Abstraction in Fixpoint Logics

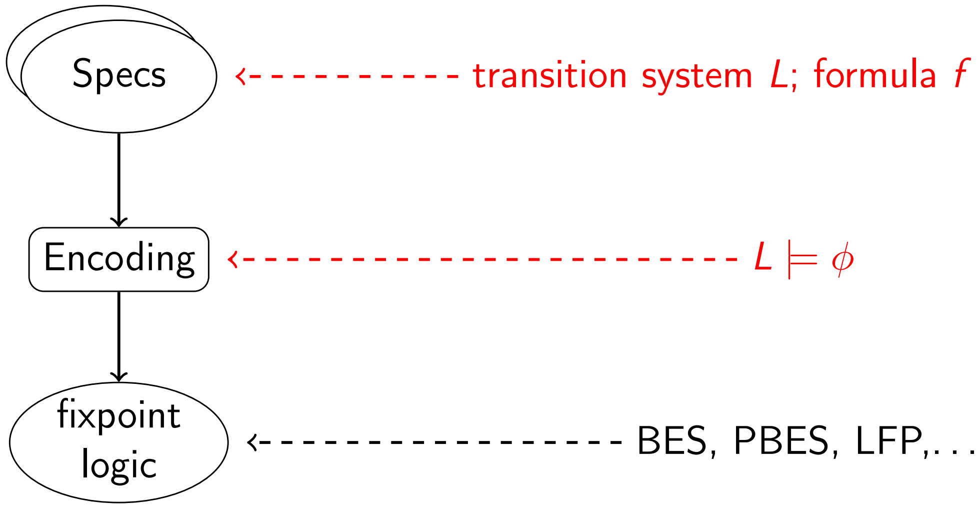
Tim Willemse (TU/e)

Joint work with Maciek Gazda, Sjoerd Cranen, Wieger Wesselink

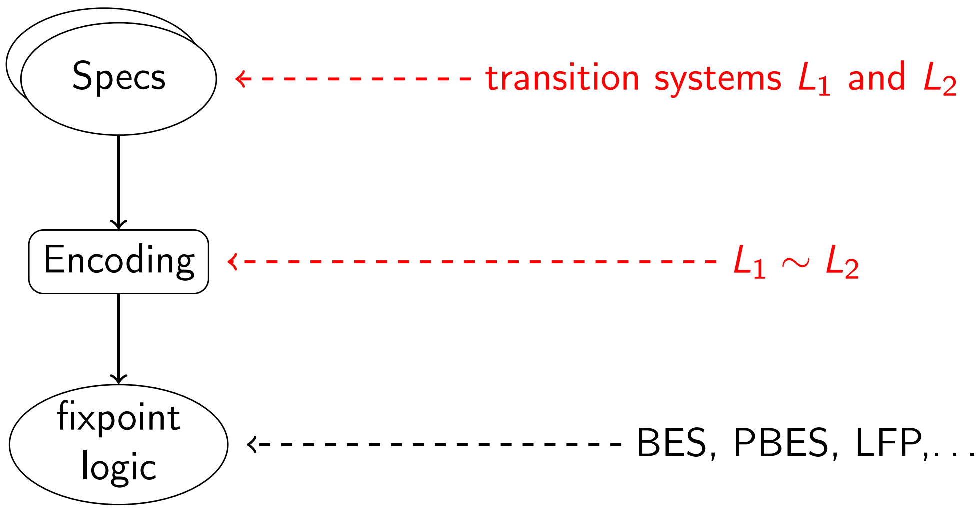
May 9, 2014 DMCD

Outline

Fixpoint Logics for Verification

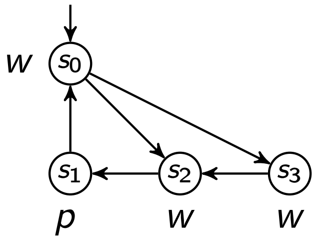


Fixpoint Logics for Verification



Fixpoint Logics for Verification

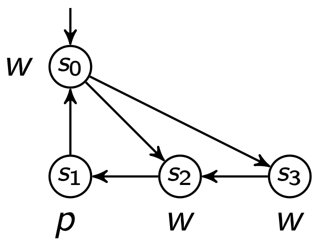
Example (All Work...)



Always $w(ork)$...

Fixpoint Logics for Verification

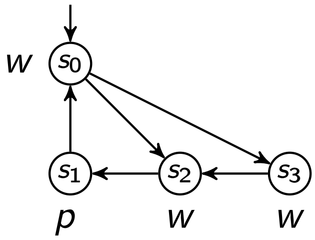
Example (All Work...)



$$X \stackrel{\nu}{=} w \wedge \Box X$$

Fixpoint Logics for Verification

Example (All Work...)



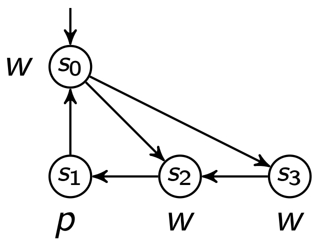
$$X \stackrel{\nu}{=} w \wedge \Box X$$

Compute where X holds by approximation:

- $X^0 = \{s_0, s_1, s_2, s_3\}$
- $X^1 = \{s_0, s_2, s_3\}$
- $X^2 = \{s_0, s_3\}$
- $X^3 = \emptyset$

Fixpoint Logics for Verification

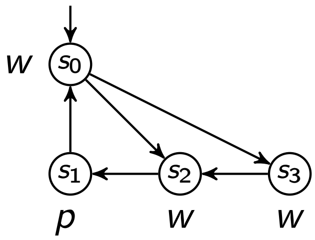
Example (All Work...)



$$\begin{aligned} X &\stackrel{\nu}{=} Y \\ Y &\stackrel{\mu}{=} (w \wedge \Box X) \vee (p \wedge \Box Y) \end{aligned}$$

Fixpoint Logics for Verification

Example (All Work...)



$$\begin{aligned} X &\stackrel{\nu}{=} Y \\ Y &\stackrel{\mu}{=} (w \wedge \Box X) \vee (p \wedge \Box Y) \end{aligned}$$

Convert to Boolean Equation System:

$$\begin{aligned} X_{s_0} &\stackrel{\nu}{=} Y_{s_0} & \qquad Y_{s_0} &\stackrel{\mu}{=} X_{s_2} \wedge X_{s_3} \\ X_{s_1} &\stackrel{\nu}{=} Y_{s_1} & Y_{s_1} &\stackrel{\mu}{=} Y_{s_0} \\ X_{s_2} &\stackrel{\nu}{=} Y_{s_2} & Y_{s_2} &\stackrel{\mu}{=} X_{s_1} \\ X_{s_3} &\stackrel{\nu}{=} Y_{s_3} & Y_{s_3} &\stackrel{\mu}{=} X_{s_2} \end{aligned}$$

X_{s_i} is true iff $s_i \in X$; same for Y

Outline

Boolean Equation Systems

A *Boolean Equation* is an equation of the form

$$X \stackrel{\mu}{=} f_X$$

fixpoint equality; can also be $\stackrel{\nu}{=}$

Boolean Equation Systems

6/18

A *Boolean Equation* is an equation of the form

$$X \stackrel{\mu}{=} f_X$$

propositional variable

Department of Mathematics and Computer Science

Technische Universiteit Eindhoven University of Technology

Boolean Equation Systems

A *Boolean Equation* is an equation of the form

$$X \stackrel{\mu}{=} f_X$$

propositional formula; propositional variables occur only positively

Boolean Equation Systems

A *Boolean Equation* is an equation of the form

$$X \stackrel{\mu}{=} f_X$$

Semantics: the least (resp. largest) Boolean satisfying the equation.

Boolean Equation Systems

A *Boolean Equation* is an equation of the form

$$X \overset{\mu}{=} f_X$$

Semantics: the least (resp. largest) Boolean satisfying the equation.

Example

- $X \overset{\mu}{=} \mathit{true}$: solution to X is *true*
- $X \overset{\mu}{=} X$: solution to X is *false*
- $(X \overset{\mu}{=} Y)$: solution to X is determined by Y.

Technische Universiteit Eindhoven University of Technology

Boolean Equation Systems

A Boolean Equation *System* is a *sequence* of the form

$$(X_1 \overset{\sigma_1}{=} f_1) \ \cdots (X_n \overset{\sigma_n}{=} f_n)$$

Semantics assigns a solution to *each* predicate variable

$$[\emptyset]\theta \quad = \theta \qquad\qquad [(X \overset{\sigma}{=} f)\mathcal{E}]\theta \quad = [\mathcal{E}]\theta[X := F_\sigma]$$

where θ is a *propositional environment* and:

$$F_\mu / F_\nu \text{ is the least/greatest } F \text{ satisfying: } F = [f]([\mathcal{E}]\theta[X := F])$$

Technische Universiteit Eindhoven University of Technology

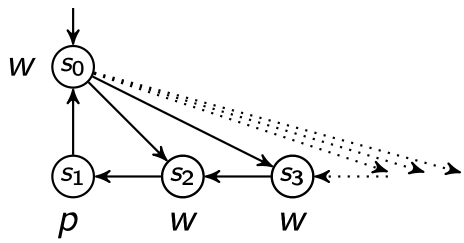
Outline

Abstraction

- Efficient algorithms for solving BESs:
  - Gauß Elimination or directly via semantics
  - Parity game solvers: Zielonka's algorithm, Small Progress Measures
- Succinct representation of large/infinite BESs:
  - PBESs: first-order logic + fixpoints
- How to solve large/infinite BESs?

Abstraction

Example (All Work...)



$$
\begin{aligned}
X &\stackrel{\nu}{=} Y \\
Y &\stackrel{\mu}{=} (w \wedge \Box X) \vee (p \wedge \Box Y)
\end{aligned}
$$

Infinite Boolean Equation System:

$$
\begin{aligned}
X_{s_0} &\stackrel{\nu}{=} Y_{s_0} & \qquad Y_{s_0} &\stackrel{\mu}{=} X_{s_2} \wedge X_{s_3} \wedge \ldots \\
X_{s_1} &\stackrel{\nu}{=} Y_{s_1} & \qquad Y_{s_1} &\stackrel{\mu}{=} Y_{s_0} \\
X_{s_2} &\stackrel{\nu}{=} Y_{s_2} & \qquad Y_{s_2} &\stackrel{\mu}{=} X_{s_1} \\
X_{s_3} &\stackrel{\nu}{=} Y_{s_3} & \qquad Y_{s_3} &\stackrel{\mu}{=} X_{s_2} \\
&\vdots & &\vdots
\end{aligned}
$$

Abstraction

How to deal with infinite BESs:

- In process theory . . . . simulation relations
- In propositional logic . . . . logical consequence

Definition (Consistent Consequence)

Essentially, add the following rule to a proof system for logical consequence:

$$
\frac{\Gamma \cup \{X \Rightarrow Y\} \vdash f_X \Rightarrow f_Y \qquad \mathrm{block}(X) = \mathrm{block}(Y)}{\Gamma \vdash X \Rightarrow Y}
$$

For bound variables X, Y: Y is a consistent consequence of X iff $\vdash X \Rightarrow Y$

Abstraction

Example (All Work...)

$$\begin{aligned} X_{s_0} &\stackrel{\nu}{=} Y_{s_0} \\ X_{s_1} &\stackrel{\nu}{=} Y_{s_1} \\ X_{s_2} &\stackrel{\nu}{=} Y_{s_2} \\ X_{s_3} &\stackrel{\nu}{=} Y_{s_3} \\ &\vdots \end{aligned} \qquad \begin{aligned} Y_{s_0} &\stackrel{\mu}{=} X_{s_2} \land X_{s_3} \land \ldots \\ Y_{s_1} &\stackrel{\mu}{=} Y_{s_0} \\ Y_{s_2} &\stackrel{\mu}{=} X_{s_1} \\ Y_{s_3} &\stackrel{\mu}{=} X_{s_2} \\ &\vdots \end{aligned}$$

Is a consistent consequence of the BES:

$$\begin{aligned} U_0 &\stackrel{\nu}{=} W_0 \\ U_1 &\stackrel{\nu}{=} W_1 \\ U_2 &\stackrel{\nu}{=} W_2 \end{aligned} \qquad \begin{aligned} W_0 &\stackrel{\mu}{=} U_2 \\ W_1 &\stackrel{\mu}{=} W_0 \\ W_2 &\stackrel{\mu}{=} U_1 \land U_2 \end{aligned}$$

$\vdash U_0 \Rightarrow X_{s_0}$ and $\vdash U_2 \Rightarrow X_{s_2}$ and $\vdash U_2 \Rightarrow X_{s_3}$ and $\ldots$;
$\vdash W_0 \Rightarrow Y_{s_0}$ and $\vdash W_2 \Rightarrow Y_{s_2}$ and $\vdash W_2 \Rightarrow Y_{s_3}$ and $\ldots$;

Abstraction

12/18

Example (All Work...)

$$\begin{aligned} X_{s_0} &\stackrel{\nu}{=} Y_{s_0} \\ X_{s_1} &\stackrel{\nu}{=} Y_{s_1} \\ X_{s_2} &\stackrel{\nu}{=} Y_{s_2} \\ X_{s_3} &\stackrel{\nu}{=} Y_{s_3} \\ &\vdots \end{aligned} \qquad \begin{aligned} Y_{s_0} &\stackrel{\mu}{=} X_{s_2} \land X_{s_3} \land \ldots \\ Y_{s_1} &\stackrel{\mu}{=} Y_{s_0} \\ Y_{s_2} &\stackrel{\mu}{=} X_{s_1} \\ Y_{s_3} &\stackrel{\mu}{=} X_{s_2} \\ &\vdots \end{aligned}$$

Is a consistent consequence of the BES:

$$\begin{aligned} U_0 &\stackrel{\nu}{=} W_0 \\ U_1 &\stackrel{\nu}{=} W_1 \\ U_2 &\stackrel{\nu}{=} W_2 \end{aligned} \qquad \begin{aligned} W_0 &\stackrel{\mu}{=} U_2 \\ W_1 &\stackrel{\mu}{=} W_0 \\ W_2 &\stackrel{\mu}{=} U_1 \land U_2 \end{aligned}$$

e.g.: $\vdash W_0 \Rightarrow Y_{s_0}$ follows if $W_0 \Rightarrow Y_{s_0} \vdash U_2 \Rightarrow X_{s_2} \land X_{s_3} \land \ldots$

Example (All Work...)

$$
\begin{array}{rcl}
X_{s_0} & \stackrel{\nu}{=} & Y_{s_0} \\
X_{s_1} & \stackrel{\nu}{=} & Y_{s_1} \\
X_{s_2} & \stackrel{\nu}{=} & Y_{s_2} \\
X_{s_3} & \stackrel{\nu}{=} & Y_{s_3} \\
 & \vdots &
\end{array}
\qquad
\begin{array}{rcl}
Y_{s_0} & \stackrel{\mu}{=} & X_{s_2} \wedge X_{s_3} \wedge \ldots \\
Y_{s_1} & \stackrel{\mu}{=} & Y_{s_0} \\
Y_{s_2} & \stackrel{\mu}{=} & X_{s_1} \\
Y_{s_3} & \stackrel{\mu}{=} & X_{s_2} \\
 & \vdots &
\end{array}
$$

Is a consistent consequence of the BES:

$$
\begin{array}{rcl}
U_0 & \stackrel{\nu}{=} & W_0 \\
U_1 & \stackrel{\nu}{=} & W_1 \\
U_2 & \stackrel{\nu}{=} & W_2
\end{array}
\qquad
\begin{array}{rcl}
W_0 & \stackrel{\mu}{=} & U_2 \\
W_1 & \stackrel{\mu}{=} & W_0 \\
W_2 & \stackrel{\mu}{=} & U_1 \wedge U_2
\end{array}
$$

e.g.: $\vdash W_2 \Rightarrow Y_{s_2}$ follows if $W_2 \Rightarrow Y_{s_2} \vdash U_1 \wedge U_2 \Rightarrow X_{s_1}$

Theorem (Soundness)

If Y is a consistent consequence of X then X's solution implies that of Y

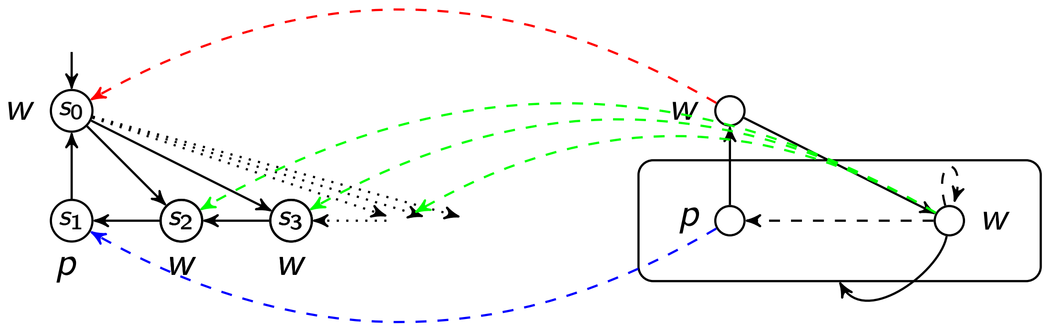
Abstraction works... but how well?

- Is there a comparable abstraction framework for transition systems?
- Which class of infinite BESs become potentially tractable to solve?

Abstraction

Generalised Kripke Modal Transition Systems

- May transitions
- Must hyper transitions



- Generalised mixed simulation

Theorem

Generalised Kripke Modal Transition Systems with generalised mixed simulation and BESs with consistent consequence are equally powerful for model checking

Theorem

Consistent consequence "abstractions" can be exponentially smaller than in generalised mixed simulation abstractions

Abstraction

Definition (Completeness for class $\mathcal{C}$ of BESs)

Consistent Consequence is complete for $\mathcal{C}$ iff for all $\mathcal{E} \in \mathcal{C}$

if equation $X \stackrel{\sigma}{=} f$ in $\mathcal{E}$ has solution *true* for X then
there must be a (finite) BES $\mathcal{E}'$ with equation $X' \stackrel{\sigma}{=} f'$ satisfying

- $\vdash X' \Rightarrow X$
- X' has solution *true*

Theorem (Completeness Classes)

Consistent consequence is complete for:

- *Greatest fixpoint-only (infinite) BESs*
- *Least fixpoint-only (infinite) BESs without infinite conjunctions*

Outline

Fixpoint Logics for Verification

Boolean Equation Systems

Abstraction

Conclusions and Outlook

Conclusions and Outlook

- Consistent consequence is an abstraction framework for BESs
  - coinductive generalisation of logical consequence
  - abstractions remain within the same formalism
  - theory extends to PBESs
- Independent of application domain!
  - model checking
  - equivalence/simulation checking
  - real-time model checking
- Consistent consequence based tooling:
  - abstraction using human-defined homomorphisms .... pbesabsinthe
  - predicate abstraction .... future work
  - CEGAR .... future work