Positive-Definite Matrices over Finite Fields

Joshua Cooper, Erin Hanna, and Hays Whitlatch
February 07, 2022

Abstract
The study of positive-definite matrices has focused on Hermitian matrices, that is, square matrices with complex (or real) entries that are equal to their own conjugate transposes. In the classical setting, positive-definite matrices enjoy a multitude of equivalent definitions and properties. In this paper, we investigate when a square, symmetric matrix with entries coming from a finite field can be called “positive-definite” and discuss which of the classical equivalences and implications carry over.

1 Introduction
Our goal in this paper is to introduce and investigate the concept of positive-definiteness over finite fields. What does it mean to be positive in a finite field? Are exactly half of the non-zero elements positive? Do the equivalences afforded to Hermitian positive-definite matrices carry over to finite fields? And naturally, why is this topic interesting, and how did this come up? We encourage the reader to pause and think about these questions before reading our proposed framework for addressing them.

The theory of positive-definiteness is vast and reaches throughout many branches of mathematics. Positive-definite matrices are used in optimization algorithms, to study convexity with multi-variable functions, in the construction of some types of linear regression models, and in principal component analysis. Positive-definite Hermitian matrices admit a “Cholesky decomposition”, that is, the matrix can be expressed as the product of a lower triangular matrix and its conjugate transpose. This decomposition can be used to efficiently solve a system of linear equations or to quickly acquire numerical solutions via repeated random sampling in a computational algorithm such as Monte Carlo simulation.

Our interest in positive-definite matrices emerged from a very different application in which the success of a graph theoretical operation (called “pressing”) corresponds to the existence of a Cholesky decomposition for its adjacency matrix (over the finite field $\mathbb{F}_2$). This correspondence was first shown in [3] and was further interpreted in [4]. The topic originated via an application in bioinformatics (see [1], [5]), where pressing sequences correspond to sortings by reversal of DNA sequences. We elaborate briefly on the connection with matrix algebra below as it is relevant to the discussion in Section 5.

Definition 1. A bicolored graph $G = (G, c)$ is a simple graph $G$ with $c : V(G) \rightarrow \{\text{blue, white}\}$ which assigns a color to each vertex. The complement of blue is white and the complement of white is blue. For $v \in V(G)$, pressing a blue vertex $v$ is the operation of transforming $(G, c)$ to $(G', c')$, a new bicolored graph in which $G[N_G(v) \cup \{v\}]$ is complemented. That is, $V(G) = V(G')$ and

$$E(G') = E(G) \triangle \left( \frac{N_G(v) \cup \{v\}}{2} \right)$$

where $\triangle$ denotes symmetric difference, $N_G(v)$ is the neighborhood of $v$ in $G$, $c'(w)$ is the complement of $c(w)$ for $w \in N_G(v) \cup \{v\}$, and $c'(w) = c(w)$ otherwise. This definition is illustrated in Example 1 where one can see that pressing a blue vertex changes its color to white and flips the colors of its neighbors, isolates the pressed vertex, and complements the set of edges induced by its neighbors.

\footnote{Some authors use black and white instead.}
A sequence of presses is referred to as a **pressing sequence**. Since a pressed vertex becomes isolated, it may not be pressed again, and will not be affected by future presses. Thus, every pressing sequence is finite in length. If the end result of a pressing sequence is the empty, edgeless, colorless graph then we say that it was a **successful pressing sequence**. As it turns out, a pressing sequence is successful exactly when the graph’s adjacency matrix (with row and column order dictated by the pressing sequence) has a Cholesky decomposition over $\mathbb{F}_2$. In fact, the Cholesky decomposition gives the instructions for pressing, revealing at each press which vertices would be affected.

**Example 1.** Below is a bicolored graph with successful pressing sequence 1,2,3,4 (blue vertices are shown in gray).

![Graph with pressing sequence 1,2,3,4](image)

The adjacency matrix of this graph (with 1’s on the diagonal when the vertex is blue) and the Cholesky decomposition corresponding to this pressing sequence (with rows and columns labelled by 1, 2, 3, 4, 5) is

\[
\begin{bmatrix}
1 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 \\
\end{bmatrix}
= \begin{bmatrix}
1 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 \\
\end{bmatrix}^T
\begin{bmatrix}
1 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 \\
\end{bmatrix}
\]

Observe that in the upper diagonal matrix, the $j^{th}$ entry of the $i^{th}$ row is 1 exactly when pressing $i$ changed the state of $j$.

In the introduction we briefly discussed that Hermitian positive-definite matrices enjoy a multitude of theoretical and computational interpretations. As such, there are several equivalent definitions for a positive-definite Hermitian matrix and the choice of which definition to use is often determined by the desired application. We will see in Proposition 1 that not all of these definitions make sense over finite fields.

**Definition 2.** ([6]) A $n \times n$ Hermitian matrix $A$ is said to be positive-definite if any (and hence all) of the following hold:

1. $z^*A z > 0$ for all non-zero column vectors $z \in \mathbb{C}^n$;
2. $A$ has positive eigenvalues;
3. The associated sesquilinear form is 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.
In addition, Hermitian positive-definite matrices enjoy numerous useful properties, only some of which will carry over to finite-fields. If $A$ and $B$ are positive-definite $n \times n$ Hermitian matrices, then the following statements hold (8):

1. $A$ is invertible;
2. $A^{-1}$ is positive-definite;
3. $rA$ is positive-definite ($r > 0$ a real number);
4. $ABA$ and $BAB$ are positive-definite;
5. if $AB = BA$ then $AB$ is positive-definite;
6. every principal submatrix of $A$ is positive-definite;
7. the Hadamard product $A \circ B$ and the Kronecker product $A \otimes B$ are positive-definite;
8. the Frobenius product $A : B \geq 0$.

## 2 Defining Positive-Definiteness in a Finite Field

In this section we will introduce the notion of positive-definiteness over a finite field. In Section 1 we presented several equivalent definitions that work over $\mathbb{C}$. Among these, the positivity of $z^*Az$ for all non-zero column vectors $z$ is perhaps the most commonly used definition for positive-definiteness (see for example [5]). Over a finite field, this definition fails to translate meaningfully for a few reasons. First, there is the ambiguity of the statement $z^*Az > 0$, which should generally mean something different than $z^*Az \neq 0$. We will resolve this issue in Definition 3. However, the following proposition demonstrates that, even if we resolve the previous issue, the definition will not apply to any finite field.

**Proposition 1.** Suppose $\mathbb{F}$ is a finite field, and $A$ is an $n \times n$ matrix over $\mathbb{F}$ for $n \geq 3$. Define $Q : \mathbb{F}^n \to \mathbb{F}$ by $Q(x) = x^TAx$. Then there exists a non-zero vector $v$ so that $Q(v) = 0$.

**Proof.** Chevalley’s Theorem (2) states that, for a collection of polynomials $\{f_1, \ldots, f_m\} \subseteq \mathbb{F}[X_1, \ldots, X_n]$ with $n > \sum_{i=1}^m \deg f_i$, if $f_i(0, \ldots, 0) = 0$ for all $i$, then there exists a nonzero $v$ so that $f_i(v) = 0$ for all $i$. Take $m = 1$ and $f_1(x) = Q(x)$, where we are treating the coordinates of $x$ as the variables $X_i$ on the left-hand side. Then, since $n \geq 3 > 2 = \deg f_1$, and $Q(0, \ldots, 0) = 0$, the proposition follows. □

The previous proposition demonstrates that it is not possible to extend all of the definitions (and implications) of Hermitian positive-definiteness to finite fields. Before proceeding, we must first resolve the question of what it means to be positive in a finite field.

**Definition 3.** For $x \in \mathbb{F}$, we say $x$ is **positive** if $x = \mu^2$ for some $\mu \neq 0 \in \mathbb{F}$ and we say $\mu$ is a square root of $x$. If $\mu$ is also positive then we say $\mu$ is a positive square root of $x$.

**Definition 4.** Define a field $\mathbb{F}$ to be a **definite field** if each positive element has a positive square root. If the field $\mathbb{F}$ is finite then we will refer to it as a **finite definite field**.

**Remark 1.** Observe that 2 is not positive in $\mathbb{F}_3$ but 2 is positive in $\mathbb{F}_7$. We strongly considered referring to the positive elements of $\mathbb{F}_q$ as “$q$-positive” elements and pronouncing $q$–positive as “quositive”.

**Example 2.** $\mathbb{R}$ is a definite field: Let $x = \mu^2$ for some $\mu \neq 0 \in \mathbb{R}$ and observe that $x = (|\mu|)^2$ as well and $|\mu| \neq 0 \in \mathbb{R}$. However $\sqrt{|\mu|} \neq 0 \in \mathbb{R}$ satisfies that $|\mu| = (\sqrt{|\mu|})^2$ so $x$ is positive and $|\mu|$ is a positive square root of $x$.

**Example 3.** $\mathbb{F}_3$ is a definite field: The non-zero elements are 1 and 2. Since $1^2 = 1$ and $2^2 = 1$ we see that 1 is positive and 2 is not positive (it has no square root). So if $x$ is positive then $x = 1$, setting $\mu = 1$ shows that $x$ has a positive square root.

The following example demonstrates that not all finite fields are definite.
Example 4. Consider $f : \mathbb{F}_5 \rightarrow \mathbb{F}_5$ by $f(x) = x^2$. Then $f(0) = 0$, $f(1) = f(4) = 1$, and $f(2) = f(3) = 4$. Then, 1 and 4 are the positive elements of $\mathbb{F}_5$. Observe that 1 has two positive square roots (itself and 4), however both of the square roots of 4 are non-positive. Therefore, $\mathbb{F}_5$ is not a definite field.

Definition 5. (7) The Legendre symbol $\left( \frac{a}{p} \right)$ for an integer $a$ and an odd prime $p$ is defined as

$$
\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if there exists a nonzero } x \text{ such that } x^2 \equiv a \pmod{p} \\
0 & \text{if } a \equiv 0 \pmod{p} \\
-1 & \text{otherwise}
\end{cases}
$$

Lemma 1 (7). Let $p$ be an odd prime. The quadratic character of $-1$ modulo $p$ depends only on whether $p$ is 1 or 3 modulo 4. That is,

$$
\left( \frac{-1}{p} \right) = \begin{cases} 
1 & \text{if } p \equiv 1 \pmod{4} \\
-1 & \text{if } p \equiv 3 \pmod{4}
\end{cases}
$$

Lemma 1 can be used to show that $\mathbb{F}_p$ (a prime of the form $p \equiv 3 \pmod{4}$) is definite if and only if $p \equiv 3 \pmod{4}$. Suppose first that $p \equiv 1 \pmod{4}$ and let $a$ be a positive element of $\mathbb{F}_p$. Then for some $\mu \not\equiv 0 \in \mathbb{F}_p$ we have $\mu^2 = a$ and therefore $(-\mu)^2 = a$ as well. Since the Legendre symbol is multiplicative

$$
\left( \frac{\mu}{p} \right) \left( \frac{-\mu}{p} \right) = - \left( \frac{-\mu}{p} \right)
$$

so either $\left( \frac{a}{p} \right) = 1$ or $\left( \frac{-a}{p} \right) = 1$ which implies that $a$ has a positive square root and therefore $\mathbb{F}_p$ is a definite field. Suppose now that $p \equiv 1 \pmod{4}$. Since squaring (non-zero elements) is a two-to-one function, it is not possible for every element to be positive. Let $b$ be a non-positive element of $\mathbb{F}_p \setminus \{0\}$ and let $a = b^2$ (so $a$ is positive). Now

$$
\left( \frac{b}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{-b}{p} \right) = \left( \frac{-b}{p} \right)
$$

so $-b$ is a non-positive as well. It follows (by the Fundamental Theorem of Algebra) that $a$ does not have a positive square root and therefore $\mathbb{F}_p$ is not a definite field. Unfortunately this simple argument doesn’t extend to $\mathbb{F}_q$ where $q$ is a proper prime power. To see this one simply needs to observe that the non-prime analog of the Legendre symbol would have (weaker) implications for $\mathbb{Z}/q\mathbb{Z}$ but not for $\mathbb{F}_q$.

Theorem 1. Let $\mathbb{F}_q$ be a finite field. $\mathbb{F}_q$ is a finite definite field if and only if $\mathbb{F}_q$ has characteristic two or $q = p^k$ where $k$ is a positive odd integer and $p \equiv 3 \pmod{4}$.

Proof. If $\mathbb{F}_q$ has characteristic 2 then the Frobenius map $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ given by $f(x) = x^2$ is an automorphism and therefore every element of $\mathbb{F}_q$ has a square root. Suppose now that $q = p^k$ where $p$ is an odd prime and $k$ is a positive integer. Let $\mathcal{P} = \mathcal{P}(\mathbb{F}_q)$ be the set of positive elements in $\mathbb{F}_q$ and $\mathcal{P}_* = (\mathbb{F}_q \setminus \{0\}, \cdot)$ be the multiplicative group of $\mathbb{F}_q$. Since $\mathcal{P}_*$ is cyclic, there exists an element $a$, such that the $q-1$ elements of $\mathcal{P}_*$ are $a, a^2, \ldots, a^{q-2}, a^{q-1} = 1$. Thus, $\mathcal{P} = \{(a)^2, (a^2)^2, \ldots, (a^{q-2})^2, (a^{q-1})^2\} = \{a^2, a^{2^2}, \ldots, a^{2^{q-2}}, a^{2^{q-1}}\}$. However $a^{q-1} = a^{q-1} = a^{q-1}$ so

$$
\mathcal{P} = \left\{a^2, a^4, \ldots, a^{2^{q-2}}, a^{2^{q-1}}\right\}
$$

Recall that $\mathcal{P}_*$ is a definite field if for each $y \in \mathcal{P}$ there is a $r \in \mathcal{P}$ such that $r^2 = y$. That is, if and only if for all $1 \leq t \leq \frac{q-1}{2}$ there is an integer $s$ such that $1 \leq s \leq \frac{q-1}{2}$ and $r^2 = (a^{2s})^2 = a^{2t} = y$. This occurs if and only if $2s \equiv t \pmod{\frac{q-1}{2}}$ has a solution for all $1 \leq t \leq \frac{q-1}{2}$. That is, if and only if $2k \equiv 1 \pmod{\frac{q-1}{2}}$ has a solution. Observe that

$$
q = \begin{cases} 
3 \pmod{4}, & \text{if } p \equiv 3 \pmod{4} \text{ and } k \text{ is odd} \\
1 \pmod{4}, & \text{otherwise}
\end{cases}
$$

2Indeed, this argument shows that every perfect field of characteristic 2 is definite.
It follows that if \( p \equiv 3 \pmod{4} \) and \( k \) is odd then \( \frac{p-1}{2} \) is an odd integer and therefore \( 2s \equiv 1 \pmod{\frac{p-1}{2}} \) has a solution. Therefore if \( p \equiv 3 \pmod{4} \) and \( k \) is odd then \( \mathbb{F}_{p^k} \) is a definite field. Suppose now that \( k \) is even or \( p \equiv 1 \pmod{4} \). Since \( q = p^k \equiv 1 \pmod{4} \) then \( \mathbb{F}_q \) has order \( q - 1 \) which is divisible by \( 4 \) so some element of \( \mathbb{F}_q^* \) has order \( 4 \). That is, there are elements \( b, c \in \mathbb{F}_q \setminus \{1\} \) such that \( c^2 = b \) and \( b^2 = 1 \). Hence \( b \neq 1 \in \mathcal{P} \). Define \( f : \mathcal{P} \to \mathcal{P} \) by \( f(x) = x^2 \). Since \( \mathbb{F}_q \) is finite but \( f(1) = f(b) \), it follows that \( f \) is not an onto map and therefore for some \( y \in \mathcal{P} \) there is no \( \mu \in \mathcal{P} \) such that \( \mu^2 = y \) and therefore \( y \) has no positive square roots. \( \square \)

**Definition 6.** A symmetric matrix, \( A \), over a finite definite field \( \mathbb{F}_q \) is said to have a **Cholesky decomposition** if \( A = LL^T \) for some lower triangular matrix \( L \in M_n(\mathbb{F}_q) \) where \( L \) has positive elements along its diagonal.

We saw in Proposition 1 that a very common definition for positive definiteness for Hermitian matrices does not translate to finite fields, however the following definition does, so it will be used throughout the paper as the main definition of positive-definite matrices over a definite field.

**Definition 7.** If \( A \) is a symmetric \( n \times n \) matrix over a definite field, \( A \) is **positive definite** if it possesses a Cholesky decomposition.

In the following theorem and throughout this paper, \( M_n(\mathbb{F}_q) \) refers to the set (or space) of \( n \times n \) matrices with entries in \( \mathbb{F} \). The following results are finite-field adaptations of standard results from elementary number theory \[7\] and linear algebra \[6\]. For the curious reader, we have included brief proofs in the appendix.

**Theorem 2.** If \( A \in M_n(\mathbb{F}_q) \) and \( A = LL^T \) for some lower triangular matrix \( L \in M_n(\mathbb{F}_q) \) whose diagonal elements are all nonzero, then the leading principal minors of \( A \) are positive.

**Lemma 2.** If \( A \) is a symmetric matrix over a definite field with an \( LDU \) decomposition where \( L \) and \( U \) have all ones along their diagonals and the diagonal entries of \( D \) are positive, then \( A \) has a Cholesky decomposition.

**Lemma 3.** Let \( A_k \) be the \( k \times k \) leading principal submatrix of an \( n \times n \) matrix \( A \). If \( A \) has an \( LDU \) factorization, \( A = LDU \), where \( L \) is a lower triangular matrix with all ones along its diagonal, \( U \) is upper triangular with all ones along its diagonal, and \( D \) is diagonal, then \( \det(A_k) = d_{11}d_{22}\cdots d_{kk} \). The 1st pivot is \( d_{11} = \det(A_1) = a_{11} \) and the \( k \)th pivot for \( k = 2, 3, \cdots, n \) is \( d_{kk} = \det(A_k)/\det(A_{k-1}) \), where \( d_{kk} \) is the \((k,k)\)-th entry of \( D \) for all \( k = 1, 2, \cdots, n \).

**Lemma 4.** If \( A \) is a symmetric matrix over a definite field with an \( LDU \) decomposition where \( L \) and \( U \) have all ones along their diagonals and the entries of \( D \) are positive, then \( A \) has a Cholesky decomposition.

**Theorem 3** (Corollary 3.5.5 of \[4\]). If \( A \) is invertible, then it admits an \( LDU \) factorization if and only if all its leading principal minors are nonsingular.

**Corollary 1.** If all leading principal minors of a symmetric matrix \( A \) over a definite field are positive, then \( A \) has a Cholesky decomposition.

**Lemma 5.** All leading principal submatrices of a Gram matrix are also Gram matrices.

**Theorem 4.** A matrix, \( M \in M_n(\mathbb{F}_q) \), is a Gram matrix if and only if it is positive definite.

### 3 Counterexamples

There are some properties of positive-definiteness, however, which no longer hold over definite fields. Since real matrices are covered by the Hermitian case, we turn our attention specifically to **finite** definite fields. In this section, we consider the a number of classical equivalences which do not hold and present counterexamples. We also take a look into some of the other properties of Hermitian positive definite matrices and provide counterexamples to show they cannot hold over finite fields.

**Theorem 5.** If \( A \) is a positive definite Hermitian matrix, that is, over \( \mathbb{R} \), or \( \mathbb{C} \), the following hold:
1. A has positive eigenvalues.
2. The associated sesquilinear form is an inner product.
3. All principal submatrices of A are positive definite.
4. \( A^{-1} \) is positive definite.
5. If \( B \) is a positive definite Hermitian matrix, then \( A + B \) is positive definite.
6. If \( B \) is a positive definite Hermitian matrix, then \( ABA \) and \( BAB \) are positive definite.
7. If \( B \) is a positive definite Hermitian matrix, then the Hadamard product \( A \circ B \) is positive definite and the Frobenius inner product, \( A : B \) is positive.

**Theorem 6.** The properties of Theorem 5 do not hold in general over finite definite fields.

**Proof.** We provide at least one counter example from a definite field for each property or explain why the described property does not hold.

1. The following matrix, in \( \mathcal{M}_2(\mathbb{F}_7) \), is positive definite as all leading principal minors are positive in \( \mathbb{F}_7 \) but has eigenvalues of 6 and 5, which are not positive in the field.

\[
\begin{bmatrix}
2 & 4 \\
4 & 2 \\
\end{bmatrix}
\]

For another example, consider the following in \( \mathcal{M}_3(\mathbb{F}_3) \), which has eigenvalues 1,2,2.

\[
\begin{bmatrix}
1 & 0 & 2 \\
0 & 1 & 1 \\
2 & 1 & 0 \\
\end{bmatrix}
\]

One might hope that the converse still holds, that positive eigenvalues always indicate that a matrix is positive definite, but this sadly is also untrue. The following matrix over \( \mathbb{F}_7 \) has eigenvalues of 1 and 2, which are positive in \( \mathbb{F}_7 \), but not all leading principal minors are positive for the matrix, thus it is not positive definite.

\[
\begin{bmatrix}
6 & 6 \\
6 & 4 \\
\end{bmatrix}
\]

2. The sesquilinear form defined by a matrix \( A \) is a function from \( \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n \) given by \( \langle x, y \rangle = y^T Ax \) for \( x, y \in \mathbb{F}_q^n \). For this to be an inner product, we must have that \( \langle x, x \rangle \) is nonzero and positive for all nonzero \( x \). However, in finite fields this form is isotropic, as seen in Proposition 1 and therefore can be zero for nonzero \( x \).

3. The following matrix, in \( \mathcal{M}_3(\mathbb{F}_3) \), is positive definite:

\[
\begin{bmatrix}
1 & 2 & 0 \\
2 & 2 & 0 \\
0 & 0 & 1 \\
\end{bmatrix}
\]

however it contains principal submatrix \( \begin{bmatrix}
2 & 0 \\
0 & 1 \\
\end{bmatrix} \) which is not positive definite (evaluate the determinant).

For another example, consider the following matrix in \( \mathcal{M}_3(\mathbb{F}_2) \), which is positive definite:

\[
\begin{bmatrix}
1 & 1 & 0 \\
1 & 0 & 0 \\
0 & 0 & 1 \\
\end{bmatrix}
\]
One principal submatrix is \[
\begin{bmatrix}
0 & 0 \\
0 & 1
\end{bmatrix},
\] which is not positive definite (evaluate the determinant). In general, there are many positive definite matrices with elements along the diagonal which are not positive. Taking a principal submatrix that causes one of these elements to be in the upper left corner will produce a submatrix that is not positive definite.

4. The following matrix, \( M_3(\mathbb{F}_3) \), is positive definite:

\[
\begin{bmatrix}
1 & 2 & 0 \\
2 & 2 & 0 \\
0 & 0 & 1
\end{bmatrix}
\]

However, we have that \( A^{-1} \) is

\[
\begin{bmatrix}
2 & 1 & 0 \\
1 & 1 & 0 \\
0 & 0 & 1
\end{bmatrix}
\]

which is not positive definite, since in particular \( A_1 = [2] \) does not have positive determinant. For another example, consider the following matrix, in \( M_3(\mathbb{F}_2) \), which is positive definite:

\[
\begin{bmatrix}
1 & 1 & 1 \\
1 & 0 & 0 \\
1 & 0 & 1
\end{bmatrix}
\]

However,

\[
A^{-1} = \begin{bmatrix}
0 & 1 & 0 \\
1 & 0 & 1 \\
0 & 1 & 1
\end{bmatrix}
\]

which is not positive definite, as \( A_1 = [0] \) does not have a positive determinant.

5. Consider the following in \( M_3(\mathbb{F}_2) \):

\[
\begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{bmatrix} + \begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{bmatrix} = \begin{bmatrix}
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0
\end{bmatrix}
\]

The identity matrix is positive definite, yet the zeros matrix is obviously not.

6. Consider the following positive definite matrices in \( M_2(\mathbb{F}_7) \):

\[
A = \begin{bmatrix}
2 & 1 \\
1 & 5
\end{bmatrix}, \quad B = \begin{bmatrix}
4 & 3 \\
3 & 6
\end{bmatrix}
\]

We have that \( ABA \) is

\[
\begin{bmatrix}
6 & 1 \\
1 & 2
\end{bmatrix}
\]

This matrix is not positive definite, since \( (ABA)_1 = [6] \) does not have positive determinant. For another example, consider the following matrices, in \( M_3(\mathbb{F}_2) \), which are positive definite:

\[
A = \begin{bmatrix}
1 & 0 & 1 \\
0 & 1 & 0 \\
1 & 0 & 0
\end{bmatrix}, \quad B = \begin{bmatrix}
1 & 0 & 1 \\
0 & 1 & 1 \\
1 & 1 & 1
\end{bmatrix}
\]

However

\[
ABA = \begin{bmatrix}
0 & 1 & 0 \\
1 & 1 & 0 \\
0 & 0 & 1
\end{bmatrix}
\]

which is not positive definite since its leading \( 1 \times 1 \) principal minor is 0.
7. Consider \[
\begin{bmatrix}
1 & 4 \\
4 & 3
\end{bmatrix}
\text{ and } \begin{bmatrix}
2 & 2 \\
2 & 3
\end{bmatrix}
\] in \( M_2(\mathbb{F}_7) \), which are both positive definite. However, their Hadamard product is \[
\begin{bmatrix}
2 & 1 \\
1 & 2
\end{bmatrix}
\] whose determinant is 3, which is not positive in \( \mathbb{F}_7 \) and therefore the matrix is not positive definite. Considering this same pair of matrices, their Frobenius inner product is 6, which is also not positive.

For another example, consider the following matrices, in \( M_3(\mathbb{F}_2) \), which are positive definite:

\[
A = \begin{bmatrix}
1 & 1 & 0 \\
1 & 0 & 1 \\
0 & 1 & 0
\end{bmatrix}, \quad B = \begin{bmatrix}
1 & 0 & 1 \\
0 & 1 & 1 \\
1 & 1 & 1
\end{bmatrix}.
\]

However, their Hadamard product is

\[
H = \begin{bmatrix}
1 & 0 & 0 \\
0 & 0 & 1 \\
0 & 1 & 0
\end{bmatrix}
\]

which is not positive definite, as \( H_2 = \begin{bmatrix}
1 & 0 \\
0 & 0
\end{bmatrix} \) does not have a positive determinant. For one more example, consider the following matrices, in \( M_3(\mathbb{F}_2) \), which are positive definite:

\[
A = \begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 1 \\
0 & 1 & 0
\end{bmatrix}, \quad B = \begin{bmatrix}
1 & 0 & 1 \\
0 & 1 & 0 \\
1 & 0 & 0
\end{bmatrix}.
\]

Their Frobenius inner product is 0, which is not positive. Observe that we need only find any pair of positive definite matrices where there is an even number of entries satisfying \( a_{ij} = b_{ij} = 1 \) and their Frobenius inner product to give a non-positive result.

\[\square\]

4 Other Properties

Some of the properties that Hermitian positive definite matrices possess do, however, analogize over definite fields.

**Theorem 7.** If \( A \) is a positive definite matrix over a definite field \( \mathbb{F} \), and \( r \) is positive in \( \mathbb{F} \), then \( rA \) is also positive definite.

**Proof.** If \( A \) is a \( n \times n \) positive definite matrix over a definite field \( \mathbb{F} \), then it possesses a Cholesky decomposition, \( A = LL^T \). If \( \det(L) = \mu \) and \( r \) is a square in \( \mathbb{F} \), that is \( r = s^2 \) for \( s \in \mathbb{F} \), then \( \det(rA) = \det(rLL^T) = \det(rL) \det(L^T) = r^n \mu \mu = s^{2n} \mu^2 = (s^n \mu)^2 \). As all leading principal submatrices have a similar decomposition, all leading principal minors of \( rA \) are positive by a similar argument and thus \( rA \) is positive definite.

In the last section, we saw that inverses of positive definite matrices over finite definite fields are not positive definite. It is true, however, that the inverse matrix conjugated by the “exchange” or “anti-diagonal identity” matrix \( \nabla \) is positive definite.

**Definition 8.** For an invertible matrix \( A \), define its anti-inverse as \( \nabla A^{-1} \nabla \) where \( \nabla \) is the exchange matrix, with ones along its antidiagonal and zeroes elsewhere. That is, in the \( n \times n \) case of \( \nabla \), \( a_{ij} = 1 \) if \( i + j = n + 1 \) and \( a_{ij} = 0 \) otherwise. For example, the \( 3 \times 3 \) case of \( \nabla \) is

\[
\begin{bmatrix}
0 & 0 & 1 \\
0 & 1 & 0 \\
1 & 0 & 0
\end{bmatrix}
\]

The following lemma will be helpful in showing that the anti-inverse is positive definite.
Lemma 6. Every principal submatrix of a lower triangular matrix is lower triangular.

Proof. Let L be a lower triangular matrix. Deleting the first column and row clearly produces a lower triangular matrix, and similarly if we delete the last row and column. Now, suppose we delete the ith row and column. We have

\[
\begin{pmatrix}
  l_{i1} & \cdots & 0 & \cdots & 0 \\
  \vdots & \ddots & \vdots & \ddots & \vdots \\
  l_{ii} & \cdots & 0 \\
  \vdots & \vdots & \ddots & \ddots & \vdots \\
  l_{n1} & \cdots & l_{ni} & \cdots & l_{nn}
\end{pmatrix} \rightarrow \begin{pmatrix}
  l_{i1} & \cdots & 0 & 0 & \cdots & 0 \\
  \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
  l_{(i-1)1} & \cdots & l_{(i-1)(i-1)} & 0 & \cdots & 0 \\
  \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\
  l_{n1} & \cdots & l_{n(i-1)} & l_{n(i+1)} & \cdots & l_{nn}
\end{pmatrix}
\]

The (i-i)th leading principal submatrix is still lower triangular. As both row and column i are removed, the original \( l_{(i+1)(i-1)} \) entry now becomes the entry \( l'_{ii} \) in the ith row and ith column of the new matrix. The rest of the matrix is shifted and retains the form of a lower triangular matrix.

Theorem 8. If A is a positive definite matrix in a definite field \( F \), then its anti-inverse is also positive definite.

Proof. Let A be a positive definite matrix in a definite field \( F \). It is invertible and thus we can consider its anti-inverse. As A is positive definite, we have \( A = LL^T \) as a Cholesky decomposition. Note that \( \nabla \nabla = I \) and therefore we have, writing \( L^{-T} = (L^{-1})^T \),

\[
A^{-1} = L^{-T}L^{-1} \\
\nabla A^{-1} \nabla = \nabla L^{-T} L^{-1} \nabla \\
= \nabla L^{-T} (\nabla \nabla) L^{-1} \nabla \\
= (\nabla L^{-T} \nabla) (\nabla L^{-1} \nabla)
\]

Note that right multiplying by \( \nabla \) reverses the columns of the matrix and left multiplication by \( \nabla \) reverses the rows. Thus, \( \nabla L^{-T} \nabla \) takes an upper triangular matrix, \( L^{-T} \), to a lower triangular matrix and \( \nabla L^{-1} \nabla \) takes a lower triangular matrix to an upper triangular matrix. In fact, we have

\[
(\nabla L^{-T} \nabla)^T = (\nabla L^{-1} \nabla)
\]

Thus, \( \nabla A^{-1} \nabla \) takes the correct form to have a Cholesky decomposition. We need only check the diagonal elements of \( \nabla L^{-T} \nabla \) are positive. As both the rows and columns are reversed by conjugating by \( \nabla \), the diagonal elements of \( L^{-T} \) are still the diagonal elements of \( \nabla L^{-T} \nabla \), simply in a different order. As \( LL^T \) is a Cholesky decomposition of A, the diagonal elements of L are positive, and we need only check that the diagonal elements of \( L^{-1} \) are positive.

When taking the inverse of L, the \( (i,i) \) entry will be 1/\( \det(L) \) multiplied by the principal minor of the submatrix created by deleting the ith row and ith column. As this submatrix will be lower triangular and have diagonal elements which are a subset of those from L, the principal minor will be positive. Thus, the ith diagonal element of \( L^{-1} \) is positive. As the diagonal elements of \( L^{-1} \) are positive, so are those of \( L^{-T} \). Thus, \( (\nabla L^{-T} \nabla)(\nabla L^{-1} \nabla) \) is a Cholesky decomposition for \( \nabla A^{-1} \nabla \).

In the last section, we provided counterexamples that proved the Hadamard product and the Frobenius product need not be positive definite nor positive respectively. It is true, however, that the Kronecker product of two positive definite matrices, even for definite fields, is positive definite.

Theorem 9. If A and B are positive definite matrices in a definite field \( F \), then so is their Kronecker product. In fact, if \( A = LL^T \) and \( B = MM^T \) then \( A \otimes B = (L \otimes M)(L \otimes M)^T \).
**Proof.** Let $A$ and $B$ be $n \times n$ positive definite matrices in a definite field $F$, with $A = LL^T$ and $B = MM^T$ their Cholesky decompositions.

\[ L \otimes M = \begin{bmatrix} l_{11}M & 0 & \cdots & 0 \\ l_{21}M & l_{22}M & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ l_{k1}M & l_{k2}M & \cdots & l_{kk}M \end{bmatrix}, \]

\[ (L \otimes M)^T = \begin{bmatrix} l_{11}M^T & l_{21}M^T & \cdots & l_{k1}M^T \\ 0 & l_{22}M^T & \cdots & l_{k2}M^T \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & l_{kk}M^T \end{bmatrix}. \]

Consider $(L \otimes M)(L \otimes M)^T$. When calculating any entry of this product, we will have a sum of scalars each multiplied by $MM^T$, and so we may factor this out by the distributivity of matrices over scalars. The sum of scalars, if considering the $(i, j)$th entry, is produced from the dot product of the $i$th row of $L$ with the $j$th column of $L^T$, exactly $a_{ij}$, the entry of $a$ in the $i$th row and $j$th column. Thus, the $(i, j)$th entry of $(L \otimes M)(L \otimes M)^T$ is $a_{ij}M^T M = a_{ij}B$ and thus $(L \otimes M)(L \otimes M)^T = A \otimes B$.

We need only check that the diagonal of $(L \otimes M)$ is positive. The diagonal elements of $L \otimes M$, as $M$ is lower triangular, are comprised of the diagonal elements of $L$ multiplied by the diagonal elements of $M$. As the diagonal elements of both $L$ and $M$ are positive, their product will also be positive. Thus, $A \otimes B$ has a Cholesky decomposition and is therefore positive definite.

\[ \square \]

## 5 Pressing Sequences

**Definition 9.** Let a $F$-pseudograph, for some field $F$, be a graph $G = (V, f)$ with $V$ the set of vertices and $f : V \times V \to F$ a function assigning a weight to each edge. That is, $f(x, y) = c$ assigns a weight of $c \in F$ to the edge $xy$, and $f(x, x)$ is a weight assigned to the vertex $x \in V$. Each edge has only one associated weight, i.e., $f(x, y) = f(y, x)$. Note every pair of distinct vertices admits an edge, though some may simply have weight 0 and sometimes $G$ is then identified with the restriction of $f$ to its support.

For a vertex, we may refer to the vertex by its weight if the vertex label is understood. That is, if there is only one vertex of weight $d$, it may be referred to as vertex $d$. If there are more than one vertex with weight $d$, it will be referred to as vertex $v$ with weight $d$.

**Definition 10.** The weighted adjacency matrix of a $F$-pseudograph $G$ is $A(G)$ defined in the following way. Let $v_1, \ldots, v_n$ be the vertices of $G$.

\[ a_{ij} = f(v_i, v_j) \]

Clearly, the resulting matrix is symmetric.

**Definition 11.** Consider a $F-$pseudograph $G = (V, f)$. For a vertex $v$, with $f(v, v)$ positive in $F$, pressing $v$ is the process of taking $G$ to $G' = (V, g)$ with

\[ g(x, y) = f(x, y) - \frac{f(x, v)f(y, v)}{f(v, v)} \]

Note that such a press will also yield a symmetric weighted adjacency matrix $A(G')$. The following figure illustrates a general press on the vertex with weight $a$:

The weighted adjacency matrices for the graphs in the figure as follows:

\[ A(G) = \begin{bmatrix} a & x & y \\ x & b & z \\ y & z & c \end{bmatrix}, \quad A(G') = \begin{bmatrix} 0 & 0 & 0 \\ 0 & b - \frac{x^2}{a} - \frac{xy}{a} & z - \frac{xy}{a} \\ 0 & \frac{xy}{a} & c - \frac{y^2}{a} \end{bmatrix} \]
Pressing in this fashion has the same effect as Gaussian elimination, except without row swaps, and such that the rows corresponding to pressed vertices are self-eliminated. A “successful pressing sequence” exists if we can complete this elimination to result in the all-zeroes matrix, which corresponds to the edgeless graph with vertices of weight 0.

**Theorem 10.** For a $\mathbb{F}$–pseudograph $G = (V, f)$, the vertices of $G$ in the usual order form a successful pressing sequence if and only if $A(G)$ is positive definite.

**Proof.** Let $G = (V, f)$ be a $\mathbb{F}$-pseudograph, and $A(G)$ its weighted adjacency matrix.

Suppose the vertices of $G$ – in the order they are presented as indices of $A(G)$ – form a successful pressing sequence. Thus, we can perform ordinary Gaussian elimination with no row swaps via the same process but omitting self-elimination steps, resulting in an $LU$ decomposition. Each such elimination step begins by multiplying $A(G)$ by an elementary matrix $E_1$ on the left; the elements on the diagonal of $E_1$ are 1 as we are not changing the entry associated with the vertex pressed, and $E_1$ is also lower triangular. As $A(G)$ is symmetric, the elimination can proceed by performing the same operations on columns, represented by right multiplication by $E_1^T$. That is, after the elimination operations arising from a press without self-elimination, we have $A(G') = E_1 A(G) E_1^T$.

If $G$ has a successful pressing sequence, it has a sequence of such Gaussian elimination steps which result in a diagonal matrix. That is, $E A(G) E^T = D$ for $E$ a product of elementary matrices representing row operations where the diagonal entries of $E$ are 1 and $D$ a diagonal matrix whose entries are the weights of the vertices before being pressed. As we only press positively weighted vertices, $D$ has all positive entries. In fact, $A(G) = E^{-1} D E^{-T}$. As $E$ is lower diagonal, so is $E^{-1}$ and in a similar fashion, $E^{-T}$ is upper triangular. Thus, $A(G)$ has a positive LDU decomposition and by Lemma 4, $A(G)$ has a Cholesky decomposition and is therefore positive definite.

If $A(G)$ is positive definite, it has a Cholesky decomposition $A(G) = LL^T$. As the diagonal entries of $L$ are positive, we have $A(G) = L'D(L')^T$ where $L'$ has all ones along its diagonal and $D$ is a diagonal matrix with all positive entries. So $L'^{-1}A(G)L'^{-T} = D$ and $A(G)$ can be row- and column-reduced without swaps to a diagonal matrix with all positive entries. Thus $G$ has a Gaussian elimination sequence without row swaps resulting in a positive diagonal matrix and also has a successful pressing sequence by pressing the vertices in the same order.

6 Future Work

Over $\mathbb{F}_2$ a graph has a successful pressing sequence if and only if each component contains at least one non-white vertex (13). This characterization does not work over other fields (for example the $\mathbb{F}_3$ pseudograph with three vertices, each of weight 1, and three edges, each of weight 2, is not pressable in any
order). Furthermore, while it is a necessary condition that each component contain a positive vertex, this characterization does not suffice. Thus, we ask the following question: Is there a polynomial-time algorithm to check whether a given pseudo-graph over a finite field is pressable in some order?

We have discussed positive definite matrices over definite fields and described many equivalences which can be analogized from the Hermitian case, and others which cannot. It would be perhaps be interesting also to consider semi-definiteness or negative definiteness over definite fields.

In particular, we briefly considered but never truly investigated the possibility of using the Frobenius endomorphism to define some kind of Hermitian-like structure on these matrices. That is, instead of a conjugate transpose, what would happen if we applied the Frobenius map to every element of the matrix and then take the transpose? This notion may still cause a problem in the positive definite case, as we can simply take a vector in the base field, for which the “Frobenius transpose” would simply be the transpose, and could still produce $x^TAx = 0$ for some nonzero vector $x$. In terms of positive semi-definiteness, however, we wonder if this can be remedied and prove interesting. We would be especially keen to restore the important role of positive eigenvalues in the theory of positive definiteness, perhaps by redefining “positive” via Frobenius endomorphisms.

It would also be interesting to consider whether nondefinite fields have some semblance of a positive definite structure given the right definitions. Furthermore, we identified counterexamples above to show that some classical properties do not hold over finite definite fields. Could there be, however, a subset of finite definite fields for which some of these properties still indeed hold? For instance, can the positive eigenvalue equivalence be salvaged over a certain subset of definite fields?

We also wonder what applications the above framework might find. As positive definite matrices are used often in optimization problems, does this notion of positive definite over definite fields induce an analogue of geometric convexity over other fields besides $\mathbb{R}$ and $\mathbb{C}$? Can we solve optimization problems over finite fields?

References

[1] Bixby, E., Flint, T. and Miklós, I. (2015) Proving the pressing game conjecture on linear graphs. Involve, a Journal of Mathematics, 9(1):41-46.
[2] Chevalley, C. (1935) Démonstration d’une hypothese de M. Artin. Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg. 11(1).
[3] Cooper, J. and Davis, J. (2016). Successful Pressing Sequences for a Bicolored Graph and Binary Matrices. Linear Algebra and its Applications, 490:162-173.
[4] Cooper, J. and Whitlatch, H. (2019). Uniquely Pressable Graphs: Characterization, Enumeration, and Recognition. Advances in Applied Mathematics, 103:13-42.
[5] Hannenhalli, S. and Pevzner, P. (1999) Transforming cabbage into turnip: Polynomial algorithm for sorting signed permutations by reversals. J. ACM, 46(1):1–27.
[6] Johnson, C. and Horn, R. (1985). Matrix Analysis. Cambridge University Press.
[7] Hardy, G. Wright, E. et al. (1979) An Introduction to the Theory of Numbers. Oxford University Press.

7 Appendix

Proof of Theorem

Proof. Let $A \in M_n(\mathbb{F}_q)$ such that $A = LL^T$ for some lower triangular matrix $L \in M_n(\mathbb{F}_q)$ whose diagonal entries are nonzero. Let $L_i$ denote the $i^{th}$ leading principal submatrix of $L$. For each $1 \leq i \leq n$, let $\mu_i = \det(L_i)$ and observe that $\mu_i \neq 0 \in \mathbb{F}_q$. Then the $i^{th}$ leading principal submatrix of $A$ will have decomposition $A_i = L_i L_i^T$ and therefore $\det(A_i) = \det(L_i)\det(L_i^T) = \mu_i^2 \neq 0$.

Proof of Lemma

Proof. Let $A$ be a symmetric matrix over a definite field with an $LDU$ decomposition such that all entries of $D$ are positive and all diagonal entries of $L$ and $U$ are 1. The symmetry of $A$ and the uniqueness of the $LDU$ decomposition will yield $U = L^T$. As the diagonal entries of $D$ are positive, $\sqrt{D}$ can be defined, and
we construct it in the following way: Set $\sqrt{D} = \text{diag}(s_{1,1}, \ldots, s_{n,n})$ where $s_{i,i}$ is the positive square root of the element in the $i^{th}$ row and column of $D$. Since both $L$ and $\sqrt{D}$ have zeros above the diagonal then $B = L\sqrt{D}$ is a lower triangular matrix and $A = BB^T$, as desired. □

Proof of Lemma 3

Proof. Let $A_k$ be the $k \times k$ leading principal submatrix of an $n \times n$ matrix $A$. Let $A$ have an $LDU$ factorization, $A = LDU$, where $L$ is a lower triangular matrix with all ones along its diagonal, $U$ is upper triangular with all ones along its diagonal, and $D$ is diagonal. Note that as $A$ has an $LU$ decomposition, all leading principal submatrices have full rank and thus all leading principal minors are nonzero.

Partition $A$ in the following way:

$$A = \begin{bmatrix} L_k & 0 \\ L_{21} & L_{22} \end{bmatrix} \begin{bmatrix} D_k & 0 \\ 0 & D_{22} \end{bmatrix} \begin{bmatrix} U_k \ 0 \\ U_{22} \end{bmatrix}$$

We thus have that $A_k$ can be written in the following manner:

$$A_k = L_k D_k U_k = \begin{bmatrix} L_{k-1} & 0 \\ d & 1 \end{bmatrix} \begin{bmatrix} D_{k-1} & 0 \\ 0 & d_{kk} \end{bmatrix} \begin{bmatrix} U_{k-1} \ 0 \\ 0 \ 1 \end{bmatrix}$$

For $k = 1$, we have $A_1 = [1][d_{11}][1]$ and thus $\det(A_1) = d_{11} = a_{11}$. If the result holds for $\ell < k$, we have $\det(A_k) = \det(D_{k-1})d_{kk} = \det(A_{k-1})d_{kk} = d_{11} \cdots d_{kk}$. The result follows as the pivots are exactly the entries of $D$. □

Proof of Lemma 4

Proof. Let $A$ be a symmetric matrix over a definite field with an $LDU$ decomposition such that all entries of $D$ are positive and all diagonal entries of $L$ and $U$ are 1. The symmetry of $A$ and the uniqueness of the $LDU$ decomposition will yield $U = L^T$. As the elements of $D$ are positive, $\sqrt{D}$ can be defined, and we construct it in the following way. If $r_{ii} = \sqrt{d_{ii}}$:

$$\sqrt{D} = \text{diag}(d'_{11}, d'_{22}, \ldots, d'_{nn}) = \begin{cases} d'_{ii} = r_{ii} & \text{if } r_{ii} \text{ is positive} \\ d'_{ii} = -r_{ii} & \text{otherwise} \end{cases}$$

Thus, $\sqrt{D}$ is a diagonal matrix with positive diagonal entries. Define $R = L\sqrt{D}$. As $L$ has a diagonal of all 1’s, $R$ is a lower triangular matrix with positive diagonal entries and $A = RR^T$ as desired. □

Proof of Corollary 1

Proof. Let $A$ be a symmetric matrix in $M_n(\mathbb{F})$ for a definite field $F$ such that all leading principal minors are positive. Thus, all leading principal submatrices have full rank and $A$ is invertible. So, $A = LDU$ where $D$ is a diagonal matrix and $U$ and $L$ have all ones on their diagonal. The symmetry of $A$ and the uniqueness of the $LDU$ decomposition will yield that $U = L^T$. As all leading principal minors are positive, the pivots of $A$, found by the process described in Lemma 3, are positive and are, in fact, the diagonal entries of $D$. Thus, as we have an $LDU$ decomposition where all the diagonal elements of $D$ are positive, by Lemma 4 we can define $R = L\sqrt{D}$, a lower triangular matrix with positive diagonal entries, and $A = RR^T$ as desired. □

Proof of Lemma 5

Proof. Let $G$ be a Gram matrix of vectors $v_1, v_2, \ldots, v_n$. That is,

$$G = \begin{bmatrix} \langle v_1, v_1 \rangle & \langle v_1, v_2 \rangle & \cdots & \langle v_1, v_n \rangle \\ \langle v_2, v_1 \rangle & \langle v_2, v_2 \rangle & \cdots & \langle v_2, v_n \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle v_n, v_1 \rangle & \langle v_n, v_2 \rangle & \cdots & \langle v_n, v_n \rangle \end{bmatrix}$$
Any leading principal submatrix, $G_k$ will take the form

\[
G_k = \begin{bmatrix}
\langle v_1, v_1 \rangle & \langle v_1, v_2 \rangle & \cdots & \langle v_1, v_k \rangle \\
\langle v_2, v_1 \rangle & \langle v_2, v_2 \rangle & \cdots & \langle v_2, v_k \rangle \\
\vdots & \vdots & \ddots & \vdots \\
\langle v_k, v_1 \rangle & \langle v_k, v_2 \rangle & \cdots & \langle v_k, v_k \rangle
\end{bmatrix}
\]

Thus, $G_k$ is a Gram matrix on the vectors $v_1, v_2, \ldots, v_k$ as these vectors are still linearly independent. □

Proof of Theorem 4

Proof. Let $M \in \mathcal{M}_n(\mathbb{F}_q)$. Suppose $M$ is a Gram matrix. Thus, $M = A^T A$ where the columns of $A$ are $x_1, x_2, \ldots, x_n \in \mathbb{F}_q^n$, which are linearly independent. Now, $M_k$ will be equivalent to $A_k^T A_k$ where $A_k$ has columns $x_1, \ldots, x_k$ by Lemma 5. We have

\[
\det(M_k) = \det(A_k^T A_k) = \det(A_k)^2
\]

for $\det(A_k)^2 \in \mathbb{F}_q$. As all leading principal minors are positive, $A$ is positive definite.

Now suppose that $M$ is a positive definite matrix. Thus, $M = LL^T$ with the columns of $L$ denoted by $l_1, l_2, \ldots, l_n$. As $M$ is invertible, so is $L$ and thus these $l_i$ are linearly independent. $M$ is therefore a Gram matrix for the vectors $l_1, l_2, \ldots, l_n$. □