Primitive matrix sets and synchronizing automata

Yinfeng Zhu
Shanghai Jiao Tong University
@SUSTech, November 7, 2021
Joint work with Yaokun Wu

Primitive matrix sets

Definition

A set $\mathcal{A} = \{A_1, \ldots, A_m\}$ of non-negative/Boolean $(n \times n)$-matrices is called **primitive** if there exists a positive product of matrices of $\mathcal{A}$, i.e., there exists

$$A_{i_1} A_{i_2} \cdots A_{i_k} > 0 \quad \text{(entrywise)},$$

where $A_{i_j} \in \mathcal{A}$.
The length of the shortest positive product is called the **primitive index** of $\mathcal{A}$, denoted by $\mathrm{p}(\mathcal{A})$.

Motivation

- Given a finite set of matrices $\mathcal{A} \subseteq \mathbb{R}_{\geq 0}^{n\times n}$, one can define a stochastic model (switched system) as

$$x_{k+1} = A_{i_k} x_k$$

where A_{i_k} is chosen randomly from $\mathcal{A}$.
- Such models are commonly used throughout stochastic control[1].
- The Lyapunov exponent of this model is defined by

$$\lambda(\mathcal{A}) := \lim_{k\to+\infty} E \log\|A_{i_k}\cdots A_{i_1}\|.$$

[1] El-Kébir Boukas (2007). *Stochastic switching systems: analysis and design*. Springer Science & Business Media, Chapter 5.

Motivation, Contd

- In genreal, it is hard to compute the Lyapunov exponent $\lambda(\mathcal{A})$.
- In the case that $\mathcal{A}$ is primitive, efficient algorithms are available[2].

[2] V.Yu. Protasov (2010). "Invariant functionals of random matrices". In: *Functional Analysis and Applications* 44, pp. 230–233.

Problems

- For a given set $\mathcal{A}$ of Boolean $(n \times n)$-matrices, how to decide if it is primitive or not?
- How to find a positive product of matrices in $\mathcal{A}$?
- How to find a shortest positive product of matrices in $\mathcal{A}$?
- How to calculate $\mathsf{p}(\mathcal{A})$?
- What is $\mathsf{p}(n) := \max\{\mathsf{p}(\mathcal{A}) : \mathcal{A} \subseteq \{0,1\}^{n\times n} \text{ is primitive}\}$?

$|\mathcal{A}| = 1$

Theorem (Perron-Frobenius, 1912)

After a suitable permutation of the basis, every irreducible matrix A has the following block form

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & B_r \\ B_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & B_2 & 0 & \cdots & 0 & 0 \\ \vdots & & & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & B_{r-1} & 0 \end{pmatrix}.$$

Theorem (Wielandt[3], 1959)

If $A \in \{0,1\}^{n \times n}$ is primitive, then $A^k > 0$ for $k \geq (n-1)^2 + 1$.

[3] H. Wielandt (1959). "Unzerlegbare, nicht negative Matrizen". In: *Mathematische Zeitschrift* 52, pp. 642–648.

$|\mathcal{A}| \geq 2$

Theorem (Gerencsér-Gusev-Jungers[4], 2018)

- *The problem of deciding whether a given set of matrices is primitive is NP-hard, even in the case of two matrices.*
- $\lim_{n \to +\infty} \frac{\log \mathsf{p}(n)}{n} = \frac{\log 3}{3}$.

[4] Balázs Gerencsér, Vladimir V. Gusev, and Raphaël M. Jungers (2018). "Primitive sets of nonnegative matrices and synchronizing automata". In: *SIAM J. Matrix Anal. Appl.* 39.1, pp. 83–98.

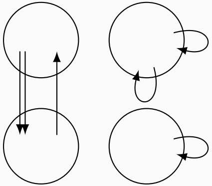
Matrices without zero lines

We use $\mathcal{NZ}$ to denote the subfamily of Boolean matrices that have no zero rows and columns.

Theorem (Protasov-Voynov[5], 2012)

Let $\mathcal{A}$ be a set of matrices belonging to $\mathcal{NZ}$. If $\sum_{A \in \mathcal{A}} A$ is irreducible, then there exists a unique minimal partition (canonical partition) $[n] = \bigsqcup_{i=1}^{r} V_i$ such that every matrix $A \in \mathcal{A}$ is a block-permutation matrix with respect to $\{V_1, \ldots, V_r\}$.

$$A = \begin{pmatrix} 0 & 0 & B_1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & B_2 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ B_{r-2} & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & B_{r-1} & \cdots & 0 \\ 0 & B_r & 0 & 0 & \cdots & 0 \end{pmatrix}.$$



[5] V.Yu. Protasov and A.S. Voynov (2012). "Sets of nonnegative matrices without positive products". In: *Linear Algebra and its Applications* 437.3, pp. 749–765.

Testing primivity for $\mathcal{NZ}$ matrix sets

Given a set of $\mathcal{NZ}$-matrices $\mathcal{A} = \{A_1, \ldots, A_m\} \subseteq \{0,1\}^{n\times n}$, there is an algorithm to determine whether $\mathcal{A}$ is primitive or not in polynomial time.

- (Protasov-Voynov[6], 2012) $O(n^3 m)$.
- (Gusev-Jungers[7], 2017) $O(n^2 m)\alpha(n+m)$.
- (Wu-Z., 2021+) $O(n^2 m)$.

Ackerman's function is defined as follows for nonnegative integers x and y:

$$
\begin{aligned}
A(0,y) &= y+1 \\
A(x+1,0) &= A(x,1) \\
A(x+1,y+1) &= A(x, A(x+1,y))
\end{aligned}
$$

Its value grows rapidly. For example, $A(4,2) = 2^{2^{2^{2^{2}}}} - 3 \approx 10^{19729}$. The function α is define as $\alpha(N) = \max\{x : A(x,x) \geq N\}$.

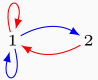
[6] V.Yu. Protasov and A.S. Voynov (2012). "Sets of nonnegative matrices without positive products". In: *Linear Algebra and its Applications* 437.3, pp. 749–765.

[7] Vladimir V. Gusev, Raphaël M. Jungers, and Elena V. Pribavkina (2017). "Generalized primitivity of labeled digraphs". In: *Electronic Notes in Discrete Mathematics* 61, pp. 549–555.

An observation on the canonical partition

- Regard $\mathcal{A} = \{A_1, \ldots, A_m\}$ as a arc-labeled digraph $G_{\mathcal{A}} = G$, where $V(G) = [n]$ and $E(G) = \{i \xrightarrow{k} j : [A_k]_{i,j} = 1\}$.
- The notation $i \xrightarrow{(c_1,\ldots,c_k)} j$ means there exists a walk $(e_1, \ldots, e_k)$ from i to j such that the label of e_t is c_t for $1 \le t \le k$.
- Note that $\mathcal{A}$ is primitive if and only if there exists a label sequence $(c_1, \ldots, c_k)$ such that every pair of vertex $i, j \in V(G)$, we have $i \xrightarrow{(c_1,\ldots,c_k)} j$.

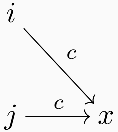
$$\left\{ \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \right\}$$



$\mathcal{C}$ = Red, Blue

An observation on the canonical partition, Contd

A pair of vertex (i, j) is **synchronizing** if there exists a label sequence $c = (c_1, \ldots, c_k)$ such that



for some $x \in V(G)$.

Observation (Wu-Z., 2021+)

Let $\mathcal{A}$ be a set of matrices belonging to $\mathcal{NZ}$. Assume $V_1, \ldots, V_r$ form the canonical partition of $\mathcal{A}$. Then $i, j \in V_k$ if and only if (i, j) is synchronizing.

Our algorithm

Let $V = \{1, \dots, n\}$.
Input $\mathcal{A} = \{A_1, \dots, A_m\} \subseteq \{0,1\}^{n \times n}$.

- Use Tarjan's algorithm to check irreducibility of $\sum_{A \in \mathcal{A}} A$ in $O(n^2 m)$-time.
- Let H be the digraph such that $V(H) = \binom{V}{\leq 2}$ and $E(H) = \{\{i,j\} \to \{p,q\} : (i,p),(j,q) \in E(G_{\mathcal{A}})\}$.
- Every pair of vertices $i, j \in V$ is synchronizing if and only if there exists a H-walk from $\{i,j\}$ to $\{x\}$ for some x. And this can be done in $O(n^2 m)$.

Primitive indices on $\mathcal{NZ}$-matrix set

$\mathsf{p}_{\mathcal{NZ}}(n) := \max\{\mathsf{p}(\mathcal{A}) : \mathcal{A} \subseteq \{0,1\}^{n\times n} \cap \mathcal{NZ} \text{ is primitive}\}$

Theorem (Blondel-Jungers-Olshevsky, 2015[8])

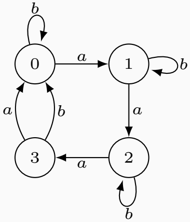
$\mathsf{p}_{\mathcal{NZ}}(n) \geq \frac{n^2}{2}$.

[8] Vincent D. Blondel, Raphaël M. Jungers, and Alex Olshevsky (2015). "On primitivity of sets of matrices". In: *Automatica J. IFAC* 61, pp. 80–88.

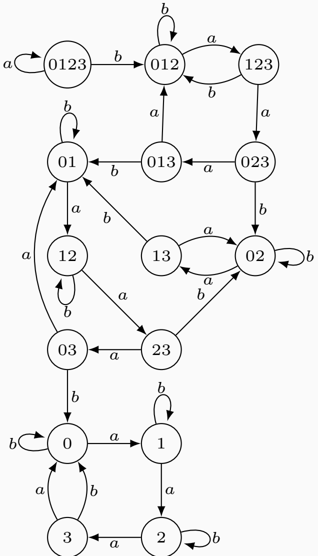
Synchronizing automata

A **(deterministic finite) automaton** $\mathcal{A} \subseteq \{0,1\}^{n\times n}$ is a set of Boolean matrices such that each row of each matrix $A \in \mathcal{A}$ contains a unique 1.
An automata is **synchronizing** if there exists a product of matrices of $\mathcal{A}$ which contains one positive column. The length of shortest such product is called **synchronizing index** of $\mathcal{A}$, denoted by $\mathrm{c}(\mathcal{A})$.

Černý automata $\mathcal{C}_4$ and its power automata



$baaabaaab$



Černý Conjecture

$\mathsf{c}(n) := \max\{\mathsf{c}(\mathcal{A}) : \mathcal{A} \subseteq \{0,1\}^{n\times n}$ is a synchronizing automata$\}$

Conjecture (Černý[9], 1964)

$\mathsf{c}(n) = (n-1)^2$

Some progress:

- (Černý, 1964) $(n-1)^2 \leq \mathsf{c}(n)$
- (Pin[10]-Frankl[11], 1982) $\mathsf{c}(n) \leq \frac{n^3-n}{6} \leq 0.1667n^3 + O(1)$.
- (Szykuła[12], 2017) $\mathsf{c}(n) \leq 0.1664n^3 + O(1)$.
- (Shitov[13], 2019) $\mathsf{c}(n) \leq 0.1654n^3 + O(1)$.

[9] J. Černý (1964). "Poznámka k homogénnym eksperimentom s konecnými automatami". In: *Mat.-Fyz. Cas. Slovensk. Akad. Vied.* 14.3, pp. 208–216.

[10] J.-E. Pin (1983). "On two combinatorial problems arising from automata theory". In: *Combinatorial mathematics (Marseille-Luminy, 1981)*. Vol. 75. North-Holland Math. Stud. Pp. 535–548.

[11] P. Frankl (1982). "An extremal problem for two families of sets". In: *European J. Combin.* 3.2, pp. 125–127.

[12] M. Szykuła (2018). "Improving the Upper Bound on the Length of the Shortest Reset Words". In: *Proc. 35th STACS*. vol. 96. LIPIcs.

[13] Yaroslav Shitov (2019). "An improvement to a recent upper bound for synchronizing words of finite automata". In: *Journal of Automata, Languages and Combinatorics* 24, pp. 367–373.

Upper bound of $\mathsf{p}_{\mathcal{NZ}}(n)$

Theorem (Blondel-Jungers-Olshevsky, 2015[14])

$\mathsf{p}_{\mathcal{NZ}}(n) \leq 2\,\mathsf{c}(n) + n - 1 = O(n^3)$.

Proof.

- Let $\mathcal{A}$ be a primitive set of matrices belonging to $\mathcal{NZ}$.
- $\mathcal{B} := \{B \leq A \in \mathcal{A} :$ each row of B has a unique $1\}$.
- $\mathcal{B}$ is a synchronizing automata.
- $\exists D \in \mathcal{A}^{\mathsf{c}(n)}$ such that the i-th column is positive for some i.
- $\exists D' \in \mathcal{A}^{\mathsf{c}(n)}$ such that the j-th row is positive for some j.
- $\exists C \in \mathcal{A}^{n-1}$ such that $C[i,j] = 1$.
- $DCD' > 0$.

□

[14] Vincent D. Blondel, Raphaël M. Jungers, and Alex Olshevsky (2015). "On primitivity of sets of matrices". In: *Automatica J. IFAC* 61, pp. 80–88.

Hurwitz products

Let $\mathcal{A} = \{A_1, \ldots, A_m\}$ be a set of Boolean $(n \times n)$-matrices. For a tuple $\alpha = (\alpha_1, \ldots, \alpha_m)$ of nonnegative intergers, we define the **Hurwitz products** $\mathcal{A}^\alpha$ to be the sum of all products of matrices from $\mathcal{A}$, in which every product contains exactly α_i factors equal to A_i.
The length of $\mathcal{A}^\alpha$ is defined by $|\alpha| := \sum_{i=1}^m \alpha_i$.

Example

- $\mathcal{A} = \{A_1, A_2, A_3\}$.
- $\mathcal{A}^{(1,3,0)} = A_1 A_2^3 + A_2 A_1 A_2^2 + A_2^2 A_1 A_2 + A_2^3 A_1$.

Weakly primitive

A family of nonnegative matrices is **weakly primitive** if there exists a positive Hurwitz product of those matrices.

Theorem (Protasov[15], 2013)

Let $\mathcal{A}$ be a set of Boolean matrices. Suppose all matrices of $\mathcal{A}$ have no zero rows. Assume $\sum_{A\in\mathcal{A}} A$ is irreducible. Then there exists a unique minimal partition $[n] = \bigsqcup_{i=1}^{r} V_i$ such that

- *(**Block Permutation Condition**) for every $A \in \mathcal{A}$, there exists a permutation σ_A on $\{1, 2, \dots, r\}$ satisfying $A[V_i, V_j] \neq 0$ if and only if $j = \sigma_A(i)$.*
- *(**Commutativity**) for all $A, A' \in \mathcal{A}$, $\sigma_A \sigma_{A'} = \sigma_{A'} \sigma_A$.*

[15] V.Yu. Protasov (2013). "Classification of k-primitive sets of matrices". In: *SIAM J. Matrix Anal.* 34.3, pp. 1174–1188.

Weakly primitive

An automaton is **weakly synchronizing** if there exists a Hurwitz product $\mathcal{A}^\alpha$ of those matrices such that A has one positive column. The length of shortest such product is called **weakly synchronizing index** of $\mathcal{A}$, denoted by $\mathrm{wc}(\mathcal{A})$.

(weakly) primitivity/synchronizing

	Primitive	Weakly Primitive
Assumptions	no zero columns and rows	no zero columns
The length of shortest (Hurwitz) positive product	$O(n^3)$	?
Decidability	$O(n^2 m)\alpha(n+m)$	$O(n^3 m + n^2 m^2)$
Find a (Hurwitz) positive product	$O(n^3 m)$	?
Find a shortest (Hurwitz) positive product	NP-hard	?
Calculate (weakly) primitive index	NP-hard	?

	Synchronizing	Weakly Synchronizing
Assuptions		
The length of shortest (weakly) synchronzing product	$O(n^3)$	?
Decidability	$O(n^2 m)$	$O(mn^2(\log n + m))$
Find a (weakly) synchronzing product	$O(n^3 m)$	?
Find a shortest (weakly) synchronzing product	NP-hard	?
Calculate (weak) synchronzing index	NP-hard	?

(weakly) primitivity/synchronizing

	Primitive	Weakly Primitive
Assumptions	no zero columns and rows	no zero columns
The length of shortest positive (Hurwitz) product	$O(n^3)$	$O(n^3)$
Decidability	$O(n^2m)$	$O(n^3m + n^2m^2)$
Find a (Hurwitz) positive product	$O(n^3m)$	$O(n^3m^2)$
Find a shortest (Hurwitz) positive product	NP-hard	?
Calculate (weakly) primitive index	NP-hard	?

	Synchronizing	Weakly Synchronizing
Assuptions		
The length of shortest synchronizing (Hurwitz) product	$O(n^3)$	$O(n^3)$
Decidability	$O(n^2m)$	$O(mn^2(\log n + m))$
Find a synchronizing (Hurwitz) product	$O(n^3m)$	$O(n^3m^2)$
Find a shortest synchronizing (Hurwitz) product	NP-hard	?
Calculate (weakly) synchronizing index	NP-hard	?

Key observation

- Let $\mathcal{A} = \{A_1, \ldots, A_m\}$ be an automaton.
- Let $E_{i,j} = A_i A_j + A_j A_i$ for $1 \leq i < j \leq m$.
- $\mathcal{B} := \mathcal{A} \cup \{B \leq E_{i,j}$: each row of B has a unique $1\}$.

Observation (Wu-Z., 2021+)

If $\mathcal{A}$ is weakly synchronizing, then $\mathcal{B}$ is synchronizing. Moreover, $\mathrm{wc}(\mathcal{A}) \leq 2\,\mathrm{c}(\mathcal{B})$.

Strongly primitive matrix set

Definition

A finite set $\mathcal{A} = \{A_1, \ldots, A_m\}$ of Boolean $(n \times n)$-matrices is called **strongly primitive** if there exists $k \geq 0$ such that every product

$$A_{i_1} A_{i_2} \cdots A_{i_k} > 0,$$

where $A_{i_j} \in \mathcal{A}$.
The minimum such k is called the **strongly primitive index** of $\mathcal{A}$, denoted by $\mathrm{sp}(\mathcal{A})$.

Upper bound of strongly primitive indices

- (Cohen-Sellers[16], 1982) $\mathrm{sp}(n) = 2^n - 2$;
- (Shao[17], 1985) For $k \leq 2^n - 2$, there exists $\mathcal{A} \subseteq \{0,1\}^{n\times n}$ such that $\mathrm{sp}(\mathcal{A}) = k$.
- (Wu-Z.[18], 2015) There exists $\mathcal{A} = \{A_1, \ldots, A_n\} \subseteq \{0,1\}^{n\times n}$ such that $\mathrm{sp}(\mathcal{A}) = 2^n - 2$.

---

[16] J. E. Cohen and P. H. Sellers (1982). "Sets of nonnegative matrices with positive inhomogeneous products". In: *Linear Algebra and its Application* 47, pp. 185–192.

[17] J.-Y. Shao (1985). *On the properties of nonnegative primitive matrices, irreducible matrices and thier associated directed graphs*. University of Wisconsin-Madison.

[18] Yaokun Wu and Yinfeng Zhu (2015). "Lifespan in a primitive Boolean linear dynamical system". In: *The Electronic Journal of Combinatorics* 22.Paper. #P4.36, pp. 1–21.

Strongly synchronizing automata

Definition

An automaton $\mathcal{A} \subseteq \{0,1\}^{n\times n}$ is called **strongly synchronizing** if there exists $k \geq 0$ such that every product

$$A_{i_1} A_{i_2} \cdots A_{i_k}$$

has exactly one nonzero column.
The minimum such k is called the **strongly primitive index** of $\mathcal{A}$, denoted by $\mathrm{sc}(\mathcal{A})$.

Theorem (Bleak-Cameron-Maissel-Navas-Olukoya, 2016[19])

- *There exists an algorithm to determine whether a given automaton is strongly synchronizing in $O(n^2 m)$-time.*
- $\mathrm{sc}(\mathcal{A}) \leq n-1$.

[19] Collin Bleak et al. (May 2016). "The further chameleon groups of Richard Thompson and Graham Higman: Automorphisms via dynamics for the Higman groups $G_{n,r}$". In: *arXiv e-prints*, arXiv:1605.09302, arXiv:1605.09302. arXiv: 1605.09302

rank conjectures

Definition

Let $\mathcal{A} \subseteq \{0,1\}^{n\times n}$ be an automaton.

- $r(A) :=$ the number of nonzero columns in A.
- $\operatorname{rank}(\mathcal{A}) := \min\{r(A) : A$ is a product of matrices of $\mathcal{A}\}$.
- $\mathcal{A}$ is **strongly** r**-synchronizing** if every long-enough product of matrices of $\mathcal{A}$ has exactly r nonzero columns.

Conjecture (Volkov)

Let $\mathcal{A} \subseteq \{0,1\}^{n\times n}$ be an automaton. Then there exists a product of length $(n-r)^2$ with exactly r nonzero columns.

Conjecture (Wu-Z., 2021+)

Let $\mathcal{A} \subseteq \{0,1\}^{n\times n}$ be a strongly r-synchronizing automaton. Then every matrix in $\mathcal{A}^{n-r}$ has exactly r nonzero columns.

Some progress

- $\mathsf{sc}^r(\mathcal{A}) :=$ the strongly r-synchronizing index of $\mathcal{A}$.
- $\mathsf{sc}^r(n) := \max\{\mathsf{sc}^r(\mathcal{A}) :$
  $\mathcal{A}$ is strongly r-synchronizing automaton$\}$.

Theorem (Wu- Z., 2021+)

- $\mathsf{sc}^2(n) = n - 2.$
- $\mathsf{sc}^3(n) = o(n^2).$
- $\mathsf{sc}^r(n) \leq \binom{n}{2} - \binom{r}{2}.$

Thank you!