Working with infinite posets

Damien Zufferey

IST Austria (Institute of Science and Technology Austria)

May 3, 2011

Well-structured transition system

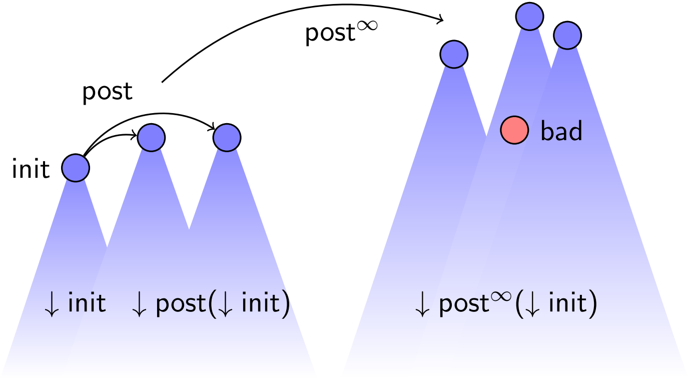
A well-structured transition system (WSTS) is a transition system $\langle S, \rightarrow, \leq \rangle$ such that:

- $\leq$ is a well-quasi-ordering (wqo),
  i.e. well-founded + no infinite antichain.
- compatibility of $\leq$ w.r.t. $\rightarrow$

$$\begin{tikzcd}
 & t \arrow[r, "*"] \arrow[d, phantom, "\rotatebox{90}{$\leq$}"] & t' \arrow[d, phantom, "\rotatebox{90}{$\leq$}"] & \exists \\
\forall & s \arrow[r] & s' &
\end{tikzcd}$$

for more detail see:
[Finkel and Schnoebelen, 2001, Abdulla et al., 1996]

Forward analysis of WSTS



Understanding what happens in *post*$^\infty$

Computing *post*$^\infty$ should not take ∞ steps. Therefore, acceleration is used.

Given a sequence of transitions as a function f, we need to be able to compute $f^\infty(x)$. Also know as the *least upper bound acceleration* of f.

Problem

The analysis converges only if the system has a finite number of *behaviours*, i.e. there is a finite number of acceleration to compute. This condition is also known as flattability. Acceleration is path dependent.

In practice, finding all the sequences to accelerate (complete algorithm) is already prohibitively expansive.

An analysis that does not depend on the paths ?

Idea

Forcing the termination of the analysis by having an analysis that is not path dependent (e.g. abstract interpretation) at the cost of precision.

As an abstract domain, we can use the set of downward-closed sets (+ ideal completion), like the usual analysis. But the acceleration is replaced by widening (∇).

Quick reminder, ∇ [Cousot and Cousot, 1977]:
for every infinite sequence $s_0, s_1, \ldots$ the sequence $C_0, C_1, \ldots$, where $C_0 = s_0, C_i = C_{i-1} \nabla s_i$, is not strictly increasing.

Hence, the termination of the analysis relies only on the properties of the underlying space, not the transitions.

What are we looking for ?

Goal: a good widening operator that is as general as possible.

Idea: jumping to the limit of ascending chains.

Problem: proving that this is actually a widening oprator.

Thus, we need to understand the structure of S.

Try to get a feeling of what is this structure by following:

[Diestel and Pikhurko, 2003]

On the cofinality of infinite partially ordered sets:
factoring a poset into lean essential subsets

Example: acceleration for Petri net

Assumes we have a Petri net with 4 places. The state space is $\mathbb{N}^4$. After adding limit elements we get $\mathbb{N}^4_\infty$.

Let t be a sequence of transitions s.t. $(1,0,1,0) \rightarrow_t (2,1,1,0)$. acceleration gives: $\bigcup_{i=0}^{\infty} \rightarrow_t^i ((1,0,1,0)) \ = \ \downarrow(\infty,\infty,1,0)$

In this case a widening operator compares two state a, b, checks that $a \leq b$, and sets to ∞ every component that is stricly greater in b.

Can we generalize this approach to a more general setting ?

Definitions (1)

- A *quasi-order* (preorder) in a reflexive and transitive relation.
- A *partial order* is a reflexive, transitive, and anti-symmetric relation.
- A *well-quasi-order* is a quasi-order that has no infinite antichain or infinite strictly decreasing sequence.
- $\uparrow x = \{x' \in S \,|\, x \leq x'\}$ is an upward-closed set.
- $\downarrow x = \{x' \in S \,|\, x' \leq x\}$ is an downward-closed set.

Why using quasi order rather than partial order:
Because anti-symmetry is not needed for the proofs.
In practice, most of the quasi-orders used are partial orders.

Hypothesis

Let S be an infinite (but countable) partially ordered set (poset).

Definitions (2)

- A *chain* is totally ordered subset of S.
- A *directed* set D is a set such that $\forall x, y \in D,\ \exists z \in D,\ x \leq z \wedge y \leq z$.
- $P \subseteq S$ is *cofinal* iff $\downarrow P = S$.
- $P \subseteq S$ is *small* iff it is not cofinal.
- The *cofinality* of S, denoted $\mathrm{cf}(S)$, is the least cardinality of the cofinal subset of S.
- P is *lean* iff all $Q \subseteq P$ with $|Q| > \mathrm{cf(P)}$ are cofinal.
- P is *divisible* iff it is the union of fewer than $\mathrm{cf}(P)$ small subsets.
- $P \subseteq S$ is *essential* iff it is the complement of a small set.

Hypothesis

$\mathrm{cf}(S) = \aleph_0$. (infinite but countable)

About directed sets

Why are directed sets important ?

They generalize chains and

acceleration ($\bigcup_{i=0}^{\infty} f^i(x)$) generates an ascending chain.

P is directed iff P contains a cofinal chain C.

$\Leftarrow$: a chain is directed.

$\Rightarrow$: build a chain by enumerating P and taking the lub.

P is directed iff P is not a union of two small subsets.

$\Leftarrow$: assume P is not directed, pick two elements without upper bounds, use them to create a partition.

$\Rightarrow$: assume P is the union of two small subsets, what about the lub of the elements in those subset ?

Indivisible posets are directed.

Directed sets and lean sets

Why lean sets ? What do they represents ?

A lean set do not contains too much "garbage".

P is directed iff P contains a lean equivalent subset.

$\Rightarrow$: we know P contains a cofinal chain and chains are lean.

$\Leftarrow$: lean sets are indivisible, equivalent sets share divisibility.

For subsets P of S, the following statements are equivalent:

- P is directed;
- P is indivisible;
- P has a cofinal chain;
- P has a lean equivalent subset.

Factoring posets into essential directed subset

We need one more concept: *essential* subset.

An essential subset is the complement of a small subset.

Hence, $P \not\leq P \setminus B$ and $B \not\leq P \setminus B$

Let $\bigcup_{i<\mathrm{cf}(S)} A_i$ be a partition of S into *essential directed subsets*.

Every essential directed subset of S is equivalent to some A_j

Let B be an essential directed subset of S. Define $B_i = B \cap A_i$.
Because B is directed (indivisible) there is j s.t. $B \leq B_j \subseteq A_j$.
If $A_j \leq B$ we are done. Otherwise, B is small in A_j which implies $(B \leq) A_j \leq A_j \setminus B_j (\subseteq P \setminus B)$. This contradicts that B is essential.

What about our original space a WQO ?

If S is well-quasi-ordered, it admits a partition into fewer than $\mathrm{cf}(S)$ indivisible (essential) subsets.

See [Diestel, 2001] for the proof.

What about our widening operator ?

Widening generates indivisible directed subsets, but not essential.

What can we do ?

Theorem by [Pouzet, 1980]

Every directed poset S without infinite antichains has a cofinal subsets that is isomorphic to the direct product of finitely many distinct regular cardinals, the largest of which is $\mathrm{cf}(S)$.

Direct product ? like the case of Petri nets.
Regular cardinals ? ...

The hope it to prove that the widening is taking the limit of one of the component of the directed product.

References I

Abdulla, P. A., Cerans, K., Jonsson, B. and Tsay, Y.-K. (1996).
General Decidability Theorems for Infinite-State Systems.
In LICS pp. 313–321,.

Cousot, P. and Cousot, R. (1977).
Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints.
In POPL pp. 238–252,.

Diestel, R. (2001).
Relating Subsets of a Poset, and a Partition Theorem for WQOs.
Order *18*, 275–279.

Diestel, R. and Pikhurko, O. (2003).
On the Cofinality of Infinite Partially Ordered Sets: Factoring a Poset into Lean Essential Subsets.
Order *20*, 53–66.

Finkel, A. and Schnoebelen, P. (2001).
Well-structured transition systems everywhere!
Theor. Comput. Sci. *256*, 63–92.

Pouzet, M. (1980).
Parties cofinales des ordres partiels ne contenant pas d'antichaines infinies.
preprint.