# Primitivity of random matrix sets and the synchronizing probability function

#### Costanza Catalano

(joint work with Raphaël M. Jungers (UCLouvain))

Gran Sasso Scince Institute, L'Aquila, Italy



RP'18, Marseille, September 25th 2018

# What is a **primitive** set of matrices?

#### Primitive matrix:

$$M = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad M^{3} = \begin{pmatrix} 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 1 & 2 & 3 & 2 \\ 3 & 2 & 1 & 2 \end{pmatrix} > 0$$

# What is a **primitive** set of matrices?

#### Primitive matrix:

$$M = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad M^3 = \begin{pmatrix} 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 1 & 2 & 3 & 2 \\ 3 & 2 & 1 & 2 \end{pmatrix} > 0$$

#### Primitive set (of matrices):

$$\mathcal{M} = \left\{ \underbrace{\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \hline M_1 \end{pmatrix}}_{M_1}, \underbrace{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ \hline M_2 \end{pmatrix}}_{M_2} \right\}, \quad M_1 M_2 M_2 M_1 M_2 M_2 M_1 = \begin{pmatrix} 1 & 1 & 2 & 1 \\ 2 & 1 & 3 & 1 \\ 1 & 1 & 1 & 1 \\ 2 & 1 & 2 & 1 \end{pmatrix} > 0$$

#### A primitive set is

a finite set of nonnegative matrices that admits an entrywise **positive product**.

• Introduced by Protasov, Voynov in 2012.

# A little bit less than primitivity: scrambling sets

#### Scrambling set (of matrices):

$$\mathcal{M} = \left\{ \underbrace{\left( \begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{smallmatrix} \right)}_{\mathcal{M}_1}, \underbrace{\left( \begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{smallmatrix} \right)}_{\mathcal{M}_2} \right\},$$

$$M_1 M_2 M_2 M_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} > 0$$

#### A scrambling set is

a finite set of nonnegative matrices that admits a product with an entrywise **positive column**.

# A little bit less than primitivity: scrambling sets

#### Scrambling set (of matrices):

$$\mathcal{M} = \left\{ \underbrace{\left( \begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{smallmatrix} \right)}_{\mathcal{M}_1}, \underbrace{\left( \begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{smallmatrix} \right)}_{\mathcal{M}_2} \right\},$$

$$M_1 M_2 M_2 M_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} > 0$$

#### A scrambling set is

a finite set of nonnegative matrices that admits a product with an entrywise **positive column**.

$$\mathsf{Primitivity} \quad \Rightarrow \quad \mathsf{Scrambing}$$

#

# A little bit less than primitivity: scrambling sets

#### Scrambling set (of matrices):

$$\mathcal{M} = \left\{ \underbrace{\left( \begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{smallmatrix} \right)}_{\mathcal{M}_1}, \underbrace{\left( \begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{smallmatrix} \right)}_{\mathcal{M}_2} \right\},$$

$$M_1 M_2 M_2 M_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} > 0$$

#### A scrambling set is

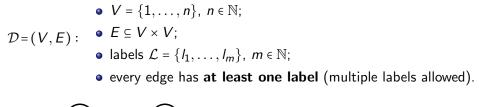
a finite set of nonnegative matrices that admits a product with an entrywise **positive column**.

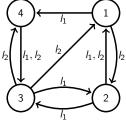
$$\begin{array}{rcl} \mathsf{Primitivity} & \Rightarrow & \mathsf{Scrambing} \end{array}$$

#

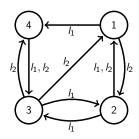
•  $\mathcal{M} = \{M_1, \dots, M_m\}, \forall i \ M_i \text{ has no zero-rows nor zero-columns and } M = \sum_i M_i \text{ is irreducible, then}$ 

Primitivity ⇔ Scrambing

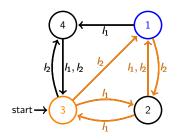




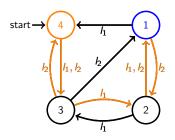
$$V = \{1, 2, 3, 4\}$$
$$\mathcal{L} = \{l_1, l_2\}$$



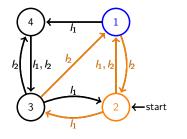
$$V = \{1, 2, 3, 4\}$$
  
$$\mathcal{L} = \{l_1, l_2\}$$



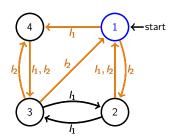
$$V = \{1, 2, 3, 4\}$$
$$\mathcal{L} = \{l_1, l_2\}$$
$$l_1 l_2 l_2 l_1 l_2 l_2 l_1$$



$$V = \{1, 2, 3, 4\}$$
$$\mathcal{L} = \{l_1, l_2\}$$
$$l_1 l_2 l_2 l_1 l_2 l_2 l_1$$

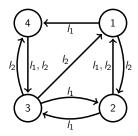


$$V = \{1, 2, 3, 4\}$$
$$\mathcal{L} = \{l_1, l_2\}$$
$$l_1 l_2 l_2 l_1 l_2 l_2 l_1$$



$$V = \{1, 2, 3, 4\}$$
  
$$\mathcal{L} = \{l_1, l_2\}$$
  
$$l_1 l_2 l_2 l_1 l_2 l_2 l_1$$

Image System System



$$V = \{1, 2, 3, 4\}$$
$$\mathcal{L} = \{l_1, l_2\}$$
$$l_1 l_2 l_2 l_1 l_2 l_2 l_1$$

Image of the sequence of labels *l* = *l*<sub>i1</sub> ... *l*<sub>ik</sub> s.t. every node reaches v following a path labeled by *l*? Minimal length of *l*?

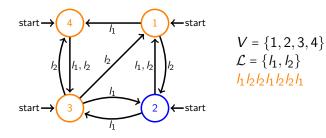


Image of the sequence of labels *l* = *l*<sub>i1</sub> ... *l*<sub>ik</sub> s.t. every node reaches v following a path labeled by *l*? Minimal length of *l*?

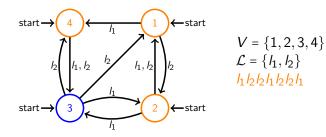


Image of the sequence of labels *l* = *l*<sub>i1</sub> ... *l*<sub>ik</sub> s.t. every node reaches v following a path labeled by *l*? Minimal length of *l*?

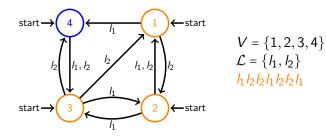
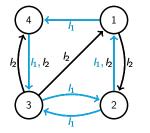


Image Structure in the sequence of labels *l* = *l*<sub>i1</sub> ... *l*<sub>ik</sub> s.t. every node reaches v following a path labeled by *l*? Minimal length of *l*?

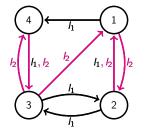
**2**  $\exists$  sequence of labels  $l = l_{i_1} \dots l_{i_k}$  s.t. every node reaches every node following a path labeled by *l*? Minimal length of *l*?



$$I_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Image Structure in the sequence of labels *l* = *l*<sub>i1</sub> ... *l*<sub>ik</sub> s.t. every node reaches v following a path labeled by *l*? Minimal length of *l*?

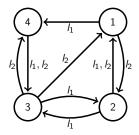
**2**  $\exists$  sequence of labels  $l = l_{i_1} \dots l_{i_k}$  s.t. every node reaches every node following a path labeled by *l*? Minimal length of *l*?



$$I_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} I_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Image Structure in the sequence of labels *l* = *l*<sub>i1</sub> ... *l*<sub>ik</sub> s.t. every node reaches v following a path labeled by *l*? Minimal length of *l*?

**2**  $\exists$  sequence of labels  $l = l_{i_1} \dots l_{i_k}$  s.t. every node reaches every node following a path labeled by *l*? Minimal length of *l*?

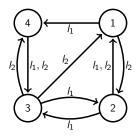


$$I_{1} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} I_{2} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$
$$\mathcal{M} = \{I_{1}, I_{2}\}$$

Image of the sequence of labels *l* = *l*<sub>i1</sub> ... *l*<sub>ik</sub> s.t. every node reaches v following a path labeled by *l*? Minimal length of *l*?

**YES** iff the set  $\mathcal{M}$  is scrambling.

|l| = length of the shortest product with a positive column.



$$I_{1} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} I_{2} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$
$$\mathcal{M} = \{I_{1}, I_{2}\}$$

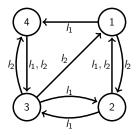
Image of the sequence of labels *l* = *l*<sub>i1</sub> ... *l*<sub>ik</sub> s.t. every node reaches v following a path labeled by *l*? Minimal length of *l*?

**YES** iff the set  $\mathcal{M}$  is scrambling.

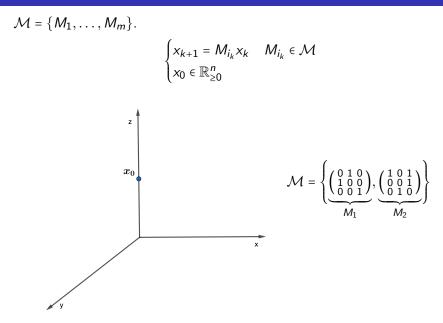
|l| = length of the shortest product with a positive column.

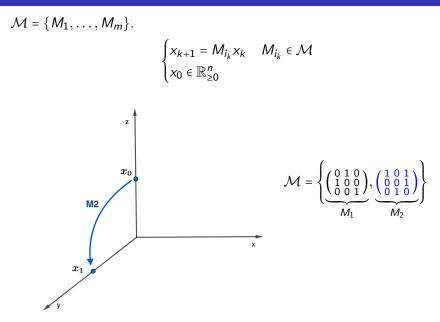
② ∃ sequence of labels *l* = *l*<sub>i1</sub> ... *l*<sub>ik</sub> s.t. every node reaches every node following a path labeled by *l*? Minimal length of *l*?

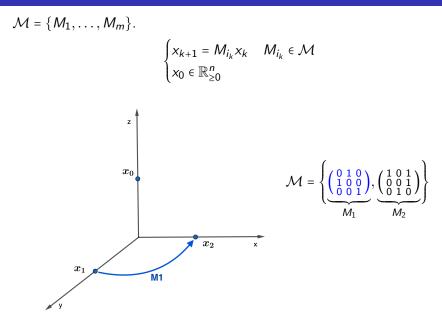
**YES** iff the set  $\mathcal{M}$  is primitive. |I| = length of the shortest positive product.

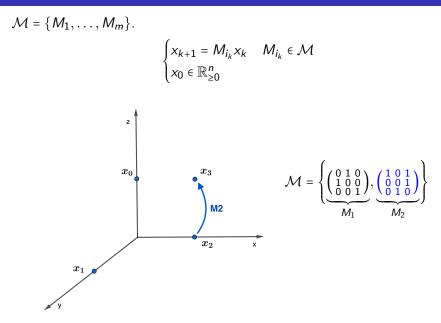


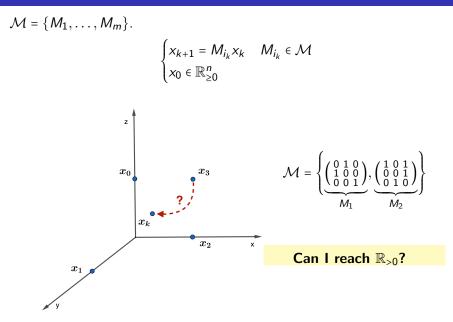
$$I_{1} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} I_{2} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$
$$\mathcal{M} = \{I_{1}, I_{2}\}$$

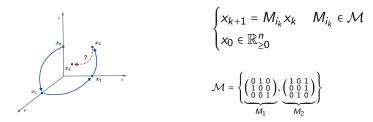




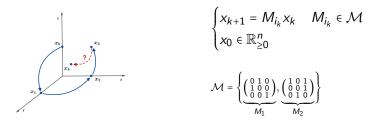






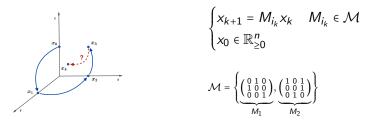


●  $\exists x_0 \in \{x, y, z\}$  and sequence of matrices of the system s.t.  $\exists k : x_k$  reaches  $\mathbb{R}^n_{\geq 0}$ ? What is the minimal k?



●  $\exists x_0 \in \{x, y, z\}$  and sequence of matrices of the system s.t.  $\exists k : x_k$  reaches  $\mathbb{R}^n_{\geq 0}$ ? What is the minimal k?

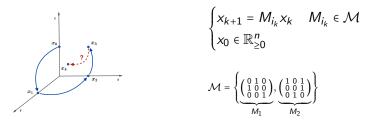
**2** Can we choose a sequence of matrices of the system s.t.  $\exists k : x_k$  reaches  $\mathbb{R}^n_{>0}$  for any  $x_0 \in \mathbb{R}^n_{\geq 0}$ ? What is the minimal k?



●  $\exists x_0 \in \{x, y, z\}$  and sequence of matrices of the system s.t.  $\exists k : x_k$  reaches  $\mathbb{R}^n_{\leq 0}$ ? What is the minimal k?

**YES** iff the set  $\mathcal{M}$  is scrambling. k = length of the shortest product with a positive column.

**2** Can we choose a **sequence of matrices** of the system s.t.  $\exists k : x_k$  reaches  $\mathbb{R}_{>0}^n$  for any  $x_0 \in \mathbb{R}_{\geq 0}^n$ ? What is the **minimal** k?



●  $\exists x_0 \in \{x, y, z\}$  and sequence of matrices of the system s.t.  $\exists k : x_k$  reaches  $\mathbb{R}_{>0}^n$ ? What is the minimal k?

**YES** iff the set M is scrambling. k =length of the shortest product with a positive column.

**2** Can we choose a **sequence of matrices** of the system s.t.  $\exists k : x_k$  reaches  $\mathbb{R}_{\geq 0}^n$  for any  $x_0 \in \mathbb{R}_{\geq 0}^n$ ? What is the minimal k?

**YES** iff the set is primitive.

k =length of the shortest positive product.

#### Exponent of a primitive set

 $exp(\mathcal{M}) = length$  of the shortest positive product of the set  $\mathcal{M}$ .

- Computing the exponent of a set is NP-hard. [Gerencsér, Gusev, Jungers, 2016]
- Asymptotics on the growth-rate of  $exp(\mathcal{M})$  w.r.t. the matrix size *n*:
  - $\max_{\mathcal{M}}(exp(\mathcal{M})) \sim \sqrt[3]{3}e^n$  [Gerencsér, Gusev, Jungers, 2016]
  - $exp(\mathcal{M}) \leq (n^3 + 2n 3)/3$  when every matrix of  $\mathcal{M}$  has neither zero-rows nor zero-columns [Blondel, Jungers, Olshevsky, 2015]

#### Exponent of a primitive set

 $exp(\mathcal{M}) = length$  of the shortest positive product of the set  $\mathcal{M}$ .

- Computing the exponent of a set is NP-hard. [Gerencsér, Gusev, Jungers, 2016]
- Asymptotics on the growth-rate of  $exp(\mathcal{M})$  w.r.t. the matrix size *n*:
  - $\max_{\mathcal{M}}(exp(\mathcal{M})) \sim \sqrt[3]{3}e^n$  [Gerencsér, Gusev, Jungers, 2016] Determining primitivity is decidable but **NP-hard**
  - $exp(\mathcal{M}) \leq (n^3 + 2n 3)/3$  when every matrix of  $\mathcal{M}$  has neither zero-rows nor zero-columns [Blondel, Jungers, Olshevsky, 2015] Determining primitivity is decidable in **polynomial** time

# What is the probability to generate a primitive set? What is their typical exponent?

- Random matrix sets:
  - Primitivity and shortest positive product
  - Scrambling and shortest column-positive product

#### Can we approximate the exponent of a set?

- A probabilistic tool for studying primitivity
- A new bound on the exponent of a class of primitive sets

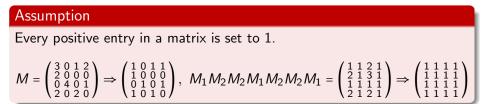
What is the probability to generate a primitive set? What is their typical exponent?

- Random matrix sets:
  - Primitivity and shortest positive product
  - Scrambling and shortest column-positive product

#### Can we approximate the exponent of a set?

- A probabilistic tool for studying primitivity
- A new bound on the exponent of a class of primitive sets

The properties of being primitive or scrambling are **not** influenced by the **magnitude** of the **positive** entries of the matrices.



# Random matrix sets

Fix m = # of matrices of size  $n \times n$ 

1  
), 
$$\begin{cases} = 1 & \text{with probability } p = p(n) \\ = 0 & \text{with probability } 1 - p \end{cases}$$

Fix m = # of matrices of size  $n \times n$ 

$$\begin{pmatrix} 1 & 0 \\ & & \end{pmatrix}, \qquad \begin{cases} = 1 & \text{with probability } p = p(n) \\ = 0 & \text{with probability } 1 - p \end{cases}$$

Fix m = # of matrices of size  $n \times n$ 

$$\begin{cases} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{cases}, \qquad \qquad \begin{cases} = 1 & \text{with probability } p = p(n) \\ = 0 & \text{with probability } 1 - p \end{cases}$$

Fix m = # of matrices of size  $n \times n$ 

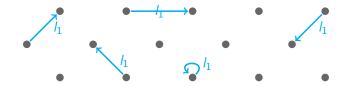
$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{cases} = 1 & \text{with probability } p = p(n) \\ = 0 & \text{with probability } 1 - p \end{cases}$$

Fix 
$$m = \#$$
 of matrices of size  $n \times n$   
 $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ ,  $\begin{cases} = 1 & \text{with probability } p = p(n) \\ = 0 & \text{with probability } 1 - p \\ m = 3, n = 4 \end{cases}$ 

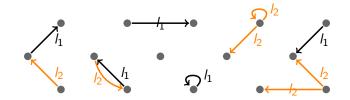
Fix 
$$m = \#$$
 of matrices of size  $n \times n$   
 $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$   $\begin{cases} = 1 & \text{with probability } p = p(n) \\ = 0 & \text{with probability } 1 - p \\ m = 3, n = 4 \end{cases}$ 



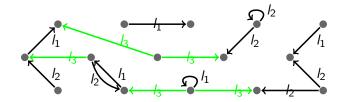
Fix 
$$m = \#$$
 of matrices of size  $n \times n$   
 $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$  = 1 with probability  $p = p(n)$   
 $= 0$  with probability  $1 - p$   
 $m = 3, n = 4$ 



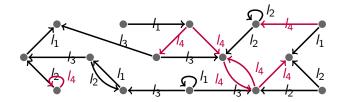
Fix 
$$m = \#$$
 of matrices of size  $n \times n$   
 $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$  = 1 with probability  $p = p(n)$   
 $= 0$  with probability  $1 - p$   
 $m = 3, n = 4$ 



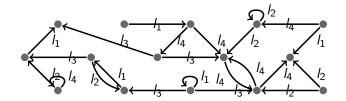
Fix 
$$m = \#$$
 of matrices of size  $n \times n$   
 $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ ,  $\begin{cases} = 1 & \text{with probability } p = p(n) \\ = 0 & \text{with probability } 1 - p \\ m = 3, n = 4 \end{cases}$ 



Fix 
$$m = \#$$
 of matrices of size  $n \times n$   
 $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ ,  $\begin{cases} = 1 & \text{with probability } p = p(n) \\ = 0 & \text{with probability } 1 - p \\ m = 3, n = 4 \end{cases}$ 



Fix 
$$m = \#$$
 of matrices of size  $n \times n$   
 $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ ,  $\begin{cases} = 1 & \text{with probability } p = p(n) \\ = 0 & \text{with probability } 1 - p \\ m = 3, n = 4 \end{cases}$ 



$$m = 4, n = 15$$

### Primitivity of random sets: our result

 $\mathcal{B}_{m}^{n}(\mathbf{p}) = \text{set of } m \text{ matrices of size } n \times n \text{ sampled as seen before.}$ 

 $\exp(\mathcal{B}_m^n(p)) =$  length of its shortest positive product.

$$\begin{cases} = 1 & \text{with prob. } p = p(n) \\ = 0 & \text{with prob. } 1 - p \end{cases}$$

### Primitivity of random sets: our result

 $\mathcal{B}_{\mathbf{m}}^{\mathbf{n}}(\mathbf{p}) = \text{set of } m \text{ matrices of size } n \times n \text{ sampled as seen before.}$ 

 $\exp(\mathcal{B}_m^n(p)) =$  length of its shortest positive product.

$$\begin{cases} = 1 & \text{with prob. } p = p(n) \\ = 0 & \text{with prob. } 1 - p \end{cases}$$

Then as  $n \to \infty$ :

$$\mathbb{P}(\mathcal{B}_m^n(p) \text{ is primitive}) \longrightarrow \begin{cases} 1 & \text{if } np - \log n \to +\infty \\ (*) & \text{if } np - \log n \to c \in \mathbb{R} \\ 0 & \text{if } np - \log n \to -\infty \end{cases}$$

 $(*) \in \left[1 - \left(1 - e^{-2e^{-c}}\right)^m - me^{-2e^{-c}} \left(1 - e^{-2e^{-c}}\right)^{m-1}, 1 - \left(1 - e^{-e^{-c}}\right)^m\right] \subset (0, 1)$ 

### Primitivity of random sets: our result

 $\mathcal{B}_{\mathbf{m}}^{\mathbf{n}}(\mathbf{p}) = \text{set of } m \text{ matrices of size } n \times n \text{ sampled as seen before.}$ 

 $\exp(\mathcal{B}_m^n(p)) =$  length of its shortest positive product.

$$\begin{cases} = 1 & \text{with prob. } p = p(n) \\ = 0 & \text{with prob. } 1 - p \end{cases}$$

Then as  $n \to \infty$ :

$$\mathbb{P}(\mathcal{B}_m^n(p) \text{ is primitive}) \longrightarrow \begin{cases} 1 & \text{if } np - \log n \to +\infty \\ (*) & \text{if } np - \log n \to c \in \mathbb{R} \\ 0 & \text{if } np - \log n \to -\infty \end{cases}$$

 $(*) \in [1 - (1 - e^{-2e^{-c}})^m - me^{-2e^{-c}} (1 - e^{-2e^{-c}})^{m-1}, 1 - (1 - e^{-e^{-c}})^m] \subset (0, 1)$ Furthermore:

- If  $np \log n \to +\infty$ :  $exp(\mathcal{B}_m^n(p)) = O(n \log n)$  with high probability
- If  $np \log n \to c \in \mathbb{R}$ :  $exp(\mathcal{B}_m^n(p)) = O(n \log n)$  with high probability conditioned to the fact that every matrix of  $\mathcal{B}_m^n(p)$  has <u>neither zero-rows nor zero-columns</u>

### Scrambling property of random sets: our result

 $\mathcal{B}_{\mathbf{m}}^{\mathbf{n}}(\mathbf{p}) = \text{set of } m \text{ matrices of size } n \times n$ sampled as seen before.

 $scr(\mathcal{B}_m^n(p)) = length of its shortest product with a positive column.$ 

$$\begin{cases} = 1 & \text{with prob. } p = p(n) \\ = 0 & \text{with prob. } 1 - p \end{cases}$$

Then as  $n \to \infty$ :

$$\mathbb{P}(\mathcal{B}_m^n(p) \text{ is scrambling}) \longrightarrow \begin{cases} 1 & \text{if } np - \log n \to +\infty \\ (*) & \text{if } np - \log n \to c \in \mathbb{R} \\ 0 & \text{if } np - \log n \to -\infty \end{cases}$$

 $(*) \in [1 - (1 - e^{-2e^{-c}})^m - me^{-2e^{-c}} (1 - e^{-2e^{-c}})^{m-1}, 1 - (1 - e^{-e^{-c}})^m] \subset (0, 1)$ Furthermore:

- If  $np \log n \to +\infty$ :  $scr(\mathcal{B}_m^n(p)) = O(n \log n)$  with high probability
- If  $np \log n \rightarrow c \in \mathbb{R}$ :  $scr(\mathcal{B}_m^n(p)) = O(n \log n)$  with high probability conditioned to the fact that every matrix of  $\mathcal{B}_m^n(p)$  has <u>neither zero-rows nor zero-columns</u>

# What is the probability to generate a primitive set? What is their typical exponent?

- Random matrix sets:
  - Primitivity and shortest positive product
  - Scrambling and shortest column-positive product

#### Can we approximate the exponent of a set?

- A probabilistic tool for studying primitivity
- A new bound on the exponent of a class of primitive sets

 $M = \{M_1, \ldots, M_m\}$  a set of  $n \times n$  matrices with neither zero-rows nor zero-columns (**NZ** matrices).

#### The directed graph $\mathcal{D} = (\mathcal{V}, \mathcal{E})$ :

• 
$$\mathcal{V} = \{ v \in \{0, 1\}^n : v \neq (0, ..., 0) \}$$

• 
$$v \rightarrow w$$
 labeled by  $M_k$  if  $\mathbf{v} \mathbf{M}_k = \mathbf{w}$ .

$$\left\{ M_{1} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, M_{2} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \right\}, \quad \{e_{1}, e_{2}, e_{3}, e_{4}\} = \text{canonical basis}$$

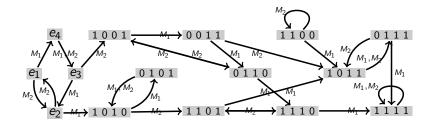
 $\mathcal{M} = \{M_1, \dots, M_m\}$  set of NZ-matrices. Fix  $t \ge 1$  integer.

#### The game's rules

**O** Player B secretly chooses an initial vertex  $e_i \in \{e_1, \ldots, e_n\}$ .

**2** Player A chooses a sequence of at most t matrices in  $\mathcal{M}$ .

So Let  $w = e_i^T M_{i_1} \cdots M_{i_t}$ . A component of w is chosen uniformly at random: if it is = 1 Player A wins, otherwise Player B wins.



 $\mathcal{M} = \{M_1, \dots, M_m\}$  set of NZ-matrices. Fix  $t \ge 1$  integer.

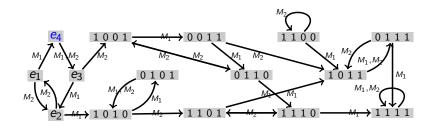
#### The game's rules

**O** Player B secretly chooses an initial vertex  $e_i \in \{e_1, \ldots, e_n\}$ .

**2** Player A chooses a sequence of at most t matrices in  $\mathcal{M}$ .

So Let  $w = e_i^T M_{i_1} \cdots M_{i_t}$ . A component of w is chosen uniformly at random: if it is = 1 Player A wins, otherwise Player B wins.

Player B: e4



 $\mathcal{M} = \{M_1, \dots, M_m\}$  set of NZ-matrices. Fix  $t \ge 1$  integer.

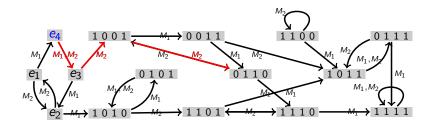
#### The game's rules

**O** Player B secretly chooses an initial vertex  $e_i \in \{e_1, \ldots, e_n\}$ .

**2** Player A chooses a sequence of at most t matrices in  $\mathcal{M}$ .

So Let  $w = e_i^T M_{i_1} \cdots M_{i_t}$ . A component of w is chosen uniformly at random: if it is = 1 Player A wins, otherwise Player B wins.

Player B:  $e_4$  Player A:  $M_1 M_2 M_2$  (t = 3)



 $\mathcal{M} = \{M_1, \dots, M_m\}$  set of NZ-matrices. Fix  $t \ge 1$  integer.

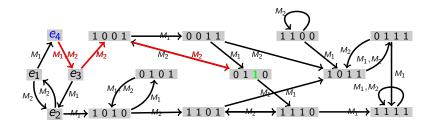
#### The game's rules

**O** Player B secretly chooses an initial vertex  $e_i \in \{e_1, \ldots, e_n\}$ .

**2** Player A chooses a sequence of at most t matrices in  $\mathcal{M}$ .

So Let  $w = e_i^T M_{i_1} \cdots M_{i_t}$ . A component of w is chosen uniformly at random: if it is = 1 Player A wins, otherwise Player B wins.

Player B:  $e_4$  Player A:  $M_1 M_2 M_2$  (t = 3) Player A wins!



 $\mathcal{M} = \{M_1, \dots, M_m\}$  set of NZ-matrices. Fix  $t \ge 1$  integer.

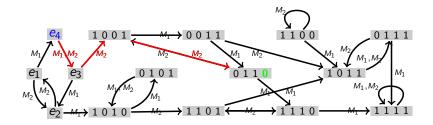
#### The game's rules

**O** Player B secretly chooses an initial vertex  $e_i \in \{e_1, \ldots, e_n\}$ .

**2** Player A chooses a sequence of at most t matrices in  $\mathcal{M}$ .

So Let  $w = e_i^T M_{i_1} \cdots M_{i_t}$ . A component of w is chosen uniformly at random: if it is = 1 Player A wins, otherwise Player B wins.

Player B:  $e_4$  Player A:  $M_1 M_2 M_2$  (t = 3) Player B wins!



 $\mathcal{M} = \{M_1, \dots, M_m\}$  set of NZ-matrices. Fix  $t \ge 1$  integer.

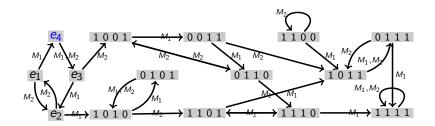
#### The game's rules

**O** Player B secretly chooses an initial vertex  $e_i \in \{e_1, \ldots, e_n\}$ .

**2** Player A chooses a sequence of at most t matrices in  $\mathcal{M}$ .

• Let  $w = e_i^T M_{i_1} \cdots M_{i_t}$ . A component of w is chosen uniformly at random: if it is = 1 Player A wins, otherwise Player B wins.

Player B: e4



 $\mathcal{M} = \{M_1, \dots, M_m\}$  set of NZ-matrices. Fix  $t \ge 1$  integer.

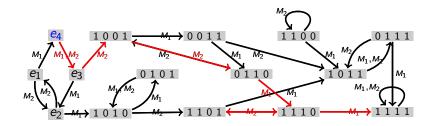
#### The game's rules

**O** Player B secretly chooses an initial vertex  $e_i \in \{e_1, \ldots, e_n\}$ .

**2** Player A chooses a sequence of at most t matrices in  $\mathcal{M}$ .

So Let  $w = e_i^T M_{i_1} \cdots M_{i_t}$ . A component of w is chosen uniformly at random: if it is = 1 Player A wins, otherwise Player B wins.

Player B:  $e_4$  Player A:  $M_1 M_2 M_2 M_1 M_2 M_2 M_1 > 0 (t = 7)$ 



 $\mathcal{M} = \{M_1, \dots, M_m\}$  set of NZ-matrices. Fix  $t \ge 1$  integer.

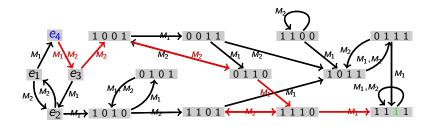
#### The game's rules

**O** Player B secretly chooses an initial vertex  $e_i \in \{e_1, \ldots, e_n\}$ .

**2** Player A chooses a sequence of at most t matrices in  $\mathcal{M}$ .

So Let  $w = e_i^T M_{i_1} \cdots M_{i_t}$ . A component of w is chosen uniformly at random: if it is = 1 Player A wins, otherwise Player B wins.

Player B:  $e_4$  Player A:  $M_1M_2M_2M_1M_2M_2M_1 > 0$  (t = 7) Player A wins!



 $\mathcal{M} = \{M_1, \dots, M_m\}$  set of NZ-matrices. Fix  $t \ge 1$  integer.

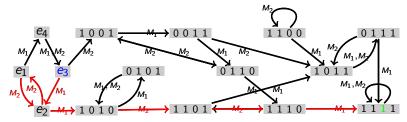
#### The game's rules

**O** Player B secretly chooses an initial vertex  $e_i \in \{e_1, \ldots, e_n\}$ .

**2** Player A chooses a sequence of at most t matrices in  $\mathcal{M}$ .

So Let  $w = e_i^T M_{i_1} \cdots M_{i_t}$ . A component of w is chosen uniformly at random: if it is = 1 Player A wins, otherwise Player B wins.

Player B:  $e_3$  Player A:  $M_1M_2M_2M_1M_2M_2M_1 > 0$  (t = 7) Player A wins! Independently of what Player B plays!



 $\mathcal{M} = \{M_1, \dots, M_m\}$  set of NZ-matrices. Fix  $t \ge 1$  integer.

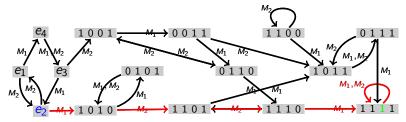
#### The game's rules

**O** Player B secretly chooses an initial vertex  $e_i \in \{e_1, \ldots, e_n\}$ .

**2** Player A chooses a sequence of at most t matrices in  $\mathcal{M}$ .

So Let  $w = e_i^T M_{i_1} \cdots M_{i_t}$ . A component of w is chosen uniformly at random: if it is = 1 Player A wins, otherwise Player B wins.

Player B:  $e_2$  Player A:  $M_1M_2M_2M_1M_2M_2M_1 > 0$  (t = 7) Player A wins! Independently of what Player B plays!



 $\mathcal{M} = \{M_1, \dots, M_m\}$  set of NZ-matrices. Fix  $t \ge 1$  integer.

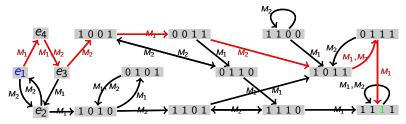
#### The game's rules

**O** Player B secretly chooses an initial vertex  $e_i \in \{e_1, \ldots, e_n\}$ .

**2** Player A chooses a sequence of at most t matrices in  $\mathcal{M}$ .

So Let  $w = e_i^T M_{i_1} \cdots M_{i_t}$ . A component of w is chosen uniformly at random: if it is = 1 Player A wins, otherwise Player B wins.

Player B:  $e_1$  Player A:  $M_1M_2M_2M_1M_2M_2M_1 > 0$  (t = 7) Player A wins! Independently of what Player B plays!



### The Synchronizing Probability Function for primitive sets

The probability that Player A wins if they both play optimally is:

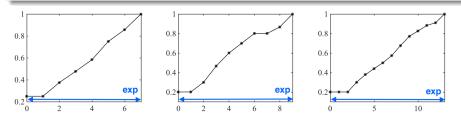
$$\mathcal{K}_{\mathcal{M}}(t) = \min_{\substack{p \in \mathbb{R}^+ \\ p^T e = 1}} \left\{ \max_{M_{i_1} \cdot \dots \cdot M_{i_l} \in \mathcal{M}^{\leq t}} p^T M_{i_1} \cdots M_{i_l} \left( \frac{\mathbf{e}}{n} \right) \right\}$$

where p is the initial distribution of player B,  $\mathcal{M}^{\leq t}$  the set of the products of length  $\leq t$  and  $\mathbf{e} = (1, 1, ..., 1)$ .

### The Synchronizing Probability Function for primitive sets

The probability that Player A wins if they both play optimally is:

$$\mathcal{K}_{\mathcal{M}}(t) = \min_{\substack{p \in \mathbb{R}^+ \\ p^T e = 1}} \left\{ \max_{\substack{M_{i_1} \cdot \dots \cdot M_{i_j} \in \mathcal{M}^{\leq t}}} p^T M_{i_1} \cdots M_{i_l} \left( \frac{\mathbf{e}}{n} \right) \right\}$$



#### Properties

•  $\mathcal{K}_{\mathcal{M}}(t)$  is nondecreasing,  $\mathcal{K}_{\mathcal{M}}(t) = 1 \iff \mathcal{M}$  is primitive.

• 
$$\min_t \{ K_{\mathcal{M}}(t) = 1 \} = exp(\mathcal{M}).$$

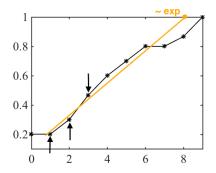
It captures the **speed** at which a set reaches its first positive product

### The Synchronizing Probability Function for primitive sets

The probability that Player A wins if they both play optimally is:

$$\mathcal{K}_{\mathcal{M}}(t) = \min_{\substack{p \in \mathbb{R}^+ \\ p^T e = 1}} \left\{ \max_{M_{i_1} \cdot \dots \cdot M_{i_l} \in \mathcal{M}^{\leq t}} p^T M_{i_1} \cdots M_{i_l} \left( \frac{\mathbf{e}}{n} \right) \right\}$$

where p is the initial distribution of player B,  $\mathcal{M}^{\leq t}$  the set of the products of length  $\leq t$  and  $\mathbf{e} = (1, 1, ..., 1)$ 



### The approximated SPF: $\overline{K}(t)$

The probability that Player A wins if they both play optimally is:

$$\bar{\mathbf{K}}_{\mathcal{M}}(t) = \min_{\mathbf{e}_{1},\dots,\mathbf{e}_{n}} \left\{ \max_{M_{i_{1}}\dots M_{i_{l}} \in \mathcal{M}^{\leq t}} \mathbf{e}_{i}^{T} M_{i_{1}} \cdots M_{i_{l}} \left( \frac{\mathbf{e}}{n} \right) \right\}$$

where  $\mathcal{E} = \{e_1, \ldots, e_n\}$  is the canonical basis.

•  $\bar{K}(t) \ge K(t)$ 

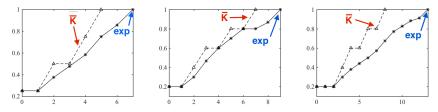
### The approximated SPF: $\bar{K}(t)$

The probability that Player A wins if they both play optimally is:

$$\bar{\mathcal{K}}_{\mathcal{M}}(t) = \min_{\boldsymbol{e}_{1},\dots,\boldsymbol{e}_{n}} \left\{ \max_{M_{i_{1}}\dots M_{i_{l}} \in \mathcal{M}^{\leq t}} \boldsymbol{e}_{i}^{T} M_{i_{1}} \cdots M_{i_{l}} \left( \frac{\mathbf{e}}{n} \right) \right\}$$

where  $\mathcal{E} = \{e_1, \ldots, e_n\}$  is the canonical basis.

•  $\bar{K}(t) \ge K(t)$ 



#### Proposition

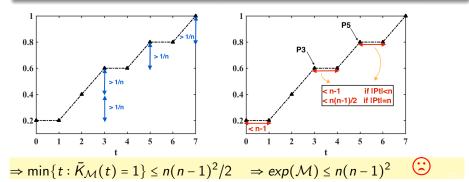
If  $\min\{t: \overline{K}_{\mathcal{M}}(t) = 1\} \leq B(n)$  then  $exp(\mathcal{M}) \leq 2B(n)$ .

### The approximated SPF: $\bar{K}(t)$

#### Linear programming formulation

$$\bar{K}_{\mathcal{M}}(t) = \min_{e_i,k} \frac{k}{n} \quad \text{s. t.} \begin{cases} e_i^T H_t \le k\mathbf{e} \\ e_i^T \mathbf{e} = 1 \\ e_i \ge 0 \end{cases}$$

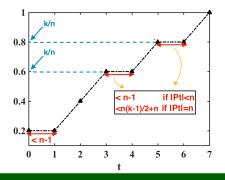
where the *i*-th column of  $H_t$  is the vector  $A_i \mathbf{e}$  with  $A_i$  the *i*-th element of  $\mathcal{M}^{\leq t}$ .  $\mathbf{P}_t \subseteq \{e_1, \ldots, e_n\}$  is the set of its **optimal solutions**.



### New upper bound for a class of primitive sets

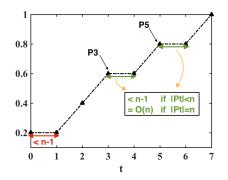
#### Assumption

For each matrix  $M_i \in \mathcal{M}$  there exists a **permutation matrix**  $P_i$  s.t.  $M_i \ge P_i$  entrywise.



#### Proposition

 $exp(\mathcal{M}) \le (n^3 - n^2 + 2n - 8)/4$  for any set  $\mathcal{M}$  that fulfils the assumption.  $\longrightarrow$  better than the known one! but still cubic...



#### Conjecture

For any NZ-primitive set  $\mathcal{M}$  of matrix size  $n \times n$ ,  $exp(\mathcal{M}) = O(n^2)$ .

## Thank you! ...questions?

- C. Catalano, R. M. Jungers, On randomized generation of slowly synchronizing automata. Mathematical Foundations of Computer Science, 2018, 117, 48:1–48:16.
- C. Catalano, R. M. Jungers, The synchronizing probability function of primitive sets of matrices. Developments in Language Theory, 2018, 194-205.
  - C. Catalano, R. M. Jungers, *Random primitive sets may generate slowly synchronizing automata*. Soon on Arxiv.