DATA SECURITY: AN APPLICATION OF LINEAR ALGEBRA

Ramasamy Jesuraj

A Thesis

in

The Department

of

Computer Science

Presented in Partial Fulfillment of the Requirements
for the degree of Master of Computer Science at
Concordia University
Montreal, Quebec, Canada

August 1982

ABSTRACT

DATA SECURITY: AN APPLICATION OF LINEAR ALGEBRA

Ramasamy Jesuraj

This thesis investigates the suitability of using involutory matrices over Z_m as cryptographic keys. The exact size of the key space, and the structure of such matrices are obtained. These results are significant in the complexity analysis of a cryptosystem that uses involutory matrices as keys. A proposal is being made to use involutory matrices in a network, both as individual secret keys, and as communication keys between participants. It is shown that the security of communication in such a network rests upon certain properties related to noncommutative involutory matrices over Z_m.

ACKNOWLEDGEMENTS

I gratefully acknowledge the invaluable assistance of my thesis advisor, Professor V. S. Alagar, in all phases of the preparation of this thesis. In particular, I acknowledge his suggestion of the problem, and constant collaboration thereafter. This collaboration took the form of two of us proposing ideas, and constantly discussing and rediscussing them. Nearly all of the results that have been obtained here are the fruits of these discussions. I also acknowledge some financial assistance from Dr. Alagar. I would like to thank Ms. Beverley Abramovitz for her accurate and fast typing of the thesis.

TABLE OF CONTENTS

PAGE

CHAPTER I

Introduction

Data security in general information systems related to both scientific and business applications is one of the most growing concerns of the modern era. An information processing system that collects, stores, shares, processes, and interprets data must assure the confidentiality and privacy of the participants in that system. The power of modern computers is not the root cause of the data security problem, but the widespread demand of computing on a large amount of centralized information, and attractive factors of speed and ever decreasing cost of computing have compounded the problem. The increased use of telecommunication facilities as a mode of operation in modern computer applications is a secondary reason for the increased concern over data security. In fact, most of the business transactions, and any kind of sensitive high-level government transactions have increasingly come to be conducted through electronic systems. The fear that there is a good chance of eavesdropping and forgery, is growing dramatically in such computer controlled electronic communications. One method of preventing eavesdropping and forgery is to transform the message (or data) so that it is made unintelligible to a person who is not authorized to know the message (or data). We call such a transformation an encryption.

This thesis addresses itself to an encryption method to provide private security, not only to send messages in electronic communications, but also to store large volumes of information such as personal data banks, medical data bases in hospitals, and credit records in banks. In general, it seems that encryption is the only method to protect both static and dynamic data. Although the degree of security offered may vary from one encryption method to another, absolute security is not guaranteed by any of the encryption methods. Usually, the encipherment of data is made so complicated, both in storage and during transmission, that it becomes extremely time consuming and uneconomical to reverse the process. Almost all encryption methods have roots, and hence derive tools from mathematics. Hence, the degree of security offered by an encryption method depends highly on the power of the tools employed.

In order to establish that a cryptosystem offers absolute security, it thus becomes essential to prove that the penetration - i.e., reversal of a transformed text by a person who is not legally entitled to know the plain-text - is either impossible or is inherently hard. We use this term hard in the sense of complexity theory. A mathematical problem that is either unsolved or whose solution is computationally intractable is an excellent candidate to develop an encryption method. In this thesis, the encryption method that we discuss is classical (see [3]). However, the results of our investigation relating to complexity analysis,

and hence the basic results on which the analysis is built is new. We also show how this classical conventional encryption method that we study can be adapted with ease, elegance, and power to communicate in networks.

Secure communication in a large network involving a number of participants, depends primarily upon the method used to encrypt the message that is to be communicated between the participants. It is essential that the personal identification keys of the participants, as well as the keys that are used in encrypting the messages in communications are not easy to be determined, either by an exhaustive search of the key space or by a systematic cryptanalysis. There is always a potential possibility of an intruder interposing in communication paths, and hence copying, or altering, or replaying, or falsifying the messages that are passing through those paths. Such a possibility should not be ruled out as an extreme view; for only under such assumptions can a basic encryption method be evaluated satisfactorily.

It has been pointed out by several people, for example, see [2], that a conventional cryptosystem is not that suitable for protecting informations that are transmitted over insecure communication channels in a network. It was also pointed out originally that the requirement of key distribution, and authentication of messages are not easy tasks in a network based on conventional encryption methods. However, Popek and Kline (see [14]) have

commented that a public-key cryptosystem offers no advantage in terms of communication protocols over the conventional encryption methods. Every identifiable task that can be recognized in a network communication can be performed with some ease, either by a conventional or by a public-key cryptosystem. Hence, a choice between a conventional and a public key cryptosystem solely rests on the strength of the security offered.

This thesis is organized as follows: Chapter II contains some basic definitions, and some elementary results that are necessary to develop further materials. We also give some notations that would be used throughout this thesis. A brief account of some conventional, and some public-key cryptosystem methods is given in Chapter III, motivating our encryption method based on involutory matrices over the ring of integers. In Chapters IV and V, we give new results on the structure of involutory matrices, and also on the size of the involutory matrix space. These results provide tools for our analysis. Chapter VI contains a possible cryptanalysis. Finally, in Chapter VII, we show the adaptation of our encryption method to communications in a network. The security of this possible adaptation is also discussed there. Some open problems are mentioned in Chapters V, VI and VII.

CHAPTER II

Notations and Basic Results

We introduce here the notations that we follow in later chapters. Unless otherwise mentioned, they will have the same meaning throughout the thesis. We also give some basic definitions and standard results that would be used later.

Encryption process transforms an intelligible text (known as plain-text) into an unintelligible text (known as cipher-text). Both the plain-text and the cipher-text are composed of elements from a finite set of symbols called an alphabet. Some examples of alphabets are:

(i) all upper case English letters A,B,...,Z.

(ii) all upper and lower case English letters A,B,...,Z,a,b,...,z.

(iii) all upper and lower case English letters augumented with digits and some punctuations.

(iv) the set of all musical notes.

(v) the set of all binary sequences of fixed length, say 6.

000000, 000001,....., 111110, 111111.

An element of an alphabet is called a letter.

An alphabet is always denoted by V. The number of elements in V is denoted by m. Let $V = \{P_0, P_1, \ldots, P_{m-1}\}$. Consider the cartesian product $V \times V = \{(P_i, P_j) : 0 \leq i, j \leq m-1\}$. This can be identified with $V^2 = \{P_i P_j : 0 \leq i, j \leq m-1\}$.

Elements of V^2 are ordered pairs of elements from V. We call elements of V^2 as 2-grams or di-grams. Similarly, we can form $V^3 = \{P_iP_jP_\ell : 0 \leq i,j,\ell \leq m-1\}$ and elements of V^3 are called 3-grams or tri-grams. More generally, for any positive integer n, we can form V^n and elements of V^n are called n-grams. Of course, an 1-gram is an element in V.

Definition 2.1.1

A set R with two operations + and · (usually known as addition and multiplication) is said to be a ring if it satisfies the following set of properties.

(1) (i) $a + b \in R$ for all a,b in R.

(ii) $(a + b) + c = a + (b + c)$ for all a,b,c in R.

(iii) $a + b = b + a$ for all a,b in R.

(iv) There is an element denoted by 0 in R such that $a + 0 = a$ for all a in R.

(v) Given a in R there is an element denoted by $(-a)$ in R such that $a + (-a) = 0$.

(2) (i) $a \cdot b \in R$ for all a,b in R.

(ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a,b,c in R.

(3) (i) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all a,b,c in R.

(ii) $(a + b) \cdot c = a \cdot c + b \cdot c$

Definition 2.1.2

(i) A ring R is said to be a commutative ring if $a \cdot b = b \cdot a$ for all a,b in R.

(ii) A commutative ring is said to have unity if there is an element, denoted by 1, in R such that

$a \cdot 1 = a$ for all a in R.

(iii) An element b in a commutative ring R with unity is said to have a multiplicative inverse if there is an element denoted by b^{-1} in R such that $bb^{-1} = 1$.

Definition 2.1.3

A commutative ring R with unity is called a field if it has the property that every nonzero element in R has a multiplicatiye inverse in R.

Example 1

For a positive integer m, let Z_m denote the integers modulo m, i.e., $Z_m = \{0,1,2,\ldots,(m-1)\}$. The addition operation can be defined as $a + b = a + b \pmod m$. That is, to add a,b in Z_m, first add them as integers and then compute the remainder of (a + b) divided by m.

Example 2

The set of all real numbers with usual addition and multiplication form a field.

Example 3

For any prime p, Z_p is a field.

The set $\{(a_1,a_2,\ldots,a_n): a_i \text{ is in } Z_m,\ 1 \leq i \leq n\}$ of all n-tuples with each of its components in Z_m, is an example of an algebraic system called a vector space of dimension n over a ring. (Sometimes it is called a module over a ring.) We denote this set by $Z_{m,n}$, and an element in $Z_{m,n}$ is called a vector. The vector whose components are all zeros is denoted by 0.

For an n-tuple $(a_1,a_2,\ldots,a_n)$ of integers, we define $(a_1,a_2,\ldots,a_n)\pmod m = (a_1 \pmod m, a_2 \pmod m, \ldots a_n \pmod m)$, a vector in $Z_{m,n}$.

Now, we define <u>addition in $Z_{m,n}$</u>. For any two vectors $u = (u_1,u_2,\ldots,u_n)$ and $v = (v_1,v_2,\ldots,v_n)$ in $Z_{m,n}$, define $u + v = (u_1 + v_1, u_2 + v_2, \ldots, u_n + v_n) \pmod m$ in $Z_{m,n}$. <u>Scalar multiplication</u> is defined as follows: for any a in Z_m, and any $v = (v_1,v_2,\ldots,v_n)$, the scalar multiplication of a and v is $av = (av_1,av_2,\ldots,av_n) \pmod m$ in $Z_{m,n}$. The following results are easy to verify.

<u>Proposition 2.1.4</u>

For any u,v,w in $Z_{m,n}$ and any a,b in Z_m we have:

(i) $u + v = v + u \pmod m$.

(ii) $u + (v + w) = (u + v) + w \pmod m$.

(iii) $(a + b)u = au + bu \pmod m$.

(iv) $a(u + v) = au + av \pmod m$.

A vector v in $Z_{m,n}$ is said to be a <u>linear combination</u> of the set $\{v_i : i=1,2,\ldots,\ell\}$ of vectors in $Z_{m,n}$, if $v = a_1v_1 + a_2v_2 + \ldots + a_\ell v_\ell$ with a_i in Z_m for $i = 1,2,\ldots,\ell$.

A set of vectors $\{v_i : i = 1,2,\ldots,\ell\}$ in $Z_{m,n}$ is said to be <u>linearly independent over Z_m</u> if the following condition holds: $a_1v_1 + \ldots + a_\ell v_\ell = 0 \pmod m$ if and only if $a_i = 0$, for $i = 1,2,\ldots,\ell$.

A set of vectors $\{v_i : i = 1,2,\ldots,\ell\}$ in $Z_{m,n}$ are said to <u>span $Z_{m,n}$</u>, if every vector in $Z_{m,n}$ is a linear combination of vectors $v_1,\ldots,v_\ell$.

A set $\{v_i : i = 1,\ldots,\ell\}$ of vectors in $Z_{m,n}$ is said

to be a <u>basis for $Z_{m,n}$</u> if they are linearly independent over Z_m, and span $Z_{m,n}$.

The following theorem is well known.

<u>Theorem 2.1.5</u>

(i) Every basis of $Z_{m,n}$ contains exactly n vectors.

(ii) Every set of n vectors in $Z_{m,n}$ which are linearly independent over Z_m is a basis for $Z_{m,n}$.

(iii) Every set of (n + 1) vectors in $Z_{m,n}$ is linearly dependent over Z_m.

A mapping $T: Z_{m,n} \to Z_{m,n}$ is said to be <u>linear</u> if $T(au + bv) = aT(u) + bT(v) \pmod m$ for any a,b in Z_m and any u,v in $Z_{m,n}$.

<u>Proposition 2.1.6</u>

(i) Every $n \times n$ matrix over Z_m is a linear mapping from $Z_{m,n} \to Z_{m,n}$.

(ii) Every linear mapping $T: Z_{m,n} \to Z_{m,n}$ can be represented by an $n \times n$ matrix over Z_m.

Due to this fact, we deal mostly with $n \times n$ matrices instead of linear mappings.

The determinant of an $n \times n$ matrix A over $Z_{m,n}$ is defined in the usual manner, i.e., the determinant of A is computed as if it is a matrix over integers and then reduced (mod m). For example, if m = 8, n = 2, and $A = \begin{pmatrix} 4 & 5 \\ 7 & 4 \end{pmatrix}$ then determinant of A is 5.

An $n \times n$ matrix A over Z_m is said to have an <u>inverse</u>

if there exists an $n \times n$ matrix A^{-1} over Z_m such that $AA^{-1} = A^{-1}A = I \pmod{m}$, where I is the $n \times n$ identity matrix over Z_m. In this case we say A is <u>invertible</u> over Z_m.

<u>Theorem 2.1.7</u>

Let A be an $n \times n$ matrix over Z_m. Then, the following are equivalent:

(i) A is invertible.

(ii) The determinant of A is relatively prime to m.

(iii) All column vectors of A are linearly independent over Z_m.

(iv) All the row vectors of A are linearly independent over Z_m.

If A is an $n \times n$ matrix over Z_m, then $\{v \in Z_{m,n} : Av = 0 \bmod m\}$ is called the <u>null space of A</u>. It is obvious that if $Au = 0 \pmod{m}$ and $Av = 0 \pmod{m}$, then $A(au + bv) = 0 \pmod{m}$ for all a, b in Z_m.

The set $\{v \in Z_{m,n}$: there is a u in $Z_{m,n}$ such that $Au = v\}$ is called the <u>image space</u> of A. It is obvious that if u,v are in image space of A, then au + bv is also in the image space of A.

The dimension of the null space of A is known as the <u>nullity of A</u>, and the dimension of the image of A is known as the <u>rank of A</u>. We state the following well known theorem:

<u>Theorem 2.1.8</u>

Let A be an $n \times n$ matrix over Z_m. Then,

(i) nullity of A + rank of A = n,

and (ii) A is invertible iff rank of A = n .

For an $n \times n$ matrix A over Z_m, the determinant of $(A - \lambda I)$ is a polynomial in λ of degree n . It is known as the characteristic polynomial of A . The roots of this polynomial are called the eigen values of A.

Proposition 2.1.9

λ is an eigen value of A if and only if there is a nonzero vector v in $Z_{m,n}$ such that $Av = \lambda v \pmod m$.

Consequently, for every eigen value λ , there is at least one nonzero vector v in $Z_{m,n}$ such that $Av = \lambda v \pmod m$. Such a vector is called an eigen vector of A corresponding to the eigen value of λ . If $E_\lambda = \{v \text{ in } Z_{m,n} : Av = \lambda v \pmod m\}$, then E_λ is the null space of $A - \lambda I$, and is known as the eigen space of A corresponding to the eigen value λ .

Proposition 2.1.10

A is $n \times n$ matrix over Z_p , p is prime. Then,

(i) A has at most n eigen values.

(ii) If $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the n eigen values (not necessarily distinct) then

(a) determinant of $A = \lambda_1 \lambda_2 \ldots \lambda_n \pmod p$

(b) trace of $A = \lambda_1 + \lambda_2 + \ldots + \lambda_n \pmod p$.

An $n \times n$ matrix A over Z_m is said to be a diagonal matrix if all off diagonal elements are zeros.

Two $n \times n$ matrices A and B are said to be similar if there is an invertible $n \times n$ matrix S such that $A = S^{-1}BS$. A matrix A is said to be diagonalizable if it is similar to a diagonal matrix.

Theorem 2.1.11

Let A be an $n \times n$ matrix over Z_p where p is a prime number. Then, A is diagonalizable if and only if there is a basis for Z_p consisting of the eigen vectors of A.

Theorem 2.1.12 (Cayley-Hamilton)

Let A be $n \times n$ matrix over Z_m, and let $X(\lambda)$ = determinant $(A - \lambda I)$. Then, $X(A) = 0 \pmod m$.

Next, we give results concerning product of rings.

Let m_1 and m_2 be two positive integers. Consider the cartesian product, $Z_{m_1} \times Z_{m_2} = \{(a,b): a \in Z_{m_1}, b \in Z_{m_2}\}$ of Z_{m_1} and Z_{m_2}. We can define addition and multiplication as:

$$(a_1,b_1) + (a_2,b_2) = (a_1 + a_2 \pmod{m_1},\ b_1 + b_2 \pmod{m_2})$$

$$(a_1,b_1) \cdot (a_2,b_2) = (a_1a_2 \pmod{m_1},\ b_1b_2 \pmod{m_2})$$

Then, it is easy to verify all the conditions that are to be satisfied to be a commutative ring. Thus, $Z_{m_1} \times Z_{m_2}$ is a commutative ring with unity, and it is called the product of the rings Z_{m_1} and Z_{m_2}.

More generally, for positive integers $m_1, m_2, \ldots, m_\ell$, we can define the product ring $Z_{m_1} \times Z_{m_2} \times \ldots \times Z_{m_\ell}$.

Two rings R_1 and R_2 are said to be isomorphic if there is a one-to-one and onto function $f: R_1 \to R_2$ such that

$$f(a + b) = f(a) + f(b),$$

and $f(ab) = f(a) \cdot f(b)$ for all a,b in R_1.

The following theorem is useful to our discussions in later chapters.

Theorem 2.1.13 (Chinese Remainder Theorem)

If m_1 and m_2 are relatively prime numbers, then the

product ring $Z_{m_1} \times Z_{m_2}$ and the ring $Z_{m_1 m_2}$ are isomorphic.

In general, if $m_1, m_2, \ldots, m_\ell$ is a set of pairwise relatively prime integers, then the product ring $Z_{m_1} \times \ldots \times Z_{m_\ell}$ is isomorphic to the ring Z_m where $m = m_1 \ldots m_\ell$. In other words, if $m_1, \ldots, m_\ell$ are pairwise relatively prime numbers, then the linear system of equations

$$x = a_i \pmod{m_i} \qquad i = 1, 2, \ldots, \ell$$

has unique solution in Z_m where $m = m_1 \ldots m_\ell$.

Summarized below are the notations that we would be using throughout this thesis.

m, n, t	: positive integers
p, q	: odd prime numbers
Z_m	: ring of integers modulo m
$Z_{m,n}$	: set of all n-tuples with entries in Z_m and with usual addition and scalar multiplication
A, B	: $n \times n$ matrices over Z_m
V	: an alphabet having m letters
f	: a one-to-one mapping from V to Z_m
ϕ	: the Euler function, i.e., $\phi(m)$ is the number of positive integers which are less than m, and relatively prime to m
I_n	: identity matrix over Z_m. (We may write I instead of I_n if there is no ambiguity.)
$M_n(m)$	: the set of all $n \times n$ matrices over Z_m
$G_n(m)$	: $\{A : A \text{ in } M_n(m) \text{ and } A \text{ is invertible}\}$
$S_n(m)$	: $\{A : A \text{ in } M_n(m) \text{ and } A^2 = I_n\}$

$T_k^{(n)}(p)$: {A:A is in $S_n(p)$ with the dimension of the eigen space of A corresponding to 1 is k}

For $t \geq 2$, we define,

$T_k^{(n)}(p^t) = \{A : A \text{ is in } S_n(p^t) \text{ and } A \pmod{p^{t-1}} \text{ is in } T_k^{(n)}(p^{t-1})\}$

Note that the definition is recursive on t. Whenever there is no ambiguity we may omit the superscript n and write $T_k(p)$ and $T_k(p^t)$ instead of $T_k^{(n)}(p)$ and $T_k^{(n)}(p^t)$. $T_k(2)$ and $T_k(2^t)$ are also defined in similar manner.

For positive integers s and t, let $K_{2s}(2^t)$ be the $2s \times 2s$ matrix over Z_{2^t}, which is the direct sum of s matrices of the form $\begin{pmatrix} 2^t-1 & 1 \\ 0 & 1 \end{pmatrix} \pmod{2^t}$.

Examples

(i) $s = 1, t = 1$ $\quad K_2(2) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \pmod 2$

(ii) $s = 1, t = 2$ $\quad K_2(4) = \begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix} \pmod 4$

(iii) $s = 2, t = 3$ $\quad K_4(8) = \begin{pmatrix} 7 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 7 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \pmod 8$

Let $\frac{n}{2} \leq k \leq n$, $s = n - k$ and $r = 2k - n$. Then; define $D_k(2^t) = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & K_{2s}(2^t) \end{array}\right) \pmod{2^t}$. Further, for

$$0 \leq k \leq n\ ,\ D_k(p^t) = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & -I_{n-k} \end{array}\right) \pmod{p^t}\ ,\ t \geq 1\ .$$

For any set X, let $|X|$ denote the cardinality of X. Let $g_n(m) = |G_n(m)|$, and $s_n(m) = |S_n(m)|$.

The following result is required from Chapter IV onwards.

Proposition 2.1.14

$$g_n(p) = (p^n - 1)(p^n - p)\ldots(p^n - p^{n-1})$$

$$= \prod_{i=1}^{n-1} (p^n - p^i)$$

Proof

We know that A is in $G_n(p)$ if and only if all the columns of A are independent over Z_p. The first column of A can be any nonzero element of $Z_{p,n}$, hence has $p^n - 1$ choices. The second column should be any vector which is independent of the first column vector, hence has $p^2 - p$ choices. Similarly, the third column has $p^n - p^2$ choices, etc. Thus, all columns of A have $\prod_{i=1}^{n-1} (p^n - p^i)$ choices. This proves the result.

CHAPTER III

A Brief Survey of Cryptographic Methods

In this Chapter, we briefly discuss and review conventional and public-key cryptosystems. Refer to [6], [7] and [18] for more details.

Throughout this Chapter, let V denote an alphabet with m letters from which a plain-text is built. Let f denote a one-to-one and onto mapping from V to Z_m. Supposing that V is the alphabet of the English language, then f can be taken as $f(A) = 0, f(B) = 1, \ldots, f(Z) = 25$. A plain-text (or message) P with alphabet V is a finite sequence $P_1P_2\ldots P_\ell$ with P_i in V for $1 \leq i \leq \ell$. For a plain-text P in the above form, let f(P) denote the sequence $f(P_1)f(P_2)\ldots f(P_\ell)$.

A cipher-system can be viewed as a set of transformations which produces a cipher-text when applied to a plain-text. The particular transformation used at any time is controlled by a parameter called key. Let E_k denote an encryption process using a key k.

In general, an encryption/decryption algorithm uses two keys, say K and K', one to encrypt the plain-text and the other to decrypt the cipher-text. A cipher-system in which either K = K' or one of K and K' can be easily computed from the knowledge of the other, is known as a symmetric system. Therefore, it is essential to keep the keys secret for a secure system.

If the keys K and K' are such that one of K and K' cannot be easily computed from the knowledge of the other, then the system is called an asymmetric system. As a particular case of the asymmetric system, Diffie and Hellaman [1] have introduced public-key cryptosystem.

Public-key cryptosystem was formulated by the inventors as a two-way communication channel. If E is the encryption process with encryption key K, and D is the decryption process with key K', then we should have

(i) for any message M, $D(E(M,K),K') = M$ and $E(D(M,K'),K) = M$,

(ii) Both E and D are fast to compute, and

(iii) Computing K' from the knowledge of E, D and K is computationally intractable.

In this communication system, a subscriber can produce his own encryption and decryption methods. Let E_A and D_A respectively denote the encryption and decryption method of a subscriber A. All the subscriber has to do is to make his encryption process public by listing E_A in a public directory. Suppose a subscriber B wants to send a message M to A, B first looks in the public directory for the encryption process E_A of A. Then, he computes the encrypted message $S = E_A(M)$, and then sends S to A. Since A has the decryption process D_A, A decrypts the message as $D_A(E_A(M)) = M$.

It is also possible to employ public-key cryptosystem

for implementing an electronic mail system and digital signature (see [17]). Needham and Schroder [13] have given protocols for authentication in large networks using public-key cryptosystem.

The security of public-key-cryptosystem lies on the requirement given in (iii) above. Therefore, in selecting the keys K and K', a trap-door function (a one-to-one function f such that it is computationally intractable to find f^{-1} using the knowledge of f) is used. So, it is natural to employ a computationally hard problem for selecting the keys to be used in a public-key cryptosystem. A public-key cryptosystem based on the knapsack problem is given in [2]. Rivest, Shamir and Adleman have proposed a public-key system based on the problem of factoring large integers. We now proceed to explain this method. For more details see [17].

Let $n = pq$, where p and q are two large primes. Let e and d be two integers such that $ed = 1 \pmod{\phi(n)}$ where ϕ is the Euler function, and $\phi(n) = (p - 1)(q - 1)$. The public-key is the pair (n,e) and the secret key is (n,d).

To encrypt a message, first the message is converted into an integer M between 0 and (n - 1). Then, the encryption is given by $E(M) = M^e \pmod{n}$ and the decryption is given by $D(C) = C^d \pmod{n}$. Since $ed = 1 \pmod{\phi(n)}$, we have, $D(E(M)) = (M^e)^d = M^{ed} = M \pmod{n}$. Similarly, $E(D(C)) = C$.

It is to be mentioned here that the security of this system solely lies in the complexity of factoring a large number.

All the conventional cryptosystems are symmetric systems. We shall illustrate two classes of symmetric systems based on substitutions and algebraic transformations respectively.

A simple substitution method is as follows: Let Π be a permutation on V. Then, a plain-text $P = P_1 \ldots P_\ell$ will be transformed into a cipher text $C = C_1 \ldots C_\ell$ with $C_i = \Pi(P_i)$, $1 \leq i \leq \ell$. Here, the key is the permutation Π. Since there are (m!) possible keys Π, an exhaustive search is impractical. However, a statistical analysis based on the frequency of occurrence of letters of V in a text, would reveal high redundancy, unless the frequency distribution is uniform. Hence, it makes it easy to determine the key Π.

Since the product of two permutations of V is another permutation of V, the above substitution method does not allow to have two or more levels of encryption to increase security. However, if $\{\Pi_i : i = 1,2,\ldots\}$ is a sequence of permutations, a plain-text $P = P_1 P_2 \ldots P_\ell$ can be ciphered as $C = C_1 \ldots C_\ell$ with $C_i = \Pi_i(P_i)$, $1 \leq i \leq \ell$. This system is called monoalphabetic substitution if Π_i is the same for all $i = 1,2,\ldots$; otherwise, it is called polyalphabetic substitution. In a polyalphabetic substitution cipher on a plain-text with n letters, there are $(m!)^n$ possible keys. It also makes the language statistics smooth. An example of this is Vigenére-type systems (see [6]).

If the encryption of a plain-text is done letter-by-letter, it is known as a stream cipher. Otherwise, the plain-text is partitioned into blocks, and then encrypted block-by-block basis, and this type of encryption is known as block cipher. For practical considerations, blocks are all assumed to be of uniform length. In fact, if n is the block length, then a block cipher can be viewed as a stream cipher over the alphabets V^n. The substitution method explained above is a stream cipher.

Transpositions is a particular case of block cipher. Each block will be ciphered using the same key. For example, let the block length be 4 and Π be the permutation: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$. To encrypt the plain text CRYPTOGRAPHY, it should be partioned into three blocks CRYP TOGR APHY each of length 4. Then, using Π we encrypt this text as YCPRGTROHAYP. They are varieties of transposition ciphers, for example, Rail-Fence Cipher System, Route Cipher System. See [5] for more details.

Since cipher systems of transposition type preserves the letter frequencies in the plain-text, a statistical approach would reveal the key. However, it destroys the obvious patterns in the plain-text. For this reason, transpositions are better than simple substitutions.

The Data Encryption Standard (DES) is the official scheme of the National Bureau of Standards (NBS) and is used by federal department and agencies for the crypto-

graphic protection in communication.

This method is a sophisticated substitution permutation mechanism from one character set to another. In fact, it operates on binary coded data obtained from a text and uses a 64 bit key to encode an information of 64 bits. More specifically, the key is divided into eight 8-bit bytes. In an 8-bit byte, 7 bits are used by the encryption algorithm and the eighth bit is used to maintain the odd parity for error detection. So, in effect, the key is of length 56 bits only.

The algorithm for encryption can be viewed as the following three steps:

(i) A transposition operation, usually referred to as the initial permutation (IP).

(ii) A key-dependent complex computation consisting of 16 functionally identical iterations on a 64-bit information.

(iii) A final transposition operation, referred to as the inverse permutation (IP^{-1}) which is the actual inverse of IP used in step (i).

For the 16 functionally identical iterations, 16 keys K_i, $1 \leq i \leq 16$, each of 64-bits are used. The algorithm for one iteration is explained below.

The input to the i-th iteration of the key dependent computation is divided into two blocks L_{i-1} and R_{i-1}, each of 32-bits. L_{i-1} contains the "left" 32 bits and R_{i-1} contains the "right" 32 bits. L_0 and R_0 are the input to

the first iteration, which is formed after permutating with IP.

If L_i, R_i is the output of the i-th iteration, then $L_i = R_{i-1}$ and $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$ where f is a complex function which is the heart of the scheme, and $\oplus$ denotes (mod 2) addition. Note that $f(R_{i-1}, K_i)$ is 32-bit long, and is obtained as follows:

(i) Using a selection process (independent of the key used) a 48-bit data S_i is selected from bits in R_{i-1}.

(ii) Using another selection process, a 48-bit data T_i is selected from the key K_i.

(iii) By adding S_i and T_i using (mod 2) addition, another 48-bit data Q_i is formed.

(iv) The 48-bit data Q_i is then partitioned into 8 groups of 6 bits each. Using a substitution cipher each of these 6-bit groups is converted into 4 bits, giving a total of 32-bits, say X_i.

(v) X_i is permutated using a simple transposition cipher. The output of this is $f(R_{i-1}, K_i)$.

Decryption process is the exact reversal of the encryption process using the keys in the reverse order $K_{16}, K_{15}, \ldots, K_1$.

In considering the security of the DES, it should be noted that there are 2^{56} possible keys. Hence, determining a key by an exhaustive search is impractical. Further, maintaining a catalogue of the frequency usage of blocks of

64-bits is also beyond the capacity of the opponent. However, critics are commenting that the key size should be increased to 128 bits, and the number of keys used is not adequate. See [7] for more details.

Now, we explain another cryptographic method known as Caesar-substitution. For a pair of elements a,b in Z_m, consider the affine linear transformation $T_{a,b}$ from Z_m to Z_m given by $T_{a,b}(x) = ax + b \pmod m$ for all x in Z_m. If a is relatively prime to m, then a^{-1} exists in Z_m, and $x \to a^{-1}(x - b) \pmod m$ is the inverse transform. In encryption each letter P in the alphabet V is transformed into a letter $C = f^{-1}(T_{a,b}(f(P)))$. In decryption, a letter C is transformed into $f^{-1}(a^{-1}(f(C) - b) \pmod m)$. Thus, (a,b) is the encryption key and $(a^{-1},-b)$ is the decryption key.

Example

Suppose that the alphabets V are the English alphabets. Then, m = 26. Let a = 3 and b = 5. We want to encrypt the plain-text CRYPTOGRAPHY using $T_{3,5}$.

The letter C in the plain-text will be replaced by the letter $f^{-1}(T_{3,5}f(C)) = f^{-1}(T_{3,5}(2)) = f^{-1}(11) = L$. Similarly, we do so for other letters, and get the following mapping:

Plain-text: C R Y P T O G R A P H Y

Cipher-text: L E Z Y K V X E F Y A Z

The security of the above cryptographic method primarily depends on the following two factors: (i) determining the key (a,b), and (ii) determining the function f.

The function f is a permutation on m objects. Hence, f can be chosen in (m!) ways. Therefore, determining f by an exhaustive search is impractical. However, some available information, like letter frequencies, might reveal f more easily. From now onwards, we assume that the function f is made known to any one who is aware of this cipher-system. Thus, the security of this cryptosystem rests on one level, i.e., in finding the key (a,b).

If an opponent is granted the option of choosing a plain-text (no restriction is placed on his choice of the plain-text) and is given the privilege of obtaining the cipher-text of the chosen plain-text, then a clever opponent can choose the plain-text with 2 letters P_1P_2 such that $P_1 = f^{-1}(1)$ and $P_2 = f^{-1}(0)$. Let C_1C_2 be the corresponding cipher-text. Then, for this choice, he can solve for a and b; in fact, $b = f(C_2)$ and $a = f(C_1) - b$. Hence, he has the complete knowledge of the cryptosystem.

If the opponent is given some plain-text and its corresponding plain-text, then determining a and b reduces to solving the system of equations:

$$at_1 + b = s_1 \pmod{m}$$

$$at_2 + b = s_2 \pmod{m}$$

for a suitable plain-cipher pair t_1t_2 and s_1s_2.

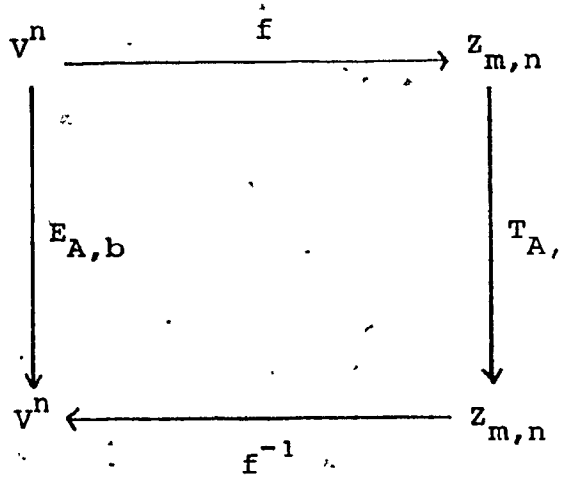
Finally, we assume that the opponent has only some cipher-text. There are only $m \cdot \phi(m)$ pairs (a,b) where $\phi(m)$ is the Euler's number. Hence, it may be possible to determine (a,b) by an exhaustive search. For example, in

the case of English, where m = 26, there are only 338 pairs of (a,b). The modern computer with its enormous power could easily handle this search in a fraction of a second.

In order to increase the security of the cipher system by increasing the complexity of determining the keys, Hill in [3] has proposed the use of matrices with entries in Z_m (instead of using just a pair of elements from Z_m). Below, we explain this method.

Choose an $n \times n$ matrix A over Z_m, and a vector b in $Z_{m,n}$. Define an affine linear transform $T_{A,b}: Z_{m,n} \to Z_{m,n}$ by $T_{A,b}(v) = Av + b \pmod m$. If the determinant of A is relatively prime to m, then A^{-1} exists and $x \to A^{-1}(x - b) \pmod m$ is the inverse transform.

To encrypt a plain-text, the plain text is first grouped into blocks of size n each. Each block is then transformed into a vector in $Z_{m,n}$ using the function f. Then, we apply $T_{A,b}$ to this transformed vector. The resulting vector in $Z_{m,n}$ is transformed back into a block of n letters using f^{-1}. More formally, if V is the alphabet and V^n is the set of all n-grams, then the encryption process $E_{A,b}$ using the key (A,b) is summarized in the following diagram:



i.e., $E_{A,b} = f^{-1}T_{A,b}f$ on V^n.

Example

Suppose that the alphabet V is the English alphabet. Then m = 26. Let n = 2, $A = \begin{pmatrix} 2 & 5 \\ 1 & 10 \end{pmatrix}$ and $b = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$. We want to encrypt the plain-text CRYPTOGRAPHY using $T_{A,b}$.

The plain-text is first grouped into blocks of size 2 as follows: CR YP TO GR AP HY. The block CR is transformed into the vector $v = \begin{pmatrix} 2 \\ 17 \end{pmatrix}$ in $Z_{26,2}$ using the function f. Then, $Av = \begin{pmatrix} 2 & 5 \\ 1 & 10 \end{pmatrix}\begin{pmatrix} 2 \\ 17 \end{pmatrix} = \begin{pmatrix} 89 \\ 172 \end{pmatrix} = \begin{pmatrix} 11 \\ 16 \end{pmatrix}$ (mod 26). $Av + b = \begin{pmatrix} 14 \\ 21 \end{pmatrix}$(mod 26). This is transformed back to the block OV using f^{-1}. Similarly, we do so for the other blocks, and obtain the following mapping:

plain-text:	CR	YP	TO	GR	AP	HY
cipher text:	OV	WX	HI	YZ	AZ	HS .

The security of this method depends on determining the secret key (A,b). In general, for large values of n, the complexity of determining A dominates the complexity of determining b. Hence, for large n we can assume b = 0 without losing much security of the system. Then, encryption key is A and decryption key is A^{-1}. Note that if A is known, then A^{-1} can be computed in $O(n^3)$ time using Gaussian elimination. Thus, the problem of determining the key A and the problem of determining the key A^{-1}, theoretically have the same complexity, and this leads us to assume $A = A^{-1}$. This assumption gives a practical advantage of using the same procedure for both enoryption and decryption.

Of course, the number of keys (A,b) with A in $G_n(m)$ and $b \in Z_{m,n}$ is greater than the number of keys A in $G_n(m)$ with $A = A^{-1}$. However, we prove in later chapters that the number of keys A with $A = A^{-1}$ is very large when n is large. These results show that an exhaustive search to find the key A used in this cryptosystem is practically impossible when n is large.

Levine [9], [10] has systematically investigated the viability of using such matrices A with $A^2 = I \pmod m$ as keys for cryptosystems. He has restricted himself for the case m = 26 and n = 2, 3. The cryptographic analysis outlined in [10] are applicable only to the cases n = 2 and n = 3, and a natural generalization to values n > 3 seems not possible.

Our results given in Chapter IV are quite general, although not conclusive. We believe a more thorough cryptanalysis is necessary before we can conclusively establish the superiority of using involutory matrices with entries in Z_m. See Chapter VI for more details.

CHAPTER IV

Solutions of $A^2 = I \pmod m$

In this chapter, we develop methods to count and characterize the number of $n \times n$ matrices A over Z_m for which $A^2 = I \pmod m$. Our characterization is complete for any n and any prime power modulus. For any modulus m let $m = \prod_{i=1}^{\ell} p_i^{e_i}$, the prime factorization of m. Then, Theorem 4.1.3 establishes that $s_n(m)$ can be computed from $s_n(p_i^{e_i})$, $i = 1,2,\ldots,\ell$. Hence, in principle, we have a complete characterization for any modulus m. The knowledge of the size of the solution space for $A^2 = I \pmod m$ enables a critical complexity analysis that we discuss in Chapter VI.

Recall from Chapter III that the order n of a chosen matrix characterizes the block length, and m is the size of the alphabet from which the plain-text is built. In view of the results proved in Sections 4.1, 4.2 and 4.3, we assert that there is abundant availability of cryptographic keys to support the texts written in any natural lenguage.

In Section 4.1, we develop a formula for $s_n(m)$ where m is any positive integer. In Section 4.2 and 4.3, we find exact expressions for $m = p, p^t$ and $2, 2^t$ respectively.

4.1 Formula for $s_n(m)$

The problem of finding $s_n(m)$, the number of $n \times n$ matrices over Z_m with $A^2 = I$, can be reduced to

finding the number of $n \times n$ matrices with $A^2 = I \pmod{p_i^{e_i}}$ where $m = \prod_{i=1}^{\ell} p_i^{e_i}$, the unique factorization of m. We need the following lemmas:

Lemma 4.1.1

Let m_1 and m_2 be relatively prime and let $h : Z_{m_1} \times Z_{m_2} \to Z_{m_1 m_2}$ be an isomorphism. Then, for a in Z_{m_1} and b in Z_{m_2} with $a^2 = 1 \pmod{m_1}$ and $b^2 = 1 \pmod{m_2}$ we have $(h(a,b))^2 = 1 \pmod{m_1 m_2}$.

Proof

Follows from the Chinese Remainder Theorem.

Lemma 4.1.2

Let m_1 and m_2 be relatively prime. Then,

(i) The product ring $M_n(m_1) \times M_n(m_2)$ is isomorphic to $M_n(m_1 m_2)$.

(ii) If h denotes such an isomorphism, then $h(S_n(m_1) \times S_n(m_2)) = S_n(m_1 m_2)$.

Proof

(i) Let $m = m_1 m_2$. We know that $M_n(m)$ is a ring. By an obvious extension of the Chinese Remainder Theorem, we establish the isomorphism between $M_n(m_1) \times M_n(m_2)$ and $M_n(m_1 m_2)$.

(ii) Let A be in $S_n(m_1)$ and B be in $S_n(m_2)$. Then

$$\begin{aligned}(h(A,B))^2 &= h(A,B) \cdot h(A,B) \\ &= h((A,B) \cdot (A,B)) \\ &= h(A^2, B^2)\end{aligned}$$

$$= h(I(\text{mod } m_1), I(\text{mod } m_2))$$

$$= I(\text{mod } m_1 m_2).$$

Hence, the proof is complete.

It is easy to see that if $m = \prod_{i=1}^{\ell} m_i$ where $m_i = p_i^{e_i}$, then $h(S_1(m_1) \times \ldots \times S_n(m_\ell)) = S_n(m)$. As a consequence, we have the following theorem:

Theorem 4.1.3

If $m = \prod_{i=1}^{\ell} p_i^{e_i}$ then $s_n(m) = \prod_{i=1}^{\ell} s_n(m_i)$.

Now, it remains to find $s_n(p^t)$, $t \geq 1$, for any prime p. The following two sections are devoted to developing an expression for $s_n(p^t)$.

4.2 Solution for $s_n(p^t)$, $t \geq 2$, $p > 2$

In this section, p always denotes an odd prime, $m = p^t$ with $t \geq 1$, and n is a fixed positive integer with $n \geq 1$. We start with a simple proposition.

Proposition 4.2.1

$S_1(p)$ has only two elements.

Proof

Note that Z_p is a field. As $n = 1$, every element in $S_1(p)$ is an element of Z_p such that $a^2 = 1 \pmod p$. This equation has exactly two solutions, namely 1 and $p - 1$ in Z_p.

From now onwards, we assume $n \geq 2$ and A is an $n \times n$ matrix.

Proposition 4.2.2

If $A^2 = I \pmod p$, then

(i) A has eigen values $\pm 1 \pmod p$,

and (ii) A is diagonalizable.

Proof

(i) Since $A^2 = I \pmod p$, the eigen values of A are the roots of the equation $x^2 - 1 = 0 \pmod p$. i.e., $x = \pm 1 \pmod p$ are the eigen values.

(ii) Let E_{+1} and E_{-1} be the eigen spaces of A corresponding to the eigen values +1 and -1 respectively. Then for a vector v in $Z_{p,n}$, $Av + v$ is in E_{+1} and $Av - v$ is in E_{-1}. Further, $v = \frac{1}{2}[(Av + v) - (Av - v)] \pmod p$. Thus, every v in $Z_{p,n}$ can be written as a sum of vectors v_1 and v_2 with v_1 in E_{+1} and v_2 in E_{-1}. Hence by Theorem 2.1.11, we prove that A is diagonalizable.

Corollary 4.2.3

Let A be an $n \times n$ matrix over Z_p such that $A^2 = I \pmod p$. If all the eigen values of A are +1 (-1), then $A = I \pmod p$ $(A = -I \pmod p)$.

From our definitions in Chapter II, it follows that

(i) $S_n(p) = \bigcup_{k=0}^{n} T_k(p)$, and it is a disjoint union.

(ii) Let I_ℓ denote the $\ell \times \ell$ identity matrix. Then, every matrix in $T_k(p)$ is similar to

$$D_k(p) = \left(\begin{array}{c|c} I_k & 0 \\ \hline 0 & -I_{n-k} \end{array}\right) \pmod p.$$

The following proposition gives a method to compute $|T_k(p)|$.

Proposition 4.2.4

For $0 \leq k \leq n$, $|T_k(p)| = \dfrac{g_n(p)}{g_k(p)\, g_{n-k}(p)}$ with $g_0(p) = 1$.

Proof

Let A be in $T_k(p)$. Then, A is diagonalizable. Therefore, there is a P in $G_n(p)$ such that $A = PD_kP^{-1} \pmod p$ where $D_k = \left(\begin{array}{c|c} I_k & 0 \\ \hline 0 & -I_{n-k} \end{array}\right) \pmod p$. However, the collection $\{PD_kP^{-1} : P \text{ in } G_n(p)\}$ has duplications.

Let R be in $G_n(p)$ such that $R^{-1}D_kR = D_k \pmod p$. Then, the first k columns of R independent vectors are chosen from the space E_{+1}, and the remaining $(n - k)$ columns are independent vectors chosen from the space E_{-1}. Thus, there are $g_k(p)\cdot g_{n-k}(p)$ matrices R such that $RD_kR^{-1} = D_k \pmod p$.

Now, fix a P in $G_n(p)$. Let there be Q in $G_n(p)$ such that $PD_kP^{-1} = QD_kQ^{-1} \pmod p$. This gives, $(Q^{-1}P)D_k(Q^{-1}P)^{-1} = D_k$, i.e., with $R = Q^{-1}P$, we get $g_k(p)\cdot g_{n-k}(p)$ matrices Q such that $PD_kP^{-1} = QD_kQ^{-1} \pmod p$.

Thus, each element in the collection $\{P^{-1}D_kP: P \text{ in } G_n(p)\}$ is duplicated exactly $g_k(p)\,g_{n-k}(p)$ times. Hence the result.

Now, we give the formula for $s_n(p)$ in the following theorem:

Theorem 4.2.5

$$s_n(p) = \sum_{k=0}^{n} \frac{g_n(p)}{g_k(p)\,g_{n-k}(p)} \quad \text{with} \quad g_0(p) = 1.$$

Proof

From our remarks preceding Proposition 4.2.4 we have, $S_n(p) = \bigcup_{k=0}^{n} T_k(p)$. Therefore,

$$s_n(p) = \sum_{k=0}^{n} |T_k(p)|,$$

$$= \sum_{k=0}^{n} \frac{g_n(p)}{g_k(p)\,g_{n-k}(p)} \quad \text{from the above proposition.}$$

So, when the modulus is an odd prime p, we not only know the number of matrices in $S_n(p)$, but we also know $|T_k(p)|$, $0 \le k \le n$. We can generate matrices in $T_k(p)$ by $S^{-1}D_kS$ with S in $G_n(p)$. Our interest now is to investigate the structure of $T_k(p^t)$, $t \ge 2$. Towards this, we need results extending the similarity property of the matrices in $T_k(p)$.

We define $\chi: M_n(p^t) \to M_n(p^{t-1})$ by $\chi(A) = A \pmod{p^{t-1}}$ for $t \ge 2$. It is clear that $\chi(S_n(p^t)) = S_n(p^{t-1})$ and

$\chi(T_k(p^t)) = T_k(p^{t-1})$.

We say that Y in $T_k(p^t)$ is an <u>extension of X</u> in $T_k(p^{t-1})$ if $\chi(Y) = X$. Note that for a given X in $T_k(p^{t-1})$ there may be more than one extension in $T_k(p^t)$. In fact, in the following Theorem, we prove that there are $p^{2k(n-k)}$ extensions of X to $T_k(p^t)$.

<u>Theorem 4.2.6</u>

Let $t \geq 2$. Then

(i) Every element in $T_k(p^{t-1})$ has exactly $p^{2k(n-k)}$ extension to $T_k(p^t)$.

(ii) $|T_k(p^t)| = p^{2k(n-k)} |T_k(p^{t-1})|$.

(iii) All the elements of $T_k(p^t)$ are similar to

$$D_k(p^t) = \left(\begin{array}{c|c} I_k & 0 \\ \hline 0 & -I_{n-k} \end{array}\right) \pmod{p^t}.$$

<u>Proof</u>

We use induction on t. So, let us first assume $t = 2$.

(i) Let X be in $T_k(p)$. Then, either

$$X = \left(\begin{array}{c|c} I_k & 0 \\ \hline 0 & -I_{n-k} \end{array}\right) \pmod{p}$$ or there exists an S in $G_n(p)$ such that $X = S^{-1}\left(\begin{array}{c|c} I_k & 0 \\ \hline 0 & -I_{n-k} \end{array}\right)S \pmod{p}$.

For notational convenience let

$$D_k(p) = \left(\begin{array}{c|c} I_k & 0 \\ \hline 0 & -I_{n-k} \end{array}\right) \pmod{p} \text{ and}$$

$$D_k(p^2) = \left(\begin{array}{c|c} I_k & 0 \\ \hline 0 & -I_{n-k} \end{array}\right) \pmod{p^2}. \text{ Note that}$$

$$D_k(p) = D_k(p^2) \pmod{p}.$$

Case 1: $X = D_k(p)$.

If Y is any extension of X, then by definition $\chi(Y) = X$. Therefore, $Y = X + pQ_1 \pmod{p^2}$ for some Q_1 in $M_n(p)$.

i.e., $Y = D_k(p) + pQ_1 \pmod{p^2}$

$$= \left(\begin{array}{c|c} I_k & 0 \\ \hline 0 & (p-1)I_{n-k} \end{array}\right) + pQ_1 \pmod{p^2}$$

$$= \left(\begin{array}{c|c} I_k & 0 \\ \hline 0 & (p^2-1)I_{n-k} \end{array}\right) + \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & p(1-p)I_{n-k} \end{array}\right) + pQ_1 \pmod{p^2}$$

$= D_k(p^2) + pQ \pmod{p}$ where

$$Q = Q_1 + \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & (1-p)I_{n-k} \end{array}\right)$$

Thus,

$$Y^2 = (D_k(p^2))^2 + p^2Q^2 + p(D_k(p^2)Q + QD_k(p^2)) \pmod{p^2}$$

If Y is in $T_k(p^2)$, then $Y^2 = I \pmod{p^2}$. Further, $(D_k(p^2))^2 = I \pmod{p^2}$. Therefore, the above

equation gives,

$$I = I + 0 + p(D_k(p^2)Q + QD_k(p^2)) \pmod{p^2}$$

i.e., $D_k(p^2)\ Q + QD_k(p^2) = 0 \pmod{p}$.

But, $D_k(p^2) \pmod{p} = D_k(p) \pmod{p}$.

Therefore, $D_k(p)Q + QD_k(p) = 0 \pmod{p}$ .....(4.1)

Now, let $Q = \left(\begin{array}{c|c} \alpha & \beta \\ \hline \gamma & \delta \end{array}\right)$ where α is a $k \times k$ matrix, β is $k \times (n-k)$ matrix, γ is $(n-k) \times k$ matrix, and δ is $(n-k) \times (n-k)$ matrix, over Z_p.

Then, $QD_k(p) + D_k(p)Q = \begin{pmatrix} 2\alpha & 0 \\ 0 & -2\delta \end{pmatrix} \pmod{p}$.

From (4.1), we get $\alpha = 0 = \delta \pmod{p}$. Hence $Q = \left(\begin{array}{c|c} 0 & \beta \\ \hline \gamma & 0 \end{array}\right)$ with β, γ arbitrary. Thus, $Y = D_k(p^2) + p\left(\begin{array}{c|c} 0 & \beta \\ \hline \gamma & 0 \end{array}\right)$. Since β and γ each can be chosen in $p^{k(n-k)}$ ways, we have $p^{2k(n-k)}$ choices for Y. Therefore, $D_k(p)$ in $T_k(p)$ has $p^{2k(n-k)}$ extensions.

Case 2: $X = S^{-1}D_k(p)S$ with S in $G_n(p)$.

Then, $SXS^{-1} = D_k(p)$. Therefore, by Case 1, SXS^{-1} has extensions of the form $D_k(p^2) + pQ \pmod{p^2}$ with

$Q = \left(\begin{array}{c|c} 0 & \beta \\ \hline \gamma & 0 \end{array}\right) (\text{mod } p)$. i.e., $SXS^{-1} (\text{mod } p)$ has exactly $p^{2k(n-k)}$ extensions. Hence, X has exactly $p^{2k(n-k)}$ extensions. In fact, extensions of X are of the form $S^{-1}(D_k(p^2) + pQ)S (\text{mod } p^2)$ with $Q = \left(\begin{array}{c|c} 0 & \beta \\ \hline \gamma & 0 \end{array}\right) (\text{mod } p)$. This completes the proof of (i).

(ii) From (i) we have

$$|T_k(p^2)| = p^{2k(n-k)} |T_k(p)|.$$

(iii) In (i) we have proved that elements of $T_k(p^2)$ are of the form $S^{-1}(D_k(p^2) + pQ)S$ with S in $G_n(p)$ and $Q = \left(\begin{array}{c|c} 0 & \beta \\ \hline \gamma & 0 \end{array}\right) (\text{mod } p)$. Let

$$Q' = \frac{1}{2}\left(\begin{array}{c|c} 0 & -\beta \\ \hline \gamma & 0 \end{array}\right) (\text{mod } p \quad \text{and } R = I + pQ' (\text{mod } p^2).$$

Then $R^{-1} = I - pQ' (\text{mod } p^2)$. We claim that

$$R^{-1}(D_k(p^2) + pQ)R = D_k(p^2) (\text{mod } p^2).$$

To prove this, consider

$$R^{-1}(D_k(p^2) + pQ)R = (I - pQ')(D_k(p^2) + pQ)(I + pQ') (\text{mod } p^2)$$

$$= (D_k(p^2) + pQ - pQ'D_k(p^2))(I + pQ') (\text{mod } p^2)$$

$$= D_k(p^2) + p[D_k(p^2)Q' - Q'D_k(p^2) + Q] (\text{mod } p^2) \quad \ldots\ldots (4.2)$$

Now, $D_k(p^2)Q' = \frac{1}{2}\left(\begin{array}{c|c} 0 & -\beta \\ \hline -\gamma & 0 \end{array}\right) \pmod p$

$$Q' D_k(p^2) = \frac{1}{2}\left(\begin{array}{c|c} 0 & \beta \\ \hline \gamma & 0 \end{array}\right) \pmod p$$

Hence, $D_k(p^2)Q' - Q'D_k(p^2) = -Q \pmod p$.

i.e.; $D_k(p^2)Q' + Q'D_k(p^2) + Q = 0 \pmod p$.

Using this in (4.2) we get

$$R^{-1}D_k(p^2)R = D_k(p^2) \pmod{p^2}.$$

Hence, the claim is proved.

Any element Y in $T_k(p^2)$ is of the form

$$Y = S^{-1}(D_k(p^2) + pQ)S \pmod{p^2}$$

$$= S^{-1}R^{-1}(D_k(p^2))RS \pmod{p^2}$$

Hence, the proof of (iii) for t = 2 is complete.

Thus, the theorem is proved for t = 2. To complete the proof by induction, we virtually follow the same steps. Any extension of $D_k(p^{t-1})$ in $T_k(p^{t-1})$ can be proved to be of the form $D_k(p^{t-1}) + p^{t-1}Q \pmod{p^t}$ with $Q = \left(\begin{array}{c|c} 0 & \beta \\ \hline \gamma & 0 \end{array}\right) \pmod p$. Hence, any element $X = S^{-1}D_k(p^{t-1})S$ with S in $G_n(p^{t-1})$ has extensions of the form $S^{-1}(D_k(p^t) + p^{t-1}Q)S \pmod{p^t}$ with $Q = \left(\begin{array}{c|c} 0 & \beta \\ \hline \gamma & 0 \end{array}\right) \pmod p$. It can be proved to be similar to $D_k(p^t)$ by choosing $R = I + p^{t-1}Q' \pmod{p^t}$ and

$$Q' = \frac{1}{2}\left(\begin{array}{c|c} 0 & -\beta \\ \hline \gamma & 0 \end{array}\right) \pmod{p^t}.$$

Thus, the theorem is proved.

From the above theorem and the fact that $S_n(p^t) = \bigcup_{k=0}^{n} T_k(p^t)$, we obtain our main result giving the expression for $s_n(p^t)$. Precisely we have,

Theorem 4.2.7

Let $0 \leq k \leq n$. Then,

(i) $|T_k(p^t)| = p^{2(t-1)k(n-k)} |T_k(p)|$, $t \geq 1$

(ii) $s_n(p^t) = \sum_{k=0}^{n} p^{2(t-1)k(n-k)} |T_k(p)|$

$$= \sum_{k=0}^{n} p^{2(t-1)k(n-k)} \frac{g_n(p)}{g_k(p) \cdot g_{n-k}(p)}$$

Finally, we describe the generation of a matrix in $T_k(p^t)$ by characterizing its structure. We claim that if elements of $T_k(p)$ are generated successively, then we can generate the elements of $T_k(p^t)$ for $t > 1$.

Let $F(p) = \left\{\left(\begin{array}{c|c} 0 & \beta \\ \hline \gamma & 0 \end{array}\right) : \beta \text{ is } k \times (n-k) \text{ matrix and } \gamma \text{ is } (n-k) \times k \text{ matrix over } Z_p\right\}$

Then, $|F(p)| = p^{2k(n-k)}$. For $\ell \geq 1$, define

$$G_\ell = \left\{B : B = I + p^\ell Q \pmod{p^{\ell+1}} \text{ where } Q \text{ is in } F(p)\right\}$$

We know that all the elements $T_k(p)$ are of the form $S^{-1}D_k(p)S$ with S in $G_n(p)$.

Choose S_j for $j = 1,2,\ldots,|T_k(p)|$ such that

$$T_k(p) = \{S_j^{-1} D_k(p) S_j : j = 1,2,\ldots,|T_k(p)|\}$$

Let $H_1 = \{S_j \pmod p : j = 1,2, \ldots, T_k(p)$ as chosen above$\}$

Define $H_2 = \{B : B = RS \pmod{p^2}$ with R in G_1 and S in $H_1\}$

$$H = G_1 \cdot H_1$$

$$H_3 = \{B : B = RS \pmod{p^3}$ with R in G_2 and S in $H_2\}$$

$$= G_2 \cdot H_2$$

$$\vdots \quad \vdots \quad \vdots$$

$$H_t = G_{t-1} \cdot H_{t-1} \quad \text{for } t \geq 2$$

Then, $T_k(p^t) = \{B^{-1} D_k(p^t) B \pmod{p^t} : B$ is in $H_t\}$.

Thus, starting with any element in $T_k(p)$, we generate an element in successive H_i's defined above. We finally arrive at an element of $T_k(p^t)$. In fact, generation of all the elements of $T_k(p^t)$ is simple, once we know how to generate all the elements in $T_k(p)$.

4.3 Solution for $s_n(2^t)$, $t \geq 1$

In this section, we characterize the solution of matrices $A^2 = I \pmod{2^t}$, $t \geq 1$, and also derive an expression for $s_n(2^t)$. We first state and prove a basic result.

Lemma 4.3.1

The equation $x^2 = 1 \pmod{2^t}$ with x in Z_m, $m = 2^t$, has

(i) exactly one solution if $t = 1$,

(ii) exactly two solutions if $t = 2$,

and (iii) exactly four solutions if $t \geq 3$.

Proof

Case 1: For $t = 1$, $X = 1$ is the only solution. For $t = 2$, it is clear that $X = \pm 1$ are the two solutions.

Case 2: Let $t \geq 3$. The equation $x^2 = 1 \pmod{2^t}$ has $x = a$ as a solution only if a is an odd integer. Therefore, let $a = 2\ell + 1$ where ℓ is an integer ≥ 0. Then, $a^2 = 1 \pmod{2^t}$ implies that

$$4\ell^2 + 4\ell = 0 \pmod{2^t}.$$

i.e., $$\ell^2 + \ell = 0 \pmod{2^{t-2}}$$

i.e., $$\ell(\ell + 1) = 0 \pmod{2^{t-2}}.$$

i.e., either 2^{t-2} divides ℓ or 2^{t-2} divides $\ell + 1$

i.e., either $\ell = \alpha 2^{t-2}$ or $\ell = \alpha 2^{t-2} - 1$ for some integer α. Then, either $a = \alpha 2^{t-1} + 1 \pmod{2^t}$ or $a = \alpha 2^{t-1} - 1 \pmod{2^t}$. Thus, α should be 0 or 1. Hence, $a = \pm 1 \pmod{2^t}$ or $a = 2^{t-1} \pm 1 \pmod{2^t}$. Thus, there are only four solutions to $x^2 = 1 \pmod{2^t}$ in Z_{2^t}. This proves the lemma.

We first consider the number of solutions to $A^2 = I \pmod 2$ when A is a 2×2 matrix over Z_2. For this case, $S_2(2)$ has only four elements as listed below:

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

a	b	c	d
1	0	0	1
0	1	1	0
1	1	0	1
1	0	1	0

It is not difficult to enumerate the matrices for $m = 4$ and $n = 2$. $S_2(4)$ has exactly 28 matrices as listed below:

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

a	b	c	d
0	1	1	0
0	3	3	0
1	0	0	1
1	0	2	1
1	2	0	1
1	2	2	1
1	0	*	3
1	*	0	3
1	2	2	3
2	1	1	2
2	3	3	2
3	2	2	1
3	0	*	1
3	*	0	1
3	0	0	3
3	0	2	3
3	2	0	3
3	2	2	3

*means any element in Z_4.

After eliminating duplicates in the list (that might arise when * is substituted by an element of Z_4) there are only 28 elements. Our expression for $s_n(2^t)$ given later agrees with this count for $t = 2$, $n = 2$.

First we calculate the number of matrices in $S_n(2)$ and then proceed to calculate the number of elements in $S_n(2^t)$ for $t \geq 2$. The following three lemmas play an essential role in computing $s_n(2)$.

Lemma 4.3.2

Let A be an $n \times n$ matrix over Z_2 such that $A^2 = I \pmod 2$. Then, the eigen space E_1 of A corresponding to the eigen value 1 has dimension at least n/2.

Proof

Let $V_n = Z_{2,n}$ and let V be a complement of E_1 in V_n. i.e., $V_n = E_1 \oplus V$. Since $A^2 = I \pmod 2$, we have for any v in V_n, $Av + v$ is in E_1. Consider the linear map $A + I: V_n \to E_1$. In particular, consider the restriction of $A + I$ to V. We claim that $A + I$ restricted to V is injective.

For, if v in V is such that $(A + I)v = 0$, then $Av = v \pmod 2$, and hence v is in E_1. Since $V \cap E_1 = \{0\}$, we have $v = 0$. Hence, the claim. Therefore, dimension of V $\leq$ dimensions of E_1. But, dimension of V + dimension of E_1 = n. Hence, dimension of $E_1 \geq n/2$, and the lemma is proved.

Lemma 4.3.3

Let $V_n = Z_{2,n}$ and $\frac{n}{2} \leq k \leq n$. Let V be a subspace of V_n of dimension k. Let d be the number of matrices in $S_n(2)$

with V as eigen space corresponding to the eigen value 1. Then, d is the cardinality of set $GL(n - k,k)$, where $GL(n - k,k)$ is the set of all $k \times (n - k)$ matrices over Z_2 of rank $(n - k)$.

Proof

Let A be in $S_n(2)$ such that eigen space of A corresponding to 1 is V. Put $B = A + I$. Then, $B^2 = A^2 + 2A + I = 2(A + I) = 0 \pmod 2$. Let W be a complement of V in V_n. i.e., $V_n = V \oplus W$. Since the null space of B is V, and $B^2 = 0$, we have B maps W into V and the restriction map $B:W \to V$ is injective. Hence, B(W) is an $(n - k)$ dimensional subspace of V. Hence, the number of B's is equal to the number of $k \times (n - k)$ matrices with rank $(n - k)$ which is $|GL(n - k,k)|$. Since $B = A + I$, the result follows.

Lemma 4.3.4

For $0 \leq k \leq n$, the number of k dimensional subspace of $Z_{2,n}$ is given by $\dfrac{g_n(2)}{g_k(2)g_{n-k}(2)\cdot 2^{k(n-k)}}$.

Proof

Let V be a k dimensional subspace of $V_n = Z_{2,n}$. Consider a nonsingular mapping $T:V_n \to V_n$ such that $T(V) = V$. A matrix representation of T is of the form $\left(\begin{array}{c|c} A_1 & A_2 \\ \hline 0 & A_3 \end{array}\right)$ where A_1 is in $G_k(2)$, A_3 is $G_{n-k}(2)$ and A_2 is a $k \times (n - k)$ matrix over Z_2. The total number of such matrices are

$g_k(2) \cdot g_{n-k}(2) \cdot 2^{k(n-k)}$.

Further, the number of k dimensional subspaces of V_n is same as the number of nonsingular matrices S over Z_2 such that $S(V) \neq V$, unless $S = I \pmod 2$. Thus, the required number is given by the quotient $\dfrac{\cdot\, g_n(2)}{g_k(2) \cdot g_{n-k}(2) \cdot 2^{k(n-k)}}$.

Now, we prove the following theorem which gives an expression for $s_n(2)$.

Theorem 4.3.5

Let k be a nonnegative integer. Then

(i) $|T_k(2)| = 0$ if $0 \leq k < \frac{n}{2}$.

(ii) $|T_k(2)| = \dfrac{g_n(2)|GL(n-k,k)|}{g_k(2) g_{n-k}(2)\ 2^{k(n-k)}}$ if $\frac{n}{2} \leq k \leq n$.

(iii) $s_n(2) = \sum\limits_{\frac{n}{2} \leq k \leq n} \dfrac{g_n(2)|GL(n-k,k)|}{g_k(2) g_{n-k}(2)\ 2^{k(n-k)}}$

Proof

Recall from the definition that $T_k(2)$ is set of all elements A in $M_n(2)$ such that $A^2 = I \pmod 2$ and the dimension of eigen space E_1 corresponding to the eigen value 1 is k.

By the Lemma 4.3.2, $T_k(2)$ is an empty set if $0 \leq k < \frac{n}{2}$. This proves (i).

Lemmas 4.3.3 and Lemma 4.3.4 together give result (ii). To prove (iii), we have $S_n(2) = \bigcup\limits_{k=0}^{n} T_k(2)$, and $T_k(2)$ is

empty if $0 \leq k < \frac{n}{2}$. Thus, $s_n(2) = \sum_{\frac{n}{2} \leq k \leq n} |T_k(2)|$.

Substituting the value of $|T_k(2)|$ from (ii), the result follows. The proof of the theorem is complete.

Example 4.3.6

Let $m = 2$ and $n = 2$. Then, $T_k(2)$ is not empty if and only if $1 \leq k \leq 2$. By the above theorem,

$$|T_1(2)| = \frac{g_2(2)\,|GL(1,1)|}{g_1(2)\cdot g_2(2)\,2}$$

$$= \frac{(2^2 - 1)(2^2 - 2)\cdot 1}{1\cdot 1\cdot 2} = 3 .$$

$$|T_2(2)| = \frac{g_2(2)\,|GL(0,2)|}{g_2(2)\,g_0(2)\cdot 2^0}$$

$$= 1$$

In fact, $T_1(2) = \left\{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right\}$

and $T_2(2) = \left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$.

(See the listing of $S_2(2)$ preceding Lemma 4.3.2.)

Example 4.3.7

Let $m = 2$ and $n = 3$. Then, $T_k(2)$ is nonempty if and only if $2 \leq k \leq 3$.

From Theorem 4.3.5 (ii), we get $|T_2(2)| = 21$ and $|T_3(2)| = 1$. Therefore $s_3(2) = 22$.

The matrices according to the dimension k of the eigen space corresponding to 1 are listed below:

$$T_3(2) = \left\{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right\} .$$

$T_2(2)$:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ c_1 & c_2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & b_1 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ c_1 & c_1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & b_1 \\ 1 & 0 & b_1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ c_1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & c_2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & b_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

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

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

where the b's and c's are arbitrary in Z_2.

Levine [10] has studied the suitability of involutory matrices of order 3 with m = 26 for encryption. In his study the matrices in $S_3(2)$ play an important role. Since there are only 22 matrices in $S_2(3)$, Levine was able to investigate their properties in depth and formulate necessary conditions to detect the given patterns in a cipher text. We comment, however, that such properties and

techniques cannot be extended over either to matrices of order $n > 3$ or m not equal to $2p$ with p an odd prime. We further deal with this in Chapter VI. For now we shall try to extend our theory for the case $m = 2^t$, $t \geq 2$.

Proposition 4.3.8

Let A be an $n \times n$ matrix over Z_2 such that $A^2 = I \pmod 2$. Then, there exists two integers r and s with $0 \leq r \leq n$ and $0 \leq 2s \leq n$ such that A is similar to $\left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & K_{2s} \end{array}\right)$ where I_r is the $r \times r$ identity matrix, and K_{2s} is a $2s \times 2s$ matrix which is the direct sum of s matrices of the form $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \pmod 2$. In fact, if k is the dimension of the eigen space corresponding to 1, then $s = n - k$ and $r = 2k - n$.

Proof

Let E_1 be the eigen space of A corresponding to 1 and let its dimension be k. Then from Lemma 4.3.2, we know that $k \geq \frac{n}{2}$. Let $\{v_1, v_2, \ldots, v_k\}$ be a basis for E_1. By choosing $v_{k+1}, v_{k+2}, \ldots, v_n$ as outlined below, we form a basis $\{v_i : i = 1,2,\ldots,n\}$ for $Z_{2,n}$.

For any vector v in $Z_{2,n}$, $Av + v$ is in E_1. In particular, for a nonzero vector v not in E_1, $Av + v$ is a nonzero vector in E_1. Hence, we can choose a nonzero vector v_{k+1} not in E_1 such that $Av_{k+1} + v_{k+1} = v_i$ for some i with $1 \leq i \leq k$. Since $n - k \leq k$, it is possible to choose $v_{k+2}, \ldots, v_n$ such that

(i) $Av_{k+j} + v_{k+j} \in \{v_i : i = 1,2,\ldots,k\}$ for

$j = 1,2,\ldots,(n - k)$,

and (ii) $Av_{k+i} + v_{k+i} \neq Av_{k+j} + v_{k+j}$ if $i \neq j$.

Put $s = n - k$ and $r = k - s$. By resequencing, if necessary, and relabelling, we can assume that $v_1,\ldots,v_r,u_1,u_2,\ldots,u_{2s}$ is a basis for $Z_{2,n}$, and

$$\begin{aligned}
Av_i &= v_i \qquad i = 1,2,\ldots,r \\
Au_1 &= u_1 + u_2 \\
Au_2 &= u_2 \\
Au_3 &= u_3 + u_4 \\
Au_4 &= u_4 \\
&\vdots \\
Au_{2s-1} &= u_{2s-1} + u_{2s} \\
Au_{2s} &= u_{2s}.
\end{aligned}$$

Thus, the matrix of A with respect to this basis of the form

$$\left(\begin{array}{c|ccccc} I_r & & & 0 & & \\ \hline & 1 & 1 & 0 & \ldots & 0 \\ & 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 0 & 1 & 1\ldots & 0 \\ & 0 & 0 & 0 & 1\ldots & 0 \\ & \cdot & \cdot & \cdot & \cdots & \cdot \end{array}\right) = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & K_{2s} \end{array}\right) \pmod 2.$$

Hence, the result is proved.

By combining Theorem 4.3.5 (ii) and the above proposition, we obtain the following corollary.

Corollary 4.3.9

The number of matrices A in $M_n(2)$ that are similar to $\left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & K_{2s} \end{array}\right)$, where $r + 2s = n$, is given by

$$\frac{g_n(2)|GL(n-k,k)|}{g_k(2)g_{n-k}(2)\ 2^{k(n-k)}} \quad \text{with} \quad k = r + s.$$

Next we find $s_n(4)$. Recall that a matrix A is in $T_k(4)$ if and only if A (mod 2) is in $T_k(2)$. An element Y in $T_k(4)$ is said to be an extension of X in $T_k(2)$ if $X = Y \pmod 2$. The following theorem gives the count of such extensions.,

Theorem 4.3.10

Let $\frac{n}{2} \leq k \leq n$. Then,

(i) Every element of $T_k(2)$ has exactly $2^{k^2+(n-k)^2}$ extensions in $T_k(4)$.

(ii) $|T_k(4)| = 2^{k^2+(n-k)^2}|T_k(2)|$.

(iii) $s_n(4) = \sum_{\frac{n}{2} \leq k \leq n} 2^{k^2+(n-k)^2}|T_k(2)|$.

(Recall that the value of $|T_k(2)|$ is given in Theorem 4.3.5.)

Proof

Proof of (i). Let $D_k = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & K_{2s} \end{array}\right) \pmod 2$. Then, we know that X in $T_k(2)$ is similar to D_k. (See Proposition

4.3.8.) We treat the case $X = D_k \pmod 2$, and X is similar to D_k separately.

Case 1: Let $X = D_k \pmod 2$.

If Y in $T_k(4)$ is an extension of X, then there is a Q_1 in $M_n(2)$ such that $Y = X + 2Q_1 \pmod 4$. Now $D_k = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & K_{2s} \end{array}\right) \pmod 2$ with K_{2s} as the direct sum of s matrices of the form $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. It can be written as a sum of two matrices $K_{2s}(4)$ and $2Q'$ where $K_{2s}(4)$ is the direct sum of s matrices of the form $\begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix} \pmod 4$, and Q' is the direct sum of s matrices of the form $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \pmod 4$. Hence,

$$Y = D_k + 2Q_1 \pmod 4$$

$$= \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & K_{2s}(4) \end{array}\right) + 2\left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & Q'' \end{array}\right) + 2Q_1 \pmod 4$$

$$= D_k(4) + 2Q' \pmod 4,$$

where $D_k(4) = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & K_{2s}(4) \end{array}\right)$ and

$Q = \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & Q' \end{array}\right) + Q_1 \pmod 2$. Hence

$$Y^2 = (D_k(4))^2 + 2(QD_k(4) + D_k(4)Q) + 4Q^2 \pmod 4.$$

Using the fact $Y^2 \equiv I \pmod 4$ and $(D_k(4))^2 = I \pmod 4$, we have $2(QD_k(4) + D_k(4)Q) = 0 \pmod 4$

i.e. $QD_k(4) + D_k(4)Q = 0 \pmod 2$

i.e. $QD_k + D_kQ = 0 \pmod 2$, ...(4.3)

Now, $D_k = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & K_{2s} \end{array}\right) \pmod 2$

$= I_n + \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & W \end{array}\right) \pmod 2$ where W is the direct sum of s matrices of the form $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Put $U = \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & W \end{array}\right)$. Therefore, $D_k = I_n + U \pmod 2$.

Substituting in (4.3), we get that

$$QU + UQ = 0 \pmod 2 \quad \text{.....(4.4)}$$

Let $Q = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ where α is $r \times r$ matrix, β is $r \times 2s$ matrix, r is $2s \times r$ matrix, and δ is $2s \times 2s$ matrix over Z_2. Then, from 4.4, we get α is arbitrary, and

$$\beta W = 0 \pmod 2 \quad \text{.....(4.5)}$$

$$W\gamma = 0 \pmod 2 \quad \text{.....(4.6)}$$

$$W\delta + \delta W = 0 \pmod 2 \quad \text{.....(4.7)}$$

(4.5) gives all the odd columns of β are zeros, and (4.6) gives all the even rows of γ are zeros.

Let $\delta = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1,2s} \\ a_{21} & a_{22} & \cdots & a_{2,2s} \\ \vdots & \vdots & \vdots & \vdots \\ a_{2s,1} & a_{2s,2} & \cdots & a_{2s,2s} \end{pmatrix}$. Thus, (4.7) gives

$$\delta = \begin{pmatrix} a_{11} & a_{12} & \cdots & \cdots & a_{1,2s} \\ 0 & a_{11} & 0 & a_{13} & \cdots & a_{1,2s-1} \\ a_{31} & a_{32} & a_{33} & \cdots & & a_{3,2s} \\ 0 & a_{31} & 0 & a_{33} & \cdots & a_{3,2s-1} \\ \vdots & & & & & \vdots \\ 0 & a_{2s-1,1} & 0 & \cdots & & a_{2s-1,2s} \end{pmatrix} \quad \ldots(4.8)$$

with a's arbitrary

Thus, $Y = D_k(4) + 2Q \pmod 4$

$= D_k(4) + 2\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \pmod 4$ with α

arbitrary $r \times r$ matrix over Z_2. β is an $r \times 2s$ matrix with odd columns having zeros. γ is an $2s \times r$ matrix with even rows having zeros. δ is an $2s \times 2s$ matrix having the form given in (4.8). We can choose α in $2r^2$ ways, β in 2^{rs} ways, γ in 2^{rs} ways and δ in 2^{2s^2} ways. Thus, Y can be chosen $2^{(r+s)^2+s^2} = 2^{k^2+(n-k)^2}$ ways.

Case 2: Let X be similar to D_k.

Then, there is an S in $G_n(2)$ such that

$$X = S^{-1}D_kS \pmod 2.$$

i.e. $$SXS^{-1} = D_k \pmod 2.$$

By Case (i), SXS^{-1} has $2^{k^2+(n-k)^2}$ extensions to

$T_k(4)$. i.e. X has $2^{k^2+(n-k)^2}$ extensions to $T_k(4)$.

This proves (i).

Proof of (ii). By (i) each element of $T_k(2)$ has $2^{k^2+(n-k)^2}$ extensions to $T_k(4)$. Hence, the result follows.

Proof of (iii). Recall that $S_n(4) = \bigcup_{\frac{n}{2} \le k \le n} T_k(4)$.

Therefore, $$s_n(4) = \sum_{\frac{n}{2} \le k \le n} |T_k(4)|$$

$$= \sum_{\frac{n}{2} \le k \le n} 2^{k^2+(n-k)^2} |T_k(2)|.$$

Hence, the proof of the theorem is complete.

For developing our theory further, we adapt the following notations in this section:

Let $F_k^{(1)}(2) = M_r(2)$,

$F_k^{(2)}(2) = \{\beta : \beta$ is a $r \times 2s$ matrix over Z_2 with all odd columns as zeros$\}$,

$F_k^{(3)}(2) = \{\gamma : \gamma$ is a $2s \times r$ matrix over Z_2 with all even rows as zeros$\}$

$F_k^{(4)}(2) = \{\delta : \delta$ is a $2s \times 2s$ matrix over Z_2 with the form given in (4.8)$\}$

and $$F_k(2) = \left\{\begin{pmatrix} P_1 & P_2 \\ P_3 & P_4 \end{pmatrix} : P_i \in F_k^{(i)}(2),\ 1 \le i \le 4\right\}$$

Note that $|F_k^{(1)}(2)| = 2^{r^2}$, $|F_k^{(2)}(2)| = |F_k^{(3)}(2)| = 2^{rs}$,

$|F_k^{(4)}(2)| = 2^{2s^2}$, and $|F_k(2)| = 2^{(r+s)^2+s^2} = 2^{k^2+(n-k)^2}$

The extension of a matrix in $T_k(2)$ to a matrix in $T_k(4)$ is established in the last theorem. Any extension of D_k in $T_k(2)$ to $T_k(4)$ is of the form $D_k(4) + 2Q$ with Q in $F_k(2)$, and any extension of $S^{-1}D_kS \pmod 2$ in $T_k(2)$ to $T_k(4)$ is of the form $S^{-1}(D_k(4) + 2Q)S \pmod 4$ with Q in $F_k(2)$.

Proposition 4.3.11

Let $Q = \left(\begin{array}{c|c} P_1 & P_2 \\ \hline P_3 & P_4 \end{array}\right)$ be in $F_k(2)$. Then, $D_k(4) + 2Q$ is similar to $D_k(4) + 2Q_1$ where $Q_1 = \left(\begin{array}{c|c} P_1 & 0 \\ \hline 0 & 0 \end{array}\right) \pmod 2$.

Proof

We want to show that there is an R in $G_n(4)$ such that

$$R^{-1}(D_k(4) + 2Q)R = D_k(4) + 2Q_1 \pmod 4 \quad \ldots\ldots (4.9)$$

It is sufficient to show that there exists an X in $M_n(2)$ so that $R = I + 2X \pmod 4$ and satisfies (4.9). First observe that if $R = I + 2X \pmod 4$, then $R^{-1} = I + 2X \pmod 4$. Therefore, (4.9) is equivalent to

$$(D_k(4) + 2Q)R = R(D_k + 2Q_1) \pmod 4$$

i.e. $D_k(4) + 2D_k(4)X + 2Q = (D_k(4) + 2XD_k(4) + 2Q_1) \pmod 4$

i.e. $D_k(4)X + Q = XD_k(4) + Q_1 \pmod 2$

i.e. $D_kX + Q = XD_k + Q_1 \pmod 2$

i.e. $D_kX + XD_k = Q + Q_1 \pmod 2$

$$= \left(\begin{array}{c|c} 0 & P_2 \\ \hline P_3 & P_4 \end{array}\right) \pmod 2 \quad \ldots\ldots\ldots\ldots (4.10)$$

We claim that such an X satisfying (4.10) exists.

Recall that if W is the direct sum of s matrices of the form $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and if $U = \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & W \end{array}\right)$, then $D_k = I_n + U$. Then, (4.10) is equivalent to

$$XU + UX = \left(\begin{array}{c|c} 0 & P_2 \\ \hline P_3 & P_4 \end{array}\right) \pmod 2 \quad \ldots\ldots\ldots (4.11)$$

Let $X = \left(\begin{array}{c|c} X_1 & X_2 \\ \hline X_3 & X_4 \end{array}\right)$ where X_1 is $r \times r$ matrix, X_2 is $r \times 2s$ matrix, X_3 is $2s \times r$ matrix, and X_4 is $2s \times 2s$ matrix over Z_2. Then, (4.11) gives

$$X_2 W = P_2 \pmod 2 \quad \ldots\ldots\ldots\ldots (4.12)$$

$$WX_3 = P_3 \pmod 2 \quad \ldots\ldots\ldots\ldots (4.13)$$

$$X_4 W + WX_4 = P_4 \pmod 2 \quad \ldots\ldots\ldots\ldots (4.14)$$

Recalling the structure P_2, P_3, P_4, it is easy to see that X_2, X_3, X_4 exist, and X_1 is arbitrary. Hence, the proposition is proved.

Corollary 4.3.12

Every element in $T_k(4)$ is similar to the $D_k(4) + 2P \pmod 4$ for some P in $F_k(2)$ with

$$P = \left(\begin{array}{c|c} P_1 & 0 \\ \hline 0 & 0 \end{array}\right) \pmod 2.$$

Proof

The proof follows from the above proposition and the following two observations:

(i) An extension of D_k in $T_k(2)$ to $T_k(4)$ is of the from $D_k(4) + 2Q$ with Q in $F_k(2)$.

(ii) If $X = S^{-1}D_kS \pmod 2$, then any extension of X to $T_k(4)$ is of the form $S^{-1}(D_k(4) + 2Q)S^{-1} \pmod 4$ with Q in $F_k(2)$.

Example 4.3.13

Let $m = 2$ and $n = 2$. Then, $T_k(2)$ is not empty if and only if $1 \leq k \leq 2$. If $k = 1$, then $s = 1$ and $r = 0$, $K_{2s} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \pmod 2$, and $D_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. But, $T_1(2)$ contains all matrices which are similar to D_1. Hence, $T_1(2) = \left\{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right\}$. If $k = 2$, then $r = 2$, $s = 0$, and $D_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Hence, $T_2(2) = \left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$.

Consider the extensions of elements in $T_1(2)$ to $T_1(4)$. Extensions of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ are of the form $\begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix} + 2\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \pmod 4$, extensions of $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ are of the form $\begin{pmatrix} 3 & 0 \\ 1 & 1 \end{pmatrix} + 2\begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \pmod 4$, and extensions of $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ are $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 3 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \pmod 4$, where a, b are arbitrary in Z_2. In total, there are 12 matrices, and hence $|T_1(4)| = 12$.

Consider the extensions of elements in $T_2(2)$ to $T_2(4)$. Since $k = 2$, we have $r = 2$ and $s = 0$. Thus, the extensions of $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ are of the form $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 2\begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod 4$ with a,b,c,d arbitrary in Z_2. There are 16 such matrices.

Thus, $s_2(4) = 12 + 16 = 28$. This agrees with the result for $s_2(4)$ obtained by the listing of $S_2(4)$ preceding Lemma 4.3.2, and hence illustrates that our extension is correct. In fact, the extension is correct and can be verified for all values.

Although our method of extension is quite similar to our earlier method, we remark that all matrices in $T_k(2)$ extendable to matrices in $T_k(4)$, whereas not all matrices in $T_k(4)$ will have an extension in $T_k(8)$. For example, if $k = n$, the identity I in $T_k(2)$ has extensions in $T_k(4)$ which are of the form $I + 2Q \pmod 4$ with Q arbitrary in $M_n(2)$. Any extension of this to $T_k(8)$ must be of the form $I + 2Q + 4R \pmod 8$ with R in $M_n(2)$, and $(I + 2Q + 4R)^2 = I \pmod 8$.

i.e. $I^2 + 4Q^2 + 16R^2 + 4Q + 8R + 8(QR + RQ) = I \pmod 8$.

i.e. $4(Q^2 + Q) = 0 \pmod 8$.

i.e. $Q^2 + Q = 0 \pmod 2$.

i.e. $Q^2 = Q \pmod 2$.

Thus, if Q^2 is not equal to $Q \pmod 2$, then $I + 2Q \pmod 4$ in $T_k(4)$ does not have an extension to $T_k(8)$. Below, we give a necessary and sufficient condition for an element in $T_k(4)$ to have an extension in $T_k(8)$.

Proposition 4.3.14

Let $\frac{n}{2} \leq k \leq n$. Then,

(i) The matrix $D_k(4) + 2P$ in $T_k(4)$ with $P = \left(\begin{array}{c|c} P_1 & 0 \\ \hline 0 & 0 \end{array}\right)$ in $F_k(2)$ has an extension to $T_k(8)$ if and only if $P_1^2 = P_1 \pmod 2$, and the extensions are of the form $D_k(8) + 2P + 4Q \pmod 8$ with Q in $F_k(2)$.

(ii) If $X = S^{-1}(D_k(4) + 2P)S \pmod 4$ in $T_k(4)$, with $P = \left(\begin{array}{c|c} P_1 & 0 \\ \hline 0 & 0 \end{array}\right)$ in $F_k(2)$, then X has extension to $T_k(8)$ if and only if $P_1^2 = P_1$ and the extension is of the form $S^{-1}(D_k(8) + 2P + 4Q)S \pmod 8$ with Q in $F_k(2)$.

(iii) If an element X in $T_k(4)$ has an extension to $T_k(8)$, then it has $2^{k^2+(n-k)^2}$ extensions.

Proof

Let $X = D_k(4) + 2P \pmod 4$ and Y be an extension of X to $T_k(8)$. Then, $Y = X + 4Q_1 \pmod 8$, with Q_1 in $M_n(2)$. i.e., $Y = D_k(4) + 2P + 4Q \pmod 8 = D_k(8) + 2P + 4Q \pmod 8$ with Q in $M_n(2)$. Since $Y^2 = I \pmod 8$, we have

$$D_k^2 + 4P^2 + 2(PD_k + D_kP) + 4(D_kQ + QD_k) = I \pmod 8 \quad \ldots\ldots\ldots (4.15)$$

But $D_k^2 = I \pmod 8$, and $PD_k + D_kP = 2P \pmod 8$

Therefore, (4.15) gives

$$4(P^2 + P) + 4(D_kQ + QD_k) = 0 \pmod 8$$

i.e. $$P^2 + P + D_kQ + QD_k = 0 \pmod 2 \quad \ldots\ldots\ldots(41.6)$$

Let $Q = \left(\begin{array}{c|c} Q_1 & Q_2 \\ \hline Q_3 & Q_4 \end{array}\right)$ where Q is $r \times r$ matrix, Q_2 is $r \times 2s$ matrix, Q_3 is $2s \times r$ matrix, and Q_4 is $2s \times 2s$ matrix over Z_2.

Then, $D_kQ + QD_k = \left(\begin{array}{c|c} 0 & Q_2W \\ \hline WQ_3 & WQ_4 + Q_4W \end{array}\right) \pmod 2$ where W is the direct sum of s matrices of the form $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Further, since $P = \left(\begin{array}{c|c} P_1 & 0 \\ \hline 0 & 0 \end{array}\right)$ we have $P^2 = \left(\begin{array}{c|c} P_1^2 & 0 \\ \hline 0 & 0 \end{array}\right)$. Hence, from (4.16) we have $\left(\begin{array}{c|c} P_1^2 + P_1 & Q_2W \\ \hline Q_3W & WQ_4 + Q_4W \end{array}\right) = 0 \pmod 2$, and Q_1 is arbitrary.

This gives that $P_1^2 + P_1 = 0 \pmod 2$, and $Q \in F_k(2)$. Thus proof of (i) is complete.

(ii) If $X = S^{-1}(D_k + 2P)S$, then $SXS^{-1} = D_k + 2P \pmod 4$.

Now, X has an extension to $T_k(8)$ if and only if $SXS^{-1} = D_k + 2P$ has an extension to $T_k(8)$, and this happens if and only if $P_1^2 = P_1 \pmod 2$. By (i), any extension of SXS^{-1} is of the form $D_k(8) + 2P + 4Q \pmod 8$ with Q in $F_k(2)$. Hence, the extension of X

is of the form $S^{-1}(D_k(8) + 2P + 4Q)S \pmod 8$ with Q in $F_k(2)$.

(iii) Follows from the fact that $|F_k(2)| = 2^{k^2+(n-k)^2}$.

The proposition of proved.

The following theorem gives an expression for $s_n(8)$.

Theorem 4.3.15

Let ℓ_r denote the number of matrices P_1 in $M_r(2)$ with the property that $P_1^2 = P_1 \pmod 2$. We let $\ell_0 = 1$. Then, $|T_k(8)| = 2^{n^2}\ell_r |T_k(2)|$. Consequently,

$$s_n(8) = \sum_{\frac{n}{2} \le k \le n} 2^{n^2}\ell_{2k-n}|T_k(2)|.$$

Proof

The matrix $D_k(2)$ in $T_k(2)$ has $2^{k^2+(n-k)^2}$ extensions in $T_k(4)$. These extensions are similar to $D_k(4) + 2P \pmod 4$ with $P = \left(\begin{array}{c|c} P_1 & 0 \\ \hline 0 & 0 \end{array}\right)$ in $F_k(2)$. For given P_1, there are $2^{rs}\cdot 2^{rs} + 2^{s^2} = 2^{2s(r+s)} = 2^{2(n-k)k}$ matrices which are similar to $D_k(4) + 2P \pmod 4$. If $P_1^2 = P_1 \pmod 2$, then each of these matrices in $T_k(4)$ has $2^{k^2+(n-k)^2}$ extensions to $T_k(8)$. Thus, if ℓ_r is the number of P_1 such that $P_1^2 = P_1 \pmod 2$, then element $D_k(2)$ in $T_k(2)$ has $2^{2k(n-k)}\cdot 2^{k^2+(n-k)^2}\cdot \ell_r = 2^{n^2}\ell_r$ extensions to $T_k(8)$. Since

all the elements in $T_k(2)$ are similar to $D_k(2)$, we have

$T_k(8) = 2^{n^2} \ell_r |T_k(2)|$ where $r = 2k - n$. Further, since

$S_n(8) = \bigcup_{\frac{n}{2} \le k \le n} T_k(8)$, we have $s_n(8) = \sum_{\frac{n}{2} \le k \le n} 2^{n^2} \ell_{2k-n} |T_k(2)|$.

Hence, the proof is complete.

Example 4.3.16

Let $m = 8$ and $n = 2$. Then, $k = 1$ or 2 and $r = 0$ or 2 accordingly. We know $\ell_0 = 1$. Let us calculate ℓ_2.

Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod 2$ be such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod 2$. i.e.,

$$a^2 + bc = a \pmod 2$$
$$(a + d)b = b \pmod 2$$
$$(a + d)c = c \pmod 2$$
$$d^2 + bc = d \pmod 2$$

This has the following 8 solutions.

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

Thus, $\ell_2 = 8$.

Hence, $|T_2(8)| = 2^4 \cdot 8 \cdot |T_2(2)|$

$= 2^4 \cdot 8$

$|T_1(8)| = 2^4 \cdot \ell_0 |T_1(2)|$

$= 2^4 \cdot 3$

Therefore, $s_2(8) = 11 \cdot 2^4$.

The following proposition for $m = 8$ can be proved in a manner similar to Proposition 4.3.11 and Corollary 4.3.12.

Proposition 4.3.17

Let $\frac{n}{2} \leq k \leq n$. Then,

(i) The matrix $D_k(8) + 2P + 4Q \pmod 8$ where $P = \left(\begin{array}{c|c} P_1 & 0 \\ \hline 0 & 0 \end{array}\right)$ in $F_k(2)$ with $P_1^2 = P_1 \pmod 8$, and $Q = \left(\begin{array}{c|c} Q_1 & Q_2 \\ \hline Q_3 & Q_4 \end{array}\right)$ in $F_k(2)$, is similar to $D_k(8) + 2P + 4Q' \pmod 8$ where $Q' = \left(\begin{array}{c|c} Q_1 & 0 \\ \hline 0 & 0 \end{array}\right)$ in $F_k(2)$.

(ii) Any matrix in $T_k(8)$ is similar to $D_k(8) + 2P + 4Q \pmod 8$ where $P = \left(\begin{array}{c|c} P_1 & 0 \\ \hline 0 & 0 \end{array}\right)$, $Q = \left(\begin{array}{c|c} Q_1 & 0 \\ \hline 0 & 0 \end{array}\right)$ in $F_k(2)$ and $P_1^2 = P_1 \pmod 2$.

The following theorem gives necessary and sufficient conditions for the extension from $T_k(2^t)$ to $T_k(2^{t+1})$, $t \geq 2$.

Theorem 4.3.18

Let $t \geq 2$, and $\frac{n}{2} \leq k \leq n$. Let $X = D_k(2^{t+1}) + \sum_{i=1}^{t-1} 2^i P_i \pmod{2^t}$ be in $T_k(2^t)$ with $P_i = \left(\begin{array}{c|c} \alpha_i & 0 \\ \hline 0 & 0 \end{array}\right)$ where α_i is in $M_r(2)$ for $1 \leq i \leq t-1$. Then,

(i) X has an extension to $T_k(2^{t+1})$ if and only if

$$\sum_{i=1}^{\ell} 2^{i-1} P_i + \sum_{i=1}^{\ell} \sum_{j=1}^{\ell} 2^{i+j-2} P_i P_j = 0 \pmod{2^\ell} \quad \ldots (4.17)$$

for $\ell = 1, 2, \ldots, (t-1)$.

(ii) If X has an extension to $T_k(2^{t+1})$, then it is of the form $X + 2^t Q \pmod{2^{t+1}}$ with $Q = \left(\begin{array}{c|c} Q_1 & Q_2 \\ \hline Q_3 & Q_4 \end{array}\right)$ in $F_k(2)$ and is similar to $X + 2^t Q' \pmod{2^{t+1}}$ where

$$Q' = \left(\begin{array}{c|c} Q_1 & 0 \\ \hline 0 & 0 \end{array}\right) \text{ in } F_k(2).$$

Proof

We prove using induction on t.

Propositions 4.3.14 and 4.3.17 give the theorem for $t = 2$.

Assume the result holds for the extension from $T_k(2^{t-1})$ to $T_k(2^t)$. i.e., we have proved,

$Y = D_k(2^{t-1}) + \sum_{i=1}^{t-2} 2^i P_i \pmod{2^{t-1}}$ has an extension to $T_k(2^t)$ iff

$$\sum_{i=1}^{\ell} 2^{i-1} P_i + \sum_{i=1}^{\ell} \sum_{j=1}^{\ell} 2^{i+j-2} P_i P_j = 0 \bmod 2^{\ell}$$

for $\ell = 1,2,\ldots,t-2$ .....(4.18)

Now, let $X = D_k(2^t) + \sum_{i=1}^{t-1} 2^i P_i \pmod{2^t}$ be in $T_k(2^t)$.

Then, $X \pmod{2^{t-1}}$ is in $T_k(2^{t-1})$. Hence, by induction, hypothesis (4.18) holds. Therefore, we are left with proving (4.17) for $\ell = t - 1$.

Any extension of X to $T_k(2^{t+1})$ is of the form

$X + 2^t(Q'')$ for some Q'' in $M_n(2)$. i.e., of the form

$$D_k(2^t) + \sum_{i=1}^{t-1} 2^i P_i + 2^t Q'' \pmod{2^{t+1}}$$

$$= D_k(2^{t+1}) + \sum_{i=1}^{t-1} 2^i P_i + 2^t Q \quad \text{where}$$

$Q = Q'' - \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & I_{n-k} \end{array}\right) \pmod 2$. Since this extension is in $S_n(2^{t+1})$, we have $\left(D_k(2^{t+1}) + \sum_{i=1}^{t-1} 2^i P_i + 2^t Q\right)^2 = I \pmod{2^{t+1}}$.

We write D_k for $D_k(2^{t+1})$ with no ambiguity. Then,

$$D_k^2 + \sum_{i=1}^{t-1} 2^i (D_k P_i + P_i D_k) + 2^t (D_k Q + Q D_k)$$

$$+ \left(\sum_{i=1}^{t-1} 2^i P_i\right)\left(\sum_{i=1}^{t-1} 2^i P_i\right) + 2^{2t} Q^2 + \sum_{i=1}^{t-1} 2^{i+t} (P_i Q + Q P_i)$$

$$= I \pmod{2^{t+1}},$$

i.e.
$$I + \sum_{i=1}^{t-1} 2^i (D_k P_i + P_i D_k) + 2^t (D_k Q + Q D_k)$$

$$+ \sum_{i=1}^{t-1} \sum_{j=1}^{t-1} 2^{i+j} P_i P_j + 0 + 0 = I \pmod{2^{t+1}}.$$

Since $P_i = \left(\begin{array}{c|c} \alpha_i & 0 \\ \hline 0 & 0 \end{array}\right)$ and $D_k = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & k_{2s} \end{array}\right)$, we have $D_k P_i = P_i$

and $P_i D_k = P_i$. Hence, we have

$$\sum_{i=1}^{t-1} 2^{i+1} P_i + 2^t (D_k Q + Q D_k) + \sum_{i=1}^{t-1} \sum_{j=1}^{t-1} 2^{i+j} P_i P_j \equiv 0 \pmod{2^{t+1}}.$$

i.e. $\sum_{i=1}^{t-1} 2^{i-1} P_i + 2^{t-2}(D_k Q + Q D_k) + \sum_{i=1}^{t-1}\sum_{j=1}^{t-1} 2^{i+j-2} P_i P_j = 0$

$$\pmod{2^{t-1}} \quad \ldots\ldots\ldots (4.19)$$

We claim that $2^{t-2}(D_k Q + Q D_k) = 0 \pmod{2^{t-1}}$.

For, if $Q = \left(\begin{array}{c|c} Q_1 & Q_2 \\ \hline Q_3 & Q_4 \end{array}\right)$ then $D_k Q + Q D_k = \left(\begin{array}{c|c} 2Q_1 & Q_2 + Q_2 K_{2s} \\ \hline K_{2s} Q_3 + Q_3 & K_{2s} Q_4 + Q_4 K_{2s} \end{array}\right)$

Therefore, $2^{t-2}(D_k Q + Q D_k) = 2^{t-2}\left(\begin{array}{c|c} 0 & Q_2 + Q_2 K_{2s} \\ \hline K_{2s} Q_3 + Q_3 & K_{2s} Q_4 + Q_4 K_{2s} \end{array}\right)$

$$\pmod{2^{t-1}} \quad \ldots\ldots\ldots (4.20)$$

Further, all P_i are of the form $\left(\begin{array}{c|c} \alpha_i & 0 \\ \hline 0 & 0 \end{array}\right)$. Hence, from (4.19) and (4.20), we have

$$\sum_{i=1}^{t-1} 2^{i-1} P_i + \sum_{i=1}^{t-1}\sum_{j=1}^{t-1} 2^{i+j-2} P_i P_j = 0 \pmod{2^{t-1}} \quad \ldots\ldots (4.21)$$

and

$$\left.\begin{array}{l} Q_1 \text{ is arbitrary in } M_r(2), \\ Q_2 + K_{2s} Q_2 = 0 \pmod 2, \\ K_{2s} Q_3 + Q_3 = 0 \pmod 2, \\ K_{2s} Q_4 + Q_4 K_{2s} = 0 \pmod 2. \end{array}\right\} \quad \ldots\ldots\ldots (4.22)$$

(4.21) is condition (4.17) for $\ell = t^* - 1$. The set of equations in (4.22) implies, Q_2 is in $F_k^{(2)}(2)$, Q_3 is in $F_k^{(2)}(2)$ and Q_4 is in $F_k^{(4)}(2)$. Hence, Q is in $F_k(2)$.

Sufficiency follows similarly.

(ii) While proving (i), we have proved that any extension of X is of the form $X + 2^t Q \pmod{2^{t+1}}$ with Q in $F_k(2)$. The similarity property can be proved as in the proof of Proposition 4.3.11 with the help of induction.

Corollary 4.3.19

Matrices in $T_k(2^{t+1})$ are similar to one of the matrices of the form $D_k(2^{t+1}) + \sum_{i=1}^{t} 2^i P_i \pmod{2^{t+1}}$ with $P_i = \left(\begin{array}{c|c} \alpha_i & 0 \\ \hline 0 & 0 \end{array}\right)$ and α_i in $M_r(2)$ for all $i = 1,2,\ldots,t$, and $\sum_{i=1}^{\ell} 2^{i-1} P_i + \sum_{i=1}^{\ell} \sum_{j=1}^{\ell} 2^{i+j-2} P_i P_j = 0 \pmod{2^{\ell}}$ for $\ell = 1,2,\ldots,t-1$.

Proof

For t = 0, the result is well known. For t = 1, the result is given by Proposition 4.3.11. For t = 2, it is Proposition 4.3.11. From the above theorem and induction on t, the result follows for any $t \geq 2$.

Remark 4.3.20

The condition given in Theorem 4.3.18 (i) makes the calculation of $|T_k(2^{t+1})|$, $t \geq 2$, very hard. In general, the choice of P_2 depends on the choice of P_1, choice of P_3 depends on the choices of P_1 and P_2, etc. Further, for each choice of P_1 there may be many choices of P_2, for each choice of the pair (P_1,P_2) there may be many choices of P_3, and so

on. However, it is interesting to note that if P_1 is the zero matrix then all the P_i's are zero matrices, and if P_1 is the identity matrix then all the P_i's are identity matrices. The proof is given below:

Proposition 4.3.21

Let P_i in $M_r(2)$ $i = 1,2,\ldots,(t-1)$ satisfy the condition $\sum_{i=1}^{\ell} 2^{i-1}P_i + \sum_{i=1}^{\ell}\sum_{j=1}^{\ell} 2^{i+j-2}P_iP_j = 0 \pmod{2^{\ell}}$ for $\ell = 1,2,\ldots,t-1$.

Then,

(a) if $P_1 = 0$, then $P_i = 0$ for all i such that $1 \leq i \leq t-1$,

and (b) if $P_1 = I_r$, the $r \times r$ identity matrix, then $P_i = I_r$ for all i such that $1 \leq i \leq t-1$.

Proof

We will use induction to prove the result.

(a) Let $\ell = 1$ in the condition. Then, we have $P_1^2 = P_1 \pmod 2$ and this is satisfied by $P_1 = 0 \pmod 2$. Let $\ell = 2$ in the condition. Then, we have $P_1 + 2P_2 + P_1^2 + 2P_1P_2 + 2P_2P_1 + 4P_2^2 = 0 \pmod 4$. i.e. $P_1 + 2(P_2 + P_1P_2 + P_2P_1) + P_1^2 = 0 \pmod 4$. If $P_1 = 0$, then $2P_2 = 0 \pmod 4$. i.e. $P_2 = 0 \pmod 2$.

Assuming that we have proved $P_i = 0$ for $i = 1,2,\ldots,(\ell-1)$, we will prove that $P_\ell = 0$. If we use the fact $P_i = 0$ for $1 \leq i \leq (\ell-1)$, the condition reduces to $2^{\ell-1}P_\ell + 2^{\ell+\ell-2}P_\ell^2 = 0 \pmod{2^{\ell}}$.

i.e. $2^{\ell-1}P_\ell + 2^{2(\ell-1)}P_\ell^2 = 0 \pmod{2^\ell}$.

i.e. $2^{\ell-1}P_\ell + 0 = 0 \pmod{2^\ell}$ as $\ell \geq 2$.

i.e. $P_\ell = 0 \pmod 2$. i.e., $P_\ell = 0$.

Hence, (a) is proved.

(b) Let $\ell = 1$ in the condition. We get, $P_1^2 = P_1 \pmod 2$ and $P_1 = I$ satisfies this equation. Let $\ell = 2$ in the condition. Then, $P_1 + P_1^2 + 2(P_2 + P_1P_2 + P_2P_1) = 0 \pmod 4$. If $P_1 = I$, then $I + I + 2(3P_2) = 0 \pmod 4$. i.e. $I + P_2 = 0 \pmod 2$, which implies $P_2 = I \pmod 2$.

Assuming that we have proved that $P_i = I$, $1 \leq i \leq \ell - 1$, we will prove that $P_\ell = I$. If we use the fact $P_i = I$, then the condition reduces to

$$\sum_{i=1}^{\ell-1} 2^{i-1}I + 2^{\ell-1}P_\ell + \sum_{i=1}^{\ell-1}\sum_{j=1}^{\ell-1} 2^{i+j-2}I + \sum_{i=1}^{\ell-1} 2^{i+\ell-2}P_\ell + \sum_{j=1}^{\ell-1} 2^{j+\ell-2}P_\ell + 2^{2\ell-2}P_\ell^2 = 0 \pmod{2^\ell}.$$

i.e. $(2^{\ell-1} - 1)I + 2^{\ell-1}P_\ell + (2^{\ell-1} - 1)^2 I + 2^\ell(2^{\ell-1} - 1)P_\ell = 0 \pmod{2^\ell}$.

i.e. $2^{\ell-1}((2^{\ell-1} - 1)I + P_\ell) = 0 \pmod{2^\ell}$

i.e. $(2^{\ell-1} - 1)I + P_\ell = 0 \pmod 2$.

i.e. $P_\ell = I \pmod 2$. Hence, (b) is proved and the proof of the proposition is complete.

Remark 4.3.22

Note that in Theorem 4.3.10 we have shown that $|T_k(4)| = 2^{k^2+(n-k)^2}|T_k(2)|$. While extending our results

(1)

from $T_k(4)$ to $T_k(8)$, we have proved that every extension is similar to $D_k(8) + 2P_1 + 2P_2 \pmod 8$ where $P_i = \left(\begin{array}{c|c} \alpha_i & 0 \\ \hline 0 & 0 \end{array}\right)$ with α_i is in $M_r(2)$, $i = 1,2$ such that $P_1^2 = P_1 \pmod 2$. It seems complicated to enumerate all such matrices P_1 satisfying the above condition. Even if an enumeration for $m = 8$ is possible, the nonlinear matrix equations (4.17) seem formidable to solve and enumerate exactly, for higher values of t. However, it is easy to see that $P_1 = 0$ (hence $P_i = 0$ for all i) and $P_1 = \left(\begin{array}{c|c} I & 0 \\ \hline 0 & 0 \end{array}\right)$ (hence $P_i = \left(\begin{array}{c|c} I & 0 \\ \hline 0 & 0 \end{array}\right)$ for all i) are two extreme solution.

Further, for fixed $P = \left(\begin{array}{c|c} \alpha & 0 \\ \hline 0 & 0 \end{array}\right)$ with α in $M_r(2)$, there are $2^{2k(n-k)}$ matrices, which are similar to $D_k(2^{t+1}) + \sum_{i=1}^{t-1} 2^i P_i + 2^t P \pmod{2^{t+1}}$, where $P_i = \left(\begin{array}{c|c} \alpha_i & 0 \\ \hline 0 & 0 \end{array}\right)$ with α_i in $M_r(2)$ for $i = 1,2,\ldots,t-1$, and satsify the condition (4.17). Therefore, we have the following results.

$$|T_k(8)| \geq 2 \cdot 2^{2k(n-k)} |T_k(2)|,$$

$$|T_k(16)| \geq 2 \cdot 2^{2 \cdot 2k(n-k)} |T_k(2)|,$$

$$\vdots \qquad\qquad \vdots$$

$$|T_k(2^t)| \geq 2 \cdot 2^{(t-2) \cdot 2k(n-k)} |T_k(2)| \text{ for } t \geq 3.$$

Consequently, $|s_n(2^t)| \geq 2 \sum_{\frac{n}{2} \leq k \leq n} 2^{(t-2)2k(n-k)} |T_k(2)|$.

Let us summarize the main results of this section in the following theorem:

Theorem 4.2.23

Let n and t be positive integers, and $S_n(2^t)$ be the set of all $n \times n$ matrices A over Z_{2^t} such that $A^2 = I \pmod{2^t}$. Let $T_k(2)$, for $0 \leq k \leq n$, denote the set of all the matrices A in $S_n(2)$ with dimension of the eigen space corresponding to 1 as k. $T_k(2^t)$ is a subset of $S_n(2^t)$ such that a matrix A is in $T_k(2^t)$ if and only if A $(\text{mod } 2^{t-1})$ is in $T_k(2^{t-1})$, $t \geq 2$. Then, the following are true:

(i) If $0 \leq k < \frac{n}{2}$, then $T_k(2^t)$ is empty for all $t \geq 1$.

(ii) $|T_k(2)| = \dfrac{g_n(2) \cdot |GL(n-k,k)|}{g_k(2) \cdot g_{n-k}(2) 2^{k(n-k)}}$ where $GL(n-k,k)$ is set of all $(n-k) \times k$ matrices of rank $(n-k)$.

(iii) $|S_n(2)| = \sum_{\frac{n}{2} \leq k \leq n} |T_k(2)|$.

(iv) $|S_n(4)| = \sum_{\frac{n}{2} \leq k \leq n} 2^{k^2+(n-k)^2} |T_k(2)|$

(v) $|S_n(2^t)| \geq 2 \cdot \sum_{\frac{n}{2} \leq k \leq n} 2^{(t-2)2k(n-k)} |T_k(2)|$, for $t \geq 3$.

Since the proofs given here are all constructive, they are extremely helpful in generating a matrix in $S_n(m)$. It would be interesting to know the exact value of $s_n(2^t)$

for $t \geq 3$. Theorem 4.3.18 can be taken as the first step in this direction. In the next chapter, we would give the structure of $S_2(2^t)$, and hence the exact value of $s_2(2^t)$.

CHAPTER V

Structure of Matrices in $S_2(m)$

For an odd prime p, the structure of the matrices in $T_k(p^t)$, $t \geq 1$, is given in Theorem 4.2.6. Also Theorem 4.2.7 gives the number of matrices in $S_n(p^t)$. When $p = 2$, the major results are summarized in Theorem 4.2.23. However, we do not have the exact number of matrices in $S_n(2^t)$ for $t \geq 3$. In this chapter we discuss the special case $n = 2$, and compute $s_2(p^t)$ for any prime p (even or odd), by characterizing the structure of matrices in $S_2(p^t)$.

Section 5.1 deals with the classification of matrices in $S_2(p^t)$ based on certain structure, for an odd prime p and $t \geq 1$ (see Theorem 5.1.2). Section 5.2 deals with the same when $p = 2$. As a consequence we derive the exact value of $s_2(2^t)$, $t \geq 1$ (see Theorem 5.2.5). In section 5.3, we comment on some significant results when $m = 2p$ and $n = 2$, where p is an odd prime.

5.1 Structure of matrices in $S_2(p^t)$, $t \geq 1$, $p > 2$

Throughout this section, let p denote an odd prime, $m = p^t$ with $t \geq 1$, and $n = 2$. The main result concerning the number of 2×2 matrices A satisfying the equation $A^2 = I \pmod{p^t}$ is contained in the results of section 4.2. The structure that we obtain in Theorem 5.1.2 for such matrices, will be helpful for practical purposes.

As $n = 2$, an $n \times n$ matrix A over Z_{p^t} can be written in the form $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with a,b,c,d in Z_{p^t}. Since $A^2 = I \pmod{p^t}$, we have

$$a^2 + bc = 1 \pmod{p^t} \quad \ldots\ldots\ldots\ldots\ldots (5.1)$$

$$(a + d)b = 0 \pmod{p^t} \quad \ldots\ldots\ldots\ldots\ldots (5.2)$$

$$(a + d)c = 0 \pmod{p^t} \quad \ldots\ldots\ldots\ldots\ldots (5.3)$$

$$d^2 + bc = 1 \pmod{p^t} \quad \ldots\ldots\ldots\ldots\ldots (5.4)$$

This system of four equations will be referred to as the primary system of equations. We begin with a lemma.

Lemma 5.1.1

The primary system of equations imply that $a = \pm d \pmod{p^t}$.

Proof

From (5.1) and (5.4) we have $a^2 = d^2 \pmod{p^t}$. i.e., $(a - d)(a + d) \equiv o \pmod{p^t}$. Hence, there are integers k, ℓ, r, s with $r \geq 0$, $s \geq 0$, $r + s \geq t$, k and ℓ are relatively prime to p such that

$$a + d = kp^r \quad \ldots\ldots\ldots\ldots\ldots (5.5)$$

$$a - d = \ell p^s \quad \ldots\ldots\ldots\ldots\ldots (5.6)$$

We claim that either $r \geq t$ or $s \geq t$. To prove the claim, let us assume that both $r < t$ and $s < t$. If $r = 0$, then $r + s \geq t$ implies that $s \geq t$. Similarly, if $s = 0$ then $r \geq t$. Therefore, let $0 < r < t$, and $0 < s < t$. Using (5.5) in (5.2) and (5.3), we get $b = xp^{t-r}$ and $c = yp^{t-r}$ for some integers x and y. Further, from (5.5) and (5.6),

$2a = kp^r + \ell p^s$. Therefore,

$$4(a^2 + bc) = (2a)^2 + 4bc$$
$$= k^2p^{2r} + \ell^2p^{2s} + 2k\ell p^{r+s} + 4xyp^{2t-2r}.$$

Reducing this to (mod p^t), and using (5.1) and the fact that $r + s \geq t$, we have

$$4 = k^2p^{2r} + \ell^2p^{2s} + 4xyp^{2t-2r} \pmod{p^t}.$$

Since $0 < r, s < t$, the expression on the right is divisible by p, and hence does not have an inverse in Z_{p^t}. But the element 4 on the left is invertible in Z_{p^t}, a contradiction. Therefore, our assumption that both $r < t$ and $s < t$ is incorrect. Therefore, either $r \geq t$ or $s \geq t$. Hence, the claim is proved.

If $r \geq t$ then $a = -d \pmod{p^t}$, and if $s \geq t$ then $a = d \pmod{p^t}$. In either case, we have $a = \pm d \pmod{p^t}$. Hence, the lemma is proved.

Next, we give a classification of matrices in $S_2(p^t)$.

Theorem 5.1.2

Let p be an odd prime, and $t \geq 1$. Then,

(i) Elements of $S_2(p^t)$ can be classified into two distinct types.

$$\text{type 1} = \left\{\begin{pmatrix} a & b \\ c & -a \end{pmatrix} : a^2 + bc = 1 \pmod{p^t}\right\},$$

and $$\text{type 2} = \left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a = \pm 1 \pmod{p^t}\right\}.$$

(ii) There are $p^{2t-1}(p + 1)$ matrices in type 1, and 2 matrices in type 2. Hence, $s_2(p^t) = p^{2t-1}(p + 1) + 2$.

Proof

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $S_2(p^t)$. By Lemma 5.1.1, $a = \pm d \pmod{p^t}$. We prove the first part of the theorem by discussing these two cases separately.

Case (i) Let $a = -d \pmod{p^t}$.

Then, from the primary equations we get b and c are arbitrary such that $a^2 + bc = 1 \pmod{p^t}$. Therefore, the matrix must be of the form $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ with $a^2 + bc = 1 \pmod{p^t}$. Hence, it is of type 1.

Case (ii) Let $a = d \pmod{p^t}$.

Then, (5.2) and (5.3) give $2ab = 0 \pmod{p^t}$ and $2ac = 0 \pmod{p^t}$. Since 2 is invertible in Z_{p^t}, we get

$$ab = 0 \pmod{p^t} \quad \ldots\ldots\ldots\ldots\ldots\ldots (5.7)$$

and

$$ac = 0 \pmod{p^t} \quad \ldots\ldots\ldots\ldots\ldots\ldots (5.8)$$

We separate the discussion into the following three subcases:

Case (iia) Let a be invertible in Z_{p^t}.

Then (5.7) implies $b = 0$, and (5.8) implies $c = 0$. Hence, (5.1) gives $a^2 = 1 \pmod{p^t}$. Therefore, the matrix is of the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ with $a^2 = 1 \pmod{p^t}$. Since $a^2 = 1 \pmod{p^t}$ has only two solutions, $a = \pm 1 \pmod{p^t}$. Thus, the matrix is in type 2.

Case (iib) Let $a = 0 \pmod{p^t}$.

Then, from (5.1), we get $bc = 1 \pmod{p^t}$. Equations (5.7) and (5.8) imply that $c = b^{-1}$, and b is an arbitrary invertible element in Z_{p^t}. Hence, the matrix is of the form $\begin{pmatrix} 0 & b \\ b^{-1} & 0 \end{pmatrix}$, which is type 1.

Case (iic) Let $a \neq 0$ and a is not invertible in Z_{p^t}.

Then there are integers k and r with $1 \leq r < t$ such that $a = kp^r$. Hence, (5.7) and (5.8) imply that $b = xp^{t-r}$ and $c = yp^{t-r}$ for some integers x and y. Substituting the values of a,b and c in (5.1), we get $k^2p^{2r} + xyp^{2t-2r} = 1 \pmod{p^t}$. The expression on the left is divisible by p and hence not invertible in Z_{p^t}, whereas the 1 on the right is invertible in Z_{p^t}. Thus, we have a contradiction. Hence, there is no matrix in $S_2(p^t)$ satisfying the conditions of this subcase.

To prove the second part of the theorem, note that n = 2, and hence $S_2(p^t) = T_0(p^t) \cup T_1(p^t) \cup T_2(p^t)$. Recall that $T_0(p^t)$ contains only $-I \pmod{p^t}$, and $T_2(p^t)$ contains only $I \pmod{p^t}$. In fact, these are the matrices of type 2. Hence, the number of matrices of type 1 is the same as the number of matrices in $T_1(p^t)$. By Theorem 4.2.6,

$$|T_1(p^t)| = p^{2(t-1)}|T_1(p)|$$

$$= p^{2(t-1)}\frac{g_2(p)}{g_1(p)g_1(p)}$$

$$= p^{2(t-1)}(p+1)p$$

$$= p^{2t-1}(p + 1)$$

Hence, type 1 has $p^{2t-1}(p + 1)$ matrices. Consequently, $s_2(p^t) = p^{2t-1}(p + 1) + 2$. Thus, the proof of the theorem is complete.

Remark 5.1.3

It is possible to prove that type 1 has $p^{2t-1}(p + 1)$ matrices just from the primary equations, without any reference to the results of the previous chapter. We omit the details of this proof. However, we remark that a similar technique is used in the next section to compute $s_2(2^t)$.

5.2 Structure of matrices in $S_2(2^t)$, $t \geq 1$

In this section, we give a complete classification and enumeration of matrices in $S_2(2^t)$, $t \geq 1$.

As before, we assume that a matrix A in $S_2(2^t)$ is of the form $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod{2^t}$. The corresponding primary equations are:

$$a^2 + bc = 1 \pmod{2^t} \quad \ldots\ldots\ldots\ldots (5.9)$$

$$(a + d)b = 0 \pmod{2^t} \quad \ldots\ldots\ldots\ldots (5.10)$$

$$(a + d)c = 0 \pmod{2^t} \quad \ldots\ldots\ldots\ldots (5.11)$$

$$d^2 + bc = 1 \pmod{2^t} \quad \ldots\ldots\ldots\ldots (5.12)$$

We begin with a lemma.

Lemma 5.2.1

The primary equations imply that either (i) $d = \pm a \pmod{2^t}$ or (ii) a is odd, and $d = 2^{t-1} \pm a \pmod{2^t}$. (Consequently d is also odd.)

Proof

We will prove that if d is not equal to $\pm a \pmod{2^t}$ then $d = 2^{t-1} \pm a \pmod{2^t}$. From (5.9) and (5.12), we get $a^2 - d^2 = 0 \pmod{2^t}$. i.e., $(a + d)(a - d) = 0 \pmod{2^t}$. Hence, there are integers r,s,k,ℓ with $1 \leq r, s < t$, $r + s \geq t$, and k,ℓ odd integers, such that

$$a + d = k2^r \quad \text{.....(5.13)}$$

$$a - d = \ell 2^s \quad \text{.....(5.14)}$$

We discuss two cases:

Case (i) Let $r = t - 1$.

Then, from (5.13) $d = k2^{t-1} - a = 2^{t-1} - a \pmod{2^t}$.

Case (ii) Let $r < (t - 1)$.

Then, we will prove that $r = 1$. From (5.13) $a = k2^r - d \pmod{2^t}$, and hence $a^2 = k^2 2^{2r} + d^2 - kd2^{r+1} \pmod{2^t}$. Reducing this equation to $\pmod{2^t}$ and using the fact $a^2 = d^2 \pmod{2^t}$, we get

$$k^2 2^{2r} - kd2^{r+1} = 0 \pmod{2^t}.$$

i.e. $$k2^{r-1} - d = 0 \pmod{2^{t-r-1}}$$

i.e. $$d = k2^{r-1} \pmod{2^{t-r-1}} \quad \text{.....(5.15)}$$

Using (5.13) in (5.10) and (5.11), we have b and c are even integers. Hence, (5.12) implies that d is an odd integer.

Therefore, from (5.15) we get $r = 1$.

Since $r + s \geq t$, $r = 1$ implies $s \geq t - 1$. If $s \geq t$, then $a \equiv d \pmod{2^t}$. Hence, $s = t - 1$. Therefore, from (5.14) we obtain $d = -k2^{t-1} + a \equiv 2^{t-1} + a \pmod{2^t}$.

Thus, in any case $d \equiv 2^{t-1} \pm a \pmod{2^t}$. Hence, the lemma is proved.

Recall that the equation $x^2 - 1 \equiv 0$ has exactly 2 solutions in Z_{2^t} if $t \leq 2$, and exactly 4 solutions if $t \geq 3$ (see Lemma 4.3.1).

The next theorem gives a classification of matrices in $S_2(2^t)$, $t \geq 3$.

Theorem 5.2.2

The elements of $S_2(2^t)$, $t \geq 3$, can be classified into the following four distinct types:

$$\text{type 1} = \left\{\begin{pmatrix} a & b \\ c & -a \end{pmatrix} : a^2 + bc \equiv 1 \pmod{2^t}\right\},$$

$$\text{type 2} = \left\{\begin{pmatrix} a & x2^{t-1} \\ y2^{t-1} & a \end{pmatrix} : \begin{array}{l} a^2 \equiv 1 \pmod{2^t}, \\ x = 0,1, \text{ and } y = 0,1. \end{array}\right\},$$

$$\text{type 3} = \left\{\begin{pmatrix} a & b \\ c & 2^{t-1} - a \end{pmatrix} : \begin{array}{l} a^2 + bc \equiv 1 \pmod{2^t}, \\ b \text{ and } c \text{ are even.} \end{array}\right\},$$

$$\text{type 4} = \left\{\begin{pmatrix} a & x2^{t-1} \\ y2^{t-1} & 2^{t-1} - a \end{pmatrix} : \begin{array}{l} a^2 \equiv 1 \pmod{2^t}, \\ x = 0,1 \text{ and } y = 0,1. \end{array}\right\}$$

Proof

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be in $S_2(2^t)$. Then, by the previous lemma, $d \equiv \pm a \pmod{2^t}$ or $d \equiv 2^{t-1} \pm a \pmod{2^t}$. We prove

the theorem by discussing these four cases separately.

Case (i) Let $d = -a \pmod{2^t}$.

Then, from the primary equations, we get that b and c are arbitrary such that $a^2 + bc = 1 \pmod{2^t}$. Therefore, the matrix must be of the form $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ with $a^2 + bc = 1 \pmod{2^t}$. Hence, it is of type 1.

Case (ii) Let $d = a \pmod{2^t}$.

Then, the equations (5.10) and (5.11) reduce to

$$2ab = 0 \pmod{2^t} \quad \ldots\ldots\ldots\ldots\ldots\ldots (5.16)$$

and

$$2ac = 0 \pmod{2^t} \quad \ldots\ldots\ldots\ldots\ldots\ldots (5.17)$$

We consider three subcases arising from the values of a.

Case (iia) Let $a = 0 \pmod{2^t}$.

Then, from (5.9) $bc = 1 \pmod{2^t}$. i.e., $c = b^{-1} \pmod{2^t}$. Thus, $A = \begin{pmatrix} 0 & b \\ b^{-1} & 0 \end{pmatrix} \pmod{2^t}$, and A is in type 1.

Case (iib) Let $a = 2^{t-1} \pmod{2^t}$.

Then, from (5.16), (5.17), and (5.9) we get $bc = 1 \pmod{2^t}$. Hence, $A = \begin{pmatrix} 2^{t-1} & b \\ b^{-1} & 2^{t-1} \end{pmatrix} \pmod{2^t}$ which is also of type 1.

Case (iic) Let a not equal to 0 or $2^{t-1} \pmod{2^t}$.

We claim that a is odd. Since 2a is not equal to 0 $\pmod{2^t}$, from (5.16) and (5.17) we get b and c are even

integers. Hence, (5.9) implies that a is an odd integer. Therefore, a has an inverse in Z_{p^t}. Thus, (5.16) and (5.17) yield $2b = 0 \pmod{2^t}$, and $2c = 0 \pmod{2^t}$. Hence, $b = x2^{t-1} \pmod{2^t}$ with $x = 0,1$, and $c = y2^{t-1} \pmod{2^t}$ with $y = 0,1$. Consequently, $bc = 0 \pmod{2^t}$ as $t \geq 2$, and $a^2 = 1 \pmod{2^t}$. Therefore, $A = \begin{pmatrix} a & x2^{t-1} \\ y2^{t-1} & a \end{pmatrix} \pmod{2^t}$ with $a^2 = 1 \pmod{2^t}$, $x = 0,1$ and $y = 0,1$. Hence, A is of type 2.

Case (iii) Let $d = 2^{t-1} - a \pmod{2^t}$.

In this case we know that both a and d are odd integers. Using $a + d = 2^{t-1} \pmod{2^t}$ in (5.10) and (5.11), we get $2^{t-1}b = 0 \pmod{2^t}$, and $2^{t-1}c = 0 \pmod{2^t}$. Thus, b and c are even integers, and satisfy the equation (5.9). Therefore, $A = \begin{pmatrix} a & b \\ c & 2^{t-1} - a \end{pmatrix}$ such that b and c are even, and $a^2 + bc = 1 \pmod{2^t}$. Thus, A is of type 3.

Case (iv) Let $d = 2^{t-1} + a \pmod{2^t}$.

Then, from (5.10) we have, $(2a + 2^{t-1})b = 0 \pmod{2^t}$. i.e., $(a + 2^{t-2})b = 0 \pmod{2^{t-1}}$. Since a is odd, $a + 2^{t-2}$ is an odd integer, and hence is invertible in $Z_{2^{t-1}}$. Therefore, $b = 0 \pmod{2^{t-1}}$. i.e., $b = x2^{t-1} \pmod{2^t}$ with $x = 0,1$. Similarly, $c = 2^{t-1} \pmod{2^t}$ with $y = 0,1$. Consequently, $bc = 0 \pmod{2^t}$ and $a^2 = 1 \pmod{2^t}$. Thus, $A = \begin{pmatrix} a & x2^{t-1} \\ y2^{t-1} & 2^{t-1} + a \end{pmatrix} \pmod{2^t}$ with $a^2 = 1 \pmod{2^t}$, $x = 0,1$, and $y = 0,1$. Hence, A is of type 4, and this completes the proof.

Note that, if $t \geq 3$ there are 16 matrices in each of type 2 and type 4. Therefore, to find the value of $s_2(2^t)$, it is sufficient to know the number of matrices in each of type 1 and type 3.

Proposition 5.2.3

There are $3 \cdot 2^{2t-1}$ matrices of type 1 in $S_2(2^t)$, $t \geq 3$.

Proof

If A is a matrix in $S_2(2^t)$ and is of type 1, then $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \pmod{2^t}$ with $a^2 + bc \equiv 1 \pmod{2^t}$. We prove the proposition by discussing the following three separate cases:

Case (i): $a^2 \equiv 1 \pmod{2^t}$.

Case (ii): $a^2 \not\equiv 1 \pmod{2^t}$ and b^{-1} exists.

Case (iii): $a^2 \not\equiv 1 \pmod{2^t}$ and b^{-1} does not exist.

Case (i) Let $a^2 \equiv 1 \pmod{2^t}$. This implies $bc \equiv 0 \pmod{2^t}$.

If $b \equiv 0 \pmod{2^t}$, then c is arbitrary in Z_{2^t}, and hence c can be chosen in 2^t ways. Similarly, if $c \equiv 0 \pmod{2^t}$, then b can be chosen in 2^t ways. But the choice $b = 0$ and $c = 0$ is counted twice. Hence, there are $2^{t+1} - 1$ choices of pair (b,c) with one of them zero in Z_{2^t}.

Let us assume that both b and c are not zero $\pmod{2^t}$. Then the equation $bc \equiv 0 \pmod{2^t}$ gives that $b = x2^r \pmod{2^t}$ for some odd integer x and $1 \leq r < t$. Therefore, $c = y2^{t-r} \pmod{2^t}$. The possible values of y are $1, 2, \ldots (2^r - 1)$. Thus, for a fixed a, b and r, there are $(2^r - 1)$ choices of c. For a fixed r, the number of choices for b is the same as the number of odd number x such that $1 \leq x \leq 2^{t-r}$. Hence,

b can be chosen in 2^{t-r-1}. Thus, for fixed a,r, we have $2^{t-r-1}(2^r - 1)$ choices of the pair (b,c).

Now, r can take any value from 1 to t - 1. Therefore, when a is fixed such that $a^2 = 1$, then we have $\sum_{r=1}^{t-1} 2^{t-r-1}(2^r - 1)$ choices of (b,c). On simplifying, we get $2^{t-1}(t - 2) + 1$ choices of (b,c).

Therefore, when a is fixed with $a^2 = 1 \pmod{2^t}$ we have $(2^{t+1} - 1) + 2^{t-1}(t - 2) + 1 = 2^{t-1}(t + 2)$ choices of (b,c) with $bc = 0 \pmod{2^t}$. But, there are 4 choices of a. Hence, in total case (i) contains $4(2^{t-1}(t + 2)) = 2^{t+1}(t + 2)$ matrices.

Case (ii) Let $a^2 \neq 1 \pmod{2^t}$, and let b^{-1} exist in Z_{2^t}.

Then, $bc = (1 - a^2) \pmod{2^t}$, and $c = b^{-1}(1 - a^2) \pmod{2^t}$. Thus, for a fixed a,b there is a unique choice of c. However, there are 2^{t-1} choices for b and $(2^t - 4)$ choices for a. Hence, in total there are $2^{t-1}(2^t - 4)$ matrices in this case.

Case (iii) $a^2 \neq 1 \pmod{2^t}$ and b is not invertible in Z_{2^t}.

Then, $b = x2^r$ for some odd integer x and $1 \leq r < t$. Since $bc = (1 - a^2) \pmod{2^t}$, we have 2^r divides $(1 - a^2)$, and hence a is an odd integer.

We claim that either 2^{r-1} divides (a - 1) or 2^{r-1} divides (1 + a). Now, 2^r divides $(1 - a^2) = (1 - a)(1 + a)$. Hence, there are integers k,ℓ,i,j such that $a - 1 = k2^i \pmod{2^t}$ and $a + 1 = \ell 2^j \pmod{2^t}$ with k,ℓ odd integer,

$1 \leq i,j < r$ and $i + j \geq r$. Thus, $2a = (k2^i + \ell 2^j) \pmod{2^t}$. i.e., $a = k2^{i-1} + \ell 2^{j-1} \pmod{2^{t-1}}$. Since, a is odd we have either $i = 1$ or $j = 1$, not both. If $i = 1$ then $j = r - 1$, and 2^{r-1} divides $a + 1$. Similarly, if $j = 1$, then 2^{r-1} divides $a - 1$. Hence, the claim is proved.

We further divide our discussion of this case into three subcases.

Case (iiia). Let $r \geq 3$.

Then, by the above claim, $a = y2^{r-1} \pm 1 \pmod{2^t}$ for some odd integer y. Thus, $1 - a^2 \equiv -y^2 2^{2r-2} \mp 2^r y \pmod{2^t}$. Therefore,

$$bc = (-y^2 2^{2r-2} \mp 2^r y) \pmod{2^t}.$$

i.e. $$x2^r c = (-y^2 2^{2r-2} \mp 2^r y) \pmod{2^t}.$$

i.e. $$xc = (-y^2 2^{r-2} \mp y) \pmod{2^{t-r}}.$$

i.e. $c = y_1 \pmod{2^{t-r}}$ where $y_1 = x^{-1}(-y^2 2^{r-2} \mp y) \pmod{2^{t-r}}$.

i.e. $$c = y_1 + u2^{t-r} \pmod{2^t} \text{ where } 0 \leq u < 2^r.$$

Thus, for a fixed a,b, and r there are 2^r choices of c. For a fixed r, there are 2^{t-r-1} choices for b, and $2(2^{t-r+1} - 2)$ choices of a. Thus, for a fixed $r \geq 3$, we have $2^r \cdot 2^{t-r-1} \cdot 2(2^{t-r+1} - 2) = 2^{t+1}(2^{t-r} - 1)$ choices of (a,b,c). Therefore, in total there are $\sum_{r=3}^{t-1} 2^{t+1}(2^{t-r} - 1) =$

$= 2^{t+1}(2^{t-2} - t + 1)$ matrices in this subcase.

Case (iiib). Let $r = 2$.

Then, $b \equiv 4x \pmod{2^t}$ and a is odd. As before, we

can prove that for fixed a,b there are 4 choices of c. Moreover, there are 2^{t-3} choices of b, and $(2^{t-1} - 4)$ choices of a. Thus, we have $4 \cdot 2^{t-3}(2^{t-1} - 4) = 2^{t+1}(2^{t-3} - 1)$ matrices in this subcase.

Case (iiic). Let r = 1.

Then, b = 2x, and a is odd. It follows that there are 2^{t-2} choices of b, $2^{t-1} - 4$ choices of a, and for fixed a,b there are 2 choices of c. Thus, there are $2 \cdot 2^{t-2}(2^{t-1} - 4) = 2^{t+1}(2^{t-3} - 1)$ matrices in this case.

Therefore, in total, case (iii) contains

$$2^{t+1}(2^{t-2} - t + 1) + 2^{t+1}(2^{t-3} - 1) + 2^{t+1}(2^{t-3} - 1)$$
$$= 2^{t+1}(2^{t-1} - t - 1) \text{ matrices.}$$

Finally, adding the counts in all the three cases, we get $3 \cdot 2^{2t-1}$ matrices in $S_2(2^t)$ of type 1. This completes the proof.

Recall the result in Theorem 5.1.2 (ii) for type 1 matrices in $S_2(p^t)$ with p an odd prime. With p = 2, what we have just shown for type 1 matrices of $S_2(2^t)$ agrees with the result in Theorem 5.1.2 (ii). We remark that p = 2 gives rise to some additional types of matrices that cannot arise when p is an odd prime.

Next we proceed to calculate the number of type 3 matrices in $S_2(2^t)$, $t \geq 3$.

Proposition 5.2.4

There are $3 \cdot 2^{2t-2}$ matrices of type 3 in $S_2(2^t)$, $t \geq 3$.

Proof

Let A be in $S_2(2^t)$ of type 3. Then, A is of the form $\begin{pmatrix} a & c \\ c & 2^{t-1} - a \end{pmatrix} \pmod{2^t}$ with b and c even and $a^2 + bc = 1 \pmod{2^t}$. We prove the theorem by discussing the following two cases:

Case (i): $a^2 = 1 \pmod{2^t}$.

Case (ii): $a^2 \neq 1 \pmod{2^t}$.

Case (i) Let $a^2 = 1 \pmod{2^t}$.

Then, $bc = 0 \pmod{2^t}$. If $b = 0 \pmod{2^t}$, then c is arbitrary and even, and hence there are 2^{t-1} choices of c. Similarly, if $c = 0 \pmod{2^t}$ then there are 2^{t-1} choices of b. But, the choice b = 0 and c = 0 is counted twice. Therefore, there are $2^t - 1$ choices of (b,c) with one of them zero and the other even.

Let us assume that both b and c are not zero $\pmod{2^t}$. Then, as discussed in the proof of the previous proposition, we have $2^{t-1}(t - 2) + 1$ choices of (b,c) when a is fixed.

Since there are 4 choices for a, we have $4[2^t - 1 + 2^{t-1}(t-2) + 1] = t2^{t+1}$ matrices in this case.

Case (ii) Let $a^2 \neq 1 \pmod{2^t}$.

As b is even, we have $b = x2^r \pmod{2^t}$ for some odd integer x and $1 \leq r < t$. As we proved in the previous proposition, we prove 2^{r-1} divides either a - 1 or a + 1. Thus, $a = y2^{r-1} \pm 1 \pmod{2^t}$.

We divide our discussion into three subcases, accordingly as $r \geq 3$, r = 2 and r = 1.

Case (iia) Let $r \geq 3$.

Then, from $bc = (1 - a^2) \pmod{2^t}$ we get

$$x2^r c = -y^2 2^{2r-2} \pm 2^r y \pmod{2^t}.$$

i.e. $$xc = -y^2 2^{r-2} \pm y \pmod{2^{t-r}}.$$

The expression on the right is odd if y is odd. However, the expression on the left is even (since c is even). Hence, y must be even. Therefore $a = u2^r \pm 1 \pmod{2^t}$ for some u with $1 \leq u < 2^{t-r}$ and $u \neq 2^{t-r-1}$. Therefore,

$$x2^r c = -u^2 2^{2r} \pm 2^{r+1} u \pmod{2^t}$$

i.e. $c = v \pmod{2^{t-r}}$ where $v = x^{-1}(-u^2 2^r \pm 2u) \pmod{2^{t-r}}$

i.e. $c = v + w2^{t-r} \pmod{2^t}$ with $w = 0, 1, \ldots, 2^r - 1$.

Thus, for fixed a,b,r, there are 2^r choices of c. For a fixed r, there are 2^{t-r-1} choices of b, and $2(2^{t-r} - 2)$ choices of a. Hence, for a fixed r, there are $2^r 2^{t-r-1} 2(2^{t-r} - 2) = 2^{t+1}(2^{t-r-1} - 1)$ choices of (a,b,c). But $3 \leq r \leq t - 1$. Thus, summing over r, there are $2^{t+1}(2^{t-3} - t + 2)$ matrices in this subcase.

Case (iib) Let $r = 2$.

Then, $b = 4x \pmod{2^t}$, and a is odd. It is easy to see that when a and b are fixed, there are 4 choices of c. Further, there are 2^{t-3} choices of b and $(2^{t-1} - 4)$ choices of a. Thus, there are $2^{t+1}(2^{t-3} - 1)$ matrices in this subcase.

Case (iic) Let $r = 1$.

Then, $b = 2x \pmod{2^t}$, and a is odd. For fixed a,b

it is easy to prove that there are 2 choices for c. Further, there are 2^{t-2} choices for b and $(2^{t-1} - 4)$ choices of a. Hence, there are $2^{t+1}(2^{t-3} - 1)$ matrices in this subcase.

Therefore, in total, case (ii) contains $2^{t+1}(3 \cdot 2^{t-3} - t)$ matrices.

Finally, adding the counts that we have obtained in both cases, we get $t2^{t+1} + 2^{t+1}(3 \cdot 2^{t-3} - t) = 3 \cdot 2^{2t-2}$ matrices of type 3 in $S_2(2^t)$. The proof is complete.

On summarizing our results we have the following theorem:

Theorem 5.2.5

Let $s_2(2^t)$ be the number of 2×2 matrices A over Z_{2^t} such that $A^2 = I \pmod{2^t}$, $t \geq 1$. Then,

(i) $s_2(2) = 4$

(ii) $s_2(4) = 28$

(iii) $s_2(2^t) = 9 \cdot 2^{2t-2} + 32$.

Proof

For $t = 1$, the result is verified by looking at the listing that precedes Lemma 4.3.2. For $t = 2$, the result is verified using the Theorem 4.3.10. For $t \geq 3$, we have proved in Theorem 5.2.2 that there are four distinct types of matrices in $S_2(2^t)$. We have already observed that there are only 16 matrices in each of type 2 and type 4. Propositions 5.2.3 and 5.2.4 give the counts of type 1 and type 3 matrices respectively. Hence, summing up the counts in all the four types, we get $3 \cdot 2^{2t-1} + 16 + 3 \cdot 2^{2t-2} + 16 =$

$= 9 \cdot 2^{2t-2} + 32$ matrices in $S_n(2^t)$. Hence the theorem is proved.

Remark 5.2.5

When $t = 3$, from the above theorem we get that $s_2(8) = 11 \cdot 2^4$, which is already verified in Example 4.3.16.

5.3 Structure of Matrices in $S_2(2p)$, $p > 2$

In this section, we characterize the structure of matrices $S_2(2p)$ where p is an odd prime. Such a characterization is significant and useful in the cryptanalysis of English text whose alphabet size m is 26.

By Theorem 4.1.3, we have that $s_n(2p) = s_n(2)s_n(p)$. If $n = 2$, then $s_2(2p) = s_2(2)s_2(p) = 4 \cdot (p(p + 1) + 2) = 4p(p + 1) + 8$. In particular, $s_2(26) = s_2(2 \cdot 13) = 4 \cdot 13 \cdot (14) + 8 = 736$, which was incorrectly mentioned as 740 in [9], and later corrected in [10].

Further, the equation $x^2 \equiv 1 \pmod{2p}$ has only two solutions, namely $x \equiv \pm 1 \pmod{2p}$. Using this fact, and following the classification method given in the previous two sections, we can prove the following theorem:

Theorem 5.3.1

Let p be an odd prime. Then, the elements of $S_2(2p)$ can be classified into the following two distinct types:

$$\text{type 1} = \left\{ \begin{pmatrix} a & b \\ c & -a \end{pmatrix} : a^2 + bc \equiv 1 \pmod{2p} \right\},$$

and

$$\text{type 2} = \left\{ \begin{pmatrix} a & b \\ c & a \end{pmatrix} : \begin{array}{l} a^2 + bc \equiv 1 \pmod{2p}, \\ b \not\equiv 0, p \text{ and } c \equiv 0, p \end{array} \right\},$$

Furthermore, there are only 8 matrices of type 2, and they are enumerated below:

a	b	c
1	0	0
1	p	0
1	0	p
2p - 1	0	0
2p - 1	p	0
2p - 1	0	p
p + 1	p	p
p - 1	p	p

Note that for any matrix A in $S_2(2p)$ of type 2, $A \pmod p \equiv \pm I \pmod p$, and $A \pmod 2$ is any one of the four matrices in $S_2(2)$. The converse statement is also true. Moreover, the number of matrices in $S_2(2p)$ of type 2 is independent of p. Hence, whenever a matrix in $S_2(2p)$ is used as a key in a cryptosystem, it is essential to choose the matrix from type 1 in order to assume a certain degree of security; otherwise, a fast and simple exhaustive search of the type 2 matrices would reveal the key matrix.

However, we caution that even an arbitrary choice of a key matrix chosen from type 1, does not assure security. In the next chapter, we shall discuss some methods for isolating and identifying a key matrix (assumed to be unknown to the user) used in a cryptosystem.

CHAPTER VI

Cryptanalysis Techniques

In this chapter, we discuss a possible cryptanalysis technique to decrypt and identify the contents from a cipher-text obtained through an $n \times n$ involutory matrix A over Z_m.

6.1 Introduction

This section describes the environment in which the cryptanalysis is supposed to be undertaken. We assume that the mapping f from the alphabet with m letters to Z_m is known to everyone using the system.

The security of the system should be analysed under each of the following environment:

(i) The opponent can have the cipher-text of any plain-text chosen by him. Then, he wishes to find the key matrix A.

(ii) The opponent can have some plain-text (not necessarily his choice) and its corresponding cipher-text. Then, he wishes to find the key matrix A.

(iii) The opponent has only a cipher-text and wishes to find the corresponding plain-text (not necessarily to find the key matrix A).

(iv) The opponent has only some cipher-text. Then, he wishes to find the key matrix A.

Note that (iv) is equivalent to (ii) and (iii) put together.

There is no security under (i) in an algebraic cryptosystem. For, by a suitable choice of a plain-text, a clever opponent can always find the column vectors of A. For example, if $e_1 = \begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix} \pmod m$ then Ae_1 would give the entries of the first column of A, and if $e_2 = \begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix}$ then Ae_2 give the entries of the second column of A, and so on. Thus, the plain-text $f^{-1}(1)f^{-1}(0)\ldots f^{-1}(0)$ would reveal the first column of A, and the plain-text $f^{-1}(0)f^{-1}(1)f^{-1}(0)\ldots f^{-1}(0)$ would reveal the second column of A, and so on.

The security of the system under the environment (ii) depends to a great degree on the length of the text involved. Let there be n linearly independent blocks $P_1, P_2, \ldots, P_n$ each of length n in the plain-text. If $C_1, C_2, \ldots, C_n$ are the corresponding cipher-text blocks, then the system of equations $AP_i = C_f \pmod m$, $i = 1,2,\ldots,n$, can be uniquely solved to get the key matrix A.

For the environment (ii) we give a probabilistic analysis under a rough assumption that the n-grams are uniformly distributed. Then, for a random variable X taking values in $Z_{m,n}$, $P_r(X = x) = m^{-n}$ for all x in $Z_{m,n}$. Assume that we have found blocks $P_1, \ldots, P_\ell$ such that they are linearly independent over Z_m. Since there are m^ℓ vectors in

$Z_{m,n}$ which are linearly dependent on $P_1,\ldots,P_\ell$, we have Prob(X = x:x is linearly dependent on $P_1,\ldots,P_\ell$) = $m^{\ell-n}$. Let $r = m^{\ell-n}$. Therefore, Prob(X = x:x is not dependent on $P_1,\ldots,P_\ell$) = 1 - r. Hence, the probability of selecting an x in the k-th trial such that x is independent of $P_1,\ldots,P_\ell$ is $r^{k-1}(1 - r)$. Therefore, the expected number of trials is given by $\sum_{K=1}^{\infty} kr^{k-1}(1 - r) = \frac{1}{1 - r}$. Hence, the expected waiting time to get n linearly independent blocks is given by $\sum_{\ell=1}^{n-1} \frac{1}{1 - m^{\ell-n}}$ which lies between (n - 1) and (n + 1).

Though our assumptions that the n-grams are uniformly distributed is not always true, this analysis gives an approximation to this problem. Due to this observation, the environments (iii) and (iv) can be considered to be equivalent. Hence, our main concern is the environment (iv), though (iii) is also important in practice.

One obvious method of finding the key matrix A is to generate all possible key matrices, and then apply each of these matrices to the cipher-text. The matrix which produces a meaningful plain-text will be the required key. If the keys are chosen at random from the matrices in $S_n(m)$, then this method requires the generation of all matrices in $S_n(m)$. Since $s_n(m)$, the number of matrices in $S_n(m)$ is very large for large n and m, this method is practically impossible.

Another method, known as the method of probable word is well known. This method involves the following three steps.

(a) Choosing probable n-grams $P_1,\ldots,P_\ell$ that would be present in the plain-text.

(b) For each P_i, somehow find an n-gram C_i in the cipher-text such that $AP_i = C_i \pmod m$ $i = 1,2,\ldots,\ell$.

(c) Solving for the key matrix A, from the system of equations $AP_i = C_i \pmod m$, $i = 1,2,\ldots,\ell$.

To choose probable n-grams that would be present in the plain-text, one needs some knowledge about the subject matter. For example, if the message is in English, a frequency table of n-grams of English text would be of great help.

For a given P_i, locating a cipher-text block C_i such that $AP_i = C_i \pmod m$ is complex. When $m = 2p$ with p being an odd prime, Levine [8] has used "binary reduction method" and pattern matching techniques for cryptanalysis. We describe this method in the next section.

After finding the C_i's in the cipher-text, the problem of solving for the key matrix A poses a great amount of difficulty. If there are n linearly independent blocks $P_1,\ldots,P_n$, and if $C_1,\ldots,C_n$ are corresponding blocks located in the cipher-text, then the system of equations $AP_i = C_i \pmod m$ can be solved to get the key matrix A. Sometimes, it may even be possible to find $P_1,\ldots,P_{n/2}$

independent probable n-grams and its corresponding cipher-blocks $C_1,\ldots,C_{n/2}$ such that $P_1,\ldots,P_{n/2}$, $C_1,\ldots,C_{n/2}$ are linearly independent over Z_m. Then, the system of equations

$$AP_i = C_i \qquad i = 1,2,\ldots,n/2$$

$$AC_i = P_i \qquad i = 1,2,\ldots,n/2$$

can be solved to get the key matrix A.

In the following sections, we describe the methods given by Levine for n = 2,3 and m = 26. We comment more on this method and show their extension to m = 2p.

6.2 Analysis for n = 2

Let n = 2, and let the cipher-text be blocked into blocks of two letters as follows: $C_1D_1C_2D_2\ldots C_iD_iC_{i+1}D_{i+1}\ldots$. Assume that the transformation of a probable plain-text with three letters PQR under a hidden key matrix (to be found) occurs in the cipher-text. Let us consider the following two cases:

Case (i): PQR* is transformed to $C_iD_iC_{i+1}D_{i+1}$.

Case (ii): *PQR is transformed to $C_iD_iC_{i+1}D_{i+1}$.

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod m$ be the key matrix. Then, in Case (i) we have,

$$aP + bQ = C_i \pmod m \qquad \ldots\ldots\ldots\ldots\ldots (6.1)$$

$$aC_i + bD_i = P \pmod m \qquad \ldots\ldots\ldots\ldots\ldots (6.2)$$

$$aC_{i+1} + bD_{i+1} = R \pmod m \qquad \ldots\ldots\ldots\ldots\ldots (6.3)$$

Eliminating a,b from these three equations, we get that the determinant,

$$\begin{vmatrix} P & Q & C_i \\ C_i & D_i & P \\ C_{i+1} & D_{i+1} & R \end{vmatrix} = 0 \pmod m \quad \ldots\ldots\ldots (6.4)$$

Similarly, in case (ii) we have

$$cC_i + dD_i = P \pmod m \quad \ldots\ldots\ldots\ldots (6.5)$$

$$cC_{i+1} + dD_{i+1} = R \pmod m \quad \ldots\ldots\ldots\ldots (6.6)$$

$$cQ + dR = D_{i+1} \pmod m \quad \ldots\ldots\ldots\ldots (6.7)$$

Eliminating C,d from the equations (6.5), (6.6) and (6.7) we get that the determinant,

$$\begin{vmatrix} C_i & D_i & P \\ C_{i+1} & D_{i+1} & R \\ Q & R & D_{i+1} \end{vmatrix} = 0 \pmod m \quad \ldots\ldots\ldots (6.8)$$

Hence, we have proved the following theorem:

Theorem 6.2.1 (For n = 2 and any m.)

The block of letters PQR* (respectively *PQR) matches with the cipher-text $C_iD_iC_{i+1}D_{i+1}$ then condition (6.4) (respectively (6.8)) holds.

We remark that this is a simple generalization of Theorem 1 in [9].

Thus, a general procedure would use a probable 3-gram PQR to test the conditions stated in Theorem 6.2.1. If the conditions are not satisfied, then we look for another block of cipher-text. If the conditions are satisfied for a

cipher-text, then we have $A\begin{pmatrix}P\\Q\end{pmatrix} = \begin{pmatrix}C_i\\D_i\end{pmatrix} \pmod m$ in case (i), and $A\begin{pmatrix}Q\\R\end{pmatrix} = \begin{pmatrix}C_{i+1}\\D_{i+1}\end{pmatrix} \pmod m$ in case (ii). Below we discuss the situation of case (i) only, as the discussion of case (ii) is similar.

Since $A^2 = I \pmod m$, the equation $A\begin{pmatrix}P\\Q\end{pmatrix} = \begin{pmatrix}C_i\\D_i\end{pmatrix} \pmod m$ implies that $A\begin{pmatrix}C_i\\D_i\end{pmatrix} = \begin{pmatrix}P\\Q\end{pmatrix} \pmod m$. Therefore,

$$A\begin{pmatrix}P & C_i\\Q & D_i\end{pmatrix} = \begin{pmatrix}C_i & P\\D_i & Q\end{pmatrix} \pmod m \quad \ldots\ldots\ldots\ldots (6.9)$$

If the vectors $\begin{pmatrix}P\\Q\end{pmatrix}$ and $\begin{pmatrix}C_i\\D_i\end{pmatrix}$ are two linearly independent vectors in $Z_{m,2}$, then $\begin{pmatrix}P & C_i\\Q & D_i\end{pmatrix} \pmod m$ is an invertible matrix, and hence $A = \begin{pmatrix}C_i & P\\D_i & Q\end{pmatrix}\begin{pmatrix}P & C_i\\Q & D_i\end{pmatrix}^{-1} \pmod m$. Note that $\begin{pmatrix}C_i & P\\D_i & Q\end{pmatrix}$ is invertible if and only if its determinant $QC_i - PD_i$ is relatively prime to m.

In case, $\begin{pmatrix}P\\Q\end{pmatrix}$ and $\begin{pmatrix}C_i\\D_i\end{pmatrix}$ are linearly dependent over Z_m, then there are several solutions for A from (6.9). We select only those matrices A for which $A^2 = I \pmod m$. Then we apply matrices to the cipher-text. The matrices which

produce meaningful plain-text are retained. (In fact, it is enough to apply these matrices to a small portion of the cipher-text.) If necessary, we may repeat the whole procedure with other choices of probable tri-grams.

When m = 26, or in general when m = 2p with p an odd prime, the problem of finding a key matrix is much easier. If the key matrix is from type 2 matrices of $S_2(2p)$ (see section 5.3), then an exhaustive search would reveal A. If the key matrix is chosen from type 1 matrices of $S_2(2p)$ then we have $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \pmod{2p}$ with $a^2 + bc = 1 \pmod{2p}$. We use this condition along with the equation $A\begin{pmatrix} P \\ Q \end{pmatrix} = \begin{pmatrix} C_i \\ D_i \end{pmatrix} \pmod{2p}$ to solve for A. In fact, (mod 2) solutions are found, and then extended to (mod 2p) solutions.

See [9] for a detailed description for n = 2, m = 26.

6.3 Analysis for n = 3

In this section, we first develop some results for any n, and then discuss the particular case n = 3. Finally, we comment on the case m = 2p for an odd prime p. As a particular case, we get the results of Levine [10].

First consider the case m = 2. Now, $Z_{2,n}$ contains 2^n elements, and each is an n-tuple with entries from $Z_2 = \{0,1\}$. Each of these n-tuples can be viewed as a binary representation of a decimal integer. Thus, elements of $Z_{2,n}$ can be identified with elements in the set

$Y_n = \{0,1,2,\ldots,2^n - 1\}$. We can define an addition operation on Y_n. To add two elements in Y_n, first convert each of them into binary number with n bits, then add them bit-by-bit (mod 2). The resulting binary number is converted back into an element of Y_n. For example, if $n = 4$, then $Y_4 = \{0,1,2,\ldots,15\}$. To compute 7 + 9, we first convert 7 = 0111 in binary, and 9 = 1001 in binary. Then, by bit-wise addition (mod 2) we have 0111 + 1001 = 1110. Now, 1110 is identified with 14 in Y_4. Therefore, 7 + 9 = 14 in Y_n. Note that $a + a = 0$ for all a in Y_n.

If A (mod 2) is an $n \times n$ invertible matrix, then A can be viewed as an automorphism of $Z_{2,n}$. Hence, it induces an automorphism on Y_n. Since $A^2 = I \bmod 2$, the induced automorphism on Y_n has the property that a is mapped to b if and only if b is mapped to a. We write (ab) to denote a is mapped to b. Note that a is mapped to 0 if and only if a is 0.

We know that if $\frac{n}{2} \leq k \leq n$, then $T_k(2)$ contains all the elements in $S_n(2)$, which fixes a k dimensional subspace of $Z_{2,n}$. Hence, if A is in $T_k(2)$, then A fixes 2^k elements of $Z_{2,n}$. Therefore, the automorphism produced by A fixes 2^k elements of Y_n. Hence, the automorphism can be represented as

$$(00)(f_1f_1)(f_2f_2)\ldots\left(f_{2^k-1}\,f_{2^k-1}\right)(g_1g_1)(g_3g_3)\ldots$$

$$\left(g_{2^n-2^k-1}\,g_{2^n-2^k}\right)$$

where f_i's and g_i's are in Y_n. For example, if $n = 4$, and $k = 2$, then the elements of Y_4 can be written as $\{0, f_1, f_2, f_3, g_1, g_2 \ldots g_{12}\}$, and the induced automorphism can be represented as $(0,0)(f_1 f_1)\ldots(f_3 f_3)(g_1 g_2)(g_3 g_4)\ldots(g_{11} g_{12})$.

The following theorem is a generalization of Theorem 3.1 of [10]. The proof by Levine is actually a verification which has been made possible because of the small value $n = 3$ and because $S_3(2)$ has only 22 elements. Here we give a theoretical proof of this result.

Theorem 6.3.1

Let A be an $n \times n$ matrix over Z such that $A^2 = I \pmod 2$. If A is in $T_{n-1}(2)$, then the automorphism induced by A on Y_n can be represented as

$$(f_0 f_0)(f_1 f_1)\ldots\left(f_{2^{n-1}-1} f_{2^{n-1}-1}\right)(g_1 h_1)(g_2 h_2)\ldots\left(g_{2^{n-2}} h_{2^{n-2}}\right)$$

where f's, g's, and h's are in Y_n, and $f_0 = 0$. Further, there exists a ℓ with $1 \leq \ell \leq 2^{n-1} - 1$ such that $g_i + h_i = f_\ell$ for all $i = 1, 2, \ldots, 2^{n-2}$.

Proof

Since A is in $T_{n-1}(2)$, the automorphism induced by A on Y_n, fixes 2^{n-1} elements. Let them be $\{f_i : 0 \leq i \leq 2^{n-1} - 1\}$ with $f_0 = 0$. The remaining 2^{n-1} can be paired as $(g_i h_i)$ with $h_i = Ag_i$, $i = 1, 2, \ldots, 2^{n-2}$. Hence, the induced automorphism can be represented as

$$(f_0 f_0)(f_1 f_1)\ldots\left(f_{2^{n-1}-1} f_{2^{n-1}-1}\right)(g_1 h_1)(g_2 h_2)\ldots\left(g_{2^{n-2}} h_{2^{n-2}}\right).$$

It remains to be proven that there exists a ℓ with $1 \leq \ell \leq 2^{n-1} - 1$ such that $g_i + h_i = f_\ell$ for all $i = 1,2,\ldots,2^{n-2}$. Fix g_1, and consider the set $\{g_1 + f_i : i = 0,1,\ldots,2^{n-1} - 1\}$. Also consider the set $\{g_1,\ldots g_{2^{n-2}}, h_1,\ldots,h_{2^{n-2}}\}$. We note that the elements in each one of these two sets are distinct, each set has 2^{n-1} elements, and none of the elements is fixed by the induced automorphism. Hence, the above sets are identical. Therefore, given any i and j with $1 \leq i,j \leq 2^{n-2}$, there exist r and s with $0 \leq r,s \leq 2^{n-1} - 1$ such that $g_i = g_1 + f_r$ and $g_j = g_1 + f_s$. Hence,

$$g_i + g_j = g_1 + f_r + g_1 + f_s$$
$$= f_r + f_s, \text{ in } Y_n$$

Thus, $$Ag_i + Af_j = Af_r + Af_s$$
$$= f_r + f_s$$

i.e. $$h_i + h_j = f_r + f_s$$
$$= g_i + g_j$$

i.e. $$g_i + h_i = g_j + h_j \text{ (as (mod 2) addition)}$$

for all i and j. Further, $A(g_i + h_i) = Ag_i + Ah_i = h_i + g_i$ for all i. Therefore, $g_i + h_i$ is fixed by A. Hence, there exists an ℓ with $1 \leq \ell \leq 2^{n-1} - 1$ such that $g_i + h_i = f_\ell$ for all $i = 1,2,\ldots,2^{n-2}$. Thus, the theorem is proved.

We remark that $|T_{n-1}(2)|$ can be obtained as a consequence of the above theorem. Moreover, if A is in $T_n(2)$ then A is the identity automorphism of Y_n.

Proposition 6.3.2

Let A be a matrix in $S_3(2p)$ with p an odd prime. Then,

(i) the determinant d of A is $\pm 1 \pmod{2p}$,

and (ii) the trace t_0 of A is either 3d or -d (mod 2p).

Proof

Since $A^2 = I \pmod{2p}$, the eigen values are the solutions of the polynomial equation $x^2 - 1 = 0 \pmod{2p}$. i.e., the eigen values are $\pm 1 \pmod{2p}$. If x_1, x_2, x_3 are the eigen values, then determinant $d = x_1x_2x_3 = \pm 1 \pmod{2p}$ as $x_i = \pm 1 \pmod{2p}$ for $i = 1,2,3$. Note also that the trace $t = x_1 + x_2 + x_3 \pmod{2p}$.

Also, the characteristic equation could be written as

$$x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_2x_3 + x_3x_1)x - x_1x_2x_3 = 0 \pmod{2p}.$$

i.e. $$x^3 - tx^2 + dtx - d = 0 \pmod{2p}$$

i.e. $$A^3 - tA^2 + dtA - dI = 0 \pmod{2p}$$

ie. $$A - tI + dtA - dI = 0 \pmod{2p}$$

i.e. $$A(1 + dt) = (t + d)I \pmod{2p}$$

Taking trace on both sides we get,

$$t(1 + dt) = 3(t + d) \pmod{2p}$$

i.e. $$dt^2 - 2t - 3d = 0 \pmod{2p}$$

i.e. $(t + d)(t - 3d) = 0 \pmod{2p}$ (as $d^2 = 1 \pmod{2p}$)

i.e. $t = -d$ or $3d \pmod{2p}$.

Note that there is only one matrix in $S_3(p)$ with trace $t = 3 \pmod{p}$, and only one matrix in $S_3(p)$ with $t = -3 \pmod{p}$. Also, $S_3(2)$ contains 22 elements. Hence, there are $2 \cdot 22 = 44$ matrices in $S_3(2p)$ with trace $t = 3d \pmod{2p}$.

Thus, if the key matrix in $S_3(2p)$ has the property that $t = 3d \pmod{2p}$, then an exhaustive search would reveal the key matrix.

An easier way is the following:

If A is $S_3(2p)$ with $t = 3d \pmod{2p}$, then $A = \pm I \pmod{p}$. For each cipher block C, if P is the corresponding plain-text block then, $P = AC = \pm C \pmod{p}$. i.e., $P = \pm C + \ell p$ with $\ell = 0,1$. Hence, $P = \pm C$ or $P = \pm C + p$. Thus, forming the four plain-text, $\pm C$, $\pm C + p$, one can look at them and choose a meaningful plain-text. See [10] for more details.

If the key matrix A is in $S_3(2p)$ with the property that $t = -d \pmod{2p}$, then the method of determining A is in two steps: first find the (mod 2) solutions, and then extend them to (mod 2p) solutions.

Every block of 3 letters would be converted to an element in Y_3. Let f be the one-to-one and onto mapping from the alphabets V to Z_{2p}. Consider the induced mapping f from V to Z_2. i.e., $f_I(A_1) = f(A_1) \pmod 2$ for all A_1 in V. For a 3-gram PQR, $f_1(PQR) = (f_1(P)f_1(Q), f_1(R)) \pmod 2$ in $Z_{2,3}$. The resulting element is identified with an

element in Y_3. For example, let m = 26, and V be the English alphabets and f be the map f(A) = 0, f(B) = 1, ..., f(Z) = 25. Consider the text CRYPTOGRAPHYAND.

(i)	C	R	Y	P	T	O	G	R	A	P	H	Y	A	N	D
(ii)	2	17	24	15	19	14	6	17	0	15	7	24	0	13	3
(iii)	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1
(iv)		2			6			2			6			3	

Here (i) is the text to be transformed, (ii) is the corresponding number representation obtained using the mapping f, (iii) is the binary representation obtained using the reduced mapping f_1, and (iv) is the number representation obtained by identifying each block with an element in Y_3.

The probable-text is also converted into elements of Y_3. Then, we try to match this with the transformed cipher-text. We need two lemmas that give necessary conditions for a match.

Lemma 6.3.3

A necessary condition that a probable-text $a_1 \ldots a_\ell$ matches with a cipher-text $b_1 \ldots b_\ell$ is that the pairing $(a_1 b_1)(a_2 b_2) \ldots (a_\ell b_\ell)$ should be consistent with at least one of the automorphisms induced on Y_3 by elements of $S_3(2)$.

Lemma 6.3.4 (Rank Test)

If P and Q are two plain-text 3-grams and, C and D are corresponding cipher-text 3-grams, then the vectors AC + dC, and AD + dD are dependent. i.e., P + dC, and Q + dD are dependent. In other words, the determinant,

$$\begin{vmatrix} P_1 + dC_1 & P_2 + dC_2 & P_3 + dC_3 \\ Q_1 + dD_1 & Q_2 + dD_2 & Q_3 + dQ_3 \end{vmatrix} = 0 \pmod{2p}.$$

for $d = \pm 1 \pmod{2p}$.

Proof

Since trace of A is $-d \pmod{2p}$ we have the eigen values are 1,1,-1 or 1,-1,-1 according as $d = -1$ or $+1 \pmod{2p}$. In either case $A + dI$ has null space of dimension 2. Hence, $A + dI$ has rank 1. Hence, the lemma follows.

Even if Q_3 is not known, the above lemma gives a useful test, i.e., the determinant

$$\begin{vmatrix} P_1 + dC_1 & P_2 + dC_2 \\ Q_1 + dD_1 & Q_2 + dD_2 \end{vmatrix} = 0 \pmod{2p}.$$

It is easy to observe that if ℓ is the length of the probable text, then the rank test is applicable for $\ell \geq 6$. In some exceptional cases ℓ may be < 6. Refer to [10] for more details.

A comprehensive listing of tests that can be used when $5 < \ell < 8$ is given on page 15 of [10]. When $\ell \geq 8$, we have at least 8 congruence equations to solve for the 9 unknowns. Along with the fact that the determinant is ± 1 we may be able to solve for A. It may be possible to solve even if $\ell = 4$ under certain special circumstances. These are explained in [10].

6.4 Probabilistic Algorithm for any m,n

Although Levine has given some analysis for n = 2,3 and m = 26, his methods cannot be extended for any m, except for m = 2p (where p is an odd prime) even for n = 2 or n = 3.

It is obvious that increasing n gives more security of the cryptosystem. Also, if we want to use this cryptosystem for different languages, then it is essential that we know the analysis for any m, the alphabet size.

As we have proved (through $s_n(m)$) that an exhaustive search for the key matrix is impractical, the method of probable word seems to be the only alternative. We have explained in section 6.1 the three main steps involved in such a method.

We propose here a naive probabilistic approach which we believe to be a general and appropriate method for cryptanalysis.

We assume that we have a frequency table of occurrences of n-grams of the language used in the cryptogram. It is expected that the n-grams in this table with "high" relative frequencies would occur in most of the sample plaintexts. It is also expected that in a specific sample plaintext, the n-grams with high relative frequencies in this text are in correspondence with the n-grams with high relative frequencies in the table.

Further, since the matrix used satisfies the equation $A^2 = I \pmod m$, the relative frequency of an n-gram U in a plain-text is the same as the relative frequency of the

n-gram AU in the corresponding cipher-text. Hence, it is expected that the n-grams with high relative frequencies in the cipher-text are in correspondence with the n-grams with high frequencies in the population table. This is the basic principle we rely upon.

We order the n-grams of the population table in decreasing order of their relative frequencies, and call this ordered table as a <u>population table</u>. Let α be the highest value of the relative frequencies of this table. For an $\varepsilon > 0$ we classify the population table as follows:

$$\text{category 1} = \left\{\begin{array}{l}\text{all n-grams having relative frequencies} \\ \text{in between } \alpha - \varepsilon \text{ and } \alpha.\end{array}\right\}$$

$$\text{category 2} = \left\{\begin{array}{l}\text{all n-grams having relative frequencies} \\ \text{in between } \alpha - 2\varepsilon \text{ and } \alpha - \varepsilon.\end{array}\right\}$$

In general, for an integer i

$$\text{category i} = \left\{\begin{array}{l}\text{all n-grams having frequencies between} \\ \alpha - i\varepsilon \text{ and } \alpha - (i-1)\varepsilon.\end{array}\right\}$$

Note that there are only a finite number of such categories. If ε is chosen too small some of the categories may even be empty. We assume that ε is chosen such that none of the categories is empty. These categories are called <u>population categories</u>.

Next we consider the cipher-text and form a table of frequencies of occurrences of the n-grams from the cipher-text. (This table is of size at most m^n. But in practice it would be much less than m^n.) We then form the relative frequency table from this table, and order the n-grams in

descending order of their relative frequencies. This table is called a sample table. We want to classify these n-grams into categories. We may group all the n-grams with the same relative frequency into one category, and thus form as many categories as there are different relative frequencies. If the cipher-text is large, we may end up with too many categories. In that case, we form the categories based on some $\varepsilon > 0$ as we did before. In any case, the sample table is partitioned into distinct categories known as sample categories.

Let $P_1, P_2, \ldots, P_r$ be the population categories, and $S_1, S_2, \ldots, S_s$ be the sample categories. By the principle that we have already explained, it is highly probable that an n-gram in the category S_1 is mapped into an n-gram in the category P_1 by the key matrix. Let $P_1 = \{u_1, u_2, \ldots, u_{r_1}\}$, and $S_1 = \{v_1, v_2, \ldots, v_{s_1}\}$. Then, consider the following system of equations:

$$\left.\begin{aligned} Au_1 &= v_1 \pmod m, \\ Av_1 &= u_1 \pmod m, \\ A^2 &= I \pmod m. \end{aligned}\right\} \quad \ldots\ldots\ldots\ldots (6.10)$$

Consider a solution A to the system (6.10). We apply A to a sizable portion of the cipher-text. If it produces a meaningful plain-text, then A is the key matrix; otherwise, we discard that solution for A. We repeat this procedure until we find the key matrix or all the solutions to (6.10) are discarded.

If the key matrix has not yet been found, we solve the following system:

$$\left.\begin{aligned} Au_i &= v_j \pmod m \\ Av_j &= u_i \pmod m \\ A^2 &= I \pmod m \end{aligned}\right\} \quad \ldots\ldots\ldots\ldots (6.11)$$

for some i and j with $1 \leq i \leq r_1$ and $1 \leq j \leq s_1$. If we have not found the key matrix even after solving (6.11) for all possible pairs (i,j), we repeat the process with categories S_1 and P_2. In general, we try with the pair (S_1,P_ℓ) when the pair $(S_1,P_{\ell-1})$ does not give the solution to the key matrix. After exhausting all P_i, if necessary, we try with $(S_2,P_1),(S_2,P_2),\ldots\ldots$ It seems that at most 4 or 5 category pairs need to be tried before finding the key matrix.

A formal algorithm to test these procedures is given below:

(1) {initialize}

i ← 1; j ← 1 {used as indices}

found ← false {used as a flag to terminate the procedure, if we have obtained the key matrix}

```
(2)  While (i ≤ r) and not found do
     begin
        P ← P_i        {get the next population category}
(3)     While (j ≤ s) and not found do
        begin
              S ← S_j  {get the next sample category}
(4)           Repeat
                 u ← next n-gram in P
(5)              Repeat
                    v ← next n-gram in S
(6)                 Solve the system:
                       Au = v (mod m)
                       Av = u (mod m)
                       A^2 = I (mod m)
(7)                 for the matrix A.
                    Apply A to a sizable cipher-text.
(8)                 If it produces meaningful message,
                    then A is the key matrix and found
                    ← true;
              until (found) or (no more n-gram left in S)
           until (found) or (no more n-gram left in P)
(9)        j := j + 1
        end; {while}
(10)    i := i + 1;
     end; {while}
```

The complexity of this approach is mainly dominated by the cost of the procedure that solves the system of equations (6.11). The worst case cost is very high for large n. However, the average cost is of interest and relevant to cryptanalysis. By average cost we mean the expected number of category pairs examined, and the expected number of equations to be solved before the key matrix is found. We do not have any theoretical results in this direction, and hence it still remains an open problem.

We have tested this approach on several small sample texts with n = 2, m = 27. The alphabet includes the blank character and the English alphabet. We used the frequency of occurrence of 2-grams obtained from [19]. A random message was encrypted using $\begin{pmatrix} 5 & 3 \\ 19 & 22 \end{pmatrix}$, $\begin{pmatrix} 22 & 4 \\ 21 & 5 \end{pmatrix}$, and $\begin{pmatrix} 22 & 2 \\ 15 & 5 \end{pmatrix}$, and three cipher-texts were obtained. The probabilistic method given above required the solution of 37 different systems of equations on the first text before finding the key matrix $\begin{pmatrix} 5 & 3 \\ 19 & 22 \end{pmatrix}$, 31 different systems of equations were solved on the second text before finding the key matrix $\begin{pmatrix} 22 & 4 \\ 21 & 5 \end{pmatrix}$, and 42 different systems were required to be solved for the third cipher-text before finding the key matrix $\begin{pmatrix} 22 & 2 \\ 15 & 5 \end{pmatrix}$ correctly. These results combined with the Levine's results [10] do convince that the security of the crypto-system based on involutory matrices is weak for small values

of n. Although our method is general, n-gram frequencies for $n \geq 4$ are needed for an exhaustive testing, and this also remains to be done.

Finally, we remark that if $n = 2$, then (6.11) may be easily solved as explained in section 6.2.

CHAPTER VII

Security of Networks - An Application of Linear Algebraic Cryptography

There is ever increasing growth in the number of computer networks, and in the kinds of distributed computing applications available on those computer networks. Hence, it is essential to have secure communication facilities.

A general approach to the security problem in communication networks is to use some encryption method to send the messages. Of course, the strength of such an approach relies on the encryption methods available.

In [13], Needham and Schroeder have presented network protocols based on both conventional and public-key cryptosystems. Though initially it was believed that the network protocols based on a public-key system would be more suitable than the protocols based on conventional system, later it was observed that the public-key system does not provide any significant advantage over the protocols based on the conventional encryption methods. Hence, it has been speculated that if strong conventional algorithms are easy to develop, research would be better devoted to that area rather than public-key systems (see page 152 [15]).

In this chapter we describe in section 7.1 the network protocols as presented by Needham and Schroeder [13]. In section 7.2, we investigate the suitability of matrix based conventional encryption method for communications in

a network. Clearly, the results that we have obtained in the previous chapters play an essential role in this investigation.

7.1 Network Protocols - A Brief Review

A communication network should serve the following three functions:

(i) Establishment of authenticated interactive communication between two participants in the network.

(ii) An authenticated one-way communication between two participants such as the electronic mail system.

(iii) Signed communication (i.e., digital signature) in which the origin of a communication, and the integrity of content can be authenticated by a third party.

By network protocols we mean the procedures explaining how one more of the above three functions are done in a network.

Considering the security of a communication network, we classify the malicious activities disturbing the secure communication mainly into the following types:

(a) Tapping of lines: This refers to recording of a message passing through a communication line without detection by the sender or the receiver.

(b) Introduction of spurious messages: This refers to introducing invalid messages with valid addresses into

the communication lines of an operating network.

(c) Replay of messages: Given that it is possible both to record and introduce messages into communication lines of a network, it is therefore possible to retransmit a copy of a previously transmitted message.

(d) Disruption: It is possible that the delivery of selected messages may be prevented, or portion of messages may be altered, or even a complete blockage of communication path may occur.

Each of the preceding threats can cause considerable damage to an operating network. Tapping of lines leads to loss of privacy in communication; introduction of false messages leads to suspect the authenticity of received messages; retransmission leads to confusion under certain circumstances, and disruption leads to inconsistent messages. When the security of a communication network is to be measured, it is better for it to be analysed primarily against the above mentioned malicious activities.

We explain below the protocols necessary for a mutual authentication of two participants who wish to communicate in the network. This is a process for a participant to assure himself of the identity of the other participant. Whether the protocols are based on the conventional encryption method or based on public-key encryption method, the authentication involves the secret keys of the participants. Hence, there is a need for a central authoritative source of information about these keys. The term authentication

server (AS) is used for such a source. We restrict our discussion to protocols based on the conventional encryption algorithms.

Each participant in the network has a secret key that is known only to himself and the authentication server. Sometimes we call these secret keys as identification keys. The essential step in setting up a secure communication between two participants A and B with A as the initiator is to generate a message with the following two properties:

(a) It must allow only B to identify himself to A.

(b) It must be evident to B that it originates from A.

For the sake of simplicity, let us first assume that both A and B have the same authentication server AS. Let KA and KB be the secret keys of A and B respectively. Let $E_K(M)$ denote the encryption of a message M with a key K. The protocols involve 5 steps. We summarize all the steps involved with A as the initiator who wants to communicate with B.

Step 1

A sends the message

$$M1 = (A,B,IA1) \quad \ldots\ldots\ldots\ldots\ldots (7.1)$$

to the authentication server AS. The entry A in the message identifies the initiator A to the AS, and the entry B identifies the participant with whom A wnats to communicate. The entry IA1 is an identification chosen by A to be used

only in this message, and it is used only once. Its use would be more clear in Step 2.

Step 2

Upon receiving the message M1, the authentication server identifies that the initiator is A and that he wants to communicate with B. Then, AS looks up the secret keys KA and KB of A and B respectively, and then computes a communication key CK to be used as the encryption key for the communication between A and B. Then, AS sends the message:

$$M2 = E_{KA}(IA1, B, CK, E_{KB}(CK, A)) \quad \ldots\ldots\ldots (7.2)$$

Note that M2 is the encryption of some message that contains the communication key. Upon receiving the message from AS, A can decode it using his secret key KA. Then, he checks for the correct name B with whom he wants to communicate. He also checks for the correct identification IA1 to verify that the message M2 is really a reply from AS to his message in (7.1). This is the reason why IA1 should not be used more than once.

Further, both B and IA1 should be present in the message (7.2); otherwise an intruder could change the name in the message (7.1), say to X, then unknowingly A would have been communicating with X instead of B. If the identification IA1 is left out, then an intruder may replay a previously recorded message (from AS to A about B), and then forcing A to use a previously used communication key.

Step 3

After decoding M2, and making verification of B and IA1, A retains the communication key CK to himself, and sends the message

$$M3 = E_{KB}(CK,A) \quad \ldots\ldots\ldots\ldots\ldots\ldots (7.3)$$

along the communication line to B.

Note M3 is encryption of some message that contains communication key. On receiving the message M , B decrypts it using his own secret key KB, and understands that A wishes to communicate with him, and that CK is the communication key selected by the AS. However, B must make sure that the message is not a replay. i.e., the key CK is originally from A, not from an intruder who is replaying the old message giving an old key. On the other hand, A is quite sure that any communication from B is encrypted using CK and any message encrypted using CK is from B.

Step 4

B sends the following message to A:

$$M4 = E_{CK}(IB1) \quad \ldots\ldots\ldots\ldots\ldots\ldots (7.4)$$

where IB1 is an identification, say a number, chosen by B, and is used only once. Thus, M4 is used as an identification of B to A.

Step 5

To acknowledge the identification, A sends back the message

$$M5 = E_{CK}(IB1 - 1) \quad \ldots\ldots\ldots\ldots (7.5)$$

to B. If this message is satisfactorily received by B, then the mutual confidence is established to enable the communication using the key CK.

In a practical communication network, it is natural and desirable to have multiple authentication servers. See [13] for details regarding protocols in such situations. We wish to stress here that every message in a protocol requires at least one key, and different messages sent at the same time or at different times require different keys even for establishing communication.

7.2 Network Protocols - A Proposal Using Involutory Matrices

In this section we investigate the suitability of adapting the conventional encryption method based on involutory matrices in a communication network. We follow the protocols that are explained in the previous section.

Recall that, if a participant wants to communicate with another participant, then he has to send a message to the authentication server requesting for an encryption key to be used in the communication. The authentication server then computes a key for the communication and sends it to the requesting participant.

We shall discuss some suitable methods for a key generation by an authentication server. Note that every participant A in a communication network must have a unique and secret identification key. In our discussion, we denote this identification key of A by A itself. Moreover, a communication between any two participants requires a key which is time varying. In general, it is desirable to have the keys satisfying the following properties:

(i) Keys of all the participants are distinct, and of the same nature; i.e., if the keys are permutations, then all the participants will have distinct permutation as secret keys.

(ii) If a participant A in a communication network wants to initiate a communication with another participant B in the same network, then the communication key generated by the authentication server will be denoted by $A \rightarrow B$. This key must be of the same nature as A and B. Moreover, we require that it is a function of A and B.

(iii) Suppose two participants A and B are communicating with a communication key $A \rightarrow B$; it should be computationally intractable to find the secret key A (the secret key B) from knowledge of $A \rightarrow B$ and the secret key B (the secret key A).

(iv) Each communication key shall be used only once in its lifetime.

We remark that, if B wants to initiate the communication with A (instead of A initiating the communication with B), then the key $B \to A$ generated by the authentication server need not be necessarily the same as $A \to B$.

Note that the secret keys of a participant is used as an encryption key mainly in the communication between a participant and the authentication server. Thus, property (i) makes a uniform communication possible between any participant and the authentication server.

The efficiency of the requirement that a communication key be of the same type as that of the participants involved in such communications, depends on the available hardware configuration, and also on the software required for the key management. Requiring that a communication key be dependent on the keys of the participants leads to the investigation of functions with some desirable properties, which in turn may lead to the results of intractability and security.

Property (iii) is essential to have privacy and security in communications between a participant and the authentication server. Property (iv) is desired because this requirement prevents a replay of a previously recorded message. For example, if the network lines are vulnerable to tapping and introduction of false messages, then the use of the same key for more than one communication may lead to the possibility of replaying an old message that has been tapped in a previous communication where the same key is used.

Now, we investigate several ways of implementing the network protocols using involutory matrices as keys. Let m be the size of the alphabet that is used in a communication, and let n be the block length available in the existing hardware used in a communication.

Strategy 1

The authentication server manages two files. The file which contains the secret keys of the participants with their addresses is called prime-file. To begin with, the authentication server generates a "large" number of matrices in $S_n(m)$, and stores them in a secondary-file. When a participant joins his network, the authentication server selects randomly a matrix from the secondary-file, and assigns this matrix as the secret key of that participant. He adds this key into the prime-file, and deletes it from the secondary-file. Thus, at any time, the prime-file contains the secret keys of the participants in the network, and the secondary-file contains the matrices that could be used either as secret keys or as communication keys.

If a participant requests for a communication key to communicate with another participant, the authentication server picks up a matrix at random from the secondary-file, and assigns it as the communication key, and then he deletes this key from the secondary-file.

By computing a random index as a function of the secret keys of the participants, the key matrix identified by this index in the secondary-file can be allocated as the

communication key. Hence, the authentication server has the overhead of not only the initial generation of matrices in $S_n(m)$, but also maintenance and updating the files every time a communication is initiated. It is easy to see that all the properties except the intractability criteria are satisfied. In view of the order of magnitude of $s_n(m)$, we comment that probabilistically the chances of a participant computing or inferring the secret key of the other participant are very slim.

Strategy 2

Let A and B be two $n \times n$ matrices over Z_m such that $A^2 = B^2 = I \pmod m$, and $AB \neq BA \pmod m$. Then define,

$$F(A,B) = \{(AB)^{2k}A \pmod m : k = 1,2,3,\ldots\},$$

and $$G(A,B) = \{B(AB)^{2k} \pmod m : k = 1,2,3,\ldots\}.$$

Note that the matrices in F(A,B) are all similar to A, and that the matrices in G(A,B) are all similar to B.

When a participant A wants to communicate with another participant B, the authentication server chooses a random integer $k \geq 1$, and then at random allocates the communication key $A \rightarrow B$ either from F(A,B) or from G(A,B).

In this strategy, properties (i) and (ii) are obviously satisfied. However, we need further analysis to establish the validity of properties (iii) and (iv). We consider several cases in order.

Case (i)

Assume that the communication key for participants A and B at one time is chosen from F(A,B) on the basis of a

random integer k, and at another time it is chosen from G(A,B) on the basis of another random integer ℓ. In this situation B knows the communication keys $C = (AB)^{2k}A \pmod m$, and $D = B(AB)^{2\ell} \pmod m$. Below, we analyse the complexity involved in B finding the secret key of his communication partner A. By symmetry, the analysis of the complexity involved in A finding the secret key of B is the same.

Note that elements of F(A,B) and G(A,B) have the involutory property. Rewriting C as $A(BA)^{2k} \pmod m$, and observing that $BDB = (AB)^{2\ell-1}A \pmod m$, we have

$$\begin{aligned} CBDB &= A(BA)^{2k}(AB)^{2\ell-1}A \pmod m \\ &= (AB)^{2k}\cdot A\cdot A(BA)^{2\ell-1} \pmod m \\ &= (AB)^{2k}\cdot(BA)^{2\ell-1} \pmod m \\ &= (AB)^{2(k-\ell)+1} \pmod m \quad \ldots\ldots\ldots\ldots (7.6) \end{aligned}$$

Suppose that k and ℓ are different; then (7.6) can be written as $X^r = Y \pmod m$ where $X = AB \pmod m$, $Y = CBDB \pmod m$, and $r = 2(k - \ell) + 1$. The participant B must then have to find an $n \times n$ matrix X, and an exponent r with $|r| \geq 3$. At this stage, we are not aware of either the existence or the enumeration of such matrices for such a problem, even when the exponent r is known.

It seems that for the case when r is known and X is unknown, one can try to solve the reduced equations for the prime power modulii occurring in the factorization of m, and then reconstruct X using the Chinese Remainder Theorem. Consider the simple case when $m = 2p$ with p an odd prime,

and assume that r is known. Then, by finding two matrices X_1 and X_2 which are solutions of the matrix equations $X_1^r = Y_1 \pmod 2$, and $X_2^r = Y_2 \pmod p$ where $Y_1 = Y \pmod 2$ and $Y_2 = Y \pmod p$, one may solve the equation $X^r = Y \pmod{2p}$ for X. The apparently simple equation $X_1^r = Y_1 \pmod 2$ may itself be too difficult to solve.

Summing up, we conclude that strategy 2 can provide a high degree of security in protection of confidentiality of the identification keys in a network. However, more complexity analysis is required before we declare that total security is assured.

If $\ell = k$, then from (7.6) we have $CBDB = (AB) \pmod m$. Since B knows the keys C,D and his own identification key, he knows A. However, we foresee that the probability of this event to be very small for the following reasons:

Let e be the period of (AB). i.e., e is the smallest positive integer such that $(AB)^e = I \pmod m$. Since $(AB)^{-1} = B^{-1}A^{-1} = BA \neq AB$, we have $(AB)^2 \neq I \pmod m$. Hence, $e \geq 3$. Observe that e divides $g_n(m)$, the number of $n \times n$ nonsingular matrices over Z_m. The probability of choosing k and ℓ in the range 1 to $\frac{e}{2}$ such that $k \neq \ell$ is $1 - \frac{2}{e}$. If e is large, then this probability is close to 1, assuring that almost all the time ℓ and k would be chosen differently. The strength of this depends on the answer to the question whether there exists noncommutative involutory matrices A and B (mod m) such that AB (as well as BA) has a large period.

Case (ii)

Assume that the communication keys allocated at two different times are from F(A,B) based on two random integers k and ℓ. Then, $C = (AB)^{2k}A \pmod m$ and $D = (AB)^{2\ell} A \pmod m$ are known to both A and B. Then $CD = (AB)^{2(k-\ell)} \pmod m$. Hence, if B(A) wants to find the key of A(B) by knowing C and D, then an equation of the form $X^{2r} = Y \pmod m$ has to be solved for a given Y to find both X and r with $|r| \geq 1$ $(k \neq \ell)$. Analysis similar to Case (i) holds.

Next, we consider the property (iv) for the strategy 2. It states that the communication keys should be different at different times of communication in the network. First of all, consider two different communications between any two participants A and B. Let us assume the worst case: the first communication key be chosen from F(A,B) for some k, and the second be also chosen from F(A,B) for some ℓ. The question is whether $(AB)^{2k}A = (AB)^{2\ell}A \pmod m$, $(k \neq \ell)$. Note that it is equivalent to the question, $(AB)^{2(k-\ell)} = I \pmod m$ with $k \neq \ell$? Since AB is not an involutory matrix, it is not possible that $(AB)^{2(k-\ell)} = I \pmod m$ for arbitrary k and ℓ. Further, if k and ℓ are chosen in the range 1 to $\frac{e}{2}$ (where e is the period of AB) then $2|k - \ell|$ cannot be divisible by e. Hence, $(AB)^{2(k-\ell)} \neq I \pmod m$ unless $k = \ell$. But, probability of choosing ℓ and k such that $\ell \neq k$ is $O(\frac{1}{e})$ which is very small when e is large. Hence, the probability of getting two different keys from F(A,B) for two different communications remains large if e is large.

Next, we comment on the abundance of available keys for distribution, and on the probability of assigning distinct keys for communications between distinct pairs of participants. Let a pair A,B of participants communicate with a key, say $(AB)^{2k}A$, and another pair P,Q communicate with a key, say $(PQ)^{2\ell}P$, where A,B, P,Q are all distinct. Then it is highly likely that the two communication keys are distinct. We have insisted that the identification keys of participants are noncommutative in pairs. Hence, in order to establish an abundant availability of identification, it is essential to investigate the size of the set of non-commutative involutory matrices over Z_m. At present, we believe that it is an open problem.

Finally, let us comment on the security of communicated message when the same message M is sent either in two different communication lines or in the same line at two different times. Let K_1 and K_2 be the involutory matrices that are used as keys in these communications. Assume that an intruder has tapped both the cipher-messages K_1M and K_2M; and he knows that they are encrypted versions of the same message. Let $C_1 = K_1M$ and $C_2 = K_2M$. By the involutory property of K_1 and K_2, we have $K_1C_1 = K_2C_2 = M$. Thus, $K_2K_1C_1 = C_2$. Putting $K = K_2K_1$, we get $KC_1 = C_2$. Note that, the intruder knows C_1 and C_2. Hence, it is probably easy to solve for the matrix K, if the message has at least n^2 letters, i.e., if it has n blocks of length n each. Let $P_1,\ldots,P_n$ be n-blocks in C_1, and let $Q_1,\ldots,Q_n$ be n-blocks

in C_2 such that

$$KP_i = Q_i \pmod m , \quad i = 1,2,\ldots,n \qquad \ldots\ldots\ldots(7.7)$$

Then, (7.7) can be solved uniquely for K if the blocks $P_1,\ldots,P_n$ (equivalently $Q_1,\ldots,Q_n$) are linearly independent over Z_m. Since the probability of getting n independent blocks in a sufficiently large message is close to 1, we may say that K can be obtained with probability 1.

The hardest problem is to find the involutory matrices K_1 and K_2 such that $K = K_2K_1 \pmod m$. Since $K^{-1} = K_1K_2 \pmod m$, we have $KK_1 = K_2 = K_1K^{-1} \pmod m$ and $KK_2 = K_2K_1K_2 = K_2K^{-1} \pmod m$. Thus, K_1 and K_2 are two involutory solutions of the matrix equation $KX = XK^{-1} \pmod m$. Solving this equation for all possible solutions X is equivalent to solving a system of n^2 linear equations over Z_m. Note that if X is a solution, then $Y = KX \pmod m$ is also a solution; further, if X is an involutory solution, then Y is also an involutory solution, and $YX = K \pmod m$. Thus, every involutory solution gives a factorization of K as a product of two involutory matrices. Hence, for a given nonsingular matrix K, the problem of finding two involutory matrices K_1 and K_2 is equivalent to solving the matrix equation

$$KX = XK^{-1} \pmod m \qquad \ldots\ldots\ldots\ldots(7.8)$$

with X an involutory matrix over Z_m.

Let e be the period of K (i.e., e is the smallest positive integer such that $K^e \equiv I \pmod m$). For any non-singular matrix Q we claim that the matrices $Q, KQ, K^2Q, \ldots, K^{e-1}Q$ are distinct. For, if $K^iQ \equiv K^jQ \pmod m$ with $0 \leq i, j < e$ and $i \neq j$ then $K^{i-j}Q \equiv Q \pmod m$. Without loss of generality we may assume $i > j$. Hence, the above equation implies $K^{i-j} \equiv I \pmod m$, and hence the period of K divides $i - j$ which is impossible as $1 \leq i - j < e$. Thus, if X_0 is an involutory solution to (7.8) then the matrices

$$X_0, KX_0, K^2X_0, \ldots, K^{e-1}X_0 \quad \ldots\ldots\ldots\ldots (7.9)$$

are also involutory solutions to (7.8) and they are distinct. In fact, we call this set of e matrices as the cycle induced by X_0. Therefore, if we define an equivalence relation in the set of all involutory solutions to (7.8), then each of the equivalence classes is a cycle of length e as given in (7.9).

Example

Let $m = 5$ and $n = 2$. Let the key matrices used be $K_1 = \begin{pmatrix} 3 & 2 \\ 1 & 2 \end{pmatrix} \pmod 5$, and $K_2 = \begin{pmatrix} 4 & 3 \\ 0 & 1 \end{pmatrix} \pmod 5$. Then,

$K = K_2K_1 = \begin{pmatrix} 0 & 4 \\ 1 & 2 \end{pmatrix} \pmod 5$, and $K^{-1} = K_1K_2 = \begin{pmatrix} 2 & 1 \\ 4 & 0 \end{pmatrix} \pmod 5$.

Further, let $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod 5$. Then, $KX = XK^{-1} \pmod 5$ implies $a \equiv 4d \pmod 5$ and $b \equiv c + 3d \pmod 5$. Hence,

$$X = \begin{pmatrix} 4d & c + 3d \\ c & d \end{pmatrix} \pmod 5 \quad \ldots\ldots\ldots (7.10)$$

Now, this X is involutory if and only if $c^2 + d^2 + 3cd \equiv 1 \pmod 5$. This equation has 10 solutions for the pair (c,d) with c,d in Z_5 as listed below:

(0,1) (0,4), (1,0), (1,2), (2,1), (2,3), (3,2), (3,4), (4,0), (4,3).

Note that the pair (1,2) corresponds to K_1, and the pair (0,1) corresponds to K_2.

It could be verified that the period of K is 5. Thus, the above 10 involutory solutions are decomposed into two disjoint cycles of length 5. We give the cycles in terms of the pairs (c,d). The actual matrices can be obtained from (7.10).

Cycle 1: (1,2), (0,1), (4,0), (3,4), (2,3)

Cycle 2: (2,1), (3,2), (4,3), (0,4), (1,0).

Note that any two consecutive pair in each cycle gives a factorization of K. Thus, there are 10 such factorizations of K. However, we have used K_1 (the pair (1,2)) and K_2 (the pair (0,1)) as our communication keys. Hence, even after knowing the cycle structure of involutory solutions to $KX = XK^{-1} \pmod 5$, in this case, the probability of getting the actual matrices that are used is $\frac{1}{10}$.

We comment that the amount of work involved in general, in finding the involutory solutions and the cycle structure is not known. The only result known in this direction is the following theorem (see [11]):

Theorem 7.2.1

Let m be a square free integer, and K be a non-singular matrix over Z_m. If two matrices K_1 and K_2 are

are drawn at random with replacement from the set $S_n(m)$, then the probability that $K_2K_1 = K \pmod m$ is

$$\frac{g_n(m)}{(s_n(m))^2} \cdot \frac{N(K)}{C(K)} \quad \ldots\ldots\ldots\ldots\ldots\ldots (7.11)$$

where $C(K)$ is the number of invertible solutions, and $N(K)$ is the number of involutory solutions to the equation (7.8).

An exact value or a good bound of $\frac{N(K)}{C(K)}$, for a given K is not known. The value of ratio $\ell n(s_n(m))/\ell n(g_n(m))$ is shown in Table 7.1 for various prime values of m. These values make us believe that $s_n(m) = O(\sqrt{g_n(m)})$.

If the probability in (7.11) for a nonsingular matrix K is large, then we can conclude that there are a large number of involutory matrix pairs whose product is K. In such a situation finding the exact pairs K_1, K_2 used in communications may involve an enormous amount of work. On the other hand, if the probability given in (7.11) is small, then we may conclude that there are only a few involutory matrix pairs whose product is K. This implies that once a factorization of K is found they are most likely to be the actual pair used as keys. We remark that the actual process of identifying the keys is related to the enumeration of all the cycles, as in (7.9). Further, it seems that the allocation of communication keys must be done in such a way that for every pair K_i, K_j of involutory matrix keys, the product K_iK_j (equivalently K_jK_i) has large period. As remarked by us earlier, determining the period, and the cycle structure

of a product of noncommutative involutory matrices is an open problem.

Table 7.1

For a prime p and an integer n, an entry in the table is of the form $\boxed{\begin{matrix} x(r) \\ y(s) \\ z(t) \end{matrix}}$ and

$$g_n(p) = x(r) = x \cdot 10^r$$

$$s_n(p) = y(s) = y \cdot 10^s$$

$$\frac{\ln s_n(p)}{\ln g_n(p)} = z(t) = z \cdot 10^t$$

p \ n	2	3	4	5	6	7	8	9	10
	2.621(004)	9.726(009)	6.103(017)	6.472(027)	1.160(040)	3.513(054)	1.798(071)	1.555(090)	2.274(111)
13	1.840(002)	6.204(004)	8.991(008)	5.078(013)	1.241(020)	1.184(027)	4.885(035)	7.876(044)	5.493(055)
	5.126(-01)	4.798(-01)	5.034(-01)	4.928(-01)	5.015(-01)	4.963(-01)	5.009(-01)	4.978(-01)	5.006(-01)
	1.231(005)	3.048(011)	2.725(020)	8.792(031)	1.024(046)	4.307(062)	6.538(081)	3.583(103)	7.089(127)
19	3.820(002)	2.755(005)	1.807(010)	4.686(015)	1.108(023)	1.037(031)	8.857(040)	2.992(051)	9.222(063)
	5.072(-01)	4.737(-01)	5.019(-01)	4.906(-01)	5.009(-01)	4.952(-01)	5.005(-01)	4.971(-01)	5.003(-01)
	6.821(005)	1.399(013)	2.413(023)	3.501(036)	4.271(052)	4.383(071)	3.782(093)	2.744(118)	1.675(146)
29	8.720(002)	1.466(006)	5.199(011)	7.338(017)	2.188(026)	2.596(035)	6.509(046)	6.497(058)	1.370(073)
	5.040(-01)	4.691(-01)	5.011(-01)	4.889(-01)	5.005(-01)	4.943(-01)	5.003(-01)	4.966(-01)	5.002(-01)
	8.928(005)	2.556(013)	7.032(023)	1.859(037)	4.724(053)	1.153(073)	2.707(095)	6.104(120)	1.323(149)
31	9.940(002)	1.910(006)	8.840(011)	1.630(018)	7.246(026)	1.284(036)	5.485(047)	9.337(059)	3.834(074)
	5.037(-01)	4.685(-01)	5.010(-01)	4.887(-01)	5.004(-01)	4.942(-01)	5.002(-01)	4.965(-01)	5.002(-01)
	1.822(006)	1.264(014)	1.200(025)	1.559(039)	2.774(056)	6.755(076)	2.253(100)	1.028(127)	6.426(156)
37	1.408(003)	3.854(006)	3.618(012)	1.354(019)	1.740(028)	8.914(037)	1.568(050)	1.100(063)	2.648(078)
	5.029(-01)	4.670(-01)	5.008(-01)	4.881(-01)	5.003(-01)	4.940(-01)	5.002(-01)	4.963(-01)	5.001(-01)
	2.755(006)	3.192(014)	6.217(025)	2.035(040)	1.120(058)	1.036(079)	1.611(103)	4.212(130)	1.851(161)
41	1.724(003)	5.794(006)	8.200(012)	4.628(019)	1.101(029)	1.044(039)	4.174(051)	6.658(064)	4.474(080)
	5.026(-01)	4.663(-01)	5.007(-01)	4.879(-01)	5.003(-01)	4.938(-01)	5.002(-01)	4.963(-01)	5.001(-01)
	7.739(006)	3.236(015)	3.802(027)	1.254(043)	1.163(062)	3.028(084)	2.214(110)	4.549(139)	2.625(172)
53	2.864(003)	1.609(007)	6.352(013)	1.002(021)	1.111(031)	4.921(041)	1.533(055)	1.908(069)	1.669(086)
	5.018(-01)	4.646(-01)	5.005(-01)	4.873(-01)	5.002(-01)	4.935(-01)	5.001(-01)	4.961(-01)	5.001(-01)

CHAPTER VIII

Conclusion

We have studied an effective conventional cryptographic method for the security of both dynamic and static data. Our interest is to study, investigate, and propose a cryptographic method arising out of a need for a strong conventional encryption method usable in a communication network. The main contribution of this thesis is an exact enumeration and characterization of involutory matrices over a ring of integers, and establishing their usefulness as cryptographic keys.

Our methods in Chapters IV and V are completely constructive. Hence, a key matrix of a desired structure can easily be generated. Although it is known that a linear algebraic transform such as the one we have considered seems to obscure the statistics of frequency of occurrences of word fragments, a more thorough statistical analysis than the one proposed for n = 2,3 (see [9],[10]) is required.

One of the major shortcomings of the currently practiced cryptography is the inability of proving the absolute security of the cryptosystems. Nowadays, one invokes the results in intractability to establish some degree of security of the cryptosystem. The real challenge is to provide rigorous assertions on the unbreakability of the system. We have related the problem of security in a communication network to algebraic problems, both deter-

ministically and probabilistically. To recall one of our results: we have shown that the complexity of finding the two distinct key matrices used in two different communication channels transmitting the same message is the same as that of finding involutory matrix factors of an arbitrary non-singular matrix over the ring of integers Z_m. To the best of our knowledge, this is an unsolved problem. We believe that finding all possible factors and then identifying the factors actually used in transmitting a message through two different channels, is computationally hard when the size of the matrix is large. The reader is referred to [7], where it is cautioned against resting the cryptocomplexity just upon the computational complexity. However, our suggested cryptocomplexity rests on an as yet unsolved mathematical problem. Both the existence and the size of the solution space of the equation $KX = XK^{-1} \pmod{m}$ would determine the extent of the security affordable in the network.

BIBLIOGRAPHY

[1] Diffie, W. and Hellman, M.E., "New Directions in Cryptography", IEEE Transactions on Information Theory, IT-22, pp.664-654, November 1976.

[2] Hellman, M.E., "The Mathematics of Public-Key Cryptography", Scientific American, pp.130-139, August 1979.

[3] Hill, L.S., "Concerning Certain Linear Transformation Apparatus of Cryptography", American Mathematical Monthly, 38, pp.135-154, March 1931.

[4] Hodges, J.H., "The Matrix Equation $X^2 + I = 0$ over a Finite Field", American Mathematical Monthly, 65, pp.518-520, 1958.

[5] Katzan, H., "The Standard Data Encryption Algorithm", Petrocelli Books Inc., 1977.

[6] Kohnheim, A.G., "Cryptography, A Primer", Wiley-Interscience, 1981.

[7] Lempel, A., "Cryptology in Transition", ACM, Computing Surveys, Vol. 11, No. 4, December 1979.

[8] Levine, J., "Some Elementary Cryptanalysis of Algebraic Cryptography", American Mathematical Monthly, 68, pp.411-418, 1961.

[9] _____, "Some Applications of High Speed Computers to the Case n = 2 of Algebraic Cryptography", Mathematics of Computation, 15, pp.254-260, 1961.

[10] _____, "Analysis of the Case n = 3 in Algebraic Cryptography with Involutory Key Matrix and Known

Alphabet", Journal Reine und Agenwante Mathematik, 213, pp.1-30, 1963/4.

[11] Levine, J. and Brawley, J.V., "Involutory Commutants with some Applicants to Algebraic Cryptography I", Journal Reine und Agendwante Mathematik, 224, pp.20-43, 1966.

[12] _____, "Involutory Commutants with some Application to Algebraic Cryptography II", Journal Reine und Agendwante Mathematik, 226, pp.1-24, 1967.

[13] Needham, R.M. and Schroeder, M.D., "Using Encryption for Authentication in Large Networks of Computers", ACM Communications, Vol. 21, Number 12, December 1978.

[14] Popek, G.J. and Kline, C.S., "Encryption Protocols, Public-Key Algorithms, and Digital Signatures in Computer Networks", Foundations of Secure Computation, Academic Press, 1978.

[15] _____, "Encryption and Secure Computer Networks", ACM Computing Surveys, Vol. 11, No. 4, December 1979.

[16] Rabin, M.O., "Digitalized Signatures", Foundations of Secure Computation, Academic Press, 1978.

[17] Rivest, R.L., Shamir, A. and Adleman, L.", A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", ACM Communications, Vol. 21, Number 2, February 1978.

[18] Simmons, G.J., "Symmetric and Asymmetric Encryption", ACM Computing Surveys, Vol. 11, No. 4, December 1979.

[19] Toussaint, G.T. and Shinghal, R., "Tables of Probabilities of Occurrence of Characters, Character-Pairs, and Character-Triplets in English Text", Technical Report No. SOCS 78.6, School of Computer Science, McGill University, Montreal, Canada.