CS 267: Automated Verification

Lecture 3: Fixpoints and Temporal Properties

Instructor: Tevfik Bultan

What is a Fixpoint (aka, Fixed Point)

Given a function

$\mathcal{F} : D \rightarrow D$

$x \in D$ is a fixpoint of $\mathcal{F}$ if and only if $\mathcal{F}(x) = x$

Temporal Properties ≡ Fixpoints

[Emerson and Clarke 80]

Here are some interesting CTL equivalences:

$$AG\ p = p \wedge AX\ AG\ p$$
$$EG\ p = p \wedge EX\ EG\ p$$

$$AF\ p = p \vee AX\ AF\ p$$
$$EF\ p = p \vee EX\ EF\ p$$

$$p\ AU\ q = q \vee (p \wedge AX\ (p\ AU\ q))$$
$$p\ EU\ q = q \vee (p \wedge EX\ (p\ EU\ q))$$

Note that we wrote the CTL temporal operators in terms of themselves and EX and AX operators

Functionals

- Given a transition system T=(S, I, R), we will define functions from sets of states to sets of states
  - $\mathcal{F} : 2^S \rightarrow 2^S$

- For example, one such function is the EX operator (which computes the precondition of a set of states)
  - EX : $2^S \rightarrow 2^S$

  which can be defined as:

  $EX(p) = \{ s \mid (s,s') \in R \text{ and } s' \in p \}$

Abuse of notation: I am using p to denote the set of states which satisfy the property p (i.e., the truth set of p)

Functionals

- Now, we can think of all temporal operators also as functions from sets of states to sets of states.
- For example:

$$AX\ p = \neg EX(\neg p)$$

or if we use the set notation

$$AX\ p = (S - EX(S - p))$$

Abuse of notation: I will use the set and logic notations interchangeably.

Logic	*Set*
$p \wedge q$	$p \cap q$
$p \vee q$	$p \cup q$
$\neg p$	$S - p$
False	$\emptyset$
True	S

Lattices

The set of states of the transition system forms a lattice:

• lattice	2^S
• partial order	$\subseteq$
• bottom element	$\emptyset$ (alternative notation: $\perp$)
• top element	S (alternative notation: T)
• Least upper bound (lub) (aka join) operator	$\cup$
• Greatest lower bound (glb) (aka meet) operator	$\cap$

Lattices

In general, a lattice is a partially ordered set with a least upper bound operation and a greatest lower bound operation.

- Least upper bound $a \cup b$ is the smallest element where

  $a \subseteq a \cup b$ and $b \subseteq a \cup b$
- Greatest lower bound $a \cap b$ is the biggest element where

  $a \cap b \subseteq a$ and $a \cap b \subseteq b$

A partial order is a
- reflexive (for all x, $x \subseteq x$),
- transitive (for all x, y, z, $x \subseteq y \wedge y \subseteq z \Rightarrow x \subseteq z$), and
- antisymmetric (for all x, y, $x \subseteq y \wedge y \subseteq x \Rightarrow x = y$)

relation.

Complete Lattices

2^S forms a lattice with the partial order defined as the subset-or-equal relation and the least upper bound operation defined as the set union and the greatest lower bound operation defined as the set intersection.

In fact, $(2^S, \subseteq, \varnothing, S, \cup, \cap)$ is a complete lattice since for each set of elements from this lattice there is a least upper bound and a greatest lower bound.

Also, note that the top and bottom elements can be defined as:

$\perp = \varnothing = \cap \{ y \mid y \in 2^S \}$

$T = S = \cup \{ y \mid y \in 2^S \}$

This definition is valid for any complete lattice.

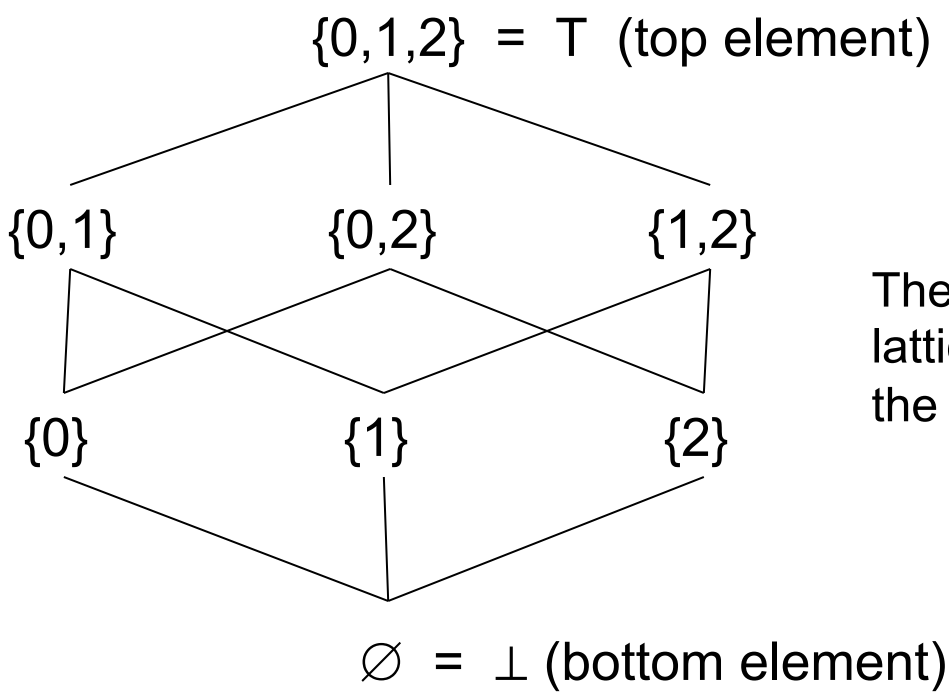
An Example Lattice

$\{\varnothing, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}\}$

partial order: $\subseteq$ (subset relation)

bottom element: $\varnothing = \perp$ top element: $\{0,1,2\} = T$

lub: $\cup$ (union) glb: $\cap$ (intersection)



The Hasse diagram for the example lattice (shows the transitive reduction of the corresponding partial order relation)

Temporal Properties ≡ Fixpoints

Based on the equivalence

$$EF\ p = p \vee EX\ EF\ p$$

we observe that EF p is a fixpoint of the following function:

$\mathcal{F}\ y = p \vee EX\ y$ (we can also write it as $\lambda\ y\ .\ p \vee EX\ y$)

$\mathcal{F}\ (EF\ p) = EF\ p$

In fact, EF p is the least fixpoint of $\mathcal{F}$, which is written as:

$EF\ p = \mu\ y\ .\ \mathcal{F}\ y = \mu\ y\ .\ p \vee EX\ y$ (μ means least fixpoint)

$EF\ p = \mu y . p \vee EX\ y$

- Let's prove this.

- First we have the equivalence $EF\ p = p \vee EX\ EF\ p$
  - Why? Because according to the semantics of EF, EF p holds in a state either if p holds in that state, or if that state has a next state in which EF p holds.
  - From this equivalence we know that EF p is a fixpoint of the function $\lambda y . p \vee EX\ y$ and since the least fixpoint is the smallest fixpoint we have:

    $\mu y . p \vee EX\ y \subseteq EF\ p$

$EF\ p = \mu y . p \vee EX\ y$

- Next we need to prove that $EF\ p \subseteq \mu y . p \vee EX\ y$ to complete the proof.
- Suppose z is a fixpoint of $\lambda y . p \vee EX\ y$, then we know that

$z = p \vee EX\ z$ which means that $EX\ z \subseteq z$ and this means that no path starting from a state that is outside of z can reach a state in z.

Since we also have $p \subseteq z$, any path that can reach p must start with a state in z.

Hence, we can conclude that $EF\ p \subseteq z$.

Since we showed that EF p is contained in any fixpoint of the function $\lambda y . p \vee EX\ y$, we get

$EF\ p \subseteq \mu y . p \vee EX\ y$

which completes the proof.

Temporal Properties ≡ Fixpoints

Based on the equivalence

$$EG\ p = p \wedge EX\ EG\ p$$

we observe that EG p is a fixpoint of the following function:

$\mathcal{F}\ y = p \wedge EX\ y$ (we can also write it as $\lambda\, y\,.\, p \wedge EX\ y$)

$\mathcal{F}\,(EG\ p) = EG\ p$

In fact, EG p is the greatest fixpoint of $\mathcal{F}$, which is written as:

$EG\ p = \nu\, y\,.\, \mathcal{F}\ y = \nu\, y\,.\, p \wedge EX\ y$ (ν means greatest fixpoint)

$EG\ p = \nu\ y\ .\ p \wedge EX\ y$

- Let's prove this too.

- First we have the equivalence $EG\ p = p \wedge EX\ EG\ p$
  - Why? Because according to the semantics of EG, EG p holds in a state if and only if p holds in that state and if that state has a next state in which EG p holds.
  - From this equivalence we know that EG p is a fixpoint of the function $\lambda\ y\ .\ p \wedge EX\ y$ and since the greatest fixpoint is the biggest fixpoint we have:

    $EG\ p \subseteq \nu\ y\ .\ p \wedge EX\ y$

EG p = ν y . p $\wedge$ EX y

- Next we need to prove that ν y . p $\wedge$ EX y $\subseteq$ EG p to complete the proof.
- Suppose z is a fixpoint of λ y . p $\wedge$ EX y, then we know that

z = p $\wedge$ EX z which means that z $\subseteq$ p and z $\subseteq$ EX z. Hence, p holds in every state in z and every state in z has a next state that is also in z. Therefore from any state that is in z, we can build a path that starts at that state and on all states on that path p holds. This means that every state in z satisfy EG p, i.e., z $\subseteq$ EG p.

Since we showed that any fixpoint of λ y . p $\wedge$ EX y is contained in EG p, we get

ν y . p $\wedge$ EX y $\subseteq$ EG p

which completes the proof.

Fixpoint Characterizations

Fixpoint Characterization	Equivalences
$AG\ p = \nu y\ .\ p \wedge AX\ y$	$AG\ p = p \wedge AX\ AG\ p$
$EG\ p = \nu y\ .\ p \wedge EX\ y$	$EG\ p = p \wedge EX\ EG\ p$
$AF\ p = \mu y\ .\ p \vee AX\ y$	$AF\ p = p \vee AX\ AF\ p$
$EF\ p = \mu y\ .\ p \vee EX\ y$	$EF\ p = p \vee EX\ EF\ p$
$p\ AU\ q = \mu y\ .\ q \vee (p \wedge AX\ (y))$	$p\ AU\ q = q \vee (p \wedge AX\ (p\ AU\ q))$
$p\ EU\ q = \mu y\ .\ q \vee (p \wedge EX\ (y))$	$p\ EU\ q = q \vee (p \wedge EX\ (p\ EU\ q))$

All of these fixpoint characterizations can be proved based on the semantics of the temporal operators (like we did for EF p and EG p).

Monotonicity

- Function $\mathcal{F}$ is monotonic if and only if, for any x and y, $x \subseteq y \Rightarrow \mathcal{F}\, x \subseteq \mathcal{F}\, y$

Note that, all the functions we used for representing temporal operators are monotonic:

$\lambda\ y \,.\, p \wedge AX\ y$

$\lambda\ y \,.\, p \wedge EX\ y$

$\lambda\ y \,.\, p \vee AX\ y$

$\lambda\ y \,.\, p \vee EX\ y$

$\lambda\ y \,.\, q \vee (p \wedge AX\ (y))$

$\lambda\ y \,.\, q \vee (p \wedge EX\ (y))$

For all these functions, if you give a bigger y as input you will get a bigger result as output

Monotonicity

- One can define non-monotonic functions:

For example: $\lambda\ y\ .\ p \wedge EX \neg y$

This function is not monotonic. If you give a bigger y as input you will get a smaller result.

- For the functions that are non-monotonic the fixpoint computation techniques we are going to discuss will not work. For such functions a fixpoint may not even exist.

- The functions we defined for temporal operators are all monotonic because there is no negation in front of the input variable y. In general, if you have an even number of negations in front of the input variable y, then you will get a monotonic function.

Least Fixpoint

Given a monotonic function $\mathcal{F}$, its least fixpoint exists, and it is the greatest lower bound (glb) of all the reductive elements :

$$\mu\, y \,.\, \mathcal{F}\, y = \cap \{\, y \mid \mathcal{F}\, y \subseteq y \,\}$$

$\mu\, y\,.\, \mathcal{F}\, y = \cap \{ y \mid \mathcal{F}\, y \subseteq y \}$

- Let's prove this property.
- Let us define z as $z = \cap \{ y \mid \mathcal{F}\, y \subseteq y \}$

We will first show that z is a fixpoint of $\mathcal{F}$ and then we will show that it is the least fixpoint which will complete the proof.

- Based on the definition of z, we know that:

  for any y, $\mathcal{F}\, y \subseteq y$, we have $z \subseteq y$.

Since $\mathcal{F}$ is monotonic, $z \subseteq y \Rightarrow \mathcal{F}\, z \subseteq \mathcal{F}\, y$.

But since $\mathcal{F}\, y \subseteq y$, then $\mathcal{F}\, z \subseteq y$.

I.e., for all y, $\mathcal{F}\, y \subseteq y$, we have $\mathcal{F}\, z \subseteq y$.

This implies that, $\mathcal{F}\, z \subseteq \cap \{ y \mid \mathcal{F}\, y \subseteq y \}$,

and based on the definition of z, we get $\mathcal{F}\, z \subseteq z$

$\mu y \,.\, \mathcal{F}\, y = \cap \{ y \mid \mathcal{F}\, y \subseteq y \}$

- Since $\mathcal{F}$ is monotonic and since $\mathcal{F}\, z \subseteq z$, we have

$\mathcal{F}\,(\mathcal{F}\, z) \subseteq \mathcal{F}\, z$ which means that $\mathcal{F}\, z \in \{ y \mid \mathcal{F}\, y \subseteq y \}$.
Then by definition of z we get, $z \subseteq \mathcal{F}\, z$

- Since we showed that $\mathcal{F}\, z \subseteq z$ and $z \subseteq \mathcal{F}\, z$, we conclude that $\mathcal{F}\, z = z$, i.e., z is a fixpoint of the function $\mathcal{F}$.

- For any fixpoint of $\mathcal{F}$ we have $\mathcal{F}\, y = y$ which implies $\mathcal{F}\, y \subseteq y$

So any fixpoint of $\mathcal{F}$ is a member of the set $\{ y \mid \mathcal{F}\, y \subseteq y \}$ and z is smaller than any member of the set $\{ y \mid \mathcal{F}\, y \subseteq y \}$ since it is the greatest lower bound of all the elements in that set.

Hence, z is the least fixpoint of $\mathcal{F}$.

Computing the Least Fixpoint

The least fixpoint μ y . $\mathcal{F}$ y is the limit of the following sequence (assuming $\mathcal{F}$ is $\cup$-continuous):

$\emptyset$, $\mathcal{F}\,\emptyset$, $\mathcal{F}^2\,\emptyset$, $\mathcal{F}^3\,\emptyset$, ...

$\mathcal{F}$ is $\cup$-continuous if and only if

$p_1 \subseteq p_2 \subseteq p_3 \subseteq \ldots$ implies that $\mathcal{F}\,(\cup_i\, p_i) = \cup_i\, \mathcal{F}\,(p_i)$

If S is finite, then we can compute the least fixpoint using the sequence $\emptyset$, $\mathcal{F}\,\emptyset$, $\mathcal{F}^2\,\emptyset$, $\mathcal{F}^3\,\emptyset$, ... This sequence is guaranteed to converge if S is finite and it will converge to the least fixpoint.

Computing the Least Fixpoint

Given a monotonic and union continuous function $\mathcal{F}$

$$\mu\, y\,.\,\mathcal{F}\, y = \cup_i\, \mathcal{F}^i\,(\emptyset)$$

We can prove this as follows:

- First, we can show that for all i, $\mathcal{F}^i\,(\emptyset) \subseteq \mu\, y\,.\,\mathcal{F}\, y$ using induction

for i=0, we have $\mathcal{F}^0\,(\emptyset) = \emptyset \subseteq \mu\, y\,.\,\mathcal{F}\, y$

Assuming $\mathcal{F}^i\,(\emptyset) \subseteq \mu\, y\,.\,\mathcal{F}\, y$

and applying the function $\mathcal{F}$ to both sides and using monotonicity of $\mathcal{F}$ we get: $\mathcal{F}\,(\mathcal{F}^i\,(\emptyset)) \subseteq \mathcal{F}\,(\mu\, y\,.\,\mathcal{F}\, y)$

and since $\mu\, y\,.\,\mathcal{F}\, y$ is a fixpoint of $\mathcal{F}$ we get:

$\mathcal{F}^{i+1}\,(\emptyset) \subseteq \mu\, y\,.\,\mathcal{F}\, y$

which completes the induction.

Computing the Least Fixpoint

- So, we showed that for all i, $\mathcal{F}^{\,i}(\emptyset) \subseteq \mu\, y \,.\, \mathcal{F}\, y$

- If we take the least upper bound of all the elements in the sequence $\mathcal{F}^{\,i}(\emptyset)$ we get $\cup_i \mathcal{F}^{\,i}(\emptyset)$ and using above result, we have:

  $$\cup_i \mathcal{F}^{\,i}(\emptyset) \subseteq \mu\, y \,.\, \mathcal{F}\, y$$

- Now, using union-continuity we can conclude that

$$\mathcal{F}(\cup_i \mathcal{F}^{\,i}(\emptyset)) = \cup_i \mathcal{F}(\mathcal{F}^{\,i}(\emptyset)) = \cup_i \mathcal{F}^{\,i+1}(\emptyset)$$
$$= \emptyset \cup_i \mathcal{F}^{\,i+1}(\emptyset) = \cup_i \mathcal{F}^{\,i}(\emptyset)$$

- So, we showed that $\cup_i \mathcal{F}^{\,i}(\emptyset)$ is a fixpoint of $\mathcal{F}$ and $\cup_i \mathcal{F}^{\,i}(\emptyset) \subseteq \mu\, y \,.\, \mathcal{F}\, y$, then we conclude that $\mu\, y \,.\, \mathcal{F}\, y = \cup_i \mathcal{F}^{\,i}(\emptyset)$

Computing the Least Fixpoint

If there exists a j, where $\mathcal{F}^{j}(\emptyset) = \mathcal{F}^{j+1}(\emptyset)$, then

$$\mu y \,.\, \mathcal{F}\, y = \mathcal{F}^{j}(\emptyset)$$

- We have proved earlier that for all i, $\mathcal{F}^{i}(\emptyset) \subseteq \mu y \,.\, \mathcal{F}\, y$
- If $\mathcal{F}^{j}(\emptyset) = \mathcal{F}^{j+1}(\emptyset)$, then $\mathcal{F}^{j}(\emptyset)$ is a fixpoint of $\mathcal{F}$ and since we know that $\mathcal{F}^{j}(\emptyset) \subseteq \mu y \,.\, \mathcal{F}\, y$ then we conclude that

$$\mu y \,.\, \mathcal{F}\, y = \mathcal{F}^{j}(\emptyset)$$

EF Fixpoint Computation

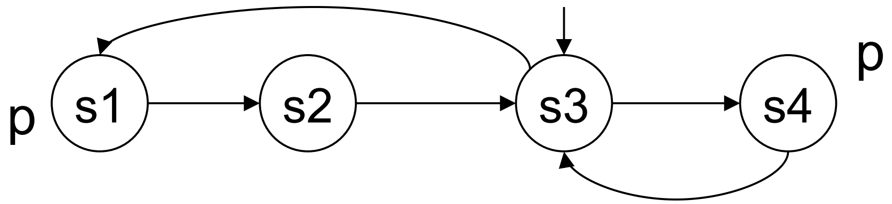
EF p = μ y . p $\vee$ EX y is the limit of the sequence:

$\emptyset$, p$\vee$EX $\emptyset$, p$\vee$EX(p$\vee$EX $\emptyset$) , p$\vee$EX(p$\vee$EX(p$\vee$ EX $\emptyset$)) , ...

which is equivalent to

$\emptyset$, p, p $\vee$ EX p , p $\vee$ EX (p $\vee$ EX (p)) , ...

EF Fixpoint Computation



Start

$\emptyset$

1^{st} iteration

$p \vee EX\ \emptyset = \{s1,s4\} \cup EX(\emptyset) = \{s1,s4\} \cup \emptyset = \{s1,s4\}$

2^{nd} iteration

$p \vee EX(p \vee EX\ \emptyset) = \{s1,s4\} \cup EX(\{s1,s4\}) = \{s1,s4\} \cup \{s3\} = \{s1,s3,s4\}$

3^{rd} iteration

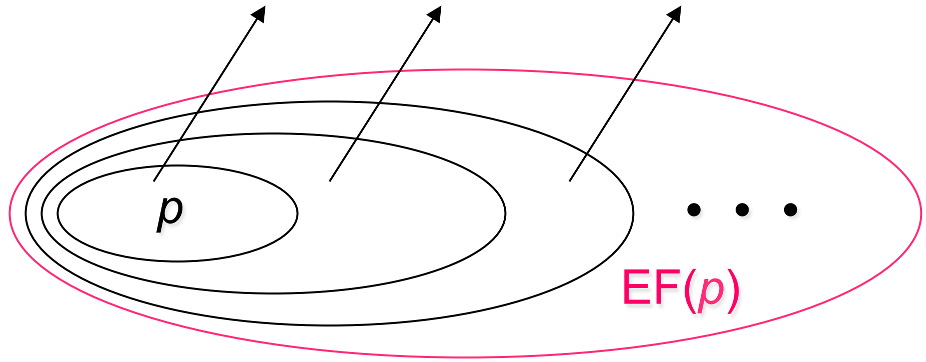
$p \vee EX(p \vee EX(p \vee EX\ \emptyset)) = \{s1,s4\} \cup EX(\{s1,s3,s4\}) = \{s1,s4\} \cup \{s2,s3,s4\} = \{s1,s2,s3,s4\}$

4^{th} iteration

$p \vee EX(p \vee EX(p \vee EX(p \vee EX\ \emptyset))) = \{s1,s4\} \cup EX(\{s1,s2,s3,s4\}) = \{s1,s4\} \cup \{s1,s2,s3,s4\}$
$= \{s1,s2,s3,s4\}$

EF Fixpoint Computation

EF(p) ≡ states that can reach p ≡ $p \cup \text{EX}(p) \cup \text{EX}(\text{EX}(p)) \cup \ldots$



Greatest Fixpoint

Given a monotonic function $\mathcal{F}$, its greatest fixpoint exists and it is the least upper bound (lub) of all the extensive elements:

$$\nu\, y.\, \mathcal{F}\, y = \cup \{ y \mid y \subseteq \mathcal{F}\, y \}$$

This can be proved using a proof similar to the one we used for the dual result on least fixpoints

Computing the Greatest Fixpoint

The greatest fixpoint $\nu y . \mathcal{F} y$ is the limit of the following sequence (assuming $\mathcal{F}$ is $\cap$-continuous):

$S, \mathcal{F} S, \mathcal{F}^2 S, \mathcal{F}^3 S, ...$

$\mathcal{F}$ is $\cap$-continuous if and only if

For any sequence $p_1, p_2, p_3 \ldots$ if $p_{i+1} \subseteq p_i$ for all i, then $\mathcal{F} (\cap_i p_i) = \cap_i \mathcal{F} (p_i)$

If S is finite, then we can compute the greatest fixpoint using the sequence $S, \mathcal{F} S, \mathcal{F}^2 S, \mathcal{F}^3 S, \ldots$ This sequence is guaranteed to converge if S is finite and it will converge to the greatest fixpoint.

Computing the Greatest Fixpoint

Given a monotonic and intersection continuous function $\mathcal{F}$

$$\nu\, y.\ \mathcal{F}\, y = \cap_I\, \mathcal{F}^i\, (S)$$

If there exists a j, where $\mathcal{F}^j\, (S) = \mathcal{F}^{j+1}\, (S)$, then

$$\nu\, y.\ \mathcal{F}\, y = \mathcal{F}^j\, (S)$$

Again, these can be proved using proofs similar to the ones we used for the dual results for the least fixpoint.

EG Fixpoint Computation

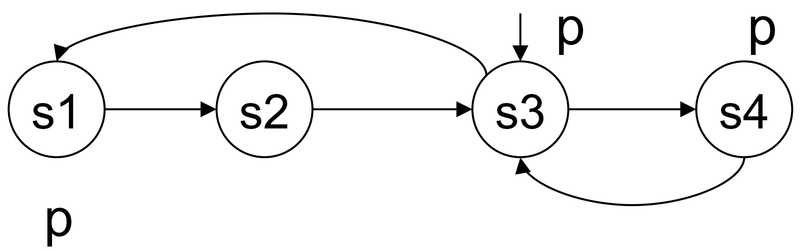
Similarly, $EG\ p = \nu y \,.\, p \wedge EX\ y$ is the limit of the sequence:

$S,\ p \wedge EX\ S,\ p \wedge EX(p \wedge EX\ S),\ p \wedge EX(p \wedge EX\ (p \wedge EX\ S)),\ \ldots$

which is equivalent to

$S,\ p,\ p \wedge EX\ p,\ p \wedge EX\ (p \wedge EX\ (p)),\ \ldots$

EG Fixpoint Computation



Start
S = {s1,s2,s3,s4}

1st iteration
$p \wedge EX\ S = \{s1,s3,s4\} \cap EX(\{s1,s2,s3,s4\}) = \{s1,s3,s4\} \cap \{s1,s2,s3,s4\} = \{s1,s3,s4\}$

2nd iteration
$p \wedge EX(p \wedge EX\ S) = \{s1,s3,s4\} \cap EX(\{s1,s3,s4\}) = \{s1,s3,s4\} \cap \{s2,s3,s4\} = \{s3,s4\}$

3rd iteration
$p \wedge EX(p \wedge EX(p \wedge EX\ S)) = \{s1,s3,s4\} \cap EX(\{s3,s4\}) = \{s1,s3,s4\} \cap \{s2,s3,s4\} = \{s3,s4\}$

EG Fixpoint Computation

EG(p) ≡ states that can avoid reaching $\neg p$ ≡ $p \cap$ EX(p) $\cap$ EX(EX(p)) $\cap$ ...