

# Computing the linear hull: Deciding Deterministic? and Unambiguous? for weighted automata over fields

Jason Bell<sup>1</sup>, Daniel Smertnig<sup>2</sup>

<sup>1</sup> Dept. of Pure Mathematics, University of Waterloo, Canada

<sup>2</sup> Dept. of Mathematics and Scientific Computing, University of Graz, Austria

arXiv:2209.02260

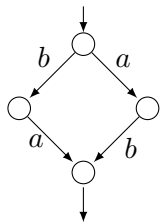
LICS 2023

Boston, June 28, 2023

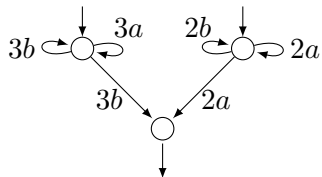
# The problem

- Weighted finite automata (WFAs) over a **field**  $K$  ( $K$  f.g.; for simplicity  $\text{char } K = 0$ , e.g.,  $K = \mathbb{Q}$ ).
- Given a WFA  $\mathcal{A}$ , is there a WFA  $\mathcal{A}'$ , equivalent to  $\mathcal{A}$ , such that
  - **(Deterministic?)**  $\mathcal{A}'$  is deterministic?
  - **(Unambiguous?)**  $\mathcal{A}'$  is unambiguous?

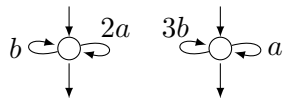
A trim WFA  $\mathcal{A}$  is **unambiguous** if every word has  $\leq 1$  accepting paths.



deterministic



unambiguous



neither

## History (over fields)

---

- *Deterministic?*: Problem 1 in the survey of Lombardy–Sakarovitch 2006 (for  $K = \mathbb{Q}$  and  $K = \mathbb{Z}$ ).
- For one-letter alphabets  $\Sigma$  (=linear recurrences) *Deterministic?* and *Unambiguous?* are decidable ( $K = \mathbb{Q}$ ):
  - *Unambiguous?*: Pólya (1920) + Berstel–Mignotte (1976),
  - *Deterministic?*: Kostolyáni (2022).
- $|\Sigma| > 1$ : Bell-S. (2019) reduces the problem to computation of the **linear hull** of a WFA.

# Linear hull: a topology

---

## Definition (Linear Zariski topology)

Let  $V$  be a finite-dimensional  $K$ -vector space. A set  $X \subseteq V$  is **closed** if and only if  $X$  is a union of finitely many vector subspaces.

(Colcombet–Petrisan (2017): FUSS)

- Every closed  $X$  is uniquely an irredundant union of vector spaces

$$X = Z_1 \cup \dots \cup Z_l.$$

- $\dim X = \max\{\dim Z_1, \dots, \dim Z_l\}$ .
- Linear maps on  $V$  are continuous & closed (preimages and images of closed sets are closed).

# Linear hull

---

Recall: WFA  $\mathcal{A} \leftrightarrow$  linear representation  $(u, \mu, v)$  with  $u, v \in K^d$ ,  $\mu : \Sigma^* \rightarrow M_d(K)$ .

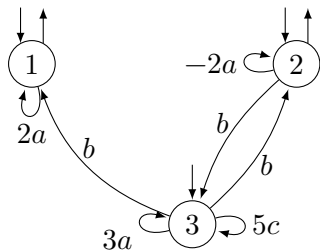
## Definition

Given a WFA  $\mathcal{A}$  with linear representation  $(u, \mu, v)$ , the **(left) linear hull** is

$$L_{\mathcal{A}} := \overline{u^T \mu(\Sigma^*)} \subseteq K^{1 \times d}.$$

# Example

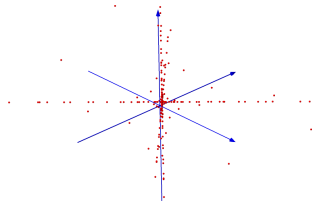
$$\Sigma = \{a, b, c\}, K = \mathbb{Q}.$$



$$u = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, v = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 3 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, C = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$

$$\begin{aligned} L_{\mathcal{A}} &= \underbrace{\text{span}\{e_1 + e_2, e_3\}}_{Z_1} \cup \underbrace{\text{span}\{e_1 - e_2, e_3\}}_{Z_2} \\ &= (x, -x, y) \cup (x, x, y) \end{aligned}$$



# Reduction of Deterministic? to linear hull

---

## Theorem

TFAE:

- 1  $\mathcal{A}$  is equivalent to a deterministic WFA.
- 2 The reachability set  $\Omega = u^T \mu(\Sigma^*)$  can be covered by finitely many lines.
- 3  $\dim L_{\mathcal{A}} \leq 1$ .

# Reduction of Unambiguous? to linear hull

Given  $L_{\mathcal{A}} = Z_1 \cup \dots \cup Z_l$ , construct a new (equivalent) WFA  $\widehat{\mathcal{A}}$  on

$$Z_1 \oplus \dots \oplus Z_l.$$

## Example

$$u' = (1, 1, 0, 0)^T, v' = (2, 0, 0, 0)^T,$$

$$A' = \left( \begin{array}{cc|cc} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ \hline 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \end{array} \right), \quad B' = \left( \begin{array}{cc|cc} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hline 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{array} \right), \quad C' = \left( \begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5 \end{array} \right).$$

## Theorem (Bell-S. 2019)

TFAE for a minimal (=reduced) WFA  $\mathcal{A}$  (with “correct” choice of basis):

- $\mathcal{A}$  is equivalent to an unambiguous WFA  $\mathcal{A}'$ .
- $\widehat{\mathcal{A}}$  is unambiguous.
- $\widehat{\mathcal{A}}$  is semimonomial. (uses Diophantine number theory)

It seems like a good idea to compute  $L_{\mathcal{A}}$ !

# How to compute $L_{\mathcal{A}}$ ?

---

Compute  $\overline{\mu(X^*)} \subseteq M_d(K)$ , then project by multiplying by  $u^T$ .

## One possibility:

- 1 Compute Zariski closure  $\widetilde{\mu(X^*)}$ , using
  - Derksen–Jeandel–Koiran (2005) — group case,
  - Hrushovski–Ouaknine–Pouly–Worrell (2018) — semigroup case.
  - (Semigroup structure: Okninski '80s)
- 2 From components of  $\widetilde{\mu(X^*)}$  find  $\overline{\mu(X^*)}$   
(Lefauchaux–Ouaknine–Purser–Worrell (2021)).

## But:

- We want  $\overline{\mu(X^*)}$  directly, without going through  $\widetilde{\mu(X^*)}$ .
- Bounds on the output size (=number of components of  $\overline{\mu(X^*)} / L_{\mathcal{A}}$ )?

## Direct computation of $L_{\mathcal{A}}$

---

### Theorem

Given a closed set  $X \subseteq M_d(K)$ , one can compute  $\overline{\langle X \rangle} \subseteq M_d(K)$  (essentially staying within linear algebra).

Follows strategy of Zariski closure. Three steps:

- 1 Single invertible matrix (essentially Jordan normal form) — easier.
- 2 All generating matrices are invertible (“group case”) — same.
- 3 General case (“semigroup case”) — more tricky.

## Example

---

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 3 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, C = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 5 \end{pmatrix}, u^T = (1, 1, 1)$$

$$Y = \overline{\langle A, B, C \rangle}$$

$$\begin{aligned} &= \begin{pmatrix} x & \cdot & \cdot \\ \cdot & x & \cdot \\ \cdot & \cdot & y \end{pmatrix} \cup \begin{pmatrix} x & \cdot & \cdot \\ \cdot & -x & \cdot \\ \cdot & \cdot & y \end{pmatrix} \cup \begin{pmatrix} \cdot & \cdot & \cdot \\ x & x & \cdot \\ \cdot & \cdot & y \end{pmatrix} \cup \begin{pmatrix} \cdot & \cdot & \cdot \\ x & -x & \cdot \\ \cdot & \cdot & y \end{pmatrix} \cup \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & y \\ x & -x & \cdot \end{pmatrix} \cup \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & y \\ x & x & \cdot \end{pmatrix} \\ &\cup \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & x \end{pmatrix} \cup \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & x \\ \cdot & \cdot & \cdot \end{pmatrix} \cup \begin{pmatrix} \cdot & \cdot & \cdot \\ x & x & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix} \cup \begin{pmatrix} \cdot & \cdot & \cdot \\ x & -x & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix} \cup \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ x & x & \cdot \end{pmatrix} \cup \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ x & -x & \cdot \end{pmatrix} \end{aligned}$$

$$u^T Y = (x, x, y) \cup (x, -x, y)$$

# Bounds on output size ( $K = \mathbb{Q}$ )

## Theorem

- Group case:

$$c(\overline{\langle X \rangle}) \leq 2^{2^{P(d)}}.$$

- General case:

$$c(\overline{\langle X \rangle}) \leq c(X)^{2^{P(d)}}.$$

Key point: If  $G \leq M_d(K)$  is linear algebraic and linear Zariski closed, then  $G/G_0 \subseteq M_{d'}(K)$  where  $d' \leq (2^{d^2} + d)^2$ .

## Example

- Group case: signed permutation matrix have size  $2^d d!$ .



$$n \geq 1, \quad X = \bigcup_{m \in [n]} \begin{pmatrix} x & xm \\ 0 & 0 \end{pmatrix} \subseteq M_2(K).$$