Real-Time Logics: Complexity and Expressiveness

by

Rajeev Alur and Thomas A. Henzinger

Departments of Computer Science and Medicine
Stanford University
Stanford, California 94305
Abstract. The theory of the natural numbers with linear order and monadic predicates underlies propositional linear temporal logic. To study temporal logics for real-time systems, we combine this classical theory of infinite state sequences with a theory of time, via a monotonic function that maps every state to its time. The resulting theory of timed state sequences is shown to be decidable, albeit nonelementary, and its expressive power is characterized by w-regular sets. Several more expressive variants are proved to be highly undecidable.

This framework allows us to classify a wide variety of real-time logics according to their complexity and expressiveness. In fact, it follows that most formalisms proposed in the literature cannot be decided. We are, however, able to identify two elementary real-time temporal logics as expressively complete fragments of the theory of timed state sequences, and give tableau-based decision procedures. Consequently, these two formalisms are well-suited for the specification and verification of real-time systems.
Real-time Logics: Complexity and Expressiveness$^{1,2}$

Rajeev Alur
Thomas A. Henzinger
Department of Computer Science
Stanford University

March 15, 1990

Abstract. The theory of the natural numbers with linear order
and monadic predicates underlies propositional linear temporal logic.
To study temporal logics for real-time systems, we combine this
classical theory of infinite state sequences with a theory of time,
via a monotonic function that maps every state to its time. The
resulting theory of timed state sequences is shown to be decidable,
albeit nonelementary, and its expressive power is characterized by
w-regular sets. Several more expressive variants are proved to be
highly undecidable.

This framework allows us to classify a wide variety of real-time
logics according to their complexity and expressiveness. In fact, it
follows that most formalisms proposed in the literature cannot be
decided. We are, however, able to identify two elementary real-time
temporal logics as expressively complete fragments of the theory of
timed state sequences, and give tableau-based decision procedures.
Consequently, these two formalisms are well-suited for the specifi-
cation and verification of real-time systems.

1 Introduction

Linear propositional temporal logic (PTL) has been demonstrated to be a working tool
for the specification and verification of reactive systems ([Pl77],[OL82],
[LP84],[MP89]). Its practical appeal stems from the strong theoretical connec-
tions that PTL, which is interpreted over infinite sequences of states, enjoys with
the underlying classical first-order theory of the natural numbers with linear
order and monadic predicates: PTL captures an elementary, yet expressively

---

$^1$This research was supported in part by an IBM graduate fellowship to the second author,
by the National Science Foundation under grant CCR-8812595, by the Defense Advanced
Research Projects Agency under contract N00019-84-C-0211, and by the United States Air
Force Office of Scientific Research under contracts 880281 and 90-0057.

$^2$An abbreviated version of this paper appears in the proceedings of the 5th Annual IEEE
complete, fragment of this nonelementary theory ([SC85], [GPSS80], [St74]); that is, any property of state sequences expressible in the monadic first-order theory of \((\mathbb{N}, \leq)\) can also be specified in PTL, which has a much simpler decision problem.

PTL admits, however, only the specification of qualitative time requirements, such as an event occurring “eventually.” To enable quantitative reasoning about the timing delays in real-time applications, real-time logics include explicit time references and are interpreted over timed state sequences, which associate a time with every state ([JM86], [Os87], [Ha88], [AH89], [Ko89], [HLPSO]). Even though the suitability as specification language has often been demonstrated, most of these previous attempts remain ad hoc, with little regard to complexity and expressiveness questions.

The prime objective of this paper is to develop a unifying framework for the study of real-time logics. In analogy to the untimed case, we identify the underlying classical theory of timed state sequences, show it to be nonelementarily decidable, and use its complexity and expressiveness as point of reference. We are able to define two orthogonal extensions of PTL that inherit its appeal: they capture elementary, yet expressively complete, fragments of the theory of timed state sequences, and thus are excellent candidates for practical real-time specification languages.

Outline

In Section 2, we define the theory of timed state sequences by combining a theory of state sequences with a theory of time, via a unary monotonic function that maps every state to its time. As for PTL, the monadic first-order theory of \((\mathbb{N}, \leq)\) serves as the theory of states. To model time, we choose the theory of \((\mathbb{N}, \leq, \equiv)\). We show that the resulting combined theory is still decidable, and characterize its expressiveness by w-regular sets.

We claim that this theory of timed state sequences is indeed the theory for reasoning about finite-state real-time systems. All conceivable extensions and variations, like additional primitives over time (such as addition), or a dense time domain, result in highly undecidable (\(\Pi^1_1\)-hard) theories. It follows from our results that none of the real-time logics proposed by [JM86], [Os87], [Ha88], and [Ko89] can be decided, which vividly demonstrates that it has not been understood, so far, how expressive a theory of time may be added, without sacrificing decidability, to reasoning about state sequences.

In [AH89], we proposed timed PTL (TPTL) as a natural specification language, and developed a tableau-based decision procedure. It turns out that TPTL captures precisely the fragment of the theory of timed state sequences obtained by combining PTL (the temporal fragment of the states component) with the quantifier-free fragment of the time component. We argued, in [AH89], that it is this restriction of disallowing quantification over time, what yields readable specifications as well as finite-state-based verification methods. In Section
3 we show it to be both harmless, by proving the expressive completeness of TPTL with respect to the underlying classical theory, and essential, by proving the nonelementary nature of TPTL extended by quantification over time variables.

There are, in fact, second-order versions of all our theorems: the second-order theory of timed state sequences is still decidable, and just as PTL is generalizable to ETL ([Wo83]), TPTL can be extended to be as expressive as this second-order theory, at no cost in complexity.

Surprisingly, the addition of past operators renders TPTL nonelementary. This induces us to introduce, in Section 4, another expressively complete fragment of the theory of timed state sequences, MTL, which includes past operators, but restricts the states that may be related by timing constraints. We present a tableau-based decision procedure for MTL, thus demonstrating its applicability for the verification of real-time systems.

Both TPTL and MTL are, while being elementary, still quite expensive; the respective decision procedures work in doubly exponential time. In Section 5 we show that this cost is, however, intrinsic to real-time reasoning: any reasonably succinct and reasonably expressive extension of PTL is necessarily EXPSPACE-hard. Even the special case of identifying next-time with next-state, which restricts us to reasoning about synchronous systems, is not cheaper.

2 The Theory of Timed State Sequences

Real-time logics are interpreted over timed state sequences. Given a finite set of propositions $P$ and a time domain $\text{TIME}$, a timed state sequence $\rho = (\sigma, \tau)$ is a pair consisting of an infinite sequence $\sigma_i \subseteq P, i \geq 0$, and a map $\tau : \mathbb{N} \to \text{TIME}$ that associates a time with every state. We introduce the classical theory of timed state sequences, show its decidability, and characterize its expressiveness by $\omega$-regular sets.

2.1 The classical theory of state sequences

First, we recapitulate briefly why the theory of the natural numbers with linear order and monadic predicates underlies linear-time propositional temporal logics, which are interpreted over infinite sequences of states.

Let $L^2$ be the second-order language with unary predicate symbols and the binary predicate symbol $\leq$, and let $L$ be its first-order fragment. We interpret $L^2$ over the natural numbers, with $\leq$ being interpreted as the usual linear order. Throughout we consider only formulas that contain no free individual variables. Thus, given a formula $\phi$ of $L^2$ with the free predicate symbols $p_1, \ldots, p_n$, an interpretation $I$ for $\phi$ specifies the sets $p_1^I, \ldots, p_n^I \subseteq \mathbb{N}$. Such an interpretation can be viewed as an infinite sequence $\sigma$ of states $\sigma_i \subseteq \{p_1, \ldots, p_n\}, i \geq 0$ (let
\( p_k \in \sigma, \text{iff } i \in p_k^f \). By \( \mathcal{M}(\phi) \) we denote the set of state sequences that satisfy \( \phi \).

Observe that \( \mathcal{L}^2 \) is essentially the language underlying the theory \( \text{S1S} \), the second-order theory of the natural numbers with successor and monadic predicates. This is because, in \( \text{S1S} \), the order predicate \( \leq \) can be defined from the successor function using second-order quantification (and vice versa). It was first shown by Büchi that the theory \( \text{S1S} \) is decidable ([Bü62]).

Formulas of the propositional linear temporal logic PTL can be faithfully translated into \( \mathcal{L} \), by replacing propositions with monadic predicates. For example, the typical response property that “Every p-state is followed by a q-state,” is expressed in PTL as

\[
\square (p \rightarrow \diamond q).
\]

It can be written in \( \mathcal{L} \) as

\[
\forall i. (p(i) \rightarrow \exists j \geq i. q(j)), \quad (\phi_R)
\]

without changing the set of models.

Although PTL corresponds to a proper subset of \( \mathcal{L} \), it has the full expressive power of \( \mathcal{L} ([\text{Ka68}], [\text{GPSS80}]) \); that is, for every L-formula there is a PTL-formula specifying the same property of state sequences. Furthermore, the validity problem for \( \mathcal{L} \) is nonelementary ([St74]), whereas PTL is only PSPACE-complete ([SC85]), and has a singly exponential decision procedure ([BMP81]).

To attain the greater expressive power of \( \mathcal{L}^2 \), PTL may be strengthened by adding operators that correspond to right-linear grammars ([Wo83]). The resulting logic, extended temporal logic (ETL), has the expressive power of \( \mathcal{L}^2 \), and like PTL, still a singly exponential decision procedure.

The expressiveness of \( \mathcal{L}^2 \) can also be characterized by w-regular expressions ([Mc66], [Th81]): for any formula \( \phi \) of \( \mathcal{L}^2 \), the set \( \mathcal{M}(\phi) \) can be defined by an w-regular expression over the alphabet \( \mathcal{P}(\{p_1, \ldots, p_n\}) \). For example, \( \mathcal{M}(\phi_R) \) is described by the expression

\[
\left[\{p, q\} + \{q\} + \{\{p\}; \text{true}^*; (\{p, q\} + \{q\})\}\right]^\omega.
\]

The restricted expressive power of \( \mathcal{L} \) corresponds to the star-free fragment of w-regular expressions (in which the Kleene star may be applied only to the expression true).

### 2.2 Adding time to state sequences

To obtain a theory of timed state sequences, we need to identify a suitable time domain \( \text{TIME} \), with appropriate primitives, and couple the theory of state sequences with this theory of time through a unary (“time”) function \( f \), which associates a time with every state. We choose, as the theory of time, the theory of the natural numbers (i.e., \( \text{TIME} = \mathbb{N} \)) with linear-order and congruence
primitives. Since the time cannot decrease from one state to the next, we require that \( f \) be monotonic. We will have an opportunity to justify these decisions later.

Let \( L_T^2 \) be a second-order language with two sorts, namely a state sort and a time sort. The vocabulary of \( L_T^2 \) consists of unary predicate symbols and the binary predicate symbol \( \leq \) over the state sort, the unary function symbol \( f \) from the state sort into the time sort, and the binary predicate symbols \( =, \equiv_2, \equiv_3, \ldots \), over the time sort. By \( L_T \) we denote the first-order fragment of \( L_T^2 \).

We restrict our attention to structures that choose the set of natural numbers \( \mathbb{N} \) as domain for both sorts, and interpret the primitives in the intended way. Thus, given a formula \( \phi \) of \( L_T^2 \) with the free predicate symbols \( p_1, \ldots, p_n \), an interpretation \( I \) for \( \phi \) specifies the sets \( p_1', \ldots, p_n' \subseteq \mathbb{N} \) and a monotonic function \( f^I : \mathbb{N} \rightarrow \text{TIME} \). The satisfaction relation is defined as usual. Every interpretation \( I \) for \( \phi \) can be viewed as a timed state sequence \((a, r)\) (choose \( 0 \) as in the untimed case, and let \( r = f^I \)); by \( M_T(\phi) \) we denote the set of timed state sequences that satisfy \( \phi \).

It follows that \( L_T^2 \)-formulas specify properties of timed state sequences. For example, the requirement of bounded response time that “Every \( p \)-state is followed by a \( q \)-state within time 1,” can be written as a formula of \( CT \):

\[
\forall i. (p(i) \rightarrow \exists j \geq i. (q(j) \land f(j) \leq f(i) + 1))
\]

(note that the successor functions, over either sort, are definable in \( L_T \)).

An \( L_T^2 \)-formula \( \phi \) is satisfiable (valid) iff it is satisfied by some (every) timed state sequence. The (second-order) theory of timed state sequences is the set of all valid sentences of \( L_T^2 \). We prove it to be decidable.

### 2.3 Decidability and expressibility

First we show that, given an interpretation \( I \) for an \( L_T^2 \)-formula \( \phi \), the information in \( f^I \) essential for determining the truth of \( \phi \) has finite-state character.

Let us consider the sample formula \( \phi_{BR} \) again. A timed state sequence for \( \phi_{BR} \) specifies, for every state, the truth values of the predicates \( p \) and \( q \), and the value of the time function. Since \( f \) is interpreted as a monotonic function, it can be viewed as a state variable \( f_6 \) recording, in every state, the increase in time from the previous state. Although \( f_6 \) ranges over the infinite domain \( \mathbb{N} \), observe that if the time increases by more than 1 from a state to its successor, then the actual value of the increase is of no relevance to the truth of \( \phi_{BR} \).

Consequently, to determine the truth of \( \phi_{BR} \), the state variable \( f_6 \) can be modeled using a finite number of unary time-difference predicates. We employ the three new predicates \( Tdiff_0, Tdiff_1, \) and \( Tdiff_2 \) in the following way: \( Tdiff_0 \) is true of a state iff the time increase from the previous state is 0, \( Tdiff_1 \) is true iff it is 1, and \( Tdiff_2 \) is true iff it is greater than 1. Accordingly, we define the notion of an extended state sequence for \( \phi_{BR} \), as a state sequence over the
propositions $p$, $q$, $T\text{diff}_0$, $T\text{diff}_1$, and $T\text{diff}_2$ such that precisely one of the propositions $T\text{diff}_0$, $T\text{diff}_1$, and $T\text{diff}_2$ is true in any state.

Given an extended state sequence, we can recover a corresponding timed state sequence: the value of the time function in a $T\text{diff}_t$-state is obtained by adding $t$ to its value in the previous state (if $T\text{diff}_t$ holds in the first state, let $t$ be its time). This establishes a many-to-one correspondence between the timed and the extended state sequences for $\phi_{\text{BR}}$: it induces an equivalence relation on the set of all interpretations for $\phi_{\text{BR}}$ such that the truth of $\phi_{\text{BR}}$ is invariant within any equivalence class. Every equivalence class is, furthermore, definable by a finite number of propositions.

For formulas with congruence primitives, we need to introduce, apart from time-difference predicates, also unary time-congruence predicates, to keep track of the congruence class of the time value of every state. For example, consider the following formula $\psi$, which states that “$p$ is true in every state with an even time value”:

$$\forall i. (f'(i) \equiv_2 0 \rightarrow p(i)).$$

Given an interpretation $I$ for $\psi$, the information in $f'$ can be captured by the two predicates $T\text{congu}_0$ and $T\text{congu}_1$: $T\text{congu}_0$ is true for states with even time, and $T\text{congu}_1$ is true for states with odd time.

Now we formalize this idea. Let $c(\phi)$ be the least common multiple of the set $\{c \mid \exists c \text{ occurs in } \phi\}$, and $d(\phi)$ the product of $c(\phi)$ and $4^Q$, where $Q$ is the number of time quantifiers (i.e., quantifiers over variables of the time sort) occurring in $\phi$.

Given a formula $\phi$ of $L_T^2$ with the free predicate symbols $p_1, \ldots, p_n$, an extended state sequence $J$ for $\phi$ specifies the sets $p_1'^J, \ldots, p_n'^J \subseteq \mathbb{N}$, a partition of $\mathbb{N}$ into the sets $T\text{diff}^J_0, \ldots, T\text{diff}^J_{d(\phi)}$, and another partition of $\mathbb{N}$ into the sets $T\text{congu}_0^J, \ldots, T\text{congu}_{c(\phi)}^J$. For any interpretation $I$ for $\phi$, the extended state sequence $J$ underlying $I$ is defined as follows:

- $J$ agrees with $I$ on $p_1, \ldots, p_n$.
- For $i \geq 0$ and $0 \leq t < d(\phi)$, $i \in T\text{diff}^J_t$ iff $f'(i) = f^I(i - 1) + t$.
- For $i \geq 0$, $i \in T\text{diff}^J_{d(\phi)}$ iff $f'(i) \geq f^I(i - 1) + d(\phi)$.
- For $i \geq 0$ and $0 \leq t < c(\phi)$, $i \in T\text{congu}^J_t$ iff $f'(i) \equiv c(\phi) t$.

(Throughout we use the convention that, for any interpretation $I$, $f^I(-1) = 0$.)

**Lemma [Finite-state character of time].** Given a formula $\phi$ of $L_T^2$ and two interpretations $I$ and $J$ for $\phi$ with the same underlying extended state sequence, $I \in \mathcal{M}_T(\phi)$ iff $J \in \mathcal{M}_T(\phi)$.

**Proof:** Consider two interpretations $I$ and $J$ for the $L_T^2$-formula $\phi$ that have the same underlying extended state sequence; that is, $I$ and $J$ agree on the free predicate symbols of $\phi$, and for each $i \geq 0$, $f'(i)$ and $f'^J(i)$ belong to...
the same congruence class modulo $c(\phi)$, and either $f'(i) = f'(i - 1)$ is the same as $f'(i) - f'(i - 1)$, or both are at least $d(\phi)$.

We use induction on the structure of $\phi$ to prove our claim. To handle subformulas with free variables properly, we need to strengthen our assumptions about the equivalence of interpretations with respect to a formula.

Let $\psi$ be a subformula of $\phi$, possibly with free variables. Let $d(\psi)$ be the product of $c(\phi)$ and $4^Q$, where $Q$ is the number of time variables bound in $\psi$. For ease of presentation, we represent the function $f$ by the countable set of variables $\{f, i_1, i_2, \ldots\}$: for any interpretation $I$, let $f(I) = f'(i)$. By $\text{Tvar}(\psi)$ we denote the union of the set of free time variables of $\psi$ with $\{f, i : i \geq 0\}$. We say that two interpretations $I'$ and $J'$ for $\psi$ are equivalent with respect to $\psi$ iff they satisfy the following conditions:

- For every predicate symbol $q$ free in $\psi$, $q' = q''$.
- For every state variable $i$ free in $\psi$, $i' = i''$.
- For all $x, y \in \text{Tvar}(\psi)$, $x'' \leq y''$ iff $x' \leq y'$.
- For every $x, y \in \text{Tvar}(\psi)$, if $0 \leq x'' - y'' < d(\psi)$, then $x' - y' = x'' - y''$ and vice versa.
- For every $x \in \text{Tvar}(\psi)$, $x' = c(\phi) x''$.

Clearly, the given two interpretations $I$ and $J$ are equivalent with respect to the given formula $\phi$. Thus, it suffices to show that, for any subformula $\psi$ of $\phi$ and equivalent interpretations $I'$ and $J'$ for $\psi$, $I' \models \psi$ implies $J' \models \psi$. We do so by induction on the structure of $\phi$.

The interpretations $I'$ and $J'$ agree on the assignment to predicate symbols and state variables of $\psi$. They may assign different values to the elements in $\text{Tvar}(\psi)$, but they agree on their ordering and modulo-$c(\phi)$ congruence classes. Clearly, if $\psi$ is an atomic formula, then $I' \models \psi$ iff $J' \models \psi$.

The case of boolean connectives is straightforward.

Suppose that $\psi$ is of the form $\exists p. \psi'$, for a predicate symbol $p$, and that $I' \models \psi$. Let $I''$ be an extension of $I'$ such that $I'' \models \psi'$. From the inductive hypothesis, the extension of $J'$ that assigns the set $p''$ to $p$ is a model of $\psi'$. Hence, $J' \models \psi$. The case that $\psi$ is of the form $\forall p. \psi'$ is similar.

If the outermost operator of $\psi$ is a quantifier for a state variable, then we can proceed as in the previous case.

Now consider the case that $\psi$ is of the form $\exists x. \psi'$, for a time variable $x$. Suppose that $I' \models \psi$. Let $I''$ be an extension of $I'$ such that $I'' \models \psi'$. First note that $d(\psi') = c(\phi) \cdot 4^Q - 1$. We extend $J'$ to an interpretation $J''$ for $\psi'$ in the following way: if for some $y \in \text{Tvar}(\psi)$, $|y' - y''| < d(\psi')$, then choose $y''$ to be $y' + z'' - y'$. Otherwise, let $y_1, y_2 \in \text{Tvar}(\psi)$ be such that $y_1' < y'' < y_2'$. Note that $y_2' - y_1''$ is at least $d(\psi')$, and hence, so is $y_2' - y_1'$. We choose $z''$, between $y_1'$ and $y_2'$ at a distance at least $d(\psi')$ from either of
them. Furthermore, since the difference between $d(\psi)$ and $2d(\psi')$ is at least $c(\phi)$, we can require the modulo-$c(\phi)$ congruence class of $z''$ to be the same as that of $z'$. Now $I'$ and $J''$ satisfy the requirements listed above. Using the inductive hypothesis, $J'' \models \psi'$, and hence, $J' \models \psi$. The case of universal quantification is similar.

It follows that the extended state sequence underlying a given interpretation for a $L_2^2$-formula $\phi$ has enough information for deciding the truth of $\phi$. Consequently, every formula $\phi$ can be viewed as characterizing a set $M_T(\phi)$ of satisfying extended state sequences, instead of a set of satisfying timed state sequences. Our next task is to show that this set is $\omega$-regular. This is achieved by constructing a formula in the language $L_2^2$ that is satisfied by the same extended state sequences.

For instance, the extended state sequences that satisfy $\phi_{BR}$ are the same as the models of the following formula:

$$\forall i. \left[ p(i) \rightarrow \exists j \geq i. \left( q(j) \land \left( \forall k. \left( i < k \leq j \rightarrow T\text{diff}_0(k) \right) \lor \exists k. \left( i < k \leq j \land T\text{diff}_1(k) \land \forall k'. \left( i < k' \leq j \rightarrow T\text{diff}_0(k') \right) \right) \right) \right]$$

**Theorem [Regular nature of the time primitives].** Given a formula $\phi$ of $L_2^2$, there exists a formula $\psi$ of $L^2$, with additional time-difference predicates $T\text{diff}_0, \ldots, T\text{diff}_d(\phi)$ and time-congruence predicates $T\text{cong}_0, \ldots, T\text{cong}_{c(\phi)-1}$, such that $M_T(\phi) = M(\psi)$. Furthermore, if $\phi \in L_2^2$ then $\psi \in L$.

**Proof:** Given an $L_2^2$-formula $\phi$, we construct an equivalent (with respect to extended state sequences) $L_2^2$-formula $\psi$ in four steps.

First, we eliminate all time quantifiers. Let $I$ be an interpretation for $\phi$, and $t = d(\phi) + c(\phi)$. We can easily find an interpretation $J$ with the same underlying extended state sequence, such that $f^J(i) \leq f^J(i-1) + t$ for all $i \geq 0$. By the previous lemma, we know furthermore that $J \models \phi$ iff $I \models \phi$. Based on this observation we perform the following transformation: a subformula $\exists y. \psi(y)$, where $y$ is a time variable, is replaced by the disjunction

$$\forall p. \psi(k) \lor \exists i. \bigvee_{k=0}^t \psi(f(i) + k),$$

for a new state variable $i$. Let $\phi'$ be the formula obtained from $\phi$ by applying the above transformation repeatedly until there are no time quantifiers left; clearly $M_T(\phi) = M_T(\phi')$.

The second step, resulting in $\phi''$, models the primitive time arithmetic of comparisons and addition by constants by the time-difference predicates. For instance, consider the subformula $f(i) + 1 \leq f(j)$, for state variables $i$ and $j$. Intuitively, for $f(i)$ to be less than $f(j)$ in any interpretation, state $i$ has to
precede state \( j \), and the time increase from the previous state has to be positive for some intermediate state. Hence, we replace the subformula by

\[ (i < j) \land 3k. \ (i < k \leq j \land \neg T_{\text{diff}}(k)). \]

Similarly, \( f(i) \leq f(j) \) and \( f(i) \leq f(j) + 1 \) can be replaced by

\[ \forall k. \ (i < k \leq i \rightarrow T_{\text{diff}}(k)) \] (\( \phi_0 \))

and

\[ \phi_0 \lor \exists k. \ (i < k \leq i \land T_{\text{diff}}(k) \land \forall k' \neq k. \ (j < k' \leq i \rightarrow T_{\text{diff}}(k'))) \]

respectively. The generalization to subformulas of the form \( f(i) + c \leq f(j) \) and \( f(i) \leq f(j) + c \), for arbitrary \( c > 1 \), is straightforward.

In a third step, we model the congruence primitives of \( \phi'' \) with the help of the time-congruence predicates. Consider a subformula of the form \( f(i) + c \equiv_d f(j) \). Since there is only a finite number of \( \text{modulo-c}(\phi) \) congruence classes to which \( f(i) \) and \( f(j) \) can belong, we can use a case analysis to express this relationship. We replace the subformula by

\[ \bigwedge_{k=1}^{d} \bigvee_{k'=1}^{c/\phi/d} T_{\text{cong}}(k + dk' \mod c(\phi))(i) \leftrightarrow \bigvee_{k'=1}^{c/\phi/d} T_{\text{cong}}(k + dk' \mod c(\phi))(j) \] (\( \phi''' \))

Subformulas of the form \( f(i) \equiv_d c \) can be handled similarly.

Let \( \phi''' \) be the formula resulting from eliminating all time primitives in the described way. The desired \( \mathcal{L}^2 \)-formula \( \psi \) is obtained by adding, to \( \phi''' \), the following conjuncts:

- For every state \( i \geq 0 \), precisely one of the time-difference predicates \( T_{\text{diff}}(0) \cdots T_{\text{diff}}(d(\phi)) \) is true.
- For every state \( i \geq 0 \), exactly one of the time-congruence predicates \( T_{\text{cong}}(0) \cdots T_{\text{cong}}(c(\phi)-1) \) is true.
- For all \( i \geq 0 \), the congruence classes of \( i \) and \( i + 1 \), and the time jump \( f(i + 1) = f(i) \) are related in a consistent fashion:

\[ \forall i. \ \bigwedge_{k=0}^{d(\phi)-1} \bigwedge_{k'=0}^{c(\phi)-1} (T_{\text{diff}}(k)(i + 1) \land T_{\text{cong}}(k)(i) \rightarrow T_{\text{cong}}(k+k' \mod c(\phi))(i + 1)) \]

The above theorem, combined with the earlier stated facts about \( \mathcal{L}^2 \), gives the following important results regarding the decidability and expressiveness of the theory of timed state sequences.
Corollary [Decidability]. The validity problem for the language $L_T$ is decidable.

Clearly, the validity problem is nonelementary even for the first-order language $L$, as $L$ is a fragment of $L_T$ (recall that $L$ was shown to be nonelementary in [St74]).

Corollary [Expressiveness]. Given a formula $\phi$ of $L_T$ with the free predicate symbols $p_1, \ldots, p_n$, the set $M_T^+(\phi)$ can be characterized by an $\omega$-regular expression over the alphabet

$$\mathcal{P}(\{p_1, \ldots, p_n\}) \times \{T\text{diff}_{1}, \ldots, T\text{diff}_{d(\phi)}\} \times \{T\text{con}_{0}, \ldots, T\text{con}_{c(\phi)-1}\}$$

Furthermore, if $\phi \in L_T$ then $M_T^+(\phi)$ can be defined by a star-free $\omega$-regular expression.

2.4 Undecidable extensions and variants

Now we justify our choice of $(N, \leq, \equiv)$ as the theory of time, by showing that several formalisms for real-time reasoning with an expressive power greater than that of $L_T$ are highly undecidable. In [AH89], we proved the $\Pi_1^1$-completeness of certain syntactic and semantic variants of the real-time temporal logic TPTL. Here, these results are refined, extended, and presented in the framework of the theory of timed state sequences.

Theorem [Undecidable theories of real time]. The following two-sorted first-order theories are $\Pi_1^1$-complete:

<table>
<thead>
<tr>
<th></th>
<th>state theory</th>
<th>time theory</th>
<th>time function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$(N, \leq)$</td>
<td>$(N, +1)$</td>
<td>$f$</td>
</tr>
<tr>
<td>2</td>
<td>$(N, \leq)$</td>
<td>$(N, \cdot 2)$</td>
<td>identity $f$</td>
</tr>
<tr>
<td>with monadic predicates</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>$(N, \leq)$</td>
<td>dense linear order $(D, \leq)$</td>
<td>strictly monotonic $f$</td>
</tr>
<tr>
<td>with monadic predicates</td>
<td></td>
<td>with “successor” $S$: $S(x) &lt; S(y)$</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>$(N, \leq)$</td>
<td>$(N, +1)$</td>
<td>identity $f$</td>
</tr>
<tr>
<td>with monadic predicates</td>
<td></td>
<td></td>
<td>st rictly monotonic $f'$</td>
</tr>
</tbody>
</table>

Proof: First, we observe that the satisfiability of a formula $\phi$ can, in all cases, be phrased as a $\xi$-sentence, asserting the existence of a model for $\phi$. For instance, in Case 2, an interpretation $I$ for $\phi$ may be encoded, in first-order arithmetic, by finitely many sets of natural numbers; say, one for each unary predicate $p$ in $\phi$, characterizing the states for which $p$ holds. It is routine to express, as a first-order formula, that $\phi$ holds in $I$. In Case 3, the Löwenheim-Skolem theorem
ensures the existence of countable models, and again, elementary arithmetic can be used to encode (and decode) such models. Thus satisfiability problem is in \( \Sigma_1^1 \) in each case.

Now let us prove \( \mathcal{E} \)-hardness. The problem of deciding whether a nondeterministic Turing machine has, over the empty tape, a computation in which the start state is visited infinitely often, is known to be \( \Sigma_1^1 \)-complete ([HPS83]). For ease of encoding, we prove our results using 2-counter machines instead of Turing machines.

A **nondeterministic 2-counter machine** \( M \) consists of two counters \( C \) and \( D \), and a sequence of \( n \) instructions, each of which may increment or decrement one of the counters, or jump, conditionally upon one of the counters being zero. After the execution of a non-jump instruction, \( M \) proceeds nondeterministically to one of two specified instructions.

We represent the configurations of \( M \) by triples \( (I, c, d) \), where \( 0 \leq l < n \), \( c \geq 0 \), and \( d \geq 0 \) are the current values of the location counter and the two counters \( C \) and \( D \), respectively. The consecution relation on configurations is defined in the obvious way. A **computation** of \( M \) is an infinite sequence of related configurations, starting with the initial configuration \( (0, 0, 0) \). It is called recurring iff it contains infinitely many configurations with the value of the location counter being 0.

The problem of deciding whether a given nondeterministic 2-counter machine has a recurring computation, is \( \Sigma_1^1 \)-hard ([AH89]). Thus, to show that the satisfiability problem of a language is \( \Sigma_1^1 \)-hard, it suffices, given a nondeterministic \( a \)-counter machine \( M \), to construct a formula \( \phi_M \) such that \( \phi_M \) is satisfiable iff \( M \) has a recurring computation.

**\( \Sigma_1^1 \)-hardness** of Case 1: We show that the **monotonicity** constraint on time is necessary for the decidability of \( \mathcal{L}_T \); otherwise, the time map can be used to encode (and decode) computations of \( M \). We write a formula \( \phi_M \) all of whose models correspond to recurring computations of \( M \). A computation \( \Gamma \) of \( M \) is encoded by the interpretation \( \Pi \), for all \( i \geq 0 \), \( f^I(3i) = l \), \( f^I(3i + 1) = n + c \), and \( f^I(3i + 2) = n + d \) for the \( i \)-th configuration \( (l, c, d) \) of \( \Gamma \).

First, specify the initial configuration, by

\[
\begin{align*}
    f(0) &= 0 \quad \text{A} \quad f(1) = n \quad \text{A} \quad f(2) = n. \quad (\phi_{\text{INIT}})
\end{align*}
\]

Then ensure proper consecution by adding a conjunct \( \phi_i \) for every instruction \( 0 \leq i < n \) of \( M \). For instance, the instruction 1 that increments the counter \( C \) and proceeds, nondeterministically, to either instruction 2 or 3, contributes the conjunct

\[
\begin{align*}
    &\forall i. \quad f(i) = 1 \rightarrow \left( \begin{array}{l}
        f(i + 3) = 2 \lor f(i + 3) = 3 \quad \text{A} \\
        f(i + 4) = f(i + 1) + 1 \land \\
        f(i + 5) = f(i + 2)
    \end{array} \right) \quad (\phi_1)
\end{align*}
\]
The recurrence condition can be expressed by the formula
\[ \forall i. \exists j \geq i. f(j) = 0. \]  
(\(\phi_{\text{RECUR}}\))

Clearly, the conjunction \(\phi_M\) of these \(n + 2\) formulas is satisfiable iff \(M\) has a recurring computation.

Note that \(\phi_M\) uses only the successor primitive over time, and no unary predicates. Case 1 follows.

Xi-hardness of Case 2: We show that a certain extremely modest relaxation of the timing constraints admitted in \(L_T\), namely allowing the primitive of multiplication by 2 over the time domain, leads to Xi-hardness. This result holds even under the restriction that the time function \(f\) is the identity function; that is, “time” acts merely as a state counter.

To encode computations of \(M\), we use the unary predicates \(p_1, \ldots, p_n, r_1, r_2\). We require that at most one of these predicates is true of any state; hence we may identify states with predicate symbols. The configuration \((I, c, d)\) of \(M\) is represented by the finite sequence of states that starts with a \(p_1\)-state, and contains precisely \(c\) \(r_1\)-states and \(a\) \(r_2\)-states.

The initial configuration as well as the recurrence condition can be expressed easily. The crucial property that allows a language to specify the consecution relation of configurations, and thus the set of computations of \(M\), is the ability to copy an arbitrary number of \(r\)-states. With the availability of multiplication by 2, we are able to have the \(i\)-th configuration of a computation correspond, for all \(i \geq 0\), to the finite sequence of states that is mapped to the time interval \([2^i, 2^{i+1})\). Then we can copy groups of \(r\)-states by establishing a one-to-one correspondence of \(r\)-states at time \(t\) and time \(2t\); clearly there are enough gaps to accommodate an additional \(r\)-state when required by an increment instruction.

For instance, the instruction 1 that increments the counter \(C\) and proceeds, nondeterministically, to either instruction 2 or 3, can be expressed as follows:

The consequent of the implication ensures that, given the configuration of \(M\) that is encoded by the states with times in the interval \(I_1 : [f(i), 2f(i)]\), the states with times in \(I_2 : [2f(i), 4f(i)]\) encode the configuration that results from
executing instruction 1. The first conjunct updates the location counter. The second conjunct requires \( I_2 \) to contain at least as many \( r_1 \)-states as \( I_1 \); together with the third conjunct it assures that \( I_2 \) has precisely one \( r_1 \)-state more than \( I_1 \). The last two conjuncts together state that the number of \( r_2 \)-states in \( I_2 \) is the same as in \( I_1 \).

**Et-hardness of Case 3:** Now we attempt to model time over a dense domain \( TIME \equiv D \); that is, between any two given time points there is another time point. We show that even the simple arithmetic of linear order \((\leq)\) and addition by a constant \((S)\) leads to a highly undecidable theory. Examples for \((D, \leq, S)\) are the rational numbers \((Q, \leq, +)\), and the reals.

As in the previous case, we employ the predicates \( p_1, \ldots, p_n, r_1, \) and \( r_2 \): a configuration \( (l, c, d) \) of \( M \) is encoded by the state sequence \( p_1 r_1^c d \). The proof depends, once more, on the ability to copy groups of \( r \)-states. This time, we are able to have the \( i \)-th configuration of a computation of \( M \) correspond, for all \( i \geq 0 \), to the finite sequence of states that is mapped to the time interval \([S^i(0), S^{i+1}(0)]\), for some arbitrary element \( 0 \in D \), because the denseness of the domain allows us to squeeze arbitrarily many states into any non-empty interval.

Since every state has a unique time, and we can establish a one-to-one correspondence of \( r_j \)-states \((j = 1, 2)\) at time \( t \) and time \( S(t) \); the formula defining the recurring computations of \( M \) can be obtained from the formula constructed in Case 2, simply by replacing the operation \( \cdot 2 \) by \( S \).

**Xi-hardness of Case 4:** This case corresponds to having two time bases, \( f \) and \( f' \), that are updated, from one state to the next, independently of each other. The result holds already for the special case in which \( f \) is the identity function, and \( f' \) is strictly increasing.

The encoding of \( M \)-computations is very similar to the one used in Case 2; the \( i \)-th configuration of \( M \) corresponds to the sequence of \( 2^i \) states in the interval \([2^i, 2^{i+1})\). The assertion language does not include the primitive of multiplication by \( 2 \), which can, however, be simulated with the help of the second time function \( f' \). We restrict ourselves to interpretations in which \( f'(i) = 2i \) for all \( i \geq 0 \). This condition is enforced by the conjunct

\[
f'(0) = 0 \land \forall i. (f'(i + 1) = f'(i) + 2).
\]

By replacing, in the formula constructed in Case 2, every term of the form \( 2f(i) \) by \( f'(i) \), we obtain again a formula encoding the recurring computations of \( M \).

Let us consider the implications of these results on developing logics for real-time systems, which justify our decisions in the choice of \( L^2_T \).

The fact that the monotonicity constraint on the time function is required for decidability (Case 1) has little consequences in the context of real-time logics, since we are interested only in monotonic time functions anyway.
When designing a real-time logic we need to select an appropriate domain for modeling time. Ideally, for asynchronous systems, where changes in the global state of the system can be arbitrarily close in time, we would like to choose a dense linear order. Since the ordering predicate and addition by constant time values are the basic primitives needed to express the simplest of timing constraints, the undecidability of the resulting theory (Case 3) is a major stumbling block in the design of useful logics over dense time. For example, the real-time (branching-time) logics considered in [AD90] and [Le90] use the set of real numbers to model time, and hence are undecidable.

Having constrained ourselves to a discrete time domain, we need to choose the operations on time admitted in the logic. While previous works have used addition as one of the primitives, the above theorem (Case 2) shows that it introduces undecidability. Using our results and techniques, we can show the undecidability (in fact, \( \Pi^1_1 \)-hardness) of various real-time logics proposed earlier, such as [JM86], [Os87], [Ha88], and [Ko89], all of which include addition. In [HLPS0], decidability is proved for a real-time logic with addition; this logic puts, however, substantial restrictions on the use of time quantifiers.

The real-time logic RTL ([JM86]) can be viewed as a two-sorted logic with multiple monotonic functions from the state sort to the time sort. Our result (Case 4) implies that RTL is undecidable, even if we restrict its syntax to allow only the successor primitive over time (RTL allows addition over time).

On the other hand, we have shown that the congruence primitives over time can be added to the language without sacrificing decidability. Furthermore, we have proved decidability for the second-order case as well. Thus we claim that the first-order theory of \((\mathbb{N}, \leq)\) with monadic predicates (for state sequences) combined with the theory of \((\mathbb{N}, \leq, \Xi)\) (for time) is the theory of timed state sequences.

3 Timed Temporal Logic: TPTL

In [AH89], we introduced an extension of PTL that is interpreted over timed state sequences. We developed a tableau-based decision procedure and model-checking algorithm for this timed propositional temporal logic (TPTL), thus demonstrating its suitability for the verification and synthesis of real-time systems.

In this section, we study the expressiveness of TPTL. We compare the properties of timed state sequences expressible in TPTL with those expressible in the underlying classical language \( \mathcal{L}_T \). TPTL is shown to correspond to an expressively complete fragment of \( \mathcal{L}_T \); that is, the set of models of any \( \mathcal{L}_T \)-formula can be characterized by a TPTL-formula. This result is important as it establishes TPTL as a sufficiently expressive specification language; it shows that the gains in complexity in moving from the full first-order theory of timed state sequences (nonelementary) to TPTL (doubly exponential) are not achieved.
at the cost of expressive power.

We also look at two natural extensions of TPTL that correspond to larger fragments of $\mathcal{L}_T$ and, therefore, are still decidable. However, both generalizations turn out to be nonelementary, thus affirming our choice of TPTL as verification formalism. TPTL can, on the other hand, be generalized to attain the full expressiveness of the second-order language $\mathcal{L}_T^2$, at no cost in complexity.

3.1 Syntax and semantics

We briefly recall the definition of TPTL. This real-time temporal logic is obtained from PTL by adding a time quantifier “$\exists.$” that binds the associated variable $x$ to the “current” time: $x. \phi(x)$ holds at state $\sigma_i$ of the timed state sequence $(\sigma, \tau)$ iff $\phi(\tau(i))$ does. For example, in the formula Ox. $\phi$, the time reference $x$ is bound to the time of the state at which $\phi$ is “eventually” true.

This extension of PTL with references to the times of states admits the addition of timing constraints; that is, atomic formulas that relate the times of different states. The formulas of TPTL are built from propositions and timing constraints by connectives, temporal operators, and time quantifiers. For instance, the typical bounded response property that “Every p-state is followed by a q-state within time 1” can be stated as

$$\Box x. (p \rightarrow o_y. (q \land y \leq z + 1)).$$

Let us be more precise. Given a set $P$ of proposition symbols and a set $V$ of variables, the terms $\pi$ and formulas $\phi$ of TPTL are inductively defined as follows:

- $\pi ::= z \mid c \mid z + c$
- $\phi ::= p \mid \pi_1 \leq \pi_2 \mid \pi_1 = \pi_2 \mid \pi_1 \equiv_d \pi_2 \mid \text{false} \mid \phi_1 \rightarrow \phi_2 \mid \Diamond \phi \mid \phi_1 \lor \phi_2 \mid x. \phi$

for $x \in V$, $p \in P$, $c \geq 0$, and $d \geq 2$. Additional temporal operators such as $0$ (eventually) and $\bullet$ (always) are defined in terms of $\Diamond$ (next) and $\lor$ (until) as usual.

The formulas of TPTL are interpreted over timed state sequences. The timed state sequence $\rho = (\sigma, \tau)$ satisfies $\phi$ iff $(p, 0) \models_\rho \phi$ for the initial environment $E_0: V \rightarrow \{\tau(0)\}$, where the truth predicate $\models_\rho$ is inductively defined as follows:

$^3$TPTL as originally defined in [AH89] differs syntactically in that the time quantifiers are coupled with the temporal operators. Observe that this coupling does not restrict us in any essential way: by separating the time quantifier “$z.$” from the temporal operators, we admit more formulas (such as $\Box x. (z.4 \rightarrow z. \psi)$), for each of which there is, however, an equivalent formula in which every quantifier follows a temporal operator ($\Box x. (\phi \rightarrow \psi)$).

$^4$In [AH89], timed state sequences are required to satisfy the two additional conditions of initiality ($z = 0$) and progress ($\Box z. o_y. y > z$). These requirements make sense for any time specification language, but we have just demonstrated that they are expressible within TPTL itself.
• \((\rho, i) \models \varepsilon \ p \iff p \in \sigma_i\)

• \((\rho, i) \models \varepsilon \ \pi_1 \leq (\exists \varepsilon) \ \pi_2 \iff \varepsilon(\pi_1) \leq (\exists \varepsilon) \ \varepsilon(\pi_2),\)
  for \(\varepsilon(x + c) = \varepsilon(x) + c\) and \(\varepsilon(c) = c\)

• \((\rho, i) \not\models \varepsilon \ false\)

• \((\rho, i) \models \varepsilon \ \phi_1 \rightarrow \phi_2 \iff (\rho, i) \models \varepsilon \ \phi_1 \implies (\rho, i) \models \varepsilon \ \phi_2\)

• \((\rho, i) \models \varepsilon \ \bigcirc \phi \iff (\rho, i + 1) \models \varepsilon \ \phi\)

• \((\rho, i) \models \varepsilon \ \phi_1 \ \mathcal{U} \ \phi_2 \iff (p, j) \models \varepsilon \ \phi_2\)
  for some \(j \geq i\), and \((p, k) \models \varepsilon \ \phi_1\) for all \(i \leq k < j\)

• \((\rho, i) \models \varepsilon \ \exists \ v \ \phi \iff (\rho, i) \models \varepsilon[\varepsilon(v)/x] \ \phi\).

(Here \(\varepsilon[t/x]\) denotes the environment that agrees with \(\varepsilon : V \rightarrow \text{TIME on all variables except } x\), which is mapped to \(t \in \text{TIME}\).) Note that every TPTL-formula is equivalent to its closure, in which all free variables are bound by a prefix of time quantifiers.

Every TPTL-formula \(\phi\) can be translated into \(\mathcal{L}_T\), while preserving the set of models \(\mathcal{M}_T(\phi)\). For every proposition \(p\) of TPTL, we have a corresponding unary state predicate \(p(i)\) of \(\mathcal{C}_T\). A closed TPTL-formula \(\phi\) is true over a timed state sequence \(\rho\) iff the \&-formula \(F_0(\phi)\) is true over \(\rho\), where \(F_i\) (for \(i \geq 0\)) is inductively defined as follows:

• \(F_0(p) = p(i)\)

• \(F_i(\pi_1 \leq \pi_2) = \pi_1 \leq \pi_2, \ F_i(\pi_1 \equiv \pi_2) = \pi_1 \equiv \pi_2\)

• \(F_i(\text{false}) = \text{false}, \ F_i(\phi_1 \rightarrow \phi_2) = F_i(\phi_1) \rightarrow F_i(\phi_2)\)

• \(F_i(\bigcirc \phi) = F_{i+1}(\phi)\)

• \(F_i(\phi_1 \ \mathcal{U} \ \phi_2) = \forall i \geq i. (F_j(\phi_2) \ \forall i \leq k < \sigma \Rightarrow F_k(\phi_1))\)

• \(F_i(\exists \ v \ \phi) = F_i(\phi)[f(i)/x]\).

(We write \(\phi[f(i)/x]\) for the formula that is obtained from \(\phi\) by replacing all free occurrences of \(x\) by \(f(i)\).)

For example, the bounded response property \(\phi_{BR}\) is equivalent to its translation \(F_0(\phi_{BR})\):

\[V i \geq 0. \ (p(i) \rightarrow \exists j \geq i. \ (q(j) \land f(j) \leq f(i) + 1))\].

Note that the mapping \(F_0\) embeds TPTL into \(\mathcal{L}_T\); its range constitutes a proper subset of all well-formed \(\mathcal{L}_T\)-formulas. Thus, just as PTL corresponds to a subset of \(\mathcal{L}\), we may view TPTL as a fragment of \(\mathcal{L}_T\): quantification over the state sort is restricted to the “temporal” way of PTL, while quantification over the time sort is prohibited entirely.
3.2 Expressiveness

In [AH89] we have shown that, in a pleasing analogy to PTL versus C, TPTL constitutes in fact an elementary fragment of CT: the satisfiability of a given TPTL-formula with N logical and temporal connectives, and K as the product of its constants, can be decided in time $2^{O(NK)}$. To complete this analogy, we show here that the restrictions imposed by TPTL on the quantification in CT-formulas do not diminish its expressive power. In other words, any property of timed state sequences that can be specified in $\mathcal{L}_T$ can already be specified in TPTL.

The natural embedding $F_0$ gives, for any TPTL-formula $\phi$, an equivalent CT-formula $F_0(\phi)$, thus demonstrating that $\mathcal{L}_T$ is as expressive as TPTL. By the following theorem, the converse is also true.

**Theorem [Expressive completeness of TPTL].** For every formula $\phi$ of $\mathcal{L}_T$, there exists a formula $\psi$ of TPTL such that $\mathcal{M}_T(\phi) = \mathcal{M}_T(\psi)$. ■

Proof: Given a CT-formula $\phi$, we construct an equivalent TPTL-formula $\psi$ in four steps. By the theorem on the regular nature of the time primitives we obtain an C-formula $\phi'$, with additional time-difference predicates $T_{\text{diff}}$, and time-congruence predicates $T_{\text{cong}}$, such that $\mathcal{M}_T(\phi) = \mathcal{M}('\phi$'). By the expressive completeness of PTL, there is a PTL-formula $\phi''$ such that $\mathcal{M}(\phi'')$ equals $\mathcal{M}(\phi'')$ ([GPSS80]).

We transform $\phi''$ into an equivalent PTL-formula $\phi'''$ such that every time-difference proposition $T_{\text{diff}}$ is either not within the scope of any temporal operator, or immediately preceded by a $\text{next}$ operator. This can be done by repeatedly rewriting subformulas of the form $\bigcirc(\phi_1 \rightarrow \phi_2)$ and $\phi_1 \bigcirc \phi_2$, to $\bigcirc\phi_1 \rightarrow \bigcirc\phi_2$ and $\phi_1 \bigcirc \phi_2 \lor (\phi_1 \land (\bigcirc\phi_1) \bigcirc (\bigcirc\phi_2))$, respectively.

Define the constants $d(\phi)$ and $c(\phi)$ as in Section 2.3. From $\phi'''$ we arrive at $\psi$ by replacing every time-difference proposition $T_{\text{diff}}$ that is not within the scope of a temporal operator by $x. x = t \land (x. x \geq t, \text{if } t = d(\phi))$, every subformula $\bigcirc T_{\text{diff}}$ by $x. \bigcirc y. y = x + t \land (x. \bigcirc y. y \geq x + t, \text{if } t = d(\phi))$, and every time-congruence proposition $T_{\text{cong}}$ by $x. x \equiv t$. ■

We conclude the discussion of properties expressible in TPTL by interpreting the logic over pure (“timeless”) state sequences, and investigating the expressive power of the congruence relations.

3.2.1 Timeless expressiveness

With every TPTL-formula $\phi$ we can associate a set of state sequences by projecting the timed state sequences in $\mathcal{M}_T(\phi)$. Given a state sequence $\sigma$ and a TPTL-formula $\phi$, let $\sigma \in \mathcal{M}_T(\phi)$ iff there is a time map $\tau$ such that $(a, \tau) \models \phi$.

Interpreted in this fashion, TPTL can specify strictly more properties of state sequences than PTL. For example, the property even(p), that “p holds in every even state,” is not expressible in pure PTL ([Wo83]). In TPTL, we may
(ab)use time to identify the even states as precisely those in which the time does not increase:

\[ \Box y. z = y \land \Box z. \Box y. (x = y \rightarrow p \land \Box z. (z > y \land \Box u. u = z)). \]

The following theorem shows that the expressive power of TPTL with respect to state sequences is that of the second-order language \( L^2 \), or equivalently, \( \omega \)-regular expressions.

**Theorem [Timeless expressiveness of TPTL].** For every formula \( \phi \) of TPTL, there is a formula \( \psi \) of \( L^2 \) such that \( \mathcal{M}_L(\phi) = \mathcal{M}(\psi) \), and vice versa. \( \blacksquare \)

**Proof:** Given a TPTL-formula \( \phi \), we know how to construct an equivalent \&-formula \( \phi' \). By the theorem on the regular nature of the time primitives we obtain an L-formula \( \phi'' \), with additional time-difference predicates \( T_{\text{diff}} \) and time-congruence predicates \( T_{\text{cong}} \), such that \( \mathcal{M}_L(\phi') = \mathcal{M}(\phi'') \). The \( L^2 \)-formula \( \psi \) that binds all of the new time predicates in \( \phi'' \) by an existential prefix is easily seen to have the desired models.

In order to show the second implication, we use a normal-form theorem for \( L^2 \): given an \( L^2 \)-formula \( \psi' \), there is an equivalent \( L^2 \)-formula \( \psi'' \) of the form

\[ \exists p_1 \ldots \exists p_n. \psi_M' \],

whose matrix \( \psi_M' \) contains no second-order quantifiers ([Bu62]). We construct a TPTL-formula \( \phi \) that characterizes the models of \( \psi'' \), by using the (existentially quantified) time map to encode the interpretation of the unary predicates \( p_j \) (1 ≤ j ≤ n), which are bound in \( \psi'' \).

Assign to every subset \( J \subseteq \{1, \ldots, n\} \) a unique code \( t \in \text{TIME} \). By the expressive completeness of PTL, \( \mathcal{M}(\psi_M') = \mathcal{M}(\psi''_M) \) for some PTL-formula \( \psi''_M \). From \( \psi''_M \), we obtain \( \phi \) by replacing every proposition \( p_j \), 1 ≤ j ≤ n, by \( z. \Box y. \bigvee_{j \in J} (y = x + t) \). It is straightforward to establish a one-to-many correspondence between the models \( I = (\sigma, p_1', \ldots, p_n') \) of \( \psi''_M \) and the timed state sequences (a, \( \tau \)) satisfying \( \phi \): given \( I \), let \( \tau(i + 1) = \tau(i) + t \) such that \( J_t = \{j \mid p_j'(i)\} \), and given \( \tau \), let \( p_j'(i) \) iff \( j \in J_{\tau(i) - \tau(i)} \) (assume that \( j \notin J_t \) if \( t \) is no proper code). \( \blacksquare \)

It follows that \( L_T \), with the time function existentially quantified, has the full expressive power of the second-order language \( L^2 \). In fact, the proof given above shows that equality and successor over the time sort are sufficient to achieve this timeless expressiveness.

### 3.2.2 Expressive power of congruences

If we disallow the use of congruence relations in TPTL, the resulting logic is strictly less expressive. Consider the following formula \( \phi \):

\[ \text{ax.} \ (x \equiv_2 0 \rightarrow p). \]

It characterizes the timed state sequences in which \( p \) is true at all even times. We show that this property is not **expressible** without congruence relations.
Suppose that the TPTL-formula $\psi$, which does not contain any congruence relations, were equivalent to $\phi$. Let $c$ be the largest constant occurring in $\psi$. It is easy to convince yourself that $\psi$ cannot distinguish between the timed state sequences $\rho_1 = (a, \lambda_i. (c + 1))$ and $\rho_2 = (\sigma, \lambda_i. (c + 2))$, for any $\sigma$. Yet if $p$ is continuously false in $\sigma$, only one of $\rho_1$ and $\rho_2$ satisfies $\phi$.

Note that TPTL without congruence relations has the same expressive power as the first-order language $\mathcal{L}_T$ without congruences. However, as has been pointed out in the previous subsection, the congruence primitives do not affect the “timeless” expressiveness of these formalisms: for example, we have demonstrated that the property that “$p$ holds in every even state” (as opposed to every state with an even time) can be specified without congruences.

3.3 Nonelementary extensions

We have seen that TPTL restricts $\mathcal{L}_T$ to “temporal” quantification over the state sort and no quantification over the time sort. Can we relax these restrictions without sacrificing elementary decidability? Arbitrary quantification over the state sort encompasses full $\mathcal{L}$ and is, therefore, clearly nonelementary. In the following subsection, we study the generalization of TPTL that admits quantification over the time sort, and show it to be nonelementary as well.

Then we try to add past temporal operators to TPTL, an extension that does not affect the complexity of pure PTL. Therefore it is quite surprising that the past operators render TPTL nonelementary.

3.3.1 TPTL with quantification over time

Several authors, such as [Os87] and [Ha88], have proposed to use first-order temporal logic with a single dynamic (state) variable, $T$, that represents the time in every state, for the specification of real-time properties. For instance, they write our typical bounded response property $\phi_{BR}$ from above essentially as

$$\forall x. (p \land T = x \rightarrow \diamond (q \land T \leq z + 1)),$$

using auxiliary rigid (global) variables like $x$ to refer to the time (i.e., the value of $T$) of different temporal contexts.

Eliminating the state variable $T$, we see that this notation corresponds to TPTL extended by classical universal and existential first-order quantification over time:

$$\forall y. \forall x. (p \land y = x \rightarrow oz. (q \land z \leq z + 1)).$$

We call this generalization of TPTL, whose syntax definition is supplemented by the new clause “If $\phi$ is a formula and $x \in V$, then $\exists z. \phi$ is also a formula,” quantified TPTL or $\text{TPTL}_3$. Given a timed state sequence $\rho$, an index $i \geq 0$, and an environment $\mathcal{E}$, the classical quantifiers are interpreted as usual:

$$(\rho, i) \models_\mathcal{E} 3x. \phi \iff (\rho, i) \models_\mathcal{E}[t/z] \phi \text{ for some } t \in \text{TIME}.$$
$TPTL_3$ seems, on the surface, more expressive than $TPTL$, because it can state properties of times that are not associated with any state. But it is easy to see that $TPTL_3$ can still be embedded into $L_T$ (let $F_i(\exists z. \phi) = 3x. F_i(\phi)$). The satisfiability of $TPTL_3$ is, therefore, decidable, and its expressive power, measured as the sets of timed state sequences specifiable in the logic, is the same as that of $TPTL$.

We show that $TPTL_3$ is, however, not elementarily decidable. This provides additional justification for our preference for $TPTL$ over the existing notation with first-order quantifiers over time; prohibiting quantification over time not only leads, as argued in [AH89], to a more natural specification language, but is necessary for the existence of feasible verification methods, such as the tableau techniques for $TPTL$.

Theorem [Complexity of $TPTL_3$]. The satisfiability problem of $TPTL_3$ is nonelementary. ⊢

Proof: We translate the nonelementary monadic first-order theory of $(N, \leq)$ ([St74]) into $TPTL_3$: by forcing the time to act as a state counter (using $\exists z. F(z \geq x) = F(z + 1)$), state quantifiers can be simulated by the time quantifiers of $TPTL_3$.

Given a formula $\phi$ of $\mathcal{L}$, we construct a formula $\psi$ of $TPTL_3$ such that $\phi$ is satisfiable iff the conjunction of $\psi$ and $\exists z. Oy. y = x + 1$ is satisfiable. The formula $\psi$ is obtained from $\phi$ by replacing every atomic subformula of $\exists z. x$ form $p(i)$ by $Ox. (p A x = i)$ (read the quantifiers of $\phi$ as quantifiers over the time sort). ⊢

3.3.2 TPTL with past

In [LPZ85], PTL is extended with the past temporal operators $\oplus$ (previous) and $\mathcal{S}$ (since), the duals of $\Box$ and $\mathcal{U}$. These operators can be added at no extra cost, and although they do not increase the expressive power of PTL, they allow a more direct and convenient expression of certain properties.

Let $TPTL_P$ be the logic that results from $TPTL$ by adding the following clause to the inductive definition of formulas: “If $\phi_1$ and $\phi_2$ are formulas, then so are $\oplus \phi_1$ and $\phi_1 S \phi_2$.” The meaning of the past operators is given by

- $(\rho, i) \models \Box \phi \text{ iff } i = 0 \text{ or } (\rho, i - 1) \models \phi$, and
- $(\rho, i) \models \phi_1 S \phi_2 \text{ iff } (\rho, j) \models \phi_2 \text{ for some } j \leq i \text{ and } (\rho, k) \models \phi_1 \text{ for all } j < k \leq i$.

Clearly, $TPTL_P$ can still be embedded into $L_T$:

- $F_0(\Box \phi) = \text{true}$, $F_{i+1}(\Box \phi) = F_i(\phi)$
- $F_i(\phi_1 S \phi_2) = \exists j \leq i. (F_j(\phi_2) \land \forall j < k \leq i. F_k(\phi_1))$. 

20
Hence the satisfiability of this logic is, again, decidable, and its expressive power is no greater than that of TPTL.

However, unlike in the case of PTL, there is a surprisingly heavy price to be paid for adding the past operators.

**Theorem [Complexity of TPTLₚ]**. The satisfiability problem of TPTLₚ is nonelementary.

**Proof**: Again, we are able to use the nonelementary nature of the monadic first-order theory of \((\mathbb{N}, \leq)\). By adopting time as a state counter, we can simulate true existential quantification over time by 0, because \(\Diamond\) allows us to restore the correct temporal context.

Given a formula \(\phi\) of \(\mathcal{L}\), we construct a formula \(\psi\) of TPTLₚ such that \(\phi\) is satisfiable if and only if the conjunction of \(\Box z. \bigcirc y. y = x + 1\) is satisfiable. The first step in translating \(\phi\) is the same as in the proof of the nonelementary complexity of TPTL₃. In a second step we replace every subformula of the form \(3x. \varphi\) by \(3x. \varphi\).

### 3.4 Timed ETL

PTL does not have the full expressive power of the second-order language \(\mathcal{L}^2\); recall that the property \(even(p)\), that \(p\) is true in every even state,

\[
\exists q. [q(0) \land \forall i. (q(i) \rightarrow p(i) \land \neg q(i + 1) \land q(i + 2))]
\]

is not expressible in PTL ([Wo83]). That is why Wolper has defined extended temporal logic (ETL), which includes a temporal operator for every right-linear grammar. ETL has the same expressiveness as \(\mathcal{L}^2\), or equivalently, w-regular expressions, and yet a singly exponential decision procedure.

The situation for TPTL is similar: there is no TPTL-formula whose models are precisely the timed state sequences in which, independent of the time map, \(p\) holds at every even state.

Suppose there were such a formula \(\phi\); we show that this would imply the expressibility of \(even(p)\) in \(\mathcal{L}\). First construct an &\(\phi\)' that is equivalent to \(\phi\) and contains the additional time-difference and time-congruence predicates \(T_{\text{diff}}\) and \(T_{\text{cong}}\), as usual. Then replace, in \(\phi\)', all occurrences of \(T_{\text{diff}}\) and \(T_{\text{cong}}\), by true or false depending on whether \(t = 0\). This simplification does not affect the truth of the formula over interpretations all of whose times are permanently 0. Thus, the resulting formula \(\psi\) is satisfied by a state sequence \(\sigma\) iff \((\sigma, \lambda i. 0) \in \mathcal{M}_T(\phi)\); that is, iff \(p\) is true in every even state of \(\sigma\).

However, analogously to PTL, we are able to generalize TPTL to timed extended temporal logic, TETL, by introducing temporal grammar operators. TETL is shown to have the full expressive power of \(\mathcal{L}_T^2\), while being no more expensive than TPTL.
3.4.1 Syntax and semantics

Given a set $P$ of propositions symbols and a set $V$ of variables, the terms of TETL are the same as in TPTL. The formulas of TETL are inductively defined as follows:

$$\phi := p \mid \tau_1 \leq \tau_2 \mid \tau_1 \equiv_d \tau_2 \mid \text{false} \mid \phi_1 \rightarrow \phi_2 \mid \mathcal{G}(\phi_1, \ldots, \phi_m) \mid z. \phi$$

where $z \in V$, $p \in P$, $d \geq 2$, and $\mathcal{G}(a_1, \ldots, a_m)$ is a right-linear grammar with the $m$ terminal symbols $a_1, \ldots, a_m$.\(^5\)

As with TPTL, TETL-formulas are interpreted over timed state sequences. Given a timed state sequence $\rho$, an index $i \geq 0$, and an environment $\mathcal{E}$, the semantics of the grammar operators is defined by the following clause:

$$(\rho, i) \models \mathcal{E} \mathcal{G}(\phi_1, \ldots, \phi_m)$$

iff there is a (possibly infinite) word $w = a_{w_1}, a_{w_2}, \ldots$ generated by $\mathcal{G}(a_1, \ldots, a_m)$ such that

$$(\rho, i + j) \models \mathcal{E} \phi_{w_j}, \text{ for all } j \geq 0.$$ All temporal operators of TPTL are expressible by the grammar operators of TETL; for example, the TPTL-operator $\square$ corresponds to the grammar $\mathcal{G}_\square(a)$ with the only production $\mathcal{G}_\square(a) \rightarrow a \mathcal{G}_\square(a)$ (we identify grammars with their starting nonterminal symbols). The formula even($p$), which is not expressible in TPTL, can be stated as $\mathcal{G}_{\text{even}}(\text{true}, p)$, for the production

$$\mathcal{G}_{\text{even}}(a_1, a_2) \rightarrow a_1 a_2 \mathcal{G}_{\text{even}}(a_1, a_2).$$

3.4.2 Complexity

By putting together the tableau methods for ETL ([Wo83]) and TPTL ([AH89]), we develop a doubly-exponential-time decision procedure for TETL. This procedure is near-optimal; we go on to show the satisfiability problem for TETL to be EXPSPACE-complete.

Our presentation follows [AH89] closely.\(^6\) For the sake of keeping the presentation simple, we assume that all grammar operators correspond to productions of the form

$$\mathcal{G}(a_1, \ldots, a_m) \rightarrow a_1 [a_2 \mathcal{G}'(a_{j_1}, \ldots, a_{j_n})].$$

Furthermore, all TETL-formulas contain a single free variable, $T$ (which refers to the initial time), and only timing assertions of the forms $x \leq y + c$, $x + c \leq y$, and $x \equiv_d y + c$, for $d > c \geq 0$. This can be achieved by renaming of variables, and easy simplifications.

\(^5\)Like ETL, TETL can alternatively be defined using automata connectives for all Büchi-automata, instead of grammar operators ([WVS83]).

\(^6\)The careful reader may have noticed that we use, throughout, time-difference propositions $T \Delta \delta i$, that indicate the time increase $t$ from the predecessor states, as opposed to [AH89], where these propositions represent the time difference to the successor states. This is necessary, because we have relaxed the initiality condition $\tau(0) = 0$ on timed state sequences $(\sigma, \tau)$.
As with TPTL, for checking the satisfiability of a given TETL-formula \( \phi \), we may restrict ourselves to timed state sequences \( \rho = (a, \tau) \) all of whose time steps \( \tau(i + 1) - \tau(i), i \geq 0 \), are bounded by the product \( K \) of all constants occurring in \( \phi \) (a constant \( c > 0 \) occurs in \( \phi \) iff \( \phi \) contains a subformula of the form \( x \leq y + (c - 1) \) or \( x + (c - 1) \leq y \), or the predicate symbol \( \equiv_c \)). The time information in \( \rho \) has, therefore, finite-state character; it can be modeled by the new propositions \( T_{\text{diff}_t}, 0 \leq t \leq K \), representing the time differences \( t \) between successive states.

This allows us to modify the tableau-based decision procedure for ETL ([Wo83]), to handle formulas with time references. It is, in fact, included in our procedure as the special case in which \( \phi \) contains no timing constraints.

The key observation underlying all tableau methods for temporal logics is that any formula can be split into two conditions: a present requirement on the initial state and a future requirement on the rest of the model. For example, the eventuality \( \Diamond \phi \) can be satisfied by either \( \phi \) or \( \Box \Diamond \phi \) being true in the initial state.

In order to propagate the requirement on the successor state properly, all timing constraints need to be updated to account for the time increase \( t \) from the initial state to its successor. Consider the formula \( \Box \phi(T) \), and recall that the free occurrences of \( T \) are references to the initial time. This condition is true in the initial state iff the next state satisfies the updated formula \( \phi(T - t) \).

If the number of conditions generated in this way is finite, checking for satisfiability is reducible to checking for satisfiability in a finite structure, the initial tableau. For \( t > 0 \), a naive replacement of \( T \) by \( T - t \) would, however, successively generate infinitely many new formulas. Fortunately, the monotonicity of time can be exploited to keep the tableau finite; the observation that \( x \) is always instantiated, in the “future,” to a value greater than or equal to \( T \), allows us to simplify timing assertions of the form \( T \leq x + c \) and \( x + c \leq T \) to true and false, respectively.

We define, therefore, the formula \( \phi^f \) that results from updating all time references \( T \) in \( \phi \), inductively as follows: \( \phi^0 = \phi \); and \( \phi^{t+1} \) is obtained from \( \phi^t \) by replacing all terms of the form \( T + c \) (for \( c > 0 \)) by \( T + (c - 1) \), and all subformulas of the form \( T \leq x + c \), \( x + c \leq T \), and \( T \equiv_d x + c \) (for \( c \geq 0 \)) by true, false, and \( T \equiv_d x + ((c + 1) \mod d) \), respectively.

Now let us collect all conditions that may arise by recursively splitting a formula into its present and future parts. The closure \( \text{Cl}(\phi) \) of a TETL-formula \( \phi \) is the smallest set containing \( \phi \) that is closed under the following operation \( \text{Sub} \):

- \( \text{Sub}((\psi_1 \rightarrow \psi_2)) = \{\psi_1, \psi_2\} \)
- \( \text{Sub}(\Box \psi) = \{\psi^t | 0 \leq t \leq K\} \)
- \( \text{Sub}(G(\psi_1, \ldots, \psi_m)) = \{\psi_1, \psi_2, \Box G'(\psi_j, \ldots, \psi_{j+n})\} \)
Let $N$ be the number of connectives, quantifiers, and grammar operators in $\phi$, where every grammar operator is counted as the number of nonterminal symbols in the corresponding grammar. By induction on the structure of $\phi$, it can be shown that $|Cl(\phi)| \leq 2N \cdot K$.

Tableaux for TETL are finite, directed state graphs (Kripke structures) with local and global consistency constraints on all states. The states are represented by consistent sets of formulas that are closed under “subformulas,” expressing conditions on the current state and the successor states. Every state contains, in addition, a proposition $Tdiff_t$, $0 \leq t \leq K$, which denotes the time difference to the predecessor states.

Formally, we define the states as the maximally consistent subsets of the finite universe

$$Cl'(\phi) = Cl(\phi) \cup \{ Tdiff_t | 0 \leq t \leq K \}$$

of TETL-formulas. The set $\Phi \subseteq Cl'(\phi)$ is (maximally) consistent iff it satisfies the following conditions (where all formulas range only over $Cl'(\phi)$):

- $Tdiff_t \in \Phi$ for precisely one $t$ with $0 \leq t \leq K$; this $t \in TIME$ is referred to as $Lastdiff(\Phi)$.
- $false \notin \Phi$.
- $\psi_1 \rightarrow \psi_2 \in \Phi$ iff either $\psi_1 \notin \Phi$ or $\psi_2 \in \Phi$.
- $\bigwedge(\psi_1, \ldots, \psi_m) \in \Phi$ iff either $\psi_1 \in \Phi$, or both $\psi_i \in \Phi$ and $\bigcirc \bigwedge(\psi_2, \ldots, \psi_n) \in \Phi$.
- $z. \psi(z) \in \Phi$ iff $\psi(T) \in \Phi$.
- $T \sim T + c \in \Phi$ iff $0 \sim c$ holds in $N$ (for $\sim$ one of $\leq$, $\geq$, $\equiv$, or its negation).

Now we are ready to define the initial tableau in a way that ensures the global consistency of both temporal and real-time constraints as well. The initial tableau $T(\phi)$ for the TETL-formula $\phi$ is a directed graph whose vertices are the consistent subsets of $Cl'(\phi)$, and which contains an edge from $\Phi$ to $\Psi$ iff, for all $\bigcirc \psi \in Cl(\phi)$,

$$\bigcirc \psi \in \Phi \iff \psi^{Lastdiff(\Psi)} \in \Psi.$$
path $\Phi_0 \Phi_1 \Phi_2 \ldots$ such that $\phi \in \Phi_0$ and, for every $i \geq 0$, $-G(\psi_1, \ldots, \psi_m) \in \Phi_i$ implies that $-G(\psi_1, \ldots, \psi_m)$ is fulfillable along $\Phi_i \Phi_{i+1} \ldots \Phi_k$ for some $k \geq i$.

This result suggests a decision procedure for TETL: construct the initial tableau, and employ the usual, polynomial techniques for checking whether the tableau contains an infinite path along which all eventualities are satisfied. Since the initial tableau contains $O(K \cdot 2^{NK})$ states, each of size $O(N \cdot K)$, $T(\phi)$ can be constructed and checked for infinite paths in deterministic time exponential in $O(N \cdot K)$.

**Theorem [Deciding TETL].** The satisfiability of a TETL-formula $\phi$ is decidable in deterministic time exponential in $O(N \cdot K)$, where $N$ is the number of connectives, quantifiers, and grammar operators in $\phi$, and $K$ is the product of all constants occurring in $\phi$ (recall that every grammar operator is counted as the number of nonterminal symbols in the corresponding grammar). $\blacksquare$

Note that the length $L$ of a formula whose constants are represented in binary, is $O(N + \log K)$. So we have a decision procedure for TETL that is doubly exponential in $L$ (although only singly exponential in $N$, the “untimed” part, and thus, singly exponential for ETL).

The algorithm outlined here may be improved along the lines of [Wo83] to avoid the construction of the entire initial tableau. This does not, however, lower the doubly exponential deterministic-time bound; in fact, TETL is EXPSPACE-hard.

**Theorem [Complexity of TETL].** The satisfiability problem of TETL is EXPSPACE-complete. $\blacksquare$

**Proof:** To show that TETL is in EXPSPACE, we follow the argument that ETL is in PSPACE, which develops a nondeterministic version of the tableau decision procedure and then applies Savitch’s theorem ([Wo83]). EXPSPACE-hardness follows immediately from the corresponding result for TPTL ([AH89]). $\blacksquare$

### 3.4.3 Expressiveness

Although TETL is no harder than TPTL, we have demonstrated that its expressiveness is strictly greater, by specifying the property even(p). The following theorem characterizes the expressiveness of TETL as equivalent to the second-order language $\mathcal{L}_T^2$.

**Theorem [Expressiveness of TETL].** For every formula $\phi$ of TETL, there exists a formula $\psi$ of $\mathcal{L}_T^2$ such that $\mathcal{M}_T(\phi) = \mathcal{M}_T(\psi)$, and vice versa. $\blacksquare$

**Proof:** We extend the translation $F_0$ that embeds TPTL into $\mathcal{L}_T$ to accommodate the grammar operators of TETL; the target formulas will contain second-order quantifiers over unary predicates, and thus belong to $\mathcal{L}_T^2$.

Again, assume that all grammar operators correspond to productions of the form

$$G(a_1, \ldots, a_m) \rightarrow a_i \mid a_i \cdot G'(a_j, \ldots, a_k).$$
We add the following clause to the definition of $F_k \ (k \geq 0)$:

$$F_k(G_0(\phi_1, \ldots, \phi_m)) = \exists p_{G_0} \ldots \exists p_{G_M} \ (p_{G_k}(k) \wedge \forall k' \geq k \ \wedge \ \phi_{G_k}(k'))$$

for some new unary predicate symbols $p_{G_0}, \ldots, p_{G_M}$, where $G_0, \ldots, G_M$ are all the nonterminal symbols occurring in the grammar $G_0(a_1, \ldots, a_s)$, and $\phi_{G_k}(k)$ stands for the $L_2^+$-formula

$$p_{G}(k) \rightarrow F_k(\phi_1) \lor (F_k(\phi_{i_2}) \land p_{G'}(k + 1)).$$

Consider an arbitrary timed state sequence $\rho$. We show, by induction on the structure of $\phi$, that $(\rho, k) \models E \phi$ iff $(\rho, k) \models E F_k(\phi)$ for all $k \geq 0$ and environments $E$.

The crucial case that $\phi$ has the form $G_0(\phi_1, \ldots, \phi_m)$ is derived as follows. To establish the existence of appropriate predicates $p_{G_i}$, let $p_{G_i}$ be true in state $k' \geq k$ iff $(\rho, k') \models E G_i(\phi_1, \ldots, \phi_m)$. On the other hand, given the predicates $p_{G_i}$ satisfying $\phi_{G_i}(k')$ for all $k' \geq k$, we can construct a word $w = a_{i_1}a_{i_2}a_{i_3} \ldots$ generated by $G_0(a_1, \ldots, a_m)$ such that $(\rho, k') \models E \phi_{G_{i_1}a_{i_2}a_{i_3}}$.

It follows that, for any TETL-formula $\phi$, the $L_2^+$-formula $F_0(\phi)$ is equivalent to $\phi$. The argument for the expressive completeness of TETL with respect to $L_2^+$ is analogous to the corresponding proof for TPTL and $L_2$ (use the expressive completeness of ETL with respect to $L_2^+$).

Let us complete the expressibility picture by a few remarks. The timeless expressiveness of TETL is clearly again that of the second-order language $L_2^+$, and thus no more than that of TPTL. It is also immediate that the congruence relations contribute even to the expressive power of TETL (and $L_2^+$) in a non-trivial way; the property that $\rho$ is true at all even times is still not expressible without congruence relations.

### 3.4.4 TPTL with quantification over propositions

There are several alternatives to the grammar operators of ETL. PTL can be extended by fixed-point operators (obtaining a variant of the propositional $\mu$-calculus of [Ko82]) or second-order quantification over propositions (QPTL of [Si83]) in order to achieve the full expressive power of $L_2^+$. While fixed-points can be viewed as generalized grammar operators and yield to tableau methods, QPTL is nonelementary.

It is straightforward to show that both extensions have, indeed, the expected, analogous effect in the TPTL-framework; they give decidable real-time specification languages with the expressiveness of $L_2^+$. However, timed QPTL is, as a superset of QPTL, nonelementary, and thus unsuitable as a verification formalism.
4 Metric Temporal Logic: MTL

Several authors have tried to adapt temporal logic to reason about real-time properties by interpreting its modalities as bounded operators. For example, [Ko89] suggests the notation $\diamond_{<c}$ to express “eventually within time $c$.” Similar temporal operators that are subscripted with constant bounds are used in [Ha88] and [EMSS89].

In this section, we extend PTL by such bounded temporal operators and interpret the resulting logic over timed state sequences. For example, the typical bounded response property that “Every $p$-state is followed by a $q$-state within time $1$” will be written as $q(p \rightarrow \diamond_{<1} q)$.

It is easy to see that we have, in-fact, only obtained a notational variant of a subset of TPTL (rewrite every subformula $\diamond_{<c} \phi$ as $x$. $Oy$. $(y < x + c \wedge \phi)$).

We show that this formalism is interesting—and worth studying in its own right, for two reasons. First, and surprisingly, it is already as expressive as full TPTL. And secondly, it may, unlike full TPTL, be enriched by past operators, thus resulting in what we call (following [Ko89]) metric temporal logic (MTL), without sacrificing its elementary decidability.

Hence we are able to conclude that MTL represents, again, a suitable specification and verification formalism: just like TPTL, MTL corresponds to an expressively complete and yet elementary fragment of $\mathcal{L}_T$ with a tableau-based decision procedure. But the two subsets of $\mathcal{L}_T$ corresponding to TPTL and MTL, respectively, are not identical; either one of them can state certain properties more directly and succinctly than the other one, and may therefore be preferred for some specifications.

4.1 Syntax and semantics

Given a set of propositions $P$, the formulas $\phi$ of MTL are defined inductively as follows:

$$\phi := p \mid \text{false} \mid \phi_1 \rightarrow \phi_2 \mid \diamond_{<c} \phi \mid \Diamond_{<c} \phi \mid \phi_1 \mathcal{U}_{<c} \phi_2 \mid \phi_1 S_{<c} \phi_2$$

for $p \in P$, $\sim$ being one of $<, =, >$, or $\equiv_d$, and $c \geq 0$, $d \geq 2$. The defined operators $\Diamond_{<c} \phi$ and $\Box_{<c} \phi$ stand for $\text{true} \mathcal{U}_{<c} \phi$ and $\neg \Box_{<c} \neg \phi$, respectively; other abbreviations include $\Diamond_{>c} \phi$ (for $\Diamond_{=c} \phi \vee \Diamond_{>c} \phi$) and unbounded $0$ (for $\Diamond_{\geq 0}$).

The formulas of MTL are interpreted over timed state sequences. Instead of giving MTL its own semantics, we translate any MTL-formula $\phi$ into a TPTL$_P$-formula $G(\phi)$ (let $\sim$ stand for $<, >, =$):

- $G(p) = p$
- $G(\text{false}) = \text{false}$, $G(\phi_1 \rightarrow \phi_2) = G(\phi_1) \rightarrow G(\phi_2)$
- $G(\Diamond_{<c} \phi) = z. G(y. (z \sim z + c \wedge \phi))$, $G(\Box_{=c} \phi) = G(y. (y \equiv_d c \wedge \phi))$
\[ G(\bigwedge_{<} \phi) = x \bigwedge y. (x \sim y + c \land \phi), \quad G(\bigwedge_{\leq} c \phi) = \bigwedge y. (y \equiv d c \land \phi) \]

\[ G(\phi_1 U_{<} \phi_2) = \bigwedge y. (\phi_1 U y. (y \sim x \land c \land \phi_2)) \]

\[ G(\phi_1 U_{\equiv} c \phi_2) = \phi_1 U y. (y \equiv d c \land \phi_2) \]

\[ G(\phi_1 S_{<} \phi_2) = \bigwedge y. (\phi_1 S y. (z \sim y + c A 42)) \]

\[ G(\phi_1 S_{\equiv} c \phi_2) = \phi_1 S z. (z \sim y \land \phi_2) \]

Note that \( \bigwedge_{=3} p \) holds in a state if \( p \) is true in some future state whose time is 3 greater than the current time. However, \( \bigwedge_{\equiv 1} p \) holds in a state if \( p \) is true in some future state whose time is odd; the congruence subscripts refer to the absolute times of states.

It follows that both TPTL and MTL are orthogonal fragments of TPTL and, hence, \( L_T \): while TPTL prohibits past operators, MTL corresponds to a subset of TPTL wherein all timing constraints relate only variables that refer to "adjacent" temporal contexts.

### 4.2 Complexity

We show that the satisfiability problem of MTL is much simpler than the corresponding nonelementary problem of full TPTL, by generalizing the standard tableau-decision procedure for PTL ([BMP81]) to MTL.

The tableau algorithm for MTL uses the techniques developed for TPTL in [AH89]. The crucial property that guarantees the finiteness of the tableau being constructed is that, in both cases, the temporal precedence between any two temporal contexts related by a timing constraint is uniquely determined. Before giving a formal definition, we indicate first how the algorithm proceeds for a sample input.

Suppose that the time increases by one unit from a state to its successor (in general, the time increase between states can be bounded for any given formula, and thus reduced to a finite number of different cases). In order to satisfy, say, \( \bigwedge_{<c} \phi \) in the current state, we have to satisfy either \( \phi \) now, or \( \bigwedge_{<c-1} \phi \) in the succeeding state. Continuing this splitting of requirements into a present and a future part, we will eventually arrive at \( 0_{<1} \phi \), forcing \( \phi \) to be satisfied in the current state.

Since every input formula \( \psi \) generates only a finite number of requirements on states in the described fashion, \( \psi \) is satisfiable iff it is satisfiable in a finite tableau. By bounding the maximal size of this tableau, we obtain the following result.

**Theorem [Deciding MTL].** The satisfiability of an MTL-formula \( \phi \) can be decided in deterministic time exponential in \( O(C \cdot N) \), where \( N \) is the number of propositional and temporal connectives in \( \phi \), and \( C - 1 \) is the largest constant occurring, as a subscript, in \( \phi \).
Proof: Throughout, let $\sim$ stand for $<, >,$ or $=.$ Define the closure $Cl(\phi)$ of the MTL-formula $\phi$ to be the smallest set containing $\phi$ that is closed under the following operation $Sub$:

- $Sub(\psi_1 \rightarrow \psi_2) = \{\psi_1, \psi_2\}$
- $Sub(\bigcirc_{\sim_c} \psi) = \{\psi\}$
- $Sub(\bigotimes_{\sim_c} \psi) = \{\psi\}$
- $Sub(\psi_1 \bigcup_{c} \psi_2) = \{\psi_1, \psi_2, \bigcirc(\psi_1 \bigcup_{c'} \psi_2) \mid 0 \leq c' < c\}$
- $Sub(\psi_1 \bigcap_{c} \psi_2) = \{\psi_1, \psi_2, \bigcirc(\psi_1 \bigcap_{c'} \psi_2) \mid 0 \leq c' \leq c\}$
- $Sub(\psi_1 \bigcup_{c} \psi_2) = \{\psi_1, \psi_2, \bigcirc(\psi_1 \bigcap_{c} \psi_2)\}$

If $C_{\sim}$ is the largest constant occurring in $\phi,$ and $N$ is the number of connectives (propositional and temporal) in $\phi,$ then $|Cl(\phi)| \leq 2^C \cdot N.$

As in TPTL, for checking the satisfiability of $\phi,$ we may restrict ourselves to timed state sequences $\rho = (\sigma, \tau)$ all of whose time steps $\tau(i + 1) - T(i), \ i \geq 0,$ are bounded by the product $K$ of all constants occurring, as subscripts, in $\phi$ (count a subscript of the form $\equiv_d c$ as $d$). The time information in $\rho$ has, therefore, finite-state character; it can be modeled by the new propositions $T\text{diff}_i$ and $T\text{cong}_\cdot,$ $0 \leq \cdot \leq K$ and $0 \leq t' < K,$ representing, in any state, the time difference $\cdot$ from the predecessor state and the remainder $t'$ modulo $K$ of the current time. For ease of presentation we use, in addition, the propositions $T\text{diff}'_i,$ $0 \leq \cdot \leq K,$ to represent the time difference $\cdot$ to the successor state.

Let $Cl'(\phi)$ denote the set obtained from $Cl(\phi)$ by adding the new propositions $T\text{diff}_i,$ $T\text{diff}'_i,$ and $T\text{cong}_\cdot.$ A subset $\Phi$ of $Cl'(\phi)$ is called (maximally) consistent iff it satisfies the following conditions (where all formulas range only over the finite set $Cl'(\phi)$):

- $T\text{diff}_i \in \Phi$ for exactly one $\cdot$ with $0 \leq \cdot \leq K; \ this \ \cdot \in TIME$ is referred to as $\text{Lastdiff}(\Phi)$.
- $T\text{diff}'_i \in \Phi$ for exactly one $\cdot$ with $0 \leq \cdot \leq K; \ this \ \cdot \in TIME$ is referred to as $\text{Neztdiff}(\Phi)$.
- $T\text{cong}_\cdot \in \Phi$ for exactly one $\cdot$ with $1 \leq \cdot \leq K; \ this \ \cdot \in TIME$ is referred to as $\text{Congclass}(\Phi)$.
- false $\notin \Phi$.
- $s_1 \rightarrow s_2 \in \Phi$ iff either $s_1 \notin \Phi$ or $s_2 \in \Phi.$
- $s_1 \bigcup_{c} s_2 \in \Phi$ iff either $c = 0$ and $s_2 \in \Phi,$ or $s_1 \in \Phi,$ $\text{Neztdiff}(\Phi) \leq c,$ and $\bigcirc(s_1 \bigcup_{c} \text{Neztdiff}(\Phi) s_2) \in \Phi.$
$\psi_1 \cup_{< c} \psi_2 \in \Phi$ iff $\psi_2 \in \Phi$, or $\psi_1 \in \Phi$, $\text{Neztdiff}(\Phi) < c$, and $\bigcirc (\psi_1 \cup_{< c - \text{Neztdiff}(\Phi)} \psi_2) \in \Phi$.

- $\psi_1 \cup_{> c} \psi_2 \in \Phi$ iff $\psi_1 \in \Phi$, and either $\text{Neztdiff}(\Phi) \leq c$ and $\bigcirc (\psi_1 \cup_{> c - \text{Neztdiff}(\Phi)} \psi_2) \in \Phi$, or $\text{Neztdiff}(\Phi) > c$ and $\bigcirc (\psi_1 \cup \psi_2) \in \Phi$.

- $\psi_1 \cup_{\equiv c} \psi_2 \in \Phi$ iff either $\text{Congclass}(\Phi) \equiv_d c$ and $\psi_2 \in \Phi$, or $\psi_1 \in \Phi$ and $\bigcirc (\psi_1 \cup_{\equiv c} \psi_2) \in \Phi$.

Similar conditions are put on the $S$-formulas in $\Phi$, to ensure their consistency with $\text{Lastdif}f(\Phi)$.

The initial tableau $T(\phi)$ for the MTL-formula $\phi$ is a directed graph whose vertices are the consistent subsets of $\text{Cl}'(\phi)$, and which contains an edge from $\Phi$ to $\Psi$ iff all of the following conditions are met:

- $\text{Neztdiff}(\Phi) = \text{Lastdif}f(\Psi)$.
- $\text{Congclass}(\Psi) \equiv_{K} \text{Congclass}(\Phi) + \text{Neztdiff}(\Phi)$.
- For all $\bigcirc_{\equiv c} \psi \in \text{Cl}(\phi)$, $\bigcirc_{\equiv c} \psi \in \Phi$ iff $\psi \in \Phi$ and $\text{Neztdiff}(\Phi) \sim c$.
- For all $\bigcirc_{\equiv c} \psi \in \text{Cl}(\phi)$, $\bigcirc_{\equiv c} \psi \in \Phi$ iff $\psi \in \Phi$ and $\text{Congclass}(\Psi) \equiv_d c$.
- For all $\bigcirc_{\equiv c} \psi \in \text{Cl}(\phi)$, $\bigcirc_{\equiv c} \psi \in \Psi$ iff $\psi \in \Phi$ and $\text{Neztdiff}(\Phi) \sim c$.
- For all $\bigcirc_{\equiv c} \psi \in \text{Cl}(\phi)$, $\bigcirc_{\equiv c} \psi \in \Phi$ iff $\psi \in \Phi$ and $\text{Congclass}(\Psi) \equiv_d c$.

It follows that an MTL-formula $\phi$ is satisfiable iff the initial tableau $T(\phi)$ contains an infinite path $\Phi = \Phi_0 \Phi_1 \Phi_2 \ldots$ such that

- $\phi \in \Phi_0$,
- $\Phi_0$ contains no $Q$-formula,
- for all $i \geq 0$, $\psi_1 \cup_{\equiv c} \psi_2 \in \Phi_i$ implies $\psi_2 \in \Phi_j$ for some $j \geq i$ with $\Sigma_{k \leq j} \text{Neztdiff}(\Phi_k) \sim c$, and
- for all $i \geq 0$, $\psi_1 \cup_{\equiv c} \psi_2 \in \Phi_i$ implies $\psi_2 \in \Phi_j$ for some $j \geq i$ with $\text{Congclass}(\Phi_j) \equiv_{d} c$.

The proof is similar to the corresponding argument for TPTL ([AH89]).

Since the initial tableau contains $O(\bar{K} \cdot 2^{C \cdot N})$ states, each of size $O(C \cdot N)$, $T(\phi)$ can be constructed and checked for infinite paths in deterministic time exponential in $O(C \cdot N)$.

Note that although the (worst-case) running time of the tableau algorithm is slightly faster for MTL than for TPTL (for which the product of all constants appears in the exponent), it is still doubly exponential in the length of the input formula. In fact, both formalisms are EXPSPACE-complete.
Theorem [Complexity of MTL]. The satisfiability problem for MTL is EXPSPACE-complete.

Proof: From a nondeterministic version of the tableau algorithm, it follows that MTL is in EXPSPACE. The corresponding lower bound can be shown similarly to the analogous result for TPTL, by simulating EXPSPACE-bounded Turing machines ([AH89]).

4.3 Expressiveness

Because of the past operators, MTL can express certain properties more succinctly than TPTL. On the other hand, consider the following TPTL-formula (“Every p-state is followed by a q-state and, later, an r-state within time 5”):

\[ \square (p \rightarrow \Diamond(q \land (\exists t. (r \land (t \leq 5))))). \]

This property has no natural expression in MTL. However, because of the discrete nature of the underlying time domain, it can be translated into MTL as follows:

\[ \square (p \rightarrow \bigvee_{c=0}^{5} (q \land (\exists t. (r \land (t \leq 5 + c)))). \]

In fact, we show that the expressiveness of MTL is no less than that of TPTL in any crucial way. Only properties that put constraints on the time of the initial state, such as “The time of the initial state is 2” (x = 2 in TPTL), are not expressible in our version of MTL. It can be argued that for the purpose of the analysis of real-time systems, the absolute time of the initial state is of no importance.

Let us call a timed state sequence \((\sigma, \tau)\) initial, if the time of its initial state is 0; that is, \(\tau(0) = 0\). The following theorem states that if expressiveness is measured by the sets of initial models definable in a real-time logic, then MTL has the same expressive power as \(L_T\), or equivalently, TPTL.

Theorem [Expressive completeness of MTL]. For every formula \(\phi\) of \(L_T\), there exists a formula \(\psi\) of MTL (without past operators) such that \(\rho \models \phi \iff \rho \models \psi\) for every initial timed state sequence \(p\).

Proof: As in the proof of the expressive completeness of TPTL, given a formula \(\phi\) of \(L_T\), construct a PTL-formula \(\phi'\) with additional time-difference propositions \(T_{\text{diff}}\), \(0 \leq t \leq d(\phi)\), and time-congruence propositions \(T_{\text{cong}}\), \(0 \leq t < c(\phi)\), such that \(M_T(\phi) = M(\phi')\). Furthermore, in \(\phi'\) all propositions \(T_{\text{diff}}\) and \(T_{\text{cong}}\) are either not within the scope of any temporal operator, or immediately preceded by a \(\text{next}\) operator.

From \(\phi'\) we obtain the desired formula \(\psi\) by eliminating the time-difference and time-congruence propositions as follows. Since we consider only initial models, replace each \(T_{\text{diff}}\) and \(T_{\text{cong}}\) that is not within the scope of any temporal operator by \text{true} or \text{false}, depending on whether \(t = 0\). Then replace
5 Discussion

We have shown that only a very weak arithmetic over a discrete domain of time can be combined with PTL to obtain decidable real-time logics. We have then identified two ways of constraining the syntax further, to find elementary real-time extensions of PTL with the full expressive power of the underlying classical theory of timed state sequences.

Thus, TPTL and MTL occupy a position among real-time logics that is as appealing as the standing of PTL for qualitative reasoning. However, both TPTL and MTL have EXPSPACE-complete satisfiability problems. Our decision algorithms are of a time complexity doubly exponential in the length of the timing constraints (though only singly exponential in the number of temporal and logical operators). On the other hand, PTL is PSPACE-complete, and has a singly exponential decision procedure. We claim that this is because reasoning in $L_T$ is intrinsically expensive.

A closer look at our proof of the EXPSPACE-hardness of TPTL ([AH89]) suggests that any extension of PTL that allows the expression of timing constraints of the form “The time of one state is within a certain (constant) distance from the time of another state,” using binary encoding for the time constants, is EXPSPACE-hard. Even the identification of nezt-time with nezt-state (time as a state counter) is of no help in complexity; introducing the abbreviation $\bigcirc^k$ for a sequence of $k$ successive nezt operators makes PTL EXPSPACE-hard! Thus the price of an extra exponential is caused by the succinctness of the notation introduced by the binary encoding of the constants.

Acknowledgements. We thank Zohar Manna for his guidance, and David Dill and Amir Pnueli for helpful discussions.

References


