Upper Bounds for a Theory of Queues

Tatiana Rybina and Andrei Voronkov

University of Manchester
{rybina,voronkov}@cs.man.ac.uk

Abstract. We prove an upper bound result for the first-order theory of a structure **W** of queues, i.e. words with two relations: addition of a letter on the left and on the right of a word. Using complexity-tailored Ehrenfeucht games we show that the witnesses for quantified variables in this theory can be bound by words of an exponential length. This result, together with a lower bound result for the first-order theory of two successors [6], proves that the first-order theory of **W** is complete in LATIME($2^{O(n)}$): the class of problems solvable by alternating Turing machines running in exponential time but only with a linear number of alternations.

1 Introduction

Theories of words are fundamental to computer science. Decision procedures for various theories of words are used in many areas of computing, for example in verification. Closely related to words are *queues* which can be regarded as words with two operations: deleting a letter on the left and adding a letter on the right. In this paper we prove upper bounds on the complexity of the first-order theory of queues. The upper bound is tight, i.e., it coincides with the respective lower bound up to a constant factor.

Denote by $\{0,1\}^*$ the set of all words over the finite alphabet $\{0,1\}$, by $ln(w)$ the length of the word w and by λ the empty word. We call the elements of $\{0,1\}^*$ simply *words*. By "$\cdot$" we denote concatenation of words. Define the following four relations on words:

$$l_0(a,b) \leftrightarrow b = 0 \cdot a; \qquad l_1(a,b) \leftrightarrow b = 1 \cdot a;$$
$$r_0(a,b) \leftrightarrow b = a \cdot 0; \qquad r_1(a,b) \leftrightarrow b = a \cdot 1.$$

The first-order structure $\mathbf{W} = \langle \{0,1\}^*, r_0, r_1, l_0, l_1 \rangle$ is called the *queue structure*. The *first-order theory of queues* is the first-order theory of **W**.

Let us formulate the main result of this paper. See [11,10] for the precise definition of the *complexity class* *LATIME*($2^{O(n)}$): it is the class of problems solvable by alternating Turing machines running in time $2^{O(n)}$ but only with a linear number of alternations. Of course, for this class polynomial-time or LOGSPACE reductions are too coarse, this class is closed with respect to LOGLIN-reductions [11], i.e., LOGSPACE reductions giving at most linear increase in length. The main result of this paper is the following.

J.C.M. Baeten et al. (Eds.): ICALP 2003, LNCS 2719, pp. 714–724, 2003.
© Springer-Verlag Berlin Heidelberg 2003

THEOREM 1 *The first-order theory of* **W** *is complete in LATIME*$(2^{O(n)})$ *with respect to LOGLIN-reductions.* ❑

This theorem will be proved using complexity-tailored Ehrenfeucht games. We will show that in the first-order theory of **W** in every sentence witnesses for quantified variables can be bound by words of the size exponential in the size of the sentence.

The decidability of the first-order theory of this structure follows from the decidability of the first-order theory of two successors with the predicates of equal length and prefix [9]. It also immediately follows from the fact that this structure is automatic [7,4].

A lower bound on the first-order theory of **W** can be derived from the lower bound on the first-order theory of two successors, i.e., of the structure $\langle \{0,1\}^*, r_0, r_1 \rangle$, proved in [11] based on [6] (a technique for proving lower bounds is also described in [5], some simple generalizations can be found in [12]). Expressive power of several theories of words, including the first-order theory of **W**, is discussed in [1].

For us the main motivation for these results was our case study of verification of a protocol with queues. Verification with queues was also extensively studied in [3,2]. In [8] we proved that first-order theories of some structures containing trees and queues are decidable. Our results were based on quantifier elimination and imply a non-elementary upper bound (a non-elementary lower bound also follows for the theory of trees [6]). However, if we consider a theory with queues only, it was clear that a non-elementary upper bound could be avoided. Indeed, the quantifier elimination arguments of [8] show that the main difference in expressive power between queues and stacks is periodicity constraints. However, these periodicity constraints, though they can express "deep" properties of queues (e.g., that all elements of a queue are 0's), still cannot distinguish queues which are indistinguishable by their "short" prefixes. Motivated by this observation we undertake a characterization of the exact complexity of the first-order theory of **W**.

In the proof of the upper bound for **W** we show, like [6], that all quantifiers in a formula can be replaced by quantifiers of an exponential size. However, our arguments are more technically involved. Moreover, some lemmas of [6] do not hold any more in this context.

2 Ehrenfeucht Games

$\mathbb{N}$ denotes the set of natural numbers. By $\bar{\mathbf{a}}_k$ we denote the sequence $a_1, \ldots, a_k$ of k elements, and similar for other letters instead of $\mathbf{a}$.

DEFINITION 2 (Norm) Let A be a structure. A *norm* on A, denoted $||\cdot||$, is a function from the domain of the structure A to $\mathbb{N}$. For an element a of A we write $||a||$ to denote the norm of a. ❑

The following definitions are similar to those of Ferrante and Rackoff [6].

Definition 3 (Ehrenfeucht Equivalence) Let $n, k \in \mathbb{N}$, A be a structure, and $\bar{\mathbf{a}}_k, \bar{\mathbf{b}}_k$ be sequences of elements of A. Then we write $\bar{\mathbf{a}}_k \underset{n,k}{\equiv\!\equiv} \bar{\mathbf{b}}_k$ if for all formulas $F(x_1, \ldots, x_k)$ of quantifier depth at most n, $\bar{\mathbf{a}}_k$ satisfies $F(x_1, \ldots, x_k)$ in A if and only if $\bar{\mathbf{b}}_k$ satisfies $F(x_1, \ldots, x_k)$ in A. (In particular $\bar{\mathbf{a}}_k \underset{0,k}{\equiv\!\equiv} \bar{\mathbf{b}}_k$ means that $\bar{\mathbf{a}}_k$ and $\bar{\mathbf{b}}_k$ satisfy the same quantifier-free formulas.) ❑

Definition 4 (Boundedness) Let A be a structure with a norm $||\cdot||$ on it and $\mathcal{H} : \mathbb{N}^3 \to \mathbb{N}$ be a function. We say that A is *$\mathcal{H}$-bounded* if for all natural numbers k, n, m, a sequence $\bar{\mathbf{a}}_k$ of elements of A, and formula $F(x_1, \ldots, x_{k+1})$ of quantifier depth $\leq n$ the following property holds. If for all $i \leq k$ we have $||a_i|| \leq m$ and $A \models \exists x_{k+1} F(\bar{\mathbf{a}}_k, x_{k+1})$, then there exists $a_{k+1} \in A$ such that $||a_{k+1}|| \leq \mathcal{H}(n, k, m)$ and $A \models F(\bar{\mathbf{a}}_k, a_{k+1})$. ❑

Theorem 5 (Ferrante and Rackoff [6]) *Let A be a structure and $\mathcal{H} : \mathbb{N}^3 \to \mathbb{N}$ be a function. Let $\mathcal{E}_{n,k}$ be relations such that for all natural numbers n, k, m and sequences of elements $\bar{\mathbf{a}}_k$, $\bar{\mathbf{b}}_k$ of A the following properties are true:*

1. *if $\mathcal{E}_{0,k}(\bar{\mathbf{a}}_k, \bar{\mathbf{b}}_k)$ then $\bar{\mathbf{a}}_k \underset{0,k}{\equiv\!\equiv} \bar{\mathbf{b}}_k$;*
2. *if $\mathcal{E}_{n+1,k}(\bar{\mathbf{a}}_k, \bar{\mathbf{b}}_k)$ and for all $i \leq k$ we have $||b_i|| \leq m$ then for all $a_{k+1} \in A$ there exists $b_{k+1} \in A$ such that $\mathcal{E}_{n,k+1}(\bar{\mathbf{a}}_{k+1}, \bar{\mathbf{b}}_{k+1})$ and $||b_{k+1}|| \leq \mathcal{H}(n, k, m)$.*

Then:

1. *$\mathcal{E}_{n,k}(\bar{\mathbf{a}}_k, \bar{\mathbf{b}}_k) \Rightarrow \bar{\mathbf{a}}_k \underset{n,k}{\equiv\!\equiv} \bar{\mathbf{b}}_k$ for all $n, k \in \mathbb{N}$,*
2. *the structure A is $\mathcal{H}$-bounded.* ❑

3 Main Argument

An Ehrenfeucht game decision procedure for $\mathbf{W}$ consists of defining a set of equivalence relations $\mathcal{E}_{n,k}$, which turn out to be refinements of the relations $\underset{n,k}{\equiv\!\equiv}$, defining a function $\mathcal{H}(n, k, m)$, and showing $\mathcal{H}$-boundedness of the structure $\mathbf{W}$. Since the structure is $\mathcal{H}$-bounded, then the witnesses for quantifiers in formulas can be restricted by elements of a fixed depth. If the number of elements of every norm is finite, then we obtain a decision procedure.

Let a, v_1, v_2 be words. By ${}_{v_1}[a]_{v_2}$ we denote the word w, if it exists, such that $a = v_1 \cdot w \cdot v_2$.

In the sequel we will extensively use partial functions. Let us make a notational convention about their use.

Convention 6 *Let e, e_1, e_2 be any expressions over words. We write $e \downarrow$ to denote that e exists. When we write $e_1 = e_2$, we mean that both e_1 and e_2 are defined and equal. If S is a set of words and we write $e \in S$, we mean that e is defined and e is a member of S.* ❑

DEFINITION 7 (ε-word, ε-length, ε-correction) Let $\varepsilon \in \mathbb{N}$. A number $\ell \in \mathbb{N}$ is said to be an *ε-length* if $\ell \leq \varepsilon$. We will normally use this terminology when we speak about lengths of words. A word is an *ε-word* if its length is an ε-length. An *ε-correction* is a partial function α such that for some ε-words v_1, v_2, w_1, w_2 and for all words a we have $\alpha(a) = w_2 \cdot {}_{w_1}[a]_{v_1} \cdot v_2$. An ε-correction α is called *trivial* if for some words v, w and all words a we have $\alpha(a) = w \cdot {}_{w}[a]_{v} \cdot v$. ❑

Let us note some useful properties of this definition.

LEMMA 8 *The following statements hold for ε-corrections.*

1. *If a is an ε_1-word and b is ε_2-word, then $a \cdot b$ is an $(\varepsilon_1 + \varepsilon_2)$-word.*
2. *If a is a ε_1-word and α is an ε_2-correction, then $\alpha(a)$ is an $(\varepsilon_1 + 2\varepsilon_2)$-word.*
3. *For every ε-correction α there exists an ε-correction* inverse *to α, denoted α^{-1}, such that for every word a we have*
   a) *if $\alpha(a) \downarrow$ then $\alpha^{-1}(\alpha(a)) = a$;*
   b) *if $\alpha(a) = b$ then $a = \alpha^{-1}(b)$ and $\alpha(\alpha^{-1}(b)) = b$;*
   c) *if $\alpha^{-1}(a) = b$ then $a = \alpha(b)$ and $\alpha^{-1}(\alpha(b)) = b$.*
4. *If α is an ε_1-correction, β is an ε_2-correction, and $\alpha(\beta(v))$ is defined for at least one word v, then their composition $\alpha\beta$ is an $(\varepsilon_1 + \varepsilon_2)$-correction.* ❑

In the sequel we will often use this lemma implicitly.

For every word a, denote $a^* = \{a^n \mid n \in \mathbb{N}\}$.

LEMMA 9 (see [8]) *Let a, b, c be words such that $a \cdot b = b \cdot c$. Then*

1. *if $a \neq c$ then there exist words a_1 and a_2 such that $a = a_1 \cdot a_2$, $c = a_2 \cdot a_1$ and $b \in \{a^n \cdot a_1 \mid n \in \mathbb{N}\}$;*
2. *if $a = c$ then there exists a word s such that $c \in s^*$ and $b \in s^*$.* ❑

LEMMA 10 *For every non-trivial ε-correction and word a, if $\alpha(a) = a$, then for some ε-word s and ε-correction γ we have $\gamma(a) \in s^*$.*

PROOF. By the definition of α there exist ε-words w_1, w_2, v_1, v_2 such that $\alpha(a) = w_2 \cdot {}_{w_1}[a]_{v_1} \cdot v_2$. On the other hand, we have $a = w_1 \cdot {}_{w_1}[a]_{v_1} \cdot v_1$. Thus $w_2 \cdot {}_{w_1}[a]_{v_1} \cdot v_2 = w_1 \cdot {}_{w_1}[a]_{v_1} \cdot v_1$. Since α is non-trivial, we have $w_1 \neq w_2$ and $v_1 \neq v_2$. The equality $\alpha(a) = a$ implies that either $ln(w_2) < ln(w_1),\ ln(v_2) > ln(v_1)$, or $ln(w_2) > ln(w_1),\ ln(v_2) < ln(v_1)$. Let us consider the case $ln(w_2) < ln(w_1),\ ln(v_2) > ln(v_1)$, the other case is similar. In this case there exist words b and c such that $w_1 = w_2 \cdot b$ and $v_2 = c \cdot v_1$. Since w_1, v_2 are ε-words, b, c must be ε-words too. We have $w_2 \cdot {}_{w_1}[a]_{v_1} \cdot c \cdot v_1 = w_2 \cdot b \cdot {}_{w_1}[a]_{v_1} \cdot v_1$, hence $b \cdot {}_{w_1}[a]_{v_1} = {}_{w_1}[a]_{v_1} \cdot c$. By Lemma 9 there exist words s_1 and s_2 such that $b = s_1 \cdot s_2,\ c = s_2 \cdot s_1$ and ${}_{w_1}[a]_{v_1} \in \{(s_1 \cdot s_2)^n \cdot s_1 \mid n \in \mathbb{N}\}$. Evidently, s_1, s_2 are ε-words. Define $s = b$ and define γ as follows: for all v we have

$$\gamma(v) \stackrel{\text{def}}{=} \lambda \cdot {}_{w_2}[v]_{v_1} \cdot s_2.$$

The property $\gamma(a) \in s^*$ is not hard to check. ❑

LEMMA 11 *Let b, c be ε-words, α, β be ε-corrections, and a be an arbitrary word.*

1. *If $\alpha(a) \in b^*$ then for all $w \in b^*$ such that $ln(w) \geq 2\varepsilon$ we have $\alpha^{-1}(w)\downarrow$.*
2. *If $ln(a) \geq 4\varepsilon$, $\alpha(a) \in b^*$, and $\beta(a) \in c^*$ then for all words $w \in b^*$ and $v \in c^*$ such that $ln(w), ln(v) \geq 4\varepsilon$ we have $\beta(\alpha^{-1}(w)) \in c^*$ and $\alpha(\beta^{-1}(v)) \in b^*$.* ❑

The proof is straightforward but tedious.

The following definition of *indistinguishability* is the main technical notion of this paper. Define the following function L of two integer arguments: $L(n,k) = 2^{3n+k}$.

DEFINITION 12 (Indistinguishability) Let $\bar{\mathbf{a}}_k$ and $\bar{\mathbf{b}}_k$ be sequences of words and n be a natural number. We say that $\bar{\mathbf{a}}_k$ and $\bar{\mathbf{b}}_k$ are $\mathcal{E}_{n,k}$-*indistinguishable*, denoted $\bar{\mathbf{a}}_k \ \mathcal{E}_{n,k} \ \bar{\mathbf{b}}_k$, if the following conditions hold for all $i, j \in \{1, \ldots, k\}$. Let $\varepsilon = L(n,k)$.

1. For every ε-correction α we have $\alpha(a_i) = a_j$ if and only if $\alpha(b_i) = b_j$.
2. If either a_i or b_i is a 4ε-word, then $a_i = b_i$.
3. For every ε-correction α and ε-word a, $\alpha(a_i) \in a^*$ if and only if $\alpha(b_i) \in a^*$.

Prefix (respectively suffix) of the length ℓ of a word a, if it exists, is denoted $\mathit{prefix}(\ell, a)$ (respectively $\mathit{suffix}(\ell, a)$).

LEMMA 13 *Let $\bar{\mathbf{a}}_k \mathcal{E}_{n,k} \bar{\mathbf{b}}_k$. Define $\varepsilon = L(n,k)$. Then for every i*

1. *either $a_i = b_i$, or $\mathit{prefix}(\varepsilon, a_i) = \mathit{prefix}(\varepsilon, b_i)$ and $\mathit{suffix}(\varepsilon, a_i) = \mathit{suffix}(\varepsilon, b_i)$;*
2. *for every ε-correction α, $\alpha(a_i)\downarrow$ if and only if $\alpha(b_i)\downarrow$.*

PROOF. The second clause evidently follows from the first one, so we will only prove the first clause.

If $ln(a_i) \leq 4\varepsilon$ then, by Clause 2 of Definition 12, $a_i = b_i$. Otherwise we have $ln(a_i) > 4\varepsilon$. Define an ε-correction α by

$$\alpha(v) \stackrel{\text{def}}{=} \mathit{prefix}(\varepsilon, a_i) \cdot {}_{\mathit{prefix}(\varepsilon,a_i)}[v]_{\mathit{suffix}(\varepsilon,a_i)} \cdot \mathit{suffix}(\varepsilon, a_i).$$

It is easy to see that $\alpha(a_i) = a_i$, hence, by Clause 1 of Definition 12, $\alpha(b_i) = b_i$. Then $\alpha(b_i)$ is defined, hence $\mathit{prefix}(\varepsilon, b_i) = \mathit{prefix}(\varepsilon, a_i)$ and $\mathit{suffix}(\varepsilon, b_i) = \mathit{suffix}(\varepsilon, a_i)$. ❑

By routine inspection of the definition of $\mathcal{E}_{n,k}$, we can also prove the following result.

COROLLARY 14 *$\mathcal{E}_{n,k}$ is an equivalence relation.* ❑

The following lemma is a key to proving that $\mathbf{W}$ is $\mathcal{H}$-bounded.

LEMMA 15 *Let k, n be natural numbers and $\bar{\mathbf{a}}_k$, $\bar{\mathbf{b}}_k$ be sequences of words such that $\bar{\mathbf{a}}_k \ \mathcal{E}_{n+1,k} \bar{\mathbf{b}}_k$. Then for every word a_{k+1} there exists a word b_{k+1} such that $\bar{\mathbf{a}}_{k+1} \ \mathcal{E}_{n,k+1} \ \bar{\mathbf{b}}_{k+1}$.*

PROOF. Let $\varepsilon = L(n, k+1)$. In the proof we will construct the word b_{k+1} and prove $\mathcal{E}_{n,k+1}$-indistinguishability of $\bar{\mathbf{a}}_{k+1}$ and $\bar{\mathbf{b}}_{k+1}$ using the hypothesis about $\mathcal{E}_{n+1,k}$-indistinguishability of $\bar{\mathbf{a}}_k$ and $\bar{\mathbf{b}}_k$. In this respect note that $L(n+1,k) = 4 \cdot L(n, k+1)$. Therefore, in the proof we will use hypothesis about 4ε-words and prove statements about ε-words.

Let us note that while verifying Clauses 1–3 of Definition 12 for $\bar{\mathbf{a}}_{k+1}$ and $\bar{\mathbf{b}}_{k+1}$ we have to consider only the case $i = k+1$ or $j = k+1$ for Clause 1 and the case $i = k+1$ for Clauses 2–3. Moreover, for Clause 1 the proofs for the case $i = k+1$ are similar to the proofs for the case $j = k+1$, so we will only consider the case $i = k+1$.

Our choice of b_{k+1} depends on the properties of a_{k+1}, so we proceed by cases.

Case 1: a_{k+1} is a 4ε-word. We choose $b_{k+1} = a_{k+1}$.

Let us prove Clauses 1–3 of Definition 12 for $\bar{\mathbf{a}}_{k+1}$ and $\bar{\mathbf{b}}_{k+1}$.

1. Suppose α is an ε-correction $\alpha(a_i) = a_{k+1}$.We have to prove $\alpha(b_i) = b_{k+1}$. We only verify the case $i \leq k$ since the case $i = k+1$ is trivial. We know that a_{k+1} is 4ε-word and $\alpha^{-1}(a_{k+1}) = a_i$. Then a_i is 6ε-word. By the hypothesis, if a_i is 16ε-word, then $a_i = b_i$. Therefore, $\alpha(b_i) = b_{k+1}$.
2. We have to prove that if a_{k+1} is a 4ε-word or b_{k+1} is a 4ε-word, then $a_{k+1} = b_{k+1}$. But we have $a_{k+1} = b_{k+1}$ by our construction.
3. By our choice $a_{k+1} = b_{k+1}$, therefore for every ε-correction α and ε-word a : $\alpha(a_{k+1}) \in a^*$ if and only if $\alpha(b_{k+1}) \in a^*$.

Case 2: a_{k+1} is not a 4ε-word but there exist $j \leq k$ and ε-correction β such that $\beta(a_j) = a_{k+1}$. By Lemma 13, $\beta(b_j)$ is defined. We choose $b_{k+1} = \beta(b_j)$. Let us show that our choice of b_{k+1} satisfies the definition of $\mathcal{E}_{n,k+1}$-indistinguishability.

1. Suppose that α is an ε-correction and $i \leq k+1$. We need to verify that $\alpha(a_i) = a_{k+1}$ if and only if $\alpha(b_i) = b_{k+1}$.
   To prove the "only if" direction, suppose $\alpha(a_i) = a_{k+1}$. Since $a_{k+1} = \beta(a_j)$, we have $\beta^{-1}(a_{k+1}) = a_j$, hence $\beta^{-1}(\alpha(a_i)) = a_j$. Consider two cases: $i \neq k+1$ and $i = k+1$.
   Suppose $i \neq k+1$. Since $\beta^{-1}\alpha$ is a 2ε-correction, by the hypothesis we have $\beta^{-1}(\alpha(b_i)) = b_j$. This implies $\alpha(b_i) = \beta(b_j) = b_{k+1}$.
   Now suppose that $i = k+1$, then $\alpha(a_{k+1}) = a_{k+1}$, that is $\alpha(\beta(a_j)) = \beta(a_j)$, hence $\beta^{-1}(\alpha(\beta(a_j))) = a_j$. By the hypothesis, since $\beta^{-1}\alpha\beta$ is a 3ε-correction, $\beta^{-1}(\alpha(\beta(b_j))) = b_j$, hence $\alpha(\beta(b_j)) = \beta(b_j)$. But $\beta(b_j) = b_{k+1}$, so $\alpha(b_{k+1}) = b_{k+1}$.
   The "if" direction is similar.
2. Since a_{k+1} is not a 4ε-word to verify Clause 2 we have to show that b_{k+1} is not a 4ε-word. By our choice of b_{k+1}, $\beta^{-1}(b_{k+1}) = b_j$. Suppose that b_{k+1} is a 4ε-word, then b_j is a 6ε-word, so by our hypothesis $a_j = b_j$. Therefore, $\beta(a_j) = \beta(b_j)$, that is $a_{k+1} = b_{k+1}$. But then a_{k+1} would be a 4ε-word. Contradiction.

3. To verify Clause 3 we only have to show that for every ε-word a and every ε-correction α the following holds:

$$\alpha(a_{k+1}) \in a^* \leftrightarrow \alpha(b_{k+1}) \in a^*.$$

Suppose that $\alpha(a_{k+1}) \in a^*$, then $\alpha(\beta(a_j)) \in a^*$ and $\alpha\beta$ is a 2ε-correction. By the hypothesis, we have $\alpha(\beta(b_j)) \in a^*$, that is $\alpha(b_{k+1}) \in a^*$.

Case 3: a_{k+1} is not a 4ε-word and there are no $j \leq k$ and ε-correction α such that $\alpha(a_j) = a_{k+1}$ but there exist an ε-correction γ and an ε-word c such that $\gamma(a_{k+1}) \in c^*$.

If $\gamma(a_{k+1})$ is a 4ε-word, then a_{k+1} is a 5ϵ-word and we can choose $b_{k+1} = a_{k+1}$ and repeat the proof of Case 1.

Suppose that $\gamma(a_{k+1})$ is not a 4ε-word. Let ℓ be a natural number such that

$$ln(c^{\ell-1}) \;\leq\; \max(6\varepsilon, 4\varepsilon + \max_{i\leq k} ln(b_i)) \;<\; ln(c^{\ell}).$$

Then we choose $b_{k+1} = \gamma^{-1}(c^\ell)$ (notice that $ln(c^\ell) > 4\varepsilon$ and hence by Lemma 11 $\gamma^{-1}(c^\ell)$ is defined).

Let us prove some simple estimations on the length of b_{k+1}. Note that by our definition for all $i \leq k$ we have $ln(c^\ell) - ln(b_i) > 4\varepsilon$. Since b_{k+1} is an ε-correction of c^ℓ, this implies $ln(b_{k+1}) - ln(b_i) > 2\varepsilon$. In a similar way we can establish

$$ln(b_{k+1}) < \max(9\varepsilon, 7\varepsilon + \max_{i\leq k} ln(b_i)). \tag{1}$$

Let us prove Clauses 1–3 of Definition 12 for $\bar{\mathbf{a}}_{k+1}$ and $\bar{\mathbf{b}}_{k+1}$.

1. Let α be an ε-correction. We have to prove that $\alpha(a_i) = a_{k+1}$ if and only if $\alpha(b_i) = b_{k+1}$. Consider two cases: $i \leq k$ and $i = k+1$.
   Let $i \leq k$. By the assumption $\alpha(a_i) \neq a_{k+1}$, so we have to prove $\alpha(b_i) \neq b_{k+1}$. Suppose, by contradiction, $\alpha(b_i) = b_{k+1}$. Then $ln(b_{k+1}) - ln(b_i) \leq 2\varepsilon$ which contradicts to $ln(b_{k+1}) - ln(b_i) > 2\varepsilon$.
   Let $i = k+1$. We have to prove that $\alpha(a_k{+}1) = a_{k+1}$ if and only if $\alpha(b_{k+1}) = b_{k+1}$. Suppose that $\alpha(a_{k+1}) = a_{k+1}$. By assumption, we have $\gamma(a_{k+1}) \in c^*$, i.e. there exists natural number z such that $\gamma(a_{k+1}) = c^z$. Without loss of generality we assume that c is non-periodic. Then $\alpha(\gamma^{-1}(c^z)) = \gamma^{-1}(c^z)$. This implies $\gamma(\alpha(\gamma^{-1}(c^z))) = c^z$. It is not hard to argue $\gamma\alpha\gamma^{-1}$ is a 2ε-correction. Since $\gamma(\alpha(\gamma^{-1}(c^z))) = c^z$, $\gamma\alpha\gamma^{-1}$ either is a trivial correction or for all $w \in c^*$ there exists $z_1 \in \mathbb{N}$ such that $ln(c^{z_1}) \leq 2\varepsilon$ and $\gamma\alpha\gamma^{-1}(w) = \lambda \cdot_{c^{z_1}} [w]_\lambda \cdot c^{z_1}$. Thus $\gamma\alpha\gamma^{-1}(c^\ell)\downarrow$. It is now easy to see that $\gamma\alpha\gamma^{-1}(c^\ell) = c^\ell$. In the other direction the proof is similar.
2. Since $ln(a_{k+1}) > 4\varepsilon$ and $ln(b_{k+1}) > 4\varepsilon$ there is no need to verify Clause 2.
3. Suppose that $\alpha(a_{k+1}) \in a^*$ for some ε-correction α and ε-word a. We have to show $\alpha(b_{k+1}) \in a^*$. Since $\gamma(a_{k+1}) \in c^*$, by Lemma 11, we have $\alpha(\gamma^{-1}(c^\ell)) \in a^*$.

Case 4: a_{k+1} *is not a* 4ε*-word, there are no* $j \leq k$ *and* ε*-correction* α *such that* $\alpha(a_j) = a_{k+1}$ *and for every* ε*-correction* α *and* ε*-word* a*:* $\alpha(a_{k+1}) \notin a^*$. Define the set of words:

$$W = \{prefix(\varepsilon, a_{k+1}) \cdot q \cdot suffix(\varepsilon, a_{k+1}) \mid ln(q) = 2\varepsilon + 1\}.$$

Note that $|W| = 2^{2\varepsilon+1}$. It is not hard to argue that for all $c,\ d \in W$ and ε-corrections α, β the following holds:

$$\alpha(c) = \beta(d) \leftrightarrow c = d.$$

Therefore for every $i \leq k$ there exists at most one element $c \in W$ which can be obtained by an ε-correction from b_i.

Let us count the number of words $w \in W$ such that for some ε-correction α and ε-word a we have $\alpha(a) \in a^*$. It is not hard to argue that the number of such words is not greater than the number of ϵ-words, that is $2^{\varepsilon+1}$.

Now define the following set of words:

$$W' = \{d \in W \mid \text{for all } i \leq k,\ \varepsilon\text{-words } a \text{ and } \varepsilon\text{-corrections } \beta : \beta(b_i) \neq d \text{ and } \beta(d) \notin a^*\}.$$

Let us prove that W' is non-empty. Indeed, W' is be obtained from W by removing all ε-corrections of the words b_i and all ε-corrections of words belonging to some a^*, where a is an ϵ. Therefore, the cardinality of W' is at least $2^{2\varepsilon+1} - k - 2^{\varepsilon+1}$. We have

$$2^{2\varepsilon+1} - k - 2^{\varepsilon+1} > 2^{2\varepsilon+1} - 2^{\varepsilon+2} \geq 0,$$

so W' contains at least one element. Choose b_{k+1} to be any element of W'. Let us check that our choice of b_{k+1} satisfies the definition of $\mathcal{E}_{n,k+1}$-indistinguishability.

1. Let α be an ε-correction. By our assumption, for every $j \leq k$ we have $\alpha(a_j) \neq a_{k+1}$. By our construction of b_{k+1} we have $\alpha(b_j) \neq b_{k+1}$. So it remains to check that $\alpha(a_k + 1) = a_{k+1}$ if and only if $\alpha(b_k + 1) = b_{k+1}$. If α is trivial, then this property is straightforward, so assume that α is non-trivial. If $\alpha(a_{k+1}) = a_{k+1}$, then by Lemma 10 for some ε-word a and ε-correction β we would have $\beta(a_{k+1}) \in c^*$. This would contradict to our assumption, so we have $\alpha(a_{k+1}) \neq a_{k+1}$. Then we have to prove $\alpha(b_{k+1}) \neq b_{k+1}$. Suppose, by contradiction, $\alpha(b_{k+1}) = b_{k+1}$. Then by Lemma 10 for some ε-word a and ε-correction β we would have $\beta(b_{k+1}) \in c^*$. But this is impossible since $b_{k+1} \in W'$.
2. Since $ln(a_{k+1}) > 4\varepsilon$ and $ln(b_{k+1}) > 4\varepsilon$ there is no need to verify Clause 2.
3. We have to show that for every ε-correction α and ε-word a we have $\alpha(b_{k+1}) \notin a^*$. This is immediate by our choice of b_{k+1}.

The proof of Lemma 15 is completed. ❏

LEMMA 16 *For all natural numbers k, n, all sequences of words $\bar{\mathbf{a}}_k$ and $\bar{\mathbf{b}}_k$, if $\bar{\mathbf{a}}_k \ \mathcal{E}_{n+1,k} \bar{\mathbf{b}}_k$ then for every word a_{k+1} there exists word b_{k+1} such that $\bar{\mathbf{a}}_{k+1}$ and $\bar{\mathbf{b}}_{k+1}$ are $\mathcal{E}_{n,k+1}$- indistinguishable and either*

1. *$ln(b_{k+1}) \leq 9 * 2^{3n+k}$, or*
2. *for some $i \leq k$, $ln(b_{k+1}) \leq ln(b_i) + 7 * 2^{3n+k}$.*

PROOF. By routine inspection of the proof of Lemma 15. These bounds appear from (1), other parts of the proof give lower bounds. ❑

For $w \in \{0,1\}^*$ and $n, k, m \in \mathbb{N}$, define $||w|| = ln(w)$ and $\mathcal{H}(n,k,m) = m + 9 * 2^{3n+k}$.

LEMMA 17 *For all natural numbers k, n, m, all sequences of words $\bar{\mathbf{a}}_k$ and $\bar{\mathbf{b}}_k$, if $\bar{\mathbf{a}}_k \ \mathcal{E}_{n+1,k} \bar{\mathbf{b}}_k$ and $||b_i|| \leq m$ for all $i \leq k$ then for every word a_{k+1} there exists word b_{k+1} such that $\bar{\mathbf{a}}_{k+1}$ and $\bar{\mathbf{b}}_{k+1}$ are $\mathcal{E}_{n,k+1}$-indistinguishable and $||b_{k+1}|| \leq \mathcal{H}(n,k,m)$.* ❑

This lemma proves the second conditions of Theorem 5, to prove the first condition note the following result.

LEMMA 18 *Let $\bar{\mathbf{a}}_k, \bar{\mathbf{b}}_k$ be sequences of words such that $\bar{\mathbf{a}}_k \ \mathcal{E}_{0,k} \ \bar{\mathbf{b}}_k$. Then $\bar{\mathbf{a}}_k \ \underset{0,k}{\equiv\!\equiv} \ \bar{\mathbf{b}}_k$.*

PROOF. Since $\bar{\mathbf{a}}_k \ \mathcal{E}_{0,k} \ \bar{\mathbf{b}}_k$, then for all $i, j \leq k$ the following equivalences hold:

$$
\begin{array}{c}
{}_\lambda[a_i]_0 = a_j \leftrightarrow {}_\lambda[b_i]_0 = b_j;\ {}_\lambda[a_i]_1 = a_j \leftrightarrow {}_\lambda[b_i]_1 = b_j; \\
{}_0[a_i]_\lambda = a_j \leftrightarrow {}_0[b_i]_\lambda = b_j;\ {}_1[a_i]_\lambda = a_j \leftrightarrow {}_1[b_i]_\lambda = b_j.
\end{array}
$$

Thus

$$
\begin{array}{c}
r_0(a_j, a_i) \leftrightarrow r_0(b_j, b_i);\ r_1(a_j, a_i) \leftrightarrow r_1(b_j, b_i); \\
l_0(a_j, a_i) \leftrightarrow l_0(b_j, b_i);\ \ l_1(a_j, a_i) \leftrightarrow l_1(b_j, b_i).
\end{array}
$$

Using Definition 3, we conclude $\bar{\mathbf{a}}_k \ \underset{0,k}{\equiv\!\equiv} \bar{\mathbf{b}}_k$. ❑

4 Main Results

Lemma 17 and Lemma 18 prove the conditions for Theorem 5. Therefore, by this theorem we have the following key result.

THEOREM 19 *For all $n, k, m \in \mathbb{N}$:*

1. *for all sequences of words $\bar{\mathbf{a}}_k$ and $\bar{\mathbf{b}}_k$, if $\bar{\mathbf{a}}_k$ and $\bar{\mathbf{b}}_k$ are $\mathcal{E}_{n,k}$-indistinguishable then $\bar{\mathbf{a}}_k \ \underset{n,k}{\equiv\!\equiv} \ \bar{\mathbf{b}}_k$ for all $n, k \in \mathbb{N}$,*
2. *the structure $\mathbf{W}$ is $\mathcal{H}$-bounded.* ❑

Let us extend the first-order language by bounded quantifiers $(\exists v \preceq C)$ and $(\forall v \preceq C)$ for all natural numbers C with the following interpretation: $(\exists v \preceq C)A(v)$ holds if there exists a C-word such v that $A(v)$, and similar for $(\forall v \preceq C)$

LEMMA 20 *Let $Q_1 x_1 \dots Q_n x_n F(\bar{\mathbf{x}}_n)$ be a sentence such that $Q_i \in \{\forall, \exists\}$ and $F(\bar{\mathbf{x}}_n)$ is quantifier-free. Let $C = 9 * 2^{3n+1}$. Then*

$$\mathbf{W} \models Q_1 x_1 \dots Q_n x_n F(\bar{\mathbf{x}}_n) \;\leftrightarrow\; \mathbf{W} \models Q_1 x_1 \preceq C \dots Q_n x_n \preceq C F(\bar{\mathbf{x}}_n). \qquad (2)$$

PROOF. Define $C_1 = 9 * 2^{3n}$ and for all $i > 1$, $C_{i+1} = C_i + 9 * 2^{3(n-i)+i}$. It follows from Theorem 19 that each of the quantifiers $Q_i x_i$ can be equivalently replaced by $(Q x_i \prec C_i)$. It is not hard to argue that $C_i < C$ for all i, which proves (2). ❑

Now we can prove our main result: Theorem 1.

PROOF (of Theorem 1). Recall that we have to prove that the first-order theory of $\mathbf{W}$ is complete in LATIME($2^{O(n)}$). It is known that the first-order theory of $\mathbf{W}$ is LATIME($2^{O(n)}$)-hard already for formulas without the relations l_0, l_1 (see [6,11,10,12], so we should prove that the first-order theory of $\mathbf{W}$ belongs to the class LATIME($2^{O(n)}$). This can be proved by the following procedure running in exponential time by alternating Turing machines with a linear number of alternations: first, using Lemma 20, replace all quantifiers by quantifiers bound by words of length $2^{O(n)}$, and then "guess" the corresponding words using alternating Turing machines. The number of alternations is less than the number of quantifiers in the formula, and is therefore at most linear in n. ❑

Acknowledgments. We thank Bakhadyr Khoussainov, Leonid Libkin, and Wolfgang Thomas for helpful remarks related to the first-order theory of $\mathbf{W}$.

References

1. M. Benedikt, L. Libkin, T. Schwentick, and L. Segoufin. A model-theoretic approach to regular string relations. In *Proc. 16th Annual IEEE Symposium on Logic in Computer Science, LICS 2001*, pages 431–440, 2001.
2. N.S. Bjørner. *Integrating Decision Procedures for Temporal Verification.* PhD thesis, Computer Science Department, Stanford University, 1998.
3. N.S. Bjørner. Reactive verification with queues. In *ARO/ONR/NSF/DARPA Workshop on Engineering Automation for Computer-Based Systems*, pages 1–8, Carmel, CA, 1998.
4. A. Blumensath and E. Grädel. Automatic structures. In *Proc. 15th Annual IEEE Symp. on Logic in Computer Science*, pages 51–62, Santa Barbara, California, June 2000.
5. K.J. Compton and C.W. Henson. A uniform method for proving lower bounds on the computational complexity of logical theories. *Annals of Pure and Applied Logic*, 48:1–79, 1990.

6. J. Ferrante and C.W. Rackoff. *The computational complexity of logical theories*, volume 718 of *Lecture Notes in Mathematics*. Springer-Verlag, 1979.
7. B. Khoussainov and A. Nerode. Automatic presentations of structures. In Daniel Leivant, editor, *Logic and Computational Complexity, International Workshop LCC '94*, volume 960 of *Lecture Notes in Computer Science*, pages 367–392. Springer Verlag, 1995.
8. T. Rybina and A. Voronkov. A decision procedure for term algebras with queues. *ACM Transactions on Computational Logic*, 2(2):155–181, 2001.
9. W. Thomas. Infinite trees and automaton definable relations over omega-words. *Theoretical Computer Science*, 103(1):143–159, 1992.
10. H. Volger. A new hierarchy of elementary recursive decision problems. *Methods of Operations Research*, 45:509–519, 1983.
11. H. Volger. Turing machines with linear alternation, theories of bounded concatenation and the decision problem of first order theories (Note). *Theoretical Computer Science*, 23:333–337, 1983.
12. S. Vorobyov and A. Voronkov. Complexity of nonrecursive logic programs with complex values. In *PODS'98*, pages 244–253, Seattle, Washington, 1998. ACM Press.