Th (*) guarantees termination, gives an upper bound on the # of iterations.

Correctness of SAT_{EG}

(1) $\boxed{[\![EG\varphi]\!] = [\![\varphi]\!] \cap pre_{\exists}([\![EG\varphi]\!])}$

$\Rightarrow$ $[\![EG\varphi]\!]$ is a fixpoint of

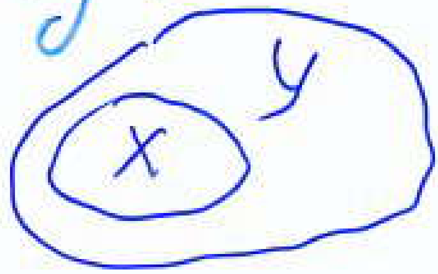
(2) $\boxed{F(X) = [\![\varphi]\!] \cap pre_{\exists}(X)}$

It turns out $[\![EG\varphi]\!]$ can be computed using Th (*).

Th(**) $\boxed{\begin{array}{l} 1)\ F_\varphi \text{ monotone} \\ 2)\ [\![EG\varphi]\!] = gfp\, F = F^{n+1}(S) \end{array}}$

Proof 1) monotonicity.

Let $X \subseteq Y$



Need to show:

$$[\![\varphi]\!] \cap pre_\exists(X) \subseteq [\![\varphi]\!] \cap pre_\exists(Y)$$

It suffices to show:

$$\underbrace{pre_\exists(X)}_{\{s \mid \exists \text{ transition from } s \text{ to some state in } X\}} \subseteq pre_\exists(Y).$$

Take any state s such that s has a transition $\boxed{\text{to } X.}$

Since $X \subseteq Y$, s also has a transition to Y

So, for any s,

$$s \in pre_\exists(X) \Rightarrow s \in pre_\exists(Y).$$

so, $pre_\exists(X) \subseteq pre_\exists(Y)$

and monotonicity holds. ●

2) Show $\llbracket EG\varphi \rrbracket = gfp\ F$.

By (1), $\llbracket EG\varphi \rrbracket$ a fixpoint of F.

We'll show it is the greatest, i.e.,

for every X s.t. $F(X) = X$,

$$X \subseteq \llbracket EG\varphi \rrbracket.$$

Need: for every s_0,

if $s_0 \in X$ then $\underbrace{s_0 \in \llbracket EG\varphi \rrbracket}$.

there is a path $s_0 \to s_1 \to \ldots$ such that

$s_i \in \llbracket \varphi \rrbracket$ for all $i \geq 0$.

Sup. $s_0 \in X$.

We know: $X = F(X) = [\![\varphi]\!] \cap pre_\exists(X)$

so, $s_0 \in [\![\varphi]\!]$

and $\exists$ transition from s_0 to some s_1 in X.

apply the same argument to s_1:

$s_1 \in [\![\varphi]\!]$

and $\exists$ tr. $s_1 \to s_2$ for some $s_2 \in X$

etc.

$\Rightarrow$ By ind. $\exists$ inf. path $s_0 \to s_1 \to s_2 \to \dots$ such that $s_i \in [\![\varphi]\!]$ for all $i \geq 0$.

$\Rightarrow \quad s_0 \in [\![EG\varphi]\!]$

So, $[\![EG\varphi]\!]$ is gfp of F, and $[\![EG\varphi]\!] = F^{n+1}(S)$ (by Th (*))

Correctness of SAT_{EG}:

Can replace $Y := Y \cap pre_\exists Y$

with $Y := SAT(\varphi) \cap pre_\exists(Y)$

in the alg.

$Y = SAT(\varphi)$ init.
$Y \subseteq SAT(\varphi)$ later

$\Rightarrow$ running this alg. is equivalent to iteratively applying the operator F starting from S.

$\Rightarrow$ the alg. computes gfp F

$\Rightarrow$ From Th (**): it terminates and computes $[\![EG\varphi]\!]$.