Bisimulation Minimisations for Boolean Equation Systems

Jeroen J.A. Keiren Tim A.C. Willemse

{j.j.a.keiren,t.a.c.willemse}@tue.nl
http://www.win.tue.nl/~{jkeiren,timw}

Department of Mathematics and Computer Science
Technische Universiteit Eindhoven

Introduction

Model Checking

μ-Calculus model checking problem: answer $L \models f$

- L is a Labelled Transition System;
- f is a μ-calculus formula;

- Model checking problem $=$ solving Boolean equation systems
- Solving BES $=$ finding the winner in Parity Games
- Algorithm solving BES $=$ algorithm for computing winner PG
- A BES is a sequence of fixed point equations
- Size BES $\mathcal{E}$ encoding $L \models f$ . . . . . $\mathcal{O}(|L| \cdot |f|)$

Introduction

- Solving BES/Computing winners in PG:
  - Small Prog. Meas. [Jurdziński'00]
  - Bigstep [Schewe'07]
  - Strat. Impr. [Jurdziński & Vöge'00]
- All are exponential, and problem is in NP $\cap$ co-NP

Contributions of this work

- Logical equivalences for BESs;
- Identified reductions for practical examples;
- Identified strengths compared to reductions on LTSs.

Boolean equation system

Definition (Boolean Equation System (BES))

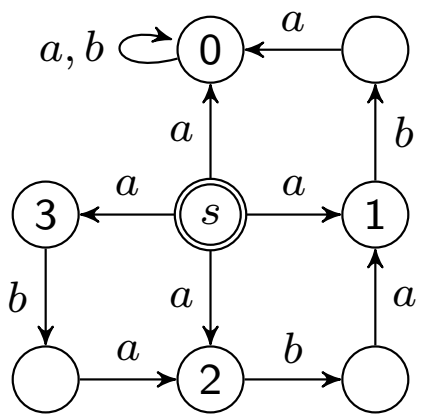
A BES $\mathcal{E}$ in Standard recursive form is defined by the following grammar:

$$\begin{aligned} \mathcal{E} &::= \epsilon \mid (\mu X = f)\ \mathcal{E} \mid (\nu X = f)\ \mathcal{E} \\ f &::= X \mid \bigvee F \mid \bigwedge F \end{aligned}$$

- ϵ is the empty BES;
- μ, ν are least, resp., greatest fixed point signs;
- X is a proposition variable from a set $\mathcal{X}$;
- F is a non-empty set of proposition variables;

Example

Consider property $\phi = \nu Y.\langle a \rangle([a]\text{false} \wedge \nu Z.\langle b \rangle \langle a \rangle Z)$
Informally: after an a action, it is possible to see infinite trace $(ba)^\omega$



$$
\begin{aligned}
(\nu Y_0 &= Z_3 \vee Z_2 \vee Z_1) \\
(\nu Z_3 &= Z_2) \\
(\nu Z_2 &= Z_1) \\
(\nu Z_1 &= Z_0) \\
(\nu Z_0 &= Z_0)
\end{aligned}
$$

Closed and well-formed BES

- $\mathsf{bnd}(\mathcal{E})$ bound variables;
- $\mathsf{occ}(\mathcal{E})$, $\mathsf{occ}(f)$ occurring variables;
- $\mathcal{E}$ is closed: $\mathsf{occ}(\mathcal{E}) \subseteq \mathsf{bnd}(\mathcal{E})$
- $\mathcal{B}$: set of closed BESses in SRF;
- $X \trianglelefteqslant Y$: the equation for X precedes Y's in $\mathcal{E}$;
- $\mathcal{E}$ is well-formed: $\trianglelefteqslant$ is acyclic.

Interpretation

Proposition formulae are interpreted in the context of an environment $\eta{:}\mathcal{X} \to \mathbb{B}$, assigning Boolean values to proposition variables;

Definition (Interpretation of proposition formulae)

Let $\eta{:}\mathcal{X} \to \mathbb{B}$ be an environment. Interpretation $[\![f]\!]\eta$ maps a proposition formula f to true or false:

$$[\![c]\!]\eta = c \qquad [\![X]\!]\eta = \eta(X)$$
$$[\![f \vee g]\!]\eta = [\![f]\!]\eta \vee [\![g]\!]\eta \qquad [\![f \wedge g]\!]\eta = [\![f]\!]\eta \wedge [\![g]\!]\eta$$

Solution

Definition (Solution)

The solution to a BES, in context $\eta{:}\mathcal{X} \to \mathbb{B}$ is inductively defined as:

$$\begin{array}{lcl} [\![\epsilon]\!]\eta & = & \eta \\ [\![(\mu X = f)\ \mathcal{E}]\!]\eta & = & [\![\mathcal{E}]\!](\eta[X := [\![f]\!]([\![\mathcal{E}]\!]\eta[X := \mathsf{false}])]) \\ [\![(\nu X = f)\ \mathcal{E}]\!]\eta & = & [\![\mathcal{E}]\!](\eta[X := [\![f]\!]([\![\mathcal{E}]\!]\eta[X := \mathsf{true}])]) \end{array}$$

Note: $\eta[X := b](Y)$ is defined as $\eta(Y)$ for $Y \neq X$ and b otherwise.

- Solution satisfies Boolean equations ignoring fixpoint symbols;
- Specific solution given by fixpoint symbols;
- Intuitively: left-most fixpoint symbols have highest priority.

Properties of BES

- Solution to closed BES independent of environment:

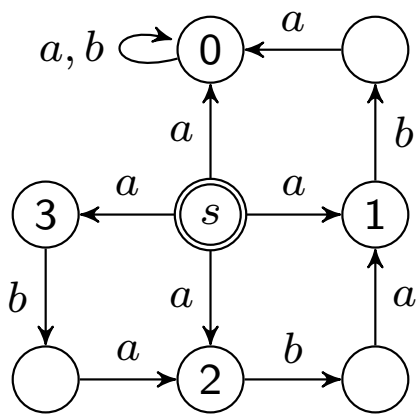
$$\forall X \in \mathsf{bnd}(\mathcal{E}) : \quad [\![\mathcal{E}]\!]\eta(X) = [\![\mathcal{E}]\!]\eta'(X) \text{ for all } \eta, \eta'$$

- Solution is order-sensitive:

$$[\![(\mu X = Y)\ (\nu Y = X)]\!] \neq [\![(\nu Y = X)\ (\mu X = Y)]\!]$$

Example of solution

Consider property $\phi = \nu Y.\langle a \rangle([a]\text{false} \wedge \nu Z.\langle b \rangle\langle a \rangle Z)$
Informally: after an a action, it is possible to see infinite trace $(ba)^\omega$



$$
\begin{aligned}
(\nu Y_0 &= Z_3 \vee Z_2 \vee Z_1) \\
(\nu Z_3 &= Z_2) \\
(\nu Z_2 &= Z_1) \\
(\nu Z_1 &= Z_0) \\
(\nu Z_0 &= Z_0)
\end{aligned}
$$

Solution: $Y_0 = Z_0 = Z_1 = Z_2 = Z_3 = \text{true}$

Rank and Op

- rank(X) indicates in which block of like-signed equations X occurs;
- rank(X) is odd iff X is defined in a μ-equation;
- op(X) indicates top-level boolean operator of equation for X.

Example (Rank/Op)

rank(_)	op(_)			
(1)	$\wedge$	μX	$=$	$X \wedge (Y \wedge Z)$
(2)	$\vee$	νY	$=$	$W \vee (X \vee Y)$
(3)	$\bot$	μZ	$=$	Z
(3)	$\vee$	μW	$=$	$Z \vee (Z \vee W)$

Solution equivalence

Definition

Let $\mathcal{E}, \mathcal{E}' \in \mathcal{B}$. We say equations for X and Y are solution equivalent, denoted $X \equiv Y$, if $[\![\mathcal{E}]\!](X) = [\![\mathcal{E}']\!](Y)$;
we say $\mathcal{E}$ and $\mathcal{E}'$ are solution equivalent, denoted $\mathcal{E} \equiv \mathcal{E}'$, if their first equations are solution equivalent.

Observation:

- $\equiv$ is the coarsest meaningful equivalence relation in possible lattice on BESs;

Local equivalences for Boolean Equation Systems

Aim

Identify finer equivalence relation for BESs that:

- is efficiently (polynomial time) computable;
- preserves solution of BES;

Strong Bisimilarity

Definition

Let $\mathcal{E}, \mathcal{E}' \in \mathcal{B}$. A relation $\mathcal{R} \subseteq \mathsf{bnd}(\mathcal{E}) \times \mathsf{bnd}(\mathcal{E}')$ is said to be a strong bisimulation if, whenever $X \mathcal{R} Y$, then:

- $\mathsf{rank}(X) = \mathsf{rank}(Y)$;
- $\mathsf{op}(X) = \mathsf{op}(Y)$;
- for all $U \in \mathsf{occ}(X)$, there is a $V \in \mathsf{occ}(Y)$, such that $U \mathcal{R} V$;
- for all $V \in \mathsf{occ}(Y)$, there is a $U \in \mathsf{occ}(X)$, such that $U \mathcal{R} V$;

Equations for X and Y are bisimilar, denoted $X \sim Y$, if there exists a bisimulation relation $\mathcal{R}$ such that $X \mathcal{R} Y$;

$\mathcal{E}$ and $\mathcal{E}'$ are bisimilar, denoted $\mathcal{E} \sim \mathcal{E}'$, if their first equations are bisimilar.

Quotienting

Definition (Quotient)

Let $\mathcal{E} \in \mathcal{B}$. The quotient of $\mathcal{E}$, denoted $\mathcal{E}_{/\sim}$ is an equation system consisting of:

- One equation per equivalence class;
- Fixpoint symbol and logical operand determined by equivalence class;
- One variable per equivalence class in each right hand side;
- Equations for equivalence class with operand $\wedge$ or $\vee$ with single class C in right hand side encoded as $C \wedge C$ and $C \vee C$.

Properties

Let $\mathcal{E}, \mathcal{E}' \in \mathcal{B}$. If $\mathcal{E}' \sim \mathcal{E}_{/\sim}$ then also $\mathcal{E}' \equiv \mathcal{E}_{/\sim}$.

Theorem

The relation $\sim$ is strictly finer than $\equiv$.

Application

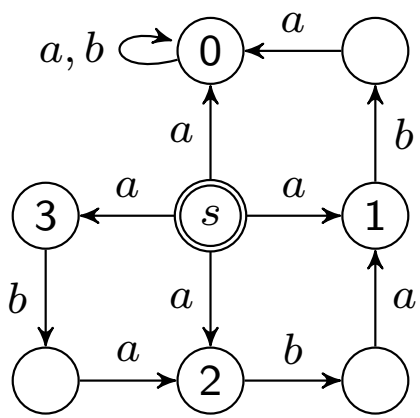
Example

Let N be an arbitrary positive natural number. Consider the process described by the following set of recursive processes (using process-algebraic notation in ACP-style):

$$\{ \quad S = \sum\{a \cdot X(n) \mid n \leqslant N\}, \\ X(0) = a.X(0) + b.X(0), \quad X(n+1) = b.a.X(n) \quad \}$$

Application

Consider property $\phi = \nu Y.\langle a \rangle([a]\text{false} \wedge \nu Z.\langle b \rangle \langle a \rangle Z)$
Informally: after an a action, it is possible to see infinite trace $(ba)^\omega$



Visualisation of S for $N = 3$

$$
\begin{aligned}
(\nu Y_0 &= Z_3 \vee Z_2 \vee Z_1) \\
(\nu Z_3 &= Z_2) \\
(\nu Z_2 &= Z_1) \\
(\nu Z_1 &= Z_0) \\
(\nu Z_0 &= Z_0)
\end{aligned}
$$

Equation system for $\mathcal{E}_3$

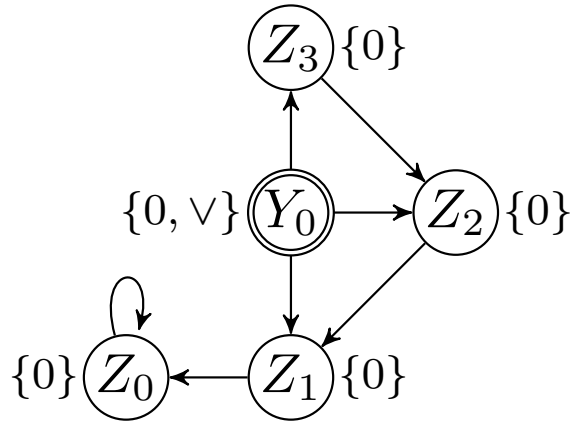
Observations:

- S consists of $2(N+1)$ states;
- S minimal modulo strong bisimilarity.

Application (Strong Bisimulation)

$$
\begin{aligned}
(\nu Y_0 &= Z_3 \vee Z_2 \vee Z_1) \\
(\nu Z_3 &= Z_2) \\
(\nu Z_2 &= Z_1) \\
(\nu Z_1 &= Z_0) \\
(\nu Z_0 &= Z_0)
\end{aligned}
$$

Equation system for $\mathcal{E}_3$

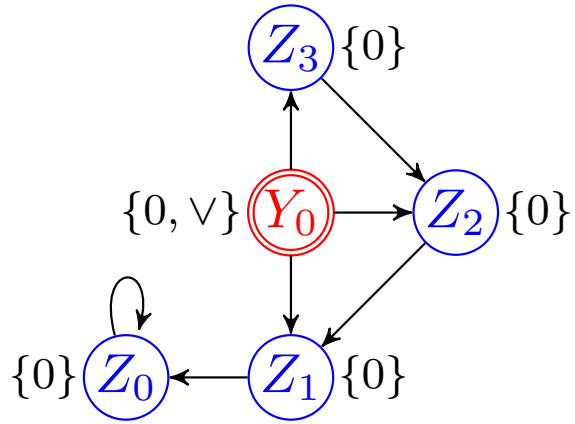


$\mathcal{E}_3$'s Dependency Graph

Application (Strong Bisimulation)

$$
\begin{aligned}
(\nu Y_0 &= Z_3 \vee Z_2 \vee Z_1) \\
(\nu Z_3 &= Z_2) \\
(\nu Z_2 &= Z_1) \\
(\nu Z_1 &= Z_0) \\
(\nu Z_0 &= Z_0)
\end{aligned}
$$

Equation system for $\mathcal{E}_3$

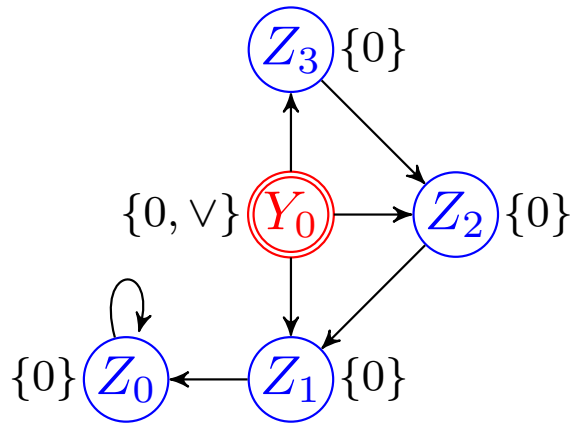


$\mathcal{E}_3$'s Dependency Graph

Application (Strong Bisimulation)

$$
\begin{aligned}
(\nu Y_0 &= Z_3 \vee Z_2 \vee Z_1) \\
(\nu Z_3 &= Z_2) \\
(\nu Z_2 &= Z_1) \\
(\nu Z_1 &= Z_0) \\
(\nu Z_0 &= Z_0)
\end{aligned}
$$

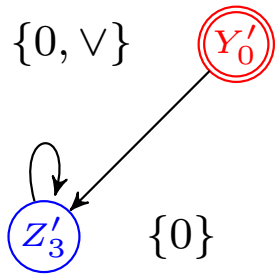
Equation system for $\mathcal{E}_3$



$\mathcal{E}_3$'s Dependency Graph

$$
\begin{aligned}
(\nu Y_{0/\sim} &= Z_{3/\sim} \vee Z_{3/\sim}) \\
(\nu Z_{3/\sim} &= Z_{3/\sim})
\end{aligned}
$$

Equation system for $\mathcal{E}_{3/\sim}$



$\mathcal{E}_{3/\sim}$'s Dependency Graph

Idempotence identifying Bisimilarity

Problem with strong bisimilarity:

- Equations $\sigma X = X' \wedge X''$, or $\sigma X = X' \vee X''$, with $X' \sim X''$ cannot be minimised to $\sigma X = X'$;
- Minimising to $\sigma X = X'$ changes operand of equation, violating $\mathcal{E} \sim \mathcal{E}'$.

Aim

Define coarser equivalence, such that logical operand is only considered when applied to proposition variables from distinguishable classes.

Idempotence identifying Bisimilarity: Definition

Definition

Let $\mathcal{E}, \mathcal{E}' \in \mathcal{B}$. A relation $R \subseteq \mathsf{bnd}(\mathcal{E}) \times \mathsf{bnd}(\mathcal{E}')$ is said to be a strong bisimulation if, whenever $X \mathcal{R} Y$, then:

- $\mathsf{rank}(X) = \mathsf{rank}(Y)$;
- $\mathsf{op}(X) = \mathsf{op}(Y)$;
- for each $U \in \mathsf{occ}(X)$ there is a $V \in \mathsf{occ}(Y)$ such that $U \mathcal{R} V$;
- for each $V \in \mathsf{occ}(Y)$ there is a $U \in \mathsf{occ}(X)$ such that $U \mathcal{R} V$.

Equations for X and Y are strongly bisimilar, denoted $X \sim Y$, if there is a strong bisimulation relation R such that $X \mathcal{R} Y$;

$\mathcal{E}$ and $\mathcal{E}'$ are strongly bisimilar, denoted $\mathcal{E} \sim \mathcal{E}'$, if their first equations are strongly bisimilar.

Idempotence identifying Bisimilarity: Definition

Definition

Let $\mathcal{E}, \mathcal{E}' \in \mathcal{B}$. A relation $R \subseteq \mathsf{bnd}(\mathcal{E}) \times \mathsf{bnd}(\mathcal{E}')$ is said to be an idempotence identifying bisimulation if, whenever $X \mathcal{R} Y$, then:

- $\mathsf{rank}(X) = \mathsf{rank}(Y)$;
- $\mathsf{op}(X) \neq \mathsf{op}(Y) \Rightarrow$ for all $U \in \mathsf{occ}(X)$ and $V \in \mathsf{occ}(Y)$: $U \mathcal{R} V$;
- for each $U \in \mathsf{occ}(X)$ there is a $V \in \mathsf{occ}(Y)$ such that $U \mathcal{R} V$;
- for each $V \in \mathsf{occ}(Y)$ there is a $U \in \mathsf{occ}(X)$ such that $U \mathcal{R} V$.

Equations for X and Y are idempotence identifying bisimilar, denoted $X \sim_{ii} Y$, if there is an idempotence identifying bisimulation relation R such that $X \mathcal{R} Y$;

$\mathcal{E}$ and $\mathcal{E}'$ are idempotence identifying bisimilar, denoted $\mathcal{E} \sim_{ii} \mathcal{E}'$, if their first equations are idempotence identifying bisimilar.

Idempotence identifying Bisimilarity: Properties

Definition

Let $\mathcal{E} \in \mathcal{B}$. The quotient of $\mathcal{E}$, denoted $\mathcal{E}_{/\sim_{ii}}$ is defined similar to $\mathcal{E}_{/\sim}$, except that:

- in case the right hand side of an equation consists of a single equivalence class, no logical operand is introduced.

This quotient avoids introducing awkward equations such as $\sigma_i C_i = C_j \wedge C_j$.

Lemma

Let $\mathcal{E}, \mathcal{E}' \in \mathcal{B}$. Then $\mathcal{E}' \sim_{ii} \mathcal{E}_{/\sim_{ii}}$ implies $\mathcal{E}' \equiv \mathcal{E}_{/\sim_{ii}}$.

Lattice

Theorem

1. *the relation* $\sim$ *is strictly finer than* $\sim_{ii}$*;*
2. *the relation* $\sim_{ii}$ *is strictly finer than* $\equiv$*;*

The following lemma demonstrates that idempotence identifying bisimilarity and solution equivalence sometimes coincide.

Lemma

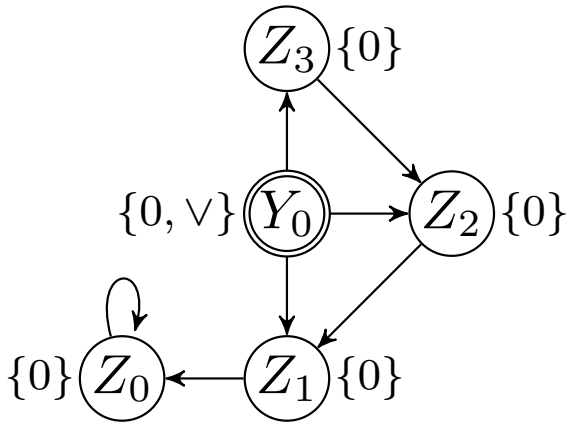
Let $\mathcal{E} \in \mathcal{B}$ *be of the form* $\mathcal{E}_0\mathcal{E}_1\mathcal{E}_2$*, with* $\mathcal{E}_1 \in \mathcal{B}$*. Suppose* $X, X' \in \mathsf{bnd}(\mathcal{E}_1)$*. Assume* $\mathsf{rank}(X)=\mathsf{rank}(X')$ *for all* $X, X' \in \mathsf{bnd}(\mathcal{E}_1)$*. Then* $\mathcal{E}_{1/\sim_{ii}} = \mathcal{E}_{1/\equiv}$*.*

Idempotence identifying Bisimilarity: Application

Recall our example:

$$
\begin{aligned}
(\nu Y_0 &= Z_3 \vee Z_2 \vee Z_1) \\
(\nu Z_3 &= Z_2) \\
(\nu Z_2 &= Z_1) \\
(\nu Z_1 &= Z_0) \\
(\nu Z_0 &= Z_0)
\end{aligned}
$$

Equation System $\mathcal{E}_3$



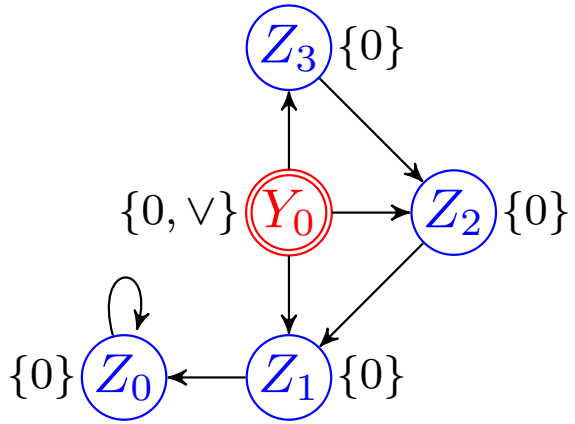
$\mathcal{E}_3$'s Dependency Graph

Idempotence identifying Bisimilarity: Application

Strong bisimulation:

$$
\begin{aligned}
&(\nu Y_0 &&= Z_3 \vee Z_2 \vee Z_1)\\
&(\nu Z_3 &&= Z_2)\\
&(\nu Z_2 &&= Z_1)\\
&(\nu Z_1 &&= Z_0)\\
&(\nu Z_0 &&= Z_0)
\end{aligned}
$$

Equation System $\mathcal{E}_3$



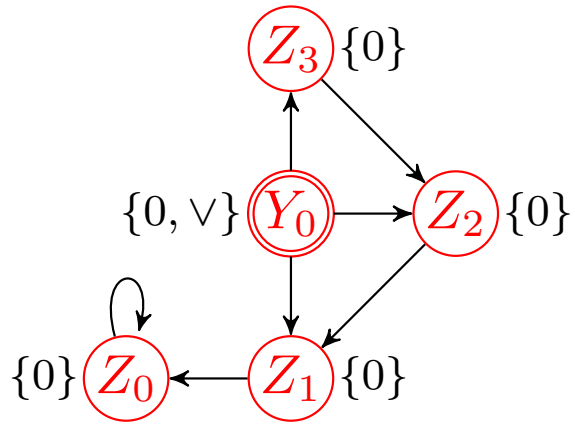
$\mathcal{E}_3$'s Dependency Graph

Idempotence identifying Bisimilarity: Application

Idempotence identifying bisimulation:

$$
\begin{aligned}
(\nu Y_0 &= Z_3 \vee Z_2 \vee Z_1) \\
(\nu Z_3 &= Z_2) \\
(\nu Z_2 &= Z_1) \\
(\nu Z_1 &= Z_0) \\
(\nu Z_0 &= Z_0)
\end{aligned}
$$

Equation System $\mathcal{E}_3$



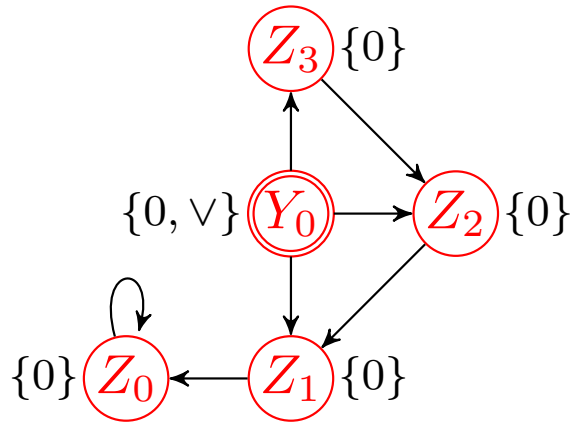
$\mathcal{E}_3$'s Dependency Graph

Idempotence identifying Bisimilarity: Application

Idempotence identifying bisimulation:

$$
\begin{aligned}
(\nu Y_0 &= Z_3 \vee Z_2 \vee Z_1) \\
(\nu Z_3 &= Z_2) \\
(\nu Z_2 &= Z_1) \\
(\nu Z_1 &= Z_0) \\
(\nu Z_0 &= Z_0)
\end{aligned}
$$

Equation System $\mathcal{E}_3$

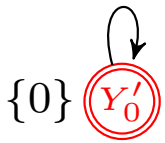


$\mathcal{E}_3$'s Dependency Graph

Reduced:

$$(\nu Y_{0/\sim_{ii}} = Y_{0/\sim_{ii}})$$

Equation system $\mathcal{E}_{3/\sim_{ii}}$

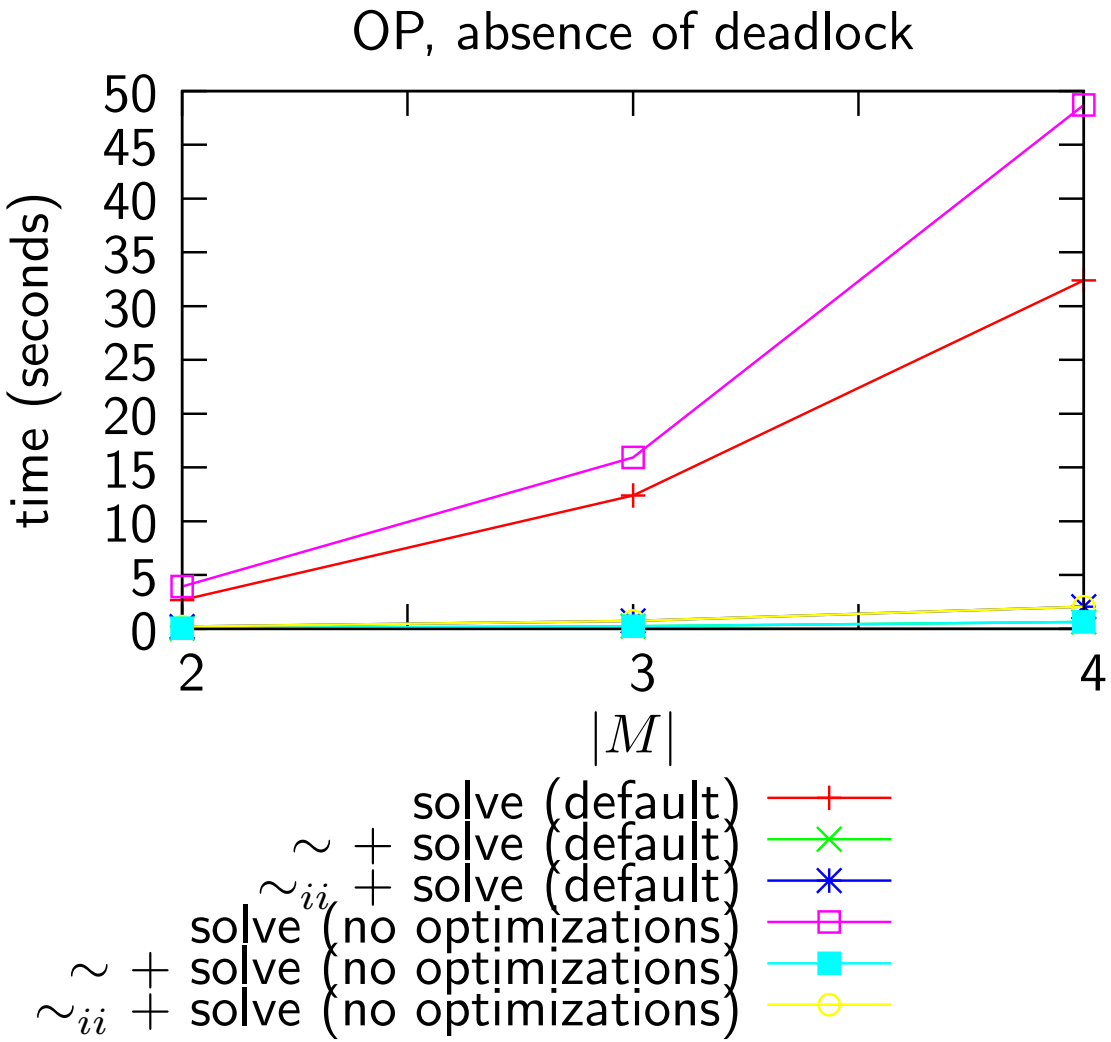


$\mathcal{E}_{3/\sim_{ii}}$'s dependency graph

Observations

- Both equivalences reduce BES, whereas LTS could not be reduced;
- Idempotence identifying bisimilarity can reduce further than strong bisimilarity;
- Idempotence identifying bisimilarity can give rise to arbitrarily large reduction;
- Both equivalences computable in $\mathcal{O}(m \log n)$ time (*e.g.* Paige-Tarjan).

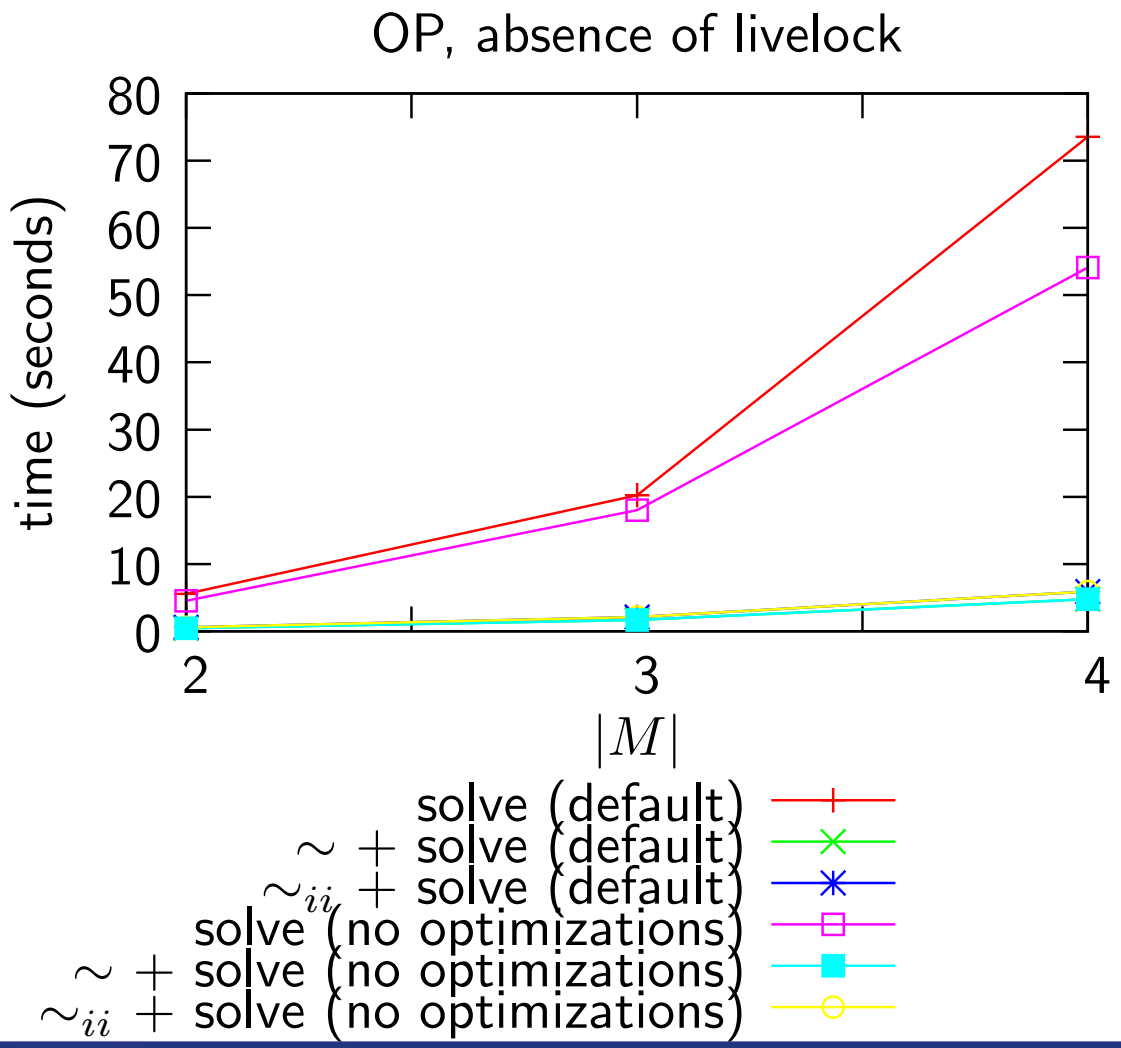
Experiments



Sizes:

Original (2)	578,050
Original (3)	2,083,394
Original (4)	5,417,986
$\sim$	5
$\sim_{ii}$	2

Experiments (2)

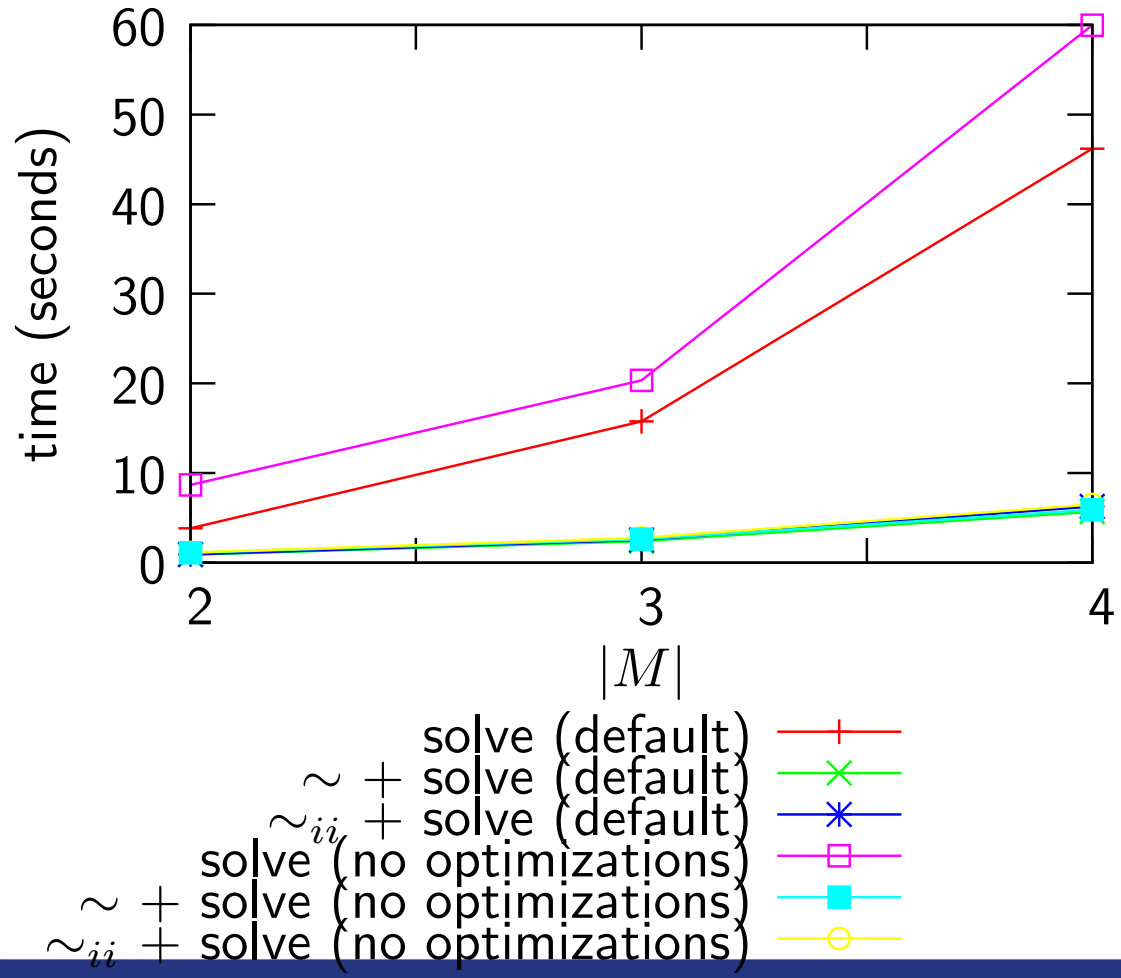


Sizes:

Original (2)	1,100,802
Original (3)	3,933,506
Original (4)	10,172,418
$\sim$	8
$\sim_{ii}$	7

Experiments (3)

OP, possibility to infinitely often receive a certain message

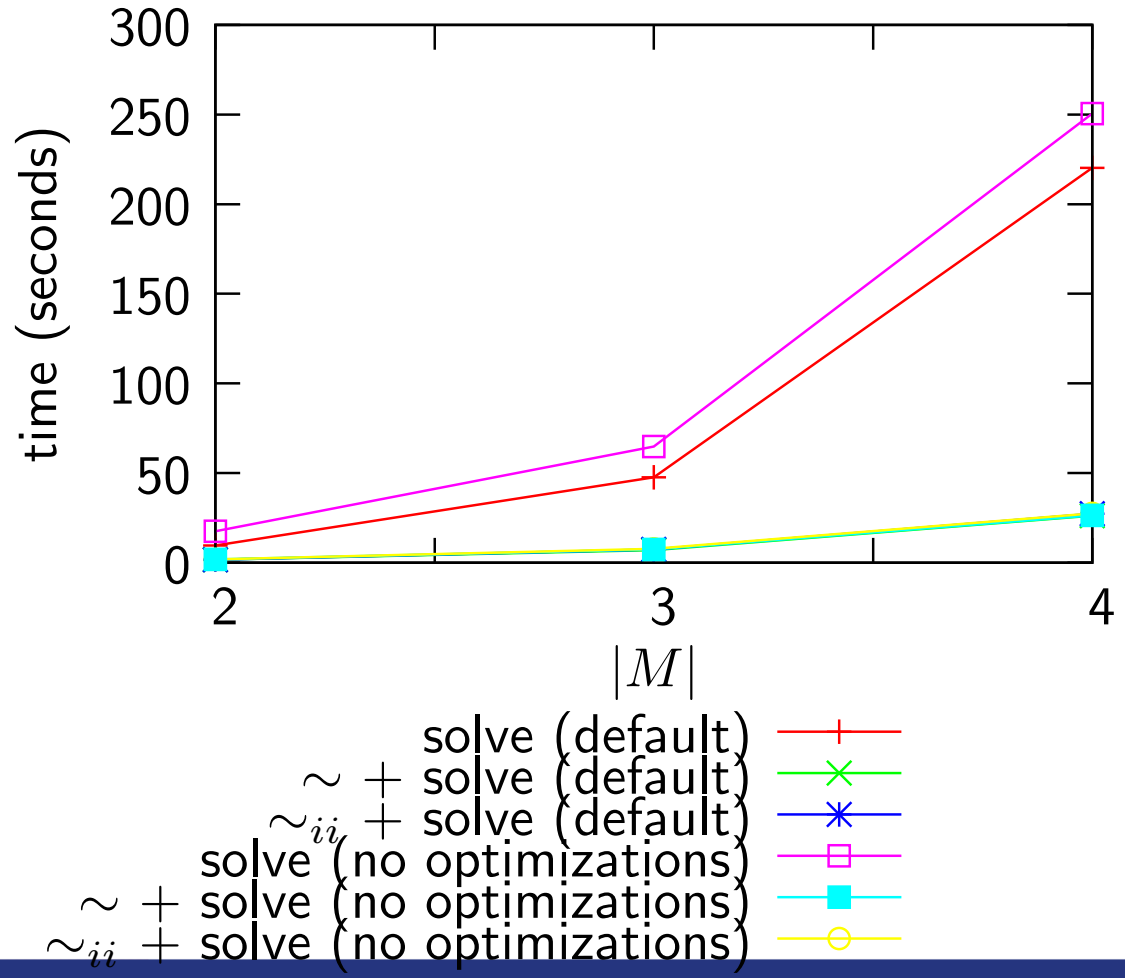


Sizes:

Original (2)	619,010
Original (3)	2,179,826
Original (4)	5,603,586
$\sim$	26,171
$\sim_{ii}$	26,171

Experiments (4)

OP, possibility to infinitely often receive all messages



Sizes:

Original (2)	1,238,023
Original (3)	6,539,482
Original (4)	22,414,349
$\sim$	71,206
$\sim_{ii}$	71,205

Conclusions

- We have defined two equivalence relations on BES, *viz.* strong bisimulation and idempotence identifying bisimulation;
- Idempotence identifying bisimulation solves some peculiarities displayed by strong bisimulation;
- Both relations preserve solution equivalence;
- Both relations are efficiently computable ($\mathcal{O}(m \log n)$);
- Minimisation is rewarding in practice.

Related & future work

Related work:

- Generalisation to arbitrary closed equation systems (Reniers & Willemse)

Future work:

- Extension to coarser notions of equivalence, *e.g.* stuttering equivalence (in progress);
- Extension to open systems of equations (in progress);
- Generalise to Parameterised Boolean Equation Systems.