Fixpoint Theory – Upside Down

Barbara König
Universität Duisburg-Essen

Joint work with Paolo Baldan, Richard Eggert,
Tommaso Padoan

(Work in progress)

Upper and Lower Bounds for Fixpoints

Let $f : \mathbb{L} \to \mathbb{L}$ be a monotone function over a complete lattice $\mathbb{L}$. By Knaster-Tarski it has a least fixpoint μf and a greatest fixpoint νf.

Any pre-fixpoint ($\ell \in \mathbb{L}$ with $f(\ell) \sqsubseteq \ell$) is an upper bound for μf and any post-fixpoint ($\ell \in \mathbb{L}$ with $\ell \sqsubseteq f(\ell)$) is a lower bound for νf.

Challenge

Can we find suitable witnesses guaranteeing that $\ell \in \mathbb{L}$ is a lower bound for μf or an upper bound for νf?

Applications: termination probability, behavioural distances, bisimilarity . . .

Aims of Working Group 1.3

To support and promote the systematic development of the fundamental mathematical theory of systems specification. To investigate the theory of formal models for systems specification, development, transformation and verification.

$\rightsquigarrow$ fixpoints as a fundamental mathematical technique for system verification (reachability analysis, dataflow analysis, model-checking, ...)

Fixpoint Theory

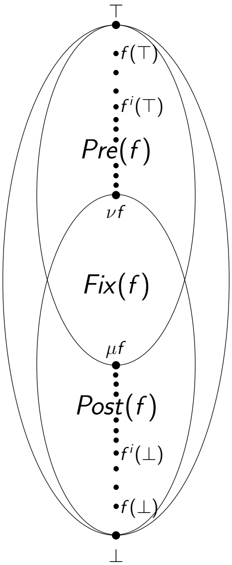
Solution techniques

- The Knaster-Tarski theorem guarantees the existence of least and greatest fixpoints for monotone functions
- We have the following proof rules for upper and lower bounds:

$$\frac{f(\ell) \sqsubseteq \ell}{\mu f \sqsubseteq \ell} \qquad \frac{\ell \sqsubseteq f(\ell)}{\ell \sqsubseteq \nu f}$$

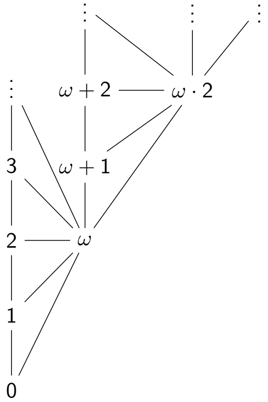
- Kleene iteration: whenever f is (co-)continuous
    - $\mu f = \bigsqcup_{i \in \mathbb{N}} f^i(\bot)$ (least fixpoint)
    - $\nu f = \bigsqcap_{i \in \mathbb{N}} f^i(\top)$ (greatest fixpoint)

Fixpoint Theory



If f is *not* (co-)continuous:

$\rightsquigarrow$ Kleene iteration over the ordinals (beyond ω)



Fixpoint Theory

The following proof rules (based on Kleene iteration) provide guarantees for the opposite bounds. By i we denote some ordinal.

$$\frac{\ell \sqsubseteq f^i(\bot)}{\ell \sqsubseteq \mu f} \qquad\qquad \frac{f^i(\top) \sqsubseteq \ell}{\nu f \sqsubseteq \ell}$$

This is related to ranking functions that are e.g. used in termination analysis.

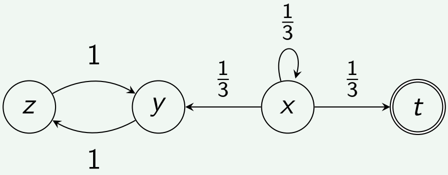
Problems: there is no straightforward witness that guarantees these bounds, (ordinals are involved)

Our aim: provide proof rules of the form

$$\frac{\ell \sqsubseteq f(\ell) + \text{extra conditions}}{\ell \sqsubseteq \mu f} \qquad\qquad \frac{f(\ell) \sqsubseteq \ell + \text{extra conditions}}{\nu f \sqsubseteq \ell}$$

Termination Probability

What is the probability of terminating from state x?



Termination Probability

Markov chain

$(X, T, (p_x)_{x \in X \setminus T})$ where

- X is the finite state space,
- $T \subseteq X$ are the terminal states and
- $p_x \colon X \to [0,1]$ is a probability distribution

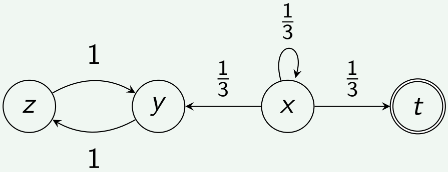
Termination probability as least fixpoint

Termination probability given by μf where $f \colon [0,1]^X \to [0,1]^X$ and for $a \colon X \to [0,1]$, $x \in X$:

$$f(a)(x) = \begin{cases} 1 & \text{if } x \in T \\ \sum_{y \in X} p_x(y) \cdot a(y) & \text{otherwise} \end{cases}$$

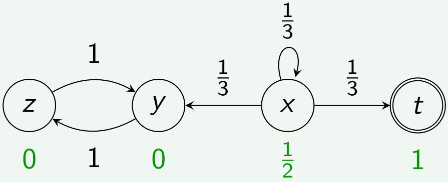
Termination Probability

What is the probability of terminating from state x?



Termination Probability

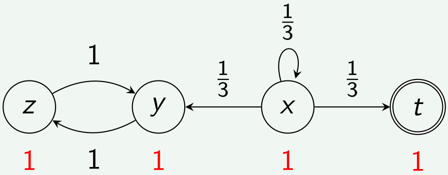
What is the probability of terminating from state x?



Least fixpoint, giving the termination probability for x

Termination Probability

What is the probability of terminating from state x?



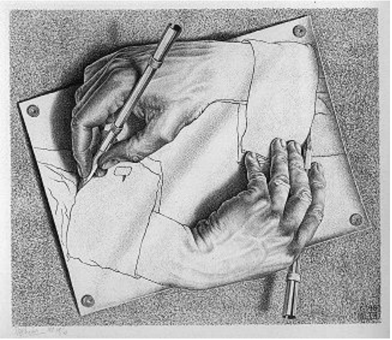
A different fixpoint, not providing a lower bound for the termation probability of x

Termination Probability

We can not trust a fixpoint or pre-fixpoint to give us a lower bound on the termination probability (given by a *least* fixpoint).

▷ Can we detect those fixpoints that are not least fixpoints? Where is the culprit?

In the example: y and z convince each other incorrectly (!) that they have termination probability 1 $\rightsquigarrow$ vicious cycle



Termination Probability

Idea: compute the set of states that still has some "wiggle room" or "slack". That is, those states that can say:

> *"If all my successors would reduce their value by δ, I could also reduce my value by δ."*

This can be computed as a greatest fixpoint on a finite set $\mathcal{P}(X)$ (instead of the infinite lattice that we considered before).

If the function is sufficiently well-behaved and this set ($=$ greatest fixpoint) is empty
$\Rightarrow$ we know that we have reached the least fixpoint (respectively a pre-fixpoint below the least fixpoint).

Abstractions for Determining the "Wiggle Room"

We use Galois connections (pairs of abstraction and concretization) in order to determine the "wiggle room" or "slack" of a fixpoint.

Requirements

The lattice is of the form $\mathbb{L} = \mathbb{M}^X$ (set of functions of the form $X \to \mathbb{M}$), where

- X finite
- $\mathbb{M}$ is a totally ordered lattice living in a group (inverses: we can add and subtract!)

We will now consider the dual problems: given $f\colon \mathbb{M}^X \to \mathbb{M}^X$ and $a\colon X \to \mathbb{M}$

- assume that $f(a) = a$. Is a the greatest fixpoint?
- assume that $f(a) \sqsubseteq a$. Is a above the greatest fixpoint?

Abstractions for Determining the “Wiggle Room”

$$\begin{tikzcd} \mathcal{P}(X) \arrow[r, bend left, "\alpha_{a,\theta}"] & \mathbb{M}^X \arrow[l, bend left, "\gamma_{a,\theta}"] \end{tikzcd}$$

$$\begin{array}{rcl} \alpha_{a,\theta}(Y) & = & a + \theta_Y \\ \gamma_{a,\theta}(b) & = & \{x \in X \mid a(x) + \theta \sqsubseteq b(x)\} \end{array}$$

where for $Y \subseteq X$, $\theta \in \mathbb{M}$, $\theta_Y \colon X \to \mathbb{M}$ with

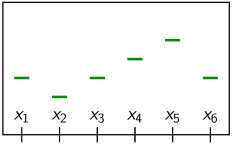
$$\theta_Y(x) = \begin{cases} \theta & \text{if } x \in Y \\ 0 & \text{otherwise} \end{cases}$$

[To be more precise:

- $\mathbb{M}^X$ should be replaced by $\{b \colon X \to \mathbb{M} \mid a \sqsubseteq b \sqsubseteq a + \theta\}$
- f restricts to this set whenever $f(a + \theta) \sqsubseteq f(a) + \theta$ (Condition 1)

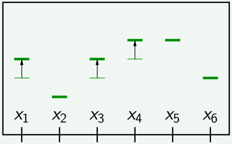
]

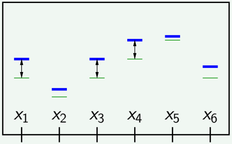
Abstractions for Determining the “Wiggle Room”

a = 

$\theta =$ 

(a is the “baseline”)

$\alpha_{a,\theta}$: $Y = \{x_1, x_3, x_4\} \quad \mapsto$ 

$\gamma_{a,\theta}$: b = 

$\mapsto \quad Y = \{x_1, x_3, x_4\}$

Abstractions for Determining the "Wiggle Room"

Galois connection

$\langle \alpha_{a,\theta}, \gamma_{a,\theta} \rangle$ satisfy the properties of a Galois connection:

- $\alpha_{a,\theta}, \gamma_{a,\theta}$ are monotone
- $id_{\mathcal{P}(X)} \subseteq \gamma_{a,\theta} \circ \alpha_{a,\theta}$
- $\alpha_{a,\theta} \circ \gamma_{a,\theta} \sqsubseteq id_{\mathbb{M}^X}$

Galois Connections and Fixpoints

$$f^{\#} = \gamma \circ f \circ \alpha \circlearrowright \mathbb{A} \underset{\gamma}{\overset{\alpha}{\rightleftarrows}} \mathbb{C} \circlearrowleft f$$

We have $\nu f^{\#} = \gamma(\nu f)$ whenever

- $\gamma \circ f \sqsubseteq f^{\#} \circ \gamma = \gamma \circ f \circ \alpha \circ \gamma$
  (equivalent to $\alpha \circ \gamma \circ f \sqsubseteq f \circ \alpha \circ \gamma$)

(see also [Cousot/Cousot], [Bonchi/Ganty/Giacobazzi/Pavlovic])

Galois Connections and Fixpoints

In our setting:

$$
\begin{tikzcd}
f^\#_{a,\theta} = \gamma_{a,\theta} \circ f \circ \alpha_{a,\theta} \arrow[r, bend left] & \mathcal{P}(X) \arrow[rr, bend left, "\alpha_{a,\theta}"] & & \mathbb{M}^X \arrow[ll, bend left, "\gamma_{a,\theta}"] \arrow[loop right, "f"]
\end{tikzcd}
$$

Whenever $f(a) = a$, $a \neq \nu f$ for $a\colon X \to \mathbb{M}$
$\Rightarrow \exists \theta \sqsupset 0 \; \exists x \in X\colon a(x) + \theta \sqsubseteq \nu f(x)$
$\Rightarrow \emptyset \neq \gamma_{a,\theta}(\nu f) = \nu f^\#_{a,\theta}$

Contraposition: If $\nu f^\#_{a,\theta} = \emptyset$, then $a = \nu f$.

Galois Connections and Fixpoints

Unfortunately, we do not know this θ. But things work fine if we require that for each fixpoint a there exists θ_a such that for each δ:

- $\alpha_{a,\theta_a} \circ \gamma_{a,\delta} \circ f \sqsubseteq f \circ \alpha_{a,\theta_a} \circ \gamma_{a,\delta}$

Since we want a proof rule for pre-fixpoints, we need the following requirement (Condition 2):

- $\alpha_{f(a),\theta_a} \circ \gamma_{f(a),\delta} \circ f \sqsubseteq f \circ \alpha_{a,\theta_a} \circ \gamma_{a,\delta}$

$$\begin{tikzcd}
f^{\#}_{a,\theta_a} \arrow[r, phantom, "\circlearrowright"] & \mathcal{P}(X) \arrow[rr, bend left, "\alpha_{a,\delta}"] & & \mathbb{M}^X \arrow[ll, bend left, "\gamma_{a,\delta}"] \arrow[r, phantom, "\circlearrowleft"] & f
\end{tikzcd}$$

Proof Rule

Proof rule

$$\frac{f(a) \sqsubseteq a \qquad \nu f^{\#}_{a,\theta_a} = \emptyset}{\nu f \sqsubseteq a}$$

This proof rule is sound and complete in the following sense:

Let $b\colon X \to \mathbb{M}$ with $\nu f \sqsubseteq b$. Then there exists $a\colon X \to \mathbb{M}$ such that $a \sqsubseteq b$, $f(a) \sqsubseteq a$ and $\nu f^{\#}_{a} = \emptyset$.

Proof Rule

The function $f^{\#} = f^{\#}_{a,\theta_a}$ can usually be defined directly on $\mathcal{P}(X)$ and can hence be computed efficiently. In the case of termination probability:

$$f^{\#}(Y) = \{x \in Y \mid x \notin T, Q(x) \subseteq Y \cap P_a\}$$

where

- $P_a = \{x \in X \mid a(x) > 0\}$
- $\theta_a = \min\{a(x) \mid x \in X, x \in P_a\}$
- $Q(x) = \{y \in X \mid p_x(y) > 0\}$ for $x \in X \backslash T$.

  $f^{\#}(Y)$ contains those states of Y that are non-terminating and whose successors are in Y and have values larger than 0 (i.e. they have the potential for reduction or "slack").

Applications

Despite the restrictions, this approach provides witnesses for:

- lower bounds of termination probabilities
- lower bounds for maximal paths
- non-bisimilarity of states
- lower bounds for behavioural distances

It can be used to iterate to νf from below (and to iterate to μf from above):

- Perform Kleene iteration starting from $\bot$ until a fixpoint a is reached. Test whether it is the greatest fixpoint.
- If it is not, continue with $a' = a + (\theta_a)_{\nu f^{\#}_{a,\theta_a}}$.

This method was developed for the special case of behavioural metrics by [Fu] and [Bacci, Bacci,Larsen, Mardare, Tang, van Breugel]. It gave us the inspiration to look for a generalization.

Future Work

- Is it possible to lift some of the restrictions? In particular: is it possible to handle partial (instead of total) orders?
- Does it make sense to generalize the Galois connection?
- Compositionality: if f, g satisfy the requirements, does the same hold for $f \circ g$?