Department of Mathematics, Computer Science and Physics, University of Udine

Succinctness of Linear Temporal Logic with Past

Luca Geatti
luca.geatti@uniud.it
Angelo Montanari
angelo.montanari@uniud.it

April 23, 2024

Outline

LTL+P is the extension of LTL with past temporal operators.

We will prove the following result.

Theorem

LTL+P *can be exponentially more succinct than* LTL.

Reference:

Nicolas Markey (2003). "Temporal logic with past is exponentially more succinct". In: *Bull. EATCS* 79, pp. 122–128

Outline:

1. Recap of past temporal operators of LTL+P
2. Transformation of LTL+P formulas into equivalent NBA (Nondeterministic Büchi Automata)
3. Proof of the succinctness result.

The syntax of LTL+P is defined as follows:

$$\begin{aligned} \phi := p \mid \neg\phi \mid \phi \vee \phi & \quad \text{Boolean Modalities with } p \in \mathcal{AP} \\ \mid \mathsf{X}\phi \mid \phi\,\mathsf{U}\,\phi & \quad \text{Future Temporal Modalities} \\ \mid \mathsf{Y}\phi \mid \phi\mathsf{S}\phi & \quad \text{Past Temporal Modalities} \end{aligned}$$

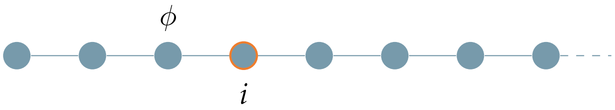
- $\mathsf{Y}\phi$ is the Yesterday operator: *the previous time point exists and it satisfies the formula* ϕ
- $\phi_1 \,\mathsf{S}\, \phi_2$ is the Since operator: *there exists a time point in the past where* ϕ_2 *is true, and* ϕ_1 *holds since (and excluding) that point up to now.*

Shortcuts:

- Once, $\mathsf{O}\phi$: *there exists a time point in the past where* ϕ *holds.* $\mathsf{O}\phi \equiv \top \,\mathsf{S}\, \phi$.
- Historically, $\mathsf{H}\phi$: *for all time points in the past* ϕ *holds.* $\mathsf{H}\phi \equiv \neg(\mathsf{O}\neg\phi)$.

We say that σ satisfies at position i the LTL formula ϕ, written $\sigma, i \models \phi$, iff:

- $\sigma, i \models \mathsf{Y}\phi$ iff $i > 0$ and $\sigma, i-1 \models \phi$

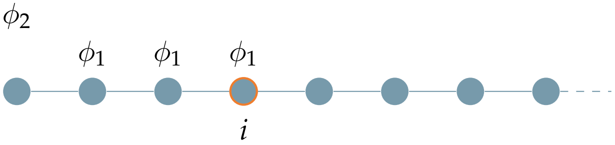


position i has a predecessor and ϕ holds at the *previous* position of i

Note: $\sigma, 0 \models \mathsf{Y}\phi$ is always false.

We say that σ satisfies at position i the LTL formula ϕ, written $\sigma, i \models \phi$, iff:

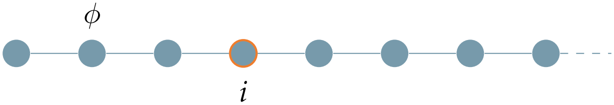
- $\sigma, i \models \phi_1 \mathsf{S}\, \phi_2$ iff $\exists j \leq i \,.\, \sigma, j \models \phi_2$ and $\forall j < k \leq i \,.\, \sigma, k \models \phi_1$



ϕ_1 holds *since* ϕ_2 held

Shortcuts:

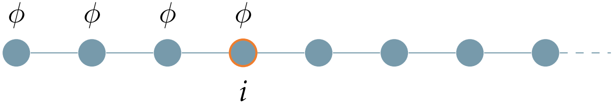
- (*once*) $\mathsf{O}\phi \equiv \top \ \mathsf{S} \ \phi$



ϕ *once* held

Shortcuts:

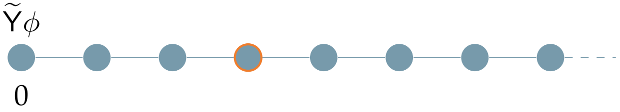
- (*historically*) $\mathsf{H}\phi \equiv \neg\mathsf{O}\neg\phi$



ϕ holds *always in the past*

Shortcuts:

- *(weak yesterday)* $\widetilde{\mathsf{Y}}\phi \equiv \neg\mathsf{Y}\neg\phi$



ϕ holds at the *previous* position of i, *if any*

Note: $\sigma, i \models \widetilde{\mathsf{Y}}\bot$ is true iff $i = 0$.

Notation

Notation:

- we will write $\phi \in \mathsf{LTL}$ (resp., $\phi \in \mathsf{LTL{+}P}$) to denote the fact that ϕ is a formula of LTL (resp., $\mathsf{LTL{+}P}$)
- we will denote with $|\phi|$ the *size* of ϕ, defined as the size of its parse tree.

Exercises useful for the succinctness proof.

Exercise 1

$$\sigma, i \models \widetilde{\mathsf{Y}}\bot \quad \Leftrightarrow \quad i \ ?$$

Exercises useful for the succinctness proof.

Exercise 1

$$\sigma, i \models \widetilde{\mathsf{Y}}\bot \quad \Leftrightarrow \quad i \quad = 0$$

Exercise

Exercises useful for the succinctness proof.

Exercise 2

$$\sigma, i \models \widetilde{\mathsf{Y}}\widetilde{\mathsf{Y}}\widetilde{\mathsf{Y}}\bot \quad \Leftrightarrow \quad i \ ?$$

Exercise

Exercises useful for the succinctness proof.

Exercise 2

$$\sigma, i \models \widetilde{\mathsf{Y}}\widetilde{\mathsf{Y}}\widetilde{\mathsf{Y}}\bot \quad \Leftrightarrow \quad i \quad \leq 2$$

Exercise

Exercises useful for the succinctness proof.

Exercise 3

$$\sigma, i \models ? \qquad \Leftrightarrow \quad i \geq 2$$

Exercises useful for the succinctness proof.

Exercise 3

$$\sigma, i \models \mathsf{Y}\mathsf{Y}\top \quad \Leftrightarrow \quad i \geq 2$$

Exercises useful for the succinctness proof.

Exercise 4

$$\sigma, i \models ? \qquad \Leftrightarrow \qquad i = 2$$

Exercises useful for the succinctness proof.

Exercise 4

$$\sigma, i \models \widetilde{\mathsf{Y}}\widetilde{\mathsf{Y}}\widetilde{\mathsf{Y}}\bot \wedge \mathsf{Y}\mathsf{Y}\top \quad \Leftrightarrow \quad i = 2$$

From LTL+P to NBA

Goal

For any formula ϕ of LTL+P over the atomic propositions $\mathcal{AP}$, we will build a NBA $\mathcal{A}_\phi$ over the alphabet $\Sigma := 2^{\mathcal{AP}}$ such that $\mathcal{L}(\phi) = \mathcal{L}(\mathcal{A}_\phi)$.

Definition (Extended Closure)

For any formula ϕ of LTL+P, we define the extended closure of ϕ, denoted with $\mathcal{C}(\phi)$, as the smallest set of formulas such that:

- $\phi \in \mathcal{C}(\phi)$;
- if $\alpha \in \mathcal{C}(\phi)$ and β is a subformula of α, then $\beta \in \mathcal{C}(\phi)$;
- if $\alpha \in \mathcal{C}(\phi)$, then $\neg\alpha \in \mathcal{C}(\phi)$; (n.b. we identify $\neg\neg\alpha$ with α)
- if $\alpha \mathsf{U} \beta \in \mathcal{C}(\phi)$, then $\mathsf{X}(\alpha \mathsf{U} \beta) \in \mathcal{C}(\phi)$;
- if $\alpha \mathsf{S} \beta \in \mathcal{C}(\phi)$, then $\{\mathsf{Y}(\alpha \mathsf{S} \beta), \widetilde{\mathsf{Y}}(\alpha \mathsf{S} \beta)\} \subseteq \mathcal{C}(\phi)$.

States of $\mathcal{A}_\phi$

A state of the NBA $\mathcal{A}_\phi$ is any subset $S \subseteq \mathcal{C}(\phi)$ such that:

- the conjunction of all *propositional formulas* in S is satisfiable; (*local consistency*)
- for all $\alpha \in \mathcal{C}(\phi)$, it holds that $\alpha \in S$ iff $\neg\alpha \notin S$;
- for all $\alpha := \alpha_1 \wedge \alpha_2$, it holds that $\alpha \in S$ iff $\{\alpha_1, \alpha_2\} \subseteq S$
- $\ldots$
- for all $\alpha := \alpha_1 \mathsf{U}\, \alpha_2$, it holds that $\alpha \in S$ iff either $\alpha_2 \in S$ or $\{\alpha_1, \mathsf{X}\alpha\} \subseteq S$;
- for all $\alpha := \alpha_1 \mathsf{S}\, \alpha_2$, it holds that $\alpha \in S$ iff either $\alpha_2 \in S$ or $\{\alpha_1, \mathsf{Y}\alpha\} \subseteq S$.

Initial states of $\mathcal{A}_\phi$

A state $S \subseteq \mathcal{C}(\phi)$ is initial for $\mathcal{A}_\phi$ iff $\phi \in S$ and S does not contain any formula of type $\mathsf{Y}\alpha$ or $\neg\widetilde{\mathsf{Y}}\alpha$.

Transitions of $\mathcal{A}_\phi$

For any two states $S, S' \subseteq \mathcal{C}(\phi)$, there is a transition from S to S' labelled with $a \in \Sigma$ in the automaton $\mathcal{A}_\phi$ iff:

- the label of the transition is consistent with the source state (recall that $\Sigma := 2^{\mathcal{AP}}$):

$$p \in a \; \leftrightarrow p \in P \qquad \forall p \in \mathcal{AP}$$

- $\mathsf{X}\alpha \in S$ iff $\alpha \in S'$, for all $\mathsf{X}\alpha \in \mathcal{C}(\phi)$;
- $\mathsf{Y}\alpha \in S'$ iff $\alpha \in S$, for all $\mathsf{Y}\alpha \in \mathcal{C}(\phi)$;
- $\widetilde{\mathsf{Y}}\alpha \in S'$ iff $\alpha \in S$, for all $\widetilde{\mathsf{Y}}\alpha \in \mathcal{C}(\phi)$.

Final states of $\mathcal{A}_\phi$

For every $\alpha := \alpha_1 U \alpha_2 \in \mathcal{C}(\phi)$, we say that a state S is α-fulfilling iff
$\alpha \in S \;\rightarrow\; \alpha_2 \in S$.
A state of $\mathcal{A}_\phi$ is final iff is α-fulfilling *for some* $\alpha := \alpha_1 U \alpha_2 \in \mathcal{C}(\phi)$.

Generalized Büchi Condition

A generalized Büchi automaton is a tuple $\mathcal{A} = \langle Q, \Sigma, I, \Delta, \mathcal{F} \rangle$ such that
$\mathcal{F} := \{F_1, \ldots, F_n\}$, for some $n \in \mathbb{N}$, where $F_i \subseteq Q$ for each $1 \leq i \leq n$.
A run π is *accepting* for $\mathcal{A}$ iff, *for all* $1 \leq i \leq n$, we have that $\mathtt{Inf}(\pi) \cap F_i \neq \varnothing$.

We define $\mathcal{A}_\phi$ as a Generalized NBA with the collection of final states defined as follows:

$$\mathcal{F} := \{F_\alpha \mid \alpha := \alpha_1 \,\mathsf{U}\, \alpha_2 \in \mathcal{C}(\phi), F_\alpha := \{S \mid S \text{ is an } \alpha\text{-fulfilling state}\}\}$$

For the details about the translation of LTL+P into Generalized NBA see:

Reference:

Rob Gerth et al. (1995). "Simple on-the-fly automatic verification of linear temporal logic". In: *International Conference on Protocol Specification, Testing and Verification*. Springer, pp. 3–18

Generalized NBA can be degeneralized, *e.g.*, using a counter.

Reference:

Yaacov Choueka (1974). "Theories of automata on ω-tapes: A simplified approach". In: *Journal of computer and system sciences* 8.2, pp. 117–141

Alternatively, we can use the Müller condition.

Müller Condition

A Müller automaton is a tuple $\mathcal{A} = \langle Q, \Sigma, I, \Delta, \mathcal{F} \rangle$ such that $\mathcal{F} := \{F_1, \ldots, F_n\}$, for some $n \in \mathbb{N}$, where $F_i \subseteq Q$ for each $1 \leq i \leq n$.
A run π is *accepting* for $\mathcal{A}$ iff, *for some* $1 \leq i \leq n$, we have that $\mathtt{Inf}(\pi) = F_i$.

We can define $\mathcal{A}_\phi$ as a Müller automaton with the collection of final states defined as follows:

$$\mathcal{F} := \{F \subseteq Q \mid \forall \alpha := \alpha_1 \mathsf{U}\, \alpha_2 \in \mathcal{C}(\phi)\ .\ \exists S_\alpha \in F \text{ and } S_\alpha \text{ is } \alpha\text{-fulfilling}\}$$

Some tools:

- LTL2BA (http://www.lsv.fr/ gastin/ltl2ba/) by Paul Gastin and Denis Oddoux (simple, does not always give a pruned automaton)
- Rabinizer 4 (https://www7.in.tum.de/ kretinsk/rabinizer4.html) by Jan Kretinsky, Tobias Meggendorfer, Salomon Sickert (et al.)
- OWL (https://owl.model.in.tum.de) by Jan Křetínský, Tobias Meggendorfer, Salomon Sickert

How can we solve LTL+P satisfiability using the translation of LTL+P formulas into NBA?

How can we solve LTL+P satisfiability using the translation of LTL+P formulas into NBA?

1. Let ϕ be a LTL+P formula
2. Build the NBA $\mathcal{A}_\phi$ equivalent to ϕ
3. Check for the emptiness of $\mathcal{A}_\phi$
   - if $\mathcal{L}(\mathcal{A}_\phi) = \varnothing$, then ...
   - otherwise, ...

How can we solve LTL+P satisfiability using the translation of LTL+P formulas into NBA?

1. Let ϕ be a LTL+P formula
2. Build the NBA $\mathcal{A}_\phi$ equivalent to ϕ
3. Check for the emptiness of $\mathcal{A}_\phi$
   - if $\mathcal{L}(\mathcal{A}_\phi) = \varnothing$, then ϕ is unsatisfiable
   - otherwise, ϕ is satisfiable

How can we solve LTL+P satisfiability using the translation of LTL+P formulas into NBA?

1. Let ϕ be a LTL+P formula
2. Build the NBA $\mathcal{A}_\phi$ equivalent to ϕ
3. Check for the emptiness of $\mathcal{A}_\phi$
   - if $\mathcal{L}(\mathcal{A}_\phi) = \varnothing$, then ϕ is unsatisfiable
   - otherwise, ϕ is satisfiable

Complexity:

- Step 2 is exponential in the size of ϕ
- Step 3 can be done in nondeterministic logarithmic space (Savitch Theorem)
- Steps 2 and 3 can be performed on-the-fly: thus, the complexity of the procedure is polynomial space (PSPACE).

We will prove the following result.

Theorem

LTL+P *can be exponentially more succinct than* LTL.

Reference:

Nicolas Markey (2003). "Temporal logic with past is exponentially more succinct". In: *Bull. EATCS* 79, pp. 122–128

- past temporal operators do *not* add expressive power
- but they add *succinctness power*

LTL+P can be exponentially more succinct than LTL

There exists a *family* of languages $\{\mathcal{L}_n\}_{n=1}^{\infty} \subseteq (2^{\mathcal{AP}_n})^\omega$ such that:

- for all $n > 0$, $\mathcal{L}_n$ is definable in LTL+P with a formula of size $\mathcal{O}(n)$, *i.e.*,

$$\forall n > 0 \;.\; \exists \phi \in \mathsf{LTL+P} \;.\; (\mathcal{L}(\phi) = \mathcal{L}_n \wedge |\phi| \in \mathcal{O}(n))$$

- for all $n > 0$, $\mathcal{L}_n$ is *not* definable in LTL with formulas of size *less* than exponential in n, *i.e.*,

$$\forall n > 0 \;.\; \forall \psi \in \mathsf{LTL} \;.\; (\mathcal{L}(\psi) = \mathcal{L}_n \rightarrow |\psi| \in 2^{\Omega(n)})$$

Definition of the candidate family of l...

Definition (Family of languages $\{A_n\}_{n=1}^{\infty}$)

For all $n > 0$, we define $\mathcal{AP}_n := \{p_0, \ldots, p_n\}$ and we define the language $A_n \subseteq (2^{\mathcal{AP}_n})^\omega$ as follows:

A_n is the set of words in which, if any position i agrees with position 0 on the interpretation of all $p_1, \ldots, p_n$, then i and 0 agree also on the interpretation of p_0.

Example with n=2 and $\mathcal{AP}_n = \{p_0, p_1, p_2\}$

- $\{p_0, p_2\} \cdot (\langle\{p_1\} \cdot \{p_1, p_2\} \cdot \varnothing\rangle)^\omega \in A_n$
- $\{p_0, p_2\} \cdot (\langle\{p_1\} \cdot \{p_0, p_2\} \cdot \varnothing\rangle)^\omega \in A_n$
- $\{p_0, p_1, p_2\} \cdot (\langle\{p_1\} \cdot \{p_1, p_2\} \cdot \varnothing\rangle)^\omega \notin A_n$

A_n is succinctly definable in LTL+P

Proposition

For all $n > 0$, the language A_n is definable by a formula of LTL+P of size $\mathcal{O}(n)$.

Proof.

For all $n > 0$, we define the LTL+P formula equivalent to A_n as follows:

$$\mathsf{G}\big((\bigwedge_{i=1}^{n}(p_i \leftrightarrow \mathsf{O}(\widetilde{\mathsf{Y}}\bot \wedge p_i))) \;\rightarrow\; (p_0 \leftrightarrow \mathsf{O}(\widetilde{\mathsf{Y}}\bot \wedge p_0))\big)$$

□

We will prove the following result which, together with the previous Proposition, proves that LTL+P can be exponentially more succinct than LTL.

Lemma

For each $n > 0$, the language A_n is not definable in LTL with formulas of size less than exponential in n.

In order to prove it, we first define another family of languages.

Definition of the family of languages B_n

Definition (Family of languages $\{B_n\}_{n=1}^{\infty}$)

For all $n > 0$, we define $\mathcal{AP}_n := \{p_0, \ldots, p_n\}$ and we define the language $B_n \subseteq (2^{\mathcal{AP}_n})^\omega$ as follows:

> *B_n is the set of words in which, if any two position i agrees with position j on the interpretation of all $p_1, \ldots, p_n$, then i and j agree also on the interpretation of p_0.*

Example with n=2 and $\mathcal{AP}_n = \{p_0, p_1, p_2\}$

- $\{p_0, p_2\} \cdot (\langle\{p_1\} \cdot \{p_1, p_2\} \cdot \varnothing\rangle)^\omega \in B_n$
- $(\langle\{p_0, p_2\} \cdot \{p_1\} \cdot \{p_0, p_2\} \cdot \varnothing \cdot \{p_1\}\rangle)^\omega \in B_n$
- $(\langle\{p_0, p_2\} \cdot \{p_1\} \cdot \{p_0, p_2\} \cdot \varnothing \cdot \{p_0, p_1\}\rangle)^\omega \notin B_n$

Connection between A_n and B_n

Lemma

For all $n > 0$, if A_n were definable in LTL *with formulas of size less than exponential in n, then also B_n is expressible in* LTL+P *with formulas of size less than exponential in n.*

Proof.

For all $n > 0$, by hypothesis there exists a formula $\phi_n \in \mathsf{LTL}$ such that $\mathcal{L}(\phi_n) = A_n$ and $|\phi_n|$ is less than $2^{\mathcal{O}(n)}$.

Connection between A_n and B_n

Lemma

For all $n > 0$, if A_n were definable in LTL *with formulas of size less than exponential in n, then also B_n is expressible in* LTL+P *with formulas of size less than exponential in n.*

Proof.

Since ϕ_n contains only *future* temporal operators, it holds that the language of the formula $\psi_n := \mathsf{G}(\phi_n)$ is exactly B_n, because:

- since ϕ_n contains only future operators, $\sigma \models \mathsf{G}(\phi_n)$ iff *all* suffixes of σ are models of ϕ_n
- by definition of ϕ_n, this is equivalent of saying that for all i and for all $j > i$, if σ_i and σ_j agree on $p_1, \ldots, p_n$, then they also agree on p_0.
- by definition of B_n, this is equivalent to $\sigma \in B_n$.

Connection between A_n and B_n

Lemma

For all $n > 0$, <u>if</u> A_n were definable in LTL with formulas of size less than exponential in n, <u>then</u> also B_n is expressible in $\mathsf{LTL{+}P}$ with formulas of size less than exponential in n.

Proof.

Moreover, $\psi_n := \mathsf{G}(\phi_n)$ is trivially a formula of $\mathsf{LTL{+}P}$ and $|\psi_n| = |\phi_n| + 1$, therefore B_n is expressible in $\mathsf{LTL{+}P}$ with a formula of size less than exponential in n. □

Connection between A_n and B_n

Lemma

For all $n > 0$, <u>if</u> A_n were definable in LTL *with formulas of size less than exponential in n, <u>then</u> also B_n is expressible in* LTL+P *with formulas of size less than exponential in n.*

Proof.

Moreover, $\psi_n := \mathsf{G}(\phi_n)$ is trivially a formula of LTL+P and $|\psi_n| = |\phi_n| + 1$, therefore B_n is expressible in LTL+P with a formula of size less than exponential in n. $\square$

We will show that the consequent of the above implication is false.

This implies that A_n cannot be defined succinctly in LTL.

Explosion of B_n

Lemma

For all $n > 0$, B_n is expressible in LTL+P *only with formulas of size at least exponential in n, i.e.:*

$$\forall n > 0 \,.\, \forall \psi \in \mathsf{LTL{+}P} \,.\, (\mathcal{L}(\psi) = B_n \;\rightarrow\; |\psi| \in 2^{\Omega(n)})$$

Proof.

The proof is based on the following two points:

1. Each LTL+P formula ϕ can be translated into an equivalent NBA of size *at most exponential* in $|\phi|$;
   - this is what we saw at the beginning of the lecture
2. Any NBA over $2^{\mathcal{AP}_n}$ recognizing B_n is of size $2^{2^{\Omega(n)}}$.
   - we will prove it later.

Lemma

For all $n > 0$, B_n is expressible in LTL+P *only with formulas of size at least exponential in n*, i.e.*:*

$$\forall n > 0 \,.\, \forall \psi \in \mathsf{LTL{+}P} \,.\, (\mathcal{L}(\psi) = B_n \;\rightarrow\; |\psi| \in 2^{\Omega(n)})$$

Proof.

- Suppose by contradiction that there exists a $n > 0$ and a formula $\phi \in \mathsf{LTL{+}P}$ such that $\mathcal{L}(\phi) = B_n$ and $|\phi|$ is less than exponential in n.
- Then, by Point 1, there exists a NBA $\mathcal{A}_\phi$ such that $\mathcal{L}(\mathcal{A}_\phi) = B_n$ and the size of $\mathcal{A}_\phi$ is less than *doubly exponential* in n.
- However, this is a contradiction with Point 2.

$\square$

The last bit that it is left to prove is the following *doubly exponential* lower bound.

Lemma

For all $n > 0$, any NBA *over $2^{\mathcal{AP}_n}$ recognizing B_n is of size $2^{2^{\Omega(n)}}$.*

Consider the set $\mathcal{AP}_n \setminus \{p_0\} := \{p_1, \ldots, p_n\}$. Let $\overline{a}$ be an *arbitrary* sequence of the 2^n subsets of $\mathcal{AP}_n \setminus \{p_0\}$:

$$\overline{a} := \langle a_0, \ldots, a_{2^n - 1} \rangle$$

From now on, we fix such a sequence $\overline{a}$.

Example with $n = 3$

$\mathcal{AP}_n \setminus \{p_0\} := \{p_1, p_2, p_3\}$.

$$\begin{aligned} \overline{a} &:= \langle a_0, \ldots, a_7 \rangle \\ &:= \langle \{p_1\}, \{p_1, p_2\}, \varnothing, \{p_3\}, \{p_3, p_2\}, \{p_1, p_2, p_3\}, \{p_2\}, \{p_2, p_3\} \rangle \end{aligned}$$

Doubly exponential lower bound
for any automaton recognizing B_n

For any $K \subseteq \{0, \ldots, 2^n - 1\}$, we define:

$$a_i^K := \begin{cases} a_i & \text{iff } i \notin K \\ a_i \cup \{p_0\} & \text{otherwise} \end{cases}$$

For any $K \subseteq \{0, \ldots, 2^n - 1\}$, we define $\overline{a^K} := \langle a_0^K, \ldots, a_{2^n-1}^K \rangle$.

Example with $n = 3$

- if $\overline{a} := \langle \{p_1\}, \{p_1, p_2\}, \varnothing, \{p_3\}, \{p_3, p_2\}, \{p_1, p_2, p_3\}, \{p_2\}, \{p_2, p_3\} \rangle$ and
- if $K := \{1, 7\}$
- then $\overline{a^K} := \langle \{p_1\}, \{p_1, p_2, p_0\}, \varnothing, \{p_3\}, \{p_3, p_2\}, \{p_1, p_2, p_3\}, \{p_2\}, \{p_2, p_3, p_0\} \rangle$

For any $K \subseteq \{0, \ldots, 2^n - 1\}$, we define:

$$a_i^K := \begin{cases} a_i & \text{iff } i \notin K \\ a_i \cup \{p_0\} & \text{otherwise} \end{cases}$$

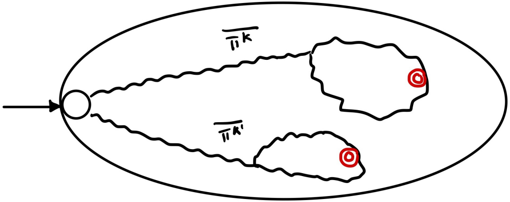
For any $K \subseteq \{0, \ldots, 2^n - 1\}$, we define $\overline{a^K} := \langle a_0^K, \ldots, a_{2^n-1}^K \rangle$.

- Clearly, two distinct $K, K' \subseteq \{0, \ldots, 2^n - 1\}$ lead to two different sequences $\overline{a^K}$ and $\overline{a^{K'}}$.
- There are 2^{2^n} different choices for $K \subseteq \{0, \ldots, 2^n - 1\}$.
- There are 2^{2^n} different words $\overline{a^K}$.

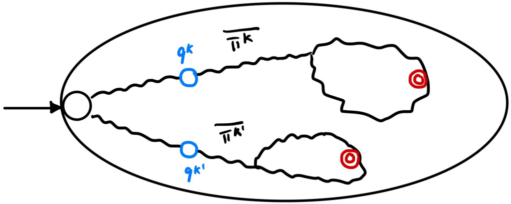
Doubly exponential lower bound
for any automaton recognizing B_n

- Let K and K' be two distinct subsets of $\{0, \ldots, 2^n - 1\}$.
- The word $(\overline{a^K})^\omega$ belongs to B_n because:
  - by construction of $\bar{a}$, two positions i and j agree on $p_1, \ldots, p_n$ iff they belong to "*different repetitions*" of $\overline{a^K}$;
  - since the set K never changes between different repetitions of $\overline{a^K}$, we have that i and j also agree on p_0.
- With the same line of reasoning, we have that also the word $(\overline{a^K})^\omega \in B_n$.
- Since by hypotesis, the automaton $\mathcal{A}$ recognizes B_n, both $(\overline{a^K})^\omega$ and $(\overline{a^{K'}})^\omega$ are *accepted* by $\mathcal{A}$.

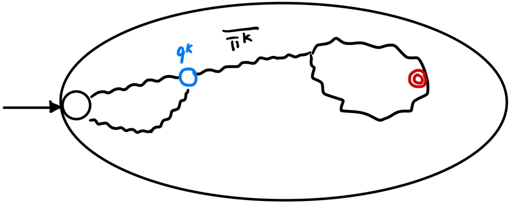
- Therefore, there exists two accepting runs $\overline{\pi^K}$ and $\overline{\pi^{K'}}$ in $\mathcal{A}$ induced by $(\overline{a^K})^\omega$ and $(\overline{a^{K'}})^\omega$, respectively.



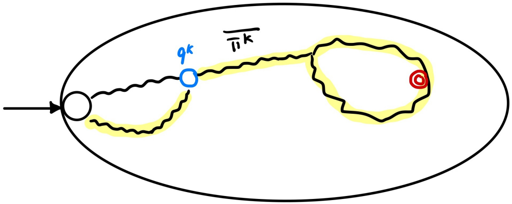
- Therefore, there exists two accepting runs $\overline{\pi^K}$ and $\overline{\pi^{K'}}$ in $\mathcal{A}$ induced by $(\overline{a^K})^\omega$ and $(\overline{a^{K'}})^\omega$, respectively.
- Let q^K (resp., $q^{K'}$) be the 2^n-th state of $\overline{\pi^K}$ (resp., $\overline{\pi^{K'}}$)



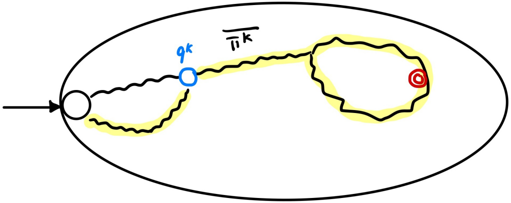
- Suppose that $q^K = q^{K'}$.



- Suppose that $q^K = q^{K'}$.
- The sequence of states made of the prefix of $\overline{\pi^{K'}}$ concatenated to the suffix of $\overline{\pi^{K}}$ is an *accepting run*
- and it is induced by the word $\overline{a^k} \cdot (\overline{a^{K'}})^{\omega}$.



- However, the word $\overline{a^K} \cdot (\overline{a^{K'}})^\omega$ does *not* belong to B_n
  - because it contains at least two positions that agree on $p_1, \ldots, p_n$ but not on p_0 (since $K \neq K'$).
- This means that it cannot be the case that $q^K = q^{K'}$.
- Therefore, since there are 2^{2^n} of different K, there are also 2^{2^n} different q^K.
- The automaton for B_n has at least 2^{2^n} states.



Lemma

For all $n > 0$, B_n *is recognizable only by* NBA *of size at least doubly exponential in* n.

Lemma

For all $n > 0$, B_n *is expressible in* LTL+P *only with formulas of size at least exponential in* n.

Lemma

For all $n > 0$, A_n *is expressible in* LTL *only with formulas of size at least exponential in* n.

Theorem

LTL+P *can be exponentially more succinct than* LTL.

REFERENCES

Bibliography I

Yaacov Choueka (1974). "Theories of automata on ω-tapes: A simplified approach". In: *Journal of computer and system sciences* 8.2, pp. 117–141.

Rob Gerth et al. (1995). "Simple on-the-fly automatic verification of linear temporal logic". In: *International Conference on Protocol Specification, Testing and Verification*. Springer, pp. 3–18.

Nicolas Markey (2003). "Temporal logic with past is exponentially more succinct". In: *Bull. EATCS* 79, pp. 122–128.