

Algorithms for Model Checking

2IW50

Lecture 6:
Boolean Equation Systems.

Jaco van de Pol
vdpol@cwi.nl
<http://www.cwi.nl/~vdpol/amc.html>

Technische Universiteit Eindhoven
Centrum voor Wiskunde en Informatica

O V E R V I E W

1. What are Boolean Equation Systems
2. Solving BES by Gauss Elimination
3. Transformation of μ -calculus to BES
4. Examples

Boolean Equation Systems: Syntax

Definition:

- Variables: $Var ::= X, Y, Z, \dots$
- Boolean Expressions:

$$Be ::= Var \mid \top \mid \perp \mid Be \wedge Be \mid Be \vee Be$$

- Equation $::= \mu X = Be \mid \nu X = Be$.
- Boolean Equation System: list of equations

Example:

$$\begin{aligned}\mu X &= (X \wedge Y) \vee Z \\ \nu Y &= X \wedge Y \\ \mu Z &= Z \wedge X\end{aligned}$$

Notes:

- Negation is not allowed, in order to ensure monotonicity.
- The order of equations is important. Intuitively, the topmost sign has priority.

BES: semantics

Intuitive Semantics:

- The solution of a BES is a valuation:
 $Val := Var \rightarrow \{\top, \perp\}$.
- Let $[B](\eta)$ be the value of B under η .
- For the solution η , we want $\eta(X) = [B](\eta)$, for each equation $\sigma X = B$ in the BES.
- Also, we want the smallest (for μ) or greatest (for ν) solution, where higher signs take priority...

Precise Semantics:

- Given a BES S , we define $\llbracket S \rrbracket : Val \rightarrow Val$ by recursion on the length of S :
- Define: $b_\mu := \perp$ and $b_\nu := \top$.

$$\begin{aligned}\llbracket \varepsilon \rrbracket(\eta) &:= \eta \\ \llbracket \sigma X = B; S \rrbracket(\eta) &:= \llbracket S \rrbracket(\eta[X \mapsto [B](\eta')]) \\ &\quad \text{where } \eta' := \llbracket S \rrbracket(\eta[X \mapsto b_\sigma])\end{aligned}$$

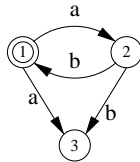
Transformation of μ -calculus to BES

- Given is the following model checking problem:
 - a closed μ -calculus formula f and a
 - a Mixed Kripke Structure $M = (S, s_0, Act, R, L)$.
- We will define a **Boolean Equation System** E , to solve the model checking question $M, s \models f$.
- This BES is defined as follows:
 - For each subformula $\sigma X.g$ ($\sigma \in \{\mu, \nu\}$), and for each state $s \in S$, we add the equation: $\sigma X_s = E_s(g)$. (defined below)
 - The order of the equations respects the subterm ordering in the formula f .
 - In the end: $s \models \sigma X.g$ if and only if the solution of X_s is \top .

Transformation of μ -calculus to BES (2)

$$\begin{aligned}
 E_s(p) &= L(s) \\
 E_s(X) &= X_s \\
 E_s(f \wedge g) &= E_s(f) \wedge E_s(g) \\
 E_s(f \vee g) &= E_s(f) \vee E_s(g) \\
 E_s([a]f) &= \bigwedge_t \{E_t(f) \mid s \xrightarrow{a} t\} \\
 E_s(\langle a \rangle f) &= \bigvee_t \{E_t(f) \mid s \xrightarrow{a} t\} \\
 E_s(\mu X.f) &= X_s \\
 E_s(\nu X.f) &= X_s
 \end{aligned}$$

Examples



- $E_1([a]X) = E_2(X) \wedge E_3(X) = X_2 \wedge X_3$
- $E_2(\langle b \rangle Y) = E_1(Y) \vee E_2(Y) = Y_1 \vee Y_2$
- $E_3(\langle b \rangle Y) = \perp$ (empty disjunction)
- $$\begin{aligned}
 E_1([a]\langle b \rangle \mu Z.Z) &= E_2(\langle b \rangle \mu Z.Z) \wedge E_3(\langle b \rangle \mu Z.Z) \\
 &= (E_1(\mu Z.Z) \vee E_2(\mu Z.Z)) \wedge \perp \\
 &= (Z_1 \vee Z_2) \wedge \perp
 \end{aligned}$$
- Translation of $\mu X.\langle b \rangle T \vee \langle a \rangle X$:

$$\begin{aligned}
 \mu X_1 &= X_3 \vee X_2 \\
 \mu X_2 &= \top \\
 \mu X_3 &= \perp
 \end{aligned}$$

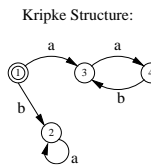
A bigger Example

mu-calculus formula:

$$\nu X. ([a]X \wedge \nu Y. \mu Z. (\langle b \rangle Y \vee \langle a \rangle Z))$$

translation:

$$\begin{aligned}
 \nu X_1 &= X_3 \wedge Y_1 \\
 \nu X_2 &= X_2 \wedge Y_2 \\
 \nu X_3 &= X_4 \wedge Y_3 \\
 \nu X_4 &= \top \wedge Y_4 \\
 \nu Y_1 &= Z_1 \\
 \nu Y_2 &= Z_2 \\
 \nu Y_3 &= Z_3 \\
 \nu Y_4 &= Z_4 \\
 \mu Z_1 &= Y_2 \vee Z_3 \\
 \mu Z_2 &= \perp \vee Z_2 \\
 \mu Z_3 &= \perp \vee Z_4 \\
 \mu Z_4 &= Y_3 \vee \perp
 \end{aligned}$$



Gauss Elimination

- We reduced the model checking problem $M \models f$ to the solution of a BES with $O(|M| \cdot |f|)$ equations.
- We now want a fast procedure to solve such BESs.
- An extremely tedious way to solve a BES is to unfold its semantics.
- A very nice way is to solve it by Gauss Elimination, which we will do next.

Ingredients of Gauss Elimination

Gauss elimination uses the following operations:

- **local solution**: eliminate X in its own equation

$$\mu X = Be \Rightarrow \mu X = Be[X := \perp]$$

$$\nu X = Be \Rightarrow \mu X = Be[X := \top]$$

- **Boolean simplification**. At least the following:

$$b \wedge \top \rightarrow b \quad b \vee \top \rightarrow \top$$

$$b \wedge \perp \rightarrow \perp \quad b \vee \perp \rightarrow b$$

- **substitute definitions backwards**

$$X = X \vee Y \Rightarrow X = X \vee (Y \wedge X)$$

$$Y = Y \wedge X \Rightarrow Y = Y \wedge X$$

- substitute **closed** equations forwards

$$X = \top \Rightarrow X = \top$$

$$Y = Y \wedge X \Rightarrow Y = Y \wedge \top$$

Gauss Elimination: Example

$$\begin{array}{l} \left\{ \begin{array}{l} \mu X = X \vee Y \\ \nu Y = X \vee (Y \wedge Z) \\ \mu Z = Y \wedge Z \end{array} \right. \\ \xrightarrow{\text{local}} \left\{ \begin{array}{l} \mu X = X \vee Y \\ \nu Y = X \vee (Y \wedge \underline{Z}) \\ \mu Z = \perp \end{array} \right. \\ \xrightarrow{\text{back}} \left\{ \begin{array}{l} \mu X = X \vee \underline{Y} \\ \nu Y = X \\ \mu Z = \perp \end{array} \right. \\ \xrightarrow{\text{back}} \left\{ \begin{array}{l} \mu X = \underline{X} \vee X \\ \nu Y = X \\ \mu Z = \perp \end{array} \right. \\ \xrightarrow{\text{local}} \left\{ \begin{array}{l} \mu X = \perp \\ \nu Y = \underline{X} \\ \mu Z = \perp \end{array} \right. \xrightarrow{\text{forward}} \left\{ \begin{array}{l} \mu X = \perp \\ \nu Y = \perp \\ \mu Z = \perp \end{array} \right. \end{array}$$

Gauss Elimination: procedure

Given: A Boolean Equation System

$$\sigma_1 x_1 = B_1$$

⋮

$$\sigma_n x_n = B_n$$

Returns: the solution for x_1

Procedure:

for $i = n \dots 1$ do

$B_i := B_i[x_i := (\text{if } \sigma_i = \mu \text{ then } \perp \text{ else } \top)]$

for $j = 1 \dots i - 1$ do

$B_j := B_j[x_i := B_i]$

Note:

- **Invariant** of the outer loop:
 B_i contains only variables x_j with $j < i$.
- In the end B_1 is **closed**, and evaluates to \top/\perp .
- One could substitute the solution for X_1 and repeat the procedure to solve for X_2 , etc.

Complexity of Gauss Elimination

- Note that in $O(n^2)$ substitutions we obtain the final answer for x_1 .
- However: B_1 can have $O(2^n)$ different copies of e_n as subterms, so intermediate expressions could become exponentially big!
- Practical efficiency increases a lot if one keeps all intermediate terms **simplified** all the time.
- Precise efficiency **depends heavily** on the set of simplification rules.
- Precise complexity of Gauss Elimination is yet **unknown**.
- **Interesting**: the complexity seems to be **independent** of the alternation depth!

Solving the Previous Example

(a few snapshots only)

$$\left\{ \begin{array}{l} \nu X_1 = X_3 \wedge Y_1 \\ \nu X_2 = X_2 \wedge Y_2 \\ \nu X_3 = X_4 \wedge Y_3 \\ \nu X_4 = Y_4 \\ \nu Y_1 = Z_1 \\ \nu Y_2 = Z_2 \\ \nu Y_3 = Z_3 \\ \nu Y_4 = Z_4 \\ \mu Z_1 = Y_2 \vee Z_3 \\ \mu Z_2 = \perp \vee Z_2 \\ \mu Z_3 = Z_4 \\ \mu Z_4 = Y_3 \end{array} \right. \Rightarrow \left\{ \begin{array}{l} \nu X_1 = X_3 \wedge Y_1 \\ \nu X_2 = X_2 \wedge Y_2 \\ \nu X_3 = X_4 \wedge Y_3 \\ \nu X_4 = Y_4 \\ \nu Y_1 = Z_1 \\ \nu Y_2 = Z_2 \\ \nu Y_3 = \underline{Y_3} \\ \nu Y_4 = \underline{Y_3} \\ \mu Z_1 = Y_2 \vee \underline{Y_3} \\ \mu Z_2 = \perp \vee Z_2 \\ \mu \underline{Z_3} = \underline{Y_3} \\ \mu \underline{Z_4} = Y_3 \end{array} \right.$$

Solving the Previous Example

(a few snapshots only)

$$\left\{ \begin{array}{l} \nu X_1 = X_3 \wedge Y_1 \\ \nu X_2 = X_2 \wedge Y_2 \\ \nu X_3 = X_4 \wedge Y_3 \\ \nu X_4 = Y_4 \\ \nu Y_1 = Z_1 \\ \nu Y_2 = Z_2 \\ \nu Y_3 = Y_3 \\ \nu Y_4 = Y_3 \\ \mu Z_1 = Y_2 \vee Y_3 \\ \mu Z_2 = \perp \vee Z_2 \\ \mu \underline{Z_3} = Y_3 \\ \mu \underline{Z_4} = Y_3 \end{array} \right. \Rightarrow \left\{ \begin{array}{l} \nu X_1 = X_3 \wedge Y_1 \\ \nu X_2 = X_2 \wedge Y_2 \\ \nu X_3 = X_4 \wedge Y_3 \\ \nu X_4 = \underline{Y_3} \\ \nu Y_1 = \underline{Y_2 \vee Y_3} \\ \nu Y_2 = \underline{\perp} \\ \nu Y_3 = Y_3 \\ \nu \underline{Y_4} = Y_3 \\ \mu \underline{Z_1} = Y_2 \vee Y_3 \\ \mu \underline{Z_2} = \perp \vee \underline{\perp} = \underline{\perp} \\ \mu \underline{Z_3} = Y_3 \\ \mu \underline{Z_4} = Y_3 \end{array} \right.$$

Solving the Previous Example

(a few snapshots only)

$$\left\{ \begin{array}{l} \nu X_1 = X_3 \wedge Y_1 \\ \nu X_2 = X_2 \wedge Y_2 \\ \nu X_3 = X_4 \wedge Y_3 \\ \nu X_4 = Y_3 \\ \nu Y_1 = Y_2 \vee Y_3 \\ \nu Y_2 = \perp \\ \nu Y_3 = Y_3 \\ \nu \underline{Y_4} = Y_3 \\ \mu \underline{Z_1} = Y_2 \vee Y_3 \\ \mu \underline{Z_2} = \perp \\ \mu \underline{Z_3} = Y_3 \\ \mu \underline{Z_4} = Y_3 \end{array} \right. \Rightarrow \left\{ \begin{array}{l} \nu X_1 = X_3 \wedge \underline{\perp} \\ \nu X_2 = X_2 \wedge \underline{\perp} \\ \nu X_3 = \underline{\perp} \wedge \underline{\perp} \\ \nu \underline{X_4} = \underline{\perp} \\ \nu \underline{Y_1} = \underline{\perp} \vee \underline{\perp} = \underline{\perp} \\ \nu \underline{Y_2} = \perp \\ \nu \underline{Y_3} = \underline{\perp} \\ \nu \underline{Y_4} = Y_3 \\ \mu \underline{Z_1} = Y_2 \vee Y_3 \\ \mu \underline{Z_2} = \perp \\ \mu \underline{Z_3} = Y_3 \\ \mu \underline{Z_4} = Y_3 \end{array} \right.$$

Solving the Previous Example

(a few snapshots only)

$$\left\{ \begin{array}{l} \nu X_1 = X_3 \wedge \top \\ \nu X_2 = X_2 \wedge \perp \\ \nu X_3 = \top \wedge \top \\ \nu X_4 = \top \\ \nu Y_1 = \top \\ \nu Y_2 = \perp \\ \nu Y_3 = \top \\ \nu Y_4 = Y_3 \\ \mu Z_1 = Y_2 \vee Y_3 \\ \mu Z_2 = \perp \\ \mu Z_3 = Y_3 \\ \mu Z_4 = Y_3 \end{array} \right. \Rightarrow \left\{ \begin{array}{l} \nu \underline{X}_1 = \underline{\top} \wedge \top = \underline{\top} \\ \nu \underline{X}_2 = \underline{\top} \wedge \perp = \underline{\perp} \\ \nu \underline{X}_3 = \underline{\top} \\ \nu \underline{X}_4 = \top \\ \nu \underline{Y}_1 = \top \\ \nu \underline{Y}_2 = \perp \\ \nu \underline{Y}_3 = \top \\ \nu \underline{Y}_4 = Y_3 \\ \mu \underline{Z}_1 = Y_2 \vee Y_3 \\ \mu \underline{Z}_2 = \perp \\ \mu \underline{Z}_3 = Y_3 \\ \mu \underline{Z}_4 = Y_3 \end{array} \right.$$

Conclusion: $X_1 = \top$, so (cf. example page 8)

$$1 \models \nu X. \left([a]X \wedge \nu Y. \mu Z. (\langle b \rangle Y \vee \langle a \rangle Z) \right)$$

Exercise

Consider the following μ -calculus formula ϕ :

$$\nu X. \left([a]X \wedge \nu Y. \mu Z. (\langle b \rangle Y \vee \langle a \rangle Z) \right)$$

Consider the following LTS M with states $\{1, 2, 3, 4\}$ and labels $\{a, b\}$:

$$\{(1, a, 3), (3, a, 4), (4, b, 3), (1, b, 2), (2, a, 2)\}$$

- Translate $M, 1 \models \phi$ to a BES
- Solve the BES by Gauss elimination