Automata-based Verification of
Linear Temporal Logic Models with Bounded Variability

Carlo A. Furia  
ETH Zurich, Switzerland  
caf@inf.ethz.ch

Paola Spoletini  
Università degli Studi dell’Insubria, Italy 
paola.spoletini@uninsubria.it

Abstract—A model has variability bounded by $v/k$ when the state changes at most $v$ times over any linear interval containing $k$ time instants. When interpreted over models with bounded variability, specification formulae that contain redundant metric information—through the usage of next operators—can be simplified without affecting their validity. This paper shows how to harness this simplification in practice: we present a translation of LTL into Büchi automata that removes redundant metric information, hence makes for more efficient verification over models with bounded variability. To show the feasibility of the approach, we also implement a proof-of-concept translation in ProMeLa and verify it using the Spin off-the-shelf model checker.

I. INTRODUCTION AND OVERVIEW

Linear temporal logic (LTL) formulae model linear sequences of discrete states that evolve “one step at a time”. The state may change between some pairs of adjacent steps and not change between others; we say that a linear model has variability bounded by $v/k$ (read “$v$ over $k$”) when the state changes at most $v$ times over any interval containing exactly $k$ steps.

Bounded variability limits the amount of information necessary to define a model: characterizing the state over $v$ time instants is sufficient to completely describe the temporal behavior over a window of length $k$. Consider now an LTL formula $\phi$ that describes distances among states by means of the next operator $X$: for example, $XXXp$ says that $p$ holds in the future, at a distance of 3 steps. If $\phi$ describes distances as large as $k$ (i.e., $k$ nested occurrences of $X$) but we are interested only in its models with variability bounded by $v/k$ for $v < k$, $\phi$ contains metric information that is redundant, as all the “action” occurs only over up to $v$ steps.

In previous work [1], we showed how to remove the redundant information and produce a smaller formula $\phi'$ whose validity is equivalent to $\phi$’s validity over models with variability bounded by $v/k$; the size of $\phi'$ depends on $v$ but not on $k$, hence the size of $\phi'$ is significantly smaller than the size of $\phi$ when $v \ll k$. Unfortunately, this result turns out to have mostly theoretical interest: the transformation from $\phi$ to $\phi'$ reduces the size due to $k$ but also introduces a polynomial blow-up that, while it does not affect the worst-case complexity of the validity problem, is too conspicuous in practice: $\phi'$ is often still too large to be verified with standard tools for LTL.

The present papers shows how to get around this practical shortcoming. The solution has two elements. First, Section III presents a different transformation of $\phi$ into a formula $\Phi$ that is equivalent for models with variability bounded by $v/k$. The size of $\Phi$ also does not depend on $k$ but, surprisingly, is otherwise exponential in another of $\phi$’s size parameters! This exponential blow-up is, however, completely immaterial: Section IV describes a direct translation of $\Phi$ into equivalent Büchi automata that can be analyzed efficiently in practice.

More precisely, some components of the translation use alternating Büchi automata extended with finite-domain counters; these make for a direct implementation of them into the ProMeLa language input to the Spin model checker. Section V presents a few details of the ProMeLa implementation and describes experiments where we used the technique presented in the rest of the paper to check for satisfiability—over models with bounded variability—an LTL example specification of a simple “elections” scenario. The large distances used in the specification, required to describe time units at different levels of granularity, make its verification unfeasible for standard LTL techniques that do not exploit the bounded variability assumption.

Related work: One of the original motivations to study models with bounded variability comes from the desire to reason about systems with heterogeneous time granularities [2], where large and small distances coexist. A few authors have discussed the modeling challenges brought by such systems [3], [4], [5], [6], [7], [8], and have demonstrated their relevance in some application domains such as medical data.

Model checking and verification using LTL and automata is a subject extensively studied for over three decades. The complexity of checking the validity of LTL formulae [9], [10] and the relations between LTL and Büchi automata [11], [12] are well-known; Section II recalls some of the main results, which are used in the rest of the paper. The automata-theoretic approach [11], [12] to LTL has produced not only a comprehensive theoretical framework, but also practical scalable implementations such as the Spin model
checker [13], which we used in the experiments discussed in Section V. The characterization of repeated “stuttering” steps in LTL models has been studied by Lamport [14] and others [15], [16], [17].

In spite of the extensive work on LTL, to our knowledge the present paper and our previous work [11] are the first approaches that target LTL verification for models with bounded variability. Some of the ideas used in our work are inspired—and named after—similar notions introduced for dense time models; in particular, Pnueli operators [18] and bounded variability itself [19], [20].

As we explain in Section II, our previous work [11] represents a theoretical counterpart to the present paper; in particular, we re-use some techniques of [11] to establish the correctness of a similar transformation. While the presentation of the present paper is entirely self-contained, we warn readers already familiar with [11] that we have occasionally changed the notation and the details of some definitions to better focus the presentation on the novel contributions.

II. PRELIMINARIES

A. Words and Variability

Words and trees: An ω-word (or simply word) w over a set S of propositional letters is a mapping w : N → 2^S that associates to every discrete instant i (also called step) the subset w(i) ⊆ S of propositions that hold at i. W(S) denotes the set of all words over S.

A tree is a set T ⊆ N^* of sequences of natural numbers that is prefix-closed, that is, if x · c ∈ T—for x ∈ N^* and c ∈ N—then x ∈ T as well. The elements of T are called nodes; the empty sequence ε denotes T’s root; and if x · c ∈ T we say that x · c is a successor of x. A node without successors is called leaf. A path of T is a sequence π_0, π_1, . . . of nodes of T such that π_0 = ε and, for every j ≥ 0, either π_j is a leaf or π_j+1 is a successor of π_j. A S-labeled tree is a pair ⟨T, λ⟩ where T is a tree and λ : T → S assigns an element of S to each node of T.

Stuttering: A step i ∈ N is stuttering in a word w if w(i + 1) = w(i) and there exists a later step j > i such that w(j) ̸= w(i). Conversely, a non-stuttering step (nss for short) i is such that either w(i + 1) ̸= w(i) or, for all j > i, w(j) = w(i). Intuitively, a stuttering step is redundant: it records information that is repeated identically in the next step, hence it only carries information about distance between states. A word is stutter-free if it has no stuttering steps. Two words are stutter-equivalent if removing all their stuttering steps reduces both to the same stutter-free word.

Bounded variability: Given two positive integers v, k, a word w has variability bounded by v/k (or simply is v/k bounded) if, for all i ∈ N, at most v steps among i, i + 1, . . . , i + k − 1 are non-stuttering in w. A set W of words has variability bounded by v/k if every word w ∈ W is v/k bounded. W(S, v/k) denotes the set of all words over S with variability bounded by v/k.

B. Linear Temporal Logic

LTL syntax: LTL formulae are defined by:

LTL := p | ¬φ | φ_1 ∧ φ_2 | φ_1 U φ_2 | X φ

where p ranges over a set P of propositional letters; we use the standard abbreviation for ⊥ (false), ∨ (or), ⇒ (implies), ⇔ (iff); and for the derived temporal operators Fφ (eventually: T U φ), Gφ (always: ¬F¬φ), and X_kφ (distance: X X X ... X φ), where k ≥ 0. The size |φ| of an LTL formula k

φ is the size of its encoding as a string.

Qualitative and propositional LTL: L(U) denotes the qualitative subset of LTL which does not use the X operator.

Pnueli operators: The qualitative extended Pnueli operators (or simply Pnueli operators) are defined by:

P^n_kφ = (ψ_1, . . . , ψ_k)

for k, n ∈ N, n_1, . . . , n_k ∈ N ∪ {∞}, and ψ_1, . . . , ψ_k ∈ L(U). L(U, Pn) denotes LTL extended with the Pnueli operators. The size |φ| of a L(U, Pn) formula φ is the size of its encoding as a string, assuming a unary encoding for k, n, n_1, . . . , n_k.

The satisfaction relation for Pnueli operators

w, i |= P^n_kφ(ψ_1, . . . , ψ_k)
holds if there exist \( k \) positions \( i = i_0 \leq i_1 \leq \cdots \leq i_k \) such that, for all \( 1 \leq j \leq k \), the following hold: (1) \( w, i_j + 1 \models \psi_j \); (2) if \( n_j \neq \infty \) then there are no more than \( n_j \) nss in \([i_j-1,i_j-1]\); (3) there are no more than \( n \) nss in \([i_1,i_k]\).

**Proposition 2 (\([1]\)).** The satisfiability problem for \( \text{L(U, Pn)} \) is \( \text{PSPACE-complete} \).

**Example 3.** Consider the word \( w \):

\[
\begin{array}{cccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
a & a & a & \pi & a & a & a & a & a \\
b & b & b & b & b & b & b & b & b \\
\end{array}
\]

where nss are in bold and underlined, and \( \pi \) denotes \( \neg x \). For the positions \( 1, 2, 6, 6, \) \( w, 1 \models P_3^{3; (3,2,\infty,3)}(a, \neg b, a \land b, b) \) holds. On the contrary, \( w, 1 \not\models P_4^{3; (3,2,2,1)}(a, \neg b, a \land b, b) \) if \( i_1, \ldots, i_4 \) are the positions that match the semantics of the operator, it must be \( i_3 \geq 6 \), but there are \( 4 > 3 \) nss in the interval \([1,6]\).

C. Alternating Büchi Automata

An alternating (Büchi) automaton \( A \) is a tuple \( \langle \Sigma, Q, q_0, \delta, F \rangle \), where \( \Sigma \) is the finite input alphabet, \( Q \) is the finite set of states, \( q_0 \in Q \) is the initial state, \( \delta : Q \times \Sigma \to P^+(Q) \) is the transition function, and \( F \subseteq Q \) is the set of final states. If \( \delta(q,\sigma) \) is purely disjunctive when it is defined, \( A \) is an ordinary nondeterministic (Büchi) automaton. The size \( |A| \) of an alternating automaton \( A \) is \( |Q| + |\delta| \), where \( |\delta| \) is the sum of the formula sizes \( |\delta(q,\sigma)| \) for all \( q,\sigma \) where \( \delta \) is defined.

A run \( r \) of an alternating automaton over a word \( w \) over \( \Sigma \) is a \( Q \)-labeled tree \( \langle T_r, \lambda_r \rangle \) such that: (1) the root \( e \in T_r \) has label \( \lambda_r(e) = q_0 \); (2) if \( x \in T_r \) is a node in the tree with label \( \lambda_r(x) = q \) and the transition function defines \( \delta(q,w(|x|)) = \theta \), then there is a set \( \Pi = \{q_1, \ldots, q_k\} \subseteq Q \) such that \( \pi \models \theta \)—where we define \( \pi(0) = \Pi \)—and, for all \( 1 \leq j \leq k \), \( x \cdot j \in T_r \) is a node of \( T_r \) with \( \lambda_r(x \cdot j) = q_j \).

A path \( \pi \) of a run \( r \) is any path in \( T_r \), hence an infinite sequence \( q_0, q_1, \ldots \) of states; it is accepting if \( q_i \in F \) for infinitely many \( i \)'s. A run \( r \) is accepting if all its infinite paths are accepting. A word \( w \) is accepted if there exists an accepting run on it. \( |A| \) denotes the set of all words accepted by \( A \) (also called the language of \( A \)).

**Proposition 4 ([12]).** The emptiness problem for languages defined by nondeterministic Büchi automata is \( \text{NLOGSPACE-complete} \).

- For any alternating automaton of size \( n \) there exists an equivalent nondeterministic automaton of size \( 2^{O(n)} \).
- For any LTL formula \( \phi \) there exists an equivalent alternating automaton of size \( O(|\phi|) \).

**Automata with counters:** Consider \( n \) integer counters, each with finite domain \([0,C_i]\) for \( i = 1, \ldots, n \). An alternating automaton \( A \) with \( n \) counters has the same components as a regular alternating automaton, but its transition function has signature \( \delta : Q \times \Sigma \times C \to P^+(Q \times C) \) where \( C = [0, C_1] \times \cdots \times [0, C_n] \) is the Cartesian product of the counters’ domains. We define the semantics of an alternating automaton \( A \) with counters as a regular alternating automaton \( \overline{A} \) with: states \( \overline{Q} = Q \times C \); initial state \( \overline{q}_0 = (q_0, 0, \ldots, 0) \); and transition function \( \overline{\delta} \) such that \( \overline{\delta}((q_1, c_1, \ldots, c_n), \sigma) = \theta \) if and only if \( \delta(q_1, c_1, \ldots, c_n) = \theta \). The size of \( \overline{A} \) also defines the size of \( A \).

**Example 5.** The following alternating automaton with one counter \( c \) over \([0,2]\) accepts the language \( \left[ G(X b \lor X^2 b) \right] \).

In the figure, a bullet marks pair of edges corresponding to conjunctive transitions, and the outgoing edges to the symbols \( \top \) and \( \bot \) denote transitions equal to the logic values \( \top \) and \( \bot \). The automaton spawns a separate parallel computation at every step (corresponding to the \( G \)); the computation counts up to two time steps and terminates successfully only if a \( b \) is encountered before the counter reaches 2.

### III. FROM LTL TO L(U, Pn)

Consider a generic LTL formula \( \phi \); without loss of generality, we can write \( \phi \) in separated-next form with the occurrences of \( X \) separated from the rest of the formula as

\[
\phi \equiv \psi_U \land \bigwedge_{1 \leq i \leq M} (x_i \Leftrightarrow X^{d_i} \pi_i) ,
\]

where: \( \psi_U \in \text{L(U)} \) is the purely qualitative part of the formula; for \( i = 1, \ldots, M, x_i \in \mathcal{P} \) is a propositional letter and \( \pi_i \in \mathcal{P}(\mathcal{P}) \) is a propositional formula; and \( 0 < d_1 \leq \cdots \leq d_M \) are nonnegative distances. Also, \( m \leq M \) denotes the number of distinct distances \( d_1 = D_1 < \cdots < D_m = d_M \) among \( d_1, \ldots, d_M \). Our ultimate goal is to determine if \( \phi \) is satisfiable over words in \( \mathcal{W}(\mathcal{P}, v/V) \) where \( v \) is any positive integer and \( V = d_M \) is the maximum distance appearing in \( \phi \).

When \( V \) is large, \( |\phi| \) is large as well; however, if \( v \ll V, \phi \) encodes information that is redundant to decide its satisfiability over words with variability bounded by \( v/V \). In [11], we described a polynomial-time transformation of \( \phi \) into an equi-satisfiable formula \( \phi' \in \text{L(U, Pn)} \) whose size is \( O(|\phi|^2 + vM^2 + v^2M) \). Since the size of \( \phi' \) does not depend on \( V \), if \( v \) is significantly smaller than \( V \)—in particular, exponentially smaller—then checking the satisfiability of \( \phi' \) is much easier than checking the original formula \( \phi \). The transformation from \( \phi \) to \( \phi' \) stands as a theoretical result but is impractical because of the quadratic increase in size it introduces, which even becomes \( O(v^4) \) when we express
the Pnueli operators in plain L(U); this blow-up is normally too conspicuous to handle with standard LTL tools.

To overcome these practical shortcomings, we follow the same principles used for $\phi'$ in Figure 1 to build

$$\Phi \equiv \psi_U \land \psi_s \land \psi_P,$$

where $\psi_U, \psi_s$ are qualitative formulae in L(U), and $\psi_P \in L(U, P_n)$ uses Pnueli operators. $\psi_U$ is the same in $\phi$ and $\Phi$. $\psi_s$ marks the firsts of propositions in $\mathcal{P}$ through a fresh letter $s \notin \mathcal{P}$ that toggles precisely when some proposition in $\mathcal{P}$ changes truth value. Namely, if no proposition ever changes value then $s$ holds, and any proposition changing triggers $s$ to do the same (see Figure 1 Sec. IV) for a formal definition in L(U), which is however straightforward.

To present $\psi_P$, we have to introduce some more notation. Let $B \in \{0,1\}^M$ denote a sequence of $M$ Boolean values $b_1, \ldots, b_M$; then, for $i = 1, \ldots, M$, $[b_i]\psi$ is $g$ if $b_i = 1$ and $\neg g$ if $b_i = 0$. $\psi_P$ enumerates all possible $2^M$ truth assignments to $x_1, \ldots, x_M$:

$$\psi_P \equiv G \left( \bigwedge_{B \in \{0,1\}^M} X_1 \land \cdots \land X_M \Rightarrow \psi_B \right),$$

where, using the notation just introduced, $X_i = [b_i x_i]$ for $i = 1, \ldots, M$. For each truth assignment $B$, $\psi_P$ constrains the truth value of $\pi_1, \ldots, \pi_M$ over the following $v$'s:

$$\psi_B \equiv P_m^0: (\delta_1, \ldots, \delta_m) (Y_1, \ldots, Y_m),$$

where $Y_j = \bigwedge_{d_k = D_j} [b_k \pi_k]$ is the conjunction of all $\pi_k$'s corresponding to the same distance $D_j$ in $\phi$, for $j = 1, \ldots, m$; and, for $j = 1, \ldots, m$ and $D_0 = 0$, $\delta_j$ is

$$\delta_j \equiv \begin{cases} D_j - D_{j-1} & \text{if } D_j - D_{j-1} \leq v - j + 1, \\ \infty & \text{otherwise}. \end{cases}$$

The intuition behind the transformation from $\phi$ to $\Phi$ is as follows. At every step, $\phi$ constrains the future values of the $\pi_i$'s over a time window of length $V = d_M$ according to the current value of the $x_i$'s. If the variability is bounded by $v/V$, however, no more than $v$ changes of the proposition in $\mathcal{P}$—which determine the value of the $\pi_i$'s—are possible. Correspondingly, $\psi_P$ converts the distance constraints in $\phi$ into qualitative constraints over $v$: rather than saying that $\pi_1$ must occur at distance $d_1$, $\pi_2$ at distance $d_2$, and so on, $\psi_P$ only requires that $\pi_1$ occurs first, followed by $\pi_2$, and so on. Since $\Phi$ is qualitative, we can transform one of its models into a model for $\phi$ by adding stuttering steps so that the $\pi_i$'s follow the original metric constraints in $\phi$. The additional constraints introduced by the $\delta_i$'s ensure that this “padding” is always possible (since we cannot remove nss, we must ensure that there are not “too many” of them between any two consecutive distances). Using the same techniques used in Figure 1, it is not difficult to make this intuition rigorous and prove the following.

**Theorem 6.** $\phi$ is satisfiable over words in $\mathcal{W}(\mathcal{P}, v/V)$ if and only if $\Phi$ is satisfiable over words in $\mathcal{W}(\mathcal{P} \cup \{s\})$.

Section IV shows how to exploit automata-theoretic techniques to check efficiently the satisfiability of $\Phi$, hence, thanks to Theorem 6, to decide the satisfiability of $\phi$ over models with bounded variability. Section V demonstrates that the automata-theoretic techniques are directly implementable using standard model-checking tools.

IV. FROM L(U, P_n) TO AUTOMATA

This section describes an efficient translation of the components of $\Phi$ into automata. Each component $\psi_k$ becomes an automaton $A_k = (\Sigma, Q^k, q^k_0, \delta^k, F^k)$ such that $[\psi_k] = [A^k]$: whenever clear from the context, we drop the superscript $k$ from the automaton components’ names. For simplicity of presentation, we assume that the alphabet $\Sigma$ of all automata equals the set of all propositional letters used in any formula, and omit the straightforward details of how to handle letters appearing only in certain components.

We do not discuss the translation of $\psi_U \in L(U)$ into $A_U$, because $\psi_U$ can have any structure, hence we just rely on standard translations of LTL into alternating automata.

A. Marking Non-stuttering Steps

The automaton $A^u$ for $\psi_s$ has $2 \cdot 2^{\lvert P \rvert} + 1 \text{ states } \{q^s_0\} \cup \{q^s_+, q^s_- \mid P \subseteq \mathcal{P}\}$: two for each subset of $\mathcal{P}$, and a distinct initial state $q^s_0$; all states other than $q^s_0$ are accepting.

Computations start in the initial state $q^s_0$. According to the initial values of the propositions in $\mathcal{P}$, the automaton goes to a state in $q^s_+$ (if $s$ holds) or in $q^s_-$ (if $s$ doesn’t):

$$\delta(q^s_0, P \cup \{s\}) = q^s_+ \text{ and } \delta(q^s_0, P) = q^s_-,$$

for $P \in 2^\mathcal{P}$.

The automaton leaves states of the form $q^s_+$ only if the values of the propositions change and $s$ turns false; otherwise, $s$ must hold continuously:

$$\delta(q^s_+, P \cup \{s\}) = q^s_+ \text{ and } \delta(q^s_+, \hat{P}) = q^s_-,$$

where $\hat{P}$ ranges over the complement set of propositions $2^\mathcal{P} \setminus P$. Similarly, $A^u$ leaves states of the form $q^s_-$ only if the values of the propositions change and $s$ turns true; otherwise, $s$ must not hold:

$$\delta(q^s_-, P) = q^s_- \text{ and } \delta(q^s_-, \hat{P} \cup \{s\}) = q^s_+.$$

Figure 1 shows $A^u$ for $\mathcal{P} = \{a, b\}$, where every transition that enters a state $q^s_+$ has label $P \cup \{s\}$, every transition that enters a state $q^s_-$ has label $P$, and the initial transitions are dotted for readability.
B. Translating Pnueli Operators

The automaton $A^B$ for $\psi_B$ has $2m + 2$ states $\{q_0, q_F\} \cup \{q_i^+, q_i^- | 1 \leq i \leq m\}$ and two counters $c_G \in [0, v]$ and $c_L \in [0, \delta]$ where $\delta = \max_i \delta_i$; $c_G$ is the "global" counter that counts the following $v$ ns, whereas $c_L$ is the "local" counter that measures each of the $\delta_i$’s. Computations start in the initial state $q_0$ and should end in the only accepting state $q_F$. At any point during a computation, $A^B$ is in state $q_i^\pm$ when it is ready to read $Y_i, \ldots, Y_{m+1}$ before $c_G$ reaches $v$, with $\circ = +$ if $s$ held in the latest step, and $\circ = -$ otherwise. In the following, $d_G$ ranges over $[0, v]$, $e_G$ over $[0, v - 1]$, $d_L$ over $[0, \delta_i] \cap \{0, v\}$, and $e_L$ over $[0, \delta_i - 1] \cap \{0, v - 1\}$.

The automaton stays in $q_i^\pm$ (resp. $q_i^-$) without changing the counters if $s$ holds (resp. does not hold) and $Y_i$ is false:

$$\delta(q_i^+, s \land \neg Y_i, d_G, d_L^+) = \langle q_i^+, d_G, d_L^+ \rangle,$$
$$\delta(q_i^-, s \land \neg Y_i, d_G, d_L^+) = \langle q_i^-, d_G, d_L^+ \rangle,$$

When $s$ toggles but $Y_i$ is false, $A^B$ rotates between $q_i^+$ and $q_i^-$ while incrementing both counters by one:

$$\delta(q_i^+, s \land \neg Y_i, e_G, e_L^+) = \langle q_i^+, e_G + 1, e_L^+ + 1 \rangle,$$
$$\delta(q_i^-, s \land \neg Y_i, e_G, e_L^+) = \langle q_i^+, e_G + 1, e_L^+ + 1 \rangle,$$

with $i \leq m$. When $Y_i$ holds, if $A^B$ nondeterministically guesses that this is the “right” occurrence of $Y_i$ it goes to $q_{i+1}^-$ and resets the local counter; otherwise, it remains in $q_i^\pm$. For $i < m$, define $\delta(q_i^+, s \land Y_i, d_G, d_L^+)$ as

$$\langle q_{i+1}^+, d_G, 0 \rangle \lor \langle q_i^+, d_G, d_L^+ \rangle,$$

and $\delta(q_i^+, s \land Y_i, e_G, e_L^+)$ as

$$\langle q_{i+1}^+, e_G + 1, 1 \rangle \lor \langle q_i^+, e_G + 1, e_L^+ + 1 \rangle.$$

The transitions outgoing $q_i^-$ when $Y_i$ holds are obtained by duality with the substitutions $\rightarrow +$ and $\neg s \leftrightarrow s$. From now on, we omit from the presentation all transitions from states of the form $q_i^-$ that follow by duality.

The transition from $q_i^+$ to $q_{i+1}^-$ is also possible when the local counter equals $\delta_i$: when $s$ takes a new value we are already past the nss that occurred in the previous step, and the new nss is counted in the next round starting with $c_L = 1$:

$$\delta(q_i^+, \neg s \land Y_i, e_G, e_L) = \langle q_{i+1}^-, e_G + 1, 1 \rangle.$$

Notice that the value of $e_L^+$ does not matter in transitions corresponding to $\delta_i = \infty$, hence we need not update the local counter (we omit the straightforward details).

Now, we define the initial and final transitions. Initially, $A^B$ goes to $q_1^+$ or $q_1^-$ according to the first value of $s$, e.g.:

$$\delta(q_0, s \land \neg Y_1, 0, 0) = \langle q_1^+, 0, 0 \rangle,$$
$$\delta(q_0, s \land Y_1, 0, 0) = \langle q_1^-, 0, 0 \rangle \lor \langle q_2^+, 0, 0 \rangle.$$

The last successful transition from $q_m^+$ may lead to $q_F$:

$$\delta(q_m^+, \neg s \land Y_m, e_G, e_L) = \langle q_F, 0, 0 \rangle \lor \langle q_m^-, e_G + 1, e_L + 1 \rangle,$$
$$\delta(q_m^+, s \land Y_m, d_G, d_L^+) = \langle q_F, 0, 0 \rangle \lor \langle q_m^+, d_G, d_L^+ \rangle.$$

The transition to $q_F$ is possible also when the local counter equals $\delta_m$, the global counter equals $v$, or both:

$$\delta(q_m^+, \neg s \land Y_m, v, d_L^+) = \langle q_F, 0, 0 \rangle,$$
$$\delta(q_m^+, \neg s \land Y_m, d_G, \delta_m) = \langle q_F, 0, 0 \rangle.$$

Finally, the accepting state is absorbing:

$$\delta(q_F, \top, 0, 0) = \top.$$

The transitions introduced so far do not allow for some of the following steps to coincide. To account for this case, we introduce $O(m^2)$ transitions that “jump” multiple states
as that is, at any step, the value of the propositions of the component $q_0$ that is immaterial in practice: if we compute the intersection and the update of the counters are omitted.

Then, for each $S \in P^\cup \{q_0\}$, with:

$$\delta(S, 0, 0) = \phi(B)^B;$$

Figure 2 shows $A^B$ for $P^\delta(3,2,\infty,1) (a, \neg b, a \land b, b)$; for readability, the “jump” edges we described last are dotted, and the update of the counters are omitted.

The automaton $A^P$ for $\psi_P$ combines the various $A^B$ through conjunctive alternation, as illustrated in Figure 3. First, coalesce all their initial states into a single one, also called $q_0$, and all their final states into another one, also called $q_F$; this gives an automaton with $2 + m2^M+1$ states. Then, for each $B \in \{0,1\}^M$, replace each initial transition of the component $A^B$ of the form $\delta(B(q_0^B), S, 0, 0) = \phi(B)$, $S \in P(P^\cup \{s\})$, with:

$$\delta(q_0, S \land X_1 \land \ldots \land X_{M}, 0, 0) = (q_0, 0, 0) \land \phi^B;$$

that is, at any step, the value of the propositions $x_1, \ldots, x_M$ activates a uniquely determined component $A^B$, while a parallel computation remains in $q_0$ ready for the next step.

Figure 2. Automaton $A^B$ for $\psi_B = P^\delta(3,2,\infty,1) (a, \neg b, a \land b, b)$.

C. Overall Automaton

The automaton $A$ for $\Phi$ is a nondeterministic Büchi automaton, given by the intersection of 3 components:

$A^U$ is a standard encoding of LTL into nondeterministic Büchi automata, of size $2O(|\Phi|)$;

$A^s$ is a nondeterministic Büchi automaton of size $O(2^{|\Psi|})$;

$A^P$ is an alternating automaton of size $O(2^Mm^2v^2)$, where the $v^2$ factor accounts for counters.

The size of $A^U$ is fixed and reflects the fact that satisfiability of LTL is PSPACE-complete; we need not worry about it.

$A^P$ is an alternating automaton; to compose it with the others, we have to convert it into a nondeterministic automaton, but this involves an additional exponential blow-up in the worst-case. The usage of universal alternation is, however, quite restricted in $A^P$: at every step, $A^P$ activates exactly one new component of size $O(m^2v^2)$ in parallel with the others, and each of these components is active for no longer than $v$ ns. Therefore, the exponential size of $A^P$ is immaterial in practice: if we compute the intersection and
Lin ProMeLa has two main components, grouped in a for such we implemented the automaton for the elections example, according to Section III. Then, windows of length \(1460\) that activates new components at every time step according to the semantics of conjunctive alternation (see Figure 3) and re-uses processes that have terminated for new computations. The process running Pnueli acts as an acceptor that filters out the models generated by PsiUOpModel that also satisfy \(\psi_p\). Finally, the functionality corresponding to \(A^\psi\), which is independent of the particular form of \(\phi\), is directly implemented in the global environment: at every new step, the previous value of the propositions is compared with the new value, and \(s\) is complemented whenever the two differ.

Experiments: We verified the ProMeLa model using the Spin model checker. The verification consisted in checking the absence of invalid end states; if successful, this guarantees that Spin can expand the complete ProMeLa model, hence it can perform emptiness check and exhaustive checking of arbitrary Buchi automata. The experiments ran Spin 6.10 on a Ubuntu box (kernel 2.6.32) with Intel Quad-Core2 CPU at 2.40 GhZ with 4 GB of RAM.

We ran verification on the model with a variability bound \(v/V = v/1460\), for values of \(v\) between 6 and 38; for all such values, the results were the following in terms of total running time (in seconds), memory used (in MB), number of primitive states generated (in millions), and maximum expansion depth reached (in thousands).

<table>
<thead>
<tr>
<th>Time (s)</th>
<th>Mem. (MB)</th>
<th># S ((10^6))</th>
<th>D ((10^3))</th>
</tr>
</thead>
<tbody>
<tr>
<td>48</td>
<td>2012</td>
<td>41.8</td>
<td>569</td>
</tr>
</tbody>
</table>

Since \(v\) is merely a global upper bound on the relative distance between events, not a distance that must be reached, the performance is insensitive to changes in the value of \(v\) as long as changing \(v\) does not change the values of the \(\delta_j\)’s (defined in Section III); this is the case for the chosen range \(6 \leq v \leq 38\), and allows for some scalability.

Even if this is only a proof-of-concept as the example is not overly complicated, it is representative of a larger class of systems, and it demonstrates that our approach is feasible and scales. On the contrary, verifying the original formula \(\phi\) “as is” is impossible with state-of-the-art techniques because of the sheer size of \(\phi\) due to the \(V = 1460\) nested occurrences of \(X\). For example, the tool LTL2BA [21]—that translates LTL formulae into Buchi automata encoded in ProMeLa—runs out of resources while generating the automaton, and even an ad hoc implementation in ProMeLa using features such as counters would become too large for Spin to exhaustively analyze. Our encoding is instead significantly more concise and requires a sustainable amount of resources.

VI. Future Work

In future work, we plan to build an automated translator of LTL into ProMeLa implementing the construction for bounded variability introduced in the paper. With the translator, we will be able to perform more experiments with some of the domain-specific examples available in the literature (see the related work in Section I). In addition, we will...
try to construct simplifications similar to those discussed in the paper that are directly applicable to automata model (as opposed to LTL formulae), with the ultimate goal of applying the model-checking paradigm—based on the combination of automata and logic—under the bounded variability assumption.

Acknowledgements: Thanks to the anonymous reviewers for useful comments.

REFERENCES


