Monadic Logic of Order over Naturals Has no Finite Base.

Danièle Beauquier[1]
Laboratory of Algorithmics, Complexity and Logic,
Department of Informatics,
University Paris-12, France

Alexander Rabinovich[2]
Department of Computer Science,
Tel-Aviv University, Israel

Abstract

A major result concerning Temporal Logics (TL) is Kamp's theorem [Kam68, GHR94], which states that the temporal logic over the pair of modalities X *until* Y and X *since* Y is expressively complete for the first order fragment of monadic logic of order over the natural numbers. We show that there is no finite set of modalities B such that the temporal logic over B and monadic logic of order have the same expressive power over the natural numbers. As a consequence of our proof, we obtain that there is no finite base temporal logic which is expressively complete for the μ-calculus.

1 Introduction

Various temporal logics have been proposed for reasoning about so-called "reactive" systems, computer hardware or software systems which exhibit (potentially) non-terminating and non-deterministic behavior. Such a system is typically represented by the (potentially) infinite sequences of computation states through which it may evolve, where we associate with each state the set of atomic propositions which are true in that state, along with the possible next state transitions to which it may evolve. Thus, its behavior is denoted by a (potentially) infinite rooted tree, with the initial state of the system represented by the root of the tree.

Temporal Logic (TL) initiated by Pnueli in [Pnu77] is a convenient framework for the specification properties of systems. This made TL a popular subject in the Computer Science community and it enjoyed extensive research during the last 20 years. In temporal logic the relevant properties of the system are described by *Atomic Propositions* that hold at some points in time but not at others. More complex properties are described by formulas built from the atoms using Boolean connectives and *Modalities* (temporal connectives): a k-place modality C transforms statements $\varphi_1 \dots \varphi_k$ on points possibly other than the given point t_0 to a statement $C(\varphi_1 \dots \varphi_k)$ on the point t_0. The rule that specifies when the statement $C(\varphi_1 \dots \varphi_k)$ is true for the given point, is called *Truth Table*. The choice of the particular modalities with their truth tables determines the different temporal logics. A Temporal Logic with modalities $M_1, \dots M_k$ is denoted by $TL(M_1, \dots, M_k)$.

The most basic modality is the one place modality $\mathsf{F}X$ saying "X holds some time in the future".

[1] *Address:* Dept. of Informatics, University Paris-12, 61 Av. du Gén. de Gaulle, 94010, Créteil, France.
E-mail: beauquier@univ-paris12.fr

[2] *Address:* Department of Computer Science, Tel-Aviv University, Israel.
E-mail: rabino-math.tau.ac.il

Its truth table is usually formalized by $\varphi_{\mathsf{F}}(t_0, X) \equiv (\exists t > t_0)\ t \in X$. This is a formula of the Monadic Logic of Order (MLO). The Monadic Logic of Order is a fundamental formalism in Mathematical Logic. Its formulas are built using atomic propositions $t \in X$, atomic relations between elements $t_1 = t_2$, $t_1 < t_2$, Boolean connectives, first-order quantifiers $\exists t$ and $\forall t$, and second order (set) quantifiers $\exists X$ and $\forall X$. Practically all the modalities used in the literature have their truth tables defined in MLO, and as a result every formula of a temporal logic translates directly into an equivalent formula of MLO. Therefore, the different temporal logics may be considered a convenient way to use fragments of MLO. MLO can also serve as a yardstick by which to check the strength of the temporal logic chosen: a temporal logic is *expressively complete* for a fragment L of MLO if every formula of L with a single variable t_0 is equivalent to a temporal formula.

Actually, the notion of expressive completeness refers to a temporal logic and to a model (or a class of models) since the question if two formulas are equivalent depends on the domain over which they are evaluated. Any partially ordered set with monadic predicates is a model for TL and MLO, but the main, *canonical*, linear time intended models are the non-negative integers $\langle \mathbb{N}, < \rangle$ for discrete time and the non-negative reals $\langle \mathbb{R}^+, < \rangle$ for continuous time.

A major result concerning TL is Kamp's theorem [Kam68, GHR94] which states that $TL(\mathbf{U}, \mathbf{S})$, the temporal logic having "*Until*" and "*Since*" as only modalities, is expressively complete for the first-order fragment of MLO over the above two linear time canonical models. Kamp's theorem also applies to *future formulas* (i.e., formulas that do not depend on points before the considered point) of the first-order fragment of MLO: this fragment has the same expressive power as $TL(\mathbf{U})$ over $\langle \mathbb{N}, < \rangle$.

Some natural properties are not expressible in the first-order logic [MP71]. For example, in the first-order fragment of MLO it is impossible to specify any of the following properties $Mult_p(X)$ $(1 < p \in \mathbb{N})$:

$Mult_p(X)$: $Mult_p(X)$ holds at point t_0 iff there is exactly one $t > t_0$ such that X holds at t, and the distance between t_0 and this t is a multiple of p plus one.

However, for every p, the property $Mult_p(X)$ is easily expressible in the future fragment of MLO. We address the question of existence of a finite base temporal logic which is expressively equivalent to MLO.

From the main technical lemma (Lemma 15) it follows that for every finite set of modalities $\{M_1, \dots M_k\}$ with truth tables in MLO there is $p \in \mathbb{N}$ such that the property $Mult_p(X)$ is not expressible in $TL(M_1, \dots M_k)$.

As a consequence of this lemma we obtain that there is no finite set of modalities such that the temporal logic over this set of modalities is expressively equivalent to monadic logic of order (over the naturals).

Another consequence of the main lemma is that there is no finite set of modalities such that the temporal logic over this set of modalities is expressively equivalent to the μ-calculus (over the trees). This negative result complements a result from [RM00] which states that an important branching time logic CTL^* [EH86] has no finite base. However, the proof of the later result is more subtle.

The paper is organized as follows. The next section provides the necessary notions from Monadic logic of order (MLO), Temporal Logics, and Automata theory. We also prove there two pumping lemmas which will be useful for the proof of the main theorem. In Section 3 we prove that MLO has no finite base. In Section 4 we show that μ-calculus has no finite base.

2 Preliminaries

2.1 Monadic Logic of Order (over Naturals)

The set of natural numbers is denoted by $\mathbb{N}$ and $\mathcal{P}(\mathbb{N})$ denotes the set of subsets of $\mathbb{N}$. The underlying structure used in this paper is $S = (\mathbb{N}, <)$. We shall use $S_{\geq a}$ to denote the structure $(\mathbb{N}_{\geq a}, <)$, where $\mathbb{N}_{\geq a} = \{n \in \mathbb{N} | \, n \geq a\}$.
The syntax of the *second order Monadic Logic of Order* (MLO) has in its vocabulary individual first order variables $x, x_0, x_1, x_2, ...$ representing time points, and set variables $X, X_0, X_1, X_2, ...$ Formulas are built up from atomic formulas of the form $x_1 < x_2$, $x \in X$ using the propositional connectives $\wedge$ and $\neg$ and quantifiers $\exists x$ and $\exists X$.
We shall write $\varphi(x_1, x_2, ..., x_k, X_1, X_2, ..., X_m)$ to indicate that the free variables of φ are among $x_1, x_2, ..., x_k, X_1, X_2, ..., X_m$. We write

$$(S, s_1, s_2, .., s_k, S_1, S_2, .., S_m) \models \varphi(x_1, x_2, ...x_k, X_1, X_2, ..., X_m)$$

if the formula $\varphi(x_1, x_2, ...x_k, X_1, X_2, ..., X_m)$ is satisfied in the structure S with x_i interpreted as the natural s_i $(1 \leq i \leq k)$, and X_j interpreted by the set of naturals S_j $(1 \leq j \leq m)$.
A MLO formula without second order quantifiers is a *first order formula.* The set of first order MLO formulas will be denoted $FOMLO$.

Definition 1 (Future MLO Formula) *A formula $\varphi(x_0, X_1, X_2, ..., X_m)$ of MLO with one free first-order variable x_0 is a future formula if for every $a \in \mathbb{N}$ and every m subsets $S_1, S_2, .., S_m$ of $\mathbb{N}$, the following holds:*

$$(S, a, S_1, S_2, .., S_m) \models \varphi(x_0, X_1, X_2, ..., X_m) \textit{ iff } (S_{\geq a}, a, S'_1, S'_2, .., S'_m) \models \varphi(x_0, X_1, X_2, ..., X_m)$$

where $S'_i = S_i \cap \mathbb{N}_{\geq a}$ for $i = 1, 2, ..., m$.

Past formulas are defined in a symmetric way.

2.2 Temporal Logics and Modalities

In this subsection we recall the syntax and semantics of temporal logics and how temporal modalities are defined using MLO truth tables with notations adopted from [GHR94] and [HR99]. The syntax of *Temporal Logic* (TL) has in its vocabulary a set of *variables* $\{q_1, q_2, ...\}$ and a set B of *modality names*, sometimes called "temporal connectives" or "temporal operators", with prescribed arity $B = \{O_1^{(l_1)}, O_2^{(l_2)}, ...\}$ (we usually omit the arity notation). The set of modality names may be infinite. A temporal logic based on a set of modalities B is denoted $TL(B)$; B is called the *base* of $TL(B)$.
Atomic temporal formulas are just variables q_i and other formulas are obtained from the atoms using boolean connectives and applying the modalities. The syntax of $TL(B)$ is given by the following grammar:

$$\varphi ::= q_i \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi_1 | \, O_i^{(l_i)}(\varphi_1, \varphi_2, ...\varphi_{l_i})$$

Temporal formulas are interpreted over structures of the form $(\mathbb{N}, <, S_1, S_2, .., S_m)$ where S_i are subsets of $\mathbb{N}$ (monadic predicates). Every modality $O^{(l)}$ is interpreted over S as an operator $\hat{O}^{(l)} : [\mathcal{P}(\mathbb{N})]^l \rightarrow \mathcal{P}(\mathbb{N})$ which assigns "the set of points where $O^{(l)}(S_1, S_2, ...S_l)$ holds" to the l-tuple $\langle S_1, S_2, ..., S_l \rangle$. Formally the semantics of a formula $\varphi \in TL$ using variables in $\{q_1, ...q_m\}$, over a structure $\mathcal{T} = (\mathbb{N}, <, S_1, S_2, .., S_m)$ is defined inductively as follows.
For atomic formulas, $\mathcal{T}, s \models q_i$ iff $s \in Q_i$; the semantics of boolean combinations is defined as usual, and the semantics of modalities is defined by:

$$\mathcal{T}, s \models O^{(l)}(\varphi_1, \varphi_2, ..\varphi_l)$$

iff

$$s \in \hat{O}^{(l)}(R_{\varphi_1}, R_{\varphi_2}, ..., R_{\varphi_l})$$

where $R_{\varphi_i} = \{a \in \mathbb{N} | \ a \models \ \varphi_i\}$ for $1 \leq i \leq l$.
We consider only temporal modalities which are defined in MLO: we assume that for every modality O with arity l, there is a formula (truth table) $\bar{O}(x_0, X_1, X_2, ..., X_l)$ of MLO with one free first-order x_0 and l free set variables $X_1, X_2, ..., X_l$, such that for every subsets S_i of $\mathbb{N}$:

$$\hat{O}(S_1, S_2, ..., S_l) = \{s \in \mathbb{N} | \ (S, s, S_1, S_2, ..., S_l) \models \bar{O}(x_0, X_1, X_2, ..., X_l)\}.$$

Example (Some common modalities and their truth table)

- The one place modality F ("eventually"); its truth table is

$$\varphi_{\mathsf{F}}(x_0, X) = \exists y(y > x_0 \wedge y \in X).$$

- The two places modality U (" until "); its truth table is

$$\varphi_{\mathsf{U}}(x_0, X_1, X_2) = \exists y(y > x_0 \wedge y \in X_1 \wedge \forall z(x_0 < z < y) \rightarrow z \in X_2).$$

- The two places modality S (" since "); its truth table is

$$\varphi_{\mathsf{S}}(x_0, X_1, X_2) = \exists y(y < x_0 \wedge y \in X_1 \wedge \forall z(x_0 > z > y) \rightarrow z \in X_2).$$

The choice of the particular modalities with their truth tables determines the different temporal logics.

Definition 2 *A temporal modality O is a (first-order) future modality if its truth table is a (first-order) future formula of MLO.*

The modalities defined in the above example, $\mathsf{F}q$, $\mathsf{U}(q_1, q_2)$ are first-order future modalities; the modality $\mathsf{S}(q_1, q_2)$ is not a future modality. One can show that the one place future modality modality "Even q", expressing that the set of future moments when q holds is finite and even, has a truth table in MLO, but is not expressible by a first order formula of MLO.

2.3 Kamp's Theorem

Different temporal logics may be considered a convenient way to use fragments of MLO. To discuss the strength of a given temporal logic, we use the following standard definition.

A temporal logic formula $\phi(X_1, \dots X_k)$ is *equivalent* to an MLO formula $\psi(x_0, X_1, \dots, X_k)$ (or to a temporal logic formula ψ) over a structure $T = (U, <)$ iff for every $a \in U$ and $S_1, \dots S_k \subseteq U$:

$$(U, <, a \models \varphi(S_1, \dots, S_k) \text{ if and only if } (U, <) \models \psi(a, S_1, \dots, S_k).$$

ϕ is equivalent to ψ (over a set C of structures) iff for every T (respectively, for every $T \in C$), ϕ is equivalent to ψ over T.

Definition 3 *Let L be a fragment of MLO and let C be a set of structures. A temporal logic TL_1 is expressively complete for L over C if for every formula $\psi(x_0, X_1, ..., X_n) \in L$ with single free first order variable x_0, there is a formula $\varphi \in TL_1$ which is equivalent to ψ over C, and for every formula $\psi \in TL_1$, there is a formula $\psi(x_0, X_1, ..., X_n) \in L$ with single free first order variable x_0 which is equivalent to φ over C.*

A major result concerning TL and $FOMLO$ is Kamp's theorem (we give here a partial result):

Theorem 4 Kamp [Kam68, GHR94] *1. The temporal logic with two modalities* $\mathbf{U}(q_1, q_2)$ *("*q_2 *until* q_1*") and* $\mathbf{S}(q_1, q_2)$ *("*q_2 *since* q_1*") is expressively complete for FOMLO over natural numbers. 2. The temporal logic with the single modality* $\mathbf{U}(q_1, q_2)$ *is expressively complete for the future fragment of* $FOMLO$ *over natural numbers.*

2.4 Regular ω-languages versus MLO

Notation

Let A be a finite alphabet, A^*, resp. A^ω stands for the set of finite words, resp. the set of ω-sequences (or ω-words) over A. The empty word is denoted by ϵ. Finite words are denoted by u, v, v... and ω-words are denoted by α, β, γ,.... If α is an ω-word, $\alpha(i)$ denotes the ith letter of α, so $\alpha = \alpha(0)\alpha(1)\alpha(2)$.... A subset of A^ω is called an ω-language.
There are several equivalent definitions of regular ω-languages. We give here the one which is more convenient for our purpose.

Definition 5 (Muller automaton)
A (complete deterministic) Muller automaton over the alphabet A is of the form $\mathcal{A} = (Q, q_0, \delta, \mathcal{F})$, *with finite state set Q, initial state* $q_0 \in Q$, *transition function* $\delta : Q \times A \to Q$ *and a family* $\mathcal{F}$ *of accepting subsets of Q.*

For $q \in Q$ and $a \in A$, we will denote $\delta(q, a)$ as $q \cdot a$.
The run of $\mathcal{A}$ on an ω-word $\alpha = \alpha(0)\alpha(1)$... is the sequence of states $\sigma = \sigma(0)\sigma(1)$... such that $\sigma_0 = q_0$, $\sigma(i+1) = \delta(\sigma(i), \alpha(i))$ for every $i \geq 0$; the run is *successful* if the set of states which occur infinitely often in σ belongs to $\mathcal{F}$. The automaton $\mathcal{A}$ *accepts* α if the run of $\mathcal{A}$ on α is successful.
Let
$L(\mathcal{A}) = \{\alpha \in A^\omega | \mathcal{A} \text{ accepts } \alpha\}$ $L(\mathcal{A}) = \{\alpha \in A^\omega \ : \ \mathcal{A} \text{ accepts } \alpha\}$ looks better; similar in other places.
be the ω-language *recognized* by $\mathcal{A}$. If $L = L(\mathcal{A})$ for some complete deterministic Muller automaton $\mathcal{A}$, L is said to be *regular.*

A classical result due to Büchi [Büc60] is the following : an ω-language is definable in MLO iff it is regular. Let us make this statement more precise.
Let $\varphi(X_1, \dots, X_n)$ be an MLO formula, and $A = \{0, 1\}^n$. If $a \in A$, we denote by a_k the k-th component of a. Each ω-word α over the alphabet A defines a n-tuple $\bar{\alpha} = (S_1, \dots, S_n)$ of subsets of $\mathbb{N}$ where $S_k = \{i \in \mathbb{N} \ : \ \alpha(i)_k = 1\}$, and conversely every n-tuple $(S_1, \dots, S_n)$ defines in a unique way an ω-word α such that $\bar{\alpha} = (S_1, \dots, S_n)$. Thus the formula $\varphi(X_1, \dots, X_n)$ defines an ω-language $L(\varphi) = \{\alpha \in \{0, 1\}^n \ : \ (S, \bar{\alpha}) \models \varphi(X_1, \dots, X_n)\}$.

Theorem 6 (Büchi [Büc60]) *An* ω*-language L over the alphabet* $\{0, 1\}^n$ *is regular iff there is an* MLO *formula* $\varphi(X_1, \dots, X_n)$ *such that* $L = L(\varphi)$.

The following Lemma is also a well-known fact [BP85]:

Lemma 7 *An* ω*-language L over the alphabet A is regular iff there is a finite monoid M and a monoid morphism* $f : A^* \to M$ *such that L is a union of sets* $f^{-1}(m)f^{-1}(e)^\omega$, *where* $m, e \in M$ *and e can be assumed to be an idempotent (i.e. ee=e) satisfying* $me = m$.

Let $\varphi(x_0, X_1, \dots, X_m)$ be an MLO-formula being the truth table of some modality of arity m. We build from φ an MLO -formula $\tilde{\varphi}(X_0, X_1, \dots, X_m)$ such that:

$$(S,a,S_1,S_2,...,S_m) \models \varphi(x_0,X_1,\ldots,X_m)$$

iff

$$(S,\{a\},S_1,S_2,...,S_m) \models \tilde{\varphi}(X_0,X_1,\ldots,X_m).$$

The formula $\tilde{\varphi}$ is the conjunction of a formula expressing that X_0 is a singleton, and a formula resulting from φ by replacing:

$x_0 < x$ (resp. $x < x_0$) by: $\forall z \in X_0\ z < x$ (resp. $\forall z \in X_0\ x < z$)

and $x_0 \in X$ by: $\forall z \in X_0\ z \in X$.

By definition of $\tilde{\varphi}$ we have:

Lemma 8 *For every MLO formula $\varphi(x_0,X_1,\ldots,X_m)$:*
$(S,a,S_1,S_2,...,S_m) \models \varphi(x_0,X_1,\ldots,X_m)$ iff $\alpha \in L(\tilde{\varphi})$ where $\bar{\alpha} = (\{a\},S_1,S_2,...,S_m)$.

Let $A' = \{0,1\}^m$, $A = \{0,1\}^{m+1}$, $A_0 = \{0\} \times \{0,1\}^m$, and $A_1 = \{1\} \times \{0,1\}^m$. Given an ω-word $\alpha \in A'^{\omega}$ representing a m-tuple $(S_1,S_2,...,S_m)$, and an integer $a \in \mathbb{N}$ representing the present time, we define a *pointed version* of α denoted by $\alpha^{[a]} \in A^{\omega}$ such that $\alpha_i^{[a]} = (0,\alpha_i)$ for $i \neq a$ and $\alpha_a^{[a]} = (1,\alpha_a)$. The ω-word $\alpha^{[a]}$ describes the $m+1$-tuple $(\{a\},S_1,S_2,...,S_m)$. Clearly, every ω-word in $L(\tilde{\varphi})$ has exactly one occurence of a letter from A_1 corresponding to present time. Moreover $L(\tilde{\varphi})$ has the following property:

Theorem 9 *$L(\tilde{\varphi})$ is a finite union of languages of the form $R_j a_j R'_j$ where R_j (resp. R'_j) is a regular language (resp. ω-language) included in A_0^* (resp. A_0^{ω}), and $a_j \in A_1$.*

Proof. Using Lemma 7, there is a finite monoid M and a monoid morphism $f : A^* \to M$ such that $L(\tilde{\varphi})$ is a union of sets $f^{-1}(m)f^{-1}(e)^{\omega}$, where $m,e \in M$, $ee = e$ and $me = m$.
Let $\alpha \in L(\tilde{\varphi})$. It can be decomposed as $\alpha = ua\beta$, $u \in A_0^*$, $a \in A_1$ $\beta \in A_0^{\omega}$. There exist $m,\ e \in M$ satisfying $me = m$, $ee = e$ and $\alpha \in f^{-1}(m)f^{-1}(e)^{\omega} \subset L(\tilde{\varphi})$. Since $me = m$ there is a decomposition $\beta = v\beta_1$ such that $f(uav) = m$ and $\beta_1 \in f^{-1}(e)^{\omega}$. Let $f(u) = m_1,\ f(v) = m_2$.
Then $\alpha \in f^{-1}(m_1)af^{-1}(m_2)f^{-1}(e)^{\omega} \subset f^{-1}(m)f^{-1}(e)^{\omega} \subset L(\tilde{\varphi})$. So $L(\tilde{\varphi})$ is a finite union of languages of the form $f^{-1}(m_1)af^{-1}(m_2)f^{-1}(e)^{\omega}$. Since $f^{-1}(m_1)$ is a regular language included in A_0^* and $f^{-1}(m_2)f^{-1}(e)^{\omega}$ is a regular ω-language included in A_0^{ω}, the theorem is proved. ■

Notice that the representation of $L(\tilde{\varphi})$ in Theorem 9 provides an automata-theoretic proof of the separation property (Lemma 3.11, [CS99]):

Theorem 10 *MLO has the separation property over natural numbers, i.e. every MLO-formula $\varphi(x_0,X_1,X_2,...X_m)$ with one free first-order variable x_0 is equivalent over natural numbers to a boolean combination of past and future formulas.*

Remark Actually the separation theorem for *MLO* is valid over the class of all linear orders. The proof of this more general separation theorem can be obtained by Shelah's compositional methods [She75].

2.5 Some Pumping Lemmas

In this subsection we introduce the transition monoid of a complete deterministic automaton to get two technical pumping lemmas which will be used to establish the main result in the next section.

Transition monoid of a complete deterministic automaton

Let $\mathcal{A} = (Q, q_0, \delta, \mathcal{F})$ be a complete deterministic Muller automaton, and $\mathcal{T}(Q)$ be the monoid of functions from Q into itself, equipped with the composition product.
The function δ is extended into a function from $Q \times A^*$ to Q in an inductive way, by setting for each $q \in Q$, $q \cdot \epsilon = q$ and for each finite word $u \in A^*$ each $a \in A$, $q \cdot ua = (q \cdot u) \cdot a$. We define a morphism from A^* into $\mathcal{T}(Q)$ which maps every finite word u into the transformation $\bar{u} : Q \to Q$ such that $\bar{u}(q) = q \cdot u$ for every $q \in Q$. The submonoid of $\mathcal{T}(Q)$ image of A^* by this morphism, $M(\mathcal{A})$, is called the transition monoid of $\mathcal{A}$. This transition monoid is finite.
We recall the following property of finite monoids:

Lemma 11 *Let M be a finite monoid. There exists an integer $n > 0$ such that for every $\sigma \in M$, σ^n is idempotent.*

We denote by $T(M)$ the smallest integer n satisfying this property.
In the following lemma which is a kind of Pumping Lemma, α is either a finite word or an ω-word.

Lemma 12 *Let R be a regular (ω-)language recognized by a complete deterministic (Muller) finite automaton $\mathcal{A}$. Let $T = T(M(\mathcal{A}))$. Then:*

$$\forall K \geq T \ \forall u \in A^* \ \forall \alpha \in A^* (resp. \ \ A^\omega) \ (u^K \alpha \in R \iff u^{K+T} \alpha \in R).$$

Proof. For $K \geq T$ we can write $u^{K+T}\alpha = u^{2T}u^{K-T}\alpha$. If q_0 is the initial state of the automaton $\mathcal{A}$, states $q_0 \cdot u^{2T}$ and $q_0 \cdot u^T$ are equal since in $M(\mathcal{A})$, $\bar{u}^T = \bar{u}^{2T}$. Thus for the two (ω)-words $u^K\alpha$ and $u^{K+T}\alpha$, before reading the suffix $u^{K-T}\alpha$, the automaton is in the same state, and so, $u^K\alpha$ is accepted iff $u^{K+T}\alpha$ is accepted by $\mathcal{A}$. The lemma is proved. ■

In the lemma below, $A_0 = \{0\} \times \{0,1\}^m$, and $A_1 = \{1\} \times \{0,1\}^m$.

Lemma 13 *Let $\varphi(x_0, X_1, ..., X_m)$ be an MLO formula with one free first order variable x_0. The language $L(\tilde{\varphi})$ has the following property: there exist an integer N and a period $T < N$ such that for all $u_0, u_1, u_2 \in {A_0}^*$, $a \in A_1$, $\alpha \in {A_0}^\omega$ for all $K_1, K_2 \geq N$*

$$u_0{u_1}^{K_1}a{u_2}^{K_2}\alpha \in L(\tilde{\varphi}) \Rightarrow \ u_0{u_1}^{K_1+T}a{u_2}^{K_2-T}\alpha \in L(\tilde{\varphi}).$$

Proof. Using Theorem 9, $L(\tilde{\varphi})$ is a finite union of languages of the form $R_j a_j R'_j$ where R_j (resp. R'_j) is a regular language (resp. ω-language) included in A_0^* (resp. A_0^ω), and $a_j \in A_1$. Let $\mathcal{A}_j$ be a complete deterministic finite automaton recognizing the mirror image $\tilde{R}_j$ of R_j and $\mathcal{A}'_j$ be a complete deterministic finite Muller automaton recognizing R'_j. Take as a value for T the maximum of the set of integers $T(M(\mathcal{A}_j))$, $T(M(\mathcal{A}'_j))$ for all j. Lemma 12 associates to $\tilde{R}_j$ (resp. R'_j) an integer N_j (resp. N'_j). Take as a value for N_0 the maximum of the set of integers N_j, N'_j for all j. Using Lemma 12 for each j we have:

$$\forall K_1 > N_0 \ (u_0{u_1}^{K_1} \in R_j \Leftrightarrow u_0{u_1}^{K_1+T} \in R_j)$$
$$\forall K_2 > N_0 \ ({u_2}^{K_2}\alpha \in R'_j \Leftrightarrow {u_2}^{K_2+T}\alpha \in R'_j).$$

As a consequence, if $K_1, K_2 \geq N_0 + T$ we have :

$$u_0{u_1}^{K_1}a{u_2}^{K_2}\alpha \in L(\tilde{\varphi}) \Rightarrow \ u_0{u_1}^{K_1+T}a{u_2}^{K_2-T}\alpha \in L(\tilde{\varphi}).$$

Thus we choose $N = N_0 + T$ and we are done. ■

3 MLO Has No Finite Base

In this section we will prove that MLO has no finite base, i.e. that there is no temporal logic over a finite base which is expressively equivalent to MLO over natural numbers.

Definition 14 *We say that a word w is* quasi-periodic *with parameters N, T (T is a period for w) if there are words u_1, u_2, u_3 and $r \in \mathbb{N}$ such that $w = u_1 u_2^r u_3$, $|u_1|, |u_3| < N$, and $|u_2| = T$.*

Observe that according to our definition if $|w| < 2N - 1$ then w is quasi-periodic with parameters N, T.
Let $\varphi(x_0, X)$ be an MLO formula with one free first order variable x_0. Define

$$b^{\varphi}_{i,n} = 1 \ \text{ iff } \ (S, i, \{n\}) \models \varphi(x_0, X) \tag{1}$$

i.e., $\varphi(x_0, X)$ holds when x_0 is interpreted as i and X is interpreted as the set $\{n\}$. Note that $b^{\varphi}_{i,n} = 1$ iff $\alpha_n^{[i]} \in L(\tilde{\varphi})$, where $\alpha_n = 0^n 1 0^{\omega}$.
Finally for every $n \in \mathbb{N}$ and a formula φ define the word d^{φ}_n as $b^{\varphi}_{0,n} b^{\varphi}_{1,n} \dots b^{\varphi}_{i,n} \dots b^{\varphi}_{n-1,n}$.
For a temporal logic formula $\varphi(X)$ and $i, n \in \mathbb{N}$, $b^{\varphi}_{i,n} \in \{0, 1\}$ and d^{φ}_n are defined in a similar way.
Let $\mathcal{P}$ be a set of positive integers. We denote by $\mathcal{P}^+$ the set of integers which can be decomposed as a product of elements of $\mathcal{P}$.

Lemma 15 *For every finite set of modalities $\mathcal{O}$, there exists a finite set of numbers $\mathcal{P}$ such that for every temporal formula $\varphi(X)$ in $TL(\mathcal{O})$ there exist integers $T \in \mathcal{P}^+$ and N such that for every $n > 2N$, d^{φ}_n is quasi-periodic with parameters N, T.*

Proof. Let $\mathcal{O} = \{O_1, O_2, ..., O_k\}$ be a finite set of modalities. The truth table of the modality O_m ($1 \le m \le k$) is an MLO formula $\bar{O}_m(x_0, X_1, ..., X_{l_m})$ with one free variable, and the formula $\tilde{\bar{O}}_m(X_0, X_1, ..., X_{l_m})$ defines a regular ω-language L_m over the alphabet $\{0, 1\}^{l_m+1}$ recognized by a Muller automaton $\mathcal{A}_m$ (Theorem 6). Lemma 13 associates to each L_m a period T_m. Define $\mathcal{P}$ as the set of divisors of the T_m's for $1 \le m \le k$.
Let $\varphi \in TL(\mathcal{O})$. The proof is by induction on the complexity of the formula φ.
• $\varphi = X$
By definition $(\mathcal{T}, i) \models X$ iff $i \in Q$, where $\mathcal{T} = (\mathbb{N}, i, Q)$. Thus, $\alpha_n^{[i]}$ belongs to $L(\tilde{\varphi})$ iff $i = n$, and then $b^{\varphi}_{i,n}$ is equal to 1 iff $i = n$. So d^{φ}_n is quasi-periodic with parameters N, T for every values of N and T.
• $\varphi = \varphi_1(X) \wedge \varphi_2(X)$ or $\varphi = \neg\varphi_1(X)$
The induction is straightforward.
• $\varphi = O_m(\varphi_1(X), ..., \varphi_{l_m}(X))$ where $\varphi_1(X), ..., \varphi_{l_m}(X)$ are formulas of $TL(\mathcal{O})$. By induction, the word $d^{\varphi_p}_n$ for $1 \le p \le l_m$ is quasi-periodic with parameters N^{φ_p} and period $T^{\varphi_p} \in \mathcal{P}^+$. For every $i \in \mathbb{N}$, define $c_{i,n}$ as the l_m-tuple $(b^{\varphi_1}_{i,n}, b^{\varphi_2}_{i,n}, ..., b^{\varphi_{l_m}}_{i,n})$. The word $c_n = c_{0,n} c_{1,n} ... c_{n-1,n}$ is also quasi-periodic with parameters T_0 equal to the least common multiplier of the T^{φ_p} ($1 \le p \le l_m$) and $N_0 = max_p\{N^{\varphi_p}\} + T_0$. Since $T^{\varphi_p} \in \mathcal{P}^+$ for all $1 \le p \le l_m$, it follows that $T_0 \in \mathcal{P}^+$.
For a fixed n, let γ_n be the ω-word $c_{0,n} c_{1,n} ... c_{i,n} ...$. For $i < n$ consider the ω-word $\gamma_n^{[i]}$. Then $\gamma_n^{[i]}$ is periodic in a left neighbour of present moment and also in a right neighbour of it. More precisely, if $i > N_0$ and $n - i > N_0$, then $\gamma_n^{[i]}$ can be written in a unique way

$$\gamma_n^{[i]} = u_0 {u_1}^{K_1} a {u_2}^{K_2} \beta, \tag{2}$$

where $|u_1| = |u_2| = T_0$, $N_0 < |u_0| \leq N_0 + T_0$, $N_0 + K_2T_0 < n - i \leq N_0 + K_2T_0 + T_0$ and $a \in A_1$ (recall that $A_1 = \{1\} \times \{0,1\}^{l_m}$).
Now apply Lemma 13 to L_m. There exist an integer N_m and a period $T_m = T(M(\mathcal{A}_m)) \in \mathcal{P}$ such that for all $K_1, K_2 \geq N_m$

$$\gamma_n^{[i]} = u_0{u_1}^{K_1}a{u_2}^{K_2}\beta \in L_m \Rightarrow\ u_0{u_1}^{K_1+T_m}a{u_2}^{K_2-T_m}\beta \in L_m. \tag{3}$$

By definition of the modality O_m, using Lemma 8 and definition (1) we have:

$$\gamma_n^{[i]} \in L_m \ \Leftrightarrow\ b_{i,n}^{\varphi} = 1 \tag{4}$$

Note that

$$u_0{u_1}^{K_1+T_m}a{u_2}^{K_2-T_m}\beta = \gamma_n^{[i+T_m]} \tag{5}$$

Define $T = T_0 \times T_m$ and $N = N_0 + (N_m + 1)T_0$.
We claim that for every $n > 2N$ the word d_n^{φ} is quasi-periodic with parameters N, T. Let i be such that $N < i < n - N$. Then $\gamma_n^{[i]}$ has the form (2), with $K_1, K_2 \geq N_m$. Thus by (3)-(4)
$(N < i < n - N) \Rightarrow\ b_{i,n}^{\varphi} = b_{i+T,n}^{\varphi}$.
Consequently, for $n > 2N$ the word d_n^{φ} is quasi-periodic with parameters N and $T \in \mathcal{P}^+$.
The lemma is proved. ■

Let $p \in \mathbb{N}$. Consider a MLO formula $Mult_p(x_0, X)$ expressing that there is exactly one occurrence of X after x_0 and the distance between x_0 and this occurrence is a multiple of p plus one. Notice that $Mult_p(x_0, X)$ is a future formula.

Lemma 16 *For every finite set $\mathcal{O}$ of modalities, there exists an integer p such that the future modality with truth table $Mult_p(x_0, X)$ is not in $TL(\mathcal{O})$.*

Proof. Suppose there is a finite set of modalities $\mathcal{O}$ expressively complete for MLO. Let $\mathcal{P}$ be the set of numbers defined in Lemma 15 for $\mathcal{O}$. Choose for p a prime number greater than all numbers in $\mathcal{P}$. The future temporal formula with truth table $Mult_p(x_0, X)$ is in $TL(\mathcal{O})$. Using Lemma 15 there exist $T_p \in \mathcal{P}^+$ and N_p such that for $n > N_p$, $d_n^{Mult_p}$ is quasi-periodic with parameters N_p, T_p. Clearly for $n > i$ we have:
$b_{i,n}^{Mult_p} = 1 \ \Leftrightarrow\ n - i \in p\mathbb{N} + 1$.
Take n and i such that $i > N_p$, $n - i > N_p$ and $n - i \in p\mathbb{N} + 1$. Then, $b_{i,n}^{Mult_p} = 1$ implies $b_{i+T_p,n}^{Mult_p} = 1$. Thus $n - i - T_p \in p\mathbb{N} + 1$ and finally $T_p \in p\mathbb{N}$. A contradiction since p is a prime number greater than all numbers in $\mathcal{P}$. ■

As an immediate corollary of Lemma 16, and the fact that $Mult_p(x_0, X)$ is a future formula, we get the main result:

Theorem 17 *(1) There is no temporal logic over a finite base which is expressively equivalent to monadic second order logic over natural numbers.*
(2) There is no temporal logic over a finite base which is expressively equivalent to the future fragment of monadic second order logic over natural numbers.

An easy modification of the proof above shows:

Theorem 18 *There is no temporal logic over a finite base which is expressively equivalent to monadic second order logic over the class of finite linear models.*

4 μ-calculus has no Finite Base

We can easily deduce from the previous section that μ-calculus [Koz83, Pra81] has no finite base:

Theorem 19 *There is no temporal logic over a finite base which is expressively equivalent to μ-calculus over the trees.*

Proof. By Niwiński theorem [Niw97], over the naturals, the μ-calculus is equivalent to Rabin's $S1S$ (the monadic second order theory of one successor), which is, in turn, equivalent to the monadic second order theory of order: actually, the successor relation is definable in terms of the order and conversely the order is definable by a monadic second order formula over the successor function. So μ-calculus over the naturals is equivalent to the monadic theory of order, hence it has no finite base, and a fortiori μ-calculus over arbitrary trees has no finite base either. ■

Acknowledgments: We are grateful to the anonymous referees for their fruitful remarks and comments.

References

[BP85] D. Beauquier and D. Perrin. Co-deterministic automata on infinite words. *Inform. Process. Letters*, 20:95–98, 1985.

[Büc60] J.R. Büchi. On a decision method in restricted second order arithmetic. In E. Nagel et al., editor, *Proc. Internat. Congr. on Logic, Methodology and Philosophy of Science*, pages 1–11. Stanford Univ. Press, Stanford CA, 1960.

[CS99] E. Clarke and B.H. Schlingloff. Model checking. In A. Robinson and A. Voronkov, editors, *Handbook on Automated Reasoning*, pages 3–157. Elsevier Science Publishers B.V., 1999.

[EH86] E. A. Emerson and J. Y. Halpern. "Sometimes" and "Not Never" revisited: On branching versus linear time temporal logic. *Journal of the ACM*, 33(1):151–178, 1986.

[GHR94] D. Gabbay, I. Hodkinson, and M. Reynolds. Temporal logic. Oxford University Press, 1994.

[HR99] Y. Hirshfeld and A. Rabinovich. Quantitative temporal logic. pages 172–187. Springer Verlag, 1999. Lect. Notes in Comput. Sci., vol. 1683.

[HR00] Y. Hirshfeld and A. Rabinovich (2000). On the Expressive Power of Temporal Logics over the Reals. *Technical Report*, Tel-Aviv University.

[Kam68] H.W. Kamp. *Tense logic and the theory of linear order.* Phd thesis, University of California, Los Angeles, 1968.

[Koz83] D. Kozen. Results on the propositional μ-calculus. *Theoretical Computer Science*, 27:333–354, 1983.

[MP71] R. McNaughton and S. Papert (1971). Counter-Free Automata. *MIT Press*, 1971.

[Niw97] D. Niwiński. Fixed point characterization of infinite behavior of finite-state systems, Fundamental Study. *Theoretical Computer Science*, 189:1–69, 1997.

[Pnu77] A. Pnueli. The temporal logic of programs. In *Proc. IEEE 18th Annu. Symp. on Found. Comput. Sci.*, pages 46–57, New York, 1977. IEEE.

[Pra81] V. Pratt. A decidable μ-calculus. In *Proc. Ann. ACM Symp. on Foundations of Computer Science (FOCS'81)*, pages 421–427, 1981.

[RM00] A. Rabinovich and S. Maoz. Why so many temporal logics climb up the trees? In *Proc. 25th Int. Symp. Math. Found. Comp. Sci. (MFCS'2000), Bratislava, Slovakia, Aug. 2000*, volume 1893 of *Lecture Notes in Computer Science*, pages 629–639. Springer, 2000.

[She75] S. Shelah (1975). The monadic theory of order. *Annals of Mathematics* **102**:379–419.