POSITIVITY PRESERVERS OVER FINITE FIELDS

DOMINIQUE GUILLOT, HIMANSHU GUPTA, AND PRATEEK KUMAR VISHWAKARMA

ABSTRACT. We resolve an algebraic version of Schoenberg's celebrated theorem [*Duke Math. J.*, 1942] characterizing entrywise matrix transforms that preserve positive definiteness. Compared to the classical real and complex settings, we consider matrices with entries in a finite field and obtain a complete characterization of such preservers for matrices of a fixed dimension. When the dimension of the matrices is at least 3, we prove that, surprisingly, the positivity preservers are precisely the positive multiples of the field's automorphisms. Our work makes crucial use of the well-known character-sum bound due to Weil, and of a result of Carlitz [*Proc. Amer. Math. Soc.*, 1960] that provides a characterization of the automorphisms of Paley graphs.

1. Introduction and main Results

Let $A = (a_{ij})$ be an $n \times n$ matrix and let f be a function defined on the entries of A. The function naturally induces an entrywise transformation of A via $f[A] := (f(a_{ij}))$. The study of such entrywise transforms that preserve various forms of matrix positivity has a rich and long history with important applications in many fields of mathematics such as distance geometry and Fourier analysis on groups – see the surveys [2, 3] and the monograph [22] for more details. Consider for example the set of $n \times n$ real symmetric or complex Hermitian matrices. By the well-known Schur product theorem [29], the entrywise product $A \circ B := (a_{ij}b_{ij})$ of two positive semidefinite matrices is positive semidefinite. As an immediate consequence of this surprising result, monomials $f(x) = x^n$ with $n \geq 1$, and more generally convergent power series $f(x) = \sum_{n=0}^{\infty} c_n x^n$ with real nonnegative coefficients $c_n \geq 0$ preserve positive semidefiniteness when applied entrywise to $n \times n$ real symmetric or complex Hermitian positive semidefinite matrices. An impressive converse of this result was obtained by Schoenberg [28], with various refinements by others collected over time.

Theorem 1.1 ([28, 27, 4])**.** *Let $I := (-\rho, \rho)$, 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 semidefinite matrices of all dimensions with entries in I.*
(2) *The function f is* 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.*

Notice that in Schoenberg's result, the characterization applies to functions preserving positivity for matrices of arbitrary large dimension. Obtaining a characterization of the entrywise preservers for matrices of a fixed dimension is a very natural endeavor, but a much harder problem that remains mostly unsolved. An interesting necessary condition given by Horn [19] shows that such preservers must have a certain degree of smoothness, with a number of non-negative derivatives. In [1], seventy-four years after the publication of Schoenberg's result, Belton–Guillot–Khare–Putinar resolved the problem for polynomials of degree at most N that preserve positivity on $N \times N$ matrices. They also provided the first known example of a non-absolutely monotone polynomial that preserves positivity in a fixed dimension. In [23], Khare and Tao characterized the sign patterns

Date: April 29, 2024.
2010 *Mathematics Subject Classification.* 15B48 (primary); 15B33, 11T06, 05E30 (secondary).
Key words and phrases. positive definite matrix, entrywise transform, finite fields, field automorphism, character sums, Paley graph.

of the Maclaurin coefficients of positivity preservers in fixed dimension. They also considered sums of real powers, and uncovered exciting connections between positivity preservers and symmetric function theory. However, apart from this recent progress, the problem of determining entrywise preservers in fixed dimension remains mostly unresolved. We note that many other variants were previously explored, including problems involving: structured matrices [4, 14, 15], specific functions [10, 12, 13, 16, 18], block actions [17, 31], different notions of positivity [5], preserving inertia [6], and multivariable transforms [6, 11].

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. As a consequence, we also obtain the positivity preservers for matrices of all dimensions, as in the setting of Schoenberg's theorem. Here, we say that a symmetric matrix in $M_n(\mathbb{F}_q)$ with entries in a finite field $\mathbb{F}_q$ is positive definite if each of its leading principal minors is equal to the square of some non-zero element in $\mathbb{F}_q$, i.e., the leading principal minors are quadratic residues in $\mathbb{F}_q$. As shown in [9], this leads to a reasonable notion of positivity for matrices with entries in finite fields. 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 combinatorial and number-theoretic arguments. Surprisingly, our characterizations unearth new connections between functions preserving positivity, field automorphisms, and automorphisms of the Paley graphs associated to finite fields. Recall that the Paley graph $P(q)$ associated to $\mathbb{F}_q$ is the graph whose vertices are $V = \mathbb{F}_q$ with edges $(a, b) \in E$ if and only if $a - b$ is a non-zero quadratic residue in $\mathbb{F}_q$. Our main result is as follows.

Theorem 1.2 (Main result). *Let $\mathbb{F}_q$ be any finite field with $q = p^k$ elements 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 preserves positivity on $M_n(\mathbb{F}_q)$ for all $n \geq 3$.*
(3) *f is a positive multiple of a field automormhism of $\mathbb{F}_q$, i.e., there exist $c = d^2 \in \mathbb{F}_q^*$ and an integer $0 \leq \ell \leq k-1$ such that $f(x) = cx^{p^\ell}$ for all $x \in \mathbb{F}_q$.*

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 $a, b \in \mathbb{F}_q$, where $\eta(x)$ denotes the quadratic character of $\mathbb{F}_q$.*

Detailed statements of all our main results including refinements are given in Theorems A, B, and C below.

1.1. Main results.

Let p be a prime number. We denote the finite field with $q = p^k$ elements by $\mathbb{F}_q$. 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.,

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

If q is odd, then $|\mathbb{F}_q^+| = \frac{q-1}{2}$. The *quadratic character* of $\mathbb{F}_q$ is the function $\eta : \mathbb{F}_q \to \{-1, 0, 1\}$ given by:

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

Observe that $\eta(xy) = \eta(x)\eta(y)$ for all $x, y \in \mathbb{F}_q$ and $\sum_{x \in \mathbb{F}_q} \eta(x) = 0$. 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 0.

In this paper, we adopt the following definition of positive definiteness.

Definition 1.3 (Positive definite matrices)**.** Let $\mathbb{F}_q$ be a finite field. We say that a matrix $A \in M_n(\mathbb{F}_q)$ is *positive definite* if A is symmetric and all the leading principal minors of A belong to $\mathbb{F}_q^+$.

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

Definition 1.4. 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 are interested in determining the functions f for which $f[A]$ is positive definite for all positive definite $A \in M_n(\mathbb{F}_q)$. When this is the case, we say that f preserves positivity on $M_n(\mathbb{F}_q)$.

In classifying the positivity preservers on $M_n(\mathbb{F}_q)$, a natural trichotomy arises. When $p = 2$, the Frobenius map $f(x) = x^2$ is an automorphism of $\mathbb{F}_q$ so that every non-zero element of $\mathbb{F}_q$ is a square. Characterizing the entrywise preservers in even characteristic thus reduces to characterizing the entrywise transformation that preserve non-singularity, a problem that is considerably different from the odd characteristic case. Our techniques in odd characteristic also differ depending on whether -1 is a square in $\mathbb{F}_q$ or not. When q is odd, it is well-known that $-1 \notin \mathbb{F}_q^+$ if and only if $q \equiv 3 \pmod 4$. As a consequence, our work is 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 $k \geq 1$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$. Then*

1. *($n = 2$ case) The following are equivalent:*
   (a) *f preserves positive definiteness on $M_2(\mathbb{F}_q)$.*
   (b) *$f(0) = 0$, f is bijective, and $f(\sqrt{xy})^2 = f(x)f(y)$ for all $x, y \in \mathbb{F}_q$.*
   (c) *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 $x \in \mathbb{F}_q$.*

Remark 1.5. The condition $\gcd(n, q-1)$ on the power in Theorem A(1c) is equivalent to the fact that $f(x) = x^n$ is bijective on $\mathbb{F}_q$ (see Theorem 2.2). The positivity preservers on $M_2(\mathbb{F}_q)$ thus coincide with the bijective monomials.

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 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 $a, b \in \mathbb{F}_q$.*
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 $q \equiv 1 \pmod 4$. 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 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 $a, b \in \mathbb{F}_q$.*
(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 $x \in \mathbb{F}_q$.*

In particular, as stated in Theorem 1.2, for any finite field $\mathbb{F}_q$ and any $n \geq 3$, the positivity preservers on $M_n(\mathbb{F}_q)$ are precisely the positive multiples of the automorphisms of $\mathbb{F}_q$.

The rest of the paper is dedicated to proving Theorems A, B, and C. Section 2 contains preliminary results including statements of classical results from finite fields theory that are needed in the proofs, a discussion of the properties of positive definite matrices with entries in a finite field, and preliminary results on entrywise preservers over finite fields. Section 3, 4, and 5 address the even case (Theorem A), the $q \equiv 3 \pmod 4$ case (Theorem B), and the $q \equiv 1 \pmod 4$ case (Theorem C), respectively. Section 6 contains supplementary results on positivity preservers. Concluding remarks are given in Section 7.

2. Preliminary results

For convenience of the reader, we begin by collecting some standard results about finite fields that we will use later. The reader who is familiar with finite fields can safely skip the next subsection. We then discuss in greater detail the properties of positive definite matrices over finite fields, and prove some preliminary properties of entrywise preservers.

2.1. Finite fields.

We first recall the characterization of automorphisms of finite fields.

Theorem 2.1 ([25, Theorem 2.21])**.** *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, $(x + y)^{p^\ell} = \sigma_\ell(x + y) = \sigma_\ell(x) + \sigma_\ell(y) = x^{p^\ell} + y^{p^\ell}$ in a field of characteristic p. Notice that in characteristic 2, the map $x \mapsto \sigma_1(x) = x^2$ is an automorphism. It follows that every non-zero element in $\mathbb{F}_{2^k}$ is a square, i.e., $\mathbb{F}_{2^k}^+ = \mathbb{F}_{2^k}^*$.

Next, recall some elementary facts about permutation polynomials over $\mathbb{F}_q$, i.e., polynomials that are bijective on $\mathbb{F}_q$.

Theorem 2.2 ([25, Theorem 7.8])**.**
(1) *Every non-constant linear polynomial over $\mathbb{F}_q$ is a permutation polynomial of $\mathbb{F}_q$.*
(2) *The monomial x^n is a permutation polynomial of $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$.*

The following simple facts will be useful later. We provide a short proof for completeness.

Proposition 2.3. *Let $\mathbb{F}_q$ be a finite field of odd characteristic. Then the following are equivalent:*
(1) $q \equiv 3 \pmod 4$.
(2) *-1 is not a square in $\mathbb{F}_q$.*
(3) *We have*
$$\mathbb{F}_q = \{0\} \sqcup \mathbb{F}_q^+ \sqcup (-\mathbb{F}_q^+).$$
(4) *Every element in $\mathbb{F}_q^+$ has a unique positive square root.*

Proof. The equivalence between (1) and (2) is folklore (see e.g. [24, Corollary II.2.2]).

Next, suppose (2) holds. Let $x \in \mathbb{F}_q^* \setminus \mathbb{F}_q^+$. Since -1 is not a square in $\mathbb{F}_q$, we have $\eta(-x) = \eta(-1)\eta(x) = 1$. It follows that $-x \in \mathbb{F}_q^+$ and so $x \in -\mathbb{F}_q^+$. This proves $\mathbb{F}_q = \{0\} \cup \mathbb{F}_q^+ \cup (-\mathbb{F}_q^+)$. That the union is disjoint follows again from the fact that $\eta(-x) = -\eta(x)$.

Now, suppose (3) holds. Let $x \in \mathbb{F}_q^+$, say $x = y^2$. Then y and $-y$ are exactly the square roots of x because every element in $\mathbb{F}_q$ has at most 2 square roots. Since only one of these is positive, the positive square root of x must be unique. Finally, suppose (4) holds. Since $1^2 = (-1)^2 = 1$, both 1 and -1 are square roots of 1 in $\mathbb{F}_q$. Since $1 \in \mathbb{F}_q^+$ the uniqueness implies that $-1 \notin \mathbb{F}_q^+$. $\square$

When q is even, since $x \mapsto x^2$ is a bijective map, every non-zero element also has a unique positive square root. When q is even or $q \equiv 3 \pmod 4$, we denote the unique positive square root of $x \in \mathbb{F}_q^+$ by $\sqrt{x}$ or by $x^{1/2}$. We also define $\sqrt{0} = 0$.

We will also need the following well-known character sum bound due to André Weil.

Theorem 2.4 (Weil [25, Theorem 5.41])**.** *Let Ψ be a multiplicative character of $\mathbb{F}_q$ of degree $m > 1$ and let $f \in \mathbb{F}_q[x]$ be a monic polynomial that is not an m-th power of a polynomial. Let d be the number of distinct roots of f in its splitting field over $\mathbb{F}_q$. Then for every $a \in \mathbb{F}_q$, we have*

$$\left| \sum_{c \in \mathbb{F}_q} \Psi(af(c)) \right| \leq (d-1)\sqrt{q}.$$

The next classical lemma shows that two polynomials in $\mathbb{F}_q[x]$ coincide as functions, i.e., when evaluated at every point of $\mathbb{F}_q$, if and only if they are equal as polynomials modulo $x^q - x$.

Lemma 2.5 (see e.g. [25, Lemma 7.2])**.** *For $g(x), h(x) \in \mathbb{F}_q[x]$ we have $g(c) = h(c)$ for all $c \in \mathbb{F}_q$ if and only if $g(x) \equiv h(x) \pmod{x^q - x}$.*

Notice that every function $f : \mathbb{F}_q \to \mathbb{F}_q$ can be written as an interpolation polynomial of degree at most $q-1$. When studying entrywise positivity preservers, we can thus assume, without loss of generality, that f is a polynomial of degree at most $q-1$.

Finally, we recall some of the properties of the Paley graph associated to a finite field $\mathbb{F}_q$.

Definition 2.6. Let q be an odd prime power. The Paley graph $P(q)$ is the graph whose vertices are the elements of $\mathbb{F}_q$ and where two vertices $a, b \in \mathbb{F}_q$ are adjacent if and only $a - b \in \mathbb{F}_q^+$.

Notice that when $q \equiv 1 \pmod 4$, we have $a - b \in \mathbb{F}_q^+$ if and only if $b - a \in \mathbb{F}_q^+$. The graph $P(q)$ is thus undirected. However, when $p \equiv 3 \pmod 4$, the graph becomes directed and is often referred to as the Paley digraph.

Paley graphs have been well-studied in the literature. In particular, when $q \equiv 1 \pmod 4$, they are well-known to be strongly regular. Given a graph $G = (V, E)$ and a vertex $v \in V$ let us denote the set of adjacent vertices to v by $N(v)$ and the set of non-adjacent vertices by $N^c(v) := V \setminus (N(v) \cup \{v\})$.

Definition 2.7 (see e.g. [7, Chapter 9])**.** A strongly-regular graph $\operatorname{srg}(\nu, k, \lambda, \mu)$ is a graph with ν vertices that has the following properties:

(1) For any vertex v, we have $|N(v)| = k$.
(2) For any two adjacent vertices u, v, we have $|N(u) \cap N(v)| = \lambda$.
(3) For any two non-adjacent vertices u, v, we have $|N(u) \cap N(v)| = \mu$.

Lemma 2.8 (see e.g. [7, Proposition 9.1.1])**.** *Let q be a prime power with $q \equiv 1 \pmod 4$. Then $P(q)$ is $\operatorname{srg}(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$. Consequently, for any two adjacent vertices x, y, we have*

$$|N(y) \cap N^c(x)| = |N(y)| - |N(y) \cap N(x)| - 1 = \frac{q-1}{2} - \frac{q-5}{4} - 1 = \frac{q-1}{4}.$$

An *automorphism of the Paley graph $P(q)$* is a permutation polynomial $f(x)$ which satisfies $\eta(f(a) - f(b)) = \eta(a - b)$ for all $a, b \in \mathbb{F}_q$. Thus, it follows from Theorem 2.1 that $f(x) = cx^{p^\ell} + d$ is an automorphism of $P(q)$ for any $c \in \mathbb{F}_q^+$, $d \in \mathbb{F}_q$, and $0 \leq \ell \leq k-1$. More interestingly, polynomials of this type precisely form the set of automorphisms of the Paley graph $P(q)$. Proving this result requires substantial effort. One of the first proofs follows from the following theorem due to Carlitz.

Theorem 2.9 (Carlitz [8])**.** *Let $\mathbb{F}_q$ be a finite field of odd characteristic and let $f(x)$ be a permutation polynomial 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 $0 \leq \ell \leq k-1$.*

It is worth noting that in Carlitz's work [8], there is no mention of the Paley graph or its automorphisms. Carlitz was instead motivated in answering a question raised by W. A. Pierce. For other known proofs of Theorem 2.9 and its generalizations, and for an account of the history of Paley graphs and their automorphism groups, we refer the interested reader to the survey article [21] by Jones.

2.2. **Positive definite matrices over finite fields.** For real symmetric or complex Hermitian matrices, it is well-known that many natural notions of positive definiteness coincide. Any of the following equivalent conditions can be used to define positive definiteness.

Proposition 2.10 (see e.g. [20, Chapter 7])**.** *Let $A \in M_n(\mathbb{C})$ be a Hermitian matrix. Then the following are equivalent:*

1. *$z^*Az > 0$ for all non-zero $z \in \mathbb{C}^n$.*
2. *A has positive eigenvalues.*
3. *The sesquilinar form $Q(z,w) = z^*Aw$ forms an inner product.*
4. *A is the Gram matrix of linearly independent vectors.*
5. *All leading principal minors of A are positive.*
6. *A has a unique Cholesky decomposition.*

As shown in [9], the situation is very different for matrices over finite fields. For example, the standard definition of positive definiteness via quadratic forms (as in Proposition 2.10(1)) does not yield a useful notion over finite fields.

Proposition 2.11 ([9, Proposition 1])**.** *Let $\mathbb{F}_q$ be a finite field, let $n \geq 3$, and let $A \in M_n(\mathbb{F}_q)$. Define $Q : \mathbb{F}_q^n \to \mathbb{F}_q$ by $Q(x) = x^T Ax$. Then there exists a non-zero vector $v \in \mathbb{F}_q^n$ so that $Q(v) = 0$.*

In fact, more can be said about the range of the quadratic form associated to a positive definite matrix.

Proposition 2.12. *Let $n \geq 2$ and let $A \in M_n(\mathbb{F}_q)$ be a positive definite matrix. Then the range of the quadratic form $Q(x) = x^T Ax$ is $\mathbb{F}_q$, i.e.,*

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

Proof. Suppose first $n = 2$. Let

$$A = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \in M_2(\mathbb{F}_q)$$

be positive definite. Then $a \in \mathbb{F}_q^+$ and $ac - b^2 \in \mathbb{F}_q^+$. In particular, $c - b^2a^{-1} \in \mathbb{F}_q^+$. For $x = (x_1, x_2)^T \in \mathbb{F}_q^2$, consider the quadratic form

$$Q(x) = x^T Ax = ax_1^2 + 2bx_1x_2 + cx_2^2.$$

Completing the square, we obtain

$$Q(x) = a(x_1 + ba^{-1}x_2)^2 + (c - b^2a^{-1})x_2^2.$$

Setting $y_1 := a^{1/2}\left(x_1 + ba^{-1}x_2\right)$ and $y_2 := (c - b^2a^{-1})^{1/2}x_2$ yields the equivalent diagonal quadratic form

$$\widetilde{Q}(y) = y_1^2 + y_2^2$$

having the same range as Q. Since every element of $\mathbb{F}_q$ can be written as the sum of two (not necessarily nonzero) squares, it follows that the range of Q is $\mathbb{F}_q$.

Suppose now $n \geq 3$. Let $\widetilde{A} \in M_2(\mathbb{F}_q)$ be the 2×2 leading principal submatrix of A. Then $\widetilde{A}$ is positive definite. Letting $x := (\widetilde{x}^T, \mathbf{0}_{1\times(n-2)})^T \in \mathbb{F}_q^n$ with $\widetilde{x} \in \mathbb{F}_q^2$, we obtain

$$x^T Ax = \widetilde{x}^T \widetilde{A}\widetilde{x}.$$

The result now follows from the $n = 2$ case. ∎

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 2.13 ([9, Theorem 2, Corollary 1])**.** *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 $q \equiv 1 \pmod 4$.

Proposition 2.14. *Let $q \equiv 1 \pmod 4$. Then there exists a positive definite matrix $A \in M_2(\mathbb{F}_q)$ that does not admit a Cholesky decomposition.*

Proof. For $x \in \mathbb{F}_q^*$, let

$$A(x) := \begin{pmatrix} 1 & x \\ x & 0 \end{pmatrix}.$$

Then $A(x)$ is positive definite since $-1 \in \mathbb{F}_q^+$ (Proposition 2.3). Suppose $A(x) = LL^T$, say

$$A(x) = \begin{pmatrix} 1 & x \\ x & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a^2 & ab \\ ab & b^2 + c^2 \end{pmatrix}$$

with $a, c \in \mathbb{F}_q^+$. Then $a = \pm 1$, $b = \pm x$ and $c^2 = -b^2 = -x^2$. Thus $c \in \{ix, -ix\}$ where i denotes a square root of -1 in $\mathbb{F}_q$. We can then pick $x \in \mathbb{F}_q^*$ such that $\eta(c) = \eta(i)\eta(x) = -1$. Such a choice of x forces $c \notin \mathbb{F}_q^+$ and therefore the Cholesky decompostion of $A(x)$ does not exist. $\square$

Remark 2.15. We note that, when q is even or $q \equiv 3 \pmod 4$, the authors of [9] define a symmetric matrix in $M_n(\mathbb{F}_q)$ to be positive definite if it admits a Cholesky decomposition. As Theorem 2.13 shows, this definition coincides with ours. We note, however, that verifying if a matrix admits a Cholesky decomposition is not as straightforward as computing leading principal minors. This is our motivation for adopting Definition 1.3.

Notice that in a finite field, a sum of squares is not always a square. In fact, 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 (take, for example, $M = (x, y) \in M_{1\times 2}(\mathbb{F}_q)$ with $x^2 + y^2 \notin \mathbb{F}_q^+$.) Many other standard properties of positive definite matrices over $\mathbb{R}$ or $\mathbb{C}$ fail for finite fields. For example, a positive definite matrix may not have positive eigenvalues and the Hadamard product of two positive definite matrices is not always positive definite. See [9, Section 3] for more details. As mentioned above, the behavior of the quadratic form of a positive definite matrix is also different over finite fields (see Proposition 2.12). The reader who is accustomed to working with positive definite matrices over the real or the complex field must thus take great care when moving to the finite field world.

2.3. **Entrywise preservers.** We now turn our attention to entrywise positivity preservers on $M_n(\mathbb{F}_q)$. Recall that every function $f : \mathbb{F}_q \to \mathbb{F}_q$ coincides with a polynomial of degree at most $q - 1$ (Lemma 2.5). Unless otherwise specified, we therefore always assume below that f is such a polynomial.

When $n = 1$, the preservers are precisely the functions $f : \mathbb{F}_q \to \mathbb{F}_q$ such that $f(\mathbb{F}_q^+) \subseteq \mathbb{F}_q^+$. In characteristic 2, the Frobenius map $x \mapsto x^2$ is an automorphism and as a result, every non-zero element is a square. The positivity condition thus reduces to $0 \notin f(\mathbb{F}_q^+)$. There are $(q-1)^{q-1} \times q$

such maps. In odd characteristic, the number of preservers is $\left(\frac{q-1}{2}\right)^{\frac{q-1}{2}} \times q^{\frac{q+1}{2}}$. Any such map can be explicitly written using an interpolation polynomial.

We next obtain a family of maps that preserves positivity for matrices with entries in any finite field.

Proposition 2.16. *Let $\mathbb{F}_q$ be a finite field of characteristic p. 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 $A = (a_{ij}) \in M_n(\mathbb{F}_q)$ be positive definite and let A_r denote the leading $r \times r$ principal submatrix of A. By Definition 1.3, $\det A_r = \mu^2$ for some $\mu \in \mathbb{F}_q^*$. Let $f(x) = x^{p^\ell}$. By Theorem 2.1 $(x+y)^{p^\ell} = x^{p^\ell} + y^{p^\ell}$ in $\mathbb{F}_q$. Thus, by using the Leibniz formula for the determinant we obtain

$$\begin{aligned}\det f[A_r] &= \sum_{\sigma \in S_r} \operatorname{sgn}(\sigma) a_{1,\sigma(1)}^{p^\ell} a_{2,\sigma(2)}^{p^\ell} \dots a_{r,\sigma(r)}^{p^\ell} = \left(\sum_{\sigma \in S_r} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} \dots a_{r,\sigma(r)} \right)^{p^\ell} \\ &= (\det A_r)^{p^\ell} = (\mu^2)^{p^\ell} = (\mu^{p^\ell})^2.\end{aligned}$$

Notice that the above holds even when $p = 2$ since in that case $-1 = 1$ in $\mathbb{F}_q$ and so $\operatorname{sgn}(\sigma) = 1$ for all $\sigma \in S_r$. Since the above holds for any $1 \leq r \leq n$, the matrix $f[A]$ is positive definite. Clearly, multiplying f by $c \in \mathbb{F}_q^+$ also yield a positivity preserver. $\square$

Our next result provides a necessary condition for preserving positivity on $M_2(\mathbb{F}_q)$ when q is even or $q \equiv 3 \pmod 4$.

Lemma 2.17. *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. Let $a, b \in \mathbb{F}_q^+$ with $a \neq b$. Thus, either $a - b \in \mathbb{F}_q^+$ or $b - a \in \mathbb{F}_q^+$. Say $a - b \in \mathbb{F}_q^+$ without loss of generality. Thus, the matrix

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

is positive definite. Note that $f(a), f(b) \in \mathbb{F}_q^+$ since f is preserving the positivity of the positive definite matrices aI_2 and bI_2. By assumption, $f[A]$ is also positive definite. Hence, $\det f[A] = f(b)(f(a) - f(b)) \in \mathbb{F}_q^+$. In particular, $f(a) \neq f(b)$. This proves that f is an injective map on $\mathbb{F}_q^+$, and is therefore a bijection from $\mathbb{F}_q^+$ onto itself. This proves (1).

Now, suppose $f(0) = c$ where $c \in \mathbb{F}_q^+$. By the first part, there exists $a \in \mathbb{F}_q^+$ such that $f(a) = c$. Since the matrix aI_2 is positive definite so is $f[aI_2]$. However,

$$f[aI_2] = \begin{pmatrix} c & c \\ c & c \end{pmatrix},$$

which is not positive definite. If instead $f(0) \in -\mathbb{F}_q^+$, then $c := -f(0) \in \mathbb{F}_q^+$. Now repeat the above argument to get $\det f[aI_2] = 0$, again a contradiction. Thus, it follows by Proposition 2.3 that $f(0) = 0$. $\square$

The next lemma discusses the number of square elements in the translations of the squares in $\mathbb{F}_q$. The result will be used later on to prove that preservers on $M_2(\mathbb{F}_q)$ are bijective (see Theorem 4.1). Recall that η denotes the quadratic character of $\mathbb{F}_q$ (see Equation (1.1)).

Lemma 2.18. *Let $\mathbb{F}_q$ be a finite field with $q \equiv 3 \pmod 4$. Fix $a \in \mathbb{F}_q^*$, and define*

$$G_a := \{a + g : g \in \mathbb{F}_q^+\}.$$

Then $|G_0 \cap G_a| = \frac{q-3}{4}$.

Proof. For $a \in \mathbb{F}_q^+$, we have

$$\begin{aligned}|G_0 \cap G_a| &= \sum_{x\in\mathbb{F}_q\setminus\{0,-a\}} \frac{\eta(x)+1}{2}\cdot\frac{\eta(x+a)+1}{2}\\ &= \frac{1}{4}\left(\sum_{x\in\mathbb{F}_q\setminus\{0,-a\}}\eta(x)\eta(x+a) + \sum_{x\in\mathbb{F}_q\setminus\{0,-a\}}\eta(x) + \sum_{x\in\mathbb{F}_q\setminus\{0,-a\}}\eta(x+a) + \sum_{x\in\mathbb{F}_q\setminus\{0,-a\}} 1\right)\\ &= \frac{1}{4}\left(-1-\eta(-a)-\eta(a)+q-2\right)\\ &= \frac{q-3}{4},\end{aligned}$$

where for the first term, we have

$$\begin{aligned}\sum_{x\in\mathbb{F}_q\setminus\{0,-a\}}\eta(x)\eta(x+a) &= \sum_{x\in\mathbb{F}_q^*}\eta(x)\eta(x+a) = \sum_{x\in\mathbb{F}_q^*}\eta(x^{-1})\eta(x+a) = \sum_{x\in\mathbb{F}_q^*}\eta(1+ax^{-1})\\ &= \sum_{\substack{t\in\mathbb{F}_q\\ t\neq 1}}\eta(t) = -1.\end{aligned}$$

□

The rest of the paper is mostly devoted to proving that the positive multiples of field automorphisms are the only entrywise positivity preservers on $M_n(\mathbb{F}_q)$ when $n \geq 3$. We begin by examining fields of even characteristic as they behave differently from the odd characteristic fields with respect to positivity preservers.

3. Even characteristic

In this section, we always assume $q = 2^k$ for some integer $k \geq 1$. Recall that in that case the Frobenius map $x \mapsto x^2$ is bijective and therefore $\mathbb{F}_q^+ = \mathbb{F}_q^*$. Positive definiteness thus reduces to the non-vanishing of the leading principal minors. We break down the proof of Theorem A into two parts: the $n = 2$ case (Theorem 3.1) and the $n \geq 3$ case (Theorem 3.2).

Theorem 3.1. *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 positive definiteness 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 $x \in \mathbb{F}_q$.*

Proof. (1) $\implies$ (2). Suppose (1) holds. Then $f(0) = 0$ and f is bijective on $\mathbb{F}_q^+ = \mathbb{F}_q^*$ by Lemma 2.17. Thus, f is bijective on $\mathbb{F}_q$. Fix $x, y \in \mathbb{F}_q^*$ and consider the matrix

$$A(z) = \begin{pmatrix} x & \sqrt{xy}z \\ \sqrt{xy}z & y \end{pmatrix} \qquad (z \in \mathbb{F}_q).$$

Observe that $A(z)$ is positive definite if and only if $z \neq 1$. Thus, for any $z \neq 1$, $f[A(z)]$ is positive definite and so

$$\det f[A(z)] = f(x)f(y) - f(\sqrt{xy}z)^2 \neq 0.$$

Hence, for all $z \neq 1$,

$$f(\sqrt{xy}z)^2 \neq f(x)f(y). \tag{3.1}$$

Since f and the $x \mapsto x^2$ maps are bijections, there exists a unique $w \in \mathbb{F}_q$ such that $f(w)^2 = f(x)f(y)$. Also, the map $z \mapsto \sqrt{xy}z$ is a bijection of $\mathbb{F}_q$. Using Equation (3.1), we conclude that

$w = \sqrt{xy}$ and so $f(\sqrt{xy})^2 = f(x)f(y)$. The expression $f(\sqrt{xy})^2 = f(x)f(y)$ also holds trivially when $x = 0$ or $y = 0$ since $f(0) = 0$. This proves (2).

(2) $\implies$ (3). Suppose (2) holds and let $f(x) = \sum_{k=1}^{q-1} a_k x^k$ without loss of generality. Applying the Frobenius, we obtain

$$f(\sqrt{xy})^2 = \left(\sum_{k=1}^{q-1} a_k(\sqrt{xy})^k\right)^2 = \sum_{k=1}^{q-1} a_k^2 x^k y^k.$$

Next, we compute

$$f(x)f(y) = \left(\sum_{i=1}^{q-1} a_i x^i\right)\left(\sum_{j=1}^{q-1} a_j x^j\right) = \sum_{k=1}^{q-1} a_k^2 x^k y^k + \sum_{1\leq i<j\leq q-1} a_i a_j (x^i y^j + x^j y^i).$$

Since $f(\sqrt{xy})^2 = f(x)f(y)$ for all $x, y \in \mathbb{F}_q$, we conclude that

$$Q(x,y) := \sum_{1\leq i<j\leq q-1} a_i a_j (x^i y^j + x^j y^i) = 0$$

for all $x, y \in \mathbb{F}_q$. Now, for any fixed y,

$$Q(x,y) = \sum_{k=1}^{q-1}\left(\sum_{\substack{1\leq j\leq q-1\\ j\neq k}} a_j a_k y^j\right) x^k$$

is a polynomial in x of degree at most $q-1$ that is identically 0 on $\mathbb{F}_q$. Therefore, by Lemma 2.5,

$$\sum_{\substack{1\leq j\leq q-1\\ j\neq k}} a_j a_k y^j = 0 \qquad (1 \leq k \leq q-1).$$

Since this is true for all $y \in \mathbb{F}_q$ and since the above expression is a polynomial of degree at most $q-1$, we conclude that $a_j a_k = 0$ for all $j \neq k$. This proves $f(x)$ is a monomial and so $f(x) = cx^n$ for some $1 \leq n \leq q-1$. Clearly $c \neq 0$ since $f \equiv 0$ is not bijective. We conclude that $\gcd(n, q-1) = 1$ by Theorem 2.2(2).

(3) $\implies$ (1). Suppose (3) holds and let

$$A = \begin{pmatrix} u & v \\ v & w \end{pmatrix}$$

be an arbitrary positive definite matrix in $M_2(\mathbb{F}_q)$, i.e., $u \neq 0$ and $uw \neq v^2$. Clearly, $f(u) = cu^n \neq 0$. Moreover, since $x \mapsto x^n$ is injective on $\mathbb{F}_q$, we have $u^n w^n \neq v^{2n}$ and so

$$\det f[A] = c^2 u^n w^n - c^2 v^{2n} \neq 0.$$

This proves f preserves positivity on $M_2(\mathbb{F}_q)$ and so (1) holds. This concludes the proof. □

We now describe the entrywise positivity preservers on $M_3(\mathbb{F}_q)$.

Theorem 3.2. *Let $q = 2^k$ and let $f : \mathbb{F}_q \to \mathbb{F}_q$. Then the following are equivalent:*

1. *f preserves positivity on $M_3(\mathbb{F}_q)$.*
2. *There exist $c \in \mathbb{F}_q^*$ and $0 \leq \ell \leq k-1$ such that $f(x) = cx^{2^\ell}$ for all $x \in \mathbb{F}_q$.*

Proof. That (2) $\implies$ (1) follows from Proposition 2.16. Now, suppose (1) holds. By embedding 2×2 positive definite matrices A into $M_3(\mathbb{F}_q)$ via

$$\begin{pmatrix} A & \mathbf{0}_{2\times 1} \\ \mathbf{0}_{1\times 2} & 1 \end{pmatrix} \in M_3(\mathbb{F}_q),$$

it follows by Theorem 3.1 that $f(x) = cx^n$ for all $x \in \mathbb{F}_q$, where $c \in \mathbb{F}_q^*$ and $1 \leq n \leq q-1$ is such that $\gcd(n, q-1) = 1$. Without loss of generality we assume that $c = 1$. It suffices to show that the only exponents n that preserve positivity on $M_3(\mathbb{F}_q)$ are powers of 2.

For $x, y \in \mathbb{F}_q$, let

$$A(x,y) = \begin{pmatrix} 1 & x & y \\ x & 1 & 0 \\ y & 0 & 1 \end{pmatrix}.$$

The matrix $A(x,y)$ is positive definite if and only if $x \neq 1$ and $\det A = 1 - x^2 - y^2 \neq 0$. Notice that, using the fact that $-1 = 1$ in $\mathbb{F}_q$,

$$\det A(x,y) = 0 \iff x^2 + y^2 = 1 \iff (x+y)^2 = 1 \iff x + y = 1.$$

Similarly, $\det f[A] = 1 - x^{2n} - y^{2n}$ and so

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

Suppose n is not a power of 2. We will prove that there exist $x_0, y_0 \in \mathbb{F}_q$ such that $A(x_0, y_0)$ is positive definite, but $f[A(x_0, y_0)]$ is not positive definite. In order to do so, we will prove the existence of $x_0, y_0 \in \mathbb{F}_q$ such that

(1) $x_0 \neq 1$,
(2) $x_0 + y_0 \neq 1$, and
(3) $x_0^n + y_0^n = 1$.

Indeed, consider the two sets:

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

Clearly, $|S_1| = q$ since for every $x \in \mathbb{F}_q$, there is a unique $y \in \mathbb{F}_q$ such that $x + y = 1$. We claim that $|S_2| = q$ as well. To see why, recall that the map $x \mapsto x^n$ is a bijection since $\gcd(n, q-1) = 1$ (Theorem 2.2(2)). For any $a \in \mathbb{F}_q$, denote by $\sqrt[n]{a}$ the unique element $z \in \mathbb{F}_q$ such that $z^n = a$. Then, for any $x \in \mathbb{F}_q$, there is a unique $y \in \mathbb{F}_q$ such that $x^n + y^n = 1$, namely, $y = \sqrt[n]{1 - x^n}$. It follows that $|S_2| = q$. Now, suppose the desired pair x_0, y_0 does not exist. Then for every $(x,y) \in S_2$, either $x = 1$ or $x + y = 1$. But if $x = 1$ then $y = 0$ (since $(x,y) \in S_2$) and so $x + y = 1$. In all cases, $(x,y) \in S_1$ and it follows that $S_2 \subseteq S_1$. Since the two sets have the same cardinality, we conclude that $S_1 = S_2$. Thus,

$$x^n + y^n = 1 \iff x + y = 1.$$

We claim that this implies $(x+y)^n = x^n + y^n$ for all $x, y \in \mathbb{F}_q$. Indeed, let $x, y \in \mathbb{F}_q$ and assume $x^n + y^n = c$ for some $c \in \mathbb{F}_q$. If $c = 0$, then $x^n = -y^n = y^n$ since $-1 = 1$ in characteristic 2, and it follows that $x = y$. Thus $(x+y)^n = (x+x)^n = 0^n = 0$ and $x^n + y^n = x^n + x^n = 0$ as well. Thus, $(x+y)^n = x^n + y^n$. If $c \neq 0$, then

$$\left(\frac{x}{\sqrt[n]{c}}\right)^n + \left(\frac{y}{\sqrt[n]{c}}\right)^n = 1$$

and so

$$\frac{x}{\sqrt[n]{c}} + \frac{y}{\sqrt[n]{c}} = 1$$

by assumption. Hence $x + y = \sqrt[n]{c}$ and so $x^n + y^n = c = (x+y)^n$. This proves the map $f(x) = x^n$ is an automorphism of $\mathbb{F}_q$. By Theorem 2.1, we therefore must have $n \equiv 2^\ell \pmod{q-1}$ for some ℓ. This is impossible since $1 \leq n \leq q-1$ and n is not a power of 2. We therefore conclude that there exists $x_0 \neq 1$ such that $x_0 + y_0 \neq 1$ and $x_0^n + y_0^n = 1$. This proves (1) $\implies$ (2). $\square$

Using Theorem 3.1 and 3.2, we immediately obtain Theorem A.

Proof of Theorem A. The $n = 2$ case is exactly Theorem 3.1. Consider now the $n \geq 3$ case. Clearly (b) $\implies$ (a). Suppose (a) holds. If $n > 3$, then using matrices of the form $A \oplus I_{n-3}$ with $A \in M_3(\mathbb{F}_q)$, we conclude that f preserves positivity on $M_3(\mathbb{F}_q)$. Theorem 3.2 then implies that (c) holds. The (c) $\implies$ (b) implication is Proposition 2.16. $\square$

4. Odd characteristic: $q \equiv 3 \pmod 4$

We now move to the case where $q \equiv 3 \pmod 4$. Equivalently, we assume $-1 \notin \mathbb{F}_q^+$. We break down the proof of Theorem B into several lemmas. Interestingly, the $n = 2$ case of the theorem is considerably more difficult to prove as very little structure is available to work with. Most of the results below rely on indirect combinatorial arguments to obtain relevant properties of the preservers. When $n \geq 3$, although the result follows from the $n = 2$ case, the supplementary structure of 3×3 matrices can be used to give a shorter proof of the theorem. We first show how to obtain the $n = 2$ case, and then explain how a simpler approach can be used to deduce the $n \geq 3$ case.

Theorem 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 $\mathbb{F}_q$).*

Proof. By Lemma 2.17, the function f satisfies $f(0) = 0$ and its restriction to $\mathbb{F}_q^+$ is a bijection onto $\mathbb{F}_q^+$. We will conclude the proof by proving that $f(-\mathbb{F}_q^+) \subseteq -\mathbb{F}_q^+$ and that f is injective on $-\mathbb{F}_q^+$.

Step 1: $f(-\mathbb{F}_q^+) \subseteq -\mathbb{F}_q^+$. Suppose for a contradiction that $f(-b) \in \mathbb{F}_q^+$ for some $b \in \mathbb{F}_q^+$. Since f is bijective from $\mathbb{F}_q^+$ onto itself, $f(-b) = f(a)$ for some $a \in \mathbb{F}_q^+$. Let $y := f(a) = f(-b)$. For $x \in \mathbb{F}_q^+$, consider the matrix

$$A(x) = \begin{pmatrix} x & a \\ a & -b \end{pmatrix}.$$

Observe that $\det f[A(x)] = f(x)f(-b) - f(a)^2 = y\,(f(x) - y)$. Since $y = f(a) \in \mathbb{F}_q^+$, it follows that

$$f[A(x)] \text{ is positive definite } \iff f(x) - y \in \mathbb{F}_q^+.$$

Define

$$L := \{x \in \mathbb{F}_q^+ : f(x) - y \in \mathbb{F}_q^+\}.$$

Since f is bijective on $\mathbb{F}_q^+$, by Lemma 2.18, we have $|L| = \frac{q-3}{4}$. Now, let

$$M_A := \{x \in \mathbb{F}_q^+ : -bx - a^2 \in \mathbb{F}_q^+\}.$$

Observe that

$$A(x) \text{ is positive definite } \iff x \in M_A.$$

We claim $|M_A| = \frac{q+1}{4} > \frac{q-3}{4}$. Indeed,

$$\begin{aligned} x \in M_A &\iff x \in \mathbb{F}_q^+ \text{ and } -bx - a^2 \in \mathbb{F}_q^+ \\ &\iff x \in \mathbb{F}_q^+ \text{ and } -x - a^2b^{-1} \in \mathbb{F}_q^+ \\ &\iff x \in \mathbb{F}_q^+ \text{ and } x + a^2b^{-1} \in -\mathbb{F}_q^+. \end{aligned}$$

Using Lemma 2.18 again, the cardinality of the set

$$S := \{x \in \mathbb{F}_q^+ : x + a^2b^{-1} \in \mathbb{F}_q^+\}$$

is $|S| = \frac{q-3}{4}$. Observe that $x + a^2b^{-1} = 0$ implies $x = -a^2b^{-1} \in -\mathbb{F}_q^+$. It follows that $M_A = \mathbb{F}_q^+ \setminus S$ and so

$$|M_A| = \frac{q-1}{2} - \frac{q-3}{4} = \frac{q+1}{4}.$$

Therefore, there exists $x^* \in M_A$ such that $x^* \notin L$. Thus, $A(x^*)$ is positive definite, but $f[A(x^*)]$ is not positive definite, contradicting the assumption of the theorem. We therefore conclude that

$f(-\mathbb{F}_q^+) \subseteq -\mathbb{F}_q^+ \cup \{0\}$. Finally, suppose $f(-b) = 0$ for some $b \in \mathbb{F}_q^+$. Taking any $x \in M_A$, we have that $A(x)$ is positive definite, but

$$\det f[A(x)] = \det \begin{pmatrix} f(x) & f(a) \\ f(a) & 0 \end{pmatrix} = -f(a)^2 \notin \mathbb{F}_q^+.$$

We therefore conclude that $f(-b) \neq 0$ and so $f(-\mathbb{F}_q^+) \subseteq -\mathbb{F}_q^+$.

Step 2: f is injective on $-\mathbb{F}_q^+$. Suppose $f(-a) = f(-b) =: y$ for some $a, b \in \mathbb{F}_q^+$ with $a \neq b$. Notice that $y \in -\mathbb{F}_q^+$ by Step 1. Thus $-y \in \mathbb{F}_q^+$ and so there exists $\alpha \in \mathbb{F}_q^+$ such that $f(\alpha) = -y$. Consider the matrices

$$A(x) = \begin{pmatrix} x & -a \\ -a & \alpha \end{pmatrix}, \qquad B(x) = \begin{pmatrix} x & -b \\ -b & \alpha \end{pmatrix}.$$

Let

$$M_A := \{x \in \mathbb{F}_q^+ : \alpha x - a^2 \in \mathbb{F}_q^+\},$$
$$M_B := \{x \in \mathbb{F}_q^+ : \alpha x - b^2 \in \mathbb{F}_q^+\}.$$

Clearly, $A(x)$ is positive definite if and only if $x \in M_A$ and $B(x)$ is positive definite if and only if $x \in M_B$. Also,

$$\det f[A(x)] = \det f[B(x)] = -y(f(x) + y).$$

Since $-y \in \mathbb{F}_q^+$, the matrices $f[A(x)]$ and $f[B(x)]$ are positive definite if and only if $x \in \mathbb{F}_q^+$ and $f(x) + y \in \mathbb{F}_q^+$. Using Lemma 2.18,

$$|\{x \in \mathbb{F}_q^+ : f(x) + y\}| = \frac{q-3}{4}.$$

We will now prove that $|M_A \cup M_B| > \frac{q-3}{4}$. First, notice that

$$x \in M_A \iff x, x - a^2\alpha^{-1} \in \mathbb{F}_q^+.$$

Thus, by Lemma 2.18, we have $|M_A| = \frac{q-3}{4}$. Similarly, $|M_B| = \frac{q-3}{4}$. To prove that $|M_A \cup M_B| > \frac{q-3}{4}$, it therefore suffices to show $|M_A \cap M_B| < \frac{q-3}{4}$. Let $s := a^2\alpha^{-1}$ and $t := b^2\alpha^{-1}$. Then $s, t \in \mathbb{F}_q^+$ and

$$|M_A \cap M_B| = \sum_{c \in \mathbb{F}_q \setminus \{0,s,t\}} \frac{\eta(c)+1}{2} \cdot \frac{\eta(c-s)+1}{2} \cdot \frac{\eta(c-t)+1}{2}.$$

Thus,

$$\begin{aligned} 8|M_A \cap M_B| = \sum_{c \in \mathbb{F}_q \setminus \{0,s,t\}} & [\eta(c)\eta(c-s)\eta(c-t) + \eta(c)\eta(c-s) \\ & + \eta(c)\eta(c-t) + \eta(c) + \eta(c-s)\eta(c-t) + \eta(c-s) + \eta(c-t) + 1]. \end{aligned}$$

We examine each term separately. First, using Weil's bound (Theorem 2.4),

$$\sum_{c \in \mathbb{F}_q \setminus \{0,s,t\}} \eta(c)\eta(c-s)\eta(c-t) = \sum_{c \in \mathbb{F}_q} \eta(c)\eta(c-s)\eta(c-t) \leq 2\sqrt{q}.$$

Next,

$$\begin{aligned} \sum_{c \in \mathbb{F}_q \setminus \{0,s,t\}} \eta(c)\eta(c-s) &= \sum_{c \in \mathbb{F}_q \setminus \{0,s,t\}} \eta(c^{-1})\eta(c-s) = \sum_{c \in \mathbb{F}_q \setminus \{0,s,t\}} \eta(1-sc^{-1}) = \sum_{\gamma \in \mathbb{F}_q \setminus \{1,0,1-st^{-1}\}} \eta(\gamma) \\ &= -1 - \eta(1-st^{-1}) \\ &= -1 - \eta(t-s) \end{aligned}$$

since $t \in \mathbb{F}_q^+$. Similarly,

$$\sum_{c\in\mathbb{F}_q\setminus\{0,s,t\}} \eta(c)\eta(c-t) = -1-\eta(s-t) = -1+\eta(t-s).$$

Next,

$$\sum_{c\in\mathbb{F}_q\setminus\{0,s,t\}} \eta(c) = -\eta(s)-\eta(t)+\sum_{c\in\mathbb{F}_q}\eta(c) = -2$$

since $s,t \in \mathbb{F}_q^+$. For the next term, setting $y = c-s$ yields

$$\begin{aligned}\sum_{c\in\mathbb{F}_q\setminus\{0,s,t\}} \eta(c-s)\eta(c-t) &= \sum_{y\in\mathbb{F}_q\setminus\{-s,0,t-s\}} \eta(y)\eta(y+s-t) = \sum_{y\in\mathbb{F}_q\setminus\{-s,0,t-s\}} \eta(y^{-1})\eta(y+s-t)\\ &= \sum_{y\in\mathbb{F}_q\setminus\{-s,0,t-s\}} \eta(1+(s-t)y^{-1})\\ &= -\eta(ts^{-1})-\eta(1)-\eta(0)+\sum_{\gamma\in\mathbb{F}_q}\eta(\gamma)\\ &= -2.\end{aligned}$$

Finally,

$$\sum_{c\in\mathbb{F}_q\setminus\{0,s,t\}} \eta(c-s) = -\eta(-s)-\eta(0)-\eta(t-s)+\sum_{c\in\mathbb{F}_q}\eta(c) = 1-\eta(t-s)$$

and similarly,

$$\sum_{c\in\mathbb{F}_q\setminus\{0,s,t\}} \eta(c-t) = 1-\eta(s-t) = 1+\eta(t-s).$$

Combining all the above, we obtain

$$\begin{aligned}8|M_A\cap M_B| &\leq 2\sqrt{q}-1-\eta(t-s)-1+\eta(t-s)-2-2+1-\eta(t-s)+1+\eta(t-s)+q-3\\ &= 2\sqrt{q}+q-7.\end{aligned}$$

Now,

$$2\sqrt{q}+q-7 < 8\cdot\frac{q-3}{4} = 2q-6 \iff q+1-2\sqrt{q} = (\sqrt{q}-1)^2 > 0,$$

which holds for $q>1$. This proves $|M_A\cup M_B| > \frac{q-3}{4}$. As a consequence, there exists $x^* \in M_A\cup M_B$ such that $f(x)+y \notin \mathbb{F}_q^+$. For such an x^* we have either $A(x^*)$ is positive definite, but $f[(A(x^*)]$ is not or $B(x^*)$ is positive definite, but $f[B(x^*)]$ is not. This contradicts our assumption and therefore proves that f is bijective on $-\mathbb{F}_q^+$. This concludes the proof. ☐

As a consequence of Theorem 4.1, even functions cannot preserve positivity. Formally:

Corollary 4.2. *Let $\mathbb{F}_q$ be a finite field with $q\equiv 3 \pmod 4$. If $f:\mathbb{F}_q\to\mathbb{F}_q$ is an even function then it does not preserve positive definiteness on $M_2(\mathbb{F}_q)$.*

We next show that the positivity preservers over $M_2(\mathbb{F}_q)$ are necessarily odd functions.

Lemma 4.3. *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 $M_2(\mathbb{F}_q)$. Then f is odd.*

Proof. Fix $x\in\mathbb{F}_q^+$ and let

$$g(y) := f(x)f(y)-f(-x)^2 \qquad (y\in\mathbb{F}_q).$$

By Theorem 4.1, f is bijective on $\mathbb{F}_q$. It follows that g is bijective on $\mathbb{F}_q$ as well. Thus, there exists y^* such that $g(y^*)=0$, i.e.,

$$g(y^*) = f(x)f(y^*)-f(-x)^2 = 0 \iff f(y^*) = f(-x)^2 f(x)^{-1}. \tag{4.1}$$

Using Theorem 4.1 we have that $f(x) \in \mathbb{F}_q^+$, which in turn implies that $f(y^*) \in \mathbb{F}_q^+$. Applying Theorem 4.1, we conclude that $y^* \in \mathbb{F}_q^+$. Now, consider

$$A = \begin{pmatrix} y^* & -x \\ -x & x \end{pmatrix}.$$

Since $x, y^* \in \mathbb{F}_q^+$, the matrix A is positive definite if and only if $xy^* - x^2 = x(y^* - x) \in \mathbb{F}_q^+$ which happens if and only if $y^* - x \in \mathbb{F}_q^+$. Since f is bijective on $\mathbb{F}_q$, its entrywise action on $M_2(\mathbb{F}_q)$ is also bijective. Thus, since

$$\det f[A] = f(x)f(y^*) - f(-x)^2 = 0,$$

and since $f[-]$ maps positive definite matrices bijectively onto themselves, the matrix A cannot be positive definite. We conclude that either $y^* - x = 0$ or $x - y^* \in \mathbb{F}_q^+$. In the first case, we have

$$0 = f(x)^2 - f(-x)^2 = (f(x) - f(-x))\,(f(x) + f(-x)).$$

It follows that $f(x) = -f(-x)$ or $f(x) = f(-x)$. The second choice here is not possible by Theorem 4.1 and so we conclude that $f(x) = -f(-x)$ for all $x \in \mathbb{F}_q^+$. The same holds for $x = 0$ since $f(0) = 0$ (Theorem 4.1) and for $x \in -\mathbb{F}_q^+$ by symmetry of the expression. Thus f is odd.

Suppose instead that $x - y^* \in \mathbb{F}_q^+$. Consider the matrix

$$B = \begin{pmatrix} x & y^* \\ y^* & y^* \end{pmatrix}.$$

By assumption, $x \in \mathbb{F}_q^+$ and we have

$$\det B = xy^* - (y^*)^2 = y^*(x - y^*) \in \mathbb{F}_q^+.$$

Thus B is positive definite and so

$$\det f[B] = f(x)f(y^*) - f(y^*)^2 \in \mathbb{F}_q^+.$$

Using Equation (4.1), we obtain

$$\det f[B] = f(x)f(y^*) - f(y^*)^2 = f(-x)^2 - f(-x)^4 f(x)^{-2} \in \mathbb{F}_q^+.$$

It follows that $1 - f(-x)^2 f(x)^{-2} \in \mathbb{F}_q^+$ and so $f(x)^2 - f(-x)^2 \in \mathbb{F}_q^+$. Now, consider

$$C = \begin{pmatrix} x & -x \\ -x & x \end{pmatrix}.$$

Then $f(x) \in \mathbb{F}_q^+$ and $\det f[C] = f(x)^2 - f(-x)^2 \in \mathbb{F}_q^+$. Thus $f[C]$ is positive definite. Using the same reasoning as in the $y^* = x$ case above, the matrix C needs to be positive definite. This is a contradiction since C is singular. We conclude that $y^* = x$ and therefore f must be odd. $\square$

Lemma 4.4. *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 $f(x^2) = f(x)^2$ for all $x \in \mathbb{F}_q$.*

Proof. Clearly, the conclusion holds when $x = 0$ since $f(0) = 0$ (Theorem 4.1). Also, notice that it suffices to prove the result for $x \in \mathbb{F}_q^+$ since $f(-x)^2 = (-f(x))^2 = f(x)^2$ by Lemma 4.3.

Now, fix $x \in \mathbb{F}_q^+$ and consider the function

$$g(y) := f(x^2)f(y) - f(x)^2.$$

Since f is bijective (Theorem 4.1), so is g. Thus, there exists $y^* \in \mathbb{F}_q$ such that

$$g(y^*) = f(x^2)f(y^*) - f(x)^2 = 0,$$

i.e.,

$$f(y^*) = f(x)^2 f(x^2)^{-1}. \tag{4.2}$$

Therefore $f(y^*) \in \mathbb{F}_q^+$ and so $y^* \in \mathbb{F}_q^+$ by Theorem 4.1. We will prove $y^* = 1$. Indeed, consider the matrix

$$A = \begin{pmatrix} x^2 & x \\ x & y^* \end{pmatrix}.$$

We have $\det f[A] = f(x^2)f(y^*) - f(x)^2 = 0$. It follows that A is not positive definite since f preserves positivity on $M_2(\mathbb{F}_q)$ by assumption. Thus, $x^2y^* - x^2 = x^2(y^* - 1) \notin \mathbb{F}_q^+$ and so either $y^* = 1$ or $1 - y^* \in \mathbb{F}_q^+$. If $y^* = 1$ we are done. Suppose for a contradiction that we instead have $1 - y^* \in \mathbb{F}_q^+$. Let

$$B = \begin{pmatrix} 1 & y^* \\ y^* & y^* \end{pmatrix}.$$

Then $\det B = y^* - (y^*)^2 = y^*(1-y^*) \in \mathbb{F}_q^+$ and so B is positive definite. Since f preserves positivity on $M_2(\mathbb{F}_q)$, the matrix $f[B]$ is positive definite and so

$$\det f[B] = f(1)f(y^*) - f(y^*)^2 \in \mathbb{F}_q^+.$$

Using Equation (4.2) and the $f(1) = 1$ assumption, we obtain

$$f(y^*) - f(y^*)^2 = f(x)^2 f(x^2)^{-1} - f(x)^4 f(x^2)^{-2} \in \mathbb{F}_q^+.$$

Equivalently, $1 - f(x)^2 f(x^2)^{-1} \in \mathbb{F}_q^+$. Since $f(x^2) \in \mathbb{F}_q^+$ (Theorem 4.1), it follows that $f(x^2) - f(x)^2 \in \mathbb{F}_q^+$. Now, consider the matrix

$$C = \begin{pmatrix} x^2 & x \\ x & 1 \end{pmatrix}.$$

We have $f(x^2) \in \mathbb{F}_q^+$ and $\det f[C] = f(x^2) - f(x)^2 \in \mathbb{F}_q^+$. Thus $f[C]$ is positive definite. But since f is bijective on $\mathbb{F}_q$, its entrywise action on $M_2(\mathbb{F}_q)$ is also bijective and maps positive definite matrices onto themselves. Since C is singular, the matrix $f[C]$ cannot be positive definite, a contradiction. We therefore conclude that $y^* = 1$ and so $f(x^2) = f(x)^2$. □

With the above preliminary results in hand, we can now prove the main result of this section, which immediately implies Theorem B.

Theorem 4.5. *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 $f(x) = x^{p^\ell}$ for some $\ell = 0, 1, \ldots, k-1$.*

Proof. First notice that by Lemma 4.3, $f(-a) = -f(a)$ for all $a \in \mathbb{F}_q$. We will now show that $\eta(a - b) = \eta(f(a) - f(b))$ for all $a, b \in \mathbb{F}_q$. This is clear when $a = 0$ or $b = 0$ since by Theorem 4.1, we have $\eta(c) = \eta(f(c))$ for all $c \in \mathbb{F}_q$. Let us consider the remaining cases as follows.

Case 1: Let $\eta(a) = \pm 1$, $\eta(b) = 1$, and $\eta(a - b) = 1$. Consider the positive definite matrix $A = \begin{pmatrix} b & b \\ b & a \end{pmatrix}$. Then $f[A] = \begin{pmatrix} f(b) & f(b) \\ f(b) & f(a) \end{pmatrix}$ is also positive definite, which implies that $\eta(f(a) - f(b)) = 1$.

Case 2: Let $\eta(a) = 1$, $\eta(b) = \pm 1$, and $\eta(a - b) = -1$. Consider the positive definite matrix $A = \begin{pmatrix} a & a \\ a & b \end{pmatrix}$. Then $f[A] = \begin{pmatrix} f(a) & f(a) \\ f(a) & f(b) \end{pmatrix}$ is also positive definite, which implies that $\eta(f(b) - f(a)) = 1$, and hence, $\eta(f(a) - f(b)) = -1$.

Case 3: Let $\eta(a) = -1$, $\eta(b) = -1$, and $\eta(a - b) = -1$. Consider $a' = -a$, $b' = -b$, and $a' - b' = (-a) - (-b)$. Note that $\eta(a') = 1$, $\eta(b') = 1$, and $\eta(a' - b') = 1$. According to Case 1 above and since f is odd, we have $-1 = -\eta(f(a') - f(b')) = -\eta(f(-a) - f(-b)) = -\eta(-f(a) + f(b)) = \eta(f(a) - f(b))$.

Case 4: Let $\eta(a) = -1$, $\eta(b) = -1$, and $\eta(a-b) = 1$. Consider $a' = -a$, $b' = -b$, and $a' - b' = (-a) - (-b)$. Note that $\eta(a') = 1$, $\eta(b') = 1$, and $\eta(a' - b') = -1$. According to Case 2 above and since f is odd, we have $1 = -\eta(f(a') - f(b')) = -\eta(f(-a) - f(-b)) = -\eta(-f(a) + f(b)) = \eta(f(a) - f(b))$.

Case 5: Let $\eta(a) = 1$, $\eta(b) = -1$, and $\eta(a-b) = 1$. Here we use Lemma 4.4 which asserts that f satisfies $f(x^2) = f(x)^2$ for all $x \in \mathbb{F}_q$. Now, consider $a+b$. If $b = -a$, then $1 = \eta(a-b) = \eta(2a) = \eta(a)\eta(2) = \eta(2)$. Hence, since f is odd, we get $\eta(f(a) - f(b)) = \eta(f(a) - f(-a)) = \eta(2f(a)) = \eta(2)\eta(f(a)) = \eta(2) = 1$. If instead $\eta(a+b) = 1$, then $\eta(a^2 - b^2) = \eta((a+b)(a-b)) = 1$. By using Case 1 we have $1 = \eta(f(a) - f(-b)) = \eta(f(a) + f(b))$ and $1 = \eta(f(a^2) - f(b^2)) = \eta(f(a)^2 - f(b)^2)$. Thus, $\eta(f(a) - f(b)) = 1$. Similarly, if $\eta(a+b) = -1$, then $\eta(a^2 - b^2) = \eta((a+b)(a-b)) = -1$. By using Case 2 we have $-1 = \eta(f(a) - f(-b)) = \eta(f(a) + f(b))$ and $-1 = \eta(f(a^2) - f(b^2)) = \eta(f(a)^2 - f(b)^2)$. Thus, $\eta(f(a) - f(b)) = 1$.

Case 6: Let $\eta(a) = -1$, $\eta(b) = 1$, and $\eta(a-b) = -1$. Consider $a' = -a$, $b' = -b$, and $a' - b' = (-a) - (-b)$. Note that $\eta(a') = 1$, $\eta(b') = -1$, and $\eta(a' - b') = 1$. According to Case 5 above and since f is odd, we have $-1 = -\eta(f(a') - f(b')) = -\eta(f(-a) - f(-b)) = -\eta(-f(a) + f(b)) = \eta(f(a) - f(b))$.

Hence, the result follows from Theorem 2.9. □

With the above results in hand, we can now prove Theorem B.

Proof of Theorem B. Suppose (4) holds. Since $c \in \mathbb{F}_q^+$, we have $\eta(ca^{p^l} - cb^{p^l}) = \eta(a^{p^l} - b^{p^l})$ and so we can assume $c = 1$. Next, using the fact that $(a+b)^{p^\ell} = a^{p^\ell} + b^{p^\ell}$ for all $a, b \in \mathbb{F}_q$, we have

$$\eta(a^{p^\ell} - b^{p^\ell}) = \eta((a-b)^{p^\ell}) = \eta(a-b)^{p^\ell} = \eta(a-b)$$

since p is odd. This proves (4) $\implies$ (3). The converse implication is Theorem 2.9 applied to $f(1)^{-1}f$. Thus (3) $\iff$ (4).

That (4) $\implies$ (2) follows from Proposition 2.16 and (2) $\implies$ (1) is trivial. We now prove (1) $\implies$ (4). It suffices to prove the result for $n = 2$. If $n > 2$, then one can embed any 2×2 positive definite matrix A into $M_n(\mathbb{F}_q)$ using a block matrix $A \oplus I_{n-2}$, where I_{n-2} denotes the $(n-2)$-dimensional identity matrix. We therefore assume below that $n = 2$ and f preserves positivity on $M_2(\mathbb{F}_q)$.

Since $f(1) \in \mathbb{F}_q^+$ (Theorem 4.1), replacing f by $f(1)^{-1}f$, we may assume without loss of generality that $f(1) = 1$ and prove that $f(x) = x^{p^\ell}$ for some $0 \leq \ell \leq k-1$. Now, using Lemmas 4.3 and 4.4, f satisfies the assumptions of Theorem 4.5. We immediately conclude that $f(x) = x^{p^\ell}$ for some $0 \leq \ell \leq k-1$, as claimed. □

As explained at the beginning of Section 4, the (1) $\implies$ (4) implication of Theorem B is easier to prove under the assumption that f preserves positivity on $M_3(\mathbb{F}_q)$. In that case, the larger test set of 3×3 matrices makes it easier to deduce the properties of the preservers. We therefore provide a simpler proof of Theorem B below under the assumption that $n \geq 3$ in (1) and (2). The proof avoids using Lemma 4.3, Lemma 4.4, and Theorem 4.5.

Theorem 4.6 (Special Case of Theorem B for $n \geq 3$)**.** *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 $n \geq 3$.*
2. *f preserves 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 $x \in \mathbb{F}_q$.*

Proof. We only prove (1) $\implies$ (3). The other implications are proved as in the proof of Theorem B.

Without loss of generality, we assume $f(1) = 1$. Suppose (1) holds. Without loss of generality, we can assume $n = 3$ (the general case follows by embedding 3×3 positive definite matrices into larger matrices of the form $A \oplus I_{n-3}$). By Lemma 2.17(2) we have $f(0) = 0$. 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 $b = 0$. Then $\eta(a) = 1$, and therefore by using Lemma 2.17(1) we have $\eta(f(a) - f(0)) = \eta(f(a)) = 1$.

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,

$$f[A] = \begin{pmatrix} f(b) & f(b) & 0 \\ f(b) & f(a) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is also positive definite. Note that $\det f[A] = f(b)(f(a) - f(b))$. Thus, $\eta(f(a) - f(b)) = 1$ since $\eta(f(b)) = 1$.

Case 3: Assume $\eta(b) = -1$. Consider the linear map $g : \mathbb{F}_q \to \mathbb{F}_q$ as $g(x) = x + b$. Note that g is bijective (Theorem 2.2(1)), $g(0) = b$ and $g(-b) = 0$. Thus, there must exist x_0 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

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

is positive definite. Hence,

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

is also positive definite. Note that $\det f[A] = f(c)(f(b) - f(c))(f(a) - f(b))$. 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, $\eta(f(a) - f(b)) = 1$.

On the other hand, 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. □

5. Odd characteristic: $q \equiv 1 \pmod 4$

We now address the case where $q \equiv 1 \pmod 4$ and prove Theorem C. We start with two lemmas that will be useful in the proof.

Lemma 5.1. *Let $\mathbb{F}_q$ be a finite field with $q \equiv 1 \pmod 4$. Let $a \in \mathbb{F}_q$ such that $\eta(a) \in \{0, -1\}$. Then there exists $c \in \mathbb{F}_q$ such that $\eta(c) = 1$ and $\eta(a - c) = 1$.*

Proof. If $\eta(a) = 0$, then any $c \in \mathbb{F}_q^+$ works since $-1 \in \mathbb{F}_q^+$. If $\eta(a) = -1$, then we consider the linear map $g : \mathbb{F}_q \to \mathbb{F}_q$ as $g(x) = a - x$. Note that g is bijective (Theorem 2.2(1)), $g(0) = a$ and $g(a) = 0$. Thus, there must exist c such that $\eta(c) = 1$ and $\eta(g(c)) = \eta(a - c) = 1$. □

Lemma 5.2. *Let $\mathbb{F}_q$ be a finite field with $q \equiv 1 \pmod 4$. Let $a, b \in \mathbb{F}_q$ such that $a \neq b$, $\eta(a) = 1$ and $\eta(b) \in \{0, 1\}$. Then there exists $c \in \mathbb{F}_q$ such that $\eta(c) = -1$, $\eta(a-c) = 1$, and $\eta(b-c) = -1$. Consequently, if $a \neq b$ with $\eta(a) = -1$ and $\eta(b) \in \{0, -1\}$, then there exists $c \in \mathbb{F}_q$ with $\eta(c) = 1$ such that $\eta(c-a) = -1$ and $\eta(c-b) = 1$.*

We provide two proofs of Lemma 5.2: one using character sums and Weil's bound (Theorem 2.4) and one using properties of Paley graphs. Both proofs are of independent interest.

Proof of Lemma 5.2 (using character sums). Suppose first that $\eta(b) = 0$. Pick $\omega \in \mathbb{F}_q$ with $\eta(\omega) = -1$ and consider the map $g(x) := a^{-1}x - \omega$ for $x \in \mathbb{F}_q$. Note that $g(a\omega) = 0$ and $g(0) = -\omega$. Since g is bijective, there exists $z \in \mathbb{F}_q$ with $\eta(z) = 1$ such that $\eta(g(z)) = \eta(a^{-1}z - \omega) = 1$. This implies $\eta(a - a^2 z^{-1}\omega) = 1$ with $\eta(z) = 1$. Now take $c = a^2 z^{-1}\omega$ to get $\eta(c) = -1$ and $\eta(a-c) = 1$.

Next suppose $a \neq b \in \mathbb{F}_q$ and $\eta(a) = \eta(b) = 1$. Let

$$S := \{c \in \mathbb{F}_q : \eta(c) = -1, \eta(a-c) = 1 \text{ and } \eta(b-c) = -1\}.$$

Then

$$\begin{aligned}|S| &= \sum_{c \in \mathbb{F}_q \setminus \{0,a,b\}} \frac{1-\eta(c)}{2}\frac{1+\eta(a-c)}{2}\frac{1-\eta(b-c)}{2} \\ &= \frac{1}{8}\sum_{c \in \mathbb{F}_q \setminus \{0,a,b\}} \Big(1 - \eta(c) + \eta(a-c) - \eta(b-c) - \eta(c)\eta(a-c) + \eta(c)\eta(b-c) \\ &\qquad\qquad - \eta(a-c)\eta(b-c) + \eta(c)\eta(a-c)\eta(b-c)\Big)\end{aligned}$$

We examine each sum individually:

$$\sum_{c \in \mathbb{F}_q \setminus \{0,a,b\}} \eta(c) = -2.$$

$$\sum_{c \in \mathbb{F}_q \setminus \{0,a,b\}} \eta(a-c) = \sum_{c \in \mathbb{F}_q \setminus \{0,a,b\}} \eta(b-c) = -1 - \eta(a-b).$$

$$\sum_{c \in \mathbb{F}_q \setminus \{0,a,b\}} \eta(c)\eta(a-c) = \sum_{c \in \mathbb{F}_q \setminus \{0,a,b\}} \eta(ac^{-1} - 1) = \sum_{t \in \mathbb{F}_q \setminus \{0, ab^{-1}-1, -1\}} \eta(t) = -1 - \eta(a-b).$$

Similarly,

$$\sum_{c \in \mathbb{F}_q \setminus \{0,a,b\}} \eta(c)\eta(b-c) = -1 - \eta(a-b).$$

Next, setting $y = a - c$, we obtain

$$\begin{aligned}\sum_{c \in \mathbb{F}_q \setminus \{0,a,b\}} \eta(a-c)\eta(b-c) &= \sum_{y \in \mathbb{F}_q \setminus \{a,0,a-b\}} \eta(y)\eta(y+b-a) = \sum_{y \in \mathbb{F}_q \setminus \{a,0,a-b\}} \eta(1 + (b-a)y^{-1}) \\ &= -\eta(1) - \eta(1 + (b-a)a^{-1}) - \eta(0) = -2.\end{aligned}$$

Finally, using Weil's bound (Theorem 2.4) we get

$$\sum_{c \in \mathbb{F}_q \setminus \{0,a,b\}} \eta(c)\eta(a-c)\eta(b-c) \geq -2\sqrt{q}.$$

Therefore,

$$|S| \geq \frac{1}{8}\big(q - 3 + 2 - 1 + 1 + 1 - 1 + 2 - 2\sqrt{q}\big) = \frac{1}{8}\big(q + 1 - 2\sqrt{q}\big) = \frac{1}{8}(\sqrt{q} - 1)^2 \geq 1$$

provided $q \geq 15$. The only remaining case are $q \in \{5, 9, 13\}$. It is not difficult to see that $\mathbb{F}_5^+ = \{1, 4\}$, and when $(a, b) = (1, 4)$, $c = 2$ provides the required solution, and $c = 3$ works for $(a, b) = (4, 1)$. We now deal with the $\mathbb{F}_9$ and $\mathbb{F}_{13}$ cases.

Since $\eta(x) = \eta(-x)$, note that c is such that $\eta(c) = -1$ with $\eta(c - a) = 1$ and $\eta(c - b) = -1$ if and only if $-c$ is such that $\eta(-c) = -1$ with $\eta(-c + a) = 1$ and $\eta(-c + b) = -1$. This means that if c is a solution for the pair (a, b) then $-c$ is a required solution for the inverse pair $(-a, -b)$, and vice versa. This simplifies the resolution of the following cases.

$\mathbb{F}_9$: $\mathbb{F}_9^+ = \{1, 2, x, 2x\}$, where we identify $\mathbb{F}_9 \cong \mathbb{F}_3[x]/(x^2 + 1)$. Using the observation above, we reduce the number of cases into the following:

Case 1: For $a \neq b \in \{1, x\}$, one of $c \in \{x + 2, 2x + 1\}$ provides the solution. This implies that $c \in \{2x + 1, x + 2\}$ provides solutions for $a \neq b \in \{2, 2x\}$.

Case 2: For each $a \neq b \in \{1, 2\}$, one of $c \in \{x+1, 2x+2\}$ works; for each $a \neq b \in \{1, 2x\}$, one of $c \in \{x + 1, 2x + 2\}$ works; for each $a \neq b \in \{x, 2\}$, one of $c \in \{x + 1, 2x + 2\}$ works; for each $a \neq b \in \{2x, x\}$, one of $c \in \{2x + 1, x + 2\}$ works.

$\mathbb{F}_{13}$: $\mathbb{F}_{13}^+ = \{1, 3, 4, 9, 10, 12\}$. Here as well, we use the observation mentioned above to break the cases into the following:

Case 1: $a \neq b \in \{1, 3, 4\}$. For each $a \neq b \in \{1, 3\}$, one of $c \in \{5, 6\}$ works; for each $a \neq b \in \{1, 4\}$ one of $c \in \{2, 8\}$ works; for each $a \neq b \in \{3, 4\}$ one of $c \in \{5, 2\}$ works. This means the required c also exists if $a \neq b \in \{9, 10, 12\}$.

Case 2: $a \in \{1, 3, 4\}$ and $b \in \{9, 10, 12\}$ and vice versa. There are thus nine cases: $\{a, b\} = \{1, 9\}, \ldots, \{4, 12\}$. For each of these cases, the following table gives two values of c, exactly one of which works.

$a \neq b$	c	$a \neq b$	c	$a \neq b$	c
$1, 9$	$2, 8$	$1, 10$	$2, 7$	$1, 12$	$3, 5$
$3, 9$	$2, 5$	$3, 10$	$2, 9$	$3, 12$	$6, 8$
$4, 9$	$6, 7$	$4, 10$	$5, 6$	$4, 12$	$2, 5$

The second statement of the lemma follows by replacing a, b by $\theta a', \theta b'$ respectively, where θ is any element such that $\eta(\theta) = -1$. This completes the proof. $\square$

We now provide our second proof of Lemma 5.2 using a graph theoretic approach.

Proof of Lemma 5.2 (using graph theory). Let us consider the Paley graph $P(q)$ for $q \geq 9$. Note that $N(0) = \mathbb{F}_q^+$ and $N^c(0) = \mathbb{F}_q^* \setminus \mathbb{F}_q^+$. Thus, $a \in N(0)$ and $b \in \{0\} \cup N(0)$. We want to show that there exists $c \in N^c(0)$ such that $c \in N(a)$ but $c \notin N(b)$.

If $b = 0$, then $a \in N(b)$. Thus, by Lemma 2.8 there exists $c \in N(a) \cap N^c(0)$ with the required property. Suppose that $b \neq 0$. Note that $0 \in N(a) \cap N(b)$. So $|N(a) \cap N(b) \cap \mathbb{F}_q^*| = \frac{q-5}{4} - 1 = \frac{q-9}{4} < \frac{q-1}{4}$ or $|N(a) \cap N(b) \cap \mathbb{F}_q^*| = \frac{q-1}{4} - 1 = \frac{q-5}{4} < \frac{q-1}{4}$ depending on whether a, b are adjacent or non-adjacent, respectively. Now, by Lemma 2.8 we have that $|N(a) \cap N^c(0)| = |N(b) \cap N^c(0)| = \frac{q-1}{4}$. Thus, there must exist $c \in N^c(0)$ such that $c \in N(a)$ but $c \notin N(b)$. Note that the lemma is easy to verify by using the Paley graph $P(5)$.

A similar argument works for the second part, that is, if $\eta(a) = \eta(b) = -1$. However, we need to consider the complement graph of $P(q)$ and use the fact that it is isomorphic to $P(q)$ (see e.g. [7, Section 9.1]). $\square$

We next show a partial analogue of Theorem 4.1 in the $q \equiv 1 \pmod 4$ case.

Theorem 5.3. *Let $\mathbb{F}_q$ be a finite field with $q \equiv 1 \pmod 4$ and let f preserves positivity on $M_3(\mathbb{F}_q)$. Then $f(0) = 0$ and f is bijective on $\mathbb{F}_q^+$ and on $\mathbb{F}_q^* \setminus \mathbb{F}_q^+$ (and hence on $\mathbb{F}_q$).*

Proof. We first prove that f is bijective over $\mathbb{F}_q^*$. Let $a, b \in \mathbb{F}_q^*$ with $a \neq b$.

Case 1: Let $\eta(a-b) = 1$. Suppose that at least one of a or b is positive. Since $\eta(b-a) = \eta(a-b) = 1$, we assume without loss of generality that $\eta(a) = 1$. Thus, the matrix

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

is positive definite. Hence,

$$f[A] = \begin{pmatrix} f(a) & f(a) & f(0) \\ f(a) & f(b) & f(0) \\ f(0) & f(0) & f(1) \end{pmatrix}$$

is also positive definite. In particular, examining the leading 2×2 minor of $f[A]$, we conclude that $f(a) \neq f(b)$. Next, assume neither a nor b is positive, i.e., $\eta(a) = \eta(b) = -1$. By Lemma 5.1 there exists $c \in \mathbb{F}_q$ such that $\eta(c) = 1$ and $\eta(a-c) = 1$. Thus, the matrix

$$A := \begin{pmatrix} c & c & c \\ c & a & a \\ c & a & b \end{pmatrix}$$

is positive definite since the leading principal minors $c, c(a-c), c(a-c)(b-a) \in \mathbb{F}_q^+$. Hence, $f[A]$ is also positive definite. In particular, $f(a) \neq f(b)$ (else the last two rows of $f[A]$ would be identical).

Case 2: Let $\eta(a-b) = -1$. Suppose that at least one of a or b is non-zero and non-positive. Since $\eta(b-a) = \eta(a-b) = -1$ we can assume without loss of generality that $\eta(a) = -1$. If $\eta(b) = -1$, then using Lemma 5.2, there exist $c \in \mathbb{F}_q$ such that $\eta(c) = \eta(b-c) = 1$, and $\eta(a-c) = -1$. Therefore the matrix

$$A := \begin{pmatrix} c & c & c \\ c & b & a \\ c & a & a \end{pmatrix}$$

is positive definite since all its leading principal minors $c, c(b-c), c(a-c)(b-a) \in \mathbb{F}_q^+$. It follows that $f[A]$ is positive definite. In particular $f(a) \neq f(b)$. On the other hand if $\eta(b) = 1$, i.e., $\eta(a) = -1 = -\eta(b)$ then using Lemma 5.1 pick $c \in \mathbb{F}_q$ with $\eta(c) = 1$ such that $\eta(a-c) = 1$. Then the matrix

$$A := \begin{pmatrix} b & a & a \\ a & a & a \\ a & a & c \end{pmatrix}$$

is positive definite since all its leading principal minors $b, a(b-a), a(c-a)(b-a) \in \mathbb{F}_q^+$. This implies $f[A]$ is positive definite. In particular, $f(a) \neq f(b)$.

Next, assume $\eta(a) = \eta(b) = 1$. By Lemma 5.2 there exists $c \in \mathbb{F}_q$ such that $\eta(c) = -1$, $\eta(a-c) = 1$, and $\eta(b-c) = -1$. Thus, the matrix

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

is positive definite since the leading principal minors $a, a(c-a), a(b-c)(a-b) \in \mathbb{F}_q^+$. Hence, $f[A]$ is also positive definite. In particular, $f(a) \neq f(b)$. Hence, f is injective over $\mathbb{F}_q^*$.

Since f preserves positivity of matrices of the form aI_3 with $a \in \mathbb{F}_q^+$, we must have $f(\mathbb{F}_q^+) = \mathbb{F}_q^+$. In particular, $f(a) \neq 0$ for all $a \in \mathbb{F}_q^+$. Therefore, if there exists $a \in \mathbb{F}_q$ such that $f(a) = 0$ then $\eta(a) \in \{0, -1\}$. Assume $\eta(a) = -1$. Lemma 5.1 implies that there exists $b \in \mathbb{F}_q$ with $\eta(b) = 1$ such that $\eta(a-b) = 1$. Now using Lemma 5.2 (applied with

$a' = a$ and b' any element such that $\eta(b') = -1$) there exists $c \in \mathbb{F}_q$ such that $\eta(c) = 1$ with $\eta(a-c) = -1$. Consider

$$A := \begin{pmatrix} c & a & a \\ a & a & a \\ a & a & b \end{pmatrix}.$$

The matrix A is positive definite since $c, a(c-a), a(a-b)(a-c) \in \mathbb{F}_q^+$. However

$$f[A] := \begin{pmatrix} f(c) & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & f(b) \end{pmatrix}$$

is not positive definite, a contradiction. Therefore $a = 0$, and f maps $\mathbb{F}_q^* \setminus \mathbb{F}_q^+$ bijectively onto itself, and thus it is bijective over $\mathbb{F}_q^*$.

Now if $\eta(f(0)) = 1$ then there exists $a \in \mathbb{F}_q$ with $\eta(a) = 1$ such that $f(a) = f(0)$. But then $f[aI_3]$ is not positive definite, which is a contradiction. On the other hand if $\eta(f(0)) = -1$, then there exists $a \in \mathbb{F}_q^* \setminus \mathbb{F}_q^+$ such that $f(a) = f(0)$. Now suppose $\omega \in \mathbb{F}_q$ with $\eta(\omega) = -1$, and consider

$$A = \begin{pmatrix} \omega a & a & 0 \\ a & 0 & 0 \\ 0 & 0 & \omega a \end{pmatrix}.$$

The matrix A is positive definite since its leading principal minors $\omega a, -a^2, -\omega a^3 \in \mathbb{F}_q^+$. Therefore

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

is positive definite. However, since $\eta(f(0)) = -1$, $\det f[A] = f(0)(f(\omega a) - f(0))^2 \notin \mathbb{F}_q^+$. This is a contradiction. Hence, $f(0) = 0$. Thus f is bijective, $f(0) = 0$, $f(\mathbb{F}_q^+) = \mathbb{F}_q^+$, and $f(\mathbb{F}_q^* \setminus \mathbb{F}_q^+) = \mathbb{F}_q^* \setminus \mathbb{F}_q^+$.

□

We can now prove Theorem C.

Proof of Theorem C. Assume without loss of generality that $f(1) = 1$. We only prove (1) $\implies$ (3). The other equivalences are proved in the same way as in the proof of Theorem B. Suppose (1) holds. As before, it suffices to assume $n = 3$ as the general case follows by embedding 3×3 matrices into $M_n(\mathbb{F}_q)$. By Theorem 5.3, f is bijective and $f(0) = 0$. If $\eta(a-b) = 0$, then the statement holds trivially. Moreover, if $a = 0$ or $b = 0$, then the statement follows from Theorem 5.3. So we assume that $a, b \in \mathbb{F}_q^*$ with $a \neq b$.

Case 1: Let $\eta(a-b) = 1$. Suppose that at least one of a or b is positive. Since $\eta(b-a) = \eta(a-b) = 1$ we assume without loss of generality that $\eta(a) = 1$. Thus, the matrix

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

is positive definite. Hence,

$$f[A] = \begin{pmatrix} f(a) & f(a) & 0 \\ f(a) & f(b) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is also positive definite. Note that $\det f[A] = f(a)(f(b)-f(a))$. Thus, $\eta(f(a)-f(b)) = \eta(f(b)-f(a)) = 1$ since $\eta(f(a)) = 1$. Now, suppose that $\eta(a) = -1$ and $\eta(b) = -1$. By Lemma 5.1 there exists $c \in \mathbb{F}_q$ such that $\eta(c) = 1$ and $\eta(a-c) = 1$. Thus, the matrix

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

is positive definite since the leading principal minors $c, c(a-c), c(a-c)(b-a) \in \mathbb{F}_q^+$. Hence,

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

is also positive definite. Note that $\det f[A] = f(c)(f(a)-f(c))(f(b)-f(a))$. We have $\eta(f(c)) = 1$ and $\eta(f(a)-f(c)) = 1$ by the previous case. Hence, $\eta(f(a)-f(b)) = \eta(f(b)-f(a)) = 1$.

Case 2: Let $\eta(a-b) = -1$. Suppose that at least one of a or b is non-positive. Since $\eta(b-a) = \eta(a-b) = -1$ we assume without loss of generality $\eta(a) = -1$. Suppose $\eta(b) = 1$, and using Lemma 5.1 pick $c \in \mathbb{F}_q$ with $\eta(c) = 1$ such that $\eta(a-c) = 1$. Then the matrix

$$A := \begin{pmatrix} b & a & a \\ a & a & a \\ a & a & c \end{pmatrix}$$

is positive definite since all its leading principal minors $b, a(b-a), a(c-a)(b-a) \in \mathbb{F}_q^+$. This implies

$$f[A] := \begin{pmatrix} f(b) & f(a) & f(a) \\ f(a) & f(a) & f(a) \\ f(a) & f(a) & f(c) \end{pmatrix}$$

is positive definite. In particular, $\det f[A] = f(a)(f(c)-f(a))(f(b)-f(a)) \in \mathbb{F}_q^+$. By Case 1 above, $\eta(f(c)-f(a)) = 1$, and as f maps non-zero non-positive elements bijectively onto themselves, $\eta(f(a)) = -1$. Therefore, $\eta(f(a)-f(b)) = \eta(f(b)-f(a)) = -1$.

For the other case when $\eta(b) = -1$ (along with $\eta(a) = \eta(a-b) = -1$), using Lemma 5.2 there exists $c \in \mathbb{F}_q$ with $\eta(c) = 1$ with $\eta(a-c) = -1$ and $\eta(b-c) = 1$. Now the matrix

$$A := \begin{pmatrix} c & c & c \\ c & b & a \\ c & a & a \end{pmatrix}$$

is positive definite since its leading principal minors $c, c(b-c), c(a-c)(b-a) \in \mathbb{F}_q^+$. Thus

$$f[A] := \begin{pmatrix} f(c) & f(c) & f(c) \\ f(c) & f(b) & f(a) \\ f(c) & f(a) & f(a) \end{pmatrix}.$$

is positive definite, and $\det f[A] = f(c)(f(a)-f(c))(f(b)-f(a)) \in \mathbb{F}_q^+$. Since f maps $\mathbb{F}_q^+$ onto itself, $\eta(f(c)) = 1$. By the previous case above, $\eta(f(a)-f(c)) = -1$. Therefore $\eta(f(b)-f(a)) = -1$. This concludes the proof when $\eta(a) = -1$ and $\eta(b) = \pm 1$.

Now, suppose that $\eta(a) = 1$ and $\eta(b) = 1$. By Lemma 5.2 there exists $c \in \mathbb{F}_q$ such that $\eta(c) = -1$, $\eta(a-c) = 1$, and $\eta(b-c) = -1$. Thus, the matrix

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

is positive definite since the leading principal minors $a, a(c-a), a(b-c)(a-b) \in \mathbb{F}_q^+$. Hence,

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

is also positive definite. Note that $\det f[A] = f(a)(f(b)-f(c))(f(a)-f(b))$. We have $\eta(f(a)) = 1$ and $\eta(f(b)-f(c)) = -1$ by the previous case. Hence, $\eta(f(a)-f(b)) = -1$.

In all cases, we proved $\eta(f(a)-f(b)) = \eta(a-b)$. The result follows. □

Remark 5.4. The proofs of Theorem 5.3 and Theorem C used Lemmas 5.1 and 5.2. These intermediary results provide a certain $c \in \mathbb{F}_q$ for the given field elements a, b assuming $\eta(a) = \eta(b)$. The following lemma is analogous to Lemma 5.2, but when a and b have opposite signs, i.e., $\eta(a) = -\eta(b)$. This can be applied to resolve some of the cases in the proof of Theorem 5.3 and provide an alternative proof. Its proof is similar to the proof of Lemma 5.2 and is omitted.

Lemma 5.5. *Let $\mathbb{F}_q$ be a finite field with $q \equiv 1 \pmod 4$ and $q \geq 9$. Suppose $s \in \{-1, 1\}$, and let $a, b \in \mathbb{F}_q$ such that $\eta(a) = -1 = -\eta(b)$. Then there exists $c \in \mathbb{F}_q$ such that $\eta(c) = s$, $\eta(a-c) = 1$, and $\eta(b-c) = -1$.*

6. Other results and applications

We now briefly return to the $q \equiv 3 \pmod 4$ case. Recall that by Theorem B, the only power functions $f(x) = x^n$ that preserve positivity on $M_2(\mathbb{F}_q)$ are the field automorphisms $f(x) = x^{p^\ell}$ for some $\leq k-1$. Our proof of Theorem B relied on several lemmas and on Weil's character bound (Theorem 2.4). We now provide an elementary proof for power functions that is of independent interest. The proof only relies on Lucas' Theorem [26], which we now recall.

For $a \in \{1, 2, \dots, q-1\}$, we denote the representation of a in base p by $a := (a_{k-1}, \dots, a_1, a_0)_p$, i.e., $a = a_{k-1}p^{k-1} + \dots + a_1 p + a_0$ where $0 \leq a_i \leq p-1$ for all $i = 0, 1, \dots, k-1$. For any $a, b \in \{1, 2, \dots, q-1\}$ we have $a < b$ if and only if $(a_{k-1}, \dots, a_1, a_0) < (b_{k-1}, \dots, b_1, b_0)$ in the lexicographic order (meaning, for the largest integer s such that $a_s \neq b_s$ we must have $a_s < b_s$). The following classical result of Lucas provides an effective way to evaluate binomial coefficients modulo a prime.

Theorem 6.1 (Lucas [26])**.** *Let $a, b \in \{1, 2, \dots, q-1\}$. Then*

$$\binom{a}{b} \equiv \prod_{i=0}^{k-1} \binom{a_i}{b_i} \pmod p,$$

where, $a = (a_{k-1}, \dots, a_1, a_0)_p$ and $b = (b_{k-1}, \dots, b_1, b_0)_p$. □

We now directly examine the properties of power functions that preserve positivity on $M_2(\mathbb{F}_q)$.

Lemma 6.2. *Let $f(x) = x^n$ for some $n \in \{1, 2, \dots, q-1\}$. If n is even, then $f(x)$ does not preserve positive definiteness on $M_2(\mathbb{F}_q)$.*

Proof. Suppose $f(x)$ preserves positive definiteness on $M_2(\mathbb{F}_q)$. Thus, by Lemma 2.17, $f(x)$ must be bijective on $\mathbb{F}_q^+$ onto itself and $f(0) = 0$. Since $f(x)$ is even it maps $-\mathbb{F}_q^+$ bijectively onto $\mathbb{F}_q^+$. By Lemma 2.18 we have $|G_0 \cap G_{-1}| = \frac{q-3}{4}$ and $|G_0 \cap G_1| = \frac{q-3}{4}$. Let us define $g(x) := x - 1$. Then g is bijective on $\mathbb{F}_q$ (Theorem 2.2(1)) and satisfies $g(0) = -1$, $g(1) = 0$, and $g^{-1}(x) = x + 1$. Therefore, we have

$$|\{z : z \in -\mathbb{F}_q^+ \text{ and } z+1 \in \mathbb{F}_q^+\}| = |\{z : z \in \mathbb{F}_q^+ \text{ and } z-1 \in -\mathbb{F}_q^+\}| = \frac{q-1}{2} - \frac{q-3}{4} - 1 = \frac{q-3}{4},$$

$$|\{z : z \in -\mathbb{F}_q^+ \text{ and } z-1 \in \mathbb{F}_q^+\}| = |\{z : z \in \mathbb{F}_q^+ \text{ and } z+1 \in -\mathbb{F}_q^+\}| = \frac{q-1}{2} - \frac{q-3}{4} = \frac{q+1}{4}.$$

Thus, there exists $z \in \mathbb{F}_q^+$ such that $f(z+1) - 1 \notin \mathbb{F}_q^+$. For such z, the matrix $A = \begin{pmatrix} 1 & 1 \\ 1 & z+1 \end{pmatrix}$ is positive definite but $f[A] = \begin{pmatrix} 1 & 1 \\ 1 & f(z+1) \end{pmatrix}$ is not, a contradiction. This completes the proof. $\square$

Lemma 6.3. *Let $f(x) = x^n$ for some $n \in \{1, 2, \ldots, q-1\}$.*

(1) *If there exists $a \in \mathbb{F}_q$ such that $a - 1$ is positive but $a^n - 1$ is non-positive, then $f(x) = x^n$ does not preserve positive definiteness on $M_2(\mathbb{F}_q)$.*
(2) *If there exists $a \in \mathbb{F}_q$ such that $a - 1$ is non-positive but $a^n - 1$ is positive, then $f(x) = x^n$ does not preserve positive definiteness on $M_2(\mathbb{F}_q)$.*

Proof. By Lemma 6.2, we assume that n is odd. First, suppose (1) holds. Consider the matrix $A = \begin{pmatrix} 1 & 1 \\ 1 & a \end{pmatrix}$. Then A is positive definite, but $f[A] = \begin{pmatrix} 1 & 1 \\ 1 & a^n \end{pmatrix}$ is not. Hence, f does not preserve positive definiteness on $M_2(\mathbb{F}_q)$.

Now, suppose (2) holds. Notice that a is non-zero since $-1 \notin \mathbb{F}_q^+$. Thus, it either belongs to $\mathbb{F}_q^+$ or to $-\mathbb{F}_q^+$.

Case 1: Suppose $a \in \mathbb{F}_q^+$. Then $\sqrt{a}$ exists and consider the matrix $A = \begin{pmatrix} 1 & \sqrt{a} \\ \sqrt{a} & 1 \end{pmatrix}$. Then A is positive definite, but $f[A] = \begin{pmatrix} 1 & (\sqrt{a})^n \\ (\sqrt{a})^n & 1 \end{pmatrix}$ is not.

Case 2: If instead $a \in -\mathbb{F}_q^+$, then consider $\sqrt{-a}$. If $a = -1$, then $a - 1 = -2$ is non-positive but on the other hand $a^n - 1 = -2$ is positive by assumption, which is impossible. Thus $a \neq -1$ and we now consider $a + 1 \neq 0$. Suppose $a + 1 \in \mathbb{F}_q^+$. Consider the matrix $A = \begin{pmatrix} 1 & \sqrt{-a} \\ \sqrt{-a} & 1 \end{pmatrix}$. Then A is positive definite and therefore so is $f[A] = \begin{pmatrix} 1 & (\sqrt{-a})^n \\ (\sqrt{-a})^n & 1 \end{pmatrix}$. Thus, $\det f[A] = a^n + 1$ is positive. Now, $a^2 - 1 = (a-1)(a+1)$ is non-positive and $(a^2)^n - 1 = (a^n - 1)(a^n + 1)$ is positive. Taking $b = a^2$, we have $b \in \mathbb{F}_q^+$, $b - 1 \notin \mathbb{F}_q^+$ and $b^n - 1 \in \mathbb{F}_q^+$. By Case 1 above applied to b, we conclude that f does not preserve positivity. Finally, suppose $a + 1 \in -\mathbb{F}_q^+$. Consider the matrix $A = \begin{pmatrix} \sqrt{-a} & 1 \\ 1 & \sqrt{-a} \end{pmatrix}$. Then A is positive definite and so is $f[A] = \begin{pmatrix} (\sqrt{-a})^n & 1 \\ 1 & (\sqrt{-a})^n \end{pmatrix}$. Thus, $\det f[A] = -(a^n + 1)$ is positive. Hence, $a^2 - 1 = (a-1)(a+1)$ is positive and $(a^2)^n - 1 = (a^n - 1)(a^n + 1)$ is non-positive. Applying (1) to $b = a^2$, we conclude that f does not preserve positive definiteness on $M_2(\mathbb{F}_q)$.

$\square$

Lemma 6.4. *Let $n \in \{1, 2, \ldots, q-1\}$ such that $\gcd(n, q-1) = 1$ and $n \neq p^i$ for any $i = 0, 1, \ldots, k-1$. Then there exists a positive integer $r = r_{k-1}p^{k-1} + \ldots + r_1 p + r_0$, where $0 \leq r_i \leq \frac{p-1}{2}$ for all $0 \leq i \leq k-1$, and such that if $s \equiv nr \pmod{q-1}$, then $\frac{q-1}{2} < s < q-1$.*

Proof. Note that $\frac{q-1}{2} = \left(\frac{p-1}{2}, \ldots, \frac{p-1}{2}, \frac{p-1}{2}\right)_p$. Let $n = (n_{k-1}, \ldots, n_1, n_0)_p$ and $t = \max\{n_i : 0 \leq i \leq k-1\}$. Denote by j the largest integer such that $n_j = t$. Let us consider the following two cases.

Case 1: Suppose $t > 1$. Consider $r_j = \left\lfloor \frac{\frac{p-1}{2}}{t} \right\rfloor + 1$ and $r = r_j p^{k-1-j}$. Then we obtain

$$\begin{aligned} nr &= nr_j p^{k-1-j} \\ &= \left(\sum_{i=0}^{k-1} n_i p^i\right) r_j p^{k-1-j} = \sum_{i=0}^{k-1} n_i r_j p^{k+i-(j+1)} = \sum_{i=0}^{j} n_i r_j p^{k-1-(j-i)} + \sum_{i=j+1}^{k-1} n_i r_j p^{k+i-(j+1)} \\ &= \sum_{i=0}^{j} n_i r_j p^{k-1-(j-i)} + p^k \sum_{i=j+1}^{k-1} n_i r_j p^{i-(j+1)} = \sum_{i=0}^{j} n_i r_j p^{k-1-(j-i)} + q \sum_{\ell=0}^{k-j-2} n_{\ell+j+1} r_j p^{\ell} \\ &= \sum_{i=0}^{j} n_i r_j p^{k-1-(j-i)} + \sum_{\ell=0}^{k-j-2} n_{\ell+j+1} r_j p^{\ell} + (q-1) \sum_{\ell=0}^{k-j-2} n_{\ell+j+1} r_j p^{\ell}. \end{aligned}$$

Letting

$$s = \sum_{i=0}^{j} n_i r_j p^{k-1-(j-i)} + \sum_{\ell=0}^{k-j-2} n_{\ell+j+1} r_j p^{\ell},$$

we have $s \in \{1, \dots, q-1\}$ and $s \equiv nr \pmod{q-1}$. Moreover, the representation of s in base p is $s = (n_j r_j, n_{j-1} r_j, \dots, n_0 r_j, n_{k-1} r_j, n_{k-2} r_j \dots, n_{j+1} r_j)_p$. Note that $1 \leq r_j \leq \frac{p-1}{2}$, $n_j r_j > \frac{p-1}{2}$, and $0 \leq n_i r_j \leq p-1$ for all $i = 0, 1, \dots, k-1$. Also, $s \neq q-1$ since $\gcd(n, q-1) = 1$. It follows that $q - 1 > s > \frac{q-1}{2}$ by using the lexicographic ordering.

Case 2: Now assume $t = 1$. Then $n_i \in \{0, 1\}$ for all $i = 0, 1, \dots, k-1$. Since $n \neq p^i$ for any $i = 0, 1, \dots, k-1$, there exist two distinct integers, say j and ℓ, such that $n_j = n_\ell = 1$. Let $r_j = r_\ell = \frac{p-1}{2}$ and let $r = r_j p^{k-1-j} + r_\ell p^{k-1-\ell}$. By a similar calculation as in the previous case, if $s = (s_{k-1}, \dots, s_1, s_0)_p$ with $s \equiv nr \pmod{q-1}$, then $s_{k-1} = p-1$ and $s_i \in \{0, \frac{p-1}{2}, p-1\}$ for all $i = 0, 1, \dots, k-1$. Since $\gcd(n, q-1) = 1$, $s \neq q-1$ and it follows that $q - 1 > s > \frac{q-1}{2}$ by using the lexicographic ordering. ☐

Let $g(x) = \sum_{i=0}^m a_i x^i$ be a polynomial of degree m in $\mathbb{F}_q[x]$. Suppose $r(x)$ is the remainder obtained from $g(x)$ when dividing it by $x^q - x$. Then g has degree at most $q-1$. We have $g(x) \equiv r(x) \pmod{x^q - x}$. We may avoid long division when dividing a polynomial by $x^q - x$ since $x^q = x$ for all $x \in \mathbb{F}_q$. More precisely, $r(x) = a_0 + \sum_{i=1}^m a_i x^{m \pmod{q-1}}$ with the convention that $m \equiv q-1 \pmod{q-1}$ if $m = s(q-1)$ for $s \neq 0$, instead of $m \equiv 0 \pmod{q-1}$.
Our next lemma is key to characterizing powers that preserve positivity on $M_2(\mathbb{F}_q)$.

Lemma 6.5. *Let $n \in \{1, 2, \dots, q-1\}$ such that $\gcd(n, q-1) = 1$. Define $g(x) = (x^n - 1)^{\frac{q-1}{2}}$ and $h(x) = (x-1)^{\frac{q-1}{2}}$. Then $g(c) = h(c)$ for all $c \in \mathbb{F}_q$ if and only if $n = p^i$ for some $i = 0, 1, \dots, k-1$.*

Proof. Suppose $n = p^i$ for some $i = 0, 1, \dots, k-1$. Then for any $c \in \mathbb{F}_q$ we have

$$g(c) = (c^n - 1)^{\frac{q-1}{2}} = (c^{p^i} - 1)^{\frac{q-1}{2}} = (c-1)^{p^i \cdot \frac{q-1}{2}} = h(c)^{p^i}.$$

So $g(c) = h(c)$ for all $c \in \mathbb{F}_q$ since $g(c), h(c) \in \{-1, 0, 1\}$ and p is odd. Conversely, suppose $n \neq p^i$ for any $i = 0, 1, \dots, k-1$. Note that $\deg(h(x)) \leq \frac{q-1}{2}$. On the other hand, we have

$$\begin{aligned} g(x) = (x^n - 1)^{\frac{q-1}{2}} &= \sum_{r=0}^{\frac{q-1}{2}} (-1)^{\frac{q-1}{2} - r} \binom{\frac{q-1}{2}}{r} x^{nr} \\ &\equiv \left(-1 + \sum_{r=1}^{\frac{q-1}{2}} \left\{ (-1)^{\frac{q-1}{2} - r} \binom{\frac{q-1}{2}}{r} \pmod{p} \right\} x^{nr \pmod{q-1}} \right) \pmod{x^q - x}. \end{aligned}$$

Since $\frac{q-1}{2} = (\frac{p-1}{2}, \ldots, \frac{p-1}{2}, \frac{p-1}{2})_p$, by Lucas's theorem (Theorem 6.1) we have

$$\binom{\frac{q-1}{2}}{r} = \prod_{i=0}^{k-1} \binom{\frac{p-1}{2}}{r_i} \pmod{p}.$$

By Lemma 6.4 we must have $\deg (g(x) \pmod{x^q - x}) > \frac{q-1}{2}$. Thus $g(x) \neq h(x) \pmod{x^q - 1}$. The result now follows from Lemma 2.5. □

An immediate corollary of Lemmas 2.5 and 6.5 is the following:

Corollary 6.6. *Let $n \in \{1, 2, \ldots, q-1\}$ such that $\gcd(n, q-1) = 1$. Then there exists a polynomial $s(x) \in \mathbb{F}_q[x]$ such that $(x^n - 1)^{\frac{q-1}{2}} = s(x)(x^q - x) + (x-1)^{\frac{q-1}{2}}$ if and only if $n = p^i$ for some $i = 0, 1, \ldots, k-1$.*

Finally, we obtain the desired result.

Theorem 6.7. *Let $n \in \{1, 2, \ldots, q-1\}$. Then $f(x) = x^n$ preserves positive definiteness on $M_2(\mathbb{F}_q)$ if and only if $n = p^i$ for some $i = 0, 1, \ldots, k-1$.*

Proof. Suppose $n = p^i$ for some $i = 0, 1, \ldots, k-1$. Then by Proposition 2.16 $f(x) = x^n$ preserves positive definiteness on $M_2(\mathbb{F}_q)$. Conversely, suppose $n \neq p^i$ for any $i = 0, 1, \ldots, k-1$. If n is even, by Lemma 6.2, $f(x) = x^n$ does not preserve positive definiteness on $M_2(\mathbb{F}_q)$. So we assume that n is odd and hence, together with Lemma 2.17, $f(x) = x^n$ must be a bijective map. By Theorem 2.2(2), we must have $\gcd(n, q-1) = 1$. Now, consider the following two functions

$$\begin{aligned} g(x) &= (x^n - 1)^{\frac{q-1}{2}} = \eta(x^n - 1), \\ h(x) &= (x-1)^{\frac{q-1}{2}} = \eta(x-1). \end{aligned}$$

Since $\gcd(n, q-1) = 1$, we have $x^n = 1$ if and only if $x = 1$. If there exists $a \in \mathbb{F}_q \setminus \{1\}$ such that $g(a) \neq h(a)$, then by Lemma 6.3, $f(x) = x^n$ does not preserve positive definiteness on $M_2(\mathbb{F}_q)$. Hence, we assume that $g(c) = h(c)$ for all $c \in \mathbb{F}_q$. But Lemma 6.5 shows that this is impossible, a contradiction. □

7. Conclusion

The astute reader will have noticed that one case was not addressed in the paper: the characterization of entrywise preservers on $M_2(\mathbb{F}_q)$ when $q \equiv 1 \pmod{4}$. While the authors were able to gather evidence that the analogue of Theorem B should hold when $q \equiv 1 \pmod{4}$, our techniques did not allow us to resolve this case. This will be the object of future work.

Acknowledgements. The authors would like to acknowledge the American Institute of Mathematics (CalTech) for their hospitality and stimulating environment during a workshop on Theory and Applications of Total Positivity in July 2023 where authors met and initial discussions occurred. The authors would also like to thank Apoorva Khare for his comments on the paper.

D.G. was partially supported by a Simons Foundation collaboration grant for mathematicians. H.G. and P.K.V. acknowledge support from PIMS (Pacific Institute for the Mathematical Sciences) Postdoctoral Fellowships. P.K.V. was additionally supported by a SwarnaJayanti Fellowship from DST and SERB (Govt. of India), and is moreover thankful to the SPARC travel support (Scheme for Promotion of Academic and Research Collaboration, MHRD, Govt. of India; PI: Tirthankar Bhattacharyya, Indian Institute of Science), and the University of Plymouth (UK) for hosting his visit during part of the research.

References

[1] Alexander Belton, Dominique Guillot, Apoorva Khare, and Mihai Putinar. Matrix positivity preservers in fixed dimension. I. *Adv. Math.*, 298:325–368, 2016.

[2] Alexander Belton, Dominique Guillot, Apoorva Khare, and Mihai Putinar. A panorama of positivity. I: Dimension free. In: Alexandru Aleman, Håkan Hedenmalm, Dmitry Khavinson, and Mihai Putinar, editors, *Analysis of Operators on Function Spaces, The Serguei Shimorin memorial volume*, Trends in Mathematics, pp. 117–165. Birkhauser, Basel, 2019.

[3] Alexander Belton, Dominique Guillot, Apoorva Khare, and Mihai Putinar. A panorama of positivity. II: Fixed dimension. In: Javad Mashreghi, Garth Dales, and Dmitry Khavinson, editors, *Complex Analysis and Spectral Theory: Proceedings of the CRM Workshop held at Laval University, QC, May 21–25, 2018*, CRM Proceedings, AMS Contemporary Mathematics 743, pp. 109–150. American Mathematical Society, Providence, RI, 2020.

[4] Alexander Belton, Dominique Guillot, Apoorva Khare, and Mihai Putinar. Moment-sequence transforms. *J. Eur. Math. Soc.*, 24(9):3109–3160, 2022.

[5] Alexander Belton, Dominique Guillot, Apoorva Khare, and Mihai Putinar. Totally positive kernels, pólya frequency functions, and their transforms. *J. Anal. Math.*, 150(1):83–158, 2023.

[6] Alexander Belton, Dominique Guillot, Apoorva Khare, and Mihai Putinar. Negativity-preserving transforms of tuples of symmetric matrices. *Preprint, arXiv:2310.18041*, 2023.

[7] Andries E. Brouwer and Willem H. Haemers. *Spectra of Graphs*. Springer Science & Business Media, 2011.

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

[9] Joshua Cooper, Erin Hanna, and Hays Whitlatch. Positive-definite matrices over finite fields. *Rocky Mountain J. Math.*, to appear.

[10] Carl H. FitzGerald and Roger A. Horn. On fractional hadamard powers of positive definite matrices. *J. Math. Anal. Appl.*, 61(3):633–642, 1977.

[11] Carl H. FitzGerald, Charles A. Micchelli, and Allan Pinkus. Functions that preserve families of positive semidefinite matrices. *Linear Algebra Appl.*, 221:83–102, 1995.

[12] Dominique Guillot, Apoorva Khare, and Bala Rajaratnam. Complete characterization of hadamard powers preserving Loewner positivity, monotonicity, and convexity. *J. Math. Anal. Appl.*, 425(1):489–507, 2015.

[13] Dominique Guillot, Apoorva Khare, and Bala Rajaratnam. Critical exponents of graphs. *J. Combin. Theory Ser. A*, 139:30–58, 2016.

[14] Dominique Guillot, Apoorva Khare, and Bala Rajaratnam. Preserving positivity for matrices with sparsity constraints. *Trans. Amer. Math. Soc.*, 368(12):8929–8953, 2016.

[15] Dominique Guillot, Apoorva Khare, and Bala Rajaratnam. Preserving positivity for rank-constrained matrices. *Trans. Amer. Math. Soc.*, 369(9):6105–6145, 2017.

[16] Dominique Guillot and Bala Rajaratnam. Retaining positive definiteness in thresholded matrices. *Linear Algebra Appl.*, 436(11):4143–4160, 2012.

[17] Dominique Guillot and Bala Rajaratnam. Functions preserving positive definiteness for sparse matrices. *Trans. Amer. Math. Soc.*, 367(1):627–649, 2015.

[18] Fumio Hiai. Monotonicity for entrywise functions of matrices. *Linear Algebra Appl.*, 431(8):1125–1146, 2009.

[19] Roger A. Horn. The theory of infinitely divisible matrices and kernels. *Trans. Amer. Math. Soc.*, 136:269–286, 1969.

[20] Roger A. Horn and Charles R. Johnson. *Matrix Analysis*. Cambridge University Press, 2012.

[21] Gareth A. Jones. Paley and the Paley graphs. In *Isomorphisms, Symmetry and Computations in Algebraic Graph Theory: Pilsen, Czech Republic, October 3–7, 2016*, pp. 155–183. Springer, 2020.

[22] Apoorva Khare. *Matrix Analysis and Entrywise Positivity Preservers*. London Mathematical Society Lecture Note Series, Cambridge University Press, and Vol. 82 in Texts and Readings In Mathematics (TRIM Series), Hindustan Book Agency, 2022.

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

[24] Neal Koblitz. *A Course in Number Theory and Cryptography*, volume 114. Springer Science & Business Media, 1994.

[25] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications, Cambridge University Press, second edition, 1997.

[26] Edouard Lucas. Théorie des fonctions numériques simplement périodiques. *Amer. J. Math.*, 1(2):289–321, 1878.

[27] Walter Rudin. Positive definite sequences and absolutely monotonic functions. *Duke Math. J.*, 26:617–622, 1959.

[28] Isaac J. Schoenberg. Positive definite functions on spheres. *Duke Math. J.*, 9:96–108, 1942.

[29] Issai Schur. Bemerkungen zur Theorie der beschränkten Bilinearformen mit unendlich vielen Veränderlichen. *J. reine angew. Math.*, 140:1–28, 1911.

[30] Barry Simon. *Loewner's theorem on monotone matrix functions*. Vol. 10. Berlin: Springer, 2019.

[31] Prateek K. Vishwakarma. Positivity preservers forbidden to operate on diagonal blocks. *Trans. Amer. Math. Soc.*, 376:5261–5279, 2023.

(D. Guillot) University of Delaware, Newark, DE, USA
Email address: `dguillot@udel.edu`

(H. Gupta) University of Regina, Regina, SK, Canada
Email address: `himanshu.gupta@uregina.ca`

(P. K. Vishwakarma) Indian Institute of Science, Bangalore, India
Email address: `prateekv@alum.iisc.ac.in`