Matrix convertibility over finite fields

Mikhail V. Budrevich
(Lomonosov Moscow State University)

Ljubljana, Slovenia
7 june 2014

Permanent and determinant functions

Definition

Let $A = (a_{ij})$ be a square matrix of order n and S_n is a symmetric group on n elements, then

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}$$

$$\operatorname{per}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i\sigma(i)}$$

Permanent and determinant functions

Definition

Let $A = (a_{ij})$ be a square matrix of order n and S_n is a symmetric group on n elements, then

$$\det(A) = \sum_{\sigma \in S_n} \text{sign}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}$$

$$\text{per}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i\sigma(i)}$$

Example

- *Number of domino tiling's*
- *Number of derangements of order n*
- *Ménage numbers*
- *Number of perfect matching in bipartite graph*

Pólya permanent problem

Example (Pólya)

$$\phi : \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \to \begin{pmatrix} a_{11} & -a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

The following equation is true:

$$\mathrm{per}(A) = \det(\phi(A))$$

Pólya permanent problem

Example (Pólya)

$$\phi : \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \to \begin{pmatrix} a_{11} & -a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

The following equation is true:

$$\mathrm{per}(A) = \det(\phi(A))$$

Definition

The matrix A of order n is convertible if there is matrix $X = X(A) \in M_n(\pm 1)$ such that the following equation is true:

$$\mathrm{per}(A) = \det(A \circ X)$$

Previous results, part 1

Example (Pólya, Szegö)

Matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

is inconvertible.

Previous results, part 1

Example (Pólya, Szegö)

Matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

is inconvertible.

Theorem (Gibson)

Let $A \in M_n(0,1)$ *and* $\mathrm{per}(A) > 0$. *If* A *is convertible then* $\nu(A) \leq \Omega_n = \frac{n^2+3n-2}{2}$. *If* $\nu(A) = \Omega_n$ *then there exist permutation matrices* P, Q *such that* $PAQ = G_n$, *where*

$$\begin{cases} g_{ij} = 1, & \text{if } j \leq i+1 \\ g_{ij} = 0, & \text{otherwise.} \end{cases}$$

Previous results, part 2

Theorem (Brualdi, Shader)

Matrix $A \in M_n(0,1)$ *is convertible iff there is sing-nonsingular matrix* S *with zero elements on the same positions as in matrix* A*.*

Previous results, part 2

Theorem (Brualdi, Shader)

Matrix $A \in M_n(0, 1)$ *is convertible iff there is sing-nonsingular matrix* S *with zero elements on the same positions as in matrix* A*.*

Definition

Matrix $A \in M_n(\mathbb{R})$ *is sign-nonsingular if every matrix with the same position of zeros, positive and negative elements is nonsingular.*

Previous results, part 2

Theorem (Brualdi, Shader)

Matrix $A \in M_n(0,1)$ *is convertible iff there is sing-nonsingular matrix* S *with zero elements on the same positions as in matrix* A.

Definition

Matrix $A \in M_n(\mathbb{R})$ *is sign-nonsingular if every matrix with the same position of zeros, positive and negative elements is nonsingular.*

Theorem (Little)

Bipartient graph G *admits Pfaffian orientation iff incidence matrix* A *is convertible.*

Previous results, part 2

Theorem (Brualdi, Shader)

Matrix $A \in M_n(0,1)$ is convertible iff there is sing-nonsingular matrix S with zero elements on the same positions as in matrix A.

Definition

Matrix $A \in M_n(\mathbb{R})$ is sign-nonsingular if every matrix with the same position of zeros, positive and negative elements is nonsingular.

Theorem (Little)

Bipartient graph G admits Pfaffian orientation iff incidence matrix A is convertible.

Theorem (Valiant)

Computing permanent of $A \in M_n(0,1)$ is $\# - P$-complete problem.

Bijective convertation over finite field

Theorem (Dolinar, Guterman, Kuzma, Orel)

Suppose $n \geq 3$. *Then there exist* $q_0 = q_0(n)$ *such that for any finite field* $\mathbb{F}$ *with at least* q_0 *elements and* $\mathrm{ch}(\mathbb{F}) > 2$ *no bijective map* $\phi : M_n(\mathbb{F}) \to M_n(\mathbb{F})$ *satisfies* $\mathrm{per}(A) = \det(\phi(A))$.

Bijective convertation over finite field

Theorem (Dolinar, Guterman, Kuzma, Orel)

Suppose $n \geq 3$. Then there exist $q_0 = q_0(n)$ such that for any finite field $\mathbb{F}$ with at least q_0 elements and $\mathrm{ch}(\mathbb{F}) > 2$ no bijective map $\phi : M_n(\mathbb{F}) \to M_n(\mathbb{F})$ satisfies $\mathrm{per}(A) = \det(\phi(A))$.

Example

Growing of q_0 depending on n

n	3	4	5	6	7	8	9	10	11
q_0	3	43	79	121	167	223	289	367	449

Bijective convertation over finite field

Theorem (Dolinar, Guterman, Kuzma, Orel)

Suppose $n \geq 3$. Then there exist $q_0 = q_0(n)$ such that for any finite field $\mathbb{F}$ with at least q_0 elements and $\mathrm{ch}(\mathbb{F}) > 2$ no bijective map $\phi : M_n(\mathbb{F}) \to M_n(\mathbb{F})$ satisfies $\operatorname{per}(A) = \det(\phi(A))$.

Example

Growing of q_0 depending on n

n	3	4	5	6	7	8	9	10	11
q_0	3	43	79	121	167	223	289	367	449

Theorem (Budrevich, Guterman)

Let $\mathbb{F}$ be a finite field with characteristic $p \geq 3$. Then for each $n \geq 3$ there is no bijective map $\phi : M_n(\mathbb{F}) \to M_n(\mathbb{F})$ such that $\operatorname{per}(A) = \det(\phi(A))$.

Convertibility over finite fields

How can we define (sign) convertibility over finite field?

Convertibility over finite fields

How can we define (sign) convertibility over finite field?

Definition

The matrix $A \in M_n(\mathbb{F})$ *of order* n *is convertible if there is matrix* $X = X(A) \in M_n(\pm 1)$ *such that the following equation is true:*

$$\mathrm{per}(A) = \det(A \circ X) \pmod{\mathbb{F}}$$

Convertibility over finite fields

How can we define (sign) convertibility over finite field?

Definition

The matrix $A \in M_n(\mathbb{F})$ *of order* n *is convertible if there is matrix* $X = X(A) \in M_n(\pm 1)$ *such that the following equation is true:*

$$\mathrm{per}(A) = \det(A \circ X) \pmod{\mathbb{F}}$$

Example

If $\mathbb{F}$ *is a finite field with characteristic* 2 *then* $\mathrm{per}(A) = \det(A)$*.*

Field with 3 elements

Theorem (Budrevich, Guterman)

Let $A \in M_n(\mathbb{F}_3)$*. Then there is matrix* $X \in M_n(\pm 1)$ *such that* $\operatorname{per}(A) = \det(A \circ X)$.

Field with 3 elements

Theorem (Budrevich, Guterman)

Let $A \in M_n(\mathbb{F}_3)$*. Then there is matrix* $X \in M_n(\pm 1)$ *such that* $\mathrm{per}(A) = \det(A \circ X)$.

Remark

There is no unique matrix $X \in M_n(\pm 1)$ *such that any matrix* $A \in M_n(\mathbb{F}_3)$ *satisfies the equation* $\mathrm{per}(A) = \det(A \circ X)$.

Field with 3 elements

Theorem (Budrevich, Guterman)

Let $A \in M_n(\mathbb{F}_3)$. Then there is matrix $X \in M_n(\pm 1)$ such that $\mathrm{per}(A) = \det(A \circ X)$.

Remark

There is no unique matrix $X \in M_n(\pm 1)$ such that any matrix $A \in M_n(\mathbb{F}_3)$ satisfies the equation $\mathrm{per}(A) = \det(A \circ X)$.

Example

Matrix J_3 with all ones is convertible over field $\mathbb{F}_3$ as $\mathrm{per}(J_3) = \det(J_3)$.

Nonconvertible matrices over finite fields

Example

Matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

is nonconvertible as a matrix over finite field with characteristic $p \geq 5$.

Nonconvertible matrices over finite fields

Example

Matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

is nonconvertible as a matrix over finite field with characteristic $p \geq 5$.

Example

Let $\mathbb{F}_q$ *be a finite field with* $q = 3^k$ *elements and* $k > 1$. *If* $\mathbb{F}_q = \mathbb{F}_p[x]/ < h(x) >$, *where* $h(x)$ *is irreducable polynom of order* k, *then matrix*

$$\begin{pmatrix} x & 2 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

is nonconvertible as a matrix over field $\mathbb{F}_q$.

Sufficient condition of convertibility

$$S(A) = (s_{ij}) : \begin{cases} s_{ij} = 1, & \text{if } a_{ij} \neq 0 \\ s_{ij} = 0, & \text{if } a_{ij} = 0. \end{cases}$$

Theorem (Idea 1)

Let $A \in M_n(\mathbb{F})$. If $S(A)$ is convertible as a matrix over $\mathbb{R}$ then A is convertible as a matrix over finite field $\mathbb{F}$.

Sufficient condition of convertibility

$$S(A) = (s_{ij}) : \begin{cases} s_{ij} = 1, & \text{if } a_{ij} \neq 0 \\ s_{ij} = 0, & \text{if } a_{ij} = 0. \end{cases}$$

Theorem (Idea 1)

Let $A \in M_n(\mathbb{F})$. If $S(A)$ is convertible as a matrix over $\mathbb{R}$ then A is convertible as a matrix over finite field $\mathbb{F}$.

Theorem (Idea 2)

Let $A \in M_n(\mathbb{F}_p)$, where $\mathbb{F}_p$ is a prime field with p elements. If there is a row (or column) in A such that in Laplace decomposition by this row (column) at least $p-1$ nonzero summands, then A is convertible.

Gibson theorem over finite field

Theorem (Gibson)

Let $A \in M_n(0,1)$ and $\mathrm{per}(A) > 0$. If A is convertible then $\nu(A) \leq \Omega_n = \frac{n^2+3n-2}{2}$. If $\nu(A) = \Omega_n$ then there exist permutation matrices P, Q such that $PAQ = G_n$.

Question: Can we construct the condition same to Gibson theorem for proving nonconvertability for some matrices?

Gibson theorem over finite field

Theorem (Gibson)

Let $A \in M_n(0,1)$ and $\mathrm{per}(A) > 0$. If A is convertible then $\nu(A) \le \Omega_n = \frac{n^2+3n-2}{2}$. If $\nu(A) = \Omega_n$ then there exist permutation matrices P, Q such that $PAQ = G_n$.

Question: Can we construct the condition same to Gibson theorem for proving nonconvertability for some matrices?

Example

Let $\mathbb{F}$ be a finite field of $q = p^k$ elements and $p \ge 3$. For any $n \ge p-1$ there is a convertible nonsingular matrix $A \in M_n(\mathbb{F})$ with all nonzero elements.

Gibson theorem over finite field

Theorem (Gibson)

Let $A \in M_n(0,1)$ and $\mathrm{per}(A) > 0$. If A is convertible then $\nu(A) \leq \Omega_n = \frac{n^2+3n-2}{2}$. If $\nu(A) = \Omega_n$ then there exist permutation matrices P, Q such that $PAQ = G_n$.

Question: Can we construct the condition same to Gibson theorem for proving nonconvertability for some matrices?

Example

Let $\mathbb{F}$ be a finite field of $q = p^k$ elements and $p \geq 3$. For any $n \geq p-1$ there is a convertible nonsingular matrix $A \in M_n(\mathbb{F})$ with all nonzero elements.

New question: Can we somehow reverse Gibson result for finite field?

Reverse Gibson theorem

We want to prove some condition that guarantee convertibility of a matrix A over finite field.

Reverse Gibson theorem

We want to prove some condition that guarantee convertibility of a matrix A over finite field.

Theorem

Let $A \in M_n(\mathbb{F}_p)$*, where* $\mathbb{F}_p$ *is a prime finite field with* p *elements and* $n \geq 2p - 6$*, satisfies the folowing conditions:*

Reverse Gibson theorem

We want to prove some condition that guarantee convertibility of a matrix A over finite field.

Theorem

Let $A \in M_n(\mathbb{F}_p)$, where $\mathbb{F}_p$ is a prime finite field with p elements and $n \geq 2p - 6$, satisfies the folowing conditions:

1. *There is a column in A with all nonzero elements.*

Reverse Gibson theorem

We want to prove some condition that guarantee convertibility of a matrix A over finite field.

Theorem

Let $A \in M_n(\mathbb{F}_p)$, where $\mathbb{F}_p$ is a prime finite field with p elements and $n \geq 2p - 6$, satisfies the folowing conditions:

1. *There is a column in A with all nonzero elements.*
2. *There a row in A with at least $M = (p-3)\log_2(n-1)(p-1) + 2$ nonzero elements.*

Reverse Gibson theorem

We want to prove some condition that guarantee convertibility of a matrix A over finite field.

Theorem

Let $A \in M_n(\mathbb{F}_p)$, where $\mathbb{F}_p$ is a prime finite field with p elements and $n \geq 2p - 6$, satisfies the folowing conditions:

1. *There is a column in A with all nonzero elements.*
2. *There a row in A with at least $M = (p-3)\log_2(n-1)(p-1) + 2$ nonzero elements.*
3. *Matrix A is fully indecomposable.*

Reverse Gibson theorem

We want to prove some condition that guarantee convertibility of a matrix A over finite field.

Theorem

Let $A \in M_n(\mathbb{F}_p)$, where $\mathbb{F}_p$ is a prime finite field with p elements and $n \geq 2p - 6$, satisfies the folowing conditions:

1. *There is a column in A with all nonzero elements.*
2. *There a row in A with at least $M = (p-3)\log_2(n-1)(p-1) + 2$ nonzero elements.*
3. *Matrix A is fully indecomposable.*
   Then matrix A is converible.

Reverse Gibson theorem

We want to prove some condition that guarantee convertibility of a matrix A over finite field.

Theorem

Let $A \in M_n(\mathbb{F}_p)$, where $\mathbb{F}_p$ is a prime finite field with p elements and $n \geq 2p - 6$, satisfies the folowing conditions:

1. *There is a column in A with all nonzero elements.*
2. *There a row in A with at least $M = (p-3)\log_2(n-1)(p-1) + 2$ nonzero elements.*
3. *Matrix A is fully indecomposable.*
   Then matrix A is converible.

Example

Let $A \in M_{14}(\mathbb{F}_5)$ be a fully indecomposable matrix and at least one row and one column of A consist of nonzero elements. Then A is convertible.

Some corollaries

Corollary

Let $A \in M_n(\mathbb{F}_p)$ *where* $\mathbb{F}_p$ *is a prime field with* p *elements. If* $n \geq (p-3)\log_2(n-1)(p-1)+2$ *then* A *is convertible.*

Some corollaries

Corollary

Let $A \in M_n(\mathbb{F}_p)$ where $\mathbb{F}_p$ is a prime field with p elements. If $n \geq (p-3)\log_2(n-1)(p-1)+2$ then A is convertible.

Corollary

Suppose $n \geq (p-3)\log_2(n-1)(p-1)+2$. Let $A \in M_n(\mathbb{F}_p)$ be a symmetric matrix satisfies the following condition

1. *There is a row in A with all nonzero elements.*
2. *There is $\sigma \in S_n$ full cycle such that $\prod_{i=1}^{n} a_{i\sigma(i)} \neq 0$.*

Then matrix A is convertible.

Ideas of the proof

Idea 1. We prove that for any $z \in \mathbb{F}_p$ there is a matrix $X \in M_n(\pm 1)$ such that $\det(A \circ X) = z$.

Ideas of the proof

Idea 1. We prove that for any $z \in \mathbb{F}_p$ there is a matrix $X \in M_n(\pm 1)$ such that $\det(A \circ X) = z$.

Idea 2.

Lemma

Let $a_1, \ldots, a_k$ be nonzero elements of $\mathbb{F}_p$ and $k \geq p$. Then any $z \in \mathbb{F}_p$ is equal to some linear combination $\sum_{i=1}^{k} \delta_i a_i$, $\delta_i \in \{\pm 1\}$.

Ideas of the proof

Idea 1. We prove that for any $z \in \mathbb{F}_p$ there is a matrix $X \in M_n(\pm 1)$ such that $\det(A \circ X) = z$.

Idea 2.

Lemma

Let $a_1, \ldots, a_k$ be nonzero elements of $\mathbb{F}_p$ and $k \geq p$. Then any $z \in \mathbb{F}_p$ is equal to some linear combination $\sum_{i=1}^{k} \delta_i a_i$, $\delta_i \in \{\pm 1\}$.

Idea 3. Find $X \in M_n(\pm 1)$ such that for matrix $A \circ X$ there is a row (column) for which in Laplace decomposition formula at least $p - 1$ nonzero summands.

Thank you!

Thank you!

M.V.Budrevich
mbudrevich@yandex.ru