Is fully shuffling a rational operation?

Ignacio Mollo Cunningham
Instituto de Ciencias de la Computación
Universidad de Buenos Aires

November 25, 2025

Interests:

- Randomness
- Finite Automata
- Combinatorics on Words

Members:

- Verónica Becher
- Pablo Turjanski
- Martin Mereb
- Eda Cesaratto
- Olivier Carton
- Nicolás Alvarez

Intereses:

- Randomness
- **Finite Automata**
- Combinatorics on Words

Members:

- **Verónica Becher**
    - **Ignacio Mollo**
    - Simon Lew Deveali
- Pablo Turjanski
- Martin Mereb
- Eda Cesaratto
- Olivier Carton
- Nicolás Alvarez

Shuffling Words

**“If you spend all day shuffling words around,
you can make anything sound bad, Morty.”**
– Rick Sanchez

Shuffle of Words

Shuffle of words

Given two words $u, v \in A^\star$ we define its shuffle $u \between v$ to be the language of $A^\star$ comprised by all words that can be obtained by shuffling u, v. Formally:

$$u \between v = \{w \mid w = u_1 v_1 \dots u_n v_n \text{ with } u = u_1 \dots u_n \text{ and } v = v_1 \dots v_n\}$$

Shuffle of Languages

Shuffle of languages

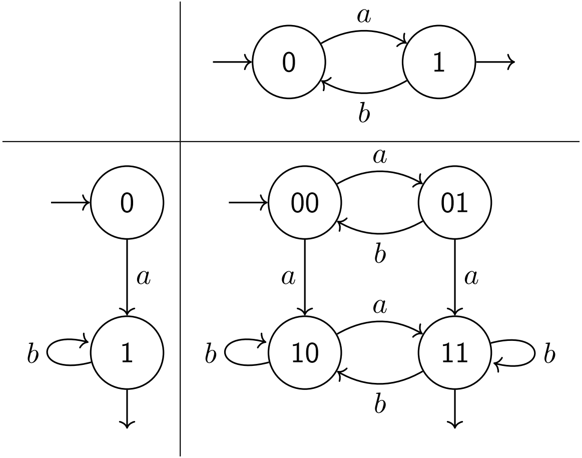
Given two languages $L, M \subseteq A^\star$, its shuffle $L \between M$ is defined as follows:

$$L \between M = \bigcup_{u \in L, v \in M} u \between v$$

Proposition

The shuffle of two regular languages is also a regular language.

Shuffle of Languages



Shuffling Monoid

Shuffling Monoid

The shuffling monoid U is the submonoid of $A^\star \times A^\star \times A^\star$ defined as

$$U = \{(u, v, w) : u, v, w \in A^\star \text{ and } w \in u \between v\}$$

Shuffling Monoid

Shuffling Monoid

The shuffling monoid U is the submonoid of $A^\star \times A^\star \times A^\star$ defined as

$$U = \{(u, v, w) : u, v, w \in A^\star \text{ and } w \in u \between v\}$$

- $(aa, bb, abab) \in U$

Shuffling Monoid

Shuffling Monoid

The shuffling monoid U is the submonoid of $A^\star \times A^\star \times A^\star$ defined as

$$U = \{(u, v, w) : u, v, w \in A^\star \text{ and } w \in u \between v\}$$

- $(aa, bb, abab) \in U$
- $(a^n, b^n, (ab)^n) \in U$

Shuffling Monoid

Shuffling Monoid

The shuffling monoid U is the submonoid of $A^\star \times A^\star \times A^\star$ defined as

$$U = \{(u, v, w) : u, v, w \in A^\star \text{ and } w \in u \between v\}$$

- $(aa, bb, abab) \in U$
- $(a^n, b^n, (ab)^n) \in U$
- $(abaca, abca, abacabaca) \in U$

Shuffling Monoid

Shuffling Monoid

The shuffling monoid U is the submonoid of $A^\star \times A^\star \times A^\star$ defined as

$$U = \{(u, v, w) : u, v, w \in A^\star \text{ and } w \in u \between v\}$$

- $(aa, bb, abab) \in U$
- $(a^n, b^n, (ab)^n) \in U$
- $(abaca, abca, abacabaca) \in U$
- $(cara, lave, calavera) \in U$

Shuffling Monoid

Shuffling Monoid

The shuffling monoid U is the submonoid of $A^\star \times A^\star \times A^\star$ defined as

$$U = \{(u, v, w) : u, v, w \in A^\star \text{ and } w \in u \between v\}$$

- $(aa, bb, abab) \in U$
- $(a^n, b^n, (ab)^n) \in U$
- $(abaca, abca, abacabaca) \in U$
- $(cara, lave, calavera) \in U$
- $(cara, lave, caverala) \notin U$

Shuffling Monoid

Shuffling Monoid

The shuffling monoid U is the submonoid of $A^\star \times A^\star \times A^\star$ defined as

$$U = \{(u, v, w) : u, v, w \in A^\star \text{ and } w \in u \between v\}$$

- $(aa, bb, abab) \in U$
- $(a^n, b^n, (ab)^n) \in U$
- $(abaca, abca, abacabaca) \in U$
- $(cara, lave, calavera) \in U$
- $(cara, lave, caverala) \notin U$
- $(pass, word, password) \in U$

Shuffling Monoid

The shuffling monoid is generated by the following set of elements:

$$G = \{(a, \varepsilon, a) : a \in A\} \cup \{(\varepsilon, a, a) : a \in A\}$$

Shuffling Monoid

The shuffling monoid is generated by the following set of elements:

$$G = \{(a, \varepsilon, a) : a \in A\} \cup \{(\varepsilon, a, a) : a \in A\}$$

- $(aa, bb, abab) = (a, \varepsilon, a)(\varepsilon, b, b)(a, \varepsilon, a)(\varepsilon, b, b)$

Shuffling Monoid

The shuffling monoid is generated by the following set of elements:

$$G = \{(a, \varepsilon, a) : a \in A\} \cup \{(\varepsilon, a, a) : a \in A\}$$

- $(aa, bb, abab) = (a, \varepsilon, a)(\varepsilon, b, b)(a, \varepsilon, a)(\varepsilon, b, b)$
- $(a^n, b^n, (ab)^n) = ((a, \varepsilon, a)(\varepsilon, b, b))^n$

Shuffling Monoid

The shuffling monoid is generated by the following set of elements:

$$G = \{(a, \varepsilon, a) : a \in A\} \cup \{(\varepsilon, a, a) : a \in A\}$$

- $(aa, bb, abab) = (a, \varepsilon, a)(\varepsilon, b, b)(a, \varepsilon, a)(\varepsilon, b, b)$
- $(a^n, b^n, (ab)^n) = ((a, \varepsilon, a)(\varepsilon, b, b))^n$
- $(abaca, abca, abacabaca) =$ $(a, \varepsilon, a)(b, \varepsilon, b)(a, \varepsilon, a)(c, \varepsilon, c)(\varepsilon, a, a)(\varepsilon, b, b)(a, \varepsilon, a)(\varepsilon, c, c)(\varepsilon, a, a) =$ $(\varepsilon, a, a)(\varepsilon, b, b)(a, \varepsilon, a)(\varepsilon, c, c)(\varepsilon, a, a)(b, \varepsilon, b)(a, \varepsilon, a)(c, \varepsilon, c)(a, \varepsilon, a)$

Shuffling Monoid

The shuffling monoid is generated by the following set of elements:

$$G = \{\overline{a} : a \in A\} \cup \{\underline{a} : a \in A\}$$

- $(aa, bb, abab) = \overline{a}\underline{b}\overline{a}\underline{b}$
- $(a^n, b^n, (ab)^n) = (\overline{a}\underline{b})^n$
- $(abaca, abca, abacabaca) = \overline{abac}\underline{ab}\overline{a}\underline{ca} = \underline{ba}\overline{a}\underline{ca}\overline{baca}$

Shuffling Monoid

The shuffling monoid is generated by the following set of elements:

$$G = \{\overline{a} : a \in A\} \cup \{\underline{a} : a \in A\}$$

- $(aa, bb, abab) = \overline{a}\underline{b}\overline{a}\underline{b}$
- $(a^n, b^n, (ab)^n) = (\overline{a}\underline{b})^n$
- $(abaca, abca, abacabaca) = \overline{abac}\,\underline{ab}\,\overline{a}\,\underline{ca} = \underline{ba}\,\overline{a}\,\underline{ca}\,\overline{baca}$
- For any word w in $A^\star$:

$$\overline{w}\underline{w} = \underline{w}\overline{w} = (w, w, ww)$$

Shuffling Automata

Shuffler

A Shuffler is an automaton defined over the shuffling monoid, with its transitions labeled in the generator set.

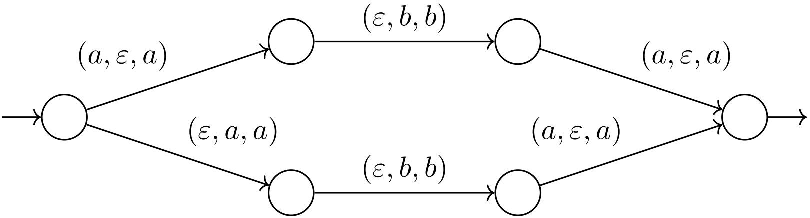


Figura: A simple shuffler realizing the set $\{(aa, b, aba), (a, ab, aba)\}$

Shuffling Automata

Shuffler

A Shuffler is an automaton defined over the shuffling monoid, with its transitions labeled in the generator set.

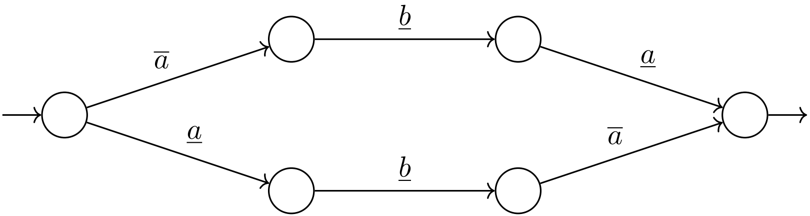


Figura: A simple shuffler realizing the set $\{(aa, b, aba), (a, ab, aba)\}$

Successful Computations in a Shuffler

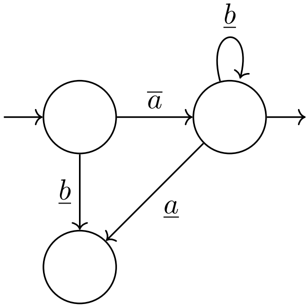


Figura: This automata realizes the set $\overline{a}\underline{b}^{\star} = \{(a, b^n, ab^n) : n \geq 0\}$.

Rational Sets

Behavior of a Shuffler

The behavior of a shuffler $\mathcal{S}$ is defined as

$$|\mathcal{S}| = \{(u, v, w) \in U : \text{ there is a succesful computation in } \mathcal{S} \text{ with label } (u, v, w)\}.$$

In that case we say that $\mathcal{S}$ realizes $|\mathcal{S}|$.

Rational Set of the Shuffling Monoid

A subset $X \subseteq U$ is rational if it's the behavior of a finite-state shuffler.

Shuffling it All

“Oil and water don’t mix, but I will defend to the death your right to try it.”
– Voltaire (possibly apocryphal)

Full Shuffle

Full Shuffle of a Domain

Let $D \subseteq A^\star \times A^\star$. The full shuffle of D is the set

$$(\between D) = \{(u, v, w) : (u, v) \in D \text{ and } w \in u \between v\} \subseteq U$$

Full Shuffle

Full Shuffle of a Domain

Let $D \subseteq A^\star \times A^\star$. The full shuffle of D is the set

$$(\between D) = \{(u, v, w) : (u, v) \in D \text{ and } w \in u \between v\} \subseteq U$$

Is it always rational to fully shuffle a domain D?

Recognizable Case

Proposición

If $D = D_1 \times D_2$ where D_1, D_2 are regular languages, then $(\between D)$ is always rational.

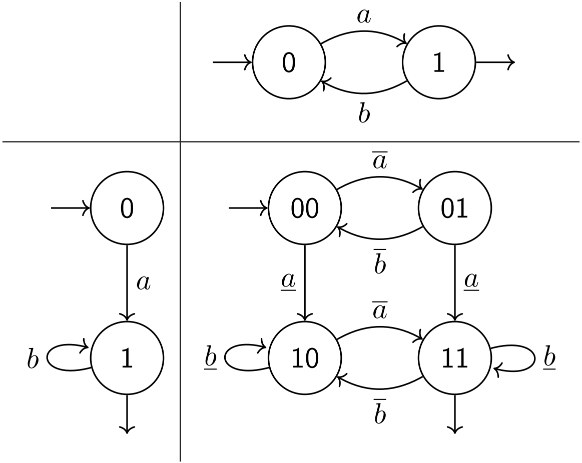
Recognizable Case

Proposición

If $D = D_1 \times D_2$ where D_1, D_2 are regular languages, then $(\between D)$ is always rational.

- Example: $D = (ab)^\star \times ab^\star = \{((ab)^n, ab^m) : n, m \geq 0)\}$
- $(abababab, abbb), (ab, abbbbb), (\varepsilon, abb), (abab, a) \in D$

Product Shuffler



Beyond the Recognizable

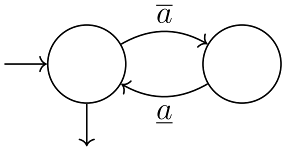
Which of the following domains feature a rational full shuffle?

$$D = (a, a)^\star = \{(a^n, a^n) : n \geq 0\}$$

Beyond the Recognizable

Which of the following domains feature a rational full shuffle?

$$D = (a, a)^{\star} = \{(a^n, a^n) : n \geq 0\}$$



Beyond the Recognizable

Which of the following domains feature a rational full shuffle?

$$D = (a, b)^{\star} = \{(a^n, b^n) : n \geq 0\}$$

Beyond the Recognizable

Which of the following domains feature a rational full shuffle?

$$D = (a, b)^{\star} = \{(a^n, b^n) : n \geq 0\}$$

No, because the projection onto the third coordinate results in a non-regular language:

$$\{w \in A^{\star} : |w|_a = |w|_b\}$$

Beyond the Recognizable

Which of the following domains feature a rational full shuffle?

$$D = (ab, ab)^\star = \{((ab)^n, (ab)^n) : n \geq 0\}$$

Beyond the Recognizable

Which of the following domains feature a rational full shuffle?

$$D = (ab, ab)^\star = \{((ab)^n, (ab)^n) : n \geq 0\}$$

???

Self-Shuffling a word

$$\overline{abababab}\underline{abababab} =$$

Self-Shuffling a word

$$\overline{abababab}\underline{abababab} = \overline{ab}\underline{ab}\overline{ab}\underline{ab}\overline{ab}\underline{ab}\overline{ab}\underline{ab}$$

Self-Shuffling a word

$$(\overline{ab})^N(\underline{ab})^N =$$

Self-Shuffling a word

$$(\overline{ab})^N(\underline{ab})^N = (\overline{ab}\underline{ab})^N$$

Self-Shuffling a word

$$\overline{aba}\underline{abababab}\overline{babab} =$$

Self-Shuffling a word

$$\overline{aba}\underline{abababab}\overline{babab} = \overline{ab}\underline{a}\overline{a}\underline{ba}\overline{ba}\underline{ba}\overline{b}\underline{b}\overline{ab}\underline{ab}$$

Self-Shuffling a word

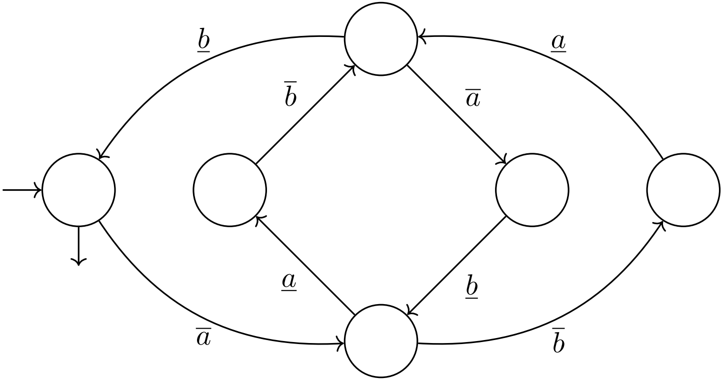


Figura: A shuffler which realizes the full shuffle $(\between\,(ab, ab)^{\star})$

Fully Self-shuffling a word

Theorem

Let $w \in A^\star$ be any word. Then $(\shuffle(w, w)^\star)$ is rational in U.

Fully Self-shuffling a word

Theorem

Let $w \in A^\star$ be any word. Then $(\shuffle\,(w, w)^\star)$ is rational in U.

This result is very fragile.

- If w features more than one symbol, $(\shuffle\,(w, ww)^\star)$ is never rational.

Fully Self-shuffling a word

Theorem

Let $w \in A^\star$ be any word. Then $(\shuffle\,(w,w)^\star)$ is rational in U.

This result is very fragile.

- If w features more than one symbol, $(\shuffle\,(w,ww)^\star)$ is never rational.
- If $\#$ is a symbol not in w, then $(\shuffle\,(\#,\varepsilon)(w,w)^\star)$ is never rational.

Fully Self-shuffling a word

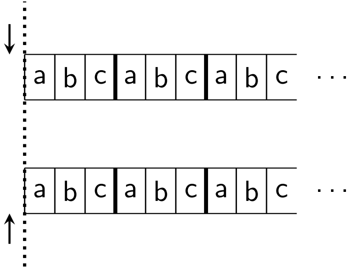
Theorem

Let $w \in A^\star$ be any word. Then $(\between (w, w)^\star)$ is rational in U.

This result is very fragile.

- If w features more than one symbol, $(\between (w, ww)^\star)$ is never rational.
- If $\#$ is a symbol not in w, then $(\between (\#, \varepsilon)(w, w)^\star)$ is never rational.
- $(\between \mathsf{Id})$ is not rational.

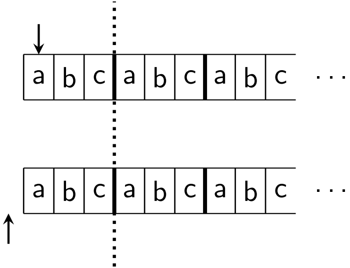
Idea



Read so far:
$(\varepsilon, \varepsilon, \varepsilon)$

Left to read per tape:
$(0, 0)$

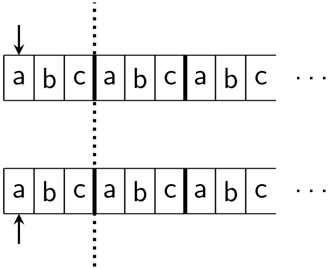
Idea



Read so far:
(a, ε, a)

Left to read per tape:
$(2, 3)$

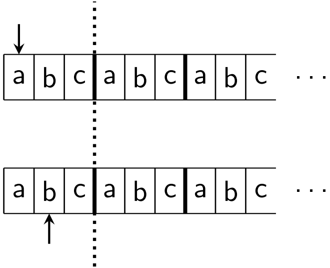
Idea



Read so far:
(a, a, aa)

Left to read per tape:
$(2, 2)$

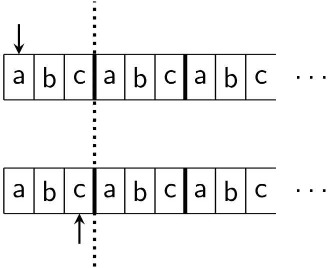
Idea



Read so far:
(a, ab, aab)

Left to read per tape:
$(2, 1)$

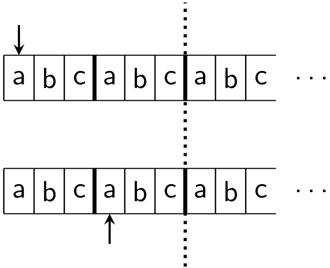
Idea



Read so far:
$(a, abc, aabc)$

Left to read per tape:
$(2, 0)$

Idea



Read so far:
$(a, abca, aabca)$

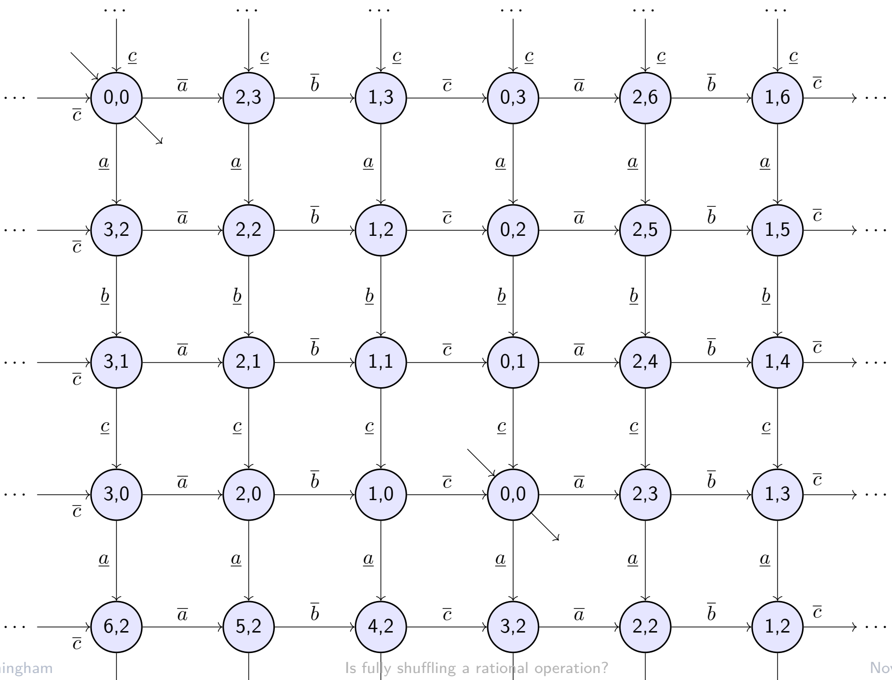
Left to read per tape:
$(5, 2)$

Idea

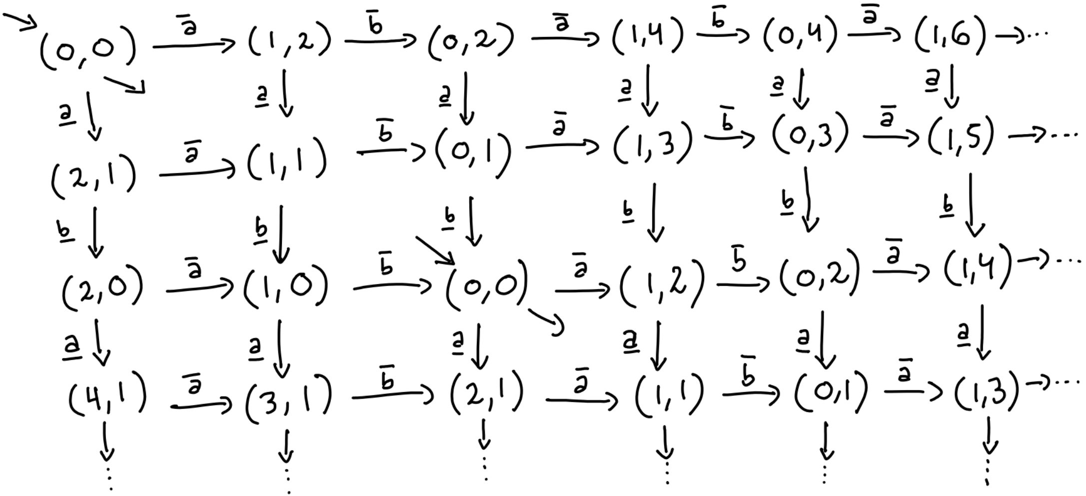
This procedure is determined by the numbers (k, l) that count how much is left to read per tape.

$$\to (0,0) \xrightarrow{\text{“up”}} (2,3) \xrightarrow{\text{“down”}} (2,2) \xrightarrow{\text{“down”}} (2,1) \xrightarrow{\text{“down”}} (2,0) \xrightarrow{\text{“down”}} (5,2)$$

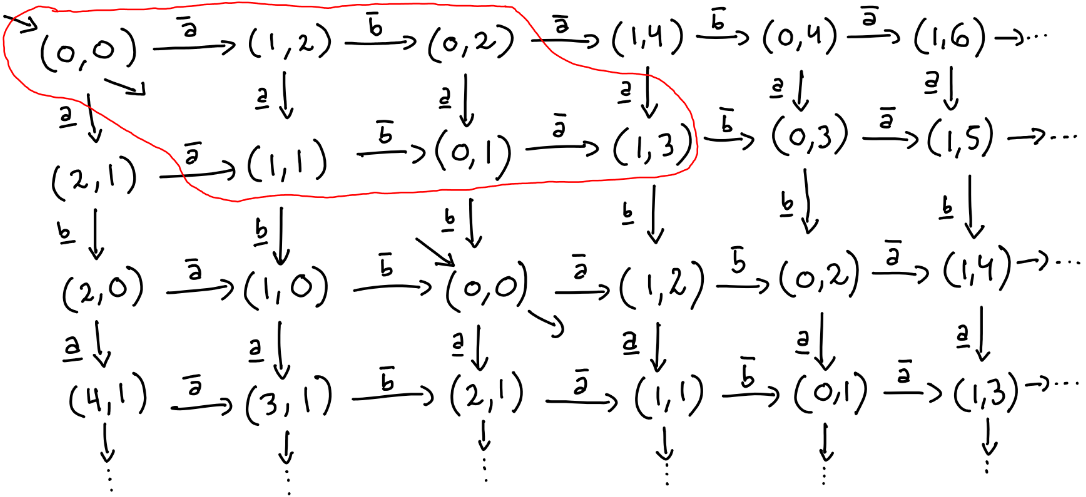
This allows the definition of an **infinite** shuffler that fully self-shuffles a word.


0,0
2,3
1,3
0,3
2,6
1,6
3,2
2,2
1,2
0,2
2,5
1,5
3,1
2,1
1,1
0,1
2,4
1,4
3,0
2,0
1,0
0,0
2,3
1,3
6,2
5,2
4,2
3,2
2,2
1,2

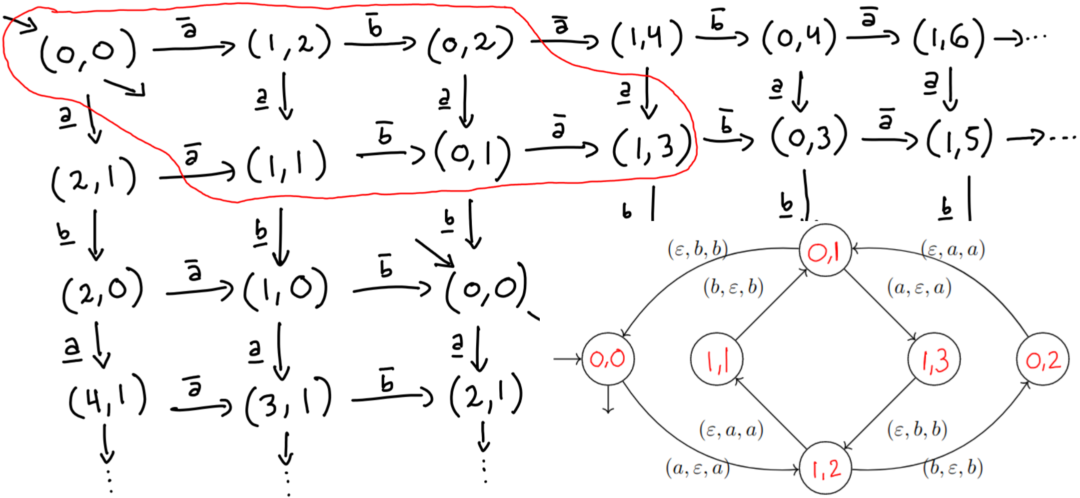
Sketch of Proof (case $w = ab$)



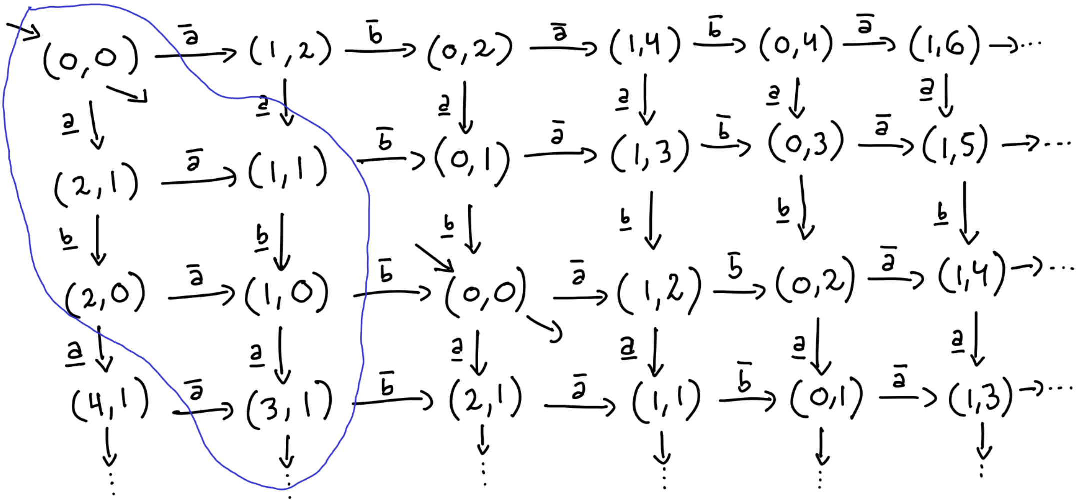
Sketch of Proof (case $w = ab$)



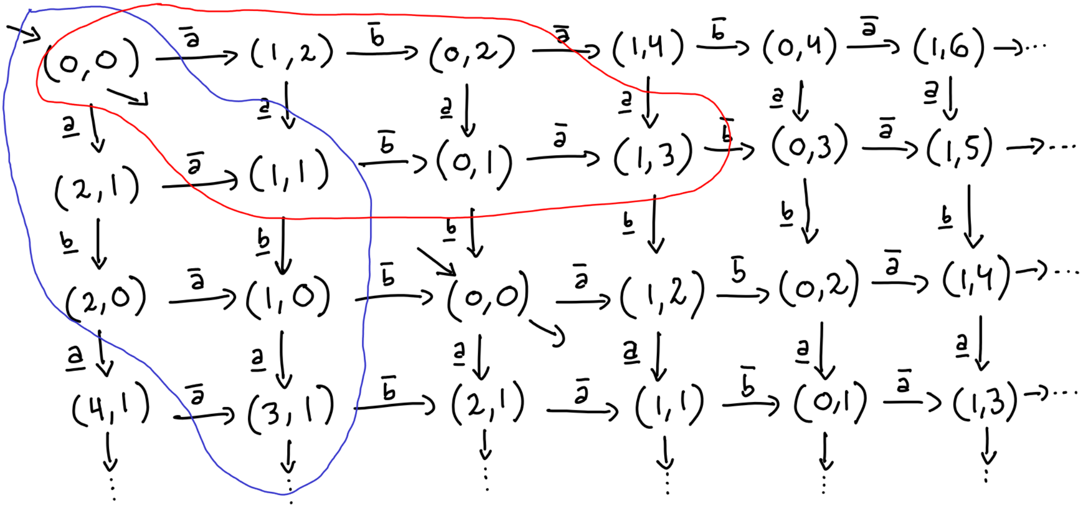
Sketch of Proof (case $w = ab$)



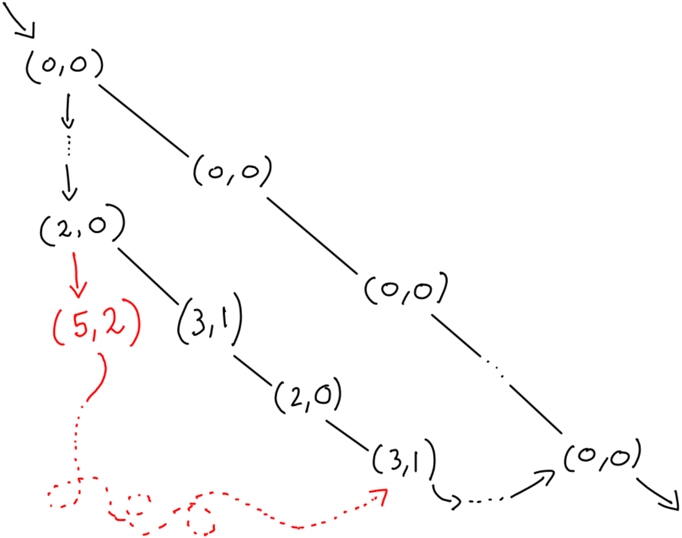
Sketch of Proof (case $w = ab$)



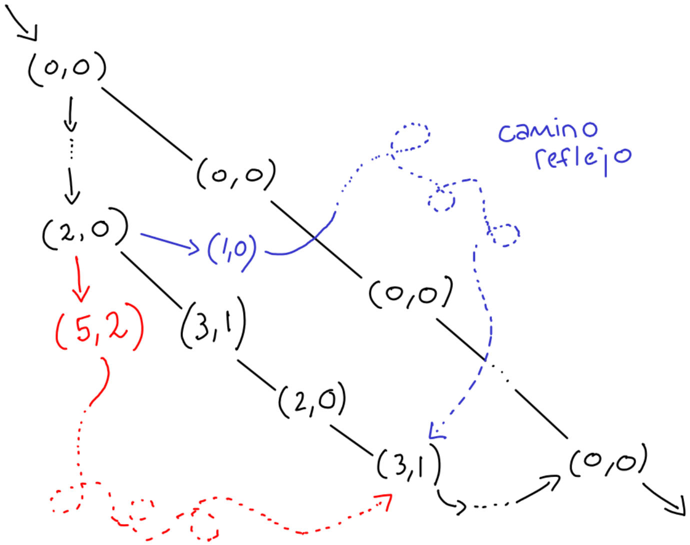
Sketch of Proof (case $w = ab$)



Sketch of Proof (case $w = ab$)



Sketch of Proof (case $w = ab$)



Corollaries

Regularity of Projection

The language $\pi_3\left(\between(w,w)^\star\right)$ consisting of all the self-shuffles of the words in $w^\star$, is a regular language in $A^\star$.

Conjugates

If w_1, w_2 are conjugate words then $\left(\between(w_1,w_2)^\star\right)$ is rational.

Prefixes

If u, v are prefixes of w then $\left(\between(w,w)^\star(u,v)\right)$ es racional.

Future Work

“For if the fool persists on their folly, they shall become wise”
– William Blake

- Finite Presentation of the Shuffling Monoid.
- Fatou Property for the Shuffling Monoid: if the behavior of a transducer is a shuffling relation, then it can be realized by a shuffler.
- The full shuffle of $(u, v)^\star$ is rational only if u, v are conjugate words?
- Decidability of equivalence of shufflers.

Future Work

"For if the fool persists on their folly, they shall become wise"
– William Blake

- Finite Presentation of the Shuffling Monoid.
- Fatou Property for the Shuffling Monoid: if the behavior of a transducer is a shuffling relation, then it can be realized by a shuffler.
- The full shuffle of $(u, v)^\star$ is rational only if u, v are conjugate words?
- ~~Decidability of equivalence of shufflers.~~ **Recently proved that equivalence is undecidable alongside Luc Passemard.**

Thank you!