to $\textsc{Free}(kd + 1)\big[S\big]$. □

If $\textsc{Free}(k_0)\big[S\big]$ is undecidable for some integer $k_0 \geq 2$ then it follows from Theorem 5.6 that $\textsc{Free}(1 + (k_0 - 1)d)\big[S\big]$ is undecidable for every integer $d \geq 1$.

Corollary 5.7. *Let S be a semigroup with a computable operation.*

(i) *If there exists an integer $k \geq 2$ such that* $\textsc{Free}(k)\big[S\big]$ *is decidable then* $\textsc{Free}(2)\big[S\big]$ *is decidable;*
(ii) *if there exists an odd integer $k \geq 3$ such that* $\textsc{Free}(k)\big[S\big]$ *is decidable then* $\textsc{Free}(3)\big[S\big]$ *is decidable.*

6. Two-by-two matrices

The most exciting open questions about the decidability of freeness problems arise from two-by-two matrix semigroups [8, 11, 15, 30].

It is noteworthy that matrix mortality is also tricky in dimension two. In 1970, Paterson introduced $\textsc{Mortal}\big[\mathbb{Z}^{3\times 3}\big]$ and showed that the problem is undecidable [40]. Since then, the decidability of $\textsc{Mortal}\big[\mathbb{Z}^{2\times 2}\big]$ has been repeatedly reported as an open question [9, 20, 22, 31, 38, 45]. The only partial results obtained so far are: $\textsc{Mortal}(2)\big[\mathbb{Z}^{2\times 2}\big]$ is decidable [9] and $\textsc{Mortal}\big[\mathbb{N}^{d\times d}\big]$ is decidable for each integer $d \geq 1$ [6].

6.1. Toward undecidability

Although the decidabilities of $\textsc{Free}\big[\mathbb{N}^{2\times 2}\big]$, $\textsc{Free}\big[\mathbb{Z}^{2\times 2}\big]$, and $\textsc{Free}\big[\mathbb{Q}^{2\times 2}\big]$ are still open, Bell and Potapov have proven that $\textsc{Free}(7)\big[\mathcal{H}^{2\times 2}\big]$ is undecidable, where

$$\mathcal{H} := \left\{ \begin{bmatrix} x & y & z & t \\ -y & x & -t & z \\ -z & t & x & -y \\ -t & -z & y & x \end{bmatrix} : x, y, z, t \in \mathbb{Q} \right\}$$

is the skew field of rational quaternions [2]. Besides, it follows from Theorem 2.7 that $\textsc{Free}(1)\big[\mathcal{H}^{2\times 2}\big]$ is decidable: for every $M \in \mathcal{H}^{2\times 2}$, M is torsion iff $M^8 = M^{8+r(8)}$. A natural question is thus:

Open question 5. *Does there exist a commutative semiring D with a recursive underlying set and satisfying the following two properties:* $\textsc{Free}(1)\big[D^{2\times 2}\big]$ *is decidable and* $\textsc{Free}\big[D^{2\times 2}\big]$ *is undecidable?*

Let D be a semiring with a recursive underlying set such that $\textsc{Free}(1)\big[D^{2\times 2}\big]$ is decidable. Then, the set of those elements of D that are torsion under multiplication is recursive: for every $t \in D$, t is torsion under multiplication iff $\left[\begin{smallmatrix} t & 0 \\ 0 & 1 \end{smallmatrix}\right]$ is torsion under matrix multiplication. Moreover, the set of those elements of D that are torsion under addition is also recursive: for every $t \in D$, t is torsion under addition iff $\left[\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right]$ is torsion under matrix multiplication. Hence, the decidability of $\textsc{Free}(1)\big[D^{2\times 2}\big]$ nicely polices D.

Let K be an extension field of $\mathbb{Q}$ with degree d. Since there exists an injective ring homomorphism from K to $\mathbb{Q}^{d\times d}$ [27], Theorem 2.7 ensures that for every $M \in K^{2\times 2}$, M is torsion iff $M^{2d} = M^{2d+r(2d)}$. Therefore, $\textsc{Free}(1)\big[K^{2\times 2}\big]$ is decidable. Proving the undecidability of $\textsc{Free}\big[K^{2\times 2}\big]$ for some field extension K of $\mathbb{Q}$ with finite degree would solve Question 5 and be a significant advance towards proving the undecidability of $\textsc{Free}\big[\mathbb{Q}^{2\times 2}\big]$.

Let us now introduce a more general question than Question 5.

Lemma 6.1. *Let A be a commutative ring and let $X \in A^{2\times 2}$ be such that the determinant of X equals* 0.

(i) *For every $Y \in A^{2\times 2}$, equality $XXYX = XYXX$ holds;*
(ii) *the matrix X is torsion iff its trace is torsion under multiplication.*

Proof. Let t denote the trace of X.

The characteristic polynomial of X equals $\mathtt{z}^2 - t\mathtt{z}$, so $X^2 = tX$ by the Cayley-Hamilton theorem. It follows that $XXYX = tXYX = XYXX$ for every $Y \in A^{2\times 2}$, and thus part (i) holds.

Let us now turn to part (ii). On the one hand, we have $X^{n+1} = t^n X$ for every $n \in \mathbb{N}$. Therefore, t is torsion only if X is torsion. On the other hand, the trace of X^n equals t^n for every integer $n \geq 1$. Therefore, X is torsion only if t is torsion. We have thus shown part (ii). □

Part (i) of Lemma 6.1 previously appeared in [11].

Let K be a field. The *general linear group* of degree d over K is denoted $\mathrm{GL}(d, K)$:

$$\mathrm{GL}(d, K) = \left\{X \in K^{d\times d} : \det(X) \neq 0\right\}.$$

Assume that the underlying set of K is recursive and that the addition and the multiplication of K are computable. By Lemma 4.7 (ii), the additive inversion in K and the multiplicative inversion in $K \setminus \{0\}$ are also computable. In particular, determinants of matrices over K are computable, and thus $\mathrm{GL}(d, K)$ is a recursive set.

Proposition 6.2. *Let K be a field with computable operations.* $\textsc{Free}\big[K^{2\times 2}\big]$ *is decidable iff* $\textsc{Free}\big[\mathrm{GL}(2, K)\big]$ *is decidable*

Proof. The "only if part" is trivial since $\mathrm{GL}(2, K)$ is a subsemigroup of $K^{2\times 2}$. Let us now prove the "if part".

Assume that $\textsc{Free}\big[\mathrm{GL}(2, K)\big]$ is decidable. Let us explain how to decide whether a finite subset $\mathcal{X} \subseteq K^{2\times 2}$ is a code. The case where $\mathcal{X}$ is a subset of $\mathrm{GL}(2, K)$ is trivial. If $\mathcal{X}$ is not a subset of $\mathrm{GL}(2, K)$ and if the cardinality of $\mathcal{X}$ is greater than 1 then $\mathcal{X}$ is not a code by Lemma 6.1 (i). It remains to deal with the case where $\mathcal{X} = \{X\}$ for some $X \notin \mathrm{GL}(2, K)$. We rely on Lemma 6.1 ($ii$). Let t denote the trace of X. If $t = 0$ then X is torsion (and even nilpotent). If $t \neq 0$ then $\left[\begin{smallmatrix} t & 0 \\ 0 & 1 \end{smallmatrix}\right]$ belongs to $\mathrm{GL}(2, K)$, and moreover, X is torsion iff $\left[\begin{smallmatrix} t & 0 \\ 0 & 1 \end{smallmatrix}\right]$ is torsion. □

Note that the decidability of $\textsc{Free}\big[\mathrm{GL}(2, \mathbb{Q})\big]$ is *not* trivially implied by Corollary 4.9: the structure of $\mathrm{GL}(2, \mathbb{Q})$ is far more complicated than the one of $\mathrm{GL}(2, \mathbb{Z})$.

Corollary 6.3. *Let K be a field with computable operations. If* $\textsc{Free}\big[K^{2\times 2}\big]$ *is undecidable then* $\textsc{Accept}\big[K^{2\times 2}\big]$ *is undecidable.*

Proof. Assume that $\textsc{Accept}\big[K^{2\times 2}\big]$ is decidable. Then, its restriction $\textsc{Accept}\big[\mathrm{GL}(2, K)\big]$ is decidable. Since $\mathrm{GL}(2, K)$ is a group, it follows from Theorem 4.8 (ii) that $\textsc{Free}\big[\mathrm{GL}(2, K)\big]$ is decidable. Thus, Proposition 6.2 ensures that $\textsc{Free}\big[K^{2\times 2}\big]$ is decidable. □

The reader who conjectures that the answer to Question 5 is "yes" might want to first tackle:

Open question 6. *Does there exist a commutative semiring D with a recursive underlying set and satisfying the following two properties:* $\textsc{Free}(1)\big[D^{2\times 2}\big]$ *is decidable and* $\textsc{Accept}\big[D^{2\times 2}\big]$ *is undecidable?*

6.2. Toward decidability

This section focuses on the following open question.

Open question 7 ([8, 11])**.** *Is* $\textsc{Free}(2)\big[\mathbb{N}^{2\times 2}\big]$ *decidable?*

Note that if $\textsc{Free}(k)\big[\mathbb{N}^{2\times 2}\big]$ is decidable for some integer $k \geq 2$ then, by Corollary 5.7 (i), $\textsc{Free}(2)\big[\mathbb{N}^{2\times 2}\big]$ is decidable.

6.2.1. Two upper-triangular matrices

For each semiring D and each integer $d \geq 1$, let $\mathrm{Tri}(d, D)$ denote the set of all d-by-d upper-triangular matrices over D: $\mathrm{Tri}(d, D)$ is a subsemiring of $D^{d \times d}$, so in particular, $\mathrm{Tri}(d, D)$ is a multiplicative semigroup. For instance, $\mathrm{Tri}(2, D)$ is the set of all matrices of the form $\left[\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right]$ with a, b, $c \in D$.

Open question 8. *Is* $\textsc{Free}(2)\big[\mathrm{Tri}(2, \mathbb{N})\big]$ *decidable?*

For all integers k, $d \geq 1$, $\textsc{Free}(k)\big[\mathrm{Tri}(d, \mathbb{Q})\big]$ is decidable iff $\textsc{Free}(k)\big[\mathrm{Tri}(d, \mathbb{Z})\big]$ is decidable: the proof is the same as for Theorem 3.13. In particular, $\textsc{Free}(2)\big[\mathrm{Tri}(2, \mathbb{Q})\big]$ is decidable iff $\textsc{Free}(2)\big[\mathrm{Tri}(2, \mathbb{Z})\big]$ is decidable. Put

$$D_\lambda := \begin{bmatrix} \lambda & 0 \\ 0 & 1 \end{bmatrix} \qquad \text{and} \qquad T_\lambda := \begin{bmatrix} \lambda & 1 \\ 0 & 1 \end{bmatrix}.$$

for each $\lambda \in \mathbb{C}$.

Example 6.4. The sets $\{D_2, T_2\}$, $\{D_2, T_3\}$, and $\big\{D_{2/7}, T_{3/4}\big\}$ are codes under matrix multiplication [11].

Example 6.5. The sets $\big\{D_2, T_{1/2}\big\}$ and $\big\{D_{2/3}, T_{-3/5}\big\}$ are not codes under matrix multiplication since $D_2 T_{1/2} = \left[\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right] = T_{1/2} D_2 T_{1/2} D_2$ [11] and $D_{2/3} T_{-3/5} D_{2/3} T_{-3/5} = \left[\begin{smallmatrix} 4/25 & 2/5 \\ 0 & 1 \end{smallmatrix}\right] = T_{-3/5} T_{-3/5} D_{2/3} D_{2/3}$ [15].

Let $\varPi$ denote the set of all $(\lambda, \mu) \in \mathbb{C} \times \mathbb{C}$ such that $\{D_\lambda, T_\mu\}$ is not a code under matrix multiplication. One reason why it might be easier to deal with triangular matrices is that $\textsc{Free}(2)\big[\mathrm{Tri}(2, \mathbb{Q})\big]$ reduces to recognizing $\varPi \cap (\mathbb{Q} \times \mathbb{Q})$ [11]. Moreover, for all λ, $\mu \in \mathbb{C} \setminus \{0, 1\}$, the following four assertions are equivalent: $(\lambda, \mu) \in \varPi$, $(\mu, \lambda) \in \varPi$, $(\lambda^{-1}, \mu^{-1}) \in \varPi$, and $(\mu^{-1}, \lambda^{-1}) \in \varPi$ [11].

Two partial algorithms for recognizing $\varPi \cap (\mathbb{Q} \times \mathbb{Q})$ have been proposed [11,15]. The latest one, which is by Gawrychowski, Gutan, and Kisielewicz [15], seems more efficient in practice: it solves the following example much faster than the older algorithm.

Example 6.6. Put $D := D_{2/3}$ and $T := T_{3/5}$. The set $\{D, T\}$ is not a code under matrix multiplication because both products

$$DTTTTTTTTTTDDTDDTDDDDDDDDDD$$

and

$$TTDDDDDDTTDDTDTDTDDTTDDTDTT$$

are equal to

$$\begin{bmatrix} \frac{32768}{6591796875} & \frac{242996824}{146484375} \\ 0 & 1 \end{bmatrix}.$$

Note that D and T satisfy no shorter non-trivial equation [15].

In addition to showing a surprising combinatorial explosion, Example 6.6 answers an open question from [8, 11].

6.2.2. One upper-triangular and one lower-triangular matrix

Put

$$A_\lambda := \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix} \qquad \text{and} \qquad B_\lambda := \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}$$

for each $\lambda \in \mathbb{C}$. Let Λ denote the set of all $\lambda \in \mathbb{C}$ such that $\{A_\lambda, B_\lambda\}$ is not a code under matrix multiplication. The study of Λ was initiated by Brenner and Charnow [10]. Our motivation to continue is that $\text{FREE}(2)\left[\mathbb{Q}^{2\times 2}\right]$ is decidable only if $\Lambda \cap \mathbb{Q}$ is recursive. We first prove that $\Lambda = -\Lambda$.

Lemma 6.7. *For every $\lambda \in \mathbb{C}$, $\{A_\lambda, B_\lambda\}$ is a code under matrix multiplication iff $\{A_{-\lambda}, B_{-\lambda}\}$ is a code under matrix multiplication.*

Proof. For every group G and every subset $X \subseteq G$, X is a code iff $\left\{x^{-1} : x \in X\right\}$ is a code. Since $A_\lambda^{-1} = A_{-\lambda}$ and $B_\lambda^{-1} = B_{-\lambda}$ for every $\lambda \in \mathbb{C}$, the desired result holds. □

Let us now prove that every element of $\Lambda \cap \mathbb{R}$ is comprised between -1 and $+1$ exclusive.

Proposition 6.8. *For every real number λ with $|\lambda| \geq 1$, $\{A_\lambda, B_\lambda\}$ is a code under matrix multiplication.*

Proof. By Lemma 6.7, we only have to prove that $\{A_\lambda, B_\lambda\}$ is a code for every real number $\lambda \geq 1$.

Let $\mathcal{A}$ denote the set of all $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \in \mathbb{R}^{2\times 1}$ such that $0 < y < x$. Let $\mathcal{B}$ denote the set of all $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \in \mathbb{R}^{2\times 1}$ such that $0 < x < y$. Remark that for all real numbers x, $y > 0$, $A_\lambda \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$ belongs to $\mathcal{A}$ while $B_\lambda \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$ belongs to $\mathcal{B}$. Let M, $N \in \{A_\lambda, B_\lambda\}^\star$. From the previous remark, we deduce that $A_\lambda M \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right]$ belongs to $\mathcal{A}$ while $B_\lambda N \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right]$ belongs to $\mathcal{B}$. Since $\mathcal{A} \cap \mathcal{B} = \emptyset$, we have $A_\lambda M \neq B_\lambda N$. The desired result now follows from Lemma 3.4. □

Note that Λ contains complex numbers with moduli 1 or more. For instance, the imaginary unit, denoted i, belongs to Λ because

$$A_i B_i A_i = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = B_i A_i B_i .$$

Moreover, $3i \,/\, 2$ also belongs to Λ because

$$AABBABBABA = \begin{bmatrix} -41 \,/\, 4 & 33i \,/\, 8 \\ 33i \,/\, 8 & 25 \,/\, 16 \end{bmatrix} = BABAABAABB\,,$$

with $A := A_{3i/2}$ and $B := B_{3i/2}$.

Finally, let us prove the main result of the section: the supremum of $\Lambda \cap \mathbb{Q}$ equals 1.

Lemma 6.9 (Brenner and Charnow [10]). *Let λ be a real number. If there exist two integers m, $n \geq 1$ such that*

$$\lambda^2 = \frac{mn - m - n - 1}{mn} \tag{6.1}$$

then $\{A_\lambda, B_\lambda\}$ is not a code under matrix multiplication.

Proof. Let m, $n \in \mathbb{Z}$. It is easy to check that $A_\lambda^m = A_{m\lambda}$, $B_\lambda^n = B_{n\lambda}$,

$$A_\lambda B_\lambda^n A_\lambda^m B_\lambda = \begin{bmatrix} mn\lambda^4 + (m+n+1)\lambda^2 + 1 & mn\lambda^3 + (m+1)\lambda \\ mn\lambda^3 + (n+1)\lambda & mn\lambda^2 + 1 \end{bmatrix},$$

and

$$B_\lambda A_\lambda^m B_\lambda^n A_\lambda = \begin{bmatrix} mn\lambda^2 + 1 & mn\lambda^3 + (m+1)\lambda \\ mn\lambda^3 + (n+1)\lambda & mn\lambda^4 + (m+n+1)\lambda^2 + 1 \end{bmatrix}.$$

It follows that $A_\lambda B_\lambda^n A_\lambda^m B_\lambda = B_\lambda A_\lambda^m B_\lambda^n A_\lambda$ iff $mn\lambda^2 + 1 = mn\lambda^4 + (m + n + 1)\lambda^2 + 1$. Therefore, $B_\lambda A_\lambda^m B_\lambda^n A_\lambda = A_\lambda B_\lambda^n A_\lambda^m B_\lambda$ holds whenever m and n satisfy equation (6.1). □

For each integer $n \geq 3$, put $\lambda_n := \sqrt{1 - 2n^{-1} - n^{-2}}$. On the one hand, λ_n tends to 1 as n tends to infinity, and on the other hand, it follows from Lemma 6.9 that $\lambda_n \in \Lambda$: consider the special case where $m = n$ in Equation (6.1). We have thus proven that the supremum of $\Lambda \cap \mathbb{R}$ equals 1. However, λ_n is irrational.

Proposition 6.10. *For every real number $\delta > 0$, there exists $\lambda \in \mathbb{Q}$ such that $1 - \delta < \lambda < 1$ and $\{A_\lambda, B_\lambda\}$ is not a code under matrix multiplication.*

Proof. Let $(n_0, n_1, n_2, n_3, \dots)$ be the sequence of integers inductively defined by: $n_0 = 3$, $n_1 = 6$ and $n_{k+2} = 6n_{k+1} - n_k - 6$ for every $k \in \mathbb{N}$. It is easy to check that:

$$n_k = \frac{3}{4}\left((3 + 2\sqrt{2})^k + (3 - 2\sqrt{2})^k\right) + \frac{3}{2}$$

for every $k \in \mathbb{N}$. Hence, n_k is positive for every $k \in \mathbb{N}$ and

$$\lambda_k := 1 - \frac{n_{k+1} + n_k + 3}{2n_{k+1}n_k}$$

is a rational number that tends to 1 as k tends to infinity.

Now, remark that the bivariate polynomial

$$p(\mathtt{x}, \mathtt{y}) := \mathtt{x}^2 + \mathtt{y}^2 - 6\mathtt{xy} + 6\mathtt{x} + 6\mathtt{y} + 9$$

satisfies:

$$p(6\mathtt{x} - \mathtt{y} - 6, \mathtt{x}) = p(\mathtt{x}, \mathtt{y}) \tag{6.2}$$

and

$$\left(1 - \frac{\mathtt{x} + \mathtt{y} + 3}{2\mathtt{xy}}\right)^2 - \frac{\mathtt{xy} - \mathtt{x} - \mathtt{y} - 1}{\mathtt{xy}} = \frac{p(\mathtt{x}, \mathtt{y})}{4\mathtt{x}^2\mathtt{y}^2}. \tag{6.3}$$

Relying on Equation (6.2), it is easy to check by induction that $p(n_{k+1}, n_k) = 0$ for every $k \in \mathbb{N}$. Therefore, Equation (6.3) ensures that

$$\lambda_k^2 = \frac{n_{k+1}n_k - n_{k+1} - n_k - 1}{n_{k+1}n_k},$$

and thus $\{A_{\lambda_k}, B_{\lambda_k}\}$ is not a code by Lemma 6.9. □

Let Λ' denote the set of all $\lambda \in \mathbb{C}$ such that $\{A_\lambda, B_\lambda, A_{-\lambda}, B_{-\lambda}\}^\star$ is not a free group. A large literature is devoted to the study of Λ'. It is clear that $\Lambda \subseteq \Lambda'$, that $-\Lambda' = \Lambda'$, and that no transcendental number belongs to Λ'. Moreover, it is well-known that for every $\lambda \in \Lambda'$, $|\lambda| < 2$ [34]. Many rational and algebraic numbers have been identified in Λ' [1, 18]: in particular, $\sup(\Lambda' \cap \mathbb{R}) = 2$ [1]. However, the existence of a rational number λ such that $0 < |\lambda| < 2$ and $\lambda \notin \Lambda'$ is still open [18, 34]. Similarly, we state:

Open question 9 (Guyot [19])**.** *Is there any rational number λ with $|\lambda| < 1$ such that $\{A_\lambda, B_\lambda\}$ is a code under matrix multiplication?*

6.3. Substitutions over the binary alphabet

In this section, we examine:

Open question 10. *Is* Free(2)$\big[\operatorname{hom}(\mathbb{W})\big]$ *decidable?*

(The notation hom is introduced in Def. 2.11.) To motivate the introduction of Question 10, let us consider the function from $\operatorname{hom}(\mathbb{W})$ to $\mathbb{N}^{2\times 2}$ that maps each $\sigma \in \operatorname{hom}(\mathbb{W})$ to

$$P_\sigma := \begin{bmatrix} |\sigma(\mathtt{0})|_{\mathtt{0}} & |\sigma(\mathtt{1})|_{\mathtt{0}} \\ |\sigma(\mathtt{0})|_{\mathtt{1}} & |\sigma(\mathtt{1})|_{\mathtt{1}} \end{bmatrix}$$

(according to Definition 2.12, P_σ is the incidence matrix of σ relative to `01`). The considered function is clearly surjective, it is a morphism by Claim 2.13 (i), and it is "almost injective" by Claim 2.13 (ii). Therefore, the semigroups $\operatorname{hom}(\mathbb{W})$ and $\mathbb{N}^{2\times 2}$ have very similar structures, and thus Questions 7 and 10 are likely similar. However, we do not know whether Question 10 is easier or harder to solve than Question 7.

The following claim is an immediate corollary of Claim 2.13 (i); it provides a simple way to generate yes-instances of Free(2)$\big[\operatorname{hom}(\mathbb{W})\big]$ from yes-instances of Free(2)$\big[\mathbb{N}^{2\times 2}\big]$.

Claim 6.11. Let σ, $\tau \in \operatorname{hom}(\mathbb{W})$ be such that $P_\sigma \neq P_\tau$. If $\{P_\sigma, P_\tau\}$ is a code under matrix multiplication then $\{\sigma, \tau\}$ is a code under function composition.

For instance, let us construct four yes-intances of $\mathrm{FREE}(2)\big[\hom(\mathbb{W})\big]$ from Example 6.4:

Example 6.12. For each $p \in \mathbb{N}$, let δ_p, τ_p, $\tau'_p \in \hom(\mathbb{W})$ be defined by:

$$\begin{cases} \delta_p(\mathtt{0}) := \mathtt{0}^p \\ \delta_p(\mathtt{1}) := \mathtt{1} \end{cases}, \qquad \begin{cases} \tau_p(\mathtt{0}) := \mathtt{0}^p \\ \tau_p(\mathtt{1}) := \mathtt{10} \end{cases}, \qquad \text{and} \qquad \begin{cases} \tau'_p(\mathtt{0}) := \mathtt{0}^p \\ \tau'_p(\mathtt{1}) := \mathtt{01} \end{cases}.$$

In the notation of Section 6.2.1, we have $P_{\delta_p} = D_p$ and $P_{\tau_p} = P_{\tau'_p} = T_p$ for every $p \in \mathbb{N}$. It then follows from Example 6.4 and Claim 6.11 that $\{\delta_2, \tau_2\}$, $\{\delta_2, \tau_3\}$, $\{\delta_2, \tau'_2\}$, and $\{\delta_2, \tau'_3\}$ are codes under function composition.

The next two yes-instances of $\mathrm{FREE}(2)\big[\hom(\mathbb{W})\big]$ cannot be obtained by applying the previous method. Note that testing the injectivity of a given element $\sigma \in \hom(\mathbb{W})$ is trivial: σ is injective iff $\sigma(\mathtt{01}) \neq \sigma(\mathtt{10})$ (see Ex. 1.10). Recall also that injective functions are left-cancellative under composition (Ex. 3.3) and that left-cancellability occurs in the hypotheses of Lemma 3.4.

Example 6.13. Let υ, $\upsilon' \in \hom(\mathbb{W})$ be defined by:

$$\begin{cases} \upsilon(\mathtt{0}) := \mathtt{01} \\ \upsilon(\mathtt{1}) := \mathtt{011} \end{cases} \qquad \text{and} \qquad \begin{cases} \upsilon'(\mathtt{0}) := \mathtt{10} \\ \upsilon'(\mathtt{1}) := \mathtt{110} \end{cases}.$$

For any $x \in \{\mathtt{0},\mathtt{1}\}^+$, $\upsilon(x)$ begins with $\mathtt{0}$ while $\upsilon'(x)$ begins with $\mathtt{1}$. Therefore, for any α, $\alpha' \in \hom(\mathbb{W})$, we have $\upsilon\alpha \neq \upsilon'\alpha'$ unless $\alpha(\mathtt{0}) = \alpha(\mathtt{1}) = \alpha'(\mathtt{0}) = \alpha'(\mathtt{1}) = \varepsilon$. It then follows from Lemma 3.4 that $\{\upsilon, \upsilon'\}$ is a code under function composition. However, remark that $P_\upsilon = P_{\upsilon'} = \left[\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right]$.

Example 6.14. Let ϕ, $\mu \in \hom(\mathbb{W})$ be defined by:

$$\begin{cases} \phi(\mathtt{0}) := \mathtt{01} \\ \phi(\mathtt{1}) := \mathtt{0} \end{cases} \qquad \text{and} \qquad \begin{cases} \mu(\mathtt{0}) := \mathtt{01} \\ \mu(\mathtt{1}) := \mathtt{10} \end{cases}.$$

Morphisms ϕ and μ play a central role in combinatorics of words [32, 33]; they are usually called the *Fibonacci substitution* and the *Thue-Morse substitution*, respectively. Let α, $\beta \in \{\phi, \mu\}^+$. It is easy to see that $\alpha(\mathtt{0})$ and $\beta(\mathtt{0})$ begin with $\mathtt{01}$. Therefore, $(\phi\alpha)(\mathtt{0})$ begins with $\mathtt{010}$ while $(\mu\beta)(\mathtt{0})$ begins with $\mathtt{011}$. It follows that $\phi\alpha \neq \mu\beta$. Hence, Lemma 3.4 implies that $\{\phi, \mu\}$ is a code under function composition. However, remark that $P_\phi = \left[\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right] \neq \left[\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right] = P_\mu$ and $P_\mu P_\mu P_\phi P_\mu = P_\mu P_\phi P_\mu P_\mu$. Therefore, $\{P_\phi, P_\mu\}$ is not a code under matrix multiplication.

The similarity between the following proposition and Lemma 6.1 (i) shows further similarity between $\hom(\mathbb{W})$ and $\mathbb{N}^{2\times 2}$.

Proposition 6.15. *Let $\sigma \in \hom(\mathbb{W})$ be such that σ is non-injective. For every $\tau \in \hom(\mathbb{W})$, equality $\sigma\sigma\tau\sigma = \sigma\tau\sigma\sigma$ holds.*

Proof. Put $\alpha := \sigma\sigma\tau\sigma$ and $\beta := \sigma\tau\sigma\sigma$. Since σ is non-injective, there exist $s \in \mathbb{W}$ and p, $q \in \mathbb{N}$ such that $\sigma(\mathtt{0}) = s^p$ and $\sigma(\mathtt{1}) = s^q$ (see Ex. 1.10).

First, P_σ is singular because

$$P_\sigma = \begin{bmatrix} p\,|s|_{\mathtt{0}} & q\,|s|_{\mathtt{0}} \\ p\,|s|_{\mathtt{1}} & q\,|s|_{\mathtt{1}} \end{bmatrix} = \begin{bmatrix} |s|_{\mathtt{0}} \\ |s|_{\mathtt{1}} \end{bmatrix} \begin{bmatrix} p & q \end{bmatrix} .$$

Therefore, we have $P_\sigma P_\sigma P_\tau P_\sigma = P_\sigma P_\tau P_\sigma P_\sigma$ by Lemma 6.1 (i), and thus Claim 2.13 (i) ensures that $P_\alpha = P_\beta$.

Second, let $x \in \mathbb{W}$. For every $\rho \in \hom(\mathbb{W})$, we have

$$P_\rho \begin{bmatrix} |x|_{\mathtt{0}} \\ |x|_{\mathtt{1}} \end{bmatrix} = \begin{bmatrix} |\rho(x)|_{\mathtt{0}} \\ |\rho(x)|_{\mathtt{1}} \end{bmatrix} ,$$

and thus

$$\begin{bmatrix} 1 & 1 \end{bmatrix} P_\rho \begin{bmatrix} |x|_{\mathtt{0}} \\ |x|_{\mathtt{1}} \end{bmatrix} = |\rho(x)| .$$

In particular, the latter equality holds for $\rho = \alpha$ and $\rho = \beta$, so $|\alpha(x)| = |\beta(x)|$. Since σ maps each element of $\mathbb{W}$ to a power of s, we finally get $\alpha(x) = s^{|\alpha(x)||s|^{-1}} = s^{|\beta(x)||s|^{-1}} = \beta(x)$. $\square$

7. Three-by-three matrices

The aim of this section is to prove that, for every integer $k \geq 13$, both $\text{Free}(k)\left[\mathbb{W} \times \mathbb{W}\right]$ and $\text{Free}(k)\left[\mathbb{N}^{3\times 3}\right]$ are undecidable.

We first check that $\mathbb{W} \times \mathbb{W}$ is a well-behaved semigroup in the sense of Section 5.

Proposition 7.1. *Let k_0 be a positive integer. If $\text{Free}(k_0)\left[\mathbb{W} \times \mathbb{W}\right]$ is decidable then for every $k \in [\![1, k_0]\!]$, $\text{Free}(k)\left[\mathbb{W} \times \mathbb{W}\right]$ is also decidable.*

Proof. Let u, v, $w \in \mathbb{W}$ be such that $\{u, v, w\}$ is a 3-element code. For instance, $\mathtt{1}$, $\mathtt{01}$, and $\mathtt{001}$ are suitable choices for u, v, and w, respectively. Let $\sigma\colon \mathbb{W} \to \mathbb{W}$ be the morphism defined by: $\sigma(\mathtt{0}) := u$ and $\sigma(\mathtt{1}) := v$. For any k-element subset $X \subseteq \mathbb{W} \times \mathbb{W}$,

$$X' := \{(\sigma(x), \sigma(y)) : (x, y) \in X\} \cup \{(w, w)\}$$

is a $(k + 1)$-element subset of $\mathbb{W} \times \mathbb{W}$ that satisfies: X is a code iff X' is a code. Hence, there exists a many-one reduction from $\text{Free}(k)\left[\mathbb{W} \times \mathbb{W}\right]$ to $\text{Free}(k+1)\left[\mathbb{W} \times \mathbb{W}\right]$. $\square$

Note that we do not know whether Proposition 7.1 still holds if $\mathbb{W} \times \mathbb{W}$ is replaced with $\mathbb{N}^{3\times 3}$.

7.1. Semi-Thue systems and Post correspondence problem

In this section, we revisit Claus's reduction from the accessibility problem for semi-Thue systems to the Post correspondence problem [13]. Semi-Thue systems are introduced in Definition 4.10.

Definition 7.2 (accessibility problem for semi-Thue systems [42])**.** Let Access denote the following problem: given a finite alphabet Σ, a subset $R \subseteq \Sigma^\star \times \Sigma^\star$, and two words u, $v \in \Sigma^\star$, decide whether v is accessible from u under the semi-Thue system (Σ, R). For every integer $k \geq 1$, define Access(k) as the restriction of Access to those instances (Σ, R, u, v) such that the cardinality of R equals k.

Definition 7.3 (Post correspondence problem [41])**.** Let PCP denote the following problem: given a finite alphabet Σ and two morphisms σ, $\tau\colon \Sigma^\star \to \mathbb{W}$, decide whether there exists $w \in \Sigma^+$ such that $\sigma(w) = \tau(w)$. For every integer $k \geq 1$, PCP(k) denotes the restriction of PCP to those instances (Σ, σ, τ) such that the cardinality of Σ equals k.

Remark 7.4. Strictly speaking, PCP is not a restriction of GPCP. However GPCP is a *generalization* of PCP in the sense that there is a simple, natural reduction from PCP to GPCP: for any instance (Σ, σ, τ) of PCP, (Σ, σ, τ) is a yes-instance of PCP iff there exists $a \in \Sigma$ such that $(\Sigma, \sigma, \tau, \sigma(a), \varepsilon, \tau(a), \varepsilon)$ is a yes-instance of GPCP. An even more natural idea is to transform (Σ, σ, τ) into $(\Sigma, \sigma, \tau, \varepsilon, \varepsilon, \varepsilon, \varepsilon)$, but unfortunately, $(\Sigma, \sigma, \tau, \varepsilon, \varepsilon, \varepsilon, \varepsilon)$ is always a yes-instance of GPCP because $\sigma(\varepsilon) = \varepsilon = \tau(\varepsilon)$.

Let Σ and Γ be two finite alphabets and let σ, $\tau\colon \Sigma^\star \to \Gamma^\star$ be two morphisms. Stricly speaking, (Σ, σ, τ) is not an instance PCP, unless $\Gamma = \{\mathtt{0}, \mathtt{1}\}$. However, we abuse language by identifying (Σ, σ, τ) with $(\Sigma, \gamma\sigma, \gamma\tau)$, where $\gamma\colon \Gamma^\star \to \mathbb{W}$ is any injective morphism (see Claim 1.14).

Post proved the undecidabilities of PCP and Access in 1946 and 1947, respectively [41, 42]. Since then, his results have been tremendously refined:

Theorem 7.5 (Matiyasevich and Sénizergues [36])**.** Access(3) *is undecidable.*

Theorem 7.6 (Claus [13])**.** *Let k be a positive integer. If* PCP$(k+4)$ *is decidable then* Access(k) *is decidable.*

It follows from Theorems 7.5 and 7.6 that PCP(7) is undecidable [36]. To complete the picture, let us mention that PCP(2) is decidable [21], and that the decidabilities of Access(1), Access(2), PCP(3), PCP(4), PCP(5), and PCP(6) remain open.

To prove Theorem 7.6, Claus presents a many-one reduction from Access(k) to PCP$(k+4)$ [13] (similar proofs can be found in [22, 23, 39]). In 2007, Halava, Harju, and Hirvensalo remarked that Claus's construction is freeness-friendly. In fact, as we shall see, it turns out that for any instance (Σ, σ, τ) of PCP computed by the reduction, (Σ, σ, τ) is a yes-instance of PCP iff $\{(\sigma(a), a) : a \in \Sigma\} \cup \{(\tau(a), a) : a \in \Sigma\}$ is not a code under componentwise concatenation.

Definition 7.7 (Claus instance of PCP)**.** Define a *Claus instance* of PCP as a triple of the form (Σ, σ, τ), where Σ is a finite alphabet and $\sigma,\ \tau\colon \Sigma^\star \to \{\mathtt{0}, \mathtt{1}, \mathtt{b}, \mathtt{e}, \mathtt{d}\}^\star$ are morphisms meeting the requirements listed below:

- $\mathtt{b} \in \Sigma$, $\mathtt{e} \in \Sigma$;
- $\sigma(a) \in \{\mathtt{d0}, \mathtt{d1}\}^+$ for every $a \in \Sigma \setminus \{\mathtt{b}, \mathtt{e}\}$;
- $\tau(a) \in \{\mathtt{0d}, \mathtt{1d}\}^+$ for every $a \in \Sigma \setminus \{\mathtt{b}, \mathtt{e}\}$;
- $\sigma(\mathtt{b}) \in \mathtt{b}\{\mathtt{d0}, \mathtt{d1}\}^\star$;
- $\sigma(\mathtt{e}) \in \{\mathtt{d0}, \mathtt{d1}\}^\star\mathtt{de}$;
- $\tau(\mathtt{b}) \in \mathtt{bd}\{\mathtt{0d}, \mathtt{1d}\}^\star$; and
- $\tau(\mathtt{e}) \in \{\mathtt{0d}, \mathtt{1d}\}^\star\mathtt{e}$.

Strictly speaking, Claus's original reduction [13] does not output Claus instances in the sense of Definition 7.7, but it can be easily adapted. Other similar constructions [22, 23, 39] are also adaptable.

Theorem 7.8 (Claus's theorem revisited)**.** *Let k be a positive integer. If* $\mathrm{PCP}(k+4)$ *is decidable on Claus instances then* $\textsc{Access}(k)$ *is decidable.*

A full proof Theorem 7.8 can be found in an unpublished paper by the second author [39]. Note that Theorem 7.8 can be obtained as a corollary of the following two facts:

(1) if $\mathrm{GPCP}(k+2)$ is decidable then $\textsc{Access}(k)$ is decidable and
(2) if $\mathrm{PCP}(k+2)$ is decidable on Claus instances then $\mathrm{GPCP}(k)$ is decidable [23].

Combining Theorems 7.5 and 7.8 yields:

Corollary 7.9. $\mathrm{PCP}(7)$ *is undecidable on Claus instances.*

7.2. MIXED MODIFICATION OF THE POST CORRESPONDENCE PROBLEM

The following problem is a useful link between $\textsc{Free}\big[\mathbb{W} \times \mathbb{W}\big]$ and the restriction of PCP to Claus instances.

Definition 7.10 (mixed modification of the PCP [11])**.** Let MMPCP denote the following problem: given an instance (Σ, σ, τ) of PCP, decide whether there exist an integer $n \geq 1$, n symbols $a_1, a_2, \dots, a_n \in \Sigma$ and $2n$ morphisms $\sigma_1, \sigma_2, \dots, \sigma_n$, $\tau_1, \tau_2, \dots, \tau_n \in \{\sigma, \tau\}$ such that

$$\sigma_1(a_1)\sigma_2(a_2)\dots\sigma_n(a_n) = \tau_1(a_1)\tau_2(a_2)\dots\tau_n(a_n) \tag{7.1}$$

and

$$(\sigma_1, \sigma_2, \dots, \sigma_n) \neq (\tau_1, \tau_2, \dots, \tau_n). \tag{7.2}$$

For every integer $k \geq 1$, $\mathrm{MMPCP}(k)$ denotes the restriction of MMPCP to those instances (Σ, σ, τ) such that the cardinality of Σ equals k.

The fundamental property of MMPCP can be stated as follows:

Claim 7.11. Let (Σ, σ, τ) be an instance of MMPCP such that $\sigma(a) \neq \tau(a)$ for every $a \in \Sigma$. (Σ, σ, τ) is a yes-instance of MMPCP iff $\{(\sigma(a), a) : a \in \Sigma\} \cup \{(\tau(a), a) : a \in \Sigma\}$ is not a code under componentwise concatenation.

It is clear that every yes-instance of PCP is also a yes-instance of MMPCP. The following proposition ensures that the converse is true for Claus instances.

Proposition 7.12. *For every Claus instance (Σ, σ, τ) of* PCP*, (Σ, σ, τ) is a yes-instance of* MMPCP *iff there exists $w \in (\Sigma \setminus \{\mathtt{b}, \mathtt{e}\})^\star$ such that $\sigma(\mathtt{b}w\mathtt{e}) = \tau(\mathtt{b}w\mathtt{e})$.*

Proof. The "if part" is trivial. Let us now prove the "only if part".

For each integer $n \geq 1$, define $\mathcal{C}_n$ as the set of those n-tuples $(a_i, \sigma_i, \tau_i)_{i \in [\![1,n]\!]}$ over $\Sigma \times \{\sigma, \tau\} \times \{\sigma, \tau\}$ that satisfy equation (7.1) and define $\mathcal{C}'_n$ as the set of those $(a_i, \sigma_i, \tau_i)_{i \in [\![1,n]\!]} \in \mathcal{C}_n$ that satisfy condition (7.2). There exists an integer $n \geq 1$ such that $\mathcal{C}'_n \neq \emptyset$ iff $(\Sigma, \{\mathtt{0}, \mathtt{1}, \mathtt{b}, \mathtt{e}, \mathtt{d}\}, \sigma, \tau)$ is a yes-instance of MMPCP.

Claim 7.13. For any $(a_i, \sigma_i, \tau_i)_{i \in [\![1,n]\!]} \in \mathcal{C}'_n$, $\sigma_1 = \tau_1$ implies $(a_i, \sigma_i, \tau_i)_{i \in [\![2,n]\!]} \in \mathcal{C}'_{n-1}$.

Claim 7.14. For any $(a_i, \sigma_i, \tau_i)_{i \in [\![1,n]\!]} \in \mathcal{C}'_n$, $\sigma_n = \tau_n$ implies $(a_i, \sigma_i, \tau_i)_{i \in [\![1,n-1]\!]} \in \mathcal{C}'_{n-1}$.

Lemma 7.15. *Let $(a_i, \sigma_i, \tau_i)_{i \in [\![1,n]\!]} \in \mathcal{C}'_n$ and let $k \in [\![1, n-1]\!]$. If $a_k = \mathtt{e}$ or $a_{k+1} = \mathtt{b}$ then $(a_i, \sigma_i, \tau_i)_{i \in [\![1,k]\!]}$ belongs to $\mathcal{C}'_k$ or $(a_i, \sigma_i, \tau_i)_{i \in [\![k+1,n]\!]}$ belongs to $\mathcal{C}'_{n-k}$.*

Proof. We only prove the statement in the case where $a_k = \mathtt{e}$ because the case where $a_{k+1} = \mathtt{b}$ is handled in the same way.

Put $s := \sigma_1(a_1)\sigma_2(a_2)\ldots\sigma_k(a_k)$ and $t := \tau_1(a_1)\tau_2(a_2)\ldots\tau_k(a_k)$. We have $|\sigma(\mathtt{e})|_{\mathtt{e}} = |\tau(\mathtt{e})|_{\mathtt{e}} = 1$ and $|\sigma(a)|_{\mathtt{e}} = |\tau(a)|_{\mathtt{e}} = 0$ for every $a \in \Sigma \setminus \{\mathtt{e}\}$. From that we deduce:

$$|s|_{\mathtt{e}} = |a_1 a_2 \ldots a_k|_{\mathtt{e}} = |t|_{\mathtt{e}}\,. \tag{7.3}$$

Assume that $a_k = \mathtt{e}$. Now, both s and t end with $\mathtt{e}$. Hence, if t was a proper prefix of s then we would have $|t|_{\mathtt{e}} < |s|_{\mathtt{e}}$ in contradiction with Equation (7.3). In the same way s cannot be a proper prefix of t. Therefore, s equals t. It follows that $(a_i, \sigma_i, \tau_i)_{i \in [\![1,k]\!]} \in \mathcal{C}_k$ and $(a_i, \sigma_i, \tau_i)_{i \in [\![k+1,n]\!]} \in \mathcal{C}_{n-k}$, and at least one of them satisfies (7.2). □

Let n be the smallest positive integer such that $\mathcal{C}'_n \neq \emptyset$; let $(a_i, \sigma_i, \tau_i)_{i \in [\![1,n]\!]}$ be an element of $\mathcal{C}'_n$. Claim 7.13 ensures

$$\sigma_1 \neq \tau_1,$$

and since $\sigma_1(a_1)$ and $\tau_1(a_1)$ start with the same letter, we have

$$a_1 = \mathtt{b}.$$

In the same way, Claim 7.14 ensures $\sigma_n \neq \tau_n$, and since $\sigma_n(a_n)$ and $\tau_n(a_n)$ end with the same letter, we have

$$a_n = \mathtt{e}.$$

Furthermore, Lemma 7.15 ensures

$$a_i \neq \mathtt{b} \text{ and } a_i \neq \mathtt{e}$$

for every $i \in [\![2, n-1]\!]$. Hence, $w := a_2 a_3 \dots a_{n-1}$ belongs to $(\Sigma \setminus \{\mathtt{b}, \mathtt{e}\})^\star$.

Without loss of generality, we may assume $\sigma_1 = \sigma$ and $\tau_1 = \tau$. To complete the proof of the proposition, it suffices to show that, for every $i \in [\![2, n]\!]$, $\sigma_i = \sigma$ and $\tau_i = \tau$. We proceed by induction. Let i, $j \in [\![1, n]\!]$ be such that $\sigma = \sigma_1 = \sigma_2 = \dots = \sigma_i$ and $\tau = \tau_1 = \tau_2 = \dots = \tau_j$.

(*i*) If $\sigma(a_1 a_2 \dots a_i) = \tau(a_1 a_2 \dots a_j)$ then $a_1 a_2 \dots a_i = a_1 a_2 \dots a_j = \mathtt{b}w\mathtt{e}$. Indeed, if $\sigma(a_i)$ and $\tau(a_j)$ end with the same letter, then $a_i = a_j = \mathtt{e}$ and $i = j = n$ follows.

(*ii*) If $\sigma(a_1 a_2 \dots a_i)$ is a proper prefix of $\tau(a_1 a_2 \dots a_j)$ then $\sigma_{i+1} = \sigma$. Indeed, assume that there exists a non-empty word s such that $\sigma(a_1 a_2 \dots a_i)s = \tau(a_1 a_2 \dots a_j)$. On the one hand, s starts with the same letter as $\sigma_{i+1}(a_{i+1})$. On the other hand, s belongs to $\{\mathtt{d0}, \mathtt{d1}\}^\star\mathtt{d}$ since $\sigma(a_1 a_2 \dots a_i) \in \mathtt{b}\{\mathtt{d0}, \mathtt{d1}\}^\star$ while $\tau(a_1 a_2 \dots a_j) \in \mathtt{bd}\{\mathtt{0d}, \mathtt{1d}\}^\star$. Hence, $\sigma_{i+1}(a_{i+1})$ starts with $\mathtt{d}$, and $\sigma_{i+1} = \sigma$ follows.

(*iii*) If $\tau(a_1 a_2 \dots a_j)$ is a proper prefix of $\sigma(a_1 a_2 \dots a_i)$ then $\tau_{j+1} = \tau$. Point (*iii*) is proven in the same way as point (*ii*). ☐

Theorem 7.16 (Halava *et al.* [22])**.** MMPCP(7) *is undecidable on Claus instances.*

Proof. Proposition 7.12 ensures that PCP and MMPCP are equivalent on Claus instances. Therefore, MMPCP(7) is undecidable on Claus instances by Corollary 7.9. ☐

Note that the decidability of MMPCP(k) remains open for each $k \in [\![2, 6]\!]$.

7.3. Proofs of the main results

We first prove that $\text{Free}(k)\big[\mathbb{W} \times \mathbb{W}\big]$ is undecidable for every integer $k \geq 13$. The idea is to construct a many-one reduction from MMPCP(7) on Claus instances to $\text{Free}(13)\big[\mathbb{W} \times \mathbb{W}\big]$.

Lemma 7.17. *Let S be a semigroup, let X be a subset of S, let s_1, t_1, s_2, $t_2 \in X$ and let $Y := (X \setminus \{s_1, t_1, s_2, t_2\}) \cup \{t_2 s_1, s_2 t_1, t_2 t_1\}$. If X is a code then Y is also a code.*

Proof. If X is an alphabet and if $S = X^+$ then Y is a prefix code over X. The general case follows. ☐

The converse of Lemma 7.17 is false in general. If $S = \{\mathtt{0}, \mathtt{1}, \mathtt{2}\}^+$ and if $X = \{s_1, t_1, s_2, t_2\}$ with $s_1 := \mathtt{01}$, $t_1 := \mathtt{2}$, $s_2 := \mathtt{0}$ and $t_2 := \mathtt{12}$ then $Y = \{t_2 s_1, s_2 t_1, t_2 t_1\} = \{\mathtt{1201}, \mathtt{02}, \mathtt{122}\}$ is a prefix code; however, X is not a code since $s_1 t_1 = \mathtt{012} = s_2 t_2$.

Theorem 7.18. *Let k be a positive integer. If* $\textsc{Free}(2k-1)\left[\mathbb{W} \times \mathbb{W}\right]$ *is decidable then both* $\mathrm{PCP}(k)$ *and* $\mathrm{MMPCP}(k)$ *are decidable on Claus instances.*

Proof. Let (Σ, σ, τ) be a Claus instance of $\mathrm{PCP}(k)$. For each $w \in \Sigma^\star$, put

$$s_w := (\sigma(w), w)$$

and

$$t_w := (\tau(w), w).$$

Let X and Y denote the two subsets of $\{\mathtt{0}, \mathtt{1}, \mathtt{b}, \mathtt{e}, \mathtt{d}\}^\star \times \Sigma^\star$ defined by:

$$X := \{s_a : a \in \Sigma\} \cup \{t_a : a \in \Sigma\}$$

and

$$Y := (X \setminus \{s_{\mathtt{b}}, t_{\mathtt{b}}, s_{\mathtt{e}}, t_{\mathtt{e}}\}) \cup \{t_{\mathtt{e}} s_{\mathtt{b}}, s_{\mathtt{e}} t_{\mathtt{b}}, t_{\mathtt{e}} t_{\mathtt{b}}\}.$$

Compute two injective morphisms $\phi\colon \Sigma^\star \to \mathbb{W}$ and $\psi\colon \{\mathtt{0}, \mathtt{1}, \mathtt{b}, \mathtt{e}, \mathtt{d}\}^\star \to \mathbb{W}$ (see Claim 1.14) and

$$Z := \{(\psi(y_1), \phi(y_2)) : (y_1, y_2) \in Y\}.$$

It is clear that X, Y, and Z are computable from (Σ, σ, τ). Moreover, the cardinality of X equals $2k$, the cardinality of Y equals $2k-1$, and Z is an instance of $\textsc{Free}(2k-1)\left[\mathbb{W} \times \mathbb{W}\right]$. It remains to prove that the following five assertions are equivalent:

(*i*) (Σ, σ, τ) is a yes-instance of $\mathrm{PCP}(k)$;
(*ii*) (Σ, σ, τ) is a yes-instance of $\mathrm{MMPCP}(k)$;
(*iii*) X is not a code;
(*iv*) Y is not a code;
(*v*) Z is not a code.

By Proposition 7.12, (*i*) and (*ii*) are equivalent. By Claim 7.11, (*ii*) and (*iii*) are equivalent. By Lemma 7.17, (*iv*) implies (*iii*). Since Z is the image of Y under an injective morphism, (*iv*) and (*v*) are equivalent.

Assume that (Σ, σ, τ) is a yes-instance of $\mathrm{MMPCP}(k)$. By Proposition 7.12, there exists $w \in (\Sigma \setminus \{\mathtt{b}, \mathtt{e}\})^\star$ such that $\sigma(\mathtt{b}w\mathtt{e}) = \tau(\mathtt{b}w\mathtt{e})$. The word w satisfies $s_{\mathtt{b}} s_w s_{\mathtt{e}} = s_{\mathtt{b}w\mathtt{e}} = t_{\mathtt{b}w\mathtt{e}} = t_{\mathtt{b}} t_w t_{\mathtt{e}}$, and thus we have

$$(t_{\mathtt{e}} s_{\mathtt{b}}) s_w (s_{\mathtt{e}} t_{\mathtt{b}}) = (t_{\mathtt{e}} t_{\mathtt{b}}) t_w (t_{\mathtt{e}} t_{\mathtt{b}}). \tag{7.4}$$

Since $t_{\mathtt{e}} s_{\mathtt{b}} \in Y$, $t_{\mathtt{e}} t_{\mathtt{b}} \in Y$, $s_w (s_{\mathtt{e}} t_{\mathtt{b}}) \in Y^+$, $t_w (t_{\mathtt{e}} t_{\mathtt{b}}) \in Y^+$ and $t_{\mathtt{e}} s_{\mathtt{b}} \neq t_{\mathtt{e}} t_{\mathtt{b}}$, equation (7.4) ensures that Y is not a code. Therefore, (*ii*) implies (*iv*). $\square$

Corollary 7.19. *For every integer $k \geq 13$, $\text{Free}(k)\big[\mathbb{W} \times \mathbb{W}\big]$ is undecidable.*

Proof. Combining Corollary 7.9 and Theorem 7.18, we obtain that $\text{Free}(13)\big[\mathbb{W} \times \mathbb{W}\big]$ is undecidable. Hence, the corollary holds by Proposition 7.1. □

By way of digression, let us briefly summarize the current knowledge about the decidability of $\text{Free}(k)\big[\mathbb{W}^{\times d}\big]$ for k, $d \in \mathbb{N} \setminus \{0\}$. On the one hand, $\text{Free}(k)\big[\mathbb{W}\big]$ is decidable for every integer $k \geq 1$ [4], and so is $\text{Free}(2)\big[\mathbb{W}^{\times d}\big]$ for every integer $d \geq 1$ (Ex. 1.10). On the other hand, if $\text{Free}(k)\big[\mathbb{W}^{\times (d+1)}\big]$ is decidable then $\text{Free}(k)\big[\mathbb{W}^{\times d}\big]$ is also decidable because there exist injective morphisms from $\mathbb{W}^{\times d}$ to $\mathbb{W}^{\times (d+1)}$: for instance, the function mapping each $(u_1, u_2, \ldots, u_d) \in \mathbb{W}^{\times d}$ to $(u_1, u_2, \ldots, u_d, \varepsilon)$. Hence, it follows from Corollary 7.19 that $\text{Free}(k)\big[\mathbb{W}^{\times d}\big]$ is undecidable for every $(k, d) \in (\mathbb{N} \setminus [\![0, 12]\!]) \times (\mathbb{N} \setminus \{0, 1\})$.

Open question 11. *For each $(k, d) \in [\![3, 12]\!] \times (\mathbb{N} \setminus \{0, 1\})$, the decidability of $\text{Free}(k)\big[\mathbb{W}^{\times d}\big]$ is open.*

Let us now return to our main plot. It remains to prove that $\text{Free}(k)\big[\mathbb{N}^{3\times 3}\big]$ is undecidable for every integer $k \geq 13$.

Lemma 7.20 ([11, 22, 40])**.** *There exists an injective morphism from $\mathbb{W} \times \mathbb{W}$ to $\mathbb{N}^{3\times 3}$.*

Proof. Let $\beta \colon \mathbb{W} \to \mathbb{N}$ be defined by: $\beta(\mathtt{0}) = 0$, $\beta(\mathtt{1}) = 1$, and $\beta(uv) = \beta(u) + 2^{|u|}\beta(v)$ for every u, $v \in \mathbb{W}$. The word $a_n \ldots a_2 a_1$ is a binary expansion of the natural number $\beta(a_1 a_2 \ldots a_n)$ for any integer $n \geq 1$ and any a_1, a_2, $\ldots$, $a_n \in \{\mathtt{0}, \mathtt{1}\}$. Let $\Phi \colon \mathbb{W} \times \mathbb{W} \to \mathbb{N}^{3\times 3}$ be defined by:

$$\Phi(u, v) := \begin{bmatrix} 2^{|u|} & 0 & \beta(u) \\ 0 & 2^{|v|} & \beta(v) \\ 0 & 0 & 1 \end{bmatrix}$$

for every u, $v \in \mathbb{W}$. It is easy to check that Φ is a morphism: $\Phi(uu', vv') = \Phi(u, v)\Phi(u', v')$ for all u, u', v, $v' \in \mathbb{W}$. Note that β is not injective since $\beta(u) = \beta(u\mathtt{0})$ for every $u \in \mathbb{W}$. However, the function mapping each $u \in \mathbb{W}$ to $(|u|, \beta(u))$ is injective. Hence, Φ is injective. □

Lemma 7.20 can be easily generalized to higher dimensions: for every integer $d \geq 1$, there exists an injective morphism from $\mathbb{W}^{\times d}$ to $\mathbb{N}^{(d+1)\times(d+1)}$. However, there is no injective injective morphism from $\mathbb{W} \times \mathbb{W}$ to $\mathbb{C}^{2\times 2}$ [11].

Theorem 7.21. *Let k be a positive integer. If $\text{Free}(k)\big[\mathbb{N}^{3\times 3}\big]$ is decidable then $\text{Free}(k)\big[\mathbb{W} \times \mathbb{W}\big]$ is decidable.*

Proof. Any injective morphism from $\mathbb{W} \times \mathbb{W}$ to $\mathbb{N}^{3\times 3}$ induces a one-one reduction from $\text{Free}(k)\big[\mathbb{W} \times \mathbb{W}\big]$ to $\text{Free}(k)\big[\mathbb{N}^{3\times 3}\big]$. Hence, the desired result follows from Lemma 7.20. □

From Corollary 7.19 and Theorem 7.21 we deduce:

Corollary 7.22. *For every integer $k \geq 13$, $\text{Free}(k)\big[\mathbb{N}^{3\times 3}\big]$ is undecidable.*

8. Matrices of higher dimension

The main aim of this section is to prove that $\text{FREE}(2)\left[\mathbb{N}^{d\times d}\right]$ is undecidable for some integer $d \geq 1$. Although the result is not new [37], it has never been published before.

Theorem 8.1. *Let D be a semiring with a recursive underlying set and let k, d be positive integers. If $\text{FREE}(k+1)\left[D^{d\times d}\right]$ is decidable then $\text{FREE}(kd+1)\left[D\right]$ is decidable.*

Proof. We present a many-one reduction from $\text{FREE}(kd+1)\left[D\right]$ to $\text{FREE}(k+1)\left[D^{d\times d}\right]$. The construction is the same as in [37].

Let X be a $(kd+1)$-element subset of D. Write X in the form

$$X = \{x\} \cup \{y_{i,j} : (i,j) \in [\![1,d]\!] \times [\![1,k]\!]\},$$

and put

$$M := \begin{bmatrix} O & x \\ I_{d-1} & O \end{bmatrix} \qquad \text{and} \qquad N_j := \begin{bmatrix} & y_{d,j} \\ O & \vdots \\ & y_{1,j} \end{bmatrix}$$

for each $j \in [\![1,k]\!]$. Now,

$$\mathcal{X} := \{M, N_1, N_2, \ldots, N_k\}$$

is a $(k+1)$-element subset of $D^{d\times d}$ and $\mathcal{X}$ is computable from X. To complete the proof, it remains to check the correctness statement: X is a code under the multiplicative operation of D iff $\mathcal{X}$ is a code under matrix multiplication.

Recall that $\text{Tri}(d, D)$ is the set of all d-by-d upper-triangular matrices over D (see Sect. 6.2.1). Let $\phi\colon D^{d\times d} \to D$ be the function that maps a matrix to its bottom-right entry:

$$\phi\left([a_{i,j}]\right) := a_{d,d}\,.$$

Remark that ϕ induces a morphism from $\text{Tri}(d, D)$ to D.

Let $\mathcal{C}$ be the following instance of the gadget introduced in Definition 5.3:

$$\begin{aligned} \mathcal{C} &:= C_d\left(M, \{N_1, N_2, \ldots, N_k\}\right) \\ &= \left\{M^d\right\} \cup \bigcup_{i=0}^{d-1} \left\{M^i N_1, M^i N_2, \ldots, M^i N_k\right\}. \end{aligned}$$

Claim 8.2. $\mathcal{C}$ is a subset of $\text{Tri}(d, D)$, $\phi(M^d) = x$, and $\phi(M^{i-1}N_j) = y_{i,j}$ for $i \in [\![1,d]\!]$ and $j \in [\![1,k]\!]$.

Hence, ϕ induces a bijection from $\mathcal{C}$ onto X. In particular, $\mathcal{C}$ has cardinality $kd+1$, and thus Lemma 5.5 ensures:

Claim 8.3. $\mathcal{X}$ is a code iff $\mathcal{C}$ is a code.

By Claim 1.13, since ϕ is injective on $\mathcal{C}$, we have:

Claim 8.4. X is a code iff $\mathcal{C}$ is a code and ϕ is injective on $\mathcal{C}^+$.

As only the last column of the matrix N_1 is nonzero, straightforward computations yield that for every $P \in \mathrm{Tri}(d, D)$, $N_1 P = N_1 \phi(P)$. It follows that every P, $Q \in \mathcal{C}^+$ such that $\phi(P) = \phi(Q)$ satisfy also $N_1 P = N_1 Q$. Hence, under the assumption that $\mathcal{C}$ is a code, the morphism ϕ is injective on $\mathcal{C}^+$ because N_1 is cancellative in $\mathcal{C}^+$, so that:

Claim 8.5. If $\mathcal{C}$ is a code then ϕ is injective on $\mathcal{C}^+$.

Claims 8.3–8.5 imply the correctness statement. $\square$

Corollary 8.6. *For every $h \in \mathbb{N}$, $\textsc{Free}(7+h)\left[\mathbb{N}^{6\times 6}\right]$, $\textsc{Free}(5+h)\left[\mathbb{N}^{9\times 9}\right]$, $\textsc{Free}(4+h)\left[\mathbb{N}^{12\times 12}\right]$, $\textsc{Free}(3+h)\left[\mathbb{N}^{18\times 18}\right]$, and $\textsc{Free}(2+h)\left[\mathbb{N}^{36\times 36}\right]$ are undecidable.*

Proof. Let k and d be two positive integers. Apply Theorem 8.1 with $D := \mathbb{N}^{3\times 3}$ and identify $\left(\mathbb{N}^{3\times 3}\right)^{d\times d}$ with $\mathbb{N}^{3d\times 3d}$: if $\textsc{Free}(kd+1)\left[\mathbb{N}^{3\times 3}\right]$ is undecidable then $\textsc{Free}(k+1)\left[\mathbb{N}^{3d\times 3d}\right]$ is undecidable. Hence, Corollary 8.6 follows from Corollary 7.22. $\square$

In particular, $\textsc{Free}(2)\left[\mathbb{N}^{36\times 36}\right]$ is undecidable.

Lemma 8.7. *For any semiring D with a recursive underlying set and any integer $d \geq 1$, there exists a computable, injective morphism from $D^{d\times d}$ to $D^{(d+1)\times(d+1)}$.*

Proof. Map each $M \in D^{d\times d}$ to $\begin{bmatrix} M & O \\ O & 1 \end{bmatrix}$. $\square$

Let d and k be two positive integers. If $\textsc{Free}(k)\left[\mathbb{N}^{d\times d}\right]$ is undecidable then it follows from Lemma 8.7 that $\textsc{Free}(k)\left[\mathbb{N}^{e\times e}\right]$ is undecidable for every integer $e \geq d$. Table 1 summarizes our results on the decidability of $\textsc{Free}(k)\left[\mathbb{N}^{d\times d}\right]$ as (k, d) runs over $(\mathbb{N} \setminus \{0\}) \times (\mathbb{N} \setminus \{0, 1\})$. The table is to be understood as follows: if the symbol that occurs at the intersection of row d and column k is a "D" then $\textsc{Free}(k)\left[\mathbb{N}^{d\times d}\right]$ is decidable, if it is a "U" then the problem is undecidable, and if it is a "·" then the decidability of the problem is still open.

It is noteworthy that Lemma 8.7 does not hold the other way round in general.

Proposition 8.8. *Let D be a semiring, let K be a field, and let d be an integer greater than 1. There exists no injective morphism from $D^{d\times d}$ to $K^{(d-1)\times(d-1)}$.*

Proof. The proof is easily derived from the following two lemmas.

TABLE 1. Current knowledge about the decidability of $\mathrm{FREE}(k)\left[\mathbb{N}^{d\times d}\right]$ for all pairs (k,d).

		k															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	···
d	2	D	·	·	·	·	·	·	·	·	·	·	·	·	·	·	···
	3	D	·	·	·	·	·	·	·	·	·	·	·	U	U	U	···
	4	D	·	·	·	·	·	·	·	·	·	·	·	U	U	U	···
	5	D	·	·	·	·	·	·	·	·	·	·	·	U	U	U	···
	6	D	·	·	·	·	·	U	U	U	U	U	U	U	U	U	···
	7	D	·	·	·	·	·	U	U	U	U	U	U	U	U	U	···
	8	D	·	·	·	·	·	U	U	U	U	U	U	U	U	U	···
	9	D	·	·	·	U	U	U	U	U	U	U	U	U	U	U	···
	10	D	·	·	·	U	U	U	U	U	U	U	U	U	U	U	···
	11	D	·	·	·	U	U	U	U	U	U	U	U	U	U	U	···
	12	D	·	·	U	U	U	U	U	U	U	U	U	U	U	U	···
	13	D	·	·	U	U	U	U	U	U	U	U	U	U	U	U	···
	14	D	·	·	U	U	U	U	U	U	U	U	U	U	U	U	···
	15	D	·	·	U	U	U	U	U	U	U	U	U	U	U	U	···
	16	D	·	·	U	U	U	U	U	U	U	U	U	U	U	U	···
	17	D	·	·	U	U	U	U	U	U	U	U	U	U	U	U	···
	18	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	19	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	20	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	21	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	22	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	23	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	24	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	25	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	26	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	27	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	28	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	29	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	30	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	31	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	32	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	33	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	34	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	35	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	36	D	U	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	37	D	U	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	38	D	U	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	39	D	U	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	40	D	U	U	U	U	U	U	U	U	U	U	U	U	U	U	···
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

Lemma 8.9. *There exists $M \in D^{d\times d}$ such that $M^d \neq M^{d-1}$ and $M^{d+1} = M^d$.*

Proof. Let $M \in D^{d\times d}$ be as follows: for all indices i, $j \in [\![1, d]\!]$, the $(i,j)^{\text{th}}$ entry of M equals one if $j - i = 1$, and zero otherwise. It is easy to see that M^{d-1} has a one in its right-upper corner whereas both M^d and M^{d+1} are zero matrices. □

Lemma 8.10. *For every $N \in K^{(d-1)\times(d-1)}$, $N^d = N^{d-1}$ iff there exists $n \in \mathbb{N}$ such that $N^{n+1} = N^n$.*

Proof. The "only if part" of the statement is trivial. Let us now prove the "if part". Let $\mu(\mathsf{z})$ denote the minimal polynomial of N over K. Assume that $N^{n+1} = N^n$. Now, $\mu(\mathsf{z})$ divides $\mathsf{z}^{n+1} - \mathsf{z}^n = \mathsf{z}^n(\mathsf{z} - 1)$. Since the degree of $\mu(\mathsf{z})$ is at most $d-1$, $\mu(\mathsf{z})$ divides in fact $\mathsf{z}^{d-1}(\mathsf{z}-1) = \mathsf{z}^d - \mathsf{z}^{d-1}$. From that we deduce $N^d = N^{d-1}$. □

Lemma 8.10 ensures that there does not exist any matrix $N \in K^{(d-1)\times(d-1)}$ satisfying both $N^d \neq N^{d-1}$ and $N^{d+1} = N^d$. Combining the latter fact with Lemma 8.9 yields the proposition. □

To conclude the section, we put forth an interesting open question related to the decidabilities of $\textsc{Free}\big[\mathbb{Z}^{4\times 4}\big]$ and $\textsc{Free}\big[\mathbb{Q}^{4\times 4}\big]$.

Open question 12 (Bell and Potapov [2])**.** *Let $\mathcal{H}$ be as in Section 6.1. Is $\textsc{Free}\big[\mathcal{H}\big]$ decidable?*

Acknowledgements. The authors thank Juhani Karhumäki for his hospitality and Luc Guyot for his help in writing Section 6.2.2.

References

[1] A.F. Beardon, Pell's equation and two generator free Möbius groups. *Bull. London Math. Soc.* **25** (1993) 527–532.
[2] P. Bell and I. Potapov, Reachability problems in quaternion matrix and rotation semigroups. *Inform. Comput.* **206** (2008) 1353–1361.
[3] M. Benois, Parties rationnelles du groupe libre. *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences, Série A* **269** (1969) 1188–1190.
[4] J. Berstel, D. Perrin and C. Reutenauer, Codes and Automata, in *Encycl. Math. Appl.* **129** (2009).
[5] V.D. Blondel and V. Canterini, Undecidable problems for probabilistic automata of fixed dimension. *Theor. Comput. Syst.* **36** (2003) 231–245.
[6] V.D. Blondel and J.N. Tsitsiklis, When is a pair of matrices mortal? *Inf. Proc. Lett.* **63** (1997) 283–286.
[7] V.D. Blondel and J.N. Tsitsiklis, The boundedness of all products of a pair of matrices is undecidable. *Syst. Control Lett.* **41** (2000) 135–140.
[8] V.D. Blondel, J. Cassaigne and J. Karhumäki, Freeness of multiplicative matrix semigroups, in *Unsolved problems in mathematical systems and control theory*, edited by V.D. Blondel and A. Megretski. Princeton University Press (2004) 309–314.
[9] O. Bournez and M. Branicky, The mortality problem for matrices of low dimensions. *Theor. Comput. Syst.* **35** (2002) 433–448.

[10] J.L. Brenner and A. Charnow, Free semigroups of 2×2 matrices. *Pacific J. Math.* **77** (1978) 57–69.
[11] J. Cassaigne, T. Harju and J. Karhumäki, On the undecidability of freeness of matrix semigroups. *Int. J. Algebra Comput.* **9** (1999) 295–305.
[12] C. Choffrut and J. Karhumäki, Some decision problems on integer matrices. *RAIRO – Theor. Inf. Appl.* **39** (2005) 125–131.
[13] V. Claus, Some remarks on PCP(k) and related problems. *Bull. Eur. Assoc. Theoret. Comput. Sci.* **12** (1980) 54–61.
[14] A. Ehrenfeucht, J. Karhumäki and G. Rozenberg, The (generalized) Post correspondence problem with lists consisting of two words is decidable. *Theoret. Comput. Sci.* **21** (1982) 119–144.
[15] P. Gawrychowski, M. Gutan and A. Kisielewic, On the problem of freeness of multiplicative matrix semigroups. *Theoret. Comput. Sci.* **411** (2010) 1115–1120.
[16] R.H. Gilman, Computations with rational subsets of confluent groups, in *Proc. of the 3rd International Symposium on Symbolic and Algebraic Computation (EUROSAM 84)*, edited by J. Fitch. *Lect. Notes Comput. Sci.* **174** (1984) 207–212.
[17] Z. Grunschlag, *Algorithms in Geometric Group Theory.* Ph.D. thesis, Graduate division of the University of California at Berkeley (1999).
[18] A. Grytczuk and M. Wójtowicz, Beardon's diophantine equations and non-free Möbius groups. *Bull. Lond. Math. Soc.* **32** (2000) 305–310.
[19] L. Guyot, Private Communication (2008).
[20] V. Halava and T. Harju, Mortality in matrix semigroups. *Am. Math. Mon.* **108** (2001) 649–653.
[21] V. Halava, T. Harju and M. Hirvensalo, Binary (generalized) Post correspondence problem. *Theoret. Comput. Sci.* **276** (2002) 183–204.
[22] V. Halava, T. Harju and M. Hirvensalo, Undecidability bounds for integer matrices using Claus instances. *Int. J. Found. Comput. Sci.* **18** (2007) 931–948.
[23] T. Harju and J. Karhumäki, Morphisms, in *Handbook of formal languages*, edited by G. Rozenberg and A. Salomaa **1** (1997) 439–510.
[24] J.E. Hopcroft, R. Motwani and J.D. Ullman, *Introduction to automata theory, languages, and computation*, 2nd edition. Addison-Wesley (2001).
[25] R.A. Horn and C.R. Johnson, *Matrix analysis.* Corrected reprint of the 1985 original. Cambridge University Press (1990).
[26] G. Jacob, Un algorithme calculant le cardinal, fini ou infini, des demi-groupes de matrices. *Theoret. Comput. Sci.* **5** (1977) 183–204.
[27] G.J. Janusz, Algebraic number fields, in *Pure Appl. Math.* **55** (1973).
[28] M. Kambites, P.V. Silva and B. Steinberg, On the rational subset problem for groups. *J. Algebra* **309** (2007) 622–639.
[29] R. Kannan and R.J. Lipton, Polynomial-time algorithm for the orbit problem. *J. Assoc. Comput. Mach.* **33** (1986) 808–821.
[30] D.A. Klarner, J.-C. Birget and W. Satterfield, On the undecidability of the freeness of integer matrix semigroups. *Int. J. Algebra Comput.* **1** (1991) 223–226.
[31] M. Krom and M. Krom, More on mortality. *Am. Math. Mon.* **97** (1990) 37–38.
[32] M. Lothaire, *Combinatorics on words*, 2nd edition. Cambridge Mathematical Library, Cambridge University Press (1997).
[33] M. Lothaire, Algebraic combinatorics on words, in *Encycl. Math. Appl.* **90** (2002).
[34] R.C. Lyndon and P.E. Schupp, Combinatorial group theory, in *Ergebnisse der Mathematik und ihrer Grenzgebiete* **89** (1977).
[35] A. Mandel and I. Simon, On finite semigroups of matrices. *Theoret. Comput. Sci.* **5** (1977) 101–111.
[36] Yu. Matiyasevich and G. Sénizergues, Decision problems for semi-Thue systems with a few rules. *Theoret. Comput. Sci.* **330** (2005) 145–169.
[37] F. Mazoit, *Autour de quelques problèmes de décidabilité sur des semigroupes de matrices.* Rapport de stage MIM 2. École normale supérieure de Lyon (1998).

[38] M.A. Miller, Mortality for sets of 2×2 matrices. *Math. Mag.* **67** (1994) 210–213.
[39] F. Nicolas, (Generalized) Post correspondence problem and semi-Thue systems. Available at `http://arxiv.org/abs/0802.0726` (2008).
[40] M.S. Paterson, Unsolvability in 3×3 matrices. *Stud. Appl. Math.* **49** (1970) 105–107.
[41] E.L. Post, A variant of a recursively unsolvable problem. *Bull. Am. Math. Soc.* **52** (1946) 264–268.
[42] E.L. Post, Recursive unsolvability of a problem of Thue. *J. Symbolic Logic* **12** (1947) 1–11.
[43] G. Richomme, Private Communication (2007).
[44] J. Sakarovitch, *Éléments de théorie des automates*. Vuibert (2003).
[45] P. Schultz, Mortality of 2×2 matrices. *Am. Math. Mon.* **84** (1977) 463–464.
[46] A. Tarski, *A decision method for elementary algebra and geometry*, 2nd edition. University of California Press (1951).

Communicated by V. Diekert.
Received September 30, 2008. Accepted February 7, 2012.