Computational Modeling and Analysis for Complex Systems

CMACS PI meeting, Arlington, VA, May 16, 2013

Work in Progress Towards Liveness Verification for Infinite Systems by Abstract Interpretation

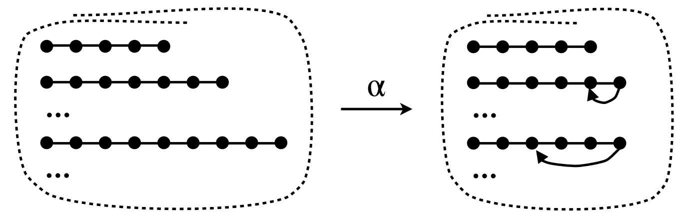
Patrick Cousot

cims.nyu.edu/~pcousot/

Joint work with Radhia Cousot www.di.ens.fr/~rcousot/

Limitations of "abstract and model-check" for liveness

- For unbounded transition systems, finite abstractions are
  - *Incomplete* for termination;
  - *Unsound* for non-termination;



  - And so the limitation is similar for *liveness*, no counter-example to infinite program execution

Unless ...

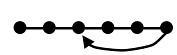
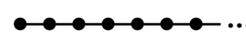
- One is only interested in liveness in the finite abstract (or the concrete is bounded) → decidable
- Or, model-checking is used for checking the termination proof inductive argument (e.g. given variant functions) → decidable

  Ittai Balaban, Amir Pnueli, Lenore D. Zuck: Ranking Abstraction as Companion to Predicate Abstraction. FORTE 2005: 1-12

- Of *very* limited interest:
  - Program executions are unbounded → undecidable
  - The hardest problem for liveness proofs is to infer the inductive argument, then the proof is "easy"

Origin of the limitations

- Model-checking is impossible because counter-examples are unbounded infinite

 versus 

- We need *automatic verification* not *checking*
- This requires
  - Infinitary abstractions
  - of well-founded relations / well-orders
  - and effectively computable approximations

  i.e. *Abstract Interpretation*

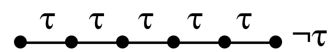
Analysis and verification with well-founded relations and well-orders

Maximal trace operational semantics

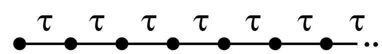
- A transition system: $\langle \Sigma, \tau \rangle$

  states ↗ ↖ transition relation

- Maximal trace operational semantics: set of
  - Finite traces:



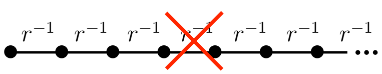
  - Infinite traces:



Well-founded relations / Well-orders

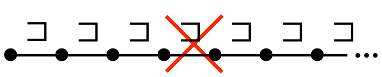
- Well-founded relation:

A relation $r \in \wp(\mathfrak{X} \times \mathfrak{X})$ on a set $\mathfrak{X}$ is well-founded *if and only if*[3] *there is no infinite descending chain $x_0, x_1, \ldots, x_n, \ldots$ of elements x_i, $i \in \mathbb{N}$ of $\mathfrak{X}$ such that $\forall n \in \mathbb{N} : \langle x_{n+1},\ x_n \rangle \in r$ (or equivalently $\langle x_n,\ x_{n+1} \rangle \in r^{-1}$).*



- Well-order:

A well-order *(or* well-order *or* well-ordering*) is a poset $\langle \mathfrak{X},\ \sqsubseteq \rangle$, which is well-founded and total.*



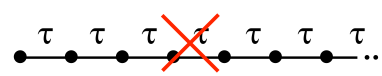
[3] Assuming the axiom of choice in set theory.

Relevance to Termination Proof

- Program termination is

$\langle \Sigma, \tau^{-1} \rangle$ *is well-founded*

i.e. no infinite execution ($(\tau^{-1})^{-1} = \tau$)



Relevance to LTL verification

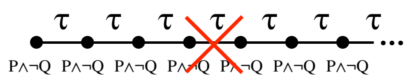
- $P \bigcup Q$ for transition system $\langle \Sigma, \tau \rangle$

  if and only if

$$\langle \{x \in \Sigma \mid P(x) \vee Q(x)\},\ \{\langle y,x \rangle \in \tau^{-1} \mid \neg Q(x) \wedge \neg Q(y)\} \rangle$$

is well-founded

invariant *variant*



General idea of the abstraction

- Combine two abstractions:
  - Abstraction of a relation to its well-founded part (to get a *necessary* condition for wellfoundedness)
  - Asbtraction of this well-founded part to a well-order (to get a *sufficient* condition for wellfoundedness)

$$\langle \wp(\mathfrak{X} \times \mathfrak{X}),\ \subseteq \rangle \underset{\alpha^{\mathfrak{wf}}}{\overset{\gamma^{\mathfrak{wf}}}{\leftrightarrows}} \langle \mathfrak{W}(\mathfrak{X}),\ \sqsubseteq \rangle \underset{\alpha^{\mathsf{O}}}{\overset{\gamma^{\mathsf{O}}}{\leftrightarrows}} \langle \mathfrak{X} \not\mapsto \mathbb{O},\ \precapprox \rangle$$

relation *well-founded part* *well-order on founded part*

Abstraction of relations to their well-founded part

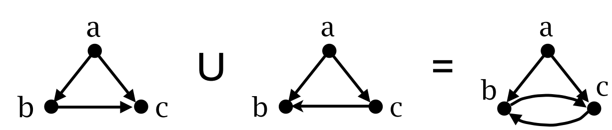
Relations

- We encode relations by a domain and a set of connections between elements of the domains (some may be unconnected)

$$\mathfrak{R}(\mathfrak{X}) \triangleq \{\langle D,\ r \rangle \mid D \in \wp(\mathfrak{X}) \wedge r \in \wp(D \times D)\}$$
$$\mathfrak{W}(\mathfrak{X}) \triangleq \{\langle D,\ r \rangle \in \mathfrak{R}(\mathfrak{X}) \mid r \in \mathfrak{Wf}(D)\}$$

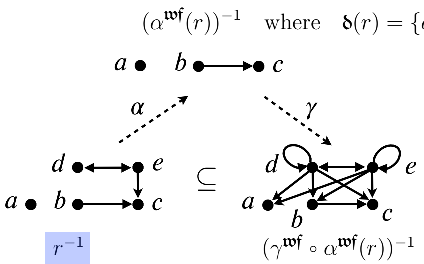
$\mathfrak{W}(\mathfrak{X})$ is the set of well-founded relations on subsets of the set $\mathfrak{X}$.

- Well-founded relations do not form a lattice for $\subseteq$:



Well-founded part of a relation

- Example of well-founded part of a relation:

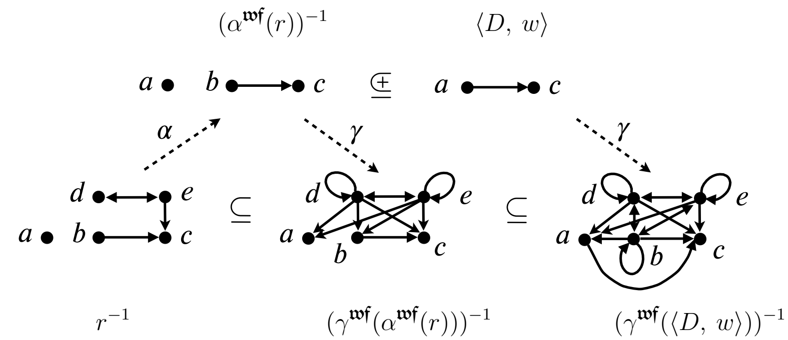


- Formally

$$
\begin{aligned}
\alpha^{\mathfrak{wf}}(r) &\triangleq \langle \mathfrak{d}(r),\ r \cap (\mathfrak{X} \times \mathfrak{d}(r))\rangle \qquad \text{where} \\
\mathfrak{d}(r) &\triangleq \{x \in \mathfrak{X} \mid \nexists \langle x_i \in \mathfrak{X},\ i \in \mathbb{N}\rangle : x = x_0 \wedge \forall i \in \mathbb{N} : x_i\ r^{-1}\ x_{i+1}\} \\
\gamma^{\mathfrak{wf}}(\langle D,\ w\rangle) &\triangleq w \cup (\mathfrak{X} \times \neg D)
\end{aligned}
$$

Partial order on relations

- Formalize the intuition of over-approximation of well-founded relations in $\mathfrak{w}(\mathfrak{X})$



- Formal definition:

$$
\begin{aligned}
\langle D,\ w\rangle \sqsubseteq \langle D',\ w'\rangle &\triangleq \gamma^{\mathfrak{wf}}(\langle D,\ w\rangle) \subseteq \gamma^{\mathfrak{wf}}(\langle D',\ w'\rangle) \\
&= D' \subseteq D \wedge w \cap (D' \times D') \subseteq w' \wedge w \cap (\neg D' \times D') = \emptyset
\end{aligned}
$$

Best abstraction of the well-founded part

- Any relation can be abstracted to its most precise well-founded part

$$\langle \wp(\mathfrak{X} \times \mathfrak{X}),\ \subseteq\rangle \underset{\alpha^{\mathfrak{wf}}}{\overset{\gamma^{\mathfrak{wf}}}{\leftrightarrows}} \langle \mathfrak{W}(\mathfrak{X}),\ \sqsubseteq\rangle$$

- The best abstraction provides a necessary and sufficient condition for well-foundedness
- An $\sqsubseteq$-over-approximation of this best abstraction yields a *sufficient* condition for well-foundedness

$$\text{if } \alpha^{\mathfrak{wf}}(r) \sqsubseteq \langle D,\ w\rangle \text{ then } r \text{ is well-founded on } D$$

Fixpoint characterization of the well-founded part of a relation

- $\alpha^{\mathfrak{wf}}(r) = \mathbf{lfp}^{\dot{\subseteq}}\ \boldsymbol{\lambda}\langle D,\ w\rangle \cdot \langle \min_r(\mathfrak{X}) \cup \widetilde{\mathbf{pre}}[\![r]\!]D,\ w \cup \{\langle x,\ y\rangle \in r \mid x \in \widetilde{\mathbf{pre}}[\![r]\!]D\}\rangle$

  where

  $\widetilde{\mathbf{pre}}[\![r]\!]X = \{x \in \mathfrak{X} \mid \forall y \in \mathfrak{X} : r(x, y) \Rightarrow y \in X\}$

  and $\langle D,\ w\rangle \dot{\subseteq} \langle D',\ w'\rangle$ *if and only if* $D \subseteq D' \wedge w \subseteq w'$.

- By abstraction $\alpha(\langle D,\ w\rangle) = D$, we get a fixpoint characterization of the wellfoundedness domain.

$$\mathfrak{d}(r) = \mathbf{lfp}^{\subseteq}\ \boldsymbol{\lambda} X \cdot \min_r(\mathfrak{X}) \cup \widetilde{\mathbf{pre}}[\![r]\!]X$$

- We have recent results on under-approximating such fixpoint equations by *Abstract Interpretation* using abstraction and convergence acceleration by widening/narrowing

Recent results

- We have studied in

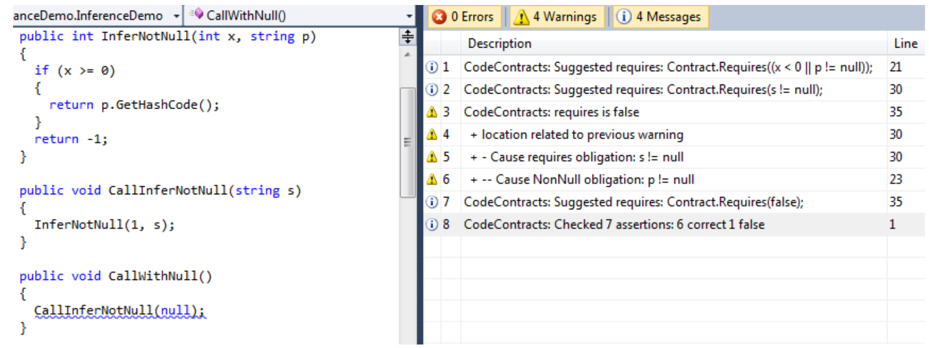
  Patrick Cousot, Radhia Cousot, Manuel Fähndrich, Francesco Logozzo: Automatic Inference of Necessary Preconditions. VMCAI 2013: 128-148

  Patrick Cousot, Radhia Cousot, Francesco Logozzo: Precondition Inference from Intermittent Assertions and Application to Contracts on Collections. VMCAI 2011: 150-168

  the static inference of such under-approximations

- The same infinitary *under-approximation* techniques do work for the inference of sufficient conditions for well-foundedness

Example



A screenshot of the error reporting with the precondition inference.

- Implemented in Visual Studio contract checker

Patrick Cousot, Radhia Cousot, Manuel Fähndrich, Francesco Logozzo: Automatic Inference of Necessary Preconditions. VMCAI 2013: 128-148

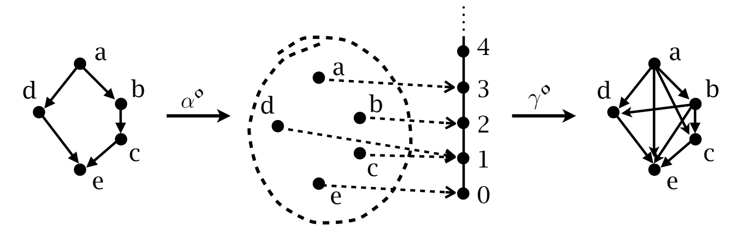
Abstraction of a relation's well-founded part to a well-order

Why well-orders?

- It is always possible to prove that a relation is well-founded by abstraction to a well order ($\langle \mathbb{N}, < \rangle$, $\langle \mathbb{O}, < \rangle$, etc).
- Well-orders are easy to represent in a computer (while arbitrary well-founded relations may not be)

Well-order abstraction of a well-founded relation

- Abstraction to a ranking function:



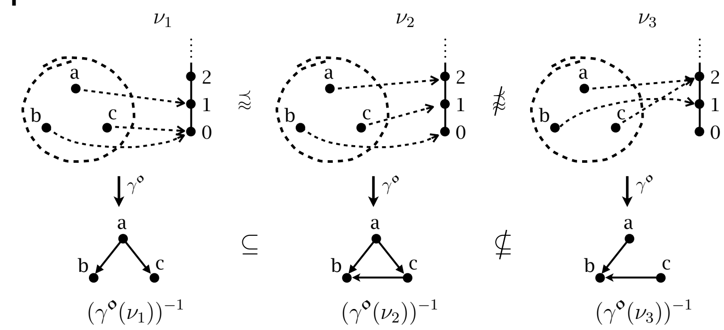
$\langle D,\ w^{-1}\rangle \in \mathfrak{w}(\mathfrak{X})$ $\qquad \nu_1 = \alpha^{\circ}(w)$ $\qquad \gamma^{\circ}(\nu_1) \supseteq w$

- Formally

$$\begin{array}{rcl}
\alpha^{\circ} & \in & \mathfrak{wf}(D) \mapsto (D \mapsto \mathbb{O}) \\
\alpha^{\circ}(w) & \triangleq & \boldsymbol{\lambda} y \in D \cdot \bigcup\{\alpha^{\circ}(w)x + 1 \mid \langle x,\ y\rangle \in w\} \\
\gamma^{\circ} & \in & (D \mapsto \mathbb{O}) \mapsto \mathfrak{wf}(D) \\
\gamma^{\circ}(\nu) & \triangleq & \{\langle x,\ y\rangle \in D \times D \mid \nu(x) < \nu(y)\}
\end{array}$$

Partial order on well-orders

- The length of maximal decreasing chains is over-approximated



- Formally

$$f \precsim g \ \triangleq\ \gamma^{\circ}(f) \subseteq \gamma^{\circ}(g)$$

Best abstraction

- Any well-founded relation can be abstracted to a most precise well-order

$$\langle \mathfrak{wf}(D),\ \subseteq\rangle \underset{\alpha^{\circ}}{\overset{\gamma^{\circ}}{\leftrightarrows}} \langle D \mapsto \mathbb{O},\ \precsim\rangle$$

- An over-approximation of this best abstraction yields over estimates of the (transfinite) lengths of maximal decreasing chains
- The generalized Turing-Floyd method is sound for any such well-order and complete for the best one.

Generalized Turing/Floyd Proof method

- $\langle \Sigma,\ \tau^{-1}\rangle$ *is well-founded* if and only if there exists a *ranking function*

$$\nu \in \Sigma \nrightarrow \mathbb{O}$$

($\nrightarrow$ is for *partial* functions, the class $\mathbb{O}$ of ordinals is a canonical representative of all well-orders) such that

$$\forall\, x \in \mathbf{dom}(\nu) \colon \forall\, y \in \Sigma \colon$$
$$\langle x,\ y\rangle \in \tau \Longrightarrow \nu(y) < \nu(x) \wedge y \in \mathbf{dom}(\nu)$$

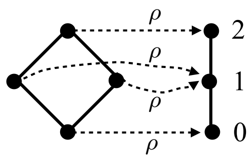
- $\mathbf{dom}(\nu)$ determines the *domain of well-foundedness* of τ^{-1} on Σ

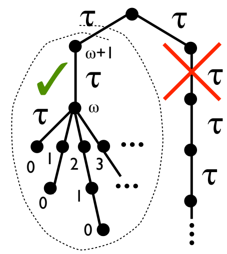
Fixpoint characterization of the ranking function

- The best/most precise ranking function is

$$\mathsf{Lfp}^{\subseteq}\ \boldsymbol{\lambda} X\cdot\{\langle x, 0\rangle \mid x \in \Sigma \wedge \forall\, y \in \Sigma: \langle x, y\rangle \notin \tau\} \bigcup \{\langle x, \bigcup\{\ \delta+1 \mid \exists\,\langle y, \delta\rangle \in X: \langle x, y\rangle \in \tau\}\rangle \ \mid x \in \Sigma\ \wedge \exists\,\langle y, \delta\rangle \in X: \langle x, y\rangle \in \tau \wedge \forall\, y \in \Sigma: \langle x, y\rangle \in \tau \Longrightarrow \exists\,\delta \in : \langle y, \delta\rangle \in X\}$$

- Examples:





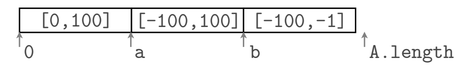
Recent results

- We have recent results on approximating such fixpoint equations by *Abstract Interpretation* using abstraction and convergence acceleraion by widening/narrowing

Patrick Cousot, Radhia Cousot: An abstract interpretation framework for termination. POPL 2012: 245-258

- Combined with segmentation

Patrick Cousot, Radhia Cousot, Francesco Logozzo: A parametric segmentation functor for fully automatic and scalable array content analysis. POPL 2011: 105-118



these techniques have been successfully implemented for termination proofs

Catarina Urban, The Abstract Domain of Segmented Ranking Functions, to appear in SAS 2013.

- The same techniques do work for the inference of ranking functions in any other contexts.

Examples

- Segmented ranking function abstract domain:

while $^1(x \geq 0)$ do

$^2x := -2x + 10$

od^3 $f(x) = 0$

$f \in \mathbb{Z} \mapsto \mathbb{N}$

$$f(x) = \begin{cases} 1 & x < 0 \\ 5 & 0 \leq x \leq 2 \\ 9 & x = 3 \\ 7 & 4 \leq x \leq 5 \\ 3 & x > 5 \end{cases}$$

(at point [1])

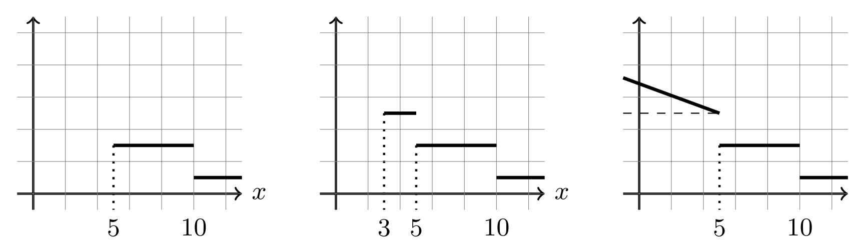
No widening:

		1st iteration	2nd iteration	...	5th/6th iteration
3	$\bot$	$f(x) = 0$	$f(x) = 0$	...	$f(x) = 0$
$3[x < 0]$	$\bot$	$f(x) = \begin{cases} 1 & x < 0 \\ \bot & x \geq 0 \end{cases}$	$f(x) = \begin{cases} 1 & x < 0 \\ \bot & x \geq 0 \end{cases}$	...	$f(x) = \begin{cases} 1 & x < 0 \\ \bot & x \geq 0 \end{cases}$
1	$\bot$	$f(x) = \begin{cases} 1 & x < 0 \\ \bot & x \geq 0 \end{cases}$	$f(x) = \begin{cases} 1 & x < 0 \\ \bot & 0 \leq x \leq 5 \\ 3 & x > 5 \end{cases}$	...	$f(x) = \begin{cases} 1 & x < 0 \\ 5 & 0 \leq x \leq 2 \\ 9 & x = 3 \\ 7 & 4 \leq x \leq 5 \\ 3 & x > 5 \end{cases}$
2	$\bot$	$f(x) = \begin{cases} \bot & x \leq 5 \\ 2 & x > 5 \end{cases}$	$f(x) = \begin{cases} 4 & x \leq 2 \\ \bot & 3 \leq x \leq 5 \\ 2 & x > 5 \end{cases}$	...	$f(x) = \begin{cases} 4 & x \leq 2 \\ 8 & x = 3 \\ 6 & 4 \leq x \leq 5 \\ 2 & x > 5 \end{cases}$
$2[x \geq 0]$	$\bot$	$f(x) = \begin{cases} \bot & x \leq 5 \\ 3 & x > 5 \end{cases}$	$f(x) = \begin{cases} \bot & x < 0 \\ 5 & 0 \leq x \leq 2 \\ \bot & 3 \leq x \leq 5 \\ 3 & x > 5 \end{cases}$	...	$f(x) = \begin{cases} \bot & x < 0 \\ 5 & 0 \leq x \leq 2 \\ 9 & x = 3 \\ 7 & 4 \leq x \leq 5 \\ 3 & x > 5 \end{cases}$

Caterina Urban: The Abstract Domain of Segmented Ranking Functions. SAS 2013: 43-62

Widening

- Example of widening of abstract piecewise-defined ranking functions. The result of widening $v_1^{\#}$ (shown in (a)) with $v_2^{\#}$ (shown in (b) is shown in (c).



(a) (b) (c)

- Widenings enforce convergence (at the cost of loss of precision on the termination domain and maximal number of steps before termination)

Caterina Urban: The Abstract Domain of Segmented Ranking Functions. SAS 2013: 43-62

Widening (cont'd)

- Example of loss of precision by widening on the termination domain ($x \in \mathbb{Q}$)

while $^1(x < 10)$ do
$^2x := 2x$
od^3

$$f(x) = \begin{cases} 3 & 5 \leq x < 10 \\ 1 & 10 \leq x \end{cases}$$

(terminates iff $x > 0$), at least a partial result!

- But with $x \in \mathbb{Z}$,

$$f(x) = \begin{cases} 9 & x = 1 \\ 7 & x = 2 \\ 5 & 3 \leq x \leq 4 \\ 3 & 5 \leq x \leq 9 \\ 1 & 10 \leq x \end{cases}$$

Caterina Urban: The Abstract Domain of Segmented Ranking Functions. SAS 2013: 43-62

Conclusion

- For well-foundedness/liveness, *Abstract interpretation* with infinitary abstractions and convergence acceleration ⋙ finitary abstractions
- The well-foundedness/liveness analysis:
  - requires no given satisfaction precondition [1],
  - requires no special form of loops (e.g. linear, no test in [1])
  - is not restricted to linear ranking functions [1],
  - always terminate thanks to the widening (which is not the case of ad-hoc methods à la Terminator and its numerous derivators based on the search of lasso counter-examples along a single path at a time) [2]

[1] Andreas Podelski, Andrey Rybalchenko: A Complete Method for the Synthesis of Linear Ranking Functions. VMCAI 2004: 239-251

[2] Byron Cook, Andreas Podelski, Andrey Rybalchenko: Proving program termination. Commun. ACM 54(5): 88-98 (2011)

What Next?

- Verification of LTL specifications for infinite unbounded transition systems (including software)
- Full automatic verification not debugging/bounded checking/etc (there are no counter-examples for infinite unbounded non-wellfoundedness)