2018

A Quest for Positive Definite Matrices over Finite Fields

Erin Patricia Hanna
University of South Carolina

A Quest for Positive Definite Matrices over Finite Fields

by

Erin Patricia Hanna

Bachelor of Arts
Eastern University 2016

Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science in

Mathematics

College of Arts and Sciences

University of South Carolina

2018

Accepted by:

Joshua Cooper, Director of Thesis

Alexander Duncan, Reader

Cheryl L. Addy, Vice Provost and Dean of the Graduate School

Acknowledgments

There are many people who have helped me reach this point in my academic career. Special thanks to Dr. Joshua Cooper for taking on yet another student and giving me an interesting question to explore, and for being the most patient, amazing adviser I could have ever hoped for. To Hays Whitlatch for being a bit of a "research big brother", helping me get back on track when I got stuck, and taking time to read my writing and suggest improvements, thank you. Thanks to Dr. Alexander Duncan for also taking the time to thoroughly comb through my writing and providing great feedback. This thesis could not have come together without their help.

To my math professors from Eastern University, Walt Huddell, Nicola McLallen and Chris Micklewright, thank you for encouraging me to pursue a graduate degree in mathematics in the first place. Thank you so much for the positive atmosphere you create and for encouraging the mathematicians of Eastern to pursue great things. I would not have arrived at the University of South Carolina without you.

Of course, thanks go out to my family for standing behind me in every endeavor I pursue. Thanks Mom and Dad, having your support is immeasurable. Likewise, great thanks to Adrian Clements, for listening to me rant about research he did not quite fully understand, and being patient when stress overwhelmed me. You always reminded me I could do this no matter how crazy it was getting. Thank you.

To all those at USC who have helped me grow mathematically, thank you. Of particular note, thanks to Dr. Alexander Duncan once again and Dr. Maria Girardi for being amazing algebra and analysis professors for us in our first year. My mathematical skills have increased more than I could have ever imagined thanks to your

patient teaching and wisdom. Also, to “the guys” of LeConte 104, immense thanks for always putting a smile on my face even when stress was crushing us. Thanks for your patient help when I got stuck, and for being really great people I was always happy to see each day.

These and so many others have helped me to get to this point of compiling this thesis and pursuing a higher degree in mathematics. I am forever grateful. A million thank-you’s.

Abstract

Positive definite matrices make up an interesting and extremely useful subset of Hermitian matrices. They are particularly useful in exploring convex functions and finding minima for functions in multiple variables. These matrices admit a plethora of equivalent statements and properties, one of which is an existence of a unique Cholesky decomposition. Positive definite matrices are not usually considered over finite fields as some of the definitions and equivalences are quickly seen to no longer hold. Motivated by a result from the theory of pressing sequences, which almost mirrors an equivalent statement for positive definite Hermitian matrices, we consider whether any of the theory of positive definiteness can be analogized for matrices over finite fields. New definitions are formed based on this motivation to be able to discuss positive definiteness in certain finite fields, relying heavily on the notion of the existence of a unique Cholesky decomposition. We explore what equivalences of positive definite Hermitian matrices can be analogized and present counterexamples for those which are still seen to fail. The final result not only holds for finite fields, but a certain subset of fields with a desired property.

Table of Contents

List of Figures

Chapter 1

Introduction

1.1 History of Positive Definiteness

The theory of positive definiteness is vast and reaches throughout many branches of mathematics. Applications for positive definiteness can reach into functional and harmonic analysis, representations of Lie groups, spectral theory, quantum physics, operator theory, and optimization. There are a few different definitions for which something is called "positive definite". The following definition is one of the most generalized. Given a nonempty set X, a symmetric function $\varphi : X \times X \to \mathbb{C}$ is called a *positive definite kernel* on X if and only if

$$\sum_{j,k=1}^{n} c_k \overline{c_k} \varphi(x_j, x_k) \geq 0$$

holds for any $n \in \mathbb{N}$, $x_1, ..., x_n \in X$ and $c_1, ..., c_n \in \mathbb{C}$. It is important to note that a positive definite kernel defined on a finite set is usually called a positive semidefinite matrix, as noted in [2]. A *positive definite function* of a real variable x is a complex-valued function $f : \mathbb{R} \to \mathbb{C}$ such that for any real numbers $x_1, ..., x_n$, the $n \times n$ matrix

$$A = (a_{ij})_{i,j=1}^{n}, \quad a_{ij} = f(x_i - x_j)$$

is positive semi-definite. It is interesting to note that for positive definite kernels restricted to finite sets, and positive definite functions for finite n, one can talk about the positive definite matrices behind them.

While positive definiteness has a long and vast history, work on positive definiteness did not gain popularity until the 20th century. However, as noted in [5], the

most famous occurrence of a positive definite kernel, the Gaussian kernel, appeared in Gauss's paper *Theoria motus corporum coelestium in sectionibus conicis solem ambientium* in 1806. The Gaussian kernel is

$$K(x, y) = e^{-\epsilon^2|x-y|^2}, \quad x, y \in \mathbb{R}, \epsilon > 0.$$

Work in the 20th century branched in two directions. Some focused on positive definite functions, while others continued to study positive definite kernels. Early work in positive definite functions began with Maximilian Mathias in 1923, see [9], and most early researchers of positive definite functions were mainly concerned with their connections to Fourier analysis. Concerning the the study of positive definite kernels, James Mercer is usually noted as the first to consider a positive definite kernel over a nonfinite set in 1909, see [2]. He defined a continuous and symmetric real-valued function to be of *positive type* if and only if

$$\int_a^b \int_a^b c(x)c(y)\varphi(x, y)dxdy \geq 0$$

holds for all continuous functions $c : [a, b] \to \mathbb{R}$. He goes on to show that this condition is equivalent to φ being a positive definite kernel.

Further work by Issai Schur in 1911 proved that the product of two positive definite kernels is positive definite, and C.H. Fitzgerald and R.A. Horn (1977) came to the conclusion that if (a_{ik}) is a positive definite $n \times n$ matrix with non-negative entries, then for all real $\alpha \geq n - 2$, (a_{jk}^{α}) is also positive definite.

E.H. Moore studied a very particular type of positive definite kernel in 1916 ([10]). Given an abstract set E, Moore calls functions $\varphi(x, y)$ defined on $E \times E$ "positive Hermitian matrices" if they satisfy

$$\sum_{j,k=1}^{n} c_j \overline{c_k} \varphi(x_j, x_k) \geq 0$$

for any $n \in \mathbb{N}$, $x_1, ..., x_n \in E$ and $c_1, ..., c_n \in \mathbb{C}$.

Studying positive definiteness has gained popularity and positive definite matrices are now covered in most linear algebra courses. A vast variety of literature is now available on the subject, such as [6], or [1], and many other seeks to tie together positive definite kernels and positive definite functions, such as [2].

1.2 Positive Definite Matrices

Positive real numbers make up an important subset of the complex numbers. They have a variety of properties that make them stand apart from other numbers. The sum, or product of two positive numbers is positive, the square root of a positive number is positive, and so on. There exists a notion that allows us to consider matrices that behave in a similar fashion to the positive real numbers. Called positive definite matrices, these square matrices behave in a similar fashion to the positive real numbers.

Positive definite matrices are usually defined as a matrix A where $z^*Az > 0$ for all nonzero column vectors z where z^* denotes the conjugate transpose. There are similar definitions for positive semi-definite, where we allow 0, and negative definite where $z^*Az < 0$. Positive definite matrices have a variety of properties that separate them from other matrices. The theory behind these matrices is vast, but so far is restricted to Hermitian matrices, that is, square matrices over the real or complex numbers that are equal to their conjugate transpose.

Positive definite matrices are most famously used for discussions of convexity with multi-variable functions. If we consider the Hessian of a multi-variable function, that is, the matrix of second degree partials, the Hessian being positive definite implies that the function obtains a minimum at that point. If the Hessian is negative definite, the function obtains a maximum.

In this thesis, we explore whether any of the theory of positive definite matrices can be expanded to finite fields. We delve into the list of equivalent statements that

arise for positive definite Hermitian matrices and discover which can be reformed to hold over other fields. The search begins a bit rough, as the most common definition for positive definiteness, that $z^*Az > 0$ for all nonzero z, no longer has much meaning over other fields.

While this inconvenience seems to have paused most curiosity for positive definite matrices in finite fields, we take a look into pressing sequences in Chapter 4, which provides an interesting motivation for the possible existence of positive definiteness over finite fields in particular. We build up some definitions and results on pressing sequences to ultimately come to a result which almost mirrors a result of positive definite Hermitian matrices. With this new found motivation in hand, we develop new definitions, which are similar to those for the Hermitian case, to bypass this inconvenience in order to discuss the remaining aspects of positive definiteness over other fields with a desired property.

By the end of this thesis, we develop a notion for positive definite matrices in certain fields. We present which notions of positive definite for Hermitian matrices remains true in these fields and provide counterexamples for those which no longer hold. This opens up a wide variety of speculation and new questions as to the consequences of this notion. Possibly most intriguingly, does this notion allow us to discuss optimization in finite fields? While the discussion of optimization and possible applications for positive definiteness in finite fields is beyond the scope of this thesis, we look forward to possible new results to come.

Chapter 2

Preliminaries

2.1 Linear Algebra

We begin by presenting some definitions and well known facts from linear algebra. Many of these can be found in a large variety of linear algebra text books, like David C. Lay's *Linear Algebra and It's Applications* ([8]).

Notation: To refer to the entry in row i and column j of a matrix A, we will us a_{ij}. Thus we can denote the $n \times n$ matrix $A = (a_{ij})_{i,j=1}^{n}$

Definition 2.1. Given an $m \times n$ matrix A, the **transpose** of A is the $n \times m$ matrix, denoted by A^T, whose columns are formed from the corresponding rows of A. A square matrix is said to be **symmetric** if it is equal to its transpose. The **conjugate transpose** of a matrix A is the transpose of A where all entries have undergone complex conjugation. A square matrix is said to be **Hermitian** if it is equal to its conjugate transpose.

Example 2.2. *An example of a Hermitian matrix is*

$$A = \begin{bmatrix} 3 & 2-i & 7 \\ 2+i & 2 & -i \\ 7 & i & 13 \end{bmatrix}$$

Definition 2.3. Given a matrix $A = (a_{ij})_{i,j=1}^{n}$, a **principal submatrix** is a matrix derived from deleting rows and their similarly indexed columns from A. A **leading principal submatrix** of an $n \times n$ matrix A is derived from the deletion of the last $n - k$ rows and the last $n - k$ columns, usually denoted A_k.

Definition 2.4. For $n \geq 2$, the **determinant** of an $n \times n$ matrix $A = (a_{ij})_{i,j=1}^{n}$ is,

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma_i}$$

Definition 2.5. For a matrix A, and a leading principal submatrix, A_k, the determinant of A_k is called the **kth leading principal minor**.

Definition 2.6. An $n \times n$ matrix is said to be **invertible**, or **non-singular**, if there exists an $n \times n$ matrix C such that $CA = I$ and an $n \times n$ matrix D such that $AD = I$ where I is the $n \times n$ identity matrix. If $D = C$, the **inverse** of A is usually denoted A^{-1}.

Definition 2.7. A matrix L is said to be **lower triangular** if all entries above the main diagonal are 0. That is, if $i < j$, $a_{ij} = 0$. A matrix U is said to be **upper triangular** if all entries below the main diagonal are 0. That is, if $i > j$, $a_{ij} = 0$.

Definition 2.8. A matrix A is said to have a **Cholesky decomposition** if $A = LL^T$ for some lower triangular matrix L.

Definition 2.9. The **rank** of a matrix A, denoted by rank(A), is the dimension of the column space of A.

Definition 2.10. If V is a finite-dimensional complex vector space, then relative to any basis $\{e_i\}$ of V, a **sesquilinear form** is represented by a matrix ϕ, w by the column vector $\mathbf{w}$, and z by the column vector $\mathbf{z}$:

$$\varphi(w, z) = \varphi\left(\sum_i w_i e_i, \sum_j z_j e_j \right) = \sum_i \sum_j \overline{w_i} z_j \varphi(e_i, e_j) = \overline{\mathbf{w}}^T \phi \mathbf{z}$$

The components of ϕ are given by $\phi_{ij} = \phi(e_i, e_j)$.

Note that a sesquilinear form can be defined if V is a vector space over $\mathbb{F}_{q^2}^n$ in the same manner.

Definition 2.11. An **inner product space** is a vector space V over the a field $\mathbb{F}$ together with an **inner product**, that is, a map $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{F}$ which satisfies conjugate symmetry, is linear in its first argument and satisfies positive definiteness. That is:

$$\begin{aligned} \langle x, y \rangle &= \overline{\langle y, x \rangle} \\ \langle ax, y \rangle &= a\langle x, y \rangle \\ \langle x + y, z \rangle &= \langle x, z \rangle + \langle y, z \rangle \\ \langle x, x \rangle &\geq 0 \\ \langle x, x \rangle = 0 &\iff x = 0 \end{aligned}$$

Definition 2.12. An **eigenvector** of an $n \times n$ matrix A is a nonzero vector x such that $Ax = \lambda x$ for some scalar λ. A scalar λ is called an **eigenvalue** of A if there is a nontrivial solution x of $Ax = \lambda x$; such an x is called an *eigenvector corresponding to* λ.

Definition 2.13. A **pivot position** in a matrix A is a location in A that corresponds to a leading 1 in the reduced echelon form of A. A **pivot** is a nonzero number in a pivot position.

Definition 2.14. Given two matrices of the same size A and B, the **Hadamard product** $A \circ B$ is formed by multiplying the entries of A and B entry-wise. That is, if $A = (a_{ij})_{i,j=1}^{n}$ and $B = (b_{ij})_{i,j=1}^{n}$ then $A \circ B$ is

$$\begin{bmatrix} a_{11}b_{11} & a_{12}b_{12} & \dots & a_{1n}b_{1n} \\ a_{21}b_{21} & a_{22}b_{22} & \dots & a_{2n}b_{2n} \\ \vdots & \cdots & \ddots & \vdots \\ a_{n1}b_{n1} & a_{n2}b_{n2} & \dots & a_{nn}b_{nn} \end{bmatrix}$$

The **Frobenius inner product** can be defined as the sum of the entries of the Hadamard product.

There are other variations on the definition of the Frobenius inner product, but the above is the easiest and most useful for the purpose of this thesis.

Definition 2.15. If A is an $n \times m$ matrix and B is a $p \times q$ matrix, then the **Kronecker Product**, $A \otimes B$ is the $mp \times nq$ block matrix

$$\begin{bmatrix} a_{11}\mathbf{B} & a_{12} & \mathbf{B} & ... & a_{1n}\mathbf{B} \\ a_{21}\mathbf{B} & a_{22} & \mathbf{B} & ... & a_{2n}\mathbf{B} \\ \vdots & \vdots & \ddots & \vdots & \\ a_{m1}\mathbf{B} & a_{m2} & \mathbf{B} & ... & a_{mn}\mathbf{B} \end{bmatrix}$$

Definition 2.16. Given linearly independent vectors $v_1, ..., v_n$, the **Gram matrix** of these vectors is:

$$G = \begin{bmatrix} \langle v_1, v_1 \rangle & \langle v_1, v_2 \rangle & \cdots & \langle v_1, v_n \rangle \\ \langle v_2, v_1 \rangle & \langle v_2, v_2 \rangle & \cdots & \langle v_2, v_n \rangle \\ \cdots & \cdots & \ddots & \cdots \\ \langle v_n, v_1 \rangle & \langle v_n, v_2 \rangle & \cdots & \langle v_n, v_n \rangle \end{bmatrix}$$

Lemma 2.17. *All leading principal submatrices of a Gram matrix are also Gram matrices.*

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

$$G = \begin{bmatrix} \langle v_1, v_1 \rangle & \langle v_1, v_2 \rangle & \cdots & \langle v_1, v_n \rangle \\ \langle v_2, v_1 \rangle & \langle v_2, v_2 \rangle & \cdots & \langle v_2, v_n \rangle \\ \cdots & \cdots & \ddots & \cdots \\ \langle v_n, v_1 \rangle & \langle v_n, v_2 \rangle & \cdots & \langle v_n, v_n \rangle \end{bmatrix}$$

Any leading principal submatrix, G_k will take the form

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

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

The following lemmas are given without proof as they are common to most linear algebra textbooks and are included simply to remind us that they are results we can use throughout this thesis.

Lemma 2.18. *A matrix A is invertible if and only if* $\det(A) \neq 0$.

Lemma 2.19. *Let A and B denote two matrices whose sizes are appropriate for the following product. Then:*

$$(AB)^T = B^T A^T$$

Lemma 2.20. *If A is an $n \times n$ matrix, then* $\det(A^T) = \det(A)$.

Lemma 2.21. *If A, B are $n \times n$ matrices, and AB is invertible, then so are A and B.*

Lemma 2.22. *If A and B are $n \times n$ matrices, then* $\det(AB) = \det(A)\det(B)$.

Lemma 2.23. *The determinant of an upper or lower triangular matrix is the product of its diagonal elements.*

Proof. Let L be an $n \times n$ lower triangular matrix. If $n = 1$, the result is trivial. Suppose the result holds for $n < k$ and let $n = k$. Then

$$\det(L) = \sum_{j=1}^{k} (-1)^{1+j} l_{1j} \det(L_{1j})$$

Now, the only l_{1i} that is nonzero is l_{11}, thus $\det(L) = a_{11}\det(A_{11})$. By induction, $\det(L_{11}) = l_{22}l_{33}\cdots l_{kk}$, and the result follows.

If U is an upper triangular matrix, then U^T is lower triangular and as $\det(U^T) = \det(U)$, the result follows. □

Lemma 2.24. *Given a matrix $A = LL^T$ for some lower triangular matrix L, the kth leading principal submatrix, A_k can be factored in the following way: $A_k = L_k L_k^T$.*

Proof. Let $A = LL^T$ for some lower triangular matrix L.

$$A = \begin{bmatrix} A_k & B \\ C & D \end{bmatrix} = \begin{bmatrix} L_k & 0 \\ L_{12} & L_{22} \end{bmatrix} \begin{bmatrix} L_k^T & L_{12}^T \\ 0 & L_{22}^T \end{bmatrix} = \begin{bmatrix} L_k L_k^T & L_k L_{12}^T \\ L_{12} L_k^T & L_{12} L_{12}^T + L_{22} L_{22}^T \end{bmatrix}$$

□

The following theorem and corollary come from *Necessary and Sufficient Conditions For Existence of the LU Factorization of an Arbitrary Matrix* ([11]). These results will be used to help prove some of our results for positive definite matrices over certain fields. The proof of Theorem 2.1, which is stated simply for its use in Corollary 2.25, is omitted, as it is quite lengthy.

In Theorem 2.1, rank(A)[{1...k}] denotes the rank of the kth leading principal submatrix of A, while rank(A)[{1...k}, {1...n}] denotes the rank of the submatrix of A created by the first k rows and the first n columns of A.

Theorem 2.1. *The matrix $A = (a_{ij}) \in \mathcal{M}_n(\mathbb{F})$ has an LU factorization if and only if it satisfies the following for all $k = 1, ..., n$:*

$$\textit{rank}(\text{A})[\{1...k\}] + k \geq \textit{rank}(\text{A})[\{1...k\}, \{1...n\}] + \textit{rank}(\text{A})[\{1...n\}, \{1...k\}]$$

Corollary 2.25. *Let A be an $n \times n$ invertible matrix. Then A has an LU factorization if and only if all principal leading submatrices of A have full rank.*

Proof. Since A is invertible, we must have

$$\text{rank(A)}[\{1...k\}] = \text{rank(A)}[\{1...n\}, \{1...k\}] = k$$

for all $k = 1, ..., n$. Thus, A has a LU factorization if and only if rank(A)[{1...k}] = k by Theorem 2.1. □

Lemma 2.26. *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 kth 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* $k = 1, 2, \cdots, n$.

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 withall 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:

$$A = \begin{bmatrix} L_k & \mathbf{0} \\ L_{21} & L_{22} \end{bmatrix} \begin{bmatrix} D_k & \mathbf{0} \\ \mathbf{0} & D_{22} \end{bmatrix} \begin{bmatrix} U_k & U_{12} \\ \mathbf{0} & U_{22} \end{bmatrix}$$

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

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

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 $n < k$, we have $\det(A_k) = \det(D_{k-1})d_{kk} = \det(A_{k-1})d_{kk} = d_{11}...d_{kk}$. The result follows as the pivots are exactly the entries of D. □

2.2 Field Theory

As one of the main focuses of this thesis is matrices over other fields besides $\mathbb{R}$ and $\mathbb{C}$, we continue with some definitions that should be well known to continue on.

Definition 2.27. A **ring**, R, is an Abelian group under addition with the properties of associative multiplication and is right and left distributive over addition. A **field**

is a commutative ring with unity in which every nonzero element is a unit. That is, every nonzero element has a multiplicative inverse.

Definition 2.28. A **finite field** is a field that contains a finite number of elements.

Definition 2.29. The **order** of a field is the number of elements contained in the field. Finite fields of order q only exist if $q = p^k$ for a prime p.

The **characteristic** of a field is the minimum positive number n such that for any element $a \in \mathbb{F}$, a added to itself n times is 0.

Definition 2.30. Two numbers are said to be **equivalent modulo** n if both numbers have the same remainder when being divided by n.

Definition 2.31. An integer k is a **quadratic residue** modulo n if it is equivalent to a perfect square modulo n. That is $k \equiv x^2 \pmod{n}$.

The simplest finite fields are those of prime order, which can be thought of as the integers modulo p with the operations of modular addition and multiplication.

Example 2.32. $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

Definition 2.33. Given a ring homomorphism $f : R \to S$, the **kernel** of f is $\{r \in R : f(r) = 0_s\}$ where 0_s represents the zero element in S.

Lemma 2.34. *Given a ring homomorphism $f : R \to S$, f is injective if and only if* $\ker(f) = \{0\}$.

Proof. Let $f : R \to S$ be a ring homomorphism.

Let f be injective and $x \in \ker(f)$. As $f(0_R) = 0_S$, we have

$$f(x) = 0_S$$

$$f(x) = f(0_R)$$

$$x = 0_R$$

Thus, $\ker(f) = \{0_R\}$.

Let $\ker(f) = 0$. Suppose that $f(x) = f(y)$. Then:

$$f(x) - f(y) = 0$$
$$f(x - y) = 0$$
$$x - y \in \ker(f)$$

Thus $x - y = 0$ and $x = y$ thus f is injective. □

Definition 2.35. Let R be a commutative ring with prime characteristic p. The **Frobenius endomorphism** F is defined by $F(r) = r^p$

Indeed, F is an endomorphism as

$$F(x + y) = (x + y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p$$
$$F(xy) = (xy)^p = x^p y^p = F(x)F(y)$$

.

Lemma 2.36. *The Frobenius endomorphism is an isomorphism for fields of prime order.*

Proof. Let $\mathbb{F}_p$ be a field of prime order, and F the frobenius endomorphism. As $\mathbb{F}_p$ is an integral domain, if $x^a = 0$ then $x = 0$ for any a. Thus $\ker(F) = 0$ and F is injective. As $\mathbb{F}_p$ is finite and F is injective, F must also be surjective. □

Lemma 2.37. *Every element in a finite field of characteristic 2 is a quadratic residue.*

Proof. Let $\mathbb{F}_q$ be a finite field of characteristic 2. We have $F : \mathbb{F}_q \to \mathbb{F}_q$ given by $F(x) = x^2$ is an isomorphism. Thus, every element of $\mathbb{F}_q$ is a quadratic residue. □

2.3 Number Theory

We continue with some results from number theory.

The presented definition and lemmas, while still somewhat common to number theory texts, are presented here as they are seen in Angelica Wong's *Primes and Quadratic Reciprocity* ([12]).

Lemma 2.38. *$f(x) = x^p$ is the identity automorphism of $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Note that $f(x) = x^p$ is the Frobenius endomorphism for $\mathbb{Z}/p\mathbb{Z}$, and thus by Lemma 2.36 is an automorphism. Thus, we need only show that it is the identity automorphism. We proceed by induction. Clearly, $0^p \equiv 0 \pmod{p}$. Assume the result holds for values up to and including x. We have $(x+1)^p = x^p + 1^p$, which by the inductive hypothesis is $x + 1$. □

Theorem 2.2 (Fermat's Little Theorem)**.** *If p is prime, then for all x such that $x \not\equiv 0 \pmod{p}$, $x^{p-1} \equiv 1 \pmod{p}$.*

Proof. Let p be a prime and $x \not\equiv 0 \pmod{p}$. This, as we have the equivalence $x^p \equiv x \pmod{p}$, $x^p x^{-1} \equiv 1 \pmod{p}$ and $x^{p-1} \equiv 1 \pmod{p}$ □

Definition 2.39. The **Legendre symbol** $\left(\frac{a}{p}\right)$ for an integer a and an odd prime p is defined as

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

For nonzero a, the Legendre symbol equals 1 when a is a quadratic residue modulo p and -1 when a is not a quadratic residue modulo p. The Legendre symbol is also known as the **quadratic character** of a modulo p.

Lemma 2.40. *If p is an odd prime and $P = \frac{1}{2}(p-1)$, then $a^P \equiv \left(\frac{a}{p}\right) \pmod{p}$.*

Proof. Case 1: $a \equiv 0$.

In this case, $a^P \equiv 0 = \left(\frac{0}{p}\right) \pmod{p}$.

Case 2: a is a nonzero quadratic residue.

It suffices to show that $a^P \equiv \left(\frac{a}{p}\right) = 1$. Let $a = b^2$, then $a^P = b^{2P} = b^{p-1}$. By Fermat's Little Theorem $b^{p-1} \equiv 1 \pmod{p}$. Thus $a \equiv \left(\frac{a}{p}\right)$.

Case 3: a is not a quadratic residue.

In this case, it suffices to show that $a^P \equiv \left(\frac{a}{p}\right) = -1$. Consider $(a^P)^2 = a^{2P} = a^{p-1}$. By Fermat's Little Theorem, this is congruent to 1. Therefore, a^P is a square root of 1 modulo p and must therefore be 1 or -1. Consider the degree P polynomial $a^P - 1 \equiv 0$, which will have at most P roots. By case 2, any quadratic residue a is such that $a^P = 1$, so each quadratic residue is a root of this polynomial. Since the function $x \to x^2$ is two-to-one in $(\mathbb{Z}/p\mathbb{Z})^*$, exactly half of the nonzero elements modulo p are quadratic residues. Thus, the P quadratic residues are exactly the P roots of the polynomial $x^P - 1$, so if a is not a quadratic residue, then $a^P \equiv -1 = \left(\frac{a}{p}\right)$. □

Proposition 1. *The Legendre symbol is multiplicative. That is:*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Proof. Write $\left(\frac{a}{p}\right)$ as a^P and $\left(\frac{b}{p}\right)$ as b^P. Then,

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = a^P b^P = (ab^P) = \left(\frac{ab}{p}\right)$$

□

Lemma 2.41. *Let p be a prime. Then the quadratic character of -1 modulo p depends only on whether p is 1 or 3 modulo 4. That is,*

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

Proof. Case 1: $p \equiv 1 \pmod 4$

If a divides $p-1$, then there exists some x such that $x^a \equiv 1 \pmod p$, but $x^b \not\equiv 1 \pmod p$ for any $0 < b < a$. Since 4 divides $p-1$, there exists some x such that $x^4 \equiv 1 \pmod p$ but $x^2 \not\equiv 1 \pmod p$. As $(x^2)^2 \equiv 1$, it must be that x^2 is either 1 or -1. We have already rules out $x^2 \equiv 1 \pmod p$ so it must be the case that $x^2 \equiv -1 \pmod p$. Therefore, -1 is a quadratic residue modulo p.

Case 2: $p \equiv 3 \pmod 4$

Suppose that $\left(\frac{-1}{p}\right) \neq -1$. That is, there exists an x such that $x^2 \equiv 1 \pmod p$. Squaring both sides produces $x^4 \equiv 1$. By Fermat's Little Theorem, we have $x^{p-1} \equiv 1 \pmod p$ and thus $x^{4k+2} = x^{4k}x^2 = (x^4)^k x^2 = 1^k x^2 = -1$. This is a contradiction as $x^{4k+2} = 1$ and thus -1 is not a quadratic residue modulo p. □

2.4 Graph Theory

As the motivation, and some results, for this work come from graph theory, we include some important definitions that should be known by the reader. Many of these definitions can be found in graph theory textbooks, including [4].

Definition 2.42. A **graph** G is a pair (V, E) of vertices v and edges e where $E \subseteq [V]^2$. $E(G)$ represents the set of edges for G and $V(G)$ represents the set of vertices. The set of edges is symmetric as a relation, that is, (x, y) is an edge if and only if (y, x) is an edge. For simplicity, we denote the edge (x, y) as xy.

Definition 2.43. A **multigraph** is a pair (V, E) of disjoint sets together with a map $E \to V \cup [V]^2$ assigning to every edge either one or two vertices as its ends. In a multigraph, two vertices may have multiple edges between them, usually called **multi-edges**. A **loop** is an edge between a vertex and itself, $e_i = v_i v_i$.

Definition 2.44. A **simple graph** is a graph $G = (V, E)$ which does not contain loops or multi-edges.

Definition 2.45. Two vertices x, y of G are **adjacent**, or **neighbors** if xy is in the edge set of G. The **neighborhood** of a vertex v is $N_G(v) = \{x \in V(G) : vx \in E(G)\}$.

Definition 2.46. The **complement** $\overline{G}$ of G is the graph on V with the edge set $[V]^2 \setminus E$.

Definition 2.47. The **adjacency matrix** $A = (a_{ij})_{i,j=1}^{n}$ of a graph G is defined to be:

$$a_{ij} := \begin{cases} 1 \text{ if } v_i v_j \in E(G) \\ 0 \text{ otherwise} \end{cases}$$

Definition 2.48. A set of edges is independent if the edges do not share vertices. A set of independent edges, M, in a graph G is called a **matching**. A matching where every vertex is incident to exactly one edge in the matching is called a **perfect matching**.

Definition 2.49. Given a graph $G = (V, E)$, if $G' \subseteq G$ and G' contains all edges $xy \in E$ for $x, y \in V'$, then G' is an **induced subgraph** of G. For a set $S \subset V(G)$, $G[S]$ is the induced subgraph of S.

Definition 2.50. A **weighted graph** is a graph whose edges are given a numerical value.

Chapter 3

Positive Definite Hermitian Matrices

Recall that the notion of a positive definite matrix allows us to classify matrices that behave in a similar way to the positive real numbers. The theory of positive definite matrices is vast and yet, up to this point, was restricted to Hermitian matrices. We seek to discover how much of this theory can be extended to matrices over other fields. In this chapter, we state common results for positive definite Hermitian matrices that will be considered over other fields, and discuss why it is not obvious that we can even consider positive definite matrices over other fields. Many of the proofs for the Hermitian results can be found in a variety of linear algebra textbooks, including [6].

Definition 3.1. A symmetric $n \times n$ Hermitian matrix M is said to be **positive definite** if $z^T M z > 0$ for all nonzero column vectors $z \in \mathbb{C}^n$.

M is said to be **positive semi-definite** if $z^T M z \geq 0$, and M is **negative definite** if $z^T M z < 0$.

One large application for positive definite matrices is their use in optimization for multi-variable equations. If the Hessian of a multi-variable function, the matrix of second degree partial derivatives, is positive definite, the function obtains a minima at that point. If instead the Hessian is negative definite, it obtains a maximum.

In this thesis, we consider, almost exclusively, the positive definite case. It would be interesting to look into the positive semi-definite and negative definite cases, but these are beyond the scope of this thesis.

One of the main results for Hermitian positive definite matrices is the variety of

equivalent statements that arise. These equivalences are part of what make positive definite matrices so special and interesting to explore. One need only check the eigenvalues of a matrix to determine whether it is positive definite, and if it is, you suddenly gain a plethora of other properties for that matrix which may have been less trivial to check. As these equivalences are so central to the theory of positive definite Hermitian matrices, looking into these main equivalences over other fields is one of the main goals of this thesis.

Theorem 3.1. *Given a symmetric $n \times n$ Hermitian matrix, A, the following are equivalent:*

1. *A is positive definite.*
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.*

Further, positive definite matrices posses a range of other properties. In Chapter 4, we seek to consider positive definite matrices in other fields. The properties of Hermitian matrices which we will consider in Chapter 4 are included here. There are other properties that positive definite Hermitian matrices possess which we do not discuss as it is beyond the scope of this thesis. The proof for Hermitian cases are easily found in a variety of linear algebra textbooks, including [6].

Theorem 3.2. *If A is a positive definite Hermitian $n \times n$ matrix, the following statements hold:*

1. *A is invertible and A^{-1} is also positive definite.*

2. *If $r > 0$ is a real number, then rA is positive definite.*

3. *If B is a positive definite Hermitian matrix, then ABA and BAB are positive definite and if $AB = BA$ then AB is positive definite.*

4. *Every principal submatrix of A is positive definite.*

5. *If B is a positive definite Hermitian matrix, then the Hadamard product $A \circ B$, and the Kronecker product $A \otimes B$ are positive definite and the Frobenius product $A : B \geq 0$.*

Many linear algebra books list the main definition of a positive definite matrix A to be that $x^T Ax > 0$ for all nonzero vectors x. Over finite fields, this definition looses its meaning. That is, we can find a nonzero column vector such that $x^T Ax = 0$ for $A \in \mathcal{G}_{n\times n}(\mathbb{F})$ a general matrix over $\mathbb{F}$. The following proof was provided by Jyrki Lahtonen in a Math Stack Exchange post ([7]).

Proposition 2. *Define $Q : \mathbb{F}^n \to \mathbb{F}$ with $Q(x) = x^T Ax$ on $n \geq 3$ variables ranging over $\mathbb{F}_p$, $p > 2$ with $A \in \mathcal{G}_{n\times n}(\mathbb{F})$. Q takes the form*

$$Q(v) = \lambda_1 v_1^2 + \lambda_2 v_2^2 + ... + \lambda_n v_n^2$$

There exists $(v_1, v_2, v_3) \neq (0, 0, 0)$ from $\mathbb{F}_p^3$ with $Q(v_1, v_2, v_3, 0, ..., 0) = 0$.

Proof. Define $Q : \mathbb{F}^n \to \mathbb{F}$ with $Q(x) = x^T Ax$ on $n \geq 3$ variables ranging over $\mathbb{F}_p$, $p > 2$ for A an arbitrary matrix. Q takes the following form, for $\lambda_i \in \mathbb{F}_p$

$$Q(v) = \lambda_1 v_1^2 + \lambda_2 v_2^2 + ... + \lambda_n v_n^2$$

We will show that there exists some $v = (v_1, v_2, v_3, 0, ..., 0)$ such that $Q(v) = 0$. Assume $\lambda_1, \lambda_2, \lambda_3 \neq 0$, otherwise the result follows. Note that squaring is a 2-to-1 map from $\mathbb{F}_p^*$ to itself. Thus, including 0, we have that each monomial $\lambda_i v_i^2$ takes on $\frac{p+1}{2}$ distinct values, 1 for 0 and each of the other $\frac{p-1}{2}$ values twice.

Next, we will show that $P(v_1, v_2) = \lambda_1 v_1^2 + \lambda_2 v_2^2$ gives a surjective function from $\mathbb{F}_p^2$ to $\mathbb{F}_p$. Let $y \in \mathbb{F}_p$, $S_1 = \{\lambda_1 v_1^2 | v_1 \in \mathbb{F}_p\}$, and $S_2 = \{y - \lambda_2 v_2^2 | v_2 \in \mathbb{F}_p\}$. Both S_1 and S_2 have $\frac{p+1}{2}$ terms and therefore must have a nonempty intersection. So, there exists some $\lambda_1, \lambda_2, v_1, v_2$ such that $y - \lambda_2 v^2 = \lambda_1 v_1^2$, which gives $y = P(v_1, v_2)$. Now, let $v_3 = 1$, $v_1, v_2 \in \mathbb{F}_p$ with $P(v_1, v_2) = -\lambda_3$. Thus, $Q(v_1, v_2, v_3, 0, ..., 0) = 0$. □

The above proof from Lahtonen excludes when $p = 2$, so we cover it separately now. Over $\mathbb{F}_2$, we need only form an even number of nonzero elements. If we consider the same set up as the given proof, if any $\lambda_i = 0$, the result is trivial. Thus, let $\lambda_1, \lambda_2, \lambda_3 = 1$, then letting v_1, v_2, v_3 be any combination of two ones and a zero will give us our result. For instance, $v = (1, 0, 1, 0, ..., 0)$ will cause $Q(v) = 0$.

With this information in hand, one can ask why we even dream of positive definite matrices in finite fields. Most searches up to this point seem to end once this realization is made. In the next chapter, we introduce pressing sequences, a seemingly unrelated topic that provides interesting motivation into the possible existence of positive definite matrices in finite fields.

Chapter 4

Pressing Sequences

In this chapter, results from the theory of pressing sequences, presented in a paper by Jeffery Davis and Joshua Cooper are considered. Their main result sparks some interest as it is reminiscent of an equivalence of positive definite matrices, which gives some motivation for our search into the theory of positive definite matrices in finite fields despite the definition's loss of meaning. We build up enough results to motivate our search and allow us to consider pressing sequences over more than simply $\mathbb{F}_2$. Full details for the pressing sequence results can be seen in their paper ([3]).

Definition 4.1. A **bicolored graph** $G = (G, c)$ is a simple graph G with $c : V(G) \to \{blue, white\}$ which assigns a color to each vertex. Say that the complement of blue is white and the complement of white is blue.

Let $N^*(v)$ be the closed neighborhood of v, that is, $N^*(v) = N_G(v) \cup \{v\}$. Note that $\begin{pmatrix} N^*(v) \\ 2 \end{pmatrix}$ represents all possible vertex pairs given the vertices of $N^*(v)$.

Definition 4.2. Consider a bicolored graph, (G, c) with a blue vertex $v \in V(G)$. **Pressing v** is the operation of transforming (G, c) to (G', c'), a new bicolored graph in which $G[N^*(v)]$ is complemented. That is, $V(G) = V(G')$ and

$$E(G') = E(G)\Delta \begin{pmatrix} N^*(v) \\ 2 \end{pmatrix}$$

where Δ represents the symmetric difference and $c'(w) = c(w)$ for $w \in N^*(v)$ and $c'(w) = c(w)$ for $w \in N^*(v)$.

The following example of a vertex press is taken directly from Cooper and Davis' paper, the black vertices in the figure note the blue pressable vertices of the graph.

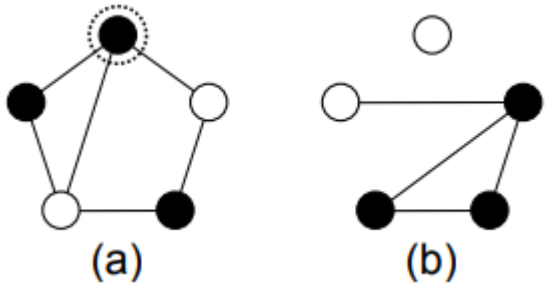

Figure 4.1 The vertex enclosed by a dotted circle is pressed in graph (a) to obtain graph (b)

Definition 4.3. The **augmented adjacency matrix** $A(G) \in \mathbb{F}_2^{n\times n}$ of a bicolored graph G on n vertices, is the the adjacency matrix of which the entries along the main diagonal correspond to the vertices of G and are indexed by the color of the vertex; 0 if white or 1 if blue.

Cooper and Davis go on to define functions which relate to pressing vertices and show their affect on the augmented adjacency matrix.

Let $f(M)$ be a function on $n \times n$ nonzero matrices over $\mathbb{F}_2$ given below. Let s denote the smallest row index of a left-most 1 in the matrix M, in other words there exists some integer t so that

1. $M_{s,t} = 1$,
2. $M_{s,j} = 0$ for $j < t$, and
3. if $i < s$ and $j < t$, then $M_{i,j} = 0$.

Let U be the set of row indices such that the entry in the t-th column is a 1. That is, $U = \{i : M_{i,t} = 1\}$.

Let $f(M)$ be the following $n \times n$ matrix:

$$f(M)_{i,j} = \begin{cases} M_{i,j} & \text{if } i \notin U \\ M_{i,j} + M_{s,j} & \text{if } i \in U \end{cases}$$

Given some M, there exists some increasing sequence of s_i and t_i which serve as indices in the above definition for $f(M), f(f(M))$ and so on. This process must terminate for some finite number of s_i and t_i as the process eventually results in the all zeroes matrix. Note that each iteration of f is essentially preforming Gaussian elimination without row swaps on $A(G)$, where we also eliminate the row of the pressed vertex. That is, if vertex v_i is pressed, the ith row of $A(G)$ is reduced to a row of all zeros.

Suppose, then, that we have a matrix M and some sequence $s_1, ..., s_p$ and $t_1, ..., t_p$ as described. We can therefore define the following function:

$$g(M)_{i,j} = \begin{cases} M_{i,j} & \text{if } i \notin U \setminus \{s\} \\ M_{i,j} + M_{s,j} & \text{if } i \in U \setminus \{s\} \end{cases}$$

We call M "leading principal nonsingular", or LPN, if we have that the elements of U are greater than or equal to s_r for each $r \in [p]$ where $[p] = \{1, ..., p\}$. If M is LPN, then $g(M), g(g(M)), ..., g^{(p)}(M)$ for $p = \text{rank}(M)$ is exactly the process of performing Gaussian elimination without row swaps. Also, $s_i = t_i = i$ for each $i \in [p]$ and therefore M is row-reducible to a matrix whose leading principal sub-matrices, of size less than or equal to p, are identity matrices.

A "successful pressing sequence" occurs when a sequence of presses results in an all white empty graph. Thus, considering the above, as $A(G)$ being the all zeroes matrix will be precisely when G is an all white empty graph, $A(G)$ being LPN is precisely when G will have a successful pressing sequence.

Definition 4.4. The **pressing number** of a graph is the minimal number of presses required to transform the graph into an all white empty graph.

The main result in [3], stated below and then reconsidered for a special case, are what provides some suspicion that positive definite matrices can be considered over other fields.

Note we may consider a bicolored graph as a "loopy" graph, where each blue vertex is viewed as a vertex with a loop and each white vertex has no such loop. These "loopy" graphs are denoted $\hat{G}$.

Theorem 4.1. *Given a bicolored graph G, and integer k, the following are equivalent:*

1. *The pressing number of G is k.*
2. *rank$(A(G)) = k$ and can can be written as $A(G) = P^T LL^T P$ for some lower-triangular matrix L and some permutation matrix P.*
3. *rank$(A(G)) = k$ and G has a black vertex in each component that is not an isolated vertex.*
4. *There is some permutation matrix P so that the j-th leading principal minor of $P^T A(G)P$ is nonzero for $j \in [n] \setminus [k]$.*
5. *There is an ordering of the vertices $v_1, ..., v_n$ of $\hat{G}$ so that the induced subgraph $\hat{G}[\{v_1, ..., v_j\}]$ has an even number of perfect matchings for each $j \in [n]$, and, for each $j \in [n] \setminus [k], \hat{G}[\{v_1, ..., v_n\}]$ has an even number of perfect matchings.*
6. *$A(G) = P^T LUP$ for some permutation matrix P, lower triangular matrix L, and upper triangular matrix U, where rank$(LU) = k$.*

When the labeling provides a successful pressing sequence, that is, the vertices $v_1, ...v_n$ pressed in order produce a successful pressing sequence, the above theorem can be restated in the following manner.

Theorem 4.2. *Given a bicolored labeled graph G on $[n]$, the following are equivalent:*

1. *The vertices of G, in the usual order, are a successful pressing sequence.*

2. *$A(G)$ can be written $A(G) = LL^T$ for some invertible lower-triangular matrix L.*

3. *Every leading principal minor of $A(G)$ is nonzero for $j \in [n]$.*

4. *The induced subgraph $G[\{1, ..., j\}]$ has an odd number of perfect matchings for each $j \in [n]$.*

5. *$A(G) = LU$ for some invertible lower triangular matrix L and invertible upper triangular matrix U.*

Equivalences 2 and 3 are very similar to results for positive definite matrices. These results make us wonder; can positive definite matrices be defined over finite fields? Is there some kind of structure for matrices over finite fields to preserve at least some of the equivalences that are present for Hermitian matrices? Chapter 5 seeks to answer these questions.

Further, can pressing sequences be defined over other fields besides $\mathbb{F}_2$? To tackle this idea in the next chapter, we present some new definitions that will allow us to talk about pressing sequences over more than $\mathbb{F}_2$.

Definition 4.5. Let a **$\mathbb{F}$-pseudograph**, for some field $\mathbb{F}$, be a graph $G = (V, f)$ with V the set of vertices and $f : V \times V \to \mathbb{F}$ a function assigning a weight to each edge. That is, $f(x, y) = c$ assigns a weight of $c \in \mathbb{F}$ to the edge xy. Each edge has only one associated weight. That is, $f(x, y) = f(y, x)$. Note every pair of vertices has an edge, some may simply have weight 0.

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

$$a_{ij} = f(v_i, v_j)$$

Note that this will create a symmetric matrix.

Definition 4.7. Consider a $\mathbb{F}-$pseudograph $G = (V, f)$. For a vertex v, with $f(v, v)$ a quadratic residue in $\mathbb{F}$, **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 this definition will clearly cause the resulting weighted adjacency matrix $A(G')$ to also be symmetric.

The following figure demonstrates a general press on the vertex with weight a:

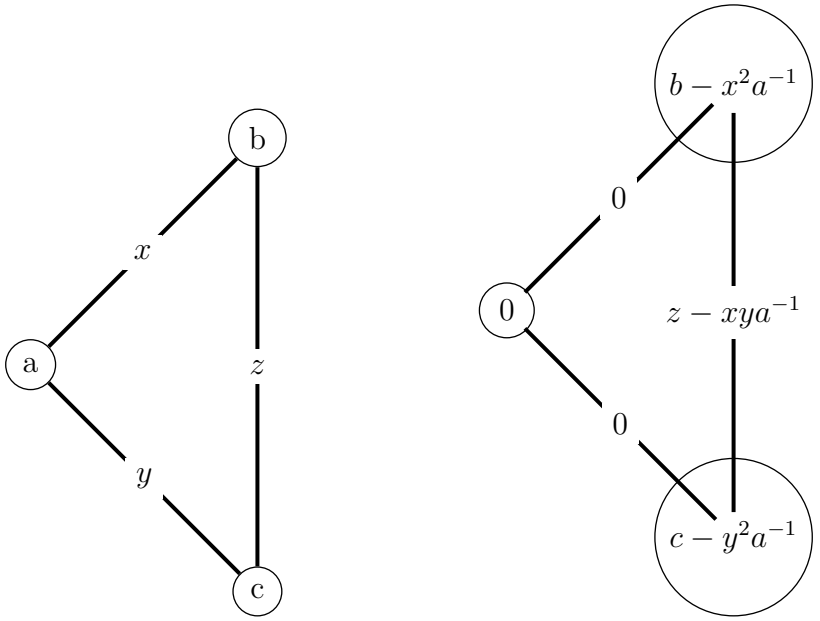

Figure 4.2 The weighted vertex a is pressed to transform G (left) to G' (right)

The weighted adjacency matrices for the figure are the following:

$$A(G) = \begin{bmatrix} a & x & y \\ x & b & z \\ y & z & c \end{bmatrix} \qquad A(G') = \begin{bmatrix} 0 & 0 & 0 \\ 0 & b - \frac{x^2}{a} & z - \frac{xy}{a} \\ 0 & z - \frac{xy}{a} & c - \frac{y^2}{a} \end{bmatrix}$$

Pressing in this fashion will result in Gaussian elimination, without row swaps, where the row of the pressed vertex is self-eliminated. A pressing sequence can be found if we can complete this elimination to result in the all zeroes matrix, which corresponds to the edge-less graph with vertices of weight 0.

Definition 4.8. Let $G = (V, f)$ be a $\mathbb{F}$-pseudograph and a vertex v, with $f(v, v)$ a quadratic residue in $\mathbb{F}$. A **self-preserving press** of v takes G to $G' = (V, g)$ with

$$g(x, y) = f(x, y) - \frac{f(x, v)f(y, v)}{f(v, v)} \text{ for } x, y \neq v$$

and with $g(v, v) = f(v, v)$.

A sequence of self-preserving presses is almost identical to a sequence of presses but after each press, instead of the vertex having weight 0, it retains its weight from when it was pressed. With this definition, a pressing sequence being successful would produce an edgeless graph where each vertex has weight indexed by a quadratic residue in the field. That is, we would be preforming Gaussian elimination on $A(G)$, both with row and column operations, without row or column swaps, to produce a diagonal matrix where all the entries are quadratic residues in the field.

Chapter 5

Positive Definite Matrices in Finite Fields

We need to find a new definition for positive definite matrices if we wish to proceed. In fact, we need to consider which elements in finite fields can be considered positive. When considering the real numbers, the non-negative reals are the only set whose square roots remain in the real numbers. The positive reals are simply nonzero non-negative numbers. We use this type of notion as our definition of positive.

Let $M_n(\mathbb{F}_q)$ be the set of $n \times n$ matrices with entries in $\mathbb{F}_q$.

Definition 5.1. For $x \in \mathbb{F}_p$, we say x is **positive** if $x = \mu^2$ for $\mu \in \mathbb{F}_p$, $\mu \neq 0$.

Currently, we have been able to analogize positive definite matrices in certain fields. This prompts the following definition in order to avoid confusion.

Definition 5.2. Define a field $\mathbb{F}$ to be a **definite field** if each positive element has a positive square root. That is, there is a square root of each positive element which is itself positive. If the field is finite, and needs to be specified as such, it will be referred to as a **finite definite field**.

Note that the real numbers are an example of a definite field, and we can discuss the notion of positive definiteness for the real numbers.

A finite field $\mathbb{F}_q$ will be a definite field if it has characteristic two, as every element is a quadratic residue as noted in Lemma 2.37, or $q = p^k$, in which -1 is not a quadratic residue modulo p. These fields occur for odd k with p congruent to 3 (mod 4) as noted in Lemma 2.41. That is, in these fields, if one square root of an

element is not a quadratic residue, we may multiply that root by -1, resulting in an element that is a quadratic residue.

5.1 Equivalences

At this point, we can finally begin to discuss what it means to be a positive definite matrix over these definite fields.

Definition 5.3. A symmetric matrix, A, over a 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.

Definition 5.4. If A is a symmetric $n \times n$ matrix over a definite field, A is **positive definite** if it possesses a Cholesky decomposition.

We can now begin stating our results, beginning with showing which equivalences remain true over definite fields.

Theorem 5.1. *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.*

Proof. Let $A \in M_n(\mathbb{F}_q)$ and $A = LL^T$ for some lower triangular matrix $L \in M_n(\mathbb{F}_q)$ whose diagonal elements are all nonzero. Let $\det(L_i) = \mu_i \in \mathbb{F}_q$, which will be nonzero, for L_i the ith leading principal submatrix of L. Every leading principal submatrix of A will also have such a decomposition by Lemma 2.24. That is, $A_i = L_i L_i^T$. Thus, $\det(A_i) = \det(L_i L_i^T) = \det(L_i)\det(L_i^T) = \mu\mu = \mu^2$. □

Lemma 5.5. *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.*

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 $r_{ii} = \sqrt{d_{ii}}$:

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

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. □

Theorem 5.2. *If all leading principal minors of a symmetric matrix A over a definite field are positive, then A has a Cholesky decomposition.*

Proof. Let A be a symmetric matrix in $M_n(\mathbb{F}_q)$ for a definite field $\mathbb{F}$ such that all leading principal minors are positive. Thus, all leading principal submatricies have full rank and A is invertible. Therefore, by Corollary 2.25, $A = LU$. 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 2.26, are positive and are, in fact, the entries of D. Thus, as we have an LDU decomposition where all the elements of D are positive, by Lemma 5.5, we can define $R = L\sqrt{D}$, a lower triangular matrix with positive diagonal entries, and $A = RR^T$ as desired. □

Theorem 5.3. *A matrix, $M \in \mathcal{M}_n(\mathbb{F}_q)$, is a Gram matrix if and only if it is positive definite.*

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 $x_1, x_2, ..., x_n \in \mathbb{F}_q^n$, which are linearly independent. Now, M_k will be equivalent to $A_k^T A_k$ where A_k has columns $x_1, ..., x_k$ by Lemma 2.17. 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 $l_1, l_2, ..., l_n$. As M is invertible, so is L and thus these l_i are linearly independent. M is therefore a Gram matrix for the vectors $l_1, l_2, ..., l_n$. □

Now, we have looked into equivalences concerning positive definite matrices, but what about linking this all back to pressing sequences? We discussed how to define pressing sequences over more than simply $\mathbb{F}_2$ in chapter 4, and now show that this is still equivalent to having a Cholesky decomposition. This will show that weighted adjacency matrices for any pressable graph are positive definite.

Theorem 5.4. *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 natural order form a successful pressing sequence. Thus, we can perform Gaussian elimination, and produce an LU decomposition. We consider this process of creating an LU decomposition with self-preserving pressing sequence. Each self-preserving press will multiply $A(G)$ by an elementary matrix on the left, E_1 representing row operations without swaps, and the elements on the diagonal of E_1 will be 1 as we are not changing the entry associated with the vertex pressed. Note that E_1 is also lower diagonal. As $A(G)$ is symmetric, performing the column operations will in fact be represented by right multiplication by E_1^T. That is, after a successful self-preserving press, we have $A(G') = E_1 A(G) E_1^T$.

If G has a successful pressing sequence, it has a successful self-preserving pressing sequence. That is, $EA(G)E^T = D$ 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 are only allowed to press positive weighted vertices, D has all positive entries. In fact, $A(G) = E^{-1}DE^{-T}$. 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 5.5, $A(G)$ 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 will all positive entries. Thus G has a successful self-preserving pressing sequence and also has a successful pressing sequence by pressing the vertices in their natural order. □

We have created new definitions for positive definite over definite fields and have explored which of the equivalences from Hermitian positive definite theory analogize. Further, we linked the notion of positive definite matrices back to pressable graphs. The following theorem puts all of these notions together and summarizes our work so far.

Theorem 5.5. *Let A be an $n \times n$ symmetric matrix over a definite field. The following are equivalent:*

1. *A is positive definite.*
2. *All leading principal minors of A are positive.*
3. *A is the Gram matrix of linearly independent vectors.*

4. *A is the weighted adjacency matrix for a pressable graph. The vertices of G, in the usual order, form a successful pressing sequence.*

5.2 Counterexamples

There are some equivalences, however, that no longer hold over definite fields. As we know that all equivalences hold for real matrices, as they are covered by the Hermitian case, we turn our attention specifically to finite definite fields. In this section, we consider the remaining 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 5.6. *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 sesquillinear 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 5.7. *The above properties do not hold, in general, over any finite definite field.*

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 $\mathcal{M}_n(\mathbb{F}_7)$, is positive definite as all leading principal minors are positive in $\mathbb{F}_7$ but has eigenvalues of 6 and 5, which are not quadratic residues in the field.

$$\begin{bmatrix} 2 & 4 \\ 4 & 2 \end{bmatrix}$$

For another example, consider the following in $M_3(\mathbb{F}_3)$, which has eigenvalues 1,2,2.

$$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 2 & 1 & 0 \end{bmatrix}$$

We could hope that the other direction is still true, that positive eigenvalues implies 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 quadratic residues 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 sesquillinear form defined by a matrix A is a function from $\mathbb{F}_{q^2}^n \to \mathbb{F}_{q^2}^n$ given by $\langle x, y\rangle = y^T Ax$ for $x, y \in \mathbb{F}_q$. 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 2, and therefore can be zero for nonzero x.

3. Consider the following matrix:

$$\begin{bmatrix} 1 & 2 & 0 \\ 2 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

which is positive definite in $\mathbb{F}_3$. One principal submatrix of this matrix is $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$, which is not positive definite. 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. In $\mathbb{F}_3$, the following matrix 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, most easily seen as $A_1 = [2]$ does not have positive determinant.

5. Consider the following in $\mathbb{F}_2$:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

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

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

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

We have that ABA is

$$\begin{bmatrix} 6 & 1 \\ 1 & 2 \end{bmatrix}$$

This matrix is not positive definite, most easily seen as $(ABA)_1 = [6]$ does not have positive determinant.

7. Consider $\begin{bmatrix} 1 & 4 \\ 4 & 3 \end{bmatrix}$ and $\begin{bmatrix} 2 & 2 \\ 2 & 3 \end{bmatrix}$ in $\mathbb{F}_7$, 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 a quadratic residue in $\mathbb{F}_7$ and therefore the matrix is not positive definite. Considering this same example, their Frobenius inner product is 6, which is also not a quadratic residue.

□

All of the above counterexamples were found by hand. It would be interesting to see if an algorithm can be created to produce a counterexample for a given finite field. It would also be interesting to explore whether, over some fields, counterexamples cannot be found and further equivalences or properties can be salvaged.

5.3 Other Properties

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

Theorem 5.8. *If A is a positive definite matrix over a definite field $\mathbb{F}$, and r is a quadratic residue 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 anti-diagonal identity matrix is positive definite.

Definition 5.6. For an invertible matrix A, define its **anti-inverse** as $\nabla A^{-1}\nabla$ where ∇ is the 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 3×3 case of ∇ is

$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

The following lemma will be helpful to prove that the anti-inverse is positive definite.

Lemma 5.7. *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

$$\begin{bmatrix} l_{11} & 0 & \cdots & 0 & \cdots & 0 \\ l_{21} & l_{22} & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ l_{i1} & l_{i2} & \cdots & l_{ii} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ l_{n1} & l_{n2} & \cdots & l_{ni} & \cdots & l_{nn} \end{bmatrix} \rightarrow \begin{bmatrix} l_{11} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ l_{(i-1)1} & l_{(i-1)2} & \cdots & l_{(i-1)(i-1)} & 0 & \cdots & 0 \\ l_{(i+1)1} & l_{(i+1)2} & \cdots & l_{(i+1)(i-1)} & l_{(i+1)(i+1)} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ l_{n1} & l_{n2} & \cdots & l_{n(i-1)} & l_{n(i+1)} & \cdots & l_{nn} \end{bmatrix}$$

The $(i-1)$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 5.9. *If A is a positive definite matrix in a definite field $\mathbb{F}$, then its anti-inverse is also positive definite.*

Proof. Let A be a positive definite matrix in a definite field $\mathbb{F}$. 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, for $L^{-T} = (L^{-1})^T$,

$$\begin{aligned} A^{-1} &= L^{-T}L^{-1} \\ \nabla A^{-1}\nabla &= \nabla L^{-T}L^{-1}\nabla \\ &= \nabla L^{-T}(\nabla\nabla)L^{-1}\nabla \\ &= (\nabla L^{-T}\nabla)(\nabla L^{-1}\nabla) \end{aligned}$$

Note that right multiplying by ∇ reverses the columns of the matrix and left multiplication by ∇ 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 ∇, 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)th entry will be $\frac{1}{\det(L)}$ 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 equivalent to 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 inner 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 5.10. *If A and B are positive definite matrices in a definite field $\mathbb{F}$, 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 $\mathbb{F}$, 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 ith row of L with the jth column of L^T, exactly a_{ij}, the entry of a in the ith row and jth column. Thus, the (i, j)th entry of $(L \otimes M)(L \otimes M)^T$ is $a_{ij}MM^T = a_{ij}B$ 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. $\square$

Chapter 6

Conclusion

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

In particular, it was considered but never quite looked into, that using the Frobenius endomorphism may allow us to define some kind of Hermitian form structure for these matrices. That is, instead of a conjugate transpose, what would happen if we put every element of the matrix through the Frobenius map 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 $x^T Ax = 0$ for some nonzero vector x. In terms of positive semi-definiteness, however, I wonder if this can be remedied and prove useful. It was also considered as to whether redefining "positive" using the Frobenius endomorphism may help to salvage the positive eigenvalue equivalence.

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

One can also consider what consequences the proven results have. As positive

definite matrices are used often in optimization problems, does this notion of positive definite over definite fields create some kind of geometric notion over other fields besides $\mathbb{R}$ and $\mathbb{C}$? Can we solve optimization problems over finite fields?

Further research with this topic has many paths one can take. Hopefully these questions and more can be solved and expanded upon to increase the impact and breadth in which positive definiteness touches mathematics.

Bibliography

[1] R. Bhatia. *Positive Definite Matrices..* Princeton University Press, 2007.

[2] J. P. C. Christian Berg and P. Ressel. *Harmonic Analysis on Semigroups: Theory of Positive Definite and Related Functions.* Springer-Verlag New York Inc., New York, New York, 1984.

[3] J. Cooper and J. Davis. Successful pressing sequences for a bicolored graph and binary matrices. *Linear Algebra and its Applications*, 490:162 – 173, 2016. ISSN 0024-3795. doi: https://doi.org/10.1016/j.laa.2015.11.001. URL `http://www.sciencedirect.com/science/article/pii/S0024379515006643`.

[4] R. Diestel. *Graph Theory.* Springer, 2010.

[5] G. E Fasshauer. Positive definite kernels: Past, present and future. 4, 01 2011.

[6] R. A. Horn and C. R. Johnson. *Matrix Analysis.* Cambridge University Press, New York, New York, 1985.

[7] J. Lahtonen. generalization of positive-definite matrices to matrices over finite fields. Mathematics Stack Exchange. URL `https://math.stackexchange.com/q/1862581`. URL:https://math.stackexchange.com/q/1862581 (version: 2016-07-17).

[8] D. C. Lay. *Linear Algebra and Its Applications.* Pearson Education, Inc., Boston, Massachusetts, 2012.

[9] M. Mathias. Über positive fourier-integrale. *Mathematische Zeitschrift*, 16:103–125, 1923. URL `http://eudml.org/doc/174954`.

[10] E. Moore. On properly positive hermitian matrices. *American Math Society*, 23, 59:pp. 66–67, 1916.

[11] P. Okunev and C. R. Johnson. Necessary And Sufficient Conditions For Existence of the LU Factorization of an Arbitrary Matrix. 2005. URL `http://arxiv.org/abs/math/0506382`.

[12] A. Wong. Primes and quadratic reciprocity. 2018. URL `https://www.researchgate.net/publication/237510055_PRIMES_AND_QUADRATIC_RECIPROCITY`.