Entrywise transforms and positive definite matrices over finite fields

Dominique Guillot [1,3] Himanshu Gupta [2] Prateek Kumar Vishwakarma [3] Chi Hoi Yip [4]

[1]University of Delaware [2]University of Regina [3]Université Laval [4]Georgia Tech

Abstract

We consider a natural notion of positive definiteness for matrices over finite fields and prove an algebraic version of Schoenberg's celebrated theorem [*Duke Math. J.*, 1942] characterizing the functions that preserve positive definiteness when applied entrywise to positive definite matrices. Our proofs build on several novel connections between positivity preservers and field automorphisms via the works of Weil, Carlitz, and Muzychuk–Kovács, and via the Erdős–Ko–Rado theorem for Paley graphs.

Positive definite matrices over finite fields

Recall that any of the following equivalent statements can be used to define the **positive definiteness** of a symmetric matrix $A \in M_n(\mathbb{R})$:

- The quadratic form $x^T Ax > 0$ for all $x \in \mathbb{R} \setminus \{0\}$.
- All the eigenvalues of A are positive.
- There exists a non-singular matrix $B \in M_n(\mathbb{R})$ such that $A = B^2$.
- There exists a full rank matrix $B \in M_{n,m}(\mathbb{R})$ such that $A = BB^T$.
- The matrix A admits a Cholesky factorization $A = LL^T$, where L is lower triangular with positive diagonal entries.
- All the principal minors of A are positive.
- **The leading principal minors of A are positive.**

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

Positive definiteness over finite fields

We say that a symmetric matrix over a finite field $\mathbb{F}_q$ is **positive definite** if all its leading principal minors are non-zero squares in $\mathbb{F}_q$.

We think of

$$\mathbb{F}_q^+ := \{x^2 : x \in \mathbb{F}_q^\times\}$$

as the **positive** elements of $\mathbb{F}_q$. Hence, the definition mimics the approach used for real and complex matrices.

Example: In $\mathbb{F}_7$, we have $\mathbb{F}_7^+ = \{1^2, 2^2, 3^2, 4^2, 5^2, 6^2\} = \{1, 2, 4\}$. Let

$$A = \begin{pmatrix} 4 & 1 \\ 1 & 6 \end{pmatrix} \qquad B = \begin{pmatrix} 4 & 1 \\ 1 & 1 \end{pmatrix}$$

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

Positive definite matrices over $\mathbb{F}_q$ were first studied by Cooper, Hanna, and Whitlatch [3]. The following result shows the quadratic form approach to postive definiteness fails over finite fields.

Proposition 1: (Cooper, Hanna, and Whitlatch (2022))

Let $\mathbb{F}_q$ be a finite field, let $n \geq 3$, and let $A \in M_n(\mathbb{F}_q)$. Suppose $Q(x) := x^T Ax$ for all $x \in \mathbb{F}_q^n$. Then there exists $v \in \mathbb{F}_q^n \setminus \{\mathbf{0}\}$ so that $Q(v) = 0$.

However, the Cholesky factorization approach can be used in some cases.

Theorem 2: (Cooper, Hanna, and Whitlatch (2022))

Let $A \in M_n(\mathbb{F}_q)$ be a symmetric matrix.

1. If A admits a Cholesky decomposition, then all its leading principal minors are positive.
2. If q is even or $q \equiv 3 \pmod 4$ and all the leading principal minors of A are positive, then A admits a Cholesky decomposition.

Entrywise positivity preservers

Given a function $f : \mathbb{F} \to \mathbb{F}$ and a matrix $A = (a_{ij}) \in M_n(\mathbb{F})$, we define an **entrywise map** by:

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

Problem

Which functions have the property that $f[A]$ is positive definite for all A positive definite?

This is a classical problem in analysis, with connections to metric space embeddings, harmonic analysis, covariance estimation, etc. – see [2] for more details.

Dimension-free result over $\mathbb{R}$: Schoenberg's theorem

Schoenberg's theorem (1942) characterizes functions that preserve the positivity of matrices **of all dimensions** $n \geq 1$.

Theorem 3: (Schoenberg (1942))

Let $I = (-\rho, \rho) \subseteq \mathbb{R}$, where $0 < \rho \leq \infty$. Given a function $f : I \to \mathbb{R}$, 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 $n \geq 1$.

Note: $(2) \implies (1)$ is a consequence of the Schur product theorem.

Theorem 4: (Schur (1911))

Let $A = (a_{ij}), B = (b_{ij}) \in M_n(\mathbb{R})$ be positive definite. Then $A \circ B := (a_{ij}b_{ij})$ is positive definite.

Results in fixed dimension over $\mathbb{R}$

For $n = 2$ (Vasudeva, (1979)): A function $f : (0, \infty) \to \mathbb{R}$ preserves positive definiteness on $M_2((0, \infty))$ iff it is positive, increasing, and $f(\sqrt{xy}) \leq \sqrt{f(x)f(y)}$ for all $x, y \in (0, \infty)$.

For polynomials and sums of powers: Partial results by Belton–Guillot–Khare–Putinar (2016) [1] and Khare–Tao (2021) [5].

Main results: Characterizations over $\mathbb{F}_q$

A simple observation provides the first examples of positivity preservers over $\mathbb{F}_q$.

Proposition 5

All the positive multiples of the field automorphisms of $\mathbb{F}_q$ preserve positivity on $M_n(\mathbb{F}_q)$ for all $n \geq 2$.

Proof. Let $f(x) \equiv x^{p^\ell}$ be an automorphism of $\mathbb{F}_q$. The result follows upon observing that, using Laplace expansion, we have

$$\det f[A] = f(\det A)$$

for all $A \in M_n(\mathbb{F}_q)$ and $n \geq 2$.

Theorem 6: Main result 1 – Even characteristic

Let $q = 2^k$ for some positive integer k and let $f : \mathbb{F}_q \to \mathbb{F}_q$. Then

(1) ($n = 2$ case) The following are equivalent:
  1. f preserves positivity on $M_2(\mathbb{F}_q)$.
  2. f is a bijective monomial on $\mathbb{F}_q$, that is, 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 $x \in \mathbb{F}_q$.

(2) ($n \geq 3$ case) 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 $n \geq 2$.
  3. f is a non-zero multiple of a field automorphism of $\mathbb{F}_q$, i.e., there exist $c \in \mathbb{F}_q^*$ and $0 \leq \ell \leq k-1$ such that $f(x) = cx^{2^\ell}$ for all $x \in \mathbb{F}_q$.

Theorem 7: Main result 2 – $q \equiv 3 \pmod 4$

Let $q \equiv 3 \pmod 4$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$. Then the following are equivalent:

(1) f preserves positivity on $M_n(\mathbb{F}_q)$ for some $n \geq 2$.
(2) f preserves positivity on $M_n(\mathbb{F}_q)$ for all $n \geq 2$.
(3) $f(0) = 0$ and $\eta(f(a) - f(b)) = \eta(a - b)$ for all $a, b \in \mathbb{F}_q$.
(4) f is a positive multiple of a field automorphism of $\mathbb{F}_q$, i.e., there exist $c \in \mathbb{F}_q^+$ and $0 \leq \ell \leq k-1$ such that $f(x) = cx^{p^\ell}$ for all $x \in \mathbb{F}_q$.

Theorem 8: Main result 3 – $q \equiv 1 \pmod 4$

Let $q \equiv 1 \pmod 4$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$. Then the following are equivalent:

(1) f preserves positivity on $M_n(\mathbb{F}_q)$ for some $n \geq 3$.
(2) f preservers positivity on $M_n(\mathbb{F}_q)$ for all $n \geq 3$.
(3) $f(0) = 0$ and $\eta(f(a) - f(b)) = \eta(a - b)$ for all $a, b \in \mathbb{F}_q$.
(4) f is a positive multiple of a field automorphism of $\mathbb{F}_q$, i.e., there exist $c \in \mathbb{F}_q^+$ and $0 \leq \ell \leq k-1$ such that $f(x) = cx^{p^\ell}$ for all $x \in \mathbb{F}_q$.

Moreover, when $q = r^2$ for some odd integer r, the above are equivalent to

(1') f preserves positivity on $M_n(\mathbb{F}_q)$ for some $n \geq 2$.

Note: In the above two results, condition (3) is equivalent to
(3') $f(0) = 0$ and f is an automorphism of the Paley (di)graph associated to $\mathbb{F}_q$.

Overview of proof techniques

1. Show positivity preservers have to be automorphisms of the Paley (di)graph $P(q)$. These are known to be of the form $f(x) = cx^{p^j} + d$ (see e.g. Carlitz 1960).
2. Show positivity preservers have to be automorphisms of $\Gamma(q)$, the subgraph of $P(q)$ induced by $\mathbb{F}_q^+$. Use Muzychuk and Kovács' characterization of such automorphisms. They are of the form $x \mapsto cx^{\pm p^j}$.
3. Use combinatorial arguments to obtain properties of f (injectivity, bijectivity, etc.). Show that if f is not bijective, then some matrix has to lose positivity under the action of f.
4. When $q \equiv 1 \pmod 4$ and $q = r^2$, we use the structure of maximum cliques in $P(q)$ (Erdős-Ko-Rado theorem for Paley graphs). All maximum cliques are of the form $\alpha\mathbb{F}_r + \beta$.

Open problem

When $q \equiv 1 \pmod 4$ and $q \neq r^2$, what are the positivity preservers over $M_2(\mathbb{F}_q)$?

Proposition 9: [4, Proposition 5.8]

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 $0 \leq \ell \leq k-1$ such that $f(x) = x^{p^\ell}$ for all $x \in \mathbb{F}_q$.

Question: 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 $\mathbb{F}_q^+$?

Link to full version of paper [4]:

[1] A. Belton, D. Guillot, A. Khare, and M. Putinar. Matrix positivity preservers in fixed dimension. I. *Adv. Math.*, 298:325–368, 2016. ISSN 0001-8708.

[2] A. Belton, D. Guillot, A. Khare, and M. Putinar. A panorama of positivity. *arXiv: 1812.05482*, 2019.

[3] J. Cooper, E. Hanna, and H. Whitlatch. Positive-definite matrices over finite fields. *Rocky Mountain J. Math.*, 54(2):423–438, 2024. ISSN 0035-7596,1945-3795.

[4] D. Guillot, H. Gupta, P. K. Vishwakarma, and C. H. Yip. Positivity preservers over finite fields. *arXiv:2404.00222*, 2024.

[5] A. Khare and T. Tao. On the sign patterns of entrywise positivity preservers in fixed dimension. *Amer. J. Math.*, 143(6):1863–1929, 2021.

dguillot@udel.edu, himanshu.gupta@uregina.ca, prateek-kumar.vishwakarma.1@ulaval.ca, cyip30@gatech.edu