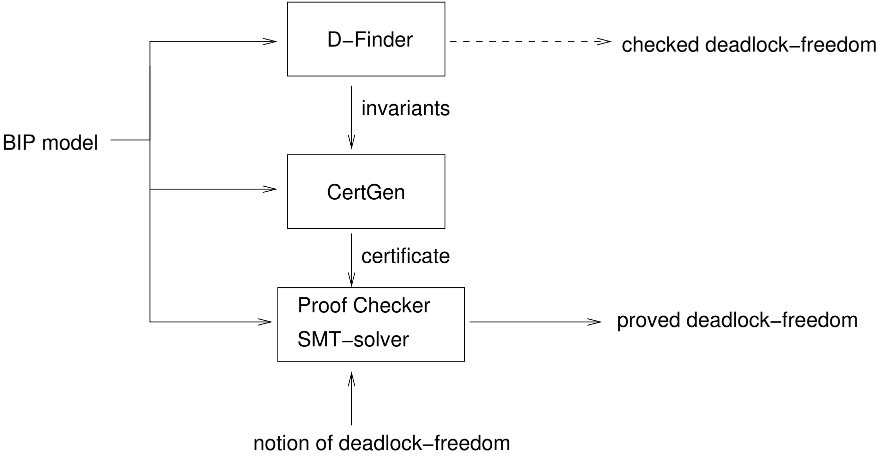
Invariants and Robustness of BIP models
(on-going work)

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

Université de Grenoble / VERIMAG

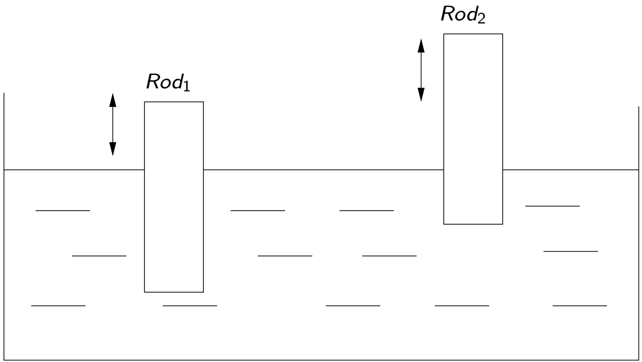
WING'09

Context: Certification of Deadlock-Freeness

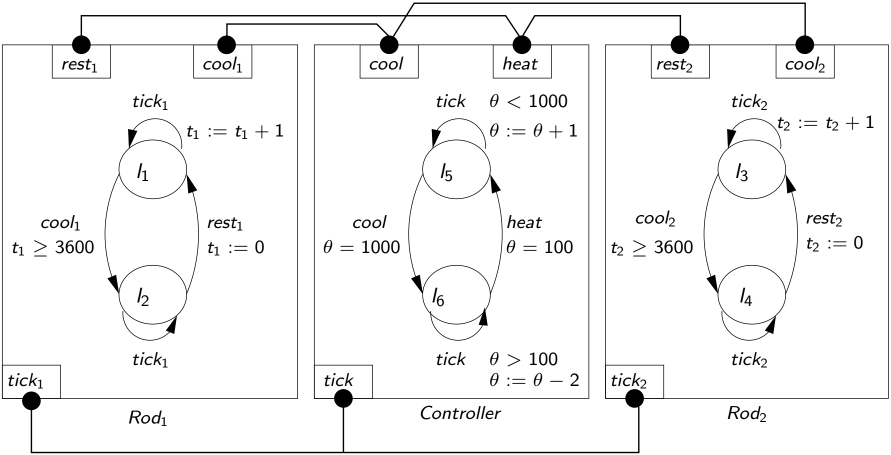


BIP is used in designing controllers for critical systems: robot and sattelite mission, autonomous systems (drones), airbus cabine.

BIP example: temperature controller (1/2)



BIP example: temperature controller (2/2)



Behavior Interactions Priorities semantics

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

  $$l \xrightarrow{\underline{port}\ guard?\ \mathrm{x:=e}} l' \quad \textit{for synchronized action}$$

  $$l \xrightarrow{\underline{C}\ guard?\ \mathrm{x:=e}} l' \qquad \textit{for internal action of comp. } \mathrm{C}$$

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

  $$\{C_1\}, \ldots, \{C_n\}, \{cool, cool_1\}, \{cool, cool_2\}, \{tick, tick_1, tick_2\}, \ldots$$

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

  $$\{tick, tick_1, tick_2\} < \{cool, cool_1\}, \{cool, cool_2\} < \{C_1\}, \ldots, \{C_n\}$$

Proof of Deadlock-Freeness for a BIP model *BM*

$$DeadlockFree(s) \stackrel{def}{=} \exists s'.\ (s, s') \in [\![BM]\!] \wedge s \neq s'$$

$$Reachable(s) \stackrel{def}{=} s \in Init_{BM} \ \vee\ \exists s'.(s', s) \in [\![BM]\!] \wedge \underbrace{Reachable}_{\textbf{recursive}}(s')$$

proof scheme for $\forall \mathbf{s}.Reachable(\mathbf{s}) \Longrightarrow DeadlockFree(\mathbf{s})$

$$\Uparrow \textit{transitivity}$$

$$\text{DFINDER} : DG \begin{cases} \forall s.DG(s) \Longrightarrow DeadlockFree(s) & [PO_1] \quad \text{YICES} \\ \forall s.Reachable(s) \Longrightarrow DG(s) & \end{cases}$$

$$\Uparrow \textit{transitivity}$$

$$\text{DFINDER} : \Phi \quad \begin{cases} \forall \mathbf{s}.\ Reachable(\mathbf{s}) \Longrightarrow \Phi(\mathbf{s}) & [\mathbf{PO_2}] \quad \text{COQ} \\ \forall s.\ \Phi(s) \Longrightarrow DG(s) & [PO_3] \quad \text{YICES} \end{cases}$$

DFINDER invariants

- Component and interaction **invariants** have the shape

$$\bigvee(@loc \wedge \psi(variable))$$

- **Component invariants are local to component**: they only mention the locations of one component
$CI_1 \stackrel{def}{=} (@l_1 \wedge t_1 \geq 0) \vee (@l_2 \wedge t_1 \geq 3600)$

- **Interaction invariants are global properties of the system**
$$\begin{aligned} II_1 \stackrel{def}{=} & (@l_1 \wedge t_1 = 0) \vee (@l_3 \wedge t_2 = 0) \\ & \vee (@l_5 \wedge 101 \leq \theta \leq 1000) \\ & \vee (@l_6 \wedge (\theta = 1000 \vee 100 \leq \theta \leq 998)) \end{aligned}$$

Proof strategy for DFINDER invariants

$$\Phi = \underbrace{CI_1 \wedge \ldots \wedge CI_n}_{Component\ \ inv.} \bigwedge \underbrace{II_1 \wedge \ldots \wedge II_k}_{Interaction\ \ inv.}$$

- CI and II invariants are **claimed to be inductive**.
- The proof of $\forall \mathbf{s}.\ \mathit{Reachable}(\mathbf{s}) \Longrightarrow \Phi(\mathbf{s})$ **[PO$_2$]** can be conducted on each CI_i and II_j separately.
- The **recursive** definition of **Reachable** leads to $n+k$ **simple proofs by induction**:

$$\begin{array}{ll} (\mathit{initially}) & \mathit{Init}_{BM}(s) \Longrightarrow CI_i(s) \\ (\mathit{stability}) & CI_i(s) \wedge (s, s') \in [\![BM]\!] \Longrightarrow CI_i(s') \end{array}$$

- 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

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

DFINDER in brief

- 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 ϕ_n sufficiently precise to prove the desired property φ

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

  Without abstraction α, all Φ_i are **inductive invariants**.

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

$$post_{BM}(\Phi)(s) \stackrel{def}{=} \exists \mathbf{s}', \Phi(s') \wedge (s, s') \in [\![BM]\!]$$

A guiding example

Loop acceleration and ∃ elimination

$$(l_2) \xrightarrow{\theta=100?} (l_3) \xrightarrow{\theta<1000? \;\; \theta:=\theta+2} (l_3)$$

- The assertion on θ at location l_3 is captured by the formula:

$$\overbrace{\theta_0 = 100}^{l_2 \to l_3} \bigwedge$$

$$(\overbrace{\theta = \theta_0}^{0 \;\; or \;\; \ldots} \bigvee \overbrace{\exists \mathbf{n} > \mathbf{0}, \theta_0 + (n-1) \times 2 < 1000 \wedge \theta = (\theta_0 + n \times 2)}^{\ldots \;\; \mathbf{n \;\; times \;\; l_3 \to l_3}})$$

- Elimination of $\exists n$ should produce $2|\theta$. It is **needed to get an inductive invariant**, but **discarded**: $2|\theta \;\; \notin$ 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

Weakening vs. Strengthening

Reachable$_{BM}$ **Strongest inductive invariant of** *BM*

$\Downarrow$

$\Phi \wedge C_1 \wedge \ldots \wedge C_n$ build an inductive invariant by **strengthening**

recording $\Downarrow$ $\uparrow$ **narrowing**, **counter-examples**

Φ **DFINDER invariant (non inductive)**

$\Downarrow$ $\downarrow$ **weakening**

?Φ_Δ Weaker **inductive?** / **non inductive?** invariant

$\Downarrow$

Φ_Δ

φ **Desired property to prove**

$\Downarrow$

?Φ_Δ **Inductive** but **too weak** (cannot happen)

$\Downarrow$

true **Weakest inductive invariant**

Reachable$_{BM}$	**Strongest inductive invariant of** BM
$\Downarrow$	
$\Phi \wedge C_1 \wedge \ldots \wedge C_n$	build an inductive invariant by **strengthening**
recording $\Downarrow$	$\uparrow$ **narrowing**, **counter-examples**
Φ	DFINDER **invariant (non inductive)**
$\Downarrow$	$\downarrow$ **weakening**
$?\Phi_\Delta$	Weaker **inductive?** / **non inductive?** invariant
$\Downarrow$	
Φ_Δ φ	**Desired property to prove**
$\Downarrow$	
$?\Phi_\Delta$	**Inductive** but **too weak** (cannot happen)
$\Downarrow$	
true	**Weakest inductive invariant**

Weakening vs. Strengthening

Reachable$_{BM}$	**Strongest inductive invariant of** BM
$\Downarrow$	
$\Phi \wedge C_1 \wedge \ldots \wedge C_n$	build an inductive invariant by **strengthening**
recording $\Downarrow$	$\uparrow$ **narrowing**, **counter-examples**
Φ	DFINDER **invariant (non inductive)**
$\Downarrow$	$\downarrow$ **weakening**
$?\Phi_\Delta$	Weaker **inductive?** / **non inductive?** invariant
$\Downarrow$	
Φ_Δ φ	**Desired property to prove**
$\Downarrow$	
$?\Phi_\Delta$	**Inductive** but **too weak** (cannot happen)
$\Downarrow$	
true	**Weakest inductive invariant**

Weakening vs. Strengthening

Reachable$_{BM}$	**Strongest inductive invariant of *BM***
$\Downarrow$	
$\Phi \wedge C_1 \wedge \ldots \wedge C_n$	build an inductive invariant by **strengthening**
recording $\Downarrow$	$\uparrow$ **narrowing**, **counter-examples**
Φ	**DFINDER invariant (non inductive)**
$\Downarrow$	$\downarrow$ **weakening**
$?\Phi_\Delta$	Weaker **inductive?** / **non inductive?** invariant
$\Downarrow$	
Φ_Δ φ	**Desired property to prove**
$\Downarrow$	
$?\Phi_\Delta$	**Inductive** but **too weak** (cannot happen)
$\Downarrow$	
true	**Weakest inductive invariant**

Weakening vs. Strengthening

Reachable$_{BM}$	**Strongest inductive invariant of** *BM*
$\Downarrow$	
$\Phi \wedge C_1 \wedge \ldots \wedge C_n$	build an inductive invariant by **strengthening**
recording $\Downarrow$	$\uparrow$ **narrowing, counter-examples**
Φ	DFINDER **invariant (non inductive)**
$\Downarrow$	$\downarrow$ **weakening**
$?\Phi_\triangle$	Weaker **inductive?** / **non inductive?** invariant
$\Downarrow$	
$\Phi_\triangle$ φ	**Desired property to prove**
$\Downarrow$	
$?\Phi_\triangle$	**Inductive** but **too weak** (cannot happen)
$\Downarrow$	
true	**Weakest inductive invariant**

Weakening vs. Strengthening

Reachable$_{BM}$	**Strongest inductive invariant of** BM
$\Downarrow$	
$\Phi \wedge C_1 \wedge \ldots \wedge C_n$	build an inductive invariant by **strengthening**
recording $\Downarrow$	$\uparrow$ **narrowing**, **counter-examples**
Φ	DFINDER **invariant (non inductive)**
$\Downarrow$	$\downarrow$ **weakening**
$?\Phi_\triangle$	Weaker **inductive?** / **non inductive?** invariant
$\Downarrow$	
$\Phi_\triangle$ φ	**Desired property to prove**
$\Downarrow$	
$?\Phi_\triangle$	**Inductive** but **too weak** (cannot happen)
$\Downarrow$	
true	**Weakest inductive invariant**

Weakening vs. Strengthening

Reachable$_{BM}$	**Strongest inductive invariant of** BM
$\Downarrow$	
$\Phi \wedge C_1 \wedge \ldots \wedge C_n$	build an inductive invariant by **strengthening**
recording $\Downarrow$	$\uparrow$ **narrowing, counter-examples**
Φ	DFINDER **invariant (non inductive)**
$\Downarrow$	$\downarrow$ **weakening**
?Φ_Δ	Weaker **inductive?** / **non inductive?** invariant
$\Downarrow$	
Φ_Δ φ	**Desired property to prove**
$\Downarrow$	
?Φ_Δ	**Inductive** but **too weak** (cannot happen)
$\Downarrow$	
true	**Weakest inductive invariant**

Weakening vs. Strengthening

Reachable$_{BM}$	**Strongest inductive invariant of** BM
$\Downarrow$	
$\Phi \wedge C_1 \wedge \ldots \wedge C_n$	build an inductive invariant by **strengthening**
recording $\Downarrow$	$\uparrow$ **narrowing**, **counter-examples**
Φ	DFINDER **invariant (non inductive)**
$\Downarrow$	$\downarrow$ **weakening**
?Φ_Δ	Weaker **inductive?** / **non inductive?** invariant
$\Downarrow$	
Φ_Δ φ	**Desired property to prove**
$\Downarrow$	
?Φ_Δ	**Inductive** but **too weak** (cannot happen)
$\Downarrow$	
true	**Weakest inductive invariant**

Weakening vs. Strengthening

Reachable$_{BM}$	**Strongest inductive invariant of** BM
$\Downarrow$	
$\Phi \wedge C_1 \wedge \ldots \wedge C_n$	build an inductive invariant by **strengthening**
recording $\Downarrow$	$\uparrow$ **narrowing, counter-examples**
Φ	DFINDER **invariant (non inductive)**
$\Downarrow$	$\downarrow$ **weakening**
?Φ_Δ	Weaker **inductive?** / **non inductive?** invariant
$\Downarrow$	
Φ_Δ φ	**Desired property to prove**
$\Downarrow$	
?Φ_Δ	**Inductive** but **too weak** (cannot happen)
$\Downarrow$	
true	**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 sattelite mission, autonomous systems, airbus cabine.

- A sensor returns a value **t** corresponding to the actual value θ with an error δ **in** $[-\Delta, +\Delta]$: $\mathbf{t} = \theta + \delta$
- We are looking for invariants that resist to variation of δ in $[-\Delta, +\Delta]$.

Definition: Φ is a robust invariant of *BM*

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

- The idea of robustness appears in tube semantics of timed automata [Gupta, Henzinger, Jagadeesan, HRTS'97]

How to drive DFINDER toward robust invariants ?

Over-approximating the guard of BM wrt. Δ

$$\overbrace{t = 100}^{\textbf{BM}} \;\rightsquigarrow\; \theta + \delta = 100 \;\rightsquigarrow\; \overbrace{100 - \Delta \leq \theta \leq 100 + \Delta}^{\textbf{BM}_{\boldsymbol{\Delta}}}$$

$\ldots \bigvee 2|\theta \wedge @l_6 \wedge 100 \leq \theta \leq 998$ **inductive**, $\neg$ **robust**

$\Downarrow$ $\uparrow$ **strengthening: recording**

$\mathbf{II_1} \stackrel{def}{=} \ldots \bigvee @l_6 \wedge 100 \leq \theta \leq 998$ DFINDER **inv.** $\neg$ **inductive**

$\Downarrow$ $\downarrow$ **weakening: Δ**

$\ldots \bigvee @l_6 \wedge \mathbf{99} - \boldsymbol{\Delta} \leq \theta \leq \mathbf{998} + \boldsymbol{\Delta}$ **inductive**, **robust**

$\Downarrow$

φ **Desired property to prove**

How to drive DFINDER toward robust invariants ?

Over-approximating the guard of BM wrt. Δ

$$\overbrace{t = 100}^{\textbf{BM}} \rightsquigarrow \theta + \delta = 100 \rightsquigarrow \overbrace{100 - \Delta \leq \theta \leq 100 + \Delta}^{\textbf{BM}_\Delta}$$

$\ldots \bigvee 2|\theta \wedge @l_6 \wedge 100 \leq \theta \leq 998$ **inductive**, $\neg$ **robust**

$\Downarrow$ $\uparrow$ **strengthening: recording**

$\mathbf{II_1} \stackrel{def}{=} \ldots \bigvee @l_6 \wedge 100 \leq \theta \leq 998$ DFINDER **inv.** $\neg$ **inductive**

$\Downarrow$ $\downarrow$ **weakening:** Δ

$\ldots \bigvee @l_6 \wedge \mathbf{99} - \mathbf{\Delta} \leq \theta \leq \mathbf{998} + \mathbf{\Delta}$ **inductive**, **robust**

$\Downarrow$

φ **Desired property to prove**

How to drive DFINDER toward robust invariants ?

Over-approximating the guard of BM wrt. Δ

$$\overbrace{t = 100}^{\textbf{BM}} \quad \rightsquigarrow \quad \theta + \delta = 100 \quad \rightsquigarrow \quad \overbrace{100 - \Delta \leq \theta \leq 100 + \Delta}^{\textbf{BM}_\Delta}$$

$\ldots \bigvee 2|\theta \wedge @l_6 \wedge 100 \leq \theta \leq 998$ **inductive, $\neg$ robust**

$\Downarrow$ $\quad\uparrow$ **strengthening: recording**

$\mathbf{II_1} \stackrel{def}{=} \ldots \bigvee @l_6 \wedge 100 \leq \theta \leq 998$ DFINDER **inv. $\neg$ inductive**

$\Downarrow$ $\quad\downarrow$ **weakening: Δ**

$\ldots \bigvee @l_6 \wedge \mathbf{99} - \mathbf{\Delta} \leq \theta \leq \mathbf{998} + \mathbf{\Delta}$ **inductive, robust**

$\Downarrow$

φ **Desired property to prove**

How to drive DFINDER toward robust invariants ?

Over-approximating the guard of BM wrt. Δ

$$\overbrace{t = 100}^{\textbf{BM}} \quad \rightsquigarrow \quad \theta + \delta = 100 \quad \rightsquigarrow \quad \overbrace{100 - \Delta \leq \theta \leq 100 + \Delta}^{\textbf{BM}_{\Delta}}$$

$\ldots \bigvee \mathbf{2}|\theta \wedge @l_6 \wedge 100 \leq \theta \leq 998$ inductive, $\neg$ robust

$\Downarrow$ $\uparrow$ **strengthening: recording**

$\mathbf{II_1} \stackrel{def}{=} \ldots \bigvee @l_6 \wedge 100 \leq \theta \leq 998$ DFINDER **inv.** $\neg$ **inductive**

$\Downarrow$ $\downarrow$ **weakening: Δ**

$\ldots \bigvee @l_6 \wedge \mathbf{99} - \mathbf{\Delta} \leq \theta \leq \mathbf{998} + \mathbf{\Delta}$ inductive, robust

$\Downarrow$

φ **Desired property to prove**

How to drive DFINDER toward robust invariants ?

Over-approximating the guard of BM wrt. Δ

$$\overbrace{t = 100}^{\textbf{BM}} \rightsquigarrow \theta + \delta = 100 \rightsquigarrow \overbrace{100 - \Delta \leq \theta \leq 100 + \Delta}^{\textbf{BM}_\Delta}$$

$\ldots \bigvee 2|\theta \wedge @l_6 \wedge 100 \leq \theta \leq 998$ **inductive**, $\neg$ **robust**

$\Downarrow$ $\uparrow$ **strengthening: recording**

$\mathbf{II_1} \stackrel{def}{=} \ldots \bigvee @l_6 \wedge 100 \leq \theta \leq 998$ DFINDER **inv.** $\neg$ **inductive**

$\Downarrow$ $\downarrow$ **weakening: Δ**

$\ldots \bigvee @l_6 \wedge \mathbf{99 - \Delta} \leq \theta \leq \mathbf{998 + \Delta}$ **inductive, robust**

$\Downarrow$

φ **Desired property to prove**

How to drive DFINDER toward robust invariants ?

Over-approximating the guard of BM wrt. Δ

$$\overbrace{t = 100}^{\textbf{BM}} \rightsquigarrow \theta + \delta = 100 \rightsquigarrow \overbrace{100 - \Delta \leq \theta \leq 100 + \Delta}^{\textbf{BM}_\Delta}$$

$\ldots \bigvee 2|\theta \wedge @l_6 \wedge 100 \leq \theta \leq 998$ **inductive**, $\neg$ **robust**

$\Downarrow$ $\uparrow$ **strengthening: recording**

$\mathbf{II_1} \stackrel{def}{=} \ldots \bigvee @l_6 \wedge 100 \leq \theta \leq 998$ DFINDER **inv.** $\neg$ **inductive**

$\Downarrow$ $\downarrow$ **weakening:** Δ

$\ldots \bigvee @l_6 \wedge \mathbf{99 - \Delta} \leq \theta \leq \mathbf{998 + \Delta}$ **inductive, robust**

$\Downarrow$

φ **Desired property to prove**

How to drive DFINDER toward robust invariants ?

Over-approximating the guard of BM wrt. Δ

$$\overbrace{t = 100}^{\textbf{BM}} \rightsquigarrow \theta + \delta = 100 \rightsquigarrow \overbrace{100 - \Delta \leq \theta \leq 100 + \Delta}^{\textbf{BM}_{\boldsymbol{\Delta}}}$$

$\ldots \bigvee 2|\theta \wedge @l_6 \wedge 100 \leq \theta \leq 998$ **inductive**, $\neg$ **robust**

$\Downarrow$ $\uparrow$ **strengthening: recording**

$\mathbf{II_1} \stackrel{def}{=} \ldots \bigvee @l_6 \wedge 100 \leq \theta \leq 998$ DFINDER **inv.** $\neg$ **inductive**

$\Downarrow$ $\downarrow$ **weakening: Δ**

$\ldots \bigvee @l_6 \wedge \mathbf{99} - \boldsymbol{\Delta} \leq \theta \leq \mathbf{998} + \boldsymbol{\Delta}$ **inductive, robust**

$\Downarrow$

φ **Desired property to prove**

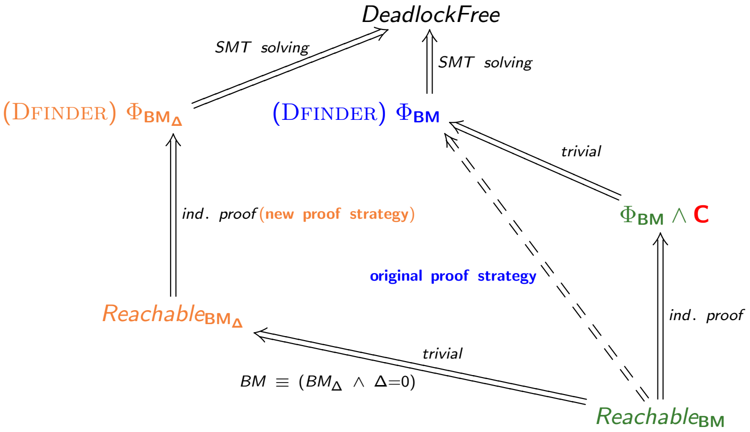
How to drive DFINDER toward robust invariants ?

Over-approximating the guard of BM wrt. Δ

$$\overbrace{t = 100}^{\text{BM}} \quad \rightsquigarrow \quad \theta + \delta = 100 \quad \rightsquigarrow \quad \overbrace{100 - \Delta \leq \theta \leq 100 + \Delta}^{\text{BM}_\Delta}$$

$$\begin{array}{rl}
\ldots \bigvee 2|\theta \wedge @l_6 \wedge 100 \leq \theta \leq 998 & \text{inductive, } \neg \text{ robust} \\
\Downarrow & \quad \uparrow \quad \text{strengthening: recording} \\
\mathbf{II_1} \stackrel{def}{=} \ldots \bigvee @l_6 \wedge 100 \leq \theta \leq 998 & \text{DFINDER inv. } \neg \text{ inductive} \\
\Downarrow & \quad \downarrow \quad \text{weakening: } \Delta \\
\ldots \bigvee @l_6 \wedge \mathbf{99} - \mathbf{\Delta} \leq \theta \leq \mathbf{998} + \mathbf{\Delta} & \text{inductive, robust} \\
\Downarrow & \\
\varphi & \text{Desired property to prove}
\end{array}$$

Relation between invariants



weaker & robust
likely inductive

non-inductive
invariant

stronger & ¬ robust
inductive

Conclusion & Open questions

Intuition & benefits

- Invariants of systems with sensors must be **robust**
- More appropriate invariants **without modifying the tool**
- Less precise guards $\rightsquigarrow$ less sensitive to abstraction $\rightsquigarrow$ **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 $\stackrel{?}{\Longrightarrow}$ inductiveness

A realistic example