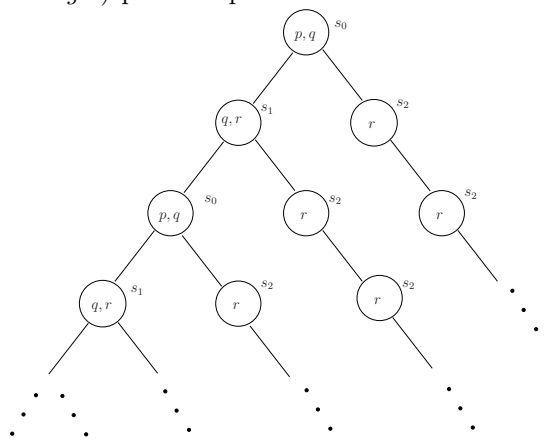
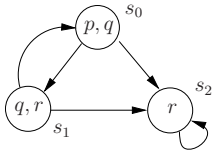
Lógica CTL

Aula 13

Lógica de tempo ramificado - CTL

A evolução de um sistema de transições corresponde a uma árvore de computação infinita. A lógica CTL (*Computation Tree Logic*) permite quantificação (existencial) sobre os caminhos dessa árvore.





Lógica de tempo ramificado - CTL

AP, conjunto de variáveis proposicionais $p, q, r, s, \ldots$

Sintaxe

$$\begin{aligned}\varphi \quad ::= \quad & \mathsf{true} \mid \mathsf{false} \mid p \mid (\neg\varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi) \mid (\varphi \rightarrow \varphi) \mid (\mathrm{AX}\varphi) \mid \\ & (\mathrm{EX}\varphi) \mid (\mathrm{AF}\varphi) \mid (\mathrm{EF}\varphi) \mid (\mathrm{AG}\varphi) \mid (\mathrm{EG}\varphi) \mid \mathrm{A}[\varphi \mathrm{U} \varphi] \mid \mathrm{E}[\varphi \mathrm{U} \varphi]\end{aligned}$$

Conectivas Temporais

A significa *ao longo de todos os caminhos* (a partir dum estado)

E significa *ao longo de pelo menos um caminho* (a partir dum estado)

F,G,X e U como no LTL

Lógica de tempo ramificado - CTL

As conectivas A e E só podem aparecer junto de uma das outras conectivas temporais.

Convensão de prioridades (omissão de parêntesis)

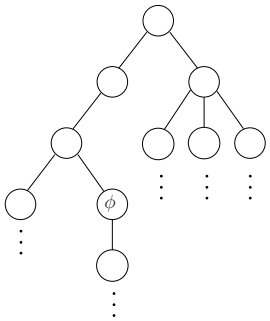
- As conectivas unárias ($\neg$, AX,EX, AF,EF,AG e EG) têm prioridade mais alta
- Depois as conectivas $\wedge$ e $\vee$.
- Depois as conectivas $\rightarrow$, AU e EU (estas duas últimas são escritas em notação infixa e prefixa simultaneamente)

Exemplos

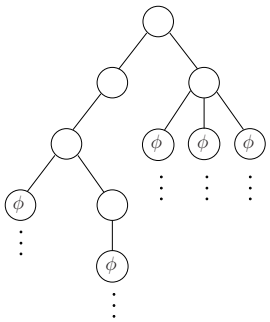
$\mathrm{AG}(p \rightarrow \mathrm{EG}r)$
$\mathrm{EFE}[r\mathrm{U}q]$
$\mathrm{E}[\mathrm{A}[r\mathrm{U}p]\mathrm{U}q]$
$\mathrm{A}[\mathrm{AX}\neg p\mathrm{UE}[\mathrm{EX}(p \wedge q)\mathrm{U}\neg p]]$

1 Semântica do CTL

Semântica do CTL

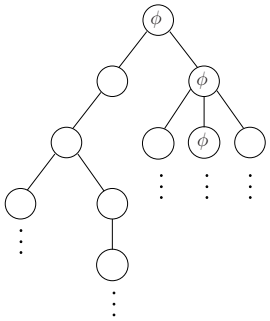


$\mathrm{EF}\phi$

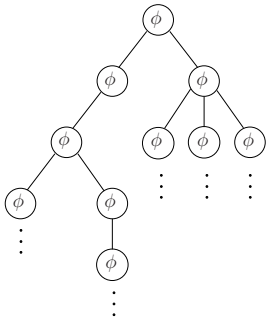


AFϕ

Semântica do CTL



EGϕ



AGϕ

Exemplos:

Exprime as propriedades seguintes através de fórmulas em CTL.

- Existe um estado atingível onde se verifica p.EFp
- A partir de todos os estados atingíveis, onde se verifica p, é possível manter p continuamente verdadeiro até chegar a um estado onde se verifica q.AG$(p \rightarrow \mathrm{E}p\mathrm{U}q)$
- Sempre que se chega a um estado onde se verifica p, é possível manter q verdadeiro para sempre. AG$(p \wedge \mathrm{AG}q)$
- Existe um estado atingível, a partir do qual se verifica p em todos os estados atingíveis. EFAGp

Sempre e Potencialmente

- EF$\varphi = \mathrm{E}\mathsf{true}\mathrm{U}\varphi$, φ *verifica-se potencialmente*

- $\mathrm{AF}\varphi = \mathrm{A}\mathsf{true}\mathrm{U}\varphi$, φ *verifica-se inevitavelmente*
- $\mathrm{EG}\varphi = \neg\mathrm{AF}\neg\varphi$, φ *verifica-se potencialmente sempre*
- $\mathrm{AG}\varphi = \neg\mathrm{EF}\neg\varphi$, φ *invariavelmente*
- $\mathrm{AGAF}\varphi$, φ verifica-se um n.i.d.v. em todos os caminhos.

Exemplos

- Exclusão mútua (*segurança*): $\{A_0A_1A_2\ldots \mid \{c_1, c_2\} \not\subseteq A_i,\ i \geq 0, A_i \subseteq AP\}$

$$\mathrm{AG}(\neg c_1 \vee \neg c_2)$$

- P_i acede à seccão critica um n.i.d.v (*vivacidade/liveness*):

$$\{A_0A_1A_2\ldots \mid (\overset{\infty}{\exists}\ j.\ c_1 \in A_j) \wedge (\overset{\infty}{\exists}\ j.\ c_2 \in A_j)\}$$

$$\mathrm{AGAF}c_1 \wedge \mathrm{AGAF}c_2$$

- *starvation freedom* (vivacidade):

$$\{A_0A_1A_2\ldots \mid \forall i \in \{1,2\}, (\overset{\infty}{\exists}\ j.\ w_i \in A_j) \rightarrow (\overset{\infty}{\exists}\ j.\ c_i \in A_j)\}$$

$$(\mathrm{AGAF}w_1 \rightarrow \mathrm{AGAF}c_1) \wedge (\mathrm{AGAF}w_2 \rightarrow \mathrm{AGAF}c_2)$$

Semântica do CTL

Satisfazibilidade

Dado um sistema de transições $T = (S, Act, \longrightarrow, AP, I, L)$, um estado $s \in S$, para $\pi \in Paths(s)$ seja $\pi = s_0s_1\ldots$, $s_0 = s$ e $\pi[i] = s_i$ é o $i+1$ estado em π.

Dada uma fórmula φ e um estado s, define-se a relação de satisfabilidade $s \models \varphi$ indutivamente na estrutura de φ:

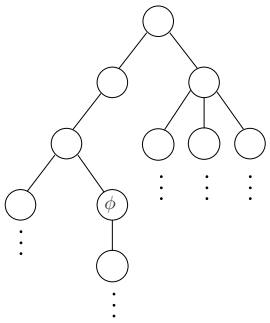
1. $s \models \mathsf{true}$ e $s \not\models \mathsf{false}$
2. $s \models p$ sse $p \in L(s)$
3. $s \models \neg\varphi$ sse $s \not\models \varphi$
4. $s \models \varphi\ \wedge\ \psi$ sse $s \models \varphi$ e $s \models \psi$
5. $s \models \varphi\ \vee\ \psi$ sse $s \models \varphi$ ou $s \models \psi$
6. $s \models \varphi \rightarrow \psi$ sse se $s \models \varphi$ então $s \models \psi$
7. $s \models \mathrm{AX}\varphi$ sse para todo $\pi \in Paths(s)$, $\pi[1] \models \varphi$
8. $s \models \mathrm{EX}\varphi$ sse existe $\pi \in Paths(s)$, $\pi[1] \models \varphi$

Semântica do CTL

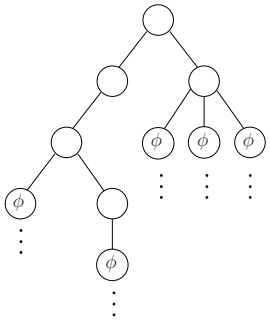
Satisfazibilidade (cont.)

9. $s \models \text{AG}\varphi$ sse para todos os caminhos $\pi \in Paths(s)$, se tem para todo $i \geq 0$ $\pi[i] \models \varphi$
10. $s \models \text{EG}\varphi$ sse existe um caminho $\pi \in Paths(s)$ tal que para todo $i \geq 0$, $\pi[i] \models \varphi$
11. $s \models \text{AF}\varphi$ sse para todos os caminhos $\pi \in Paths(s)$, existe $i \geq 0$ tal que $\pi[i] \models \varphi$
12. $s \models \text{EF}\varphi$ sse existe um caminho $\pi \in Paths(s)$ tal que existe $i \geq 0$ tal que $\pi[i] \models \varphi$
13. $\mathcal{M}, s \models \text{A}[\varphi_1 \text{U} \varphi_2]$ sse para todos os caminhos $\pi \in Paths(s)$, se tem que $\varphi_1 \text{U} \varphi_2$ é satisfeito, i.e. existe $i \geq 0$ $\pi[i] \models \varphi_2$, e para $0 \leq j < i$ $\pi[j] \models \varphi_1$
14. $s \models \text{E}[\varphi_1 \text{U} \varphi_2]$ sse existe um caminho $\pi \in Paths(s)$, tal que $\varphi_1 \text{U} \varphi_2$ é satisfeito, i.e. existe existe $i \geq 0$ $\pi[i] \models \varphi_2$, e para $0 \leq j < i$ $\pi[j] \models \varphi_1$.

Semântica do CTL

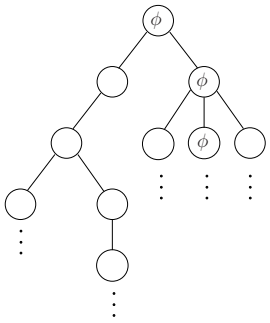


EFϕ

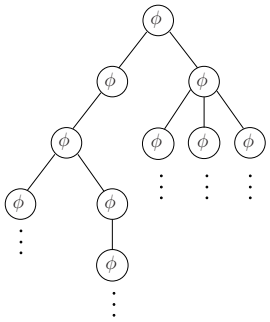


AFϕ

Semântica do CTL



EGϕ



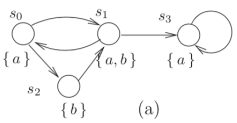
AGϕ

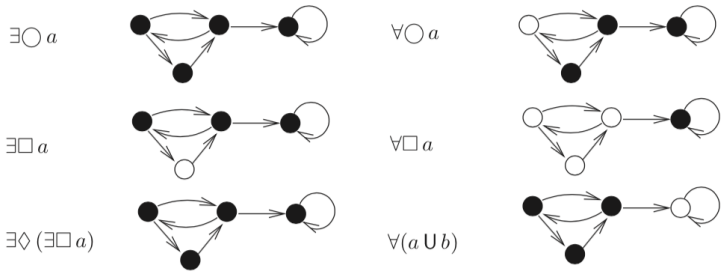
Semântica do CTL para sistemas de transições

- Dado um sistema $T = (S, Act, \longrightarrow, AP, I, L)$ e uma fórmula φ de CTL,
- O conjunto de satisfação para φ é $Sat(\varphi) = \{\ s \in S \mid s \models \varphi\ \}$
- T satisfaz φ i.e $T \models \varphi$ sse $\forall s_0 \in I, s_0 \models \varphi$ (i.e $I \subseteq Sat(\varphi)$)

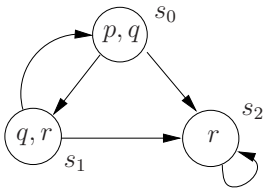
Exemplo

Indica quais os estados em que as seguintes fórmulas são satisfeitas: EXa, AXa, EGa, AGa, EFEGa e A[aUb],





Exemplo



1. $s_0 \models p \ \wedge \ q$
2. $s_0 \models \mathrm{EX}r$
3. $s_0 \models \neg\mathrm{AX}(q \ \wedge \ r)$
4. $s_0 \models \neg\mathrm{EF}(p \ \wedge \ r)$
5. $s_0 \models \mathrm{EG}r$
6. $s_0 \models \mathrm{A}[p\mathrm{U}r]$

Especificação de algumas propriedades do CTL

Exercício 13.1. *Mostra que uma formula φ é satisfeita um número infinito de vezes ao longo de qualquer caminho a partir de s de um modelo $\mathcal{M}$ sse e*

$$s \models AGAF\varphi$$

$\diamond$

Exemplos:

Exprime as propriedades seguintes através de fórmulas em CTL

- É possível atingir um estado onde se verifica `started` e onde `ready` é falso.($\mathrm{EF}(started \wedge \neg ready)$)

- Em qualquer estado, se se verificar `trying`, então existe um caminho onde `critical` se verifica mais tarde (non-blocking).(AG($trying \rightarrow$ EF$critical$))
- Um processo é `enabled` um número infinito de vezes ao longo de qualquer caminho.(AG(AF$enabled$))
- Ao longo de qualquer caminho, se `enabled` se verificar um número infinito de vezes, então `running` verifica-se um número infinito de vezes. Não é possível. Não é (AGAF$enabled \rightarrow$ AGAF$running$)
- De qualquer estado é possível atingir um estado onde se verifica `restart`.(AGEF$restart$)

Equivalência semântica

Equivalência de fórmulas

Duas fórmulas do CTL (sobre AP) são semanticamente equivalentes, $\varphi \equiv \psi$, se $Sat(\varphi) = Sat(\phi)$ para todos os sistemas de transições T sobre AP (i.e $T \models \varphi$ sse $T \models \psi$)

Temos as seguintes equivalências:

$$\begin{aligned}
\neg \mathrm{AF}\varphi &\equiv \mathrm{EG}\neg\varphi \\
\neg \mathrm{EF}\varphi &\equiv \mathrm{AG}\neg\varphi \\
\neg \mathrm{AX}\varphi &\equiv \mathrm{EX}\neg\varphi \\
\mathrm{AF}\varphi &\equiv \mathrm{A}[\mathsf{true}\mathrm{U}\varphi] \\
\mathrm{EF}\varphi &\equiv \mathrm{E}[\mathsf{true}\mathrm{U}\varphi] \\
\mathrm{A}[\varphi \mathrm{U} \psi] &\equiv \neg(\mathrm{E}[\neg\psi \mathrm{U}(\neg\varphi \wedge \neg\psi)]) \wedge \mathrm{AF}\psi \quad (*)
\end{aligned}$$

Conjuntos completos de conectivas

Teorema 13.1. *Considerando as conectivas temporais, os seguintes conjuntos são completos:* $\{AU, EU, EX\}$ *e* $\{EG, EU, EX\}$.

Teorema 13.2. *Um conjunto de conectivas temporais do CTL é completo se contiver pelo menos um elemento do conjunto* $\{AX, EX\}$*, um do conjunto* $\{EG, AF, AU\}$ *e* EU.

Mais equivalências

$$\begin{aligned}
\mathrm{AG}\varphi &\equiv \varphi \wedge \mathrm{AXAG}\varphi \\
\mathrm{EG}\varphi &\equiv \varphi \wedge \mathrm{EXEG}\varphi \\
\mathrm{AF}\varphi &\equiv \varphi \vee \mathrm{AXAF}\varphi \\
\mathrm{EF}\varphi &\equiv \varphi \vee \mathrm{EXEF}\varphi \\
\mathrm{A}[\varphi \mathrm{U} \psi] &\equiv \psi \vee (\varphi \wedge \mathrm{AXA}[\varphi \mathrm{U} \psi] \\
\mathrm{E}[\varphi \mathrm{U} \psi] &\equiv \psi \vee (\varphi \wedge \mathrm{EXE}[\varphi \mathrm{U} \psi]
\end{aligned}$$

LTL e CTL

O CTL não é estritamente mais expressivo que o LTL. Por exemplo

$$\mathrm{F}p \rightarrow \mathrm{F}q$$

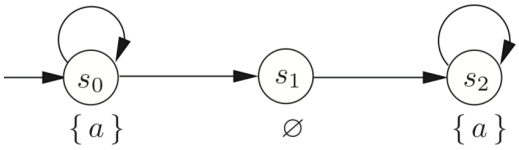
não se pode exprimir em CTL... O seu significado é

> Todos os caminhos em que p é se verifica, também se verifica q.

Vê o que significa $\mathrm{AF}p \rightarrow \mathrm{AF}q$, ou $\mathrm{AG}(p \rightarrow \mathrm{AF}q)$.

LTL E CTL

$\mathrm{FG}\varphi$ não é $\mathrm{AFAG}\varphi$



$$s_0 \models \mathrm{FG}a$$

mas

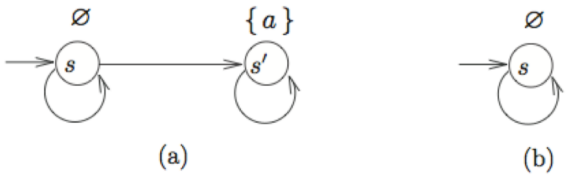
$$s_0 \not\models \mathrm{AFAG}a$$

(verifica que para s_0^ω existe um estado (s_0) e $s_0 \not\models \mathrm{AG}a$.)

LTL e CTL

Mas $\mathrm{AGEF}a$ não se pode exprimir em LTL:

> A partir de qualquer estado é possível atingir um estado em que a é verdade.



Não existe nenhuma formula φ em LTL equivalente. Suponhamos que sim. Como $TS_a \models \mathrm{AGEF}a$ então $TS_a \models \varphi$ e $Traces(TS_a) \subseteq Words(\varphi)$. Então $trace(s^\omega) = \emptyset\emptyset\cdots \subseteq Words(\varphi)$. Mas também $Traces(TS_b) \subseteq Words(\varphi)$,i.e $TS_b \models \varphi$. Mas $TS_b, \not\models \mathrm{AGEF}a$, porque $s \not\models \mathrm{EF}a$. O que é uma contradição.

LTL e CTL

Analogamente, tem-se que FX$a \equiv$ XF$a \equiv$ AXAFa mas

$$\text{FXa} \not\equiv \text{AFAX}a.$$

Teorema 13.3. *Seja ψ uma fórmula de CTL e φ a fórmula de LTL que se obtem eliminando os operadores A e E. Então ou*

$$\psi \equiv \varphi$$

ou não existe uma fórmula de LTL equivalente a ψ.

LTL versus CTL

Teorema 13.4. *a) Existem fórmulas LTL para as quais não existe fórmula CTL equivalente. Por exemplo, FGa.*

b) Existem fórmulas CTL para as quais não existe fórmula LTL equivalente. Por exemplo, AGEFa.

LTL versus CTL

Aspect	*Linear time*	*Branching time*
"behavior" in a state s	path-based: $trace(s)$	state-based: computation tree of s
temporal logic	LTL: path formulae φ $s \models \varphi$ iff $\forall \pi \in Paths(s).\, \pi \models \varphi$	CTL: state formulae existential path quantification $\exists\varphi$ universal path quantification: $\forall\varphi$
complexity of the model checking problems	PSPACE–complete $\mathcal{O}\left(\lvert TS\rvert \cdot \exp(\lvert\varphi\rvert)\right)$	*PTIME* $\mathcal{O}(\lvert TS\rvert \cdot \lvert\Phi\rvert)$
implementation-relation	trace inclusion and the like (proof is PSPACE-complete)	simulation and bisimulation (proof in polynomial time)
fairness	no special techniques needed	special techniques needed

CTL*

CTL*

CTL onde não é obrigatório que um operador LTL {X, G,F,U} seja antecedido por um operador A ou E.

Exemplos:

- $\mathrm{A}[(p\mathrm{U}r) \vee (q\mathrm{U}r)]$,
- $\mathrm{E}(\mathrm{GF}\varphi)$
- $\mathrm{A}[\mathrm{X}p \vee \mathrm{XX}p]$

O CTL* é estritamente mais expressivo que o LTL e o CTL, é computacionalmente muito menos eficiente ...

Sintaxe do CTL*

Fórmulas de Estado

São avaliadas num estado.

$$\varphi \quad ::= \quad \mathsf{true} \mid p \mid (\neg\varphi) \mid (\varphi \wedge \varphi) \mid (\mathrm{A}[\alpha]) \mid (\mathrm{E}[\alpha])$$

Fórmulas de Caminho

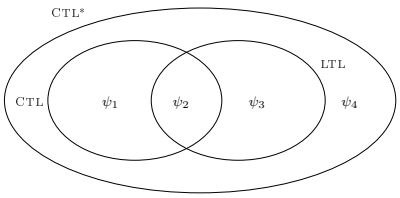
São avaliadas num caminho.

$$\alpha \quad ::= \quad \varphi \mid (\neg\alpha) \mid (\alpha \wedge \alpha) \mid (\alpha\mathrm{U}\alpha) \mid (\mathrm{G}\alpha) \mid (\mathrm{F}\alpha) \mid (\mathrm{X}\alpha)$$

LTL, CTL e CTL*

Uma fórmula α LTL corresponde a $\mathrm{A}[\alpha]$ do CTL*. O CTL é o fragmento de CTL* em que

$$\alpha \quad ::= \quad (\alpha\mathrm{U}\alpha) \mid (\mathrm{G}\alpha) \mid (\mathrm{F}\alpha) \mid (\mathrm{X}\alpha)$$



$$\begin{aligned} \psi_1 &= \mathrm{AGEF}p \\ \psi_2 &= \mathrm{AG}(p \rightarrow AFq) \\ \psi_3 &= \mathrm{A}[\mathrm{GF}p \rightarrow Fq] \\ \psi_4 &= \mathrm{E}[\mathrm{GF}p] \end{aligned}$$

$\mathbf{A}[\varphi \mathbf{U} \psi] \equiv \neg \mathbf{E}[\neg\psi \mathbf{U} (\neg\varphi \wedge \neg\psi)] \wedge \mathbf{AF}\psi$

- Em LTL, $\varphi \mathrm{U} \psi \equiv \neg(\neg\psi \mathrm{U}(\neg\varphi \wedge \neg\psi)) \wedge \mathrm{F}\psi$
- Seja $\sigma \models \varphi \mathrm{U} \psi$.
- Seja n o menor estado tal que $\sigma[n \ldots] \models \psi$ e para todo $k < n$, $\sigma[k \ldots] \models \varphi$.
- Temos que $\sigma \models \mathrm{F}\psi$
- Para $\sigma \not\models \neg(\neg\psi \mathrm{U}(\neg\varphi \wedge \neg\psi))$ queremos que
- para todo $i \geq 0$ se $\sigma[i \ldots] \models \neg\varphi \wedge \neg\psi$ então existe $j < i$ tal que $\sigma[j \ldots] \models \psi$.
- Seja i tal que $\sigma[i \ldots] \models \neg\varphi \wedge \neg\psi$; então $i > n$ e portanto podemos tomar $j = n$ e ter $\sigma[j \ldots] \models \psi$.

$\mathbf{A}[\varphi \mathbf{U} \psi] \equiv \neg \mathbf{E}[\neg\psi \mathbf{U} (\neg\varphi \wedge \neg\psi)] \wedge \mathbf{AF}\psi$

- Seja $\sigma \models \neg(\neg\psi \mathrm{U}(\neg\varphi \wedge \neg\psi)) \wedge \mathrm{F}\psi$
- Queremos $\sigma \models \varphi \mathrm{U} \psi$.
- Por $\sigma \models \mathrm{F}\psi$, temos n mínimo como caso anterior.
- Temos de mostrar que para todo $k < n$, $\sigma[k \ldots] \models \varphi$
- Suponhamos que existe $k < n$ com $\sigma[k \ldots] \models \neg\varphi$. Então também $\sigma[k \ldots] \models \neg\varphi \wedge \neg\psi$ e existiria $j < k$ tal que $\sigma[j \ldots] \models \psi$.
- o que contradiz a minimalidade de n

$\mathbf{A}[\varphi \mathbf{U} \psi] \equiv \neg \mathbf{E}[\neg\psi \mathbf{U} (\neg\varphi \wedge \neg\psi)] \wedge \mathbf{AF}\psi$

Usando o CTL^*,

$$\begin{aligned}
\mathrm{A}[\varphi \mathrm{U} \psi] &\equiv \mathrm{A}[\neg(\neg\psi \mathrm{U}(\neg\varphi \wedge \neg\psi)) \wedge \mathrm{F}\psi] \\
&\equiv \neg\mathrm{E}\neg[\neg(\neg\psi \mathrm{U}(\neg\varphi \wedge \neg\psi)) \wedge \mathrm{F}\psi] \\
&\equiv \neg\mathrm{E}[\neg\psi \mathrm{U}(\neg\varphi \wedge \neg\psi) \vee \mathrm{G}\neg\psi] \\
&\equiv \neg(\mathrm{E}[\neg\psi \mathrm{U}(\neg\varphi \wedge \neg\psi)] \vee \mathrm{EG}\neg\psi) \\
&\equiv \neg\mathrm{E}[(\neg\psi \mathrm{U}(\neg\varphi \wedge \neg\psi)]) \wedge \mathrm{AF}\psi)
\end{aligned}$$