# A Framework for Parameterised Boolean Equation Systems

Jan Friso Groote
Kaïs Klaï

/ faculteit wiskunde en informatica

# Boolean equation systems

sequence $\sigma\ X_i = \phi$ for $1 \leq i \leq n$

$\sigma \in \{\mu, \nu\}$

$\phi ::= \phi \wedge \phi \mid \phi \vee \phi \mid \mathrm{true} \mid \mathrm{false} \mid X_i$

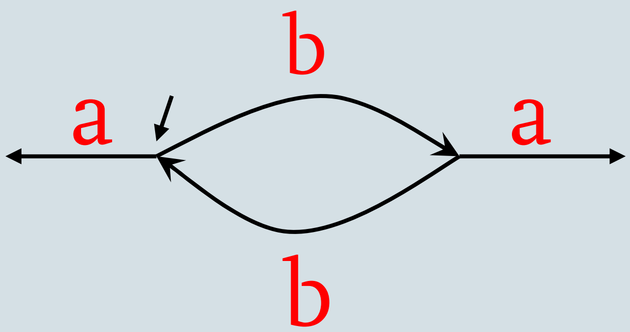
$\mu\ X = X \wedge Y$

$\nu\ Y = Y$

# Where do BESs stem from?

Always an a action is possible

$\nu X.([true]X \wedge \langle a \rangle true)$




$x=b.y+a.\delta, \quad y=b.x+a.\delta$

$\nu Z_x = Z_y \wedge Z_\delta \wedge true$

$\nu Z_y = Z_x \wedge Z_\delta \wedge true$

$\nu Z_\delta = false$

# Parameterized Boolean Equation Systems

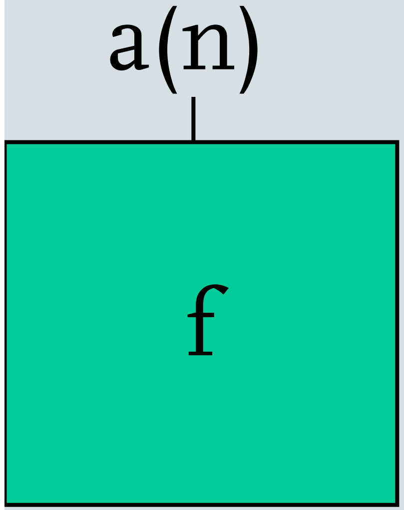
sequence $\sigma\ X_i(d_1,\ldots,d_n)=\phi$ for $1\leq i\leq n$

$\sigma\in\{\mu,\nu\}$

$\phi ::= \phi\wedge\phi \mid \phi\vee\phi \mid \text{true} \mid \text{false} \mid X_i(t_1,\ldots,t_n) \mid$
$\forall d{:}D.\phi \mid \exists d{:}D.\phi \mid \psi$

Mateescu, Local model-checking of an alternation-free value based modal mu-calculus. VMCAI'98, Pisa 1998.

# Unique number generator




$$\Box\forall m{:}\mathbb{N}.[a(m)]\ \Box\forall n{:}\mathbb{N}.[a(n)]n\neq m$$

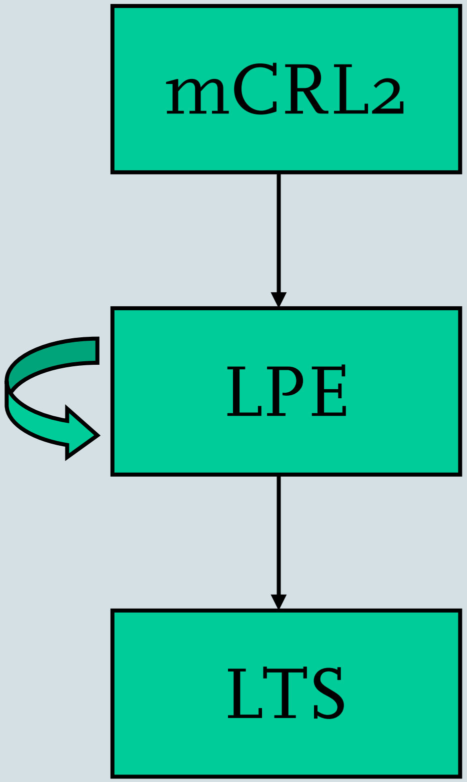
$$X(i{:}\mathbb{N})=a(f(i)).X(f(i))$$

$$\nu Y(i{:}\mathbb{N})=Y(f(i))\wedge\forall m{:}\mathbb{N}.(m=i)\rightarrow Z(f(i),m)$$

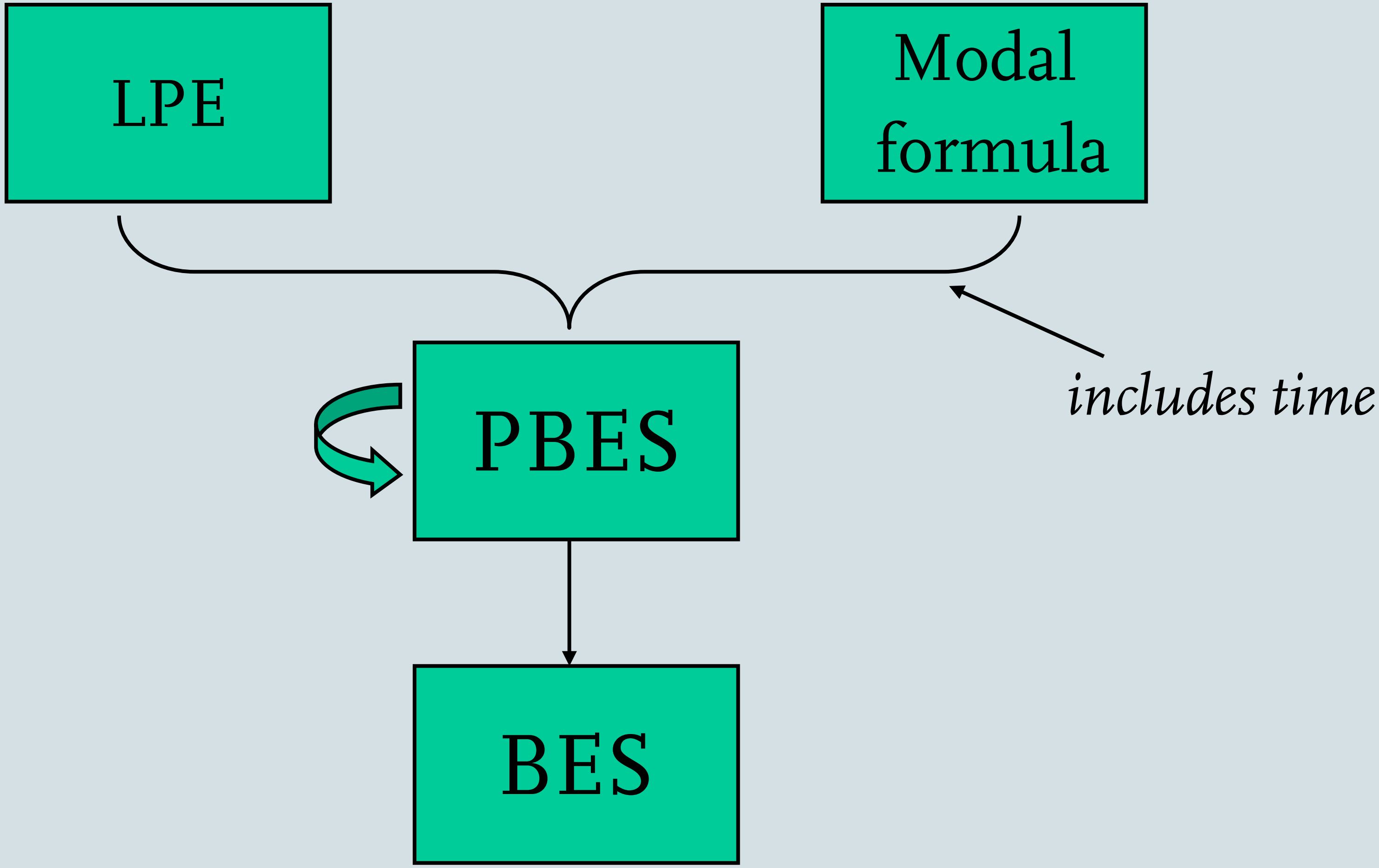
$$a(f(i))\ a(f(f(i)))\ a(f(f(f(i))))\ \ldots$$

$$\nu Z(i{:}\mathbb{N},m{:}\mathbb{N})=Z(f(i),m)\wedge\forall n{:}\mathbb{N}.(n=i)\rightarrow n\neq m$$

# μCRL/mCRL2 toolset




$$P(d{:}D) = \sum_{i \in I} \sum_{e_i : E_i} c_i(d, e_i) \rightarrow a_i(f_i(d, e_i)) \cdot P(g_i(d, e_i))$$


LPE
Modal formula
includes time
PBES
BES

Does $\nu Y(i{:}\mathbb{N}) = Y(i+1) \wedge i<3$ hold for $i=0$?

$\nu Y_0 = Y_1 \wedge 0<3$
$\nu Y_1 = Y_2 \wedge 1<3$
$\nu Y_2 = Y_3 \wedge 2<3$
$\nu Y_3 = Y_4 \wedge 3<3$

# Completeness via Gauß elimation

<u>Theorem</u>

If a for each single equation it can be proven

$$\sigma\, X(d_1,\ldots,d_n)=\phi \quad \equiv \quad \sigma\, X(d_1,\ldots,d_n)=\psi$$

where X does not occur in $\psi$ then each PBES can be solved.

# The techniques for simplifying a single equation

- Propositional and predicate simplification
- Removal of constant and unused variables
- Removal of boolean variables by substitution
- Approximate to exact transformation
- Patterns for equation systems
- Invariants

# Propositional verification and invariants: Does Y hold for some *i*?

$$\nu Y(i{:}\mathbb{N}) = Y(i+1) \wedge \forall m{:}\mathbb{N}.(m=i) \rightarrow Z(i+1,m)$$
$$\nu Z(i{:}\mathbb{N},m{:}\mathbb{N}) = Z(i+1,m) \wedge \forall n{:}\mathbb{N}.(n=i) \rightarrow n=m$$

$$\nu Y(i{:}\mathbb{N}) = Y(i+1) \wedge Z(i+1,i)$$
$$\nu Z(i{:}\mathbb{N},m{:}\mathbb{N}) = Z(i+1,m) \wedge i=m$$

Invariant in Z: i>m

$$\nu Y(i{:}\mathbb{N}) = Y(i+1) \wedge Z(i+1,i)$$
$$\nu Z(i{:}\mathbb{N},m{:}\mathbb{N}) = Z(i+1,m) \wedge \mathit{false}$$

$$\nu Y(i{:}\mathbb{N}) = \mathit{false}$$
$$\nu Z(i{:}\mathbb{N},m{:}\mathbb{N}) = \mathit{false}$$

# Simple patterns to solve a PBES (minimal fixed point).

Consider

$$\mu\ X(d) = \phi(d) \wedge (\psi(d) \vee X(f(d))) \qquad (1)$$

where X does not occur in $\phi$ and $\psi$.
Then (1) equals

$$\mu\ X(d) = \forall j{:}\mathbb{N}.((\forall i{:}\mathbb{N}.i<j \rightarrow \neg\psi(f^i(d))) \rightarrow \phi(f^j(d)))$$

# Simple patterns to solve a PBES (maximal fixed point).

Consider

$$\nu\ X(d)=\phi(d) \wedge (\psi(d) \vee X(f(d))) \qquad (1)$$

where X does not occur in $\phi$ and $\psi$.
Then (1) equals

$$\nu\ X(d)=\exists i{:}\mathbb{N}.\ \psi(f^i(d)) \wedge \forall j{:}\mathbb{N}.(j \leq i \rightarrow \phi(f^j(d)))$$