Combinatorial indices for matrix semigroups and finite automata

Alexander E. Guterman

Bar-Ilan University, Israel

Workshop on Series, Automata, Matrices,
Symbolic dynamics, and their Applications
June 2-6, Warsaw

The talk is based on a series of works with
Yu.A. Alpin,
A.M. Maksaev,
E.R. Shafeev

Positive and Non-negative matrices

Let $A \in M_n(\mathbb{R})$ be an $n \times n$ matrix with the real entries.
A is positive if all its entries are positive, $a_{ij} > 0$,
A is non-negative, if all $a_{ij} \geq 0$.

Combinatorial matrix theory is an efficient approach to investigate non-negative matrices. Here

$$\text{matrix properties} \longrightarrow \text{graph theory constructions}$$

- Directed graph (or digraph) $G = (V, E)$. Loops are permitted but multiple edges are not. Order of G is the number of vertices in it.

Graphs

- Directed graph (or digraph) $G = (V, E)$. Loops are permitted but multiple edges are not. Order of G is the number of vertices in it.
- $u \to v$ walk in a digraph G. The length of a walk is the number of edges in it. The notation $u \xrightarrow{k} v$ is used to indicate that there is a $u \to v$ walk of length k.

Graphs

- Directed graph (or digraph) $G = (V, E)$. Loops are permitted but multiple edges are not. Order of G is the number of vertices in it.
- $u \rightarrow v$ walk in a digraph G. The length of a walk is the number of edges in it. The notation $u \xrightarrow{k} v$ is used to indicate that there is a $u \rightarrow v$ walk of length k.
- A closed walk is a $u \rightarrow v$ walk where $u = v$.

Graphs

- Directed graph (or digraph) $G = (V, E)$. Loops are permitted but multiple edges are not. Order of G is the number of vertices in it.
- $u \to v$ walk in a digraph G. The length of a walk is the number of edges in it. The notation $u \xrightarrow{k} v$ is used to indicate that there is a $u \to v$ walk of length k.
- A closed walk is a $u \to v$ walk where $u = v$.
- A cycle is a closed $u \to v$ walk with distinct vertices except for $u = v$.
- The length of a shortest cycle in G is called the girth of G.

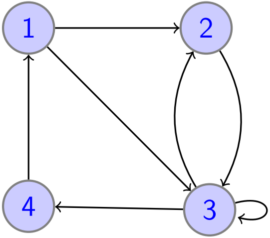
Correspondence between matrices and digraphs

Let $A = (a_{ij}) \in M_n(\mathbf{B})$. A corresponds to a digraph $G = G(A)$ of order n as follows. The vertex set is the set $V = \{1, \dots, n\}$. There is an edge (i, j) from i to j iff $a_{ij} \neq 0$. A is adjacency matrix of G.

Correspondence between matrices and digraphs

Let $A = (a_{ij}) \in M_n(\mathbf{B})$. A corresponds to a digraph $G = G(A)$ of order n as follows. The vertex set is the set $V = \{1, \ldots, n\}$. There is an edge (i, j) from i to j iff $a_{ij} \neq 0$. A is adjacency matrix of G.

$$A = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad \longleftrightarrow$$



$G(A)$

Definition

Non-negative $A \in M_n$, $A \geq 0$, $n \geq 2$, is called decomposable if $\exists$ permutation matrix $P \in M_n$ such that

$$A = P \begin{pmatrix} B & 0 \\ C & D \end{pmatrix} P^t,$$

where B, D are square matrices and C is possibly a rectangular matrix. If A is not decomposable, then it is called indecomposable.

Definition

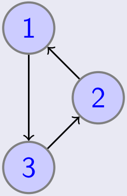
G is strongly connected iff for any $u, v \in V(G)$ there is an oriented path from u to v.

Theorem

Let $A \in M_n$, $A \geq 0$. *TFAE*

- A *is indecomposable,*
- $G(A)$ *is strongly connected,*
- $(I + A)^{n-1} > 0$,
- $\forall\ i, j,\ i \neq j,\ \exists\ k$: (i, j)*-th element of* A^k *is positive.*

Example



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

$(I + A)^2 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$.

Primitive digraphs

Definition

- A digraph G is primitive if for some positive integer t for all vertices u, v it is true that $u \xrightarrow{t} v$.

Primitive digraphs

Definition

- A digraph G is primitive if for some positive integer t for all vertices u, v it is true that $u \xrightarrow{t} v$.
- If G is primitive, the exponent of G is the smallest such t.

Primitive digraphs

Definition

- A digraph G is primitive if for some positive integer t for all vertices u, v it is true that $u \xrightarrow{t} v$.
- If G is primitive, the exponent of G is the smallest such t.

Definition

- $A \in M_n$, $A \geq 0$, is primitive if $\exists\ k \in \mathbb{Z}_{>0} : \quad A^k > 0$.
- If $A \in M_n$ is primitive, then the exponent of A is the smallest such k.

Primitive digraphs

Definition

- A digraph G is primitive if for some positive integer t for all vertices u, v it is true that $u \xrightarrow{t} v$.
- If G is primitive, the exponent of G is the smallest such t.

Definition

- $A \in M_n$, $A \geq 0$, is primitive if $\exists\ k \in \mathbb{Z}_{>0} : \quad A^k > 0$.
- If $A \in M_n$ is primitive, then the exponent of A is the smallest such k.

Then $A^{k+1} = A^k \cdot A > 0$.

Theorem

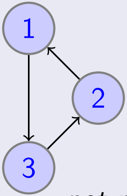
Let G be an digraph. THAE

- *G is primitive,*
- *G is strongly connected and the GCD of all cycle lengths in G is 1,*
- *$A(G)$ is primitive.*

Corollary

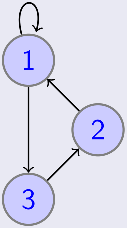
Let G be a primitive digraph. Then $\exp(G) = \exp(A(G))$.

Example



$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ *is indecomposable and is*

not primitive: $A^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, $A^3 = I$, $A^4 = A$, *etc.*



$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ *is primitive:* $A^4 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$

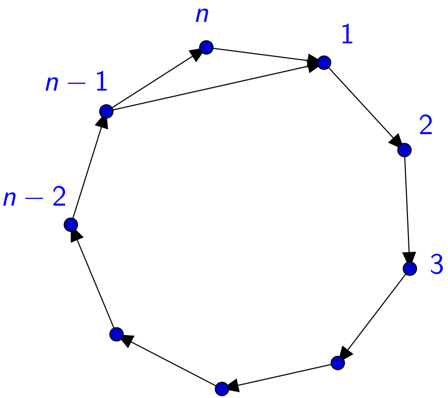
The Wielandt matrix is

$$W_n = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Theorem (Wielandt)

Let $A \in M_n$, $A \geq 0$. *Then* $\exp(A) \leq \exp(W_n) = (n-1)^2 + 1$.

Classical example



W_n

W_n is called a Wielandt digraph. It is the digraph with the maximal possible exponent, $(n-1)^2+1$.

Akelbek and Kirkland, 2009

Definition

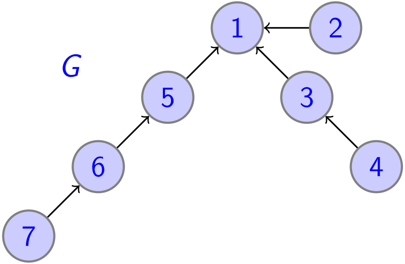
The scrambling index of a digraph G is the smallest positive integer k such that for every pair $u, v \in V(G)$, exists $w \in V(G)$ such that $u \xrightarrow{k} w$ and $v \xrightarrow{k} w$ in G.

The scrambling index of G is denoted by $k(G)$. If such w does not exist, let $k(G) = 0$.

$$k(W_n) = \left\lceil \frac{(n-1)^2+1}{2} \right\rceil < (n-1)^2 + 1 = \exp(W_n)$$

How to compute the scrambling index?

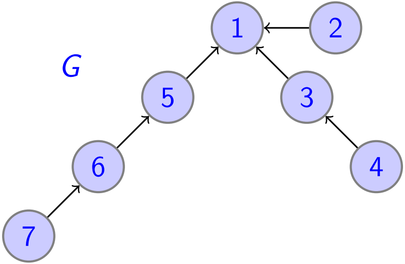
Simple structure of digraph



What is the value of $k(G)$?

How to compute the scrambling index?

Simple structure of digraph

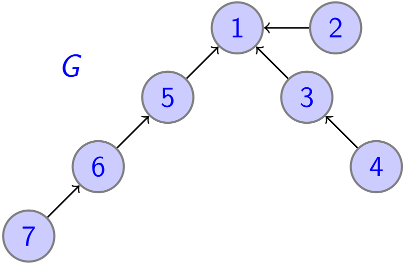


What is the value of $k(G)$?

$2 \xrightarrow{1} 1$, but $4 \xrightarrow{2} 1$, and there is no other way

How to compute the scrambling index?

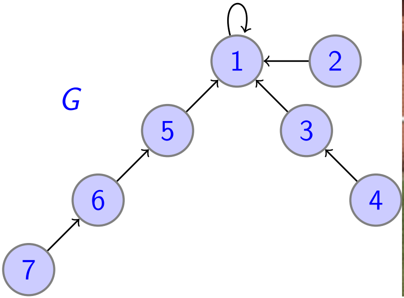
Simple structure of digraph



What is the value of $k(G)$?

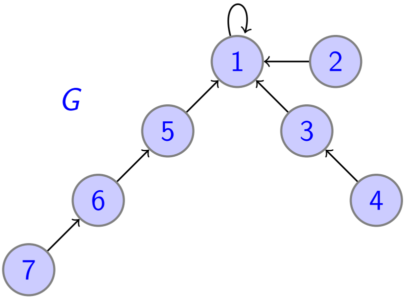
$2 \xrightarrow{1} 1$, but $4 \xrightarrow{2} 1$, and there is no other way $\Longrightarrow$ $k(G) = 0$

Applications



How to compute the scrambling index?

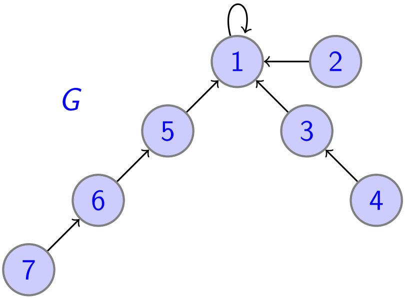
Simple structure of digraph



What is the value of $k(G)$?

How to compute the scrambling index?

Simple structure of digraph

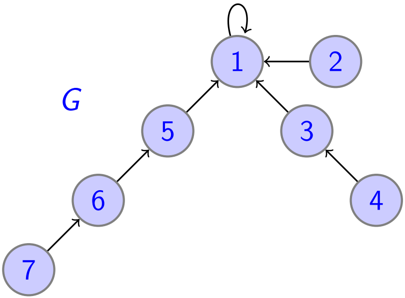


What is the value of $k(G)$?

$\forall\, a \in V(G),\ a \xrightarrow{3} 1$, but it is impossible to get from 7 to 1 less than by 3 steps

How to compute the scrambling index?

Simple structure of digraph



What is the value of $k(G)$?

$\forall\, a \in V(G),\ a \xrightarrow{3} 1$, but it is impossible to get from 7 to 1 less than by 3 steps $\Longrightarrow$ $k(G) = 3$

Applications: Markov chains

Let $P = (p_{ij})$ be a primitive stochastic matrix (thus, $\rho(P) = 1$).

Applications: Markov chains

Let $P = (p_{ij})$ be a primitive stochastic matrix (thus, $\rho(P) = 1$). The goal is to get some upper bounds for the modulus of the second largest eigenvalue of P.

Applications: Markov chains

Let $P = (p_{ij})$ be a primitive stochastic matrix (thus, $\rho(P) = 1$).
The goal is to get some upper bounds for the modulus of the second largest eigenvalue of P.
Coefficient of ergodicity (Dobrushin or delta coefficient):

$$\tau(P) = \frac{1}{2} \max_{i,j} \sum_{l=1}^{n} |p_{il} - p_{jl}|$$

Applications: Markov chains

Let $P = (p_{ij})$ be a primitive stochastic matrix (thus, $\rho(P) = 1$). The goal is to get some upper bounds for the modulus of the second largest eigenvalue of P.
Coefficient of ergodicity (Dobrushin or delta coefficient):

$$\tau(P) = \frac{1}{2}\max_{i,j}\sum_{l=1}^{n}|p_{il} - p_{jl}|$$

Theorem (Akelbek, Kirkland)

Let $P = (p_{ij})$ be an $n \times n$ primitive stochastic matrix with $k(P) = k$ and suppose that λ is a non-unit eigenvalue of P. Then $\tau(P^k) < 1$ and $|\lambda| \leq (\tau(P^k))^{1/k}$.

Application: Memoryless communication system

- A memoryless communication system is represented by a digraph G, $|G| = n$.

Application: Memoryless communication system

- A memoryless communication system is represented by a digraph G, $|G| = n$.
- Suppose that at time $t = 0$ each of two different vertices of G (in general, 2 may be replaced with an arbitrary $\lambda \in \mathbb{Z}$, $2 \leqslant \lambda \leqslant n$) 'knows' 1 bit of inf. and these bits are distinct.

Application: Memoryless communication system

- A memoryless communication system is represented by a digraph G, $|G| = n$.
- Suppose that at time $t = 0$ each of two different vertices of G (in general, 2 may be replaced with an arbitrary $\lambda \in \mathbb{Z}$, $2 \leqslant \lambda \leqslant n$) 'knows' 1 bit of inf. and these bits are distinct.
- At time $t = 1$ each v_i having some information in it passes all the information bits to each of its outputs and simultaneously it may receive some information. Then $\forall$ v_i forgets the passed information and has only the received information or nothing.

Application: Memoryless communication system

- A memoryless communication system is represented by a digraph G, $|G| = n$.
- Suppose that at time $t = 0$ each of two different vertices of G (in general, 2 may be replaced with an arbitrary $\lambda \in \mathbb{Z}$, $2 \leqslant \lambda \leqslant n$) 'knows' 1 bit of inf. and these bits are distinct.
- At time $t = 1$ each v_i having some information in it passes all the information bits to each of its outputs and simultaneously it may receive some information. Then $\forall$ v_i forgets the passed information and has only the received information or nothing.
- The system continues in this way.

Application: Memoryless communication system

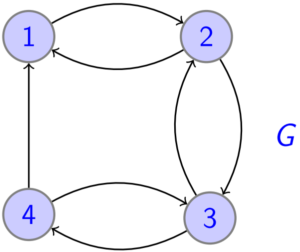
- A memoryless communication system is represented by a digraph G, $|G| = n$.
- Suppose that at time $t = 0$ each of two different vertices of G (in general, 2 may be replaced with an arbitrary $\lambda \in \mathbb{Z}$, $2 \leqslant \lambda \leqslant n$) 'knows' 1 bit of inf. and these bits are distinct.
- At time $t = 1$ each v_i having some information in it passes all the information bits to each of its outputs and simultaneously it may receive some information. Then $\forall\ v_i$ forgets the passed information and has only the received information or nothing.
- The system continues in this way.
- For some digraphs after certain time there exists a vertex that knows both bits of the information, independently on the choice of the initial two vertices. When and what digraphs?

How to compute the scrambling index?

Theorem (Lewin)

G is primitive iff G is strongly connected and $k(G) \neq 0$.

What is the value of $k(G)$?

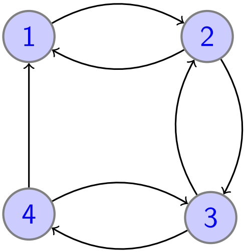


How to compute the scrambling index?

Theorem (Lewin)

G is primitive iff G is strongly connected and $k(G) \neq 0$.

What is the value of $k(G)$?



G

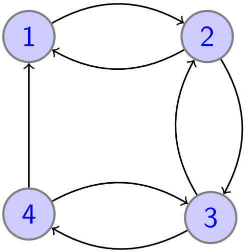
- G is strongly connected (it has a Hamilton cycle $1 \to 2 \to 3 \to 4$),
- G is not primitive (it has cycles of lengths only 2 and 4)

How to compute the scrambling index?

Theorem (Lewin)

G is primitive iff G is strongly connected and $k(G) \neq 0$.

What is the value of $k(G)$?



G

- G is strongly connected (it has a Hamilton cycle $1 \to 2 \to 3 \to 4$),
- G is not primitive (it has cycles of lengths only 2 and 4)

$\Longrightarrow$ $k(G) = 0$.

Scrambling index in terms of the matrix theory

Definition (Seneta)

Matrix $A \in M_n(\mathbf{B})$ is named scrambling matrix if no two rows of it are orthogonal. Equivalently, if any two rows have at least one non-zero element in coincident position.

Scrambling index in terms of the matrix theory

Definition (Seneta)

Matrix $A \in M_n(\mathbf{B})$ is named scrambling matrix if no two rows of it are orthogonal. Equivalently, if any two rows have at least one non-zero element in coincident position.

Definition (Akelbek, Kirkland)

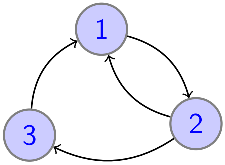
The scrambling index of a matrix $A \in M_n(\mathbf{B})$ is the smallest positive integer k such that A^k is the scrambling matrix.

The scrambling index of A is denoted by $k(A)$. If such k does not exist, let $k(A) = 0$.

Theorem (Akelbek, Kirkland)

Let G be a primitive digraph. Then $k(G) = k(A(G))$.

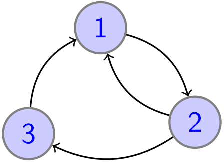
How to calculate the scrambling index?



What is the value of $k(A)$?

$G(A)$

How to calculate the scrambling index?

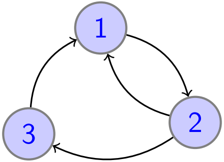


What is the value of $k(A)$?

$G(A)$

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, A^2 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, A^3 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

How to calculate the scrambling index?



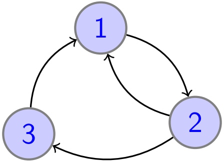
What is the value of $k(A)$?

$G(A)$

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, A^2 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, A^3 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

$$\Longrightarrow \qquad k(A) = 3$$

How to calculate the scrambling index?



What is the value of $k(A)$?

$G(A)$

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, A^2 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, A^3 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

$\Longrightarrow \quad k(A) = 3$

$u = 2, v = 3$. Then $w = 3$ and the shortest paths are $2 \to 1 \to 2 \to 3$ and $3 \to 1 \to 2 \to 3$.

Some known bounds for the scrambling index

Theorem (Huang, Liu)

Let G de a primitive digraph of order $n \geq 2$ with d loops. Then

$$k(G) \leq n - \left\lceil \frac{d}{2} \right\rceil .$$

Denote

$$K(n,s) = n - s + \begin{cases} \left(\frac{s-1}{2}\right) n, & \text{when } s \text{ is odd,} \\ \left(\frac{n-1}{2}\right) s, & \text{when } s \text{ is even.} \end{cases}$$

Theorem (Akelbek, Kirkland)

Let G be a primitive digraph with n vertices and girth s. Then $k(G) \leq K(n,s)$.

Some known bounds for the scrambling index

Theorem (Akelbek, Kirkland)

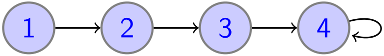
Let G be a primitive digraph of order $n \geq 3$. Then

$$k(G) \leq \left\lceil \frac{(n-1)^2+1}{2} \right\rceil.$$

Equality holds iff $G \cong W_n$.

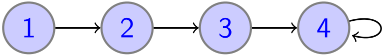
Actually, we do not need to require primitivity...

G:



Actually, we do not need to require primitivity...

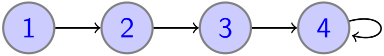
G:



- G is not primitive.

Actually, we do not need to require primitivity...

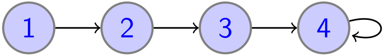
G:



- G is not primitive.
- G is not strongly connected.

Actually, we do not need to require primitivity...

G:



- G is not primitive.
- G is not strongly connected.
- $k(G) = 3 \neq 0$.

Characterization of digraphs with $k(G) \neq 0$

Theorem (GM, 2019)

For an arbitrary digraph G the following conditions are equivalent:

1. $k(G) \neq 0$.
2. *There exists a primitive subgraph G' of G s.t. $\forall$ $v \in V(G)$ $\exists$ $w \in V(G')$ for which $\exists$ a directed walk from v to w in G.*

$(G_1 \to G_2)$-partition

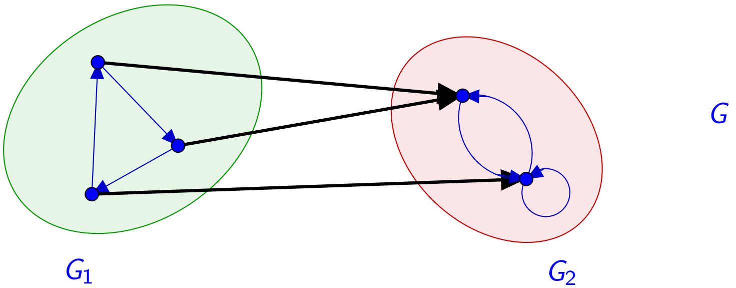
Definition

Let G be a directed graph. G has a $(G_1 \to G_2)$-partition if G_1 and G_2 are non-empty subgraphs of the digraph G such that:

1. $V(G) = V(G_1) \sqcup V(G_2)$;
2. *for each directed edge $e = (v_1, v_2) \in E(G)$, either $e \in E(G_1)$, or $e \in E(G_2)$, or $v_1 \in V(G_1), v_2 \in V(G_2)$.*

Illustration

For a not strongly connected digraph G let us consider a $(G_1 \to G_2)$-partition:



Remark

Geometrically this means that $V(G)$ is partitioned into two non-intersecting components $V(G_1)$ and $V(G_2)$ that are connected only by edges from G_1 to G_2.

New upper bounds

Let G is not strongly connected digraph of order n with $k(G) \neq 0$ and G_1, G_2 be its $(G_1 \to G_2)$-partition.

Theorem (GM, 2019)

Let s be a girth of G_2. Then

$$k(G) \leqslant 1 + K(n-1, s).$$

Here,

$$K(n,s) = n - s + \begin{cases} \left(\dfrac{s-1}{2}\right) n, & \text{when } s \text{ is odd,} \\ \left(\dfrac{n-1}{2}\right) s, & \text{when } s \text{ is even.} \end{cases}$$

New upper bounds

Let G is not strongly connected digraph of order n with $k(G) \neq 0$ and G_1, G_2 be its $(G_1 \to G_2)$-partition.

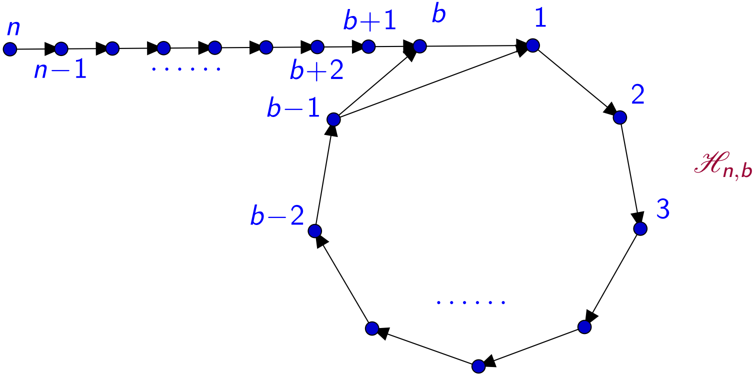
Theorem (GM, 2019)

Assume that $|G_2| = b \leqslant n-1$. *Then*

$$k(G) \leqslant n - b + \left\lceil \frac{(b-1)^2 + 1}{2} \right\rceil.$$

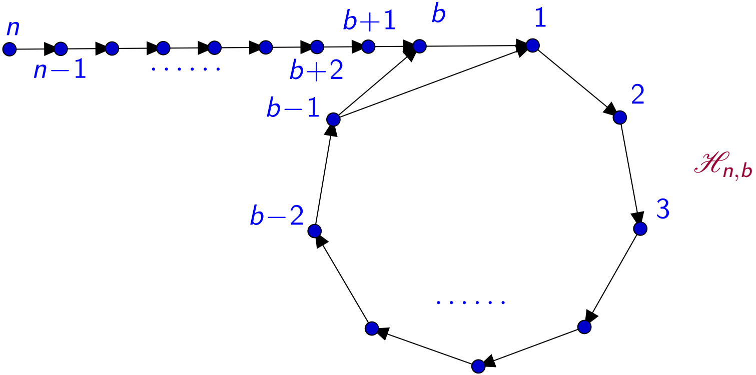
Sharpness of the upper bound

Let $n \geq 3, \ b \leq n-1$. Define a digraph $\mathscr{H}_{n,b}$:



Sharpness of the upper bound

Let $n \geq 3,\ b \leq n-1$. Define a digraph $\mathscr{H}_{n,b}$:



If $b > 1$, then $k(\mathscr{H}_{n,b}) = n - b + \left\lceil \frac{(b-1)^2+1}{2} \right\rceil$.

New upper bounds

Let G is not strongly connected digraph of order n with $k(G) \neq 0$ and G_1, G_2 be its $(G_1 \to G_2)$-partition.

Theorem (GM, 2019)

Assume that $|G_2| = b \leqslant n-1$. *Then*

$$k(G) \leqslant n - b + \left\lceil \frac{(b-1)^2+1}{2} \right\rceil.$$

If $4 \leqslant n < 2b$, *then equality holds if and only if* $G \cong \mathscr{H}_{n,b}$.

Corollaries

Theorem (GM, 2019)

Let G be an arbitrary digraph of order $n \geqslant 3$. Then

$$k(G) \leqslant \left\lceil \frac{(n-1)^2+1}{2} \right\rceil.$$

The equality holds if and only if $G \cong W_n$.

Corollaries

Theorem (GM, 2019)

Let G be an arbitrary digraph of order $n \geqslant 3$. Then

$$k(G) \leqslant \left\lceil \frac{(n-1)^2+1}{2} \right\rceil.$$

The equality holds if and only if $G \cong W_n$.

Theorem (GM, 2019)

Let G be a not strongly connected digraph of order $n \geqslant 3$. Then

$$k(G) \leqslant 1 + \left\lceil \frac{(n-2)^2+1}{2} \right\rceil.$$

When $n \geqslant 4$, the equality holds if and only if $G \cong \mathscr{H}_{n,n-1}$.

Maps preserving scrambling index

Definition

- *We say that T is a map preserving the scrambling index, if for all $A \in M_n(\mathbf{B})$ we have that $k(T(A)) = k(A)$.*
- *We say that T is a map preserving the non-zero scrambling index, if for all $A \in M_n(\mathbf{B})$, for which $k(A) \neq 0$, we have that $k(T(A)) = k(A)$.*
- *We say that T is a map preserving the scrambling index on the set of primitive matrices if $\forall$ primitive $A \in M_n(\mathbf{B})$ we have that $k(T(A)) = k(A)$.*

Theorem (Frobenius, 1896)

$T : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ — *linear, bijective,*

$$\det(T(A)) = \det A \qquad \forall A \in M_n(\mathbb{C})$$

$$\Downarrow$$

$$\exists P, Q \in GL_n(\mathbb{C}), \det(PQ) = 1 :$$

$$T(A) = PAQ \quad \forall A \in M_n(\mathbb{C})$$

or

$$T(A) = PA^t Q \quad \forall A \in M_n(\mathbb{C})$$

Definition

$T : M_{m\,n}(\mathbb{F}) \to M_{m\,n}(\mathbb{F})$ is standard iff
$\exists P \in GL_m(\mathbb{F}),\ Q \in GL_n(\mathbb{F})$:

$$T(A) = PAQ \quad \forall A \in M_{m,n}(\mathbb{F})$$

or $m = n$ and

$$T(A) = PA^tQ \quad \forall A \in M_{m,n}(\mathbb{F})$$

Let $X \in M_{m,n}(\mathbb{C})$. Then $C_r(X) \in M_{\binom{m}{r},\binom{n}{r}}(\mathbb{C})$ consists from r-minors of X ordered lexicographically by rows and columns.

Theorem

[Schur, 1925] Let $T : M_{m\,n}\mathbb{C}) \to M_{m\,n}(\mathbb{C})$ be bijective and linear, r, $2 \leq r \leq \min\{m, n\}$, be given. $\exists$ bijective linear $S : M_{\binom{m}{r},\binom{n}{r}}(\mathbb{C}) \to M_{\binom{m}{r},\binom{n}{r}}(\mathbb{C})$ s.t.

$$C_r(T(X)) = S(C_r(X)) \ \ \forall \ \in M_{m,n}(\mathbb{C})$$

iff T is standard.

Theorem (Dieudonné, 1949)

$\Omega_n(\mathbb{F})$ *is the set of singular matrices*
$T : M_n(\mathbb{F}) \to M_n(\mathbb{F})$ *— linear, bijective,* $T(\Omega_n(\mathbb{F})) \subseteq \Omega_n(\mathbb{F})$

$$\Downarrow$$

$$\exists P, Q \in GL_n(\mathbb{F})$$

$$T(A) = PAQ \quad \forall A \in M_n(\mathbb{F})$$

or

$$T(A) = PA^tQ \quad \forall A \in M_n(\mathbb{F})$$

E.B. Dynkin, Maximal subgroups of classical groups // The Proceedings of the Moscow Mathematical Society, **1** (1952) 39-166.

$$St_n(\mathbb{F}) \subseteq Fix(S) \subseteq GL_{n^2}(\mathbb{F})$$

The quantity of Linear Preservers for a given matrix invariant is a measure of its complexity. Indeed, to compute the invariant for a given matrix, we reduce it to a certain good form, where computations are easy.

$$\det(A) = \sum_{\sigma \in S_n} (-1)^n a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

• Computations of det require $\sim O(n^3)$ operations

$$\mathrm{per}\,(A) = \sum_{\sigma \in S_n} a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

• Computations of per require
$\sim (n-1) \cdot (2^n - 1)$ multiplicative operations (Raiser formula).

The explanation

There are just few linear preservers of permanent in comparison with the determinant. Indeed,

Theorem (Marcus, May)

Linear transformation T *is permanent preserver iff*
$T(A) = P_1 D_1 A D_2 P_2 \quad \forall A \in M_n(\mathbb{F})$, *or*
$T(A) = P_1 D_1 A^t D_2 P_2 \quad \forall A \in M_n(\mathbb{F})$
where D_i *are invertible diagonal matrices,* $i = 1, 2, \det(D_1 D_2) = 1$
P_i *are permutation matrices,* $i = 1, 2$

- Group theory

Question Is it possible that two non-isomorphic finite groups have the same group determinant?

Theorem (E. Formanek, D. Sibley)

A group determinant determines the group up to an automorphism

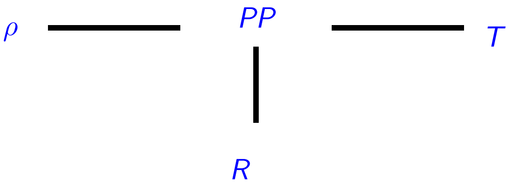
Proof is based on an extension of Dieudonne singularity preserver theorem to the direct products of matrix algebras.

Preserve Problems

$\rho : M_n(R) \to S$ is a certain matrix invariant
$T : M_n(R) \to M_n(R)$

$$\rho(T(A)) = \rho(A) \quad \forall A \in M_n(R)$$

$$T = ?$$



Let $\mathbb{F}$ be a field

$\emptyset \neq S \subseteq M_n(\mathbb{F})$	$T(S) \subseteq S$
$\rho : M_n(\mathbb{F}) \to \mathbb{F}\ \forall A \in M_n(\mathbb{F})$	$\rho(T(A)) = \rho(A)$
$\sim: M_n(\mathbb{F})^2 \to \{0, 1\}$	$A \sim B \Rightarrow T(A) \sim T(B)$ $\forall A, B \in M_n(\mathbb{F})$
P – property in $M_n(\mathbb{F})$	$A \in P \Rightarrow T(A) \in P$

$T = ?$

The standard solution in linear case

There are $P, Q \in GL_n(\mathbb{F})$:

$$T(X) = PXQ \quad \forall X \in M_n(\mathbb{F})$$

or

$$T(X) = PXQ \quad \forall X^t \in M_n(\mathbb{F})$$

Basic methods to investigate PPs

1. Matrix theory
2. Theory of classical groups
3. Projective geometry
4. Algebraic geometry
5. Differential geometry
6. Dualisations
7. Tensor calculus
8. Functional identities
9. Model theory

Maps preserving scrambling index

Theorem

Let $n \geq 3$ and $T : M_n(\mathbf{B}) \to M_n(\mathbf{B})$ be an arbitrary mapping. Then T is a bijective additive operator which preserves non-zero scrambling index

$$\Updownarrow$$

$\exists$ *permutation matrix P such that $T(A) = P^T A P$, $\forall A \in M_n(\mathbf{B})$.*

Maps preserving scrambling index

Theorem

Let $n \geq 3$ *and* $T: M_n(\mathbf{B}) \to M_n(\mathbf{B})$ *be an arbitrary mapping. Then* T *is a bijective additive operator which preserves non-zero scrambling index*

$$\Updownarrow$$

$\exists$ *permutation matrix* P *such that* $T(A) = P^T A P$, $\forall A \in M_n(\mathbf{B})$.

For $A \in M_n(\mathbf{B})$ let us use the notation:

$$A_{id} = \sum_{k:\ A(k,k)=1} E_{kk}; \quad A_{od} = \sum_{i \neq j:\ A(i,j)=1} E_{ij}.$$

Maps preserving distinct values of the scrambling index

Theorem

Let $n \geqslant 3$ *and* $T : M_n(\mathbf{B}) \to M_n(\mathbf{B})$ *be an additive bijective map.*

- T *preserves* $k = 1$ *iff* $\exists$ *permutation matrices* P, Q *s.t.*

$$T(A) \;=\; PA\,Q.$$

- T *preserves* $k = 0$ *iff* $\exists$ *a permutation matrix* P, *s.t.*

$$T(A) \;=\; P^T A\,P.$$

- T *preserves* $k = \max$ *iff* $\exists$ *permutation matrices* P, Q *s.t.*

$$T(A) = P^T A_{od}\,P + Q^T A_{id}\,Q \quad \textit{for all } A \in M_n(\mathbf{B})$$

$$T(A) = P^T A_{od}^T\,P + Q^T A_{id}\,Q \quad \textit{for all } A \in M_n(\mathbf{B})$$

Maps preserving scrambling index

Theorem

Let $n \geqslant 3$ *and* $T\colon M_n(\mathbf{B}) \to M_n(\mathbf{B})$ *be the additive map preserves the scrambling index. Then* T *is a bijection.*

Steps of the proof

1. Let $A, B \in M_n$. If A is primitive, then $A + B$ is primitive.
2. Let $A, B \in M_n$. If $k(A) \neq 0$, then $k(A+B) \neq 0$ and $k(A+B) \leqslant k(A)$.
3. Some notations: $C_n = E_{n,1} + \sum_{i=1}^{n-1} E_{i,i+1}$ is the adjacency matrix of the elementary cycle $(12\dots n)$. Then $W_n = C_n + E_{n-1,1}$ is the Wielandt matrix.

$\mathcal{W} = \{A \in M_n(\mathbf{B}) \,|\, \exists\ P \in \mathcal{P}_n \colon P^T A P = W_n\}$ – Wielandt like
$\mathcal{C} = \{A \in M_n(\mathbf{B}) \,|\, \exists\ P \in \mathcal{P}_n \colon P^T A P = C_n\}$ – cycles
$\mathcal{E} = \{E_{ij} \in M_n(\mathbf{B}) \,|\, 1 \leqslant i, j \leqslant n\}$ – cells
$\mathcal{D} = \{E_{ii} \in M_n(\mathbf{B}) \,|\, 1 \leqslant i \leqslant n\}$ – diagonal cells
$\mathcal{N} = \mathcal{E} \setminus \mathcal{D} = \{E_{ij} \in \mathcal{E} \,|\, i \neq j\}$ – off-diagonal cells

4. By 2. $A \in \mathcal{W} \Rightarrow T(A) \in \mathcal{W}$.

Steps of the proof

5. T is bijective on $\mathcal{W}$.
6. Let $n \geqslant 4$, $E_{ij} \in \mathcal{N}$. Then there exist two distinct matrices $W_1, W_2 \in \mathcal{W}$ such that $W_1 \circ W_2 = E_{ij}$, i.e. W_1 and W_2 have a unique non-zero entry in the position (i, j).
7. For any pair $E_{ij}, E_{kl} \in \mathcal{N}$, $E_{ij} \neq E_{kl}$, there exists a matrix $W \in \mathcal{W}$ such that $W \geqslant E_{ij}$, $W \ngeqslant E_{kl}$. 8. Let $A \in M_n$. Then $T(A) = O$ iff $A = 0$. 9. $T(\mathcal{N}) \subseteq \mathcal{N}$, and moreover, $T(\mathcal{N}) = \mathcal{N}$.
10. For any digraph G the edge number $|E(G)| = |E(G(T(A(G))))|$.
11. G does not have loops iff $G(T(A(G)))$ does not have loops.
12. $T(\mathcal{C}) = \mathcal{C}$
13. $T(\mathcal{D}) \subseteq \mathcal{D}$, and moreover, $T(\mathcal{D}) = \mathcal{D}$.

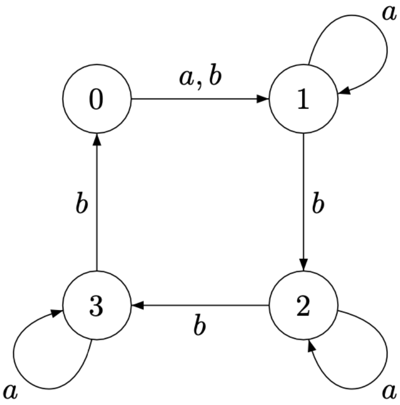
Hence T is bijective!

Application to minimal synchronizing automaton

Application to minimal synchronizing automaton

Definition

A word w is called a synchronizing (reset) word of a deterministic finite automaton DFA if w brings all states of the automaton to some specific state.



abbbabbba

Conjecture (Černý, 1964)

The shortest synchronizing word for any n-state complete DFA has length $\leq (n-1)^2$.

Theorem (Černý, 1964)

There are DFAs with minimal synchronizing words of length exactly

$$(n-1)^2.$$

Theorem

All known bounds are of order n^3.

Graphs of large exponent and/or scrambling index lead to examples of slowly synchronizing automata.

Thank you!