Xishun Zhao *

October 19, 2012

Abstract

Key words:

Let $Prop$ be the set of all propositional variables.

A model is a triple $\mathcal{S} = (S, \mu, \pi)$ such that

- S is a countable set of symbols representing states.
- $\mu : \mathbb{N} \to S$ is a bijection.
- $\pi : S \to \mathcal{P}(Prop)$ is a mapping which induces a propositional assignment of $Prop$ for each state.
- In many literature, μ is just written as a sequence $s_0, s_1, \cdots ,$.

In fact same as following definition

A linear-time structure is a mapping $\pi : \mathbb{N} \to 2^{Prop}$, where 2^{Prop} is the power set of $Prop$ which is the set propositional variables.

Given $x \in Prop$, two models π_1 and π_2. We say π_1 is an x-variant if for any $i \in \mathbb{N}$ we have $\pi_1(i) \setminus \{x\} = \pi_2(i) \setminus \{x\}$.

- X for next (or $\bigcirc$) .
- F for future, i.e., eventually holds (or $\Diamond$)

*Corresponding author. Tel: 0086-20-84114036, Fax:0086-20-84110298.

- U for until
- U^- for flat until, $A\mathbf{U}^-B$ implicitly means that A is just a propositional formula without temporal operators.
- $\mathsf{F}A$ iff $\top\mathbf{U}A$
- G (or $\Box$) for always hold in the future.
- $\mathsf{G}A$ iff $\neg\mathsf{F}\neg A$.

Satisfaction Relation

- $\pi, i \models p$, for $p \in Prop$, iff $p \in \pi(i)$
- $\pi, i \models \mathsf{X}A$ iff $\pi, i+1 \models A$
- $\pi, i \models \mathsf{F}A$ iff there is $j \geq i$ such that $\pi, j \models A$
- $\pi, i \models A\mathsf{U}B$ iff there is $j \geq i$ such that $\pi, j \models B$ and $\pi, j' \models A$ for $i \leq j' < j$
- we write $\pi \models A$ if $\pi, 0 \models A$.
- SAT for LTL($\cdots$): determining whether a given formula A in LTL($\cdots$) is satisfiable, i.e.,there is a linear-time structure π such that $\pi \models A$.
- SAT for LTL(X, F) is PSPACE-complete.
- SAT for LTL(U) is PSPACE-complete
- LTL(F) is nothing but S4.3Dum (also called S4.3.1 or D) SAT for S4.3Dum is NP-complete by H. Ono and A. nakamura in 1980 [Studia Logic 39(4), 325-333, 1980]
- LTL(X) is KDAlt$_1$. SAT for LTL(X) is studied in P. Y. Schobbens and J.F. Raskin. [The Logic of "initially" and "next": complete axiomatization and complexity. IPL 69(5), 221-225,1999]
- Prop(A) is the set of propositional variables occurring in A.
- th(A), the temporal height of A, is the maximum number of nested temporal operators.

- $\mathrm{LTL}^k_m(\cdots)$ denotes the class of formulas $A \in$L$(\cdots)$ such that th$(A) \leq m$ and A has at most m variables.

- Likewise for $\mathrm{LTL}^k(\cdots)$ and $\mathrm{LTL}_m(\cdots)$.

- Example $(p \to \mathsf{XF}q)\mathsf{U}(\neg\mathsf{X}p) \in \mathrm{LTL}^3_2(\mathsf{X},\mathsf{U},\mathsf{F})$

Model Checking Problem.

- A Kripke structure $T = (S, R, \epsilon)$: S is a non-empty set of states; $R \subseteq S \times S$ is a *total* relation, i.e., for any $s_1 \in S$ there is at leat one $s_2 \in S$ such that $s_1 R s_2$; and $\epsilon : S \to \mathcal{P}(Prop)$

- A path in T is an infinite sequence $s_0, s_1, \cdots$, such that $s_i R s_{i+1}$ for each i.

- A path in T, together with ϵ, is nothing but a linear time structure. And inversely, a linear-time structure is a (simple) Kripke structure.

- path(T) is the set of all pathes in T.

- (Traditionally) $T \models A$ if and only if $\pi \models A$ for all $\pi \in path(T)$.

- (Traditionaly) $T, s \models A$ iff $\pi \models A$ **for all** $\pi \in path(T)$ starting from s.

- (But this paper) $T, s \models A$ iff $\pi \models A$ **for some** $\pi \in path(T)$ starting from s.

- MC(LTL$(\cdots)$) is the problem of determining whether $T, s \models A$ for a given Kripke structure T, a state $s \in T$ and a formula $A \in$ LTL$(\cdots)$.

Tiling Problem:

- A set of colors $C = \{c_1, \cdots, c_l\}$.

- A set of tile type $D \subseteq C^4$. each $d \in D$ has the form $(c_{up}, c_{right}, c_{down}, c_{left}\}$.

- A tile is a unit square with a type d (left side colored by c_{left}, $\cdots$,). Please note that we can not rotated

- A region $\mathcal{R} \subseteq \mathbb{Z}^2$. My understanding, (i, j) represents the grid with vertices $(i, j), (i, j + 1), (i + 1, j + 1), (i + 1, j)$.

- Two grid (i_1, j_1) and (i_2, j_2) are neighboring if they share an edge, that is, if

$$((i_1 = i_2) \wedge (|j_1 - j_2| = 1))\text{xor}((j_1 = j_2) \wedge |i_1 - i_2| = 1).$$

- A tiling for a region $\mathcal{R}$ is a map $t : R \to D$ such that any two neighboring tiles have matching colors on the shared edge.
- Informally, $t(i, j) = d$ means that the grid (i, j) is paved by a tile with type d.
- TILING PROBLEM: Instance: D and two colors $c_0, c_1 \in C$. Query: does there exists m and a tiling for the region $n \times m$ such that the bottom line of the region is colored with c_0, and the top line is colored with c_1, here $n = |D|$, i.e., the number of types in D.
- Tiling Problem is PSPACE-complete, where is the citation?

Reduction from tiling problem to MC(LTL).
$D = \{d_1, \cdots, d_n\}$, C, c_0, c_1. Define

$$Prop = \{lmost, rmost, end\} \cup \{x = c \mid x \in \{up, right, down, left\}, c \in C\}$$

$$\begin{array}{lcl}
S_D & = & \{s(0), s(n+1), s(e)\} \cup \{s(d, i) \mid d \in D, i = 1, \cdots, n\} \\
R & = & \{(s(0), s(d, 1)) \mid d \in D\} \cup \{(s(d, n), s(n+1)) \mid d \in D\} \cup \\
 & & \{(s(n+1), s(e)), (s(e), s(e))\} \cup \\
 & & \{(s(d', i), s(d, i+1)) \mid d', d \in D, i = 1, \cdots, n-1\} \\
\epsilon(s(0)) & = & \{lmost\}, \\
\epsilon(s(n+1)) & = & \{rmost\}, \\
\epsilon(s(e)) & = & \{end\}, \\
\epsilon(s(d, i)) & = & \{up = c_{up}, right = c_{right}, down = c_{down}, left = c_{letf} \mid \\
 & & \text{ if } d = (c_{up}, c_{right}, c_{down}, c_{left}).
\end{array}$$

Bottom line has color c_0 can be expressed as

$$\bigwedge_{k=1}^{n} \mathsf{X}^k (down = c_0)$$

Top line should have color c_1.

$$\mathsf{F}\left(lmost \wedge \left(\bigwedge_{k=1}^{k} \mathsf{X}^k (up = c_1) \right) \wedge \mathsf{X}^{n+2} end \right)$$

Neighboring tilts should have matching edges.

$$\mathsf{G}\left(\begin{array}{l} (right = c \to \mathsf{X}(rmost \vee left = c)) \wedge \\ (up = c \to \mathsf{X}^{n+2}(end \vee down = c)) \end{array} \right)$$

Theorem: MC(LTL) is PSPACE-hard.
Natural Deduction System

$$\vdash \mathsf{X}A \vee \mathsf{X}\neg A, \quad \vdash A \mathsf{U} \neg A$$

$$B \vdash A\mathsf{U}B, \quad A \wedge (A\mathsf{U}B) \vdash \mathsf{F}B$$

$$(\mathsf{X}^n B) \wedge \left(\bigwedge_{k=0}^{n-1} \mathsf{X}^k A \right) \vdash A\mathsf{U}B, \quad n \geq 1,$$

$$(\mathsf{X}^n(\neg A \wedge \neg B)) \wedge \left(\bigwedge_{k=0}^{n-1} \mathsf{X}^k A \right) \vdash \neg(A\mathsf{U}B), \quad n \geq 1,$$

$$A \wedge \mathsf{X}(A\mathsf{U}B) \vdash A\mathsf{U}B$$

$$\mathsf{X}(A \circ B) \vdash\dashv \mathsf{X}A \circ \mathsf{X}B, \quad \circ \in \{\wedge, \vee\}$$

$$\mathsf{F}(A \vee B) \vdash\dashv \mathsf{F}A \vee \mathsf{F}B$$

$$\mathsf{F}(A \wedge B) \vdash\dashv \mathsf{F}A \wedge \mathsf{F}B$$

$$A \wedge \mathsf{X}A \wedge (A\mathsf{U}B) \vdash \mathsf{X}(A\mathsf{U}B)$$

$$A \vdash \mathsf{F}A, \quad \mathsf{X}A \vdash \mathsf{F}A, \quad \mathsf{FF}A \vdash \mathsf{F}A$$

$$\frac{A \vdash B}{\mathsf{X}A \vdash \mathsf{X}B}, \quad \frac{A \vdash B}{\mathsf{F}A \vdash \mathsf{F}B}$$

$$\frac{A \vdash C, B \vdash D}{(A \mathsf{U} B) \vdash (C \mathsf{U} D)}$$

$$\frac{\vdash A}{\vdash \mathsf{F} A}, \quad \frac{\vdash A}{\vdash \neg \mathsf{F} \neg A}, \quad \frac{\vdash A}{\vdash \mathsf{X}^n A}, \quad n \geq 1$$

$\mathrm{SAT}(\mathrm{LTL}_n(H_1, \cdots)) \leq_{\mathrm{logs}} \mathrm{MC}(\mathrm{LTL}_n(H_1, \cdots))$
Consider $\varphi \in \mathrm{LTL}_n(\cdots)$ s.t.$\mathrm{Prop}(\varphi) \subseteq \{A_1, \cdots, A_n)$.
Define $T := (N, R, \epsilon)$

- $N = \mathrm{Pow}(\{A_1, \cdots, A_n\})$
- R is the full relation, i.e. $N \times N$.
- $\epsilon(s)$ is the valuation determined by s.

φ is SAT $\iff \exists s \in N$ s.t. $T, s \models \varphi$. Pick some s_0 we have

$$(\exists s \in N,\ T, s \models \varphi) \iff T, s_0 \models \mathsf{X}\varphi \iff T, s_0 \models \mathsf{F}\varphi$$

$\mathrm{MC}(\mathrm{LTL}(\cdots)) \leq_{\mathrm{logs}} \mathrm{MC}(\mathrm{LTL}_2(\mathsf{U}))$
Consider an arbitrary structure $T(N, R, \epsilon)$ and a formula $\varphi \in \mathrm{LTL}(\cdots)$. Suppose *varphi* contains n propositional atoms $P_1, \cdots, P_n$. We shall define a new structure $D_n(T) := (N', R', \epsilon')$ over $\{A, B\}$.

$$\begin{aligned}
&N' := \{(s, i) \mid s \in N, 1 \leq i \leq 2n+2\} \\
&(s, i) R' (t, j) \iff \begin{cases} s = t \text{ and } j = i + 1, \text{ or} \\ sRt \text{ and } i = 2n+2, j = 1 \end{cases} \\
&\epsilon'((s, 1)) := \{A, B\} \\
&\epsilon((s, 2)) = \{\ \} \\
&\epsilon((s, 2i+1)) = \{A\} \\
&\epsilon((s, 2i+2)) = \begin{cases} \{B\} & \text{if } Pi \in \epsilon(s) \\ \{\ \} & \text{otherwise} \end{cases}
\end{aligned}$$

$(s, 2i+1), s(s, 2i+2)$ together encode the truth of P_i in $\epsilon(s)$. $A, \neg B$ always hold in $(s, 2i+1)$. $\neg A$ always holds in $(s, 2i+2)$. Whether B holds in $(s, 2i+2)$ depends whether P_i holds in s.

Let At_D be $A \wedge B$. Define

$$
\begin{aligned}
&Alt_n^0 := At_D = A \wedge B\\
&Alt_n^1 := \neg B \wedge A \wedge \left(A\mathsf{U}^- \left(\neg A \wedge \left(\neg A\mathsf{U}^- Alt_n^0\right)\right)\right)\\
&Alt_n^{k+1} := \neg B \wedge A \wedge \left(A\mathsf{U}^- \left(\neg A \wedge \left(\neg A\mathsf{U}^- Alt_n^k\right)\right)\right)
\end{aligned}
$$

For $k \geq 1$, Alt_n^k means there remain exactly k many "$A - \neg A$" alternations before the next state satisfying $A \wedge B$.

Define $D_n(\varphi)$ inductively.

$$
\begin{aligned}
&D_n(P_i) := A\mathsf{U}^- \left(\neg At_D \wedge \neg At_D\mathsf{U}^- \left(Alt_n^{n+1-i} \wedge (A\mathsf{U}^- B)\right)\right)\\
&D(\neg\varphi) = \neg D_n(\varphi)\\
&D_n(\varphi \wedge \psi) := D_n(\varphi) \wedge D_n(\psi)\\
&D_n(\mathsf{X}\varphi) := At_D\mathsf{U}^- \left(\neg A \wedge \neg B \wedge \left(\neg At_D\mathsf{U}^-(At_D \wedge D_n(\varphi)\right)\right)\\
&D_n(\mathsf{F}\varphi) := F(At_D \wedge D_n(\varphi))\\
&D_n(\varphi\mathsf{U}^-\psi) := (At_D \to D_n(\varphi))\mathsf{U}(At_D \wedge D_n(\psi))
\end{aligned}
$$

Model checking for $\mathrm{LTL}_2(\mathsf{U}^-)$ is PSPACE-complete since MC(LTL(X,F)) is PSPACE-complete.

$\mathrm{MC}(\mathrm{LTL}(\cdots)) \leq_{\mathrm{logs}} \mathrm{MC}(\mathrm{LTL}_1(\mathsf{X}, \cdots))$.

Given a Kripke structure $T = (N, R, \epsilon)$ and a formula $\varphi \in \mathrm{LTL}(\cdots)$ with propositions $P_1, \cdots, P_n$. Define $C_n := (N', R', \epsilon')$ as follows.

$$
\begin{aligned}
&N' := \{(s,i) \mid s \in N, 1 \leq i \leq 2n+2\}\\
&(s,i)R'(t,j) \iff \left(\begin{array}{l} s = t, j = i+1, \text{ or}\\ sRt, i = 2n+2, j = 1 \end{array}\right)\\
&\epsilon'((s,1)) = \epsilon'(s,2) := \{A\}\\
&\epsilon'((s,2i+1)) := \{\ \}\\
&\epsilon'((s,2i+2)) := \begin{cases} \{A\} & \text{if } P_i \in \epsilon(s)\\ \{\ \} & \text{otherwise} \end{cases}
\end{aligned}
$$

For $i \geq 1$, we use truth values of A in $(s, 2i+1)$ and $(s, 2i+2)$ to encode the truth of P_i in s. $\neg A - \neg A$ means $\neg P_i$, and $\neg A - A$ means P_i. That is, A never holds in $(s, 2i+1)$.

Let $At_C := A \wedge \mathsf{X}A \wedge \mathsf{X}^2\neg A$. Define

$$
\begin{aligned}
&C_n(P_i) := \mathsf{X}^{2i+1}A \\
&C_n(\neg\varphi) := \neg C_n(\varphi) \\
&C_n(\varphi \wedge \psi) := C_n(\varphi) \wedge C_n(\psi) \\
&C_n(\mathsf{X}\varphi) := \mathsf{X}^{2n+2}C_n(\varphi) \\
&C_n(\mathsf{F}\varphi) := \mathsf{F}(At_C \wedge C_n(\varphi)) \\
&C_n(\varphi\mathsf{U}\psi) := (At_C \to C_n(\varphi))\mathsf{U}(At_C \wedge C_n(\psi))
\end{aligned}
$$

We have

$$(T, s \models \varphi) \Longleftrightarrow (C_n(T), (s, 1) \models C_n(\varphi))$$

Model checking for $\mathrm{LTL}_1(\mathsf{X},\mathsf{F})$) is PSPACE-complete.

We have the similar results for SAT.
$\mathrm{MC}(\mathrm{LTL}(\cdots)) \leq_{\mathrm{logs}} \mathrm{MC}(\mathrm{LTL}_1(\mathsf{X}, \cdots))$.
$\mathrm{MC}(\mathrm{LTL}(\cdots)) \leq_{\mathrm{logs}} \mathrm{MC}(\mathrm{LTL}_2(\mathsf{U}))$
$\mathrm{SAT}(\mathrm{LTL}_2(\mathsf{U}))$ is PSPACE-complete
$\mathrm{SAT}(\mathrm{LTL}_1(\mathsf{X},\mathsf{F}))$ is PSPACE-complete

Non-deterministic finite ω-automata

$$M = (Q, \Sigma, \delta, q_0, Acc)$$

1.

2.

3. $\delta : Q \times \Sigma \to \mathrm{Pow}(Q)$ transition function

4.

5. Acc acceptance component given as.
   - $F \subseteq Q$, or
   - $\mathcal{F} \subseteq \mathrm{Pow}(Q)$, or
   - $\Omega = \{(E_i, F_i) \mid E_i, F_i \subseteq Q, i = 1, \cdots, n\}$

A run of M on $\alpha = a_1 a_2 \cdots \in \Sigma^\omega$ is an infinite sequence of states $\mathbf{r} = r_0 r_1 r_2 \cdots \in Q^\omega$ such that

$r_0 = q_0$
$r_{i+1} \in \delta(q_i, a_{i+1})$

Büchi automata $M = (Q, \Sigma, \delta, q_0, F)$ with $F \subseteq Q$.

We say M accept α iff there is a run $\mathbf{r}$ of M on α such that there is a state $q \in F$ such that it occurs in $\mathbf{r}$ infinitely often.

$$L(M) := \{\alpha \mid M \text{ accept } \alpha\}$$

is called the language recognized by M.

A ω-language) $A \subseteq \Sigma^\omega$ is called regular if there is a Büchi automata M such that $A = L(M)$.

1. If $A \subseteq \Sigma^*$ is a regular language then A^ω is a regular ω-language.

2. (Büchi Characterization Theorem) Every regular ω-language A is of the form
$$A = \bigcup_{i=1}^{n} A_i B_i^\omega$$
where $A_i, B_i \subseteq \Sigma^*$ are regular languages.