Invariants and Robustness of BIP models  
(on-going work)

Jan-Olaf Blech     Thanh-Hung Nguyen     Michaël Périm

Université de Grenoble / VERIMAG

WING’09
Context: Certification of Deadlock-Freeness

BIP is used in designing controllers for critical systems: robot and satellite mission, autonomous systems (drones), airbus cabine.

Jan-Olaf Blech, Thanh-Hung Nguyen, Michaël Périn

Invariants and Robustness of BIP models
BIP example: temperature controller (1/2)
Rod 2

cool

θ < 1000
θ := θ + 1

heat

θ ≥ 100
θ := θ − 2

rest

Rod 1

cool

θ = 1000

l1

tick

t1 := t1 + 1

rest

l2

tick

l3

tick

t2 := t2 + 1

cool

θ ≥ 3600

rest

l4

tick

t2 := 0

l5

tick

θ < 1000
θ := θ + 1

l6

tick

θ ≥ 3600

rest

l1

tick

t1 := 0

Cool

heat

θ := 100

rest

heat

θ := 100

Rod

l1

tick

t1 := t1 + 1

rest

l2

tick

θ ≥ 3600

rest

l3

tick

t2 := 0

l4

tick

θ ≥ 3600

rest

l5

tick

θ < 1000
θ := θ + 1

l6

tick

θ ≥ 3600

rest

l1

tick

t1 := 0

Cool

heat

θ := 100

rest

heat

θ := 100

Rod

Behavior Interactions Priorities semantics

- **Behavior** of a component = transition system

  \[
  l \xrightarrow{\text{port guard? } x := e} l' \quad \text{for synchronized action}
  \]

  \[
  l \xrightarrow{C \text{ guard? } x := e} l' \quad \text{for internal action of comp. } C
  \]

- **Interaction** between components = set of ports

  \[
  \{C_1\}, \ldots, \{C_n\}, \{\text{cool, cool}_1\}, \{\text{cool, cool}_2\}, \{\text{tick, tick}_1, \text{tick}_2\}, \ldots
  \]

- **Priorities** between interactions = partial order on interactions

  \[
  \{\text{tick, tick}_1, \text{tick}_2\} < \{\text{cool, cool}_1\}, \{\text{cool, cool}_2\} < \{C_1\}, \ldots, \{C_n\}
  \]
Proof of Deadlock-Freeness for a BIP model $BM$

$DeadlockFree(s) \overset{\text{def}}{=} \exists s'. (s, s') \in \llbracket BM \rrbracket \land s \neq s'$

$Reachable(s) \overset{\text{def}}{=} s \in Init_{BM} \lor \exists s'. (s', s) \in \llbracket BM \rrbracket \land \text{reachable}(s')$

proof scheme for $\forall s. Reachable(s) \implies DeadlockFree(s)$

$\\textbf{Dfinder} : DG$

$\forall s. DG(s) \implies DeadlockFree(s)$ \hspace{1cm} [$PO_1$] \hspace{1cm} YICES

$\forall s. Reachable(s) \implies DG(s)$

$\\textbf{Dfinder} : \Phi$

$\forall s. Reachable(s) \implies \Phi(s)$ \hspace{1cm} [$PO_2$] \hspace{1cm} COQ

$\forall s. \Phi(s) \implies DG(s)$ \hspace{1cm} [$PO_3$] \hspace{1cm} YICES
Component and interaction **invariants** have the shape

$$\bigvee (\@loc \land \psi(\text{variable}))$$

**Component invariants are local to component**: they only mention the locations of one component

$$Cl_1 \overset{\text{def}}{=} (\@l_1 \land t_1 \geq 0) \lor (\@l_2 \land t_1 \geq 3600)$$

**Interaction invariants are global properties of the system**

$$II_1 \overset{\text{def}}{=} (\@l_1 \land t_1 = 0) \lor (\@l_3 \land t_2 = 0) \lor (\@l_5 \land 101 \leq \theta \leq 1000) \lor (\@l_6 \land (\theta = 1000 \lor 100 \leq \theta \leq 998))$$
Proof strategy for DFINER invariants

\[ \Phi = Cl_1 \land \ldots \land Cl_n \land II_1 \land \ldots \land II_k \]

- Component inv.
- Interaction inv.

- *Cl* and *II* invariants are claimed to be inductive.
- The proof of \( \forall s. \text{Reachable}(s) \implies \Phi(s) \) \[[PO_2]\] can be conducted on each *Cl* \( i \) and *II* \( j \) separately.
- The recursive definition of *Reachable* leads to \( n + k \) simple proofs by induction:
  - (initially) \( \text{Init}_{BM}(s) \implies Cl_i(s) \)
  - (stability) \( Cl_i(s) \land (s, s') \in [BM] \implies Cl_i(s') \)
- Those implications can be proved by COQ tactics or an SMT-solver.
Is that all?

Thank you for your attention

The claim “DFinder computes inductive invariants” would be true without the many abstraction steps used in the implementation.
The claim "**DFINDER computes inductive invariants**" would be true without the **many abstraction steps** used in the implementation.
An **interaction invariant** corresponds to a **minimal trap** in Petri-net: “a **set of locations that cannot be deserted**”. It is, by construction, **inductive**, but ...

A **component invariant** is computed using the **strengthening sequence**, until reaching a $\phi_n$ sufficiently precise to prove the desired property $\varphi$

$$
\begin{align*}
\Phi_0 &= true \\
\Phi_{i+1} &= Init_{BM} \lor \alpha \circ post_{BM}(\Phi_i)
\end{align*}
$$

Without abstraction $\alpha$, all $\Phi_i$ are **inductive invariants**.

This abstraction consists in **$\exists$ quantifier elimination** from the definition of post:

$$
post_{BM}(\Phi)(s) \overset{def}{=} \exists s', \Phi(s') \land (s, s') \in \llbracket BM \rrbracket
$$
A guiding example

Loop acceleration and ∃ elimination

\[ (l_2) \xrightarrow{\theta=100?} (l_3) \xrightarrow{\theta<1000?} (l_3) \]

- The assertion on \( \theta \) at location \( l_3 \) is captured by the formula:

\[
\begin{align*}
\forall l_2 \rightarrow l_3 \\
\theta_0 &= 100 \land \\
0 \text{ or } ... \\
(\exists n > 0, \theta_0 + (n - 1) \times 2 < 1000 \land \theta = (\theta_0 + n \times 2))
\end{align*}
\]

- Elimination of ∃n should produce \( 2|\theta \). It is needed to get an inductive invariant, but discarded: \( 2|\theta \notin \text{DFINDER logic} \).

- Can be retrieved by recording unrepresentable facts.
The approach

- avoid new costly developments
- at most, modify `DFINDER` strategy

1. **narrowing**
   more strengthening steps?

2. **recording**
   export additional useful informations to `CERTGEN`?

3. **weakening**
   drive `DFINDER` to find weaker (strong enough) inductive invariants?

This talk is about

*weakening without modifying the tool*
The approach

- avoid new costly developments
- at most, modify Dfinder strategy
  1. **narrowing**
     more strengthening steps?
  2. **recording**
     export additional useful informations to CERTGEN?
  3. **weakening**
     drive Dfinder to find weaker (strong enough) inductive invariants?

This talk is about

**weakening without modifying the tool**
Reachable_{BM} \downarrow \Phi \land C_1 \land \ldots \land C_n \downarrow \Phi \Downarrow \text{DFINDER invariant (non inductive)} \downarrow \text{weakening} \uparrow \text{narrowing, counter-examples} \downarrow \Phi \downarrow \varphi \downarrow \text{Desired property to prove} \downarrow \text{Inductive but too weak (cannot happen)} \downarrow \text{true} \downarrow \text{Weakest inductive invariant}
Weakening vs. Strengthening

Reachable\textsubscript{BM} \quad \text{Strongest inductive invariant of BM}

\[ \Phi \land C_1 \land \ldots \land C_n \]
build an inductive invariant by strengthening
recording
\[ \Phi \]
\text{DFINDER invariant (non inductive)}
\[ ?\Phi \Delta \]
\text{weakening}

\[ ?\Phi \Delta \]
\text{Desired property to prove}

\[ ?\Phi \Delta \]
\text{Inductive but too weak (cannot happen)}

\[ \text{true} \]
\text{Weakest inductive invariant}
Reachable\textsubscript{BM} \downarrow \Phi \land C_1 \land \ldots \land C_n \downarrow \text{build an inductive invariant by \textit{strengthening}} \uparrow \text{narrowing, counter-examples} \downarrow \Phi \text{ \textsc{D}Finder \textit{invariant (non inductive)}} \downarrow \text{weakening} \downarrow \Phi_\Delta \text{\textit{Weaker inductive? / non inductive? \textit{invariant}}} \\
\Phi_\Delta \downarrow \varphi \downarrow \text{\textit{Desired property to prove}} \downarrow ?\Phi_\Delta \downarrow \text{Inductive but too weak (cannot happen)} \downarrow true \text{\textit{Weakest inductive invariant}}
Reachable$_{BM}$  
\[ \Phi \land C_1 \land \ldots \land C_n \]

\[ \downarrow \]

build an inductive invariant by **strengthening** recording  
\[ \Phi \]

\[ \uparrow \quad \text{narrowing, counter-examples} \]

\[ \Phi \]

\[ \downarrow \]

**DFINDER** invariant (non inductive)  
\[ \Phi \Delta \]

\[ \downarrow \]

Weaker inductive? / non inductive? invariant

\[ \Phi \Delta \]

\[ \downarrow \]

\[ \varphi \]

\[ \downarrow \]

Inductive but too weak (cannot happen)

\[ ?\Phi \Delta \]

\[ \downarrow \]

\[ true \]

**Weakest inductive invariant**
Reachable_{BM} \downarrow \Phi \land C_1 \land \ldots \land C_n \downarrow \Phi \Downarrow \Phi \triangle \Downarrow \varnothing \Downarrow \Phi \triangle \Downarrow true

Strongest inductive invariant of BM

build an inductive invariant by strengthening recording \uparrow \text{narrowing, counter-examples}

\text{DFINDER invariant (non inductive)}

Weaker inductive? / non inductive? invariant

Desired property to prove

Inductive but too weak (cannot happen)

Weakest inductive invariant
Reachable_{BM} \downarrow \Phi \land C_1 \land \ldots \land C_n \uparrow \text{weakening, counter-examples}\downarrow \Phi \downarrow \text{weakening} \Phi_{\Delta} \downarrow \varphi \downarrow \text{Inductive but too weak (cannot happen)} \Phi_{\Delta} \downarrow \text{true} \Phi_{\Delta} \downarrow \text{Weakest inductive invariant}

Weakening vs. Strengthening

Strongest inductive invariant of BM

build an inductive invariant by strengthening recording

\text{DFINDER invariant (non inductive)}

Desired property to prove
Weakening vs. Strengthening

**Reachable**\(_{BM}\) \(\Downarrow\)

\(\Phi \land C_1 \land \ldots \land C_n\)

build an inductive invariant by strengthening
recording \(\Downarrow\)

\(\Phi\)

\(\uparrow\)

narrowing, counter-examples

\(\Downarrow\)

\(\Phi\)  

**DFINDER** invariant (non inductive)

\(\Downarrow\)

weakening

\(\Downarrow\)

Weaker inductive? / non inductive? invariant

\(\Phi \Delta\)

\(\Downarrow\)

\(\varphi\)

\(\Downarrow\)

\(\Phi \Delta\)

\(\Downarrow\)

Inductive but too weak (cannot happen)

\(\Downarrow\)

true

**Weakest inductive invariant**

Jan-Olaf Blech, Thanh-Hung Nguyen, Michaël Pépin  
Invariants and Robustness of BIP models
Weakening vs. Strengthening

Reachable_{BM} \downarrow \Phi \land C_1 \land \ldots \land C_n \downarrow \Phi \downarrow ?\Phi_\Delta \downarrow \varphi \downarrow ?\Phi_\Delta \downarrow true

Strongest inductive invariant of BM

build an inductive invariant by strengthening recording \uparrow narrowing, counter-examples

\Phi \downarrow\downarrow \text{DFINDER invariant (non inductive)} \downarrow weakening

Weaker inductive? / non inductive? invariant

Desired property to prove

Inductive but too weak (cannot happen)

Weakest inductive invariant
Reachable\(_{BM}\) \[\downarrow\] \(\Phi \land C_1 \land \ldots \land C_n\) build an inductive invariant by \textit{strengthening} recording \[\downarrow\] \(\Phi\) \textsc{DFinder} \textit{invariant} \textit{(non inductive)} \[\downarrow\] \(?\Phi_{\Delta}\) \textit{weakening} \[\downarrow\] \(\varphi\) \textit{Desired property to prove} \[\downarrow\] \(?\Phi_{\Delta}\) \textit{Inductive but too weak} \textit{(cannot happen)} \[\downarrow\] \textit{true} \textit{Weakest inductive invariant}
The intuition: domain specific invariants

BIP is used in several projects to design controllers of critical systems based on *measurements by sensors*. robot and satellite mission, autonomous systems, airbus cabine.

- A sensor returns a value $t$ corresponding to the actual value $\theta$ with an error $\delta$ in $[-\Delta, +\Delta]$: $t = \theta + \delta$

- We are looking for invariants that resist to variation of $\delta$ in $[-\Delta, +\Delta]$.

**Definition:** $\Phi$ is a **robust invariant** of $BM$ if

$$\forall \delta \in [-\Delta, +\Delta], \; \Phi[t/\theta + \delta] \; \text{is an invariant of } BM$$

- The idea of robustness appears in tube semantics of timed automata [Gupta, Henzinger, Jagadeesan, HRTS’97]
How to drive D\textsc{finder} toward robust invariants?

Over-approximating the guard of BM wrt. $\Delta$

$$
\begin{align*}
\text{BM} & \quad \left\{ \begin{array}{l}
t = 100 \\
\theta + \delta = 100
\end{array} \right. \\
\leadsto & \quad 100 - \Delta \leq \theta \leq 100 + \Delta
\end{align*}
$$

\[ \ldots \bigvee 2|\theta \land @l6 \land 100 \leq \theta \leq 998 \]

$$
\llbracket 1 \rrbracket \overset{\text{def}}{=} \ldots \bigvee @l6 \land 100 \leq \theta \leq 998
$$

\[ \ldots \bigvee @l6 \land 99 - \Delta \leq \theta \leq 998 + \Delta \]

\[ \llbracket D\textsc{finder} \textsc{inv.} \rrbracket \overset{\text{def}}{=} \ldots \bigvee @l6 \land 99 - \Delta \leq \theta \leq 998 + \Delta \]

Desired property to prove
How to drive \textbf{D}finder toward robust invariants?

### Over-approximating the guard of BM wrt. $\Delta$

| BM | $t = 100$ $\leadsto$ $\theta + \delta = 100$ $\leadsto$ $100 - \Delta \leq \theta \leq 100 + \Delta$ |
| BM$\Delta$ |

\[
\ldots \bigvee 2|\theta \wedge @l_6 \wedge 100 \leq \theta \leq 998 \\
\Downarrow \\
\Pi_1 \overset{\text{def}}{=} \ldots \bigvee @l_6 \wedge 100 \leq \theta \leq 998 \\
\Downarrow \\
\ldots \bigvee @l_6 \wedge 99 - \Delta \leq \theta \leq 998 + \Delta \\
\Downarrow \\
\varphi \quad \text{Desired property to prove}
\]

\[\text{inductive, } \neg \text{ robust} \]
\[\uparrow \quad \text{strengthening: recording} \]
\[\text{DFinder inv. } \neg \text{ inductive} \]
\[\downarrow \quad \text{weakening: } \Delta \]
\[\text{inductive, robust} \]
How to drive \textsc{Dfinder} toward robust invariants?

**Over-approximating the guard of BM wrt. $\Delta$**

\[
\begin{align*}
\text{BM} &\quad \left\{\begin{array}{l}
t = 100 \\
\theta + \delta = 100
\end{array}\right. \\
\implies &\quad \theta + \delta = 100 \\
\implies &\quad 100 - \Delta \leq \theta \leq 100 + \Delta \\
\end{align*}
\]

\[
\begin{align*}
\ldots &\lor \theta \land \@l_6 \land 100 \leq \theta \leq 998 \\
\implies &\lor \theta \land \@l_6 \land 100 \leq \theta \leq 998 \\
\Downarrow &\lor \theta \land \@l_6 \land 99 - \Delta \leq \theta \leq 998 + \Delta \\
\Downarrow &\phi \quad \text{Desired property to prove}
\end{align*}
\]

\text{\textsc{Dfinder} inv.} \; \neg \text{inductive} \\
\text{\textsc{Dfinder} inv.} \; \neg \text{robust} \\
\text{\textsc{Dfinder} inv.} \; \neg \text{inductive, \neg robust} \\
\text{\textsc{Dfinder} inv.} \; \neg \text{inductive, robust} \\
\text{\textsc{Dfinder} inv.} \; \neg \text{inductive, \neg robust} \\
\text{\textsc{Dfinder} inv.} \; \neg \text{inductive, robust}
How to drive Dfinder toward robust invariants?

Over-approximating the guard of BM wrt. $\Delta$

\[
\begin{align*}
\text{BM} & \quad t = 100 \implies \theta + \delta = 100 \\
\text{BM}_\Delta & \quad 100 - \Delta \leq \theta \leq 100 + \Delta
\end{align*}
\]

\[
\begin{align*}
\ldots & \lor 2|\theta \land @l_6 \land 100 \leq \theta \leq 998 \\
\implies & \quad \ldots \lor @l_6 \land 100 \leq \theta \leq 998 \\
\text{II}_1 & \quad \overset{\text{def}}{=} \ldots \lor @l_6 \land 100 \leq \theta \leq 998 \\
\implies & \quad \ldots \lor @l_6 \land 99 - \Delta \leq \theta \leq 998 + \Delta \\
\implies & \quad \varphi \quad \text{Desired property to prove}
\end{align*}
\]

inductive, $\neg$ robust

\[
\uparrow \quad \text{strengthening:} \quad \text{recording}
\]

\[
\Delta
\]

weakening: \quad \text{inductive, robust}

\[
\neg \text{inductive}
\]

$\neg$ robust

Invariants and Robustness of BIP models
How to drive **DFINDER** toward robust invariants?

**Over-approximating the guard of BM wrt. $\Delta$**

\[
\text{BM} \quad \begin{array}{c}
\begin{aligned}
\[ t = 100 \] & \leadsto \[ \theta + \delta = 100 \]
\end{aligned}
\end{array} \quad \Rightarrow \quad \text{BM}_\Delta
\quad \begin{array}{c}
\begin{aligned}
100 - \Delta & \leq \theta \leq 100 + \Delta
\end{aligned}
\end{array}
\]

\[ \ldots \bigvee \ 2|\theta \land @l_6 \land 100 \leq \theta \leq 998 \]
\[ \downarrow \quad \uparrow \quad \text{inductive, } \neg \text{robust} \]
\[ \text{II}_1 \overset{\text{def}}{=} \ldots \bigvee @l_6 \land 100 \leq \theta \leq 998 \]
\[ \downarrow \]
\[ \text{DFINDER inv. } \neg \text{inductive} \]
\[ \bigvee @l_6 \land 99 - \Delta \leq \theta \leq 998 + \Delta \]
\[ \downarrow \quad \downarrow \quad \text{weakening: } \Delta \quad \text{inductive, robust} \]
\[ \varphi \quad \text{Desired property to prove} \]
How to drive DFINDER toward robust invariants?

Over-approximating the guard of BM wrt. $\Delta$

$$\begin{align*}
    \text{BM: } & \quad t = 100 \quad \Rightarrow \quad \theta + \delta = 100 \\
    \text{BM}_\Delta: & \quad 100 - \Delta \leq \theta \leq 100 + \Delta
\end{align*}$$

$$\ldots \bigvee 2|\theta \land \oplus l_6 \land 100 \leq \theta \leq 998$$

$$\Downarrow$$

$$\exists \theta_1 \equiv \ldots \bigvee \oplus l_6 \land 100 \leq \theta \leq 998$$

$$\Downarrow$$

$$\ldots \bigvee \oplus l_6 \land 99 - \Delta \leq \theta \leq 998 + \Delta$$

$$\Downarrow$$

$$\varphi \quad \text{Desired property to prove}$$

inductive, $\neg$ robust

stiffening: recording

DFINDER inv. $\neg$ inductive

weakening: $\Delta$

inductive, robust
Over-approximating the guard of BM wrt. $\Delta$

$$\begin{align*}
BM & \quad t = 100 \quad \implies \quad \theta + \delta = 100 \quad \implies \quad 100 - \Delta \leq \theta \leq 100 + \Delta \\
BM_{\Delta} & 
\end{align*}$$

$$\ldots \bigvee 2|\theta \land @l_6 \land 100 \leq \theta \leq 998 \quad \Downarrow \quad \Downarrow$$

$$II_1 \overset{\text{def}}{=} \ldots \bigvee @l_6 \land 100 \leq \theta \leq 998 \quad \Downarrow \quad \Downarrow$$

$$\ldots \bigvee @l_6 \land 99 - \Delta \leq \theta \leq 998 + \Delta \quad \Downarrow \quad \Downarrow \quad \Downarrow$$

inductive, $\neg$ robust

$\Uparrow$ strengthening: recording

DFINDER inv. $\neg$ inductive

$\Uparrow$ weakening: $\Delta$

inductive, robust

$\varphi$ Desired property to prove
How to drive \texttt{DFINDER} toward robust invariants?

Over-approximating the guard of BM wrt. $\Delta$

\[
\begin{align*}
\overline{t = 100} & \mapsto \theta + \delta = 100 & \overline{100 - \Delta \leq \theta \leq 100 + \Delta}
\end{align*}
\]

\[
\begin{align*}
\ldots \lor 2|\theta \land @l_6 \land 100 \leq \theta \leq 998 & \quad \text{inductive, } \neg \text{ robust} \\
\ll_1 \overset{\text{def}}{=} \ldots \lor @l_6 \land 100 \leq \theta \leq 998 & \quad \uparrow \quad \text{strengthening: recording} \\
\ldots \lor @l_6 \land 99 - \Delta \leq \theta \leq 998 + \Delta & \quad \downarrow \quad \text{weakening: } \Delta \\
\varphi & \quad \text{Desired property to prove}
\end{align*}
\]
Relation between invariants

\[ \text{(DFINDER)} \Phi_{BM_\Delta} \quad \text{DeadlockFree} \quad \Phi_{BM} \]

\[ \text{SMT solving} \quad \text{SMT solving} \]

\[ \text{ind. proof (new proof strategy)} \]

\[ \text{original proof strategy} \]

\[ BM \equiv (BM_\Delta \land \Delta=0) \]

\[ \text{trivial} \]

\[ \text{Reachable}_{BM_\Delta} \quad \text{Reachable}_{BM} \]

\[ \Phi_{BM} \land C \]

weaker & robust
likely inductive

non-inductive invariant

stronger & \text{\neg} robust
inductive

Jan-Olaf Blech, Thanh-Hung Nguyen, Michaël Pépin

Invariants and Robustness of BIP models
Conclusion & Open questions

Intuition & benefits

- Invariants of systems with sensors must be robust
- More appropriate invariants without modifying the tool
- Less precise guards $\leadsto$ less sensitive to abstraction $\leadsto$ inductive invariants
- A guess that is a posteriori certified by CERTGEN
- by automatic generation of a deductive proof by induction

Open questions for future work

- Robustness: Just a trick? or a sound notion?
- Less precise property $\Rightarrow$ inductiveness
A realistic example

\[ \text{Controllers} \]

\[ \begin{align*}
A_1 \ t_1 &:= m \\
A_2 \ t_2 &:= m
\end{align*} \]

\[ \begin{align*}
\text{Sensor} \ \delta &\in [-\Delta, \Delta] \\
A_1, A_2 &\text{ \ if } |m - c| > \epsilon
\end{align*} \]

\[ m := c \]

\[ \theta \text{ \ if } \]

\[ \begin{align*}
\text{Controller 1:} \\
\text{Controller 2:}
\end{align*} \]

\[ \text{Actuators:} \]

\[ \begin{align*}
A_1 &\text{ \ if } t_1 \geq \text{High}_1 \\
A_2 &\text{ \ if } t_2 \geq \text{High}_2 \\
\text{CONTROLLER 1} &\text{ \ if } |m - c| > \epsilon \\
\text{CONTROLLER 2} &\text{ \ if } |m - c| > \epsilon
\end{align*} \]