From CTL to μ

Want a μ assertion equivalent to $EG\ A$

$\rightsquigarrow$ A fixpoint of what equation?

$X = \varphi(X)$ where $\varphi(X) = A \wedge ([-]F \vee \langle - \rangle X)$

... Consider the transition system

$\mu X.\ A \wedge ([-]F \vee \langle - \rangle X) = \emptyset$

$\nu X.\ A \wedge ([-]F \vee \langle - \rangle X) = \{s, t\}$

Without a clever example, just consider (informally)

LFP: $\varphi(\emptyset) \vee \varphi^2(\emptyset) \vee \varphi^3(\emptyset) \vee \ldots$

GFP: $\varphi(T) \wedge \varphi^2(T) \wedge \varphi^3(T) \wedge \ldots$

$\varphi(\emptyset) = A \wedge ([-]F \vee \langle - \rangle \emptyset)$

$\varphi^2(\emptyset) = A \wedge ([-]F \vee \langle - \rangle (A \wedge [-]F))$

$\vdots$

$\varphi(T) = A \wedge ([-]F \vee \langle - \rangle T)$

$\varphi^2(T) = A \wedge ([-]F \vee \langle - \rangle (A \wedge ([-]F \vee \langle - \rangle T)))$

Translating the CTL modalities into the modal μ-calculus:

$$EX\,A \equiv \langle\cdot\rangle A$$

$$EG\,A \equiv \nu Y.\ A \wedge ([\cdot]F \vee \langle\cdot\rangle Y)$$

$$E[A\,\mathcal{U}\,B] \equiv \mu Z.\ B \vee (A \wedge \langle\cdot\rangle Z)$$

Based on this we get a translation of CTL into the modal μ-calculus.

Propn 4.6 $s \models \nu Y.\ A \wedge ([\cdot]F \vee \langle\cdot\rangle Y)$ in a finite state trans. sys. iff

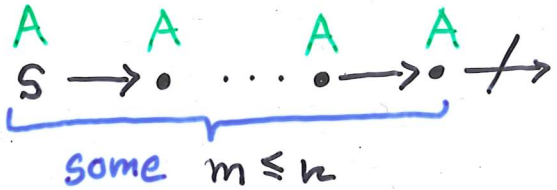
$\exists$ path π from s s.t. $\pi_i \models A$ for all i.

Proof: $\varphi(Y) \underset{\text{def}}{=} A \wedge ([\cdot]F \vee \langle\cdot\rangle Y)$

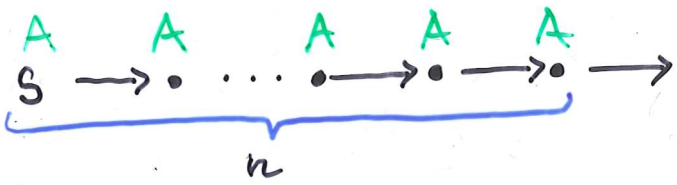
$\nu Y.\ \varphi(Y) = \bigcap_n \varphi^n(T)$ where $T \supseteq \varphi(T) \supseteq \cdots \supseteq \varphi^n(T) \supseteq \cdots$

By induction,

$s \models \varphi^n(T)$ iff



or



Assuming no. of states is k, $\nu Y.\varphi(Y) = \varphi^k(T) = \varphi^{k+1}(T)$

$s \models \nu Y.\ \varphi(Y)$ iff $s \models \varphi^k(T)$

iff $\exists$ maxℓ A-path lgth $\leq k$ from s

or $\exists$ (looping) A-path lgth k from s.

Propn. 4.8 (weakened)

$$s \models \mu Z.\ B \vee (A \wedge \langle\cdot\rangle Z)$$

in a finite state trans. sys. iff

$\exists$ path π from s s.t. $\exists i.\ \pi_i \models B$ & $\forall j < i.\ \pi_j \models A$.

Proof:

$$\varphi(Z) = B \vee (A \wedge \langle\cdot\rangle Z)$$

$$\mu Z.\ \varphi(Z) = \bigcup_n \varphi^n(\phi) \quad \text{where } \phi \subseteq \varphi(\phi) \subseteq \cdots \subseteq \varphi^n(\phi) \subseteq \cdots$$

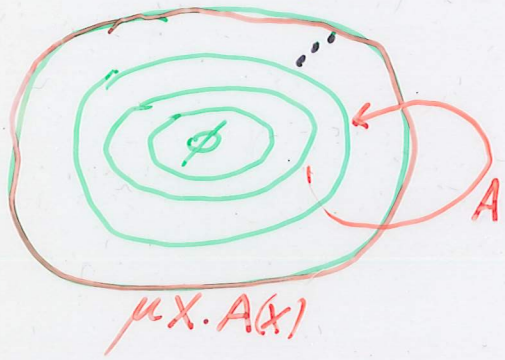
By induction,

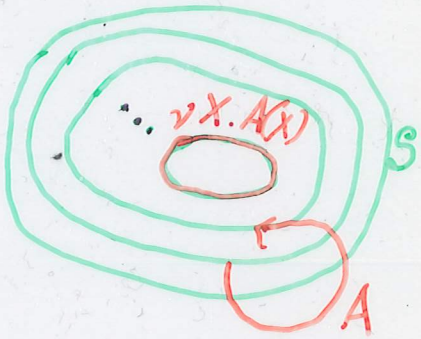
$s \models \varphi^n(\phi)$ *iff* $s \xrightarrow{B}$ or $s \xrightarrow{A}\ \xrightarrow{A}\ \xrightarrow{A}\ \xrightarrow{A}\ \xrightarrow{B}$ (under the A-steps: $\exists m.\ 1 < m \leq n$)

How to model-check the modal μ-calculus:

Assume processes are finite-state.

- Brute force + optimisations [Emerson + Li]:





- Local model checking [Larsen, Stirling + Walker, gus]:

"~~Silly idea~~" Reduction Lemma:

$$p \in \nu X.\, \varphi(X) \iff p \in \varphi(\nu X.\, \{p\} \cup \varphi(X))$$

The modal μ-calculus w.r.t. $(S, L, tran)$

$$P = P$$

$$T = S \qquad F = \emptyset$$

$$\neg A = S \setminus A$$

$$A \wedge B = A \cap B \qquad A \vee B = A \cup B$$

$$\langle a \rangle A = \{ p \in S \mid \exists q.\ p \xrightarrow{a} q \ \&\ q \in A \}$$

$$\langle \cdot \rangle A = \{ p \in S \mid \exists q, a.\ p \xrightarrow{a} q \ \&\ q \in A \}$$

~~$\nu X.\ A = \bigcup \{ u \subseteq S \mid u \subseteq A[u/X] \}$~~

NEW SYNTAX: X must occur +vely

$$\mu X.\ A = \neg \nu X.\ \neg A[\neg X / X]$$

$$\nu X \{p_1, \cdots, p_n\}\ A = \bigcup \{ u \subseteq S \mid u \subseteq \{p_1, \cdots, p_n\} \vee A[u/X] \}$$

Now $\nu X.\ A = \nu X \{\}\ A$

The Reduction Lemma

Let $\varphi : \mathcal{P}(S) \to \mathcal{P}(S)$ be monotonic. For $U \subseteq S$,

$$U \subseteq \nu X.\, \varphi(X)$$

$$\Leftrightarrow$$

$$U \subseteq \varphi(\nu X.\, (U \cup \varphi(X)))$$

In particular,

$$p \in \nu X.\, \varphi(X)$$

$$\Leftrightarrow$$

$$p \in \varphi(\nu X.\, (\{p\} \cup \varphi(X)))$$

With respect to $(S, L, tran)$:

$p \models U \Rightarrow$ true if $p \in U$

$p \models U \Rightarrow$ false if $p \notin U$

$p \models T \Rightarrow$ true

$p \models F \Rightarrow$ false

$p \models \neg B \Rightarrow$ not$(p \models B)$

$p \models A \wedge B \Rightarrow p \models A$ and $p \models B$

$p \models A \vee B \Rightarrow p \models A$ or $p \models B$

$p \models \langle a \rangle B \Rightarrow q_1 \models B$ or $\cdots$ or $q_n \models B$

$\{q_1, \cdots, q_n\} = \{q \mid p \xrightarrow{a} q\}$

$p \models \nu X\{\vec{r}\}B \Rightarrow$ true if $p \in \{\vec{r}\}$

$p \models \nu X\{\vec{r}\}B \Rightarrow p \models B[\nu X\{p, \vec{r}\}B / X]$ if $p \notin \{\vec{r}\}$

a reduction relation reducing satisfaction assertions to true/false provided S is finite.

§1.4

The principle of Well-founded Induction

A binary relation $\prec$ on a set A is <u>well-founded</u> iff there are <u>no</u> infinite descending chains $\ldots \prec a_n \prec \ldots \prec a_1 \prec a_0$

Let $\prec$ be a well-founded relation on a set A. Let P be a property. Then,

$$\forall a \in A.\ P(a)$$

if

$$\forall a \in A \left((\forall b \prec a.\ P(b)) \Rightarrow P(a) \right)$$

Proof the reduction terminates (sketch):

By wfd. induction on assertions w.r.t.

$A' \prec A$ iff A' proper subassn. of A

or $A \equiv \nu X \{\vec{r}\} B$ &

$A' \equiv \nu X \{\vec{r}, p\} B$, $p \notin \{\vec{r}\}$.

Want, for all closed assn. A,

$$\mathcal{Q}(A) \Leftrightarrow_{def} \forall q \in S \forall t. (q \models A) \xrightarrow{*} t \text{ iff } (q \models A) = t$$

Need to extend $\mathcal{Q}$ to open assertions:

$$\mathcal{Q}^+(A) \Leftrightarrow_{def} \forall \overset{\text{closed}}{\text{subst}^{ns}} B_1/X_1, \ldots, B_n/X_n \text{ for } FreeV(A).$$

$$\mathcal{Q}(B_1) \& \cdots \& \mathcal{Q}(B_n) \Rightarrow \mathcal{Q}(A[B_1/X_1, \ldots, B_n/X_n])$$

Show $\mathcal{Q}^+(A)$ for all A by wfd. ind. on $\prec$.

[NB. $\mathcal{Q}^+(A) \Leftrightarrow \mathcal{Q}(A)$ when A is closed.]