# Adequacy and Expressiveness, of Timed Modal Logic

REVISITED

## Workshop in Honour of Anna Ingólfsdóttir


Kim G. Larsen

Aalborg University, DENMARK

AALBORG UNIVERSITET

# First meeting – 1985


# First meeting – 1985

## Algebraic Specification: List

### Sorts

```bash
sort Elem, List
```

### Constructors

```mathematica
nil        : → List
cons       : Elem × List → List
```

### Selectors / Observers

```mathematica
head       : List → Elem
tail       : List → List
isEmpty    : List → Bool
```

ChatGPT

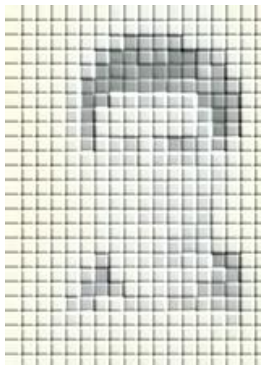
### Axioms

For all `x : Elem`, `xs : List`:

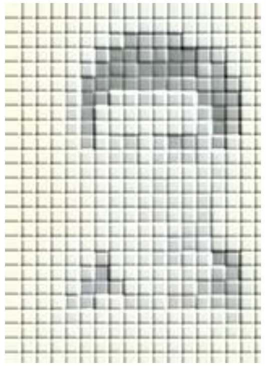
```csharp
isEmpty(nil)            = true
isEmpty(cons(x, xs))    = false

head(cons(x, xs))       = x
tail(cons(x, xs))       = xs
```







Michael Zeeberg

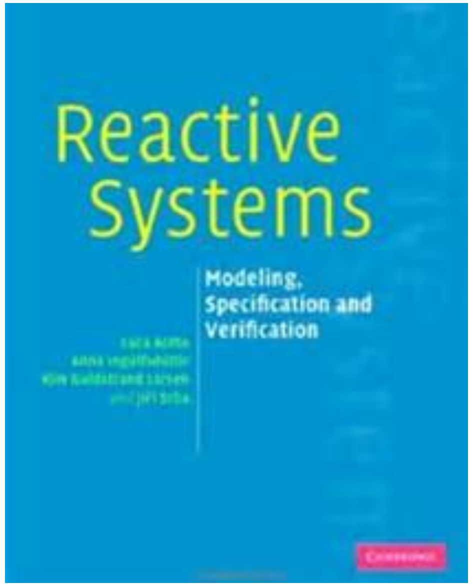


Jens Peter Christensen

**GAS (Generator for Algebraic Specifications)**

# Observing & Monitoring Anna

- Reactive Systems (2007)
- Allegro version 2 (2005)
- Characteristic Formulas (1994)
- Timed Rebecca (2014)
- Value-Passing (1993, 2001)
- Runtime Monitoring (2017, 2017, 2017, 2019, ..)
- Leikur og læsi í leikskólum (2011)
- Axiomatizing Finite Prefixes (1995)
- MM for Learning Stochastic Models (2021)
- Finite Equational Bases in Process Algebra (2005)
- Characteristic Formulas for Time (2000)




# “Master Thesis” by Anna

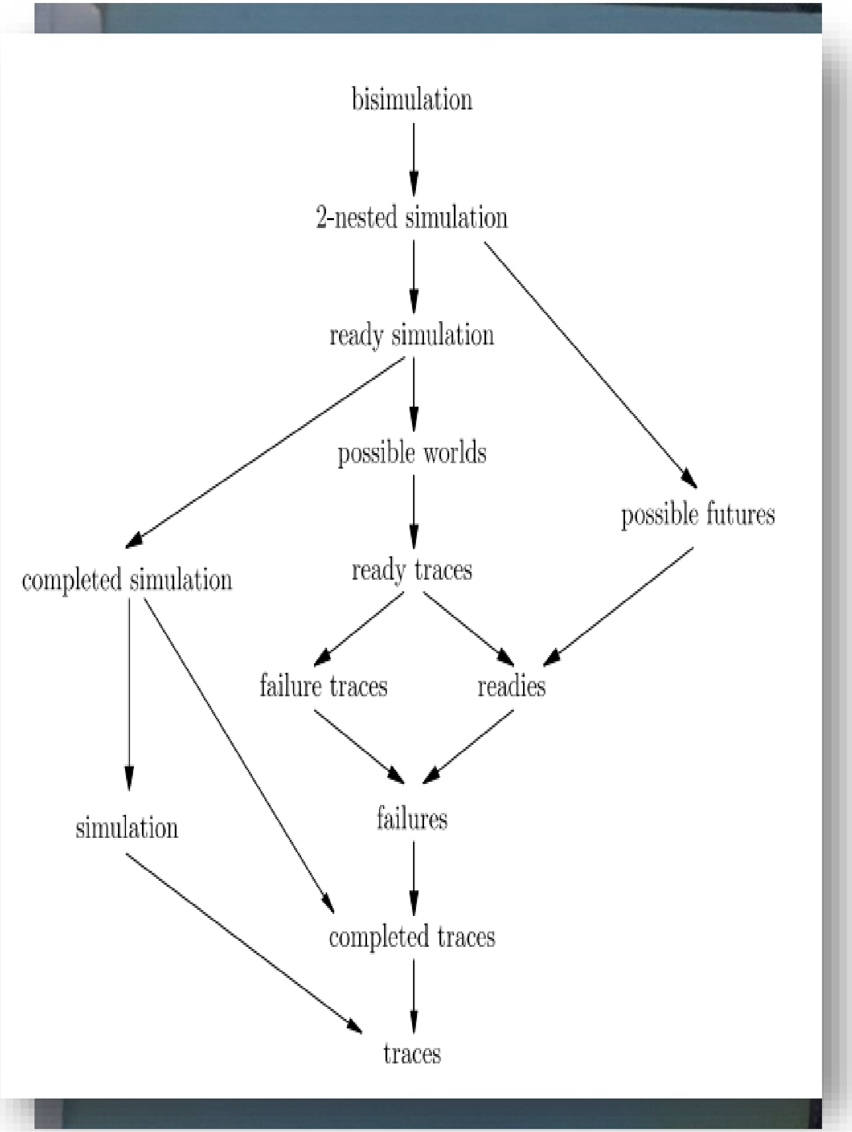

Fra Hennessy-Milner logik til
*CCS*-processer

Michael Zeeberg
Anna Ingólfsdóttir
Jens Christian Godskesen

A.U.C. I.E.S. Okt. 1987



# Characteristic Formulas by Anna




- **Michael Zeeberg, Anna Ingólfsdóttir, Jens Chr Godskesen: Fra Hennessy-Milner Logic til CCS Processer, 1987**
- Bernhard Steffen, Anna Ingólfsdóttir: Characteristic Formulae for Processes with Divergence. Inf. Comput.,1994
- Luca Aceto, Anna Ingólfsdóttir, Mikkel Lykke Pedersen, Jan Poulsen: Characteristic formulae for timed automata. ITA 2000.
- Luca Aceto, Anna Ingólfsdóttir: Characteristic Formulae: From Automata to Logic. Bulletin of the EATCS 91, 2007.
- Luca Aceto, Anna Ingólfsdóttir, Joshua Sack: Characteristic Formulae for Fixed-Point Semantics: A General Framework. EXPRESS 2009
- Luca Aceto, Dario Della Monica, Ignacio Fábregas, Anna Ingólfsdóttir: When Are Prime Formulae Characteristic? MFCS, 2015
  Luca Aceto, Dario Della Monica, Ignacio Fábregas, Anna Ingólfsdóttir: When are prime formulae characteristic? Theor. Comput. Sci. 777: 3-31 (2019)
- Luca Aceto, Antonis Achilleos, Adrian Francalanza, Anna Ingólfsdóttir: The complexity of identifying characteristic formulae. J. Log. Algebraic Methods Program, 2020
- Luca Aceto, Antonis Achilleos, Aggeliki Chalki, Anna Ingólfsdóttir: The Complexity of Deciding Characteristic Formulae in Van Glabbeek's Branching-Time Spectrum. CSL 2025

# Process Calculi

Process Calculi Ingrediences:

Models=Processes $A, B, \ldots$

Operators $+, |, ||, \ldots$

Equivalences, Preorders $\sim, \approx, \leq, \ldots$

Specifications=Logical Properties $\phi, \psi, \ldots$

Equivalence Checking

Given $A$ and $B$: $A \sim B$ ?

Model Checking:

Given $\phi$ and $A$: $A \models \phi$?

Satisfiability:

Given $\phi$: $\exists A.\, A \models \phi$ ?

Adequacy:

$A \sim B$ iff $\forall \phi.\, A \models \phi \Leftrightarrow B \models \phi$.

Characteristic Properties ($\phi_A$):

Given $A$: $B \models \phi_A$ iff $A \sim B$?

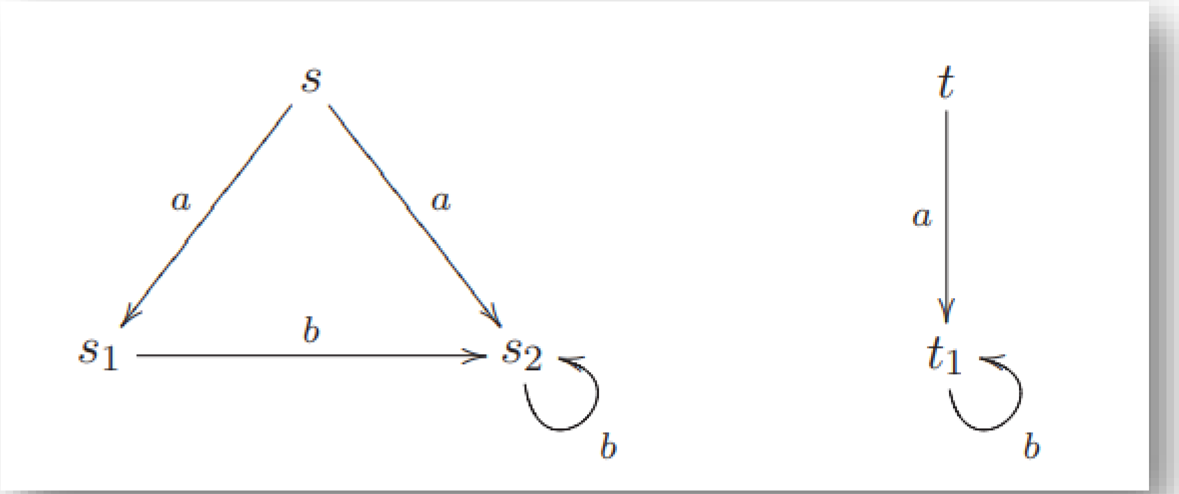
Quotienting ($\phi/B$):

Given $B, \phi$: $(A|B) \models \phi$ iff $A \models \phi/B$?



Kim Larsen [7]

# Finite State Systems



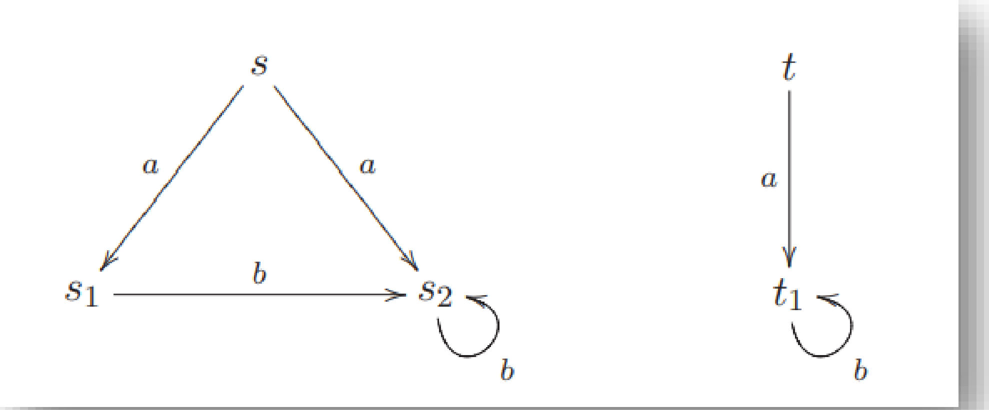

AALBORG UNIVERSITET

# Bisimulation

**Definition** A transition system is as structure $T = (S, \rightarrow, Act)$ where:

- $S$ is a finite set of states
- $Act$ is a finite set of actions
- $\rightarrow \subseteq S \times Act \times S$ is the transition relation.

Robin Milner
David Park



# Bisimulation

**Definition** A transition system is as structure $T = (S, \to, Act)$ where:

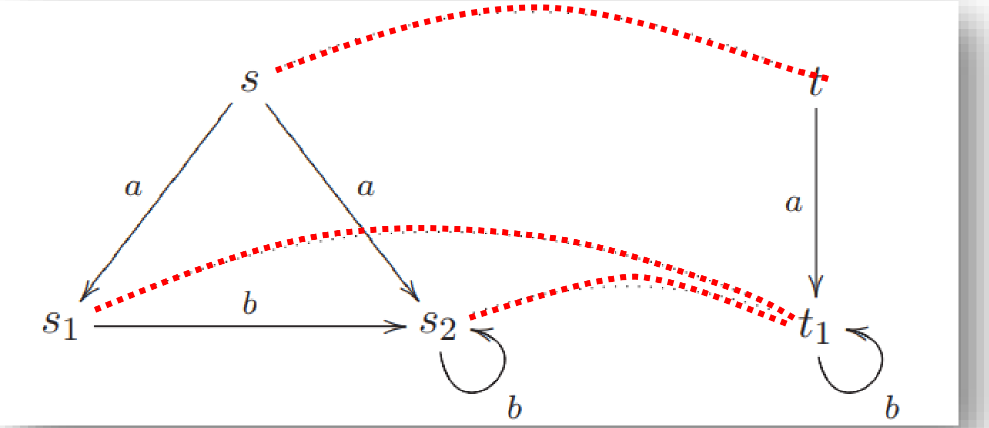
- $S$ is a finite set of states
- $Act$ is a finite set of actions
- $\to \subseteq S \times Act \times S$ is the transition relation.

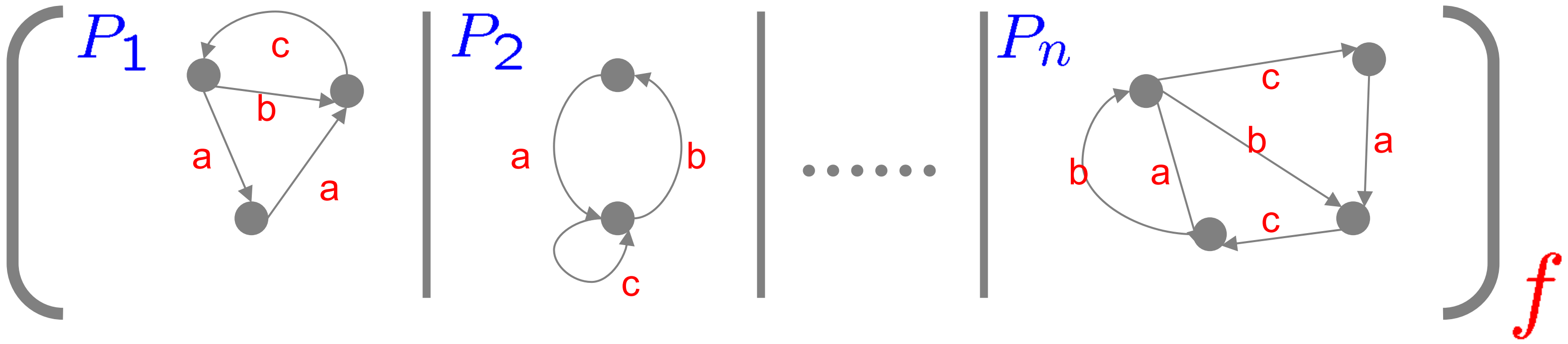
Robin Milner
David Park

**Definition** $\mathcal{B} \subseteq S \times S$ is a bisimulation iff whenever $(P, Q) \in \mathcal{B}$ then

- Whenever $P \to_a P'$ then $Q \to_a Q'$ with $(P', Q') \in \mathcal{B}$
- Whenever $Q \to_a Q'$ then $P \to_a P'$ with $(P', Q') \in \mathcal{B}$

$P \sim Q$ if and only if $(P, Q) \in \mathcal{B}$ for some bisimulation $\mathcal{B}$.






Synchronization function:

$f : (Act \cup \{0\})^n \rightharpoonup Act$

## Semantics

$$\frac{[P_i \xrightarrow{a_i} P_i'] \quad i{=}1..n}{(P_1,\ldots,P_n)[f] \xrightarrow{a} (P_1',\ldots,P_n')[f]} \quad f(a_1,\ldots,a_n) = a$$

where $P_i \xrightarrow{0} P_i$

**Examples**:

$f_{inter}(0,...,a,0...) = a$

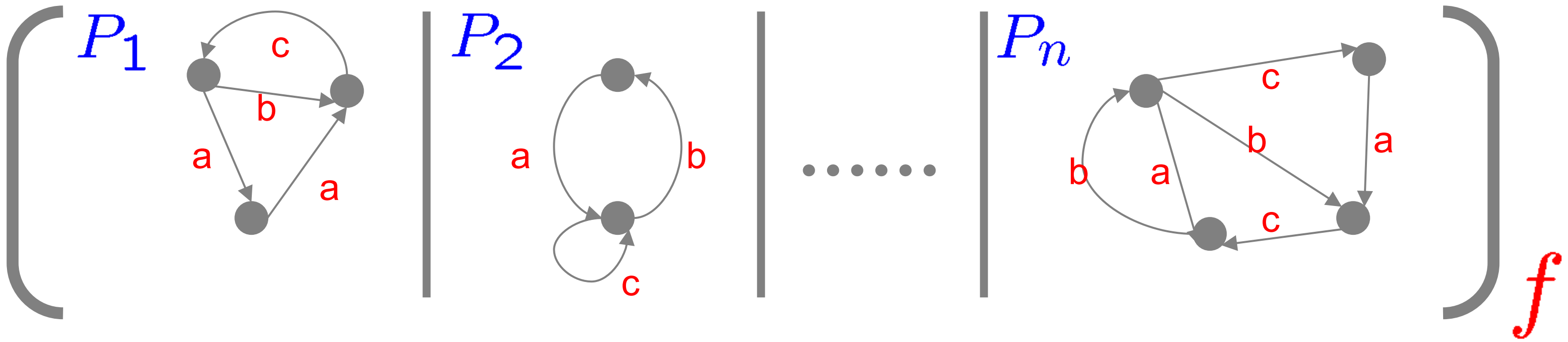
$f_{sync}(a,a,...,a) = a$

**Notation**:

$(P_1 \,|\, \ldots \,|\, P_n)$: Interleaving

$(P_1 \,||\, \ldots \,||\, P_n)$: Synchronous

# Networks of Finite Automata




Synchronization function:

$f : (Act \cup \{0\})^n \rightharpoonup Act$

## Semantics

$$\frac{[P_i \xrightarrow{a_i} P_i'] \quad i{=}1..n}{(P_1,\ldots,P_n)[f] \xrightarrow{a} (P_1',\ldots,P_n')[f]} \quad f(a_1,\ldots,a_n) = a$$

where $P_i \xrightarrow{0} P_i$

**Theorem**

Whenever $P_1 \sim Q_1 \;\ldots\ldots\ldots\; P_n \sim Q_n$

Then $(P_1,\ldots,P_n)[f] \sim (Q_1,\ldots,Q_n)[f]$

# Modal Logic

Hennessy-Milner Logic

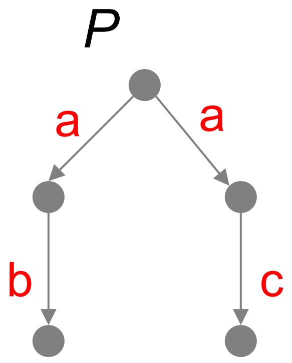
**Syntax:**

$$\phi \ ::= \ \mathsf{tt} \mid \mathsf{ff} \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \langle a \rangle \phi \mid [a]\phi$$

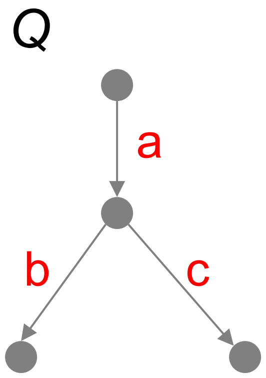
**Semantics:**

$$P \models \langle a \rangle \phi \text{ iff } \exists P'. P \xrightarrow{a} P' \wedge P' \models \phi$$
$$P \models [a]\phi \text{ iff } \forall P'. P \xrightarrow{a} P' \Rightarrow P' \models \phi$$

**Example:**




$[a]\langle b \rangle \mathsf{tt}$

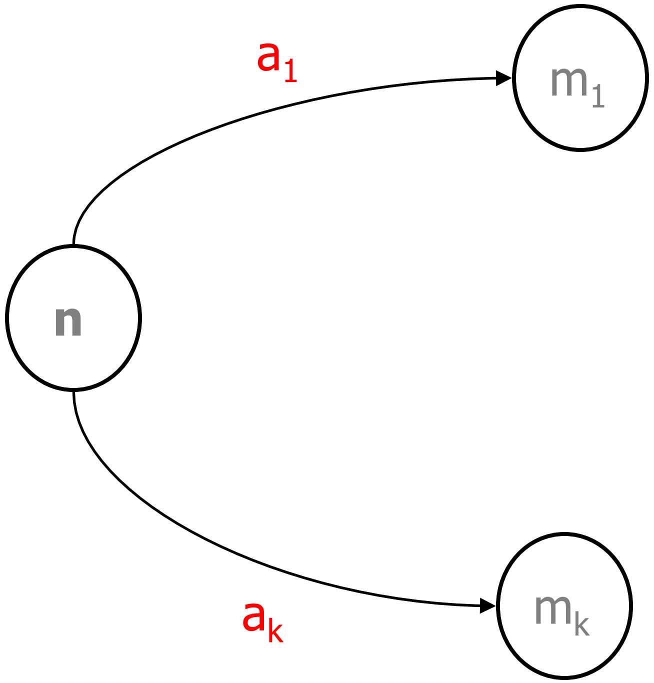



**Adequacy Theorem**

$$P \sim Q$$
if and only if
$$\forall \phi. P \models \phi \Leftrightarrow Q \models \phi$$

# Characteristic Property

*for finite state automata*

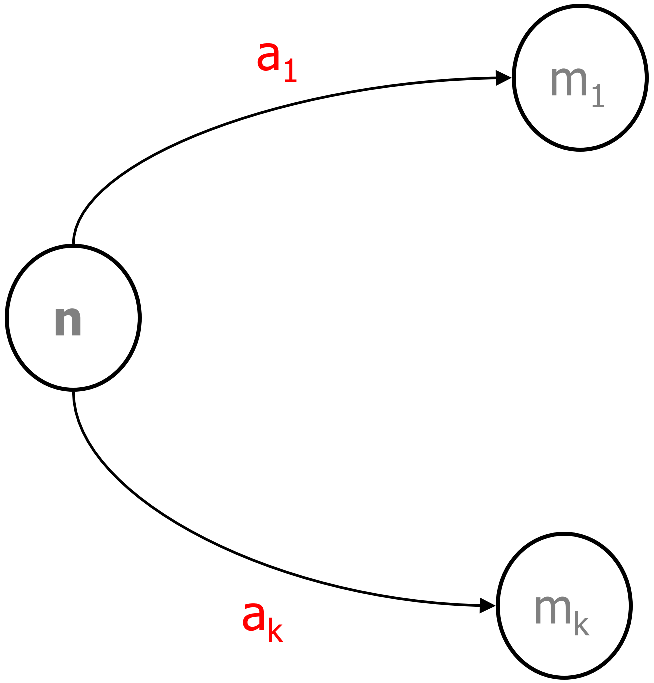



Graf&Sifakis'87
Zeeberg&Ingolfsdottir&Godskesen'87
Ingolfsdottir&Steffen'94

# Characteristic Property

*for finite state automata*

Given $A$: $\exists \phi_A . B \models \phi_A$ iff $A \sim B$ ?



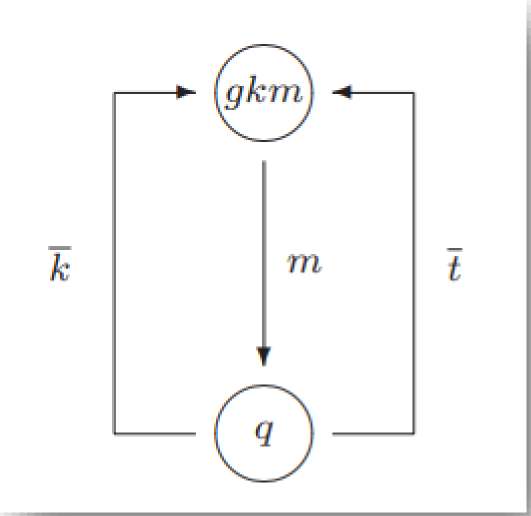

$$\phi_n \quad = \quad \bigwedge_i \langle a_i \rangle \phi_{m_i} \wedge \bigwedge_a [a] \Big( \bigvee_{i.a_i = a} \phi_{m_i} \Big)$$

Graf&Sifakis'87
Zeeberg&Ingolfsdottir&Godskesen'87
Ingolfsdottir&Steffen'94

# Characteristic Property

*for finite state automata*

Given $A$: $\exists \phi_A . B \models \phi_A$ iff $A \sim B$ ?




$$\phi_n = \bigwedge_i \langle a_i \rangle \phi_{m_i} \wedge \bigwedge_a [a]\Big(\bigvee_{i.a_i=a} \phi_{m_i}\Big)$$

$$X_{gkm} \equiv \langle m \rangle X_q \wedge [m] X_q \wedge [\{\bar{t}, \bar{k}\}] \mathit{ff},$$

$$X_q \equiv \langle \bar{t} \rangle X_{gkm} \wedge \langle \bar{k} \rangle X_{gkm} \wedge [\{\bar{t}, \bar{k}\}] X_{gkm} \wedge [m] \mathit{ff}.$$

Graf&Sifakis'87
Zeeberg&Ingolfsdottir&Godskesen'87
Ingolfsdottir&Steffen'94

# Timed Systems

# Timed Automata

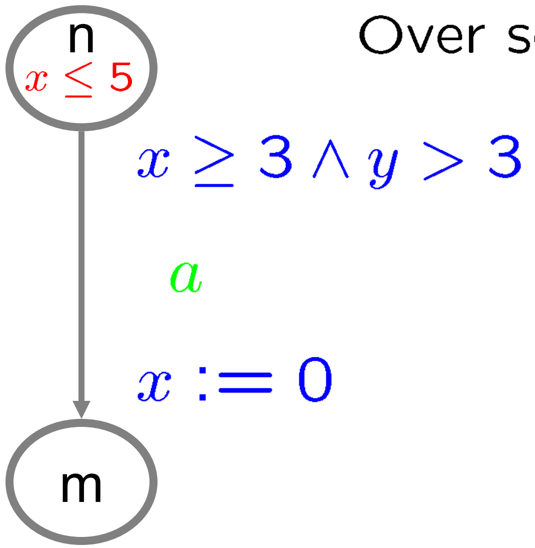
Over set of clocks $C$.

Invariants

Guard

Action

Reset




## Semantics

**States:** $(n, \nu)$ where $\nu : C \longrightarrow$ R.

**Transitions:**

Delay: $(n, x = 0, y = \pi) \xrightarrow{\epsilon(\pi)} (n, x = \pi, y = 2\pi)$

Action: $(n, x = \pi, y = 2\pi) \xrightarrow{a} (m, x = 0, y = 2\pi)$

# Timed Logic $\mathcal{L}_\nu$

Over formula clocks $K$.

**Syntax**

$$
\begin{aligned}
\phi \quad ::= \quad & tt \mid ff \mid Z \mid \\
& \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \\
& \langle a \rangle \phi \mid [a]\phi \mid \\
& \exists \phi \mid \forall \phi \mid \\
& x \text{ in } \phi \mid x \sim n \mid x - y \sim n
\end{aligned}
$$

Action Quant.

Delay Quant.

Intr. Formula Clock

Test Formula Clock

where $\sim \in \{,=,<,>,\leq,\geq\}$, $Z$ is an identifier.

**Declarations**

$$
\mathcal{E}: \quad
\begin{aligned}
Z_1 &=_\nu \phi_1 \\
Z_2 &=_\nu \phi_2 \\
&\cdots \\
Z_m &=_\nu \phi_m
\end{aligned}
$$

# Derived Operators

$\phi$ holds between $l$ and $u$: $x$ in $\exists(l \leq x \leq u \wedge \phi)$

Invariantly $\phi$: $X =_{\nu} \phi \wedge \bigwedge_{a \in A}[a]X \wedge \forall X$

$\phi$ Until $\psi$: $X =_{\nu} \psi \vee (\phi \wedge \bigwedge_{a \in A}[a]X \wedge \forall X)$

$\phi$ $\text{Until}_{\leq t}$ $\psi$: $x$ in $((\phi \wedge x \leq t)$ Until $\psi)$

# Semantics

**Interpretation**

$$\langle (n, v), u \rangle \models \phi$$

Formula over K

State of TA over C

Time assignment over K

**Semantics**

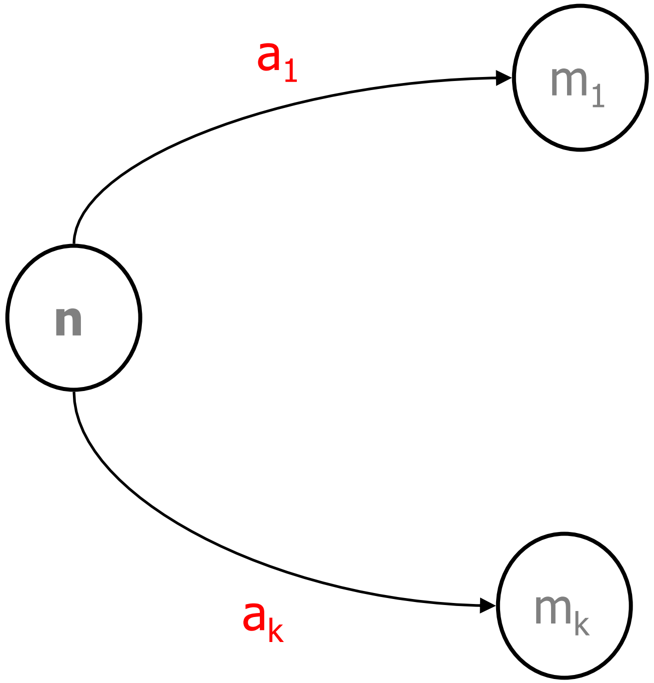
$$\langle (n, v), u \rangle \models \langle a \rangle \phi \text{ iff}$$
$$\exists (n, v) \xrightarrow{a} (n', v') \text{ st. } \langle (n', v'), u \rangle \models \phi$$

$$\langle (n, v), u \rangle \models \exists \phi \text{ iff}$$
$$\exists d \in \mathrm{R} \text{ st. } \langle (n, v + d), u + d \rangle \models \phi$$

# Characteristic Property

*for finite state automata*

Given $A$: $\exists \phi_A . B \models \phi_A$ iff $A \sim B$ ?




$$\phi_n \; = \; \bigwedge_i \langle a_i \rangle \phi_{m_i} \wedge \bigwedge_a [a] (\bigvee_{i.a_i = a} \phi_{m_i})$$

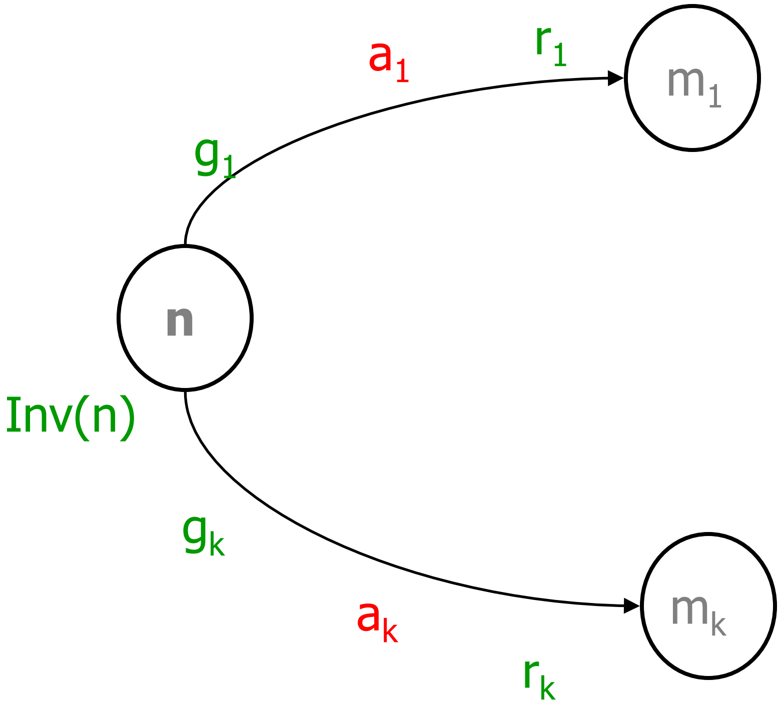
Graf&Sifakis'87
Zeeberg&Ingolfsdottir&Godskesen'87
Ingolfsdottir&Steffen'94

# Characteristic Property

*for timed automata*

**Larsen, Laroussinie, Weise, 1995**

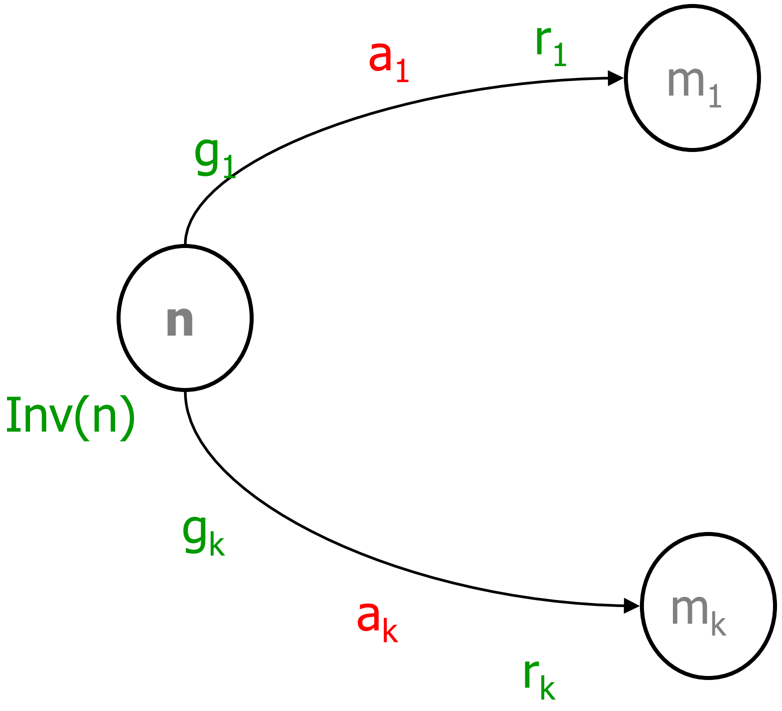
Aceto, Ingólfsdóttir, Pedersen, Poulsen, 2000

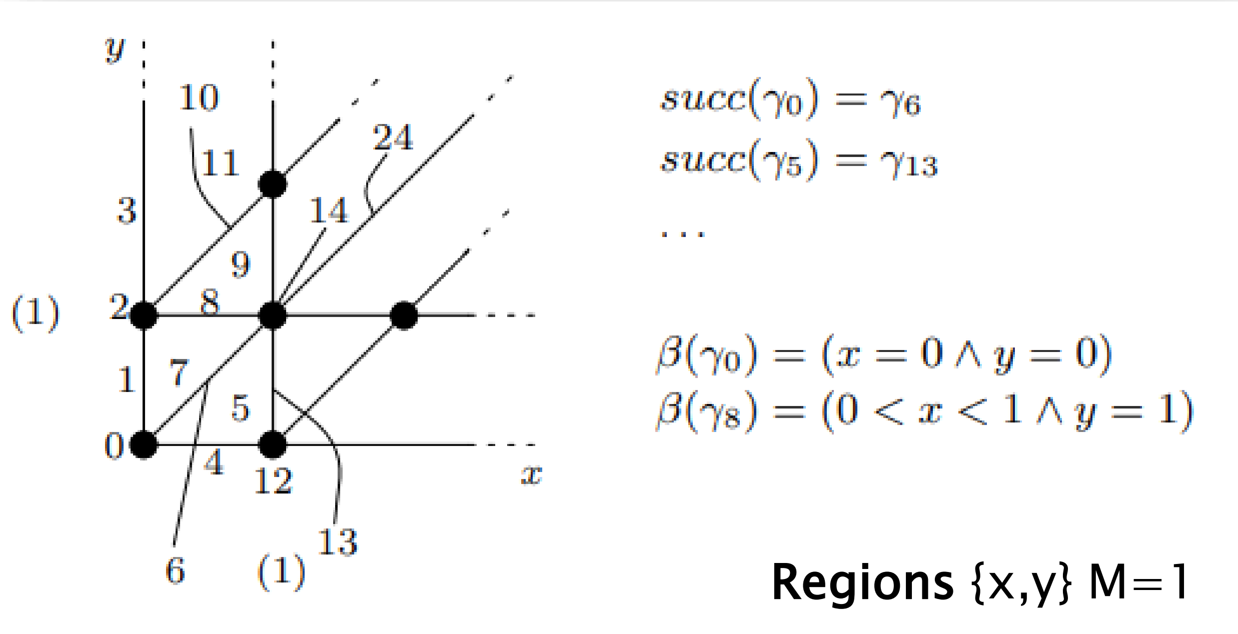



IDEA: Automata clocks become formula clocks

# Characteristic Property
*for timed automata*

**Larsen, Laroussinie, Weise, 1995**
Aceto, Ingólfsdóttir, Pedersen, Poulsen, 2000




# regions grow explonentially in #clock & M

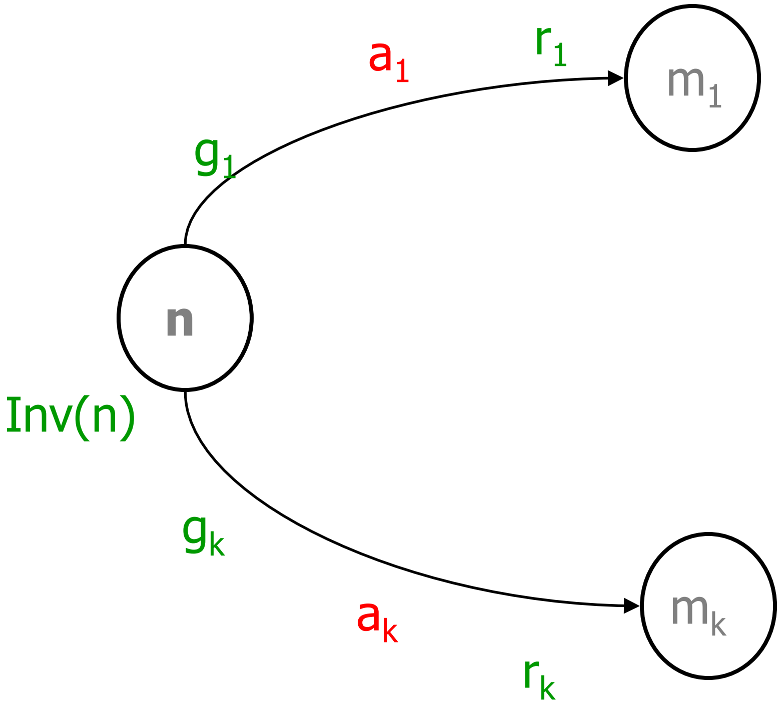
IDEA: Automata clocks become formula clocks

# Characteristic Property

*for timed automata*

**Larsen, Laroussinie, Weise, 1995**

Aceto, Ingólfsdóttir, Pedersen, Poulsen, 2000




$$\Phi(\eta,\gamma) \stackrel{\text{def}}{=} \left( \bigwedge_{e\in E(\eta,\gamma)} \langle a_e\rangle \left(r_e \text{ in } \Phi(\eta'_e, r_e(\gamma))\right) \wedge \bigwedge_a [a]\left(\bigvee_{e\in E(\eta,\gamma,a)} \left(r_e \text{ in } \Phi(\eta'_e, r_e(\gamma))\right)\right) \wedge \forall\left(\bigwedge_{l=0..l_\gamma} \beta(\gamma^l) \Rightarrow \Phi(\eta,\gamma^l)\right)\right)$$

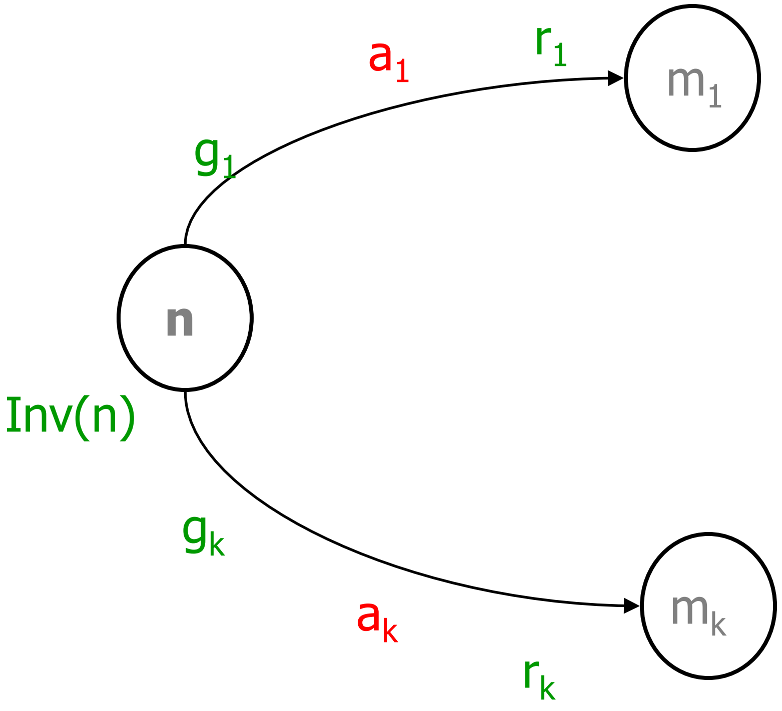
# regions grow explonentially in #clock & M

IDEA: Automata clocks become formula clocks

# Characteristic Property

*for timed automata*

**Larsen, Laroussinie, Weise, 1995**
**Aceto, Ingólfsdóttir, Pedersen, Poulsen, 2000**




$$\phi_n =$$
$$\forall[\mathrm{Inv}(n) \wedge$$
$$\bigwedge_i g_i \Rightarrow (\langle a_i \rangle r_i \text{ in } \phi_{m_i}) \wedge$$
$$\bigwedge_a [a](\bigvee_{i.a_i=a}(r_i \text{ in } \phi_{m_i}) \wedge g_i))$$
$$]$$
$$\exists \mathrm{Inv}(n)\,\mathrm{boarder}$$

$$(l,u) \sim (n,v) \text{ iff } \langle (l,u), v \rangle \models \phi_n$$

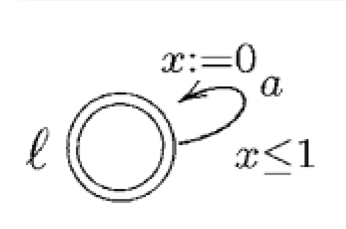
IDEA: Automata clocks become formula clocks

# Characteristic Property

*for timed automata*

**Larsen, Laroussinie, Weise, 1995**

**Aceto, Ingólfsdóttir, Pedersen, Poulsen, 2000**




$$X_\ell \stackrel{\max}{=} (y \leq 1 \Rightarrow (\langle a \rangle y \ \underline{\mathtt{in}}\ X_\ell)) \\ \wedge [a](y \leq 1 \wedge (y \ \underline{\mathtt{in}}\ X_\ell)) \\ \wedge \forall\!\!\forall X_\ell .$$

$$\begin{aligned} \phi_n \ = \ & \\ & \forall[\mathsf{Inv}(n) \wedge \\ & \textstyle\bigwedge_i g_i \Rightarrow (\langle a_i \rangle r_i \ \mathsf{in}\ \phi_{m_i}) \wedge \\ & \textstyle\bigwedge_a [a](\bigvee_{i.a_i=a}(r_i \ \mathsf{in}\ \phi_{m_i}) \wedge g_i)) \\ & ] \\ & \exists \mathsf{Inv}(n) \mathsf{boarder} \end{aligned}$$

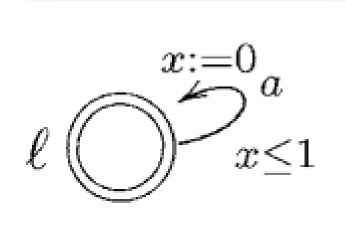
$$(l, u) \sim (n, v) \ \text{iff} \ \langle (l, u), v \rangle \models \phi_n$$

IDEA: Automata clocks become formula clocks

# Characteristic Property

*for timed automata*

**Larsen, Laroussinie, Weise, 1995**
**Aceto, Ingólfsdóttir, Pedersen, Poulsen, 2000**




$$X_\ell \overset{\max}{=} (y \leq 1 \Rightarrow (\langle a \rangle y \ \underline{\text{in}}\ X_\ell)) \\ \wedge [a](y \leq 1 \wedge (y \ \underline{\text{in}}\ X_\ell)) \\ \wedge \forall\!\!\!\forall X_\ell.$$

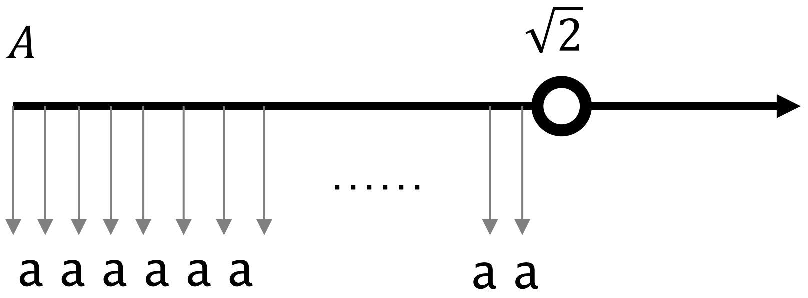
$$\phi_n = \\ \forall[\mathrm{Inv}(n) \wedge \\ \textstyle\bigwedge_i g_i \Rightarrow (\langle a_i \rangle r_i \text{ in } \phi_{m_i}) \wedge \\ \textstyle\bigwedge_a [a](\bigvee_{i.a_i=a}(r_i \text{ in } \phi_{m_i}) \wedge g_i)) \\ ] \\ \exists \mathrm{Inv}(n)\text{boarder}$$

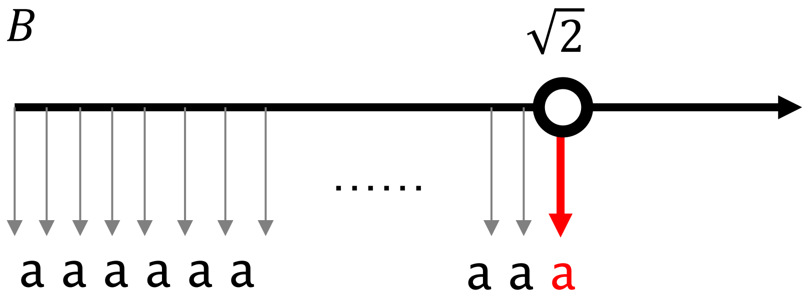
Timed (bi)similarity
Timed ready simulation
Faster–than bisimilarity
Timed Trace Inclusion

$$(l, u) \sim (n, v) \text{ iff } \langle (l, u), v \rangle \models \phi_n$$

IDEA: Automata clocks become formula clocks

# Adequacy ☹



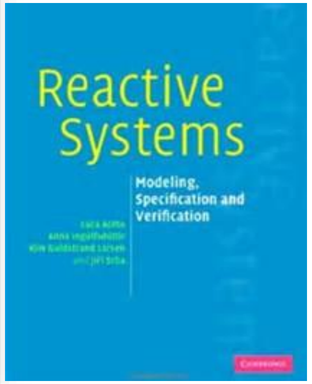

$\neg(A \sim B)$ but

$\forall \phi.\ A \models \phi \quad \Leftrightarrow \quad B \models \phi$

**Exercise 12.12 (For the keenest)** *Show the claim made in the above proof. To this end, you might find it useful to begin by proving the claim by induction on the structure of formulae, assuming the following auxiliary statements:*

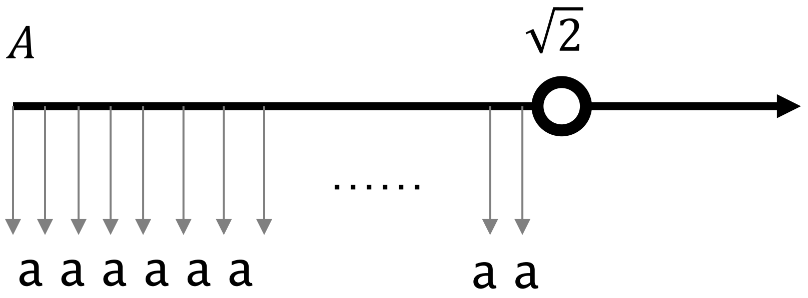
1. $(A, \sqrt{2})$ *and* $(B, d)$ *are timed bisimilar for each* $d > \sqrt{2}$*;*
2. *for each* $d, e > \sqrt{2}$ *the states* $(A, d)$ *and* $(B, e)$ *are timed bisimilar; and*
3. *for each* $d < \sqrt{2}$*, for clock valuations* $u, u'$ *and for each formula* $F$*,* $((A, \sqrt{2}), u) \models F$ *and* $((A, d), u') \models F$ *imply* $((B, \sqrt{2}), u) \models F$*.*

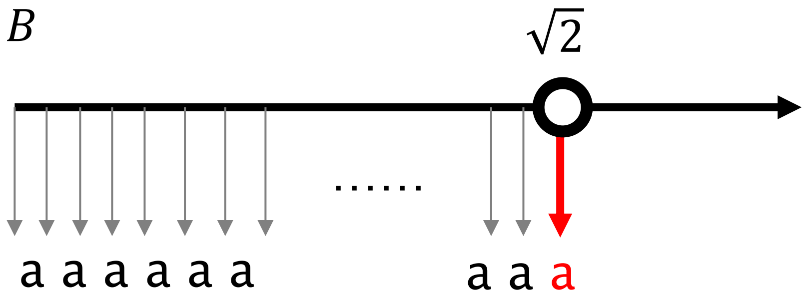
*Next you should proceed to establish each of the above auxiliary statements. For the last statement, use structural induction on* $F$*.* ♦



# Adequacy ☺

**MFPS2014**




$$\phi = \text{\forall\!\!\!\forall}(x = 2 \to [a]\bot)$$
$$i = [x = (2 - \sqrt{2})]$$

$(A, i) \models \phi \quad (B, i) \not\models \phi$

TML

$\mathcal{L}$: $\quad \phi ::= \bot \mid x \trianglelefteq r \mid \phi \to \phi \mid [a]\phi \mid \text{\forall\!\!\!\forall}\, \phi \mid \forall x.\, \phi$

where: $r \in \mathbb{Q}_{\geq 0}, \trianglelefteq \in \{\leq, \geq\}, x \in \mathcal{K}$

Samy Jaziri, L, Radu Mardare, Bingtian Xue, 2014

### Semantics

$M, m, i \models \forall x.\phi$ iff

for any $t \in \mathbb{R}_{\geq 0}, M, m, i[x \mapsto t] \models \phi$

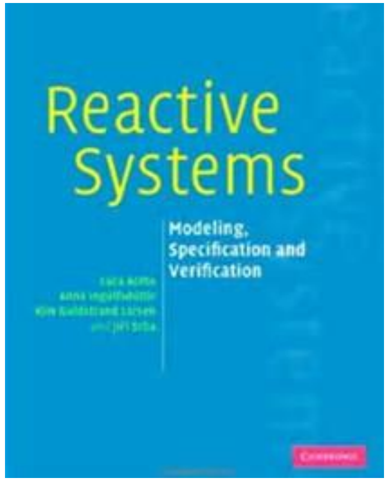
### Theorem (Adequacy)

$m \sim m'$ iff for any $\phi$ and $i$,

$M, m, i \models \phi \Leftrightarrow M, m', i \models \phi$

# Summary & Next

| | Finite State Systems | Timed Systems | Probabilistic Systems | Quantum Systems |
|---|---|---|---|---|
| Model Checking XML+rec=> XCTL | P Y | PSPACE Y | P N | y |
| Adequacy | Y | N (Y when modifying logic) | Y | Y |
| Characteristic Property | Y | Y | Y | ? |
| Quotient | Y | Y | N (Y when extending logic) | ? |
| Finite Model Property | Y | N | Y (N for PCTL) | ? |
| Satisfiability (decidability) | Y | N (Y restricting #cl & max const) | Y (? PCTL) | ? |
| Validity (axiom.) | Y (Kozen) | Y | Y | ? |




2nd Edition


Giorgio


Giovanni


Max


Jens Chr


Elli

# Congratulation & Best Wishes Kim & Merete