Word problem of the Perkins semigroup via directed acyclic graphs

Sergey Kitaev[*] and Steve Seif[†‡]

February 24, 2008

Abstract

For a word w in an alphabet Γ, the alternation word digraph $Alt(w)$, a certain directed acyclic graph associated with w, is presented as a means to analyze the free spectrum of the Perkins monoid $\mathbf{B}_\mathbf{2}^\mathbf{1}$. Let $(f_n^{\mathbf{B}_\mathbf{2}^\mathbf{1}})$ denote the free spectrum of $\mathbf{B}_\mathbf{2}^\mathbf{1}$, let a_n be the number of distinct alternation word digraphs on words whose alphabet is contained in $\{x_1, \ldots, x_n\}$, and let p_n denote the number of distinct labeled posets on $\{1, \ldots, n\}$.

The word problem for the Perkins semigroup $\mathbf{B}_\mathbf{2}^\mathbf{1}$ is solved here in terms of alternation word digraphs: Roughly speaking, two words u and v are equivalent over $\mathbf{B}_\mathbf{2}^\mathbf{1}$ if and only if certain alternation graphs associated with u and v are equal. This solution provides the main application, the bounds: $p_n \leq a_n \leq f_n^{\mathbf{B}_\mathbf{2}^\mathbf{1}} \leq 2^n a_{2n}^2$. A result of the second author in a companion paper states that $(\log\ a_n) \in O(n^3)$, from which it follows that $(\log f_n^{\mathbf{B}_\mathbf{2}^\mathbf{1}}) \in O(n^3)$ as well.

Alternation word digraphs are of independent interest combinatorially. It is shown here that the computational complexity problem that has as instance $\{u, v\}$ where u, v are words of finite length, and question "Is $Alt(u) = Alt(v)$?", is co-NP-complete. Additionally, alternation word digraphs are acyclic, and certain of them are natural

[*] Institute of Mathematics, Reykjavík University, Ofanleiti 2, IS-103 Reykjavík, Iceland; e-mail: sergey@ru.is

[†] Mathematics Department, University of Louisville, Louisville KY 40292, USA; e-mail: swseif01@louisville.edu

[‡] The authors thank the Mathematics Department at the University of Kentucky for its support of both authors during the preliminary stages of this work.

extensions of posets; each realizer of a finite poset determines an extension by an alternation word digraph.

1 Introduction

Let w be a word in an alphabet Γ. The **alternation word digraph** of w, denoted $Alt(w)$, is a directed acyclic graph that encodes an aspect of the symmetry of the word w. Alternation word digraphs were defined by the second author in order to better understand the free spectrum of the Perkins semigroup $\mathbf{B_2^1}$. Definitions of alternation word digraphs, free spectra, and word problems will be given in Section 1.1 and 1.2.

Let $f_n^{\mathbf{B_2^1}}$ be the cardinality of the n-generated $\mathbf{B_2^1}$-free semigroup. The sequence $(f_n^{\mathbf{B_2^1}})$ is the free spectrum of $\mathbf{B_2^1}$. Let a_n be the number of distinct alternation word digraphs on words whose alphabet is contained in $\{x_1, \ldots, x_n\}$, and let p_n be the number of distinct labeled partially ordered sets on an n-element set. A main result of this paper, Theorem 1.8, is a solution to the word problem for $\mathbf{B_2^1}$ via alternation word digraphs. Theorem 1.11, which follows from Theorem 1.8 and its proof, connects p_n, a_n and $f_n^{\mathbf{B_2^1}}$ via the following bounds: $p_n \leq a_n \leq f_n^{\mathbf{B_2^1}} \leq 2^n a_{2n}^2$. In [15], the second author has proven that $(\log\ a_n) \in O(n^3)$, from which it follows directly (using that $O(\log p_n) = O(n^2)$) that $(\log f_n^{\mathbf{B_2^1}}) \in O(n^3)$, a result of some importance in the classification of free spectra of finite monoids and universal algebras.

As the reader might have already surmised, the foremost goal of this paper is to present alternation word digraphs as a tool to analyze the free spectrum of $\mathbf{B_2^1}$. But a second important goal is to make it evident that the alternation word digraph is a complex and rich structure. To this end, we show that given two finite words u and v, recognizing whether $Alt(u) = Alt(w)$ is co-NP-complete; the proof uses Theorem 1.8 here and an algebra-complexity result, Theorem 3.1 from [14]. More surprisingly, it is shown here that the question "Given a word w, does $Alt(w)$ have an edge?" is NP-complete, a result that follows from Theorem 1.8 and an algebra-complexity result of O. Klima [9].

In Section 1.1, we provide the definition of alternation word digraphs and briefly describe a connection between posets and alternation word digraphs. In Section 1.2, we provide background on $\mathbf{B_2^1}$ and the statements of the main results of this paper. In Section 2, we prove Theorem 1.8 and also provide a solution to the word problem for $\mathbf{B_2^1}$ as an inverse semigroup. In Section 3, we prove Theorem 1.10, a theorem with five computational complexity results. In the Conclusion, Section 4, are open problems.

We assume familiarity with basic graph theory, posets, and computational complexity. Posets are assumed to be strict (that is, non-reflexive) and thus can be regarded as loopless acyclic transitive directed graphs. Section 3 uses results from [14] and [9] concerning certain subproblems of the term-equivalence problem for $\mathbf{B_2^1}$; otherwise the paper is self-contained.

1.1 Alternation word digraphs

For a finite word w in the alphabet $\{x_1, x_2, \ldots\}$, we define $Alt(w)$, the alternation word digraph of w. Alternation word digraphs arise as a natural tool in the study of $\mathbf{B_2^1}$ (see Section 2.1); they were implicit in [14] but, to our knowledge, are defined here for the first time. Unless otherwise stated, "word" will refer to a finite word in the alphabet $\{x_1, x_2, \ldots\}$.

Definition 1.1 *Let w be a word.*

1. *Let $Var(w)$ denote the variables occurring in w.*
2. *For a word w, let $|w|$ denote the number of variables, including multiplicities, occurring in w.*
3. *If $w = a_1 \ldots a_k$ where $a_1, \ldots, a_k \in \{x_1, x_2, \ldots\}$, and if i and j are positive integers such that $1 \leq i \leq j \leq k$, then the word $a_i a_{i+1} \ldots a_j$ is said to be a* **divisor** *of w.*
4. *If y is obtained by striking out (possibly no) symbols from a word w, then y is said to be a* **subword** *of w.*
5. *For $X \subseteq Var(w)$, let w_X denote the word that results by eliminating from w all occurrences of variables not in X.*
6. *Let $w = x_{i_1} \ldots x_{i_k}$ be a word. For $c \leq k$, let $w(c) = x_{i_c}$. We say that x_{i_c} occurs in the c-th* **position** *of w.*
7. *For a word w with $|w| = k$, we say that $w(1)$ is the* **left-most variable** *of w and $w(k)$ is the* **right-most variable** *of w.*
8. *Let w^r denote the "reverse" of w.*
9. *Let $V_1(w)$ be the subset of $Var(w)$ consisting of variables that occur exactly one time in w.*
10. *Let $\overline{w}$ be the word over the alphabet $\{x_1, \ldots, x_n\} \cup \{y_1, \ldots, y_n\}$ formed from w by replacing each instance $x_i \in Var(w)$ with $x_i y_i$.*

For example, with $w = x_1x_2x_1x_2x_4x_6$, we have that $Var(w) = \{x_1, x_2, x_4, x_6\}$, that $V_1(w) = \{x_4, x_6\}$, that x_2x_1 is a divisor of w, that $x_1x_4x_6$ is not a divisor of w but is a subword of w, that $w_X = x_1x_1x_4x_6$ with $X = \{x_1, x_4, x_6\}$, that $w^r = x_6x_4x_2x_1x_2x_1$, and that $\overline{w} = x_1y_1x_2y_2x_1y_1x_2y_2x_4y_4x_6y_6$.

Definition 1.2 *Let w be a word and let X and Y be disjoint non-empty subsets of $Var(w)$. Then X and Y are* **alternating** *if for all length-two divisors x_ix_j of $w_{X \cup Y}$, we have that exactly one of $\{x_i, x_j\}$ is in X.*

Definition 1.3 *Let w be a word. $Alt(w)$, the alternation word digraph of w, has a vertex set consisting of the non-empty proper subsets of $Var(w)$. For two disjoint non-empty proper subsets $X, Y \subset Var(w)$, let $X \to Y$ be an edge of $Alt(w)$ (written $X \to Y \in E(Alt(w))$) if*

1. *X and Y are alternating in w and*
2. *the left-most variable of $w_{X\cup Y}$ is contained in X.*

Observe that X and Y alternate in w if and only if X and Y alternate in $w_{X\cup Y}$, from which it follows that $X \to Y \in Alt(w)$ if and only if $X \to Y \in Alt(w_{X\cup Y})$. In the example that follows, we use i in place of x_i and suppress commas when there is no chance of ambiguity. For example, the edge $\{x_2, x_4\} \to \{x_3\}$ will be written $24 \to 3$. In Example 1.1 below is a brief discussion of $Alt(x_1x_2x_3x_1x_4)$, whose graph is given in Figure 1.

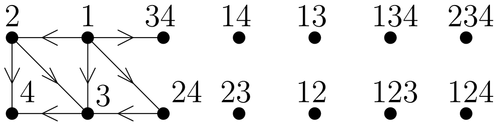

Figure 1: The digraph $Alt(x_1x_2x_3x_1x_4)$.

Example 1.1

Let $u = x_1x_2x_3x_1x_4$. The graph $Alt(u)$ has $2^4 - 2 = 14$ vertices; the edges of $Alt(u)$ are $\{1 \to 2,\ 1 \to 3,\ 2 \to 3,\ 2 \to 4,\ 3 \to 4,\ 1 \to 24,\ 1 \to 34,\ 24 \to 3\}$ (see Figure 1). For example,

- $1 \to 3$ is an edge since in $u_{\{x_1,x_3\}} = x_1x_3x_1$ occurrences of $\{x_1\}$ and $\{x_3\}$ alternate and the left-most variable of u_{x_1,x_3} is in $\{x_1\}$.

- $1 \to 34$ is an edge of $Alt(u)$ because in $u_{\{x_1,x_3,x_4\}}$ occurrences of $\{x_1\}$ alternate with occurrences of $\{x_3, x_4\}$ and the left-most variable of $u_{\{x_1,x_3,x_4\}}$ is in $\{x_1\}$.

- $24 \to 3$ is an edge because in $u_{\{x_2,x_3,x_4\}}$ occurrences of $\{x_2, x_4\}$ alternate with those of $\{x_3\}$ and the left-most variable of $u_{\{x_2,x_3,x_4\}}$ is contained in $\{x_2, x_4\}$.

- $13 \to 24$ is not an edge because x_3x_1 is a divisor of $u_{\{x_1,x_2,x_3,x_4\}} = u$.

Though they will play no essential role in the paper, we consider acyclicity and transitivity of alternation word digraphs. In general, they are not transitive, as we show in Example 1.2. A directed acyclic graph (a DAG) is a directed graph with no directed cycles; alternation word digraphs are DAGs, as we show next. For a word w and a non-empty subset $X \subseteq Var(w)$, let $n_w(X)$ be the position in w of the left-most variable contained in X.

Lemma 1.4 *Let w be a word. Then $Alt(w)$ is a DAG.*

Proof. If $A_1 \to A_2, A_2 \to A_3, \dots, A_{k-1} \to A_k$ are edges of $Alt(w)$, then $n_w(A_1) < n_w(A_2) < \dots < n_w(A_{k-1}) < n_w(A_k)$, from which it follows that $A_k \to A_1 \notin E(Alt(w))$. □

Example 1.2 *With $t = x_1x_2x_3x_1x_2x_1$, we have $1 \to 2$ and $2 \to 3$ are both in $E(Alt(t))$, but $1 \to 3$ is not. Also, with $u = x_1x_2x_3x_1x_4$, an inspection of the graph of $Alt(u)$ in Figure 1 shows that $24 \to 3$ and $3 \to 4$ are in $Alt(u)$, but $24 \to 4$ is not an edge.*

In Section 1.1.1, we provide some bounds involving the definitions below.

Definition 1.5

1. *For a positive integer n, let $Alt(n) = \{Alt(w) : Var(w) = \{x_1, \dots, x_n\}\}$.*
2. *Let a_n be the number of labeled alternation word digraphs on words with alphabet contained (properly or otherwise) in $\{x_1, \dots, x_n\}$ (or any other fixed n-letter alphabet).*
3. *Let p_n be the number of labeled posets on an n-element set.*
4. *For a word w and a vertex $U \subset Var(w)$, let $|U|$ be the* **order** *of U.*
5. *For a word w and a positive integer k, let $Alt_{\leq k}(w)$ be the graph induced by $Alt(w)$ on the set of vertices of order less than or equal to k.*
6. *Let $Alt_1(w)$ be the graph induced by $Alt(w)$ on the vertices of order 1.*

With $u = x_1x_2x_3x_1x_4$ in Example 1.1 above, we have $Alt_1(u)$ has four vertices and edges $\{1 \to 2,\ 1 \to 3,\ 2 \to 3,\ 2 \to 4,\ 3 \to 4\}$.

1.1.1 Connection between posets and alternation word digraphs

Every finite strict poset can be extended to an alternation word digraph; in fact, each realizer of a finite poset $\langle X; P\rangle$ determines an alternation word digraph $Alt(w)$ in which $\langle X; P\rangle$ (as a directed acyclic graph) is $Alt_1(w)$.

Let $\mathbf{P} = \langle\{1, \dots, n\}, P\rangle$ be a finite poset with a realizer $\mathcal{R} = \{L_1, \dots, L_k\}$. For $i = 1, \dots, k$, we have L_i is a total-ordering $\sigma_i(1) > \dots > \sigma_i(n)$, where σ_i is a permutation of $\{1, \dots, n\}$. Let $w_{\mathcal{R}} = \sigma_1(1) \dots \sigma_1(n) \dots \sigma_k(1) \dots \sigma_k(n)$, a word of length kn in the alphabet $\{1, \dots, n\}$. With a moment's thought, it will be clear that for $i \neq j \in \{1, \dots, n\}$, we have iPj if and only if i and j alternate in $w_{\mathcal{R}}$, and the left-most occurrence of i precedes the left-most occurrence of j in $w_{\mathcal{R}}$. That is, iPj if and only if $i \to j \in Alt(w_{\mathcal{R}})$. We have proved the following.

Proposition 1.6 *If $\langle X; P\rangle$ is a finite labeled poset, then there exists a finite word w with $Var(w) = X$ such that $Alt_1(w) = \langle X; P\rangle$.*

Example 1.3 *For example, with $X = \{1, 2, 3, 4\}$ and relation P such that $\langle X; P\rangle$ is the connected labeled poset with unique maximal element 1, and with $\{2, 3, 4\}$ forming an antichain, with realizers $\mathcal{R} = \{[1, 2, 3, 4], [1, 4, 3, 2]\}$ and $\mathcal{S} = \{[1, 2, 3, 4], [1, 3, 4, 2], [1, 2, 4, 3]\}$, we have $\langle X; P\rangle = Alt_1(w_{\mathcal{R}}) = Alt_1(w_{\mathcal{S}})$. Notice that $13 \to 24 \in Alt(w_{\mathcal{R}})$ but that in $Alt(w_{\mathcal{S}})$ all vertices of order greater than one are isolated.*

We have defined p_n as the number of distinct labeled posets on an n-element set. It is well-known (and not difficult to show) that $O(\log p_n)) = O(n^2)$.

Corollary 1.7 *For $n \in \mathbb{N}$, we have the following:*

1. $p_n \leq a_n$
2. $n^2 \in O(\log a_n)$

1.2 $\mathbf{B_2^1}$ background

Recall that a *semigroup* $\mathbf{S} = \langle S; * \rangle$ is a set S equipped with an associative binary operation $*$. For $a, b \in S$, we write "ab" rather than "$a*b$". A *monoid* is a semigroup with an identity element 1, satisfying $1a = a = a1$. $\mathbf{B_2}$ consists of five two-by-two matrices: the two-by-two 0-matrix (referred to as "0"), $a = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $a' = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $aa' = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, and $a'a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. $\mathbf{B_2}$ is a semigroup (but not a monoid) under the operation matrix multiplication. The six-element monoid $\mathbf{B_2^1}$, the Perkins semigroup, is formed by adding the two-by-two identity matrix (referred to as "1") to $\mathbf{B_2}$. Let $w = x_{i_1} \ldots x_{i_j}$ be a word and let K be a set of variables containing $Var(w)$. An *evaluation* $e : K \to B_2^1$ is an assignment $x_i \to s_i \in B_2^1$ (for all $x_i \in K$). Let $e(w) = e(x_{i_1}) \cdots e(x_{i_j})$, the *evaluation of w under e*. For example, with $w = x_2 x_1 x_2$ and the evaluation $e : Var(w) = \{x_1, x_2\} \to B_2^1$ given $e(x_1) = a$ and $e(x_2) = a'$, we have $e(w) = a'aa' = a'$. In like manner, evaluations can be defined for any semigroup $\mathbf{S}$. If u and v are words such that for all evaluations $e : Var(u) \cup Var(v) \to S$, we have $e(u) = e(v)$, then u and v are said to be $\mathbf{S}$-*equivalent* (denoted $u \approx_{\mathbf{S}} v$) and $u \approx_{\mathbf{S}} v$ is said to be an *identity* of $\mathbf{S}$. For example, a semigroup $\mathbf{S}$ is commutative if and only if $x_1 x_2 \approx_{\mathbf{S}} x_2 x_1$. It is not difficult to verify that $x_1^2 x_2^2 \approx_{\mathbf{B_2^1}} x_2^2 x_1^2$ and that $x_1^3 \approx_{\mathbf{B_2^1}} x_1^2$, two $\mathbf{B_2^1}$ identities that play a role in this paper. The importance of the monoid $\mathbf{B_2^1}$ was established when, in 1969, P. Perkins [12] proved that there exists no finite set Γ of $\mathbf{B_2^1}$-identities such that all identities of $\mathbf{B_2^1}$ can be derived from Γ. That is, $\mathbf{B_2^1}$ does not have a *finite basis for its identities.* Later work further established the central role of $\mathbf{B_2^1}$ in algebraic theory. We will not pursue finite basis properties in this paper as we continue our discussion of $\mathbf{B_2^1}$ as a small monoid with complex structure.

The word problem for a semigroup $\mathbf{S}$: For a given finite semigroup $\mathbf{S}$, given words u and v, is $u \approx_{\mathbf{S}} v$? The word problem for a finite semigroup $\mathbf{S}$ is decidable. Here is the statement of a main theorem of the paper, a solution to the word problem of $\mathbf{B_2^1}$. See Definition 1.1.10 for $\overline{u}, \overline{v}$ etc.

Theorem 1.8 *Let u and v be words. Then $u \approx_{\mathbf{B_2^1}} v$ over $\mathbf{B_2^1}$ if and only if*

1. $V_1(u) = V_1(v)$,
2. $Alt(\overline{u}) = Alt(\overline{v})$, *and*
3. $Alt(\overline{u^r}) = Alt(\overline{v^r})$.

The term-equivalence problem for a semigroup S, TERM-EQ(S): An instance consists of two finite words, u and v, having size $|u|+|v|$, with question, "Is $u \approx_{\mathbf{S}} v$?".[1] The term-equivalence problem for a finite semigroup is in co-NP, as is not difficult to check. It can be quite difficult to determine the computational complexity of the term-equivalence problem for a given finite semigroup. See [2], [7], [9], [4], [17], [14], [19], [20], [21]. For example, while it is known (and non-trivial) that TERM-EQ($\mathbf{G}$) is co-NP-complete when $\mathbf{G}$ is a non-solvable group ([4]), a particularly interesting open problem is to determine if all finite solvable groups have tractable term-equivalence problems.

TERM-EQ($\mathbf{B_2}$) is in P, as is evident from any of the algorithms provided in [13], [10], [17][2]. So it was somewhat surprising that TERM-EQ($\mathbf{B_2^1}$) is co-NP-complete, a result proved independently by the second author in [14] and in [9]. In this paper, we use the quite different approaches used in the proofs in [14], [9] to prove a number of hardness results involving alternation word digraphs.

Definition 1.9 1. *For a fixed positive integer k, let ALT-EQ$_{\leq k}$ have as an instance a pair of words $\{u, v\}$, with question, "Is $Alt_{\leq k}(u)$ equal to $Alt_{\leq k}(v)$?".*

2. *ALT-EQ has as an instance a pair of words $\{u, v\}$, with size $|u| + |v|$, and asks, "Is $Alt(u)$ equal to $Alt(v)$?".*

3. *Let w be a word and let $U \to V \in E(Alt(w))$. Then the* **support** *of $U \to V$ is $U \cup V$.*

   SUPPORT has as an instance a word w and a variable $x_i \in Var(w)$, with size $|w|$, and asks, "Is x_i contained in the support of some edge of $Alt(w)$?".

4. *E–ALT $= \emptyset$ has an instance a word w with size $|w|$ and asks, "Is the edge set of $Alt(w)$ empty?".*

5. *Because $x_1^2 x_2^2 \approx_{\mathbf{B_2^1}} x_2^2 x_1^2$ and $x_1^3 \approx_{\mathbf{B_2^1}} x_1^2$, it follows for a word w satisfying $Var(w) \subseteq \{x_1, \ldots, x_n\}$, we have that $wx_1^2 \ldots x_n^2 \approx_{\mathbf{B_2^1}} x_1^2 \ldots x_n^2 \approx x_1^2 \ldots x_n^2 w$. That is, $x_1^2 \ldots x_n^2$ is, a "zero", in a sense discussed below in the third footnote.*

   Let FREE–0 have as an instance (w, n), where w is a word and $n \in \mathbb{N}$, with size $|w|$, with question, "Is $w \approx_{\mathbf{B_2^1}} x_1^2 \ldots x_n^2$?".

Theorem 1.10 1. *For a fixed positive integer k, ALT-EQ$_{\leq k}$ is in P.*

2. *ALT-EQ is co-NP-complete.*

3. *SUPPORT is NP-complete.*

4. *E(ALT)$= \emptyset$ is co-NP-complete.*

5. *FREE–0 is co-NP-complete.*

[1] The term-equivalence problem is also referred to as the *identity-checking* problem.

[2] In [13], [10], $\mathbf{B_2}$ is treated as an *inverse semigroup*; in Section 2.3 we provide an alternation word digraph solution to the word problem of $\mathbf{B_2^1}$ as an inverse semigroup.

At the end of the paper, motivated by Theorem 1.10,5, we propose a conjecture that would classify all term-equivalence problems for the pseudovariety of aperiodic monoids with commuting idempotents (of which $\mathbf{B_2^1}$ is one).

1.2.1 Free spectra

As mentioned, in this paper we provide an application to free spectra of monoids. Let $\mathbf{M}$ be a finite monoid, and let w be a finite word such that $Var(w) \subseteq \{x_1, \ldots, x_n\}$. Then w determines an n-ary function $w^{\mathbf{M}} : M^n \to M$ where for $(a_1, \ldots, a_n) \in M^n$, we let $w^{\mathbf{M}}(a_1, \ldots, a_n) = e(w)$ where $e : \{x_1, \ldots, x_n\} \to M$ is the evaluation such that $e(x_i) = a_i$, for $i = 1, \ldots, n$. (If $i \leq n$ and $x_i \notin Var(w)$, then x_i is an inessential variable in the function $w^{\mathbf{M}}$.) Observe that $u \approx_{\mathbf{M}} v$ if and only if $u^{\mathbf{M}} = v^{\mathbf{M}}$. Let $F_n(\mathbf{M}) = \{w^{\mathbf{M}} : Var(w) \subseteq \{x_1, \ldots, x_n\}\}$.[3]

Let $f_n^{\mathbf{M}}$ be the cardinality of $F_n(\mathbf{M})$, and let $(f_n^{\mathbf{M}})$ denote the **free spectrum** of $\mathbf{M}$. For example, with $\mathbf{G}$ a finite Abelian group of exponent k, it is not difficult to verify that $f_n^{\mathbf{G}} = k^n$, and with $\mathbf{U_2}$ the two-element semilattice, we have $f_n^{\mathbf{U_2}} = 2^n - 1$. If $\mathbf{N}$ is contained in the pseudovariety[4] generated by a monoid $\mathbf{M}$ then for all $n \in \mathbb{N}$, we have $f_n^{\mathbf{N}} \leq f_n^{\mathbf{M}}$. If $\mathbf{M}$ is a finite non-trivial monoid, then it has either a non-trivial group homomorphic image or a non-trivial semilattice homomorphic image; thus, $f_n^{\mathbf{M}} \geq 2^n - 1$. For this reason, free spectra of a finite monoid $\mathbf{M}$ are typically analyzed up to $O(\log f_n^{\mathbf{M}})$.

Note that $f_n^{\mathbf{M}} \leq |M|^{|M|^n}$. A free spectrum is said to be *log-exponential* (or, *doubly exponential*) if there exists a finite real number c such that for all n high enough $f_n^{\mathbf{M}} \geq 2^{2^{cn}}$; otherwise, $\mathbf{M}$ is said to be *sub-log-exponential.* Well-known works of G. Higman [3] and A. Neumann [11] state that a finite group $\mathbf{G}$ is sub-log-exponential if and only if it is nilpotent; morever, $\mathbf{G}$ has nilpotency index $k \in \mathbb{N}$ if and only if $O(\log f_n^{\mathbf{G}}) = O(n^k)$, an extraordinary result correlating properties of finite algebras and their free spectra.

Much remains to be understood about free spectra of finite monoids. There is a growing literature on the asymptotic growth of sub-log-exponential free spectra of finite monoids, stimulated by a result of K. Kearnes [6] that associated, in a non-trivial way, to each finite algebra $\mathbf{A}$ a finite monoid $\mathrm{Tw}(\mathbf{A})$, the *twin monoid* of $\mathbf{A}$ in such a way that properties of the free spectrum of $\mathrm{Tw}(\mathbf{A})$ are transferred to the free spectrum of $\mathbf{A}$. For example, if $\mathrm{Tw}(\mathbf{A})$ has a log-exponential free spectrum, then so does $\mathbf{A}$, and for k a positive integer, if $n^k \in O(\log f_n^{\mathrm{Tw}(\mathbf{A})})$, then $n^k \in O(\log f_n^{\mathbf{A}})$. In [6] Kearnes asks for a classification of the growth of free spectra of finite monoids. In notes from the workshop **A Course in Tame Congruence Theory** [5], held in Budapest, July

[3] For a fixed n, the set of all functions $F_n(\mathbf{M}) = \{w^{\mathbf{M}} : Var(w) \subseteq \{x_1, \ldots, x_n\}\}$ forms a semigroup under point-wise multiplication, one that is isomorphic to the n-generated relatively free monoid in the variety generated by $\mathbf{M}$, this last fact one that we will not use in this paper. Observe that $x_1^2 \ldots x_n^2$ is the zero of the semigroup $F_n(\mathbf{B_2^1})$.

[4] The pseudovariety generated by $\mathbf{M}$ consists of all monoids in $\mathrm{HSP}_{fin}(\mathbf{M})$, the smallest class of algebras containing $\mathbf{M}$ and closed under taking of finite direct products, submonoids, and homomorphic images. If $\mathbf{N}$ is in the pseudovariety generated by $\mathbf{M}$, then, since identities are "preserved" by homomorphic images, products and submonoids, every identity of $\mathbf{M}$ is satisfied by $\mathbf{N}$. Hence, as stated above, $f_n^{\mathbf{N}} \leq f_n^{\mathbf{M}}$.

2–13, 2001, it was asked (slightly paraphrased here) whether it was true or false that for a finite monoid $\mathbf{M}$ with sub-log-exponential free spectrum, either $O(\log f_n^{\mathbf{M}})= O(p(n))$, where $p(n)$ is a polynomial, or $O(\log f_n^{\mathbf{M}}) = O(n \ \log n)$. In [18], it was shown that the answer to the above question is "no": for each $k \in \mathbb{N}$, there exists a finite monoid $\mathbf{M}$ such that $O(\log f_n^{\mathbf{M}}) = O(n^k \ \log n)$. To date there has been no complete classification of the asymptotic classes of $(\log f_n^{\mathbf{M}})$, where $(f_n^{\mathbf{M}})$ is sub-log-exponential. Nor has there been a description of finite monoids with sub-log-exponential free spectra.[5]

The free spectrum problem for a finite monoid M: Is the free spectrum of $\mathbf{M}$ sub-log-exponential? If so, determine $O(\log f_n^{\mathbf{M}})$.

$\mathbf{B_2^1}$'s history might lead one to expect difficulty with the free spectrum problem for $\mathbf{B_2^1}$. As mentioned, the principal application is a set of bounds that link the free spectrum of $\mathbf{B_2^1}$ and the sequence (a_n). Note that by Theorem 1.8, the mapping $\{w : Var(w) \subseteq \{x_1, \ldots, x_n\}\}$ into $(2^{\{x_1,\ldots,x_n\}}, Alt(2n), Alt(2n))$, given by $w \to (V_1(w), Alt(\overline{w}), Alt(\overline{w^r})$, separates all pairs of $\mathbf{B_2^1}$–inequivalent words. Thus $f_n^{\mathbf{B_2^1}} \leq 2^n a_{2n}^2$. That $p_n \leq a_n$ was proven in Section 1.1.1, and that $a_n \leq f_n^{\mathbf{B_2^1}}$ is proven in Section 2.1.

Theorem 1.11 *For all $n \in \mathbb{N}$, we have $p_n \leq a_n \leq f_n^{\mathbf{B_2^1}} \leq 2^n a_{2n}^2$.*

Theorem 1.11 is used in the companion paper [14], where a more extensive analysis of alternation word digraphs leads to certain bounds on (a_n) and provides the answer to the first question above–$(f_n^{\mathbf{B_2^1}})$ is indeed sub-log-exponential–and limits $O(\log f_n^{\mathbf{B_2^1}})$ to a quite small range, as some interval of functions in $[n^2, n^3]$. The precise determination of $O(\log f_n^{\mathbf{B_2^1}})$ remains an important open problem.

2 Word problems for $\mathbf{B_2^1}$

In Sections 2.1 and 2.2, Theorem 1.8 is proven. In Section 2.3, alternation word digraphs for inverse semigroup words are defined, and a solution to the word problem for $\mathbf{B_2^1}$, as an inverse semigroup, is given in terms of alternation word digraphs for inverse semigroup words.

2.1 $Alt(u) \neq Alt(v)$ implies $u \not\approx_{\mathbf{B_2^1}} v$

Proposition 2.1 below links alternation word digraphs with the word problem for $\mathbf{B_2^1}$. Let $\mathbf{S}$ be a semigroup. An element $e \in S$ is said to be **idempotent** if $e^2 = e$; an element $s \in S$ is said to be **nil** if there exists a positive integer k such that $s^k = 0$. Note that

[5] In [15] the second author conjectured that a finite monoid $\mathbf{M}$ is sub-log-exponential if and only if it is in $\mathbf{EDA} \cap \mathbf{G_{nil}}$, monoids with nilpotent subgroups and whose idempotents generate a monoid all of whose regular elements are idempotent. ($a \in M$ is **regular** if there exists an element $b \in M$ such that $aba = a$ and $bab = b$; all idempotent are regular.)

$\{0, 1, aa', a'a\}$ is the subset of idempotents of $\mathbf{B_2^1}$ and that a and a' are both nil. For the remainder of the paper, for words u and v, we write "$u \approx v$" rather than "$u \approx_{\mathbf{B_2^1}} v$".

Suppose that u, v are words and $x_i \in Var(u) \setminus Var(v)$. Let $e : Var(u) \cup Var(v) \to B_2^1$ be as follows: $e(x_i) = 0$ and for all $x_j \in Var(u) \cup Var(v) - \{x_i\}$, let $e(x_j) = 1$. Then $e(u) = 0$ but $e(v) = 1$; therefore, $u \not\approx v$. Unless otherwise stated, we will assume that $Var(u) = Var(v) = \{x_1, \ldots, x_n\}$. The next proposition led to the definition of alternation word digraphs.

Proposition 2.1 *Let u, v be words with $Var(u) = Var(v)$. Then $Alt(u) \neq Alt(v)$ implies $u \not\approx v$.*

Proof. Suppose that U and V are disjoint proper non-empty subsets of $Var(u) = Var(v)$, that $U \to V \in E(Alt(u))$, and that $U \to V \notin E(Alt(v))$. Consider the evaluation $e : Var(u) \cup Var(v) \to \{a, a', 1\} \subset B_2^1$ such that $e(x_i) = a$ if $x_i \in U$, $e(x_i) = a'$ if $x_i \in V$, and $e(x_i) = 1$ if $x_i \notin U \cup V$. Because instances of U and V alternate in u and the left-most variable of $u_{U \cup V}$ is in U, it follows that for some positive integer k, we have either $e(u) = (aa')^k$ or $e(u) = (aa')^k a$ (depending on whether the right-most variable in $u_{U\cup V}$ is in U or is in V).

By assumption, $U \to V \notin E(Alt(v))$. If $V \to U \in E(Alt(v))$, then with the evaluation e above, we have for some positive integer k that $e(v) = (a'a)^k$ or $e(v) = (a'a)^k a'$. Observe that $aa'a = a$ and $a'aa' = a'$; thus, $\{aa', aa'a\} \cap \{a'a, a'aa'\} = \emptyset$. Thus $e(u) \neq e(v)$ and $u \not\approx v$ for this case. If neither $U \to V$ nor $V \to U$ is in $E(Alt(v))$, then U and V do not alternate in v, and there are consecutive occurrences of U-variables or consecutive occurrences of V-variables in $v_{U\cup V}$. In particular, with the evaluation e as above, that $a^2 = 0 = (a')^2$ implies that $e(v) = 0$. Now $0 \notin \{a, a', aa', a'a\}$ implies that $e(u) \neq e(v)$, completing the proof. □

Corollary 2.2 *For all $n \in \mathbb{N}$, we have $a_n \leq f_n^{\mathbf{B_2^1}}$.*

Example 2.1 *In general, even $Alt(u) = Alt(v)$ and $Alt(u^r) = Alt(v^r)$ do not imply that $u \approx_{\mathbf{B_2^1}} v$. Consider $w = x_1x_2x_3x_4x_5x_4x_5x_3x_1x_2$ and $v = wx_1x_3x_2x_4x_5$. As can be verified, $E(Alt(w)) = \{1 \to 2,\ 4 \to 5,\ 14 \to 25\} = E(Alt(v))$ and $E(Alt(w^r)) = \{2 \to 1,\ 5 \to 4,\ 25 \to 14\} = E(Alt(v^r))$. Let $e : Var(u) = Var(v) \to B_2^1$ be defined as follows: $e(x_1) = e(x_4) = a,\ \ e(x_2) = e(x_5) = a'$, and $e(x_3) = aa'$. Now $e(v) = 0$ but $e(w) = aa' \neq 0$.*

2.2 Completion of proof of Theorem 1.8

We begin the proof by considering evaluations of words into the set $\{1, a, a'\} \subset B_2^1$.

Definition 2.3 *Let u and v be words.*

1. *Let $N = \{1, a, a'\} \subseteq B_2^1$.*
2. *If for every evaluation e with range in N we have $e(u) = e(v)$, then u is* **N-equivalent** *to v, denoted $u \approx_N v$.*

A quick reading of the proof of Proposition 2.1 reveals that for words u and v such that $Var(u) = Var(v)$, we have if $\mathit{Alt}(u) \neq \mathit{Alt}(v)$ or $\mathit{Alt}(u^r) \neq \mathit{Alt}(v^r)$ then $u \not\approx_N v$.

Suppose $x_i \in V_1(u) \setminus V_1(v)$. Then for the evaluation $e : Var(u) \to \{1, a, a'\}$ that sends x_i to $e(x_i) = a$ and the remaining variables in $Var(u)$ to 1, we have $e(u) = a$ and $e(v) = 1$. Thus $V_1(u) \neq V_1(v)$ implies $u \not\approx_N v$. We have proven one direction of the following proposition.

Proposition 2.4 *Let u, v be words with $Var(u) = \{x_1, \ldots, x_n\} = Var(v)$. Then $u \approx_N v$ if and only if*

1. $\mathit{Alt}(u) = \mathit{Alt}(v)$*;*
2. $\mathit{Alt}(u^r) = \mathit{Alt}(v^r)$*; and*
3. $V_1(u) = V_1(v)$*.*

Proof. Let u, v be words with $Var(u) = \{x_1, \ldots, x_n\} = Var(v)$. To prove the proposition, we need only prove that the three conditions above guarantee that $u \approx_N v$. Let $e : Var(u) \to N$ be an evaluation with range in N. If $e(Var(u)) = \{1\}$, then $e(u) = 1 = e(v)$. So we assume $e(Var(u)) \cap \{a, a'\} \neq \emptyset$.

Suppose there exists $x_i \in Var(u)$ such that $e(x_i) \in \{a, a'\}$ and for all $x_j \in Var(u) \setminus \{x_i\}$, we have $e(x_j) = 1$. If $x_i \in V_1(u) = V_1(v)$, we have $e(u) = e(x_i) = e(v)$. If $x_i \notin V_1(u) = V_1(v)$, we have $e(u) = 0 = e(v)$.

Assume at least two variables are contained in $e^{-1}(\{a, a'\})$. With this assumption, $e(Var(u)) \subseteq \{1, a\}$ or $e(Var(u)) \subseteq \{1, a'\}$ implies $e(u) = 0 = e(v)$. So assume $\{a, a'\} \subseteq e(Var(u))$. In that case, with $U = e^{-1}(a)$ and $V = e^{-1}(a')$ (thus $x_i \notin U \cup V$ implies $e(x_i) = 1$), we have one of the following:

- Neither $U \to V$ nor $V \to U$ is in $\mathit{Alt}(u) = \mathit{Alt}(v)$. Then U and V do not alternate in either u or v and $e(u) = 0 = e(v)$; or
- $U \to V \in \mathit{Alt}(u) = \mathit{Alt}(v)$ or $V \to U \in \mathit{Alt}(u) = \mathit{Alt}(v)$. Without loss of generality, assume $U \to V \in \mathit{Alt}(u) = \mathit{Alt}(v)$. Thus, U and V alternate in u and alternate in v, from which it follows that U and V alternate in u^r and alternate in v^r. Hence one of $U \to V$ or $V \to U$ is in $\mathit{Alt}(u^r) = \mathit{Alt}(v^r)$. We have $U \to V \in \mathit{Alt}(u^r) = \mathit{Alt}(v^r)$ implies $e(u) = aa'a = a = e(v)$, and $V \to U \in \mathit{Alt}(u^r) = \mathit{Alt}(v^r)$ implies $e(u) = aa' = e(v)$.

For all cases, $e(u) = e(v)$. Since e was an arbitrary evaluation with range contained in N, we have $u \approx_N v$. $\Box$

We complete the proof of Theorem 1.8.

Let u, v be words. For the remainder of the proof, we assume

- $Var(u) = Var(v)$: otherwise, there exists an evaluation $e : Var(v) \cup Var(u) \to B_2^1$ such that $\{e(u), e(v)\} = \{0, 1\}$.

- $V_1(u) = V_1(v)$: otherwise, as the first paragraph of the proof of Proposition 2.4 shows, there exists an evaluation $e : Var(u) \cup Var(v) \to B_2^1$ such that $\{e(u), e(v)\} = \{0, a\}$.
- If $e : Var(u) = Var(v) \to B_2^1$ is an evaluation, then $0 \notin e(Var(u))$: otherwise, $e(u) = e(v) = 0$, which, if that is the case, is of no help in showing $u \not\approx v$.

Claim 1 *For words u and v, we have $u \approx v$ if and only if $\overline{u} \approx \overline{v}$.*

Suppose $u \approx v$. Let $\overline{e} : Var(\overline{u}) = Var(\overline{v}) \to B_2^1$ be an evaluation. Define $e : Var(u) = Var(v) \to B_2^1$ as follows: for $x_i \in Var(u)$, let $e(x_i) = \overline{e}(x_i)\overline{e}(y_i)$. Note that $e(u) = \overline{e}(\overline{u})$ and $e(v) = \overline{e}(\overline{v})$. Now $u \approx v$ implies $e(u) = e(v)$, which in turn implies $\overline{e}(\overline{u}) = \overline{e}(\overline{v})$. Thus, $\overline{u} \approx \overline{v}$.

Conversely, assume $\overline{u} \approx \overline{v}$. Let $e : Var(u) = Var(v) \to B_2^1$ be an evaluation and define $\overline{e} : Var(\overline{u}) \to B_2^1$ as follows: let $\overline{e}(x_i) = e(x_i)$ and let $\overline{e}(y_i) = 1$. Of course, $\overline{e}(\overline{u}) = e(u)$ and $\overline{e}(\overline{v}) = e(v)$. This completes the proof of the claim.

By Claim 1 we have $u \approx v$ implies $\overline{u} \approx \overline{v}$, which in turn implies $\overline{u} \approx_N \overline{v}$, and which by Proposition 2.4 gives us that $Alt(\overline{u}) = Alt(\overline{v})$ and $Alt(\overline{u^r}) = Alt(\overline{v^r})$.

For the converse, assume that $Alt(\overline{u}) = Alt(\overline{v})$ and $Alt(\overline{u^r}) = Alt(\overline{v^r})$. By Proposition 2.4 we have $\overline{u} \approx_N \overline{v}$. Let $e : Var(u) \to B_2^1$ be an evaluation. For each $e(x_i) \notin \{1, a, a'\}$, there exists a uniquely determined $c_i, d_i \in \{a, a'\}$ such that $c_i d_i = e(x_i)$. Construct an evaluation $\overline{e} : Var(\overline{u}) \to B_2^1$, as follows: if $e(x_i) \notin \{0, 1, a, a'\}$, let $\overline{e}(x_i) = c_i$ and $\overline{e}(y_i) = d_i$, where c_i, d_i are uniquely determined; if $e(x_i) \in \{1, a, a'\}$, let $\overline{e}(x_i) = e(x_i)$ and let $\overline{e}(y_i) = 1$. Observe that $\overline{e}$ is an evaluation with range in N. Also, $V_1(u) = V_1(v)$ clearly implies $V_1(\overline{u}) = V_1(\overline{v})$. By Proposition 2.4 we have $\overline{u} \approx_N \overline{v}$, from which it follows that $\overline{e}(u) = \overline{e}(v)$. By construction, $e(u) = \overline{e}(u)$ and $e(v) = \overline{e}(v)$. Thus $e(u) = e(v)$. It follows that $u \approx v$. This completes the proof of the theorem. □

2.3 Word problem for the inverse semigroup $\mathbf{B_2^1}$

A semigroup $\mathbf{S}$ equipped with a unary operation $^{-1}$ such that $xx^{-1}x = x$, $x^{-1}xx^{-1} = x^{-1}$, and $xx^{-1}yy^{-1} = yy^{-1}xx^{-1}$ for all $x, y \in S$ is said to be an *inverse semigroup.* There is an extensive literature on word problems for inverse semigroups, and it turns out that a fairly obvious modification of alternation word digraphs for words over an alphabet $\{x_1, x_2, \ldots\} \cup \{x_1^{-1}, x_2^{-1}, \ldots\}$ leads to our modest contribution to this area, a solution of the word problem for $\mathbf{B_2^1}$, as an inverse semigroup, one that closely resembles Theorem 1.8. Section 2.3 will not be referred to in Sections 3 and 4.

1. $\mathbf{B_2}$ is an inverse semigroup with an unary operation $^{-1}$ defined as follows: $a^{-1} = a'$, $(a')^{-1} = a$, $(aa')^{-1} = a'a$, $(a'a)^{-1} = aa'$, $0^{-1} = 0$.
2. $\mathbf{B_2^1}$ is an inverse semigroup with $1^{-1} = 1$ (and other inverses as in $\mathbf{B_2}$ above).

A finite word w in the alphabet $\{x_1, x_2, \ldots\} \cup \{x_1^{-1}, x_2^{-1}, \ldots\}$ is said to be an *inverse semigroup word.* Let $\mathbf{I}$ be an inverse semigroup. Let $e : \{x_1, \ldots, x_n\} \to I$ be a mapping. The mapping e gives rise to an evaluation of w, denoted $e(w)$, via the convention $e(x_i^{-1}) = e(x_i)^{-1}$. Two inverse semigroup words u, v are $\mathbf{I}$-equivalent (denoted $u \approx_{\mathbf{I}} v$) if for every evaluation $e : Var(u) \cup Var(v) \to I$ we have $e(u) = e(v)$. The word problem for $\mathbf{I}$ is as follows: given two words u, v in the alphabet $\{x_1, x_2, \ldots\} \cup \{x_1^{-1}, x_2^{-1}, \ldots\}$, is it true that $u \approx_{\mathbf{I}} Iv$?

- In [13] the author presents a solution to the word problem for the inverse semigroup $\mathbf{B_2}$.
- Independently, the authors of [10] provide a quite different solution to the word problem for the inverse semigroup $\mathbf{B_2}$. From both [13], [10], it is clear that the associated computational complexity problem, the term-equivalence problem for the inverse semigroup $\mathbf{B_2}$, is in P.
- As mentioned, the term-equivalence problem for the semigroup $\mathbf{B_2^1}$ is co-NP-complete [14], [9]. The term-equivalence problem for the semigroup $\mathbf{B_2^1}$ is a sub-problem of the term-equivalence problem for the inverse semigroup $\mathbf{B_2^1}$; thus, this last problem is also co-NP-complete.

We define a variation of the alternation word digraph, $Alt_{inv}(w)$, as follows: For U, V non-empty disjoint subsets of $Var(w)$, let $U \to V \in Alt_{inv}(w)$ if $U \to V \in Alt(w)$, and for each $x_i \in U \cup V$, we have x_i, x_i^{-1} are not both contained in U nor are both contained in V.

Let w be an inverse semigroup word. Assume at least one of x_i, x_i^{-1} occurs in w. Using the inverse semigroup identities $x_i x_i^{-1} x_i \approx_I x_i$ and $x_i^{-1} x_i x_i^{-1} \approx_I x_i^{-1}$, we can replace the left-most instance of x_i (if x_i occurs in w) with $x_i x_i^{-1} x_i x_i^{-1} x_i$, or if x_i does not occur in w, we can replace the left-most instance of x_i^{-1} with $x_i^{-1} x_i x_i^{-1} x_i x_i^{-1}$. Let $\mathbf{w}$ be the word that results from the above substitution. Of course $\mathbf{w} \approx_{\mathbf{I}} w$ and $V_1(\mathbf{w}) = \emptyset$. For w, a finite word in $\{x_1, x_2, \ldots\} \cup \{x_1^{-1}, x_2^{-1}, \ldots\}$, we define $\overline{w}$ as follows: each occurrence of x_i (an "ordinary variable") is replaced by $x_i y_i$, and each occurrence of x_i^{-1} is replaced by $y_i^{-1} x_i^{-1}$.

The proof of Theorem 2.5 is very similar to that of Theorem 1.8, modified in the appropriate places to take into account the treatment of the inverse operation in Alt_{inv} graphs.

Theorem 2.5 *Let u, v be finite words in the alphabet $\{x_1, x_2, \ldots\} \cup \{x_1^{-1}, x_2^{-1}, \ldots\}$. Then u is equivalent to v in the inverse semigroup $\mathbf{B_2^1}$ if and only if*

1. $Alt_{inv}(\overline{\mathbf{u}}) = Alt_{inv}(\overline{\mathbf{v}})$*; and*
2. $Alt_{inv}(\overline{\mathbf{u}^r}) = Alt_{inv}(\overline{\mathbf{v}^r})$.

3 Proof of Theorem 1.10: complexity proofs

In this section we prove Theorem 1.10. As mentioned, the hardness results in Theorem 1.10 depend on algebraic computational complexity results from [14] and [9]. We begin by proving Theorem 1.10.1.

Proof of Theorem 1.10.1. Observe that if w is a word and U and V are vertices of $Alt(w)$, then determining whether $U \to V \in E(Alt(w))$ obviously can be checked in linear time (with respect to $|w|$) by simply scanning w from left to right and recording whether the most recent variable from $U \cup V$ is in U or in V. Let k be a fixed positive integer and u, v words such that $Var(u) = Var(v)$, with $|Var(u)| = n$. For each disjoint non-empty pair of subsets U and V of $Var(u)$ such that $|U|, |V| \leq k$, test whether $U \to V$ is in $E(Alt(u))$ and then whether it is in $E(Alt(v))$. So, to determine if $Alt_{\leq k}(u) = Alt_{\leq k}(v)$, it suffices to perform no more than $(\binom{n}{k} + \binom{n}{k-1} + \cdots + \binom{n}{1})^2$ such checks. Each such check requires $O(|u| + |v|)$ time. Because $n < |u| + |v|$, it follows that an answer to the question for a given instance $\{u, v\}$ can be provided in $c(|u| + |v|)^{2k}$ time, where c is a (fixed) positive integer. □

As a corollary of Theorem 1.8 and [14, Theorem 1.2], we shall prove that SUPPORT and ALT-EQ are both co-NP-complete. We provide a statement of [14, Theorem 1.2]. (We have substituted "word" for "term" in the statement of [14, Theorem 1.2] and, following the convention used here, variables are contained in the $\{x_1, x_2, \ldots\}$.)

Theorem 3.1 *[14, Theorem 1.2] Let $\mathcal{U}$ be the sub-problem of the term equivalence problem for $\mathbf{B_2^1}$ involving only instances of the form $\{qx_{n+1}x_i, qx_{n+1}x_i^2\}$, where q is a word such that $Var(q) = \{x_1, \ldots, x_n\}$ and $i \leq n$. Then $\mathcal{U}$ is co-NP-complete. In particular TERM-EQ($\mathbf{B_2^1}$) is co-NP-complete.*

Proof of Theorem 1.10.2 and 10.3. The first part of the following claim was noted in the first paragraph of page 325, [14]. Let w be a word $f : Var(w) \to \{1, a, a'\}$, an N-evaluation of w. Suppose that $f(w) \neq 0$. Thus $0 \notin f(Var(w))$. By substituting $e(x_i)$ for x_i for all $x_i \in Var(w)$, the result is a word (possibly the empty word) in the alphabet $\{a, a'\}$, which we denote by w_e.

Claim 2 *Let w be a word and $e : Var(w) \to B_2^1$ be an evaluation. Let $\underline{e} : Var(w) \to \{a, a', 1\}$ be the N-evaluation defined as follows: if $x_i \in Var(w)$ and $e(x_i) \in \{aa', a'a\}$, let $\underline{e}(x_i) = 1$; otherwise $\underline{e}(x_i) = e(x_i)$. Then the following hold:*

1. *$e(w) \neq 0$ implies $\underline{e}(w) \neq 0$; and*
2. *if $e(w) \neq 0$ and $w_{\underline{e}}$ has length greater than 1, then $e^{-1}(a) \to e^{-1}(a')$ or $e^{-1}(a') \to e^{-1}(a)$ is in $E(Alt(w))$.*

We prove the claim. If $e(Var(w)) = \{1\}$, the first part of the claim is obviously true. So assume $e(Var(w)) \neq \{1\}$. If aa' is a divisor of $e(w)$, then with a moment's thought it can be seen that replacing aa' with 1 results in a new word (in the alphabet $\{a, a'\}$) whose value in $\mathbf{B_2^1}$ is non-0. The first part of Claim 2 now follows. For the second part of the claim, suppose that $e(w) \neq 0$ and that $w_{\underline{e}}$ has length greater than 1. Then both a and a' must appear in $w_{\underline{e}}$, from which it follows that $e^{-1}(\{a, a'\}) = \underline{e}^{-1}(\{a, a'\})$ has more than one variable. Because $\underline{e}$ is an N-evaluation, it follows that both $\underline{e}^{-1}(a)$ and $\underline{e}^{-1}(a')$ are non-empty. Now $\underline{e}(w) \neq 0$ implies that $\underline{e}^{-1}(a)$ and $\underline{e}^{-1}(a')$ alternate. The second part of the claim follows.

Claim 3 *Let q be a word with $Var(q) = \{x_1, \ldots, x_i, \ldots, x_n\}$ and let $1 \leq i \leq n$. The following are equivalent:*

1. $qx_{n+1}x_i \approx qx_{n+1}x_i^2$
2. $Alt(qx_{n+1}x_i) = Alt(qx_{n+1}x_i^2)$
3. *x_i is not contained in the support of any edge of $Alt(qx_{n+1}x_i)$.*

Claim 3, in conjunction with Theorem 3.1, suffices to prove both Theorem 1.10.3 and Theorem 1.10.4. Proposition 2.4 guarantees that the first statement implies the second statement. Next suppose $Alt(qx_{n+1}x_i) = Alt(qx_{n+1}x_i^2)$. Because x_i^2 is a factor of $qx_{n+1}x_i^2$, we have x_i is not contained in the support of any edge of $Alt(qx_{n+1}x_i) = Alt(qx_{n+1}x_i^2)$. Lastly, suppose x_i is not contained in the support of any edge of $Alt(qx_{n+1}x_i)$. Let $e : Var(qx_{n+1}x_i) \rightarrow B_2^1$ be an evaluation. If $e(x_i) \in \{a, a'\}$, then because x_i occurs more than once in $qx_{n+1}x_i$, by Claim 2.2, if $e(qx_{n+1}x_i) \neq 0$, then x_i is contained in the support of an edge, which would be a contradiction. Thus $e(qx_{n+1}x_i) \neq 0$ implies $e(x_i) \in \{1, aa', a'a\}$, from which it follows that $e(qx_{n+1}x_i) \neq 0$ implies $e(qx_{n+1}x_i^2) = e(qx_{n+1}x_i)$. Obviously $e(qx_{n+1}x_i) = 0$ implies $e(qx_{n+1}x_i^2) = 0 = e(qx_{n+1}x_i)$. We have shown that $Alt(qx_{n+1}x_i) = Alt(qx_{n+1}x_i^2)$, thereby completing the proof of Theorem 1.10.3 and Theorem 1.10.4. □

3.1 Applications of a result of Klima: proofs of Theorem 1.10,4 and 5

Let $\mathbf{S}$ be a finite semigroup and let TERM-IDEM($\mathbf{S}$) be the problem which has an instance a word w, with size $|w|$, and which asks, "Is $w \approx_{\mathbf{S}} w^2$?". As mentioned, O. Klima independently proved the co-NP-completeness result for TERM-EQ($\mathbf{B_2^1}$) [9]. He did so by showing the co-NP-completeness of its sub-problem TERM-IDEM($\mathbf{S}$).

Theorem 3.2 ([9], page 5) *TERM-IDEM($\mathbf{B_2^1}$) is co-NP-complete.*

Proof of Theorem 1.10.4 We need a lemma that shows that TERM-IDEM($\mathbf{B_2^1}$) and E(Alt)= $\emptyset$ are very closely related.

Lemma 3.3 *If w is a word such that $Var(w) = \{x_1, \ldots, x_n\}$ and $V_1(w) = \emptyset$, then $Alt(w) = \emptyset$ if and only if $w \approx x_1^2 \ldots x_n^2$.*

Proof. Assume w is a word $Var(w) = \{x_1, \ldots, x_n\}$ and that $V_1(w) = \emptyset$. If $w \approx x_1^2 \ldots x_n^2$, then $Alt(w) = Alt(x_1^2 \ldots x_n^2)$, the latter graph having no edges since for each $x_i \in Var(x_1^2 \ldots x_n^2)$, we have x_i^2 divides $x_1^2 \ldots x_n^2$. Thus, $Alt(w) = \emptyset$.

Suppose $E(Alt(w)) = \emptyset$ and let $e : Var(w) \rightarrow B_2^1$ be an evaluation satisfying $e(w) \neq 0$. Let $\underline{e} : Var(w) \rightarrow \{1, a, a'\}$ be as in Observation 2. As observed there, we have $\underline{e}(w) \neq 0$. Because $V_1(w) = \emptyset$ and $\underline{e}(w) \neq 0$, it follows that $w_{\underline{e}}$ has length greater than 1. By the second part of Claim 2, we have $\underline{e}^{-1}(a) \neq \emptyset$ and $\underline{e}^{-1} \neq \emptyset$, from which it follows that $\underline{e}^{-1}(\{a, a'\})$ is the support of an edge of $Alt(w)$, contradicting that $Alt(w) = \emptyset$. Thus

$x_i \in Var(w)$ implies that $e(x_i) \in \{aa', a'a, 1\}$. Given that $(aa')(a'a) = 0 = (a'a)(aa')$, we have that $e(Var(w)) \setminus \{1\}$ consists of a single non-0 idempotent c and that $e(w) = c$. But then $e(w) = c = e(x_1^2 \dots x_n^2)$. Now suppose $e(w) = 0$. Then $e(Var(w)) \not\subseteq \{1, c\}$ where c is some non-0, non-1 idempotent. Thus $e(x_1^2 \dots x_n^2) = 0 = e(w)$. We have proven that $w \approx x_1^2 \dots x_n^2$. □

We provide a lemma that characterizes idempotent words.

Lemma 3.4 *Let w be a word. Then the following are equivalent:*

1. $w \approx w^2$
2. $V_1(w) = \emptyset$ *and* $U \to V \in Alt(\overline{w})$ *if and only if* $V \to U \in Alt(\overline{w^r})$
3. $V_1(w) = \emptyset$ *and* $Alt(\overline{w}\overline{w^r}) = \emptyset$

Proof. Suppose that $w \approx w^2$. Observe that $V_1(w) = \emptyset$. So $V_1(w) = V_1(w^2)$. Now by Theorem 1.8, we have $Alt(\overline{w}) = Alt(\overline{w^2})$ and $Alt(\overline{w^r}) = Alt(\overline{(w^r)^2})$. It is not difficult to verify that $Alt(\overline{w}) = Alt(\overline{w^2})$ implies $U \to V \in Alt(\overline{w})$ if and only if $V \to U \in Alt(\overline{w^r})$. Thus the first statement of this lemma implies the second statement of this lemma. Note that Theorem 1.8 implies that the second statement implies the first.

Suppose the second statement holds. For contradiction assume that $U \to V \in Alt(\overline{w}\overline{w^r})$. Because $Var(\overline{w}) = Var(\overline{w^r})$, we have $U \to V \in Alt(\overline{w}\overline{w^r})$ implies that $U \to V \in Alt(\overline{w})$, which by the second statement implies that $V \to U \in Alt(\overline{w^r})$. But then U and V do not alternate in $\overline{w}\overline{w^r}$, contradicting that $U \to V \in Alt(\overline{w}\overline{w^r})$.

Suppose the third statement holds and $U \to V \in E(Alt(\overline{w}))$. Then $U \to V \notin E(Alt(\overline{w}\overline{w^r}))$ implies $U \to V \notin E(Alt(\overline{w^r}))$, which in turn implies that $V \to U \in E(Alt(\overline{w^r}))$. As remarked, the second statement implies the first; thus, the third statement implies the first. □

We complete the proof of Theorem 1.10.4. Let $\{w\}$ be an instance of TERM-IDEM($\mathbf{B_2^1}$). We map $\{w\}$, with $Var(w) \subseteq \{x_1, \dots, x_n\}$, to an instance of E(ALT)= $\emptyset$ as follows: if $V_1(w) \neq \emptyset$, then map $\{w\}$ to $\{wx_{n+1}\}$; otherwise, map $\{w\}$ to $\{\overline{w}\overline{w^r}\}$. Determining whether $V_1(w) = \emptyset$ can be done in polynomial time; thus, the mapping above is polynomial with respect to size.

Note that $Alt_1(w) \neq \emptyset$ implies $w \not\approx w^2$ and that $Alt(wx_{n+1}) \neq \emptyset$. If $V_1(w) = \emptyset$, then by Lemma 3.4, we have $w \approx w^2$ if and only if $Alt(\overline{w}\overline{w^r}) = \emptyset$. This completes the proof.□

We provide a second proof of the co-NP-completeness of ALT-EQ.

Corollary 3.5 *ALT-EQ is co-NP-complete.*

Proof. That E(ALT)= $\emptyset$ is co-NP-complete implies that the sub-problem of ALT-EQ consisting of instances of the form $\{w, x_1^2 \dots x_n^2\}$ is co-NP-complete. □

Proof of Theorem 1.10.5 Let $\{w\}$ be an instance of TERM-IDEM($\mathbf{B_2^1}$). We assume that there exists $n \in \mathbb{N}$ such that $Var(w) = \{x_1, \dots, x_n\}$, an assumption that can easily be verified to have no effect on hardness.

We map $\{w\}$, with $Var(w) = \{x_1, \ldots, x_n\}$, to an instance of FREE–0 as follows: if $V_1(w) \neq \emptyset$, map $\{w\}$ to $\{(w, n)\}$; if $V_1(w) = \emptyset$, map $\{w\}$ to $(\overline{w}\overline{w^r}, n)$. This mapping is polynomial in size.

If $V_1(w) \neq \emptyset$, then as mentioned $w \not\approx w^2$. Obviously, $V_1(w) \neq \emptyset$ implies $w \not\approx x_1^2 \ldots x_n^2$, for any n. If $V_1(w) = \emptyset$, then by Lemma 3.4, we have $w \approx w^2$ if and only if $Alt(\overline{w}\overline{w^r}) = \emptyset$. Because $V_1(\overline{w}\overline{w^r}) = \emptyset$ by Lemma 3.3 we have that $\overline{w}\overline{w^r} \approx x_1^2 \ldots x_n^2$. This completes the proof.□

4 Conclusion

We finish with questions that may be of interest for further research.

Definition 4.1

1. For a positive integer k, a word w is *k-letter-uniform* if each letter in w appears exactly k times.
2. If w is k-uniform for some k, then w is said to be *letter-uniform*. Let $UniAlt$ be the set of all alternation word digraphs of letter-uniform words.
3. A word $w = w_1 \ldots w_j$ is a *permutation-product* if for $1 \leq a \leq b \leq j$, we have $Var(w_a) = Var(w_b)$ and w_a is 1-letter-uniform. Let P^*Alt be the set of all alternation word digraphs of permutation products.
4. For a word w, let **alternation word graph** of w, denoted $alt(w)$, be the undirected graph version of $Alt(w)$. Let alt_1 be $\{alt_1(w) : w\ is\ a\ finite\ word\}$.

Problem 1 *Is the restriction of either ALT-EQ or ALT $= \emptyset$ to uniform words or to permutation products still co-NP-complete?*

The alt_1 graphs were studied in [8], where it is shown that every alt_1 graph is locally comparable; that is, for x_i a vertex of a $alt_1(w)$, the induced subgraph on $Nbd(x_1)$, the set of neighbors of x_1 in $alt_1(w)$, is the comparability graph of a poset. The following is a slight reformuation of Problem 1, [8].

Problem 2 *True or false? If G is a finite locally comparable graph with vertices V, then there exists a word w, with $Var(w) = V$ such that $alt_1(w) = G$.*

Let C be a type of word graphs (or digraphs) and let $\mathcal{C}$ be the set of words associated with C. For example, C might be P^*Alt graphs with $\mathcal{C}$ the permutation products, or C might be the set of all alt_1 graphs, in which case, $\mathcal{C}$ is then the set of all words. For a word $s \in \mathcal{C}$, let $G_C(s)$ denote the graph in C associated with s.

Definition 4.2 *1. For a fixed word graph type, and for $w \in \mathcal{C}$, let $l^C(w) = \min\{|u| : u \in \mathcal{C}, G_C(u) = G_C(w)\}$, the C–length of w.*

2. *For a fixed word graph type, and for $w \in \mathcal{C}$, let $l_n^C = \max\{l^C(w) : w \in \mathcal{C}$ and $Var(w) \subseteq \{x_1, \ldots, x_n\}\}$.*

It is not difficult to prove that $2^{n-1} \in O(l_n^{Alt})$[6], but more difficult to show that $(l_n^{P^* Alt})$ is in $O(n^3)$, as in proven in [16].

Problem 3 1. *Find a polynomial $p(n)$ such that $(l_n^{alt_1}) \in O(p(n))$, if such a polynomial exists.*

2. *Find a polynomial $p(n)$ such that $(l_n^{UniAlt}) \in O(p(n))$, if such a polynomial exists.*

A monoid $\mathbf{M}$ is **aperiodic** if all its subgroups are trivial. It is not difficult to show that a finite monoid $\mathbf{M}$ is aperiodic if and only if there exists a positive integer k such that $x^{k+1} \approx_{\mathbf{M}} x^k$ and that $x^{k+1} \approx_{\mathbf{M}} x^k$ implies $x^k \approx_{\mathbf{M}} x^{2k}$. Thus, if $\mathbf{M}$ is a finite aperiodic monoid with commuting idempotents, then $x_1^k \ldots x_n^k$ is the zero of $F_n(\mathbf{M})$. For a finite aperiodic monoid with commuting idempotents $\mathbf{M}$, define the computational complexity problem FREE–0($\mathbf{M}$) as follows: an instance is $\{w, n\}$, where w is a word in the alphabet $\{x_1, \ldots, x_n\}$, with size $|w|$, and the question is, "Is $w \approx x_1^k \ldots x_n^k$?".

Conjecture 1 *The following conjecture is a variant of [Problem 3, page 321, [14]]: Let $\mathbf{M}$ be a finite aperiodic monoid with commuting idempotents. Then TERM-EQ($\mathbf{M}$) is co-NP-complete if and only if FREE–0($\mathbf{M}$) is co-NP-complete if and only if $\mathbf{B_2^1}$ is in the pseudovariety generated by $\mathbf{M}$.*

Note Though it has no bearing on this paper, it is important to point out that in [15], the usage of "subword" differs from its usage here: A subword in [15] has the same meaning as "divisor" in this paper; "subsequence" in [15] has the same meaning as "subword" in this paper. The usage here of "subword" is more standard.

References

[1] S. Burris and J. Lawrence, *The equivalence problem for finite rings*, Journal of Symbolic Computation **15** (1993), 67–71.

[2] S. Burris and J. Lawrence, *Results on the equivalence problem for finite groups*, Alg. Univ. **52**, no.4, (2004), 495–500.

[3] G. Higman, *The orders of relatively free groups*, Proc. Internat. Conf. Theory of Groups, Austral. Nat. Univ. Canberra (1965), 153–165.

[4] G. Horvath, J. Lawrence, L. Merai, and C. Szabo, *The complexity of the equivalence problem for non-solvable groups*, Bull. Lond. Math. Soc., **39**, (2007), 253–260.

[6] Let $Z_1 = x_1$ and for $n \geq 2$, let $Z_n = Z_{n-1} x_n Z_{n-1}$. The word Z_n is a Zimin word (on the sequence $x_1, x_2, \ldots, x_n$). It is not difficult to show that $(Z_n)_{\{x_2,\ldots,x_n\}}$ is a Zimin word on the sequence $x_2, \ldots, x_n$, and for $n \geq 2$ that $Alt(Z_n)$ has $n-1$ edges, $\{1 \to 2 \ldots n,\ 2 \to 3 \ldots n,\ 3 \to 4 \ldots n, \ldots, n-1 \to n\}$. It follows that $l^{Alt}(Z_n) \geq 2(l^{Alt}(Z_{n-1}))$.

[5] *64 Problems in Universal Algebra*, workshop notes from *A COURSE IN TAME CONGRUENCE THEORY*, Budapest, July 2–13, 2001, `http://www.math.u-szeged.hu/confer/algebra/2001/64problems.ps`

[6] K.A. Kearnes, *Congruence modular varieties with small free spectra.* Algebra Universalis 42 (1999), 165–181.

[7] A. Kisielewicz, *Complexity of identity checking for semigroups*, Internat. J. Algebra Comput., **14** (2004), 455–464.

[8] S. Kitaev and A. Pyatkin, *On representable graphs*, http://www.ru.is/kennarar/sergey/index_files/Papers/repgr.pdf, Automata, Languages and Combinatorics, to appear.

[9] O. Klima, *Complexity Issues of Checking Identities in Finite Monoids*, http://www.math.muni.cz/∼klima/Math/coNPidcheck.ps.

[10] S.W. Margolis, J.C. Meakin, and J. Stephen, *Free objects in certain varieties of inverse semigroups*, Canad. J. Math. **42** (6) (1990), 1084–1097.

[11] P.M. Neumann, *Some indecomposable varieties of groups*, Quart J. Math. Oxford, **14**, (1963), 46–58.

[12] P. Perkins, *Bases for equational theories of semigroups*, J. Algebra **11** (1969), 298–314.

[13] N.R. Reilly, *Free combinatorial strict inverse semigroups*, J. London Math. Soc. (2), **39**(1) (1989), 102–120.

[14] S. Seif, *The Perkins Semigroup has Co-NP-complete term-equivalence problem*, Int. J. Alg. Comp. (IJAC), **15** (2) (2005), 317–326.

[15] S. Seif, *Monoids with sub-log-exponential free spectra*, Journal of Pure and Applied Algebra, **212**, 5, (2008), 1162–1174.

[16] S. Seif, *Letter-uniform words and their graphs*, manuscript.

[17] S. Seif, C. Szabo, *Computational Complexity of Checking Identities in 0-Simple Semigroups and Matrix Semigroups over Finite Fields*, Semigroup Forum, **72** (2), (2006), 207–222.

[18] S. Seif and J. Wood, *Asymptotic growth of free spectra of band monoids*, Semigroup Forum **75**, no. 1, (2007), 77–94.

[19] C. Szabo, and V. Vertesi, *The complexity of the word-problem for finite matrix rings*, Proc. Amer. Math. Soc. **132** (2004), no. 12, 3689–3695.

[20] C. Szabo, C. and V. Vertesi, *The complexity of checking identities for finite matrix rings*, Alg.Univ. **51**, no. 4 (2004), 439–445.

[21] M. Volkov, *Checking Identities in a finite semigroup may be computationally hard*, Studia Logica, **78**, nos. 1-2, (2004), 349–356.