

Reasoning about transfinite sequences

Stéphane Demri

Laboratoire Specification and Verification
CNRS & INRIA & ENS de Cachan
France

Joint work with David Nowak (The University of Tokyo)

Motivation

- Question: How to model the interaction of a computer with a physical system?
 - A physical system can have Zeno behaviors: an infinite number of events happens in a finite amount of time.
Example: a bouncing ball.
 - But, in a finite amount of time, a computer can only make a finite number of computations.
- Our response: Linear-time Temporal Logic + Ordinals.

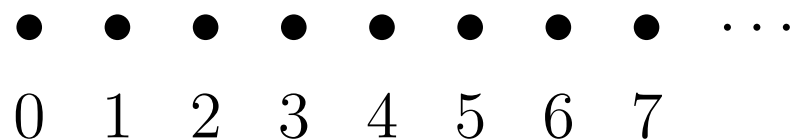
Linear-time temporal logic (LTL)

- LTL is useful to specify and verify temporal properties of computer systems.

$G (\text{Request} \Rightarrow F \text{Grant})$

Always, if there is a request, then, eventually, there is a grant.

- A model for LTL is an infinite sequence of states.



- A state is the set of atomic propositions true at this state.
- A formula describes the set of sequences for which it is true.
(a qualitative property)

A brief recall

- **Syntax**

$$\phi ::= \perp \mid p \mid \neg \phi \mid \phi_1 \wedge \phi_2 \mid \mathbf{X} \phi \mid \phi_1 \mathbf{U} \phi_2$$

- **Semantics**

A model σ is a map from positive integers to sets of atomic formulas.

$$\begin{array}{ll} \sigma, i \models p & \text{iff } p \in \sigma(i) \\ \sigma, i \models \neg \phi & \text{iff not } \sigma, i \models \phi \\ \sigma, i \models \phi_1 \wedge \phi_2 & \text{iff } \sigma, i \models \phi_1 \text{ and } \sigma, i \models \phi_2 \\ \sigma, i \models \mathbf{X} \phi & \text{iff } \sigma, i + 1 \models \phi \\ \sigma, i \models \phi_1 \mathbf{U} \phi_2 & \text{iff there exists } j \text{ such that} \\ & \sigma, i + j \models \phi_2 \\ & \text{and, for all } k < j, \\ & \sigma, i + k \models \phi_1 \end{array}$$

Ordinals

- An ordinal is a totally ordered set which is well ordered, i.e. all its non-empty subsets have a least element. Order-isomorphic ordinals are considered equal.

- Examples:

– $0 = \emptyset, 1 = \bullet, 2 = \bullet\bullet, 3 = \bullet\bullet\bullet, \omega = \bullet\bullet\bullet\bullet\bullet\bullet\bullet\cdots$

– $1 + \omega = \underbrace{\bullet\bullet\bullet\bullet\bullet\bullet\bullet\cdots}_{\omega} = \omega$

– $\omega + 1 = \underbrace{\bullet\bullet\bullet\bullet\bullet\bullet\bullet\cdots}_{\omega} \bullet \neq \omega$

– $2 \times \omega = \underbrace{\underbrace{\bullet\bullet}_{\omega} \underbrace{\bullet\bullet}_{\omega} \underbrace{\bullet\bullet}_{\omega} \underbrace{\bullet\bullet}_{\omega} \underbrace{\bullet\bullet}_{\omega} \underbrace{\bullet\bullet}_{\omega} \cdots}_{\omega} = \omega$

– $\omega \times 2 = \omega + \omega = \underbrace{\bullet\bullet\bullet\bullet\bullet\bullet\bullet\cdots}_{\omega} \underbrace{\bullet\bullet\bullet\bullet\bullet\bullet\bullet\cdots}_{\omega} \neq \omega$

- $\alpha < \beta$ implies there is a unique γ ($\beta - \alpha$) such that $\alpha + \gamma = \beta$.

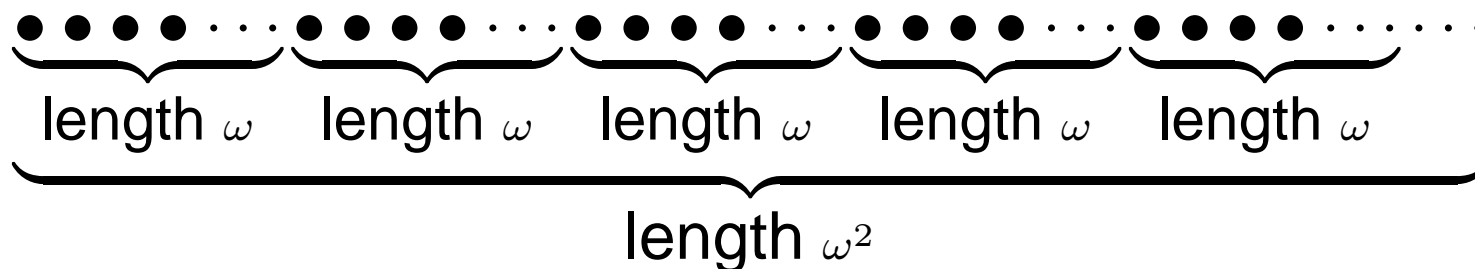
LTL + Ordinals

- A model for LTL is an ω -sequence of states.



- We define a family of logics $LTL(\alpha)$ parameterized by an ordinal α .
- A model for $LTL(\alpha)$ is an α -sequence of states.

Example: $\alpha = \omega^2 = \omega \times \omega$



LTL(α): *syntax and semantics*

- α is closed under addition: for all $\beta, \beta' < \alpha$, $\beta + \beta' < \alpha$.
- $\phi ::= \perp \mid p \mid \neg \phi \mid \phi_1 \wedge \phi_2 \mid \mathbf{X}^\beta \phi \mid \phi_1 \mathbf{U}^{\beta'} \phi_2$
where $\beta < \alpha$ and $\beta' \leq \alpha$.
- Model σ is a map $\alpha \rightarrow 2^{\text{AP}}$ ($\alpha = \{\beta : \beta < \alpha\}$).

$$\sigma, \beta \models p \quad \text{iff} \quad p \in \sigma(\beta)$$

$$\sigma, \beta \models \neg \phi \quad \text{iff} \quad \text{not } \sigma, \beta \models \phi$$

$$\sigma, \beta \models \phi_1 \wedge \phi_2 \quad \text{iff} \quad \sigma, \beta \models \phi_1 \quad \text{and} \quad \sigma, \beta \models \phi_2$$

$$\sigma, \beta \models \mathbf{X}^{\beta'} \phi \quad \text{iff} \quad \sigma, \beta + \beta' \models \phi$$

$$\sigma, \beta \models \phi_1 \mathbf{U}^{\beta'} \phi_2 \quad \text{iff} \quad \text{there exists } \gamma < \beta' \text{ such that}$$

$$\sigma, \beta + \gamma \models \phi_2 \text{ and,}$$

$$\text{for all } \gamma' < \gamma, \text{ we have } \sigma, \beta + \gamma' \models \phi_1$$

- Abbreviations: $\mathbf{F}^{\beta'} \phi \equiv \top \mathbf{U}^{\beta'} \phi$ $\mathbf{G}^{\beta'} \phi \equiv \neg \mathbf{F}^{\beta'} \neg \phi$

Representing ordinals

We use a special case of Cantor Normal Form.

- For any ordinal $\alpha < \omega^\omega$, there are unique integers k_1, \dots, k_p and n_1, \dots, n_p such that $k_1 > \dots > k_p$ and

$$\alpha = \omega^{k_1} \times n_1 + \dots + \omega^{k_p} \times n_p$$

- This provides a representation for ordinals in formula.
- Integers can be represented essentially in unary or in binary.

Logics and formulae

- LTL(1) is the propositional calculus.
- LTL is expressively equivalent to LTL(ω)
Conciseness depends on the encoding of natural numbers.
- “ p holds true on limit ordinals strictly less than ω^k ”:

$$G^{\omega^k} (X^{\omega} p \wedge \dots \wedge X^{\omega^{k-1}} p).$$

- For $1 \leq k' \leq k - 2$, “if p holds infinitely often in states indexed by ordinals of the form $\omega^{k'} \times n$, $n \geq 1$, then q holds in the state indexed by $\omega^{k'+1}$ ”:

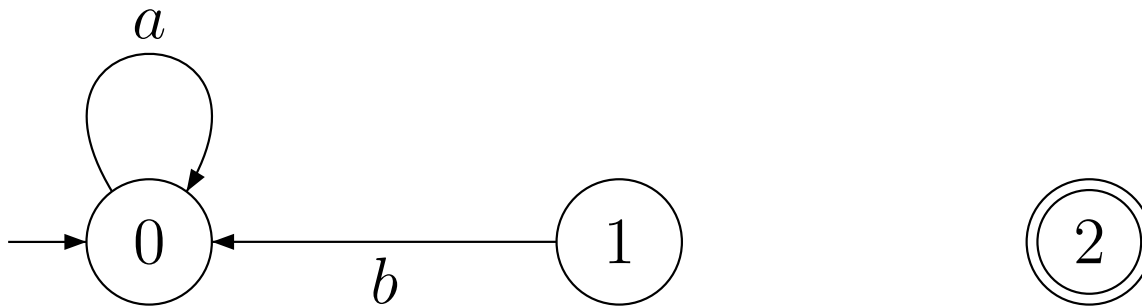
$$(G^{\omega^{k'+1}} F^{\omega^{k'+1}} X^{\omega^{k'}} p) \Rightarrow (X^{\omega^{k'+1}} q).$$

Decidability result

- The satisfiability problem for $LTL(\alpha)$
input : an $LTL(\alpha)$ formula ϕ .
question : is there an $LTL(\alpha)$ model σ such that $\sigma, 0 \models \phi$?
- **Proposition.** Satisfiability for $LTL(\omega^\alpha)$ is decidable with $0 \leq \alpha \leq \omega$.
- Proof by translation into the monadic second order theory of $\langle \omega^\omega, < \rangle$ [Buchi & Siefkes 73].
Translation into first-order fragment [Cachat 05].
- This proof provides a non-elementary complexity upper bound.
- In order to refine complexity results:
 - we restrict ourselves to $LTL(\omega^k)$ where k is an integer.
 - we provide a translation from formula to automata.

Ordinal automata

- Ordinal automata generalize Muller automata:
 - A Muller automaton recognizes ω -sequences.
 - An ordinal automaton recognizes α -sequences.
- Example



Limit transitions: $\{0\} \rightarrow 1$ and $\{0, 1\} \rightarrow 2$

The language $L(\mathcal{A})$ recognized by this automaton \mathcal{A} is $(a^\omega.b)^\omega$.

Definition

- Ordinal automaton $(Q, \Sigma, \delta, E, I, F)$
 - Q is a finite set of states, Σ is a finite alphabet,
 - $\delta \subseteq Q \times \Sigma \times Q$ is a one-step transition relation,
 - $E \subseteq 2^Q \times Q$ is a limit transition relation,
 - $I \subseteq Q$ [resp. $F \subseteq Q$] is a finite set of initial [resp. final] states.
- A path of length $\alpha + 1$ $r : \alpha + 1 \rightarrow Q$
 - for every $\beta \in \alpha$, $r(\beta) \rightarrow r(\beta + 1)$,
 - for every limit ordinal $\beta \in \alpha$, there is $P \rightarrow r(\beta) \in E$ s.t. $P = \text{inf}(\beta, r)$ with
$$\text{inf}(\beta, r) \stackrel{\text{def}}{=} \{q \in Q : \text{for every } \gamma \in \beta, \text{ there is } \gamma' \text{ such that } \gamma < \gamma' < \beta \text{ and } r(\gamma') = q\}.$$

Languages of α -sequences

- Run of length $\alpha + 1$: path of length $\alpha + 1$ such that $r(0) \in I$. If $r(\alpha) \in F$ then r is said to be accepting.
- $L(\mathcal{A})$: set of α -sequences $\sigma : \alpha \rightarrow \Sigma$ for which there is an accepting run r of length $\alpha + 1$ verifying for every $\beta \in \alpha$,
 $r(\beta) \xrightarrow{\sigma(\beta)} r(\beta + 1)$.
- Automata for α -sequences:
 - [Hemmer & Wolper 95], [Bedon 98] (identical definitions),
 - [Bruyère & Carton 01] (more general),
 - [Buchi 64], [Choueka 78], [Wojciechowski 84].

Problems

- Satisfiability.
- Model checking for $LTL(\alpha)$.
input : an ordinal automaton \mathcal{A} with alphabet 2^{AP} and an $LTL(\alpha)$ formula ϕ .
question : is there an α -sequence σ accepted by \mathcal{A} such that $\sigma, 0 \models \phi$?
- Control problem for $LTL(\omega^k)$.
input : an ordinal automaton \mathcal{A} recognizing ω^k -sequences and an $LTL(\omega^k)$ formula ϕ .
question : is there a controller \mathcal{C} such that all the sequences accepted by \mathcal{A} controlled by \mathcal{C} satisfy ϕ ?

Satisfiability and model checking

LTL	PSPACE-complete [Sistla & Clarke 85]
LTL(ω^k) with integers in unary	PSPACE-complete
LTL(ω^k) with integers in binary	EXSPACE-complete
LTL(ω^ω)	?

From formulae to automata

Generalization of the construction for LTL [Vardi & Wolper 94].

- From a formula ϕ , we build an automaton \mathcal{A}_ϕ such that:
 - Its alphabet is 2^{AP} , where AP is the finite set of atomic propositions occurring in ϕ .
 - Its language $L(\mathcal{A}_\phi)$ is precisely the set of $\text{LTL}(\omega^k)$ models satisfying ϕ :

$$L(\mathcal{A}_\phi) = \{\sigma \mid \sigma, 0 \models \phi\}$$

- ϕ is satisfiable iff $L(\mathcal{A}_\phi) \neq \emptyset$.

Closure $cl(\phi)$

- Smallest set of $LTL(\omega^k)$ formulae such that
 - $\perp, \phi \in cl(\phi)$,
 - $\neg\psi \in cl(\phi)$ implies $\psi \in cl(\phi)$,
 - $\psi \in cl(\phi)$ implies $\neg\neg\psi \in cl(\phi)$ (we identify $\neg\neg\psi$ with ψ),
 - $\psi_1 \wedge \psi_2 \in cl(\phi)$ implies $\psi_1, \psi_2 \in cl(\phi)$,
 - $X^\beta\psi \in cl(\phi)$ and $\beta \geq \omega^n$ ($0 \leq n < k$) imply $X^{\beta-\omega^n}\psi \in cl(\phi)$,
 - $\psi_1 U^\beta \psi_2 \in cl(\phi)$ and $\beta \geq \omega^n$ ($0 \leq n \leq k$) imply the formulae below belong to $cl(\phi)$:
 - ψ_1, ψ_2 ,
 - $X^{\omega^n}(\psi_1 U^{\beta-\omega^n} \psi_2), \top U^{\omega^n} \neg\psi_1, \psi_1 U^{\omega^n} \psi_2$.
- There exists a polynomial $p(\cdot)$ such that $\text{card}(cl(\phi))$ is in $2^{\mathcal{O}(p(|\phi|))}$ [resp. $\text{card}(cl(\phi))$ is in $\mathcal{O}(p(|\phi|))$] when integers are encoded in binary [resp. in unary].

Max. consistent set $X \subseteq cl(\phi)$

(mc1) $\perp \notin X$,

(mc2) for every $\psi \in cl(\phi)$, $\psi \in X$ iff $\neg\psi \notin X$,

(mc3) for every $\psi_1 \wedge \psi_2 \in cl(\phi)$, $\psi_1 \wedge \psi_2 \in X$ iff $\psi_1, \psi_2 \in X$,

(mc4) for every $X^0\psi \in cl(\phi)$, $X^0\psi \in X$ iff $\psi \in X$,

(mc5) for every $\psi_1 U^0 \psi_2 \in cl(\phi)$, $\psi_1 U^0 \psi_2 \notin X$,

(mc6) for all $\psi_1 U^\beta \psi_2 \in cl(\phi)$ and $\beta \geq \omega^n \geq 1$, $\psi_1 U^\beta \psi_2 \in X$ iff either
 $\psi_1 U^{\omega^n} \psi_2 \in X$ or $\neg(\top U^{\omega^n} \neg\psi_1)$, $X^{\omega^n}(\psi_1 U^{\beta-\omega^n} \psi_2) \in X$,

(mc7) for all $\psi_1 U^\beta \psi_2, \psi_1 U^{\beta'} \psi_2 \in cl(\phi)$ with $\beta \leq \beta'$, $\psi_1 U^\beta \psi_2 \in X$ implies
 $\psi_1 U^{\beta'} \psi_2 \in X$,

(mc8) for every $\psi_1 U^1 \psi_2 \in cl(\phi)$, $\psi_1 U^1 \psi_2 \in X$ iff $\psi_2 \in X$.

Automaton $\mathcal{A}_\phi = \langle Q, \Sigma, \delta, E, I, F \rangle$

- $\Sigma = 2^{\text{AP}}$,
- $Q = \text{maxcons}(\phi) \times \{0, \dots, k\}$,
- $I = \{\langle X, 0 \rangle \in Q : \phi \in X\}$,
- $F = \{\langle X, n \rangle \in Q : n = k\}$,
- $\langle X, n \rangle \xrightarrow{a} \langle X', n' \rangle \in \delta$ iff (one-step transition)
 - (A1) $n < k$ and $n' = 0$,
 - (A2) $X \cap \text{AP} = a$,
 - (A3) for every $x^\beta \psi \in \text{cl}(\phi)$ such that $\beta \geq 1$, $x^\beta \psi \in X$ iff $x^{\beta-1} \psi \in X'$.

Limit transitions

- $\psi_1 U^\alpha \psi_2 \in cl(\phi)$:

$$P_{\psi_1 U^\alpha \psi_2} = \{ \langle X, n \rangle : \text{either } \psi_2 \in X \text{ or } \neg(\psi_1 U^\alpha \psi_2) \in X \}.$$

- For every $\langle X, n \rangle \in Q$ we write $Q_{\langle X, n \rangle}$ to denote the subset of Q such that for every $\langle X', n' \rangle \in Q$, $\langle X', n' \rangle \in Q_{\langle X, n \rangle} \stackrel{\text{def}}{\iff}$

(A4) $n' < n$,

(A5) for every $X^\alpha \psi \in cl(\phi)$ with $\alpha \geq \omega^n$, $X^\alpha \psi \in X'$ iff $X^{\alpha - \omega^n} \psi \in X$.

- For every $\langle X, n \rangle \in Q$, $Z \rightarrow \langle X, n \rangle \in E$ iff

(A6) $n \geq 1$,

(A7) $Z \subseteq Q_{\langle X, n \rangle}$,

(A8) Z contains a state of the form $\langle Y, n - 1 \rangle$,

(A9) for all $\psi_1 U^\beta \psi_2 \in cl(\phi)$ and $\beta \geq \omega^n$ such that $\neg(\psi_1 U^{\beta - \omega^n} \psi_2) \in X$, $P_{\psi_1 U^\beta \psi_2} \cap Z \neq \emptyset$.

Complexity

- **Proposition.** $L(\mathcal{A}_\phi)$ is the set of models for ϕ .
- \mathcal{A}_ϕ has $2^{2^{\mathcal{O}(|\phi|)}}$ states.
- \mathcal{A}_ϕ has $2^{2^{2^{\mathcal{O}(|\phi|)}}$ transitions.
- The emptiness problem for ordinal automata is in P [Carton 02].
- **Corollary.** For every $k \in \mathbb{N}$, $LTL(\omega^k)$ satisfiability can be solved in triple exponential time.
- We can do better!

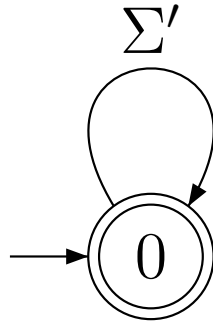
How to get the optimal upper bound

- Introduction of $p(\cdot)$ -succinct ordinal automaton of level k .
 $\langle P_0, P_1, \dots, P_n, q \rangle$ with $n \leq p(|Q|)$ encodes
$$\{P \rightarrow q : P \subseteq Q, \forall i P_i \cap P \neq \emptyset \text{ and } \forall q' \in P, l(q') < l(q)\}.$$
- The translation from ϕ to \mathcal{A}'_ϕ can be done in polynomial [resp. exponential] space.
- **Proposition.** For all $k \geq 0$ and polynom $p(\cdot)$, the emptiness problem for $p(\cdot)$ -succinct ordinal automata of level k is NLOGSPACE-complete.

Hardness of model checking

- Turing machine $M = \langle \Sigma, Q, q_0, \delta \rangle$.
 $\delta : Q \times \Sigma \rightarrow Q \times \Sigma \times \{-1, 0, 1\}$.
Looping for the accepting state `accept`.
- M runs in space 2^{nK} with n the size of the input.

- $\Sigma' = \Sigma \times (Q \times \Sigma)$



$\{0\} \rightarrow 0$.

- input $x = x_1, \dots, x_n$.

$$\triangleright \bigwedge \mathbf{X}^1 \langle q_0, x_1 \rangle \wedge \mathbf{X}^2 x_2 \wedge \dots \wedge \mathbf{X}^n x_n \wedge \mathbf{X}^n \mathbf{G}^{2^{nK} - n} \text{blank}.$$

Encoding acceptance

- Reaching accepting configuration:

$$F^\omega\left(\bigvee_{a \in \Sigma} \langle \text{accept}, a \rangle\right)$$

- Updating configuration (I):

$$G^\omega\left(\bigwedge_{a,b,c \in \Sigma} (a \wedge X^1 b \wedge X^2 c) \Rightarrow X^{2^{n^K} + 1} b\right).$$

- Updating configuration (II):

$$G^\omega\left(\bigwedge_{a,b,c,q,\delta(q,b)=\langle q',b',1 \rangle} (a \wedge X^1 \langle q, b \rangle \wedge X^2 c) \Rightarrow X^{2^{n^K}} a \wedge X^{2^{n^K} + 1} b' \wedge X^{2^{n^K} + 2} \langle q', b' \rangle\right)$$

- etc.

Modelling a physical system

- A physical system is modelled by:
 - a set of actions Act ,
 - a subset of observable actions $Act_o \subseteq Act$,
 - a subset of controllable actions $Act_c \subseteq Act_o$,
 - an ordinal automaton \mathcal{A} with alphabet 2^{Act} (to model *Zeno behaviors*).
- **Example:** A bouncing ball

$$Act = \{\text{lift-up, bounce, stop}\}$$

$$Act_o = \{\text{lift-up, stop}\}$$

$$Act_c = \{\text{lift-up}\}$$

$$\mathcal{A} = \mathcal{A}_\phi$$

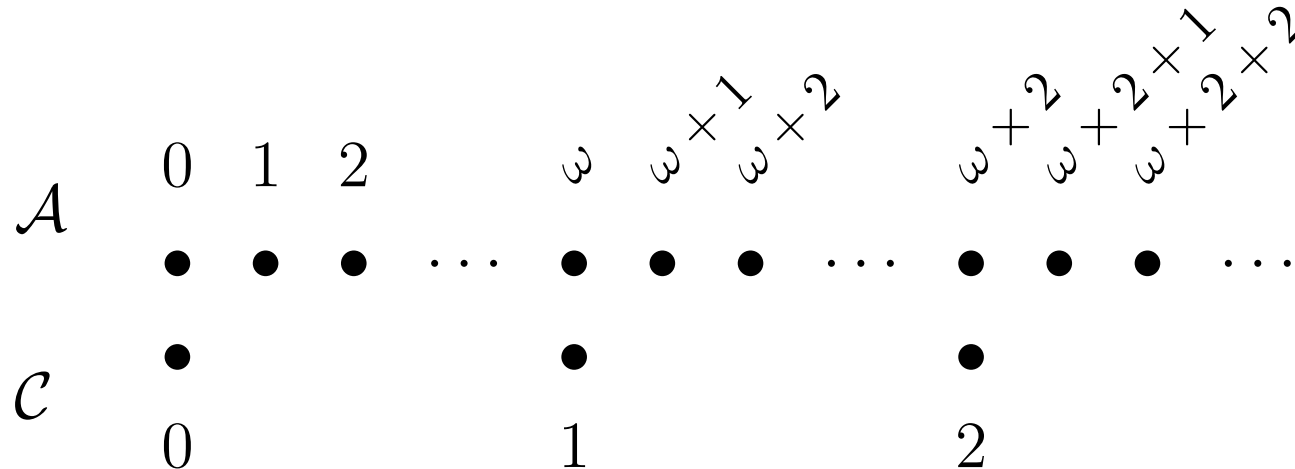
where $\phi = G^{\omega^2} (\text{lift-up} \Rightarrow X^1 (G^\omega \text{ bounce} \wedge X^\omega \text{ stop}))$

When it is lifted-up, it bounces an infinite number of times (in a finite time) and then stops.

Controlling a physical system

- Controller modelled as a Muller automaton \mathcal{C} (recognizing ω -sequences).
- Given a physical system modelled by $\langle Act, Act_o, Act_c, \mathcal{A} \rangle$, and a formula ϕ , a controller \mathcal{C} is a Muller automaton such that

$$lift_k(\mathcal{C}) \times \mathcal{A} \models \phi$$

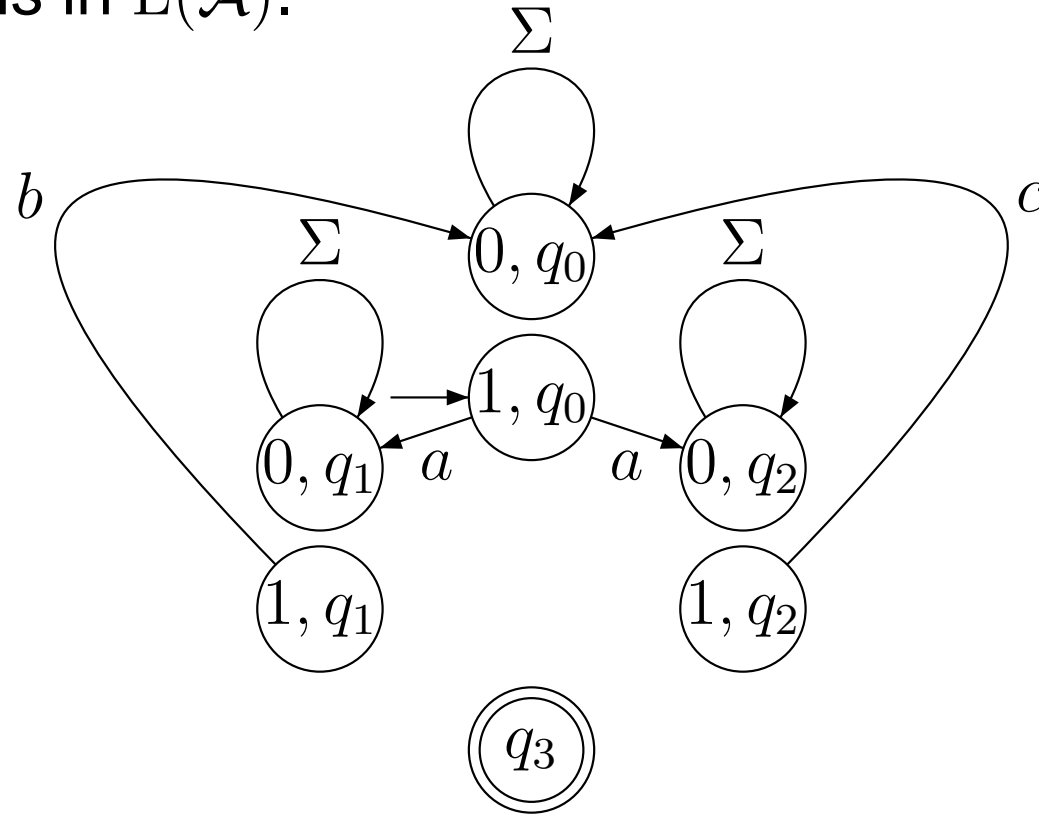
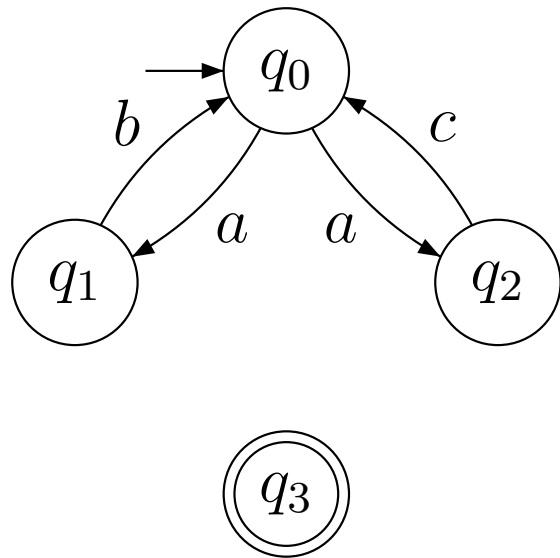


- **Example:** In the case of the bouncing ball, the specification might be that the ball is almost always bouncing:

$$\phi = G^{\omega^2} X^1 \text{ bounce}$$

Lifting

For all $w \in \Sigma^{\omega^k}$, $w \in L(\text{lift}_k(\mathcal{A}))$ iff the word $w' \in \Sigma^\omega$, defined by $w'(i) = w(\omega^{k-1} \times i)$, is in $L(\mathcal{A})$.



$$\{(0, q_0)\} \rightarrow (1, q_0),$$

$$\{(0, q_1)\} \rightarrow (1, q_1), \{(0, q_2)\} \rightarrow (1, q_2)$$

$$\{(0, q_0), (1, q_0), (0, q_1), (1, q_1), (0, q_2), (1, q_2)\} \rightarrow q_3$$

$$\{q_0, q_1, q_2\} \rightarrow q_3$$

Control problem for $LTL(\omega^k)$

input : a physical system $\langle Act, Act_o, Act_c, \mathcal{A} \rangle$ where \mathcal{A} recognizes ω^k -sequences and an $LTL(\omega^k)$ formula ϕ .

question : is there a Büchi/Muller automaton \mathcal{C} on the alphabet 2^{Act_o} such that

- all the sequences accepted by \mathcal{A} synchronized with $lift_k(\mathcal{C})$ satisfy ϕ ,
- for every state q of \mathcal{C} , $q \xrightarrow{\emptyset} q$,
- $\forall q \cdot \forall a \subseteq Act_o \setminus Act_c$, there is a transition $q \xrightarrow{b} q'$ in \mathcal{C} such that $b \cap Act_{nc} = a$.

The synchronization vectors $\langle a, b, c \rangle \in 2^{Act} \times 2^{Act_o} \times 2^{Act}$ satisfy $a = c$ and $a \cap Act_o = b$.

Some other related works

- [Buchi 64]: decidability of monadic second-order theory of $\langle \alpha, < \rangle$ for countable α .
- [Godefroid and Wolper 94]
 - First use of automata recognizing transfinite words for verification problem.
 - Model concurrency by limiting state explosion.
- [Berard and Picaronny 97]
 - Timed automata accepting Zeno words.
 - Modeling physical phenomena with convergent execution.
 - Decidability of the emptiness problem.
- [Rohde, 97]: LTL(X, U) interpreted over α -sequences.
 - The satisfiability problem can be decided in EXPTIME.
(input: a formula and an ordinal)
- [Baaz & Leitsch & Zach 96]: temporal logic with time-gaps.

Summary of contributions

- Family of logics $LTL(\alpha)$ where α is any countable ordinal closed under addition.
- Translation from formulae to automata.
- Succinct ordinal automata.
- Complexity results which extend the ones for LTL.
- Application to the control of a physical system by a computer.

Work in progress

- Controller synthesis / Games (T. Cachat).
- $LTL(\alpha)$ + variables and limits (with D. Nowak).
- Decidability of each $LTL(\alpha)$ with α countable and closed under addition.
- Computational complexity of $LTL(\omega^\omega)$.
- P-hardness of the emptiness problem for ordinal automata.
- Axiomatization, extension of Kamp's Theorem.