PROOF OF SAFETY GAMES

$$\langle 1\rangle \Diamond R \geq \mu X.\left([R] \sqcup Pre_1(X)\right) \qquad (1)$$

$$\langle 1\rangle \Box B \geq \nu X.\left([B] \sqcap Pre_1(X)\right) \qquad (2)$$

(1) : See before.

(2) : LET US PROVE IT!

Let $X^* = [B] \sqcap Pre_1(X^*)$

I show that I have π_1 st $\forall \pi_2$:

$$Pr_s^{\pi_1,\pi_2}(\Box B) \geq X^*(s).$$

Choose π_1 so that at all $t \in S$ your π_1 plays as in

$$\arg Pre_1(X^*)$$

$$= \arg \sup_{\xi_1 \in D_1(t)} \inf_{\xi_2 \in D_2(t)} E_t^{\xi_1,\xi_2}(X^*).$$

π_1 is memoryless.

Consider any π_2.

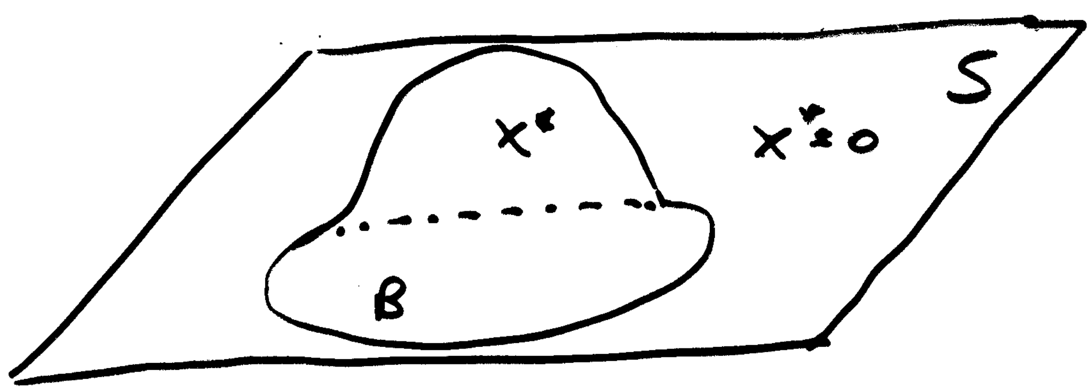
Let :

$\bigcirc_n X^*$: The expected value of X^* after n steps.

$\Box_n B$: the prob of always in B for n steps.

Note : $s \notin B \rightarrow X^*(s) = 0$.

$X^* = B \sqcap \mathrm{Pre}_1 (X^*)$



$X^*(s) \leq E_s^{\pi_1, \pi_2} (\bigcirc_1 X^*)$ because $\exists_1$ optimal π_2 arbitrary.

$X^*(s) \leq E_s^{\pi_1, \pi_2} (\bigcirc_1 E^{\pi_1 \pi_2'} (\bigcirc_1 X^*))$

$X^*(s) \leq E_s^{\pi_1, \pi_2} (\bigcirc_2 X^*)$

X^* is a submartingale.

$$X^* \leq [B]$$

$$X^*(s) \leq E_s^{\pi_1 \pi_2} (\bigcirc_2 B)$$

$$X^*(s) \leq E_s^{\pi_1 \pi_2} (\Box_2 B)$$

Cheating: modify G so that from out of B, you cannot go back in.
Then, $\quad \bigcirc_2 B = \Box_2 B$.

One more step:

$$X^*(s) \leq E_s^{\pi_1 \pi_2} (\Box_3 B)$$

$$\vdots$$

$$n$$

$$\vdots$$

$$\infty$$

$$E_s^{\pi_1 \pi_2} (\Box B) = \lim_{n \to \infty} E_s^{\pi_1 \pi_2} (\Box_n B)$$

Because $\Box B = \bigcap_{n \geq 0} \bigcup_{\sigma \in B^n} \mathrm{Cone}(\sigma)$.

$X^* \leq E^{\pi_1 \pi_2} (\Box B)$ so $\langle 1 \rangle \Box B \geq X^*$ $\underline{\underline{\text{ok}}}$

$$\langle 1 \rangle \; \Diamond R \geq \mu X.\left([R] \sqcup \mathrm{Pre}_1(X)\right)$$

$$\langle 2 \rangle \; \Box \neg R \geq \nu X.\left([\neg R] \sqcap \mathrm{Pre}_2(X)\right)$$

$$1 - \mu X.\left([R] \sqcup \mathrm{Pre}_1(X)\right) =$$

$\neg \alpha = 1 - \alpha.$

$$= \nu X.\left([\neg R] \sqcap \neg \mathrm{Pre}_1(\neg X)\right)$$

$$\neg \mathrm{Pre}_1(\neg X) =$$

$$= 1 - \sup_{\xi_1 \in D_1} \inf_{\xi_2 \in D_2} E^{\xi_1, \xi_2}(1 - X)$$

$$= \inf_{\xi_1} \sup_{\xi_2} E^{\xi_1, \xi_2}(X)$$

because this is a Matrix game (minimax thm of von Neumann, 1929).

$$\sup_{\xi_2} \inf_{\xi_1} E^{\xi_1, \xi_2}(X)$$

$$\neg \mathrm{Pre}_1(\neg X) = \mathrm{Pre}_2(X).$$

$$1 - \underset{\langle 1 \rangle \Diamond R}{\underset{\rotatebox{90}{$\geq$}}{\mu X. \big([R] \sqcup Pre_1(X) \big)}} = \underset{\langle 2 \rangle \Box \neg R}{\underset{\rotatebox{90}{$\geq$}}{\nu X. \big([\neg R] \sqcap Pre_2(X) \big)}}$$

So:

$$\boxed{\begin{aligned} \langle 1 \rangle \Diamond R &= \mu X. \big([R] \sqcup Pre_1(X) \big) \\ \langle 1 \rangle \Box R &= \nu X. \big([R] \sqcap Pre_1(X) \big) \end{aligned}}$$

MDP = Markov Decision Process
= no player 2.

Reachability.

$$\langle 1 \rangle \Diamond R = \mu X \left([R] \cup Pre_1(X) \right) = X^*$$

$$s \notin R \quad X^*(s) = \max_{a \in \Gamma_1(s)} \sum_t p(t \mid s, a) \cdot X^*(t)$$

$p(s,a)(t)$

$$= \max_{a \in \Gamma_1(s)} E_s^a(X^*).$$

Why? Because

$$\sup_{\xi_1} E_s^{\xi_1}(X^*) = \max_a E_s^{\xi_1}(X^*).$$

$$x^*(s) = \max_{a \in \Gamma_1(s)} \sum_t p(s,a)(t) \cdot x^*(t)$$

Want the $\underline{\text{least}}$ such x^* which is 1 in R.

Linear Programming on

$$\{x(s) \mid s \notin R\}$$

Minimize $\sum_{s \in S} x(s)$ subj to:

$\forall s \notin R,\ \forall a \in \Gamma_1(s)$:

$$x(s) \geq \sum_{t \notin R} p(s,a)(t) \cdot x(t) + \sum_{t \in R} p(s,a)(t)$$

Key: μ is the <u>least</u> fp,
and max also requires
minimization!

<u>Thm</u> Given MDP, $\langle 1 \rangle \diamond R$
can be computed via LP
in poly time.

How to compute $\langle 1 \rangle \Box R$ (safety) in MDPs?

<u>Def</u> END COMPONENT

is a set $T \subseteq S$ such that:

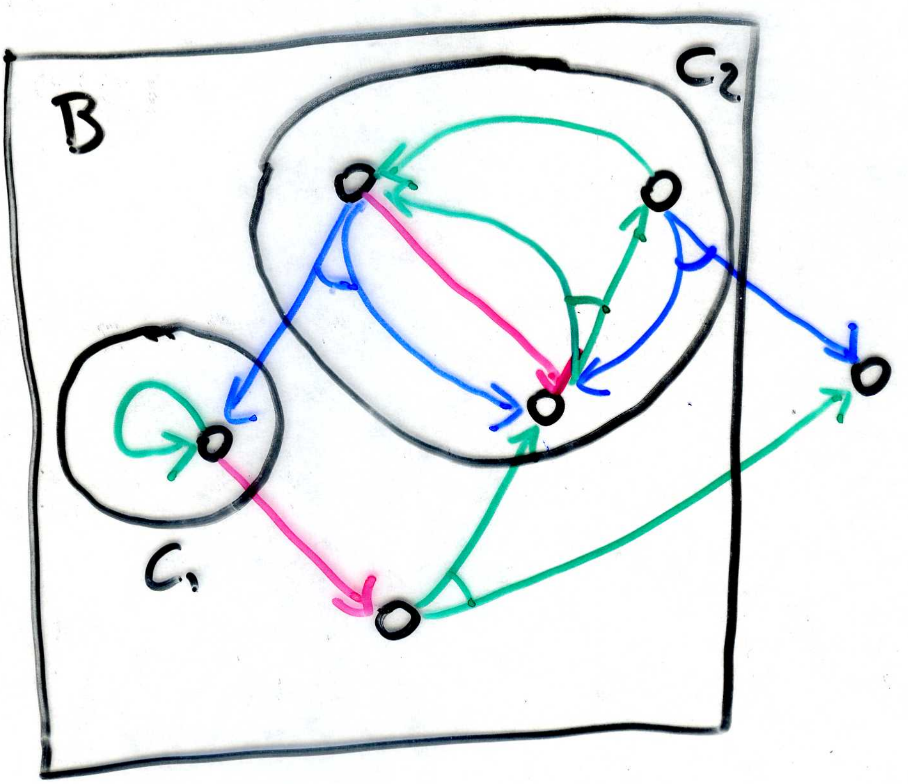
- Let $\Gamma_T(s) = \{ a \in \Gamma_1(s).$
$$p(s,a)(t) > 0 \to t \in T \}$$

These are the "safe" actions that guarantee staying in T.

- Let $E_T = \{ (s,t) \mid$
$$\exists a \in \Gamma_T(s).\ p(s,a)(t) > 0 \}$$

graph of safe transitions.

- T is an end-component if (T, E_T) is strongly connected.



What are the maximal EC in B?
C_1 and C_2. Note: $C_1 \cup C_2$ <u>not</u> EC.

<u>Thm</u> For <u>all</u> π_1,

$$Pr_s^{\pi_1}\left(\begin{array}{c}\text{the set of states visited}\\ \infty \text{ often is an EC}\end{array}\right) = 1.$$

To compute the maximal EC in B:

loop{

- compute E_B.
- compute the maximal strongly connected components $C_1 .. C_n$ in (B, E_B).
- replace B by each $C_i, 1 \le i \le n$, and recur.

}