
subLTL

An NP-complete fragment of LTL

Anca Muschol and Igor Walukiewicz

Plan

- Complexity of LTL and its fragments
- (A, B) -lemma.
- Small model property for subLTL.

- Models: Infinite words over an alphabet Σ .

subLTL ::= tt | ff | $X_b\varphi$ | $F\varphi$ | $G\varphi$ | $\varphi_1 \vee \varphi_2$ | $\varphi_1 \wedge \varphi_2$

- Semantics:

$v \models X_b\varphi$ if $v = bv'$ and $v' \models \varphi$.

- Negation is definable:

- $\neg(F\varphi) = G(\neg\varphi)$

- $\neg(X_a\varphi) = X_a(\neg\varphi) \vee \bigvee_{b \neq a} X_b\text{tt}$

- Propositional constants: $\text{Prop} = \{P, Q, \dots\}$.

$$\varphi ::= P \mid \neg P \mid X\varphi \mid F\varphi \mid G\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2$$

- Models: infinite sequences of valuations.
- Models are words over the alphabet $\Delta = 2^{\text{Prop}}$.
- P translates to $\bigvee \{X_a \text{tt} : a \in \Delta, P \in a\}$.
- $X\varphi$ translates to $\bigvee_{a \in \Delta} X_a \varphi$.

Thm[Sistla & Clarke]: Propositional version of LTL without until is PSPACE-complete.

- Formula: $G(P \Rightarrow X^n P)$
says that if there is P then after n steps there is P too.
- Coding of a computation of n space-bounded TM.

Thm[Sistla & Clarke]: If X is not allowed then the satisfiability problem is NP-complete.

- If φ has a model then it has one which is a lasso of poly-size.

Complexity (alphabetic variant)

Obs: If X (without subscript) is added to the logic then the satisfiability is PSPACE-complete.

Obs: If X_a is allowed only in the context $X_a \text{tt}$ then the fragment is NP-complete (Sistla-Clarke fragment).

Question: What about subLTL? (the fragment with arbitrary use of X_a but no X).

Obs: If X (without subscript) is added to the logic then the satisfiability is PSPACE-complete.

Obs: If X_a is allowed only in the context $X_a t t$ then the fragment is NP-complete (Sistla-Clarke fragment).

Question: What about subLTL? (the fragment with arbitrary use of X_a but no X).

Thm [Muschol & W.]: The satisfiability problem for subLTL is NP-complete. If a formula has a model then it has one which is a lasso of a poly-size.

- $G(X_a \text{tt} \Rightarrow X_{ab} \text{tt})$
- $G(X_{ab} \text{tt} \vee X_{ba} \text{tt})$
- $G(F(P_a \wedge FP_b) \vee F(P_b \wedge FP_a))$
- $G(X_{abc} \vee X_{bca} \vee X_{cab})$
- $G(F(P_a \wedge F(P_b \wedge FP_c)) \vee \dots)$

- Coding of SAT.

- For a formula over variables x_1, \dots, x_n we consider an alphabet $\Sigma = \{a_1, \dots, a_n, b\}$

- A valuation $V : \{x_1, \dots, x_n\} \rightarrow \{0, 1\}$ is represented by a word w_V such that:

$$a_i \text{ occurs in } w_V \text{ iff } V(a_i) = 1.$$

- A propositional formula is satisfiable iff the subLTL formula obtained by replacing each x_i by FX_{a_i} is.

- Let $A, B \subseteq \Sigma^*$ be two finite sets of words.
- $\text{Swords}(w)$ the set of finite factors of w .
- (A, B) -word is a word w such that
$$A \subseteq \text{Swords}(w) \text{ and } B \cap \text{Swords}(w) = \emptyset.$$

Thm: If there is a finite (A, B) -word then there is one of polynomial size.

Thm: If there is a finite (A, B) -word then there is one of polynomial size.

- Consider a finite automaton whose states are (u, v) with u and v a prefix of a word from A and B respectively.

- Transition relation: $(u, v) \xrightarrow{a} (u', v')$

- $u' = ua$ or if ua is not a prefix of a word in A then u' is the longest suffix of ua which is a prefix of a word from A .

- for v' the same rule but with respect to B .

- Initial state $(\varepsilon, \varepsilon)$.

- Rejecting states (u, v) with v in B .

- (A, B, p) -word is an (A, B) -word that starts with p .

Proposition: Let ϕ be a subLTL formula of size n . Then there exists a set $\mathcal{T}(\phi)$ of triples (A, B, p) , where $A, B \subseteq \Sigma^{\leq n}$ are of polynomial size in n and $p \in \Sigma^{\leq n}$, such that for any word $v \in \Sigma^*$:

$$v^\omega \models \phi \quad \text{iff} \quad v^\omega \text{ is an } (A, B, p)\text{-word for some } (A, B, p) \in \mathcal{T}(\phi).$$

- Proof:

By induction on the structure of the formula.

- A word w is an (A, B, p) -word iff $\$w$ is an (A', B') -word where:

$$A' = A \cup \{\$p\} \text{ and } B' = B \cup \{b\$: b \in \Sigma\}.$$

Lemma: If there is a periodic (A, B) -word then there is one of the form s^ω with $|s|$ polynomial in the sizes of A, B .

- If φ has a model of the form v^ω then there is $(A, B, p) \in \mathcal{T}(\varphi)$ such that v is a (A, B, p) -word.
- We know that A, B, p are of polynomial size.
- Then there is another (A, B, p) -word s^ω with $|s|$ poly in $|\varphi|$. It is a model of φ .

Ultimately periodic models of subLTL

- If a formula has a model then it has an ultimately periodic model, i.e., of the form uv^ω .
- If $uv^\omega \models \varphi$ then there is ψ of poly-size, s.t., $us^\omega \models \varphi$ for all $s^\omega \models \psi$.
- The previous lemma gives us means to shorten v . We want to shorten u .

Observation:

If $u[i, |u|]v \models G\psi$ then $u[j, |u|]v \models G\psi$ for all $j > i$.

If $u[i, |u|]v \models F\psi$ then $u[j, |u|]v \models F\psi$ for all $j < i$.

● **Important position:** the last position where some F -formula is true or the position just before some G -formula becomes true.

Obs: There is a poly-number of important positions.

● **Important position** The last position where some F -formula is true or the position just before some G -formula becomes true.

Obs: There is a poly-number of important positions.

● Between two important positions the same F and G formulas hold (but the truth of X -formulas may vary).

Lemma: Any subLTL formula ψ using only the operators X_a ($a \in \Sigma$) is equivalent to a disjunction of the form $\bigvee_{v \in V} X_v \text{tt}$, for some set $V \subseteq \Sigma^{\leq |\psi|}$ of at most $|\psi|$ words.

- We fix an interval between some two consecutive important positions i and j .
- Let R be the set of F and G -formulas that hold between i and j .
- For a formula ψ let $\hat{\psi}$ be obtained by putting tt for every F or G -subformula in R and ff for all the others.
- We have that there is V_ψ such that $\hat{\psi}$ is equivalent to $\bigvee_{v \in V_\psi} X_v \text{tt}$.

- An (Y, p, s) -word is a word w which:
- starts with p and finishes with s ;
- for all positions $1 \leq k \leq |w| - |s|$, the suffix $w[k, |w|]$ starts with a word from Y .

Lemma: If there is an (Y, p, s) -word then there is one of poly-size in Y, p, s .

- For each $G\alpha$ from R consider $\hat{\alpha} = \bigvee_{v \in V_\alpha} X_v$.
Let Y be such that $\bigwedge_{G\alpha} \hat{\alpha} = \bigvee_{v \in Y} X_v$.
Let $p = u[i + 1, i + n]$ and $s = u[j - n + 1, j]$.

Lemma: If w is (Y, p, s) word then for all $k \leq |w| - n$ the word $w[k, |w|]$ has a prefix in V_α for all subformulas $G\alpha \in R$.

Lemma: The word $u[i + 1, j]$ is a (Y, p, s) -word.

● We know that $u[i + 1, j]$ is a (Y, p, s) word.

Lemma: If w is a (Y, p, s) word then $wu[j + 1, |u|] \models S_{i+1}$.

Proposition: If $uv^\omega \models \varphi$ and $i, j \in \text{VIP}$ are successive important positions then there is a word w of size polynomial in $n = |\varphi|$ such that $u[1, i] w u[j + 1, |u|] v^\omega \models \varphi$.

Thm: If a formula has a model then it has one which is a lasso of a poly-size.

- subLTL is a quite natural fragment of LTL that was overlooked because of the syntactic conventions.
- Adding X or U to subLTL makes it PSPACE-hard. Any other suggestions for extensions?
- What about LTrL version of subLTL? LTrL without U is EXPSPACE-complete but X seems to be needed in the coding.
- What about complexity of model-checking a path for subLTL.