A Supplementary Material: Proof Appendix

Proposition 3 Let φ be a CTL formula, then $\varphi \equiv_{\langle V',I\rangle} T_\varphi$.

Proof. (sketch) This can be proved from T_i to T_{i+1} ($0 \leq i < n$) by using one transformation rule on T_i. We will prove this proposition from the following several aspects:

(1) $\varphi \equiv_{\langle \{p\},\emptyset\rangle} T_0$.

($\Rightarrow$) $\forall(\mathcal{M}_1, s_1) \in Mod(\varphi)$, *i.e.* $(\mathcal{M}_1, s_1) \models \varphi$. We can construct an Ind-model structure $\mathcal{M}_2$ is identical to $\mathcal{M}_1$ except $L_2(s_2) = L_1(s_1) \cup \{p\}$. It is apparent that $(\mathcal{M}_2, s_2) \models T_0$ and $(\mathcal{M}_1, s_1) \leftrightarrow_{\langle\{p\},\emptyset\rangle} (\mathcal{M}_2, s_2)$.

($\Leftarrow$) $\forall(\mathcal{M}_1, s_1) \in Mod(T_0)$, it is apparent that $(\mathcal{M}_1, s_1) \models \varphi$ by the sematic of **start**.

By $\psi \rightarrow_t R_i$ we mean using transformation rules t on formula ψ (the formulae ψ as the premises of rule t) and obtaining the set R_i of transformation results. Let X be a set of formulas we will show $T_i \equiv_{\langle V',I\rangle} T_{i+1}$ by using the transformation rule t. Where $T_i = X \cup \{\psi\}, T_{i+1} = X \cup R_i$, V' is the set of atoms introduced by t and I is the set of indexes introduced by t. (We will prove this result in $t \in$ {Trans(1), Trans(4), Trans(6)}, other cases can be proved similarly.)

(2) For t=Trans(1):

($\Rightarrow$) $\forall(\mathcal{M}_1, s_1) \in Mod(T_i)$ *i.e.* $(\mathcal{M}_1, s_1) \models X \wedge \mathrm{AG}(q \supset \mathrm{EX}\varphi)$

$\Rightarrow (\mathcal{M}_1, s_1) \models X$ and for every π starting from s_1 and every state $s_1^j \in \pi$, $(\mathcal{M}, s_1^j) \models \neg q$ or there exists a path π' starting from s_1^j such that there exists a state s_1^{j+1} such that $(s_1^j, s_1^{j+1}) \in R_1$ and $(\mathcal{M}, s_1^{j+1}) \models \varphi$

We can construct an Ind-model structure $\mathcal{M}_2$ is identical to $\mathcal{M}_1$ except $[ind]_2 = \bigcup_{s\in S} R_s \cup R_y$, where $R_{s_1^j} = \{(s_1^j, s_1^{j+1}), (s_1^{j+1}, s_1^{j+2}), \dots\}$ and $R_y = \{(s_x, s_y) | \forall s_x \in S$ if $\forall(s_1', s_2') \in \bigcup_{s\in S} R_s, s_1' \neq s_x$ then find a unique $s_y \in S$ such that $(s_x, s_y) \in R\}$. It is apparent that $(\mathcal{M}_1, s_1) \leftrightarrow_{\langle\emptyset,\{ind\}\rangle} (\mathcal{M}_2, s_2)$ (let $s_2 = s_1$).

$\Rightarrow$ for every path starting from s_1 and every state s_1^j in this path, $(\mathcal{M}_2, s_1^j) \models \neg q$ or $(\mathcal{M}_2, s_1^j) \models \mathrm{EX}\varphi_{\langle ind\rangle}$ (by the semantic of EX)

$\Rightarrow (\mathcal{M}_2, s_1) \models \mathrm{AG}(q \supset \mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi)$

$\Rightarrow (\mathcal{M}_2, s_1) \models X \wedge \mathrm{AG}(q \supset \mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi)$

($\Leftarrow$) $\forall(\mathcal{M}_1, s_1) \in Mod(T_{i+1})$ *i.e.* $(\mathcal{M}_1, s_1) \models X \wedge \mathrm{AG}(q \supset \mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi)$

$\Rightarrow (\mathcal{M}_1, s_1) \models X$ and $(\mathcal{M}_1, s_1) \models \mathrm{AG}(q \supset \mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi)$

$\Rightarrow$ for every path starting from s_1 and every state s_1^j in this path, $(\mathcal{M}_1, s_1^j) \models \neg q$ or there exits a state s' such that $(s_1^j, s') \in [ind]_1$ and $(\mathcal{M}_1, s') \models \varphi$ (by the semantic of $\mathrm{E}_{\langle ind\rangle}\mathrm{X}$)

$\Rightarrow$ for every path starting from s_1 and every state s_1^j in this path, $(\mathcal{M}_1, s_1^j) \models \neg q$ or $(\mathcal{M}_1, s_1^j) \models \mathrm{EX}\varphi$ (by the semantic of EX)

$\Rightarrow (\mathcal{M}_1, s_1) \models \mathrm{AG}(q \supset \mathrm{EX}\varphi)$

$\Rightarrow (\mathcal{M}_1, s_1) \models X \wedge \mathrm{AG}(q \supset \mathrm{EX}\varphi)$

It is apparent that $(\mathcal{M}_1, s_1) \leftrightarrow_{\langle\emptyset,\{ind\}\rangle} (\mathcal{M}_1, s_1)$.

(3) For t=Trans(4):

($\Rightarrow$) $\forall(\mathcal{M}_1, s_1) \in Mod(T_i)$, *i.e.* $(\mathcal{M}_1, s_1) \models X \wedge \mathrm{AG}(q \supset \varphi_1 \vee \varphi_2)$

$\Rightarrow (\mathcal{M}_1, s_1) \models X$ and $\forall s_1' \in S, (\mathcal{M}_1, s_1') \models q \supset \varphi_1 \vee \varphi_2$

$\Rightarrow (\mathcal{M}_1, s_1') \models \neg q$ or $(\mathcal{M}_1, s_1') \models \varphi_1 \vee \varphi_2$

The we can construct an Ind-model structure $\mathcal{M}_2$ as follows. $\mathcal{M}_2$ is the same with $\mathcal{M}_1$ when $(\mathcal{M}_1, s_1') \models \neg q$. When $(\mathcal{M}_1, s_1') \models q$, $\mathcal{M}_2$ is identical to $\mathcal{M}_1$ except if $(\mathcal{M}_1, s_1') \models \varphi_1$ then $L_2(s_1') = L_1(s_1')$ else $L_2(s_1') = L_1(s_1') \cup \{p\}$. It is apparent that $(\mathcal{M}_2, s_1') \models (q \supset \varphi_1 \vee p) \wedge (p \supset \varphi_2)$, then $(\mathcal{M}_2, s_1) \models T_{i+1}$ and $(\mathcal{M}_1, s_1) \leftrightarrow_{\langle\{p\},\emptyset\rangle} (\mathcal{M}_2, s_2)$.

($\Leftarrow$) $\forall(\mathcal{M}_1, s_1) \in Mod(T_{i+1})$, *i.e.* $(\mathcal{M}_1, s_1) \models X \wedge \mathrm{AG}(q \supset \varphi_1 \vee p) \wedge \mathrm{AG}(p \supset \varphi_2)$. It is apparent that $(\mathcal{M}_1, s_1) \models T_i$.

(4) For t=Trans(6):

We prove for $\mathrm{E}_{\langle ind\rangle}\mathrm{X}$, while for the AX can be proved similarly.

($\Rightarrow$) $\forall(\mathcal{M}_1, s_1) \in Mod(T_i)$, *i.e.* $(\mathcal{M}_1, s_1) \models X \wedge \mathrm{AG}(q \supset \mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi)$

$\Rightarrow (\mathcal{M}_1, s_1) \models X$ and $\forall s_1' \in S, (\mathcal{M}_1, s_1') \models q \supset \mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi$

$\Rightarrow (\mathcal{M}_1, s_1') \models \neg q$ or there exists a state s' such that $(s_1', s') \in [ind]$ and $(\mathcal{M}_1, s') \models \varphi$

We can construct an Ind-model structure $\mathcal{M}_2$ as follows. $\mathcal{M}_2$ is the same with $\mathcal{M}_1$ when $(\mathcal{M}_1, s_1') \models \neg q$. When $(\mathcal{M}_1, s_1') \models q$, $\mathcal{M}_2$ is identical to $\mathcal{M}_1$ except for s' there is $L_2(s') = L_1(s') \cup \{p\}$. It is apparent that $(\mathcal{M}_2, s_1) \models \mathrm{AG}(q \supset \mathrm{E}_{\langle ind\rangle}\mathrm{X}p) \wedge \mathrm{AG}(p \supset \varphi)$, $(\mathcal{M}_2, s_2) \models T_{i+1}$ and $(\mathcal{M}_1, s_1) \leftrightarrow_{\langle\{p\},\emptyset\rangle} (\mathcal{M}_2, s_2)$ ($s_2 = s_1$).

($\Leftarrow$) $\forall(\mathcal{M}_1, s_1) \in Mod(T_{i+1})$, *i.e.* $(\mathcal{M}_1, s_1) \models X \wedge \mathrm{AG}(q \supset \mathrm{E}_{\langle ind\rangle}\mathrm{X}p) \wedge \mathrm{AG}(p \supset \varphi)$. It is apparent that $(\mathcal{M}_1, s_1) \models T_i$.

$\square$

Proposition 4 Let φ be a CTL formula, then $T_\varphi \equiv_{\langle V\cup V',\emptyset\rangle} Res$.

Proof. (sketch) This can be proved from T_i to T_{i+1} ($0 \leq i < n$) by using one resolution rule on T_i.

By $\psi \rightarrow_r R_i$ we mean using resolution rules r on set ψ (the formulae in ψ as the premises of rule r) and obtaining the set R_i of resolution results. we will show $T_i \equiv_{\langle V,I\rangle} T_{i+1}$ by using the resolution rule r. Where $T_i = X \cup \psi$, $T_{i+1} = X \cup R_i$, X be a set of $\mathrm{SNF}^g_{\mathrm{CTL}}$ clauses, p be the proposition corresponding with literal l used to do resolution in r.

(1) If $\psi \rightarrow_r R_i$ by an application of $r \in$ {**(SRES1)**, ..., **(SRES8)**, **RW1**, **RW2**}, then $T_i \equiv_{\langle\{p\},\emptyset\rangle} T_{i+1}$.

On one hand, it is apparent that $\psi \models R_i$ and then $T_i \models T_{i+1}$. On the other hand, $T_i \subseteq T_{i+1}$ and then $T_{i+1} \models T_i$.

(2) If $\psi \rightarrow_r R_i$ by an application of $r =$**(ERES1)**, then $T_i \equiv_{\langle\{l, w^{\mathrm{A}}_{\neg l}\},\emptyset\rangle} T_{i+1}$.

It has been proved that $\psi \models R_i$ in (Bolotov 2000), then there is $T_{i+1} = T_i \cup \Lambda^{\mathrm{A}}_{\neg l}$ and then $\forall(\mathcal{M}_1, s_1) \in Mod(T_i = X \cup \psi)$ there is a $(\mathcal{M}_2, s_2) \in Mod(T_{i+1} = T_i \cup \Lambda^{\mathrm{A}}_{\neg l})$ s.t. $(\mathcal{M}_1, s_1) \leftrightarrow_{\langle\{p, w^{\mathrm{A}}_{\neg l}\},\emptyset\rangle} (\mathcal{M}_2, s_2)$ and vice versa by Proposition 3.

For rule **(ERES2)** we have the same result.

$\square$

Proposition 6 Let $V'' = V \cup V'$, $\Gamma = Instantiate(Res, V')$ and $\Gamma_1 = Removing\_atoms\ (Connect(\Gamma), \Gamma)$, then $\Gamma_1 \equiv_{\langle V'',\emptyset\rangle} Res$ and $\Gamma_1 \equiv_{\langle V'',I\rangle} \varphi$.

Proof. Take note the fact that for each clause $C = T \supset H$ in *Connect*(Γ), if $\Gamma \cap Var(C) \neq \emptyset$ then there must be an atom $p \in \Gamma \cap Var(H)$. It is apparent that *Connect*$(\Gamma) \models \Gamma_1$, we will show $\forall(\mathcal{M}, s_0) \in Mod(\Gamma_1)$ there is a $(\mathcal{M}', s_0)$ such that $(\mathcal{M}', s_0) \models Connect(\Gamma)$ and $(\mathcal{M}, s_0) \leftrightarrow_{\langle \Gamma, \emptyset \rangle} (\mathcal{M}', s_0)$. Let $C = T \supset H$ in *Connect*(Γ) with $\Gamma \cap Var(C) \neq \emptyset$, $\forall(\mathcal{M}, s_0) \in Mod(\Gamma_1)$ we construct $(\mathcal{M}', s_0)$ as $(\mathcal{M}, s_0)$ except for each $s \in S$, if $(\mathcal{M}, s) \not\models T$ then $L'(s) = L(s)$, else:

(i) if $(\mathcal{M}, s) \models H$, then $L'(s) = L(s)$;

(ii) else if $(\mathcal{M}, s) \models T$ with $p \in Var(H) \cap \Gamma$, then if p appearing in H negatively, then if C is a global (or an initial) clause then let $L'(s) = L(s) \setminus \{p\}$ else let $L'(s^*) = L(s^*) \setminus \{p\}$ for (each (if C is an A-step or A-sometime clause)) $s^* \in \pi_s$, else if C is a global (or an initial) clause then let $L'(s) = L(s) \cup \{p\}$ else let $L'(s^*) = L(s^*) \cup \{p\}$ for (each (if C is a A-step or A-sometime clause)) $s^* \in \pi_s$. Where s^* is a next or future state of s (it depends on the type of the clause: if the clause is a X-step ($X \in \{\text{A}, \text{E}\}$) clause then s^* is the next state, else if the clause is a X-sometime clause then s^* is a future state).

It is apparent that $(\mathcal{M}, s_0) \leftrightarrow_{\langle \Gamma, \emptyset \rangle} (\mathcal{M}', s_0)$, we will show that $(\mathcal{M}', s_0) \models Connect(\Gamma)$ from the following two points:

(1) For (i), it is apparent $(\mathcal{M}', s_0) \models C$;

(2) For (ii) talked-above, we show it from the form of $\text{SNF}^g_{\text{CTL}}$ clauses. Supposing C_1 and C_2 are instantiate formula of Γ:

  (a) If C is a global clause, i.e. $C = \top \supset p \vee C_1$ with C_1 is a disjunction of literals (we suppose p appearing in C positively). If there is a $C' = \top \supset \neg p \vee C_2 \in Connect(\Gamma)$, then there is $\top \supset C_1 \vee C_2 \in Connect(\Gamma)$ by the resolution ($(\mathcal{M}, s) \models C_2$ due to we have suppose $(\mathcal{M}, s) \not\models C$). It is apparent that $(\mathcal{M}', s_0) \models C \wedge C'$.

  (b) If $C = T \supset \text{E}_{\langle ind \rangle}\text{X}(p \vee C_1)$. If there is a $C' = T' \supset \text{E}_{\langle ind \rangle}\text{X}(\neg p \vee C_2) \in Connect(\Gamma)$, then there is $T \wedge T' \supset \text{E}_{\langle ind \rangle}\text{X}(C_1 \vee C_2) \in Connect(\Gamma)$ by the resolution ($(\mathcal{M}, s) \models \text{E}_{\langle ind \rangle}\text{X}C_2$ due to we have suppose $(\mathcal{M}, s) \not\models C$). It is apparent that $(\mathcal{M}', s_0) \models C \wedge C'$.

  (c) Other cases can be proved similarly.

Therefore, we have $\Gamma_1 \equiv_{\langle V'', \emptyset \rangle} Res$ by Proposition 2 and Proposition 5.

And then $\Gamma_1 \equiv_{\langle V'', I \rangle} \varphi$ follows. $\square$

proposition 10 Let φ be a CTL formula and $V \subseteq \mathcal{A}$. The time and space complexity of Algorithm 1 are $O((m+1)2^{4(n+n')}$. Where $|Var(\varphi)| = n$, $|V'| = n'$ (V' is set of atoms introduced in transformation) and m is the number of indices introduced during transformation.

Proof. It follows from the lines 19-31 of the algorithm 1, which is to compute all the possible resolution. The possible number of $\text{SNF}^g_{\text{CTL}}$ clauses under the give V, V' and Ind is $(m+1)2^{4(n+n')} + (m*(n+n')+n+n'+1)2^{2(n+n')+1})$. $\square$