IC3

following [The lattice-theoretic essence of property directed reachability analysis, Kori, Urabe, Katsumata, Suenaga, Hasuo, CAV'22]

Reminder:

Let $(L, \leq)$ be a complete lattice
and $f : L \to L$ continuous.

1) $\mathrm{lfp}.f \leq \alpha$ iff $\exists x \in L.\ f x \leq x \leq \alpha$. (KT)

 x: KT witness

2) $\mathrm{lfp}.f \not\leq \alpha$ iff $\exists x \in L.\ \exists n \in \mathbb{N}.\ x \leq f^n \bot\ \wedge\ x \not\leq \alpha$. (Kleene)

 x: Kleene witness

The problem of interest is to check whether a given value in a lattice over-approximates a least fixed point.

LFP-OA:

Given: $(L, \leq)$ a complete lattice,
$f : L \to L$ continuous,
$\alpha \in L$.

Question: $\mathrm{lfp}.f \leq \alpha$?

Two algorithms:

Positive LT-PDR: Build KT witnesses bottom-up, to answer LFP-OA positively.

Negative LT-PDR: Build Kleene witnesses to answer LFP-OA negatively.

Key: Intermediate results on one side give informed guesses on the other.

Positive LT-PDR:

Goal:
- Introduce KT^{ω} witnesses – KT witnesses constructed in a sequential manner.
- Positive LT-PDR finds KT^{ω} witnesses by growing finitary approximations.

Definition:

Let $(L, \leq)$ be a complete lattice.

One can understand $x \in L$ as a predicate on states, and then $x \leq y$ means x is stronger than y.

- The complete lattice $[n, L]$ consists of increasing chains of length n:

  $x_0 \leq \ldots \leq x_{n-1}$, ordered elementwise.

  We let $[\omega, L]$ denote the infinite such chains.

- We lift $f: L \to L$ to

  $f^{\#} : [\omega, L] \to [\omega, L]$ and

  $f^{\#}_n : [n, L] \to [n, L]$

  with

  $$f^{\#}(x_0 \leq x_1 \leq \ldots) = (\bot \leq f x_0 \leq f x_1 \leq \ldots)$$

  $$f^{\#}_n(x_0 \leq \ldots \leq x_{n-1}) = (\bot \leq f x_0 \leq \ldots \leq f x_{n-2}).$$

Definition:

Let $(L, \le), f, \alpha$ be an instance of LFP-OR.

Define $\Delta\alpha = \alpha \le \alpha \le \dots$

A KT^ω witness is $X \in [\omega, L]$ with $f^\# X \le X \le \Delta\alpha$.

Theorem: Let L, f, α be as before.

There is a KT witness iff there is a KT^ω witness.

Proof:

"$\Rightarrow$" Let x be a KT witness, meaning $fx \le x \le \alpha$.

Then $X = x \le x \le \dots$ is a KT^ω witness,

meaning

$$\begin{aligned} fX &= (\bot \le fx \le fx \le \dots) \\ &\le \underbrace{(x \le x \le x \le \dots)}_{X} \\ &\le (\alpha \le \alpha \le \dots) = \Delta\alpha. \end{aligned}$$

"$\Leftarrow$" Let $X = (x_0 \le x_1 \le \dots)$ be a KT^ω witness,

meaning $f^\# X \le X \le \Delta\alpha$.

Then $\bigvee_{n \in \mathbb{N}} x_n$ is a KT witness.

$\boxed{f(x_i) \le x_{i+1} \le \alpha \text{ f.a. } i}$

Indeed,

$$f\Big(\bigvee_{n \in \mathbb{N}} x_n\Big) \overset{\text{(continuity)}}{=} \bigvee_{n \in \mathbb{N}} f(x_n) \le \bigvee_{n \in \mathbb{N}} x_n \le \alpha$$

$\square$

<u>Motivation for KT$^\omega$ witnesses</u>:

- The chain $\bot \leq f\bot \leq f^2\bot \leq \dots$ is a KT$^\omega$ witness for $\mathrm{lfp}.f \leq \alpha$.
- But there are more: use heuristics to accelerate the search.

<u>Goal</u>: Define a finite object that characterizes the existence of a KT$^\omega$ witness.

<u>Definition</u>: Let L, f, α be as before.

- A <u>KT sequence</u> for this LFP-OA instance is a finite chain

  $X = (x_0 \leq \dots \leq x_{n-1})$ with $n \geq 2$

  so that

  1.) $x_{n-2} \leq \alpha$

  2.) X is a prefix point of $f^{\#}_n$, $f^{\#}_n X \leq X$,

  meaning

  $$f x_i \leq x_{i+1} \quad \text{f.a. } 0 \leq i \leq n-2.$$

  // f is post in our slides.

- The KT sequence is <u>conclusive</u>, if $x_{j+1} \leq x_j$ for some j.

<u>Remark</u>:

- The upper bound α is imposed on all x_i <u>except</u> x_{n-1}.

  This freedom in x_{n-1} allows us to apply heuristics, in particular incorporate information from negative LT-PDR.

We use KT sequences to <u>approximate</u> KT^ω witnesses.

<u>Definition</u>:

We define the partial order $\preccurlyeq$ between KT sequences:

$$(x_0 \leq \dots \leq x_{n-1}) \preccurlyeq (y_0 \leq \dots \leq y_{m-1}),$$

if

$n \leq m$ and $x_j \geq y_j$ f.a. $0 \leq j \leq n-1$

// The sequence gets longer // The predicates become stronger.

<u>Theorem</u>: Let L, f, α be an LFP-OR instance.

- The set of KT sequences enriched with the set of KT^ω witnesses is an <u>ω-cpo</u> with $\preccurlyeq$ as the ordering.
  ↳ (the join of all chains $x_0 \preccurlyeq x_1 \preccurlyeq \dots$ belongs to the set)
- In this ω-cpo, each KT^ω witness X is the join of an infinite chain of KT sequences, namely
  $$X = \bigvee_{n \geq 2} X|_n \quad \text{with } X|_n \in [n, L] \text{ the prefix of length } n.$$

<u>Proposition</u>: Let L, f, α be as before.

There is a KT^ω witness iff there is a conclusive KT sequence.

<u>Proof</u>:

"$\Rightarrow$" If there is a KT^ω witness, there is a KT witness by the above theorem.

By the initial reminder, the KT witness shows $\mathrm{lfp}.f \leq \alpha$.

Then $(\mathrm{lfp}.f \leq \mathrm{lfp}.f)$ is a conclusive KT sequence.

"$\Leftarrow$" If X is a conclusive KT sequence with $x_{j+1} \leq x_j$, then

$$X' = (x_0 \leq x_1 \leq \dots \leq x_j = x_j = \dots) \text{ is a } KT^\omega \text{ witness.}$$

To see

$f^\#(X') \leq X'$, note that $f(x_i) \leq x_{i+1}$ by the definition of KT sequences.

For $X' \leq \Delta\alpha$, use $x_j \leq \alpha$. $\square$

<u>Algorithm</u> (<u>positive LT-PDR</u>):

<u>Input</u>: L, f, α.

<u>Output</u>: True + conclusive KT sequence.

<u>Data</u>: KT sequence $X = (x_0 \leq x_1 \leq \dots \leq x_{n-1})$.

<u>Initial</u>: $\boxed{X = (\bot \leq f\bot)}$

<u>while</u> true <u>do</u>

non-deterministic choice

<u>Valid</u>: If $x_{j+1} \leq x_j$ for some $j \leq n-1$ <u>return</u> true + conclusive KT sequence X.

+ <u>Unfold</u>: If $x_{n-1} \leq \alpha$, let $X = (x_0 \leq \dots \leq x_{n-1} \leq \top)$.

+ <u>Induction</u>: If $k \geq 2$ and $x \in L$ satisfying $x_k \not\leq x$ and $f(x_k \wedge x) \leq x$

$$\text{let } X = X[x_j \mapsto x_j \wedge x]_{2 \leq j \leq k}.$$

<u>od</u>

Rule <u>Induction</u> strengthens X by replacing the j-th element with $x_j \wedge x$.

Note that

$$f(x_k \wedge x) \leq x_{k+1} \wedge x.$$

This holds by

$$f(x_k \wedge x) \leq x \quad // \text{ the check we have}$$

and $f(x_k \wedge x) \leq f(x_k) \leq x_{k+1}$.

(continuity implies monotonicity) — X is a KT sequence

Hence, $f(x_k \wedge x)$ is a lower bound of x and x_{k+1}.

So the greatest lower bound $x \wedge x_{k+1}$ will be larger.

<u>Theorem</u>:

- Positive LT-PDR is <u>sound</u>:

  if it outputs true, then $\mu f \leq \alpha$ holds.

- Positive LT-PDR is <u>weakly terminating</u>:

  suitable choices of x in <u>Induction</u> make it terminate.
  (guess μf)

We show proper termination under reasonable assumptions.

<u>Lemma</u>:

- If $\mu f \leq \alpha$, for any KT sequence X,
  at least one of the three rules is enabled.
- Let X' be obtained from X using <u>Unfold</u> or <u>Induction</u>.
  Then $X \preceq X'$ and $X \neq X'$.

<u>Theorem</u>: Assume $(L, \leq)$ is well-founded and $\mu f \leq \alpha$.

- Any non-terminating run of positive LT-PDR
  converges to a KT^ω witness (gives a KT^ω witness in ω-many steps).
- If there is no strictly increasing chain below α, then the algorithm terminates.

Negative LT-PDR:

Idea: · Use Kleene sequences as a lattice-theoretic counterpart of proof obligations in IC3.

· Sufficient conditions to conclude reachability of a bad state.

Definition:

· A Kleene sequence for the LFP-OA instance L, f, α is a finite sequence

$$C = (c_0, \dots, c_{n-1}) \qquad \text{(empty if } n=0\text{)}$$

with

1. $c_j \leq f c_{j-1}$ f. a. $1 \leq j \leq n-1$
2. $c_{n-1} \not\leq \alpha$.

· The sequence is conclusive, if $c_0 = \bot$.

// We under-approximate $\bot \leq f\bot \leq \dots$ and still do not land below α.

Proposition:

There is a Kleene witness iff there is a conclusive Kleene sequence.

Proof:

"⇒" If there is a Kleene witness, we have $x \leq f^n\bot$ and $x \not\leq \alpha$.

Then $(\bot, f\bot, \dots, f^n\bot)$ is a conclusive Kleene sequence ($f^n\bot \leq \alpha$ would imply $x \leq \alpha$ ↯).

"⇐" Let C be a conclusive Kleene sequence.

We claim that c_{n-1} is a Kleene witness.

Indeed, $c_1 \overset{(1)}{\leq} f c_0 \overset{\text{(conclusive)}}{=} f \bot$.

Moreover, $c_2 \overset{(1)}{\leq} f c_1 \overset{\text{(monotonicity)}}{\leq} f^2 \bot$.

Hence, $c_{n-1} \leq f^{n-1} \bot$.

Moreover, $c_{n-1} \not\leq \alpha$ by 2. $\square$

Algorithm (negative LT-PDR):

Input: L, f, α.

Output: false + conclusive Kleene sequence.

Data: Kleene sequence $C = (c_0, \dots, c_{n-1})$

Initial: $C = \varepsilon$.

while true do

Candidate: Choose $x \in L$ with $x \not\leq \alpha$.

Let $C = x$.

+ Model: If $c_0 = \bot$, return false + conclusive Kleene seq. C

+ Decide: If there is x so that $c_0 \leq f x$,

let $C = (x, c_0, \dots, c_{n-1})$.

od

Theorem:

- Negative LT-PDR is sound:

  if it outputs false, then $\mathrm{lfp}\, f \not\leq \alpha$.

- Assume $\mathrm{lfp}\, f \not\leq \alpha$ holds.

  Then negative LT-PDR is weakly terminating:

  there are choices of x for Candidate and Decide

  that make the algorithm terminate.

LT-PDR:

Problem: · Positive and negative LT-PDR may be inefficient:

↳ How to choose $x \in L$ in Induction?

↳ How to choose $x \in L$ in Candidate and Decide?

· Negative LT-PDR easily diverges.

we only need to pick $x \nleq f(p.)$

and will never get a conclusive Kleene sequence out of it.

↳ We want to detect useless Kleene sequences early on.

Key to efficiency of IC3:

KT sequences can identify Kleene sequences as useless.

Proposition:

Let $C = (c_i, \dots, c_{n-1})$ be a Kleene sequence, $(n \geq 2,\ 0 < i \leq n-1)$

Let $X = (x_0 \leq \dots \leq x_{n-1})$ be a KT sequence.

1.) $c_i \nleq x_i \Rightarrow C$ cannot be extended to a conclusive Kleene sequence $C = (c_0, \dots, c_{n-1})$.

2.) $c_i \nleq f x_{i-1} \Rightarrow$ —— " ——

3.) There is no conclusive Kleene sequence of length $n-1$.

The result needs two lemmas.

Lemma 1:

Every KT sequence $(x_0 \leq \ldots \leq x_{n-1})$
over-approximates the sequence $\bot \leq f\bot \leq \ldots \leq f^{n-1}\bot$
in that $f^i\bot \leq x_i$ f.a. $0 \leq i \leq n-1$.

Lemma 2:

Let $C = (c_i, \ldots, c_{n-1})$ be a Kleene sequence, $0 < i \leq n-1$.

Let $X = (x_0 \leq \ldots \leq x_{n-1})$ be a KT sequence.

Then (1) $\Longleftrightarrow$ (2) and (2) $\Rightarrow$ (3):

(1) The Kleene sequence can be extended to a conclusive one.

(2) $c_i \leq f^i\bot$

(3) $c_i \leq f^j x_{i-j}$ f.a. $0 \leq j \leq i$.

Algorithm (LT-PDR):

Input: L, f, α.

Output: true + conclusive KT sequence
or false + conclusive Kleene sequence.

Data: (X, C) with · $X = (x_0 \leq \ldots \leq x_{n-1})$ a KT sequence
· $C = (c_i, \ldots, c_{n-1})$ a Kleene sequence, empty if $n = i$.

Initial: $X = (\bot, f\bot)$, $C = \varepsilon$.

while true do

Essentially positive LT-PDR

Valid: If $x_{j+1} \leq x_j$ for some j, return true + X

+ Unfold: If $x_{n-1} \leq \alpha$, let $X = (x_0 \leq \ldots \leq x_{n-1} \leq \top)$
$C = \varepsilon$.

+ Induction: If $x_k \nleq x$ and $f(x_k \wedge x) \leq x$ for some $k \geq 2$ and some $x \in L$,

let $X = X[x_j \mapsto x_j \wedge x]_{2 \leq j \leq k}$.

Eventually negative LT-PDR

+ Candidate: If $C = \varepsilon$ and $x_{n-1} \nleq \alpha$,

choose $x \in L$ with $x \leq x_{n-1}$ and $x \nleq \alpha$,

let $C = x$.

+ Model: If c_1 is defined, return false + $(\bot, c_1, \ldots, c_{n-1})$

+ Decide: If $c_i \leq f x_{i-1}$

choose $x \in L$ with $x \leq x_{i-1}$ and $c_i \leq f x$,

let $C = x, c_i, \ldots, c_{n-1}$.

Conflict: If $c_i \nleq f x_{i-1}$

Choose $x \in L$ satisfying $c_i \nleq x$ and $f(x_{i-1} \wedge x) \leq x$.

Let $X = [x_j \mapsto x_j \wedge x]_{2 \leq j \leq i}$

$C = c_{i+1}, \ldots, c_{n-1}$.

Comments:

- Unfold: We reset C due to Proposition. (3).
- Candidate + Decide: $x \leq x_{n-1}$ resp. $x \leq x_{i-1}$, other choices do not work by Proposition. (1).
- Model: If c_1 is defined, $c_1 \leq x_1 = f\bot$ holds by (Candidate or Decide) and Initial
- Conflict: This is a new rule.

$c_i \nleq f x_{i-1} \Rightarrow C$ cannot be extended to a conclusive Kleene seq. by Prop. (2).

↳ Eliminate c_i from C

↳ Strengthen X so that

we cannot choose c_i again: $c_i \not\leq x_i \wedge x$.

How? $c_i \not\leq x$ and $f(x_{i-1} \wedge x) \leq x$.

Very similar to Induction.

Remark:

Canonical choices of x:

Candidate: $x = x_{n-1}$

Decide: $x = x_{i-1}$

Conflict: $x = f\, x_{i-1}$

There are better choices.

When the lattice is $L = \mathcal{P}(S)$,

Conflict: $x = S \setminus (c_i \setminus f\, x_{i-1})$ // Everything except c_i (modulo $f\, x_{i-1}$).

Lemma: Each rule of LT-PDR,

when applied to a pair of KT and Kleene sequences,

yields a pair of KT and Kleene sequences.

Theorem: LT-PDR is sound: if it outputs true, then $\mu p. f \leq \alpha$,

if it outputs false, then $\mu p. f \not\leq \alpha$.

Proposition: LT-PDR terminates regardless of the order of rule applications,

if the following holds:

(1) Valid and Model are applied immediately when applicable.

(2) $(L, \leq)$ is well-founded

(3) Either of the following holds:

a) $\llbracket p \rrbracket \leq \alpha$ and
$(L, \leq)$ has no infinite strictly increasing chains below α

b) $\llbracket p \rrbracket \nleq \alpha$.

<u>Remark</u>:

Soundness and termination still hold without rule <u>Induction</u>.
It is there for efficiency.