Automata for Real-time Systems

B. Srivathsan

Chennai Mathematical Institute

System *Specification*

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

$$\updownarrow$$

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

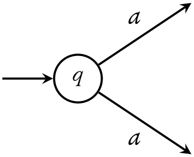
System *Specification*

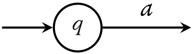
$$\mathcal{L}(A) \subseteq \mathcal{L}(B)$$

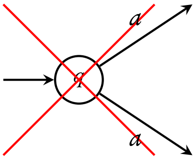
Is $\mathcal{L}(A) \cap \overline{\mathcal{L}(B)}$ empty?

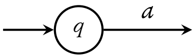
first ***determinize*** *B*

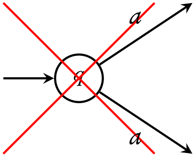
Determinizing timed automata

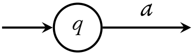

q
a
a

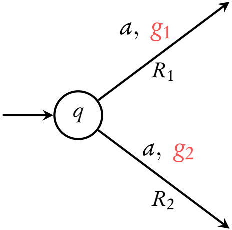

q
a

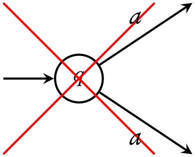

a
q
a

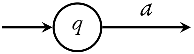

q
a

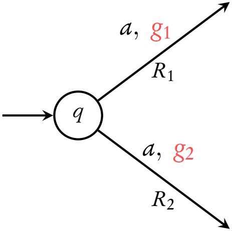

a
q
a


q
a


q
a, g1
R1
a, g2
R2



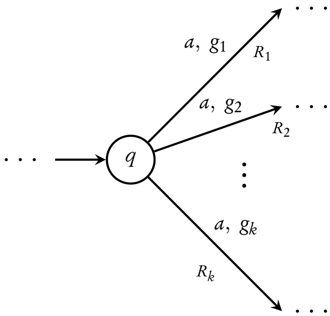




g_1 and g_2 should be mutually exclusive

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

Deterministic Timed Automata



$g_i \wedge g_j$ is

unsatisfiable

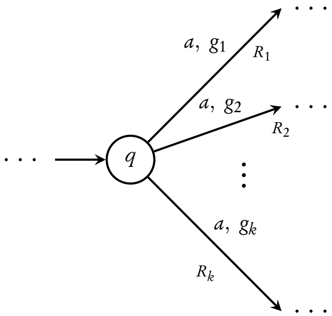
complete if

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

A theory of timed automata

R. Alur and D. Dill, TCS'94

Deterministic Timed Automata



$g_i \wedge g_j$ is

unsatisfiable

complete if

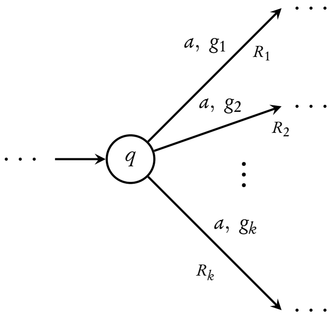
$$g_1 \vee g_2 \vee \ldots g_k = \top$$

+ **single initial state**

A theory of timed automata

R. Alur and D. Dill, TCS'94

Deterministic Timed Automata



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

complete if

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

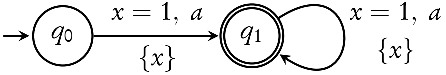
$+$ **single initial** state

Unique run

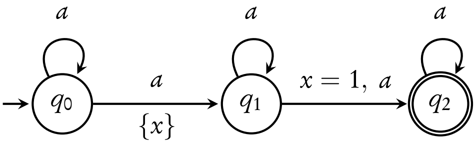
A DTA has a **unique** run on **every** timed word

A theory of timed automata

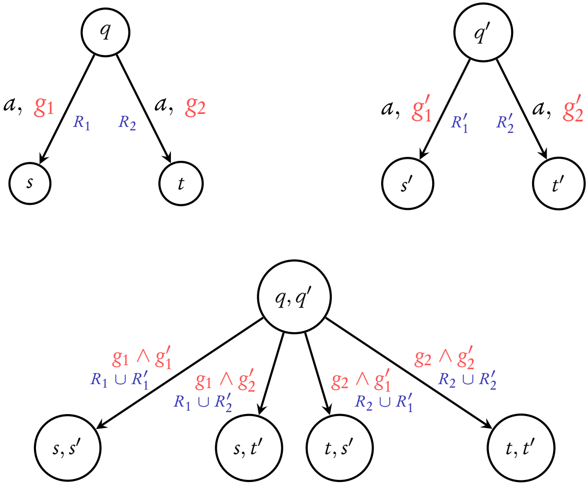
R. Alur and D. Dill, TCS'94



a DTA

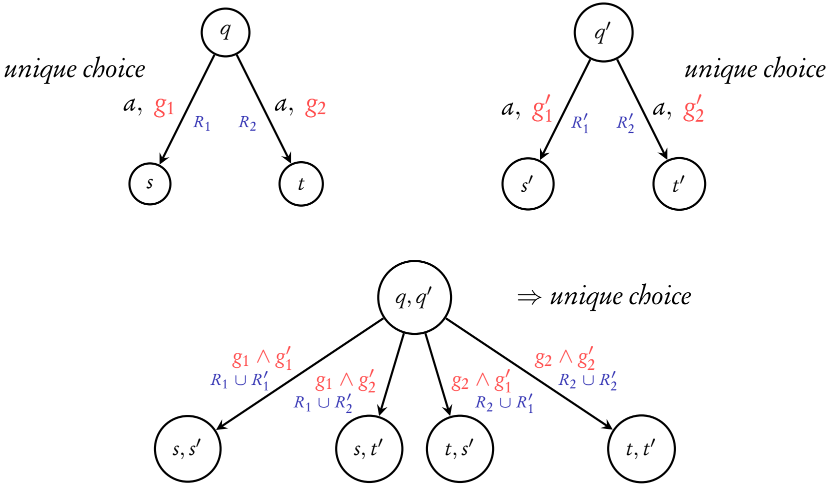


not a DTA



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** (*Previous Lecture*)

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

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]

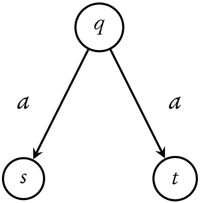
Given a TA, checking **if** it can be determinized is **undecidable**

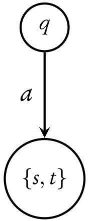
Given a TA, **when** do we know if we **can determinize** it?

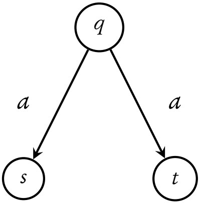
Theorem [Finkel'06]

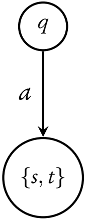
Given a TA, checking **if** it can be determinized is **undecidable**

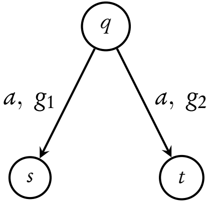
Following next: some **sufficient** conditions for determinizing

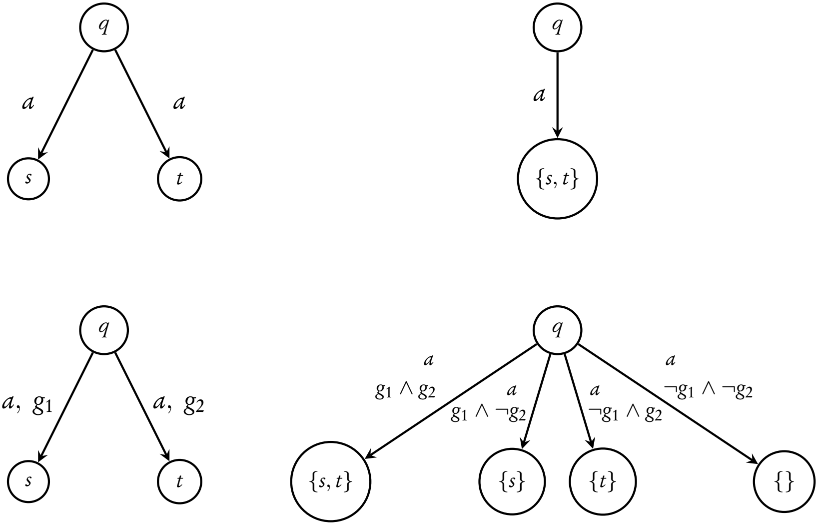

q
a
a
s
t

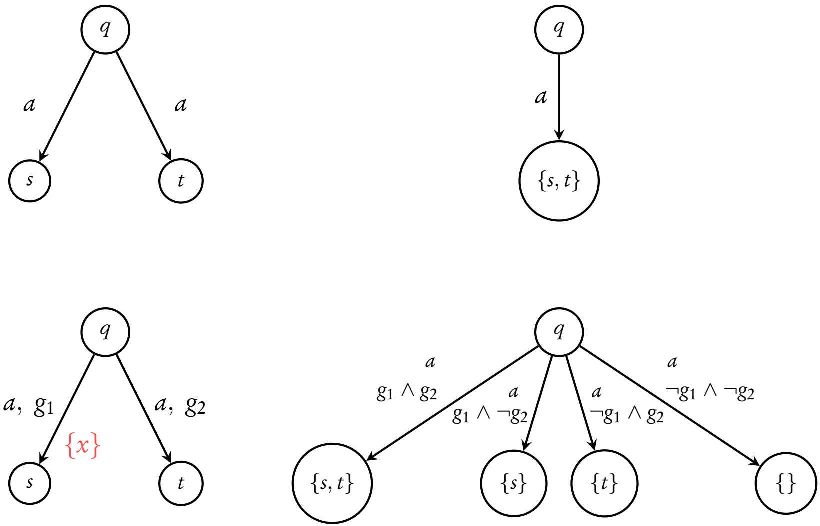

q
a
{s, t}

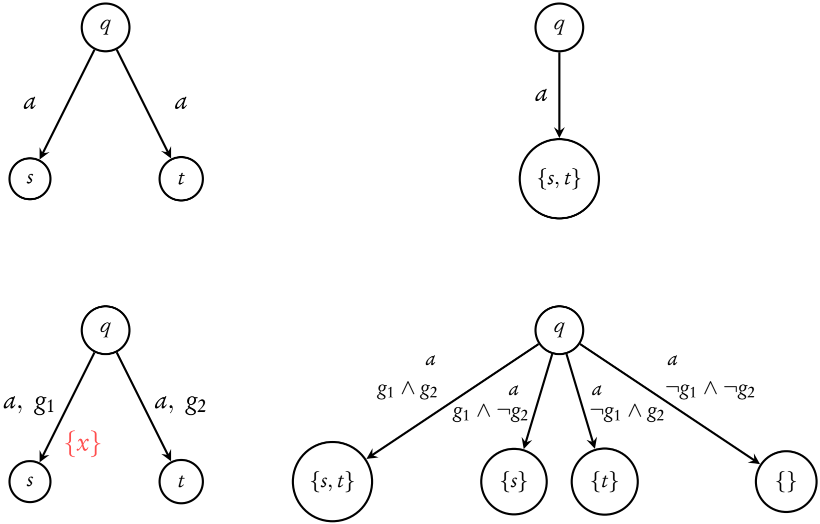

q
a
a
s
t


q
a
{s, t}

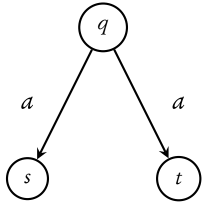

q
a, g1
a, g2
s
t

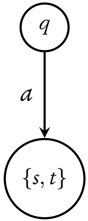

q
a
a
s
t
q
a
{s, t}
q
a, g1
a, g2
s
t
q
a
g1 ∧ g2
a
g1 ∧ ¬g2
a
¬g1 ∧ g2
a
¬g1 ∧ ¬g2
{s, t}
{s}
{t}
{}

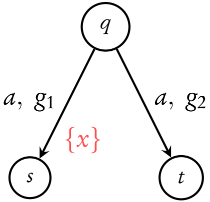

q
a
a
s
t
q
a
{s, t}
q
a, g1
a, g2
{x}
s
t
q
a
g1 ∧ g2
a
g1 ∧ ¬g2
a
¬g1 ∧ g2
a
¬g1 ∧ ¬g2
{s, t}
{s}
{t}
{}

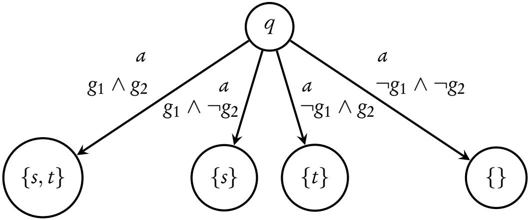


To **reset** or **not to reset**?









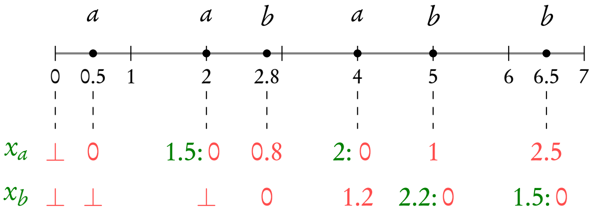
First solution:

Whenever a, reset x_a

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

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

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

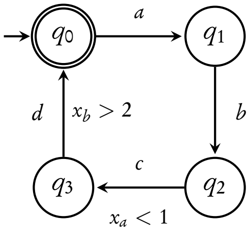


Event-clock automata: a determinizable subclass of timed automata

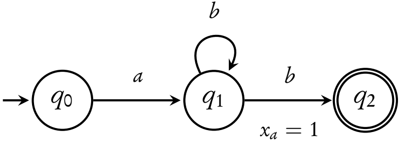
Alur, Henzinger, Fix. *TCS'99*

Event-recording automata

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

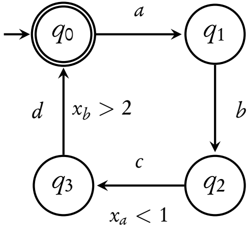


$\{\ (ab^*b, \tau)\ |\ $ distance between first and last letters is 1$\}$

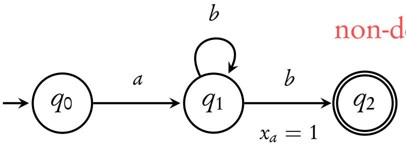


Event-recording automata

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

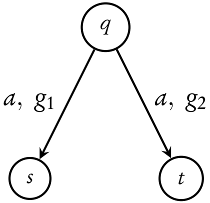


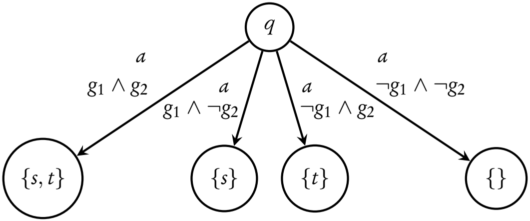
$\{\ (ab^*b, \tau)\ |\ \text{distance between first and last letters is } 1\}$



non-deterministic

Determinizing ERA: modified **subset** construction





exponential in the number of states

DTA

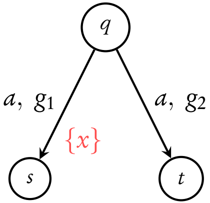
Unique run

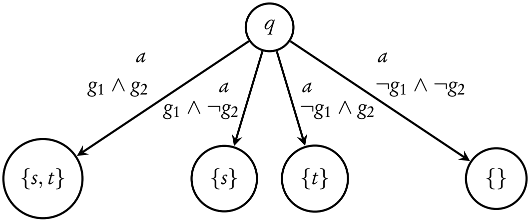
Closed under $\cup$, $\cap$, comp.

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

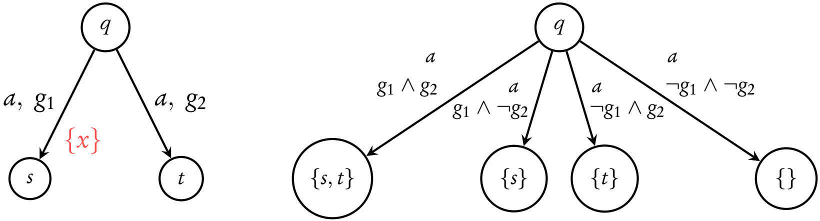
Determinizable subclasses

ERA





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

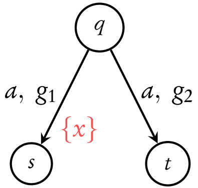


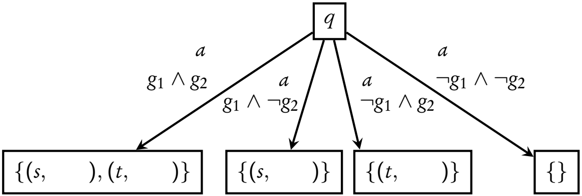
To **reset** or **not to reset**?

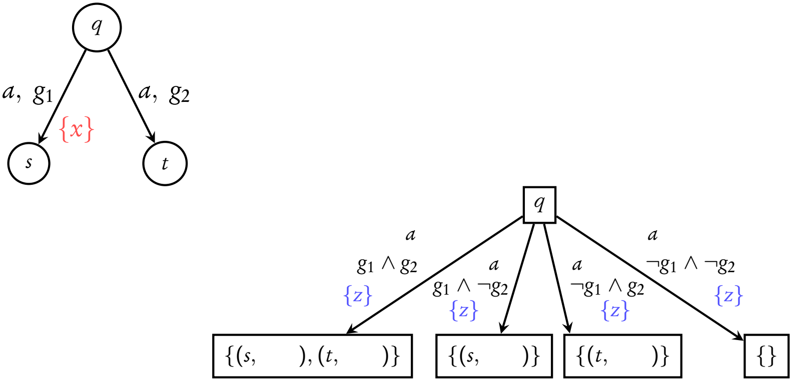
Coming next: slightly modified version of BBBB-09

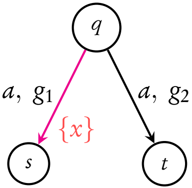
When are timed automata determinizable?

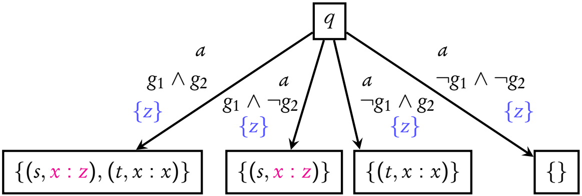
Baier, Bertrand, Bouyer, Brihaye. *ICALP'09*

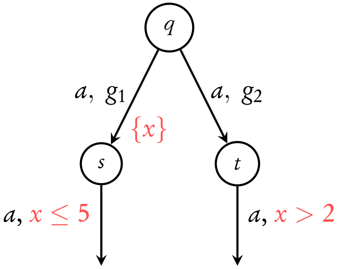

q
a, g1
a, g2
{x}
s
t

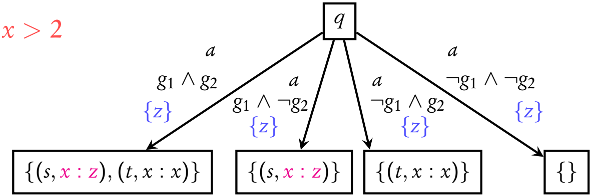

q
a
g1 ∧ g2
a
g1 ∧ ¬g2
a
¬g1 ∧ g2
a
¬g1 ∧ ¬g2
{(s,), (t,)}
{(s,)}
{(t,)}
{}

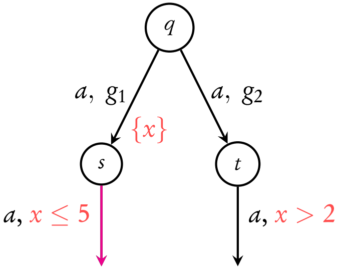

q
a, g1
{x}
a, g2
s
t
q
a
g1 ∧ g2
{z}
a
g1 ∧ ¬g2
{z}
a
¬g1 ∧ g2
{z}
a
¬g1 ∧ ¬g2
{z}
{(s,), (t,)}
{(s,)}
{(t,)}
{}

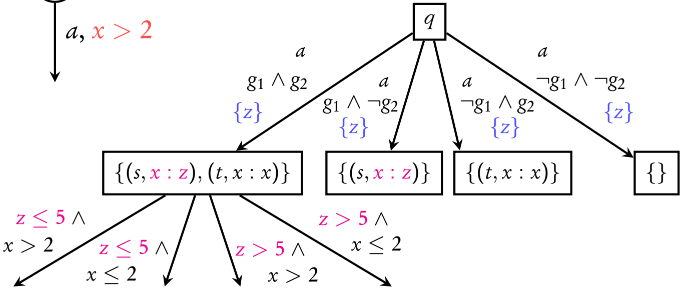

q
a, g1
{x}
a, g2
s
t

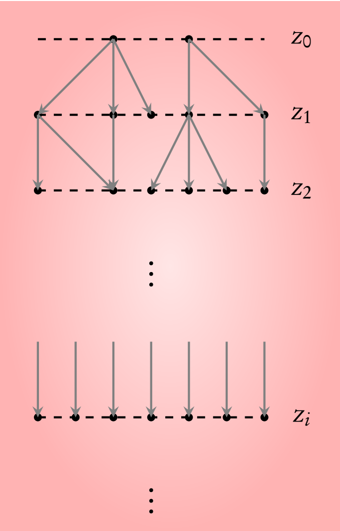

q
a
g1 ∧ g2
{z}
a
g1 ∧ ¬g2
{z}
a
¬g1 ∧ g2
{z}
a
¬g1 ∧ ¬g2
{z}
{(s, x : z), (t, x : x)}
{(s, x : z)}
{(t, x : x)}
{}


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

Coming next: An example illustrating the construction

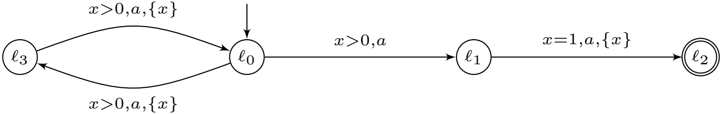


Fig. 1. A timed automaton $\mathcal{A}$

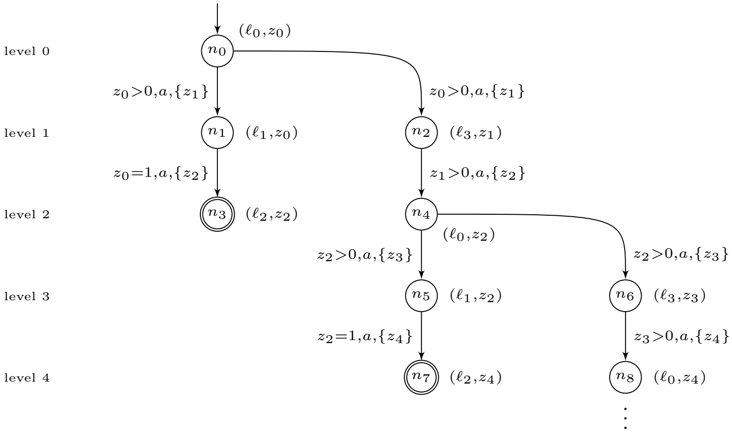
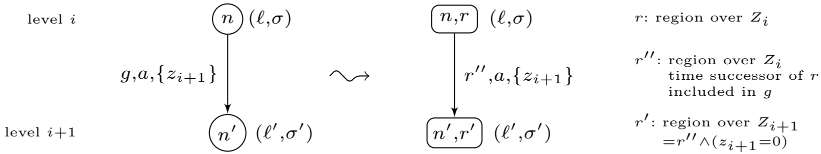


Fig. 2. The infinite timed tree $\mathcal{A}^\infty$ associated with the timed automaton $\mathcal{A}$ of Fig. 1.


level i
level $i+1$
n (ℓ,σ)
$g,a,\{z_{i+1}\}$
n' (ℓ',σ')
n,r (ℓ,σ)
$r'',a,\{z_{i+1}\}$
n',r' (ℓ',σ')
r: region over Z_i
r'': region over Z_i time successor of r included in g
r': region over Z_{i+1} $=r''\wedge(z_{i+1}=0)$

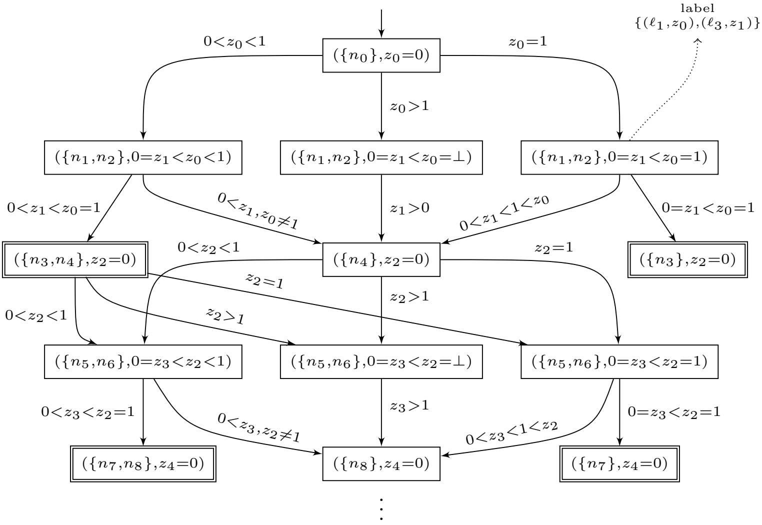


Fig. 3. The DAG induced by the infinite timed tree $\mathsf{SymbDet}(R(\mathcal{A}^\infty))$

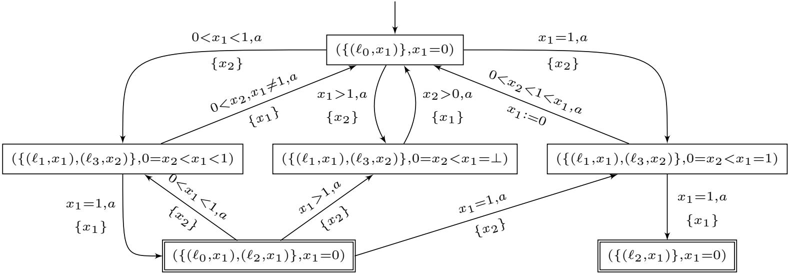
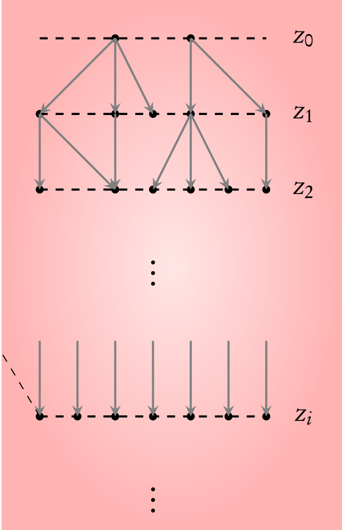


Fig. 4. The deterministic version of $\mathcal{A}$: the timed automaton $\mathcal{B}_{\mathcal{A},\gamma}$

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

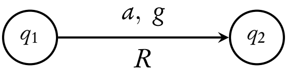
$$\sigma_j : X \mapsto \{z_0, \ldots, z_i\}$$

When do finitely many clocks suffice ?



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

Integer reset timed automata



Conditions:

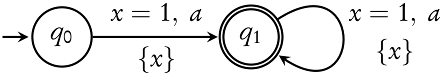
- g has **integer** constants
- R is **non-empty iff** g has some constraint $x = c$

Implication:

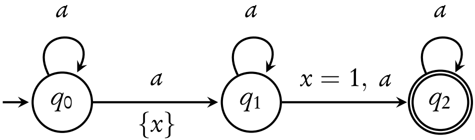
- Along a timed word, a **reset** of an IRTA happens only at **integer timestamps**

Timed automata with integer resets: Language inclusion and expressiveness

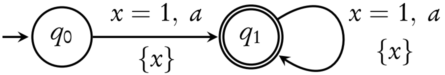
Suman, Pandya, Krishna, Manasa. *FORMATS'08*



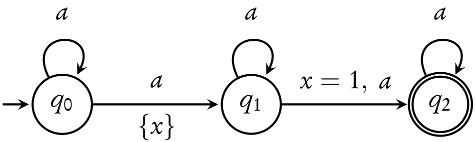
an IRTA



not an IRTA



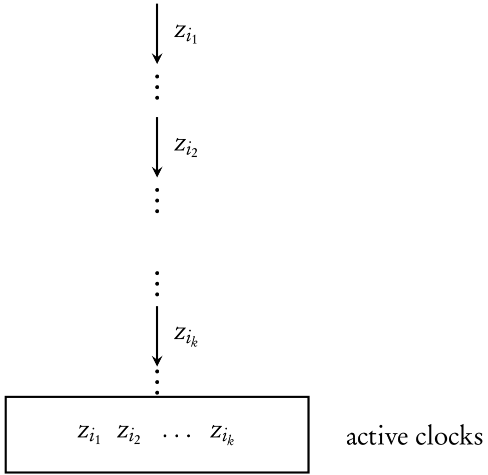
an IRTA



not an IRTA

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

M: **max constant** from among guards



- 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

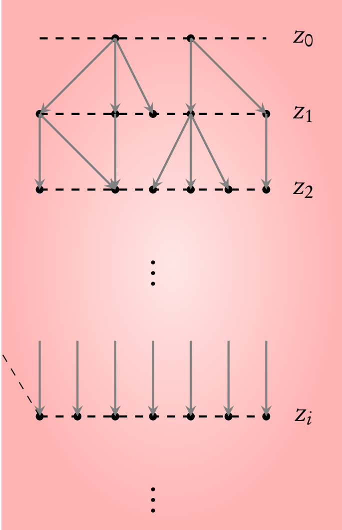
ERA

IRTA

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

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

When do finitely many clocks suffice ?

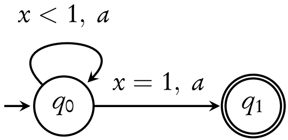


Reset a **new** clock z_i at level i

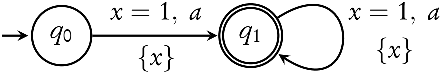
Strongly non-Zeno automata

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

Doubly-exponential in the size of the automaton

DTA

Unique run

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

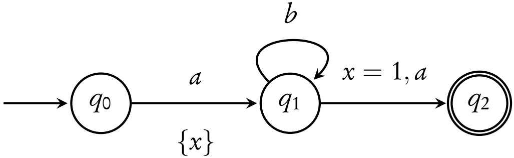
$\mathcal{L}(DTA) \subset \mathcal{L}(TA)$

Determinizable subclasses

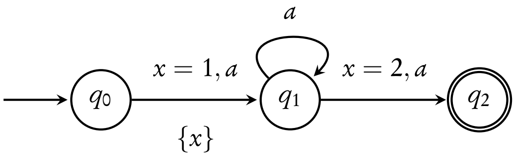
ERA

IRTA

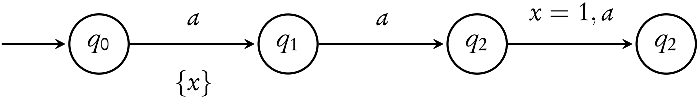
SNZ



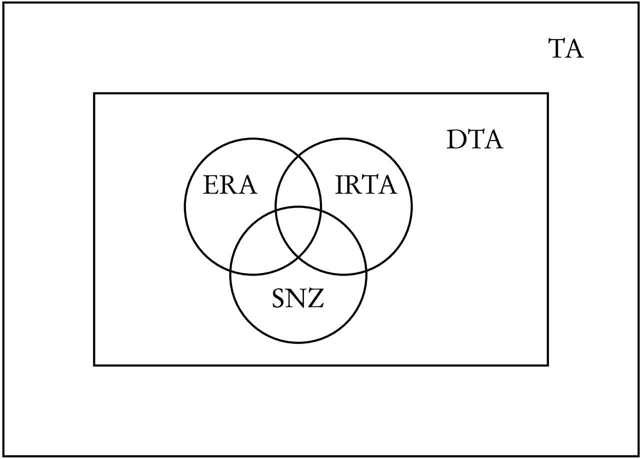
ERA ~~IRTA~~ ~~SNZ~~



~~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