Topics in Timed Automata

B. Srivathsan

RWTH-Aachen

Software modeling and Verification group

Universality (Lecture 3)

Checking if a TA accepts all timed words is **undecidable**

Universality (Lecture 3)

Checking if a TA accepts all timed words is **undecidable**

Alternating timed automata

Emptiness of alternating timed automata is **undecidable**

Time: the real line

Bounded time: $[0, N)$ for an *a priori* given $N \in \mathbb{N}$

Alternating timed automata

Time-bounded emptiness of alternating timed automata is **decidable**

Alternating timed automata over bounded time

Jenkins, Ouaknine, Rabinovich, Worrell. *LICS'10*

Universality

Given a time-bound N, checking if a TA accepts all timed words **of duration at most** N is **decidable**

Alternating timed automata

Time-bounded emptiness of alternating timed automata is **decidable**

Alternating timed automata over bounded time

Jenkins, Ouaknine, Rabinovich, Worrell. *LICS'10*

Lecture 9:

Time-bounded theory of verification

For the rest of the talk...

Assume that $N \in \mathbb{N}$ is given and let $\mathbb{T} = [0, N)$

Section 1:
Alternating timed automata

- X : set of **clocks**
- $\Phi(X)$: set of clock constraints σ (**guards**)

$$\sigma : \; x < c \mid x \leq c \mid \sigma_1 \wedge \sigma_2 \mid \neg\sigma$$

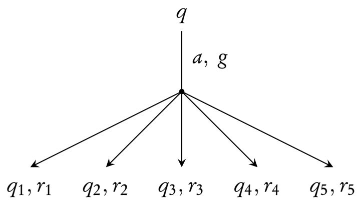
  c is a non-negative **integer**

- Timed automaton A: $(Q, Q_0, \Sigma, X, T, F)$

$$T \subseteq Q \times \Sigma \times \Phi(X) \times Q \times \mathcal{P}(X)$$

$$T \subseteq Q \times \Sigma \times \Phi(X) \times Q \times \mathcal{P}(X)$$

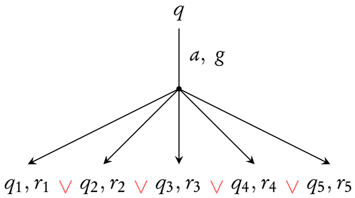
$$T : Q \times \Sigma \times \Phi(X) \mapsto \mathcal{P}(Q \times \mathcal{P}(X))$$



$$T \subseteq Q \times \Sigma \times \Phi(X) \times Q \times \mathcal{P}(X)$$

$$\downarrow$$

$$T : Q \times \Sigma \times \Phi(X) \mapsto \mathcal{P}(Q \times \mathcal{P}(X))$$



$$T : Q \times \Sigma \times \Phi(X) \mapsto \mathcal{P}(Q \times \mathcal{P}(X))$$

$$T : Q \times \Sigma \times \Phi(X) \mapsto \mathcal{P}(Q \times \mathcal{P}(X))$$

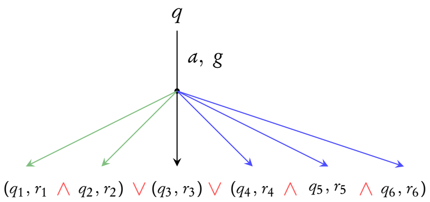
$\downarrow$ $\mathcal{B}^+(S)$ is all $\phi ::= S \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2$

$$T : Q \times \Sigma \times \Phi(X) \; \mapsto \; \mathcal{B}^+(Q \times \mathcal{P}(X))$$

$$T : Q \times \Sigma \times \Phi(X) \mapsto \mathcal{P}(Q \times \mathcal{P}(X))$$

$\downarrow$ $\mathcal{B}^+(S)$ is all $\phi ::= S \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2$

$$T : Q \times \Sigma \times \Phi(X) \mapsto \mathcal{B}^+(Q \times \mathcal{P}(X))$$



Alternating Timed Automata

An **ATA** is a tuple $A = (Q, q_0, \Sigma, X, T, F)$ where:

$$T : Q \times \Sigma \times \Phi(X) \mapsto \mathcal{B}^+(Q \times \mathcal{P}(X))$$

is a **finite partial function.**

Alternating Timed Automata

An **ATA** is a tuple $A = (Q, q_0, \Sigma, X, T, F)$ where:

$$T : Q \times \Sigma \times \Phi(X) \mapsto \mathcal{B}^+(Q \times \mathcal{P}(X))$$

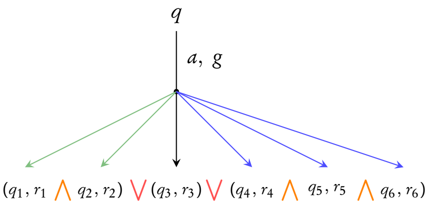
is a **finite partial function.**

Partition: For every q, a the set

$$\{ [\sigma] \mid T(q, a, \sigma) \text{ is defined } \}$$

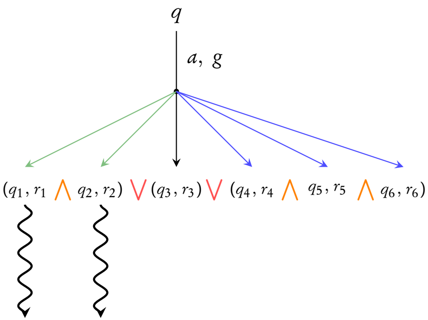
gives a finite partition of $\mathbb{R}^X_{\geq 0}$

Acceptance



Accepting run from q iff:

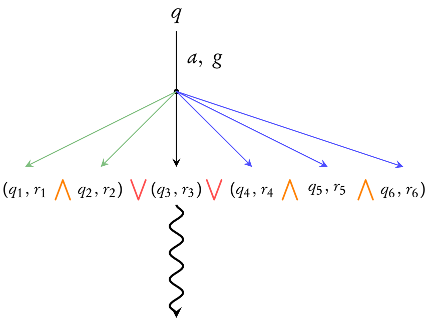
Acceptance



Accepting run from q iff:

- accepting run from q_1 **and** q_2,

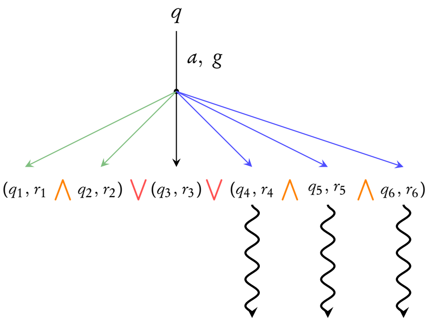
Acceptance



Accepting run from q iff:

- accepting run from q_1 **and** q_2,
- **or** accepting run from q_3,

Acceptance



Accepting run from q iff:

- accepting run from q_1 **and** q_2,
- **or** accepting run from q_3,
- **or** accepting run from q_4 **and** q_5 **and** q_6

Example

L : timed words over $\{a\}$ containing **no two** $a's$ at distance 1

(Not expressible by non-deterministic TA)

Example

L : timed words over $\{a\}$ containing **no two** $a's$ at distance 1

(Not expressible by non-deterministic TA)

ATA:

$$q_0, a, tt \mapsto (q_0, \emptyset) \wedge (q_1, \{x\})$$

$$q_1, a, x = 1 \mapsto (q_2, \emptyset)$$

$$q_1, a, x \neq 1 \mapsto (q_1, \emptyset)$$

$$q_2, a, tt \mapsto (q_2, \emptyset)$$

q_0, q_1 are acc., q_2 is non-acc.

- Given ATA A and timed word $w = (a_1, t_1) \ \ldots \ (a_n, t_n)$
- **Acceptance game** $\mathbb{G}(A, w)$ has n rounds
- Starts at $(0, q_0, v_0)$

- Given ATA A and timed word $w = (a_1, t_1) \; \ldots \; (a_n, t_n)$
- **Acceptance game** $\mathbb{G}(A, w)$ has n rounds
- Starts at $(0, q_0, v_0)$

(a_i, t_i) (i, q_i, v_i)

(a_{i+1}, t_{i+1})

- Given ATA A and timed word $w = (a_1, t_1)\ \ldots\ (a_n, t_n)$
- **Acceptance game** $\mathbb{G}(A, w)$ has n rounds
- Starts at $(0, q_0, v_0)$

(a_i, t_i) (i, q_i, v_i)

$v' = v_i + t_{i+1} - t_i$

unique $T(q_i, a_{i+1}, \sigma)$ s.t. $v' \models \phi$

(a_{i+1}, t_{i+1}) $(\circ \wedge \circ \wedge \circ)\ \vee\ (\circ \wedge \circ)\ \vee\ (\circ)$

- Given ATA A and timed word $w = (a_1, t_1) \ldots (a_n, t_n)$
- **Acceptance game** $\mathbb{G}(A, w)$ has n rounds
- Starts at $(0, q_0, v_0)$

(a_i, t_i) (i, q_i, v_i)

Automaton $(\circ \wedge \circ \wedge \circ)$ $v' = v_i + t_{i+1} - t_i$

unique $T(q_i, a_{i+1}, \sigma)$ s.t. $v' \models \phi$

(a_{i+1}, t_{i+1}) $(\circ \wedge \circ \wedge \circ) \vee (\circ \wedge \circ) \vee (\circ)$

- Given ATA A and timed word $w = (a_1, t_1) \ \ldots \ (a_n, t_n)$
- **Acceptance game** $\mathbb{G}(A, w)$ has n rounds
- Starts at $(0, q_0, v_0)$

(a_i, t_i) $\qquad$ (i, q_i, v_i)

$\downarrow$

Automaton $\qquad$ $(\circ \wedge \circ \wedge \circ)$ $\qquad$ $v' = v_i + t_{i+1} - t_i$

$\downarrow$

Pathfinder $\qquad$ $\circ$ $\qquad$ unique $T(q_i, a_{i+1}, \sigma)$ s.t. $v' \models \phi$

(a_{i+1}, t_{i+1}) $\qquad$ $(\circ \wedge \circ \wedge \circ) \ \vee \ (\circ \wedge \circ) \ \vee \ (\circ)$

- Given ATA A and timed word $w = (a_1, t_1) \ \ldots \ (a_n, t_n)$
- **Acceptance game** $\mathbb{G}(A, w)$ has n rounds
- Starts at $(0, q_0, v_0)$

(a_i, t_i)	(i, q_i, v_i)	
	$\downarrow$	
Automaton	$(\circ \ \wedge \ \circ \ \wedge \ \circ)$	$v' = v_i + t_{i+1} - t_i$
	$\downarrow$	
Pathfinder	$\circ$	unique $T(q_i, a_{i+1}, \sigma)$ s.t. $v' \models \phi$
	$\downarrow$	
(a_{i+1}, t_{i+1})	$(i+1, q_{i+1}, v_{i+1})$	$(\circ \wedge \circ \wedge \circ) \ \vee \ (\circ \wedge \circ) \ \vee \ (\circ)$

- Given ATA A and timed word $w = (a_1, t_1) \ \ldots \ (a_n, t_n)$
- **Acceptance game** $\mathbb{G}(A, w)$ has n rounds
- Starts at $(0, q_0, v_0)$

(a_i, t_i)	(i, q_i, v_i)	
	$\downarrow$	
Automaton	$(\circ \ \wedge \ \circ \ \wedge \ \circ)$	$v' = v_i + t_{i+1} - t_i$
	$\downarrow$	
Pathfinder	$\circ$	unique $T(q_i, a_{i+1}, \sigma)$ s.t. $v' \models \phi$
	$\downarrow$	
(a_{i+1}, t_{i+1})	$(i+1, q_{i+1}, v_{i+1})$	$(\circ \wedge \circ \wedge \circ) \ \vee \ (\circ \wedge \circ) \ \vee \ (\circ)$

- Automaton wins if game ends in accepting state

Time-bounded emptiness problem

Is there a timed word with timestamps in $\mathbb{T}$ accepted by ATA A?

Is there a timed word w with timestamps in $\mathbb{T}$ such that **Automaton wins** the game $\mathbb{G}(A, w)$?

Section 2:
Monadic second-order logic

MSO over $(\mathbb{T}, <, +1)$

$$\forall t : \big(\, A(t) \;\Rightarrow\; (\, \exists t_1 : \; +1(t, t_1) \;\wedge\; B(t_1)\,)\,\big)$$

whenever *A* occurs, *B* occurs after 1 time unit

$$\exists t : \big(\, A(t) \;\wedge\; \forall t' : \;(\, (t' \neq t) \;\Rightarrow\; \neg A(t)\,)\,\big)$$

A is true at exactly one time instant

MSO$(<, +1)$

- Syntax:
  - **vocabulary:** first-order variables $t_1, t_2, \dots,$
    second-order monadic predicates $X_1, X_2, \dots$
  - **atomic formulas:** $t_1 < t_2$, $+1(t_1, t_2)$, $t_1 = t_2$, $X(t)$
  - $\wedge$, $\vee$, $\neg$, $\forall t$, $\forall X$, $\exists t$, $\exists X$
  - $\phi(X_1, \dots, X_k)$: **free** second order variables from $X_1, \dots, X_k$
- Interpretation: of a second-order variable is a **subset** of $\mathbb{T}$
- Models: of $\phi(X_1, \dots, X_k)$ are the **set of interpretations** of $X_1, \dots, X_k$ satisfying ϕ

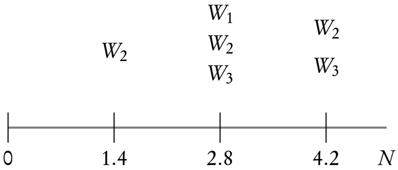
Finiteness assumption

Free second-order variables interpreted by **finite sets**

Second-order **quantification over finite sets**

Interpretations and timed words

- $W_1, \ldots, W_k$: monadic predicate variables
- $\Sigma = \mathcal{P}_+(\{W_1, \ldots, W_k\})$



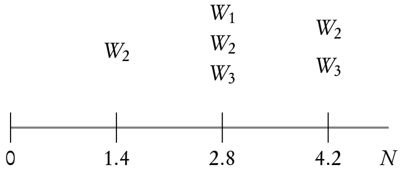
$$\mathrm{Int}(W_1) = \{2.8\}$$

$$\mathrm{Int}(W_2) = \{1.4, 2.8, 4.2\}$$

$$\mathrm{Int}(W_3) = \{2.8, 4.2\}$$

Interpretations and timed words

- $W_1, \ldots, W_k$: monadic predicate variables
- $\Sigma = \mathcal{P}_+(\{W_1, \ldots, W_k\})$



$$\mathrm{Int}(W_1) = \{2.8\}$$
$$\mathrm{Int}(W_2) = \{1.4, 2.8, 4.2\}$$
$$\mathrm{Int}(W_3) = \{2.8, 4.2\}$$

interpretations $\leftrightarrow$ timed words

Section 3:
McNaughton games

$\mathbb{W}$: $W_1, \ldots, W_k$

$\mathbf{X}$: $X_1, \ldots, X_m$

$\mathbf{Y}$: $Y_1, \ldots, Y_l$

$\varphi(\mathbb{W}, \mathbf{X}, \mathbf{Y})$: an $\mathsf{MSO}(<, +1)$ formula

$\mathbf{W}$: $W_1, \ldots, W_k$

$\mathbf{X}$: $X_1, \ldots, X_m$

$\mathbf{Y}$: $Y_1, \ldots, Y_l$

$\varphi(\mathbf{W}, \mathbf{X}, \mathbf{Y})$: an $\mathsf{MSO}(<, +1)$ formula

$\mathbf{X}$: Player I variables

$\mathbf{Y}$: Player II variables

$\mathbf{W}$: parameters

Let $\mathbf{P}$ be an interpretation of $\mathbf{W}$

$\mathbb{W}$: $W_1, \ldots, W_k$

$\mathbf{X}$: $X_1, \ldots, X_m$

$\mathbf{Y}$: $Y_1, \ldots, Y_l$

$\varphi(\mathbb{W}, \mathbf{X}, \mathbf{Y})$: an $\mathsf{MSO}(<, +1)$ formula

$\mathbf{X}$: Player I variables

$\mathbf{Y}$: Player II variables

$\mathbb{W}$: parameters

Let $\mathbf{P}$ be an interpretation of $\mathbb{W}$

Each interpretation $\mathbf{P}$ of $\mathbb{W}$ gives McNaughton game $\mathbb{G}(\varphi, \mathbf{P})$

$\mathbb{G}(\varphi, \mathbf{P})$

$$\mathbf{P} = (a_1, t_1)\,(a_2, t_2)\;\ldots\;(a_n, t_n)$$

$$t_1 < t_2 < \cdots < t_n$$

$$a_i \in \{0, 1\}^{\mathbb{W}}$$

$\mathbb{G}(\varphi, \mathbf{P})$

$$\mathbf{P} = (a_1, t_1)\ (a_2, t_2)\ \dots\ (a_n, t_n)$$

$$t_1 < t_2 < \cdots < t_n$$

$$a_i \in \{0, 1\}^{\mathbb{W}}$$

- an **n-round** turn-based game

$\mathbb{G}(\varphi, \mathbf{P})$

$$\mathbf{P} = (a_1, t_1)\ (a_2, t_2)\ \ldots\ (a_n, t_n)$$

$$t_1 < t_2 < \cdots < t_n$$

$$a_i \in \{0, 1\}^{\mathbf{W}}$$

- an **n-round** turn-based game
- In i^{th} round, Player I chooses $b_i \in \{0, 1\}^{\mathbf{X}}$ and then Player II chooses $b'_i \in \{0, 1\}^{\mathbf{Y}}$

$\mathbb{G}(\varphi, \mathbf{P})$

$$\mathbf{P} = (a_1, t_1)\ (a_2, t_2)\ \dots\ (a_n, t_n)$$

$$t_1 < t_2 < \dots < t_n$$

$$a_i \in \{0, 1\}^{\mathbf{W}}$$

- an **n-round** turn-based game
- In i^{th} round, Player I chooses $b_i \in \{0, 1\}^{\mathbf{X}}$ and then Player II chooses $b'_i \in \{0, 1\}^{\mathbf{Y}}$
- After n rounds, Player I has constructed an interpretation $\mathbf{Q}$ of $\mathbf{X}$, and Player II an interpretation $\mathbf{R}$ of $\mathbf{Y}$

$\mathbb{G}(\varphi, \mathbf{P})$

$$\mathbf{P} = (a_1, t_1)\ (a_2, t_2)\ \ldots\ (a_n, t_n)$$

$$t_1 < t_2 < \cdots < t_n$$

$$a_i \in \{0, 1\}^{\mathbf{W}}$$

- an **n-round** turn-based game
- In i^{th} round, Player I chooses $b_i \in \{0, 1\}^{\mathbf{X}}$ and then Player II chooses $b'_i \in \{0, 1\}^{\mathbf{Y}}$
- After n rounds, Player I has constructed an interpretation $\mathbf{Q}$ of $\mathbf{X}$, and Player II an interpretation $\mathbf{R}$ of $\mathbf{Y}$
- If $\varphi(\mathbf{P}, \mathbf{Q}, \mathbf{R})$ is true, Player I wins. Otherwise, Player II wins

Section 4:
ATA emptiness to McNaughton games

Recall...

- Given ATA A and timed word $w = (a_1, t_1)\ \ldots\ (a_n, t_n)$
- **Acceptance game** $\mathbb{G}(A, w)$ has n rounds
- Starts at $(0, q_0, v_0)$

(a_i, t_i) (i, q_i, v_i)

$v' = v_i + t_{i+1} - t_i$

unique $T(q_i, a_{i+1}, \sigma)$ s.t. $v' \models \phi$

(a_{i+1}, t_{i+1}) $(i+1, q_{i+1}, v_{i+1})$ $(\circ \wedge \circ \wedge \circ)\ \vee\ (\circ \wedge \circ)\ \vee\ (\circ)$

- Automaton wins if game ends in accepting state

Recall...

- Given ATA A and timed word $w = (a_1, t_1) \ \ldots \ (a_n, t_n)$
- **Acceptance game** $\mathbb{G}(A, w)$ has n rounds
- Starts at $(0, q_0, v_0)$

(a_i, t_i) (i, q_i, v_i)

Automaton $(\circ \ \wedge \ \circ \ \wedge \ \circ)$ $v' = v_i + t_{i+1} - t_i$

unique $T(q_i, a_{i+1}, \sigma)$ s.t. $v' \models \phi$

(a_{i+1}, t_{i+1}) $(i+1, q_{i+1}, v_{i+1})$ $(\circ \wedge \circ \wedge \circ) \ \vee \ (\circ \wedge \circ) \ \vee \ (\circ)$

- Automaton wins if game ends in accepting state

Recall...

- Given ATA A and timed word $w = (a_1, t_1)\ \dots\ (a_n, t_n)$
- **Acceptance game** $\mathbb{G}(A, w)$ has n rounds
- Starts at $(0, q_0, v_0)$

(a_i, t_i) $\quad$ (i, q_i, v_i)

Automaton $\quad (\circ \wedge \circ \wedge \circ)$ $\quad v' = v_i + t_{i+1} - t_i$

Pathfinder $\quad \circ$ $\quad$ unique $T(q_i, a_{i+1}, \sigma)$ s.t. $v' \models \phi$

(a_{i+1}, t_{i+1}) $\quad (i+1, q_{i+1}, v_{i+1})$ $\quad (\circ \wedge \circ \wedge \circ) \vee (\circ \wedge \circ) \vee (\circ)$

- Automaton wins if game ends in accepting state

$$\mathbb{G}(A, w) \;\rightarrow\; \mathbb{G}(\varphi_A, \mathbf{P})$$

$$\begin{aligned} \text{Automaton} &\rightarrow \text{Player I} \\ \text{Pathfinder} &\rightarrow \text{Player II} \\ w &\rightarrow \mathbf{P} \end{aligned}$$

φ_A should ensure:

- only one X_θ is true at time point
- only one Y_α is true and α belongs to θ
- the transition function of A is respected
- initial, accepting

$$\mathbb{G}(A, w) \;\rightarrow\; \mathbb{G}(\varphi_A, \mathbf{P})$$

$$\begin{aligned} \text{Automaton} &\;\rightarrow\; \text{Player I} \\ \text{Pathfinder} &\;\rightarrow\; \text{Player II} \\ w &\;\rightarrow\; \mathbf{P} \\ \theta : (\circ \;\wedge\; \circ \;\wedge\; \circ) &\;\rightarrow\; X_\theta \in \mathbf{X} \end{aligned}$$

φ_A should ensure:

- only one X_θ is true at time point
- only one Y_α is true and α belongs to θ
- the transition function of A is respected
- initial, accepting

$$\mathbb{G}(A, w) \rightarrow \mathbb{G}(\varphi_A, \mathbf{P})$$

$$\begin{aligned} \text{Automaton} &\rightarrow \text{Player I} \\ \text{Pathfinder} &\rightarrow \text{Player II} \\ w &\rightarrow \mathbf{P} \\ \theta : (\circ \wedge \circ \wedge \circ) &\rightarrow X_\theta \in \mathbf{X} \\ \alpha : \circ &\rightarrow Y_\alpha \in \mathbf{Y} \end{aligned}$$

φ_A should ensure:

- only one X_θ is true at time point
- only one Y_α is true and α belongs to θ
- the transition function of A is respected
- initial, accepting

$$\bigwedge_{\alpha} \left(Y_{\alpha}(t) \Rightarrow \bigvee_{\theta \models \alpha} X_{\theta}(t) \right) \wedge \bigwedge_{\alpha \neq \beta} \neg (Y_{\alpha}(t) \wedge Y_{\beta}(t))$$

α belongs to θ and only one α is true

For every $T(q, a, g)$ that is defined:

$$\forall t : \left(state_q(t) \ \wedge \ next(t, t') \ \wedge \ W_a(t') \ \wedge \ const_g(t') \ \Rightarrow \bigvee_{\theta \models T(q,a,g)} X_\theta(t') \right)$$

- Automaton chooses θ respecting the transition function $T(q, a, g)$

For every $T(q,a,g)$ that is defined:

$$\forall t : \left(state_q(t) \;\wedge\; next(t,t') \;\wedge\; W_a(t') \;\wedge\; const_g(t') \;\Rightarrow \bigvee_{\theta \models T(q,a,g)} X_\theta(t') \right)$$

- Automaton chooses θ respecting the transition function $T(q,a,g)$
- $state_q(t)$: formula to say that the automaton state at t is q
- $next(t,t')$: t and t' are consecutive time-stamps in input word
- $const_g(t')$: clock constraint g is true at t'

$$\exists u : \Big(u < t \ \wedge \ reset_x(u) \ \wedge \ \forall w : \ (u < w < t \ \Rightarrow \ \neg\, reset_x(w)) \\ \wedge\, t - u \sim k \Big)$$

- $const_g(t)$ for $g \equiv x \sim k$
- $reset_x(u)$: formula to say x was reset at u (information available from $Y_\alpha(u)$)

Automaton wins $\mathbb{G}(A, w)$

$$\Leftrightarrow$$

Player I wins $\mathbb{G}(\varphi_A, \mathbf{P})$

Section 5:

Deciding McNaughton games

Theorem

Let $\mathbb{T} = [0, N)$. Given an $\mathsf{MSO}(<, +1)$ formula $\varphi(\mathbf{W}, \mathbf{X}, \mathbf{Y})$,
it is **decidable** whether
there exists an interpretation $\mathbf{P}$ of $\mathbf{W}$ over $\mathbb{T}$
such that Player I wins $\mathbb{G}(\varphi, \mathbf{P})$

→ proof on the board

Section 6:

Complexity

Time-bounded emptiness problem

Given an ATA A and a time bound N, is some finite word of duration **at most** N accepted by A?

- The above problem has **non-elementary** lower-bound
- If N is fixed and not part of input, the algorithm is elementary

Take-away

- Time-bounded emptiness of ATA is decidable
- Inclusion and universality for TA over bounded time is decidable
- Decidability of automata through logic

Recommended: Slides of Ouaknine on Time-bounded verification (see course page)