Matrix positivity preservers over finite fields

Dominique Guillot

University of Delaware

Applied Matrix Positivity II
ICMS Edinburgh
November 2024

Joint work with Himanshu Gupta (U. Regina), Prateek Kumar Vishwakarma (IISc Bangalore), and Chi Hoi (Kyle) Yip (Georgia Tech)

Positive definite matrices (real case)

Let A be a real symmetric matrix.

Theorem

The following are equivalent for a symmetric matrix $A \in M_n(\mathbb{R})$:

1. *A is positive definite ($x^T A x > 0 \ \forall x \in \mathbb{R}^n \setminus \{\mathbf{0}_n\}$.).*
2. *All the eigenvalues of A are positive.*
3. *There exist a non-singular matrix $B \in M_n(\mathbb{R})$ such that $A = B^2$.*
4. *There exist a full rank matrix $B \in M_{n,m}(\mathbb{R})$ such that $A = BB^T$.*
5. *The matrix A admits a Cholesky factorization $A = LL^T$ (L is lower triangular with positive diagonal entries).*
6. *All the principal minors of A are positive.*
7. **The leading principal minors of A are positive.**

Moreover, the entrywise product $A \circ B = (a_{ij} b_{ij})$ of two positive definite matrices is positive definite.

What about positive definite matrices over finite fields?

What about positive definite matrices over finite fields?

- $\mathbb{F}_q =$ finite field with $q = p^k$ elements. We let $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$. (e.g. $k = 1$: $\mathbb{F}_p = \mathbb{Z}_p =$ integers mod p)

What about positive definite matrices over finite fields?

- $\mathbb{F}_q =$ finite field with $q = p^k$ elements. We let $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$. (e.g. $k = 1$: $\mathbb{F}_p = \mathbb{Z}_p =$ integers mod p)
- Positive elements in $\mathbb{F}_q$ (non-zero quadratic residues):

$$\mathbb{F}_q^+ := \{a^2 : a \in \mathbb{F}_q^*\}.$$

What about positive definite matrices over finite fields?

- $\mathbb{F}_q$ = finite field with $q = p^k$ elements. We let $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$. (e.g. $k = 1$: $\mathbb{F}_p = \mathbb{Z}_p$ = integers mod p)
- Positive elements in $\mathbb{F}_q$ (non-zero quadratic residues):

$$\mathbb{F}_q^+ := \{a^2 : a \in \mathbb{F}_q^*\}.$$

Definition: (see Cooper, Hanna, and Whitlatch, 2022) A matrix $A \in M_n(\mathbb{F}_q)$ is *positive definite* if it is symmetric and its leading principal minors are **positive**.

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}$$

Example

- For example, consider $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. Then

Example

- For example, consider $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. Then

$$\mathbb{F}_7^+ = \{1^2, 2^2, 3^2, 4^2, 5^2, 6^2\} = \{1, 2, 4\}.$$

Example

- For example, consider $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. Then
$$\mathbb{F}_7^+ = \{1^2, 2^2, 3^2, 4^2, 5^2, 6^2\} = \{1, 2, 4\}.$$
- The matrix
$$\begin{pmatrix} 4 & 1 \\ 1 & 6 \end{pmatrix}$$

Example

- For example, consider $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. Then

$$\mathbb{F}_7^+ = \{1^2, 2^2, 3^2, 4^2, 5^2, 6^2\} = \{1, 2, 4\}.$$

- The matrix

$$\begin{pmatrix} 4 & 1 \\ 1 & 6 \end{pmatrix}$$

is positive definite.

Example

- For example, consider $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. Then

$$\mathbb{F}_7^+ = \{1^2, 2^2, 3^2, 4^2, 5^2, 6^2\} = \{1, 2, 4\}.$$

- The matrix

$$\begin{pmatrix} 4 & 1 \\ 1 & 6 \end{pmatrix}$$

is positive definite.

- However,

$$\begin{pmatrix} 4 & 1 \\ 1 & 1 \end{pmatrix}$$

is not positive definite since $\det A = 3 \notin \mathbb{F}_7^+$.

(Lack of) Equivalent definitions

Theorem (Cooper, Hanna, and Whitlatch, 2022)

The following are equivalent for a symmetric matrix $A \in M_n(\mathbb{F}_q)$:

1. ~~$x^T A x \in \mathbb{F}_q^+ \ \forall x \in (\mathbb{F}_q^*)^n$.~~
2. ~~*All the eigenvalues of A are positive.*~~
3. ~~*There exist a non-singular matrix $B \in M_n(\mathbb{R})$ such that $A = B^2$.*~~
4. ~~*There exist a full rank matrix $B \in M_{n,m}(\mathbb{R})$ such that $A = BB^T$.*~~
5. *Only if q is even or $q \equiv 3 \pmod 4$ The matrix A admits a Cholesky factorization $A = LL^T$*
   (L is lower triangular with positive diagonal entries).
6. ~~*All the principal minors of A are positive.*~~
7. **The leading principal minors of A are positive.**

~~Moreover, the entrywise product $A \circ B = (a_{ij} b_{ij})$ of two positive definite matrices is positive definite.~~

In particular, the quadratic form approach does not yield a useful notion of matrix positivity.

Proposition (Cooper, Hanna, and Whitlatch, 2022)

Let $\mathbb{F}_q$ be a finite field, let $n \geq 3$, and let $A \in M_n(\mathbb{F}_q)$. Then there exists a non-zero vector $x \in \mathbb{F}_q^n$ so that $x^T Ax = 0$.

Equivalent Definitions (cont.)

In particular, the quadratic form approach does not yield a useful notion of matrix positivity.

Proposition (Cooper, Hanna, and Whitlatch, 2022)

Let $\mathbb{F}_q$ be a finite field, let $n \geq 3$, and let $A \in M_n(\mathbb{F}_q)$. Then there exists a non-zero vector $x \in \mathbb{F}_q^n$ so that $x^T Ax = 0$.

The range of the quadratic form of a positive definite matrix is not contained in $\mathbb{F}_q^+$.

Equivalent Definitions (cont.)

In particular, the quadratic form approach does not yield a useful notion of matrix positivity.

Proposition (Cooper, Hanna, and Whitlatch, 2022)

Let $\mathbb{F}_q$ be a finite field, let $n \geq 3$, and let $A \in M_n(\mathbb{F}_q)$. Then there exists a non-zero vector $x \in \mathbb{F}_q^n$ so that $x^T A x = 0$.

The range of the quadratic form of a positive definite matrix is not contained in $\mathbb{F}_q^+$.

Proposition (Guillot, Gupta, Vishwakarma, Yip, 2024)

Let $n \geq 2$ and let $A \in M_n(\mathbb{F}_q)$ be a positive definite matrix. Then

$$\{x^T A x : x \in \mathbb{F}_q^n\} = \mathbb{F}_q.$$

Non-linear entrywise transformers

- The theory of positive definiteness is still in its infancy. There are a lot of opportunities to develop the theory and find applications (algebra? combinatorics? cryptography? total positivity/ finite Grassmannian (Machacek, 2024)).

Non-linear entrywise transformers

- The theory of positive definiteness is still in its infancy. There are a lot of opportunities to develop the theory and find applications (algebra? combinatorics? cryptography? total positivity/ finite Grassmannian (Machacek, 2024)).

Given a function $f : \mathbb{F} \to \mathbb{F}$ and a matrix $A = (a_{ij}) \in M_n(\mathbb{F})$, let

$$f[A] := (f(a_{ij})).$$

Non-linear entrywise transformers

- NEW The theory of positive definiteness is still in its infancy. There are a lot of opportunities to develop the theory and find applications (algebra? combinatorics? cryptography? total positivity/ finite Grassmannian (Machacek, 2024)).

Given a function $f : \mathbb{F} \to \mathbb{F}$ and a matrix $A = (a_{ij}) \in M_n(\mathbb{F})$, let

$$f[A] := (f(a_{ij})).$$

- We say f *preserves positivity* on $M_n(\mathbb{F})$ if $f[A]$ is positive definite for all positive definite $A \in M_n(\mathbb{F})$.

- NEW The theory of positive definiteness is still in its infancy. There are a lot of opportunities to develop the theory and find applications (algebra? combinatorics? cryptography? total positivity/ finite Grassmannian (Machacek, 2024)).

Given a function $f : \mathbb{F} \to \mathbb{F}$ and a matrix $A = (a_{ij}) \in M_n(\mathbb{F})$, let

$$f[A] := (f(a_{ij})).$$

- We say f *preserves positivity* on $M_n(\mathbb{F})$ if $f[A]$ is positive definite for all positive definite $A \in M_n(\mathbb{F})$.
- **(Entrywise) Positivity Preserver Problems:**
  1. Determine the functions preserving positivity on $M_n(\mathbb{F})$ for a fixed dimension n (usually very hard).

Non-linear entrywise transformers

- The theory of positive definiteness is still in its infancy. There are a lot of opportunities to develop the theory and find applications (algebra? combinatorics? cryptography? total positivity/ finite Grassmannian (Machacek, 2024)).

Given a function $f : \mathbb{F} \to \mathbb{F}$ and a matrix $A = (a_{ij}) \in M_n(\mathbb{F})$, let

$$f[A] := (f(a_{ij})).$$

- We say f *preserves positivity* on $M_n(\mathbb{F})$ if $f[A]$ is positive definite for all positive definite $A \in M_n(\mathbb{F})$.
- **(Entrywise) Positivity Preserver Problems:**
  1. Determine the functions preserving positivity on $M_n(\mathbb{F})$ for a fixed dimension n (usually very hard).
  2. Determine the functions preserving positivity on $M_n(\mathbb{F})$ for **all** $n \geq 1$.

- The $\mathbb{F} = \mathbb{R}$ case was first considered by Pólya-Szegö (1925), and resolved by Schoenberg (1942) and Rudin (1959).

- The $\mathbb{F} = \mathbb{R}$ case was first considered by Pólya-Szegö (1925), and resolved by Schoenberg (1942) and Rudin (1959).

Theorem (Schoenberg, 1942; Rudin, 1959)

Let $f : \mathbb{R} \to \mathbb{R}$. The following are equivalent:

1. *The function f acts entrywise to preserve the set of positive* **definite** *matrices of all dimensions with entries in I.*

- The $\mathbb{F} = \mathbb{R}$ case was first considered by Pólya-Szegö (1925), and resolved by Schoenberg (1942) and Rudin (1959).

Theorem (Schoenberg, 1942; Rudin, 1959)

Let $f : \mathbb{R} \to \mathbb{R}$. The following are equivalent:

1. *The function f acts entrywise to preserve the set of positive* **definite** *matrices of all dimensions with entries in I.*
2. *The function f is* **non-constant** *and absolutely monotone, that is, $f(x) = \sum_{n=0}^{\infty} c_n x^n$ for all $x \in I$ with $c_n \geq 0$ for all n and $c_n > 0$ for at least one $n \geq 1$.*

Schoenberg's theorem

- The $\mathbb{F} = \mathbb{R}$ case was first considered by Pólya-Szegö (1925), and resolved by Schoenberg (1942) and Rudin (1959).

Theorem (Schoenberg, 1942; Rudin, 1959)

Let $f : \mathbb{R} \to \mathbb{R}$. The following are equivalent:

1. *The function f acts entrywise to preserve the set of positive* **definite** *matrices of all dimensions with entries in I.*
2. *The function f is* **non-constant** *and absolutely monotone, that is, $f(x) = \sum_{n=0}^{\infty} c_n x^n$ for all $x \in I$ with $c_n \geq 0$ for all n and $c_n > 0$ for at least one $n \geq 1$.*

Lots of variants considered (for matrices in $M_n(\mathbb{R})$ or $M_n(\mathbb{C})$).

Schoenberg's theorem

- The $\mathbb{F} = \mathbb{R}$ case was first considered by Pólya-Szegö (1925), and resolved by Schoenberg (1942) and Rudin (1959).

Theorem (Schoenberg, 1942; Rudin, 1959)

Let $f : \mathbb{R} \to \mathbb{R}$. The following are equivalent:

1. *The function f acts entrywise to preserve the set of positive* **definite** *matrices of all dimensions with entries in I.*
2. *The function f is* **non-constant** *and absolutely monotone, that is, $f(x) = \sum_{n=0}^{\infty} c_n x^n$ for all $x \in I$ with $c_n \geq 0$ for all n and $c_n > 0$ for at least one $n \geq 1$.*

Lots of variants considered (for matrices in $M_n(\mathbb{R})$ or $M_n(\mathbb{C})$).
For more details, see e.g.:

- A. Belton et al, *A panorama of positivity. I, II.*, 2019, 2020.
- A. Khare, *Matrix analysis and entrywise positivity preservers*, London Math Society Lecture Notes Series, 2022.

Other preserver problems over finite fields

Other settings:

- A lot of work has been done to characterize transformations that preserve various matrix quantities.
- The focus is usually on **linear** maps (linear preserver problems).

Other preserver problems over finite fields

Other settings:

- A lot of work has been done to characterize transformations that preserve various matrix quantities.
- The focus is usually on **linear** maps (linear preserver problems).

Typical result:

Theorem (Dieudonné, 1949)

Let $\phi : M_n(\mathbb{F}) \to M_n(\mathbb{F})$ be an invertible linear map over a field $\mathbb{F}$. Suppose ϕ maps the set of singular matrices into itself. Then

Other preserver problems over finite fields

Other settings:

- A lot of work has been done to characterize transformations that preserve various matrix quantities.
- The focus is usually on **linear** maps (linear preserver problems).

Typical result:

Theorem (Dieudonné, 1949)

Let $\phi : M_n(\mathbb{F}) \to M_n(\mathbb{F})$ be an invertible linear map over a field $\mathbb{F}$. Suppose ϕ maps the set of singular matrices into itself. Then

$$\phi(A) = MAN \quad or \quad \phi(A) = MA^T N$$

for some $M, N \in M_n(\mathbb{F})$ with $\det(MN) \neq 0$.

See e.g. Marko Orel, "Preserver problems over finite fields" for more details.

What about entrywise positivity preservers for finite fields?

What about entrywise positivity preservers for finite fields?

- A bijective function $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ is called field automorphism if for all $x, y \in \mathbb{F}_q$

$$\sigma(x+y) = \sigma(x) + \sigma(y)$$
$$\sigma(xy) = \sigma(x)\sigma(y)$$

What about entrywise positivity preservers for finite fields?

- A bijective function $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ is called field automorphism if for all $x, y \in \mathbb{F}_q$

$$\sigma(x+y) = \sigma(x) + \sigma(y)$$
$$\sigma(xy) = \sigma(x)\sigma(y)$$

- Let $q = p^k$. Then the distinct automorphisms of $\mathbb{F}_q$ are exactly the mappings $\sigma_0, \sigma_1, \ldots, \sigma_{k-1}$ defined by $\sigma_\ell(x) = x^{p^\ell}$.

What about entrywise positivity preservers for finite fields?

- A bijective function $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ is called field automorphism if for all $x, y \in \mathbb{F}_q$

$$\sigma(x+y) = \sigma(x) + \sigma(y)$$
$$\sigma(xy) = \sigma(x)\sigma(y)$$

- Let $q = p^k$. Then the distinct automorphisms of $\mathbb{F}_q$ are exactly the mappings $\sigma_0, \sigma_1, \dots, \sigma_{k-1}$ defined by $\sigma_\ell(x) = x^{p^\ell}$.
- In particular, in $\mathbb{F}_q$, we have $(x+y)^p = x^p + y^p$.

Theorem (Guillot, Gupta, Vishwakarma, Yip, 2024)

Let $q = p^k$. Then all the positive multiples of the field automorphisms of $\mathbb{F}_q$ preserve positivity on $M_n(\mathbb{F}_q)$ for all $n \geq 1$.

Theorem (Guillot, Gupta, Vishwakarma, Yip, 2024)

Let $q = p^k$. Then all the positive multiples of the field automorphisms of $\mathbb{F}_q$ preserve positivity on $M_n(\mathbb{F}_q)$ for all $n \geq 1$.

Proof: Let $f(x) = x^{p^\ell}$ and $A = (a_{ij}) \in M_n(\mathbb{F}_q)$.

Theorem (Guillot, Gupta, Vishwakarma, Yip, 2024)

Let $q = p^k$. Then all the positive multiples of the field automorphisms of $\mathbb{F}_q$ preserve positivity on $M_n(\mathbb{F}_q)$ for all $n \geq 1$.

Proof: Let $f(x) = x^{p^\ell}$ and $A = (a_{ij}) \in M_n(\mathbb{F}_q)$.

- We have

$$\begin{aligned}
\det f[A] &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)}^{p^\ell} a_{2,\sigma(2)}^{p^\ell} \cdots a_{n,\sigma(n)}^{p^\ell} \\
&= \left(\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)} \right)^{p^\ell} \\
&= f(\det A).
\end{aligned}$$

Theorem (Guillot, Gupta, Vishwakarma, Yip, 2024)

Let $q = p^k$. Then all the positive multiples of the field automorphisms of $\mathbb{F}_q$ preserve positivity on $M_n(\mathbb{F}_q)$ for all $n \geq 1$.

Proof: Let $f(x) = x^{p^\ell}$ and $A = (a_{ij}) \in M_n(\mathbb{F}_q)$.

- We have

$$\begin{aligned}
\det f[A] &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)}^{p^\ell} a_{2,\sigma(2)}^{p^\ell} \cdots a_{n,\sigma(n)}^{p^\ell} \\
&= \left(\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)} \right)^{p^\ell} \\
&= f(\det A).
\end{aligned}$$

The result follows by applying the above to all leading principal minors of A. $\square$

Paley graphs

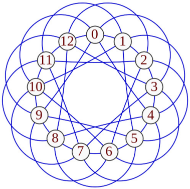
- The *quadratic character* $\eta : \mathbb{F}_q \to \{-1, 0, 1\}$ is:

$$\eta(x) = x^{\frac{q-1}{2}} = \begin{cases} 1 & \text{if } x \in \mathbb{F}_q^+ \\ -1 & \text{if } x \notin \mathbb{F}_q^+ \text{ and } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

- The *quadratic character* $\eta : \mathbb{F}_q \to \{-1, 0, 1\}$ is:

$$\eta(x) = x^{\frac{q-1}{2}} = \begin{cases} 1 & \text{if } x \in \mathbb{F}_q^+ \\ -1 & \text{if } x \notin \mathbb{F}_q^+ \text{ and } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

- Let $q = p^k$ where p is odd. The *Paley graph* $P(q) = (V, E)$ is the graph such that
  1. $V = \mathbb{F}_q$ and
  2. $(a, b) \in E$ if and only if $\eta(a - b) = 1$.



The Paley graph $P(13)$.

Credits: David Eppstein – Wikipedia.

- A function f is an *automorphism of the Paley graph* $P(q)$ if

$$\eta(f(a) - f(b)) = \eta(a - b)$$

for all $a, b \in \mathbb{F}_q$.

- A function f is an *automorphism of the Paley graph* $P(q)$ if

$$\eta(f(a) - f(b)) = \eta(a - b)$$

  for all $a, b \in \mathbb{F}_q$.
- In other words, an automorphism is a bijective map that preserve edges and non-edges.

- A function f is an *automorphism of the Paley graph* $P(q)$ if

$$\eta(f(a) - f(b)) = \eta(a - b)$$

for all $a, b \in \mathbb{F}_q$.

- In other words, an automorphism is a bijective map that preserve edges and non-edges.

Theorem (Carlitz, 1960)

Suppose $q = p^k$ where p is odd. Let $f : \mathbb{F}_q \to \mathbb{F}_q$ such that $f(0) = 0$, $f(1) = 1$ and $\eta(f(a) - f(b)) = \eta(a - b)$ for all $a, b \in \mathbb{F}_q$. Then $f(x) = x^{p^\ell}$ for some $0 \leq \ell \leq k - 1$.

Main result: $n \geq 3$

Theorem (Main Result, Guillot, Gupta, Vishwakarma, Yip, 2024)

Let $q = p^k$ and $f : \mathbb{F}_q \to \mathbb{F}_q$. Then the following are equivalent:

1. *f preserves positivity on $M_n(\mathbb{F}_q)$ for some $n \geq 3$.* Fixed dimension

Main result: $n \geq 3$

Theorem (Main Result, Guillot, Gupta, Vishwakarma, Yip, 2024)

Let $q = p^k$ and $f : \mathbb{F}_q \to \mathbb{F}_q$. Then the following are equivalent:

1. *f preserves positivity on $M_n(\mathbb{F}_q)$ for some $n \geq 3$.* Fixed dimension
2. *f preserves positivity on $M_n(\mathbb{F}_q)$ for all $n \geq 3$.* All dimensions

Main result: $n \geq 3$

Theorem (Main Result, Guillot, Gupta, Vishwakarma, Yip, 2024)

Let $q = p^k$ and $f : \mathbb{F}_q \to \mathbb{F}_q$. Then the following are equivalent:

1. f *preserves positivity on* $M_n(\mathbb{F}_q)$ *for some* $n \geq 3$. *Fixed dimension*
2. f *preserves positivity on* $M_n(\mathbb{F}_q)$ *for all* $n \geq 3$. *All dimensions*
3. $f(x) = cx^{p^\ell}$ *for some* $c \in \mathbb{F}_q^+$ *and* $0 \leq \ell \leq k-1$.

Theorem (Main Result, Guillot, Gupta, Vishwakarma, Yip, 2024)

Let $q = p^k$ *and* $f : \mathbb{F}_q \to \mathbb{F}_q$. *Then the following are equivalent:*

1. f *preserves positivity on* $M_n(\mathbb{F}_q)$ *for some* $n \geq 3$. *Fixed dimension*
2. f *preserves positivity on* $M_n(\mathbb{F}_q)$ *for all* $n \geq 3$. *All dimensions*
3. $f(x) = cx^{p^\ell}$ *for some* $c \in \mathbb{F}_q^+$ *and* $0 \leq \ell \leq k-1$.

Moreover, when p *is odd, the above are equivalent to*

4. $f(0) = 0$ *and* f *is an automorphism of the Paley graph associated to* $\mathbb{F}_q$, *i.e.,* $\eta(f(a) - f(b)) = \eta(a - b)$ *for all* $a, b \in \mathbb{F}_q$.

Main result: $n \geq 3$

Theorem (Main Result, Guillot, Gupta, Vishwakarma, Yip, 2024)

Let $q = p^k$ and $f : \mathbb{F}_q \to \mathbb{F}_q$. Then the following are equivalent:

1. *f preserves positivity on $M_n(\mathbb{F}_q)$ for some $n \geq 3$. Fixed dimension*
2. *f preserves positivity on $M_n(\mathbb{F}_q)$ for all $n \geq 3$. All dimensions*
3. *$f(x) = cx^{p^\ell}$ for some $c \in \mathbb{F}_q^+$ and $0 \leq \ell \leq k-1$.*

Moreover, when p is odd, the above are equivalent to

4. *$f(0) = 0$ and f is an automorphism of the Paley graph associated to $\mathbb{F}_q$, i.e., $\eta(f(a) - f(b)) = \eta(a - b)$ for all $a, b \in \mathbb{F}_q$.*

Our proofs rely on algebraic and combinatorial arguments.

Main result: $n \geq 3$

Theorem (Main Result, Guillot, Gupta, Vishwakarma, Yip, 2024)

Let $q = p^k$ and $f : \mathbb{F}_q \to \mathbb{F}_q$. Then the following are equivalent:

1. *f preserves positivity on $M_n(\mathbb{F}_q)$ for some $n \geq 3$.* *Fixed dimension*
2. *f preserves positivity on $M_n(\mathbb{F}_q)$ for all $n \geq 3$.* *All dimensions*
3. *$f(x) = cx^{p^\ell}$ for some $c \in \mathbb{F}_q^+$ and $0 \leq \ell \leq k-1$.*

Moreover, when p is odd, the above are equivalent to

4. *$f(0) = 0$ and f is an automorphism of the Paley graph associated to $\mathbb{F}_q$, i.e., $\eta(f(a) - f(b)) = \eta(a - b)$ for all $a, b \in \mathbb{F}_q$.*

Our proofs rely on algebraic and combinatorial arguments.
Trichotomy of proofs

- When $p = 2$, $\mathbb{F}_q^+ = \mathbb{F}_q^*$.

Theorem (Main Result, Guillot, Gupta, Vishwakarma, Yip, 2024)

Let $q = p^k$ and $f : \mathbb{F}_q \to \mathbb{F}_q$. Then the following are equivalent:

1. *f preserves positivity on $M_n(\mathbb{F}_q)$ for some $n \geq 3$.* Fixed dimension
2. *f preserves positivity on $M_n(\mathbb{F}_q)$ for all $n \geq 3$.* All dimensions
3. *$f(x) = cx^{p^\ell}$ for some $c \in \mathbb{F}_q^+$ and $0 \leq \ell \leq k-1$.*

Moreover, when p is odd, the above are equivalent to

4. *$f(0) = 0$ and f is an automorphism of the Paley graph associated to $\mathbb{F}_q$, i.e., $\eta(f(a) - f(b)) = \eta(a - b)$ for all $a, b \in \mathbb{F}_q$.*

Our proofs rely on algebraic and combinatorial arguments.
Trichotomy of proofs

- When $p = 2$, $\mathbb{F}_q^+ = \mathbb{F}_q^*$.
- When $q \equiv 1 \pmod 4$, -1 is a square.

Theorem (Main Result, Guillot, Gupta, Vishwakarma, Yip, 2024)

Let $q = p^k$ and $f : \mathbb{F}_q \to \mathbb{F}_q$. Then the following are equivalent:

1. *f preserves positivity on $M_n(\mathbb{F}_q)$ for some $n \geq 3$. Fixed dimension*
2. *f preserves positivity on $M_n(\mathbb{F}_q)$ for all $n \geq 3$. All dimensions*
3. *$f(x) = cx^{p^\ell}$ for some $c \in \mathbb{F}_q^+$ and $0 \leq \ell \leq k-1$.*

Moreover, when p is odd, the above are equivalent to

4. *$f(0) = 0$ and f is an automorphism of the Paley graph associated to $\mathbb{F}_q$, i.e., $\eta(f(a) - f(b)) = \eta(a - b)$ for all $a, b \in \mathbb{F}_q$.*

Our proofs rely on algebraic and combinatorial arguments.
Trichotomy of proofs

- When $p = 2$, $\mathbb{F}_q^+ = \mathbb{F}_q^*$.
- When $q \equiv 1 \pmod 4$, -1 is a square.
- When $q \equiv 3 \pmod 4$, -1 is not a square, $\mathbb{F}_q = \{0\} \sqcup \mathbb{F}_q^+ \sqcup (-\mathbb{F}_q^+)$.

Key ingredient: bijectivity on $\mathbb{F}_q^+$

Lemma

Let $\mathbb{F}_q$ be a finite field with q even or $q \equiv 3 \pmod 4$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$. Suppose f preserves positive definiteness on $M_2(\mathbb{F}_q)$. Then:

1. *The restriction of f to $\mathbb{F}_q^+$ is a bijection of $\mathbb{F}_q^+$ onto itself.*
2. $f(0) = 0$.

Proof.

Key ingredient: bijectivity on $\mathbb{F}_q^+$

Lemma

Let $\mathbb{F}_q$ be a finite field with q even or $q \equiv 3 \pmod 4$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$. Suppose f preserves positive definiteness on $M_2(\mathbb{F}_q)$. Then:

1. *The restriction of f to $\mathbb{F}_q^+$ is a bijection of $\mathbb{F}_q^+$ onto itself.*
2. $f(0) = 0$.

Proof.

1. For $a \in \mathbb{F}_q^+$, $f[aI_2]$ is PD $\implies$

Key ingredient: bijectivity on $\mathbb{F}_q^+$

Lemma

Let $\mathbb{F}_q$ be a finite field with q even or $q \equiv 3 \pmod 4$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$. Suppose f preserves positive definiteness on $M_2(\mathbb{F}_q)$. Then:

1. *The restriction of f to $\mathbb{F}_q^+$ is a bijection of $\mathbb{F}_q^+$ onto itself.*
2. $f(0) = 0$.

Proof.

1. For $a \in \mathbb{F}_q^+$, $f[aI_2]$ is PD $\implies f(a) \in \mathbb{F}_q^+$. Thus $f(\mathbb{F}_q^+) \subseteq \mathbb{F}_q^+$.

Key ingredient: bijectivity on $\mathbb{F}_q^+$

Lemma

Let $\mathbb{F}_q$ be a finite field with q even or $q \equiv 3 \pmod 4$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$. Suppose f preserves positive definiteness on $M_2(\mathbb{F}_q)$. Then:

1. *The restriction of f to $\mathbb{F}_q^+$ is a bijection of $\mathbb{F}_q^+$ onto itself.*
2. $f(0) = 0$.

Proof.

1. For $a \in \mathbb{F}_q^+$, $f[aI_2]$ is PD $\implies$ $f(a) \in \mathbb{F}_q^+$. Thus $f(\mathbb{F}_q^+) \subseteq \mathbb{F}_q^+$.
2. Let $a, b \in \mathbb{F}_q^+$ with $a \neq b$. WLOG $a - b \in \mathbb{F}_q^+$.

Lemma

Let $\mathbb{F}_q$ be a finite field with q even or $q \equiv 3 \pmod 4$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$. Suppose f preserves positive definiteness on $M_2(\mathbb{F}_q)$. Then:

1. *The restriction of f to $\mathbb{F}_q^+$ is a bijection of $\mathbb{F}_q^+$ onto itself.*
2. $f(0) = 0$.

Proof.

1. For $a \in \mathbb{F}_q^+$, $f[aI_2]$ is PD $\implies f(a) \in \mathbb{F}_q^+$. Thus $f(\mathbb{F}_q^+) \subseteq \mathbb{F}_q^+$.
2. Let $a, b \in \mathbb{F}_q^+$ with $a \neq b$. WLOG $a - b \in \mathbb{F}_q^+$. Consider the PD matrix

$$A = \begin{pmatrix} b & b \\ b & a \end{pmatrix}, \qquad \det A = b(a-b) \in \mathbb{F}_q^+.$$

Key ingredient: bijectivity on $\mathbb{F}_q^+$

Lemma

Let $\mathbb{F}_q$ be a finite field with q even or $q \equiv 3 \pmod 4$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$. Suppose f preserves positive definiteness on $M_2(\mathbb{F}_q)$. Then:

1. *The restriction of f to $\mathbb{F}_q^+$ is a bijection of $\mathbb{F}_q^+$ onto itself.*
2. $f(0) = 0$.

Proof.

1. For $a \in \mathbb{F}_q^+$, $f[aI_2]$ is PD $\implies f(a) \in \mathbb{F}_q^+$. Thus $f(\mathbb{F}_q^+) \subseteq \mathbb{F}_q^+$.
2. Let $a, b \in \mathbb{F}_q^+$ with $a \neq b$. WLOG $a - b \in \mathbb{F}_q^+$. Consider the PD matrix

$$A = \begin{pmatrix} b & b \\ b & a \end{pmatrix}, \qquad \det A = b(a-b) \in \mathbb{F}_q^+.$$

$$\det f[A] = f(b)\,(f(a) - f(b)) \in \mathbb{F}_q^+ \implies f(a) \neq f(b).$$

3. Finally, suppose $f(0) = c \in \mathbb{F}_q^+$. By the above, $f(a) = c$ for some $a \in \mathbb{F}_q^+$.

3. Finally, suppose $f(0) = c \in \mathbb{F}_q^+$. By the above, $f(a) = c$ for some $a \in \mathbb{F}_q^+$. Consider

$$f[aI_2] = \begin{pmatrix} f(a) & f(0) \\ f(0) & f(a) \end{pmatrix} = \begin{pmatrix} c & c \\ c & c \end{pmatrix}$$

which is not PD, a contradiction.

3. Finally, suppose $f(0) = c \in \mathbb{F}_q^+$. By the above, $f(a) = c$ for some $a \in \mathbb{F}_q^+$. Consider

$$f[aI_2] = \begin{pmatrix} f(a) & f(0) \\ f(0) & f(a) \end{pmatrix} = \begin{pmatrix} c & c \\ c & c \end{pmatrix}$$

which is not PD, a contradiction. A similar argument can be used if $f(0) \in -\mathbb{F}_q^+$. Thus $f(0) = 0$. $\square$

Characteristic 2: preservers on $M_2(\mathbb{F}_q)$

- Assume $q = 2^k$ for some $k \geq 1$.
- Since $f(x) = x^2$ is bijective, every $x \in \mathbb{F}_q$ has a unique square root $\sqrt{x}$.
- Well known result: $f(x) = x^n$ is bijective on $\mathbb{F}_q$ iff $\gcd(n, q-1) = 1$.

Characteristic 2: preservers on $M_2(\mathbb{F}_q)$

- Assume $q = 2^k$ for some $k \geq 1$.
- Since $f(x) = x^2$ is bijective, every $x \in \mathbb{F}_q$ has a unique square root $\sqrt{x}$.
- Well known result: $f(x) = x^n$ is bijective on $\mathbb{F}_q$ iff $\gcd(n, q-1) = 1$.

Theorem

Let $q = 2^k$ for some $k \geq 1$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$. Then the following are equivalent:

1. *f preserves positivity on $M_2(\mathbb{F}_q)$.*

- Assume $q = 2^k$ for some $k \geq 1$.
- Since $f(x) = x^2$ is bijective, every $x \in \mathbb{F}_q$ has a unique square root $\sqrt{x}$.
- Well known result: $f(x) = x^n$ is bijective on $\mathbb{F}_q$ iff $\gcd(n, q-1) = 1$.

Theorem

Let $q = 2^k$ for some $k \geq 1$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$. Then the following are equivalent:

1. *f preserves positivity on $M_2(\mathbb{F}_q)$.*
2. *$f(0) = 0$, f is bijective, and $f(\sqrt{xy})^2 = f(x)f(y)$ for all $x, y \in \mathbb{F}_q$.*

Characteristic 2: preservers on $M_2(\mathbb{F}_q)$

- Assume $q = 2^k$ for some $k \geq 1$.
- Since $f(x) = x^2$ is bijective, every $x \in \mathbb{F}_q$ has a unique square root $\sqrt{x}$.
- Well known result: $f(x) = x^n$ is bijective on $\mathbb{F}_q$ iff $\gcd(n, q-1) = 1$.

Theorem

Let $q = 2^k$ for some $k \geq 1$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$. Then the following are equivalent:

1. *f preserves positivity on $M_2(\mathbb{F}_q)$.*
2. *$f(0) = 0$, f is bijective, and $f(\sqrt{xy})^2 = f(x)f(y)$ for all $x, y \in \mathbb{F}_q$.*
3. *There exist $c \in \mathbb{F}_q^*$ and $1 \leq n \leq q-1$ with $\gcd(n, q-1) = 1$ such that $f(x) = cx^n$ for all $x \in \mathbb{F}_q$.*

Idea of proof

$(1) \implies (2)$. For $x, y \neq 0$, consider

$$A(z) = \begin{pmatrix} x & \sqrt{xy}z \\ \sqrt{xy}z & y \end{pmatrix} \qquad (z \in \mathbb{F}_q). \quad \det A(z) = xy(1 - z^2).$$

Idea of proof

$(1) \implies (2)$. For $x, y \neq 0$, consider

$$A(z) = \begin{pmatrix} x & \sqrt{xy}z \\ \sqrt{xy}z & y \end{pmatrix} \qquad (z \in \mathbb{F}_q). \quad \det A(z) = xy(1 - z^2).$$

- We have $\det A(z) = 0 \iff z = 1$.

Idea of proof

$(1) \implies (2)$. For $x, y \neq 0$, consider

$$A(z) = \begin{pmatrix} x & \sqrt{xy}z \\ \sqrt{xy}z & y \end{pmatrix} \qquad (z \in \mathbb{F}_q). \quad \det A(z) = xy(1-z^2).$$

- We have $\det A(z) = 0 \iff z = 1$.
- Thus $z \neq 1 \implies f(x)f(y) \neq f(\sqrt{xy}z)^2$.

Idea of proof

$(1) \implies (2)$. For $x, y \neq 0$, consider

$$A(z) = \begin{pmatrix} x & \sqrt{xy}z \\ \sqrt{xy}z & y \end{pmatrix} \qquad (z \in \mathbb{F}_q). \quad \det A(z) = xy(1-z^2).$$

- We have $\det A(z) = 0 \iff z = 1$.
- Thus $z \neq 1 \implies f(x)f(y) \neq f(\sqrt{xy}z)^2$.
- The map $z \mapsto f(\sqrt{xy}z)^2$ is bijective on $\mathbb{F}_q$ since f is bijective.

Idea of proof

$(1) \implies (2)$. For $x, y \neq 0$, consider

$$A(z) = \begin{pmatrix} x & \sqrt{xy}z \\ \sqrt{xy}z & y \end{pmatrix} \qquad (z \in \mathbb{F}_q). \quad \det A(z) = xy(1 - z^2).$$

- We have $\det A(z) = 0 \iff z = 1$.
- Thus $z \neq 1 \implies f(x)f(y) \neq f(\sqrt{xy}z)^2$.
- The map $z \mapsto f(\sqrt{xy}z)^2$ is bijective on $\mathbb{F}_q$ since f is bijective.
- This forces $f(x)f(y) = f(\sqrt{xy})^2$.

Idea of proof

$(1) \implies (2)$. For $x, y \neq 0$, consider

$$A(z) = \begin{pmatrix} x & \sqrt{xy}z \\ \sqrt{xy}z & y \end{pmatrix} \qquad (z \in \mathbb{F}_q). \quad \det A(z) = xy(1 - z^2).$$

- We have $\det A(z) = 0 \iff z = 1$.
- Thus $z \neq 1 \implies f(x)f(y) \neq f(\sqrt{xy}z)^2$.
- The map $z \mapsto f(\sqrt{xy}z)^2$ is bijective on $\mathbb{F}_q$ since f is bijective.
- This forces $f(x)f(y) = f(\sqrt{xy})^2$.

$(2) \implies (3)$. With some effort, we prove the only polynomials satisfying $f(x)f(y) = f(\sqrt{xy})^2$ are monomials.

Idea of proof

$(1) \implies (2)$. For $x, y \neq 0$, consider

$$A(z) = \begin{pmatrix} x & \sqrt{xy}z \\ \sqrt{xy}z & y \end{pmatrix} \qquad (z \in \mathbb{F}_q). \quad \det A(z) = xy(1-z^2).$$

- We have $\det A(z) = 0 \iff z = 1$.
- Thus $z \neq 1 \implies f(x)f(y) \neq f(\sqrt{xy}z)^2$.
- The map $z \mapsto f(\sqrt{xy}z)^2$ is bijective on $\mathbb{F}_q$ since f is bijective.
- This forces $f(x)f(y) = f(\sqrt{xy})^2$.

$(2) \implies (3)$. With some effort, we prove the only polynomials satisfying $f(x)f(y) = f(\sqrt{xy})^2$ are monomials.

$(3) \implies (1)$. Trivial.

Theorem

Let $q = 2^k$ *and let* $f : \mathbb{F}_q \to \mathbb{F}_q$ *preserve positivity on* $M_3(\mathbb{F}_q)$*. Then* $f(x) = cx^{2^l}$ *for some* $0 \leq l \leq k-1$ *and* $c \in \mathbb{F}_q^+$*.*

Theorem

Let $q = 2^k$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$ preserve positivity on $M_3(\mathbb{F}_q)$. Then $f(x) = cx^{2^l}$ for some $0 \leq l \leq k-1$ and $c \in \mathbb{F}_q^+$.

Proof.

1. By the 2×2 case, $f(x) = cx^n$ and is bijective. WLOG, assume $c = 1$.

Characteristic 2: dimension ≥ 3

Theorem

Let $q = 2^k$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$ preserve positivity on $M_3(\mathbb{F}_q)$. Then $f(x) = cx^{2^l}$ for some $0 \leq l \leq k-1$ and $c \in \mathbb{F}_q^+$.

Proof.

1. By the 2×2 case, $f(x) = cx^n$ and is bijective. WLOG, assume $c = 1$.
2. Consider

$$A(x,y) = \begin{pmatrix} 1 & x & y \\ x & 1 & 0 \\ y & 0 & 1 \end{pmatrix}, \qquad \det A(x,y) = 1 - x^2 - y^2.$$

Theorem

Let $q = 2^k$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$ preserve positivity on $M_3(\mathbb{F}_q)$. Then $f(x) = cx^{2^l}$ for some $0 \leq l \leq k-1$ and $c \in \mathbb{F}_q^+$.

Proof.

1. By the 2×2 case, $f(x) = cx^n$ and is bijective. WLOG, assume $c = 1$.
2. Consider
$$A(x,y) = \begin{pmatrix} 1 & x & y \\ x & 1 & 0 \\ y & 0 & 1 \end{pmatrix}, \qquad \det A(x,y) = 1 - x^2 - y^2.$$
Since f preserves positivity, $A(x,y)$ is PD $\implies$ $f[A(x,y)]$ is PD.

Theorem

Let $q = 2^k$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$ preserve positivity on $M_3(\mathbb{F}_q)$. Then $f(x) = cx^{2^l}$ for some $0 \leq l \leq k-1$ and $c \in \mathbb{F}_q^+$.

Proof.

1. By the 2×2 case, $f(x) = cx^n$ and is bijective. WLOG, assume $c = 1$.
2. Consider

$$A(x,y) = \begin{pmatrix} 1 & x & y \\ x & 1 & 0 \\ y & 0 & 1 \end{pmatrix}, \qquad \det A(x,y) = 1 - x^2 - y^2.$$

Since f preserves positivity, $A(x,y)$ is PD $\implies$ $f[A(x,y)]$ is PD.

Observe:

$$\det A = 0 \iff x^2 + y^2 = (x+y)^2 = 1 \iff x + y = 1$$
$$\det f[A] = 0 \iff x^{2n} + y^{2n} = (x^n + y^n)^2 = 1 \iff x^n + y^n = 1.$$

3. Consider

$$S_1 := \{(x,y) \in \mathbb{F}_q^2 : x + y = 1\}, \qquad S_2 := \{(x,y) \in \mathbb{F}_q^2 : x^n + y^n = 1\}.$$

3. Consider

$$S_1 := \{(x,y) \in \mathbb{F}_q^2 : x + y = 1\}, \qquad S_2 := \{(x,y) \in \mathbb{F}_q^2 : x^n + y^n = 1\}.$$

Clearly $|S_1| = q$.

3. Consider

$$S_1 := \{(x,y) \in \mathbb{F}_q^2 : x + y = 1\}, \qquad S_2 := \{(x,y) \in \mathbb{F}_q^2 : x^n + y^n = 1\}.$$

Clearly $|S_1| = q$. Also, $|S_2| = q$ since we know $f(x) = x^n$ is bijective.

3. Consider

$$S_1 := \{(x,y) \in \mathbb{F}_q^2 : x+y=1\}, \qquad S_2 := \{(x,y) \in \mathbb{F}_q^2 : x^n+y^n=1\}.$$

Clearly $|S_1| = q$. Also, $|S_2| = q$ since we know $f(x) = x^n$ is bijective.

4. Claim: if f preserves positivity, we have $S_2 \subseteq S_1$.

3. Consider

$$S_1 := \{(x,y) \in \mathbb{F}_q^2 : x + y = 1\}, \qquad S_2 := \{(x,y) \in \mathbb{F}_q^2 : x^n + y^n = 1\}.$$

Clearly $|S_1| = q$. Also, $|S_2| = q$ since we know $f(x) = x^n$ is bijective.

4. Claim: if f preserves positivity, we have $S_2 \subseteq S_1$.

$$\begin{aligned}(x,y) \in S_2 &\implies \det f[A(x,y)] = 0 \implies A(x,y) \text{ is not PD} \\ &\implies x = 1 \text{ or } \det A(x,y) = 0 \\ &\implies x + y = 1 \\ &\implies (x,y) \in S_1.\end{aligned}$$

3. Consider

$$S_1 := \{(x,y) \in \mathbb{F}_q^2 : x + y = 1\}, \qquad S_2 := \{(x,y) \in \mathbb{F}_q^2 : x^n + y^n = 1\}.$$

Clearly $|S_1| = q$. Also, $|S_2| = q$ since we know $f(x) = x^n$ is bijective.

4. Claim: if f preserves positivity, we have $S_2 \subseteq S_1$.

$$\begin{aligned}
(x,y) \in S_2 &\implies \det f[A(x,y)] = 0 \implies A(x,y) \text{ is not PD} \\
&\implies x = 1 \text{ or } \det A(x,y) = 0 \\
&\implies x + y = 1 \\
&\implies (x,y) \in S_1.
\end{aligned}$$

5. We conclude that $S_1 = S_2$. That means $x + y = 1 \iff x^n + y^n = 1$.

3. Consider

$$S_1 := \{(x,y) \in \mathbb{F}_q^2 : x+y=1\}, \qquad S_2 := \{(x,y) \in \mathbb{F}_q^2 : x^n+y^n=1\}.$$

   Clearly $|S_1| = q$. Also, $|S_2| = q$ since we know $f(x) = x^n$ is bijective.

4. Claim: if f preserves positivity, we have $S_2 \subseteq S_1$.

$$\begin{aligned}(x,y) \in S_2 &\implies \det f[A(x,y)] = 0 \implies A(x,y) \text{ is not PD} \\ &\implies x = 1 \text{ or } \det A(x,y) = 0 \\ &\implies x+y = 1 \\ &\implies (x,y) \in S_1.\end{aligned}$$

5. We conclude that $S_1 = S_2$. That means $x+y=1 \iff x^n+y^n=1$.
6. Not hard to show that this implies $(x+y)^n = x^n + y^n$:

3. Consider

$$S_1 := \{(x,y) \in \mathbb{F}_q^2 : x+y=1\}, \qquad S_2 := \{(x,y) \in \mathbb{F}_q^2 : x^n + y^n = 1\}.$$

Clearly $|S_1| = q$. Also, $|S_2| = q$ since we know $f(x) = x^n$ is bijective.

4. Claim: if f preserves positivity, we have $S_2 \subseteq S_1$.

$$\begin{aligned}(x,y) \in S_2 &\implies \det f[A(x,y)] = 0 \implies A(x,y) \text{ is not PD} \\ &\implies x = 1 \text{ or } \det A(x,y) = 0 \\ &\implies x + y = 1 \\ &\implies (x,y) \in S_1.\end{aligned}$$

5. We conclude that $S_1 = S_2$. That means $x + y = 1 \iff x^n + y^n = 1$.
6. Not hard to show that this implies $(x+y)^n = x^n + y^n$:

$$\begin{aligned}x + y = a \implies \frac{x}{a} + \frac{y}{a} = 1 &\implies \left(\frac{x}{a}\right)^n + \left(\frac{y}{a}\right)^n = 1 \\ &\implies x^n + y^n = a^n = (x+y)^n.\end{aligned}$$

3. Consider

$$S_1 := \{(x,y) \in \mathbb{F}_q^2 : x+y=1\}, \qquad S_2 := \{(x,y) \in \mathbb{F}_q^2 : x^n+y^n=1\}.$$

Clearly $|S_1| = q$. Also, $|S_2| = q$ since we know $f(x) = x^n$ is bijective.

4. Claim: if f preserves positivity, we have $S_2 \subseteq S_1$.

$$\begin{aligned}(x,y) \in S_2 &\implies \det f[A(x,y)] = 0 \implies A(x,y) \text{ is not PD} \\ &\implies x = 1 \text{ or } \det A(x,y) = 0 \\ &\implies x + y = 1 \\ &\implies (x,y) \in S_1.\end{aligned}$$

5. We conclude that $S_1 = S_2$. That means $x + y = 1 \iff x^n + y^n = 1$.

6. Not hard to show that this implies $(x+y)^n = x^n + y^n$:

$$\begin{aligned}x + y = a \implies \frac{x}{a} + \frac{y}{a} = 1 &\implies \left(\frac{x}{a}\right)^n + \left(\frac{y}{a}\right)^n = 1 \\ &\implies x^n + y^n = a^n = (x+y)^n.\end{aligned}$$

7. Thus $x \mapsto x^n$ is a field automorphism and so $n = 2^l$ for some $0 \leq l \leq k-1$. $\square$

Theorem (Main Result, Guillot, Gupta, Vishwakarma, Yip, 2024)

Let $q = p^k$ and $f : \mathbb{F}_q \to \mathbb{F}_q$. Then the following are equivalent:

1. *f preserves positivity on $M_n(\mathbb{F}_q)$ for some $n \geq 3$.*
2. *f preserves positivity on $M_n(\mathbb{F}_q)$ for all $n \geq 3$.*
3. *$f(x) = cx^{p^\ell}$ for some $c \in \mathbb{F}_q^+$ and $0 \leq \ell \leq k-1$.*

Moreover, when p is odd, the above are equivalent to

4. *$f(0) = 0$ and f is an automorphism of the Paley graph associated to $\mathbb{F}_q$, i.e., $\eta(f(a) - f(b)) = \eta(a-b)$ for all $a, b \in \mathbb{F}_q$.*

- The key idea for resolving the $p \neq 2$ cases is to show that the positivity preservers are automorphisms of the associated Paley graph, i.e.,

$$\eta(f(a) - f(b)) = \eta(a-b) \text{ for all } a, b \in \mathbb{F}_q.$$

Proof of $(1) \implies (3)$ when $q \equiv 3 \pmod 4$

Assume $q \equiv 3 \pmod 4$. We already know $f(0) = 0$ and f is bijective on $\mathbb{F}_q^+$.

Proof of $(1) \implies (3)$ when $q \equiv 3 \pmod 4$

Assume $q \equiv 3 \pmod 4$. We already know $f(0) = 0$ and f is bijective on $\mathbb{F}_q^+$. If $\eta(a-b) = 0$, then we are done.

Assume $q \equiv 3 \pmod 4$. We already know $f(0) = 0$ and f is bijective on $\mathbb{F}_q^+$. If $\eta(a-b) = 0$, then we are done. Let us assume that $\eta(a-b) = 1$ and consider the following three cases.

Proof of $(1) \implies (3)$ when $q \equiv 3 \pmod 4$

Assume $q \equiv 3 \pmod 4$. We already know $f(0) = 0$ and f is bijective on $\mathbb{F}_q^+$. If $\eta(a-b) = 0$, then we are done. Let us assume that $\eta(a-b) = 1$ and consider the following three cases.

Case 1 Assume $b = 0$.

Proof of $(1) \implies (3)$ when $q \equiv 3 \pmod 4$

Assume $q \equiv 3 \pmod 4$. We already know $f(0) = 0$ and f is bijective on $\mathbb{F}_q^+$. If $\eta(a-b) = 0$, then we are done. Let us assume that $\eta(a-b) = 1$ and consider the following three cases.

Case 1 Assume $b = 0$. Since $f(\mathbb{F}_q^+) = \mathbb{F}_q^+$,

$$\eta(a-b) = \eta(a) = 1 \implies \eta(f(a)) = 1 = \eta(f(a) - f(0)).$$

Proof of $(1) \implies (3)$ when $q \equiv 3 \pmod 4$

Assume $q \equiv 3 \pmod 4$. We already know $f(0) = 0$ and f is bijective on $\mathbb{F}_q^+$. If $\eta(a-b) = 0$, then we are done. Let us assume that $\eta(a-b) = 1$ and consider the following three cases.

Case 1 Assume $b = 0$. Since $f(\mathbb{F}_q^+) = \mathbb{F}_q^+$,

$$\eta(a-b) = \eta(a) = 1 \implies \eta(f(a)) = 1 = \eta(f(a) - f(0)).$$

Case 2 Assume $\eta(b) = 1$. Then the matrix

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

is positive definite.

Proof of $(1) \implies (3)$ when $q \equiv 3 \pmod 4$

Assume $q \equiv 3 \pmod 4$. We already know $f(0) = 0$ and f is bijective on $\mathbb{F}_q^+$. If $\eta(a-b) = 0$, then we are done. Let us assume that $\eta(a-b) = 1$ and consider the following three cases.

Case 1 Assume $b = 0$. Since $f(\mathbb{F}_q^+) = \mathbb{F}_q^+$,

$$\eta(a-b) = \eta(a) = 1 \implies \eta(f(a)) = 1 = \eta(f(a) - f(0)).$$

Case 2 Assume $\eta(b) = 1$. Then the matrix

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

is positive definite. Hence,

$$\det f[A] = f(b)(f(a) - f(b)) \in \mathbb{F}_q^+.$$

Thus, $\eta(f(a) - f(b)) = 1$ since $\eta(f(b)) = 1$.

Case 3 Assume $\eta(b) = -1$.

Case 3 Assume $\eta(b) = -1$. Consider the matrix

$$A = A(c) = \begin{pmatrix} c & c & c \\ c & b & b \\ c & b & a \end{pmatrix}, \qquad \det A = c(b-c)(a-b)$$

where $c \in \mathbb{F}_q^+$ and $\eta(b-c) = 1$.

Case 3 Assume $\eta(b) = -1$. Consider the matrix

$$A = A(c) = \begin{pmatrix} c & c & c \\ c & b & b \\ c & b & a \end{pmatrix}, \qquad \det A = c(b-c)(a-b)$$

where $c \in \mathbb{F}_q^+$ and $\eta(b-c) = 1$. Consider the linear map $g : \mathbb{F}_q \to \mathbb{F}_q$ given by $g(x) = x + b$.

Case 3 Assume $\eta(b) = -1$. Consider the matrix

$$A = A(c) = \begin{pmatrix} c & c & c \\ c & b & b \\ c & b & a \end{pmatrix}, \qquad \det A = c(b-c)(a-b)$$

where $c \in \mathbb{F}_q^+$ and $\eta(b-c) = 1$. Consider the linear map $g : \mathbb{F}_q \to \mathbb{F}_q$ given by $g(x) = x + b$. We have

- g is bijective,
- $g(0) = b$, and
- $g(-b) = 0$.

Case 3 Assume $\eta(b) = -1$. Consider the matrix

$$A = A(c) = \begin{pmatrix} c & c & c \\ c & b & b \\ c & b & a \end{pmatrix}, \qquad \det A = c(b-c)(a-b)$$

where $c \in \mathbb{F}_q^+$ and $\eta(b-c) = 1$. Consider the linear map $g : \mathbb{F}_q \to \mathbb{F}_q$ given by $g(x) = x + b$. We have

- g is bijective,
- $g(0) = b$, and
- $g(-b) = 0$.

Thus, there must exist $x_0 \in \mathbb{F}_q$ such that $\eta(x_0) = -1$ and $\eta(g(x_0)) = 1$.

Case 3 Assume $\eta(b) = -1$. Consider the matrix

$$A = A(c) = \begin{pmatrix} c & c & c \\ c & b & b \\ c & b & a \end{pmatrix}, \qquad \det A = c(b-c)(a-b)$$

where $c \in \mathbb{F}_q^+$ and $\eta(b-c) = 1$. Consider the linear map $g : \mathbb{F}_q \to \mathbb{F}_q$ given by $g(x) = x + b$. We have

- g is bijective,
- $g(0) = b$, and
- $g(-b) = 0$.

Thus, there must exist $x_0 \in \mathbb{F}_q$ such that $\eta(x_0) = -1$ and $\eta(g(x_0)) = 1$.
Let $x_0 = -c$ where $\eta(c) = 1$, and hence $\eta(b-c) = 1$.

Case 3 Assume $\eta(b) = -1$. Consider the matrix

$$A = A(c) = \begin{pmatrix} c & c & c \\ c & b & b \\ c & b & a \end{pmatrix}, \qquad \det A = c(b-c)(a-b)$$

where $c \in \mathbb{F}_q^+$ and $\eta(b-c) = 1$. Consider the linear map $g : \mathbb{F}_q \to \mathbb{F}_q$ given by $g(x) = x + b$. We have

- g is bijective,
- $g(0) = b$, and
- $g(-b) = 0$.

Thus, there must exist $x_0 \in \mathbb{F}_q$ such that $\eta(x_0) = -1$ and $\eta(g(x_0)) = 1$.

Let $x_0 = -c$ where $\eta(c) = 1$, and hence $\eta(b-c) = 1$. Thus, the matrix A is positive definite.

Case 3 Assume $\eta(b) = -1$. Consider the matrix

$$A = A(c) = \begin{pmatrix} c & c & c \\ c & b & b \\ c & b & a \end{pmatrix}, \qquad \det A = c(b-c)(a-b)$$

where $c \in \mathbb{F}_q^+$ and $\eta(b-c) = 1$. Consider the linear map $g : \mathbb{F}_q \to \mathbb{F}_q$ given by $g(x) = x + b$. We have

- g is bijective,
- $g(0) = b$, and
- $g(-b) = 0$.

Thus, there must exist $x_0 \in \mathbb{F}_q$ such that $\eta(x_0) = -1$ and $\eta(g(x_0)) = 1$.

Let $x_0 = -c$ where $\eta(c) = 1$, and hence $\eta(b-c) = 1$. Thus, the matrix A is positive definite. It follows that

$$\det f[A] = f(c)(f(b) - f(c))(f(a) - f(b)) \in \mathbb{F}_q^+.$$

Case 3 Assume $\eta(b) = -1$. Consider the matrix

$$A = A(c) = \begin{pmatrix} c & c & c \\ c & b & b \\ c & b & a \end{pmatrix}, \qquad \det A = c(b-c)(a-b)$$

where $c \in \mathbb{F}_q^+$ and $\eta(b-c) = 1$. Consider the linear map $g : \mathbb{F}_q \to \mathbb{F}_q$ given by $g(x) = x + b$. We have

- g is bijective,
- $g(0) = b$, and
- $g(-b) = 0$.

Thus, there must exist $x_0 \in \mathbb{F}_q$ such that $\eta(x_0) = -1$ and $\eta(g(x_0)) = 1$.
Let $x_0 = -c$ where $\eta(c) = 1$, and hence $\eta(b-c) = 1$. Thus, the matrix A is positive definite. It follows that

$$\det f[A] = f(c)(f(b) - f(c))(f(a) - f(b)) \in \mathbb{F}_q^+.$$

We know that $\eta(f(c)) = 1$, and using the previous case applied with $a' = b$ and $b' = c$, we conclude that $\eta(f(b) - f(c)) = 1$. Thus, $\eta(f(a) - f(b)) = 1$.

Finally, if $\eta(a-b) = -1$, then $\eta(b-a) = 1$. Hence, by the above argument $\eta(f(b) - f(a)) = 1$. That implies $\eta(f(a) - f(b)) = -1$. Thus, $(1) \implies (3)$ and the result follows.

For 2×2 matrices...

- When $p = 2$, we saw that the preservers are $f(x) = cx^n$ for some $c \in \mathbb{F}_q^*$ and n such that $\gcd(n, q-1) = 1$. (Bijective power functions.)

For 2×2 matrices...

- When $p = 2$, we saw that the preservers are $f(x) = cx^n$ for some $c \in \mathbb{F}_q^*$ and n such that $\gcd(n, q-1) = 1$. (Bijective power functions.)
- When $q \equiv 3 \pmod 4$, all positivity preservers are $f(x) = cx^{p^\ell}$ for some $c \in \mathbb{F}_q^+$ and $0 \leq \ell \leq k-1$. Proof is much more complicated for $M_2(\mathbb{F}_q)$!

For 2×2 matrices...

- When $p = 2$, we saw that the preservers are $f(x) = cx^n$ for some $c \in \mathbb{F}_q^*$ and n such that $\gcd(n, q-1) = 1$. (Bijective power functions.)
- When $q \equiv 3 \pmod 4$, all positivity preservers are $f(x) = cx^{p^\ell}$ for some $c \in \mathbb{F}_q^+$ and $0 \leq \ell \leq k-1$. Proof is much more complicated for $M_2(\mathbb{F}_q)$!
- When $q \equiv 1 \pmod 4$, we resolved the case $q = r^2$. Otherwise, this is an open problem.

Proposition

Let $q = p^k$ be a prime power with $q \equiv 1 \pmod 4$ and let f be a positivity preserver over $M_2(\mathbb{F}_q)$ with $f(1) = 1$. **Assume additionally that f is injective on $\mathbb{F}_q^+$.** *Then there exists $0 \leq l \leq k-1$ such that $f(x) = x^{p^l}$ for all $x \in \mathbb{F}_q$.*

The proof relies on the following result of Muzychuk and Kovács.

General approach when $q \equiv 1 \pmod 4$

Proposition

Let $q = p^k$ be a prime power with $q \equiv 1 \pmod 4$ and let f be a positivity preserver over $M_2(\mathbb{F}_q)$ with $f(1) = 1$. **Assume additionally that f is injective on $\mathbb{F}_q^+$.** *Then there exists $0 \leq l \leq k-1$ such that $f(x) = x^{p^l}$ for all $x \in \mathbb{F}_q$.*

The proof relies on the following result of Muzychuk and Kovács.

Theorem (Muzychuk and Kovács, 2005)

Let p be a prime and $q = p^k \equiv 1 \pmod 4$. The automorphisms of the subgraph of $P(q)$ induced by $\mathbb{F}_q^+$ are precisely given by the maps $x \mapsto ax^{\pm p^l}$, where $a \in \mathbb{F}_q^+$ and $l \in \{0, 1, \ldots, k-1\}$.

General approach when $q \equiv 1 \pmod 4$

Proposition

Let $q = p^k$ be a prime power with $q \equiv 1 \pmod 4$ and let f be a positivity preserver over $M_2(\mathbb{F}_q)$ with $f(1) = 1$. **Assume additionally that f is injective on $\mathbb{F}_q^+$.** *Then there exists $0 \leq l \leq k-1$ such that $f(x) = x^{p^l}$ for all $x \in \mathbb{F}_q$.*

The proof relies on the following result of Muzychuk and Kovács.

Theorem (Muzychuk and Kovács, 2005)

Let p be a prime and $q = p^k \equiv 1 \pmod 4$. The automorphisms of the subgraph of $P(q)$ induced by $\mathbb{F}_q^+$ are precisely given by the maps $x \mapsto ax^{\pm p^l}$, where $a \in \mathbb{F}_q^+$ and $l \in \{0, 1, \dots, k-1\}$.

- We show that a positivity preserver on $M_2(\mathbb{F}_q)$ that is injective on $\mathbb{F}_q^+$ is an automorphism of the above subgraph of $P(q)$. Thus $ax^{\pm p^l}$.

General approach when $q \equiv 1 \pmod 4$

Proposition

Let $q = p^k$ be a prime power with $q \equiv 1 \pmod 4$ and let f be a positivity preserver over $M_2(\mathbb{F}_q)$ with $f(1) = 1$. **Assume additionally that f is injective on $\mathbb{F}_q^+$.** *Then there exists $0 \leq l \leq k-1$ such that $f(x) = x^{p^l}$ for all $x \in \mathbb{F}_q$.*

The proof relies on the following result of Muzychuk and Kovács.

Theorem (Muzychuk and Kovács, 2005)

Let p be a prime and $q = p^k \equiv 1 \pmod 4$. The automorphisms of the subgraph of $P(q)$ induced by $\mathbb{F}_q^+$ are precisely given by the maps $x \mapsto ax^{\pm p^l}$, where $a \in \mathbb{F}_q^+$ and $l \in \{0, 1, \dots, k-1\}$.

- We show that a positivity preserver on $M_2(\mathbb{F}_q)$ that is injective on $\mathbb{F}_q^+$ is an automorphism of the above subgraph of $P(q)$. Thus $ax^{\pm p^l}$.
- With (quite a bit of) extra work, we rule out the ax^{-p^l} case.

When $q \equiv 1 \pmod 4$,

- Not hard to show that a preserver on $M_n(\mathbb{F}_q)$ is injective on $\mathbb{F}_q^+$ if $n \geq 3$.
- This implies our main result.

When $q \equiv 1 \pmod 4$,

- Not hard to show that a preserver on $M_n(\mathbb{F}_q)$ is injective on $\mathbb{F}_q^+$ if $n \geq 3$.
- This implies our main result.
- In general, we were not able to show that a positivity preserver on $M_2(\mathbb{F}_q)$ needs to be injective on $\mathbb{F}_q^+$.

When $q \equiv 1 \pmod 4$,

- Not hard to show that a preserver on $M_n(\mathbb{F}_q)$ is injective on $\mathbb{F}_q^+$ if $n \geq 3$.
- This implies our main result.
- In general, we were not able to show that a positivity preserver on $M_2(\mathbb{F}_q)$ needs to be injective on $\mathbb{F}_q^+$.
- When $q = r^2$, we can exploit extra structure of $P(q)$ to show a preserver on $M_2(\mathbb{F}_q)$ is injective on $\mathbb{F}_q^+$.

When $q \equiv 1 \pmod 4$,

- Not hard to show that a preserver on $M_n(\mathbb{F}_q)$ is injective on $\mathbb{F}_q^+$ if $n \geq 3$.
- This implies our main result.
- In general, we were not able to show that a positivity preserver on $M_2(\mathbb{F}_q)$ needs to be injective on $\mathbb{F}_q^+$.
- When $q = r^2$, we can exploit extra structure of $P(q)$ to show a preserver on $M_2(\mathbb{F}_q)$ is injective on $\mathbb{F}_q^+$.

Open problem: If f preserves positivity on $M_2(\mathbb{F}_q)$ where $q \equiv 1 \pmod 4$ is not a square, does f have to be injective on $\mathbb{F}_q^+$?

The $q = r^2$ case

When $q = r^2$, we can exploit known structure of $P(q)$ to determine the positivity preservers on $M_2(\mathbb{F}_q)$.

The $q = r^2$ case

When $q = r^2$, we can exploit known structure of $P(q)$ to determine the positivity preservers on $M_2(\mathbb{F}_q)$.

- Note $\mathbb{F}_r \subset \mathbb{F}_{r^2}^+ \subset \mathbb{F}_{r^2}$.
- The maximal cliques of $P(r^2)$ are known.

The $q = r^2$ case

When $q = r^2$, we can exploit known structure of $P(q)$ to determine the positivity preservers on $M_2(\mathbb{F}_q)$.

- Note $\mathbb{F}_r \subset \mathbb{F}_{r^2}^+ \subset \mathbb{F}_{r^2}$.
- The maximal cliques of $P(r^2)$ are known.

Theorem (Erdős-Ko-Rado for Paley graphs of square order)

In the Paley graph $P(q)$, the clique number of $P(q)$ is r. Moreover, all maximum cliques are of the form $\alpha\mathbb{F}_r + \beta$, where $\alpha \in \mathbb{F}_q^+$ and $\beta \in \mathbb{F}_q$ (squares translates of the subfield $\mathbb{F}_r$).

The $q = r^2$ case

When $q = r^2$, we can exploit known structure of $P(q)$ to determine the positivity preservers on $M_2(\mathbb{F}_q)$.

- Note $\mathbb{F}_r \subset \mathbb{F}_{r^2}^+ \subset \mathbb{F}_{r^2}$.
- The maximal cliques of $P(r^2)$ are known.

Theorem (Erdős-Ko-Rado for Paley graphs of square order)

In the Paley graph $P(q)$, the clique number of $P(q)$ is r. Moreover, all maximum cliques are of the form $\alpha\mathbb{F}_r + \beta$, where $\alpha \in \mathbb{F}_q^+$ and $\beta \in \mathbb{F}_q$ (squares translates of the subfield $\mathbb{F}_r$).

- Note that $\mathbb{F}_q^*/\mathbb{F}_r^*$ is a well-defined group.
- We can thus write $\mathbb{F}_q^* = a_1\mathbb{F}_r^* \sqcup a_2\mathbb{F}_r^* \sqcup \cdots \sqcup a_{r+1}\mathbb{F}_r^*$.

The $q = r^2$ case

When $q = r^2$, we can exploit known structure of $P(q)$ to determine the positivity preservers on $M_2(\mathbb{F}_q)$.

- Note $\mathbb{F}_r \subset \mathbb{F}_{r^2}^+ \subset \mathbb{F}_{r^2}$.
- The maximal cliques of $P(r^2)$ are known.

Theorem (Erdős-Ko-Rado for Paley graphs of square order)

In the Paley graph $P(q)$, the clique number of $P(q)$ is r. Moreover, all maximum cliques are of the form $\alpha\mathbb{F}_r + \beta$, where $\alpha \in \mathbb{F}_q^+$ and $\beta \in \mathbb{F}_q$ (squares translates of the subfield $\mathbb{F}_r$).

- Note that $\mathbb{F}_q^*/\mathbb{F}_r^*$ is a well-defined group.
- We can thus write $\mathbb{F}_q^* = a_1\mathbb{F}_r^* \sqcup a_2\mathbb{F}_r^* \sqcup \cdots \sqcup a_{r+1}\mathbb{F}_r^*$.
- We say that a coset of the form $a\mathbb{F}_q^*$ with $a \in \mathbb{F}_q^+$ is a *square coset*.

Outline of proof for $q = r^2$

Let f be a positivity preserver on $M_2(\mathbb{F}_q)$ where $q = r^2$.

1. The function f maps a square coset to a square coset.

Outline of proof for $q = r^2$

Let f be a positivity preserver on $M_2(\mathbb{F}_q)$ where $q = r^2$.

1. The function f maps a square coset to a square coset.
2. **Action of f on a square coset $\alpha\mathbb{F}_r^*$:** there exist a positive integer $m = m(\alpha)$ such that $\gcd(m, r-1) = 1$ and $f(\alpha x) = \beta x^m$ for all $x \in \mathbb{F}_r$, where $\beta = f(\alpha) \in \mathbb{F}_q^+$.

Outline of proof for $q = r^2$

Let f be a positivity preserver on $M_2(\mathbb{F}_q)$ where $q = r^2$.

1. The function f maps a square coset to a square coset.
2. **Action of f on a square coset $\alpha\mathbb{F}_r^*$:** there exist a positive integer $m = m(\alpha)$ such that $\gcd(m, r-1) = 1$ and $f(\alpha x) = \beta x^m$ for all $x \in \mathbb{F}_r$, where $\beta = f(\alpha) \in \mathbb{F}_q^+$.
3. The function f maps different square cosets to different square cosets. Equivalently, f is injective on $\mathbb{F}_q^+$.

Let f be a positivity preserver on $M_2(\mathbb{F}_q)$ where $q = r^2$.

1. The function f maps a square coset to a square coset.
2. **Action of f on a square coset $\alpha\mathbb{F}_r^*$:** there exist a positive integer $m = m(\alpha)$ such that $\gcd(m, r-1) = 1$ and $f(\alpha x) = \beta x^m$ for all $x \in \mathbb{F}_r$, where $\beta = f(\alpha) \in \mathbb{F}_q^+$.
3. The function f maps different square cosets to different square cosets. Equivalently, f is injective on $\mathbb{F}_q^+$.
4. We conclude $f(x) = ax^{p^j}$ for all $x \in \mathbb{F}_q$.

The above steps are highly non-trivial and exploit the known maximal clique structure of $P(r^2)$.

Ongoing work

Ongoing work:

- Linear positivity preservers.
- k-positive, completely positive linear maps.

Ongoing work:

- Linear positivity preservers.
- k-positive, completely positive linear maps.

Possible research directions:

- New connections to other areas/problems? Applications?
- Applications of positive definite matrices over $\mathbb{F}_q$?

Reference

D. Guillot, H. Gupta, P.K. Vishwakarma, and C.H. Yip. Positivity preservers over finite fields. arXiv:2404.00222 (2024) 32 pages.

Thank you!