Séminaire Lotharingien de Combinatoire **93B** (2025)
Article #69, 12 pp.

Proceedings of the 37th Conference on Formal Power Series and Algebraic Combinatorics (Sapporo)

Entrywise transforms and positive definite matrices over finite fields

Dominique Guillot*[1], Himanshu Gupta †[2],
Prateek Kumar Vishwakarma ‡[3], and Chi Hoi Yip §[4]

[1]*University of Delaware, DE, USA*
[2]*University of Regina, SK, Canada*
[3]*Université Laval, QC, Canada*
[4]*Georgia Institute of Technology, GA, USA*

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.

Keywords: positive definite matrix, entrywise transform, finite fields, field automorphism, Paley graph

1 Introduction and main results

In this article we examine functions $f : \mathbb{F}_q \to \mathbb{F}_q$ defined on a finite field $\mathbb{F}_q$ that operate on matrices $A := (a_{ij})$ in the entrywise fashion, i.e., $f[A] := (f(a_{ij}))$, and preserve positivity of matrices in $M_n(\mathbb{F}_q)$. The study of such entrywise transforms that preserve various forms of matrix positivity has a rich and long history with important connections and applications in many areas – metric geometry and positive definite functions in early 20th century, analysis in late 20th century, and high-dimensional covariance estimations in 21st century – see the surveys [3, 4] and the monograph [14] for more details. For

*dguillot@udel.edu. D.G. was partially supported by a Simons Foundation collaboration grant for mathematicians and by NSF grant #2350067.

†himanshu.gupta@uregina.ca. H.G. was supported by a Pacific Institute for the Mathematical Sciences (PIMS) fellowship.

‡prateek-kumar.vishwakarma.1@ulaval.ca. P.K.V. is supported by the Centre de recherches mathématiques and Laval (CRM-Laval) Postdoctoral Fellowship. He also acknowledges the Pacific Institute for the Mathematical Sciences (PIMS), a SwarnaJayanti Fellowship from DST and SERB, Govt. of India (PI: Apoorva Khare), the SPARC travel support (Scheme for Promotion of Academic and Research Collaboration, MHRD, Govt. of India; PI: Tirthankar Bhattacharyya), and the University of Plymouth (UK).

§cyip30@gatech.edu. C.H.Y. was partially supported by an NSERC fellowship.

matrices with real entries by the well-known Schur product theorem [22], the entrywise product $A \circ B := (a_{ij}b_{ij})$ of two $n \times n$ positive definite matrices is positive definite. As an immediate consequence of this surprising result, all convergent non-constant power series $f(x) = \sum_{n=0}^{\infty} c_n x^n$ with real nonnegative coefficients $c_n \geq 0$ preserve positive definiteness when applied entrywise to positive definite matrices. An impressive converse of this result was obtained by Schoenberg [21], with various refinements collected over time [20, 5, 14].

Theorem 1.1 ([14, Chapter 18]). *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 $n \geq 1$.*

Given Schoenberg's characterization of "dimension-free" entrywise preservers, it is natural to understand the preservers for each fixed size N. This is a far harder problem: the $N = 1$ case is trivial, and the $N = 2$ case was resolved by Vasudeva [23] in 1979; but the other cases $N > 2$ remain open to date. There has been recent progress wherein either the test matrices or the test functions are refined; one interesting refinement involves classifying the entrywise polynomials preserving positivity on $N \times N$ matrices. Characterizations can be found in the works of Belton–Guillot–Khare–Putinar [2] and Khare–Tao [15, 16], and these involve novel connections to Schur polynomials and symmetric function theory. Several other variants were also previously explored – see e.g. [3, 4] and the references therein. Many other types of preserver problems were also previously considered for matrices over finite fields (see e.g. [12, 17, 19] for more details).

To the authors' knowledge, all previous work on entrywise preservers has focused on matrices with real or complex entries. In this paper, we consider matrices with entries in a finite field and describe the associated entrywise positivity preservers in the harder fixed-dimensional setting. Recall that in the real setting, a symmetric matrix in $M_n(\mathbb{R})$ is positive definite if and only if all its leading principal minors are positive. By analogy, we think of non-zero squares in a finite field $\mathbb{F}_q$ as positive elements in $\mathbb{F}_q$ and say that a symmetric matrix in $M_n(\mathbb{F}_q)$ is positive definite if all its leading principal minors are equal to the square of some non-zero element in $\mathbb{F}_q$. As shown in [9] (which we briefly discuss in Section 2), this leads to a reasonable notion of positive definiteness over finite fields. We therefore adopt the following definition.

Definition 1.2 (Positive definite matrices over $\mathbb{F}_q$). A matrix $A \in M_n(\mathbb{F}_q)$ is *positive definite* if A is symmetric and all its leading principal minors are non-zero squares in $\mathbb{F}_q$.

Our goal is to classify entrywise preservers of positive definite matrices.

Definition 1.3. Given a matrix $A = (a_{ij}) \in M_n(\mathbb{F}_q)$ and a function $f : \mathbb{F}_q \to \mathbb{F}_q$, we denote by $f[A]$ the matrix obtained by applying f to the entries of A:

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

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

Compared to previous work on $\mathbb{R}$ or $\mathbb{C}$ that uses analytic techniques to characterize preservers, the flavor of our work is considerably different and relies mostly on algebraic, combinatorial, and number-theoretic arguments. Surprisingly, our characterizations unearth new connections between functions preserving positivity, field automorphisms, and automorphisms of Paley graphs. For each prime power q, we show that the positivity preservers on $M_n(\mathbb{F}_q)$, for a fixed $n \geq 3$, are precisely positive multiples of field automorphisms of $\mathbb{F}_q$. With a much more delicate analysis, we also give a complete classification of positivity preservers on $M_2(\mathbb{F}_q)$ for all prime powers q other than those with $q \equiv 1 \pmod 4$ that are not a perfect square. When $q = r^2$, we leverage the supplementary structure of $\mathbb{F}_q$ as well as the well-known structure of the maximal cliques of the associated Paley graph $P(q)$ to obtain the classification.

This extended abstract provides an overview of our results and techniques. For more details, we refer the reader to [11].

1.1 Main results

Let p be a prime number and k a positive integer. We denote the finite field with $q = p^k$ elements by $\mathbb{F}_q$. The distinct automorphisms of $\mathbb{F}_q$ are exactly the mapings $\sigma_0, \dots, \sigma_{k-1}$ defined by $\sigma_\ell(x) = x^{p^\ell}$. We let $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$ denote the non-zero elements of the field. We say that an element $x \in \mathbb{F}_q$ is *positive* if $x = y^2$ for some $y \in \mathbb{F}_q^*$. In that case, we say y is a square root of x. We denote the set of positive elements of $\mathbb{F}_q$ by $\mathbb{F}_q^+$, i.e., $\mathbb{F}_q^+ := \{x^2 : x \in \mathbb{F}_q^*\}$. Similarly, we denote the set of *negative* elements of $\mathbb{F}_q$ by $\mathbb{F}_q^- = \mathbb{F}_q^* \setminus \mathbb{F}_q^+$. If q is odd, then $|\mathbb{F}_q^+| = |\mathbb{F}_q^-| = \frac{q-1}{2}$. When q is odd, the *quadratic character* of $\mathbb{F}_q$ is the function $\eta : \mathbb{F}_q \to \{-1, 0, 1\}$ given by:

$$\eta(x) = x^{\frac{q-1}{2}} = \begin{cases} 1 & \text{if } x \in \mathbb{F}_q^+ \\ -1 & \text{if } x \in \mathbb{F}_q^- \\ 0 & \text{if } x = 0. \end{cases} \tag{1.1}$$

Finally, we denote by $M_n(\mathbb{F}_q)$ the set of $n \times n$ matrices with entries in $\mathbb{F}_q$, by I_n the $n \times n$ identity matrix, and by $\mathbf{0}_{m \times n}$ the $m \times n$ matrix whose entries are all 0.

When $n = 1$, the positivity preservers are precisely the functions $f : \mathbb{F}_q \to \mathbb{F}_q$ such that $f(\mathbb{F}_q^+) \subseteq \mathbb{F}_q^+$. Any such map can be explicitly written using an interpolation polynomial. We thus focus on $n \geq 2$. We first obtain a family of well-known maps that naturally preserve positivity of matrices over a finite field.

Proposition 1.4. *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 p be the prime such that $q = p^k$, and let $f(x) \equiv x^{p^\ell}$ be an automorphism of $\mathbb{F}_q$. The result follows from the fact that $\det f[A] = f(\det A)$ for all $A \in M_n(\mathbb{F}_q)$ and $n \geq 2$, which is easy to show by expanding the determinants. $\square$

The main content of this article is to present the converse of Proposition 1.4, along with various algebraic and combinatorial connections. Recall that, in the real or complex case, Schoenberg's theorem (Theorem 1.1) provides such a characterization when the dimension of matrices is unbounded. In sharp contrast, for finite fields, we obtain the precise classification of entrywise positivity preservers in the harder setting where the dimension of the matrices is fixed. In classifying these preservers a natural trichotomy arises. When q is even, every non-zero element of $\mathbb{F}_q$ is a square. Characterizing the entrywise preservers in even characteristic thus reduces to characterizing the entrywise transformations that preserve non-singularity. Our techniques in odd characteristics also differ depending on whether -1 is a square in $\mathbb{F}_q$. As a consequence, our results are organized into three parts: (1) the even characteristic case, (2) the $q \equiv 3 \pmod 4$ case where $-1 \notin \mathbb{F}_q^+$, and (3) the $q \equiv 1 \pmod 4$ case where $-1 \in \mathbb{F}_q^+$. Our first main result addresses the even characteristic case.

Theorem A. *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:

- *(a) f preserves positivity on $M_2(\mathbb{F}_q)$.*
- *(b) 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:

- *(a) f preserves positivity on $M_n(\mathbb{F}_q)$ for some $n \geq 3$.*
- *(b) f preserves positivity on $M_n(\mathbb{F}_q)$ for all $n \geq 2$.*
- *(c) 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 $x \in \mathbb{F}_q$.*

Our second main result addresses the case where $q \equiv 3 \pmod 4$.

Theorem B. *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 $x \in \mathbb{F}_q$.

Finally, our last main result addresses the $q \equiv 1 \pmod 4$ case.

Theorem C. *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 $n \geq 2$.

Recall that each finite field $\mathbb{F}_q$ with q odd has an associated Paley graph $P(q)$ whose vertices are the elements of $\mathbb{F}_q$ and where two vertices $a, b \in \mathbb{F}_q$ have an edge (a, b) if and only if $\eta(a - b) = 1$. The graph is directed when $q \equiv 3 \pmod 4$ and is sometimes called the Paley tournament or the Paley digraph, and is undirected when $q \equiv 1 \pmod 4$. Condition (3) in Theorems B and C can thus be rephrased as

(3′) $f(0) = 0$ and f is an automorphism of the Paley (di)graph $P(q)$.

Paley (di)graphs and their connection with positivity preservers play a crucial role in our proofs. We demonstrate some of these in Section 3, and prove the following corollary.

Corollary 1.5. *For any finite field $\mathbb{F}_q$ and any fixed $n \geq 3$, the positivity preservers on $M_n(\mathbb{F}_q)$ are precisely the positive multiples of the field automorphisms of $\mathbb{F}_q$.*

Our characterizations of the preservers over $M_2(\mathbb{F}_q)$ involve a further delicate analysis involving applications of Weil's character sum bounds, Muzychuk–Kovács' classification of the automorphisms of the subgraph $\Gamma(q)$ of the Paley graph $P(q)$ induced by $\mathbb{F}_q^+$, and the characterization of maximum cliques of Paley graphs of square order.

2 Positive definite matrices over finite fields

For real symmetric or complex Hermitian matrices, it is well-known that there are several equivalent ways to define positive definiteness. To name a few, a Hermitian matrix A is positive definite if and only if any of the following holds: (1) $z^*Az > 0$ for all non-zero $z \in \mathbb{C}^n$; (2) all eigenvalues of A are positive; (3) the sesquilinear form z^*Aw defines an inner product; (4) A is a Gram matrix of linearly independent vectors; (5) all leading principal minors of A are positive; or (6) A has a unique Cholesky decomposition [13, Chapter 7].

As shown by Cooper, Hanna, and Whitlatch [9], the situation is very different for matrices over finite fields. E.g., it is not hard to show that the standard definition of positive definiteness via quadratic forms (as in real/complex cases) does not yield a useful notion over finite fields.

Proposition 2.1 ([9, Proposition 4])**.** *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, when q is even or $q \equiv 3 \pmod 4$, some of the classical real/complex positivity theory can be recovered. Recall that a symmetric matrix $A \in M_n(\mathbb{F}_q)$ is said to have a *Cholesky decomposition* if $A = LL^T$ for some lower triangular matrix $L \in M_n(\mathbb{F}_q)$ with positive elements on its diagonal. When q is even or $q \equiv 3 \pmod 4$, it is known that the positivity of the leading principal minors of a matrix in $M_n(\mathbb{F}_q)$ is equivalent to the existence of a Cholesky decomposition.

Theorem 2.2 ([9, Theorem 16, Corollary 24])**.** *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.*

We note however that the equivalence fails in general when $q \equiv 1 \pmod 4$ [11, Proposition 2.10]. The authors of [9] define a symmetric matrix in $M_n(\mathbb{F}_q)$ to be positive definite if it admits a Cholesky decomposition, when q is even or $q \equiv 3 \pmod 4$. In light of Theorem 2.2, this definition coincides with ours when $q \not\equiv 1 \pmod 4$ (in Definition 1.2 and also with the definition over real/complex fields). We also note, however, that verifying if a matrix admits a Cholesky decomposition is not as straightforward as computing its leading principal minors. This is our motivation for adopting Definition 1.2.

It is well-known that every element in a finite field can be written as a sum of two squares. As a consequence, sums of positive definite matrices are not always positive definite. Similarly, a Gram matrix $A = MM^T$ with $M \in M_{n\times m}(\mathbb{F}_q)$ is not always positive definite (consider, for example, $M = (x_1, x_2) \in \mathbb{F}_q^2$). Many other standard properties of positive definiteness over $\mathbb{R}$ or $\mathbb{C}$ fail for finite fields. For example, a positive definite matrix may not have positive eigenvalues, and the entrywise product of two positive definite matrices is not always positive definite [9, Section 3]. Taking all these into account, the reader who is accustomed to working with positive definite matrices over the real/complex fields must thus take great care when moving to the finite field world. We now discuss selected proofs and ideas.

3 Dimension ≥ 3 : Paley (di)graph and its automorphisms

We adopt the combinatorial viewpoint of identifying the elements of $\mathbb{F}_q$ with the vertices of the Paley (di)graph $P(q)$. Paley (di)graphs have been well-studied in the literature. We recall their definition and some basic properties.

Definition 3.1. If $q \equiv 1 \pmod 4$ is a prime power, the *Paley graph* $P(q)$ is a graph with the elements of $\mathbb{F}_q$ as vertices, in which $\{a, b\}$ is an edge if and only $a - b \in \mathbb{F}_q^+$. Similarly, if $q \equiv 3 \pmod 4$ is a prime power, the *Paley digraph* $P(q)$ is a directed graph with the elements of $\mathbb{F}_q$ as vertices, in which (a, b) is a directed edge if and only $a - b \in \mathbb{F}_q^+$.

Lemma 3.2 ([7, Proposition 9.1.1])**.** *Let $q \equiv 1 \pmod 4$. The Paley graph $P(q)$ is a strongly regular graph with parameters $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$.*

We say that $f : \mathbb{F}_q \to \mathbb{F}_q$ is an automorphism of the Paley (di)graph $P(q)$ if $\eta(f(a) - f(b)) = \eta(a - b)$ for all $a, b \in \mathbb{F}_q$. Recall that a well-known theorem of Carlitz [8] provides the classification of these automorphisms.

Theorem 3.3 ([8])**.** *Let p be an odd prime and $q = p^k$. A function $f : \mathbb{F}_q \to \mathbb{F}_q$ is an automorphism of $P(q)$ if and only if $f(x) \equiv cx^{p^\ell} + d$, for some $c \in \mathbb{F}_q^+, d \in \mathbb{F}_q$, and $\ell \in \{0, \dots, k-1\}$.*

Using the theory of Paley (di)graphs, we can prove Theorems B and C for $n \geq 3$. For this we use certain test matrices: let $a, b, c \in \mathbb{F}_q$ and define,

$$\mathcal{A}(a, b, c) := \begin{pmatrix} a & a & a \\ a & b & b \\ a & b & c \end{pmatrix}. \tag{3.1}$$

Our general approach is to show that positivity preservers are automorphisms of Paley graphs. We first provide a necessary condition for preserving positivity on $M_n(\mathbb{F}_q)$.

Lemma 3.4 ([11, Lemma 2.13, 2.14])**.** *Let q be a prime power, and $f : \mathbb{F}_q \to \mathbb{F}_q$ be a positivity preserver over $M_n(\mathbb{F}_q)$. Then $f(\mathbb{F}_q^+) \subseteq \mathbb{F}_q^+$. Moreover, if $q \equiv 3 \pmod 4$ then $f(\mathbb{F}_q^+) = \mathbb{F}_q^+$ and $f(0) = 0$.*

Using the above, we provide a short proof of Theorem B for $n \geq 3$.

Proof of Theorem B for $n \geq 3$. (1) $\implies$ (3) for $n \geq 3$: Using Lemma 3.4, without loss of generality, we assume $f(1) = 1$. We can further assume $n = 3$ (as the general case follows by embedding 3×3 positive definite matrices into larger matrices of the form $A \oplus I_{n-3}$). By Lemma 3.4 we have $f(0) = 0$.

Now, if $\eta(a-b) = 0$, then we are done. So assume $\eta(a-b) = 1$. Additionally if $b = 0$, then $\eta(a) = 1$, and by Lemma 3.4 we have $\eta(f(a) - f(0)) = 1$. So assume $b \in \mathbb{F}_q^*$, along with $\eta(a-b) = 1$, and consider two cases.

Case 1: Assume $\eta(b) = 1$. Then the matrix $A := \begin{pmatrix} b & b \\ b & a \end{pmatrix} \oplus I_1$ is positive definite. Hence $\det f[A] = f(b)(f(a) - f(b)) \in \mathbb{F}_q^+$. Since $\eta(f(b)) = 1$ (Lemma 3.4), $\eta(f(a) - f(b)) = 1$.

Case 2: Assume $\eta(b) = -1$. Consider $g(x) := x + b$ over $\mathbb{F}_q$. Since g is bijective, $g(0) = b$ and $g(-b) = 0$, there exists $-c \in \mathbb{F}_q^-$ such that $g(-c) \in \mathbb{F}_q^+$. Hence $\eta(b-c) = 1$, where $c \in \mathbb{F}_q^+$. The matrix $\mathcal{A}(c,b,a)$ is positive definite, and so is $f[\mathcal{A}(c,b,a)]$. In particular

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

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

Finally, if $\eta(a-b) = -1$, then $\eta(b-a) = 1$. Hence, via above $\eta(f(b) - f(a)) = 1$, which implies $\eta(f(a) - f(b)) = -1$. Thus, (1) $\implies$ (3). That (3) $\implies$ (4) follows from Theorem 3.3, (4) $\implies$ (2) is via Proposition 1.4, and (2) $\implies$ (1) is obvious. $\square$

A similar, but more technical route can be taken to resolve the $q \equiv 1 \pmod 4$ case when $n \geq 3$ (Theorem C). The first step is to show the injectivity of preservers.

Theorem 3.5 ([11, Proposition 5.13]). *Let $\mathbb{F}_q$ be a finite field with $q \equiv 1 \pmod 4$ and let f preserve positivity on $M_3(\mathbb{F}_q)$. Then f is injective on $\mathbb{F}_q^+$.*

One can then show that a positivity preserver on $M_3(\mathbb{F}_q)$ has to be an automorphism of the Paley graph $P(q)$. See [11] for the details.

4 Dimension 2: Weil, Muzychuk–Kovács, Erdős–Ko–Rado

Interestingly, when working over $M_2(\mathbb{F}_q)$, determining the positivity preservers is significantly more challenging. In that case, very little structure is available to work with and combinatorial arguments need to be used to construct matrices with specific properties.

4.1 $q \equiv 3 \pmod 4$: Weil's character sum bounds

When $q \equiv 3 \pmod 4$, we first prove that positivity preservers on $M_2(\mathbb{F}_q)$ need to be bijective. The proof involves a non-trivial application of the well-known Weil's bound on complete character sums and proceeds by showing that, if f is not bijective, there must exist a positive definite matrix that loses positivity when f is applied to its entries.

Lemma 4.1 ([11, Lemma 4.1])**.** *Let $\mathbb{F}_q$ be a finite field with $q \equiv 3 \pmod 4$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$ preserve positivity on $M_2(\mathbb{F}_q)$. Then $f(0) = 0$ and f is bijective on $\mathbb{F}_q^+$ and on $\mathbb{F}_q^-$ (and hence on $\mathbb{F}_q$).*

Knowing that f is bijective greatly helps to study the structure of the image set $\{f[A] : A \in M_2(\mathbb{F}_q) \text{ is positive definite}\}$. Our next result shows that a positivity preserver f over $M_2(\mathbb{F}_q)$ must be an odd function satisfying a multiplicative property.

Lemma 4.2 ([11, Lemma 4.2])**.** *Let $\mathbb{F}_q$ be a finite field with $q \equiv 3 \pmod 4$. Suppose $f : \mathbb{F}_q \to \mathbb{F}_q$ preserves positivity on $M_2(\mathbb{F}_q)$ and $f(1) = 1$. Then $f(-x) \equiv -f(x)$ and $f(x^2) \equiv f(x)^2$.*

With the above two preliminary results in hand, we can show that a positivity preserver on $M_2(\mathbb{F}_q)$ has to be an automorphism of the Paley digraph $P(q)$, which immediately implies the $n = 2$ case of Theorem B.

Theorem 4.3 ([11, Theorem 4.3])**.** *Let $\mathbb{F}_q$ be a finite field with $q \equiv 3 \pmod 4$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$ be such that f preserves positivity on $M_2(\mathbb{F}_q)$, and $f(1) = 1$. Then $f(x) \equiv x^{p^\ell}$ for some $\ell = 0, 1, \ldots, k-1$.*

4.2 $q \equiv 1 \pmod 4$: Muzychuk–Kovács's automorphisms

When $q \equiv 1 \pmod 4$, our techniques did not allow us to prove the analogue of Lemma 4.1 showing that a preserver on $M_2(\mathbb{F}_q)$ needs to be bijective on $\mathbb{F}_q^+$. However, under that assumption, we provide a general argument to conclude the classification.

Proposition 4.4 ([11, 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 $0 \le \ell \le k-1$ such that $f(x) = x^{p^\ell}$ for all $x \in \mathbb{F}_q$.*

Our proof of Proposition 4.4 relies on the following result from Muzychuk and Kovács. Let $\Gamma(q)$ be the subgraph of $P(q)$ induced by $\mathbb{F}_q^+$. Muzychuk and Kovács [18] confirmed a conjecture of Brouwer on the automorphisms of $\Gamma(q)$.

Theorem 4.5 ([18])**.** *Let p be a prime and $q = p^k \equiv 1 \pmod 4$. The automorphisms of the graph $\Gamma(q)$ are precisely given by the maps $x \mapsto cx^{\pm p^\ell}$, where $c \in \mathbb{F}_q^+$ and $\ell \in \{0, 1, \ldots, k-1\}$.*

To prove Proposition 4.4, we first show that f induces an automorphism of $\Gamma(q)$.

Lemma 4.6 ([11, Lemma 5.9])**.** *Let q be a prime power with $q \equiv 1 \pmod 4$ and let f be a positivity preserver over $M_2(\mathbb{F}_q)$ with $f(1) = 1$. If f is injective on $\mathbb{F}_q^+$, then $f(0) = 0$, and f (restricted to $\mathbb{F}_q^+$) is an automorphism of $\Gamma(q)$.*

As a consequence of Theorem 4.5, under the assumptions of Proposition 4.4, we obtain $f(x) = x^{\pm p^l}$ for some $l \in \{0, 1, \ldots, k-1\}$. With considerably more effort, we rule out the case $f(x) = x^{-p^l}$ (see [11] for more details).

In view of Proposition 4.4, we provide 3 sufficient conditions for a preserver f on $M_2(\mathbb{F}_q)$ to be injective on $\mathbb{F}_q^+$.

Proposition 4.7 ([11, Proposition 5.11])**.** *Let $q \equiv 1 \pmod 4$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$. If f maps nonsingular matrices to nonsingular matrices, then f is injective on $\mathbb{F}_q^+$.*

We say $f : \mathbb{F}_q \to \mathbb{F}_q$ is a *sign preserver* on $M_n(\mathbb{F}_q)$ if for all symmetric $A \in M_n(\mathbb{F}_q)$, A is positive definite if and only if $f[A]$ is positive definite. Thus, a sign preserver maps positive definite and non-positive definite matrices into themselves, respectively.

Proposition 4.8 ([11, Proposition 5.12])**.** *Let $q \equiv 1 \pmod 4$ and let f be a sign preserver on $M_2(\mathbb{F}_q)$. Then f is injective on $\mathbb{F}_q^+$.*

Finally, when working on $M_n(\mathbb{F}_q)$ with $n \geq 3$, it is not difficult to establish the injectivity of f on $\mathbb{F}_q^+$. This immediately shows $(1) \implies (4)$ in Theorem C.

Proposition 4.9 ([11, Proposition 5.13])**.** *Let $q \equiv 1 \pmod 4$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$. If f is a positivity preserver on $M_3(\mathbb{F}_q)$, then f is injective on $\mathbb{F}_q^+$.*

4.3 The $q = r^2$ case: Erdős–Ko–Rado theorem for Paley graphs

When $q = r^2$ where r is an odd prime power, we exploit the supplementary structure of $\mathbb{F}_q$ to classify the preservers on $M_2(\mathbb{F}_q)$. First notice that $\mathbb{F}_r$ is a clique in $P(q)$. A *square translate* of $\mathbb{F}_r$ has the form $\alpha\mathbb{F}_r + \beta$, where $\alpha \in \mathbb{F}_q^+$ and $\beta \in \mathbb{F}_q$. Such square translates are maximum cliques in $P(q)$ and it is well-known that these are the only maximum cliques in $P(q)$; this is known as the Erdős–Ko–Rado theorem for Paley graphs [10, Section 5.9].

Theorem 4.10 ([6, 1])**.** *In the Paley graph $P(q)$, the clique number of $P(q)$ is r. Moreover, all maximum cliques are given by squares translates of the subfield $\mathbb{F}_r$.*

Note that $\mathbb{F}_q^*/\mathbb{F}_r^*$ is a well-defined group. One can thus write $\mathbb{F}_q^*$ as a disjoint union of $\mathbb{F}_r^*$-cosets. We say such a coset is a *square coset* if it has the form $a\mathbb{F}_r^*$, where a is a non-zero square in $\mathbb{F}_q$. Theorem 4.10 implies the following corollary.

Corollary 4.11 ([11, Corollary 6.2])**.** *Let $C \subset \mathbb{F}_q^+$ be a clique in $P(q)$. Then $|C| \leq r - 1$ and equality holds if and only if C is a square coset.*

Now, let $f : \mathbb{F}_q \to \mathbb{F}_q$ preserve positivity on $M_2(\mathbb{F}_q)$. Using the above supplementary structure of $\mathbb{F}_q$, we obtain the form of f via several non-trivial intermediary results.

Corollary 4.12 ([11, Corollary 6.7, 6.8])**.** *The function f maps a square coset to a square coset and $f(0) = 0$.*

Proposition 4.13 ([11, Proposition 6.9]). *Let $\alpha \in \mathbb{F}_q^+$. 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 $\beta = f(\alpha) \in \mathbb{F}_q^+$.*

Proposition 4.14 ([11, Proposition 6.10]). *The function f maps different square cosets to different square cosets. Equivalently, f is injective on $\mathbb{F}_q^+$.*

Finally, using the above, we determine the structure of f, thereby completing the proof of Theorem C.

Theorem 4.15 ([11, Theorem 6.11]). *If f is a positivity preserver over $M_2(\mathbb{F}_q)$, where $q = p^k \equiv 1 \pmod 4$ is a square, then there exists $c \in \mathbb{F}_q^+$ and $0 \leq \ell \leq k-1$, such that $f(x) = cx^{p^\ell}$ for all $x \in \mathbb{F}_q$.*

One case was not addressed in the paper: the characterization of entrywise preservers on $M_2(\mathbb{F}_q)$ when $q \equiv 1 \pmod 4$ and q is not a square. A possible approach for resolving that case is to show that such preservers need to be injective on $\mathbb{F}_q^+$ (and then invoke Proposition 4.4). This was verified when $q = 5$. The general case is open.

Question 4.16. 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 $\mathbb{F}_q^+$?

Acknowledgements

The authors thank the American Institute of Mathematics (CalTech) for their hospitality and stimulating environment during the workshop "Theory and Applications of Total Positivity" in July 2023 where the first three authors met. The authors would also like to thank Apoorva Khare, Felix Lazebnik, and two anonymous referees for their comments.

References

[1] S. Asgarli and C. H. Yip. "Van Lint–MacWilliams' conjecture and maximum cliques in Cayley graphs over finite fields". *J. Combin. Theory Ser. A* **192** (2022), Paper No. 105667, 23. DOI.

[2] A. Belton, D. Guillot, A. Khare, and M. Putinar. "Matrix positivity preservers in fixed dimension. I". *Adv. Math.* **298** (2016), pp. 325–368. DOI.

[3] A. Belton, D. Guillot, A. Khare, and M. Putinar. "A panorama of positivity. I: Dimension free". *Analysis of operators on function spaces*. Trends Math. Birkhäuser/Springer, Cham, 2019, pp. 117–164. DOI.

[4] A. Belton, D. Guillot, A. Khare, and M. Putinar. "A panorama of positivity. II: Fixed dimension". *Complex analysis and spectral theory*. Vol. 743. Contemp. Math. Amer. Math. Soc., 2020, pp. 109–150. DOI.

[5] A. Belton, D. Guillot, A. Khare, and M. Putinar. "Moment-sequence transforms". *J. Eur. Math. Soc.* **24**.9 (2022), pp. 3109–3160. DOI.

[6] A. Blokhuis. "On subsets of $\mathrm{GF}(q^2)$ with square differences". *Nederl. Akad. Wetensch. Indag. Math.* **46**.4 (1984), pp. 369–372.

[7] A. E. Brouwer and W. H. Haemers. *Spectra of graphs*. Universitext. Springer, New York, 2012, xiv+250 pp. DOI.

[8] L. Carlitz. "A theorem on permutations in a finite field". *Proc. Amer. Math. Soc.* **11**.3 (1960), pp. 456–459. DOI.

[9] J. Cooper, E. Hanna, and H. Whitlatch. "Positive-definite matrices over finite fields". *Rocky Mountain J. Math.* **54**.2 (2024), pp. 423–438. DOI.

[10] C. Godsil and K. Meagher. *Erdős-Ko-Rado theorems: algebraic approaches*. Vol. 149. Cambridge Stud. Adv. Math., Cambridge University Press, 2016, xvi+335 pp. DOI.

[11] D. Guillot, H. Gupta, P. K. Vishwakarma, and C. H. Yip. "Positivity preservers over finite fields". 2024. arXiv:2404.00222v3.

[12] A. Guterman, C.-K. Li, and P. ˇ Semrl. "Some general techniques on linear preserver problems". *Linear Algebra Appl.* **315**.1-3 (2000), pp. 61–81. DOI.

[13] R. A. Horn and C. R. Johnson. *Matrix analysis*. Second. Cambridge University Press, Cambridge, 2013, xviii+643 pp.

[14] A. Khare. *Matrix analysis and entrywise positivity preservers*. Vol. 471. London Math. Soc. Lecture Note Ser. Cambridge University Press, 2022, xxii+292 pp.

[15] A. Khare and T. Tao. "Schur polynomials, entrywise positivity preservers, and weak majorization". *Sem. Lothar. Combin. B* **80** (2018).

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

[17] C.-K. Li and S. Pierce. "Linear preserver problems". *Amer. Math. Monthly* **108**.7 (2001), pp. 591–605. DOI.

[18] M. Muzychuk and I. Kovács. "A solution of a problem of A. E. Brouwer". *Des. Codes Cryptogr.* **34**.2-3 (2005), pp. 249–264. DOI.

[19] M. Orel. "Preserver problems over finite fields". *Int. J. Math. Game Theory Algebra.* **25**.3 (2016).

[20] W. Rudin. "Positive definite sequences and absolutely monotonic functions". *Duke Math. J.* **26** (1959), pp. 617–622.

[21] I. J. Schoenberg. "Positive definite functions on spheres". *Duke Math. J.* **9** (1942), pp. 96–108.

[22] J. Schur. "Bemerkungen zur Theorie der beschränkten Bilinearformen mit unendlich vielen Veränderlichen". *J. Reine Angew. Math.* **140** (1911), pp. 1–28. DOI.

[23] H. Vasudeva. "Positive definite matrices and absolutely monotonic functions". *Indian J. Pure Appl. Math* **10**.7 (1979), pp. 854–858.