Topics in Timed Automata

B. Srivathsan

RWTH-Aachen

Software modeling and Verification group

System

Specification

$$\mathcal{L}(A) \subseteq \mathcal{L}(B)$$

Is $\mathcal{L}(A) \cap \overline{\mathcal{L}(B)}$ empty?

System *Specification*

$$\mathcal{L}(A) \subseteq \mathcal{L}(B)$$

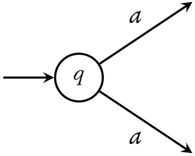
$$\updownarrow$$

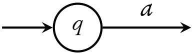
Is $\mathcal{L}(A) \cap \overline{\mathcal{L}(B)}$ empty?

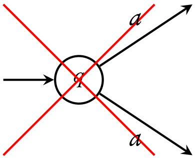
first ***determinize*** B

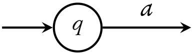
Lecture 2:

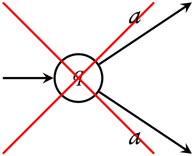
Determinizing timed automata

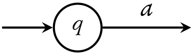

a
q
a

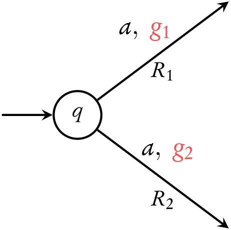

q
a

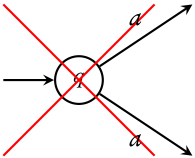

a
q
a

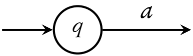

q
a

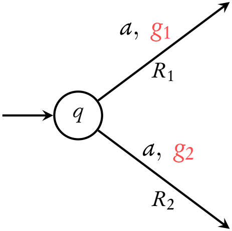

a
q
a


q
a


a, g_1
R_1
q
a, g_2
R_2



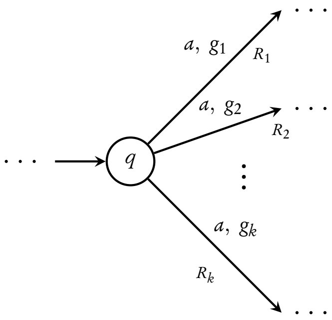




g_1 and g_2 should be mutually exclusive

For **every** (q, v) there is **only one** choice

Deterministic Timed Automata



$g_i \wedge g_j$ is **unsatisfiable**

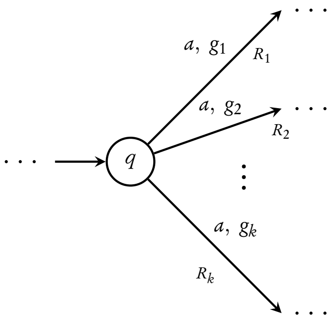
complete if

$g_1 \vee g_2 \vee \ldots g_k = \top$

A theory of timed automata

R. Alur and D. Dill, TCS'90

Deterministic Timed Automata



$g_i \wedge g_j$ is **unsatisfiable**

complete if

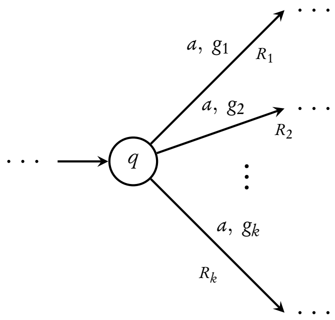
$g_1 \vee g_2 \vee \ldots g_k = \top$

+ **single initial** state

A theory of timed automata

R. Alur and D. Dill, TCS'90

Deterministic Timed Automata



$g_i \wedge g_j$ is

unsatisfiable

complete if

$g_1 \vee g_2 \vee \dots g_k = \top$

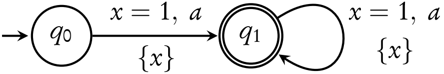
$+$ **single initial** state

Unique run

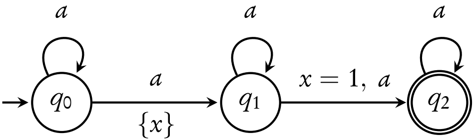
A DTA has a **unique** run on **every** timed word

A theory of timed automata

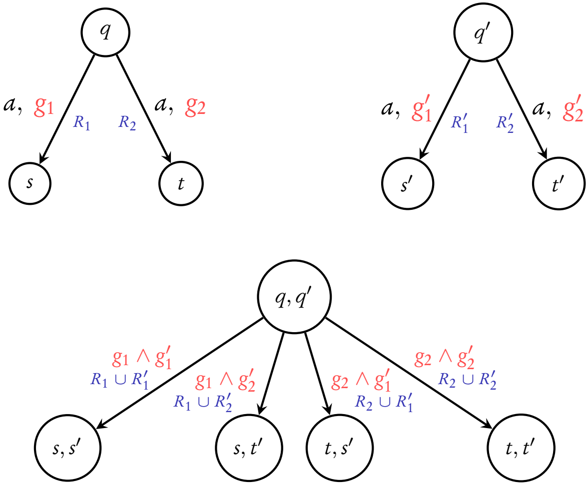
R. Alur and D. Dill, TCS'90



a DTA

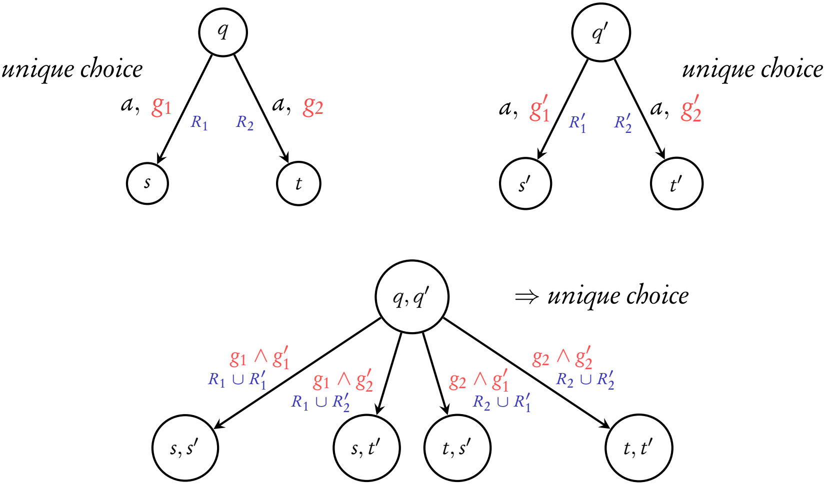


not a DTA



Accepting states: $(q_F, \star)$ and $(\star, q'_F)$ for union

(q_F, q'_F) for intersection



Accepting states: $(q_F, \star)$ and $(\star, q'_F)$ for union

(q_F, q'_F) for intersection

Theorem

DTA are **closed** under **union** and **intersection**

Complementation

Unique run

A DTA has a **unique** run on **every** timed word

$\Rightarrow$ DTA are **closed under complement**

(interchange accepting and non-accepting states)

Every DTA is a TA: $\mathcal{L}(DTA) \subseteq \mathcal{L}(TA)$

But there is a TA that **cannot be complemented** (*Lecture 1*)

$$\therefore \quad \mathcal{L}(DTA) \subset \mathcal{L}(TA)$$

DTA

Unique run

Closed under $\cup$, $\cap$, comp.

$\mathcal{L}(DTA) \subset \mathcal{L}(TA)$

Given a TA, **when** do we know if we **can determinize** it?

Given a TA, **when** do we know if we **can determinize** it?

Theorem [Finkel'06]

Given a TA, checking **if** it can be determinized is **undecidable**

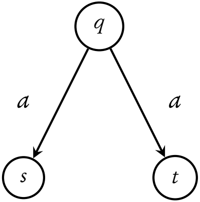
Given a TA, **when** do we know if we **can determinize** it?

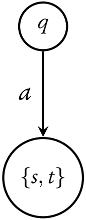
Theorem [Finkel'06]

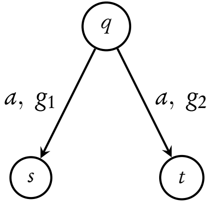
Given a TA, checking **if** it can be determinized is **undecidable**

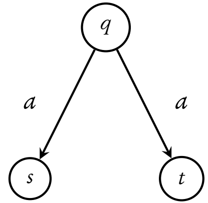
Following next: some **sufficient** conditions for determinizing

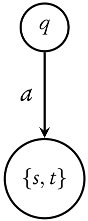

q
a
a
s
t
q
a
{s, t}

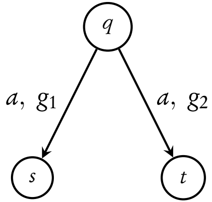

q
a
a
s
t

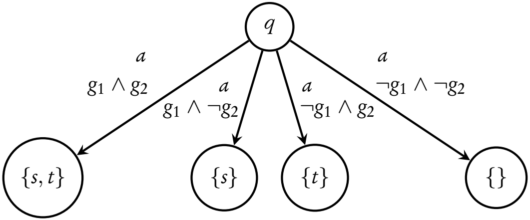

q
a
{s, t}

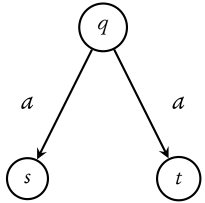

q
a, g1
a, g2
s
t

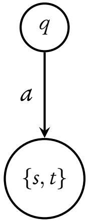

q
a
a
s
t

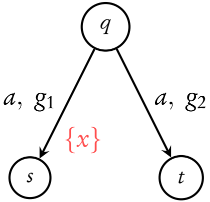

q
a
{s, t}

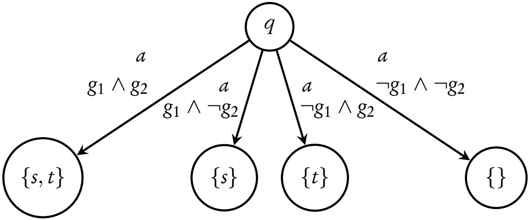

q
a, g1
a, g2
s
t

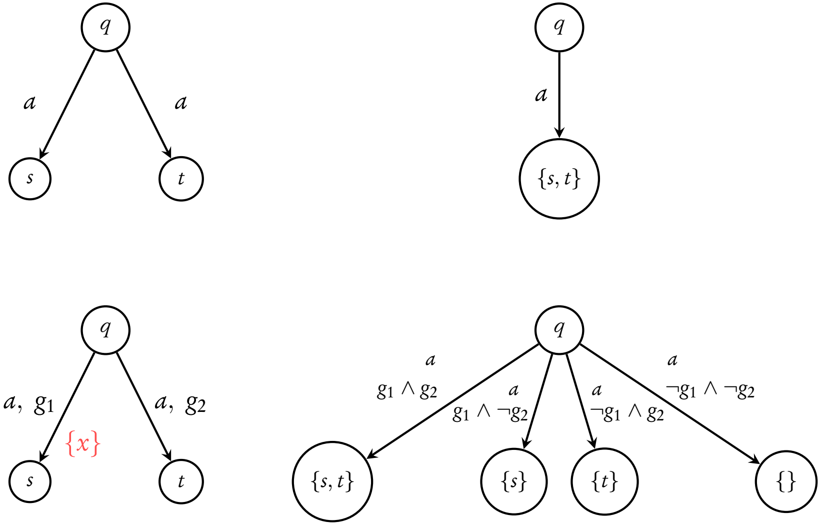

q
a
g1 ∧ g2
a
g1 ∧ ¬g2
a
¬g1 ∧ g2
a
¬g1 ∧ ¬g2
{s, t}
{s}
{t}
{}


q
a
a
s
t

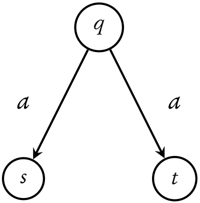

q
a
{s, t}

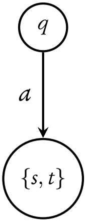

q
a, g1
a, g2
{x}
s
t

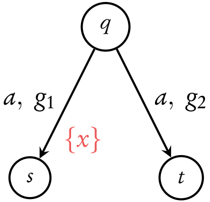

q
a
g1 ∧ g2
a
g1 ∧ ¬g2
a
¬g1 ∧ g2
a
¬g1 ∧ ¬g2
{s, t}
{s}
{t}
{}

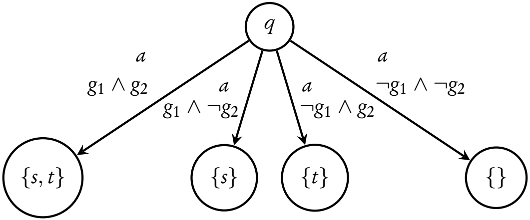


To **reset** or **not to reset**?









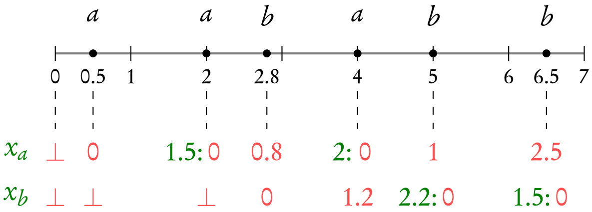
First solution:

Whenever a, reset x_a

To **reset** or **not to reset**?

Event-recording clocks: time since **last occurence** of event

$$a \quad \mapsto \quad x_a$$

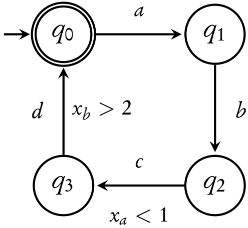


Event-clock automata: a determinizable subclass of timed automata

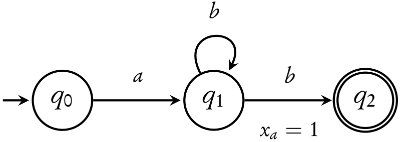
Alur, Henzinger, Fix. *TCS'99*

Event-recording automata

$\{ \ (\ (abcd)^k, \tau \ ) \mid a - c$ distance is < 1 and $b - d$ distance is $> 2\}$

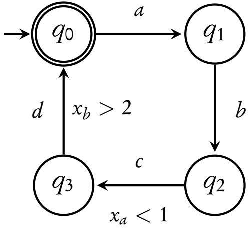


$\{ \ (ab^* b, \tau) \mid$ distance between first and last letters is $1\}$

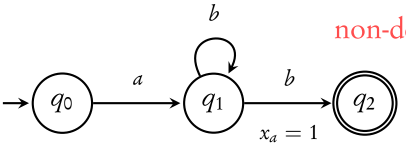


Event-recording automata

$\{ ((abcd)^k, \tau) \mid a - c \text{ distance is } < 1 \text{ and } b - d \text{ distance is } > 2\}$

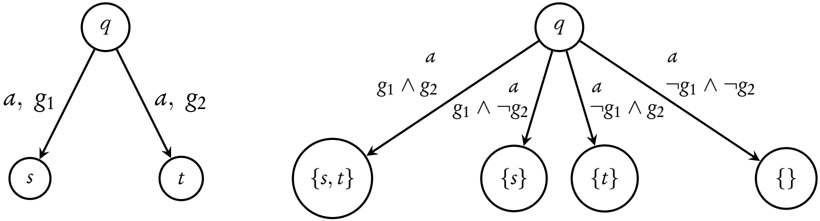


$\{ (ab^*b, \tau) \mid \text{ distance between first and last letters is } 1\}$



non-deterministic

Determinizing ERA: modified **subset** construction



exponential in the number of states

DTA

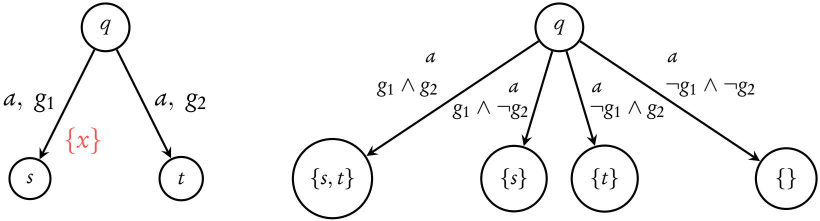
Unique run

Closed under ∪, ∩, comp.

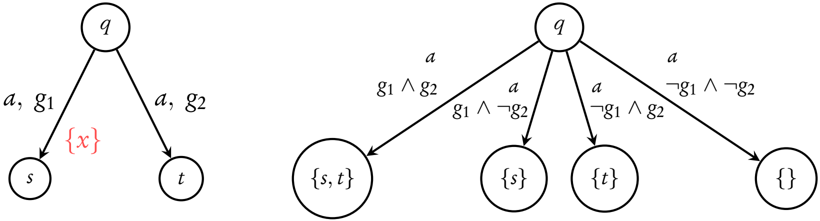
$\mathcal{L}(DTA) \subset \mathcal{L}(TA)$

Determinizable subclasses

ERA



To **reset** or **not to reset?**

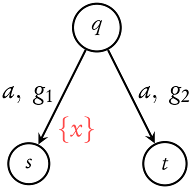


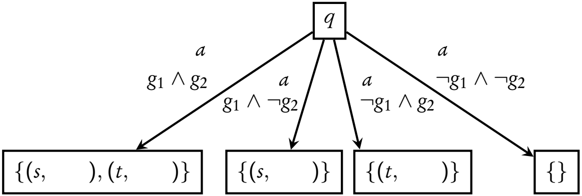
To **reset** or **not to reset**?

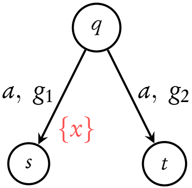
Coming next: slightly modified version of BBBB-09

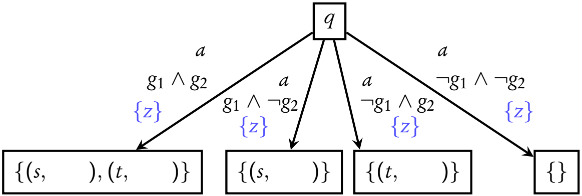
When are timed automata determinizable?

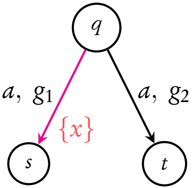
Baier, Bertrand, Bouyer, Brihaye. *ICALP'09*

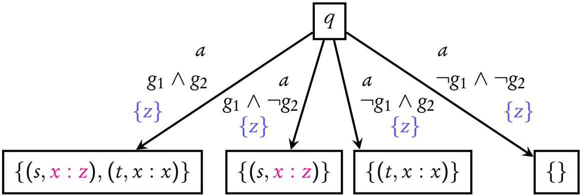

q
a, g1
{x}
a, g2
s
t

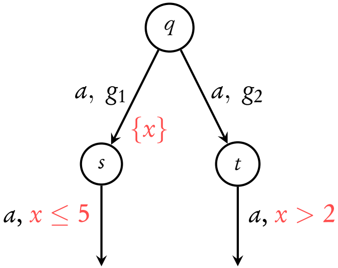

q
a
g1 ∧ g2
a
g1 ∧ ¬g2
a
¬g1 ∧ g2
a
¬g1 ∧ ¬g2
{(s,), (t,)}
{(s,)}
{(t,)}
{}

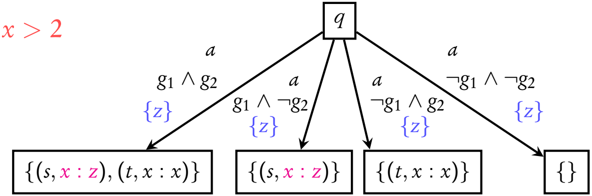

q
a, g1
{x}
a, g2
s
t

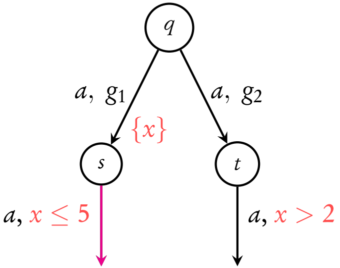

q
a
g1 ∧ g2
{z}
a
g1 ∧ ¬g2
{z}
a
¬g1 ∧ g2
{z}
a
¬g1 ∧ ¬g2
{z}
{(s,), (t,)}
{(s,)}
{(t,)}
{}

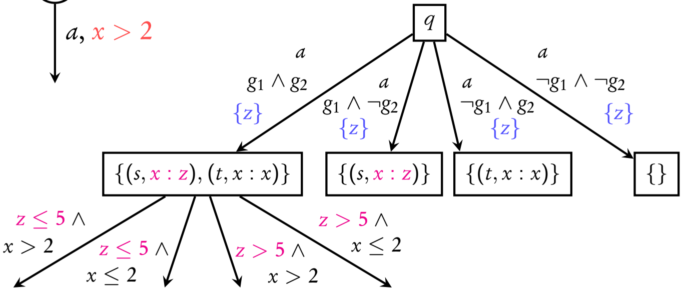

q
a, g1
{x}
a, g2
s
t

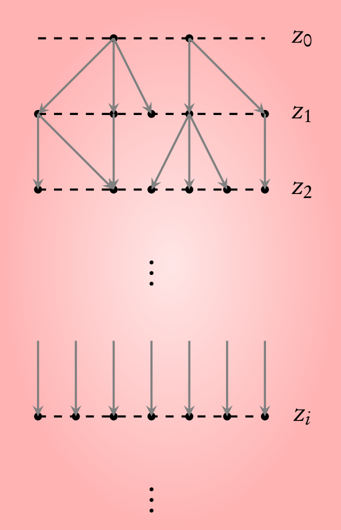

q
a
g1 ∧ g2
{z}
a
g1 ∧ ¬g2
{z}
a
¬g1 ∧ g2
{z}
a
¬g1 ∧ ¬g2
{z}
{(s, x : z), (t, x : x)}
{(s, x : z)}
{(t, x : x)}
{}


q
a, g1
{x}
a, g2
s
t
a, x ≤ 5
a, x > 2


q
a
g1 ∧ g2
{z}
a
g1 ∧ ¬g2
{z}
a
¬g1 ∧ g2
{z}
a
¬g1 ∧ ¬g2
{z}
{(s, x : z), (t, x : x)}
{(s, x : z)}
{(t, x : x)}
{}


q
a, g1
{x}
a, g2
s
t
a, x ≤ 5
a, x > 2

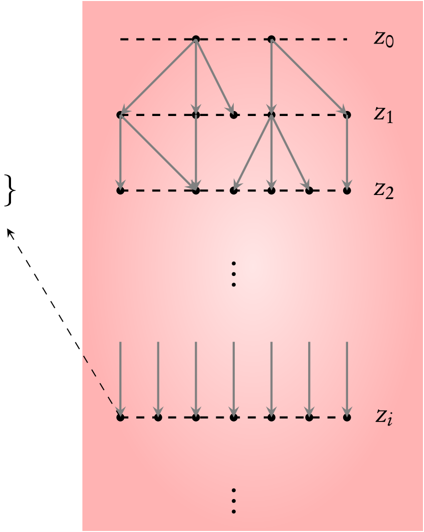

q
a
g1 ∧ g2
{z}
a
g1 ∧ ¬g2
{z}
a
¬g1 ∧ g2
{z}
a
¬g1 ∧ ¬g2
{z}
{(s, x : z), (t, x : x)}
{(s, x : z)}
{(t, x : x)}
{}
z ≤ 5 ∧
x > 2
z ≤ 5 ∧
x ≤ 2
z > 5 ∧
x > 2
z > 5 ∧
x ≤ 2



Reset a **new** clock z_i at level i

$$\{(q_1, \sigma_1), (q_2, \sigma_2), \ldots, (q_k, \sigma_k)\}$$

$$\sigma_j : X \mapsto \{z_0, \ldots, z_i\}$$

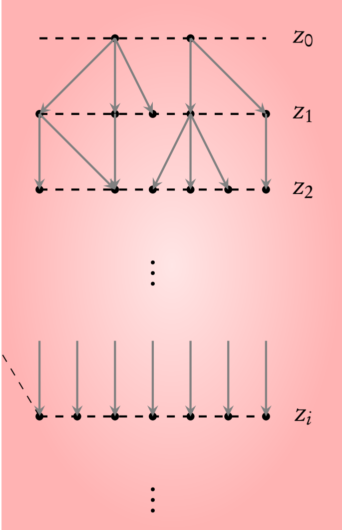


Reset a **new** clock z_i at level i

$$\{(q_1, \sigma_1), (q_2, \sigma_2), \ldots, (q_k, \sigma_k)\}$$

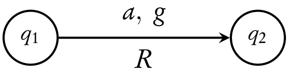
$$\sigma_j : X \mapsto \{z_0, \ldots, z_i\}$$

When do finitely many clocks suffice ?



Reset a **new** clock z_i at level i

Integer reset timed automata



Conditions:

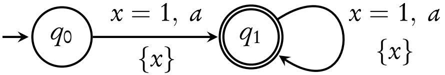
- g has **integer** constants
- R is **non-empty iff** g has some constraint $x = c$

Implication:

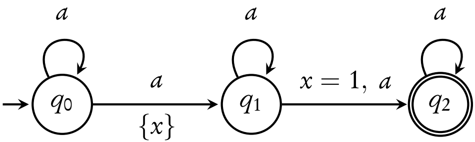
- Along a timed word, a **reset** of an IRTA happens only at **integer timestamps**

Timed automata with integer resets: Language inclusion and expressiveness

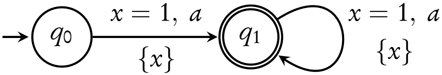
Suman, Pandya, Krishna, Manasa. *FORMATS'08*



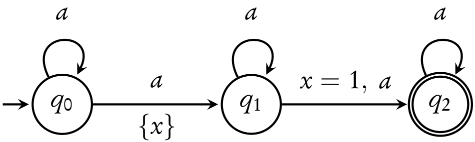
an IRTA



not an IRTA



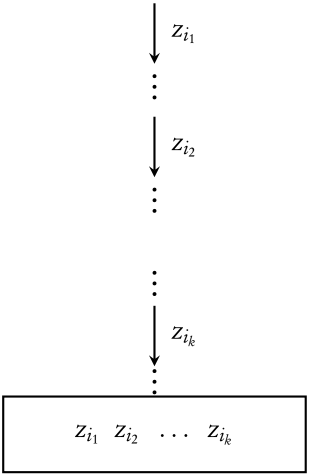
an IRTA



not an IRTA

Next: **determinizing** IRTA using the **subset construction**

M: **max constant** from among guards



active clocks

assume the semantics of timed word (w, τ) such that $\tau_1 < \tau_2 < \cdots < \tau_k$

- If $k \geq M + 1$, then $z_{i_1} > M$ (as reset is **only** in integers)
- Replace z_{i_1} with $\perp$ and **reuse** z_{i_1} further

DTA

Unique run

Closed under $\cup$, $\cap$, comp.

$\mathcal{L}(DTA) \subset \mathcal{L}(TA)$

Determinizable subclasses

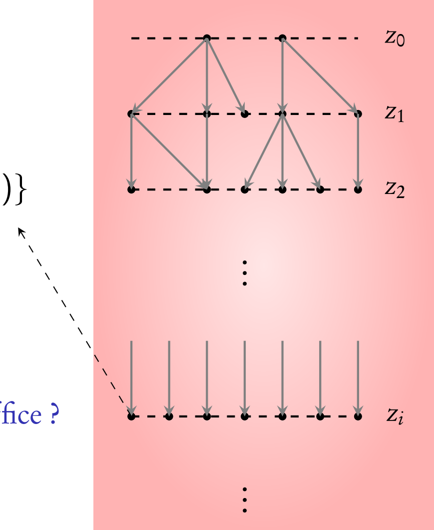
ERA

IRTA

$$\{(q_1, \sigma_1), (q_2, \sigma_2), \ldots, (q_k, \sigma_k)\}$$

$$\sigma_j : X \mapsto \{z_0, \ldots, z_i\}$$

When do finitely many clocks suffice ?

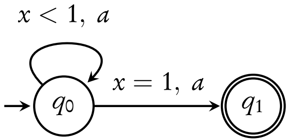


Reset a **new** clock z_i at level i

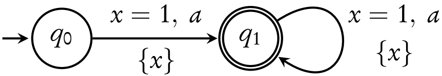
Strongly non-Zeno automata

A TA is strongly non-Zeno if there is $K \in \mathbb{N}$:

every sequence of greater than K transitions **elapses** at least **1 time unit**



not SNZ



SNZ

Theorem

Finitely many clocks **suffice** in the subset construction for strongly non-Zeno automata

(The number of clocks depends on size of region automaton...)

When are timed automata determinizable?

Baier, Bertrand, Bouyer, Brihaye. *ICALP'09*

Complexity of subset construction

$$\{(q_1, \sigma_1), (q_2, \sigma_2) \ldots (q_k, \sigma_k)\}$$

$$\sigma_j : X \mapsto \{z_0, \ldots, z_{p-1}\}$$

Complexity of subset construction

$$\{(q_1, \sigma_1), (q_2, \sigma_2) \dots (q_k, \sigma_k)\}$$

$$\sigma_j : X \mapsto \{z_0, \dots, z_{p-1}\}$$

$\sigma_j :$ __ __ __ … __ $|X|$ places

↑ p choices

Complexity of subset construction

$$\{(q_1, \sigma_1), (q_2, \sigma_2) \dots (q_k, \sigma_k)\}$$

$$\sigma_j : X \mapsto \{z_0, \dots, z_{p-1}\}$$

σ_j : — — — … — $|X|$ places

↑ p choices

$$\text{no. of } \sigma_j : \quad p^{|X|}$$

$$\text{no. of } \quad (q_j, \sigma_j) : \quad |Q| \cdot p^{|X|}$$

Complexity of subset construction

$$\{(q_1, \sigma_1), (q_2, \sigma_2) \ldots (q_k, \sigma_k)\} \qquad 2^{|Q| \cdot p^{|X|}}$$

$$\sigma_j : X \mapsto \{z_0, \ldots, z_{p-1}\}$$

$$\sigma_j : \quad \_\_ \quad \_\_ \quad \_\_ \quad \cdots \quad \_\_ \qquad |X| \text{ places}$$

$\uparrow$

p choices

$$\text{no. of } \sigma_j : \quad p^{|X|}$$

$$\text{no. of } \quad (q_j, \sigma_j) : \quad |Q| \cdot p^{|X|}$$

$\rightarrow$ **doubly exponential** in the size of initial automaton

DTA

Unique run

Closed under $\cup$, $\cap$, comp.

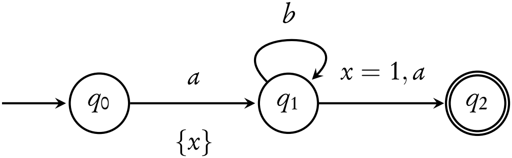
$\mathcal{L}(DTA) \subset \mathcal{L}(TA)$

Determinizable subclasses

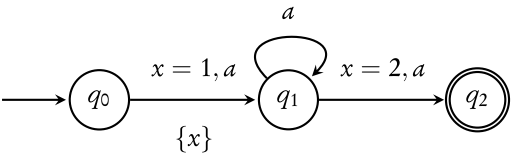
ERA

IRTA

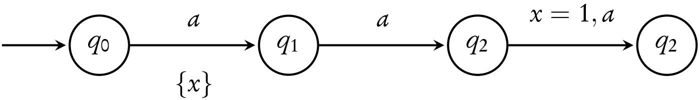
SNZ



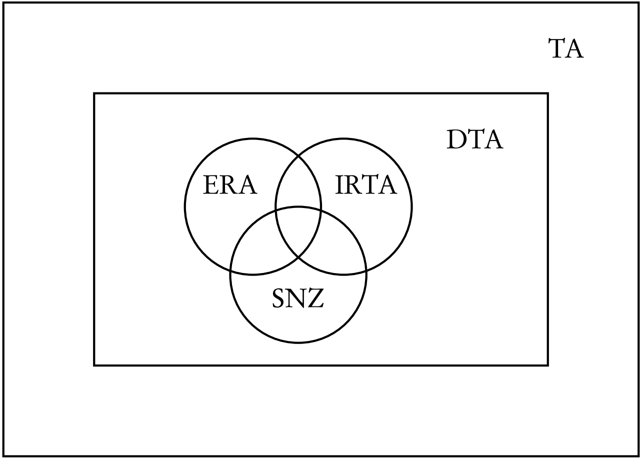
ERA ~~IRTA~~ ~~SNZ~~



~~ERA~~ IRTA ~~SNZ~~



~~ERA~~ ~~IRTA~~ SNZ


TA
DTA
ERA
IRTA
SNZ

Closure properties of ERA, IRTA, SNZ

- Union: **disjoint** union $\surd$
- Intersection: **product** construction $\surd$
- Complement: **determinize** & **interchange** acc. states $\surd$

DTA

Unique run

Closed under $\cup$, $\cap$, comp.

$\mathcal{L}(DTA) \subset \mathcal{L}(TA)$

Determinizable subclasses

ERA

IRTA

SNZ

ERA, IRTA, SNZ

Incomparable

Closed under $\cup$, $\cap$, comp.

Perspectives

Other related work:

- Event-predicting clocks (*Alur, Henzinger, Fix'99*)
- Bounded two-way timed automata (*Alur, Henzinger'92*)

For the future:

- Infinite timed words: Safra?
- Efficient algorithms