

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

The Safety Fragment of Temporal Logics on Infinite Sequences

Lesson 14

Luca Geatti

luca.geatti@uniud.it

Angelo Montanari

angelo.montanari@uniud.it

May 20th, 2024



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:

$\phi := p \mid \neg\phi \mid \phi \vee \phi$	Boolean Modalities with $p \in \mathcal{AP}$
$\mid X\phi \mid \phi U \phi$	Future Temporal Modalities
$\mid Y\phi \mid \phi S\phi$	Past Temporal Modalities

- $Y\phi$ is the **Yesterday** operator: *the previous time point exists and it satisfies the formula ϕ*
- $\phi_1 S \phi_2$ 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.*

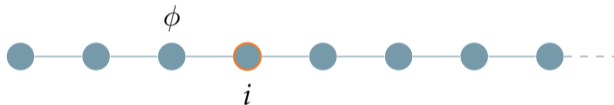
Shortcuts:

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



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

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



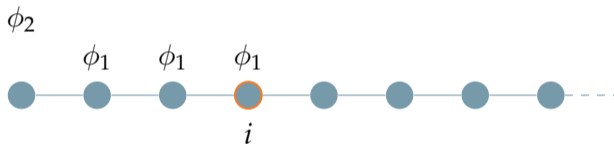
position i has a predecessor and ϕ holds at the *previous* position of i

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



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

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

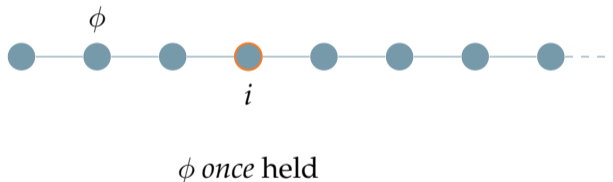


ϕ_1 holds *since* ϕ_2 held



Shortcuts:

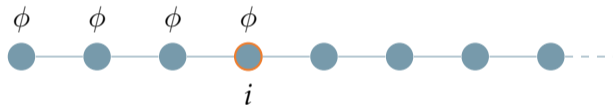
- (once) $O\phi \equiv \top S \phi$





Shortcuts:

- (historically) $H\phi \equiv \neg O\neg\phi$

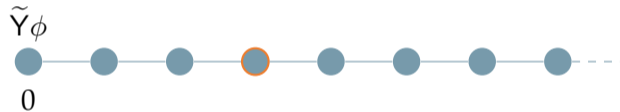


ϕ holds *always in the past*



Shortcuts:

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



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

Note: $\sigma, i \models \tilde{Y}\perp$ is true iff $i = 0$.



Notation:

- we will write $\phi \in \text{LTL}$ (resp., $\phi \in \text{LTL+P}$) to denote the fact that ϕ is a formula of LTL (resp., 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

$$\sigma, i \models \tilde{Y} \perp \Leftrightarrow i ?$$



Exercises useful for the succinctness proof.

Exercise 1

$$\sigma, i \models \tilde{Y} \perp \Leftrightarrow i = 0$$



Exercises useful for the succinctness proof.

Exercise 2

$$\sigma, i \models \tilde{Y}\tilde{Y}\tilde{Y}\perp \Leftrightarrow i ?$$



Exercises useful for the succinctness proof.

Exercise 2

$$\sigma, i \models \tilde{Y}\tilde{Y}\tilde{Y}\perp \Leftrightarrow i \leq 2$$



Exercises useful for the succinctness proof.

Exercise 3

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



Exercises useful for the succinctness proof.

Exercise 3

$$\sigma, i \models \text{YYT} \Leftrightarrow i \geq 2$$



Exercises useful for the succinctness proof.

Exercise 4

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



Exercises useful for the succinctness proof.

Exercise 4

$$\sigma, i \models \tilde{Y}\tilde{Y}\tilde{Y}\perp \wedge Y\tilde{Y}T \Leftrightarrow i = 2$$



Goal

For any formula ϕ of LTL+P over the atomic propositions \mathcal{AP} , we will build a NBA \mathcal{A}_ϕ 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 $\alpha \cup \beta \in \mathcal{C}(\phi)$, then $X(\alpha \cup \beta) \in \mathcal{C}(\phi)$;
- if $\alpha \text{ S } \beta \in \mathcal{C}(\phi)$, then $\{Y(\alpha \text{ S } \beta), \tilde{Y}(\alpha \text{ S } \beta)\} \subseteq \mathcal{C}(\phi)$.



States of \mathcal{A}_ϕ

A **state** of the NBA \mathcal{A}_ϕ 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 $\{\alpha_1, \alpha_2\} \subseteq S$
- ...
- for all $\alpha := \alpha_1 \cup \alpha_2$, it holds that $\alpha \in S$ iff either $\alpha_2 \in S$ or $\{\alpha_1, X\alpha\} \subseteq S$;
- for all $\alpha := \alpha_1 S \alpha_2$, it holds that $\alpha \in S$ iff either $\alpha_2 \in S$ or $\{\alpha_1, Y\alpha\} \subseteq S$.

Initial states of \mathcal{A}_ϕ . A state $S \subseteq \mathcal{C}(\phi)$ is **initial** for \mathcal{A}_ϕ iff $\phi \in S$ and S does not contain any formula of type $Y\alpha$ or $\neg\tilde{Y}\alpha$.



Transitions of \mathcal{A}_ϕ

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}_ϕ iff:

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

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

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



Final states of \mathcal{A}_ϕ

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}_ϕ 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 $\mathcal{F} := \{F_1, \dots, F_n\}$, 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 $\text{Inf}(\pi) \cap F_i \neq \emptyset$.

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

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



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 $\mathcal{F} := \{F_1, \dots, F_n\}$, 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 $\text{Inf}(\pi) = F_i$.

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

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



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 an LTL+P formula
- 2 Build the NBA \mathcal{A}_ϕ equivalent to ϕ
- 3 Check for the **emptiness** of \mathcal{A}_ϕ
 - if $\mathcal{L}(\mathcal{A}_\phi) = \emptyset$, then ...
 - otherwise, ...



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

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

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

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

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



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

For all $n > 0$, we define $\mathcal{AP}_n := \{p_0, \dots, p_n\}$ 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, \dots, p_n , then i and 0 agree also on the interpretation of p_0 .

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

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



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:

$$G\left(\left(\bigwedge_{i=1}^n (p_i \leftrightarrow O(\tilde{Y} \perp \wedge p_i))\right)\right) \rightarrow (p_0 \leftrightarrow O(\tilde{Y} \perp \wedge p_0))$$

□



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 $\mathcal{AP}_n := \{p_0, \dots, p_n\}$ 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 positions i and j agree on the interpretation of all p_1, \dots, p_n , then i and j agree also on the interpretation of p_0 .

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

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



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 $\phi_n \in \text{LTL}$ such that $\mathcal{L}(\phi_n) = A_n$ and $|\phi_n|$ is less than $2^{\mathcal{O}(n)}$.



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 $\psi_n := G(\phi_n)$ is exactly B_n , because:

- since ϕ_n contains only future operators, $\sigma \models G(\phi_n)$ 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, \dots, 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 $n > 0$, 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.

Moreover, $\psi_n := G(\phi_n)$ 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



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.

Moreover, $\psi_n := G(\phi_n)$ 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.



Lemma

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

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

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 , that is,

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

Proof.

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





Doubly exponential lower bound for any automaton recognizing B_n

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^{AP_n} recognizing B_n is of size $2^{2^{\Omega(n)}}$.

Reference:

Kousha Etessami, Moshe Y Vardi, and Thomas Wilke (2002). “First-order logic with two variables and unary temporal logic”. In: *Information and computation* 179.2, pp. 279–295



Doubly exponential lower bound for any automaton recognizing B_n

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

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

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

Example with $n = 3$

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

$$\bar{a} := \langle a_0, \dots, a_7 \rangle$$

$$:= \langle \{p_1\}, \{p_1, p_2\}, \emptyset, \{p_3\}, \{p_3, p_2\}, \{p_1, p_2, p_3\}, \{p_2\}, \{p_2, p_3\} \rangle$$



Doubly exponential lower bound for any automaton recognizing B_n

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

Example with $n = 3$

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



Doubly exponential lower bound for any automaton recognizing B_n

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

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



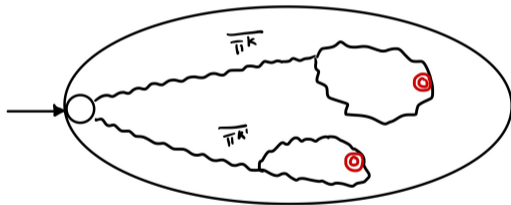
Doubly exponential lower bound for any automaton recognizing B_n

- Let K and K' be two distinct subsets of $\{0, \dots, 2^n - 1\}$.
- The word $(\overline{a^K})^\omega$ belongs to B_n because:
 - by construction of \overline{a} , two positions i and j agree on p_1, \dots, 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 hypothesis the automaton \mathcal{A} recognizes B_n , both $(\overline{a^K})^\omega$ and $(\overline{a^{K'}})^\omega$ are accepted by \mathcal{A} .



Doubly exponential lower bound for any automaton recognizing B_n

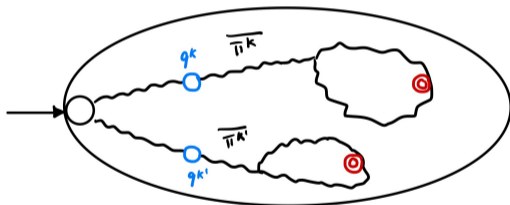
- Therefore, there exists two accepting runs $\overline{\pi^K}$ and $\overline{\pi^{K'}}$ in \mathcal{A} induced by $(\overline{a^K})^\omega$ and $(\overline{a^{K'}})^\omega$, respectively.





Doubly exponential lower bound for any automaton recognizing B_n

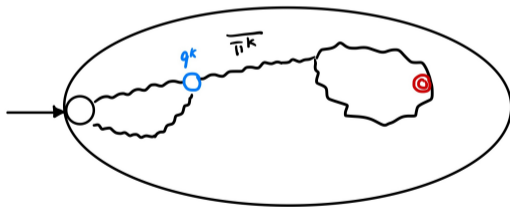
- Therefore, there exists two accepting runs $\overline{\pi^K}$ and $\overline{\pi^{K'}}$ in \mathcal{A} induced by $(\overline{a^K})^\omega$ and $(\overline{a^{K'}})^\omega$, respectively.
- Let q^K (resp., $q^{K'}$) be the 2^n -th state of $\overline{\pi^K}$ (resp., $\overline{\pi^{K'}}$)





Doubly exponential lower bound for any automaton recognizing B_n

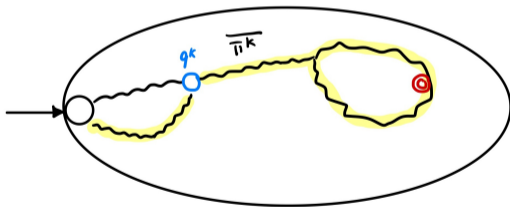
- Suppose that $q^K = q^{K'}$.



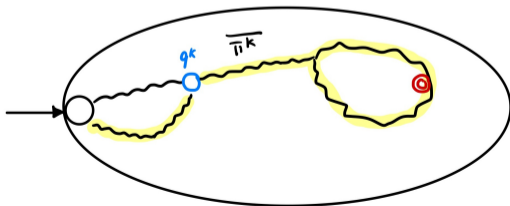


Doubly exponential lower bound for any automaton recognizing B_n

- 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, \dots, 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



- Yaacov Choueka (1974).** “Theories of automata on ω -tapes: A simplified approach”. In: *Journal of computer and system sciences* 8.2, pp. 117–141.
- Kousha Etessami, Moshe Y Vardi, and Thomas Wilke (2002).** “First-order logic with two variables and unary temporal logic”. In: *Information and computation* 179.2, pp. 279–295.
- 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.