Game-Theoretic Approach to Planning and Synthesis

Fixpoints and Mu-Calculus

Giuseppe De Giacomo Antonio Di Stasio Giuseppe Perelli Shufang Zhu

ERC Advanced Grant
WhiteMech:
White-box Self Programming Mechanisms

PhD-AI Course
4-8 July, 2022

We briefly recall few notions on fixpoints.

- Consider the equation:
$$X = f(X)$$
where f is an operator from $2^{\mathcal{S}}$ to $2^{\mathcal{S}}$ ($2^{\mathcal{S}}$ denotes the set of all subsets of a set $\mathcal{S}$).
- Every solution $\mathcal{E}$ of this equation is called a **fixpoint** of the operator f
- every set $\mathcal{E}$ such that $f(\mathcal{E}) \subseteq \mathcal{E}$ is called **pre-fixpoint**, and
- every set $\mathcal{E}$ such that $\mathcal{E} \subseteq f(\mathcal{E})$ is called **post-fixpoint**.
- In general, an equation as the one above may have either no solution, a finite number of solutions, or an infinite number of them. Among the various solutions, the smallest and the greatest solutions (with respect to set-inclusion) have a prominent position, if they exist.
- The the smallest and the greatest solutions are called **least fixpoint** and **greatest fixpoint**, respectively.

We say that f is **monotonic** wrt $\subseteq$ (set-inclusion) whenever $\mathcal{E}_1 \subseteq \mathcal{E}_2$ implies $f(\mathcal{E}_1) \subseteq f(\mathcal{E}_2)$.

Theorem (Tarski'55)

Let $\mathcal{S}$ be a set, and f an operator from $2^{\mathcal{S}}$ to $2^{\mathcal{S}}$ that is monotonic wrt $\subseteq$. Then:

- *There exists a unique least fixpoint of f, which is given by $\bigcap\{\mathcal{E} \subseteq \mathcal{S} \mid f(\mathcal{E}) \subseteq \mathcal{E}\}$.*
- *There exists a unique greatest fixpoint of f, which is given by $\bigcup\{\mathcal{E} \subseteq \mathcal{S} \mid \mathcal{E} \subseteq f(\mathcal{E})\}$.*

SAPIENZA UNIVERSITÀ DI ROMA

We start by showing the proof for the **least fixpoint** part. (The proof for the greatest fixpoint is analogous, see later).

Let us define $\mathcal{L} = \bigcap\{\mathcal{E} \subseteq \mathcal{S} \mid f(\mathcal{E}) \subseteq \mathcal{E}\}$.

Lemma

$f(\mathcal{L}) \subseteq \mathcal{L}$

Proof.

- For every $\mathcal{E}$ such that $f(\mathcal{E}) \subseteq \mathcal{E}$, we have $\mathcal{L} \subseteq \mathcal{E}$, by definition of $\mathcal{L}$.
- By monotonicity of f, we have $f(\mathcal{L}) \subseteq f(\mathcal{E})$.
- Hence $f(\mathcal{L}) \subseteq \mathcal{E}$ (for every $\mathcal{E}$ such that $f(\mathcal{E}) \subseteq \mathcal{E}$).
- But then $f(\mathcal{L})$ is contained in the intersection of all such $\mathcal{E}$, so we have $f(\mathcal{L}) \subseteq \mathcal{L}$.

□

Lemma

$\mathcal{L} \subseteq f(\mathcal{L})$

Proof.

- By the previous lemma, we have $f(\mathcal{L}) \subseteq \mathcal{L}$.
- But then $f(f(\mathcal{L})) \subseteq f(\mathcal{L})$, by monotonicity.
- Hence, $\bar{\mathcal{E}} = f(\mathcal{L})$ is such that $f(\bar{\mathcal{E}}) \subseteq \bar{\mathcal{E}}$.
- Thus, $\mathcal{L} \subseteq f(\mathcal{L})$, by definition of $\mathcal{L}$.

□

The previous two lemmas together show that $\mathcal{L}$ is indeed a fixpoint: $\mathcal{L} = f(\mathcal{L})$. We still need to show that is the **least** fixpoint.

Lemma

$\mathcal{L}$ is the least *fixpoint: for every $f(\mathcal{E}) = \mathcal{E}$ we have $\mathcal{L} \subseteq \mathcal{E}$.*

Proof.

By contradiction.

- Suppose not. Then there exists an $\hat{\mathcal{E}}$ such that $f(\hat{\mathcal{E}}) = \hat{\mathcal{E}}$ and $\hat{\mathcal{E}} \subset \mathcal{L}$.
- Being $\hat{\mathcal{E}}$ a fixpoint (i.e., $f(\hat{\mathcal{E}}) = \hat{\mathcal{E}}$), we have in particular $f(\hat{\mathcal{E}}) \subseteq \hat{\mathcal{E}}$.
- Hence by definition of $\mathcal{L}$, we get $\mathcal{L} \subseteq \hat{\mathcal{E}}$. Contradiction.

□

Now we prove the **greatest fixpoint** part.

Let us define $\mathcal{G} = \bigcup\{\mathcal{E} \subseteq \mathcal{S} \mid \mathcal{E} \subseteq f(\mathcal{E})\}$.

Lemma

$\mathcal{G} \subseteq f(\mathcal{G})$

Proof.

- For every $\mathcal{E}$ such that $\mathcal{E} \subseteq f(\mathcal{E})$, we have $\mathcal{E} \subseteq \mathcal{G}$, by definition of $\mathcal{G}$.
- Consider now $e \in \mathcal{G}$. Then there exists an $\hat{\mathcal{E}}$ such that $\hat{\mathcal{E}} \subseteq f(\hat{\mathcal{E}})$, $e \in \hat{\mathcal{E}}$, by definition of $\mathcal{G}$.
- But $\hat{\mathcal{E}} \subseteq \mathcal{G}$, and by monotonicity $f(\hat{\mathcal{E}}) \subseteq f(\mathcal{G})$, hence $e \in f(\mathcal{G})$.

□

Lemma

$f(\mathcal{G}) \subseteq \mathcal{G}$

Proof.

- By the previous lemma we have $\mathcal{G} \subseteq f(\mathcal{G})$
- But then, we have that $f(\mathcal{G}) \subseteq f(f(\mathcal{G}))$, by monotonicity.
- Hence, $\bar{\mathcal{E}} = f(\mathcal{G})$ is such that $\bar{\mathcal{E}} \subseteq f(\bar{\mathcal{E}})$.
- Thus, $f(\mathcal{G}) \subseteq \mathcal{G}$, by definition of $\mathcal{G}$.

□

The previous two lemmas together show that $\mathcal{L}$ is indeed a fixpoint: $\mathcal{G} = f(\mathcal{G})$. We still need to show that is the **greatest** fixpoint.

Lemma

$\mathcal{G}$ is the greatest *fixpoint: for every $\mathcal{E} = f(\mathcal{E})$ we have $\mathcal{E} \subseteq \mathcal{G}$.*

Proof.

By contradiction.

- Suppose not. Then there exists an $\hat{\mathcal{E}}$ such that $\hat{\mathcal{E}} = f(\hat{\mathcal{E}})$ and $\mathcal{G} \subset \hat{\mathcal{E}}$.
- Being $\hat{\mathcal{E}}$ a fixpoint, we have $\hat{\mathcal{E}} \subseteq f(\hat{\mathcal{E}})$.
- Hence by definition of $\mathcal{G}$, we get $\hat{\mathcal{E}} \subseteq \mathcal{G}$. Contradiction.

□

The approximates for a least fixpoint $\mathcal{L} = \bigcap\{\mathcal{E} \subseteq \mathcal{S} \mid f(\mathcal{E}) \subseteq \mathcal{E}\}$ are as follows:

$$Z_0 \doteq \varnothing$$
$$Z_1 \doteq f(Z_0)$$
$$Z_2 \doteq f(Z_1)$$
$$\ldots$$

Lemma

For all i, $Z_i \subseteq Z_{i+1}$.

Proof.

By induction on i.

- Base case: $i = 0$. By definition $Z_0 = \varnothing$, and trivially $\varnothing \subseteq Z_1$.
- Inductive case: $i = k + 1$. By inductive hypothesis we assume $Z_{k-1} \subseteq Z_k$, and we show that $Z_k \subseteq Z_{k+1}$.
  - $f(Z_{k-1}) \subseteq f(Z_k)$, by monotonicity.
  - But $f(Z_{k-1}) = Z_k$ and $f(Z_k) = Z_{k+1}$, hence we have $Z_k \subseteq Z_{k+1}$.

□

SAPIENZA UNIVERSITÀ DI ROMA

Lemma

For all i, $Z_i \subseteq \mathcal{L}$.

Proof.

By induction on i.

- Base case: $i = 0$. By definition $Z_0 = \emptyset$, and trivially $\emptyset \subseteq \mathcal{L}$.
- Inductive case: $i = k + 1$. By inductive hypothesis we assume $Z_k \subseteq \mathcal{L}$, and we show that $Z_{k+1} \subseteq \mathcal{L}$.
  - $f(Z_k) \subseteq f(\mathcal{L})$, by monotonicity.
  - But then $f(Z_k) \subseteq \mathcal{L}$, since $\mathcal{L} = f(\mathcal{L})$.
  - Hence, considering that $f(Z_k) = Z_{k+1}$, we have $Z_{k+1} \subseteq \mathcal{L}$.

□

SAPIENZA UNIVERSITÀ DI ROMA

Theorem (Tarski-Knaster on approximates of least fixpoints)

If for some n, $Z_{n+1} = Z_n$, then $Z_n = \mathcal{L}$.

Proof.

- $Z_n \subseteq \mathcal{L}$ by the above lemma.
- On the other hand, since $Z_{n+1} = f(Z_n) = Z_n$, we trivially get $f(Z_n) \subseteq Z_n$, and hence $\mathcal{L} \subseteq Z_n$ by definition of $\mathcal{L}$.

□

Observe also that once for some n, $Z_{n+1} = Z_n$, then for all $m \geq n$ we have $Z_{m+1} = Z_m$, by definition of approximates.

In fact this theorem can be generalized by ranging n over ordinals instead of natural numbers.

The above theorem gives us a simple sound procedure to compute the least fixpoint:

Least fixpoint algorithm

$Z_{old} := \emptyset;$
$Z := f(Z_{old});$
while $(Z \neq Z_{old})\{$
    $Z_{old} := Z;$
    $Z := f(Z);$
$\}$

If in $\mathcal{L} = \bigcap\{\mathcal{E} \subseteq \mathcal{S} \mid \ f(\mathcal{E}) \subseteq \mathcal{E}\}$ the set $\mathcal{S}$ **is finite** then the above procedure **terminates** in $|\mathcal{S}|$ steps and becomes **sound and complete**.

Notice the above procedure is **polynomial** in the size of $\mathcal{S}$.

The approximates for the greatest fixpoint $\mathcal{G} = \bigcup\{\mathcal{E} \subseteq \mathcal{S} \mid \mathcal{E} \subseteq f(\mathcal{E})\}$ are as follows:

$$Z_0 \doteq \mathcal{S}$$
$$Z_1 \doteq f(Z_0)$$
$$Z_2 \doteq f(Z_1)$$
$$\ldots$$

Lemma

For all i, $Z_{i+1} \subseteq Z_i$.

Proof.

By induction on i.

- Base case: $i = 0$. By definition $Z_0 = \mathcal{S}$, and trivially $Z_1 \subseteq \mathcal{S}$.
- Inductive case: $i = k + 1$: by inductive hypothesis we assume $Z_k \subseteq Z_{k-1}$, and we show that $Z_{k+1} \subseteq Z_k$.
  - $f(Z_k) \subseteq f(Z_{k-1})$, by monotonicity.
  - But $f(Z_k = Z_{k+1}$ and $f(Z_{k-1}) = Z_k$ hence $Z_{k+1} \subseteq Z_k$.

□

SAPIENZA UNIVERSITÀ DI ROMA

Lemma

For all i, $\mathcal{G} \subseteq Z_i$.

Proof.

By induction on i.

- Base case: $i = 0$. By definition $Z_0 = \mathcal{S}$, and trivially $\mathcal{G} \subseteq \mathcal{S}$.
- Inductive case: $i = k + 1$: by inductive hypothesis we assume $\mathcal{G} \subseteq Z_k$, and we show that $G \subseteq Z_{k+1}$.
  - $f(\mathcal{G}) \subseteq f(Z_k)$, by monotonicity.
  - But then $\mathcal{G} \subseteq f(Z_k)$, since $\mathcal{G} = f(\mathcal{G})$.
  - Hence, considering that $f(Z_k) = Z_{k+1}$, we get $\mathcal{G} \subseteq Z_{k+1}$.

□

SAPIENZA UNIVERSITÀ DI ROMA

Theorem (Tarski-Knaster on approximates of greatest fixpoint)

If for some n, $Z_{n+1} = Z_n$, then $Z_n = \mathcal{G}$.

Proof.

- $\mathcal{G} \subseteq Z_n$ by the above lemma.
- On the other hand, since $Z_{n+1} = f(Z_n) = Z_n$, we trivially get $Z_n \subseteq f(Z_n)$, and hence $Z_n \subseteq \mathcal{G}$ by definition of $\mathcal{G}$.

□

Observe also that once for some n, $Z_{n+1} = Z_n$, then for all $m \geq n$ we have $Z_{m+1} = Z_m$, by definition of approximates.

In fact this theorem can be generalized by ranging n over ordinals instead of natural numbers.

The above theorem gives us a simple sound procedure to compute the greatest fixpoint:

Greatest fixpoint algorithm

$Z_{old} := \mathcal{S}$;
$Z := f(Z_{old})$;
while $(Z \neq Z_{old})\{$
    $Z_{old} := Z$;
    $Z := f(Z)$;
$\}$

If in $\mathcal{G} = \bigcup\{\mathcal{E} \subseteq \mathcal{S} \mid \mathcal{E} \subseteq f(\mathcal{E})\}$ the set $\mathcal{S}$ **is finite** then the above procedure **terminates** in $|\mathcal{S}|$ steps and becomes **sound and complete**.

Notice the above procedure is **polynomial** in the size of $\mathcal{S}$.

For simplicity we have considered fixpoint wrt set-inclusion. In fact, the only property of set inclusion that we have used is the **lattice** implicitly defined by it.

We recall that a lattice is a the partial order (defined by set inclusion in our case), with the minimal element ($\varnothing$ in our case) and maximal element ($\mathcal{S}$ in our case).

We can immediately extend all the results presented here to arbitrary lattices substituting to the relation $\subseteq$ the relation $\leq$ of the lattice.

The (modal) Mu-Calculus is basically constituted by three kinds of components:

- **Propositions** to denote properties of the global store in a given configuration.
- **Modalities** to denote the capability of performing certain actions in a given configuration.
- **Least and greatest fixpoint constructs** to denote "temporal" properties of the system, typically defined by **induction** and **coinduction**.

Formulae of Mu-Calculus are formed inductively from action in some fixed set $\mathcal{A}$, primitive (or atomic) propositions in some fixed set $\mathcal{P}$, and variable symbols in some fixed set $\mathcal{V}$, according to the following abstract syntax:

Mu-Calculus syntax

$$\Phi ::= A \mid \mathit{true} \mid \mathit{false} \mid \neg\Phi \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid \langle a \rangle \Phi \mid [a]\Phi \mid \mu X.\Phi \mid \nu X.\Phi \mid X$$

where A is a primitive proposition in $\mathcal{P}$, X is a variable symbol in $\mathcal{V}$, and a is an action in $\mathcal{A}$.
The symbols μ and ν can be considered as quantifiers, and we make use of notions of scope, bound and free occurrences of variables, closed formulas, etc. The definitions of these notions are the same as in first-order logic, treating μ and ν as quantifiers.

For formulae of the form $\mu X.\Phi$ and $\nu X.\Phi$, we require the **syntactic monotonicity** of Φ wrt X:

Syntactic monotonicity of Φ wrt X

Every occurrence of the variable X in Φ must be within the scope of an even number of negation signs.

Syntactic monotonicity implies **monotonicity**, guaranteeing, by Tarski-Knaster theorem the actual existence of least and greatest fixpoints.

Existence of least and greatest fixpoints

In Mu-Calculus, given the requirement of syntactic monotonicity, the least fixpoint $\mu X.\Phi$ and the greatest fixpoint $\nu X.\Phi$ always exist.

The semantics of Mu-Calculus is based on the notions of **transition system** (i.e., Kripke structure) and variables' **valuation**.

Definition

Transition system Given a set $\mathcal{P}$ of propositions, and set $\mathcal{A}$ of atomic actions, a **transition system** is a triple $\mathcal{T} = (\mathcal{S}, \{\mathcal{R}_a | a \in \mathcal{A}\}, \Pi)$, with a set of states $\mathcal{S}$, a family of transition relations $\mathcal{R}_a \in \mathcal{S} \times \mathcal{S}$, and a mapping Π from $\mathcal{P}$ to subsets of $\mathcal{S}$.

Definition

Valuation Given a transition system $\mathcal{T}$, a **valuation** $\mathcal{V}$ on $\mathcal{T}$ is a mapping from variables in $\mathcal{V}$ to subsets of the states in $\mathcal{T}$.

Given a valuation $\mathcal{V}$, we denote by $\mathcal{V}[X \leftarrow \mathcal{E}]$, the valuation identical to $\mathcal{V}$ except for $\mathcal{V}[X \leftarrow \mathcal{E}](X) = \mathcal{E}$, i.e. for every variable Y,

$$\mathcal{V}[X \leftarrow \mathcal{E}](Y) = \begin{cases} \mathcal{E} & \text{if } Y = X \\ \mathcal{V}(Y) & \text{if } Y \neq X \end{cases}$$

Let $\mathcal{T} = (\mathcal{S}, \{\mathcal{R}_\alpha | \alpha \in 2^{\mathcal{A}}\}, \Pi)$ be a transition system, and $\mathcal{V}$ a valuation on $\mathcal{T}$. We assign meaning to Mu-Calculus formulae by associating to $\mathcal{T}$ and $\mathcal{V}$ an **extension function** $(\cdot)^{\mathcal{M}}_{\mathcal{V}}$, which maps Mu-Calculus formulae to subsets of $\mathcal{S}$.

The extension function $(\cdot)^{\mathcal{M}}_{\mathcal{V}}$ is defined inductively as follows:

Mu-Calculus semantics

$$
\begin{array}{lcl}
(A)^{\mathcal{M}}_{\mathcal{V}} & = & \Pi(A) \subseteq \mathcal{S} \\
(X)^{\mathcal{M}}_{\mathcal{V}} & = & \mathcal{V}(X) \subseteq \mathcal{S} \\
(\mathit{true})^{\mathcal{M}}_{\mathcal{V}} & = & \mathcal{S} \\
(\mathit{false})^{\mathcal{M}}_{\mathcal{V}} & = & \varnothing \\
(\neg\Phi)^{\mathcal{M}}_{\mathcal{V}} & = & \mathcal{S} - (\Phi)^{\mathcal{M}}_{\mathcal{V}} \\
(\Phi_1 \wedge \Phi_2)^{\mathcal{M}}_{\mathcal{V}} & = & (\Phi_1)^{\mathcal{M}}_{\mathcal{V}} \cap (\Phi_2)^{\mathcal{M}}_{\mathcal{V}} \\
(\Phi_1 \vee \Phi_2)^{\mathcal{M}}_{\mathcal{V}} & = & (\Phi_1)^{\mathcal{M}}_{\mathcal{V}} \cup (\Phi_2)^{\mathcal{M}}_{\mathcal{V}} \\
(\langle a \rangle \Phi)^{\mathcal{M}}_{\mathcal{V}} & = & \{s \in \mathcal{S} \mid \exists s'.\ (s, s') \in \mathcal{R}_a \text{ and } s' \in (\Phi)^{\mathcal{M}}_{\mathcal{V}}\} \\
([a]\Phi)^{\mathcal{M}}_{\mathcal{V}} & = & \{s \in \mathcal{S} \mid \forall s'.\ (s, s') \in \mathcal{R}_a \text{ implies } s' \in (\Phi)^{\mathcal{M}}_{\mathcal{V}}\} \\
(\mu X.\Phi)^{\mathcal{M}}_{\mathcal{V}} & = & \bigcap\{\mathcal{E} \subseteq \mathcal{S} \mid \quad (\Phi)^{\mathcal{T}}_{\mathcal{V}[X \leftarrow \mathcal{E}]} \subseteq \mathcal{E}\ \} \\
(\nu X.\Phi)^{\mathcal{M}}_{\mathcal{V}} & = & \bigcup\{\mathcal{E} \subseteq \mathcal{S} \mid \quad \mathcal{E} \subseteq \ (\Phi)^{\mathcal{T}}_{\mathcal{V}[X \leftarrow \mathcal{E}]}\}
\end{array}
$$

Note that, the semantics shows that not all Mu-Calculus constructs are independent. In particular, we have:

- The usual boolean abbreviations: $\mathit{false} = A \wedge \neg A$; $\mathit{true} = \neg \mathit{false}$; $\Phi_1 \vee \Phi_2 = \neg(\neg\Phi_1 \wedge \neg\Phi_2)$; and also $\Phi_1 \supset \Phi_2 = \neg\Phi_1 \vee \Phi_2$.
- $[\varrho]\Phi = \neg\langle\varrho\rangle\neg\Phi$;
- $\nu X.\Phi = \neg\mu X.\neg\Phi[X/\neg X]$ where $\Phi[X/\neg X]$ is the formula obtained by substituting all free occurrences of X by the formula $\neg X$.

Note also that if Φ is closed (no free variables are present in Φ) then the extension of $(\Phi)^{\mathcal{M}}_{\mathcal{V}}$ is in fact independent of the valuation $\mathcal{V}$ so we could write $(\Phi)^{\mathcal{T}}$, dropping any reference to $\mathcal{V}$. It is usual to say that **a closed Φ is true in a state s of the transition system $\mathcal{T}$** iff $s \in (\Phi)^{\mathcal{T}}$.

Formally $s \in (\Phi)^{\mathcal{T}}$ stands or $s \in (\Phi)^{\mathcal{M}}_{\mathcal{V}}$ for every valuation $\mathcal{V}$ (the extension of Φ is in fact independent of $\mathcal{V}$ with Φ closed).

Intuitively, the extension function $(\cdot)^{\mathcal{M}}_{\mathcal{V}}$ assigns to the various constructs of Mu-Calculus the following meanings:

Intuition on $(\cdot)^{\mathcal{M}}_{\mathcal{V}}$

- The boolean connectives have the expected meaning.
- The extension of $\langle a \rangle \Phi$ includes the states $s \in \mathcal{S}$ such that starting from s, there is an execution of action a that leads to a successive state s' included in the extension of Φ.
- The extension of $[a]\Phi$ includes the states s such that starting from s, each execution of action a leads to some successive state s' included in the extension of Φ.

For the fixpoint constructs we have:

Intuition on $(\mu X.\Phi)^{\mathcal{M}}_{\mathcal{V}}$ and $(\nu X.\Phi)^{\mathcal{M}}_{\mathcal{V}}$

- The extension of $\mu X.\Phi$ is the **smallest subset** $\mathcal{E}_\mu$ of $\mathcal{S}$ such that, assigning to X the extension $\mathcal{E}_\mu$, the resulting extension of Φ is contained in $\mathcal{E}_\mu$. That is, the extension of $\mu X.\Phi$ is the **least fixpoint** of the operator $\lambda\mathcal{E}.(\Phi)^{\mathcal{T}}_{\mathcal{V}[X\leftarrow\mathcal{E}]}$.
- Similarly, the extension of $\nu X.\Phi$ is the **greatest subset** $\mathcal{E}_\nu$ of $\mathcal{S}$ such that, assigning to X the extension $\mathcal{E}_\nu$, the resulting extension of Φ contains $\mathcal{E}_\nu$. That is, the extension of $\nu X.\Phi$ is the **greatest fixpoint** of the operator $\lambda\mathcal{E}.(\Phi)^{\mathcal{T}}_{\mathcal{V}[X\leftarrow\mathcal{E}]}$.

The syntactic monotonicity of Φ wrt X guarantees the monotonicity of the operator $\lambda\mathcal{E}.(\Phi)^{\mathcal{T}}_{\mathcal{V}[X\leftarrow\mathcal{E}]}$ and hence, by Tarski-Knaster Theorem, the unique existence of the least fixpoint.

Let us consider the case we have a single action *next* represent generic transitions. Then:

Example

$$\langle next \rangle true$$

expresses the capability of making a *next*-transition

Example

$$[next]false$$

expresses the inability of executing any *next*-transition.

Example

$$\langle next \rangle true \wedge [next]P$$

says that *next*-transitions are allowed and they all reach states where P holds.

SAPIENZA UNIVERSITÀ DI ROMA

Example

$$\mu X.P \vee \langle next \rangle X$$

expresses that there **exists an evolution** of the system such that P **eventually** holds. Indeed, its extension $\mathcal{E}_\mu$ is the smallest set that includes (1) the states in the extension of Φ; and (2) the states that can execute a transition leading to a successive state that is in $\mathcal{E}_\mu$. In other words, the extension $\mathcal{E}_\mu$ includes each state s such that there exists a run from s leading eventually (i.e. in a finite number of steps) to a state in the extension of P. Note the inductive nature of this property which is typical of properties defined by least fixpoint.

SAPIENZA UNIVERSITÀ DI ROMA

Example

$$\nu X.P \wedge [next]X$$

i.e. $\neg(\mu X.\neg P \vee \langle next\rangle X)$ – expresses the **invariance** of P under all of the evolutions of the system. Indeed, its extension $\mathcal{E}_\nu$ is the largest set of states in the extension of P from which every transition leads to a successive state which is still in $\mathcal{E}_\nu$. In other words, the extension $\mathcal{E}_\nu$ includes each state s such that every state along every run from s is in the extension of P. Note the coinductive nature of this property which is typical of properties defined by greatest fixpoint.

SAPIENZA UNIVERSITÀ DI ROMA

Example

$$\mu X.P \vee (\langle next \rangle true \wedge [next]X)$$

expresses that for **all evolutions** of the system, P **eventually** holds. Indeed, its extension $\mathcal{E}_\mu$ is the smallest set that includes (1) the states in the extension of P; and (2) the states that can make a transition and such that every transition leads to a state in $\mathcal{E}_\mu$. In other words, the extension $\mathcal{E}_\mu$ includes each state s such that every run from s leads eventually (i.e. in a finite number of steps) to a state in the extension of P.

Example

$$\nu X.\mu Y.(P \wedge \langle next \rangle X) \vee (\langle next \rangle Y)$$

expresses a **strong fairness** of a run: there exists a run where P is true infinitely often.

In general, Mu-Calculus allows for expressing very sophisticated properties of dynamic systems, such as very general forms of **liveness**, **safety**, *and* **fairness**.

Often, we use the notation $\Phi(X)$ to indicate that the variable X occurs free in the formula Φ (other variables could occur free in Φ as well), and the notation $\Phi(\Psi)$, where Ψ is a formula, as a shorthand for the formula obtained by syntactically substituting all free occurrences of X in $\Phi(X)$ by the concept Ψ).

Simple properties

Below σ stands for μ or ν

- $\sigma X.\Phi(X)$ is equivalent to $\sigma Y.\Phi(Y)$, as long as Y is free for X in $\Phi(X)$.
- $\sigma X.\Phi$ and X does not occur in Φ, then $\sigma X.\Phi$ equivalent to Φ.
- $\Phi(\sigma X.\Phi(X))$ is equivalent to $\sigma X.\Phi(X)$, indeed $\sigma X.\Phi(X)$ is a fixpoint.
- $\mu X.\Phi(X)$ logically implies $\nu X.\Phi(X)$, indeed the least fixpoint is always smaller/equal to the greatest fixpoint.

The reasoning problem we are interested in is **model checking**:

Definition

Let $\mathcal{T} = (\mathcal{S}, \{\mathcal{R}_a \mid a \in \mathcal{A}\}, \Pi)$ be a transition system, let $s \in \mathcal{S}$ be one of its states, and let Φ be a closed (no free variables are present) Mu-Calculus formula. The related **model checking** problem is to verify whether

$$s \in (\Phi)^{\mathcal{M}}_{\mathcal{V}}$$

where $\mathcal{V}$ is any valuation, since Φ is closed.

Often we abbreviate $s \in (\Phi)^{\mathcal{M}}_{\mathcal{V}}$ by $\mathcal{T}, s \models \Phi$ or simply by $s \models \Phi$ referring to $\mathcal{T}$ only implicitly.

SAPIENZA UNIVERSITÀ DI ROMA

Theorem

Checking (closed) a Mu-Calculus formula Φ over a transition system $\mathcal{T} = (\mathcal{S}, \{\mathcal{R}_a \mid a \in \mathcal{A}\}, \Pi)$ can be done in time

$$O((|\mathcal{T}| \cdot |\Phi|)^k)$$

where $|\mathcal{T}| = |\mathcal{S}| + \Sigma_{a \in \mathcal{A}} |\mathcal{R}_a|$, i.e., the number of states plus the number of transitions of $\mathcal{T}$, $|\Phi|$ is the size of formula Φ (in fact, considering propositional formulas as atomic), and k is the number of nested fixpoints, i.e., fixpoints whose variables are one within the scope of the other.

Also, in general model checking is in $NP \cap coNP$.

Theorem

Checking satifiability/validity/logical implication in Mu-Calculus is decidable and more precisely EXPTIME-complete.

Given a Mu-Calculus formula Φ over a transition system $\mathcal{T} = (\mathcal{S}, \{\mathcal{R}_a \mid a \in \mathcal{A}\}, \Pi)$ and a valuation $\mathcal{V}$, the **model checking algorithm** is based on recursively **labeling the states** of the transition systems with the formulas that are true in them, following closely the semantics.

Mu-Calculus model checking algorithm

$$
\begin{array}{rcl}
[\![A]\!]^{\mathcal{T}}_{\mathcal{V}} & = & \Pi(A) \\
[\![X]\!]^{\mathcal{T}}_{\mathcal{V}} & = & \mathcal{V}(X) \\
[\![\mathit{true}]\!]^{\mathcal{T}}_{\mathcal{V}} & = & \mathcal{S} \\
[\![\mathit{false}]\!]^{\mathcal{T}}_{\mathcal{V}} & = & \varnothing \\
[\![\neg\Phi]\!]^{\mathcal{T}}_{\mathcal{V}} & = & \mathcal{S} - [\![\Phi]\!]^{\mathcal{T}}_{\mathcal{V}} \\
[\![\Phi_1 \wedge \Phi_2]\!]^{\mathcal{T}}_{\mathcal{V}} & = & [\![\Phi_1]\!]^{\mathcal{T}}_{\mathcal{V}} \cap [\![\Phi_2]\!]^{\mathcal{T}}_{\mathcal{V}} \\
[\![\Phi_1 \vee \Phi_2]\!]^{\mathcal{T}}_{\mathcal{V}} & = & [\![\Phi_1]\!]^{\mathcal{T}}_{\mathcal{V}} \cup [\![\Phi_2]\!]^{\mathcal{T}}_{\mathcal{V}}
\end{array}
\qquad
\begin{array}{rcl}
[\![\langle a\rangle\Phi]\!]^{\mathcal{T}}_{\mathcal{V}} & = & \mathit{PreE}(a, [\![\Phi]\!]^{\mathcal{T}}_{\mathcal{V}}) \\
[\![[a]\Phi]\!]^{\mathcal{T}}_{\mathcal{V}} & = & \mathit{PreA}(a, [\![\Phi]\!]^{\mathcal{T}}_{\mathcal{V}})
\end{array}
\qquad
\begin{array}{rcl}
[\![\mu X.\Phi]\!]^{\mathcal{T}}_{\mathcal{V}} & = & \mathrm{LFP}X.[\![\Phi]\!]^{\mathcal{T}}_{\mathcal{V}} \\
[\![\nu X.\Phi]\!]^{\mathcal{T}}_{\mathcal{V}} & = & \mathrm{GFP}X.[\![\Phi]\!]^{\mathcal{T}}_{\mathcal{V}}
\end{array}
$$

where $\mathit{PreE}, \mathit{PreA}, \mathrm{GFP}, \mathrm{LFP}$ are defined below.

For the atomic propositions, variables and propositional operator the labeling works in an obvious way.

Let $\mathcal{E} \subseteq \mathcal{S}$ be a set of state and $a \in \mathcal{A}$ an action. Then $PreE$ and $PreA$ label the existential and universal a-preimage of $\mathcal{E}$ respectively.

Existential a-preimage of $\mathcal{E}$

$PreE(a, \mathcal{E})$, i.e., the **existential a-preimage of $\mathcal{E}$**, is defined as follows:

$$PreE(a, \mathcal{E}) = \{s \in \mathcal{S} \mid \exists s'.\ (s, s') \in \mathcal{R}_a \text{ and } s' \in \mathcal{E}\}$$

Universal a-preimage of $\mathcal{E}$

$PreA(a, \mathcal{E})$, i.e., the **universal a-preimage of $\mathcal{E}$**, is defined as follows:

$$PreA(a, \mathcal{E}) = \{s \in \mathcal{S} \mid \forall s'.\ (s, s') \in \mathcal{R}_a \text{ implies } s' \in \mathcal{E}\}$$

Notice the preimage operators follow the semantics of the $\langle a \rangle \cdot$ and $[a] \cdot$ very closely.

Procedures $\text{LFP}X.[\![\Phi]\!]^{\mathcal{T}}_{\mathcal{V}}$ and $\text{GFP}X.[\![\Phi]\!]^{\mathcal{T}}_{\mathcal{V}}$ apply Tarski-Knaster approximates theorem to compute **least fixpoint** and **greatest fixpoint** of operator $[\![\Phi]\!]^{\mathcal{T}}_{\mathcal{V}}$:

Procedure $\text{LFP}X.[\![\Phi]\!]^{\mathcal{T}}_{\mathcal{V}}$

$\mathcal{X}_{old} := [\![\mathit{False}]\!]^{\mathcal{T}}_{\mathcal{V}}$;
$\mathcal{X} := [\![\Phi]\!]^{\mathcal{T}}_{\mathcal{V}[X \leftarrow \mathcal{X}_{old}]}$;
while $(\mathcal{X} \neq \mathcal{X}_{old})$ {
  $\mathcal{X}_{old} := \mathcal{X}$;
  $\mathcal{X} := [\![\Phi]\!]^{\mathcal{T}}_{\mathcal{V}[X \leftarrow \mathcal{X}_{old}]}$;
}
return $\mathcal{X}$;

Procedure $\text{GFP}X.[\![\Phi]\!]^{\mathcal{T}}_{\mathcal{V}}$

$\mathcal{X}_{old} := [\![\mathit{True}]\!]^{\mathcal{T}}_{\mathcal{V}}$;
$\mathcal{X} := [\![\Phi]\!]^{\mathcal{T}}_{\mathcal{V}[X \leftarrow \mathcal{X}_{old}]}$;
while $(\mathcal{X} \neq \mathcal{X}_{old})$ {
  $\mathcal{X}_{old} := \mathcal{X}$;
  $\mathcal{X} := [\![\Phi]\!]^{\mathcal{T}}_{\mathcal{V}[X \leftarrow \mathcal{X}_{old}]}$;
}
return $\mathcal{X}$;

Notice the number of interations of the while *is at most equal to the number of states $\mathcal{S}$ of the transition system $\mathcal{T}$.*