CHOLESKY DECOMPOSITION FOR SYMMETRIC MATRICES OVER FINITE FIELDS

PRATEEK KUMAR VISHWAKARMA

Abstract. Inspired by the seminal work of André-Louis Cholesky – whose contributions remain crucial even after more than a century in broader sciences – Cooper, Hanna and Whitlatch (2024) developed a theory of positive matrices over finite fields, and Khare and Vishwakarma (2025) described a general Cholesky factorization for a family of the dense cone of Hermitian matrices over real/complex fields, whose leading principal minors (LPM) are nonzero. Building on this, we develop a parallel theory within the finite field setting. Specifically *(i)* we extend the general Cholesky factorization to the LPM cone over finite fields which has asymptomatic density 1. We show that *(ii)* this factorization is compatible with the entrywise Frobenius map, recently studied in the context of positivity preservers by Guillot, Gupta, Vishwakarma, and Yip [*J. Algebra*, 2025]. We also *(iii)* leverage the Cholesky-structures to define meaningful group operations on the matrix cone, and as an application *(iv)* enumerate sub-cones of LPM matrices using our general Cholesky factorizations.

1. Introduction and main results

For an integer $n \geqslant 1$, over a real or complex field $\mathbb{F}$, a Hermitian matrix $A \in \mathbb{F}^{n\times n}$ is called positive definite if the quadratic form $z^*Az > 0$ for all nonzero $z \in \mathbb{F}^n$. Among more than half a dozen equivalent definitions of these matrices, André-Louis Cholesky's Factorization Theorem stands out for its applicability in broader sciences and mathematics, even after one hundred years of its publication in 1924 [1]. While the applicability of Cholesky's factorization of the positive definite cone of matrices has extensively been explored for over several decades now, there have been fewer attempts made to extend it to a broader class of matrices, and for fields that are not necessarily real or complex. We explore this extension over finite fields, and we begin by mentioning two such recent works [2, 7] that inspired the current article in such algebraic setting.

In a recent work by Cooper, Hanna, and Whitlatch [2], the cone of positive definite matrices over a finite field $\mathbb{F}_q$ (with q elements) is introduced. The authors define a field element as positive if it is a nonzero square in the field. Then, a symmetric matrix with entries in $\mathbb{F}_q$ is called positive definite if all its leading principal minors are positive – that is, they are squares in the field. The authors show that such matrices admit a Cholesky-type factorization:

Theorem 1.1 ([2]). *Only when q is even or $q \equiv 3 \pmod 4$, a symmetric matrix A with entries in $\mathbb{F}_q$ is positive definite if and only if there exists a unique lower triangular matrix L with positive diagonal entries such that $A = LL^T$.*

While this result establishes a compelling analogue of Cholesky factorization in the finite field setting, other characterizations of positive definiteness familiar from the real or complex

Date: August 7, 2025.

2020 *Mathematics Subject Classification.* 15B48, 15A23, 15B33.

Key words and phrases. Finite field, Cholesky decomposition, Cholesky factorization, sign pattern, LPM matrix, TPM matrix, Frobenius map.

cases do not yet appear to have meaningful analogues over finite fields. Nonetheless, the existence of a Cholesky factorization in the finite field context is leveraged in [2] to demonstrate the existence of certain pressing sequences for weighted graphs. Furthermore, this work has served as a key motivation for developing a theory of positivity-preserving entrywise transformations over finite fields [4, 3], which we will discuss in more detail in a subsection later.

The second relevant work is more recent and is by Khare and Vishwakarma [7], who introduce a general Cholesky factorization and develop a rich theory for a dense set of real/complex Hermitian matrices. Their framework decomposes the space into cones of matrices determined by the sign patterns of their leading principal minors. Additionally, the framework explores several implications of this decomposition.

We adopt an idea from [7] and explore the following points (and others discussed later):

(a) We extend Theorem 1.1, which addresses positive definite matrices via Cholesky decomposition, to broader cones of symmetric matrices over a finite field.
(b) The general Cholesky decomposition discussed in [7] is done for fields (including the real-closed fields) in which the underlying/base field is totally ordered. In the current work over finite fields, the Cholesky decomposition is discussed over fields that do not have a total order, and hence demonstrating such factorizations in a different algebraic settings.
(c) We explore implications that arise specifically in the finite field context, particularly in light of recent developments regarding entrywise transforms in this direction in [3].

Let us now introduce the new matrix cones over a finite field.

1.1. **Notations.**

Throughout this article, we let $\mathbb{F}_q$ denote the finite field with $q = p^k$ elements, where p is a prime and $k \geqslant 1$ an integer. The multiplicative cyclic group of nonzero elements of $\mathbb{F}_q$ is denoted by $\mathbb{F}_q^\times$. An element $a \in \mathbb{F}_q^\times$ is called *positive* if there exists $b \in \mathbb{F}_q^\times$ such that $a = b^2$. We denote the set of all positive elements by $\mathbb{F}_q^+$, and define the set of *negative* elements as $\mathbb{F}_q^- := \mathbb{F}_q^\times \setminus \mathbb{F}_q^+$. We distinguish these elements using the *quadratic/sign character*

$$\chi : \mathbb{F}_q^\times \to \{\pm 1\} \quad \text{defined by} \quad \chi(a) := \begin{cases} 1 & \text{if } a \in \mathbb{F}_q^+, \\ -1 & \text{if } a \in \mathbb{F}_q^-, \end{cases}$$

extended multiplicatively to all of $\mathbb{F}_q$ by setting $\chi(0) := 0$. It is well known that if q is odd, then $-1 \in \mathbb{F}_q^-$ if and only if $q \equiv 3 \pmod 4$ if and only if $\mathbb{F}_q^- = -\mathbb{F}_q^+$ [3, Proposition 2.3]. In this case, the field $\mathbb{F}_q$ is referred to as *definite*; otherwise, when $q \equiv 1 \pmod 4$, it is called *non-definite*. Finally, we use I_n to denote the $n \times n$ identity matrix over the field in context, and $A^{-T} = (A^{-1})^T$ for invertible matrices.

Definition 1.2 (Matrix cones with sign patterns)**.** Given an integer $n \geqslant 1$ and a sign pattern $\epsilon \in \{\pm 1\}^n \subseteq \mathbb{R}^n$, we define $LPM_n^{\mathbb{F}_q}(\epsilon)$ to be the cone of symmetric matrices $A \in \mathbb{F}_q^{n\times n}$ such that, for each $k = 1, \dots, n$, the $k \times k$ leading principal minor of A has quadratic character ϵ_k.

Similarly define $TPM_n^{\mathbb{F}_q}(\epsilon)$ as the cone of symmetric matrices $A \in \mathbb{F}_q^{n\times n}$ with all its $k \times k$ *trailing* principal minors having quadratic characters ϵ_k.

Each $LPM_n^{\mathbb{F}_q}(\epsilon)$ is nonempty, and so are $TPM_n^{\mathbb{F}_q}(\epsilon)$: define $\nabla, \mathbb{D}_\epsilon(\omega_\pm) \in \mathbb{F}_q^{n\times n}$ via,

$$\mathbb{D}_\epsilon(\omega_\pm) := \begin{pmatrix} \omega_1 & 0 & 0 & \cdots & 0 \\ 0 & \omega_1\omega_2 & 0 & \cdots & 0 \\ 0 & 0 & \omega_2\omega_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \omega_{n-1}\omega_n \end{pmatrix} \quad \text{and} \quad \nabla := \begin{pmatrix} 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{pmatrix}, \tag{1.1}$$

where each $\omega_k \in \{\omega_+, \omega_-\}$ for some fixed $\omega_+ \in \mathbb{F}_q^+$ and $\omega_- \in \mathbb{F}_q^-$ such that $\chi(\omega_k) = \epsilon_k$. Then

$$\mathbb{D}_\epsilon(\omega_\pm) \in LPM_n^{\mathbb{F}_q}(\epsilon) \quad \text{and} \quad \nabla \cdot \mathbb{D}_\epsilon(\omega_\pm) \cdot \nabla \in TPM_n^{\mathbb{F}_q}(\epsilon). \tag{1.2}$$

The cones $LPM_n^{\mathbb{F}_q}$ and $TPM_n^{\mathbb{F}_q}$, defined as the set of all symmetric matrices with nonzero leading, and respectively trailing, principal minors, decompose into disjoint unions:

$$LPM_n^{\mathbb{F}_q} = \bigsqcup_{\epsilon \in \{\pm 1\}^n} LPM_n^{\mathbb{F}_q}(\epsilon) \quad \text{and} \quad TPM_n^{\mathbb{F}_q} = \bigsqcup_{\epsilon \in \{\pm 1\}^n} TPM_n^{\mathbb{F}_q}(\epsilon), \tag{1.3}$$

provided q is odd. And when q is even, each $LPM_n^{\mathbb{F}_q}(\epsilon) = LPM_n^{\mathbb{F}_q}$ and $TPM_n^{\mathbb{F}_q}(\epsilon) = TPM_n^{\mathbb{F}_q}$.

1.2. **Cholesky decomposition and enumerations.** Our first main result addresses the Cholesky decompositions for the LPM and TPM matrix cones over a finite field.

Theorem A (Cholesky decomposition over finite fields)**.** *Fix an integer $n \geqslant 1$ and a finite field $\mathbb{F}_q$. Suppose a sign pattern $\epsilon \in \{\pm 1\}^n \subseteq \mathbb{R}^n$ and a matrix $A_\epsilon \in LPM_n^{\mathbb{F}_q}(\epsilon)$ are given. Then:*

(1) For each invertible lower triangular $L \in \mathbb{F}_q^{n\times n}$, the matrix $LA_\epsilon L^T \in LPM_n^{\mathbb{F}_q}(\epsilon)$.

(2) In particular, if $\mathbb{F}_q$ is a definite field or has characteristic 2, then for each $A \in LPM_n^{\mathbb{F}_q}(\epsilon)$, there exists a unique lower triangular matrix $L \in \mathbb{F}_q^{n\times n}$ with positive diagonal entries such that $A = LA_\epsilon L^T$.

Moreover, the following linear and nonlinear transforms are bijections:

$$LPM_n^{\mathbb{F}_q}(\epsilon) \to TPM_n^{\mathbb{F}_q}(\epsilon') \quad \textit{defined by} \quad A \mapsto \nabla A \nabla, \quad \textit{and} \quad A \mapsto A^{-1},$$

where $\epsilon = \epsilon'$ in the linear, and $\epsilon' = (\epsilon_n\epsilon_{n-1}, \epsilon_n\epsilon_{n-2}, \dots, \epsilon_n\epsilon_1, \epsilon_n)$ in the nonlinear case.

Therefore, the analogues of (1) and (2) hold for each fixed $A^\epsilon \in TPM_n^{\mathbb{F}_q}(\epsilon)$: for each invertible upper triangular $U \in \mathbb{F}_q^{n\times n}$, the matrix $UA^\epsilon U^T \in TPM_n^{\mathbb{F}_q}(\epsilon)$; and if $\mathbb{F}_q$ is a definite field or has characteristic 2, then for each $A \in TPM_n^{\mathbb{F}_q}(\epsilon)$, there exists a unique upper triangular matrix $U \in \mathbb{F}_q^{n\times n}$ with positive diagonal entries such that $A = UA^\epsilon U^T$.

A couple of remarks are in order:

Remark 1.3 (Two-fold refinement in Theorem A)**.** Theorem A establishes that for a definite field $\mathbb{F}_q$, the map $L \mapsto LA_\epsilon L^T$ is a bijection from the set of lower triangular matrices with positive diagonal entries to the cone $LPM_n^{\mathbb{F}_q}(\epsilon)$. As such, it constitutes a twofold extension of Theorem 1.1:

(a) it applies to *every* sign pattern $\epsilon \in \{\pm 1\}^n$, including the all-ones vector $\epsilon = (1, 1, \dots, 1)$, which corresponds to the positive definite cone considered in Theorem 1.1; and

(b) for each cone $LPM_n^{\mathbb{F}_q}(\epsilon)$, including the positive definite cone, it provides $LPM_n^{\mathbb{F}_q}(\epsilon)$-many Cholesky-type factorizations, one for *each* matrix A_ϵ. For instance, the "classical" Cholesky decomposition in Theorem 1.1 arises as the special case when $A_\epsilon = \mathrm{I}_n$, but Theorem A allows one to consider distinct Cholesky decompositions for arbitrary choices of positive definite $A_{(1,\dots,1)}$.

Note, both of these extensions apply to a definite field $\mathbb{F}_q$, and exactly one applies in the case where q is even. However, they do not apply to the remaining finite fields (of non-definite type), as such fields do not admit Cholesky factorizations, pointed out in the next remark.

Remark 1.4 (Theorem A for non-definite fields)**.** Theorem A(2) fails to hold over non-definite fields $\mathbb{F}_q$, as every matrix of the form $L\mathbb{D}_\epsilon(\omega_\pm)L^T$ coincides with $(LD)\mathbb{D}_\epsilon(\omega_\pm)(LD)^T$ for all diagonal matrices D with diagonal entries in $\{\pm 1\} \subset \mathbb{F}_q$, where $\mathbb{D}_\epsilon(\omega_\pm)$ is defined as in (1.1). Consequently, the uniqueness of the corresponding factorization also breaks down for the TPM cones over non-definite fields.

As an immediate corollary of Theorem A, we provide enumeration of the LPM and TPM (sub-)cones.

Corollary 1.5 (Enumerations)**.** *Fix an integer $n \geqslant 1$, and let $\mathbb{F}_q$ be a finite field with q odd. Then we have*

$$\#TPM_n^{\mathbb{F}_q} = \#LPM_n^{\mathbb{F}_q} = 2^n \#LPM_n^{\mathbb{F}_q}(\epsilon) = 2^n \#TPM_n^{\mathbb{F}_q}(\epsilon) = (q-1)^n q^{\binom{n}{2}}$$

for all sign patterns $\epsilon \in \{\pm 1\}^n$, where $q^{\binom{1}{2}} := 1$. Alternately, if q is even, then

$$\#TPM_n^{\mathbb{F}_q} = \#LPM_n^{\mathbb{F}_q} = \#LPM_n^{\mathbb{F}_q}(\epsilon) = \#TPM_n^{\mathbb{F}_q}(\epsilon) = (q-1)^n q^{\binom{n}{2}}.$$

While this enumerative result can be established directly through inductive arguments, a more elegant and often preferred approach in enumerative combinatorics involves constructing a bijection with a well-structured set for which the counting problem is more tractable (a perspective beautifully illustrated by the numerous celebrated interpretations of the Catalan numbers catalogued by Richard Stanley [13]). In the case at hand, rather than pursuing a purely combinatorial classification, we draw upon the structural insights afforded by our general Cholesky factorizations in a finite field setting, which provide a natural (and powerful!) framework for approaching the enumerations.

Proof of Corollary 1.5. For definite fields and for fields with characteristic 2: one needs to count the number of lower triangular matrices with positive diagonal entries. For the remaining non-definite fields: use induction and the fact that

$$x \mapsto \det \begin{pmatrix} A & \mathbf{u} \\ \mathbf{u}^T & x \end{pmatrix}_{n\times n} \quad \text{is a bijection over } \mathbb{F}_q,$$

for a given vector $\mathbf{u} \in \mathbb{F}^{n-1}$ and nonsingular $A \in \mathbb{F}^{(n-1)\times(n-1)}$. □

Remark 1.6 (A disclaimer on the asymptotic density)**.** Let $\mathrm{Sym}_n^{\mathbb{F}_q}$ denotes the set of all $n \times n$ symmetric matrices over a finite field $\mathbb{F}_q$. For a fixed $n \geqslant 1$, the proportion of matrices in $\mathrm{Sym}_n^{\mathbb{F}_q}$ that lie in the cone $LPM_n^{\mathbb{F}_q}$ (and similarly $TPM_n^{\mathbb{F}_q}$) tend to 1 as $q \to \infty$; that is,

$$\lim_{q\to\infty} \frac{\#LPM_n^{\mathbb{F}_q}}{\#\mathrm{Sym}_n^{\mathbb{F}_q}} = 1.$$

It may be worth reiterating that the asymptotic density in question pertains to the setting where the matrix size n is fixed, and the field size $q = p^k$ grows without bound, i.e., the integer $k \to \infty$.

1.3. The compatibility of Cholesky and Frobenius via Entrywise Transforms.

As we saw in Theorem A(1) and (2), that the following map is a bijection for a definite field $\mathbb{F}_q$:

$$\Psi_{A_\epsilon} : \mathbf{L}_n^{\mathbb{F}_q^+} \to LPM_n^{\mathbb{F}_q}(\epsilon) \quad \text{defined by} \quad L \mapsto LA_\epsilon L^T,$$

for any fixed $A_\epsilon \in LPM_n^{\mathbb{F}_q}(\epsilon)$, where $\mathbf{L}_n^{\mathbb{F}_q^+}$ denotes the cone of lower triangular matrices with positive diagonal entries in $\mathbb{F}_q$. Consequently, we obtain the bijective composition:

$$\Psi_{A_{\epsilon'} \to A_\epsilon} := \Psi_{A_\epsilon} \circ \Psi_{A_{\epsilon'}}^{-1} : LPM_n^{\mathbb{F}_q}(\epsilon') \to \mathbf{L}_n^{\mathbb{F}_q^+} \to LPM_n^{\mathbb{F}_q}(\epsilon) \quad \text{given by} \quad LA_{\epsilon'}L^T \mapsto LA_\epsilon L^T.$$

This provides a Cholesky-based mechanism for transitioning between the cones $LPM_n^{\mathbb{F}_q}(\epsilon')$ and $LPM_n^{\mathbb{F}_q}(\epsilon)$. Moreover, it prompts the following question: do there exist other maps – perhaps unrelated to Cholesky factorization and over any given finite field – that facilitate such transitions between the LPM cones? We address this question for a special class of transformations whose study dates back over a century to Schur – the student of Frobenius – including recent developments in the finite field setting.

Definition 1.7 (Entrywise Transforms)**.** Suppose $\mathbb{F}_q$ is a finite field, and consider a map $f : \mathbb{F}_q \to \mathbb{F}_q$. Then this map has a natural extension over all of the matrix space $\mathbb{F}_q^{n\times n}$, for integer $n \geqslant 1$ by considering:

$$f[-] : \mathbb{F}_q^{n\times n} \to \mathbb{F}_q^{n\times n} \quad \text{defined by} \quad f[A] := (f(a_{ij}))_{i,j=1}^n,$$

for all $A = (a_{ij})_{i,j=1}^n \in \mathbb{F}_q^{n\times n}$. These matrix functions are referred to as Entrywise Transforms.

These transforms over finite fields were recently studied by Guillot, Gupta, Vishwakarma, and Yip [4, 3], who extended celebrated classical results of Schoenberg [11] and Rudin [10] to the algebraic framework of finite fields. The foundational work of Schoenberg and Rudin itself traces back to a product theorem [12] of Schur, and to a seminal observation by Pólya and Szegő [9]. For a comprehensive account of recent advances in the theory of entrywise transforms, see the monograph by Khare [6].

We now bring entrywise transforms to the present setting. We will show that our Cholesky decomposition is compatible with applying the Frobenius entrywise. Namely for any sign pattern $\epsilon \in \{\pm 1\}^n \subseteq \mathbb{R}^n$, and for special choices of $A_\epsilon = \mathbb{D}_\epsilon := \mathbb{D}_\epsilon(\pm 1)$ for $\omega_\pm = \pm 1$ in (1.1),

$$\Psi_{\mathbb{D}_\epsilon}^{-1}(\mathrm{Frob}_p[A]) = \mathrm{Frob}_p[\Psi_{\mathbb{D}_\epsilon}^{-1}(A)] \quad \text{for all} \quad A \in LPM_n^{\mathbb{F}_q}(\epsilon). \tag{1.4}$$

This compatibility question can be pursued within a natural framework. Recall that the map $\Psi_{A'_\epsilon \to A_\epsilon}$ provides a bijection between the cones $LPM_n^{\mathbb{F}_q}(\epsilon')$ and $LPM_n^{\mathbb{F}_q}(\epsilon)$. While this map is algorithmic, it is natural to ask whether a simpler, less nuanced map can be obtained in this context. To explore this, we consider entrywise transforms. The following theorem characterizes such entrywise maps over a finite definite field, subject to a certain 2-*by*-2 sign pattern constraint.

Theorem B (Entrywise transforms and their compatibility with Frobenius)**.** *Suppose that integers $2 \leqslant s \leqslant n$ are given, and let $\mathbb{F}_q$ be a finite definite field with $q = p^k$, where p is prime. Let $\epsilon, \epsilon' \in \{\pm 1\} \subseteq \mathbb{R}^{n\times n}$ be sign patterns satisfying $\epsilon_1 = \cdots = \epsilon_s = \epsilon'_1 = \cdots = \epsilon'_s = 1$. Then for a given function $f : \mathbb{F}_q \to \mathbb{F}_q$, the following are equivalent:*

(1) The entrywise transform $f[-]$ sends $LPM_n^{\mathbb{F}_q}(\epsilon')$ into $LPM_n^{\mathbb{F}_q}(\epsilon)$.

(2) The sign patterns are equal, and f is a positive multiple of a power of the Frobenius:

$$\epsilon' = \epsilon \qquad \textit{and} \qquad f \equiv c \cdot \mathrm{Frob}_p^{\ell} \quad \textit{for some} \quad 0 \leqslant \ell \leqslant k-1 \ \textit{and}\ c \in \mathbb{F}_q^{+}.$$

Moreover, every such map $f[-] \equiv c \cdot \mathrm{Frob}_p^{\ell}[-]$ is compatible with Cholesky maps $\Psi_{A_\epsilon}^{\pm 1}$ in the following sense: for all $A \in LPM_n^{\mathbb{F}_q}(\epsilon)$, $L \in \mathbf{L}_n^{\mathbb{F}_q^+}$ and $0 \leqslant \ell \leqslant k-1$, we have

$$\Psi_{A_\epsilon}^{-1}(c \cdot \mathrm{Frob}_p^{\ell}[A]) = \mathrm{Frob}_p^{\ell}[\Psi^{-1}_{c\cdot \mathrm{Frob}_p^{\ell}[A_\epsilon]}(A)] = \sqrt{c} \cdot \mathrm{Frob}_p^{\ell}[\Psi^{-1}_{\mathrm{Frob}_p^{\ell}[A_\epsilon]}(A)]$$

$$\textit{and} \qquad c \cdot \mathrm{Frob}_p^{\ell}[\Psi_{A_\epsilon}(L)] = \Psi_{c\cdot \mathrm{Frob}_p^{\ell}[A_\epsilon]}(\mathrm{Frob}_p^{\ell}[L]) = \Psi_{\mathrm{Frob}_p^{\ell}[A_\epsilon]}(\sqrt{c} \cdot \mathrm{Frob}_p^{\ell}[L]),$$

where $\sqrt{c}$ denotes the unique $d \in \mathbb{F}_q^{+}$ such that $d^2 = c$.

In particular if $c = 1$ and the chosen $A_\epsilon = \mathbb{D}_\epsilon := \mathbb{D}_\epsilon(\pm 1)$ for $\omega_{\pm} = \pm 1$ as in (1.1), then

$$\Psi_{\mathbb{D}_\epsilon}^{\pm 1} \circ \mathrm{Frob}_p = \mathrm{Frob}_p \circ \Psi_{\mathbb{D}_\epsilon}^{\pm 1} \qquad \textit{i.e.,} \qquad \Psi_{\mathbb{D}_\epsilon}^{\pm 1}(\mathrm{Frob}_p[M_{\pm}]) = \mathrm{Frob}_p[\Psi_{\mathbb{D}_\epsilon}^{\pm 1}(M_{\pm})],$$

for all $M_{-} \in LPM_n^{\mathbb{F}_q}(\epsilon)$ and all $M_{+} \in \mathbf{L}_n^{\mathbb{F}_q^+}$.

Remark 1.8 (Two main aspects of Theorem B)**.**

(a) Theorem B establishes the existence of an entrywise transform $f[-]$ from $LPM_n^{\mathbb{F}_q}(\epsilon')$ to $LPM_n^{\mathbb{F}_q}(\epsilon)$, under the assumption that the sign patterns ϵ' and ϵ are identical and take the value 1 in at least the first two coordinates (the 2-*by*-2 constraints). In this case, the function f must be a positive scalar multiple of a power of the Frobenius map. This, in turn, implies that *no* entrywise transform can exist between two distinct LPM cones when the common sign pattern begins with two or more entries equal to 1.

(b) Although this places a limitation on the existence of entrywise transforms between different LPM cones, it simultaneously highlights a structural coherence: the permitted transforms between the same LPM cones align naturally with the positive scalar multiples of the automorphisms of the underlying field, as captured by the final identities in Theorem B. In particular, it shows that each Cholesky map $\Psi_{\mathbb{D}_\epsilon}^{\pm 1}$ commutes with the automorphisms of the definite field $\mathbb{F}_q$ via the entrywise tranforms.

We now come to the possibilities over non-definite fields parallel to Theorem B. As we show later, the proof of Theorem B is an application of a key result from [3]. Other main results from [3] similarly yield a parallel statement for non-definite fields. (However, the compatibility question does not arise here as non-definite fields do not admit a Cholesky factorization.) We mention this result for completeness under a 3-*by*-3 and a 2-*by*-2 constraint. Note that slightly modified Remark 1.8(a) applies here.

Theorem 1.9 (Entrywise transforms for non-definite fields)**.** *Suppose integers $3 \leqslant s \leqslant n$ are given, and let $\mathbb{F}_q$ be a finite non-definite field with $q = p^k$, where p is prime. Let $\epsilon, \epsilon' \in \{\pm 1\} \subseteq \mathbb{R}^{n\times n}$ be sign patterns satisfying $\epsilon_1 = \cdots = \epsilon_s = \epsilon'_1 = \cdots = \epsilon'_s = 1$. Then for a given function $f : \mathbb{F}_q \to \mathbb{F}_q$, the following are equivalent:*

(1) The entrywise transform $f[-]$ sends $LPM_n^{\mathbb{F}_q}(\epsilon')$ into $LPM_n^{\mathbb{F}_q}(\epsilon)$.

(2) The sign patterns are equal, and f is a positive multiple of a power of Frobenius:

$$\epsilon' = \epsilon \quad \textit{and} \quad f \equiv c \cdot \mathrm{Frob}_p^{\ell} \quad \textit{for some} \quad 0 \leqslant \ell \leqslant k-1 \ \textit{and}\ c \in \mathbb{F}_q^{+}.$$

Moreover, if we consider the special class of non-definite fields $\mathbb{F}_q$ of square order, then for any fixed $n \geqslant 2$ and $s = 2$, statements (1) and (2) are equivalent.

We conclude this subsection with a question for future investigation:

Question 1.10. What are the corresponding entrywise transforms in Theorems B and 1.9 when the 3-*by*-3 and 2-*by*-2 conditions, i.e., "$\epsilon_1 = \cdots = \epsilon_s = \epsilon'_1 = \cdots = \epsilon'_s = 1$", are removed? And how do those transforms behave with the Cholesky factorization, whenever applicable?

1.4. Two group structures over the LPM cones and their compatibility with the Frobenius map.

One of the key differences between positive definite matrices over the real/complex fields and those over a finite field is that, in the former setting, the square of a positive definite matrix A, namely A^2, is again positive definite. In contrast, this property does not necessarily hold over finite fields [2]. In the next result, we introduce a group structure on the bigger cone $LPM_n^{\mathbb{F}_q}$ (the collection of symmetric $n \times n$ matrices over a definite field $\mathbb{F}_q$ whose leading principal minors are all nonzero) under which the square of each matrix is guaranteed to be positive definite.

Recall that for a definite field $\mathbb{F}_q$, the cone $LPM_n^{\mathbb{F}_q}$ is the disjoint union of the sub-cones $LPM_n^{\mathbb{F}_q}(\epsilon)$, indexed by sign patterns ϵ. We refer to the Cholesky factorization within each of these sub-cones, taking the representative matrix $A_\epsilon = \mathbb{D}_\epsilon := \mathbb{D}_\epsilon(\pm 1)$ for $\omega_\pm = \pm 1$, as defined in (1.1). With this setup, we now state the group structures:

Theorem C (Group structures on the bigger LPM cone)**.** *Let $n \geqslant 1$ be an integer, and let $\mathbb{F}_q$ be a definite finite field. Consider that a group $(\mathbf{L}_n^{\mathbb{F}_q^+}, \circledcirc)$ with identity element I_n is given. Define a binary operation $\boxdot$ on the set $LPM_n^{\mathbb{F}_q}$ as follows: for any $A, B \in LPM_n^{\mathbb{F}_q}$, write their unique Cholesky factorizations as*

$$A = L\mathbb{D}_\epsilon L^T \in LPM_n^{\mathbb{F}_q}(\epsilon), \quad \textit{and} \quad B = K\mathbb{D}_{\epsilon'}K^T \in LPM_n^{\mathbb{F}_q}(\epsilon'),$$

where $\epsilon, \epsilon' \in \{\pm 1\}^n \subseteq \mathbb{R}^n$ and $L, K \in \mathbf{L}_n^{\mathbb{F}_q^+}$. Then define

$$A \boxdot B := (L \circledcirc K)(\mathbb{D}_\epsilon \mathbb{D}_{\epsilon'})(L \circledcirc K)^T. \tag{1.5}$$

This makes $(LPM_n^{\mathbb{F}_q}, \boxdot)$ a group with identity element I_n, and inverse given by

$$A = L\mathbb{D}_\epsilon L^T \mapsto L^{\circledcirc -1}\mathbb{D}_\epsilon (L^{\circledcirc -1})^T.$$

Finally, for every $A \in LPM_n^{\mathbb{F}_q}$, the square $A^{\boxdot 2} := A \boxdot A$ is positive definite by Theorem 1.1.

Proof. It can be shown by direct verification. □

We present two examples of group structures on $LPM_n^{\mathbb{F}_q}(\epsilon)$, one abelian and one non-abelian, obtained via the transport described in Theorem C from the group $\mathbf{L}_n^{\mathbb{F}_q^+}$.

Example 1.11. Suppose we define two binary operations $\circledcirc_1, \circledcirc_2 : \mathbf{L}_n^{\mathbb{F}_q^+} \times \mathbf{L}_n^{\mathbb{F}_q^+} \to \mathbf{L}_n^{\mathbb{F}_q^+}$ by

$$L \circledcirc_1 K := LK, \quad \text{and} \quad L \circledcirc_2 K := \lfloor L \rfloor + \lfloor K \rfloor + \mathbb{D}(L)\mathbb{D}(K),$$

where, for $L = (l_{ij})$, the diagonal and strict lower triangular parts are defined by

$$\mathbb{D}(L) := \operatorname{diag}(l_{11}, \ldots, l_{nn}), \quad \text{and} \quad \lfloor L \rfloor_{ij} := \begin{cases} l_{ij}, & i > j, \\ 0, & \text{otherwise.} \end{cases}$$

The operation $\circledcirc_2$ was introduced in [8]. Both operations endow $\mathbf{L}_n^{\mathbb{F}_q^+}$ with a group structure, with identity element I_n, and respective inverse maps given by

$$L \mapsto L^{-1} \quad \text{for } \circledcirc_1, \qquad \text{and} \qquad L \mapsto -\lfloor L \rfloor + \mathbb{D}(L)^{-1} \quad \text{for } \circledcirc_2\,.$$

Note, the transported $\boxdot_1$ is non-abelian; and $\boxdot_2$ is abelian.

Moreover, these transported groups are compatible with the Frobenius map:

$$\mathrm{Frob}_p[A \boxdot_j B] = \mathrm{Frob}_p[A] \boxdot_j \mathrm{Frob}_p[B] \qquad \forall A, B \in LPM_n^{\mathbb{F}_q}, \quad \text{for} \quad j = 1, 2.$$

Remark 1.12 (Group structures on individual LPM cones and future directions)**.** In addition to the transported group structure $\boxdot$ on the "global" cone $LPM_n^{\mathbb{F}_q}$ for definite fields $\mathbb{F}_q$, one can also define "internal" group structures $\circledast$ on each individual cone $LPM_n^{\mathbb{F}_q}(\epsilon)$ by modifying the operation in (1.5):

$$A \circledast B := (L \circledcirc K)\mathbb{D}_\epsilon (L \circledcirc K)^T \tag{1.6}$$

where $A, B \in LPM_n^{\mathbb{F}_q}(\epsilon)$ with their unique Cholesky factorizations as

$$A = L\mathbb{D}_\epsilon L^T \quad \text{and} \quad B = K\mathbb{D}_\epsilon K^T.$$

This construction endows each individual cone $LPM_n^{\mathbb{F}_q}(\epsilon)$, indexed by $\epsilon \in \{\pm 1\}^n \subseteq \mathbb{R}^n$, with a group structure. In particular, all such cones are mutually isomorphic as groups.

Furthermore, given a natural metric over a finite definite field, it would be interesting to investigate analogues of Riemannian geometric properties – similar to the setting explored in [7] over the real field.

Remark 1.13 (Similar results for TPM cones)**.** All results (and future directions) presented above in Subsections 1.3 and 1.4 for the LPM cones admit direct analogues for the TPM cones as well. Since the necessary modifications are straightforward, we omit the explicit statements in the interest of brevity.

2. Proofs

2.1. **Proof of Theorem A.** Fix two notations hereafter: $[m] := \{1, \dots, m\}$ for all integers $m \geqslant 1$, and $A_{I \times J}$ for the submatrix of a matrix A indexed by row set I and column set J.

Proof of Theorem A. It is along the lines of [7, Theorem A].

(1) For a given $A_\epsilon \in LPM_n^{\mathbb{F}_q}(\epsilon)$ and a non-singular lower triangular $L \in \mathbb{F}_q^{n\times n}$, we need to show that the minor $\det(LA_\epsilon L^T)_{[k]\times[k]}$ has the quadratic character ϵ_k. Using the Cauchy–Binet formula, we compute:

$$\det(LA_\epsilon L^T)_{[k]\times[k]} = \det(L_{[k]\times[n]} A_\epsilon (L_{[k]\times[n]})^T) = \sum_{\substack{J,K\subseteq[n],\\ |J|=|K|=k}} \det(L_{[k]\times J}) \det(A_\epsilon)_{J\times K} \det(L_{[k]\times K})^T.$$

Now as L is lower triangular, the submatrices $L_{[k]\times J}$ are singular unless $J = [k]$. So,

$$\det(LA_\epsilon L^T)_{[k]\times[k]} = (\det L_{[k]\times[k]})^2 \det(A_\epsilon)_{[k]\times[k]}.$$

Therefore, as L is non-singular, we have the desired outcome.

(2) Here $\mathbb{F}_q$ is a definite field or a field of even order. For convenience, consider the "positive square root" map $\sqrt{\cdot} : \mathbb{F}_q^+ \to \mathbb{F}_q^+$, where $\sqrt{a}$ is the unique $b \in \mathbb{F}_q^+$ such that $b^2 = a$. Since $\mathbb{F}_q$ is definite or has even order, this map is a bijection.

The proof is based on two key observations on block matrices, and their products:

$$\begin{pmatrix} K & \mathbf{0} \\ \mathbf{p}^T & s \end{pmatrix} \begin{pmatrix} B_\epsilon & \mathbf{u} \\ \mathbf{u}^T & v \end{pmatrix} \begin{pmatrix} K^T & \mathbf{p} \\ \mathbf{0}^T & s \end{pmatrix} = \begin{pmatrix} KB_\epsilon K^T & K(B_\epsilon \mathbf{p} + s\mathbf{u}) \\ (\mathbf{p}^T B_\epsilon + s\mathbf{u}^T)K^T & \mathbf{p}^T B_\epsilon \mathbf{p} + vs^2 + 2s\mathbf{u}^T\mathbf{p} \end{pmatrix},$$

$$A_\epsilon = \begin{pmatrix} B_\epsilon & \mathbf{u} \\ \mathbf{u}^T & v \end{pmatrix} \in LPM_n^{\mathbb{F}_q}(\epsilon) \quad \Longrightarrow \quad B_\epsilon \in LPM_{n-1}^{\mathbb{F}_q}((\epsilon_1, \dots, \epsilon_{n-1})),$$

where $\mathbf{u} \in \mathbb{F}_q^{n-1}$ and $v \in \mathbb{F}_q$.

Collectively they show that for a given $A = \begin{pmatrix} B & \mathbf{b} \\ \mathbf{b}^T & c \end{pmatrix} \in LPM_n^{\mathbb{F}_q}(\epsilon)$, to obtain the required solution L for $LA_\epsilon L^T = A$, we first need to be able to solve for a unique lower triangular $K \in \mathbb{F}_q^{(n-1)\times(n-1)}$ with positive diagonal entries, such that $B = KB_\epsilon K^T$. Assuming this can be solved, we show that $\mathbf{p} \in \mathbb{F}_q^{n-1}$ and $s \in \mathbb{F}_q^+$ can be solved uniquely from this. Note that if

$$\mathbf{b} = K(B_\epsilon \mathbf{p} + s\mathbf{u}) \quad \text{and} \quad c = \mathbf{p}^T B_\epsilon \mathbf{p} + vs^2 + 2s$$

then, from the first equation, one obtains

$$\mathbf{p} = B_\epsilon^{-1}(K^{-1}\mathbf{b} - s\mathbf{u})$$

and then, up on its substitution in the second, one gets

$$s^2 = \frac{c - \mathbf{b}^T B^{-1}\mathbf{b}}{v - \mathbf{u}^T B_\epsilon^{-1}\mathbf{u}}.$$

Now, recall the theory of Schur complements: $\det \begin{pmatrix} P & \mathbf{q} \\ \mathbf{q}^T & t \end{pmatrix} = (\det P)(t - \mathbf{q}^T P^{-1}\mathbf{q})$ if P^{-1} exists. This gives

$$s^2 = \frac{\det A}{\det B} \cdot \frac{\det B_\epsilon}{\det A_\epsilon}, \tag{2.1}$$

in which the right side has positive quadratic character as both $A, A_\epsilon \in LPM_n^{\mathbb{F}_q}(\epsilon)$. Now take the positive square root to solve for the unique $s \in \mathbb{F}_q^+$. This solves for s and therefore for $\mathbf{p}$ uniquely – given a unique lower triangular $K \in \mathbb{F}_q^{(n-1)\times(n-1)}$ with positive diagonals.

Thus, all that remains to show is: given $B, B_\epsilon \in LPM_{n-1}^{\mathbb{F}_q}((\epsilon_1, \dots, \epsilon_{n-1}))$, can one solve for the lower triangular K with positive diagonals such that $B = KB_\epsilon K^T$? Considering the aforementioned algorithmic process, it is sufficient to show this for $n = 2$: given $a, a_\epsilon \in \mathbb{F}_q^\pm$, does there exists a unique $\kappa \in \mathbb{F}_q^+$ such that $\kappa \cdot a_\epsilon \cdot \kappa = \kappa^2 a_\epsilon = a$? Indeed, since $a/a_\epsilon \in \mathbb{F}_q^+$ – where $\mathbb{F}_q$ is either a definite field or has characteristic 2 – it has a unique positive square root, which is our required $\kappa \in \mathbb{F}_q^+$.

Now, the second half of the proof.

Since $\nabla A \nabla$ reverses the rows and columns of a square matrix, it interchanges the leading and trailing $k \times k$ principal minors for every k. Therefore it is the required linear bijection.

For the inverse map, recall Jacobi's complementary minor formula [5]. Let $A \in \mathbb{F}_q^{n\times n}$ be invertible, and let $J, K \subseteq [n]$ of equal size $0 < p < n$. Then:

$$\det A \cdot \det(A^{-1})_{K^c \times J^c} = (-1)^{\sum_J j + \sum_K k} \det A_{J\times K}, \tag{2.2}$$

where $J^c := [n] \setminus J$, and similarly K^c. Apply this identity for $J = K = [k]$ for $0 < k < n$. If $A \in LPM_n^{\mathbb{F}_q}(\epsilon)$, then the trailing principal minors of A^{-1} satisfy:

$$\det(A^{-1})_{[k]^c\times[k]^c} = \frac{\det A_{[k]\times[k]}}{\det A}.$$

Therefore, the quadratic character of this ratio, and hence of the trailing principal minor, is $\epsilon_k \epsilon_n$. If $k = n$, we have $\det A^{-1} = 1/\det A$, which has the character ϵ_n.

Moreover, starting with $A \in TPM_n^{\mathbb{F}_q}(\epsilon')$, one may apply (2.2) with $J = K = [k]^c$ instead, ensuring that the map is a bijection.

The final steps of showing (1) and (2) for the TPM cones is a direct application of the assertions proved above for the linear and non-linear bijections. □

Remark 2.1. The only step in the Proof of Theorem A(2) that does not work out for non-definite fields is the last paragraph of (2). More precisely, if $\mathbb{F}_q$ is non-definite, then for each $a \in \mathbb{F}_q^+$, there exists distinct $b_1, b_2 \in \mathbb{F}_q^{\pm}$ such that $b_j^2 = a$. Therefore, the "positive square root" function here is not well-defined, and as a result a Cholesky factorization does not exist for non-definite fields.

2.2. **Proof of Theorems B and 1.9.**

Here the proofs are applications of the results in [3] in the context of positivity preservers.

Proof of Theorem B (1) $\iff$ (2). The implication (2) $\implies$ (1) follows from [3, Proposition 2.12]. For the other implication, suppose $A' \in LPM_s^{\mathbb{F}_q}((1,1,\dots,1))$. Then $A := A' \oplus \mathbb{D}_{\epsilon''} \in LPM_n^{\mathbb{F}_q}(\epsilon')$, where $\epsilon'' = (\epsilon_{s+1}, \dots, \epsilon_n)$. Therefore $f[A] \in LPM_n^{\mathbb{F}_q}(\epsilon)$, and in particular, $f[A'] = f[A]_{[s]\times[s]} \in LPM_s^{\mathbb{F}_q}((1,1,\dots,1))$. This means that $f[-]$ is an entrywise positivity preserver over $s \times s$ positive definite matrices, where $\mathbb{F}_q$ is a finite definite field. Therefore [3, Theorem B] implies that $f \equiv c \cdot \mathrm{Frob}^{\ell}$ for some $c \in \mathbb{F}_q^+$ and $\ell \in 0, 1, \dots, k-1$. Moreover, it follows from [3, Proposition 2.12] that $\epsilon' = \epsilon$. □

The proof of Theorem 1.9 is similarly completed, using [3, Theorem C] instead.

The final identities in Theorem B and the final assertion in Example 1.11 require the next:

Lemma 2.2. *Let $\mathbb{F}_q$ be a finite field with $q = p^k$ for p a prime. Suppose A and B are matrices with entries in $\mathbb{F}_q$, such that AB is well defined. Then* $\mathrm{Frob}_p[AB] = \mathrm{Frob}_p[A]\mathrm{Frob}_p[A]$.

Proof. We have the following as Frob_p preserves the field operations:

$$\mathrm{Frob}_p((AB)_{ij}) = \mathrm{Frob}_p(\sum_k a_{ik}b_{kj}) = \sum_k \mathrm{Frob}_p(a_{ik})\mathrm{Frob}_p(b_{kj}) = (\mathrm{Frob}_p[A]\mathrm{Frob}_p[B])_{ij}.$$

This completes the proof. □

Proof of Theorem B (compatibility with the Frobenius map). It follows precisely due to Lemma 2.2 and the fact that $\Psi_{A_\epsilon}^{\pm 1}$ are bijections. Moreover, when we restrict to $A_\epsilon = \mathbb{D}_\epsilon$, then $\mathrm{Frob}_p[\mathbb{D}_\epsilon] = \mathbb{D}_\epsilon$. This yields the final identities on commutativity. □

Acknowledgments

I am thankful for the support by the Centre de recherches mathématiques and Université Laval and their CRM-Laval Postdoctoral Fellowship, and the Alliance grant. I would also like to sincerely thank Apoorva Khare for comments and discussions.

References

[1] Benoit. *Note sur une méthode de résolution des équations normales provenant de l'application de la méthode des moindres carrés à un système d'équations linéaires en nombre inférieur à celui des inconnues (Procédé du Commandant Cholesky).* Bull. géodésique, I. – Notices Scientifiques, 2:67–77, 1924.

[2] Joshua Cooper, Erin Hanna, and Hays Whitlatch. *Positive-definite matrices over finite fields.* Rocky Mountain J. Math., 54(2): 423–438, 2024.

[3] Dominique Guillot, Himanshu Gupta, Prateek Kumar Vishwakarma, Chi Hoi Yip. *Positivity preservers over finite fields.* J. Algebra, 684:479–523, 2025.

[4] Dominique Guillot, Himanshu Gupta, Prateek Kumar Vishwakarma, Chi Hoi Yip. *Entrywise transforms and positive definite matrices over finite fields.* 37th International Conference on Formal Power Series and Algebraic Combinatorics (FPSAC 2025), Sém. Lothar. Combin. 93B (2025), Article #69, 12 pp.

[5] Carl Gustav Jacob Jacobi. *De formatione et proprietatibus Determinatium.* J. reine angew. Math., 22:285–318, 1841.

[6] Apoorva Khare. *Matrix Analysis and Entrywise Positivity Preservers.* London Mathematical Society Lecture Note Series, Cambridge University Press, 2022.

[7] Apoorva Khare and Prateek Kumar Vishwakarma. *Cholesky decomposition for symmetric matrices, Riemannian geometry, and random matrices.* arXiv:2508.02715, 2025.

[8] Zhenhua Lin. *Riemannian geometry of Symmetric Positive Definite matrices via Cholesky decomposition.* SIAM J. Matrix Anal. Appl., 40(4):1353–1370, 2019.

[9] Georg Pólya and Gabor Szegő. *Aufgaben und Lehrsätze aus der Analysis. Band II: Funktionentheorie, Nullstellen, Polynome Determinanten, Zahlentheorie, volume Band 74 of Heidelberger Taschenbücher [Heidelberg Paperbacks].* Springer-Verlag, Berlin-New York, 1971.

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

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

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

[13] Richard Peter Stanley. *Enumerative Combinatorics. Vol. 1, 2nd Ed.* Cambridge University Press, 2012.

Département de mathématiques et de statistique, Université Laval, Québec, Canada
Email address: prateek-kumar.vishwakarma.1@ulaval.ca, prateekv@alum.iisc.ac.in