Temporal Logic with Past is Exponentially More Succinct

Nicolas MARKEY

Lab. Informatique Fondamentale d’Orléans
Univ. Orléans & CNRS FRE 2490
Rue Léonard de Vinci - BP 6759
45067 Orléans Cedex 2 - France

markey@lifo.univ-orleans.fr

Abstract

We positively answer the old question whether temporal logic with past is more succinct than pure-future temporal logic. Surprisingly, the proof is quite simple and elementary, although the question has been open for twenty years.

Introduction

Temporal logics with past. Temporal logic have been defined by Arthur Prior in 1957 [Pri57] as a tool for reasoning about temporal informations in a logical framework. This logic uses temporal modalities for referencing to past or future events. It has been introduced in the field of formal verification by Amir Pnueli in 1977 [Pnu77]. Leslie Lamport suggested to classify temporal logics into two general kinds: linear-time temporal logic and branching-time temporal logic [Lam80]. In linear-time temporal logic (LTL), we can express for instance that any request is eventually granted:

\[ G (\text{request} \Rightarrow F \text{grant}). \] (1)

With past-time modalities, we can express that a grant should be preceded by a request:

\[ G (\text{grant} \Rightarrow F^{-1} \text{request}). \] (2)

With or without past? In 1980, Gabbay proved that past-time modalities did not add expressive power to pure future linear-time temporal logic [GPSS80]. He also provided an algorithm for translating formulas with past-time modalities into equivalent pure future ones [Gab89]. Another procedure was given in
[MMKR94] for temporal logic without next. For instance, equation (2) above can be written
\[ \neg((\neg \text{request}) U (\text{grant} \land \neg \text{request})). \] (3)
This formula is more intricate than the natural formula of equation (2). Moreover, the size of the formula computed by the algorithm is assumed to be non elementary in the size of the initial one. But Gabbay’s theorem has been used as an argument for dropping past-time modalities from linear-time temporal logic. What we show here is that, as regards succinctness, past-time modalities do add expressive power (this result has been published in [LMS02]).

Outline. I will first briefly recall some definitions about linear-time temporal logics with past, and the possibility to “remove” past-time modalities. I will then focus on the translation of LTL formulas into Büchi automata, and more precisely on the size of the resulting automaton. I will then use this result for proving the succinctness gap between LTL+Past and pure future LTL.

1 From PLTL to LTL

Let Prop = \{p, q, \ldots\} be a finite set of atomic propositions. Linear-time temporal logic with past-time modalities (which we denote PLTL in the sequel\(^1\)) is defined with the following syntax:

\[ \text{PLTL} \ni \phi, \psi ::= \neg \phi \mid \phi \lor \psi \mid \phi U \psi \mid X \phi \mid \phi S \psi \mid X^{-1} \phi \mid p \mid q \mid \ldots \]

The pure future fragment of PLTL, denoted by LTL, is defined as follows:

\[ \text{LTL} \ni \phi, \psi ::= \neg \phi \mid \phi \lor \psi \mid \phi U \psi \mid X \phi \mid p \mid q \mid \ldots \]

Formulas are interpreted at some position along linear paths, i.e. along infinite sequences (\(\omega\)-orders) of elements of \(2^{\text{Prop}}\). The semantics for atomic propositions and boolean operators are the classical ones. For modalities, given a path \(\pi\) and a position \(i\), we have:

\[ \pi, i \models \phi U \psi \text{ if, and only if, } \exists k \geq i. (\pi, k \models \psi \land \forall i < j < k. \pi, j \models \phi) \]
\[ \pi, i \models X \phi \text{ if, and only if, } \pi, i + 1 \models \phi \]
\[ \pi, i \models \phi S \psi \text{ if, and only if, } \exists k \leq i. (\pi, k \models \psi \land \forall k < j < i. \pi, j \models \phi) \]
\[ \pi, i \models X^{-1} \phi \text{ if, and only if, } i \geq 1 \text{ and } \pi, i - 1 \models \phi \]

The classical abbreviations F (eventually) and G (always), and their past-time counterparts, are defined by:

\[ F \phi \overset{\text{def}}{=} \top U \phi \quad G \phi \overset{\text{def}}{=} \neg F \neg \phi \quad F^{-1} \phi \overset{\text{def}}{=} \top S \phi \quad G^{-1} \phi \overset{\text{def}}{=} \neg F^{-1} \neg \phi \]

\(^1\)Here, P in PLTL stands for Past.
Two formulas $\phi, \psi$ of PLTL are said to be equivalent (which we write $\phi \equiv \psi$) if, and only if, they verify the following property:

for any path $\pi$ and any position $i$, $\pi, i \models \phi \iff \pi, i \models \psi$.

Initial equivalence is a weaker notion of equivalence: $\phi$ and $\psi$ are initially equivalent ($\phi \equiv_i \psi$) if, and only if,

for any path $\pi$, $\pi, 0 \models \phi \iff \pi, 0 \models \psi$.

Both notions of equivalence clearly coincide for LTL, but not for PLTL formulas.

Translations to pure-future temporal logic. [GPSS80] proves that LTL is expressive complete, thus as expressive as PLTL [Kam68]. Moreover, [Gab89] presents a syntactic algorithm for translating a PLTL formula into an initially equivalent LTL one. For many computer scientists, this has been one reason for not considering past in temporal logics, by concern of minimality.

However, since 1980, the cost of the translation has not been precisely characterized. The algorithm provided by [Gab89] is assumed to be non elementary.

By a detour through counter-free Büchi automata, it is possible to get a more efficient algorithm: first translate the formula $\phi \in$ PLTL into a Büchi automaton [LPZ85], then translate that automaton into an equivalent deterministic Muller automaton. The resulting automaton can be assumed to be counter free, since otherwise, the language it defines would not be star free. Then [MP90, MP94] provides a translation of counter free Muller automaton into LTL. All of the three steps possibly involves an exponential blowup, and the size of the final formula is at most triply exponential in the size of the initial one.

In the sequel, we prove that at least one exponential is unavoidable, i.e. there exists a family of PLTL formulas $\phi_n$ with size $O(n)$, whose equivalent formulas have size $\Omega(2^n)$.

2 LTL and Büchi automata

Let's get back to the aforementioned translation of LTL formulas into Büchi automata. The important theorem is the following:

**Theorem 1 ([WVS83, VW86])**

Given an LTL formula $\phi$, one can build a Büchi automaton $A_\phi = (\Sigma, S, \rho, S_0, F)$ where $\Sigma = 2^{\text{Prop}}$ and $|S| = 2^{O(|\phi|)}$, such that $L(A_\phi)$ is exactly the set of paths satisfying the formula $\phi$.

Let $n$ be a nonnegative integer, Prop = $\{p_0, p_1, \ldots, p_n\}$. We consider the following path property, mentioned in [EVW02]:

Any two positions of the path that agree on propositions $p_1, p_2, \ldots, p_n$ also agree on proposition $p_0$. (4)
This property can be expressed by the following \textsf{LTL} formula, which tests all the possible valuations for the atomic propositions:

\[
\phi_n \overset{\text{def}}{=} \bigwedge_{a_i \in \{\top, \bot\}} \left( \big( \bigwedge_{i=0}^{n} p_i = a_i \big) \Rightarrow \big( \bigwedge_{i=1}^{n} p_i = a_i \big) \Rightarrow (p_0 = a_0) \right)
\]

This formula has size \(2^O(n)\).

We now prove that there is no polynomial size \textsf{LTL} formula expressing the same statement. The proof is adapted from [EVW02]. Assume that there exists a Büchi automaton of size single exponential whose language is exactly the set of computations verifying \(\phi_n\).

We show that this is not possible: any automaton recognizing \(L(\phi_n) = \{ u \in (2^{\text{Prop}})^\omega \mid u \models \phi_n \}\) requires at least \(2^{2^n}\) states. Indeed, let \(A\) be an automaton recognizing exactly \(L(\phi_n)\), let \(a_0, \ldots, a_{2^n-1}\) be any sequence of the \(2^n\) subsets of \(\{p_1, \ldots, p_n\}\), and let \(K\) be a subset of \(\{0, \ldots, 2^n - 1\}\). We define a sequence of letters \(b_i \in \Sigma\) as follows:

\[
b_i \overset{\text{def}}{=} \begin{cases} a_i & \text{if, and only if, } i \notin K \\ a_i \cup \{p_0\} & \text{if, and only if, } i \in K \\ \end{cases}
\]

We also define the finite word \(w_K \overset{\text{def}}{=} b_0 b_1 \cdots b_{2^n-1}\). Clearly, two different choices of \(K\) lead to two different sequences of \((b_i)_{i=0, 2^n-1}\), thus to two different words \(w_K\). Therefore, there exists exactly \(2^{2^n}\) such words.

Let \(K\) and \(K'\) be two distinct subsets of \(\{0, \ldots, 2^n - 1\}\). Obviously, the words \(w_K'\) and \(w_K\) are accepted by the automaton \(A\). There exist two paths \(\pi_K\) and \(\pi_K'\) in the automaton \(A\) accepting the words \(w_K\) and \(w_K'\), respectively. Consider the \(2^n\)-th state of each of these paths, which we name \(q_K\) and \(q_K'\). If these states were identical, then the suffix \(\pi_K'\) starting from state \(q_K\) could be appended to the prefix of \(\pi_K\) up to state \(q_K\), thus giving an accepting path (since the Büchi acceptance conditions are satisfied along \(\pi_K\)) for the word \(w_K' \cdot w_K\). But that word \(w_K' \cdot w_K\) should not be accepted by \(A\) since it does not satisfy the formula \(\phi_n\). Thus any automaton recognizing exactly \(L(\phi_n)\) has at least \(2^{2^n}\) states, so that \(|\phi_n|\) is in \(\Omega(2^n)\).

3 \textbf{PLTL is exponentially more succinct than LTL}

In order to prove the succinctness result, we will use a slightly modified property, namely:

Any position of the path that agrees on propositions \(p_1, p_2, \ldots, p_n\) with the initial state also agrees on proposition \(p_0\).

This property can be expressed in \textsf{PLTL} through the following formula:

\[
\psi_n \overset{\text{def}}{=} G \left( \bigwedge_{i=1}^{n} (p_i \leftrightarrow F^{-1} G^{-1} p_i) \right) \Rightarrow (p_0 \leftrightarrow F^{-1} G^{-1} p_0).
\]
This formula clearly expresses property (5), since $F^{-1}G^{-1}p$ means that $p$ holds in the initial state of the path. Moreover, $\phi_n$ has size $O(n)$.

Since any PLTL formula can be translated into an initially equivalent LTL formula, we let $\psi_n^\prime$ be an LTL formula initially equivalent to $\psi_n$, and we define $\phi_n^\prime = G\psi_n^\prime$. We claim that $\phi_n$ and $\phi_n^\prime$ are equivalent. Indeed, that some path $\pi$ satisfies $\phi_n^\prime$ exactly means that for all $i$, $\pi_i \models \psi_n^\prime$. Since $\psi_n^\prime \in$ LTL, this amounts to say that $\pi^i, 0 \models \psi_n^\prime$. Since $\psi_n^\prime \equiv \psi_n$, it is equivalent to the fact that, for all $i$, $\pi^i, 0 \models \psi_n$, that is "for all position $i$, for all position $j$, if position $j$ agrees with position $i$ on propositions $p_1, p_2, \ldots, p_n$, then it also agrees with position $i$ on proposition $p_0$", which we means that $\pi$ satisfies $\phi_n$.

Bringing all the pieces together, we get the following theorem:

**Theorem 2**

PLTL can be exponentially more succinct than LTL.

The proof is quite simple now: consider formula $\psi_n$, and its LTL equivalent $\psi_n^\prime$. We know that $\phi_n$ has size linear in $n$, and we know that $G\psi_n^\prime$ has size $\Omega(2^n)$, since it is an LTL formula expressing property (4). Thus $\psi_n^\prime$ has size at least $\Omega(2^n)$. In fact, this even proves that $\psi_n^\prime$ has at least $\Omega(2^n)$ distinct subformulas, since in the construction of $A_\phi$, the states are the subsets of the set of subformulas of $\phi$ (thus $\psi_n^\prime$ cannot even be succinctly represented as a dag sharing common subformulas).

Remark that the proof requires formulas with bounded temporal height, and uses an unbounded number of atomic propositions. It can be adapted in order to use only finitely many atomic propositions, but with an unbounded temporal height (by encoding atomic propositions with only one atomic proposition [DS02]). Moreover, the proof uses neither the $U$ nor the $S$ modalities. The result thus carries over to $L(F, F^{-1})$. It can be shown however that $L(F, F^{-1})$ is strictly more expressive (as regards to the classical notion of expressivity) than $L(F)$.

**Conclusion**

This simple proof only partially answers the question on the size of the optimal translation from PLTL to LTL: we proved that the gap is at least single exponential, but the best known upper bound is triply exponential.

**References**


