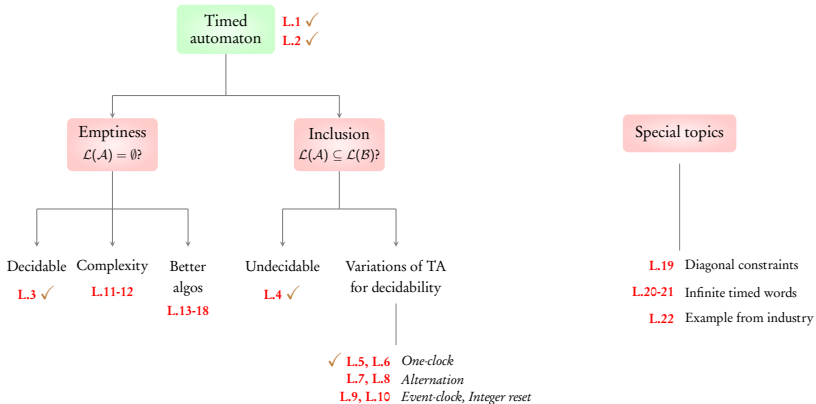
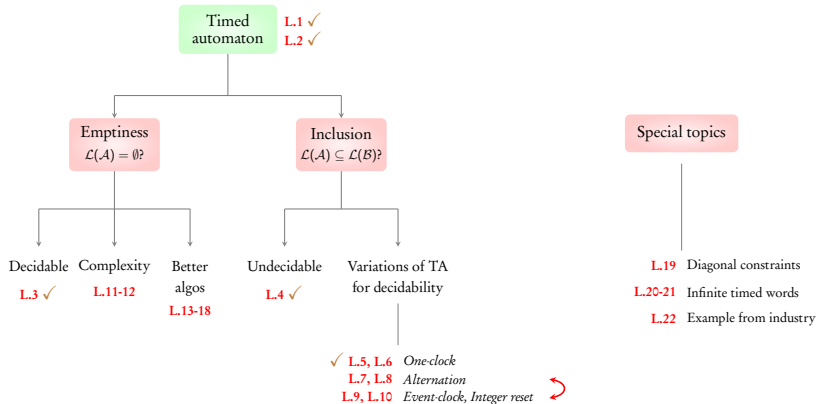


Automata for Real-time Systems

B. Srivathsan

Chennai Mathematical Institute





Today's lecture: Event-clock, Integer reset

System

Specification



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



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

System

Specification



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



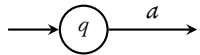
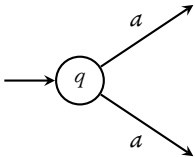
Is $\mathcal{L}(A) \cap \overline{\mathcal{L}(B)}$ empty?

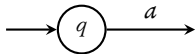
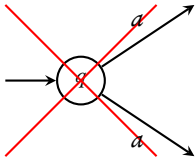


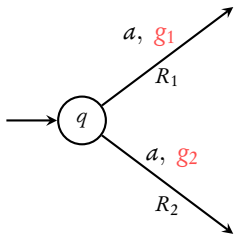
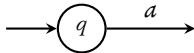
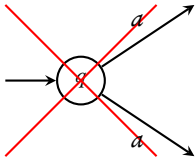
first determinize B

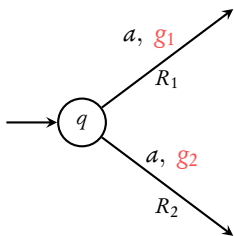
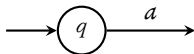
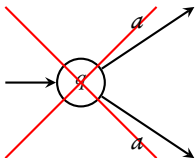
Lecture 7:

Determinizing timed automata





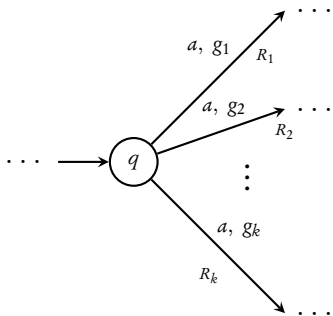




g_1 and g_2 should be
mutually exclusive

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

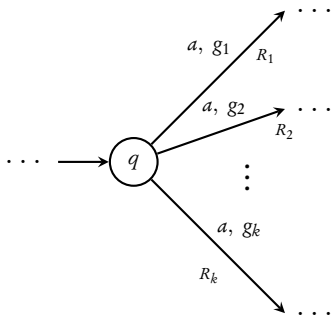
Deterministic Timed Automata



$g_i \wedge g_j$ is
unsatisfiable

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

Deterministic Timed Automata



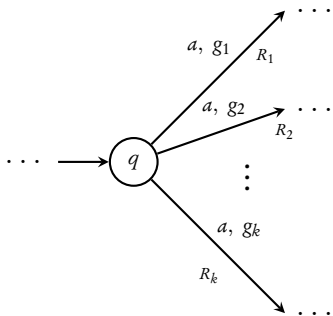
$g_i \wedge g_j$ is
unsatisfiable

complete if

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

+ **single initial** state

Deterministic Timed Automata



$g_i \wedge g_j$ is
unsatisfiable

complete if

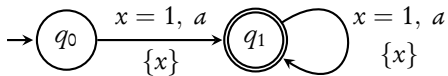
$$g_1 \vee g_2 \vee \dots \vee g_k = \top$$

+ single initial state

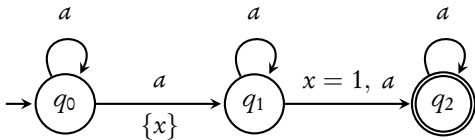
Unique run

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

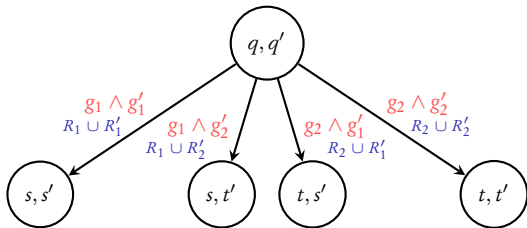
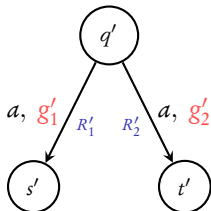
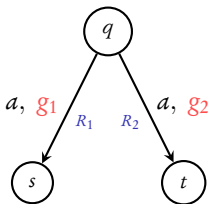
A theory of timed automata



a DTA

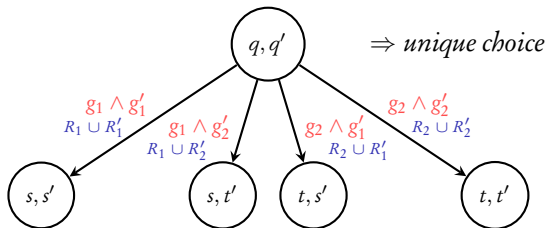
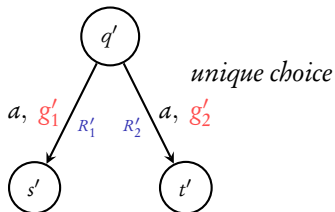
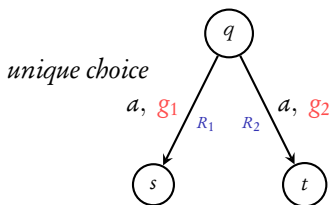


not a DTA



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*)

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

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]

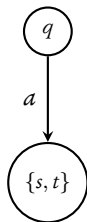
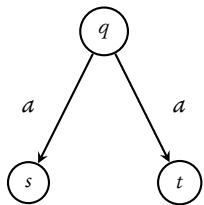
Given a TA, checking **if** it can be determinized is **undecidable**

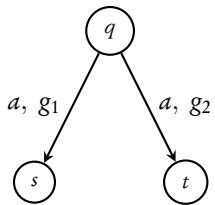
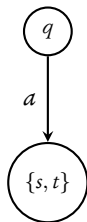
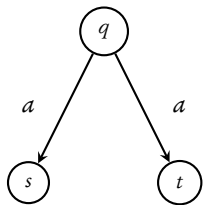
Given a TA, **when** do we know if we **can determinize** it?

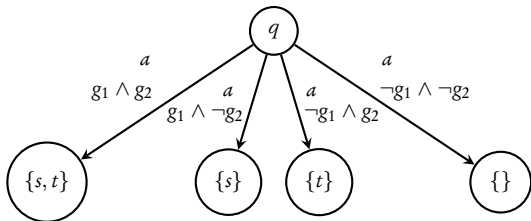
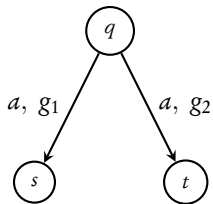
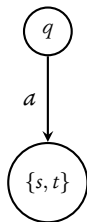
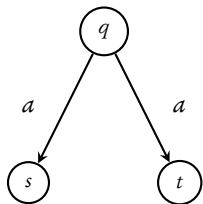
Theorem [Finkel'06]

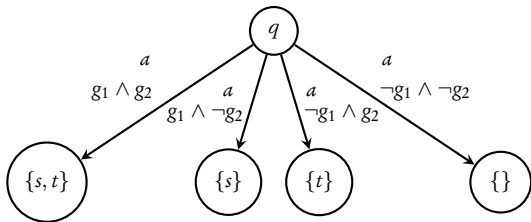
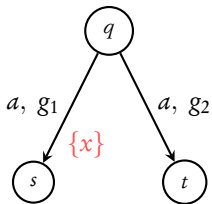
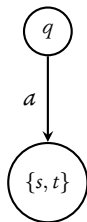
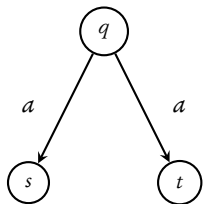
Given a TA, checking **if** it can be determinized is **undecidable**

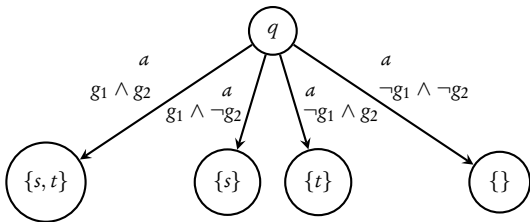
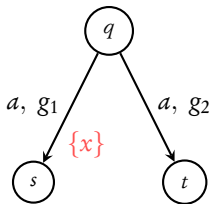
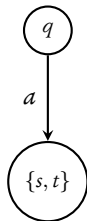
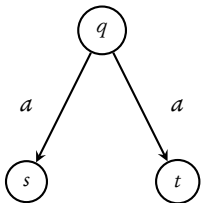
Following next: some **sufficient** conditions for determinizing



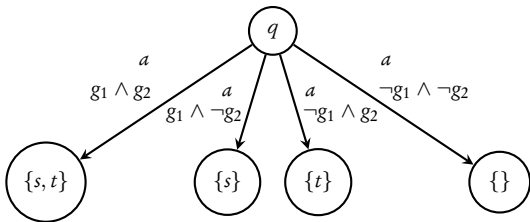
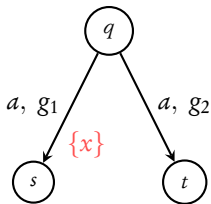
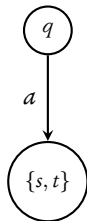
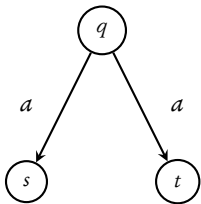








To reset or not to reset?



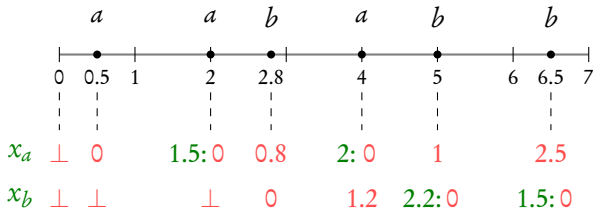
First solution:

Whenever a , reset x_a

To reset or not to reset?

Event-recording clocks: time since last occurrence of event

$$a \mapsto x_a$$

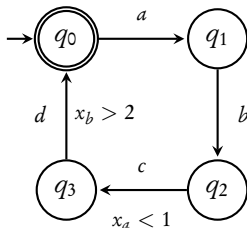


Event-clock automata: a determinizable subclass of timed automata

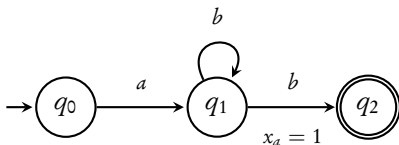
Alur, Henzinger, Fix. TCS'99

Event-recording automata

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

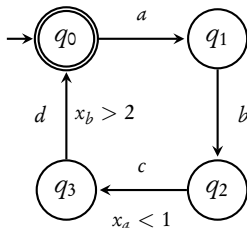


$\{ (ab^*b, \tau) \mid \text{distance between first and last letters is } 1 \}$

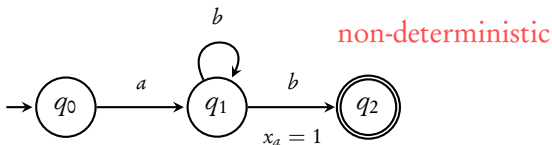


Event-recording automata

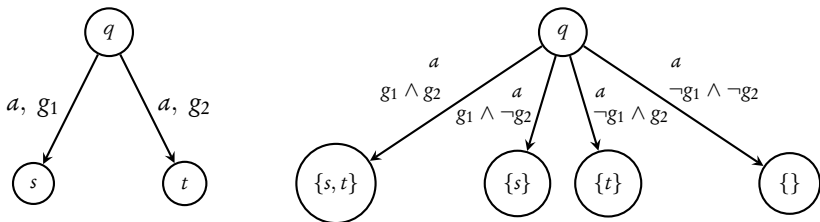
$\{ ((abcd)^k, \tau) \mid a - c \text{ distance is } < 1 \text{ and } b - d \text{ distance is } > 2 \}$



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



Determinizing ERA: modified subset construction



exponential in the number of states

DTA

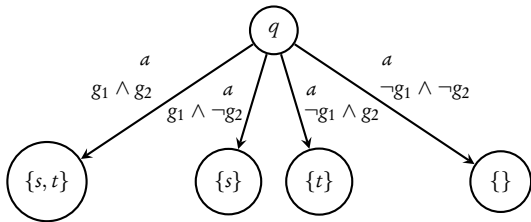
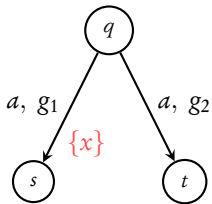
Unique run

Closed under \cup , \cap , comp.

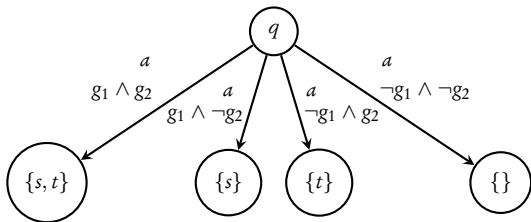
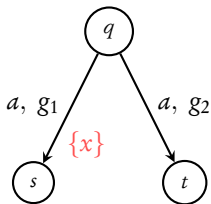
$$\mathcal{L}(DTA) \subset \mathcal{L}(TA)$$

Determinizable subclasses

ERA



To reset or not to reset?

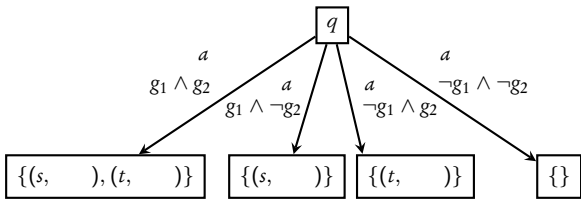
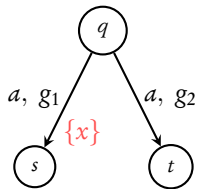


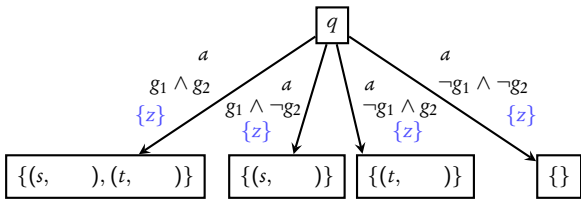
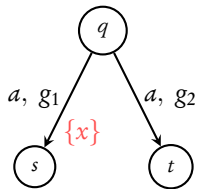
To reset or not to reset?

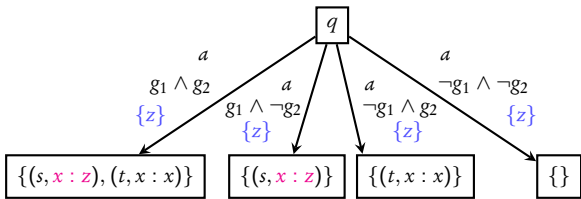
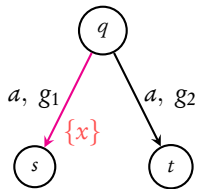
Coming next: slightly modified version of BBBB-09

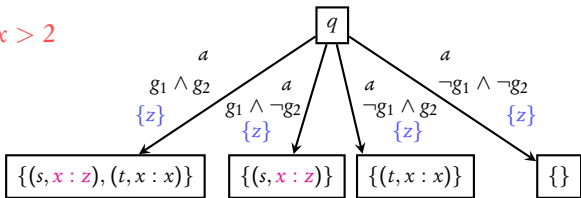
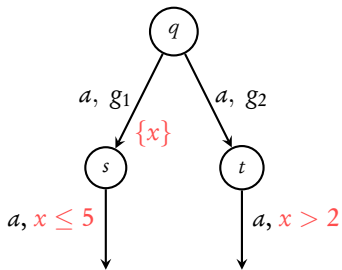
When are timed automata determinizable?

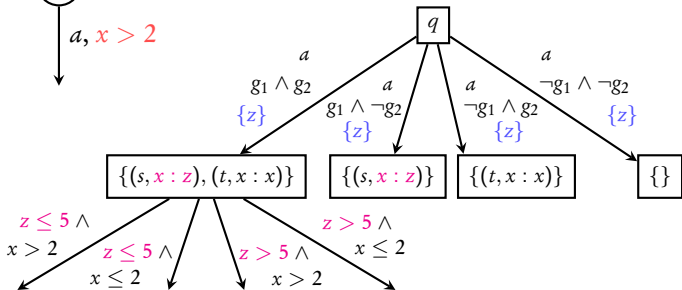
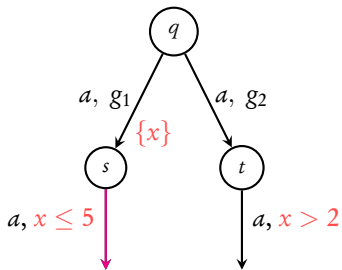
Baier, Bertrand, Bouyer, Brihaye. *ICALP'09*

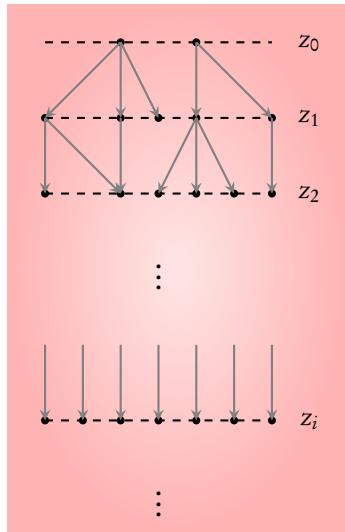








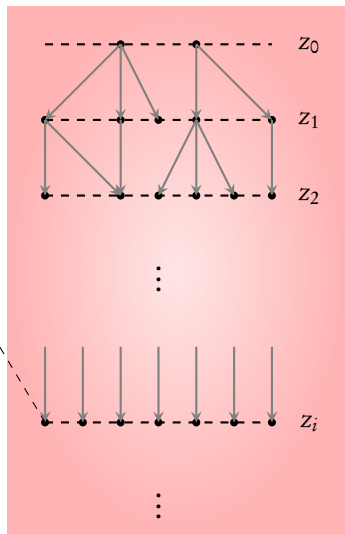




Reset a **new** clock z_i at level i

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

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

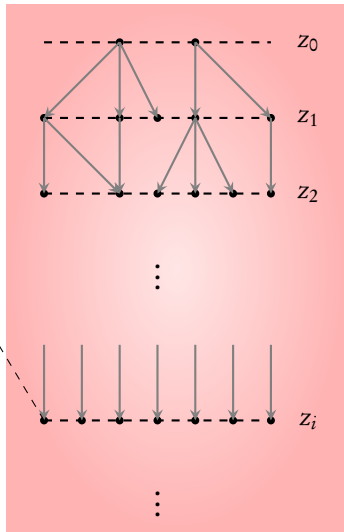


Reset a **new** clock z_i at level i

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

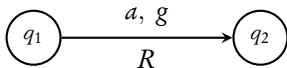
$$\sigma_j : X \mapsto \{z_0, \dots, z_i\}$$

When do finitely many clocks suffice ?



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

Integer reset timed automata



Conditions:

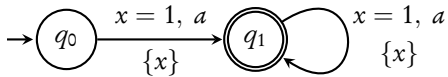
- ▶ g has **integer** constants **other than zero**
- ▶ R is **non-empty** iff g has some constraint $x = c$

Implication:

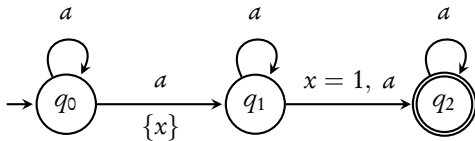
- ▶ Along a timed word, a **reset** of an IRTA happens only at **integer timestamps**

Timed automata with integer resets: Language inclusion and expressiveness

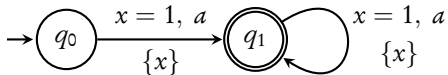
Suman, Pandya, Krishna, Manasa. *FORMATS'08*



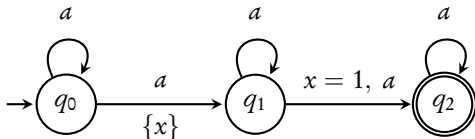
an IRTA



not an IRTA



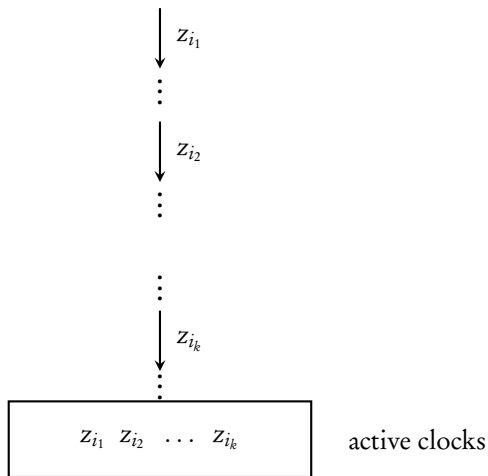
an IRTA



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

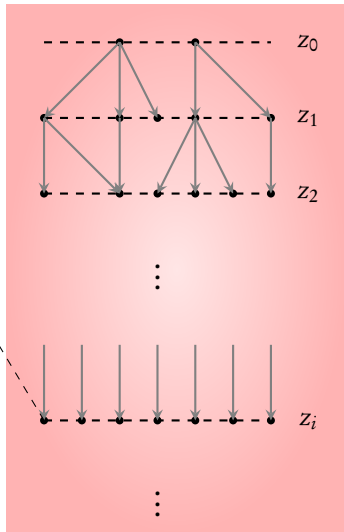
ERA

IRTA

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

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

When do finitely many clocks suffice ?

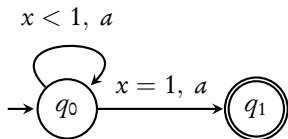


Reset a **new** clock z_i at level i

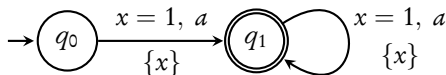
Strongly non-Zeno automata

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

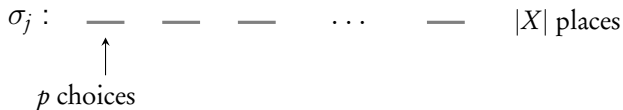
$$\{(q_1, \sigma_1), (q_2, \sigma_2) \dots (q_k, \sigma_k)\}$$

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

Complexity of subset construction

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

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



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

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

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

Complexity of subset construction

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

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

$$\sigma_j : \quad \text{---} \quad \text{---} \quad \text{---} \quad \dots \quad \text{---} \quad |X| \text{ places}$$

↑
 p choices

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

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

→ **doubly exponential** in the size of initial automaton

DTA

Unique run

Closed under \cup , \cap , comp.

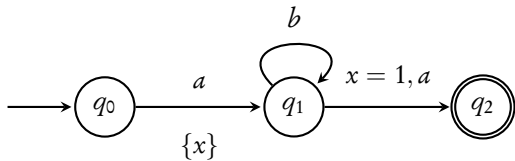
$$\mathcal{L}(DTA) \subset \mathcal{L}(TA)$$

Determinizable subclasses

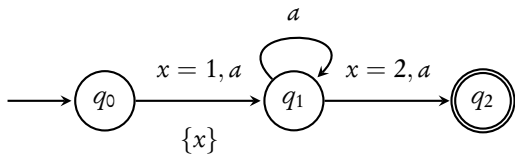
ERA

IRTA

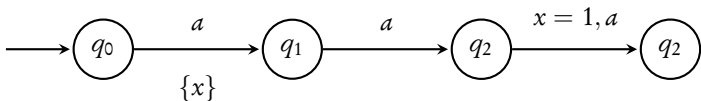
SNZ



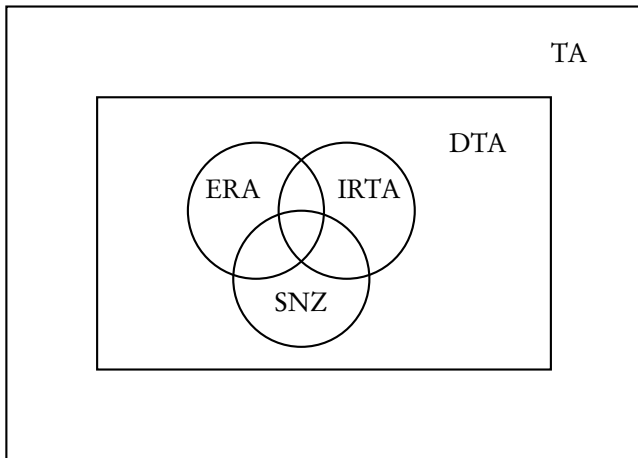
ERA ~~IRTA~~ ~~SNZ~~



~~ERA~~ IRTA ~~SNZ~~



~~ERA~~ ~~IRTA~~ SNZ



Closure properties of ERA, IRTA, SNZ

- ▶ **Union:** disjoint union ✓
- ▶ **Intersection:** product construction ✓
- ▶ **Complement:** determinize & interchange acc. states ✓

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