DOKUZ EYLÜL UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

GENERALIZED INVERSES OF MATRICES AND APPLICATIONS TO CODING THEORY

by

Meltem GÜLLÜSAÇ

January, 2016

İZMİR

GENERALIZED INVERSES OF MATRICES AND APPLICATIONS TO CODING THEORY

A Thesis Submitted to the
Graduate School of Natural and Applied Sciences of Dokuz Eylül University
In Partial Fullfillment of the Requirements for the Degree of Master of Science
in Mathematics

by
Meltem GÜLLÜSAÇ

January, 2016
İZMİR

M.Sc THESIS EXAMINATION RESULT FORM

We have read the thesis entitled **"GENERALIZED INVERSES OF MATRICES AND APPLICATIONS TO CODING THEORY"** completed by **MELTEM GÜLLÜSAÇ** under supervision of **PROF. DR. CENAP ÖZEL** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Prof. Dr. Cenap ÖZEL

Supervisor

Doç.Dr. Mustafa ÖZEL

(Jury Member)

Doç. Dr Özlem EGE OKUR

(Jury Member)

Prof.Dr. Ayşe OKUR
Director
Graduate School of Natural and Applied Sciences

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my supervisor Prof. Dr. Cenap ÖZEL, for his excellent guidance, encouragement, help, advise, and endless patience during my study with him. I also would like to express my gratitude to all members of Dokuz Eylül University Department of Mathematics. Finally, I am deeply thankful to my family for their love, support and sacrificies. Without them, this thesis would never have been written.

Meltem GÜLLÜSAÇ

GENERALIZED INVERSES OF MATRICES AND APPLICATIONS TO CODING THEORY

ABSTRACT

This thesis deals with the application of generalized inverses of matrices over finite fields and the method of least squares in linear codes. It is proven that if the Moore-Penrose inverse of a generator matrix of a linear code exists, a unique word approaching to a received word near the codewords of the code can be found.

Together with the introduction, this thesis consists of six chapters. In the first chapter, historical development of generalized inverses is mentioned, shortly. In the second chapter, existence, construction and characterization of generalized inverses of matrices and their relation with linear systems are given. In the last section of chapter two, minimal properties of generalized inverses are investigated. In the third chapter, importantant properties of generalized inverses over finite fields, which are used as our tool to get our results in the fifth chapter, are described. The fourth chapter provides a brief description on error correcting codes and basic definitions in coding theory. In the fifth chapter, the concept of generalized inverses over finite fields and least square solutions applied to the codes. In the final chapter, the conclusion of this dissertation is given.

Keywords: Inconsistent linear systems, least-squares solutions, generalized inverses, Moore-Penrose inverses, linear codes, finite fields, error correcting codes, coding theory.

MATRİSLERİN GENELLEŞTİRİLMİŞ TERSLERİ VE KODLAMA TEORİSİNE UYGULAMALARI

ÖZ

Bu tez sonlu cisimler üzerindeki matrislerin genelleştirilmiş tersleri kavramının ve en küçük kareler metodunun doğrusal kodlara uygulanmasıyla ilgilidir. Bir doğrusal kodun üreteç matrisinin Moore-Penrose tersi var olduğunda, kodun kod kelimeleri yakınında elde edilmiş olan kod kelimesine yaklaşan tek bir kelime bulunabildiği kanıtlanmıştır.

Tez giriş bölümü ile altı bölümden oluşmaktadır. Birinci bölümde kısaca Genelleştirilmiş terslerin tarihsel gelişiminden bahsedilmiştir. İkinci bölümde matrislerin genelleştirilmiş terslerinin varlığı, inşası, karakterizasyonu ve doğrusal sistemlerle ilişkileri verilmiştir. İkinci bölümün sonunda, genelleştirilmiş terslerin minimal özellikleri incelemiştir. Üçüncü bölümde sonlu cisimler üzerindeki matrislerin beşinci bölümdeki sonuçlarımızı elde etmemiz için araç olacak önemli özellikleri ifade edilmiştir. Dördüncü bölüm, hata düzelten kodlar ve kodlama teorisindeki temel tanımlardan bahsetmektedir. Beşinci bölümde sonlu cisimler üzerindeki matrislerin genelleştirilmiş tersleri ve en küçük kareler çözümleri doğrusal kodlara uygulanmıştır. Son bölümde tezle ilgili sonuçlar verilmiştir.

Anahtar kelimeler: Tutarsız doğrusal sistemler, en küçük kareler çözümleri, genelleştirilmiş tersler, Moore-Penrose tersleri, doğrusal kodlar, sonlu cisimler, hata düzelten kodlar, kodlama teorisi.

CONTENTS

Page

CHAPTER ONE
INTRODUCTION

The theory of Generalized Inverses of Matrices has been addressed from the fifties for its numerous applications which include areas such as Markov chains, robotics, differential equations. The first written work on the concept of a generalized inverse seems to be the Fredholm (1903) on the generalized inverse of an integral operator. He called a particular generalized inverse as pseudo inverse. The class of all pseudo inverses was characterized by Hurwitz (1912). He used the finite dimensionality of the null spaces of the Fredholm operators to given an algebraic construction. Generalized inverses of differential operators studied by many authors. Moore (1920) formulated the generalized inverse of a matrix in an algebraic setting but his first publication on the subject appeared in 1920. Generalized inverses for operators were given by Murray & Von Neumann (1936) and others. Big expansion of interest in the area came in the 1950s by the study of the least squares properties. Bjerhammar (1951), Bjerhammar (1958) recognized these properties and he rediscovered Moore's inverse, additionally noted the relationship of generalized inverses to solutions of linear systems. Penrose (1955) showed that the Moore's inverse should satisfy the four equations and is unique. This unique inverse is now called the Moore-Penrose inverse. Since then, many papers on this subject have appeared.

The theory of generalized inverses has a potential for its wide applications, especially generalized inverses of matrices over finite fields. This subject is studied by many authors some of them are Fulton (1978), Pearl (1968) and Wu & Dawson (1998a).

Finite fields play fundamental role in applications including error correcting codes and Cryptography. For instance, Wu & Dawson (1998b) used generalized inverses in public key cryptosystem design.

In this thesis, we investigate the conditions of existence of the Moore-Penrose inverses over finite fields and the algebraic properties of them. We used these properties

of generalized inverses in error correction.

CHAPTER TWO
GENERALIZED INVERSES OF MATRICES

2.1 Existence and Construction of Generalized Inverses

2.1.1 Penrose Equations

Penrose (1955) showed that, for every finite matrix A (square or rectangular) of real or complex elements, there is a unique matrix X satisfying the four equations; (that we call the Penrose equations)

$$AXA = A \tag{2.1}$$

$$XAX = X \tag{2.2}$$

$$(AX)^* = AX \tag{2.3}$$

$$(XA)^* = XA \tag{2.4}$$

where A^* denotes the conjugate transpose of A. Because this unique generalized inverse had previously been studied (though defined in a different way) by Moore (1920), Moore (1935), it is commonly known as the Moore-Penrose inverse, and is often denoted by A^+.

If A is nonsingular, it is clear that $X = A^{-1}$ trivially satisfies the four equations. Since the Moore-Penrose inverse is known to be unique it follows that the Moore-Penrose inverse of a nonsingular matrix is the same as the ordinary inverse.

Throught this thesis, we will deal with a number of different subsets of the set offo ur Penrose equations, so we need a convenient notation for a generalized inverse satisfying certain specified equations. Let $\mathbb{C}^{m\times n}$ and [$\mathbb{R}^{m\times n}$] denote the class of $m \times n$ complex (real) matrices.

Definition 2.1.1. (Ben-Israel & Greville, 2003, Definition 1) For any $A \in \mathbb{C}^{m\times n}$, let

$A\{i,j,...,k\}$ denote the set of matrices $X \in \mathbb{C}^{n\times m}$ which satisfy equations $(2.i),(2.j),...,(2.k)$ from among the equations $(2.1)-(2.4)$. A matrix $X \in A\{i,j,...,k\}$ is called an $i,j,...,k-$*inverse* of A, and also denoted by $A^{(i,j,...k)}$.

2.1.2 Existence and Construction of {1}-Inverses

It is easy to construct a $\{1\}$-inverse of the matrix $R \in \mathbb{C}_r^{m\times n}$ given by

$$R = \begin{bmatrix} I_r & K \\ 0 & 0 \end{bmatrix} \tag{2.5}$$

For any $L \in \mathbb{C}^{(n-r)\times(m-r)}$, the $n \times m$ matrix

$$S = \begin{bmatrix} I_r & 0 \\ 0 & L \end{bmatrix}$$

is a $\{1\}$-inverse of (2.5). If R is of full column (row) rank, the two lower (right-hand) submatrices are interpreted as absent.

The construction of $\{1\}$-inverses for an arbitrary $A \in \mathbb{C}^{m\times n}$ is simplified by transforming A into a Hermite normal form, as shown in the following theorem, where E is the product of elementary matrices and P is a permutation matrix.

Theorem 2.1.2. *(Ben-Israel & Greville, 2003, Theorem 1) Let $A \in \mathbb{C}_r^{m\times n}$, and let $E \in \mathbb{C}_m^{m\times m}$ and $P \in \mathbb{C}_n^{n\times n}$ be such that*

$$EAP = \begin{bmatrix} I_r & K \\ 0 & 0 \end{bmatrix}. \tag{2.6}$$

Then for any $L \in \mathbb{C}^{(n-r)\times(m-r)}$, the $n \times m$ matrix

$$X = P \begin{bmatrix} I_r & K \\ 0 & 0 \end{bmatrix} L \tag{2.7}$$

is a {1}-inverse of A. The partitioned matrices in (2.6) and (2.7) must be suitably interpreted in case $r = m$ or $r = n$.

Proof. Rewriting (2.6) as

$$A = E^{-1} \begin{bmatrix} I_r & K \\ 0 & 0 \end{bmatrix} P^{-1} \tag{2.8}$$

it is easily verified that any X given by (2.7) satisfies $AXA = A$.

In the trivial case of $r = 0$, when A is therefore $m \times n$ null matrix, any $n \times m$ matrix is a $\{1\}$-inverse.

We note that since P and E are both nonsingular, the rank of X as given by (2.7) is the rank of the partitioned matrix in the right member. In view of the form of the latter matrix,

$$rankX = r + rankL \tag{2.9}$$

Since L is arbitrary, it follows that a $\{1\}$-inverse of A exists having any rank between r and $min\{m,n\}$, inclusive.

This theorem shows that every finite matrix with elements in the complex field has a $\{1\}$-inverse, and suggests how such an inverse can be constructed.

□

2.1.3 Properties of {1}-Inverses

Certain properties of $\{1\}$-inverse are given in Lemma 2.1.3. For a given matrix A, we denote any $\{1\}$-inverse by $A^{(1)}$. Note that, in general, $A^{(1)}$ is not uniquely defined matrix. For any scalar λ we define λ^+ by

$$\lambda^+ = \begin{cases} \lambda^{-1}, & \text{if } (\lambda \neq 0) \\ 0, & \text{if } (\lambda = 0) \end{cases} \tag{2.10}$$

.

Lemma 2.1.3. *(Ben-Israel & Greville, 2003, Lemma 1) Let $A \in \mathbb{C}_r^{m \times n}$, $\lambda \in \mathbb{C}$. Then,*

1. $(A^1)^* \in A^*\{1\}$.

2. *If A is nonsingular, $A^{(1)} = A^{-1}$ uniquely.*

3. $\lambda^{+}A^{(1)} \in (\lambda A)\{1\}$

4. $rankA^{(1)} \geq rankA$.

5. *If S and T are nonsingular, $T^{-1}A^{(1)}S^{-1} \in SAT\{1\}$.*

6. *$AA^{(1)}$ and $A^{(1)}A$ are idempotent and have the same rank as A.*

Proof. These are immediate consequences of the defining relation (2.1); (4) and the latter part of (6) depend on the fact that the rank of a product of matrices does not exceed the rank of any factor. □

If an $m \times n$ matrix A is of full column rank, its $\{1\}$-inverses are its left inverses. If it is full row rank, its $\{1\}$-inverses are its right inverses.

Lemma 2.1.4. *(Ben-Israel & Greville, 2003, Lemma 2) Let $A \in \mathbb{C}_r^{m\times n}$. Then ,*

1. *$A^{(1)}A = I_n$ if and only if $r = n$.*

2. *$AA^{(1)} = I_m$ if and only if $r = m$.*

Proof. (1) If : Let $A \in \mathbb{C}_r^{m\times n}$. Then $n \times n$ matrix $A^{(1)}A$ is, by Lemma 2.1.3(6), idempotent and nonsingular. Multiplying $(A^{(1)}A)^2 = A^{(1)}A$ by $(A^{(1)}A)^{-1}$ gives $A^{(1)}A = I_n$.
Only if : $A^{(1)}A = I_n \Longrightarrow rankA^{(1)}A = n \Longrightarrow rankA = n$, by Lemma 2.1.3.(6).
(2) Similarly proved. □

2.1.4 Bases for the Range and Null Space of a Matrix

For any $A \in \mathbb{C}^{m\times n}$ we denote by

$$R(A) = \{y \in \mathbb{C}^m : y = Ax \quad for \quad some \quad x \in \mathbb{C}^n\}, \text{the range of } A \text{ ,}$$

$$N(A) = \{x \in \mathbb{C}^n : Ax = 0\}, \text{the null space of } A \ .$$

A basis for $R(A)$ is useful in many applications, such as, in the numerical computation of the Moore-Penrose inverse.

The need for a basis of $N(A)$ is illustrated by the fact that the general solution of the linear inhomogeneous equation

$$Ax = b$$

is the sum of any particular solution x_0 and the general solution of the homogeneous equation

$$Ax = 0$$

The latter general solution consists of all linear combinations of the elements of any basis for $N(A)$.

A further advantage of the Hermite normal form EA of A (and its column permuted form EAP) is that from them bases for $R(A)$, $N(A)$, and $R(A^*)$ can be read off directly.

A basis for $R(A)$ consists of the c_1th, c_2th,...,c_rth-columns of A. Let P_1 denote the submatrix consisting of the first r columns of the permutation matrix P.Then, because of the way in which these r columns of P were chosen

$$EAP_1 = \begin{pmatrix} I_r \\ 0 \end{pmatrix}$$

Now, AP_1 is an $m \times r$ matrix, and is of rank r, since the right hand side of the above is of rank r. But AP_1 is merely the submatrix of A consisting of the c_1th,c_2th,...,c_rth columns. The columns of the $n \times (n-r)$ matrix

$$P \begin{pmatrix} -K \\ I_{n-r} \end{pmatrix}$$

are a basis for $N(A)$. Moreover it is evident that the first r rows of the Hermite normal form of EA are linearly independent, and each is some linear combination of the rows A. Thus they are basis for the space spanned by the rows of A. Consequently, if

$$EA = \begin{pmatrix} G \\ 0 \end{pmatrix}$$

then the columns of the $n \times r$ matrix

$$G^* = P \begin{pmatrix} I_r \\ K^* \end{pmatrix}$$

are a basis for $R(A^*)$.

2.1.5 Existence and Construction of {1,2}-Inverses

It was first noted by **?** that the existence of a $\{1\}$-inverse of a matrix A implies the existence of a $\{1,2\}$-inverse. This easily verified observation is stated as a lemma.

Lemma 2.1.5. *(Ben-Israel & Greville, 2003, Lemma 3) Let $Y,Z \in A\{1\}$, and let*

$$X = YAZ$$

Then $X \in A\{1,2\}$.

Since the matrices A and X occur symmetrically in (2.1) and (2.2), $X \in A\{1,2\}$ and $A \in X\{1,2\}$ are equivalent statements, and in either case we can say that A and X are $\{1,2\}$-inverses of each other.

From (2.1) and (2.2) and the fact that the rank of a product of matrices does not exceed the rank of any factor, it follows at once that if A and X are $\{1,2\}$-inverses of each other, they have the same rank. Less obvious is the fact, first noted by **?**, that if X is a $\{1\}$-inverse of A and of the same rank as A, it is a $\{1,2\}$-inverse of A.

Theorem 2.1.6. *(Ben-Israel & Greville, 2003, Theorem 2) Given A and $X \in A\{1,2\}$ if and only if rank$X$ = rank$A$.*

Proof. If : Clearly $R(AX) \subset R(X)$. But $rankXA = rankA$ by Lemma 2.1.3(6), and so, if $rankX = rankA$, $rank(XA) = rank(X)$. Thus,

$$XAY = X$$

for some Y. Premultiplication by A gives

$$AX = AXAY = AY$$

and therefore

$$XAX = X$$

Only if : This follows at once from (2.1) and (2.2). □

Corollary 2.1.7. *(Ben-Israel & Greville, 2003, Corollary 1) Any two of the following three statement imply the third:*

$$X \in A\{1\}$$

$$X \in A\{2\}$$

$$rankX = rankA$$

In view of Theorem 2.1.6, (2.9) shows that the $\{1\}$-inverse obtained from the Hermite normal form is a $\{1,2\}$-inverse if we take $L = 0$. In other words,

$$X = P \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} E$$

is a $\{1,2\}$-inverse of A is E and O are nonsingular and satisfy (2.6).

2.1.6 Existence and Construction of {1,2,3}-, {1,2,4}- and {1,2,3,4}-Inverses

Urquhart (1968) has shown that the existence of a $\{1\}$-inverse of every finite matrix with elements in $\mathbb{C}$ implies the existence of a $\{1,2,3\}$-inverse and a $\{1,2,4\}$-inverse of every such matrix. However, in order to show the nonemptiness of $A\{1,2,3\}$ and

$A\{1,2,4\}$ for any given A, we shall utilize the $\{1\}$-inverse not of A itself but a related matrix.

Lemma 2.1.8. *(Ben-Israel & Greville, 2003, Lemma 4) For any finite matrix A,*

$$rankAA^* = rankA = rankA^*A$$

Proof. If $A \in \mathbb{C}^{m\times n}$, both A and A^*A have m rows. The rank of any m-rowed matrix is equal to m minus the number of independent relations among its rows. To show that $rankAA^* = rankA$, it is sufficient, therefore, to show that every linear relation among the rows of A holds for the corresponding rows of A^*A, and vice versa. Any non trivial linear relation among the rows of a matrix H is equivalent to the existence of a nonzero row vector x^* such that $x^*H = 0$.
Now evidently,

$$x^*A = 0 \Longrightarrow x^*AA^* = 0$$

and conversely,

$$x^*AA^* = 0 \Longrightarrow 0 = x^*AA^*x = ((A^*X))^*A^*x \Longrightarrow A^*x = 0 \Longrightarrow 0 = ((A^*X))^* = x^*A$$

Here we have used the fact that, for any column vector y of complex elements y^*y is the sum of squares of the absolute values of the elements, and this sum vanishes only if every element is zero.

Applying this result to the matrix A^* gives $rankA^*A = rankA^*$, and of course, $rankA^* = rankA$.

□

Corollary 2.1.9. *(Ben-Israel & Greville, 2003, Corollary 2) For any finite matrix A,* $R(AA^*) = R(A)$ *and* $N(AA^*) = N(A)$.

Proof. This follows from Lemma 2.1.8. □

Theorem 2.1.10. *(Ben-Israel & Greville, 2003, Theorem 3) For every finite matrix A with complex elements,*

$$Y = (A^*A)^{(1)}A^* \in A\{1,2,3\} \tag{2.11}$$

and

$$Z = A^*(AA^*)^{(1)} \in A\{1,2,4\} \tag{2.12}$$

Proof. Applying Corollary 2.1.9 to A^* gives

$$R(A^*A) = R(A^*)$$

and so,

$$A^* = A^*AU \tag{2.13}$$

for some U. Taking conjugate transpose gives

$$A = U^*A^*A \tag{2.14}$$

Consequently,

$$AYA = U^*A^*A(A^*A)^{(1)}A^*A = U^*A^*A = A$$

Thus, $Y \in A\{1\}$. But $rankY \geq rankA$ by Lemma 2.1.3(4), and $rankY \leq rankA^* = rankA$ by the definition of Y. Therefore

$$rankY = rankA$$

and by Theorem 2.1.6, $Y \in A\{1,2\}$. Finally, (2.13) and (2.14) give

$$AY = U^*A^*A(A^*A)^{(1)}A^*AU = U^*A^*AU$$

, which is clearly Hermitian. Thus (2.11) is established.

(2.12) is similarly proved. □

If we can establish the existence of a {1,2,3,4}-inverse, we will have demonstrated the existence of an {i,j,...,k}-inverse for all possible choices of one, two or three integers $i, j, ..., k$ from the set {1,2,3,4}. If a {1,2,3,4}-inverse exists, it is unique. We know that it does exist, because it is the well-known Moore-Penrose inverse, A^+.

Theorem 2.1.11. *(Ben-Israel & Greville, 2003, Theorem 4) For any finite matrix A of complex elements,*

$$A^{(1,4)}AA^{1,3} = A^+ \tag{2.15}$$

Proof. Let X denote the left hand side of (2.15). It follows from Lemma 2.1.5 that $X \in A\{1,2\}$. Moreover, (2.15) gives

$$AX = AA^{(1,3)}, \quad XA = A^{(1,4)}A$$

But both $AA^{(1,3)}$ and $A^{(1,4)}A$ are Hermitian, by the definition of $A^{(1,3)}$ and $A^{(1,4)}$. Thus

$$X \in A\{1,2,3,4\}.$$

However, $A\{1,2,3,4\}$ contains at most a single element. Therefore, it contains exactly one element, which we denote by A^+, and $X = A^+$. □

2.1.7 Full Rank Factorization

A non-null matrix that is not of full (column or row) rank can be expressed as the product of a matrix of full column rank and a matrix of full row rank. Such factorizations turn out to be a powerful tool in the study of generalized inverses.

Lemma 2.1.12. *(Ben-Israel & Greville, 2003, Lemma 5) Let $A \in \mathbb{C}_r^{m\times n}$, $r > 0$. Then there exists matrices $F \in \mathbb{C}_r^{m\times r}$ and $G \in \mathbb{C}_r^{r\times n}$, such that*

$$A = FG. \tag{2.16}$$

Proof. Let F be any matrix whose columns are a basis for $R(A)$. Then $F \in \mathbb{C}_r^{m\times r}$. The matrix $G \in \mathbb{C}_r^{r\times n}$ is then uniquely determined by (2.16), since every column of

A is uniquely representable as a linear combination of the columns of F. Finally, $rankG = r$, since

$$rankG \geq rankFG = r$$

The columns of F can, in particular, be chosen as any maximal linearly independent set of columns of A. Also, G could be chosen first as any matrix whose rows are a basis for the space spanned by the rows of A, then F is uniquely determined by (2.16).

We shall call a factorization (2.16) with properties stated in Lemma 2.1.12. a full-rank factorization of A. □

2.1.8 Explicit Formula for A^+

C.C. MacDuffee apparently was the first to point out, about 1959, that a full-rank factorization of a matrix A leads to an explicit formula for its Moore-Penrose inverse, A^+. However, he did so in private communications, there is no published work that can be cited.

Theorem 2.1.13. *(Ben-Israel & Greville, 2003, Theorem 5) If $A \in \mathbb{C}_r^{m\times n}$, $r > 0$, has a full-rank factorization*

$$A = FG, \tag{2.17}$$

then

$$A^+ = G^*(F^*AG^*)^{-1}F^*. \tag{2.18}$$

Proof. First, we must show that F^*AG^* is nonsingular. By (2.17),

$$F^*AG^* = (F^*F)(GG^*), \tag{2.19}$$

and both factors of the right member are $r \times r$ matrices. Also, by Lemma 2.1.8, both are of rank r. Thus, F^*AG^* ,s the product of two nonsingular matrices, and therefore

nonsingular. Moreover, (2.19) gives

$$(F^*AG^*)^{-1} = (GG^*)^{-1}(F^*F)^{-1}.$$

Denoting by X the right member of (2.18), we now have

$$X = G^*(GG^*)^{-1}(F^*F)^{-1}F^*, \tag{2.20}$$

and this expression for X satisfies the Penrose equations (2.1)-(2.4). As A^+ is the sole element of $A\{1,2,3,4\}$ (2.17) is therefore established.

□

2.1.9 An Algorithm for computing the Generalized Inverse of a matrix

To obtain the full rank factorization and the generalized inverse for any $A \in \mathbb{C}^{m\times n}$, we can use the following algorithm; see (Campbell & Meyer, 2009, Algorithm 1.3.2) ,

1. Reduce A to row echelon form E_A
2. Select the distinguished columns of A and place them as the columns in a matrix F in the same order as they appear in A
3. Select the nonzero rows from E_A and place them as rows in a matrix G in the same order as they appear in E_A
4. Compute $(GG^*)^{-1}$ and $(F^*F)^{-1}$
5. Compute A^+ as $A^+ = G^*(GG^*)^{-1}(F^*F)^{-1}F^*$

Remark 2.1.14. If E_A is the row echelon form for A and the unit vectors in E_A appear in columns $i_1, i_2, ..., i_r$ then the correspoding columns of A are a basis for $R(A)$. This particular basis is called the distinguished columns of A.

Example 2.1.15. (Campbell & Meyer, 2009, Example 1.3.3) We will use this algorithm to find A^+ where

$$A = \begin{pmatrix} 1 & 2 & 1 & 4 & 1 \\ 2 & 4 & 0 & 6 & 6 \\ 1 & 2 & 0 & 3 & 3 \\ 2 & 4 & 0 & 6 & 6 \end{pmatrix}$$

1. Using elementary row operations we reduce A to its row echelon form

$$E_A = \begin{pmatrix} 1 & 2 & 0 & 3 & 3 \\ 0 & 0 & 1 & 1 & -2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

2. The first and third columns are distinguished. Thus

$$F = \begin{pmatrix} 1 & 1 \\ 2 & 0 \\ 1 & 0 \\ 2 & 0 \end{pmatrix}$$

3. The matrix G is made up of the nonzero rows of E_A so that

$$G = \begin{pmatrix} 1 & 2 & 0 & 3 & 3 \\ 0 & 0 & 1 & 1 & -2 \end{pmatrix}$$

4. Now $GG^* = \begin{pmatrix} 23 & -3 \\ -3 & 6 \end{pmatrix}$ and $F^*F = \begin{pmatrix} 10 & 1 \\ 1 & 1 \end{pmatrix}$. Calculating $(GG^*)^{-1}$ and $(F^*F)^{-1}$ we get $(GG^*)^{-1} = \frac{1}{129}\begin{pmatrix} 6 & 3 \\ 3 & 23 \end{pmatrix}$ and $(F^*F)^{-1} = \frac{1}{9}\begin{pmatrix} 1 & -1 \\ -1 & 10 \end{pmatrix}$ 5. Substituing

the results of steps 2., 3., and 4., into the formula for A^+ gives

$$A^+ = G^*(GG^*)^{-1}(F^*F)^{-1}F^* = \frac{1}{1161}\begin{pmatrix} 27 & 6 & 3 & 6 \\ 54 & 12 & 6 & 12 \\ 207 & -40 & -20 & -40 \\ 288 & -22 & -11 & -22 \\ -333 & 98 & 49 & 98 \end{pmatrix}$$

For more methods and algorithms to calculate A^+ see Campbell & Meyer (2009).

2.2 Linear Systems and Characterization of Generalized Inverses

2.2.1 Solutions of Linear Systems

The principal application of $\{1\}$-inverses is to the solution of Linear systems, where they are used in much the same way as ordinary inverses in nonsingular case.

Theorem 2.2.1. *Ben-Israel & Greville (2003) Let $A \in \mathbb{C}^{m\times n}$, $B \in \mathbb{C}^{p\times q}$, $C \in \mathbb{C}^{m\times q}$. Then the matrix equation*

$$AXB = D \tag{2.21}$$

is consistent if and only if for some $A^{(1)}$, $B^{(1)}$,

$$AA^{(1)}DB^{(1)}B = D \tag{2.22}$$

in which case the general solution is

$$X = A^{(1)}DB^{(1)} + Y - A^{(1)}AYBB^{(1)} \tag{2.23}$$

for arbitrary $Y \in \mathbb{C}^{n\times p}$.

Proof. If (2.22) holds, then $X = A^{(1)}DB^{(1)}$ is a solution of (2.21). Conversely, if X is

any solution of (2.21), then

$$D = AXB = AA^{(1)}AXBB^{(1)}B = AA^{(1)}DBB^{(1)}.$$

Moreover, it follows from (2.22) and the definition of $A^{(1)}$ and $B^{(1)}$ that every matrix X of the form (2.21) satisfies (1). On the other hand, let X be any solution of (2.20). Then,

$$X = A^{(1)}DB^{(1)} + X - A^{(1)}AXBB^{(1)}$$

which is of the form (2.22). □

The following corollary is the characterization of the set $A\{1\}$.

Corollary 2.2.2. *Ben-Israel & Greville (2003) Let $A \in \mathbb{C}^{m\times n}$, $A \in A\{1\}$. Then*

$$A\{1\} = \{A^{(1)} + Z - A^{(1)}AZAA^{(1)} : Z \in \mathbb{C}^{n\times m}\} \tag{2.24}$$

Proof. The set described in right hand side of (2.24) is obtained by writing $Y = A^{(1)} + Z$ in the set of solutions of $AXA = A$ as given by Theorem 2.2.1. □

Corollary 2.2.3. *Ben-Israel & Greville (2003) Let $A \in \mathbb{C}^{m\times n}$, $b \in \mathbb{C}^m$. Then the equation*

$$Ax = b \tag{2.25}$$

is consistent if and only if for some $A^{(1)}$

$$AA^{(1)}b = b \tag{2.26}$$

in which case the general solution of (2.25) is

$$x = A^{(1)}b + (I - A^{(1)}A)Y \tag{2.27}$$

for arbitrary $y \in \mathbb{C}^n$.

Theorem 2.2.4. *Ben-Israel & Greville (2003) Let $A \in \mathbb{C}^{m\times n}$, $X \in \mathbb{C}^{n\times m}$. Then $X \in A\{1\}$ if and only if for all b such that $Ax = b$ is consistent, $x = Xb$ is a solution.*

Proof. If: Let a_j denote the jth column of A. Then

$$Ax = a_j$$

is consistent, and Xa_j is a solution,

$$AXa_j = a_j \quad (j \in \bar{1,n})$$

So,

$$AXA = A$$

Only if: This follows from (2.26). □

2.2.2 Characterization of A{1,3} and A{1,4}

Theorem 2.2.5. *Ben-Israel & Greville (2003) The set $A\{1,3\}$ consists of all solutions for X of*

$$AX = AA^{(1,3)} \tag{2.28}$$

where $A^{(1,3)}$ is an arbitrary element of $A\{1,3\}$.

Proof. If X satisfies (2.28), then clearly

$$AXA = AA^{(1,3)}A = A$$

and , AX is Hermitian since $AA^{(1,3)}$ is Hermitian by definition. Thus $X \in A^{(1,3)}$.

On the other hand, if $X \in A^{(1,3)}$ then,

$$AA^{(1,3)} = AXAA^{(1,3)} = (AX)^*AA^{(1,3)} = X^*A^*(A^{(1,3)})^*A^* = X^*A^* = AX$$

We have used Lemma 2.1.3.(1). □

Corollary 2.2.6. *Ben-Israel & Greville (2003) Let $A \in \mathbb{C}^{m\times n}$, $A^{(1,3)} \in A\{1,3\}$. Then*

$$A\{1,3\} = \{A^{(1,3)} + (I - A^{(1,3)}A)Z : \quad Z \in \mathbb{C}^{n\times m}\} \tag{2.29}$$

Proof. Applying Theorem 2.2.1 to (2.28) and substituting $Z + A^{(1,3)}$ for Y gives (2.29). □

Theorem 2.2.7. *Ben-Israel & Greville (2003) The set $A\{1,4\}$ consists of all solutions for X of*

$$XA = A^{(1,4)}A$$

where $A^{(1,4)}$ is an arbitrary element of $A\{1,4\}$.

Corollary 2.2.8. *Ben-Israel & Greville (2003) Let $A \in \mathbb{C}^{m\times n}$, $A^{(1,4)} \in A\{1,4\}$. Then*

$$A\{1,4\} = \{A^{(1,4)} + Y(I - AA^{(1,4)}) : \quad Y \in \mathbb{C}^{n\times m}\}.$$

2.2.3 Idempotent Matrices and Projectors

Some basic properties of Idempotent matrices are listed in the following Lemma.

Lemma 2.2.9. *Ben-Israel & Greville (2003) Let $E \in \mathbb{C}^{n\times n}$ be idempotent. Then,*

1. *E^* and $I - E$ are idempotent.*
2. *The eigenvalues of E are 0 and 1. The multiplicity of the eigenvalue 1 is rank E.*
3. *$rankE = traceE$*
4. *$E(I - E) = (I - E)E = 0$*
5. *$Ex = x$ if and only if $x \in R(E)$*
6. *$E \in E\{1,2\}$*
7. *$N(E) = R(I - E)$*

Proof. Parts (a) to (f) are consequences of the definition of idempotency. (c) follows from (b) and the fact that the trace of any square matrix is the sum of its eigenvalues counting multiplicities. (g) is obtained by applying Corollary 2.2.3 to the equation $Ex = 0$. □

Lemma 2.2.10. *Ben-Israel & Greville (2003) Let a square matrix have the full-rank factorization*

$$E = FG$$

Then E is idempotent if and only if $GF = I$.

Proof. If $GF = I$ then

$$(FG)^2 = FGFG = FG \tag{2.30}$$

On the other hand, since F is of full column rank and G is of full row rank,

$$F^{(1)}F = GG^{(1)} = I$$

by Lemma 1.2. Thus if (2.30) holds, $GF = I$. □

Let $P_{L,M}$ denote the transformation that carries any $x \in \mathbb{C}^n$ into its projection on L along M. We shall call the transformation $P_{L,M}$ the projector on L along M.

It is well-known that every linear transformation from one finite-dimensional vector space to another can be represented by a matrix, which is uniquely determined by the linear transformation and by the choice of bases for the spaces involved. Suppose that we have fixed the bases as the standard basis for any finite dimensional vector space, there is one-to-one correspondence between $\mathbb{C}^{m\times n}$, $m \times n$ complex matrices and $\mathcal{L}(\mathbb{C}^n, \mathbb{C}^n)$, the space of linear transformations mapping $x \in \mathbb{C}^n$ into $x \in \mathbb{C}^m$. This correspondence permits using the same symbol, say A, to denote both the linear transformation $A \in \mathcal{L}(\mathbb{C}^n, \mathbb{C}^n)$ and its matrix representation $A \in \mathbb{C}^{m\times n}$. Thus the matrix-vector equation,

$$Ax = y$$

can equally be regarded as a statement that the linear transformation A maps x into y.

In particular, linear transformations mapping $\mathbb{C}^n$ into itself are represented by the square matrices of order n. Next theorem shows that there is a one to one correspondence between the idempotent matrices of order n and the projectors $P_{L,M}$ where $L \oplus M = \mathbb{C}^n$. Furthermore, for any two complementary subspaces L and M, there is a method for computing $P_{L,M}$

Theorem 2.2.11. *Ben-Israel & Greville (2003) For every idempotent matrix $E \in \mathbb{C}^{n\times n}$, $R(E)$ and $N(E)$ are complementary subspaces with*

$$E = P_{R(E),N(E)}. \tag{2.31}$$

Conversely, if L and M are complementary subspaces, there is a unique idempotent $P_{L,M}$ such that $R(P_{L,M}) = L$ and $N(P_{L,M}) = M$

Proof. Let E be idempotent of order n. Then it follows from Lemma 1(e) and 1(g) and from the equation

$$x = Ex + (I - E)x \tag{2.32}$$

the $\mathbb{C}^n$ is the sum of $R(E)$ and $N(E)$. Moreover $R(E) \cap N(E) = \{0\}$, since

$$Ex = (I - E)y \Longrightarrow Ex = E^2x = E(I - E)y = 0$$

by Lemma 1(d). Thus $R(E)$ and $N(E)$ are complementary and (2.32) shows that for every x, Ex is the projection of x on $R(E)$ along $N(E)$. This establishes (2.31).

On the other hand, let $\{x_1, x_2, ..., x_l\}$ and $\{y_1, y_2, ..., y_m\}$ be any two bases for L and M, respectively. Then $P_{L,M}$ if it exists, is uniquely determined by

$$\begin{cases} P_{L,M}x_i = x_i & (i \in 1, l) \\ P_{L,M}y_i = 0 & (i \in 1, m) \end{cases} \tag{2.33}$$

Let $X = [x_1, x_2, ..., x_l]$ denote the matrix whose columns are the vectors x_i. Similarly,

let $Y = [y_1, y_2, ..., y_m]$. Then (2.30) is equivalent to

$$P_{L,M}[XY] = [X0] \tag{2.34}$$

Since $[XY]$ is nonsingular, the unique solution of (2.34) is

$$P_{L,M} = [XO][XY]^{-1} \tag{2.35}$$

Since (2.33) implies

$$P_{L,M}[XO] = [XO]$$

$P_{L,M}$ as given by (2.35) is clearly idempotent. □

Corollary 2.2.12. *Ben-Israel & Greville (2003) Let L and M be complementary subspaces of $\mathbb{C}^n$. Then for every $x \in \mathbb{C}^n$, the unique decomposition is given by*

$$P_{L,M}x = y, \quad (I - P_{L,M})x = z$$

If $A^{(1)} \in A\{1\}$, we know that $AA^{(1)}$ and $A^{(1)}A$ are idempotent and $R(AA^{(1)}) = R(A)$ and $N(A^{(1)}A) = N(A)$. The next corollary is the consequence of these results.

Corollary 2.2.13. *Ben-Israel & Greville (2003) If A and X are {1,2}-inverses of each other, AX is the projector on $R(A)$ along $N(X)$, and XA is projector on $R(X)$ along $N(A)$.*

Theorem 2.2.14. *Ben-Israel & Greville (2003) Let $A \in \mathbb{C}^{n\times n}$ with k distinct eigevalues $\lambda_1, \lambda_2, ..., \lambda_k$. Then A is diagonable if and only if there exists projectors $E_1, E_2, ..., E_k$ such that*

$$E_i E_j = 0, \quad if \quad i \neq j \tag{2.36}$$

$$I_n = \sum_{1}^{k} E_i \tag{2.37}$$

$$A = \sum_{i=1}^{k} \lambda_i E_i \tag{2.38}$$

Proof. If: For $i \in 1, k$, let $r_i = rank E_i$ and let $X_i \in \mathbb{C}^{n\times r_i}$ be a matrix whose columns

are basis for $R(E_i)$. Let

$$X = [X_1 X_2 ... X_k]$$

Then by Lemma 2.2.9(3), the number of columns of X is

$$\sum_{i=1}^{k} r_i = \sum_{i=1}^{k} traceE_i = trace \sum_{i=1}^{k} E_i = traceI_n = n$$

by (2.37). Thus X is square of order n. By the definition of X_i, there exists for each i a Y_i such that

$$E_i = X_i Y_i$$

Let

$$Y = \begin{bmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_k \end{bmatrix}$$

Then

$$XY = \sum_{i=1}^{k} \lambda_i E_i X_i = XD \tag{2.39}$$

where

$$D = diag(\lambda_1 I_1, \lambda_2 I_2, ..., \lambda_k I_k) \tag{2.40}$$

I_i is being used to denote the unit matrix of order r_i. Since X is nonsingular, it follows from (2.35) that A and D are similar.

Only if: If A is diagonable,

$$AX = XD \tag{2.41}$$

where X is nonsingular, and D can be represented in the form (33). Let X be partitioned by columns into $X_1, X_2, \ldots, X_k$ i conformity with the diagonal blocks of D, and for $i = 1, 2, \ldots, k$, let

$$E_i = [O \ldots O X_i O \ldots O] X^{-1}$$

In other words, $E_i = \breve{X}_i X^{-1}$, where $\breve{X}_i$ denotes the matrix obtained from X by replacing all its columns except the the columns of X_i by columns of zeros. It is easily verified

that E_i is idempotent, and (2.36), (2.37) hold.

$$\sum_{i=1}^{k} \lambda_i E_i = [\lambda_1 X_1 \lambda_2 X_2 \ldots \lambda_k X_k] X^{-1} = XDX^{-1} = A$$

by (2.41). The idempotent matrices E_i are called its principal idempotents. Relation (2.38) is called the spectral decomposition of A. □

2.2.4 Orthogonal Projections and Orthogonal Projectors

Given a vector $x \in \mathbb{C}^n$ and a subspace L of $\mathbb{C}^n$, there is in L a unique vector u_x that is closest to x in the sense that the distance $\|x-u\|$ is smaller for $u = u_x$ than for any other $u \in L$. Here $\|v\|$ denotes the Euclidean norm of the vector v,

$$\|v\| = +\sqrt{(v,v)} = +\sqrt{v^* v} = +\sqrt{\sum_{j=1}^{n} |v_j|^2}$$

where (v,w) denotes the standart inner product, defined for $v,w \in \mathbb{C}^n$ by

$$(v,w) = w^* v = \sum_{j=1}^{n} \bar{w}_j v_j$$

The vector u_x that is closest to x of all vectors in L is uniquely characterized by the fact that $x-u_x$ is orthogonal to u_x, we we can denote by

$$x - u_x \perp u_x$$

We call u_x the orthogonal projection of x on L. The transformation that carries each $x \in \mathbb{C}^n$ into its orthogonal projection on L we shall denote by P_L and shall call the orthogonal projector on L. The orthogonal projector on L is the same as the projector on L along $L^\perp$.

Being a particular case of the more general projector, the orthogonal projector is representable by a square matrix, which, in this case, is not only idempotent but also Hermitian.

To prove this we need the following relation

$$N(A) = R(A^*)^\perp \tag{2.42}$$

Let L and M be complementary orthogonal subspaces of $\mathbb{C}^n$ and consider the matrix $P^*_{L,M}$. By Lemma 2.2.9.(1) it is idempotent therefore a projector by Theorem 2.2.11. By the use of (2.42) and its dual

$$N(A^*) = R(A)^\perp \tag{2.43}$$

it is found that,

$$R(P^*_{L,M}) = M^\perp, \qquad N(P^*_{L,M}) = L^\perp$$

Thus by Theorem 2.2.11.,

$$P^*_{L,M} = P_{M^\perp,L^\perp} \tag{2.44}$$

Lemma 2.2.15. *Ben-Israel & Greville (2003) Let $C^n = L \oplus M$. Then $M = L^\perp$ if and only if $P_{L,M}$ is Hermitian.*

Just as there is a one to one correspondence between projectors and idempotent matrices, Lemma 2.2.15 shows that there is a one to one correspondence between orthogonal projectors and Hermitian idempotents.

For any subspace L for which a basis is available, it is easy to construct the matrix P_L. The basis must first be orthonormalized. Let $\{x_1, x_2, \ldots x_l\}$ be an orthonormal basis for L. Then

$$P_L = \sum_{j=1}^{l} x_j x_j^* \tag{2.45}$$

(2.45) is the orthogonal projector on L and (2.35) reduces to (2.45) if $M = L^\perp$.

We recall that a square matrix A is called normal if it commutes with its conjugate transpose

$$AA^* = A^*A$$

It is well known that every normal matrix is diagonable. Also a normal matrix A has the property that the eigenvalues of A^* are the conjugates of those of A, and every eigevector of A associated with the eigenvalue λ is also an eigenvector of A^* associated with the eigenvalue $\bar{\lambda}$.

The following theorem relates normal matrices to orthogonal projectors.

Theorem 2.2.16. *Ben-Israel & Greville (2003) Let $A \in \mathbb{C}^{n\times n}$ with k distinct eigevalues $\lambda_1, \lambda_2, ..., \lambda_k$. Then A is normal if and only if there exists orthogonal projectors $E_1, E_2, ..., E_k$ such that*

$$E_i E_j = 0, \quad if \quad i \neq j \tag{2.46}$$

$$I_n = \sum_{1}^{k} E_i \tag{2.47}$$

$$A = \sum_{i=1}^{k} \lambda_i E_i \tag{2.48}$$

Proof. If: Let A be given by (2.48) where the principal idempotents are Hermitian. Then

$$AA^* = \left(\sum_{i=1}^{k} \lambda_i E_i\right)\left(\sum_{j=1}^{k} \bar{\lambda}_j E_j\right) = \sum_{i=1}^{k} |\lambda_i|^2 E_i = A^*A$$

Only if: Since A is normal, it is diagonable; let $E_1, E_2, ..., E_k$ be its principal idempotents. We must show that they are Hermitian. $R(E_i)$ the eigenspace of A associated with the eigenvalue λ_i is the same as the eigenspace of A^* associated with $\bar{\lambda}_i$. Because of (2.46), the null spaces corresponding principal idempotents of A and A^* are also the same.

Therefore, A and A^* have the same principal idempotents, by Theorem 2.2.11. Consequently,

$$A^* = \sum_{i=1}^{k} \bar{\lambda}_i E_i$$

by Theorem 2.2.14. But taking conjugate transposes in (2.48) gives

$$A^* = \sum_{i=1}^{k} \bar{\lambda}_i E_i^*$$

and it is easily seen that the idempotents E_i^* satisfy (2.46) and (2.47). Since the spectral decomposition is unique, we must have

$$E_i = E_i^* \qquad i \in \bar{1,k}.$$

□

2.3 Minimal Properties of Generalized Inverses

2.3.1 Least Squares Solutions of Inconsistent Linear Systems

For a given $A \in \mathbb{C}^{m\times n}$, and $b \in \mathbb{C}^m$, the linear system

$$Ax = b \tag{2.49}$$

is consistent, i.e., has a solution for x, if and only if $b \in R(A)$. Otherwise, the residual vector

$$r = b - Ax \tag{2.50}$$

is nonzero for all $x \in \mathbb{C}^n$ and it may desired to find to find an approximate solution of (2.49), by which is meant a vector x making the residual vector (2.49) closest to zero in some sense, i.e., minimizing some norm of (2.50). An approximate solution that is often used is the least-squares solution of (2.49), defined as a vector x minimizing the Euclidean norm of the residual vector, i.e., minimizing the sum of squares of moduli of the residuals

$$\sum_{i=1}^{m} \mid r_i \mid^2 = \sum_{i=1}^{m} \mid b_i - \sum_{j=1}^{n} a_{ij}x_j \mid^2 = \|b - Ax\|^2 \tag{2.51}$$

The following theorem shows that $\|Ax - b\|$ is minimized by choosing $x = Xb$, where $X \in A\{1,3\}$, thus establishing a relation between the $\{1,3\}$-inverses and the least squares solutions of $Ax = b$, characterizing each of these two concepts in terms of the other.

Theorem 2.3.1. *Ben-Israel & Greville (2003) Let $A \in \mathbb{C}^{m\times n}$, $b \in \mathbb{C}^m$. Then $\|Ax-b\|$ is smallest when $x = A^{(1,3)}b$, where $A^{(1,3)} \in A\{1,3\}$. Conversely, if $X \in \mathbb{C}^{n\times m}$ has the property that, for all b, $\|Ax-b\|$ is smallest when $x = Xb$, then $X \in A\{1,3\}$.*

Proof.

$$b = (P_{R(A)} + P_{R(A)^\perp}) \tag{2.52}$$

$$b - Ax = (P_{R(A)}b - Ax) + P_{N(A^*)}b$$

$$\|Ax-b\|^2 = \|Ax - P_{R(A)}b\|^2 + \|P_{N(A^*)}b\|^2 \tag{2.53}$$

(2.53) assumes its minimum value if and only if

$$Ax = P_{R(A)}b \tag{2.54}$$

which holds if $x = A^{(1,3)}b$ for any $A^{(1,3)} \in A\{1,3\}$, since by Theorem 2.2.11, and Lemma 2.2.15.

$$AA^{(1,3)} = P_{R(A)}.$$

Conversely, if X is such that for all b, $\|Ax-b\|$ is smallest when $x = Xb$, (2.54) gives $AXb = P_{R(A)}b$ for all b, and therefore

$$AX = P_{R(A)}.$$

Thus, by Theorem 2.3, $X \in A\{1,3\}$. □

Corollary 2.3.2. *Ben-Israel & Greville (2003) A vector x is a least squares solution of $Ax = b$ if and only if*

$$Ax = P_{R(A)}b = AA^{(1,3)}b.$$

Thus the general least squares solution is

$$x = A^{(1,3)}b + (I_n - A^{(1,3)}A)y \tag{2.55}$$

with $A^{(1,3)} \in A\{1,3\}$ and arbitrary $y \in \mathbb{C}^n$.

It is important to note that the least-squares solution is unique only when A is of full column rank. Otherwise, (2.55) is an infinite set of such solutions.

CHAPTER THREE
GENERALIZED INVERSES OVER FINITE FIELDS

3.1 Some Properties of Finite Fields

Let p be a prime, $q = p^m$ with $m \geq 1$. Denote by F_q the finite field with q elements. Let $M_{m\times n}$ be the set of all matrices over F_q of order $m \times n$. It is known that any $A \in M_{m\times n}$ corresponds uniquely to a linear mapping L_A from F_q^n to F_q^m given by

$$L_A x = Ax, \qquad \forall x \in F_q^n \tag{3.1}$$

In addition, A^t, the transposed matrix of A, corresponds uniquely to a linear mapping L_{A^t} from F_q^m to F_q^n given by

$$L_{A^T}(y) = A^T y = (y^T A)^T, \qquad \forall y \in F_q^m \tag{3.2}$$

Conversely, let L_A be a linear mapping from F_q^n to F_q^m, then there must exist an unique matrix $A \in M_{m\times n}$ such that (3.1) holds for every F_q^n.

Definition 3.1.1. Wu & Dawson (1998a) Let $V \subset F_q^n$, $x = (x_1, x_2, ...x_n)$ and $y = y_1, y_2, ...y_n$ be two vectors of F_q^n. Then

$$< x, y >= x^T y = y^T x = \sum_{i=1}^{n} x_i y_i \qquad (mod p)$$

is called the inner product of x and y and $V^\perp = y \in F_q^n :< x, y >= 0$ holds for every $x \in V$ is called the orthogonal vector space of V.

Definition 3.1.2. Wu & Dawson (1998a) Let V be a vector subspace of F_q^n. Then F_q^n is said to be able to be decomposed into the direct orthogonal sum of V, denoted

$$F_q^n = V \oplus V^\perp$$

if for any $x \in F_q^n$, there exists a unique $x_1 \in V$ and a unique $x_2 \in V^{\perp}$ such that $x = x_1 + x_2$. In this case $V^{\perp}$ is called the orthogonal complement of V.

3.2 Existence of Generalized Inverses over Finite Fields

Lemma 3.2.1. *(Wu & Dawson, 1998a, Lemma 1) For any matrix A over an arbitrary field, there exist a $A\{1,2\}$ inverse.*

Over the real number field there always exists a Moore-Penrose inverse for an arbitrary matrix. However this is not the case over finite fields. For example the matrix $A = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ *over the binary field has only four {1,2}-inverses,* $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$. *Only* $B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ *satisfies that AB is symmetric and none satisfies that BA is symmetric as well.*

Lemma 3.2.2. *(Wu & Dawson, 1998a, Lemma 2) Let V be a vector subspace of F_q^n. Then F_q^n can be decomposed into the orthogonal direct sum of V if and only if $V \cap V^{\perp} = 0$.*

Lemma 3.2.3. *(Wu & Dawson, 1998a, Lemma 3) Let $A \in M_{m\times n}$, $A^{(1,2)}$ be {1,2}-inverse of A. Then we have*

$$Ker(A^{(1,2)}A) = Ker(A)$$

$$Im(AA^{(1,2)}) = Im(A)$$

$$rank(A) = rank(A^{(1,2)}) = rank(A^{(1,2)}A) = rank(AA^{(1,2)})$$

Lemma 3.2.4. *(Wu & Dawson, 1998a, Lemma 4) Let $A \in M_{n\times n}$. Then A is symmetric, i.e, $A^T = A$, if and only if for any $x, y \in F_q^n$ we have*

$$< Ax, y > = < x, Ay >$$

Lemma 3.2.5. *(Wu & Dawson, 1998a, Lemma 5) Let $A \in M_{n\times n}$ and $A^2 = A$. Then A is symmnetric if and only if*

$$(Ker(A))^{\perp} = Im(A)$$

Proof. Necessity: For $x \in Im(A)$ and $y \in Ker(A)$, since A is symmetric, by Lemma 3.2.4 we have

$$< Ax, y >=< x, Ay >=< x, 0 >= 0$$

Thus $Im(A) \subset (Ker(A))^{\perp}$. But $dim(Ker(A)) + dim(Im(A)) = n$, so $(Ker(A))^{\perp} = Im(A)$.

Sufficiency : Suppose we have $A^2 = A$ and $(Ker(A))^{\perp} = Im(A)$. Let $x_1, x_2 \in F_q^n$. Then they can be written as

$$x_1 = Ax_1 + (I_n - A)x_1 \qquad x_2 = Ax_2 + (I_n - A)x_2$$

Note that $(I_n - A)x_i \in Ker(A) = (Im(A))^{\perp}$, $i = 1, 2..$ We then have

$$< Ax_1, x_2 >=< Ax_1, Ax_2 + (I_n - A)x_2 >=< Ax_1, Ax_2 >$$

In the same way it can be shown that $< x_1, Ax_2 >=< Ax_1, Ax_2 >$. So A is symmetric. □

Theorem 3.2.6. *(Wu & Dawson, 1998a, Theorem 1) Let $A \in M_{m \times n}$. Then a necessary and sufficient condition for the existence of a A{1,2}-inverse A_r of A which satisfies $(A_r A)^T = (A_r A)$ is that F_q^n has the following orthogonal direct sum decomposition :*

$$F_q^n = Ker(A) \oplus (Ker(A))^{\perp} \tag{3.3}$$

Proof. Necessity: Let A_r be a A{1,2}-inverse of A which satisfies $(A_r A)^T = (A_r A)$. Then by Lemma 3.2.5 we have

$$(Ker(A_r A))^{\perp} = Im(A_r A)$$

For any $x \in Ker(A_r A) \cap Im(A_r A)$, since $x \in Im(A_r A)$, there exists $y \in F_q^n$ such that $x = A_r Ay$. Thus we have

$$A_r Ax = A_r A A_r Ay = A_r Ay = x$$

On the other hand, $x \in Ker(A_rA)$ implies that $A_rAx = 0$, i.e, $x = 0$. Therefore $Ker(A_rA) \cap Im(A_rA) = 0$ and hence $F_q^n = Ker(A_rA) + Im(A_rA) = Ker(A_rA) + Ker(A_rA)^{\perp}$. By Lemma 3.2.3, we have (3.3).

Sufficiency: Assume the validity of (3.3). Denote by $M = (Ker(A))^{\perp}$ and $N = Ker(A)$. Then we can write

$$S = \{Ax : x \in F_q^n\} = \{Ax : x \in M\}$$

For any $y \in S$, there must exist an $x \in M$ such that $y = Ax$. Moreover the existence of x is unique, as otherwise we would have $Ax_1 = Ax_2$ for some $x_1, x_2 \in M$ and $x_1 - x_2 \in Ker(A) \cap Ker(A)^{\perp}$. This leads to a contradiction of Lemma 3.2.2. Since S is a vector subspace of F_2^m, we denote by T its complement (not necessary orthogonal) subspace, and any $y \in F_2^m$ can be written as $y_1 + y_2$, where $y_1 \in S$ and $y_2 \in T$. Now define a mapping L_B from F_2^m to F_2^n as follows: for an arbitrary $y = y_1 + y_2 \in F_2^m$, where $y_1 = Ax \in S$ with $x \in M$ and $y_2 \in T$, $L_B(y) = x$. The linearity of L_B is as follows : Let $y = y_1 + y_2$ and $z = z_1 + z_2$ be two arbitrary vectors of F_2^m, where $y_1 = Ax_1$,$z_1 = Ax_2$, $y_2, z_2 \in T$. By definition we have $L_B(y+z) = x_1 + x_2 = L_B(y) + L_B(z)$. Thus L_B corresponds uniquely to a matrix $B \in M_{n\times m}$ such that for every $y = y_1 + y_2 \in F_q^m$, $By = x$ for some $X \in M$ such that $y_1 = Ax$. For any $x \in F_q^n$ this can be written as $x = x_M + X_N$, where $x_M \in M$ and $x_N \in MN$.

$$ABAx = ABAx_M = Ax_M = Ax$$

Thus we get $ABA = A$. For any $y = y_1 + y_2 \in F_q^m$, where $y_1 = Ax \in S$ and $y_2 \in T$, we have $BABy = BAx = x = BY$. This shows that B is a {1,2}-inverse of A. By the initial assumption and $Ker(A) = Ker(BA)$ from Lemma 3.2.3 we have

$$F_q^n = Ker(BA) \oplus (Ker(BA))^{\perp} = Ker(BA) \oplus Im(BA)$$

Notice that $(BA)^2 = BA$: by Lemma 3.2.5 we have $(BA)^T = BA$. □

Theorem 3.2.7. *(Wu & Dawson, 1998a, Theorem 2) Let $A \in M_{m\times n}$. Then a necessary*

and sufficient condition for the existence of a A{1,2}-inverse A_r of A which satisfies $(A_rA)^T = (A_rA)$ is that for any $x \in F_q^m$, $A^Tx = 0$ if and only if $AA^Tx = 0$.

Proof. By Theorem 1, a necessary and sufficient condition for the existence of a A{1,2}-inverse A_r of A which satisfies $(A_rA)^T = (A_rA)$ is

$$F_q^n = Ker(A) \oplus (Ker(A))^{\perp}$$

It is known that this decomposition is equivalent to

$$rank(A) = rank(AA^T).$$

and the conclusion follows. □

Theorem 3.2.8. *(Wu & Dawson, 1998a, Theorem 3) Let $A \in M_{m\times n}$. Then a necessary and sufficient condition for the existence of a A{1,2}-inverse A_r of A which satisfies $(AA_r)^T = (AA_r)$ is that F_q^m has the following orthogonal direct sum decomposition :*

$$F_q^m = Im(A) \oplus (Im(A))^{\perp} \tag{3.4}$$

Proof. Necessity : Let A_r be a A{1,2}-inverse of A which satisfies $(AA_r)^T = (AA_r)$. Notice that the matrix A is a {1,2}-inverse of A_r satisfying $(A_rA)^T = (A_rA)$. By Theorem 3.2.6 we have

$$F_q^m = Ker(A_r) \oplus (Ker(A_r))^{\perp}$$

For any $y \in Ker(A_r)$ and $Ax \in Im(A)$, since $(AA_r)^T = AA_r$ we have

$$< Ax, y >=< AA_rAx, y >=< Ax, AA_ry >=< Ax, 0 >= 0$$

Thus $Ker(A_r) \cap (Im(A))^{\perp}$. $dim(Ker(A_r)) + dim(Im(A)) = m$. This supplies that $Ker(A_r) = Im(A)^{\perp}$ So we have (3.4).

Sufficiency: Assume the validity of (3.4). Denote by $S = Im(A)$ and $T = (Im(A)^{\perp})$. Any $y \in F_q^m$ can uniquely be written as $y = y_S + y_T$, where $y_S \in S$ and $y_T \in T$. Now

define a mapping L_B from F_q^m to F_q^n which satisfies $L_B(y_S + y_T) = x$ where $y_S = Ax \in S$. Similar to the proof of Theorem 1 it can be proven that L_B is a linear mapping corresponding uniquely to a matrix $B \in M_{n\times m}$. Moreover B is a {1,2}-inverse of A and $Im(AB) = \{ABy : y \in F_q^m\} = \{ABy : y \in S\}$. For any $y \in T$ we have $By = 0$, so $y \in Ker(B)$. But $dim(T) = dim(Ker(B))$. $T = Ker(B = Ker(AB))$ and by Lemma 3.2.3 we have $Ker(AB) = (Im(AB))^T$. By Lemma 3.2.5 and $(AB)^2 = AB$ we have $(AB)^T = AB$. □

Theorem 3.2.9. *(Wu & Dawson, 1998a, Theorem 4) Let $A \in M_{m\times n}$. Then a necessary and sufficient condition for the existence of a A{1,2}-inverse A_r of A which satisfies $(AA_r)^T = (AA_r)$ is that for any $y \in F_q^n$, $Ay = 0$ if and only if $A^T Ay = 0$.*

Proof. Similar to the proof of Theorem 3.2.7. □

Theorem 3.2.10. *(Wu & Dawson, 1998a, Theorem 5) Let $A \in M_{m\times n}$. Then a necessary and sufficient condition for the existence of a Moore-Penrose inverse of A is that both equaitons (3.3) and (3.4) holds simultaneously.*

Proof. Necessity is obvious from Theorems 3.2.6 and 3.2.8. The sufficiency is as follows. Denote by $M = (Ker(A))^\perp$, $N = Ker(A)$, $S = Im(A)$, $T = Im(A)^\perp$. Then $\{Ax : x \in F_q^n\} = \{Ax : x \in M\}$. Define a mapping $L^B : F_q^m \to F_q^n$ such that for any $y = y_S + y_T$, where $y_S = Ax \in S$ and $y_T \in T$, $L_B(y) = x$. Then L^B is linear corresponding to a matrix $B \in M_{n\times m}$. The constructed matrix B is a Moore-Penrose inverse of A. □

Corollary 3.2.11. *(Wu & Dawson, 1998a, Corollary 1) Let $A \in M_{m\times n}$. We have,*

1. *A necessary and sufficient condition for the existence of a A{1,2}-inverse A_r of A satisfying $(A_rA)^T = (A_rA)$ is that $rank(A) = rank(AA^T)$.*
2. *A necessary and sufficient condition for the existence of a A{1,2}-inverse A_r of A satisfying $(AA_r)^T = (AA_r)$ is that $rank(A) = rank(A^TA)$.*
3. *A necessary and sufficient condition for the existence of a Moore-Penrose inverse of A is that $rank(A) = rank(AA^T) = rank(A^TA)$.*

CHAPTER FOUR
ERROR CORRECTING CODES

4.1 Introduction

When transferring or storing information there is always a risk of errors occuring in the process. To increase the possibility of detecting and possibly correcting such errors, one can add a certain redundance to the text carrying the information, for example, in form of control digits. We shall now give two simple examples.

Example 4.1.1. Andersson (2015) Assume that a sender transmits a text which is divided into a number of six digit binary words. Each such word consists of six digits which each is either 0 or 1. To increase the possibility for a receiver to detect possible errors, that might have occured during a transfer, to each word the sender can add the seventh binary digit in a such way that in each seven digit word there always is an even number of ones. If the receiver registers a word with an odd number of ones, then he will know that an error has occured and can possibly ask the sender to repeat the message.

Example 4.1.2. Andersson (2015) If the receiver in Example 4.1.1 does not have the oppurtunity to ask for a repetition, the sender can proceed in a different way. Instead of adding the seventh digit he can send every six digit word three times in a row. If the three words are not identical when they reach the receiver, he will know that an error has occured and could try to correct it at each place by choosing a digit that occurs at the corresponding places in at least two of the received words. He can of course not be completely sure that the erroneous word has been corrected, but if the probability for more than one error to occur is low, then the chances are good.

One disadvantage of the method in Example 4.1.2 is that, compared with the original text, the message with the error-correcting mechanism takes three times as long to send. Hence it seems a worthwhile exercise to find more effective methods and this is the purpose of the theory of error-correcting codes. This was started off by the work of Shannon, Golay and Hamming at the end of the 1940s and has since evolved

rapidly using ever more sophisticated mathematical methods. Here the theory of finite fields plays a particularly important role.

For writing a text we must have an alphabet. This is a finie set F of symbols called letters. As is common in coding theory, we assume that F is a finite field. When $F = \mathbb{Z}_2$, as in the above examples, the code is said to be binary. A word is a finite sequence $x_1x_2...x_m$ of letters. We shall here only deal with so called block codes. This means that the words are all of the same length m and can therefore be seen as elements in the vector space F^m. When appropriate, we write the words as vectors $x = (x_1, x_2, ...x_m)$ in F^m. A coding function E is an injective map

$$E : F^m \to F^n$$

from F^m into a vector space F^n of higher dimension i.e $m < n$. The image $C = E(F^m)$ is what we call a code. To improve the possibility for detecting and correcting errors, it is useful that the elements of the code C lie far apart from each other in F^n. This is to minimize the probability that a sent codeword is received erroneously as a different codeword.

Definition 4.1.3. Andersson (2015) The Hamming Distance $d(x,y)$ between two vectors $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_n)$ in F^n is defined as the number of coordinates i where $x_i \neq y_i$.

Example 4.1.4. Andersson (2015) In the space $\mathbb{Z}_2^5$ the Hamming distance satisfies $d(10111, 11001) = 3$ and in $\mathbb{Z}_3^4$ we have $d(1122, 1220) = 2$.

Definition 4.1.5. Andersson (2015) Let C be a code in F^n. Then we define its separation $d(C)$ as the least distance between two different words in the code i.e.

$$d(C) = min\{d(x,y); x,y \in C, x \neq y\}$$

Theorem 4.1.6. *Andersson (2015) Let C be a code with separation $d(C)$.*
(1) If $d(C) \geq k+1$ then C can detect up to k errors in each word.
(2) If $d(C) \geq 2k+1$ then C can correct up to k errors in each word.

Remark 4.1.7. The consequence of (2) is that if $d(C) \geq 2k+1$ then, for each word containing at most k errors, there exists a uniquely determined closest codeword. We assume that the erroneous word is corrected by picking instead the closest word in the code. For practical purposes, it is of great importance to find effective algorithms correcting errors and the existence of such algorithms can be a strong argument for the choice of a particular code. In the following we will focus on how to construct codes with high separation and not on error-correcting algorithms.

Proof. (1) If $d(C) \geq k+1$, then any two codewords are different at least $k+1$ places. A received word with at most k letters wrong cannot be a codeword and is therefore detected as erroneous.

To prove (2) we assume that x is a received word different from a codeword y at most k places. If z was another codeword with this property then the triangular inequality gives $d(y,z) \leq d(y,x) + d(x,z) \leq 2k$. This contradicts the assumption that $d(C) \geq 2k+1$. This means that we can correct x to y.

□

If we are interested in constructing a code $C = E(F^m)$ in F^n with a given separation $\sigma = d(C)$, then there is a natural limit for which m we can choose. We shall now give a theoretical estimate of the largest possible value of m.

Definition 4.1.8. Andersson (2015) For every non-negative integer r we define the sphere $S(x,r)$, witch centre $x \in F^n$ and radius r, by

$$S(x,r) = \{y \in F^n; d(x,y) \leq r\}$$

Lemma 4.1.9. *Andersson (2015) If F has q elements then the sphere $S(x,r)$ contains exactly*

$$\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + ... + \binom{n}{r}(q-1)^r$$

words.

Proof. The result follows from the fact that if $0 \leq j \leq r$, then there exists $\binom{n}{j}(q-1)^j$ words which have exactly j coordinates different from x.

□

Theorem 4.1.10. *Andersson (2015) Assume that F has q elements, that the code C in F^n contains M words and has separation $2k+1$. Then*

$$M\left[\binom{n}{0}+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\ldots+\binom{n}{K}(q-1)^K\right] \leq q^n \tag{4.1}$$

Proof. The spheres of radius k and centre in different codewords in C cannot intersect, since $d(C) = 2k+1$. Because the number of elements in F^n is q^n, the result then follows from Lemma 4.1.9.

□

Remark 4.1.11. If $C = E(F^m)$ then $M = q^m$.

Remark 4.1.12. The inequality (4.1) is called the sphere packing bound or the Hamming bound. In case of equality, the corresponding code C is said to be perfect. For such a code, every word y in F^n lies in exactly one sphere $S(x,k)$ with x in C.

4.2 Linear Codes and Generating Matrices

Definition 4.2.1. Andersson (2015) A code C in F^n is said to be linear if it is a linear subspace of F^n. If the dimension of C is m then it is called an $[n,m]$ code.

Remark 4.2.2. That C is a linear subspace of F^n means that every linear combination of vectors in C is also contained in C. Then C is itself a vector space with the same operations as F^n, so the dimension of C is well-defined.

In practice, most error-correcting codes are linear or can be obtained from linear ones. A great advantage of linear codes is that it is much easier to determine their separation than in general case.

Remark 4.2.3. By the weight $w(x)$ of a codeword $x = (x_{1,\ldots,x_n})$ in F^n we mean the number of coordinates in x that are different from zero. The weight $w(C)$ of a linear code C in F^n is defined by

$$w(C) = min\{w(x); x \in C, x \neq 0\}$$

Theorem 4.2.4. *Andersson (2015) For a linear code C the separation $d(C)$ is equal to its weight $w(C)$.*

Proof. A linear code that contains the two words x and y also contains their difference $x - y$. The result follows from the fact that the Hamming distance $d(x,y)$ is equal to the weight $w(x-y)$. □

Remark 4.2.5. If we are interested in determining the separation for a general code containing M words, then we must, in principle, determine $M(M-1)/2$ different Hamming distances, one of each pair in the code. For a linear code, it is enough to calculate the weight of the $M-1$ non-zero codewords.

Definition 4.2.6. Andersson (2015) A generator matrix for a linear $[n,m]$ code C in F^n is a $m \times n$ matrix G, with elements in F, such that its rows form a basis for C.

Example 4.2.7. Andersson (2015) Consider the following 3×7 matrix with elements in $F = \mathbb{Z}_3$

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 2 & 1 & 1 & 2 \\ 2 & 1 & 2 & 1 & 2 & 1 & 2 \end{pmatrix}$$

Buy substracting the first row from the second and adding the first to the third, we obtain the matrix,

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

Multiplying the third row by 2 gives

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

Finally, subtracting both the second and the third row from the first yields

$$\grave{G} = \begin{pmatrix} 1 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

The rows of $\grave{G}$ generate the same subspace of F^7 as the rows of G, because we can write the rows in one matrix as a linear combination of the rows of the other. The two matrices G and $\grave{G}$ are therefore generator matrices for the same code C in F^7. We now observe that the first three columns of $\grave{G}$ are columns in the identity matrix of order 3. If we interchange the second and the third columns of $\grave{G}$ we get

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

This matrix generates a code C' in F^7 that is obtained from C by interchanging the letters in position 2 and 3 for all words in C.

Definition 4.2.8. Andersson (2015) Two codes C and C' in F^n are said to be equivalent if there exists a permutation π of the numbers $1,...,n$ such that

$$C' = \{x_{\pi(1)}x_{\pi(2)}...x_{\pi(n)}; x_1x_2...x_n \in C\}$$

Remark 4.2.9. If two codes C and C' are equivalent then their separations are equal i.e. $d(C) = d(C')$.

Theorem 4.2.10. *Andersson (2015) Every linear $[n,m]$ code C is equivalent to a code*

with generator matrix of the form

$$[I_m|A]$$

where I_m is the identity matrix of order m and A is an $m \times (n-m)$ matrix.

Definition 4.2.11. Andersson (2015) When a generator matrix for a linear code takes the form as in Theorem 4.2.10 we say that it is of normal form.

Let $G = (I_m|A)$ be the generator matrix, of a linear $[n,m]$ code C in F^n, of normal form. If the elements in F^m and F^n are seen as row matrices, then the map

$$F^m \ni x \to xG \in F^n$$

gives a natural linear coding function. The first m letters in the word xG are given by x in K^m and the last $n-m$ letters (control digits) by xA.

4.3 Control Matrices and Decoding

Definition 4.3.1. Andersson (2015) The scalar product $< x,y >$ of two vectors $x = (x_1,...x_n)$ and $y = (y_1,...,y_n)$ in F^n is defined by

$$< x,y >= x_1y_1 + ... + x_ny_n$$

Definition 4.3.2. Andersson (2015) The dual code $C^\perp$ of a linear code C in F^n is a linear code

$$C^\perp = \{y \in F^n; < x,y >= 0\, for all\, x \in C\}$$

Remark 4.3.3. As for subspaces in R^n, it is easy to show that if the code C in F^n has dimension m, then the dual code $C^\perp$ is of dimension $n-m$. For vector spaces F^n over a finite field F, it is not true in general that every vector in F^n can, in a unique way, be written as the sum of a vector in C and a vector in $C^\perp$ It can even happen that $C^\perp = C$. In that case the code is said to be self-dual.

Example 4.3.4. Andersson (2015) For the matrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

the scalar product of the first row with itself is 3, the scalar product of the second row with itself is 6, and the scalar product of the two rows is 3. This means that each scalar product is 0 modulo 3. From this we see that the $[4,2]$ code over $\mathbb{Z}_3$ with generator matrix G is self dual.

Definition 4.3.5. Andersson (2015) A generator matrix for the dual code $C^{\perp}$ of C is called a control matrix for C.

A word $x \in F^n$ is contained in the code C if and only if the scalar product of x and any row of a control matrix C is zero. In this way we can easily check if a word belongs to the code or not.

If G is a generator matrix for an $[n,m]$ code C and H is a control matrix for C, then G is an $m \times n$ matrix and H is an $(n-m) \times n$ matrix of rank $(n-m)$. The condition that H is a control matrix for C can be written as

$$G.H^t = 0 \tag{4.2}$$

where H^t denotes the transpose of the matrix H. The content of equation (4.2) is namely that the scalar product of the rows of G and the rows of H are zero.

Let us now assume that the generator matrix G is of normal form $[I_m|A]$, where A is an $m \times (n-m)$ matrix. If we then choose

$$H = [-A^t|I_{n-m}]$$

then it is easily verified that condition (4.2) is satisfied. We now formulate this as the following theorem.

Theorem 4.3.6. *Andersson (2015) If a linear $[n,m]$ code C has the generator matrix*

$[I_m|A]$, *then* $[-A^t|I_{n-m}]$ *is a control matrix for* C.

Remark 4.3.7. If the field F is $\mathbb{Z}_2$, then $-A^t = A^t$ so we can take $[A^t|I_{n-m}]$ as a control matrix.

Example 4.3.8. Andersson (2015) The binary $[5,2]$ code which has the generator matrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

has as control matrix

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

The following theorem tells us how to determine the separation of a code from its control matrix.

Theorem 4.3.9. *Andersson (2015) A linear code* C *with the control matrix* H *has separation* σ *if and only if there exists* σ *columns in* H *that are linearly dependent and furthermore any* $\sigma - 1$ *of the columns in* H *are linearly independent.*

Proof. That σ columns in H are linearly dependent means that there exists a word x of weight at most σ such that $xH^t = 0$. The weight of such a word can never be less than σ, since $\sigma - 1$ columns in H are always linearly independent. Hence $w(C) = \sigma$ and the result follows from Theorem 4.2.4. □

CHAPTER FIVE
LEAST SQUARES SOLUTIONS IN LINEAR CODES

Lemma 5.0.10. *Let A be a square matrix of order n over a finite field $\mathbb{K}$ such that $A^2 = A$. Then A is symmetric if and only if*

$$\mathbb{K}^n = R(A) \oplus (R(A)))^{\perp}.$$

Proof. Since $A^2 = A$, then A is with index 1. Then we have the direct sum decomposition as follows

$$\mathbb{K}^n = R(A) \oplus N(A).$$

If A is symmetric, then, $N(A) = N(A^t) = (R(A))^{\perp}$. Therefore, we get the desired result.

Conversely, let $A^2 = A$ such that $N(A) = (R(A))^{\perp}$. Since $A^2 = A$, we have $N(A) = R(I_n - A)$. Therefore, $\forall x, y \in \mathbb{K}^n$ we have the following decompositions

$$x = Ax + (I_n - A)x,\ y = Ay + (I_n - A)y.$$

Now,

$$\langle Ax, y\rangle = \langle Ax, Ay + (I_n - A)y\rangle = \langle Ax, Ay\rangle + \langle Ax, (I_n - A)y\rangle = \langle Ax, Ay\rangle + 0 = \langle Ax, Ay\rangle.$$

Similarly we have $\langle x, Ay\rangle = \langle Ax, Ay\rangle$. Consequently, $\langle Ax, y\rangle = \langle x, Ay\rangle$. By Lemma 3.2.4, A is symmetric. □

From Zekraoui (2011) we have the following useful Lemma.

Lemma 5.0.11. *Let A be a $m \times n$ matrix over an arbitrary field $\mathbb{K}$ and let X be a $\{1,2\}$-inverse of A. Then we have*
1) $(AX)^2 = AX$ and $(XA)^2 = XA$,
2) $R(AX) = R(A), N(AX) = N(X)$,

3) $\mathbb{K}^n = R(X) \oplus N(A)$,

4) $\mathbb{K}^m = R(A) \oplus N(X)$.

The existence of the $\{1,2\}-$inverses of a matrix over a finite field is proved in Pearl (1968), Fulton (1978).

From Lemma 5.0.10 and 5.0.11, we can deduce the following corollary.

Corollary 5.0.12. *Let A be a $m \times n$ matrix over a finite field $\mathbb{K}$. Then $A^{\{1,2,3\}}$ exists if and only if $\mathbb{K}^m = R(A) \oplus (R(A))^{\perp}$.*

Proof. Suppose that $A^{\{1,2,3\}}$ exists. Then, from Lemma 5.0.11 we have

$$\mathbb{K}^m = R\left(AA^{\{1,2,3\}}\right) \oplus N\left(AA^{\{1,2,3\}}\right).$$

From Lemma 5.0.10 we have $\mathbb{K}^m = R\left(AA^{\{1,2,3\}}\right) \overset{\perp}{\oplus} (R\left(AA^{\{1,2,3\}}\right))^{\perp}$. From 2) of Lemma 5.0.11 we have $R\left(AA^{\{1,2,3\}}\right) = R(A)$. Then we get the desired result.

Let $\mathbb{K}^m = R(A) \overset{\perp}{\oplus} (R(A))^{\perp}$. From Pearl (1968), if X is a $\{1,2\}$- inverse of A such that $N(X) = (R(A))^{\perp}$, then from Lemma 5.0.11 we have

$$\mathbb{K}^m = R(A) \oplus N(X) = R(AX) \overset{\perp}{\oplus} (R(AX))^{\perp}.$$

Since $(AX)^2 = AX$, by Lemma 5.0.10, AX is symmetric. Consequently X is a $\{1,2,3\}$-inverse of A. □

In Section 2, the results about the least squares solutions were given. In Corollary 2.2.3, It has been showed that the general solutions of $Ax = b$ are given by

$$x = A^{\{1\}}b + \left(I - A^{\{1\}}A\right)y, y \in \mathbb{C}^n.$$

Also, in Corollary 2.3.2, it has been shown that r is minimized if and only

if $x = A^{\{1,3\}}b$ for any $\{1,3\}$- inverses of A. Consequently, there is a one-to-one correspondence between the least squares solutions of the equation $Ax = b$ and the $\{1,3\}$- inverses of A. It will be noted that if A is of full column rank, then the least squares solution is unique. In fact, $A^{\{1,3\}}$ is one of the left inverses of A. So, $I - A^{\{1,3\}}A = 0$, and $\left(A^{\{1,3\}}A\right)^* = I^* = I$ and $r\left(A^{\{1,3\}}\right) = r(A)$. Hence $A^{\{1,3\}}$ becomes $A^{\{1,2,3,4\}} = A^+$ (see Zekraoui (2011) , Lemme 1.5.1, page 23). Then, $x = A^+b$.

5.1 Matter of Conditioning in Linear Codes

Let G be a generator matrix of a $[n,k]$-code C over a finite field $\mathbb{K}$ and let H be a parity check matrix. Then we have $G \in M_{k\times n}(\mathbb{K}), r(G) = k$. So G^t is of full column rank and the $[n,n-k]$-code is the $C^\perp$ orthogonal of C according to the standard inner product. However, the orthogonality over a finite field is not necessary the complement.

In linear codes, G^t is a $n \times k$ matrix of rank k, i.e. G^t is of column rank, so if $(G^t)^{\{1,3\}}$ exists, then it is a left inverse of G^t. So, it is $(G^t)^+$of G^t. Therefore we have

$$\mathbb{K}^n = R(G^t) \oplus N\left(\left(G^t\right)^+\right), \tag{5.1}$$

or equivalently $r(G) = r(GG^t) = r(G^tG)$ (See Wu & Dawson (1998a)). Since $R(G^t) = C$, then $N\left((G^t)^+\right)$ is the orthogonal code $C^\perp = R(H^t)$.

Equation 5.1 becomes

$$\mathbb{K}^n = R(G^t) \overset{\perp}{\oplus} R\left(H^t\right). \tag{5.2}$$

Equation 5.2 gives us that for $b \in \mathbb{K}^n$,

$$b = (G^t)\left((G^t)\right)^+ b \tag{5.3}$$

Now, for a message $x \in \mathbb{K}^k$, we have $G^t x = b \in C$. If a received message is not in C,

it means $b \notin R(G^t)$. Then the equality $G^t x = b$ is inconsistent, so it will be desirable to find the codeword the nearest to b. Then, from Equation 5.3, we have

$$b - G^t x = \left((G^t) \left((G^t) \right)^+ b - G^t x \right) + H^t b'. \tag{5.4}$$

Since we have the orthogonal direct sum decomposition, Equation 5.4 gives the following

$$w_H \left(b - G^t x \right) = w_H \left((G^t) \left((G^t) \right)^+ b - G^t x \right) + w_H \left(H^t b' \right) \geq d + w_H \left(H^t b' \right), \tag{5.5}$$

where $w_H(.)$ and d are the weight and the minimal Hamming distance respectively. The minimizing of $b - G^t x$ for d in Equation 5.5 is equivalent that x is a solution of the consistent equation

$$G^t x = (G^t) \left((G^t) \right)^+ b = \left(G^+ G \right) b. \tag{5.6}$$

i.e., $w_H \left((G^t) \left((G^t) \right)^+ b - G^t x \right) = 0$. Then $x = \left((G^t) \right)^+ b$ is the unique least squares solution of $G^t x = b$. We should note that when Equation 5.2 is satisfied, the code and its dual are complementary or equivalently $r(G) = r(GG^t) = r(G^t G)$.

In this case, a received word will be decode correctly to a word of the code. Hence we reach our main result.

Theorem 5.1.1. *Let G be a generator matrix of an $[n,k]-$linear code C over a finite field $\mathbb{K}$. Then, there is the unique word $x \in \mathbb{K}^k$ approaching a received word b near the codewords of C if and only if Equation 5.2 (or equivalently $r(G) = r(G^t G) = r(GG^t)$) is satisfied. In this case, we have $x = \left((G^+) \right)^t b$.*

It will be noted that $G^+ = G^t \left(GG^t \right)^{-1}$. So the calculation of the Moore-Penrose inverse of a matrix of full rank is not required and is not expensive.

The following example clarify the relation between the existence of the Moore-Penrose inverse and the existence of the least squares solution, and hence it gives the possibility of decoding of a received word to a word of the code correctly.

Example 5.1.2. Let $G = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 1 & 0 \end{pmatrix}$ over $\mathbb{F}_3$, then the $[3,2]$-code C is

$$\{(0,0,0),(1,2,0),(1,1,0),(2,1,0)(2,2,0),(2,0,0),(0,2,0),(0,1,0),(1,0,0)\}.$$

Let $b = (1,1,1)$. Then $b \notin C$ means that equality $G^t x = b$ is inconsistent. On the other hand we have, $G^t G = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $r(G) = 2 = r(G^t G)$. Then there exists the unique $x = (G^+)^t b = \begin{pmatrix} 2 & 1 & 0 \\ 2 & 2 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = (0,1)$ such that $b - G^t x = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = r$ and $W_H(r) = 1$ minimum distance. Consequently the received word b will be decoded correctly to $G^t x = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$.

The following example shows that if the Moore-Penrose inverse does not exist, then the least squares solution is not unique when it still exists. In other words, a received word b will not be decoded to a word of the code correctly.

Example 5.1.3. Let $G = \begin{pmatrix} 1 & 2 & 1 \end{pmatrix}$ over $\mathbb{F}_3$, then the $[3,1]$-code C is

$$C = \{(0,0,0),(1,2,1),(2,1,2)\}.$$

Now, if we take $b = (0,1,1)$, then $b \notin R(G) = C$, so the equality $G^t x = b$ is inconsistent. There are two words of the code $c_1 = (1,2,1)$ and $c_2 = (2,1,2)$ such that $W_H(b - c_1) = W_H(b - c_2) = 2 \leq 3 = d$ (i.e. $b - c_1$ and $b - c_2$ are with minimum distance), so the word b will be decoded to $c_1$or to c_2. Now if we look for the conditions of the existence of the least squares solutions and the existence the Moore-Penrose inverse of G, we find that $r(G) = 1 = r(G^t G) = r \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 2 \\ 1 & 2 & 1 \end{pmatrix} \neq 0 = r(GG^t)$. That is, the least squares solution exists but not unique.

CHAPTER SIX
CONCLUSION

In real and complex case the Moore-Penrose inverse exists and unique but in finite fields we need extra conditions.

In finite fields, a necessary and sufficient condition for the existence of a Moore-Penrose inverse of a matrix G is that $rank(G) = rank(GG^T) = rank(G^TG)$.

Suppose that G is a generator matrix of a [n,k]-linear code C over a finite field $\mathbb{K}$. When the condition above holds, we can find a unique codeword approaching a received word, near the codewords of the code C.

If the Moore-Penrose inverse over a finite field does not exist, then the least squares solution is not unique i.e a received word will not be decoded to a word of the code correctly.

REFERENCES

Andersson, K. G. (2015). *Finite fields and error-correcting codes*. Retrieved December 10, 2015, from http://www.matematik.lu.se/matematiklu/personal/sigma/andersson.pdf.

Ben-Israel, A., & Greville, T. (2003). *Generalized inverses: Theory and applications*. Springer: CMS Books in Mathematics.

Bjerhammar, A. (1951). Application of calculus of matrices to method of least squares with special reference to geodetic calculations. *Transactions of the Royal Institute of Technology Stockholm, 49*, 86.

Bjerhammar, A. (1958). *A generalized matrix algebra*. Bulletin from the Division of Geodesy: Institutionen for Geodesi. Lindstahl.

Campbell, S. L., & Meyer, C. D. (2009). *Generalized inverses of linear transformations*. Classics in Applied Mathematics. Philadelphia: Society forIndustrial and Applied Mathematics.

Fredholm, I. (1903). Sur une classe d'équations fonctionnelles. *Acta Mathematica, 27*(1), 365–390.

Fulton, J. D. (1978). Generalized inverses of matrices over a finite field. *Discrete Mathematics, 21*(1), 23–29.

Hurwitz, W. A. (1912). On the pseudo-resolvent to the kernel of an integral equation. *Transactions of the American Mathematical Society*, *13*(4), 405–418.

Moore, E. H. (1920). On the reciprocal of the general algebraic matrix. *Bulletin of the American Mathematical Society*, *26*, 394–395.

Moore, E. H. (1935). *General Analysis*, vol. 1 of *Memories of the American Philosophical Society*. Philadelphia: American Philosophical Society.

Murray, F. J., & Von Neumann, J. (1936). On rings of operators. *Annals of Mathematics*. *Second Series, 37*(1), 116–229.

Pearl, M. H. (1968). Generalized inverses of matrices with entries taken from anarbitrary field. *Linear Algebra and Applications*, *1*, 571–587.

Penrose, R. (1955). A generalized inverse for matrices. *Mathematical Proceedings of the Cambridge Philosophical Society*, *51*, 406–413.

Urquhart, N. (1968). Computation of generalized inverse matrices which satisfy specified conditions. *SIAM Review*, *10*, 216–218.

Wu, C.-K., & Dawson, E. (1998a). Existence of generalized inverse of linear transformations over finite fields. *Finite Fields and their Applications*, *4*(4), 307–315.

Wu, C. K., & Dawson, E. (1998b). Generalized inverses in public key crypto system design. *IEE-Proceedings-Computers and Digital Techniques*, *145*(1), 321–326.

Zekraoui, H. (2011). *Sur les proprietes algebriques des G^k-inverses des matrices*. Ph.D. Thesis, Universite El Hadj Lakhdar, Batna.