Coding CTL models and specs

$M = (S, \rightarrow, L)$

$\varphi \rightsquigarrow f^{\varphi}$

CTL f-la

LM function representing φ
encodes the set of states $s \in S$ where $s \models \varphi$

Model Checking problem

$M, I \overset{?}{\models} \varphi$

$I =$ set of initial states

yes if $\underbrace{f^{I}}_{\text{characteristic function of } I} \cdot \overline{f^{\varphi}}$ is unsatisfiable

Recall: can represent
the transition relation $\rightarrow$
as a boolean formula $f^{\rightarrow}$

States: bool. vectors $(v_1, \ldots, v_n)$
denoted $\hat{x}$

Code CTL f-las inductively:

$f^{x} \stackrel{\text{def}}{=} x$ for var. x

$f^{\perp} \stackrel{\text{def}}{=} 0$

$f^{\varphi \wedge \psi} \stackrel{\text{def}}{=} f^{\varphi} \cdot f^{\psi}$

$$\boxed{f^{EX\varphi} \stackrel{\text{def}}{=} \exists \hat{x}' \left(f^{\rightarrow} \cdot f^{\varphi}[\hat{x} := \hat{x}'] \right)}$$

$\hat{x}$ - current state
$\hat{x}'$ - next state

Computes 1 iff $\underset{\underset{\hat{x}}{\parallel}}{s} \models EX\varphi$

Explanation:

Recall: $s \models EX\varphi$ iff

there is s' s.t. $s \to s'$ and $s' \models \varphi$

The f-la $f^{EX\varphi}$ encodes

precisely that:

it computes 1 iff. .... (same)

computes 1 on the states where $EX\varphi$ is true

- $f^{\to}$ is a function on $(\hat{x}, \hat{x}')$, encodes transitions
- $\exists x'$ means "some next state"
- $[\hat{x} := \hat{x}']$ for f^{φ}

forces φ to be true for some

next state

EF: Recall equivalence:

$$\underbrace{EF\varphi}_{} \equiv \varphi \vee EX\,\underbrace{EF\varphi}_{}$$

So, $f^{\underline{EF\varphi}}$ is equivalent

to $f^{\varphi} + f^{EX\,EF\varphi}$,

which is equiv. to

$$f^{\varphi} + \exists \hat{x}' : \left(f^{\rightarrow} \cdot f^{\underline{EF\varphi}}_{[\hat{x} := \hat{x}']} \right)$$

by using the expression for EX.

Recall: need lfp to compute EF

$\Rightarrow$ use μ.

$$f^{EF\varphi} \stackrel{def}{=} \mu Z.\left(f^{\varphi} + \exists \hat{x}' \left(f^{\vec{\cdot}} \cdot Z[\hat{x} := \hat{x}']\right)\right)$$

EU

$$f^{E[\varphi U \psi]} \stackrel{def}{=}$$

$$\mu Z.\left(f^{\psi} + f^{\varphi} \cdot \exists \hat{x}' \left(f^{\vec{\cdot}} \cdot Z[\hat{x} := \hat{x}']\right)\right)$$

AF :

$$f^{AF\varphi} \stackrel{\text{def}}{=} \mu Z.$$

$$\left(f^{\varphi} + \forall \hat{x}'\left(\overline{f^{\rightarrow}} + Z[\hat{x} := \hat{x}']\right)\right)$$

$$\forall \hat{x}'\left(f^{\rightarrow} \longrightarrow Z[\hat{x} := \hat{x}']\right)$$

EG

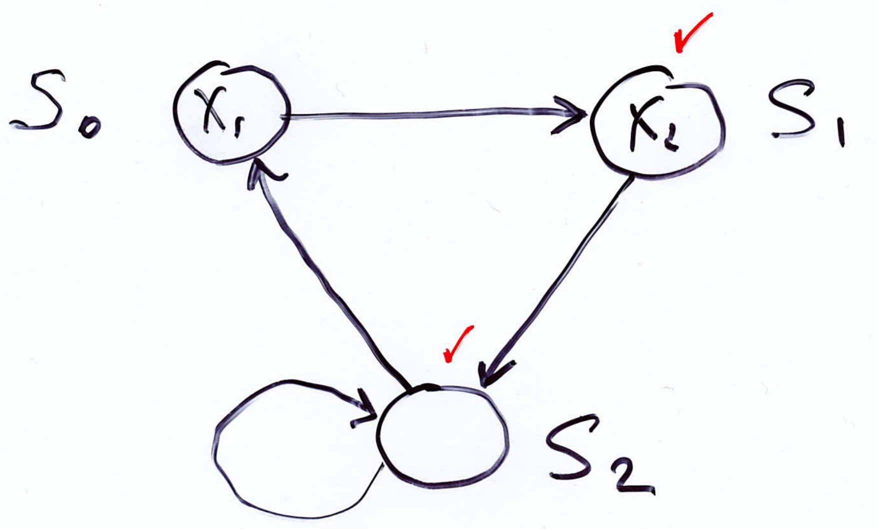
$$f^{EG\varphi} \overset{def}{=} \nu Z.\left(f^{\varphi} \cdot \exists \vec{x}'\left(f^{\rightarrow} \cdot Z[x := x'\right.\right.$$

Intuition: show φ holds in the current state;

find a successor which satisfies EG again.

Do it forever (maximize).

Example: Computing $EX(x_1 \vee \neg x_2)$



Compute $EX(x_1 \vee \neg x_2)$

$[\![EX(x_1 \vee \neg x_2)]\!] = \{s_1, s_2\}$

The BLA returns this.

We'll check if this is the case using bool. func. for EX.

A step aside: a different representation for $\vec{f}$.

In these examples, we'll use an encoding of $\vec{f}$ (the bool. func. representing the tr. relation) which is constructed directly from SMV code.

We'll use primes instead of "next":

$$x_i' \longleftrightarrow \underbrace{f_i}_{\text{some bool. function}}$$

iff

Clarification about

iff: $q \leftrightarrow r$

if they compute the same value, i.e., $\overline{q \oplus r}$.

The tr. relation is represented by

$$\prod_{1 \le i \le n} (x_i' \leftrightarrow f_i)$$

f_i^* may contain "don't care" input variable u to model non-determinism of the transitions.

i.e., there is no $u' \leftrightarrow f_u$ conjunct

$$\vec{f} = (x_1' \leftrightarrow \bar{x}_1 \cdot \bar{x}_2 \cdot u) \cdot \underbrace{(x_2' \leftrightarrow x_1)}$$

(for our example)

the truth value of x_2 in the next state coincides with the truth value for x_1 now.

$$f^{EX(x_1 \vee \neg x_2)}$$

$$= \exists x_1' \exists x_2' \left(f^{\to} \cdot f^{x_1 \vee \neg x_2}_{[\hat{x} := \hat{x}']} \right)$$

$$= \exists x_1' \exists x_2' \left(\underbrace{(x_1' \leftrightarrow \bar{x}_1 \cdot \bar{x}_2 \cdot u) \cdot (x_2' \leftrightarrow x_1)}_{} \cdot \right.$$

$$\left. \cdot \left(\underset{0}{x_1'} + \underset{\bar{1}}{\bar{x}_2'} \right) \right)$$

$$\underline{0 + \bar{1}}$$

$$0$$

To check $s_0 \models EX(x_1 \vee \neg x_2)$,

evaluate $\rho_0 \overset{?}{\models} f^{EX(x_1 \vee \neg x_2)}$

where $\left.\begin{array}{l} \rho_0(x_1) = 1 \\ \rho_0(x_2) = 0 \end{array}\right\} s_0$

$\rho_0(u) = 0/1$ - does not matter

$\rho_0(x_1') = 0$

$$\rho_0(x_2') = 1$$

(from the diagram)

~~s_0~~ state "next" to s_0

The conjunction is false,

so $\rho_0 \not\models_f EX(x_1 \vee \neg x_2)$