On some Algorithms for Reverse Engineering Certain Finite Dynamical Systems

By

Edusmildo Orozco

This thesis is submitted for the partial fulfillment of the requirements for the

Doctor of Philosophy in

Computing and Information Sciences and Engineering

UNIVERSITY OF PUERTO RICO

MAYAGUEZ CAMPUS

2005

Approved by:

Dorothy Bollman, Ph.D President, Graduate Committee	Date
Oscar Moreno, Ph.D Member, Graduate Committee	Date
Wilson Rivera, Ph.D Member, Graduate Committee	Date
Domingo Rodríguez, Ph.D Member, Graduate Committee	Date
Jaime Seguel, Ph.D Member, Graduate Committee	Date
Haedeh Gooransarab, Ph.D Member, Graduate Committee	Date
Joseph Bonaventura, Ph.D Representative, Graduate Studies	Date
Jaime Seguel, Ph.D Director, Ph.D CISE Program	Date
José A. Mari Mutt, Ph.D Director, Graduate Studies	Date

Abstract

There are two general problems related to finite dynamical systems (FDS): the analysis and the synthesis (also known as the *reverse engineering*) problems. In the former, we are interested in uncovering the sequential structure of a given FDS. In the latter, given a prescribed structure, we have to find an appropriate FDS that accomplishes the intended behavior. In this work we reverse engineer FDSs related to two recent applications. One is the problem of finding an optimal linear (i.e., a matrix) FDS over the integers mod a prime p to efficiently compute FFTs with linear symmetries. For this, we propose $O(p^2 \log p)$ and $O(p^3 \log p)$ time algorithms for the two and three dimensional cases as opposed to $O(p^6)$ and $O(p^{12})$ time of exhaustive searchs, respectively. Also, we characterize those important cases for which the symmetric FFT with prime edge–length can be computed through a single cyclic convolution. For the second problem, the reverse engineering problem in bioinformatics, we study and compare two finite field models for genetic networks and provide algorithms for converting one model into the other via a DFT. Also, we develop efficient methods for performing arithmetic over finite fields. We propose a new efficient parallel algorithm based on the Chinese remaindering theorem to interpolate over finite fields.

Resumen

Con respecto a *sistemas dinámicos finitos* (SDF), se consideran dos problemas generales: el problema del análisis y el problema de síntesis (también conocido como "reverse engineering"). En el primero, dado un SDF, el interés es descubrir la estructura secuencial del mismo. Para el segundo problema, dada una estructura secuencial, se requiere hallar un SDF que cumpla con todos los requisitos previamente impuestos. Esta investigación trata el problema del "reverse engineering" relacionado a dos aplicaciones recientes. La primera aplicación consiste en encontrar un SDF lineal sobre los enteros módulo un primo p que optimice el cómputo de una transformada rápida de Fourier (FFT, por sus siglas en inglés) con simetrías lineales. Para resolver este problema en dos y tres dimensiones, las búsquedas exaustivas usadas anteriormente tenían complejidades del tipo $O(p^6)$ y $O(p^{12})$. Este trabajo desarrolla algoritmos cuyas complejidades son del tipo $O(p^2 \log p)$ y $O(p^3 \log p)$, respectivamente. Además, este trabajo caracteriza aquellos casos donde la FFT simétrica de longitud prima puede ser computada a través de una sola convolución cíclica. Para el segundo problema, conocido como el problema del "reverse engineering" en bioinformática, este trabajo estudia y compara dos modelos de redes genéticas sobre cuerpos finitos y da algoritmos que convierten un modelo al otro usando una transformada discreta de Fourier. Además, este trabajo desarrolla métodos eficientes para llevar a cabo aritmética sobre cuerpos finitos y propone un algoritmo paralelo nuevo y eficiente para interpolar sobre cuerpos finitos el cual está basado en el teorema del residuo chino.

Contents

Dedicatory

This work is dedicated to my family. To my wife, Mara, from whom I am greatly indebted for her help, encouragement, understanding, and most of all, for her love. To my son, Miguel Antonio, from whom I have borrowed precious childhood time to finish this project. To my parents-in-law Mayra and Miguel who are always there for me and happy to do whatever they can to make life easier for me.

Last, but not least, this is also dedicated to my friend and mentor of this work: Dr. Dorothy Bollman, whose patience, commitment and wisdom not only has opened my mind for research thinking with formal and technical knowledge, but also has taught me about life, friendship, and responsibility.

Acknowledgments

This work was partially supported by the National Science Foundation Grant No. 9817642 under the AGEP Program and Grant No. EIA9977071 under the PRECISE Program.

Thanks are also due to the following people. To Dr. Dorothy Bollman and Dr. Oscar Moreno for their intellectual support and encouragement. To Dr. Haedeh Gooransarab for calling our attention to a known result about nonderogatory matrices and for her help in improving the presentation. To Dr. Jaime Seguel, who suggested and motivated the study of the MS–orbits problem. To Dr. William Frey from the "Centro de Recursos para la Ética en las Profesiones" for his helpful discussions on professional ethics. To the High Performance Computing Facilities (HPCF) for the use of computer time in their SGI Origin 2000 and 3000 systems. Finally, to Dr. John Feo of the Cray Company for his help with openMP.

List of tables

Glossary of symbols

Chapter 1

Introduction

The idea of a finite dynamical system (FDS) is a very general concept that plays an important role in a variety of relevant applications. In this work we define such a system to be a triple $\mathcal{S} = (V, f, F)$ where V is a set of n–tuples over a finite field F and $f : V \to V$.

An FDS can be interpreted as a (deterministic) *finite automaton* (without inputs and outputs) where V is the set of states and f can be regarded as the *transition function* from state to state. The state diagram for an FDS is a directed graph where the nodes are the states and there is an arc from state x to state y if and only if $f(x) = y$.

There are two general problems associated with FDSs. The problem of analysis is the problem of given an FDS, determine its sequential structure. The synthesis problem is the problem of given some representation of the structure, determine a FDS having the given structure. In more modern parlance this last problem is called the "reverse engineering problem."

The analysis and synthesis problems for FDSs have been studied for various special cases. In turn, these cases correspond to problems in diverse applications.

One of the most widely studied cases is when V is a vector space over Z_p, p a prime, and f is linear. Such a system, called an "autonomous linear sequential machine" (ALSM), or simply "linear modular system" (LMS), can be realized by a sequential circuit with mod p logic and unit delay elements [4, 12, 25]. Important special cases of such circuits are shift registers, which in turn have implications in radar and digital communication systems and error correction.

In this work we concentrate on two recent applications. These arise from the use of FDSs of vectors over $GF(p^n)$ to model genetic networks [23, 24, 27] and the use of FDSs of equivalence classes of vectors over Z_p to efficiently compute prime edge–length fast Fourier transforms (FFTs) with linear symmetries [42].

We have completely solved the MS–orbits problem for the two and three dimensional cases, thus providing the theory for optimizing the computation of prime edge–length symmetric FFTs. For these cases, given a nonsingular matrix S over Z_p, p prime, we propose, as opposed to exhaustive searchs which yield $O(p^6)$ and $O(p^{12})$ algorithms, more efficient $O(p^2 \log p)$ and $O(p^3 \log p)$ algorithms to compute matrices M that minimize the number of cyclic convolutions (i.e., minimize the number of MS–orbits), respectively. For n dimensions, we characterize those important cases where there is only a single cyclic convolution, called the M–minimal case, and provide a general procedure to compute a maximal matrix which gives one nontrivial MS–orbit. Also, for the n dimensional cases, we propose a general procedure to compute the optimal matrix M when the characteristic polynomial of the nonsingular matrix S factors as the product of two distinct irreducible polynomials.

On the other hand, we have studied and compared two finite field models for genetic networks and provided algorithms for converting one model into the other via a discrete Fourier transform. We have developed efficient methods for performing arithmetic over finite fields and proposed a new efficient parallel algorithm based on the Chinese remaindering theorem to interpolate over finite fields and have C/openMP implementations of these methods.

1.1 Justification

We consider two types of FDSs (V, f, F): those with V equal to a set of n–tuples $(x_1, x_2, \cdots, x_n)$, from $F = GF(p^n)$, p prime, and those with V equal to a set of equivalence classes of vectors over $F = Z_p$ modulo a nonsingular matrix S. In each case we seek algorithms to solve associated reverse engineering problems.

Solutions to these two problems will have important implications for the well known reverse engineering problem in bioinformatics, as well as the problem of optimally computing symmetric FFTs in terms of cyclic convolutions.

The reverse engineering problem in bioinformatics is an important problem of current interest. That is, given some experimental data from a set of genes of a living organism, determine the intrinsic relations among them; that is, which genes influence which. The set of genes and their interactions is called a *genetic network*.

In essence, the reverse engineering in bioinformatics consists of finding the genetic network that satisfies all interactions between the underlying genes. The solution to this problem is of great importance in the treatment of a variety of diseases ranging from cancer to schizophrenia. An adequate mathematical model for a genetic network together with the appropriate algorithms would permit one to simulate the network, thus yielding insight into the dynamics of the network and eliminating unnecessary direct experimentation.

The fast Fourier transform is one of the most widely used and important algorithms in scientific computing. For some data intensive problems, such as x-ray atomic structure determination or the computation of cyclic convolutions with multidimesional Volterra kernels, a reduction in the amount of data can make a significant difference, even though the computational complexity remains the same. It is thus of great interest to take advantage of structured redundancy patterns, called symmetries, in the inputs. In [42], it is shown that for prime edge length multidimensional FFTs, redundant data can be eliminated and computations induced by linear symmetries can be eliminated by an optimal choice of a certain matrix M that depends on the symmetry matrix S. Presently, the only method known to determine such an M is by exhaustion. We propose to find an algorithm to completely determine $MS-$orbits structure, thus greatly reducing computing time.

Chapter 2

Mathematical background

In this chapter we give some preliminaries in algebra, linear algebra, and number theory that we need in the rest of the work. We give proofs of all results that, to the best of our knowledge, have not been published elsewhere. Unless otherwise noted, all other proofs can be found in standard textbooks in finite fields (e.g., [25], [4]), abstract algebra (e.g., [19], [28]), linear algebra (e.g., [14], [21], [37]), number theory (e.g., [29]), or algorithms (e.g., [1], [8]).

2.1 Algebraic structures and finite fields

Definition 2.1.1 *A* **group** *is a set G together with a binary operation $*$ on G such that the following three properties hold:*

1. *$*$ is* **associative***; that is, for any $a, b, c \in G$,*

$$a * (b * c) = (a * b) * c.$$

2. *There is an* **identity** *(or unity) element e in G such that for all $a \in G$,*

$$a * e = e * a = a.$$

3. *For each $a \in G$, there exists an* **inverse** *element $a^{-1} \in G$ such that*

$$a * a^{-1} = a^{-1} * a = e.$$

If, for all $a, b \in G$, $a * b = b * a$, then G is called an **abelian** group (i.e., G is a commutative group). If G is finite, we denote its number of elements by $|G|$. For our purposes, we are interested only in finite sets. Hence, from now on when we mention groups, rings, or fields we refer only to those having a finite number of elements.

Definition 2.1.2 *A group G is said to be* **cyclic** *if there is an element $a \in G$ such that for any $b \in G$, there is some integer j with $b = a^j$. Such an element a is called a* **generator** *of the cyclic group.*

Definition 2.1.3 *If a is a generator of a cyclic group G and $b \in G$, the* **index** *of b with respect to a is the smallest positive integer m, denoted by $Ind_a(b)$, or simply $Ind(b)$, for which $a^m = b$.*

Definition 2.1.4 *The* **order** *of an element a in a group G with identity e is defined to be the least positive integer k such that $a^k = e$.*

Definition 2.1.5 *Let S be a set and R be a subset of $S \times S$. R is an* **equivalence relation** *on S if it has the following three properties:*

1. *$(s, s) \in R$ for all $s \in S$ (***reflexivity***).*
2. *If $(s, t) \in R$, then $(t, s) \in R$ (***symmetry***).*
3. *If $(s, t), (t, u) \in R$, then $(s, u) \in R$ (***transitivity***).*

Definition 2.1.6 *A* **ring** *$(R, +, *)$ is a set R, together with two binary operations $+$ and $*$, such that:*

1. *R is an abelian group with respect to $+$.*
2. *$*$ is associative.*
3. *The distributive laws hold:*

$$a * (b + c) = a * b + a * c \text{ and } (b + c) * a = b * a + c * a \text{ for all } a, b, c \in F.$$

Definition 2.1.7 *A ring R is said to be* **commutative** *if $a*b = b*a$ for all $a, b \in R$. If a ring R contains an element* $\mathbf{e}$ *with the property that $a * \mathbf{e} = \mathbf{e} * a = a$ for all $a \in R$, we say that R is a* **ring with identity**.

Definition 2.1.8 *A ring R is said to be a* **division ring** *if its nonzero elements form a group under multiplication.*

Definition 2.1.9 *A* **field** *$(F, +, *)$ is a set F, together with two binary operations $+$ and $*$ such that*

1. *F is an abelian group with respect to $+$ having 0 as the identity for addition.*
2. *$F^* = F - \{0\}$ is an abelian group with identity 1 with respect to $*$.*
3. *The distributive laws hold:*

$$a * (b + c) = a * b + a * c \text{ for all } a, b, c \in F.$$

Theorem 2.1.1 (Wedderburn) *Every finite division ring is a field.*

Let $F[x]$ be the ring of polynomials over the field F.

Definition 2.1.10 *A polynomial $p(x) \in F[x]$ is said to be irreducible over F if $p(x)$ has positive degree and $p(x) = q(x)t(x)$ with $q(x), t(x) \in F[x]$ implies that either $q(x)$ or $t(x)$ is a constant polynomial.*

Definition 2.1.11 *A subset S of a ring R is called a subring of R provided S is closed under $+$ and $\cdot$ and forms a ring under these operations.*

Definition 2.1.12 *A subset J of a ring R is called an ideal provided J is a subring of R and for all $a \in J$ and $r \in R$ we have $ar \in J$ and $ra \in J$.*

Definition 2.1.13 *Let R be a commutative ring. An ideal J of R is said to be principal if there is an $a \in R$ such that $J = (a) = \{ra | r \in R\}$.*

Definition 2.1.14 *Let R be a ring and J be an ideal of R. The set*

$$R/J = \{a + J | a \in R\}$$

is called the residue class ring of R modulo J.

Theorem 2.1.2 *For $f(x) \in F[x]$, the residue class ring $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible over F.*

Theorem 2.1.3 *Let F be a finite field. Then F has p^n elements, where p is a prime and n is the degree of some irreducible polinomial over Z_p.*

Corollary 2.1.1 *Z_p, the integers mod a prime p, is a field with p elements.*

If F is a finite field of p^n elements, it is customary to call it a *Galois field* of p^n elements and denote it by $GF(p^n)$.

Lemma 2.1.1 *Every element $a \in GF(p^n)$ satisfies $a^{p^n} = a$.*

Let $GF(p^n)$ be a Galois field of p^n elements and let $GF(p^n)^*$ denote the multiplicative group of nonzero elements of $GF(p^n)$.

Theorem 2.1.4 *For every Galois field $GF(p^n)$ the multiplicative group $GF(p^n)^*$ is a cyclic group.*

Definition 2.1.15 *A generator of the cyclic group $GF(p^n)^*$ is called a* **primitive element** *of $GF(p^n)$.*

Definition 2.1.16 *A* **primitive polynomial** *of positive degree n over Z_p is a monic irreducible polynomial that has a primitive element of $GF(p^n)$ as a root. As a consequence, all its roots are primitive elements of $GF(p^n)$.*

Lemma 2.1.2 *For any polynomial $q(x)$ over Z_p of positive degree, with $q(0) \neq 0$, there is a positive integer k for which $q(x)$ divides $x^k - 1$.*

The smallest such k is called the *period* or *order* of $q(x)$.

Lemma 2.1.3 *For each irreducible polynomial $q(x)$ of degree n over Z_p, $q(x)$ divides $x^{p^n-1} - 1$.*

Lemma 2.1.4 *The period of a primitive polynomial of degree n is $p^n - 1$.*

In this work, *maximal* polynomial and primitive polynomial are the same concept.

Lemma 2.1.5 *The number of maximal polynomials of degree n over Z_p is $\varphi(p^n - 1)/n$, where φ denotes the Euler's φ–function.*

2.2 Matrices and vector spaces

Definition 2.2.1 *A nonempty set $(V, F, +, \cdot)$ is a* **vector space** *if $(V, +)$ is an abelian group and if $a \in F$, $\mathbf{x} \in V$ there is defined an element $a\mathbf{x} \in V$ subject to*

1. $a(\mathbf{x} + \mathbf{y}) = a\mathbf{x} + a\mathbf{y}$;
2. $(a + b)\mathbf{x} = a\mathbf{x} + a\mathbf{x}$;
3. $a \cdot (b\mathbf{x}) = (a \cdot b)\mathbf{x}$;
4. $1\mathbf{x} = \mathbf{x}$;

for all $a, b \in F$, $\mathbf{x}, \mathbf{y} \in V$ (where the 1 represents the unit element of F under $\cdot$).

Definition 2.2.2 *A subset W of a vector space V over a field F is called a* **subspace** *of V if W is a vector space over F under the operations of addition $(+)$ and scalar multiplication $(\cdot)$ defined on V.*

There are two important polynomials related to an $n \times n$ matrix S. On the one hand, the *characteristic polynomial* $\phi_S(x)$ of a square matrix S is defined by the determinant $|S - xI|$. The Cayley Hamilton Theorem states that every square matrix

satisfies its own characteristic equation, i.e., $\phi_S(S) = 0$.

On the other hand, if $m(x)$ is a monic polynomial such that $m(S) = 0$ with the property that $m(x)$ divides any $q(x)$ for which $q(S) = 0$, then, $m(x)$ is called the *minimal polynomial* of S and we denote it by $m_S(x)$.

Similarly, for any nonsingular square matrix S over Z_p, there is a least positive integer k such that $S^k = I$, where I denotes an identity matrix of appropriate size. This k is called the *period* of S. Matrix S is *maximal* if its period is $p^n - 1$. Thus, S is maximal if and only if the smallest positive integer k for which $m_S(x)$ divides $x^k - 1$ is $k = p^n - 1$.

For a monic polynomial $q(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ over Z_p of degree n, its *companion matrix* is given by

$$C_q = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & -a_{k-2} \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

Then, $q(x)$ is the characteristic polynomial and the minimal polynomial of C_q.

Definition 2.2.3 *$\mathcal{M}_n(Z_p)$, abbreviated $\mathcal{M}_n$, is the set of all $n \times n$ matrices over Z_p.*

Lemma 2.2.1 *$\mathcal{M}_n$ is a finite ring.*

Definition 2.2.4 *Let $S \in \mathcal{M}_n$. The* **normalizer** *of S is the set*

$$\mathcal{N}(S) = \{M \in \mathcal{M}_n | MS = SM\}.$$

Theorem 2.2.1 *Let $S \in \mathcal{M}_n$. Then, $\mathcal{N}(S)$ is a commutative ring with identity I_n, the $n \times n$ identity matrix.*

Lemma 2.2.2 *Let $S \in \mathcal{M}_n$ and $q(x)$ be any polynomial over Z_p. The set*

$$V_q = \{\mathbf{x} \in Z_p^n | q(S)\mathbf{x} = \mathbf{0}\}$$

is a subspace of Z_p^n. V_q *is called the* **null space** *of* $q(S)$ *sometimes denoted by* $N(q(S))$.

There are various representations of a finite field $GF(p^n)$. In our work it is useful to consider the following three:

1. $K_1(p^n) = \{a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_1\alpha + a_0 | a_i \in Z_p\}$, where α is a root of an irreducible polynomial of degree n over Z_p.
2. $K_2(p^n) = \{0\} \cup \{\alpha^i | i = 0, 1, \cdots, p^n - 1\}$ where α is a root of a primitive polynomial of degree n over Z_p.
3. $K_3(p^n) = \{a_{n-1}S^{n-1} + a_{n-2}S^{n-2} + \cdots + a_1 S + a_0 I_n | a_i \in Z_p\}$ where $S \in \mathcal{M}_n$ with $\phi_S(x)$ irreducible.

These three representations are isomorphic to each other and it is useful to examine the mappings that give these isomorphisms.

Theorem 2.2.2 *Let* $P(x)$ *be a primitive polynomial of degree* n *over* Z_p *and let* β *be a root of* $P(x)$ *in* $GF(p^n)$. *Also, let* $\alpha \in GF(p^n)$ *be a root of an irreducible polynomial* $R(x)$ *of degree* n *over* Z_p. *Then there exists a polynomial*

$$Q(x) = c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$$

over Z_p *such that*

$$P(Q(\alpha)) = 0.$$

The coefficients $c_0, c_1, \cdots, c_{n-1}$ *constitute a solution of the system of equations obtained by setting each coefficient of* $P(c_0 + c_1 x + \cdots + c_{n-1}x^{n-1})$ *mod* $R(x)$ *to* 0. *Now define*

$$\begin{aligned} h_1(\beta^i) &= Q(\alpha)^i \text{ and} \\ h_2(\beta^i) &= Q(S^i) \end{aligned}$$

for each $i = 0, 1, \ldots, p^n - 1$. *Then*

$$\begin{aligned} h_1 : K_2(p^n) &\rightarrow K_1(p^n) \text{ and} \\ h_2 : K_2(p^n) &\rightarrow K_3(p^n) \end{aligned}$$

are isomorphisms, where $S \in \mathcal{M}_n$ *is nonsingular with* $\phi_S(x)$ *irreducible.*

Corollary 2.2.1 *Let $S \in \mathcal{M}_n$ be nonsingular with $\phi_S(x)$ irreducible. Then $Q(S) \in \mathcal{N}(S)$ is a maximal matrix (i.e., period $p^n - 1$).*

Proof
Let P be a primitive polynomial of degree n and $S \in \mathcal{M}_n$ be nonsingular with $\phi_S(x)$ irreducible. By Theorem 2.2.2, there is a polynomial $Q(x)$ such that $P(Q(S)) = 0$, hence, $Q(S)$ is a primitive element of $GF(p^n)$, i.e., order of $Q(S)$ is $p^n - 1$.$\diamondsuit$

Another concept that plays an important role in this work is **matrix similarity**.

Definition 2.2.5 *Let $S, S' \in \mathcal{M}_n$. We say that S is similar to S', if there exists a nonsingular $A \in \mathcal{M}_n$ such that $A^{-1}SA = S'$.*

Theorem 2.2.3 *Let $S, S' \in \mathcal{M}_n$. Then the following properties hold:*

i. Similarity between matrices is an equivalence relation.

ii. If S and S' are similar, then they share the same characteristic polynomial.

iii. If S and S' are similar, then for any polynomial $q(x)$, $q(S)$ and $q(S')$ are similar.

v. For any polynomial $q(x)$, S commutes with $q(S)$.

Definition 2.2.6 *A* **Jordan matrix** *of size n associated with $\lambda \in Z_p$ is a matrix of the form*

$$J_n(\lambda) = \begin{pmatrix} \lambda & 1 & \cdots & 0 \\ 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & & \\ 0 & 0 & \cdots & 1 \\ 0 & 0 & \cdots & \lambda \end{pmatrix}.$$

Proof of the following theorem can be found in [14].

Theorem 2.2.4 (Jordan canonical form) *Let $S \in \mathcal{M}_n$ be a given matrix such that $\phi_S(x)$ factors into a product of factors of degree 1. Suppose that $\lambda_1, \lambda_2, \ldots, \lambda_k$*

are the distinct eigenvalues of $\phi_S(x)$ *and that the multiplicity of* λ_i *is* m_i, $i = 1, 2, \ldots, k$. *Then,* S *is similar to the matrix*

$$\begin{pmatrix} \mathbf{J}_1(\lambda_1) & & & \mathbf{0} \\ & \mathbf{J}_2(\lambda_2) & & \\ & & \ddots & \\ \mathbf{0} & & & \mathbf{J}_k(\lambda_k) \end{pmatrix},$$

where $\mathbf{J}_r(\lambda) = J_{N_1}(\lambda_r) \bigoplus J_{N_2}(\lambda_r) \bigoplus \cdots \bigoplus J_{N_r}(\lambda_r)$, $N_1 + N_2 + \cdots + N_t = m_r$, *and* $m_1 + m_2 + \cdots + m_k = n$.

Corollary 2.2.2 *Let* $S \in \mathcal{M}_3$ *such that* $\phi_S(x)$ *factors into a product of factors of degree 1. Then, matrix* S *is similar to one and only one of the following:*

1. $J_1(\lambda_1) \bigoplus J_1(\lambda_2) \bigoplus J_1(\lambda_3)$, $\lambda_i \neq \lambda_j$, $i \neq j$.
2. $J_1(\lambda) \bigoplus J_1(\lambda) \bigoplus J_1(\lambda) \bigoplus$. *That is,* $S = \lambda I_3$.
3. $J_3(\lambda)$.
4. $J_2(\lambda) \bigoplus J_1(\lambda)$.
5. $J_2(\lambda_1) \bigoplus J_1(\lambda_2)$, $\lambda_1 \neq \lambda_2$.
6. $J_1(\lambda_1) \bigoplus J_1(\lambda_1) \bigoplus J_1(\lambda_2)$, $\lambda_1 \neq \lambda_2$.

Definition 2.2.7 *Let* $S \in \mathcal{M}_n$. *A subspace* V *of* Z_p^n *is said to be* S–**invariant** *if* $S\mathbf{x} \in V$, *for all* $\mathbf{x} \in V$.

Definition 2.2.8 *Let* $S \in \mathcal{M}_n$ *be nonsingular. A subspace* W *of* Z_p^n *is called a* S–**cyclic** *subspace of* Z_p^n *if there exists a vector* $\mathbf{x} \in W$ *such that*

$$W = span(\{\mathbf{x}, S\mathbf{x}, S^2\mathbf{x}, \ldots\}).$$

For a proof of the following theorem, see for instance, [37].

Theorem 2.2.5 (Rational canonical form) *Let V be a finite dimensional vector space, and suppose that τ is a linear transformation of V to V that has minimal polynomial*

$$m_\tau(x) = p_1^{e_1}(x) \cdots p_n^{e_n}(x)$$

where the monic polynomials $p_j(x)$ are distinct and irreducible. Then we can write

$$V = (< \mathbf{v_{1,1}} > \oplus \cdots \oplus < \mathbf{v_{1,k_1}} >) \oplus \cdots \oplus (< \mathbf{v_{n_1,1}} > \oplus \cdots \oplus < \mathbf{v_{n,k_n}} >)$$

where $< \mathbf{v_{i,j}} >$ is a τ cyclic subspace of V. The minimal polynomials for $\tau_{i,j} = \tau|_{< \mathbf{v_{i,j}} >}$ are the elementary divisors

$$min(\tau_{i,j}) = p_i^{e_{i,j}}(x)$$

of V, where

$$e_i = e_{i,1} \geq e_{i,2} \geq \cdots \geq e_{i,k_i}$$

These elementary divisors are uniquely determined by τ. Furthermore, if $deg(p_i^{e_{i,j}}(x)) = d_{i,j}$, then

$$\beta_{i,j} = (\mathbf{v_{i,j}}, \tau_{i,j}(\mathbf{v_{i,j}}), \ldots, \tau_{i,j}^{d_{i,j}-1}(\mathbf{v_{i,j}}))$$

is an oredered basis for $\mathbf{v_{i,j}}$, and the matrix of τ with respect to the ordered basis

$$\beta = (\beta_{1,1}, \ldots, \beta_{n,k_n})$$

is the block diagonal matrix

$$[\tau]_\beta = \begin{pmatrix} C_{p_1^{e_{1,1}}(x)} & & & & & & \\ & \ddots & & & & & \\ & & C_{p_1^{e_{1,k_1}}(x)} & & & & \\ & & & \ddots & & & \\ & & & & C_{p_n^{e_{n,n_1}}(x)} & & \\ & & & & & \ddots & \\ & & & & & & C_{p_n^{e_{n,k_n}}(x)} \end{pmatrix}$$

The matrix on the right is called the **rational canonical form of** τ.

The following corollary will be used later in section 4.2.1.

Corollary 2.2.3 *Let $S \in \mathcal{M}_n$ with $m_S(x) = q(x)$, where $q(x)$ is a monic irreducible polynomial. Then, there exists a nonsingular matrix A such that*

$$A^{-1}SA = \begin{pmatrix} C_q & & \\ & \ddots & \\ & & C_q \end{pmatrix}.$$

Lemma 2.2.3 *Let $S \in \mathcal{M}_n$ be nonsingular with $\phi_S(x)$ irreducible and let $M \in \mathcal{N}(S)$. Then, $m_M(x)$ is irreducible.*

Proof
By Corollary 2.2.1, there exists a polynomial $Q(x) = c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ over Z_p such that $N = Q(S)$ is a maximal matrix.

Thus, $MS = SM$ implies that M commutes with any polynomial combination of S, in particular with $N = Q(S)$.

Now, by way of contradiction, suppose that $m_M(x)$ is reducible and let $q_1(x)$ and $q_2(x)$ be polynomials of positive degree such that $m_M(x) = q_1(x)q_2(x)$ with

$$\gcd(q_1(x), q_2(x)) = 1.$$

Then, V_{q_i}, $i = 1, 2$ are nontrivial disjoint proper subspaces of Z_p^n. Thus, $|V_{q_i}| < p^n - 1$. Let $\mathbf{0} \neq \mathbf{x} \in V_{q_i}$. Note that the set

$$< N\mathbf{x} >= \{\mathbf{x}, N\mathbf{x}, \ldots, N^{p^n-2}\mathbf{x}\}$$

contains $p^n - 1$ vectors since N is maximal and $\mathbf{x} \neq \mathbf{0}$. Also, note that

$$q_i(M)N\mathbf{x} = Nq_i(M)\mathbf{x} = N\mathbf{0} = \mathbf{0}.$$

Hence, $N\mathbf{x} \in V_{q_i}$. Thus, $< N\mathbf{x} > \subset V_{q_i}$, which is a contradiction. The only possibility left is that $m_M(x) = q^e(x)$, for some irreducible polynomial $q(x)$ and some positive integer e. Assume $e > 1$. Then, $V_{q^e} - V_q$ is nonempty and V_q is a nontrivial subspace of Z_p^n. Let $\mathbf{x} \in V_{q^e} - V_q$ and $\mathbf{0} \neq \mathbf{y} \in V_q$. Thus, $< N\mathbf{x} > \subset V_{q^e} - V_q$ and $< N\mathbf{y} > \subset V_q$. Which cannot be the case since $| < N\mathbf{x} > | = | < N\mathbf{y} > | = p^n - 1$. Hence, $m_M(x) = q(x)$.$\diamondsuit$

Corollary 2.2.4 *Let $S \in \mathcal{M}_n$ be nonsingular with $\phi_S(x)$ irreducible and let $M \in \mathcal{N}(S)$. Then, $\det(M) = 0$ if and only if $M = \mathbf{0}$, the $n \times n$ zero matrix.*

Corollary 2.2.5 *Let $S \in \mathcal{M}_n$ be a nonsingular with $\phi_S(x)$ irreducible. Then, $\mathcal{N}(S)$ is a finite division ring.*

The following definition appears in [37].

Definition 2.2.9 *$S \in \mathcal{M}_n$ is* **nonderogatory** *if $\phi_S(x) = m_S(x)$.*

The following theorem is a consequence of exercise 19 of section 7.2 in [20].

Theorem 2.2.6 *Let $S \in \mathcal{M}_n$ be nonsingular. Then,*

$$\mathcal{N}(S) = \{c_{n-1}S^{n-1} + c_{n-2}S^{n-2} + \cdots + c_1 x + c_0 | c_i \in Z_p\}$$

if and only if S is nonderogatory.

Corollary 2.2.6 *Let $S \in \mathcal{M}_n$ be nonsingular with $\phi_S(x)$ irreducible. Then $\mathcal{N}(S)$ is the finite field $GF(p^n)$.*

Proof
By Corollary 2.2.5, $\mathcal{N}(S)$ is a finite division ring. Hence, by the Wedderburn Theorem (Theorem 2.1.1), $\mathcal{N}(S)$ is a finite field of p^n elements. Note that

$$\{c_{n-1}S^{n-1} + c_{n-2}S^{n-2} + \cdots + c_1 S + c_0 I_n | c_i \in Z_p\}$$

contains p^n elements and that it is a subset of $\mathcal{N}(S)$. Therefore,

$$\mathcal{N}(S) = \{c_{n-1}S^{n-1} + c_{n-2}S^{n-2} + \cdots + c_1 S + c_0 I_n | c_i \in Z_p\}.\diamondsuit$$

Corollary 2.2.7 *Let $S \in \mathcal{M}_n$ be nonsingular such that $\phi_S(x)$ is the product of n distinct factors of degree 1. Then, $M \in \mathcal{N}(S)$ implies that*

$$M = c_{n-1}S^{n-1} + \cdots + c_1 S + c_0 I_n$$

for some $c_i \in Z_p$, $i = 0, 1, \ldots, n-1$.

2.2.1 Special constructions

Construction I

Let S be a nonsingular matrix over Z_p with characteristic and minimal polynomials given by

$$\begin{aligned} \phi_S(x) &= (x-\lambda_1)^2(x-\lambda_2) \text{ and} \\ m_S(x) &= (x-\lambda_1)(x-\lambda_2). \end{aligned}$$

Let A be a nonsingular matrix of Theorem 2.2.5 for which

$$A^{-1}SA = S' = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{pmatrix}.$$

We can show, by direct calculation, that if N commutes with S', then $N = \begin{pmatrix} C & 0 \\ 0 & \beta \end{pmatrix}$, where C is any 2×2 matrix and $\beta \in Z_p$. Let $P(x) = x^2 + ax + b$ be a primitive polynomial over Z_p and let $C_P = \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$ be the companion matrix associated to $P(x)$. Therefore, in particular, S' commutes with $N = \begin{pmatrix} C_P^t & 0 \\ 0 & \beta \end{pmatrix}$, for any integer t. However, in general, if M commutes with this type of matrices S, it is not always the case that $M = Q(S)$, for some polynomial $Q(x)$.

Example 2.2.1 *Let* $S = \begin{pmatrix} 5 & 0 & 14 \\ 0 & 1 & 0 \\ 4 & 0 & 15 \end{pmatrix}$ *be defined over* Z_{17}. *Then* $\phi_S(x) = (x-1)^2(x-2)$, *and* $m_S(x) = (x-1)(x-2)$. *Thus, there exists a nonsingular matrix* A *such that* $A^{-1}SA = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$. *Matrix* $M = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 10 & 0 & 9 \end{pmatrix}$ *commutes with* S.

By the Cayley–Hamilton Theorem, if N *is an* $n \times n$ *matrix and* $t \geq n$ *is an integer, then* $N^t = f(N)$, *for some polynomial* $f(x)$ *of degree less than* n. *Let us assume there is a polynomial* $Q(x)$ *for which* $M = Q(S)$. *Thus, for our example, we can think of this polynomial as* $Q(x) = c_2x^2 + c_1x + c_0$, *for some* $c_0, c_1, c_2 \in Z_p$.

In order to find coefficients c_0, c_1, *and* c_2 *we have to solve* $Q(S) = M$, *which is equivalent to*

$$c_2 \begin{pmatrix} 5 & 0 & 14 \\ 0 & 1 & 0 \\ 4 & 0 & 15 \end{pmatrix}^2 + c_1 \begin{pmatrix} 5 & 0 & 14 \\ 0 & 1 & 0 \\ 4 & 0 & 15 \end{pmatrix} + c_0 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 10 & 0 & 9 \end{pmatrix}$$

Which is equivalent to solving the system of linear equations

$$\begin{aligned} 13c_2 + 5c_1 + c_0 &= 1 \\ 12c_2 + 4c_1 &= 10 \\ 8c_2 + 14c_1 &= 1 \\ 9c_2 + 15c_1 + c_0 &= 9 \\ c_2 + c_1 + c_0 &= 1 \end{aligned} \tag{2.1}$$

Which is equivalent to solving

$$\begin{aligned} 14c_1 + 4c_0 &= 6 \\ 7c_1 + 2c_0 &= 3 \\ 12c_1 + c_0 &= 3 \end{aligned}$$

Which is equivalent to

$$\begin{aligned} 14c_1 + 4c_0 &= 6 \\ 14c_1 + 4c_0 &= 12 \end{aligned}$$

Which is equivalent to

$$0 = 16.$$

Therefore, system (2.1) *is inconsistent and, hence, there is no such polynomial* $Q(x)$ *for which* $M = Q(S)$.

The following lemma is a standard result in linear algebra and its proof can be found, for instance, in [14].

Lemma 2.2.4 *Let* $S \in \mathcal{M}_3$ *be nonsingular with* $\phi_S(x) = (x - \lambda_1)^2(x - \lambda_2)$ *and* $m_S(x) = (x - \lambda_1)(x - \lambda_2)$, *where* $\lambda_1 \neq \lambda_2$, *respectively. Let* $N(S - \lambda_i I_3) = \{\mathbf{x} \in$

$Z_p^3 | (S - \lambda_i I_3)\mathbf{x} = \mathbf{0}\}$, $i = 1, 2$. *Then,* $A^{-1}SA = diag(\lambda_1, \lambda_1, \lambda_2)$, *where the first two columns of* A *form a basis for* $N(S - \lambda_1 I_3)$ *and the last column forms a basis for* $N(S - \lambda_2 I_3)$.

An important fact that derives from Lemma 2.2.4 is that matrix $S - \lambda_1 I_3$ has at least one nonzero row. Let $[a_0\ a_1\ a_2]$ be a nonzero row corresponding to $S - \lambda_1 I_3$. The remaining two rows are simply scalar multiples of $[a_0\ a_1\ a_2]$. Thus, equation

$$(S - \lambda_1 I_3)\mathbf{x} = \mathbf{0}$$

is equivalent to

$$a_0 x_0 + a_1 x_1 + a_2 x_2 = 0, \tag{2.2}$$

which is the equation of a plane that goes through the origin $(0, 0, 0)$. Thus, a basis for $N(S - \lambda_1 I_3)$ consists of two linearly independent vectors $\mathbf{x}$, $\mathbf{y}$ which lay on the plane described by (2.2). Let j be the index of the first nonzero component of $[a_0\ a_1\ a_2]$ (i.e., $a_j \neq 0$.) Also, let $\mathbf{x}[j]$ be the $j - th$ component of vector $\mathbf{x}$ and define

$$\begin{array}{lcl} \mathbf{x}[j] & = & -a_j^{-1} a_{j+1 \bmod 3}, \\ \mathbf{x}[j+1 \bmod 3] & = & 1, \\ \mathbf{x}[j+2 \bmod 3] & = & 0, \end{array}$$

and

$$\begin{array}{lcl} \mathbf{y}[j] & = & -a_j^{-1} a_{j+2 \bmod 3}, \\ \mathbf{y}[j+1 \bmod 3] & = & 0, \\ \mathbf{y}[j+2 \bmod 3] & = & 1. \end{array}$$

It is easy to see that both, $\mathbf{x}$ and $\mathbf{y}$, are nonzero linearly independent vectors that satisfy equation (2.2) and, hence, $\{\mathbf{x}, \mathbf{y}\}$ is a basis for $N(S - \lambda_1 I_3)$.

Using similar arguments as before, matrix $S - \lambda_2 I_3$ has at least two nonzero independent rows $[b_0\ b_1\ b_2]$ and $[c_0\ c_1\ c_2]$. Thus, equation

$$(S - \lambda_1 I_3)\mathbf{x} = \mathbf{0}$$

is equivalent to

$$\begin{array}{lcll} b_0 x_0 + b_1 x_1 + b_2 x_2 & = & 0, & (2.3) \\ c_0 x_0 + c_1 x_1 + c_2 x_2 & = & 0 & (2.4) \end{array}$$

which are the equations of two non parallel planes crossing the origin $(0, 0, 0)$. Thus, a basis for $N(S - \lambda_2 I_3)$ is any nonzero vector $\mathbf{z}$ laying in the line which is the intersection of the two planes described by equations (2.3) and (2.4).

Let $\mathbf{b} = (b_0, b_1, b_2)$ and $\mathbf{c} = (c_0, c_1, c_2)$ and define the *cross product* of $\mathbf{b}$ and $\mathbf{c}$ by

$$\mathbf{b} \times \mathbf{c} = (b_1c_2 - b_2c_1, b_2c_0 - b_0c_2, b_0c_1 - b_1c_0).$$

It is a well known fact that if $\mathbf{b}$ and $\mathbf{c}$ are nonzero indepedent vectors, then $\mathbf{b} \times \mathbf{c}$ is a nonzero vector perpendicular to $\mathbf{b}$ and $\mathbf{c}$. Furthermore,

$$\mathbf{z} = \mathbf{b} \times \mathbf{c}$$

satisfies equations (2.3) and (2.4). Therefore, $\mathbf{z} = \mathbf{b} \times \mathbf{c}$ serves as a basis for $N(S - \lambda_2 I_3)$.

The following lemma summarizes the construction of matrix A of Lemma 2.2.4.

Lemma 2.2.5 *Let $S \in \mathcal{M}_3$ be nonsingular with $\phi_S(x) = (x - \lambda_1)^2(x - \lambda_2)$ and $m_S(x) = (x - \lambda_1)(x - \lambda_2)$, where $\lambda_1 \neq \lambda_2$, respectively. Let $[a_0\ a_1\ a_2]$ be a nonzero row of $S - \lambda_1 I_3$, and $[b_0\ b_1\ b_2]$, and $[c_0\ c_1\ c_2]$ be two nonzero independent rows of $S - \lambda_2 I_3$. Let j be the index of the first nonzero component of $[a_0\ a_1\ a_2]$. Then, a matrix A for which $A^{-1}SA = diag(\lambda_1, \lambda_1, \lambda_2)$, is $A = (\mathbf{x}\ \mathbf{y}\ \mathbf{z})$, where*

$$\begin{aligned}
\mathbf{x}[j] &= -a_j^{-1}a_{j+1 \bmod 3}, & \mathbf{y}[j] &= -a_j^{-1}a_{j+2 \bmod 3},\\
\mathbf{x}[j+1 \bmod 3] &= 1, & \mathbf{y}[j+1 \bmod 3] &= 0,\\
\mathbf{x}[j+2 \bmod 3] &= 0, & \mathbf{y}[j+2 \bmod 3] &= 1,
\end{aligned}$$

and

$$\begin{aligned}
\mathbf{z}[0] &= b_1c_2 - b_2c_1,\\
\mathbf{z}[1] &= b_2c_0 - b_0c_2,\\
\mathbf{z}[2] &= b_0c_1 - b_1c_0.
\end{aligned}$$

It is straightforward to see that the computational cost for constructing matrix A in Lemma 2.2.5 is constant.

Example 2.2.2 *Let* $S = \begin{pmatrix} 5 & 0 & 14 \\ 0 & 1 & 0 \\ 4 & 0 & 15 \end{pmatrix}$ *be defined over Z_{17} (see Example 2.2.1.) The characteristic and minimal polynomials of S are $\phi_S(x) = (x - 1)^2(x - 2)$, and $m_S(x) = (x - 1)(x - 2)$, respectively. Thus, $\lambda_1 = 1$, and $\lambda_2 = 2$. Hence, $S - \lambda_1 I_3 =$*

$\begin{pmatrix} 4 & 0 & 14 \\ 0 & 0 & 0 \\ 4 & 0 & 14 \end{pmatrix}$, *and* $S - \lambda_2 I_3 = \begin{pmatrix} 3 & 0 & 14 \\ 0 & 16 & 0 \\ 4 & 0 & 13 \end{pmatrix}$. *A nonzero row of* $S - \lambda_1 I_3$ *is* [4 0 14] *and the index of its first nonzero component is* $j = 0$. *Hence,*

$$\begin{aligned} \mathbf{x}[0] &= -4^{-1} * 0 = 0, & \mathbf{y}[0] &= -4^{-1} * 14 = 5, \\ \mathbf{x}[1] &= 1, & \mathbf{y}[1] &= 0, \\ \mathbf{x}[2] &= 0, & \mathbf{y}[2] &= 1, \end{aligned}$$

Two nonzero independent rows of $S - \lambda_2 I_3$ *are* [3 0 14] *and* [0 16 0]. *Thus,*

$$\mathbf{z} = \begin{pmatrix} 0 * 0 - 14 * 16 \\ 3 * 0 - 14 * 0 \\ 3 * 16 - 0 * 0 \end{pmatrix} = \begin{pmatrix} 14 \\ 0 \\ 14 \end{pmatrix}.$$

Hence, $A = \begin{pmatrix} 0 & 5 & 14 \\ 1 & 0 & 0 \\ 0 & 1 & 14 \end{pmatrix}$. *It is easy to verify that, indeed,* $A^{-1}SA = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$.

Lemma 2.2.6 *Let* $S \in \mathcal{M}_3$ *be nonsingular with* $\phi_S(x) = (x - \lambda_1)^2(x - \lambda_2)$ *and* $m_S(x) = (x - \lambda_1)(x - \lambda_2)$, *where* $\lambda_1 \neq \lambda_2$. *Also, let* $M \in \mathcal{N}(S)$ *be nonsingular. Then* $\phi_M(x) = -q(x)(x - \beta)$, *for some monic quadratic polynomial* $q(x)$ *for which* $q(0) \neq 0$ *and some* $\beta \neq 0$.

Proof

Let A be a nonsingular matrix for which $A^{-1}SA = S' = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{pmatrix}$. Let $M \in \mathcal{N}(S)$ be nonsingular$M$ be any nonsingular. Thus, $MS = SM$ is equivalent to

$$M(AS'A^{-1}) = (AS'A^{-1})M$$

if and only if

$$(A^{-1}MA)S' = S'(A^{-1}MA).$$

Now, since S' is a diagonal matrix and $A^{-1}MA$ commutes with S', we can easily show that $A^{-1}MA = \begin{pmatrix} B & 0 \\ 0 & \beta \end{pmatrix}$ for some nonsingular 2×2 matrix B and some $\beta \neq 0$. Therefore, $\phi_M(x) = \phi_{A^{-1}MA}(x) = -\phi_B(x)(x - \beta)$.$\diamondsuit$

Construction II

Let $S \in \mathcal{M}_3$ be nonsingular with characteristic and minimal polynomials $\phi_S(x) = (x-\lambda)^3$ and $m_S(x) = (x-\lambda)^2$, respectively. Then, by Theorem 2.2.4, there is a nonsingular matrix A for which

$$A^{-1}SA = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}.$$

This matrix A can be computed as follows.

Lemma 2.2.7 *Let $S \in \mathcal{M}_3$ be nonsingular with $\phi_S(x) = (x-\lambda)^3$ and $m_S(x) = (x-\lambda)^2$, respectively. Let $N(S-\lambda I_3) = \{\mathbf{x} \in Z_p^3 | (S-\lambda I_3)\mathbf{x} = \mathbf{0}\}$, and $\mathbf{x_1}$ and $\mathbf{x_2}$ be nonzero vectors such that $\mathbf{x_1} \notin N(S-\lambda I_3)$ and $\mathbf{x_2} \in N(S-\lambda I_3)$ is linearly independent of $(S-\lambda I_3)\mathbf{x_1}$. Also, let A be the matrix whose columns are the vectors $(S-\lambda I_3)\mathbf{x_1}$, $\mathbf{x_1}$, and $\mathbf{x_2}$, respectively. Then,*

$$A^{-1}SA = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}.$$

Proof
First, let us see that $\mathbf{x_1}$ and $(S-\lambda I_3)\mathbf{x_1}$ are linearly independent. Assume the contrary. Suppose there is a $c \in Z_p$ for which $(S-\lambda I_3)\mathbf{x_1} = c\mathbf{x_1}$. Then, c must not be 0 since $\mathbf{x_1} \notin N(S-\lambda I_3)$. But, $(S-\lambda I_3)\mathbf{x_1} = c\mathbf{x_1}$ implies that $S\mathbf{x_1} = (c+\lambda)\mathbf{x_1}$. Which implies that $c+\lambda$ is an eigenvalue of S. That is, $\lambda = c+\lambda$, since the only eigenvalue of S is λ. Hence, $c = 0$. A contradiction. A similar argument shows that $\mathbf{x_1}$ and $\mathbf{x_2}$ are linearly independent. Hence, the columns of A forms a basis for Z_p^3, and, in particular, A is invertible.

Second, note that

$$\begin{aligned} (S-\lambda I_3)A &= (S-\lambda I_3)\,(\,(S-\lambda I_3)\mathbf{x_1} \quad \mathbf{x_1} \quad \mathbf{x_2}\,) \\ &= (\,(S-\lambda I_3)^2\mathbf{x_1} \quad (S-\lambda I_3)\mathbf{x_1} \quad (S-\lambda I_3)\mathbf{x_2}\,). \end{aligned}$$

Now, since $m_S(S) = (S-\lambda I_3)^2 = \mathbf{0_{3\times 3}}$ (i.e., the zero 3×3 matrix) and $\mathbf{x_2} \in N(S-\lambda I_3)$, then

$$\begin{aligned} (S-\lambda I_3)A &= (\,\mathbf{0_{3\times 3}x_1} \quad (S-\lambda I_3)\mathbf{x_1} \quad \mathbf{0}\,) \\ &= (\,\mathbf{0} \quad (S-\lambda I_3)\mathbf{x_1} \quad \mathbf{0}\,). \end{aligned}$$

Third, note that

$$\begin{aligned} A\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} &= \begin{pmatrix} A\mathbf{0} & A\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} & A\mathbf{0} \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{0} & A\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} & \mathbf{0} \end{pmatrix} \\ &= (\,\mathbf{0} \quad (S-\lambda I_3)\mathbf{x_1} \quad \mathbf{0}\,) \end{aligned}$$

Henceforth,

$$(S-\lambda I_3)A = A\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

which implies that

$$A^{-1}(S-\lambda I_3)A = A^{-1}SA - \lambda I_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Therefore,

$$A^{-1}SA = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}.\diamondsuit$$

Example 2.2.3 *Let* $S = \begin{pmatrix} 2 & 0 & 0 \\ 13 & 2 & 4 \\ 0 & 0 & 2 \end{pmatrix}$ *over* Z_{17}. *The characteristic and minimal polynomials of* S *are* $\phi_S(x) = (x-2)^3$, *and* $m_S(x) = (x-2)^2$, *respectively. Now,*

$$S - 2I_3 = \begin{pmatrix} 0 & 0 & 0 \\ 13 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix},$$

and

$$N(S-2I_3) = \{\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} \mid \begin{pmatrix} 0 & 0 & 0 \\ 13 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}\}$$

$$= \{\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} | 13x_0 + 4x_1 = 0\}$$

$$= \{\begin{pmatrix} x_0 \\ x_1 \\ x_0 \end{pmatrix} | x_0, x_1 \in Z_{17}\}.$$

Let $\mathbf{x_1} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$. *Thus,* $(S - 2I_3)\mathbf{x_1} = \begin{pmatrix} 0 \\ 13 \\ 0 \end{pmatrix}$. *Next, let us choose* $\mathbf{x_2} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \in N(S - 2I_3)$, *which is linearly independent of* $(S - 2I_3)\mathbf{x_1}$. *Finally, form the matrix* A. $A = \begin{pmatrix} 0 & 1 & 1 \\ 13 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. *We can easily verify that* $A^{-1}SA = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$.

2.3 Number theory

Definition 2.3.1 *The integer* d *is a common divisor of* a *and* b *in case* $d|a$ *and* $d|b$. *Since there is only a finite number of divisors of any nonzero integer, there is only a finite number of common divisors of* a *and* b, *except in the case* $a = b = 0$. *If at least one of* a *and* b *is not* 0, *the greatest among their common divisors is called the greatest common divisor of* a *and* b *and is denoted by* $\gcd(a, b)$.

Note that the greatest common divisor is defined for every pair of integers a and b not both 0 and that $\gcd(a, b) \geq 1$.

Theorem 2.3.1 *If* $d = \gcd(a, b)$, *then there exist integers* x_0 *and* y_0 *such that*

$$ax_0 + by_0 = d.$$

Theorem 2.3.2 *For any positive integer* t,

$$\gcd(ta, tb) = t \gcd(a, b).$$

Theorem 2.3.3 *If $t|a$ and $t|b$ and $t > 0$, then*

$$\gcd(\frac{a}{t}, \frac{b}{t}) = \frac{\gcd(a,b)}{t}.$$

If $d = \gcd(a,b)$, then

$$\gcd(\frac{a}{d}, \frac{b}{d}) = 1.$$

Theorem 2.3.4 *For any integer x,*

$$\gcd(a,b) = \gcd(b,a) = \gcd(a,-b) = \gcd(a, b+ax).$$

Theorem 2.3.5 *If $t|ab$ and $\gcd(b,t) = 1$, then $t|a$.*

Theorem 2.3.6 $\gcd(a,b,c) = \gcd(\gcd(a,b),c) = \gcd(a,\gcd(b,c))$.

Theorem 2.3.7 *For any positive integers a, b, x, y,*

$$\gcd(a,b) | \gcd(ax,by).$$

Proof
Let

$$L = \gcd(x, \frac{b}{\gcd(a,b)}) \gcd(\frac{ax}{\gcd(ax,b)}, y).$$

Thus,

$$\begin{aligned}
\gcd(a,b)L &= \gcd(\gcd(a,b)x, b) \gcd(\frac{ax}{\gcd(ax,b)}, y) \\
&= \gcd(ax, bx, b) \gcd(\frac{ax}{\gcd(ax,b)}, y) \\
&= \gcd(ax, b) \gcd(\frac{ax}{\gcd(ax,b)}, y) \\
&= \gcd(ax, \gcd(ax,b)y) \\
&= \gcd(ax, axy, by) \\
&= \gcd(ax, by).
\end{aligned}$$

Corollary 2.3.1 *If $\gcd(a,y) = 1$ and $\gcd(b,x) = 1$. Then,*

$$\gcd(ax,by) = \gcd(a,b)\gcd(x,y).$$

Theorem 2.3.8 *Let a and b be given integers not both 0. If $\gcd(a,b)=1$, then for each positive integer m, there exist integers x and y for which $\gcd(ax+by,m)=1$.*

Proof
Since $\gcd(a,b)=1$, by Theorem 2.3.1, there exist integers x_0 and y_0 such that $ax_0+by_0=1$. Thus, $\gcd(ax_0+by_0,m)=\gcd(1,m)=1$ for any positive integer m.$\diamondsuit$

The following theorem can be found in [25].

Theorem 2.3.9 (Dirichlet's on primes in arithmetic progressions) *Let b and $n>0$ be integers with $\gcd(b,n)=1$, then there exist infinitely many primes in*

$$\{b, b+n, b+2n, \ldots, b+kn, \ldots\}.$$

Corollary 2.3.2 *Let m be any positive integer, then there are infinitely many integers k for which $\gcd(b+kn,m)=1$.*

Definition 2.3.2 *The nonzero integers a and b have a common multiple t if $a|t$ and $b|t$. The least of the common multiples is called the least common multiple, and its denoted by $lcm(a,b)$.*

Theorem 2.3.10 *If $t>0$, $lcm(ta,tb)=tlcm(a,b)$. Also, $lcm(a,b)\gcd(a,b)=|ab|$, where $|\ |$ stands for the absolut value function.*

Theorem 2.3.11 *Let a,b, and $m>0$ be given integers, and put $d=\gcd(a,m)$. The congruence equation*

$$ax = b \ (mod\ m)$$

has a solution if and only if $d|b$. If this condition is met, then the solutions form the arithmetic progression

$$\{rb', rb'+\frac{m}{d}, rb'+2\frac{m}{d}, \ldots, rb'+(d-1)\frac{m}{d}\},$$

where r is such that $r\frac{a}{d}=1\ (mod\ \frac{m}{d})$ and $b'=\frac{b}{d}$.

Theorem 2.3.12 *Let a, b, and $m > 0$ be integers a and b not both 0 and suppose that $\gcd(a, b, m) = 1$. Then, the set of solutions of $ax = by \pmod m$ is*

$$\{(rbt_1 + \frac{m}{d}t, dt_1) | t_1 = 0, 1, \ldots, \frac{m}{d} - 1, t = 0, 1, \ldots, d - 1\},$$

where $d = \gcd(a, m)$, and $r\frac{a}{d} = 1 \pmod{\frac{m}{d}}$.

Proof
Let

$$x_0 = rbt_1' + \frac{m}{d}t_2'$$

and

$$y_0 = dt_1'$$

for some $t_1' \in \{0, 1, \ldots, \frac{m}{d} - 1\}$ and $t_2' \in \{0, 1, \ldots, d - 1\}$.
Now, since $r\frac{a}{d} = 1 \pmod{\frac{m}{d}}$, then $ar = d \pmod m$. Thus,

$$\begin{aligned} ax_0 &= arbt_1' + a\frac{m}{d}t_2' \\ &= (d + mt_3)bt_1' + m\frac{a}{d}t_2', \text{ for some integer } t_3 \\ &= dbt_1' + mt_3bt_1' + m\frac{a}{d}t_2' \\ &= b(dt_1') \pmod m \\ &= by_0 \pmod m \end{aligned}$$

Therefore (x_0, y_0) is a solution of $ax = by \pmod m$.

On the other hand, let (x_1, y_1) be any solution of $ax = by \pmod m$. Thus,

$$ax_1 = by_1 \pmod m \tag{2.5}$$

Note that, by Theorem 2.3.11, $d = \gcd(a, m) | by_1$. But d does not divide b since, by assumption, $\gcd(d, b) = 1$. Thus, $y_1 = dt_1''$ for some $t_1'' \in \{0, 1, \ldots, \frac{m}{d} - 1\}$ and

$$ax_1 = bdt_1'' \pmod m.$$

Which is equivalent to

$$\frac{a}{d}x_1 = bt_1'' \pmod{\frac{m}{d}}.$$

Thus $x_1 = rbt_1'' \pmod{\frac{m}{d}}$, where $r\frac{a}{d} = 1 \pmod m$. Or, equivalently, $x_1 = rbt_1'' + \frac{m}{d}t_2''$, for some $t_2'' \in \{0, 1, \ldots, d - 1\}$.$\diamondsuit$

Theorem 2.3.13 *Let a, b, and $m > 0$ be integers and $d = \gcd(a, b, m)$. Also, let $a' = \frac{a}{\gcd(a,m)}$, $b' = \frac{b}{d}$, $m' = \frac{m}{\gcd(a,m)}$, and $d' = \frac{\gcd(a,m)}{d}$. Then, the set of solutions of the congruence*

$$ax = by \ (mod\ m) \tag{2.6}$$

is

$$\{(rb't_1 + m't_2, d't_1) | t_1 = 0, 1, \ldots, \frac{m}{d'} - 1; t_2 = 0, 1, \ldots, \gcd(a, m) - 1\},$$

where $ra' = 1 \ (mod\ m')$.

Proof
Let us transform equation (2.6) into the equivalent equation

$$\frac{a}{d}x = \frac{b}{d}y \ (\text{mod } \frac{m}{d}), \tag{2.7}$$

and apply Theorem 2.3.12 to (2.7).$\diamondsuit$

Remark 2.3.1 *Note that*

$$y = \frac{\gcd(a, m)}{\gcd(a, b, m)}$$

is the smallest positive integer for which (x, y) is a solution of $ax = by \ (mod\ m)$, for some x.

Lemma 2.3.1 and Theorem 2.3.14 can be found in [29] (in particular, Lemma 2.3.1 is suggested as an exercise in page 72).

Lemma 2.3.1 *Let m_1 and m_2 be arbitrary positive integers, and let a_1 and a_2 be arbitrary integers. Then the congruences*

$$x = a_1 \ (mod\ m_1)$$

$$x = a_2 \ (mod\ m_2)$$

have a simultaneous solution if and only if $a_1 = a_2 \ (mod \gcd(m_1, m_2))$. If this condition is met, the solution is unique mod $lcm(m_1, m_2)$.

Theorem 2.3.14 *Let p be a prime. Then $x^2 + 1 = 0 \ (mod\ p)$ has solutions if and only if $p = 2$ or $p = 1 \ (mod\ 4)$.*

Lemma 2.3.2 *Let $a_1 \neq a_2, b_1, b_2$, and $m > 0$ be integers. Also, let*

$$d_i = \frac{\gcd(a_i, m)}{\gcd(a_i, b_i, m)},\ i = 1, 2,$$

and let (x_0, y_0) be a simultaneous solution of

$$\left.\begin{aligned} a_1 x &= b_1 y \\ a_2 x &= b_2 y \end{aligned}\right\} \ (mod\ m) \tag{2.8}$$

Then, $lcm(d_1, d_2)$ divides y_0.

Proof
(x_0, y_0) is a solution of (2.8) implies that

$$\left.\begin{aligned} a_1 x_0 &= b_1 y_0 \\ a_2 x_0 &= b_2 y_0 \end{aligned}\right\} \ (\text{mod } m) \tag{2.9}$$

Let $n_i = \gcd(a_i, b_i, m),\ i = 1, 2$. Thus,

$$\frac{a_i}{n_i} x_0 = \frac{b_i}{n_i} y_0 \ (\text{mod } \frac{m}{n_i}).$$

Then, by Theorem 2.3.11, $\gcd(\frac{a_i}{n_i}, \frac{m}{n_i}) | \frac{b_i}{n_i} y_0$. Which implies that $\frac{\gcd(a_i, m)}{n_i} | \frac{b_i}{n_i} y_0$. But,

$$\gcd(\frac{\gcd(a_i, m)}{n_i}, \frac{b_i}{n_i}) = \frac{\gcd(a_i, b_i, m)}{\gcd(a_i, b_i, m)} = 1.$$

Hence, $d_i = \frac{\gcd(a_i, m)}{n_i} | y_0$. Now, since both d_1 and d_2 divide y_0, it is straightforward to see that $\text{lcm}(d_1, d_2)$ divides y_0.$\diamondsuit$

Theorem 2.3.15 *Let $a_1 \neq a_2, b_1, b_2$, and $m > 0$ be integers. Also, let $e_i = \frac{lcm(a_1, a_2)}{a_i}$, $d_i = \frac{\gcd(a_i, m)}{\gcd(a_i, b_i, m)}$, $i = 1, 2$, $l_1 = \frac{m}{lcm(d_1, d_2)}$, and $l_0 = e_1 b_1 - e_2 b_2$. Then, the smallest positive integer y_{min}, for some x', for which (x', y_{min}) is a solution of*

$$\left.\begin{aligned} a_1 x &= b_1 y \\ a_2 x &= b_2 y \end{aligned}\right\} \ (mod\ m) \tag{2.10}$$

is

$$y_{min} = \frac{m}{\gcd(l_0, l_1)}.$$

Proof
First, let us show that there exists x' for which (x', y_{min}) is a simultaneous solution of (2.10). It is easy to see that $d_i = \gcd(a_i, m)$ divides y_{min}. Thus, by Theorem 2.3.11, there exist integers x_1' and x_2' such that

$$a_1 x_1' = b_1 y_{min} \pmod{m} \tag{2.11}$$
$$a_2 x_2' = b_2 y_{min} \pmod{m}. \tag{2.12}$$

Congruences (2.11) and (2.12) are equivalent to

$$r_1 x_1' = \frac{b_1 y_{min}}{d_1} \pmod{m_1} \tag{2.13}$$
$$r_2 x_2' = \frac{b_2 y_{min}}{d_2} \pmod{m_2}, \tag{2.14}$$

where $r_i = \frac{a_i}{d_i}$ and $m_i = \frac{m}{d_i}$, $i = 1, 2$. Note that $\gcd(r_i, m_i) = 1$. Thus, there exist integers $r_i^{-1} \bmod m_i$ such that

$$x_1' = r_1^{-1} \frac{b_1 y_{min}}{d_1} \pmod{m_1} \tag{2.15}$$
$$x_2' = r_2^{-1} \frac{b_2 y_{min}}{d_2} \pmod{m_2}. \tag{2.16}$$

Hence,

$$\begin{aligned} x_1' - x_2' &= r_1^{-1} \frac{b_1 y_{min}}{d_1} + m_1 t_1 - (r_2^{-1} \frac{b_2 y_{min}}{d_2} + m_2 t_2) \\ &= r_1^{-1} \frac{b_1 y_{min}}{d_1} - r_2^{-1} \frac{b_2 y_{min}}{d_2} \pmod{\gcd(m_1, m_2)} \\ &= \frac{(r_1^{-1} b_1 m_1 - r_2^{-1} b_2 m_2) y_{min}}{m} \pmod{\gcd(m_1, m_2)} \\ &= \frac{(r_1^{-1} b_1 m_1 - r_2^{-1} b_2 m_2)}{\gcd(l_0, l_1)} \pmod{\gcd(m_1, m_2)} \end{aligned}$$

since $d_i = \frac{m}{m_i}$ and $y_{min} = \frac{m}{\gcd(l_0, l_1)}$.

$$\begin{aligned} x_1' - x_2' &= \frac{r_1 r_2 (r_1^{-1} \frac{m_1}{\gcd(m_1, m_2)} b_1 - r_2^{-1} \frac{m_2}{\gcd(m_1, m_2)} b_2) \gcd(m_1, m_2)}{r_1 r_2 \gcd(l_0, l_1)} \pmod{\gcd(m_1, m_2)} \\ &= \frac{(\frac{r_2}{\gcd(r_1, r_2)} \frac{m_1}{\gcd(m_1, m_2)} b_1 - \frac{r_1}{\gcd(r_1, r_2)} \frac{m_2}{\gcd(m_1, m_2)} b_2) \gcd(m_1, m_2)}{\mathrm{lcm}(r_1, r_2) \gcd(l_0, l_1)} \pmod{\gcd(m_1, m_2)}. \end{aligned}$$

Let $\bar{r_i} = \frac{r_i}{\gcd(r_1, r_2)}$ and $\bar{m_i} = \frac{m_1}{\gcd(m_1, m_2)}$. We can show that $e_1 = \bar{r_2} \bar{m_1}$ and that $e_2 = \bar{r_1} \bar{m_2}$. Thus, $l_0 = \bar{r_2} \bar{m_1} b_1 - \bar{r_1} \bar{m_2} b_2$. Therefore,

$$x_1' - x_2' = \frac{(\bar{r_2} \bar{m_1} b_1 - \bar{r_1} \bar{m_2} b_2) \gcd(m_1, m_2)}{\mathrm{lcm}(r_1, r_2) \gcd(\bar{r_2} \bar{m_1} b_1 - \bar{r_1} \bar{m_2} b_2, l_1)} \pmod{\gcd(m_1, m_2)}$$

$$= \frac{t_1 \gcd(m_1, m_2)}{\mathrm{lcm}(r_1, r_2)} \pmod{\gcd(m_1, m_2)},$$

since $\gcd(l_0, l_1)$ divides $(\bar{r_2}\bar{m_1}b_1 - \bar{r_1}\bar{m_2}b_2)$. Recall that $\gcd(r_i, m_i) = 1$, thus $\mathrm{lcm}(r_1, r_2)$ does not divide $\gcd(m_1, m_2)$). Henceforth,

$$\begin{aligned} x_1' - x_2' &= \frac{t_1}{\mathrm{lcm}(r_1, r_2)} \gcd(m_1, m_2) \pmod{\gcd(m_1, m_2)} \\ &= 0 \pmod{\gcd(m_1, m_2)}. \end{aligned}$$

Therefore, by Lemma 2.3.1, there exists an integer x' for which (x', y_{min}) is a simultaneous solution of (2.10).

Finally, let (x_0, y_0) be any other simulteneous solution of (2.10). In this part we will show that $y_{min} \leq y$. By Lemma 2.3.2, $y_0 = \mathrm{lcm}(d_1, d_2)r_0$, for some positive integer r_0, Now, multiply each equation in (2.10) by e_1 and e_2, respectively.

$$e_1 a_1 x_0 = e_1 b_1 y_0 \pmod{m} \tag{2.17}$$

$$e_2 a_2 x_0 = e_2 b_2 y_0 \pmod{m} \tag{2.18}$$

Subtracting equation (2.18) from (2.17) to eliminate x_0, we endup with

$$(e_1 b_1 - e_2 b_2) y_0 = 0 \pmod{m} \tag{2.19}$$

and replacing y_0 by $\mathrm{lcm}(d_1, d_2)r_0$ in (2.19),

$$(e_1 b_1 - e_2 b_2)\mathrm{lcm}(d_1, d_2) r_0 = 0 \pmod{m}. \tag{2.20}$$

Or,

$$r_0 = \frac{m}{\mathrm{lcm}(d_1, d_2)\gcd(l_0, l_1)} t_0, \tag{2.21}$$

for some positive t_0 since y is positive. Therefore

$$\begin{aligned} y_0 &= \mathrm{lcm}(d_1, d_2) r_0 \\ &= \mathrm{lcm}(d_1, d_2) \frac{m}{\mathrm{lcm}(d_1, d_2)\gcd(l_0, l_1)} t_0 \\ &= y_{min} t_0 \geq y_{min}. \diamondsuit \end{aligned}$$

Let us recall from section 2.1 that $GF(p^n)^*$, $n > 0$, is a cyclic group of order $p^n - 1$. Let g be a generator of $G(p^n)^*$. Then, for each $a \in G(p^n)^*$, there is a unique nonnegative integer $\mathrm{Ind}_g(a)$, (or simply $\mathrm{Ind}(a)$, if it can be understood from the context), called the *index* of a with respect to g, such that $a = g^{\mathrm{Ind}(a)}$. Also, let k_a be the order (i.e., period) of $a \in G(p^n)^*$. Note that the identity of $G(p^n)^*$, denoted by 1, has index $p^n - 1$.

Lemma 2.3.3 *Let $a \in GF(p^n)^*$ and k_a be the order of a. Then, the order of a^t is $\frac{k_a}{\gcd(k_a,t)}$, for any nonnegative integer t.*

Lemma 2.3.4 *Let $a \in GF(p^n)^*$ and k_a be its order. Then, there exists a positive integer r_a, such that $\gcd(r_a, k_a) = 1$ for which $Ind(a) = r_a\mu_a$, where $\mu_a = \frac{p^n-1}{k_a}$.*

Proof
Let k_a be the order of $a \in G(p^n)^*$ and g be a primitive of $G(p^n)^*$. Thus, $a^{k_a} = 1 \pmod{p^n}$. Or, equivalently, $k_a\mathrm{Ind}_g(a) = \mathrm{Ind}_g(1) = p^n - 1 = 0 \pmod{p^n - 1}$. Then, $\mathrm{Ind}_g(a) = 0 \pmod{\frac{p^n-1}{k_a} = \mu_a}$, since the order of an element always divides the order of its group. Hence, $\mathrm{Ind}_g(a) = r_a\frac{p^n-1}{k_a}$ for some positive integer r_a. Note that $1 \le r_a \le k_a$, since $1 \le \mathrm{Ind}_g(a) \le p^n - 1$.

Now, let us show that r_a and k_a are relatively prime. Assume the contrary. Suppose that $\gcd(r_a, k_a) = d > 1$. Then, there exist relatively prime positive integers t_1 and t_2 with $k_a = dt_1$ and $r_a = dt_2$. So, $a = g^{\frac{p^n-1}{k_a}r_a} = g^{\frac{p^n-1}{dt_1}dt_2} = g^{\frac{p^n-1}{t_1}t_2}$.
Thus, applying Lemma 2.3.3,

$$\begin{aligned} k_a &= \frac{p^n - 1}{\gcd(p^n - 1, \frac{p^n-1}{t_1}t_2)} \\ &= \frac{(p^n - 1)t_1}{(p^n - 1)\gcd(t_2, t_1)} \\ &= \frac{t_1}{1} = t_1 < k_a, \end{aligned}$$

which is a contradiction and the proof is completed.$\diamondsuit$

Lemma 2.3.5 *Let $a \in GF(p^n)^*$, k_a be the order of a and $\mu_a = \frac{p^n-1}{k_a}$. Then*

$$\gcd(Ind(a), p^n - 1) = \mu_a.$$

Proof
Note that, by means of Lemma 2.3.4, there exists a positive integer $r_a < k_a$, such that $\gcd(r_a, k_a) = 1$. Hence,

$$\begin{aligned} \gcd(\mathrm{Ind}(a), p^n - 1) &= \gcd(r_a\frac{p^n - 1}{k_a}, p^n - 1) \\ &= \frac{p^n - 1}{k_a}\gcd(r_a, k_a) \\ &= \mu_a * 1 \\ &= \mu_a.\diamondsuit \end{aligned}$$

Theorem 2.3.16 *Let a_1, $a_2 \in G(p^n)^*$ and g be a primitive of $G(p^n)^*$. Also, for $t = 1, 2$, let k_{a_t}, be the order of a_t. Define $\mu_{a_t} = \frac{p^n-1}{k_{a_t}}$. Then, the smallest positive integer i that solves*

$$a_1^j = a_2^i \ (mod\ p^n), \tag{2.22}$$

for some j, is

$$i_{min} = \frac{k_{a_2}}{\gcd(k_{a_1}, k_{a_2})}.$$

Proof
The index form of equation (2.22) is

$$\mathrm{Ind}_g(a_1)j = \mathrm{Ind}_g(a_2)i \ (\mathrm{mod}\ p^n - 1) \tag{2.23}$$

By Theorem 2.3.13, the smallest positive integer i_{min} that solves (2.23), for some j is

$$i_{min} = \frac{\gcd(\mathrm{Ind}_g(a_1), p^n - 1)}{\gcd(\mathrm{Ind}_g(a_1), p^n - 1, \mathrm{Ind}_g(a_2))}.$$

Applying Lemma 2.3.5,

$$i_{min} = \frac{\mu_{a_1}}{\gcd(\mu_{a_1}, \mathrm{Ind}_g(a_2))}.$$

Now, by Lemma 2.3.4, there exists a positive integer r_{a_2} for which $\mathrm{Ind}_g(a_2) = \mu_{a_2} r_{a_2}$ and $\gcd(k_{a_2}, r_{a_2}) = 1$. Thus,

$$i_{min} = \frac{p^n - 1}{k_{a_1} \gcd(\frac{p^n-1}{k_{a_1}}, \frac{p^n-1}{k_{a_2}} r_{a_2})} = \frac{k_{a_2}}{\gcd(k_{a_2}, k_{a_1} r_{a_2})}.$$

Finally, since $\gcd(k_{a_2}, r_{a_2}) = 1$ and applying Lemma 2.3.1, we endup with

$$i_{min} = \frac{k_{a_2}}{\gcd(k_{a_1}, k_{a_2})}. \diamondsuit$$

Theorem 2.3.17 *Let $a_1 \neq a_2, b_1, b_2, g \in G(p^n)^*$, g a primitive of $G(p^n)^*$. Also, let k_i be the order of a_i and define $n_i = \gcd(\frac{p^n-1}{k_i}, Ind_g(b_i))$, $i = 1, 2$. Also, let y_{min_i} be the smallest positive integer for which (x_i', y_{min_i}) is a simultaneous solution of equations (2.24) and (2.25), for some x_i', $i = 1, 2$*

$$a_1^x = b_1^y \ (mod\ p^n) \tag{2.24}$$

$$a_2^x = b_2^y \ (mod\ p^n) \tag{2.25}$$

Then, the smallest positive integer y_{min}, for some x', for which (x', y_{min}) is a solution of equations (2.24) *and* (2.25) *is*

$$y_{min} = \frac{p^n - 1}{\gcd(e_1 Ind_g(b_1) - e_2 Ind_g(b_2), \gcd(k_1 n_1, k_2 n_2))},$$

where

$$e_i = \frac{lcm(Ind_g(a_1), Ind_g(a_2))}{Ind_g(a_i)},\ i = 1, 2.$$

Proof
Let $l_1 = \frac{p^n - 1}{\mathrm{lcm}(y_{min_1}, y_{min_2})}$. Then,

$$\begin{aligned} l_1 &= \frac{(p^n - 1)\gcd(y_{min_1}, y_{min_2})}{y_{min_1} * y_{min_2}} \\ &= \gcd(\frac{p^n - 1}{y_{min_1}}, \frac{p^n - 1}{y_{min_2}}) \\ &= \gcd(\frac{p^n - 1}{\frac{\mu_1}{n_1}}, \frac{p^n - 1}{\frac{\mu_2}{n_2}}) \\ &= \gcd(\frac{p^n - 1}{\frac{p^n - 1}{k_1 n_1}}, \frac{p^n - 1}{\frac{p^n - 1}{k_2 n_2}}) \\ &= \gcd(k_1 n_1, k_2 n_2). \end{aligned}$$

System of equations (2.24) and (2.25), in index form, is equivalent to

$$\left.\begin{array}{l} \mathrm{Ind}(a_1)x = \mathrm{Ind}(b_1)y \pmod{p^n - 1} \\ \mathrm{Ind}(a_2)x = \mathrm{Ind}(b_2)y \pmod{p^n - 1} \end{array}\right\} \tag{2.26}$$

Finally, apply Theorem 2.3.15 to (2.26) and replace l_1 by previous value.$\diamondsuit$.

Our next result is a generalization of Theorem 2.3.17.

Theorem 2.3.18 *Let $a_1, b_1 \in G(p_1^N)^*$, and $a_2, b_2 \in G(p_2^N)^*$, $a_1 \neq a_2$, and g_1, g_2 be primitives of $G(p_1^N)^*$ and $G(p_2^N)^*$, respectively. Let k_i be the order of a_i and y_{min_i} be the smallest positive integer for which (x_i', y_{min_i}) is a solution of equations* (2.27) *and* (2.28)*, for some x_i', $i = 1, 2$,*

$$a_1^x = b_1^y \ (mod\ p^{N_1}) \tag{2.27}$$

$$a_2^x = b_2^y \ (mod\ p^{N_2}) \tag{2.28}$$

Then, the smallest positive integer y_{min}, for some x', for which (x', y_{min}) is a simultaneous solution of (2.27) *and* (2.28) *is*

$$y_{min} = \frac{m}{\gcd(l_0, l_1)},$$

where, for $i = 1, 2$,

$$\begin{aligned}
m &= lcm(p^{N_1} - 1, p^{N_2} - 1), \\
l_0 &= e_1 m_1' Ind_{g_1}(b_1) - e_2 m_2' Ind_{g_2}(b_2), \\
m_i' &= \frac{m}{p^{N_i} - 1}, \\
\mu_i &= \frac{p^{N-i} - 1}{k_i}, \\
n_i &= \frac{\mu_i}{y_{min_i}}, \\
l_1 &= \gcd(k_1 m_1' n_1, k_2 m_2' n_2) \\
e_i &= \frac{lcm(m_1' Ind_{g_1}(a_1), m_2' Ind_{g_2}(a_2))}{m_i' Ind_{g_i}(a_i)}.
\end{aligned}$$

Chapter 3

Previous work

In this chapter we give a synopsis of the work on reverse engineering MS–orbits, as well as genetic networks, with particular emphasis on those results which we use in this work.

3.1 Linear modular systems

One of the classical and most important works in linear modular systems is the work of B. Elspas [12] whose main interest was to study sequential circuits. However, this same theory describes the orbital structure of the symmetry matrix for symmetric FFTs with prime edge–length, which in turn affects the structure of the MS–orbits that we wish to study. In this section we present the most relevant ideas and results of Elspas' work. Proofs of the theorems stated here can be found in [12].

Definition 3.1.1 *A linear modular system, abbreviated LMS, is a finite dynamical system* (Z_p^n, S, Z_p) *where* $S : Z_p^n \to Z_p^n$ *is linear.*

Given a linear modular system (LMS), it is of interest for many applications to know its orbit (cycle or sequential) structure. In particular, the structure of LMSs over Z_p, the integers modulo a prime p, is of considerable importance in areas such as finite–state machines, linear sequential networks, symmetric fast Fourier transforms, digital communication, error correction codes, etc.

Let S be a nonsingular $n \times n$ matrix over Z_p representing an LMS. Also, let $\mathbf{x}$ be a particular initial state of the system. State $\mathbf{x}$ can be regarded as a n–tuple

$(x_1, x_2, \ldots, x_n)$ where each x_i is an element from Z_p. Since any LMS is a deterministic finite system, each state $\mathbf{x}$ can be reached in only one way and from a particular state, the system can move to only one next state. In other words, if an LMS starts in $\mathbf{x}$, it will run through the sequence of states $\mathbf{x}$, $S\mathbf{x}$, $S^2\mathbf{x}$, $S^3\mathbf{x}$, ..., which is represented by $O_S(\mathbf{x})$. In fact, $O_S(\mathbf{x})$ is a finite sequence of states having, at most, k states, where k is the period of S.

Given a nontrivial state $\mathbf{x}$ (i.e., $\mathbf{x} \neq \mathbf{0}$) and a nonsingular $n \times n$ matrix S, there exists a nonnegative integer $t \leq k$ such that $S^t\mathbf{x} = \mathbf{x}$. Assume that t is the smallest such an integer. Hence, $O_S(\mathbf{x}) = \{\mathbf{x}, S\mathbf{x}, S^2\mathbf{x}, \ldots, S^{t-1}\mathbf{x}\}$. That is, the state diagram of the entire system consists only of *orbits* (or *cycles*). In particular, if $\mathbf{x} = (0, 0, \ldots, 0) = \mathbf{0}$ (i.e., the zero state), then the orbit for $\mathbf{x}$, $O_S(\mathbf{x})$, contains only the zero state. This orbit is sometimes called the *trivial* orbit. In general, the number of states in $O_S(\mathbf{x})$ is called the *orbit length* or *cycle length.*

The entire orbit structure of any LMS can be completely derived from the algebraic properties of the matrix S.

The following two theorems illustrate two important cases when the characteristic polynomial is irreducible. The first one is known as a *maximal* system.

Theorem 3.1.1 *Let $S \in \mathcal{M}_n$ with $\phi_S(x)$ irreducible and maximal. Then, the LMS associated with S has only two orbits; one orbit of length one, the trivial orbit, and the other of length $p^n - 1$ that accounts for all the nonzero states.*

Theorem 3.1.2 *Let $S \in \mathcal{M}_n$ be such that $\phi_S(x)$ is irreducible but not maximal. Then, the LMS associted with S has μ nontrivial orbits of length k, where k is the period of $\phi_S(x)$ and $\mu = \frac{p^n-1}{k}$.*

It is customary to use the notation $(1, \mu(k))$ to indicate that the orbit structure of a LMS has μ orbits of length k, besides the trivial orbit of length one.

From the theoretical and computational points of view, the orbit structure of linear systems with reducible characteristic polynomials are, in general, more difficult to determine.

Let S be an $n \times n$ matrix over Z_p such that $\phi_S(x) = P_1(x)P_2(x)$, where $P_1(x)$ and $P_2(x)$ are distinct irreducible polynomials of degree d_1 and d_2, respectively. Let V_{P_i} be the null space associated to $P_i(S)$, $i = 1, 2$. The restriction of S to V_{P_i} yields

the orbit structure $(1, \mu_{P_i}(k_{P_i}))$, where k_{P_i} is the period of $P_i(x)$ and $\mu_{P_i} = \frac{p^{d_i}-1}{k_{P_i}}$. Let us represent $(1, \mu_{P_i}(k_{P_i}))$ by the *formal sum* $1 + \mu_{P_i}(k_{P_i})$. The *formal product* of $1 + \mu_{P_1}(k_{P_1})$ and $1 + \mu_{P_2}(k_{P_2})$ is defined by the rule

$$(1 + \mu_{P_1}(k_{P_1}))(1 + \mu_{P_2}(k_{P_2})) = 1 + \mu_{P_1}(k_{P_1}) + \mu_{P_2}(k_{P_2}) + \mu_{P_1,P_2}(k_{P_1,P_2}),$$

where

$$\mu_{P_1,P_2} = \mu_{P_1}\mu_{P_2}\gcd(k_{P_1}, k_{P_2})$$

and

$$k_{P_1,P_2} = \mathrm{lcm}(k_{P_1}, k_{P_2}).$$

Theorem 3.1.3 *Let $S \in \mathcal{M}_n$ be nonsingular with $\phi_S(x) = P_1(x)P_2(x)$, where $P_1(x)$ and $P_2(x)$ are distinct irreducible polynomials of degree d_1 and d_2, respectively. Then, the orbit structure of (Z_p^n, S, Z_p) is*

$$(1, \mu_{P_1}(k_{P_1}), \mu_{P_2}(k_{P_2}), \mu_{P_1,P_2}(k_{P_1,P_2})).$$

The following theorem summarizes the case when the characteristic and minimal polynomials are equal to a power of an irreducible polynomial.

Theorem 3.1.4 *Let $S \in \mathcal{M}_n$ with characteristic and minimal polynomials equal to $(P(x))^e$, where $P(x)$ is an irreducible polynomial of degree d and $e > 1$. Then,*

1. *There is a nested sequence of subspaces $U_{P^0} \subset U_{P^1} \subset \cdots \subset U_{P^j} \subset \cdots \subset U_{P^e}$, where U_{P^j} is the null space of $(P(S))^j$ and its dimension is jd.*

2. *The number of states in U_{P^j} is p^{jd}, of which $p^{(j-1)d}$ states are in $U_{P^{j-1}}$ and hence, $p^{jd} - p^{(j-1)d} = p^{d(j-1)}(p^d - 1)$ are in $U_{P^j} - U_{P^{j-1}}$.*

3. *All the orbits in $U_{P^j} - U_{P^{j-1}}$ are of length $k_P p^{r_j}$, where k_P is the period of $P(x)$ and r_j is the smallest nonnegative integer for which $p^{r_j} \geq j$.*

4. *The orbit structure of (Z_p^n, S, Z_p) is*

$$(1, \mu_P(k_P p^{r_1}), \mu_{P^2}(k_P p^{r_2}), \ldots, \mu_{P^e}(k_P p^{r_e})),$$

where $\mu_{P^j} = \frac{p^{d(j-1)}(p^d-1)}{k_P p^{r_j}}$.

For the general case where the characteristic polynomial $\phi_S(x)$ of S contains irreducible factors with multiplicities greater than one, the orbit structure of (Z_p^n, S, Z_p) depends on what are known as the *elementary divisors* of S; irreducible factors of $\phi_S(x)$ having the form $(P_i(x))^{e_{ij}}$, where $e_{i1} \geq e_{i2} \geq \cdots \geq e_{ir_i}$, $i = 1, 2, \ldots, r$.

Two important properties of elementary divisors are the following. First, the product of all elementary divisors is $\phi_S(x)$. Second, the minimal polynomial, $m_S(x)$, is the product of the highest degree elementary divisors.

Theorem 3.1.5 *The orbit structure of (Z_p^n, S, Z_p) is the formal product of the orbits of the elementary divisors of S.*

Let $S \in \mathcal{M}_n$ be nonsingular and let k be the period of S. For any $\mathbf{x}, \mathbf{y} \in Z_p^n$, define $\mathbf{x} \approx_S \mathbf{y}$ if and only if $\mathbf{y} = S^j\mathbf{x}$ for some integer j. It is readily verified that $\approx_S$ is an equivalence relation. The equivalence class containing $\mathbf{x} \in Z_p^n$,

$$O_S(\mathbf{x}) = \{S^j\mathbf{x} \bmod p : \ j \text{ integer } \}, \tag{3.1}$$

is called the *orbit* of the action of S on $\mathbf{x}$. A set of representatives of equivalence classes is called a *fundamental set*, denoted by $\mathcal{F}_S$. The number of elements in $O_S(\mathbf{x})$, denoted $|O_S(\mathbf{x})|$, is called its *orbit length*. The orbit length is always a divisor of k. Thus, the set of all orbits for the action of S constitutes a partition of Z_p^n and there exists a non–unique collection of elements $\{\mathbf{x}_1, \ldots, \mathbf{x}_t\}$ such that

$$Z_p^n = \cup_{j=1}^t O_S(\mathbf{x}_j) \tag{3.2}$$

$$\emptyset = O_S(\mathbf{x_i}) \cap O_S(\mathbf{x_j}), \text{ for } i \neq j. \tag{3.3}$$

Let M be a nonsingular matrix that commutes with S. The action of M induces a relation $\approx_{MS}$ on the set of S–orbits, or equivalently on $\mathcal{F}_\mathcal{S}$, defined by

$$O_S(\mathbf{x}) \approx_{MS} O_S(\mathbf{y}) \text{ if and only if } M^i\mathbf{x} = S^j\mathbf{y} \text{ for some integers } i \text{ and } j.$$

Lemma 3.1.1 *Let $S \in \mathcal{M}_n$ and $M \in \mathcal{N}(S)$ be nonsingular. Then, the relation $\approx_{MS}$ is an equivalence relation on the set of S–orbits.*

Proof
Let $\mathbf{x} \in \mathcal{F}_\mathcal{S}$. Then, $M^0\mathbf{x} = S^0\mathbf{x}$. Thus, $O_S(\mathbf{x}) \approx_{MS} O_S(\mathbf{x})$ (*reflexive*).

Let $\mathbf{x}, \mathbf{y} \in \mathcal{F}_\mathcal{S}$ with $O_S(\mathbf{x}) \approx_{MS} O_S(\mathbf{y})$. Let i_1 and j_1 be the integers for which $M^{i_1}\mathbf{x} = S^{j_1}\mathbf{y}$. Also, let k_M and k_S be the periods of M and S, respectively. We can

assume without loose of generality that $i_1 \leq k_M$ and that $j_1 \leq k_S$. Thus, by the commutativity of M and S

$$M^{k_M - i_1} S^{k_S - j_1}(M^{i_1}\mathbf{x}) = M^{k_M - i_1} S^{k_S - j_1}(S^{j_1}\mathbf{y})$$

if and only if

$$S^{k_S - j_1} M^{k_M - i_1} M^{i_1}\mathbf{x} = M^{k_M - i_1} S^{k_S - j_1 + j_1}\mathbf{y}$$

if and only if

$$S^{k_S - j_1} M^{k_M}\mathbf{x} = M^{k_M - i_1} S^{k_S}\mathbf{y}$$

if and only if

$$S^{k_S - j_1}\mathbf{x} = M^{k_M - i_1}\mathbf{y},$$

which implies that $O_S(\mathbf{y}) \approx_{MS} O_S(\mathbf{x})$ (*symmetric*).

Let $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathcal{F}_{\mathcal{S}}$ with $O_S(\mathbf{x}) \approx_{MS} O_S(\mathbf{y})$ and $O_S(\mathbf{y}) \approx_{MS} O_S(\mathbf{z})$. Let i_1, j_1, i_2, and j_2 be the integers for which $M^{i_1}\mathbf{x} = S^{j_1}\mathbf{y}$ and $M^{i_2}\mathbf{y} = S^{j_2}\mathbf{z}$. Note that $M^{i_1+i_2}\mathbf{x} = M^{i_2}S^{j_2}\mathbf{y} = S^{j_1}(M^{i_2}\mathbf{y}) = S^{j_1+j_2}\mathbf{z}$. Therefore, $O_S(\mathbf{x}) \approx_{MS} O_S(\mathbf{z})$ (*transitivity*). Therefore, $\approx_{MS}$ is an equivalence relation on the set of S–orbits.$\diamondsuit$

We call the equivalence classes induced by $\approx_{MS}$ *MS–orbits* and denote them by O_{MS}. The number of such classes is denoted by $|O_{MS}|$.

3.2 Symmetric prime edge–length FFTs

For some data intensive problems, for instance, x–ray crystal diffraction intensity analysis, reductions in the amount of data can make a significant difference even though the arithmetic complexity remains the same. These reductions are induced by structured redundancy patterns in the input, which in turn induce redundancies patterns in the output. Such a problem, which has recently received attention [42], [43], [44], is the problem of making more efficient the computation of multidimensional discrete Fourier transforms (DFT) with linear symmetries.

For an n–dimensional prime edge–length DFT such a symmetry can be expressed as a $n \times n$ nonsingular matrix S over Z_p where p is the prime edge–length. Auslander and Shenefelt [3] have shown that by reordering $\mathcal{F}_S$ under the action of a generator g of the cyclic group Z_p^*, the arithmetic complexity of the DFT can be reduced through the use of cyclic convolutions. Seguel et al [42] has shown that a further reduction in arithmetic count is possible if instead of reordering $\mathcal{F}_S$ by the action of a generator of Z_p^* we reorder $\mathcal{F}_S$ by the action of an $n \times n$ nonsingular matrix M that commutes

with S.

In the rest of this section we explain the problem more fully and outline the approach given in [42].

For the purposes of this work it suffices to think of the d–dimensional discrete Fourier transform (DFT) with edge–length N as simply a function

$$F_N : \mathcal{A}_{d,N}(C) \to \mathcal{A}_{d,N}(C)$$

defined by

$$\hat{f} = F_N(f) = \frac{1}{\sqrt{N}} \sum_{\mathbf{l} \in Z_N^d} f(\mathbf{l}) w_N^{\mathbf{k}\cdot\mathbf{l}}, \ \mathbf{k} \in Z_N^d \tag{3.4}$$

where C denotes the set of complex (or real) numbers, $\mathcal{A}_{d,N}(C)$ denotes the set of d–dimensional arrays with edge–length N over C, $w_N = \exp(\frac{2\pi i}{N})$, $i = \sqrt{-1}$, $\cdot$ denotes the dot product, and f is a real– or complex–valued function defined on Z_N^d.

The time required to compute the d–dimensional DFT with edge–length N using the definition is $O(N^{2d})$. However, the *fast* Fourier transform ("FFT") can be computed in time $O(N^d log\ N)$. A fast Fourier transform (FFT) for $d = 1$ reduces the number of operations from $O(N^2)$ to $O(N \log(N))$. The usual method for computing an FFT for $d \geq 2$ consists of applying N^{d-1} one–dimensional FFTs along each of the d dimensions.

This yields $O(N^d \log(N))$ operations, a complexity estimate that cannot be improved.

As was stated above, the input of a DFT (or FFT) is a complex–valued mapping f defined on Z_N^d. A *linear symmetry* on such a function f is defined as a $d \times d$ nonsingular matrix S over Z_N such that $f(\mathbf{k}) = f(S\mathbf{k})$ for all $\mathbf{k} \in Z_N^d$. In the case that $\det(S) = \pm 1 \bmod N$, S is called *unimodular*. Of particular interest are the linear symmetries in two– and three–dimensional crystallographic FFTs.

Let $S_* = (S^{-1})^t$, where A^t denotes the transpose of matrix A. It is well known in linear algebra that $S\mathbf{k} \cdot \mathbf{l} = \mathbf{k} \cdot S^t\mathbf{l}$. Thus, if S is unimodular and f is S–symmetric, $\hat{f}(S_*\mathbf{k}) = \hat{f}(\mathbf{k})$. Then, $\hat{f}$ is S_*–symmetric.

We call an orbit determined by the symmetry matrix S a *symmetry orbit*. Values of f are constant on each symmetry orbit. Let $\mathcal{F}_S$ and $\mathcal{F}_{S_*}$ be fundamental sets corresponding to $\approx_S$ and $\approx_{S_*}$, respectively. The set $f(\mathcal{F}_S) = \{f(\mathbf{k}) | \mathbf{k} \in \mathcal{F}_S\}$ is called a *fundamental input set*, while the set $\hat{f}(\mathcal{F}_{S_*}) = \{\hat{f}(\mathbf{k}) | \mathbf{k} \in \mathcal{F}_{S_*}\}$ is called a *fundamental output set*.

Let $N = p$ be any prime. A *prime edge–length symmetric DFT* is thus a linear transformation defined by the equations

$$\hat{f}(\mathbf{k}) = \sum_{\mathbf{a}\in\mathcal{F}_S} K_p(\mathbf{k},\mathbf{a}) f(\mathbf{a}), \quad \mathbf{k} \in \mathcal{F}_{S_*}, \tag{3.5}$$

where for each $\mathbf{k} \in \mathcal{F}_{\mathcal{S}_*}$ and each $\mathbf{l} \in \mathcal{F}_{\mathcal{S}}$,

$$K_p(\mathbf{k},\mathbf{a}) = \sum_{\mathbf{l}\in O_S(\mathbf{a})} w_p^{\mathbf{k}\cdot\mathbf{l}} \tag{3.6}$$

Since the output is S_*–symmetric, the DFT is completely determined by (3.5). However, equation (3.5) involves

$$\sum_{\mathbf{k}\in\mathcal{F}_{S_*}} \sum_{l\in\mathcal{F}_S} |O_S(\mathbf{l})| = \sum_{\mathbf{k}\in\mathcal{F}_{S_*}} p^d \leq p^{2d}$$

or $O(p^{2d})$ arithmetic operations. That is, computing a DFT by simply taking into account linear symmetries may not, in general, be enough for reducing the total arithmetic count and, hence, it is justified the search for more economical methods.

Example 3.2.1 *Let us consider a two–dimensional example. The mapping f defined on Z_5^2 by the matrix*

$$f = \begin{pmatrix} 2.9 & 2.3 & 1.5 & 1.5 & 2.3 \\ 1.2 & 6.0 & 4.3 & 4.6 & 2.8 \\ 1.4 & 3.3 & 5.1 & 4.2 & 1.7 \\ 1.4 & 1.7 & 4.2 & 5.1 & 3.3 \\ 1.2 & 2.8 & 4.6 & 4.3 & 6.0 \end{pmatrix} \tag{3.7}$$

is S–symmetric where

$$S = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} \tag{3.8}$$

(We assume that rows and columns are numbered 0, 1, 2, 3, 4.*) For instance, if we let* $\mathbf{k} = (2,1)$*, then* $S\mathbf{k} = (-2,-1) = (3,4)$*. Thus,* $f(\mathbf{k}) = f(S\mathbf{k}) = 3.3$.

For instance, a fundamental set for the S–orbits induced by the symmetry matrix S over Z_5 given by (3.8) *is*

$$\mathcal{F}_S = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(1,3),(1,4),(2,0),(2,1),(2,2),(2,3),(2,4)\}.$$

An matrix of the form

$$H = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & & a_n \\ a_1 & a_2 & a_3 & \cdots & a_n & a_{n+1} \\ a_2 & a_3 & & & & a_{n+2} \\ \vdots & & & \ddots & & \vdots \\ & a_n & & & \ddots & \\ a_n & a_{n+1} & a_{n+2} & \cdots & & a_{2n} \end{pmatrix}$$

is called a *Hankel matrix*. If matrix H has the form

$$H = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & & a_n \\ a_1 & a_2 & a_3 & \cdots & a_n & a_0 \\ a_2 & a_3 & & & & a_1 \\ \vdots & & & \ddots & & \vdots \\ & a_n & & & \ddots & \\ a_n & a_{n+1} & a_{n+2} & \cdots & & a_{n-1} \end{pmatrix}$$

it is called *Hankel circulant*. A product of the form $\mathbf{Y} = H\mathbf{X}$, where H is an $N \times N$ Hankel–circulant matrix and $\mathbf{X}$ and $\mathbf{Y}$ are N–point vectors, is called an N–point *cyclic convolution*. Cyclic convolutions can be performed in $O(N \log N)$ operations by using the *fast cyclic convolution algorithm* [42].

An S–symmetric function f is constant on each S–orbit and is thus completely determined by its values on a fundamental set. Auslander and Shenefelt [3] have shown that, for prime edge–length symmetric DFTs, a fundamental set can be reordered by a generator g of the multiplicative cyclic group of Z_p in such a way that the DFT can be computed solely in terms of cyclic convolutions. This approach presents a method in which the complexity is reduced to $O(p^{2d-1})$.

Efficiency increases with decreasing the number of cyclic convolutions. In [42] it is shown that the number of cyclic convolutions can be decreased if, instead of reordering $\mathcal{F}_{\mathcal{S}_*}$ by a generator of the cyclic group Z_p^*, we reorder it via an $n \times n$ nonsingular matrix M that commutes with S^t (equivalently, $MS_* = S_*M$). This method is sometimes called the *M–method*. By Lemma 3.1.1, such a matrix M induces an equivalence relation $\approx_{MS}$ on the set of S–orbits, or equivalently on $\mathcal{F}_{\mathcal{S}}$. Then (3.5) can be written as

$$[\hat{f}(\mathcal{F}_{\mathcal{S}_*})] = [[W_{(\mathbf{a},\mathbf{b})}(k,l)]_{(k,l)}]_{(\mathbf{a},\mathbf{b})}[f(\mathcal{F}_{\mathcal{S}})], \tag{3.9}$$

where the nested brakets denote a block matrix, $\mathbf{a} \in \mathcal{F}_{MS_*}$ and $\mathbf{b} \in \mathcal{F}_{M^tS}$, and each block $W_{(\mathbf{a},\mathbf{b})}$ is Hankel. Thus, we can compute $\hat{f}$ solely in terms of cyclic convolutions. In the method of Auslander–Shenefelt, which we call the *generator method*,

the S–orbits are reordered under the action of a generator g of Z_p^*. This can be considered as a special case of our procedure in which M is the scalar matrix gI.

The arithmetic complexity of computing $\hat{f}$ by means of (3.9) is

$$O(|\mathcal{F}_{MS_*}||F_{M^tS}|N\log N) = O(|\mathcal{F}_{\mathcal{MS}}|^{\in}\mathcal{N}\log\mathcal{N}) \tag{3.10}$$

arithmetic operations. The goal is to minimize the number $|\mathcal{F}_{MS}|$ of MS–orbits in order to reduce the arithmetic complexity. In general, a nonsingular matrix M gives fewer segments than the action of gI. The best case is when $|\mathcal{F}_{MS}| = 1$. The following result is proved in [42].

Theorem 3.2.1 *Let $S \in \mathcal{M}_n$ be nonsingular with $\phi_S(x)$ irreducible and let $M \in \mathcal{N}(S)$ be maximal. Then there is exactly one MS–orbit and its size is $i_{\phi_S} = \frac{p^n-1}{k_{\phi_S}}$, where k_{ϕ_S} is the size of the S–orbits.*

Example 3.2.2 *Let us consider an example in which we compare the generator method with the M–method discussed in the previous section. Let $d = 2$, $p = 7$, and*

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 6 & 0 \end{pmatrix} \ mod\ 7.$$

Matrix S partitions Z_7^2 into thirteen S–orbits: the trivial S–orbit, $O_S(\mathbf{0})$, plus twelve S–orbits of length 4, as shown below.

$$\begin{aligned}
O_S((0,0)) &= \{(0,0)\} \\
O_S((0,1)) &= \{(0,1),(1,0),(0,6),(6,0)\} \\
O_S((0,2)) &= \{(0,2),(2,0),(0,5),(5,0)\} \\
O_S((0,3)) &= \{(0,3),(3,0),(0,4),(4,0)\} \\
O_S((1,1)) &= \{(1,1),(1,6),(6,6),(6,1)\} \\
O_S((1,2)) &= \{(1,2),(2,6),(6,5),(5,1)\} \\
O_S((1,3)) &= \{(1,3),(3,6),(6,4),(4,1)\} \\
O_S((1,4)) &= \{(1,4),(4,6),(6,3),(3,1)\}
\end{aligned}$$

$$
\begin{aligned}
O_S((1,5)) &= \{(1,5),(5,6),(6,2),(2,1)\} \\
O_S((2,2)) &= \{(2,2),(2,5),(5,5),(5,2)\} \\
O_S((2,3)) &= \{(2,3),(3,5),(5,4),(4,2)\} \\
O_S((2,4)) &= \{(2,4),(4,5),(5,3),(3,2)\} \\
O_S((3,3)) &= \{(3,3),(3,4),(4,4),(4,3)\}
\end{aligned}
$$

An S–fundamental set consists of, for example,

$$\mathcal{F}_S = \{(0,0),(0,1),(0,2),(0,3),(1,1),(1,2),(1,3),(1,4),(1,5),(2,2),(2,3),(2,4),(3,3)\}.$$

Let us reorder $\mathcal{F}_S$ through a generator for the cyclic group of Z_7. For this case, take $g = 5$ (i.e., set $M = 5I$). Note that, for instance, $5(0,1) = (0,5) \in O_S((0,2))$, $5(0,5) = (0,4) \in O_S((0,3))$, and $5(0,4) = (0,6) \in O_S((0,1))$. Hence, $O_S((0,1)) \approx_{MS} O_S((0,2)) \approx_{MS} O_S((0,3))$. And so on, for the the remaining S–orbits. The following is the list of MS–orbits:

$$
\begin{aligned}
O_{MS_0}((0,0)) &= \{(0,0)\}, \\
O_{MS_1}((0,1)) &= \{(0,1),(0,2),(0,3)\}, \\
O_{MS_2}((1,1)) &= \{(1,1),(2,2),(3,3)\}, \\
O_{MS_3}((1,2)) &= \{(1,2),(2,4),(1,3)\}, \\
O_{MS_4}((1,4)) &= \{(1,4),(1,5),(2,3)\}.
\end{aligned}
$$

The computation of $\hat{f}$ reduces to computing

$$
\begin{pmatrix}
1 & e^t & e^t & e^t & e^t \\
e & W_{11} & W_{12} & W_{13} & W_{14} \\
e & W_{21} & W_{22} & W_{23} & W_{24} \\
e & W_{31} & W_{32} & W_{33} & W_{34} \\
e & W_{41} & W_{42} & W_{43} & W_{44}
\end{pmatrix}
\begin{pmatrix}
f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4
\end{pmatrix}
$$

where each W_{ij} is a 3×3 Hankel circulant matrix, each e denotes a column vector of ones of size 3, and each f_i is determined by MS–orbit O_{MS_i}. For instance,

$f_0 = (\, f((0,0))\,)$, $f_1 = \begin{pmatrix} f((0,1)) \\ f((0,2)) \\ f((0,3)) \end{pmatrix}$ *and similarly for* f_2, f_3, *and* f_4. *Thus, by using the generator method, the computation of* $\hat{f}$ *can be done by means of 16 cyclic convolutions.*

However, the number of MS*–orbits can be reduced even further if instead of reordering the fundamental set* $\mathcal{F}_S$ *under the action of a generator* g *of* Z_7, *we reorder under the action of a nonsingular* 2×2 *matrix over* Z_7. *For instance, if* $\mathcal{F}_S$ *is reorder by* $M = \begin{pmatrix} 1 & 2 \\ 5 & 1 \end{pmatrix}$, *we observe that*

$$\begin{aligned} M \begin{pmatrix} 0 \\ 1 \end{pmatrix} &= \begin{pmatrix} 2 \\ 1 \end{pmatrix} \in O_S((1,5)), \\ M^2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} &= \begin{pmatrix} 4 \\ 4 \end{pmatrix} \in O_S((3,3)), \\ &\vdots \\ M^{11} \begin{pmatrix} 0 \\ 1 \end{pmatrix} &= \begin{pmatrix} 4 \\ 1 \end{pmatrix} \in O_S((1,3)), \\ M^{12} \begin{pmatrix} 0 \\ 1 \end{pmatrix} &= \begin{pmatrix} 6 \\ 0 \end{pmatrix} \in O_S((0,1)). \end{aligned}$$

Hence, through this M, *we obtain only one nontrivial* MS*–orbit of length* 12*:*

$$O_{MS}((0,1)) = \{(0,1),(1,5),(3,3),(2,4),(0,3),(1,4),(2,2),(1,2),(0,2),(2,3),(1,1),(1,3)\}.$$

Therefore, $\hat{f}$ *can be computed by only one cyclic convolution of size* 12.

Given nonsingular commuting matrices S and M, we say that M induces the MS–orbit structure $(\eta_1[i_1], \eta_2[i_2], \ldots, \eta_r[i_r])$ if in addition to the trivial orbit $O_{MS}(\mathbf{0})$ of length one, M induces η_j MS–orbits of length $\imath_j$, $j = 1, 2, \ldots, r$. In such a case, the DFT can be computed in terms of η_j^2 cyclic convolutions of length i_j, $j = 1, 2, \ldots, r$.

For instance, in Example (3.2.2), the generator method and M–method induce the MS–orbit structures (4[3]) and (1[12]), respectively. The goal is, given nonsingular

matrix S, find a nonsingular matrix M with $MS = SM$ that minimizes

$$\eta_{\phi_S} = \eta_1 + \eta_2 + \cdots + \eta_r.$$

To date, the only known method for choosing such a matrix M is by exhaustion (i.e., a brute–force search of all possible matrices M that commute with S that minimize the number of cyclic convolutions without taking into account any algebraic property of S). However, this is very costly. For instance, the time for computing M by exhaustion is $O(p^6)$ in the two dimensional case and is $O(p^{12})$ in the three dimensional case. In this work we study methods for computing M directly.

3.3 Some discrete models of genetic networks

Identification of a gene regulatory network from experimental data (e.g., gathered by microarray technologies) is a very important area of current research due to its potential applications to biological and biomedical sciences; for instance, in drug design and cancer research, among others.

This problem is receiving a considerable amount of attention and many researchers from different disciplines have approached this problem in many different ways ranging from continuous models like differential equation models [7] to discrete models like Boolean networks models [2, 22], probabilistic Boolean networks models [40], multivariable polynomials over finite field models [16, 23], and single–variable polynomial models over finite fields [27].

In general, a genetic network is represented by a directed graph $G(V, f)$, where $V = \{a_1, a_2, \ldots, a_n\}$ is a set of n genes and $f = \{f_1, f_2, \ldots, f_n\}$ represents the relationship among the n genes.

Section 3.3.1 presents a formalization of the Boolean model proposed by Ideker *et al* [22]. Section 3.3.2 presents two finite field polynomial generalizations of the Boolean model. On the one hand, the multivariable polynomial proposed by Laubenbacher *et al* [23], and, on the other hand, the one that concerns this work, the single–variable polynomial, proposed by Moreno *et al* [27].

3.3.1 Boolean models

In [22], Ideker and Karp describe a genetic network model based on Boolean networks, the deterministic Boolean network model or dBnm. In their model, gene level

expression can be either 1 (On) or 0 (Off). Despite the simplicity of this model, it gives important information about the rough logic (gene x either activates or inhibits gene y) governing the regulatory network.

In any genetic network $G(V, f)$ each gene a_i has an expression level w_i which is a function of the expression levels of a subset of genes in V. If the expression level w_i of each gene a_i is regarded as *high* or *low*, then w_i is a binary function of the expression levels (1/0) of a subset of V. In this case, the genetic network is called a deterministic Boolean network or dBn.

Example 3.3.1 (Ideker [22]) *Consider the following network of four genes* a_0, a_1, a_2, *and* a_3 *where* $f_0(x_0, x_1, x_2, x_3) = 1$, $f_1(x_0, x_1, x_2, x_3) = 1$, $f_2(x_0, x_1, x_2, x_3) = x_0 \cap x_1$, *and* $f_3(x_0, x_1, x_2, x_3) = x_1 \cap \tilde{x}_2$.

In this example, expression level of gene a_0 *and* a_1 *do not depend on any other gene. Gene* a_2 *expresses if gene* a_0 *is expressed and gene* a_1 *is not expressed. Gene* a_3 *expresses if* a_1 *is expressed and gene* a_2 *is not expressed.*

3.3.2 Polynomial models over finite fields

In the Boolean model, either a gene can affect another gene or not. An alternative model that has been studied by several researchers [16], [23], [24], [27] is the finite field genetic network. In this model, one is able to capture graded differences in gene expression. Another advantage of the finite field model approach is that it can be considered as a generalization of the Boolean model since each Boolean operation can be expressed in terms of the sum and product in Z_2. In particular,

$$x \cap y = x \cdot y \tag{3.11}$$
$$x \cup y = x + y + x \cdot y \tag{3.12}$$
$$\tilde{x} = x + 1 \tag{3.13}$$

It is natural to generalize the Boolean model as follows.

Definition 3.3.1 *A finite field genetic network over* $GF(q)$ *consists of a directed graph* G *having* n *numbered nodes such that for each node* i *there is an associated*

function

$$f_i : GF(q)^n \to GF(q).$$

We denote such a network by

$$(G, \{f_0, f_1, \ldots, f_{n-1}\}, GF(q)).$$

Each such f_i can be expressed as a polynomial in n variables. For this reason, we refer to a network of the type defined above as a multivariable finite field genetic network ("MFFGN").

Clearly, every BGN is also a MFFGN over $GF(2)$. Each of the f_i can be expressed as a polynomila over $GF(2)$ by replacing each Boolean operation by one of the expressions given in equations (3.11)– (3.13).

Example 3.3.2 *The BGN of Example 1 can be expressed as a MFFGN over $GF(2)$ where the functions f_i are given by*

$$\begin{aligned} f_0(x_0, x_1, x_2, x_3) &= 1, \\ f_1(x_0, x_1, x_2, x_3) &= 1, \\ f_2(x_0, x_1, x_2, x_3) &= x_0 \cdot x_1, \\ f_3(x_0, x_1, x_2, x_3) &= x_1 \cdot (x_2 + 1). \end{aligned}$$

Multivariable polynomial interpolation over $GF(q)^d$

Let $f : GF(q)^d \longrightarrow GF(q)^d$. For each $i = 1, 2, \ldots, d$, define

$$f_i : GF(q)^d \longrightarrow GF(q)^d$$

to be the function such that for any x in $GF(q)^d$, $f_i(x) = x_i$, where $f(x) = (x_1, x_2, \ldots, x_d)$. We write $f = (f_1, f_2, \ldots, f_d)$.

Given a function $f : GF(q)^d \longrightarrow GF(q)^d$ and $n+1$ values a_k, $k = 0, 1, \ldots, n$, in $GF(q)^d$, there exist polynomials P_i, $i = 1, 2, \ldots, d$ of degree at most n such that

$$P_i(a_k) = f_i(a_k)$$

for all $i = 1, 2, \ldots, d$ and for all $k = 0, 1, \ldots, n$. Such $P_i(x)$ can be defined by

$$P_i(x) = \sum_{k=0}^{n} f_i(a_k) \prod_{j=0,\, j\neq k}^{n} \frac{(x_{l_{jk}} - a_{jl_{jk}})}{(a_{kl_{jk}} - a_{jl_{jk}})}, \tag{3.14}$$

where each l_{jk} is the index (numbered $1, 2 \ldots, d$) of the first coordinate where a_k and a_i differ.

Example 3.3.3 *Let $d = 3$, $n = 2$, and $q = 3$. Also, let $a_0 = (0, 1, 0)$, $a_1 = (0, 2, 1)$, $a_2 = (0, 2, 2)$, and suppose that*

$$f(0, 1, 0) = (0, 2, 1)$$
$$f(0, 2, 1) = (0, 2, 2)$$
$$f(0, 2, 2) = (2, 0, 0)$$

Then,

$$\begin{aligned} P_i(x) = \quad & f_i(a_0)\frac{(x_{l_{10}} - a_{1l_{10}})}{(a_{0l_{10}} - a_{1l_{10}})}\frac{(x_{l_{20}} - a_{2l_{20}})}{(a_{0l_{20}} - a_{2l_{20}})}\frac{(x_{l_{30}} - a_{3l_{30}})}{(a_{0l_{30}} - a_{2l_{30}})} \\ + \quad & f_i(a_1)\frac{(x_{l_{01}} - a_{0l_{01}})}{(a_{1l_{01}} - a_{0l_{01}})}\frac{(x_{l_{21}} - a_{2l_{21}})}{(a_{1l_{21}} - a_{2l_{21}})}\frac{(x_{l_{31}} - a_{3l_{31}})}{(a_{1l_{31}} - a_{3l_{31}})} \\ + \quad & f_i(a_2)\frac{(x_{l_{02}} - a_{0l_{02}})}{(a_{2l_{02}} - a_{0l_{02}})}\frac{(x_{l_{12}} - a_{1l_{12}})}{(a_{2l_{12}} - a_{1l_{12}})}\frac{(x_{l_{32}} - a_{3l_{31}})}{(a_{2l_{32}} - a_{3l_{32}})} \end{aligned}$$

Thus,

$$\begin{aligned} P_i(x) = \quad & f_i(a_0)\frac{x_2 - 2}{1 - 2}\frac{x_2 - 2}{1 - 2}\frac{x_1 - 2}{0 - 2} \\ + \quad & f_i(a_1)\frac{x_2 - 1}{2 - 1}\frac{x_3 - 2}{1 - 2}\frac{x_1 - 2}{0 - 2} \\ + \quad & f_i(a_2)\frac{x_2 - 1}{2 - 1}\frac{x_3 - 1}{2 - 1}\frac{x_1 - 2}{0 - 2} \end{aligned}$$

Hence,

$$\begin{aligned} P_i(x) \quad = \quad & f_i(a_0)(x_2 - 2)^2(x_1 - 2) + 2f_i(a_1)(x_2 - 1)(x_3 - 2)(x_1 - 2) \\ & + f_i(a_2)(x_2 - 1)(x_3 - 1)(x_1 - 2). \end{aligned}$$

Therefore,

$$\begin{aligned}
P_1(x) &= 0 + 0 + 2(x_2 - 1)(x_3 - 1)(x_1 - 2) \\
&= -x_1x_2x_3 + 2x_2x_3 + x_1x_3 - 2x_3 + x_1x_2 - 2x_2 - x_1 + 2 \\
P_2(x) &= 2(x_2 - 2)^2(x_1 - 2) + (x_2 - 1)(x_3 - 2)(x_1 - 2) \\
&= 2x_1x_2^2 + 2x_1x_2 + x_1 + x_1x_2x_3 + 2x_1x_3 + 2x_2^2 + 2x_2 + x_2x_3 + 2x_3 + 1 \\
P_3(x) &= (x_2 - 2)^2(x_1 - 2) + (x_2 - 1)(x_3 - 2)(x_1 - 2) + 0 \\
&= x_1x_2^2 + x_1 + x_1x_2x_3 + 2x_1x_3 + 2x_1 + x_2^2 + x_2x_3 + 2x_3
\end{aligned}$$

The polynomial produced by formula (3.14) is not unique. For instance, one could define l_{jk} to be the index of the highest numbered coordinate in which a_k and a_j differ. For example, in the previous example we would have $l_{10} = l_{20} = l_{21} = l_{31} = l_{32} = 3$, $l_{30} = 2$, and so

$$\begin{aligned}
P_i(x) = \quad & f_i(a_0)\frac{x_3 - 1}{0 - 1}\frac{x_3 - 2}{0 - 2}\frac{x_2 - 0}{1 - 0} \\
+ \quad & f_i(a_1)\frac{x_3 - 0}{1 - 0}\frac{x_3 - 2}{1 - 2}\frac{x_3 - 0}{1 - 0} \\
+ \quad & f_i(a_2)\frac{x_3 - 0}{2 - 0}\frac{x_3 - 1}{2 - 1}\frac{x_3 - 0}{2 - 0}
\end{aligned}$$

Thus,

$$P_i(x) = 2f_i(a_0)(x_3 - 1)(x_3 - 2)x_2 + 2f_i(a_1)x_3^2(x_3 - 2) + f_i(a_2)x_3^2(x_3 - 1).$$

Hence, another triple of polynomials having the desired property (i.e., $P_i(a_k) = f_i(a_k)$) is given by

$$\begin{aligned}
P_1(x) &= 0 + 0 + 2x_3(x_3 - 1) \\
&= 2x_3^3 + x_3^2 \\
&= 2x_3 + x_3^2 \\
P_2(x) &= (x_3 - 1)(x_3 - 2)x_2 + x_3^2(x_3 - 2) + 0 \\
&= x_3^2x_2 + 2x_2 + x_3^3 + x_3^2 \\
&= x_3^2x_2 + 2x_2 + x_3 + x_3^2 \\
P_3(x) &= 2(x_3 - 1)(x_3 - 2)x_2 + x_3^2(x_3 - 2) + 0 \\
&= 2x_2x_3^2 + x_2 + x_3^3 + x_3^2 \\
&= 2x_2x_3^2 + x_2 + x_3 + x_3^2
\end{aligned}$$

Single–variable finite field model

Another approach taken by Moreno *et al* [27] is to replace the n functions f_i defined on $GF(q)$ by a single function f that maps $GF(q^n)$ to $GF(q^n)$. We justify this idea in what follows.

Let α be a root of an irreducible polynomial over $GF(q)$. We define

$$\phi : GF(q^n) \to GF(q^n)$$

by

$$\phi(a_{n-1}, \ldots, a_1, a_0) = a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0,\ a_i \in GF(q).$$

Now, every MFFGN $(G, \{f_0, f_1, \cdots, f_{n-1}\}, GF(q))$ defines a function

$$f : (GF(q))^n \to (GF(q))^n$$

where

$$f(a_{n-1}, \ldots, a_1, a_0) = (f_0(a_{n-1}, \ldots, a_1, a_0), \ldots, f_{n-1}(a_{n-1}, \ldots, a_1, a_0)).$$

We define $\phi_f : GF(q^n) \to GF(q^n)$ by

$$\phi_f(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) = \phi(f_0(a_{n-1}, \ldots, a_0), \ldots, f_{n-1}(a_{n-1}, \ldots, a_0))$$

The function ϕ_f essentially does the work of the functions f_i. This motivates

Definition 3.3.2 *A univariable finite field genetic network ("UFFGN") over $GF(q)$ consists of a directed graph having n numbered nodes and a function $f : GF(q^n) \to GF(q^n)$. We denote such a network by $(G, f, GF(q))$.*

Moreno et al [27] propose solving the reverse engineering problem by regarding each tuple of the time series data as an element of a Galois field through a *lifting* method. This framework finds an interpolating single–variable polynomial over an appropriate finite field. This polynomial model can be expressed by the following equation.

$$f(x) = P(x) + g(x)\prod_{i=1}^{r}(x - s_i),$$

where $P(x)$ is a polynomial that interpolates the given r time points from the time seris data and $g(x)\prod_{i=1}^{r}(x - s_i)$ is a polynomial that vanishes at all interpolating points. That is, $g(x)\prod_{i=1}^{r}(x - s_i)$ belongs to the ideal generated by the linear functions $\{x - s_1, x - s_2, \ldots, x - s_r\}$.

Chapter 4

A Solution to reverse engineering MS–orbits

In this chapter we solve the problem of reverse engineering MS–orbits. In section 4.1 we give some preliminaries that are needed in the rest of the chapter. In section 4.2 we give some results that hold for arbitrary dimension n and, in particular, we characterize those symmetry matrices S for which there exists exactly one nontrivial MS–orbit. Then, in section 4.3 and 4.4 we give solutions to the MS–orbit problem for $n = 2$ and $n = 3$, respectively.

4.1 Preliminaries

Let us first briefly review some important terms introduced in Chapter 3. Any $n \times n$ nonsingular matrix S partitions Z_p^n into equivalence classes called S–orbits. A set of representatives of these classes is called a fundamental set $\mathcal{F}_S$. Any nonsingular matrix M over Z_p that commutes with S partitions $\mathcal{F}_S$ into equivalence classes called MS–orbits. The MS–orbit containing $\mathbf{x} \in \mathcal{F}_S$ is denoted by $O_{MS}(\mathbf{x})$ and the number of elements in $O_{MS}(\mathbf{x})$, denoted by $|O_{MS}(\mathbf{x})|$, is called its length. Our aim is as follows: Given S, determine an M that minimizes the number of MS–orbits. This motivates the following definitions.

Definition 4.1.1 *A* **reduced linear modular system** *(RLMS) is a finite dynamical system $R = (\mathcal{F}_S^n, M, Z_p)$ where $\mathcal{F}_S^n$ is a fundamental set of vectors in Z_p^n corresponding to an $n \times n$ nonsingular matrix S over Z_p and M is an $n \times n$ nonsingular*

matrix over Z_p that commutes with S.

Just as the state diagram of an LMS consist entirely of S–orbits, so does the state diagram of an RLMS consist entirely of MS–orbits. The *reverse engineering problem for RLMSs* is the problem of determining an M that commutes with S that minimizes the number of MS–orbits in $(\mathcal{F}_S^n, M, Z_p)$. A solution M to this problem is called *optimal.*

Lemma 4.1.1 *Let $S \in \mathcal{M}_n$ and $M \in \mathcal{N}(S)$ be nonsingular and let $\mathbf{x} \in \mathcal{F}_S$. Then, the MS–orbit length of $\mathbf{x}$, $|O_{MS}(\mathbf{x})|$, is the smallest positive integer i for which*

$$M^i\mathbf{x} = S^j\mathbf{x} \ (mod\ p) \text{ for some } j.$$

Proof
Note that the number of elements in $O_{MS}(\mathbf{x})$ is equal to, at most, the period of M, i.e., $O_{MS}(\mathbf{x})$ is finite. It is straightforward to see that there is a one–to–one correspondence between $O_{MS}(\mathbf{x})$ and the set $\{\mathbf{x}, M\mathbf{x}, M^2\mathbf{x}, \ldots, M^{i-1}\mathbf{x}\}$, where i is the smallest positive integer for which $M^i\mathbf{x} \in O_S(M^l\mathbf{x})$, for some integer $0 \leq l \leq i-1$. Now, it will be shown that $M^i\mathbf{x} \in O_S(\mathbf{x})$. Assume the contrary. Then, $M^i\mathbf{x} \in O_S(M^l\mathbf{x})$ for some $0 < l < i$. Thus, there is an integer t such that $M^i\mathbf{x} = S^tM^l\mathbf{x} = M^lS^t\mathbf{x}$. Which implies that $M^{i-l}\mathbf{x} = S^t\mathbf{x}$. Which implies that $M^{i-l}\mathbf{x} \in O_S(\mathbf{x})$. Which is a contradiction. Finally, since $M^i\mathbf{x} \in O_S(\mathbf{x})$, there exists an integer j such that $M^i\mathbf{x} = S^j\mathbf{x}$.$\diamondsuit$

Lemma 4.1.2 *If $A \in \mathcal{M}_n$ then $A\mathbf{x} = \mathbf{0}$ mod p for all $\mathbf{x} \in Z_p^n$ if and only if $A = 0$.*

Proof
$A\mathbf{x} = \mathbf{0}$ for all $\mathbf{x} \in Z_p^n$ if and only if $A\mathbf{e} = \mathbf{0}$ for each vector $\mathbf{e}$ in the standard basis for Z_p^n, i.e. if and only if $A = AI = 0$.$\diamondsuit$

Corollary 4.1.1

$$M^i\mathbf{x} = S^j\mathbf{x} \ (mod\ p) \text{ for all } \mathbf{x} \in Z_p^n \tag{4.1}$$

is equivalent to

$$M^i = S^j \ (mod\ p). \tag{4.2}$$

Given nonsingular commuting matrices S and M, for the purpose of computing the MS–orbit structure it is convenient to replace S and M by some equivalent similar commuting matrices S' and M', for S and M, respectively. Thus, equation (4.2) becomes $B^{-1}M'^{i}B = A^{-1}S'^{j}A$, for some nonsingular matrices A and B. If $A = B$, then (4.2) becomes

$$S'^{j} = M'^{i} \pmod{p} \tag{4.3}$$

which gives us all possible MS–orbit lengths.

The following lemma is a standard result in basic linear algebra (see, for instance, [28].)

Lemma 4.1.3 *Let $A \in \mathcal{M}_n$ with $\det(A) = 0$.*

1. *If A is nonzero, then the equation $A\mathbf{x} = \mathbf{0}$ has a nontrivial solution.*

2. *If A^r is nonzero with $r > 1$, then there is $\mathbf{x} \neq \mathbf{0}$ which is a solution of $A^r\mathbf{x} = \mathbf{0}$ but $A\mathbf{x} \neq \mathbf{0}$.*

The proof of the following is immediate.

Lemma 4.1.4 *Let $S \in \mathcal{M}_n$ and $M \in \mathcal{N}(S)$. Then, $Mq(S) = q(S)M$ for any polynomial $q(x)$.*

Notation: Let $S \in \mathcal{M}_n$ be nonsingular with characteristic polynomial

$$\phi_S(x) = P_1(x)P_2(x),$$

where P_1 and P_2 are relatively prime polynomials. Then,

$$Z_p^n = V_{P_1} \oplus V_{P_2},$$

where

$$V_{P_t} = \{\mathbf{x} \in Z_p^n | P_t(S)\mathbf{x} = \mathbf{0}\}.$$

Let

$$V_{P_1,P_2} = V_{P_1P_2} - V_{P_1} \cup V_{P_2}.$$

Each V_{P_t} as well as V_{P_1,P_2} is invariant under any matrix M that commutes with S.

Let $\mathcal{O}_{P_t}$ and $\mathcal{O}_{P_1,P_2}$ be the set of MS–orbits contained in V_{P_t} and V_{P_1,P_2}, respectively. Also, let $\mathcal{O}_{m_S}$ be the set of all MS–orbits in Z_p^n.

In the case that $P(x)^r$, $r > 1$, is a factor of $m_S(x)$, define

$$V_{P^{t_2},P^{t_1}} = V_{P^{t_2}} - V_{P^{t_1}}, \text{ for } t_1 < t_2 \leq r,$$

and $\mathcal{O}_{P^{t_2},P^{t_1}}$ be the set of MS–orbits in $V_{P^{t_2},P^{t_1}}$. This notation might create some ambiguity with V_{P_1,P_2}. However, it will be clear from the context which one we are refering to.

Let $S \in \mathcal{M}_n$ be nonsingular.

Properties of $\mathcal{O}_{\phi_S}$

1. If $\phi_S(x) = (-1)^n P(x)$ is irreducible and $M \in \mathcal{N}(S)$ is nonsingular, then all MS–orbits in $\mathcal{O}_P$ are of the same length say i_P. Denote the MS–orbit structure of $\mathcal{O}_P$ by
$$1 + \eta_P[i_P],$$
where 1 stands for the trivial MS–orbit and η_P is the number of the MS–orbits in $\mathcal{O}_P$.

2. If $\phi_S(x) = (-1)^n P^r(x)$, $r > 1$, then for any nonsingular $M \in \mathcal{N}(S)$, there are at least r MS–orbits not necessarily the same length and the MS–orbit structure in $\mathcal{O}_{P^r}$ is
$$1 + \sum \mathcal{O}_{P,P^0} + \sum \mathcal{O}_{P^2,P} + \cdots + \sum \mathcal{O}_{P^r,P^{r-1}}$$

3. If $\phi_S(x) = (-1)^n P_1(x)P_2(x)$, where P_1 and P_2 are relatively prime polynomials, then, the MS–orbit structure in $\mathcal{O}_{\phi_S}$ is
$$\sum \mathcal{O}_{P_1} + \sum \mathcal{O}_{\phi_S/P_1} + \sum \mathcal{O}_{P_1,\phi_S/P_2}.$$

Proof

Part 1 : Let $S \in \mathcal{M}_n$ with $\phi_S(x) = (-1)^n P(x)$ irreducible. Then, by Corollary 2.2.5, $\mathcal{N}(S)$ is a finite division ring with $p^n - 1$ elements. Let $M, N \in \mathcal{N}(S)$, where M is nonsingular and N is maximal.

Let $\mathbf{x}, \mathbf{y}$ be any two distinct nonzero vectors from Z_p^n. We will show that

$$|O_{MS}(\mathbf{x})| = |O_{MS}(\mathbf{y})|.$$

Let $i_{\mathbf{x}} = |O_{MS}(\mathbf{x})|$ and $i_{\mathbf{y}} = |O_{MS}(\mathbf{y})|$. By Lemma 4.1.1 $i_{\mathbf{x}}$ and $i_{\mathbf{y}}$ are the smallest positive integers such that

$$\begin{aligned} S^{j_{\mathbf{x}}}\mathbf{x} &= M^{i_{\mathbf{x}}}\mathbf{x} \bmod p \\ S^{j_{\mathbf{y}}}\mathbf{y} &= M^{i_{\mathbf{y}}}\mathbf{y} \bmod p \end{aligned}$$

for some integers $j_{\mathbf{x}}$ and $j_{\mathbf{y}}$, if and only if

$$\begin{aligned}(S^{j_{\mathbf{x}}} - M^{i_{\mathbf{x}}})\mathbf{x} &= \mathbf{0} \bmod p \\ (S^{j_{\mathbf{y}}} - M^{i_{\mathbf{y}}})\mathbf{y} &= \mathbf{0} \bmod p\end{aligned}$$

Now, since $\mathcal{N}(S)$ is a field, $\det(S^{j_{\mathbf{x}}} - M^{i_{\mathbf{x}}}) \neq 0$ or $S^{j_{\mathbf{x}}} - M^{i_{\mathbf{x}}} = \mathbf{0}$, the zero $n \times n$ matrix. If $\det(S^{j_{\mathbf{x}}} - M^{i_{\mathbf{x}}}) \neq 0$, then $S^{j_{\mathbf{x}}} - M^{i_{\mathbf{x}}} = 0$ is invertible, which implies that $\mathbf{x} = \mathbf{0}$; a contradiction. The only possibility left is that $S^{j_{\mathbf{x}}} - M^{i_{\mathbf{x}}} = \mathbf{0}$, which implies that

$$S^{j_{\mathbf{x}}} = M^{i_{\mathbf{x}}} \bmod p^n \tag{4.4}$$

$$S^{j_{\mathbf{y}}} = M^{i_{\mathbf{y}}} \bmod p^n. \tag{4.5}$$

Let t_1 and t_2 be the indexes of S and M with respect to N, respectively. Then, equations (4.4) and (4.5) become

$$t_1 j_{\mathbf{x}} = t_2 i_{\mathbf{x}} \bmod p^n - 1 \tag{4.6}$$

$$t_1 j_{\mathbf{y}} = t_2 i_{\mathbf{y}} \bmod p^n - 1. \tag{4.7}$$

Hence, both $(j_{\mathbf{x}}, i_{\mathbf{x}})$ and $(j_{\mathbf{y}}, i_{\mathbf{y}})$ are solutions of

$$t_1 j = t_2 i \bmod p^n - 1.$$

Now, by Theorem 2.3.16, the smallest positive integer i_P that solves $t_1 j = t_2 i \bmod p^n - 1$ for some integer j_P is

$$i_P = \frac{k_q}{\gcd(k_P, k_q)},$$

where $q(x)$ is the minimal polynomial of M, k_P and k_q are the orders of P and q, respectively. Thus, $i_{\mathbf{x}} = i_{\mathbf{y}} = i_P$.

By Theorem 3.1.1, the number of nontrivial S–orbits in V_P is μ_P.

Hence, the number of MS–orbits in $\mathcal{O}_P$ is

$$\eta_P = \frac{\mu_P}{i_P}.$$

Therefore the MS–orbit structure is

$$1 + \eta_P[i_P].\diamondsuit$$

Part 2 : Let $\phi_S = (-1)^n P^r(x)$, $r > 1$. The sets $V_{P^0}, V_P, V_{P^2}, \ldots, V_{P^r}$ form a nested sequence of subspaces of V_{P^r}. That is,

$$V_{P^0} \subset V_P \subset V_{P^2} \subset \cdots \subset V_{P^r}.$$

Observe that

$$V_{P^0}, V_{P,P^0}, V_{P^2,P}, \ldots, V_{P^r,P^{r-1}}$$

is a pairwise disjoint family of vectors such that

$$V_{P^r} = V_{P^0} \cup V_{P,P^0} \cup V_{P^2,P} \cup \cdots \cup V_{P^r,P^{r-1}}.$$

Let $M \in \mathcal{N}(S)$ be nonsingular. Then, each $V_{P^t,P^{t-1}}$ is non empty and invariant under M since, if $\mathbf{x} \in V_{P^t,P^{t-1}}$, $P(S)^t(M\mathbf{x}) = MP(S)^t\mathbf{x} = \mathbf{0}$ and $P(S)^{t-1}(M\mathbf{x}) = MP(S)^{t-1}\mathbf{x} \neq \mathbf{0}$. Therefore,

$$\mathcal{O}_{P^r} = \mathcal{O}_{P^0} \cup \mathcal{O}_{P,P^0} \cup \mathcal{O}_{P^2,P} \cup \cdots \cup \mathcal{O}_{P^r,P^{r-1}}$$

and

$$\sum \mathcal{O}_{P^r} = 1 + \sum \mathcal{O}_{P,P^0} + \sum \mathcal{O}_{P^2,P} + \cdots + \sum \mathcal{O}_{P^r,P^{r-1}}.\diamondsuit$$

Part 3 : Let $\phi_S(x) = (-1)^n P_1(x)P_2(x)$, where P_1 and P_2 are relatively prime polynomials. Then,

$$\begin{aligned} V_{\phi_S} &= V_{P_1} \oplus V_{\phi_S/P_1} \\ &= V_{P_1} \cup V_{\phi_S/P_1} \cup V_{P_1,\phi_S/P_1} \end{aligned}$$

Let $M \in \mathcal{N}(S)$ be nonsingular. It is straigthforward to see that each V_{P_1}, V_{ϕ_S/P_1}, as well as $V_{P_1,\phi_S/P_1}$ are all M invariant sets. Then

$$\mathcal{O}_{\phi_S} = \mathcal{O}_{P_1} \cup \mathcal{O}_{\phi_S/P_1} \cup \mathcal{O}_{P_1,\phi_S/P_1}.$$

Therefore,

$$\sum \mathcal{O}_{\phi_S} = \sum \mathcal{O}_{P_1} + \sum \mathcal{O}_{\phi_S/P_1} + \sum \mathcal{O}_{P_1,\phi_S/P_1}.\diamondsuit$$

Theorem 4.1.1 *(Primary Decomposition Theorem) Let $S \in \mathcal{M}_n$ be nonsingular with minimal polynomial $m_S(x) = P_1(x)P_2(x)$, where P_1 and P_2 have positive degree and* $\gcd(P_1(x), P_2(x)) = 1$. *Then,*

$$Z_p^n = V_{P_1} \bigoplus V_{P_2},$$

where $V_{P_i} = \{\mathbf{x} \in Z_p^n : P_i(S)\mathbf{x} = \mathbf{0}\}$ for $i = 1, 2$.

For a proof of this theorem, see for example, [14].

Let us make the following five important remarks about Theorem 4.1.1 that will be used later on.

1. Each V_{P_i} is S–invariant since if $\mathbf{x} \in V_{P_i}$, then

$$\begin{aligned} P_i(S)^{m_i}(S\mathbf{x}) &= SP_i(S)^{m_i}\mathbf{x} \\ &= S\mathbf{0} \\ &= \mathbf{0}. \end{aligned}$$

   Thus, $S\mathbf{x} \in V_{P_i}$. Which means that if $\mathbf{x} \in V_{P_i}$, then $O_S(\mathbf{x}) \subseteq V_{P_i}$.

2. Since $P_i(S)^{m_i}\mathbf{x} = \mathbf{0}$ has a nontrivial solution, then V_{P_i} contains at least two distinct vectors.

3. Since $\gcd(P_1(x), P_2(x)) = 1$, there exist polynomials $Q_1(x)$ and $Q_2(x)$ for which $P_1(x)Q_1(x) + P_2(x)Q_2(x) = 1$. Then, $P_1(S)Q_1(S) + P_2(S)Q_2(S) = I_n$. Let $\mathbf{x} \in V_{P_i} \cap V_{P_2}$. Thus, $P_1(S)\mathbf{x} = \mathbf{0}$ and $P_2(S)\mathbf{x} = \mathbf{0}$. But

$$\begin{aligned} \mathbf{x} &= I_n\mathbf{x} \\ &= (P_1(S)Q_1(S) + P_2(S)Q_2(S))\mathbf{x} \\ &= P_1(S)Q_1(S)\mathbf{x} + P_2(S)Q_2(S)\mathbf{x} \\ &= Q_1(S)\mathbf{0} + Q_2(S)\mathbf{0} \\ &= \mathbf{0}. \end{aligned}$$

   Therefore $V_{P_i} \cap V_{P_j}$ consists only of the zero vector.

4. Let $M \in \mathcal{N}(S)$ and let $\mathbf{0} \neq \mathbf{x} \in V_{P_i}$. Then, $P_i(S)(M\mathbf{x}) = MP_i(S)\mathbf{x} = M\mathbf{0} = \mathbf{0}$. Thus, $M\mathbf{x} \in V_{P_i}$. Therefore, $\mathcal{O}_P \subseteq V_{P_i}$.

5. Let $\mathbf{z} \in V_{P_1,P_2}$. It is easy to see that $S\mathbf{z} \in V_{P_1,P_2}$. Which implies that $O_S(\mathbf{z}) \subseteq V_{P_1,P_2}$ and, if $M \in \mathcal{N}(S)$, then $O_{MS}(\mathbf{z}) \subseteq V_{P_1,P_2}$. Hence, $\mathcal{O}_{P_1,P_2} \subseteq V_{P_1,P_2}$.

We have just shown the following

Lemma 4.1.5 *Let $S \in \mathcal{M}_n$ be nonsingular with $m_S(x) = P_1(x)P_2(x)$, where $P_1(x)$ and $P_2(x)$ have positive degree and $\gcd(P_1(x), P_2(x)) = 1$. Then, for any nonsingular $M \in \mathcal{N}(S)$ the number of nontrivial MS–orbits, η_{m_S}, is not less than 3.*

Lemma 4.1.6 *Let $S \in \mathcal{M}_n$ be nonsingular with $m_S(x) = P^r(x)$, where $P(x)$ is irreducible and $r \geq 2$. Also, let $M \in \mathcal{N}(S)$ be nonsingular. Then, the number of nontrivial MS–orbits, η_{m_S}, is not less than 2.*

Proof
The idea of the proof is as follows. First, construct two disjoint nonempty subsets V_P and V_{P^2} of vectors from Z_p^n. Each such subset contains at least one nontrivial vector. Next, those subsets will be shown to be invariants under S and M. Which implies that there are at least two nontrivial MS–orbits.

Let us define

$$\begin{aligned} V_P &= \{\mathbf{x} \in Z_p^n : p(S)\mathbf{x} = \mathbf{0}\}, \\ V_{P^2} &= \{\mathbf{x} \in Z_p^n : p(S)^2\mathbf{x} = \mathbf{0}\}, \text{ and} \\ V_{P^2,P} &= V_{P^2} - V_P. \end{aligned}$$

Let $M \in \mathcal{N}(S)$ be nonsingular. Note that

i. $V_P \cap V_{P^2,P} = \emptyset$, and that, by Lemma 4.1.3, both, V_P and $V_{P^2,P}$ contain nontrivial vectors;

ii. V_P an $V_{P^2,P}$ are S– and M– invariant sets.
Let $\mathbf{0} \neq \mathbf{x_1} \in V_P$, and $\mathbf{x_2} \in V_{P^2,P}$. Thus,

$$\begin{aligned} P(S)(S\mathbf{x_1}) &= S(P(S)\mathbf{x_1}) \\ &= S(\mathbf{0}) \\ &= \mathbf{0}. \end{aligned}$$

Hence, $S\mathbf{x_1} \in V_P$ and so, $O_S(\mathbf{x_1}) \subseteq V_P$. Similarly, $M\mathbf{x_1} \in V_P$. Hence, $O_{MS}(\mathbf{x_1}) \subseteq V_P$.
On the other hand,

$$\begin{aligned} P(S)^2(S\mathbf{x_2}) &= S(P(S)^2\mathbf{x_2}) \\ &= S(\mathbf{0}) \\ &= \mathbf{0}, \end{aligned}$$

and

$$\begin{aligned} P(S)(S\mathbf{x_2}) &= S(P(S)\mathbf{x_2}) \\ &\neq \mathbf{0} \end{aligned}$$

since $\mathbf{x_2} \in V_{P^2,P}$ and S is nonsingular. Thus, $S\mathbf{x_2} \in V_{P^2,P}$. Which means that $O_S(\mathbf{x_2}) \subseteq V_{P^2,P}$. The same argument also shows that $O_{MS}(\mathbf{x_2}) \subseteq V_{P^2,P}$.

We have found two distinct nontrivial MS–orbits and the proof is done.$\diamondsuit$

4.2 General cases

4.2.1 An exhaustive algorithm for finding optimal matrices

Given that there is a finite number of $n \times n$ matrices over Z_p, one way to find an optimal M for a given S is by determining all M over Z_p that commutes with S and determining which of these gives the minimal number of MS–orbits. This is summarized in Algorithm 4.2.1.

Algorithm 4.2.1

Inputs: *prime p and nonsingular $n \times n$ matrix S over Z_p.*

Output: *pair $(M,\ \eta_{m_S})$, where M is a $n \times n$ nonsingular matrix over Z_p that commutes with S and minimizes η_{m_S}, the number of nonzero MS–orbits.*

0. initialize η_{m_S} to p^n //Just a large number

1. compute the S–orbit structure.

2. compute a fundamental set of S.

3. **for** (*each matrix M' over Z_p*) **do**

3.1 **if**($\det(M') > 0$ *and* $M'S = SM'$)

3.1.2 *compute the $M'S$–orbit structure and η'_{m_S}.*

3.1.3 **if**($\eta'_{m_S} < \eta_{m_S}$)

3.1.4 $(M,\ \eta_{m_S}) \leftarrow (M',\ \eta'_{m_S})$

return $(M,\ \eta_{m_S})$

The complexity of Algorithm 4.2.1 is as follows. The cost of step 1 is $O(p^n)$ time, since there are $p^n - 1$ products of S and vectors in Z_p^n. Step 2 also costs $O(p^n)$ time, since a fundamental set of S–orbits is constructed by sequentially searching an n–dimensional table whose edge–length is $p-1$. Now, step 3.1.2 costs $O(p^n)$ time, since in the worst case, a fundamental set of S contains $p^n - 1$ elements. Steps 0, 3.1, 3.1.3, and 3.1.4 cost constant time. Thus, the cost of steps 3.1, 3.1.2, 3.1.3, and 3.1.4 is $O(p^n)$ time. Therefore, entire step 3 costs $O(p^{n^2} * p^n) = O(p^{n^2+n})$ time, since there are p^{n^2} $n \times n$ matrices over Z_p. In particular, for the two– and three–dimensional cases the complexity is $O(p^6)$ or $O(p^{12})$ time in the worst case, respectively. We will show that these complexities can be reduced to $O(p^2 \log p)$ and $O(p^3 \log p)$, respectively.

4.2.2 M–minimal cases

The ideal symmetry is one for which the DFT can be computed via just one cyclic convolution. We call an $n \times n$ matrix S over Z_p *M–minimal* if there exists an $n \times n$ matrix M over Z_p for which there is exactly one nontrivial MS–orbit. M–minimal matrices are characterized by the following

Theorem 4.2.1 *Let $S \in \mathcal{M}_n$ be nonsingular. Then, S is M–minimal if and only if the minimal polynomial of S is irreducible over Z_p.*

Proof
First, we will prove the *if* part. Let us assume that S is M–minimal and let $M \in \mathcal{N}(S)$ be nonsingular such that $\eta_{m_S} = 1$. Assume that $m_S(x) = P_1(x)P_2(x)$, where $\gcd(P_1(x), P_2(x)) = 1$. Then, by Lemma 4.1.5, $\eta_{m_S} \geq 3$, which cannot occur. Hence, $m_S(x)$ cannot contain more than one irreducible factor. So, $m_S(x) = P^r(x)$ for some irreducible polynomial $P(x)$ and some positive integer r. However, if $r > 1$, then, by Lemma 4.1.6, $\eta_{m_S} \geq 2$, which is not the case. Therefore, the only possibility left is $r = 1$, and, henceforth, $m_S(x) = P(x)$.

The converse will be shown by construction. Assume $m_S(x) = q(x)$ is irreducible of degree t over Z_p and let C_q be its companion matrix. Then, by Corollary 2.2.3,

$$A^{-1}SA = S' = \begin{pmatrix} C_q & & \\ & \ddots & \\ & & C_q \end{pmatrix}$$

for some nonsingular matrix A. Now, since $q(x)$ is irreducible, the set

$$\mathcal{N}(C_q) = \{c_{t-1}C_q^{t-1} + \cdots + c_1 C_q + c_0 I_t | c_i \in Z_p\}$$

is isomorphic to the Galois field $GF(p^t)$. Next, we will make use of the fact that $GF(p^n)$ is isomorphic to $GF(p^t)^{\frac{n}{t}}$, for any positive divisor t of n (see [27]). Let

$$r(x) = x^d + \beta_{d-1}x^{d-1} + \cdots + \beta_1 x + \beta_0$$

be an irreducible polynomial over $\mathcal{N}(C_q)$, where $d = \frac{n}{t}$. The companion matrix of $r(x)$ is

$$C_r = \begin{pmatrix} 0 & 0 & \dots & 0 & -\beta_0 \\ I_t & 0 & \dots & 0 & -\beta_1 \\ 0 & I_t & \dots & 0 & -\beta_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & I_t & -\beta_{d-1} \end{pmatrix},$$

and

$$\mathcal{N}(C_r) = \{\gamma_{d-1}C_r^{d-1} + \cdots + \gamma_1 C_r + \gamma_0 I_d | \gamma_i \in (C_q)\}$$

is isomorphic to $GF(p^t)^{\frac{n}{t}}$. Note that $S' \in \mathcal{N}(C_r)$, and hence it commutes with any element in $\mathcal{N}(C_r)$. In particular, S' commutes with any maximal matrix M' in $\mathcal{N}(C_r)$. Thus, by Theorem 2.3.16, the length of the $M'S'$–orbits is $i_q = \frac{p^n-1}{\gcd(k_q, p^n-1)} = \mu_q$, where $\mu_q = \frac{p^n-1}{k_q}$ and k_q is the order of $q(x)$. Therefore, the number of MS–orbits is $\eta_{m_S} = \frac{\mu_q}{\mu_q} = 1$, and an optimal M for S is $M = AM'A$.$\diamondsuit$

In particular, any scalar matrix S, i.e., $S = aI_n$ for some $a \in Z_p$, and any S with irreducible characteristic polynomial are M–minimal. Theorems 4.2.2 and 4.2.3 show how to find an optimal M in each of these two cases.

Theorem 4.2.2 *For any $a \in Z_p$, $S = aI_n$ is M–minimal and the companion matrix M of any primitive polynomial is optimal for S.*

Let S be an $n \times n$ matrix over Z_p with irreducible characteristic polynomial and let $P(x)$ be a primitive polynomial of degree n. Then, by Corollary 2.2.1, there exists a polynomial $Q(x) = c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ such that $Q(S)$ is a maximal matrix.

Theorem 4.2.3 *Every nonsingular $S \in \mathcal{M}_n$ with irreducible characteristic polynomial is M–minimal and the matrix $M = Q(S)$ is optimal for S.*

Let $S \in \mathcal{M}_n$ be nonsingular with $\phi_S(x) = (-1)^n P(x)$, where $P(x)$ is irreducible and let $M, N \in \mathcal{N}(S)$ be such that N is maximal. Let t_M be the index of M with respect to N. By Remark 2.3.1,

$$i_P = \frac{\gcd(\mathrm{Ind}_N(C_P), p^n - 1)}{\gcd(\mathrm{Ind}_N(C_P), \mathrm{Ind}_N(M), p^n - 1)},$$

and by Lemma 2.3.4, $\mathrm{Ind}_N(C_P) = \mu_P r$ for some positive integer r such that

$$\gcd(k_P, r) = 1.$$

Then,

$$i_P = \frac{\mu_P}{\gcd(\mu_P r, t_M, p^n - 1)} = \frac{\mu_P}{\gcd(\mu_P, t_M)}.$$

Thus,

$$\eta_P = \frac{\mu_P}{i_P} = \gcd(\mu_P, t_M).$$

We have just shown

Lemma 4.2.1 *Let $S \in \mathcal{M}_n$ be nonsingular with $\phi_S(x) = (-1)^n P(x)$, where $P(x)$ is irreducible and let $M, N \in \mathcal{N}(S)$ be such that N is maximal. Let t_M be the index of M with respect to N. Then, $\eta_{m_S} = \gcd(\mu_P, t_M)$.*

4.2.3 Some non–minimal n–dimensional cases

In this subsection we solve the MS–orbits problem for the important n–dimensional case when the characteristic polynomial of matrix S decomposes as the product of two distinct irreducible factors. Given a nonsingular matrix S that commutes with S, Theorem 4.2.4 computes the MS–orbit structure.

Theorem 4.2.4 *Let $S \in \mathcal{M}_n$ be nonsingular with $\phi_S(x) = (-1)^n P_1(x)P_2(x)$, where $P_1(x)$ and $P_2(x)$ are distinct irreducible monic polynomials of degree d_1 and d_2, respectively. Also, let $M \in \mathcal{N}(S)$ be nonsingular. Then, $m_M(x) = q_1(x)q_2(x)$ for some irreducible polynomials q_1 and q_2, and the MS–orbit structure is*

$$1 + \eta_{P_1}[i_{P_1}] + \eta_{P_2}[i_{P_2}] + \eta_{P_1,P_2}[i_{P_1,P_2}],$$

where, for $t = 1, 2$

$$\begin{aligned}
N_t &\quad \textit{maximal matrix in } \mathcal{N}(C_{P_t}),\\
u_{P_t} &\quad \textit{index of } C_{P_t} \textit{ respect to } N_t,\\
u_{q_t} &\quad \textit{index of } C_{q_t} \textit{ respect to } N_t,\\
m &= lcm(p^{d_1}-1, p^{d_2}-1),\\
m'_t &= \tfrac{m}{p^{d_t}-1},\\
e_t &= \tfrac{lcm(m'_1 u_{C_1}, m'_2 u_{C_2})}{m'_t u_{P_t}},\\
i_{P_t} &\quad \textit{length of the } MS\textit{–orbits in } \mathcal{O}_{P_t},\\
\eta_{P_t} &\quad \textit{number of the } MS\textit{–orbits in } \mathcal{O}_{P_t},\\
i_{P_1,P_2} &= \tfrac{m}{\gcd(e_1 m'_1 u_{q_1} - e_2 m'_2 u_{q_2}, \gcd(k_{P_1}\eta_{P_1} m'_1, k_{P_2}\eta_{P_2} m'_2))},\\
\eta_{P_1,P_2} &= \tfrac{\mu_{P_1,P_2}}{i_{P_1,P_2}}.
\end{aligned}$$

Proof
Recall that $V_{P_t} = \{\mathbf{x} \in Z_p^n | P_t(S)\mathbf{x} = \mathbf{0}\}$ and that $V_{P_1,P_2} = V_{P_1P_2} - V_{P_1} \cup V_{P_2}$. Observe

that

$$Z_p^n = V_{P_1} \cup V_{P_2} \cup V_{P_1,P_2}.$$

Hence, the S–orbit structure is the formal sum of S–orbits in V_{P_1}, V_{P_2}, and V_{P_1,P_2}. Let $\sum O_T$ be the formal sum of S–orbits in V_T. Thus, the formal sum of S–orbits in Z_p^n can be expressed as

$$1 + \sum O_{P_1} + \sum O_{P_2} + \sum O_{P_1,P_2},$$

where, by Theorem 3.1.3,

$$\begin{array}{lcl} \sum O_{P_1} & = & \mu_{P_1}(k_{P_1}), \\ \sum O_{P_2} & = & \mu_{P_2}(k_{P_2}), \\ \sum O_{P_1,P_2} & = & \mu_{P_1,P_2}(k_{P_1,P_2}). \end{array}$$

Let A be a nonsingular matrix for which $A^{-1}SA = \begin{pmatrix} C_{P_1} & 0 \\ 0 & C_{P_2} \end{pmatrix}$ and let $M \in \mathcal{N}(S)$ be nonsingular. By Theorem 2.2.6, $M = Q(S)$ for some polynomial $Q(x)$ of degree at most $n-1$, since S is nonderogatory. Hence,

$$M' = A^{-1}Q(S)A = Q(A^{-1}SA) = \begin{pmatrix} Q(C_{P_1}) & 0 \\ 0 & Q(C_{P_2}) \end{pmatrix}.$$

We already know that V_{P_1}, V_{P_2}, as well as V_{P_1,P_2} are M–invariant since $M = Q(S)$. Thus, the MS–orbit structure in Z_p^n can be expressed as

$$1 + \sum \mathcal{O}_{P_1} + \sum \mathcal{O}_{P_2} + \sum \mathcal{O}_{P_1,P_2}.$$

By Corollary 2.2.6 $\mathcal{N}(C_{P_t})$ is a finite field of p^{d_t} elements. Let N_t be a maximal matrix in $\mathcal{N}(C_{P_t})$. Also, let u_{P_t} and u_{q_t} be the indexes of C_{P_t} and $Q_t(C_{P_t})$ with respect to N_t. Now, since $P_t(x)$ is irreducible, the MS–orbit structure in $\mathcal{O}_{P_t}$ is $\eta_{P_t}[i_{P_t}]$, where i_{P_t}, the length of the MS–orbits in $\mathcal{O}_{P_t}$, is the smallest positive integer that solves

$$(N_t^{u_{P_t}})^{j_t} = (N_t^{u_{q_t}})^{i_{P_t}} \bmod p^{d_t}$$

for some integer j_t. By Theorem 2.3.16,

$$i_{P_t} = \frac{k_{q_t}}{\gcd(k_{P_t}, k_{q_t})}$$

and the number of MS–orbits in $\mathcal{O}_{P_t}$ is

$$\eta_{P_t} = \frac{\mu_{P_t}}{i_{P_t}} = \frac{p^{d_1} - 1}{k_{P_t} i_{P_t}}.$$

On the other hand, the smallest positive integer i_{P_1,P_2} that simultaneously solves

$$(N_1^{u_{C_1}})^{j_{P_1,P_2}} = (N_1^{u_{Q_1}})^{i_{P_1,P_2}} \bmod p^{d_1} \quad (4.8)$$
$$(N_1^{u_{C_2}})^{j_{P_1,P_2}} = (N_2^{u_{Q_2}})^{i_{P_1,P_2}} \bmod p^{d_2} \quad (4.9)$$

for some integer j_{P_1,P_2} is the length of the MS–orbits in $\mathcal{O}_{P_1,P_2}$. By Theorem 2.3.18,

$$i_{P_1,P_2} = \frac{m}{\gcd(e_1 m_1' u_{Q_1} - e_2 m_2' u_{Q_2}, \gcd(k_{P_1}\eta_{P_1} m_1', k_{P_2}\eta_{P_2} m_2'))},$$

where, for $t = 1, 2$,

$$\begin{aligned} m &= \operatorname{lcm}(p^{d_1}-1, p^{d_2}-1), \\ m_t' &= \frac{m}{p^{d_t}-1}, \\ e_t &= \frac{\operatorname{lcm}(m_1' u_{C_1}, m_2' u_{C_2})}{m_t' u_{P_t}}. \end{aligned}$$

Henceforth, the number of MS–orbits in $\mathcal{O}_{P_1,P_2}$ is

$$\eta_{P_1,P_2} = \frac{\mu_{P_1,P_2}}{i_{P_1,P_2}}.$$

Therefore, the entire MS–orbit structure in Z_p^n is

$$\mathcal{O}_{m_S} = 1 + \eta_{P_1}[i_{P_1}] + \eta_{P_2}[i_{P_2}] + \eta_{P_1,P_2}[i_{P_1,P_2}].\diamondsuit$$

Example 4.2.1 *Let* $S = \begin{pmatrix} 0 & 3 & 0 & 0 \\ 1 & 4 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{pmatrix}$ *be defined over* Z_5. *The characteristic polynomial of* S *is* $\phi_S(x) = P_1(x)P_2(x) = x^4+3x^3+2x^2+2x+1$, *where* $P_1(x) = x^2+x+2$ *and* $P_2(x) = x^2+2x+3$. *A simple inspection shows us that* P_1 *and* P_2 *are irreducible over* Z_5 *and, furthermore, they are primitive. Thus,* $k_{P_1} = k_{P_2} = 24$. *Hence,* $\mu_{P_1} = \mu_{P_2} = \frac{5^2-1}{24} = 1$ *and* $\mu_{P_1,P_2} = 1 \cdot 1 \gcd(24, 24) = 24$. *Since both* C_{P_1} *and* C_{P_2} *are maximal matrices,* $u_{P_1} = u_{P_2} = 1$. *Hence* $e_1 = e_2 = 1$.

Let $M = \begin{pmatrix} 1 & 3 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 3 & 4 \\ 0 & 0 & 2 & 4 \end{pmatrix}$. *It is straightforward to see that* $M \in \mathcal{M}_n$ *and that*

$$m_M(x) = q_1(x)q_2(x),$$

where $q_1(x) = x^2 + 4x + 2$, *and* $q_2(x) = x^2 + 3x + 4$. *By direct computation,*

$$\begin{aligned} k_{q_1} &= 24, \quad & k_{q_2} &= 12, \\ u_{q_1} &= 17, \quad & u_{q_2} &= 14. \end{aligned}$$

Thus, applying Theorem 4.2.4, *we have that*

$$m = lcm(24, 24) = 24,\ m_1' = m_2' = 1,$$

and

$$\begin{aligned} i_{P_1} &= \tfrac{k_{q_1}}{\gcd(k_{P_1}, k_{q_1})} = 1, \quad & \eta_{P_1} &= \tfrac{\mu_{P_1}}{i_{P_1}} = 1 \\ i_{P_2} &= \tfrac{k_{q_2}}{\gcd(k_{P_2}, k_{q_2})} = 1, \quad & \eta_{P_2} &= \tfrac{\mu_{P_2}}{i_{P_2}} = 1 \end{aligned}$$

$$i_{P_1,P_2} = \frac{m}{\gcd(e_1 m_1' u_{q_1} - e_2 m_2' u_{q_2}, \gcd(k_{P_1}\eta_{P_1} m_1', k_{P_2}\eta_{P_2} m_2'))} = \frac{24}{\gcd(17 - 14, 24)} = 8,$$

and

$$\eta_{P_1,P_2} = \frac{\mu_{P_1,P_2}}{i_{P_1,P_2}} = \frac{24}{8} = 3.$$

Therefore, the MS*–orbit structure in* Z_5^4 *is*

$$1 + 1[1] + 1[1] + 3[8] = 1 + 2[1] + 3[8].$$

Remark 4.2.1 *Recall from the proof of Theorem* 4.2.4 *that, given* $S \in \mathcal{M}_n$ *with* $\phi_S(x) = (-1)^n P_1(x) P_2(x)$, *where* $P_1(x)$ *and* $P_2(x)$ *are irreducible polynomials,* S *is similar to* $\begin{pmatrix} C_{P_1} & 0 \\ 0 & C_{P_2} \end{pmatrix}$ *and any matrix* $M \in \mathcal{N}(S)$ *is similar to* $\begin{pmatrix} Q(C_{P_1}) & 0 \\ 0 & Q(C_{P_2}) \end{pmatrix}$ *for some polynomial* $Q(x)$. *Also, by Corollary* 2.2.1, *there exist maximal matrices* $N_r \in \mathcal{N}(C_{P_r})$ *such that* $Q(C_{P_r}) = N_r^{t_r}$ *for some positive integers* t_r, $r = 1, 2$. *Thus,* $M = A \begin{pmatrix} N_1^{t_1} & 0 \\ 0 & N_2^{t_2} \end{pmatrix} A^{-1}$ *for some nonsingular* $A \in \mathcal{M}_n$. *Hence,* η_{m_S} *depends on* t_1 *and* t_2 *and for this reason we denote* η_{m_S} *by* $\eta_{m_S}(t_1, t_2)$.

Let $S \in \mathcal{M}_n$ be nonsingular with $\phi_S(x) = (-1)^n p_1(x) p_2(x)$, where $p_1(x)$ and $p_2(x)$ are irreducible polynomials of degrees d_1 and d_2, respectively.

Algorithm 4.2.2 examines all possible pairs $(t_1', t_2') \in Z_{p^{d_1}}^* \times Z_{p^{d_2}}^*$ and returns a pair (t_1, t_2) for which $\eta_{m_S}(t_1, t_2)$ is minimal.

Algorithm 4.2.2

Inputs: *prime p, primitive polynomials $P_1(x)$, $P_2(x)$,*
irreducible polynomials $p_1(x)$ and $p_2(x)$.

Output: *(t_1, t_2) such that $\eta_{m_S}(t_1, t_2)$ is minimal.*

1. *compute $c_0, c_1, \ldots, c_{d_1-1} \in Z_p$ such that*
   $P_1(\sum_{i=0}^{d_1-1} c_i C_{p_1}^i) = \mathbf{0}$, *the zero $d_1 \times d_1$ matrix;*
2. *compute $c'_0, c'_1, \ldots, c'_{d_2-1} \in Z_p$ such that*
   $P_2(\sum_{i=0}^{d_2-1} c'_i C_{p_2}^i) = \mathbf{0}$, *the zero $d_2 \times d_2$ matrix;*
3. *set $N_1 = \sum_{i=0}^{d_1-1} c_i C_{p_1}^i$.*
4. *set $N_2 = \sum_{i=0}^{d_2-1} c'_i C_{p_2}^i$.*
5. *compute $e_1, e_2, k_{P_1}, k_{P_2}, k_{P_1,P_2}, \mu_{P_1}, \mu_{P_2}, \mu_{P_1,P_2}$;*
6. *Initialize t_1 to p^{d_1} and t_2 to p^{d_2};*
7. *Initialize $\eta_{P_1}, \eta_{P_2}, \eta_{P_1,P_2}, \eta_{m_S}$ to p^n;*
8. **for**$(t'_1 = 1$ *to* $t'_1 = p^{d_1} - 1)$ **do**
   compute η'_{P_1};
   for$(t'_2 = 1$ *to* $t'_2 = p^{d_2} - 1)$ **do**
   compute $\eta'_{P_2}, \eta'_{P_1,P_2}$;
   $\eta'_{m_S} \leftarrow \eta'_{P_1} + \eta'_{P_2} + \eta'_{P_1,P_2}$.
   if$(\eta'_{m_S} < \eta_{m_S})$
   $(\eta_{P_1}, \eta_{P_2}, \eta_{P_1,P_2}) \leftarrow (\eta'_{P_1}, \eta'_{P_2}, \eta'_{P_1,P_2})$.
   $(t_1, t_2) \leftarrow (t'_1, t'_2)$.

return (t_1, t_2)

Let P_1, P_2, p_1, and p_2 be the primitive and irreducible polynomials, respectively, in the input of Algorithm 4.2.2. By Corollary 2.2.1, $N_r = \sum_{i=0}^{d_r-1} c'_i C_{p_r}^i$ is a maximal matrix that commutes with C_{p_r}. Let u_{p_r} be the index of C_{p_r} with respect to N_r.

The remaining quantities in Algorithm 4.2.2 are computed according to the formulas given in Theorem 4.2.4 as follows:

$$\begin{array}{lcllcl} k_{p_r} & = & \frac{p^{d_r}-1}{\gcd(p^{d_r}-1,u_{C_r})}, & k_{p_1,p_2} & = & \mathrm{lcm}(k_{p_1},k_{p_2}), \\ \mu_{p_r} & = & \frac{p^{d_r}-1}{k_{p_r}}, & \mu_{p_1,p_2} & = & \mu_{p_1}\mu_{p_2}\gcd(k_{p_1},k_{p_2}), \\ m & = & \mathrm{lcm}(p^{d_1}-1,p^{d_2}-1), & m'_r & = & \frac{m}{p^{d_r}-1}, \\ e_r & = & \frac{\mathrm{lcm}(m'_1u_{p_1},m'_2u_{p_2})}{m'_ru_{p_r}}, & \eta_{p_r} & = & \gcd(\mu_{p_r},t'_r), \end{array}$$

and

$$\eta_{P_1,P_2} = \frac{\mu_{p_1,p_2}}{m}\gcd(e_1m'_1t'_1 - e_2m'_2t'_2, \gcd(k_{p_1}\eta_{p_1}m'_1, k_{p_2}\eta_{p_2}m'_2)).$$

Assuming we have a table of primitive polynomials as well as logs and antilogs tables for Z_p^*, the complexity of Algorithm 4.2.2 is as follows.

The cost of steps 1, 2, 3, and 4 is $O(p^d)$ where $d = \max\{d_1, d_2\}$, since when $d_r > 2$, an exhaustive search is performed. Now, in order to compute quantities in step 5 we need the index of C_{p_r} with respect to N_r. For this, we make succesive multiplications of N_r by itself. Thus, step 5 also costs $O(p^d)$ time. Steps 6 and 7 are of constant time.

The cost of the inner **for** loop is $O(p^{d_2}\log p)$ time since some gcd operations are executed $p^{d_2}-1$ times. Thus, step 8 costs $O(p^{d_1}p^{d_2}\log p) = O(p^n\log p)$ time. Therefore, the complexity of the overall algorithm is $O(p^n\log p)$.

4.3 Two dimensional cases

The question remains of how to choose an optimal M for a symmetry matrix S that is not necessarily M–minimal. In this section we completely solve the problem for two dimensions. We characterize the various cases according to the factorability of the minimal polynomial of S.

Theorem 4.3.1 *Let $S \in \mathcal{M}_2$ be nonsingular. Then $m_S(x)$ can be factored according to one, and only one of the following cases.*

I. $m_S(x) = x^2 + bx + c$ *is irreducible over* Z_p,

II. $m_S(x) = x - \lambda$,

III. $m_S(x) = (x-\lambda)^2$,

IV. $m_S(x) = (x - \lambda_1)(x - \lambda_2),\ \lambda_1 \neq \lambda_2$

Proof
Let $S \in \mathcal{M}_2$ be nonsingular. Also, let $\phi_S(x)$ and $m_S(x)$ be the characteristic and minimal polynomials of S, respectively. On the one hand, recall that $m_S(x)$ contains all distinct factors of $\phi_S(x)$. Thus, if $\phi_S(x)$ is the product of distinct irreducible factors, so is $m_S(x)$. So, if $m_S(x)$ is quadratic and irreducible, or $m_S(x)$ is the product of two distinct linear factors. This covers cases *I* and *IV*. On the other hand, if $\phi_S(x) = (x - \lambda)^2$, then $m_S(x) = (x - \lambda)^2$ or $m_S(x) = x - \lambda$, which covers cases *II* and *III*.$\diamondsuit$

The next theorem deals with the identification of matrices M that commute with a 2×2 nonsingular matrix S.

Theorem 4.3.2 *Let $S \in \mathcal{M}_2$ be nonsingular. If $m_S(x) = x - \lambda$, then $\mathcal{N}(S) = \mathcal{M}_2$. Otherwise, $\mathcal{N}(S) = \{c_1S + c_0I_2 | c_0, c_1 \in Z_p\}$.*

Proof
According to Theorem 4.3.1, $m_S(x)$ can be factor in four cases. If S is as in case *II*, $S - \lambda I_2 = 0$. Hence, S is a scalar matrix. Thus, S commutes with any 2×2 matrix in $\mathcal{M}_2$. On the other hand, if $m_S(x)$ is as in cases *I*, *III*, or *IV*, S is nonderogatory. Hence, by Theorem 2.2.6, $\mathcal{N}(S) = \{c_1S + c_0I_2 | c_0, c_1 \in Z_p\}$.$\diamondsuit$

4.3.1 M–minimal two dimensional cases: cases *I* and *II*

Theorem 4.3.4 gives us the results for finding optimal matrices M for symmetries S that fall into cases *I* and *II* of Theorem 4.3.1, respectively. In this subsection we give necessary and sufficient conditions in order for a 2×2 matrix S over Z_p to be M–minimal and we show how to find such an M.

Theorem 4.3.3 *Let $S \in \mathcal{M}_2$ be nonsingular. Then S is M–minimal if and only if S is scalar or $\phi_S(x)$ is irreducible.*

Proof
Let us assume S is M–minimal and that M is an optimal matrix for S. Thus, by Lemma 4.1.6, $m_S(x) = q(x)$, where $q(x)$ is irreducible over Z_p. Hence, $q(x)$ is either a linear or a second degree polynomial. If $q(x)$ is linear, $m_S(x) = x - \lambda$, for some $\lambda \neq 0 \in Z_p$. Hence, $S - \lambda I_2 = 0$, which implies that $S = \lambda I_2$. If, on the other hand, $q(x)$ is a quadratic polynomial, then $m_S(x) = \phi_S(x)$.

Now, let us show the converse of the theorem. Assume $S = \lambda I_2$, $\lambda \neq 0$. Thus, $m_S(x) = q(x) = x - \lambda$. Let $P(x) = x^2 + ax + b$ be a primitive polynomial over Z_p. The companion matrix of P, C_P is a maximal matrix and, since S is scalar, C_P commutes with S.

On the other hand, by Theorem 3.1.5, there are $\mu_q = \frac{p^2-1}{k_q}$ S–orbits of length k_q. By Theorem 2.3.16, the length of the MS–orbits is

$$i_q = \frac{k_P}{\gcd(k_q, k_P)} = \frac{p^2-1}{\gcd(k_q, p^2-1)} = \frac{p^2-1}{k_q} = \mu_q.$$

Hence, $\eta_q = \frac{\mu_q}{i_q} = 1$.

Finally, assume that $\phi_S(x) = q(x)$ is irreducible, then, by Corollary 2.2.1, there exists a polynomial $Q(x) = c_1 S + c_0 I_2$ such that $M = Q(S)$ is a maximal matrix that commutes with S. Thus, by Theorem 2.3.16, the length of the MS–orbits is

$$i_q = \frac{\mu_q}{\gcd(\mu_q, \mathrm{Ind}_M(M))} = \frac{\mu_q}{\gcd(\mu_q, 1)} = \mu_q,$$

and $\eta_q = \frac{\mu_q}{i_q} = 1.\diamondsuit$

In the two dimensional case, Theorem 4.3.4 describes the solution of the system of congruences that gives the coefficients of the polynomial $Q(x)$ from Corollary 2.2.1.

Theorem 4.3.4 *Let $S \in \mathcal{M}_2$ be nonsingular and let $P(x) = x^2 + ax + b$ be any primitive polynomial over Z_p. If S is a scalar matrix, then an optimal matrix M for S is $M = C_P$. On the other hand, if $m_S(x) = x^2 + cx + d$ is irreducible, then $\frac{a^2-4b}{c^2-4d}$ is a quadratic residue c_1 mod p, and $M = c_1 S + c_0 I_2$ is optimal for S, where $c_0 = 2^{-1}(c_1 c - a)$.*

Proof
If S is scalar, it was already shown in the proof of Theorem 4.3.3 that the companion matrix of $P(x)$, C_P, is optimal for S.

Now, suppose $m_S(x) = x^2 + cx + d$ is irreducible. Then, by Corollary 2.2.1, there exist $c_0, c_1 \in Z_p$ such that $M = c_1 S + c_0 I_2$ is a maximal matrix and that $P(M) = 0$. In fact, since $P(x)$ is an irreducible quadratic polynomial, there must be two such pairs (c_0, c_1). Since $m_S(S) = 0$, we have to find c_0 and c_1 such that

$$P(c_1 S + c_0 I_2) = 0 \bmod S^2 + cS + dI_2 \tag{4.10}$$

Note that $P(c_0 I_2) \neq 0$ for any $c_0 \in Z_p$. Hence $c_1 \neq 0$. Also note that $c^2 - 4d \neq 0$, since if it were the case, $m_S(-2^{-1}c) = 0$, which contradicts the irreduciblity of $m_S(x)$. Equation (4.10) is equivalent to

$$(-cc_1^2 + 2c_0c_1 + ac_1)S + (c_0^2 + ac_0 + b - dc_1^2)I_2 = 0$$

if and only if

$$\begin{aligned} -cc_1^2 + 2c_0c_1 + ac_1 &= 0 \\ c_0^2 + ac_0 + b - dc_1^2 &= 0 \end{aligned}$$

if and only if

$$\begin{aligned} -cc_1 + 2c_0 + a &= 0 \\ c_0^2 + ac_0 + b - dc_1^2 &= 0 \end{aligned}$$

if and only if

$$\begin{aligned} c_1^2 &= \frac{a^2 - 4b}{c^2 - 4d} \\ c_0 &= 2^{-1}(cc_1 - a). \diamondsuit \end{aligned}$$

Example 4.3.1 *Let* $S = \begin{pmatrix} 23 & 65 \\ 84 & 10 \end{pmatrix}$ *over* Z_{97}. *A quadratic primitive polynomial over* Z_{97} *is* $P(x) = x^2 - x + 5$ *and the minimal polynomial of* S *is* $m_S(x) = x^2 + 64x + 8$. *By direct computation we verify that* $m_S(x)$ *is irreducible. Applyng Theorem 4.3.4, we find that* $c_1^2 = 31 \ mod\ 97$ *and so* $c_1 = 15$ *or* $c_1 = 82$. *Thus,* $c_0 = 44$ *or* $c_0 = 54$. *Thus, two optimal matrices for* S *are*

$$M = 15S + 44I_2 = \begin{pmatrix} 1 & 5 \\ 96 & 0 \end{pmatrix} \text{ and } M = 82S + 54I_2 = \begin{pmatrix} 0 & 92 \\ 1 & 1 \end{pmatrix}.$$

Example 4.3.2 *Let* $S = \begin{pmatrix} 0 & 1 \\ p-1 & 0 \end{pmatrix}$ *be defined over* Z_p, *where* p *is a prime less than* 100. *The minimal polynomial of* S *is* $m_S(x) = x^2 + 1$. *By Theorem* 2.3.14, $m_S(x)$ *is irreducible mod* p *if and only if* $p = 3 \ mod\ 4$, *i.e.,* p *is of the form* $4t + 3$. *By Theorem* 4.3.4, *one such family of matrices is given by*

$$M = c_1 S + I_2 = \begin{pmatrix} 1 & c_1 \\ -c_1 & 1 \end{pmatrix}.$$

Table 4.3.1 *lists all primes* p *between* 5 *and* 100 *of the form* $4t+3$ *and values of* c_1 *that satisfy Theorem* 4.3.4.

p	c_1	MS–*orbits* $M = c_1S + I_2$	MS–*orbits* $M = gI_2$
7	2	$1+1[12]$	$1+4[3]$
11	4	$1+1[30]$	$1+6[5]$
19	3	$1+1[90]$	$1+10[9]$
23	2	$1+1[132]$	$1+12[11]$
31	4	$1+1[240]$	$1+16[15]$
43	2	$1+1[462]$	$1+22[21]$
47	2	$1+1[552]$	$1+24[23]$
59	3	$1+1[870]$	$1+30[29]$
67	7	$1+1[1122]$	$1+34[33]$
71	7	$1+1[1260]$	$1+36[35]$
79	6	$1+1[1560]$	$1+40[39]$
83	10	$1+1[1722]$	$1+42[41]$

Table 4.3.1 : M–*minimal cases*

4.3.2 Optimal two dimensional matrices for case II

In this subsection we give a specific formula to compute optimal matrices for case II of Theorem 4.3.1.

Theorem 4.3.5 *Let* $S \in \mathcal{M}_2$ *be nonsingular with* $m_S(x) = P(x)^2$, *where* $P(x) = x - \lambda$. *Also, let* $M \in \mathcal{N}(S)$ *be nonsingular. Then* $m_M(x)$ *has a factor of the form* $q(x) = x - \beta$ *and the* MS–*orbit structure is* $1 + 2\eta_P[i_P]$, *where* i_P, η_P *are the length and the number of the* MS–*orbits in* $\mathcal{O}_P$, *respectively.*

Proof
Let $S \in \mathcal{M}_2$ be nonsingular with $m_S(x) = (x-\lambda)^2$. Recall that

$$\begin{array}{lcl} V_P & = & \{\mathbf{x} \in Z_p^2 | P(S)\mathbf{x} = \mathbf{0}\} \\ & = & \{\mathbf{x} \in Z_p^2 | (S-\lambda I_2)\mathbf{x} = \mathbf{0}\}, \\ V_{P^2} & = & \{\mathbf{x} \in Z_p^2 | P(S)^2\mathbf{x} = \mathbf{0}\}, \\ V_{P^2,P} & = & V_{P^2} - V_P. \end{array}$$

Note that if M is any nonsingular matrix that commutes with S, then V_P as well as $V_{P^2,P}$ are M–invariant. Therefore, the MS–orbit structure is given by the union of the MS–orbit structures of $\mathcal{O}_P$ and $\mathcal{O}_{P^2,P}$. Now, since $P(x) = x - \lambda$ is irreducible, then the MS–orbit structure in $\mathcal{O}_P$ is $\eta_P[i_P]$, where, by Theorem 2.3.16,

$$i_P = \frac{k_q}{\gcd(k_P, k_q)} \text{ and } \eta_P = \frac{\mu_P}{i_P} = \frac{p-1}{k_P i_P}.$$

We will show that the MS–orbit structure in $\mathcal{O}_{P^2,P}$ is $\eta_P[i_P]$.

Note that, by the Jordan canonical decomposition theorem (Theorem 2.2.4), there exists a nonsingular matrix A such that

$$A^{-1}SA = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}.$$

Also, by Theorem 4.3.2, if $M \in \mathcal{N}(S)$, there exist $c_0, c_1 \in Z_p$ such that $M = c_1 S + c_0 I_2$. Hence,

$$\begin{array}{lcll} A^{-1}MA & = & c_1 \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} + c_0 I_2 & (4.11) \\ & = & \begin{pmatrix} c_1\lambda + c_0 & c_1 \\ 0 & c_1\lambda + c_0 \end{pmatrix} & (4.12) \\ & = & \begin{pmatrix} \beta & \gamma \\ 0 & \beta \end{pmatrix}, & (4.13) \end{array}$$

where $\beta = c_1\lambda + c_0$ and $\gamma = c_1$. Thus, $i_{P^2,P}$ is the smallest positive integer that solves

$$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}^{j_{P^2,P}} = \begin{pmatrix} \beta & \gamma \\ 0 & \beta \end{pmatrix}^{i_{P^2,P}} \pmod{p} \tag{4.14}$$

for some integer $j_{P^2,P}$, if and only if

$$\left.\begin{array}{ll} \lambda^{j_{P^2,P}} & = \beta^{i_{P^2,P}} \\ j_{P^2,P}\lambda^{j_{P^2,P}-1} & = i_{P^2,P}\beta^{i_{P^2,P}-1}\gamma \end{array}\right\} \pmod{p} \tag{4.15}$$

if and only if

$$\begin{aligned} \mathrm{Ind}(\lambda) j_{P^2,P} &= \mathrm{Ind}(\beta) i_{P^2,P} \pmod{p-1} && (4.16) \\ j_{P^2,P} &= \beta^{-1}\lambda\gamma i_{P^2,P} \pmod{p} && (4.17) \end{aligned}$$

Making equations (4.16) and (4.17) have the common modulo $p(p-1)$ and eliminating $j_{P^2,P}$ from both equations we endup with

$$\mathrm{Ind}(\beta) i_{P^2,P} = 0 \pmod{\mu_P}.$$

Thus, by Theorem 2.3.11,

$$i_{P^2,P} = \frac{\mu_P}{\gcd(\mu_P, \mathrm{Ind}(\beta))} = \frac{k_q}{\gcd(k_P, k_q)} = i_P,$$

which is the same as solving $\lambda^{j_P} = \beta^{i_P} \pmod{p}$. Thus, the number of MS–orbits in $\mathcal{O}_{P^2,P}$ is $\eta_{P^2,P} = \frac{\mu_{P^2,P}}{i_{P^2,P}} = \frac{\mu_P}{i_P} = \eta_P$. Therefore, the MS–orbit structure in $\mathcal{O}_{m_S}$ is

$$1 + \eta_P[i_P] + \eta_P[i_P] = 1 + 2\eta_P[i_P].\diamondsuit$$

Remark 4.3.1 *Note that, in this particular case, the MS–orbit structure does not depend on the value of γ. Thus, any nonsingular $M', M'' \in \mathcal{N}(S)$ impose the same MS–orbit structure as long as $\phi_{M'} = \phi_{M''}$.*

Given any 2×2 nonsingular matrix S with $m_S(x) = (x-\lambda)^2$ and $M = gI_2$, apply Theorem 4.3.5 and we have

Corollary 4.3.1 *Let $S \in \mathcal{M}_2$ be nonsingular with $m_S(x) = P^2(x)$, where $P(x) = x - \lambda$. Then, an optimal matrix M for S is $M = gI_2$ and the MS–orbit structure is given by $1 + 2[\mu_P]$, where g is a primitive of Z_p^*.*

4.3.3 Optimal two dimensional matrices for case IV

In this subsection we find an optimal matrix M when matrix S has two distinct nonzero eigenvalues. Theorem 4.3.7 outlines the procedure to compute such an optimal M for S.

The following theorem is a restatement of Theorem 4.2.4 for the case when matrix S has two distinct eigenvalues (i.e., the two irreducible polynomials have degree 1.) Algorithm 4.3.1 is a specialized version of Algorithm 4.2.2 for this particular case.

Theorem 4.3.6 *Let $S \in \mathcal{M}_2$ be nonsingular with $m_S(x) = P_1(x)P_2(x)$, where for $t = 1, 2$, $P_t(x) = x - \lambda_t$, $\lambda_1 \neq \lambda_2$. Then for any nonsingular $M \in \mathcal{N}(S)$, $\phi_M(x) = q_1(x)q_2(x)$, where $q_t(x) = x - \beta_t$ and the MS–orbit structure induced by M is*

$$1 + \eta_{P_1}[i_{P_1}] + \eta_{P_2}[i_{P_2}] + \eta_{P_1,P_2}[i_{P_1,P_2}],$$

where i_{P_t}, i_{P_1,P_2}, η_{P_t}, and η_{P_1,P_2} are the length and the number of the MS–orbits in $\mathcal{O}_{P_t}$ and $\mathcal{O}_{P_1,P_2}$, respectively.

Example 4.3.3 *Let S be a 2×2 matrix over Z_{17} with $m_S(x) = (x - 13)(x - 4)$. A primitive element of Z_{17}^* is $g = 3$, and a table of indexes with respect to g, together with the order of each element $a \in Z_{17}^*$, k_a, is*

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$Ind_3(a)$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8
k_a	1	8	16	4	16	16	16	8	8	16	16	16	4	16	8	2

Table 4.3.2 : Index table with respect to primitive $g = 3$ for Z_{17}^*.

In this example, $\lambda_1 = 13$ and $\lambda_2 = 4$ (i.e., $P_1(x) = x - 13$ and $P_2(x) = x - 4$) and, from Table 1,

$$Ind_3(\lambda_1) = 4,\ k_{P_1} = 4,\ Ind_3(\lambda_2) = 12, \quad \text{and } k_{P_2} = 4.$$

Thus,

$$\mu_{P_1} = \frac{16}{4} = 4,\ \mu_{P_2} = \frac{16}{4} = 4,\ k_{P_1,P_2} = lcm(4,4) = 4, \quad \text{and } \mu_{P_1,P_2} = 4 * 4 * 4 = 64.$$

Also, compute e_1 and e_2:

$$\begin{aligned} e_1 &= \frac{lcm(Ind_3(\lambda_1), Ind_3(\lambda_2))}{Ind_3(\lambda_1)} = \frac{lcm(4,12)}{4} = 3, \\ e_2 &= \frac{lcm(Ind_3(\lambda_1), Ind_3(\lambda_2))}{Ind_3(\lambda_2)} = \frac{lcm(4,12)}{12} = 1 \end{aligned}$$

There are three types of nontrivial S–orbits: the ones in V_{P_1} and V_{P_2}, which, in this case, are of length 4, and the ones in V_{P_1,P_2} of length 64. By Theorem 3.1.3, the S–orbit structure is

$$1 + 4(4) + 4(4) + 64(4).$$

Now, we will consider two different diagonal matrices and apply Theorem 4.3.6 to compute the MS–orbit structure for each of these matrices.

(a) Let $M_1 = 3I_2 = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$. *Thus,* $\beta_1 = \beta_2 = 3$, *and* $Ind_3(\beta_1) = Ind_3(\beta_2) = 1$. *Then,*

$$\eta_{P_1} = \gcd(\mu_{P_1}, Ind_g(\alpha_1)) = \gcd(4, 1) = 1,$$

and

$$\eta_{P_2} = \gcd(\mu_{P_2}, Ind_g(\alpha_2)) = \gcd(4, 1) = 1.$$

Therefore, M_1 yields one MS–orbit of size four in each V_{P_1} and V_{P_2}. The length of the MS–orbits in $\mathcal{O}_{P_1,P_2}$ is $i_{P_1,P_2} = \frac{16}{\gcd(3*1-1*1,\gcd(4*1,4*1))} = 8$. Thus, the number of MS–orbits in $\mathcal{O}_{P_1,P_2}$ is $\eta_{P_1,P_2} = \frac{\mu_{P_1,P_2}}{i_{P_1,P_2}} = \frac{64}{8} = 8$. The overall MS–orbit structure in $\mathcal{O}_{m_S}$ imposed by $M_1 = 3I_2$ is

$$1 + 1[4] + 1[4] + 8[8],$$

which gives a total of $\eta_{m_S} = \eta_{P_1} + \eta_{P_2} + \eta_{P_1,P_2} = 1 + 1 + 8 = 10$ nontrivial MS–orbits.

(b) Let $M_2 = \begin{pmatrix} 3 & 0 \\ 0 & 9 \end{pmatrix}$. *Thus,* $\beta_1 = 3$, $\beta_2 = 3^2 = 9$, *and* $Ind_3(\beta_1) = 1$, $Ind_3(\beta_2) = 2$.

Then,

$$\begin{aligned} \eta_{P_1} &= \gcd(\mu_{P_1}, Ind_g(\beta_1)) = \gcd(4, 1) = 1, \\ \eta_{P_2} &= \gcd(\mu_{P_2}, Ind_g(\beta_2)) = \gcd(4, 2) = 2, \\ i_{P_1} &= \frac{\mu_{P_1}}{\eta_{P_1}} = 4, \end{aligned}$$

$$i_{P_2} = \frac{\mu_{P_2}}{\eta_{P_2}} = 2.$$

Therefore, with matrix M_2 *there are* $\eta_{P_1} = 1$, *and* $\eta_{P_2} = 2$ *nontrivial MS–orbits of sizes* 4 *and* 2 *in* $\mathcal{O}_{P_1}$ *and* $\mathcal{O}_{P_2}$, *respectively. The length of MS–orbits in* $\mathcal{O}_{P_1,P_2}$ *is* $i_{P_1,P_2} = \frac{16}{\gcd(3*1-1*2,\gcd(4*1,4*2)} = 16$, *and the number of MS–orbits in* $\mathcal{O}_{P_1,P_2}$ *is* $\eta_{P_1,P_2} = \frac{\mu_{P_1,P_2}}{i_{P_1,P_2}} = \frac{64}{16} = 4$. *Therefore, the MS–orbit structure in* $\mathcal{O}_{m_S}$ *imposed by* M_2 *is*

$$1 + 1[4] + 2[2] + 4[16],$$

and the total number of nontrivial MS–orbits is

$$\eta_{m_S} = \eta_{P_1} + \eta_{P_2} + \eta_{P_1,P_2} = 1 + 2 + 4 = 7.$$

Remark 4.3.2 *It is worth noting that, in part (a) of Example* 4.3.3, *matrix* M_1 *yields the lowest possible number of MS–orbits in* $\mathcal{O}_{P_1}$ *and* $\mathcal{O}_{P_2}$ *(i.e., one for each* $\mathcal{O}_{P_1}$ *and* $\mathcal{O}_{P_2}$*). However, the number of MS–orbits in* $\mathcal{O}_{P_1,P_2}$, $\eta_{P_1,P_2} = 8$, *is larger than the lowest possible value which is* $\frac{\mu_{P_1,P_2}}{p-1} = \frac{64}{16} = 4$. *On the other hand, matrix* M_2 *in part (b), achieves the largest possible MS–orbit in* $\mathcal{O}_{P_1,P_2}$, *nonetheless, the number of MS–orbits in* $\mathcal{O}_{P_2}$ *is not one, which is the smallest possible value; but the overall number of MS–orbits* η_{m_S} *is less than that of part (a).*

Example 4.3.3 shows that it is not always the case that, given a nonsingular matrix S with two distinct eigenvalues, the matrix $M = gI_2$, g a primitive of Z_p, is optimal for S (this is the Auslander's method.) This justifies the search for optimal matrices for which the total number of nontrivial MS–orbits, $\eta_{m_S} = \eta_{P_1} + \eta_{P_2} + \eta_{P_1,P_2}$, is minimal.

Recall that by Corollary 2.2.7, given S with two distinct eigenvalues, any matrix M that commutes with S can be written as $A \begin{pmatrix} \beta_1 & 0 \\ 0 & \beta_2 \end{pmatrix} A^{-1}$ for some nonsingular matrix A, where g is a generator of Z_p^* and $\beta_i = g^{t_i}$ for some integer t_i. Hence, η_{m_S} depends on t_1 and t_2 and for this reason we denote η_{m_S} by $\eta_{m_S}(t_1, t_2)$.

Given two distinct nonzero values λ_1 and λ_2 from Z_p, Algorithm 4.3.1 examines all possible pairs $(t_1', t_2') \in Z_p^* \times Z_p^*$ and returns a pair (t_1, t_2) such that $\eta_{m_S}(t_1, t_2)$ is minimal, where $m_S(x) = P_1(x)P_2(x)$, $P_i(x) = x - \lambda_i$, $i = 1, 2$.

All quantities in Algorithm 4.3.1 are computed according to one of the following formulas. For $r = 1, 2$,

$$\begin{array}{lcllcl} k_{P_r} & = & \frac{p-1}{\gcd(p-1, \mathrm{Ind}_{g(\lambda_r)})}, & k_{P_1,P_2} & = & \mathrm{lcm}(k_{P_1}, k_{P_2}), \\ \mu_{P_r} & = & \frac{p-1}{k_{P_r}}, & \mu_{P_1,P_2} & = & \mu_{P_1}\mu_{P_2}\gcd(k_{P_1}, k_{P_2}), \\ e_r & = & \frac{\mathrm{lcm}(\mathrm{Ind}_{g(\lambda_1)}, \mathrm{Ind}_{g(\lambda_2)})}{\mathrm{Ind}_{g(\lambda_r)}}, & \eta'_{P_r} & = & \gcd(\mu_{P_r}, t'_r), \end{array}$$

and

$$\eta'_{P_1,P_2} = \frac{\mu_{P_1,P_2}}{p-1}\gcd(e_1t'_1 - e_2t'_2, \gcd(k_{P_1}\eta'_{P_1}, k_{P_2}\eta'_{P_2})).$$

Algorithm 4.3.1

Inputs: (λ_1, λ_2), *prime* p, *and generator* g *of* Z_p^*.

Output: (t_1, t_2) *such that* $\eta_{m_S}(t_1, t_2)$, *is minimal.*

Assumption: *Precomputed log and antilog tables with respect to a primitive element* $g \in Z_p^*$ *are available.*

1. *compute* $k_{P_1}, k_{P_2}, k_{P_1,P_2}$;
2. *compute* e_1, e_2;
3. *compute* $\mu_{P_1}, \mu_{P_2}, \mu_{P_1,P_2}$;
4. *initialize* t_1, t_2 *to* $p - 1$;
5. *initialize* $\eta_{P_1}, \eta_{P_2}, \eta_{P_1,P_2}, \eta_{m_S}$ *to* p^2;

for$(t'_1 = 1$ *to* $t'_1 = p - 1)$ **do**

  compute η'_{P_1};

  for$(t'_2 = 1$ *to* $t'_2 = p - 1)$ **do**

    compute $\eta'_{P_2}, \eta'_{P_1,P_2}$;

    $\eta'_{m_S} \leftarrow \eta'_{P_1} + \eta'_{P_2} + \eta'_{P_1,P_2}$;

    if$(\eta'_{m_S} < \eta_{m_S})$

      $(t_1, t_2) \leftarrow (t'_1, t'_2)$;

      $(\eta_{P_1}, \eta_{P_2}, \eta_{P_1,P_2}, \eta_{m_S}) \leftarrow (\eta'_{P_1}, \eta'_{P_2}, \eta'_{P_1,P_2}, \eta'_{m_S})$;

if$(\eta_{m_S} = 2 + \frac{\mu_{P_1,P_2}}{p-1}$ $)$ //*Best case*

STOP

return (t_1, t_2)

The complexity of Algorithm 4.3.1 is as follows. Steps 1, 2, and 3 cost $O(\log p)$ since a constant number of *greatest common divisor* operations are performed. Steps 4 and 5 cost constant time.

On the other hand, the two nested **for** loops contain several greatest common divisor mod p operations inside them, which can be computed in $\log p$ arithmetic operations. Hence, this part of the algorithm costs $O(p^2 \log p)$. Therefore, the complexity of Algorithm 4.3.1 is $O(p^2 \log p)$.

Theorem 4.3.7 *Let $S \in \mathcal{M}_2$ be nonsingular with $m_S(x) = P_1(x)P_2(x)$, where $P_1(x) = x - \lambda_1$ and $P_2(x) = x - \lambda_2$, $\lambda_1 \neq \lambda_2$. Let (t_1, t_2) be such that $\eta_{m_S}(t_1, t_2)$ is minimal. Then, an optimal matrix M for S is $M = c_1 S + c_0 I_2$, where $c_1 = \frac{g^{t_1} - g^{t_2}}{\lambda_1 - \lambda_2}$ and $c_0 = g^{t_1} - c_1\lambda_1$.*

Proof
Clearly, Algorithm 4.3.1 examines all pairs $(t_1', t_2') \in Z_p^* \times Z_p^*$ and selects one pair (t_1, t_2) for which $M' = \begin{pmatrix} g^{t_1} & 0 \\ 0 & g^{t_2} \end{pmatrix}$ is optimal for $S' = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_1 \end{pmatrix}$. On the other hand, by Corollary 2.2.7, there is a polynomial $Q(x) = c_1 x + c_0$ such that $Q(S') = M'$ (equivalently, $Q(S) = M$). Hence,

$$\begin{pmatrix} c_1\lambda_1 + c_0 & 0 \\ 0 & c_1\lambda_2 + c_0 \end{pmatrix} = \begin{pmatrix} g^{t_1} & 0 \\ 0 & g^{t_2} \end{pmatrix} \tag{4.18}$$

if and only if

$$\begin{aligned} c_1\lambda_1 + c_0 &= g^{t_1} \\ c_1\lambda_2 + c_0 &= g^{t_2}. \end{aligned}$$

Solving this last system of equations we arrive at $c_1 = \frac{g^{t_1} - g^{t_2}}{\lambda_1 - \lambda_2}$ and $c_0 = g^{t_1} - c_1\lambda_1$.$\diamondsuit$

We summarize the results for, given a nonsingular matrix S, choosing an optimal matrix M in the two–dimensional cases in the following

Algorithm 4.3.2

Inputs: *prime p, nonsingular $S \in \mathcal{M}_2$, and primitive polynomial $P(x) = x^2 + ax + b$ over Z_p.*

Output: *optimal matrix M*

1. *compute $\phi_S(x) = x^2 + cx + d$;*
2. *compute the roots of $\phi_S(x)$;*
3. *compute $m_S(x)$;*

I. If $\phi_S(x)$ is irreducible,

   1. *compute c_1 and c_0 such that $c_1^2 = \frac{a^2-4b}{c^2-4d} \ (mod\ p)$ and $c_0 = 2^{-1}(c_1 c - a) \ (mod\ p)$;*
   2. *set $M = c_1 S + c_0 I_2$.*

II. If $m_S(x) = x - \lambda$, set $M = \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$.

III. If $m_S(x) = (x - \lambda)^2$, set $M = gI_2$.

IV. If $m_S(x) = (x - \lambda_1)(x - \lambda_2)$, $\lambda_1 \neq \lambda_2$,

   1. *compute (t_1, t_2) such that $\eta_{m_S}(t_1, t_2)$ is minimal;*
   2. *compute*

$$\begin{aligned} c_1 &= \frac{g^{t_1} - g^{t_2}}{\lambda_1 - \lambda_2}, \\ c_0 &= g^{t_1} - c_1 \lambda_1; \end{aligned}$$

   3. *set $M = c_1 S + c_0 I_2$.*

end

In order to implement Algorithm 4.3.2, we make use of a precomputed table of quadratic primitive polynomials. It is well known [25] that for any n–degree primitive polynomial $P(x)$ over Z_p, the constant $(-1)^n P(0)$ is a generator g of the multiplicative cyclic group of Z_p. Thus, having a precomputed table of primitive polynomials also gives us generators for the cyclic group Z_p^*. Now it is easy to show that, assuming the availability of primitive polynomials as well as a log and anti–log tables for Z_p^*, each step of the algorithm takes either constant or $O(p)$ time, except for step IV which is of $O(p^2 \log p)$.

The characteristic polynomial $\phi_S(x)$ can be computed in constant time and its roots can be determined in time $O(p)$. The computation of $m_S(x)$ cost constant time since we already have the roots of $\phi_S(x)$.

The primitive polynomial in steps I and II can be found by table lookup and thus, it requires time $O(p)$ (or $O(\log p)$ time using binary search for tables with a very large number of primitive polynomials).

The calculation of c_1^2, c_0, and M in step I can be done in constant time. Now, since $\mathrm{Ind}_g(c_1) = \frac{\mathrm{Ind}_g(c_1^2)}{2}$, substep 2 also requires constant time. Hence the overall complexity for step I is constant.

The calculation of M in step IV requires time $O(p^2(\log(p))$ according to the time complexity of Algorithm 4.3.1.

Example 4.3.4 *Let* $S = \begin{pmatrix} 82 & 77 \\ 296 & 316 \end{pmatrix}$ *over* Z_{379}. *The minimal polynomial of* S *is* $m_S(x) = P_1(x)P_2(x)$, *where* $P_1(x) = x - 11$ *and* $P_2(x) = x - 8$. *A primitive element for* Z_{379}^* *is* $g = 2$. *Assume we have a table of indexes with respect to* $g = 2$. *Hence,* $Ind_2(11) = 217$ *and* $Ind_2(8) = 3$. *By Lemma 2.3.3, the orders of* P_1 *and* P_2 *respectively, are*

$$\begin{aligned} k_{P_1} &= \tfrac{378}{\gcd(378,217)} = 54, \text{ and} \\ k_{P_2} &= \tfrac{378}{\gcd(378,3)} = 126 \end{aligned}$$

Thus, $k_{P_1,P_2} = lcm(54, 126) = 378$, $\mu_{P_1} = \frac{378}{54} = 7$, *and* $\mu_{P_2} = \frac{378}{126} = 3$, $\mu_{P_1,P_2} = \mu_{P_1}\mu_{P_2}\gcd(k_{P_1}, k_{P_2}) = 7 \cdot 3 \cdot \gcd(54, 126) = 378$. *Also,*

$$\begin{aligned} e_1 &= \tfrac{lcm(Ind_2(11),Ind_2(8))}{Ind_2(11)} = 3, \text{ and} \\ e_2 &= \tfrac{lcm(Ind_2(11),Ind_2(8))}{Ind_2(8)} = 217. \end{aligned}$$

A pair (t_1, t_2)*, which is the result of running Algorithm 4.3.1 on the input* $\lambda_1 = 11$, $\lambda_2 = 8$, *and prime* $p = 379$, *that minimizes* $\eta_{m_S} = \eta_{P_1} + \eta_{P_2} + \eta_{P_1,P_2}$ *is* $(t_1, t_2) = (1, 2)$. *Then,* $q_1(x) = x - \beta_1 = x - 2^1 = x - 2$, $q_2(x) = x - \beta_2 = q_2(x) = x - 2^2 = q_2(x) = x - 4$, $k_{q_1} = \frac{378}{\gcd(378,1)} = 378$, *and* $k_{q_2} = \frac{378}{\gcd(378,2)} = 189$.

Now, let us apply Theorem 4.3.6 to compute the MS–orbit structure in $\mathcal{O}_{m_S}$. $i_{P_1} = \frac{378}{\gcd(54,378)} = 7$, $i_{P_2} = \frac{189}{\gcd(126,189)} = 3$. *Thus,* $\eta_{P_1} = \frac{7}{7} = 1$, $\eta_{P_2} = \frac{3}{3} = 1$, *and*

$$\begin{aligned} i_{P_1,P_2} &= \frac{378}{\gcd(3 \cdot 1 - 217 \cdot 2, gcd(54 \cdot 1, 126 \cdot 1))} = 378, \\ \eta_{P_1,P_2} &= \frac{\mu_{P_1,P_2}}{i_{P_1,P_2}} = \frac{378}{378} = 1. \end{aligned}$$

Then, the optimal MS–orbit structure in $\mathcal{O}_{m_S}$ *is*

$$1 + 1[7] + 1[3] + 1[378].$$

Finally, let us apply Theorem 4.3.7 to find an optimal matrix M for S. Such optimal matrix is $M = eS + fI_2$, *where* $e = \frac{g^{t_1} - g^{t_2}}{\lambda_1 - \lambda_2} = \frac{(2-4)}{(11-8)} = 252$ *and* $f = g^{t_1} - e\lambda_1 = 2 - 252 \cdot 11 = 262$. *Therefore, an optimal matrix for S is*

$$M = 252S + 262I_2 = \begin{pmatrix} 81 & 75 \\ 308 & 304 \end{pmatrix}.$$

Example 4.3.5 *Let* $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ *be defined over* Z_p. *The minimal polynomial of S is* $m_S(x) = x^2 + 1$, *which, by Theorem 2.3.14, is factorable if and only if* $p = 2$ *or p is of the form* $4t + 1$, *for some positive integer t. Applying Algorithm 4.3.2, Table* 4.3.3 *shows, for each prime p of the form* $4t+1$ *between* 5 *and* 100, *the corresponding optimal M for S. The MS–orbit structure is computed using Theorem 4.3.6 and matrix M is computed according to Theorem 4.3.7. As can be seen, the total number of nontrivial MS–orbits via M,* η_{m_S}, *is nearly half the number of nontrivial MS–orbits* η'_{m_S} *induced by the scalar matrix* gI_2, *where g is a generator of* Z_p^*.

p	*optimal* M	*MS–orbit structure*	η_{ms}	*gI$_2$–orbit structure*	η'_{ms}
5	$\begin{pmatrix} 3 & 2 \\ 3 & 3 \end{pmatrix}$	$1+2[1]+1[4]$	3	$1+2[1]+2[2]$	4
13	$\begin{pmatrix} 3 & 5 \\ 8 & 3 \end{pmatrix}$	$1+2[3]+3[12]$	5	$1+2[3]+6[6]$	8
17	$\begin{pmatrix} 6 & 12 \\ 5 & 6 \end{pmatrix}$	$1+1[4]+2[2]+4[16]$	7	$1+2[4]+8[8]$	10
29	$\begin{pmatrix} 3 & 12 \\ 17 & 3 \end{pmatrix}$	$1+2[7]+7[28]$	9	$1+2[7]+14[14]$	16
37	$\begin{pmatrix} 3 & 6 \\ 31 & 3 \end{pmatrix}$	$1+2[9]+9[36]$	11	$1+2[9]+18[18]$	20
41	$\begin{pmatrix} 21 & 12 \\ 29 & 21 \end{pmatrix}$	$1+1[10]+2[5]+10[40]$	13	$1+2[10]+20[20]$	22
53	$\begin{pmatrix} 3 & 23 \\ 30 & 3 \end{pmatrix}$	$1+2[13]+13[52]$	15	$1+2[13]+26[26]$	28
61	$\begin{pmatrix} 3 & 11 \\ 50 & 3 \end{pmatrix}$	$1+2[15]+15[60]$	17	$1+2[15]+30[30]$	32
73	$\begin{pmatrix} 15 & 51 \\ 22 & 15 \end{pmatrix}$	$1+1[18]+2[9]+18[72]$	21	$1+2[18]+36[36]$	38
89	$\begin{pmatrix} 6 & 13 \\ 76 & 6 \end{pmatrix}$	$1+1[22]+2[11]+22[88]$	25	$1+2[22]+44[44]$	46
97	$\begin{pmatrix} 15 & 26 \\ 71 & 15 \end{pmatrix}$	$1+1[24]+2[12]+24[96]$	27	$1+2[24]+48[48]$	50

Table 4.3.3 : *Non optimal scalar matrices.*

Example 4.3.6 *Let* $S = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ *be defined over* Z_p. *The minimal polynomial of* S *is* $m_S(x) = P_1(x)P_2(x)$, *where* $P_1(x) = x+1$ *and* $P_2(x) = x-1$. *Then,*

$$\lambda_1 = p-1, \quad \lambda_2 = 1, \quad k_{P_1} = 2, \quad k_{P_2} = 1,$$
$$\mu_{P_1} = \tfrac{p-1}{2}, \quad \mu_{P_2} = p-1, \quad Ind(\lambda_1) = \tfrac{p-1}{2}, \quad Ind(\lambda_2) = p-1,$$

$$e_1 = \frac{lcm(\frac{p-1}{2}, p-1)}{\frac{p-1}{2}} = 2, \; e_2 = \frac{lcm(\frac{p-1}{2}, p-1)}{p-1} = 1.$$

Thus, $\eta_{P_1} = 1$, $\eta_{P_2} = 1$, $i_{P_1,P_2} = p-1$, *and* $\eta_{P_1,P_2} = \frac{p-1}{2}$. *In this case,* $M = gI_2$ *is optimal for* S *for any prime* p *and the* MS*–orbit structure is*

$$1 + 1[\frac{p-1}{2}] + \frac{p+1}{2}[p-1].$$

Table 4.3 shows the optimal M*, the* MS*-orbit structure and the optimal number of nontrivial* MS*–orbits for primes between* 17 *and* 53.

p	*optimal* M	$\mathcal{O}_{m_S}$	η_{m_S}
17	$3I_2$	$1 + 1[8] + 9[16]$	10
19	$2I_2$	$1 + 1[9] + 10[18]$	11
23	$7I_2$	$1 + 1[11] + 12[22]$	13
29	$3I_2$	$1 + 1[14] + 15[28]$	16
31	$12I_2$	$1 + 1[15] + 16[30]$	17
37	$5I_2$	$1 + 1[18] + 19[36]$	20
41	$12I_2$	$1 + 1[20] + 21[40]$	22
43	$3I_2$	$1 + 1[21] + 22[42]$	23
47	$13I_2$	$1 + 1[23] + 24[46]$	25
53	$5I_2$	$1 + 1[26] + 27[52]$	28

Table 4.3.4 : *Optimal scalar matrices.*

4.3.4 Conjecture for an $O(p \log p)$ algorithm

As we have seen, the major expense in computing an optimal M in the two dimensional case is when $m_S(x) = (x-\lambda_1)(x-\lambda_2)$, $\lambda_1 \neq \lambda_2$, which in turn is due to the search required by Algorithm 4.3.1.

The following lemma will serve as a support for our Conjecture.

Lemma 4.3.1 *Let* $S \in \mathcal{M}_2$ *be nonsingular with* $m_S(x) = P_1(x)P_2(x)$, *where* $P_1(x) = x-\lambda_1$ *and* $P_2(x) = x-\lambda_2$, $\lambda_1 \neq \lambda_2$. *Then, there exists a pair* (t_1, t_2) *for which* $\eta_{P_1} = 1$ *and* $i_{P_1,P_2} = p-1$.

Proof
Let g be a primitive of Z_p^* and let $t_1 = 1$. Thus, by Lemma 4.2.1,

$$\eta_{P_1} = \gcd(\mu_{P_1}, \mathrm{Ind}_g(g)) = \gcd(\mu_{P_1}, 1) = 1$$

and

$$i_{P_1,P_2} = \frac{p-1}{\gcd(e_1 \cdot 1 - e_2 t_2, \gcd(k_{P_1} \cdot 1, k_{P_2}\eta_{P_2}))} = \frac{p-1}{\gcd(e_1 - e_2 t_2, \gcd(k_{P_1}, k_{P_2}\eta_{P_2}))},$$

where

$$e_r = \frac{\mathrm{lcm}(\mathrm{Ind}_g(\lambda_1), \mathrm{Ind}_g(\lambda_2))}{\mathrm{Ind}_g(\lambda_r)},\ r = 1, 2.$$

Note that $\gcd(e_1, e_2) = \gcd(e_1, -e_2) = 1$. Hence, by Dirichlet's Theorem (Theorem 2.3.9), there exist infinitely many integers t for which $e_1 + e_2 t$ is a prime. Let t' be such that $|e_1 - e_2 t'|$ is a prime not dividing k_{P_1} and let $t_2 = t' \bmod k_{P_1}$. It is easy to see that $\gcd(e_1 - e_2 t_2', \gcd(k_{P_1}, k_{P_1}\eta_{P_2})) = 1$. Therefore, $i_{P_1,P_2} = p - 1$.$\diamondsuit$

Conjecture 4.3.1 is based on a very simple *greedy strategy* that has worked very well for all examples and runs we have made so far.

Conjecture 4.3.1 *Let $S \in \mathcal{M}_2$ be nonsingular with $m_S(x) = P_1(x)P_2(x)$, where $P_1(x) = x - \lambda_1$ and $P_2(x) = x - \lambda_2$, $\lambda_1 \neq \lambda_2$. Also, let k_{P_1} and k_{P_2} be the orders of P_1 and P_2, respectively, and assume that $k_{P_1} \leq k_{P_2}$. Then, there exists a positive integer t such that $(1, t)$ minimizes η_{m_S} and the the matrix defined by $M = c_1 S + c_0 I_2$ is optimal for S, where $c_1 = \frac{g - g^t}{\lambda_1 - \lambda_2}$ and $c_0 = g - c_1\lambda_1$.*

First, note that $k_{P_1} \leq k_{P_2}$ implies that $\mu_{P_2} \leq \mu_{P_1}$. Thus, $\mu_{P_2} \leq \mu_{P_1} \leq \mu_{P_1,P_2}$. The strategy of Conjecture 4.3.1 can be explained as follows. Minimize the number of MS–orbits by getting the minimal number of MS–orbits in the two sets containing the largest number of S–orbits, V_{P_1} and V_{P_1,P_2}, and, at the same time, minimize the number of MS–orbits in V_{P_2} which contains the smallest number of MS–orbits.

That is, minimize $\eta_{m_S} = \eta_{P_1} + \eta_{P_2} + \eta_{P_1,P_2}$ by fixing η_{P_1} to be 1 and η_{P_1,P_2} to be $\frac{\mu_{P_1,P_2}}{p-1}$, and at the same time, minimize the value of η_{P_2}. By Lemma 4.3.1, it can always be achieved.

Under the assumption that Conjecture 4.3.1 is true, the complexity of Algorithm 4.3.1 would be $O(p \log p)$ since only the second **for** loop is required. In this case the complexity of Algorithm 4.3.2 would also be reduced to $O(p \log p)$.

This conjecture is also valid for the general case when the characteristic polynomial of the nonsingular $n \times n$ matrix S is the product of two distinct irreducible polynomials of degree d_1 and d_2. In this case, the complexity of Algorithm 4.2.2 would be reduced from $O(p^n \log p)$ to $O(p^d \log p)$, where $d = \max\{d_1, d_2\}$.

4.4 Three dimensional cases

The proof of Theorem 4.4.1 is similar to the one for Theorem 4.3.1 in the two dimensional cases.

Theorem 4.4.1 *Let $S \in \mathcal{M}_3$ be nonsingular. Then, the minimal polynomial of S, $m_S(x)$ can be factored according to one, and only one of the following cases:*

I. $m_S(x) = x^3 + dx^2 + ex + f$ *is irreducible over* Z_p,

II. $m_S(x) = x - \lambda$,

III. $m_S(x) = P_1(x)(x - \lambda)$, $P_1(x) = x^2 + cx + d$ *is irreducible over* Z_p,

IV. $m_S(x) = (x - \lambda_1)(x - \lambda_2)$, $\phi_S(x) = (x - \lambda_1)^2(x - \lambda_2)$, $\lambda_1 \neq \lambda_2$,

V. $m_S(x) = (x - \lambda)^3$,

VI. $m_S(x) = (x - \lambda_1)^2(x - \lambda_2)$, $\lambda_1 \neq \lambda_2$,

VII. $m_S(x) = (x - \lambda)^2$,

VIII. $m_S(x) = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$, $\lambda_i \neq \lambda_j$ $i \neq j$.

4.4.1 Three dimensional M–minimal cases: cases I and II

In this subsection we give necessary and sufficient conditions in order for a 3×3 matrix S over Z_p to be M–minimal and we show how to find such an M.

Theorem 4.4.2 *Any nonsingular $S \in \mathcal{M}_3$ is M–minimal if and only if S is scalar or has irreducible characteristic polynomial.*

Proof
Suppose S is M–minimal. Then, by Theorem 4.2.1, $m_S(x)$ is irreducible. Then, $m_S(x)$ cannot be quadratic since otherwise $\phi_S(x)$ would not be irreducible. Hence, $m_S(x)$ is either linear or cubic, i.e., either S is scalar or $\phi_S(x)$ is irreducible. Conversely, if S is scalar or $\phi_S(x)$ is irreducible and hence M–minimal.$\diamondsuit$

In general, given an $n \times n$ matrix S with irreducible characteristic polynomial, where $n \geq 3$, the construction of a maximal matrix M that commutes with S is more elusive than in the two dimensional cases. However, in the three dimensional cases we can show that, given a primitive polynomial $P(x) = x^3 + ax^2 + bx + c$ over Z_p, and a 3×3 matrix S with irreducible characteristic polynomial $\phi_S(x) = x^3 + dx^2 + ex + f$, then a matrix M that is M–minimal for S is

$$M = c_2 S^2 + c_1 S + c_0 I_3,$$

where c_0, c_1, c_2 is the solution of the system of congruences 4.19.

$$\left.\begin{aligned}
c + adfc_2^2 + d^3fc_2^3 - 2defc_2^3 + f^2c_2^3 + \\
-2afc_2c_1 - 3d^2fc_2^2c_1 + 3efc_2^2c_1 + 3dfc_2c_1^2 - fc_1^3 + \\
+bc_0 + 3dfc_2^2c_0 - 6fc_2c_1c_0 + ac_0^2 + c_0^3 &= 0 \\
\\
adec_2^2 - afc_2^2 + d^3ec_2^3 - 2de^2c_2^3 - d^2fc_2^3 + \\
+2efc_2^3 + bc_1 - 2aec_2c_1 - 3d^2ec_2^2c_1 - ec_1^3 + \\
+3e^2c_2^2c_1 + 3dfc_2^2c_1 + 3defc_2c_1^2 - 3fc_2c_1^2 + 3dec_2^2c_0 + \\
-3fc_2^2c_0 + 2ac_1c_0 - 6ec_2c_1c_0 + 3c_1c_0^2 &= 0 \\
\\
bc_2 + ad^2c_2^2 - aec_2^2 + d^4c_2^3 - 3d^2ec_2^3 + \\
+e^2c_2^3 + 2dfc_2^3 - 2adc_2c_1 - 3d^3c_2^2c_1 + 6dec_2^2c_1 + \\
-3fc_2^2c_1 + ac_1^2 + 3d^2c_2c_1^2 - 3ec_2c_1^2 - dc_1^3 + \\
+2ac_2c_0 + 3d^2c_2^2c_0 - 3ec_2^2c_0 - 6dc_2c_1c_0 + 3c_1^2c_0 + 3c_2c_0^2 &= 0
\end{aligned}\right\} \pmod{p} \quad (4.19)$$

We know of no method to solve this system of polynomial congruences. However, because of the isomorphism between representation $K_1(p^3)$ and representation $K_2(p^3)$ of a Galois field $GF(p^n)$ (see Theorem 2.2.2), we are guaranteed that a solution exists. Indeed, since c_0, c_1, c_2 is a solution of (4.19) if and only if

$$P(c_2 S^2 + c_1 S + c_0 I_3) = 0$$

and $P(x)$ is of degree 3, there are exactly three solutions. One idea is to simply use trial and error to determine one such solution c_0, c_1, c_2. We have written a program in C for this purpose. The time required for this method is $O(p^3)$.

Example 4.4.1 *The matrix*

$$S = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \tag{4.20}$$

is M–minimal over Z_p for any p since $m_S(x) = x + 1$, which is irreducible over Z_p. If, for instance, $p = 47$, then

$$M = \begin{pmatrix} 0 & 0 & 43 \\ 1 & 0 & 46 \\ 0 & 1 & 0 \end{pmatrix} \tag{4.21}$$

is optimal for S since $P(x) = x^3 + x + 4 = x^3 - 46x - 43 \pmod{47}$ is primitive over Z_{47}.

Example 4.4.2 *Let a symmetry be defined over Z_{97} by the matrix*

$$S = \begin{pmatrix} 86 & 36 & 87 \\ 43 & 8 & 90 \\ 78 & 43 & 8 \end{pmatrix}.$$

The characteristic polynomial of S is $\phi_S(x) = x^3 + 92x^2 + 3x + 96$ and this polynomial happens to be irreducible. Running our program with the primitive polynomial

$$P(x) = x^3 + x + 7,$$

we find three solutions to the system of congruences (4.19):

$$\begin{aligned} \{c_0, c_1, c_2\} &= \{14, 62, 7\}, \\ \{c_0, c_1, c_2\} &= \{38, 13, 11\}, \text{ and} \\ \{c_0, c_1, c_2\} &= \{45, 22, 79\}. \end{aligned}$$

Using the first solution, we find that a matrix M that makes S M–minimal is

$$M = 7S^2 + 62S + 14I_3 = \begin{pmatrix} 26 & 18 & 57 \\ 75 & 84 & 40 \\ 39 & 75 & 84 \end{pmatrix}.$$

4.4.2 Optimal three dimensional matrices for case III

In this subsection we find an optimal matrix M when nonsingular matrix S has minimal polynomial $m_S(x) = P_1(x)(x - \lambda)$, where $P_1(x)$ is a quadratic irreducible polynomial. Theorem 4.4.3 outlines the procedure to compute such an optimal M for S, which in turn depends on the output of Algorithm 4.4.1.

Let $S \in \mathcal{M}_3$ be such that $m_S(x) = P_1(x)(x - \lambda)$, where $P_1(x) = x^2 + cx + d$ is irreducible and $\lambda \in Z_p^*$. Recall from Remark 4.2.1 that the minimal number of MS–orbits η_{m_S} depends on some positive integers t_1 and t_2 and that we write $\eta_{m_S}(t_1, t_2)$.

Algorithm 4.4.1 examines all possible pairs $(t_1', t_2') \in Z_{p^2}^* \times Z_p^*$ and returns a pair (t_1, t_2) for which $\eta_{m_S}(t_1, t_2)$ is minimal.

Algorithm 4.4.1

Inputs: *prime p, primitive polynomial $P(x) = x^2 + ax + b$ over Z_p,*
irreducible polynomial $P_1(x) = x^2 + cx + d$ and
$P_2(x) = x - \lambda$, $\lambda \neq 0 \in Z_p$

Output: *(t_1, t_2) such that $\eta_{m_S}(t_1, t_2)$ is minimal.*

1. *compute c_0, c_1;*
2. *set $N = c_1 C_{P_1} + c_0 I_2$.*
3. *compute $e_1, e_2, k_{P_1}, k_{P_2}, k_{P_1,P_2}, \mu_{P_1}, \mu_{P_2}, \mu_{P_1,P_2}$;*
4. *Initialize t_1, t_2 to p^2;*
5. *Initialize $\eta_{P_1}, \eta_{P_2}, \eta_{P_1,P_2}, \eta_{m_S}$ to p^3;*
6. **for**$(t_1' = 1$ *to* $t_1' = p^2 - 1)$ **do**
   compute η_{P_1}';
   for$(t_2' = 1$ *to* $t_2' = p - 1)$ **do**
   compute $\eta_{P_2}', \eta_{P_1,P_2}'$;

$\eta'_{m_S} \leftarrow \eta'_{P_1} + \eta'_{P_2} + \eta'_{P_1,P_2}$.
if$(\eta'_{m_S} < \eta_{m_S})$
$(\eta_{P_1}, \eta_{P_2}, \eta_{P_1,P_2}) \leftarrow (\eta'_{P_1}, \eta'_{P_2}, \eta'_{P_1,P_2})$.
$(t_1, t_2) \leftarrow (t'_1, t'_2)$.
return (t_1, t_2)

Let $P(x) = x^2 + ax + b$ be the primitive polynomial of Algorithm 4.4.1. By Theorem 4.3.4 $N = c_1 S + c_0 I_2$ is a maximal matrix that commutes with S, where $c_1^2 = \frac{a^2-4b}{c^2-4d}$ and $c_0 = 2^{-1}(c_1 c - a)$. Hence, $\mathrm{Ind}_g(c_1) = \frac{\mathrm{Ind}_g(c_1^2)}{2}$ and so $c_1 = g^{\mathrm{Ind}_g(c_1)}$.

The remaining quantities in Algorithm 4.4.1 are computed according to the formulas given in Theorem 4.2.4 as follows:

$$\begin{array}{llll}
k_{P_1} = \frac{p^2-1}{\gcd(p^2-1, \mathrm{Ind}_N(C_{P_1}))}, & & k_{P_2} = \frac{p-1}{\gcd(p-1, \mathrm{Ind}_g(\lambda))}, & \\
k_{P_1,P_2} = \mathrm{lcm}(k_{P_1}, k_{P_2}), & & \mu_{P_1} = \frac{p^2-1}{k_{P_1}}, & \\
\mu_{P_2} = \frac{p-1}{k_{P_2}}, & & \mu_{P_1,P_2} = \mu_{P_1}\mu_{P_2}\gcd(k_{P_1}, k_{P_2}), & \\
e_1 = \frac{\mathrm{lcm}(\mathrm{Ind}_N(C_{P_1}), (p+1)\mathrm{Ind}_g(\lambda))}{\mathrm{Ind}_N(\mathrm{Ind}_N(C_{P_1}))}, & & e_2 = \frac{\mathrm{lcm}(\mathrm{Ind}_N(C_{P_1}), (p+1)\mathrm{Ind}_g(\lambda))}{(p+1)(\mathrm{Ind}_g(\lambda))}, & \\
\eta'_{P_1} = \gcd(\mu_{P_1}, t'_1), & & \eta'_{P_2} = \gcd(\mu_{P_2}, t'_2), &
\end{array}$$

and

$$\eta'_{P_1,P_2} = \frac{\mu_{P_1,P_2}}{p^2-1}\gcd(e_1 t'_1 - (p+1)e_2 t'_2, \gcd(k_{P_1}\eta'_{P_1}, k_{P_2}\eta'_{P_2}(p+1))).$$

Assuming we have a table of primitive polynomials as well as logs and antilogs tables for Z_p^*, the complexity of Algorithm 4.4.1 is as follows. The cost of Steps 1, 2, 4, and 5 is constant. Now, in order to compute quantities in step 3 we need the index of C_{P_1} with respect to N. For this, we make succesive multiplications of N by itself. Thus, step 3 costs $O(p^2)$ time. The cost of the inner **for** loop is $O(p \log p)$ time since some gcd operations are executed $p-1$ times. Thus, step 6 costs $O(p^2 \cdot p \log p) = O(p^3 \log p)$ time. Therefore, the complexity of the overall algorithm is $O(p^3 \log p)$.

Theorem 4.4.3 *Let $S \in \mathcal{M}_3$ be nonsingular with $m_S(x) = P_1(x)P_2(x)$, where $P_1(x) = x^2 + cx + d$ is irreducible and $P_2(x) = x - \lambda$. Let (t_1, t_2) be such that $\eta_{m_S}(t_1, t_2)$ is minimal. Then, there exists a maximal matrix $N \in \mathcal{N}(C_{P_1})$ such that*

$$M = c_2 S^2 + c_1 S + c_0 I_3$$

is optimal for S, where

$$\begin{aligned} c_2 &= (d^{-1}\lambda u_{12} + g^{t_2} - u_{11})P_1(\lambda)^{-1}, \\ c_1 &= cc_2 - d^{-1}u_{12}, \\ c_0 &= u_{11} + c_2 d, \\ N^{t_1} &= \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}, \\ g & \quad \textit{is a generator of } Z_p^*. \end{aligned}$$

Proof
Let $P(x) = x^2 + ax + b$ and $N \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}$ be the primitive polynomial and the maximal matrix from Algorithm 4.4.1, respectively. Now, since $\eta_{m_S}(t_1, t_2)$ is minimal, then $M' = \begin{pmatrix} N^{t_1} & 0 \\ 0 & g^{t_2} \end{pmatrix}$ is optimal for $S' = \begin{pmatrix} C_{P_1} & 0 \\ 0 & \lambda \end{pmatrix}$.

On the other hand, by Theorem 2.2.6, there is a polynomial $Q(x) = c_2x^2 + c_1x + c_0$, for which $Q(S') = M'$, since S' is nonderogatory. Hence,

$$\begin{aligned} c_2 C_{P_1}^2 + c_1 C_{P_1} + c_0 I_2 &= N^{t_1} \\ c_2\lambda^2 + c_1\lambda + c_0 I_2 &= g^{t_2}. \end{aligned}$$

Recalling that $P_1(C_{P_1}) = \mathbf{0}$, the 2×2 zero matrix, and solving for c_0, c_1, and c_2 we endup with

$$\begin{aligned} c_2 &= (d^{-1}\lambda u_{12} + g^{t_2} - u_{11})P_1(\lambda)^{-1}, \\ c_1 &= cc_2 - d^{-1}u_{12}, \\ c_0 &= u_{11} + c_2 d. \end{aligned}$$

Finally, let A be the nonsingular matrix of Theorem 2.2.5, for which $A^{-1}SA = S'$ and set $M = AQ(S')A^{-1} = Q(S)$.$\diamondsuit$

Example 4.4.3 *Let us consider the symmetry S over Z_r defined by the unimodular matrix*

$$S = \begin{pmatrix} -1 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

The whole action of S in $Z_r^3 = Z_r \times Z_r \times Z_r$ is given by

$$(x, y, z) \to (y - x, -x, z) \to (y - x, -x, z).$$

This particular transformation is known as the point group P_3, according to the terminology and notation used by crystallographers. The minimal polynomial of S is $m_S(x) = P_1(x)P_2(x)$, where $P_1(x) = x^2 + x + 1$ and $P_2(x) = (x - 1)$. Moreover, S is similar to $\begin{pmatrix} C_{P_1} & 0 \\ 0 & 1 \end{pmatrix}$, where $C_{P_1} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ is the companion matrix associated to $P_1(x)$.

Let us assume that $r = p$ is a prime. Table 1 shows the values of $p \leq 359$ for which $P_1(x)$ is irreducible.

2	5	11	17	23	29	41	47	53	59	71	89
107	113	131	137	149	167	173	179	191	197	227	233
239	251	257	263	269	281	293	311	317	347	353	359

Table 4.4.1 : *Primes for which $P_1(x) = x^2 + x + 1$ is irreducible.*

For instance, $P_1(x) = x^2 + x + 1$ is irreducible over Z_5 (i.e., $r = 5$). In order to find a maximal matrix N that commutes with C_{P_1}, we need a primitive polynomial over Z_5. Such primitive polynomial is $P(x) = x^2 + x + 2$. By Theorem 4.3.4, *$N = c_1 C_{P_1} + c_0 I_2$, where $c_1^2 = \frac{a^2 - 4*b}{c^2 - 4*d}$ and $c_0 = 2^{-1}(c_1 c - a)$. Then,*

$$c_1^2 = \frac{1^2 - 4 * 2}{1^2 - 4 * 1} = \frac{3}{-3} = -1 = 4 \ (mod\ 5) \tag{4.22}$$

Hence, $c_1 = 2$ or $c_1 = -2 = 3$ mod 5. Let us take $c_1 = 2$. Thus, $c_0 = 2^{-1}(2 * 1 - 1) = 3 * 1 = 3$ and so,

$$N \ = \ 2C_{P_1} + 3I_2 = \begin{pmatrix} 3 & 3 \\ 2 & 1 \end{pmatrix}.$$

By repeated multiplication of N by itself, we find that $Ind_N(C_{P_1}) = 8$. Now, since $\lambda = 1$, $Ind_2(\lambda) = p - 1 = 4$. Hence, by Lemma 2.3.3, *$k_{P_1} = \frac{5^2 - 1}{\gcd(5^2 - 1, 8)} = 3$, and $k_{P_2} = \frac{5 - 1}{\gcd(5 - 1, 4)} = 1$. Also, $\mu_{P_1} = \frac{p^2 - 1}{k_{P_1}} = \frac{25 - 1}{3} = 8$, $\mu_{P_2} = \frac{p - 1}{k_{P_2}} = \frac{5 - 1}{1} = 4$,*

$\mu_{P_1,P_2} = \mu_{P_1}\mu_{P_2}\gcd(k_{P_1}, k_{P_2}) = 8 * 4 * 1 = 32$, *and*

$$\begin{aligned} e_1 &= \tfrac{lcm(8,6*4)}{8} &&= 3 \\ e_2 &= \tfrac{lcm(8,6*4)}{6*4} &&= 1 \\ \eta_{P_1} &= \gcd(\mu_{P_1}, t_1) &&= \gcd(8, t_1) \\ \eta_{P_2} &= \gcd(\mu_{P_2}, t_2) &&= \gcd(4, t_2). \end{aligned}$$

Thus,

$$\begin{aligned} \eta_{P_1,P_2} &= \tfrac{(p-1)\gcd(e_1t_1-(p+1)e_2t_2, \gcd(k_{P_1}\eta_{P_1}, (p+1)k_{P_2}\eta_{P_2}))}{lcm_{(k_{P_1},k_{P_2})}} \\ &= \tfrac{4\gcd(3t_1-6t_2, \gcd(3\eta_{P_1}, 6\eta_{P_2}))}{lcm_{(3,1)}} \\ &= 4\gcd(t_1 - 2t_2, \gcd(\eta_{P_1}, 2\eta_{P_2})) \end{aligned}$$

Algorithm 4.4.1 *will return a pair* $(t_1, t_2) \in Z_{25}^* \times Z_5^*$ *such that*

$$\begin{aligned} \eta_{m_S}(t_1, t_2) &= \eta_{P_1} + \eta_{P_2} + \eta_{P_1,P_2} \\ &= \gcd(8, t_1) + \gcd(4, t_2) + 4\gcd(t_1 - 2t_2, \gcd(\gcd(8, t_1), 2\gcd(4, t_2))) \\ &= \gcd(8, t_1) + \gcd(4, t_2) + 4\gcd(t_1 - 2t_2, 8, t_1, 2t_2) \end{aligned}$$

is minimal. One such a pair (t_1, t_2) *is* $(1, 1)$. *Thus, the minimal number of nontrivial* MS*–orbits is* $\eta_{m_S}(t_1, t_2) = 1 + 1 + 4 = 6$.

Now, applying Theorem 4.4.3, *we compute* $c_2 = 4$, $c_1 = 1$, *and* $c_0 = 2$. *Therefore, an optimal matrix* M *for* S *is*

$$M = 4S^2 + S + 2I_3 = \begin{pmatrix} 1 & 2 & 0 \\ 3 & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

and the optimal MS*–orbit structure is*

$$\eta_{m_S} = 1 + 1[8] + 1[4] + 4[8] = 1 + 1[4] + 5[8].$$

4.4.3 Optimal three dimensional matrices for case IV

Let S be a nonsingular 3×3 matrix over Z_p with two distinct eigenvalues λ_1 and λ_2 and minimal polynomial $m_S(x) = P_1(x)^2P_2(x)$, where $P_1(x) = x - \lambda_1$, $P_2(x) = x - \lambda_2$,

and λ_1 has multiplicity two (this is equivalent to saying that $\phi_S(x) = P_1(x)^2 P_2(x)$). By Lemma 2.2.6, if $M \in \mathcal{N}(S)$ is nonsingular, then $\phi_M(x) = -q_1(x)q_2(x)$, where $q_1(x)$ is some monic quadratic polynomial and $q_2(x) = x - \beta$, for some $\beta \in Z_p^*$. Since $q_1(x)$ has degree two, it falls into one and only one of the following cases:

1. $q_1(x) = (x - \alpha)^2$,
2. $q_1(x)$ is irreducible,
3. $q_1(x) = (x - \alpha_1)(x - \alpha_2)$, $\alpha_1 \neq \alpha_2$,
4. $q_1(x) = x - \alpha$.

Theorems 4.4.4 and 4.4.5 determine the MS–orbit structure for cases 1 and 2, respectively. Remark 4.4.1, at the end of this section, will show that cases 3 and 4 cannot yield optimal matrices for this type of matrices S. Henceforth, we will not compute MS–orbit structure for this cases.

Theorem 4.4.4 *Let $S \in \mathcal{M}_3$ be nonsingular with $\phi_S(x) = P_1(x)^2 P_2(x)$ and $m_S(x) = P_1(x)P_2(x)$, where $P_1(x) = x - \lambda_1$ and $P_2(x) = x - \lambda_2$. Then there exists a nonsingular matrix $M \in \mathcal{N}(S)$ such that $m_M(x) = q_1(x)^2 q_2(x)$, where $q_1(x) = x - \alpha$ and $q_2(x) = x - \beta$. Also, let $\sum \mathcal{O}_{P_1}$ and $\sum \mathcal{O}_{P_1,P_2}$ be the formal sums of nontrivial MS–orbits in $\mathcal{O}_{P_1}$ and $\mathcal{O}_{P_1,P_2}$, respectively. Then, the MS–orbit structure is*

$$1 + \sum \mathcal{O}_{P_1} + \sum \mathcal{O}_{P_1,P_2} + \eta_{P_2}[i_{P_2}],$$

where

$$\begin{aligned}
\textstyle\sum \mathcal{O}_{P_1} &= \eta_{P_1,0}[i_{P_1,0}] + \eta_{P_1,0}[p \cdot i_{P_1,0}], \\
\textstyle\sum \mathcal{O}_{P_1,P_2} &= \eta_{P_1,P_2,1}[i_{P_1,P_2,1}] + \eta_{P_1,P_2,1}[p \cdot i_{P_1,P_2,1}], \\
i_{P_1,0} &= \tfrac{k_{q_1}}{\gcd(k_{P_1},k_{q_1})}, \\
\eta_{P_1,0} &= \tfrac{p-1}{k_{P_1} i_{P_1,0}}, \\
i_{P_2} &= \tfrac{k_{q_2}}{\gcd(k_{P_2},k_{q_2})}, \\
\eta_{P_2} &= \tfrac{p-1}{k_{P_2} i_{P_2}}, \\
i_{P_1,P_2,1} &= \tfrac{p-1}{\gcd(e_1 Ind_g(\alpha) - e_2 Ind_g(\beta), \gcd(k_{P_1}\eta_{P_1,0}, k_{P_2}\eta_{P_2}))}, \\
\eta_{P_1,P_2,1} &= \tfrac{(p-1)^2}{lcm(k_{P_1},k_{P_2}) i_{P_1,P_2,1}}.
\end{aligned}$$

Proof
First, let us show that such matrix M does exist. Now, since $\phi_S(x) = (x-\lambda_1)^2(x-\lambda_2)$ and $m_S(x) = (x-\lambda_1)(x-\lambda_2)$, with $\lambda_1 \neq \lambda_2$, then matrix S is similar to $\begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{pmatrix}$. Let N be any nonsingular matrix that commutes with S. Thus, by Lemma 2.2.6, $\phi_N(x) = -q(x)(x-\beta)$, for some monic quadratic polynomial $q(x)$ and some nonzero $\beta \in Z_p$. Thus, the M of the theorem is simply a special case of this result. In order to compute the MS–orbit structure we compute the $M'S'$–orbit structure, where M and S are similar to M' and S', respectively, and $M'S' = S'M'$. For this case, $S' = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{pmatrix}$ and $M' = \begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \beta \end{pmatrix}$.

Second, let us define

$$
\begin{aligned}
V_{P_1} &= \{\mathbf{x} \in Z_p^3 | P_1(S')\mathbf{x} = \mathbf{0}\} = \{\begin{pmatrix} x_0 \\ x_1 \\ 0 \end{pmatrix} | x_0, x_1 \in Z_p\}, \\
V_{P_2} &= \{\mathbf{x} \in Z_p^3 | P_2(S')\mathbf{x} = \mathbf{0}\} = \{\begin{pmatrix} 0 \\ 0 \\ x_2 \end{pmatrix} | x_2 \in Z_p\}, \\
V_{P_1,P_2} &= V_{P_1P_2} - V_{P_1} \cup V_{P_2}, \\
U_{P_1,0} &= \{\begin{pmatrix} x_0 \\ 0 \\ 0 \end{pmatrix} | x_0 \in Z_p\}, \\
U_{P_1,1} &= V_{P_1} - U_{P_1,0}, \\
U_{P_1,P_2,0} &= V_{P_1,P_2} - (U_{P_1,1} \oplus V_{P_2}), \\
U_{P_1,P_2,1} &= V_{P_1,P_2} - U_{P_1,P_2,0}.
\end{aligned}
$$

A Venn diagram shows that, indeed, they are pairwise disjoint sets and that

$$Z_p^3 = U_{P_1,0} \cup U_{P_1,1} \cup U_{P_1,P_2,0} \cup U_{P_1,P_2,1} \cup V_{P_2}.$$

Next, let us proceed to verify that each of this sets is M'–invariant.

i. Let $\mathbf{x} \in V_{P_2}$. Then, $M'\mathbf{x} = \begin{pmatrix} 0 \\ 0 \\ \beta x_2 \end{pmatrix} \in V_{P_2}$. Moreover, there are μ_{P_2} S'–orbits in this set.

ii. Let $\mathbf{x} \in U_{P_1,0}$. Then, $M'\mathbf{x} = \begin{pmatrix} \alpha x_0 \\ 0 \\ 0 \end{pmatrix} \in U_{P_1,0}$. Moreover, there are μ_{P_1} S'–orbits in this set.

iii. Let $\mathbf{x} \in U_{P_1,1}$. Then, $\mathbf{x} = \begin{pmatrix} x_0 \\ x_1 \\ 0 \end{pmatrix}$, $x_1 \neq 0$, since $\mathbf{x} \in V_{P_1}$ but $\mathbf{x} \notin U_{P_1,0}$. Therefore, $M'\mathbf{x} = \begin{pmatrix} \alpha x_0 + x_1 \\ \alpha x_1 \\ 0 \end{pmatrix} \in U_{P_1,1}$. We can show that there are $p\mu_{P_1}$ S'–orbits in $U_{P_1,1}$.

iv. Let $\mathbf{x} \in U_{P_1,P_2,0}$. Then, $\mathbf{x} = \begin{pmatrix} x_0 \\ 0 \\ x_2 \end{pmatrix}$ with $x_0 \neq 0$ and $x_2 \neq 0$ since $\mathbf{x} \in U_{P_1,0}$ and $\mathbf{x} \in V_{P_2}$ but $\mathbf{x} \notin U_{P_1,1}$. Therefore, $M'\mathbf{x} = \begin{pmatrix} \alpha x_0 \\ 0 \\ \beta x_2 \end{pmatrix} \in U_{P_1,P_2,0}$. There are $\mu_{P_1}\mu_{P_2}\gcd(k_{P_1}, k_{P_2})$ S'–orbits in $U_{P_1,P_2,0}$.

v. Let $\mathbf{x} \in U_{P_1,P_2,1}$. Then, $\mathbf{x} = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$ with $x_1 \neq 0$ and $x_2 \neq 0$ since $\mathbf{x} \in U_{P_1,1}$ and $\mathbf{x} \in V_{P_2}$ but $\mathbf{x} \notin U_{P_1,0}$. Therefore, $M'\mathbf{x} = \begin{pmatrix} \alpha x_0 + \alpha x_1 \\ \alpha x_1 \\ \beta x_2 \end{pmatrix} \in U_{P_1,P_2,1}$. There are $p \cdot \mu_{P_1}\mu_{P_2}\gcd(k_{P_1}, k_{P_2})$ S'–orbits in $U_{P_1,P_2,1}$.

In what follows, we will find the length as well as the number of $M'S'$–orbits for each $U_{P_1,0}$, $U_{P_1,1}$, $U_{P_1,P_2,0}$, and $U_{P_1,P_2,1}$. In order to do so, we find the smallest positive integer i which solves

$$S'^j\mathbf{x} = M'^i\mathbf{x} \tag{4.23}$$

for some j and all $\mathbf{x}$ in each of the underlying sets.

i. If $\mathbf{x} \in V_{P_2}$. Thus, $\mathbf{x} = \begin{pmatrix} 0 \\ 0 \\ x_2 \end{pmatrix}$ with $x_2 \neq 0$. Hence, equation (4.23) becomes

$$\lambda_2^j = \beta^i \tag{4.24}$$

Thus, the length of the $M'S'$–orbits in V_{P_2} is $i_{P_2} = \frac{k_{q_2}}{\gcd(k_{P_2}, k_{q_2})}$, and the number of $M'S'$–orbits is $\eta_{P_2} = \frac{\mu_{P_2}}{i_{P_2}} = \frac{p-1}{k_{P_2} i_{P_2}}$.

ii. If $\mathbf{x} \in U_{P_1,0}$. Thus, $\mathbf{x} = \begin{pmatrix} x_0 \\ 0 \\ 0 \end{pmatrix}$. For this case, equation (4.23) is equivalent to

$$\lambda_1^j = \alpha^i. \tag{4.25}$$

So, $i_{P_1,0} = \frac{k_{q_1}}{\gcd(k_{P_1},k_{q_1})}$, and $\eta_{P_1,0} = \frac{\mu_{P_1}}{i_{P_1,0}} = \frac{p-1}{k_{P_1} i_{P_1,0}}$.

iii. If $\mathbf{x} \in U_{P_1,1}$, $\mathbf{x} = \begin{pmatrix} x_0 \\ x_1 \\ 0 \end{pmatrix}$ with $x_1 \neq 0$. Equation (4.23) is equivalent to

$$0 = i \tag{4.26}$$
$$\lambda_1^j = \alpha^i. \tag{4.27}$$

Thus, equation (4.26) implies that $i_{P_1,1}$ is a multiple of p. Also, equation (4.27) implies that $i_{P_1,1}$ is a multiple of $i_{P_1,0}$. Hence, the smallest positive integer is $i_{P_1,1} = \mathrm{lcm}(p,\ i_{P_1,0}) = p \cdot i_{P_1,0}$. Then, the number of $M'S'$–orbits is $\eta_{P_1,1} = \frac{p \cdot \mu_{P_1}}{i_{P_1,1}} = \frac{p-1}{k_{P_1} i_{P_1,0}}$.

iv. If $\mathbf{x} \in U_{P_1,P_2,0}$, $\mathbf{x} = \begin{pmatrix} x_0 \\ 0 \\ x_2 \end{pmatrix}$ with $x_1 \neq 0$. Equation (4.23) is equivalent to

$$\lambda_1^j = \alpha^i \tag{4.28}$$
$$\lambda_2^j = \beta^i. \tag{4.29}$$

Thus,

$$i_{P_1,P_2,0} = \frac{p-1}{\gcd(e_1 \mathrm{Ind}_g(\alpha) e_2 \mathrm{Ind}_g(\beta), \gcd(k_{P_1}\eta_{P_1,0}, k_{P_2}\eta_{P_2}))},$$

and the number of $M'S'$–orbits is

$$\eta_{P_1,P_2,0} = \frac{\mu_{P_1}\mu_{P_2}\gcd(k_{P_1},k_{P_2})}{i_{P_1,i_{P_2,0}}} = \frac{(p-1)^2}{\mathrm{lcm}(k_{P_1},k_{P_2}) i_{P_1,P_2,0}}.$$

v. If $\mathbf{x} \in U_{P_1,P_2,1}$, $\mathbf{x} = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$ with $x_1 \neq 0$, $x_2 \neq 0$. Equation (4.23) is equivalent to

$$0 = i \tag{4.30}$$
$$\lambda_1^j = \alpha^i \tag{4.31}$$
$$\lambda_2^j = \beta^i. \tag{4.32}$$

Equation (4.30) implies that $i_{P_1,P_2,1}$ is a multiple of p. Equations (4.31) and (4.32) imply that $i_{P_1,P_2,0}$ is a multiple of $i_{P_1,P_2,0}$. Therefore,

$$i_{P_1,P_2,1} = p \cdot i_{P_1,P_2,0}.$$

The number of $M'S'$–orbits is

$$\eta_{P_1,P_2,1} = \frac{p \cdot \mu_{P_1}\mu_{P_2}\gcd(k_{P_1},k_{P_2})}{p \cdot i_{P_1,i_{P_2,0}}} = \eta_{P_1,P_2,0}. \diamondsuit$$

The following theorem determines the MS–orbit structure for case 2.

Theorem 4.4.5 *Let $S \in \mathcal{M}_3$ be nonsingular with $\phi_S(x) = P_1(x)^2 P_2(x)$ and $m_S(x) = P_1(x)P_2(x)$, where $P_1(x) = x - \lambda_1$ and $P_2(x) = x - \lambda_2$. Then there exists a nonsingular matrix $M \in \mathcal{N}(S)$ such that $m_M(x) = q_1(x)q_2(x)$, where $q_1(x) = x^2 + cx + d$ is irreducible and $q_2(x) = x - \beta$. Further, assume N is a 2×2 maximal matrix that commutes with C_{q_1}, the companion matrix of $q_1(x)$, $t_1 = Ind_N(C_{q_1})$ and $t_2 = Ind_g(\beta)$, g a generator of Z_p^*. Also, let $\sum \mathcal{O}_{P_1}$, $\sum \mathcal{O}_{P_2}$, and $\sum \mathcal{O}_{P_1,P_2}$ be the formal sums of nontrivial MS–orbits in $\mathcal{O}_{P_1}$, $\mathcal{O}_{P_2}$, and $\mathcal{O}_{P_1,P_2}$, respectively. Then, the MS–orbit structure is*

$$1 + \sum \mathcal{O}_{P_1} + \sum \mathcal{O}_{P_2} + \sum \mathcal{O}_{P_1,P_2},$$

where

$$\begin{aligned}
\textstyle\sum \mathcal{O}_{P_1} &= \eta_{P_1}[i_{P_1}], \\
\textstyle\sum \mathcal{O}_{P_2} &= \eta_{P_2}[i_{P_2}], \\
\textstyle\sum \mathcal{O}_{P_1,P_2} &= \eta_{P_1,P_2}[i_{P_1,P_2}], \\
i_{P_1} &= \tfrac{k_{q_1}}{\gcd(k_{P_1}, k_{q_1})}, \\
\eta_{P_1} &= \tfrac{p^2-1}{k_{P_1} i_{P_1}}, \\
i_{P_2} &= \tfrac{k_{q_2}}{\gcd(k_{P_2}, k_{q_2})}, \\
\eta_{P_2} &= \tfrac{p-1}{k_{P_2} i_{P_2}}, \\
i_{P_1,P_2} &= \tfrac{p^2-1}{\gcd(e_1 t_1 - (p+1)e_2 t_2, \gcd(k_{P_1}\eta_{P_1}, (p+1)k_{P_2}\eta_{P_2}))}, \\
\eta_{P_1,P_2} &= \tfrac{(p+1)(p-1)^2}{lcm(k_{P_1}, k_{P_2}) i_{P_1,P_2}}.
\end{aligned}$$

Proof

By Lemma 2.2.6, such a matrix M does exist. Moreover, since $q_1(x)$ is irreducible, there exist integers c_0 and c_1 for which $N = c_1 C_{q_1(x)} + c_0 I_2$ is a maximal matrix. Thus, the existence of t_1 is also assured. Similarly for t_2. Thus, M is similar to $M' = \begin{pmatrix} C_{q_1} & 0 \\ 0 & \beta \end{pmatrix}$. We already know that S is similar to $S' = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{pmatrix}$. Hence, the MS–orbit structure is equivalent to the $M'S'$–orbit structure, which can be determined by solving

$$S'^{ij}\mathbf{x} = M'^{ii}\mathbf{x}, \text{ for all } \mathbf{x} \in Z_p. \tag{4.33}$$

which is equivalent to

$$\begin{pmatrix} \lambda_1^j & 0 & 0 \\ 0 & \lambda_1^j & 0 \\ 0 & 0 & \lambda_2^j \end{pmatrix} = \begin{pmatrix} (N^{t_1})^i & 0 \\ 0 & (g^{t_2})^i \end{pmatrix} \tag{4.34}$$

if and only if

$$\lambda_1^j I_2 = (N^{t_1})^i \tag{4.35}$$
$$\lambda_2^j = (g^{t_2})^i. \tag{4.36}$$

Let k_{P_t} and k_{q_t}, $t = 1, 2$, be the orders of P_t and q_t, respectively. Also, let $\mu_{P_1} = \frac{p^2-1}{k_{P_1}}$, $\mu_{P_2} = \frac{p-1}{k_{P_2}}$, and $\mu_{P_1,P_2} = \mu_{P_1}\mu_{P_2}\gcd(k_{P_1}, k_{P_2})$. Thus, by Theorem 2.3.16, the smallest positive integers i_{P_1} and i_{P_2} that solves equations (4.35) and (4.36), for some integers j_1 and j_2, are

$$i_{P_1} = \frac{k_{q_1}}{\gcd(k_{P_1}, k_{q_1})}, \text{ and}$$
$$i_{P_2} = \frac{k_{q_2}}{\gcd(k_{P_1}, k_{q_2})},$$

and the number of MS–orbits in $\mathcal{O}_{P_1}$ and $\mathcal{O}_{P_2}$, respectively, are

$$\eta_{P_1} = \frac{\mu_{P_1}}{i_{P_1}} = \frac{p^2-1}{k_{P_1} i_{P_1}},$$
$$\eta_{P_2} = \frac{\mu_{P_2}}{i_{P_2}} = \frac{p-1}{k_{P_2} i_{P_2}}.$$

Now, let

$$e_1 = \frac{\text{lcm}(\text{Ind}_N(\lambda_1 I_2), (p+1)\text{Ind}_g(\lambda_2))}{\text{Ind}_N(\lambda_1 I_2)} \text{ and}$$
$$e_2 = \frac{\text{lcm}(\text{Ind}_N(\lambda_1 I_2), (p+1)\text{Ind}_g(\lambda_2))}{(p+1)\text{Ind}_g(\lambda_2)}.$$

Applying Theorem 2.3.18, the smallest positive integer i_{P_1,P_2}, for some j, that simultaneously solves equations (4.35) and (4.36) is

$$i_{P_1,P_2} = \frac{p^2-1}{\gcd(e_1 t_1 - (p+1)e_2 t_2, \gcd(k_{P_1}\eta_{P_1}, (p+1)k_{P_2}\eta_{P_2}))}.$$

Therefore, the number of MS–orbits in $\mathcal{O}_{P_1,P_2}$ is

$$\eta_{P_1,P_2} = \frac{\mu_{P_1}\mu_{P_2}\gcd(k_{P_1}, k_{P_2})}{i_{P_1,P_2}}$$
$$= \frac{(p+1)(p-1)^2}{\text{lcm}(k_{P_1}, k_{P_2}) i_{P_1,P_2}}. \diamondsuit$$

Remark 4.4.1 *It is worth noting that if $t_1 = t_2 = 1$, i.e., the companion matrix of $q_1(x)$ in Theorem 4.4.5 is a maximal matrix and β is a generator of Z_p^*, then $\eta_{P_1} = \eta_{P_2} = 1$, and*

$$\begin{aligned} i_{P_1,P_2} &= \frac{p^2-1}{\gcd(e_1-(p+1)e_2, \gcd(k_{P_1},(p+1)k_{P_2}))} \\ &= (p+1)\frac{p-1}{\gcd(e_1-(p+1)e_2, \gcd(k_{P_1},(p+1)k_{P_2}))} \\ &\geq p+1. \end{aligned}$$

Then,

$$\begin{aligned} \eta_{P_1,P_2} &\leq 1+1+\frac{\mu_{P_1,P_2}}{p+1} \\ &= 2+(p-1)\frac{p-1}{lcm(k_{P_1},k_{P_2})}. \end{aligned}$$

On the other hand, if M is as in cases 3 and 4, then the order of M, k_M, is at most $p-1$. Thus, since i_{P_1,P_2} divides k_M, then $i_{P_1,P_2} \leq p-1$. Let η'_{P_1,P_2} be the number of MS–orbits in $\mathcal{O}_{P_1,P_2}$ for cases 3 and 4. Thus,

$$\begin{aligned} \eta'_{P_1,P_2} &\geq 1+1+\frac{\mu_{P_1,P_2}}{p+1} \\ &\geq 2+\frac{(p+1)\mu_{P_1}\mu_{P_2}\gcd(k_{P_1},k_{P_2})}{p+1} \\ &\geq 2+(p+1)\frac{p-1}{lcm(k_{P_1},k_{P_2}))} \\ &\geq \eta_{P_1,P_2}. \end{aligned}$$

Therefore, if $m_M(x) = (x-\alpha_1)(x-\alpha_2)(x-\beta)$, $\alpha_1 \neq \alpha_2$, or $m_M(x) = (x-\alpha)(x-\beta)$, then M cannot be optimal for S.

As a consequence of Remark 4.4.1, we have

Theorem 4.4.6 *Let $S \in \mathcal{M}_3$ be nonsingular with $\phi_S(x) = P_1(x)^2P_2(x)$ and $m_S(x) = P_1(x)P_2(x)$, where $P_1(x) = x-\lambda_1$ and $P_2(x) = x-\lambda_2$. Then any $M \in \mathcal{N}(S)$ with $m_M(x) = (x-\alpha_1)(x-\alpha_2)(x-\beta)$, $\alpha_1 \neq \alpha_2$, or with $m_M(x) = (x-\alpha_1)(x-\beta)$ cannot be optimal for S. In particular, $M = gI_3$ cannot be optimal for S.*

Up to now, given a matrix S as described in this section, we have not been able to prove that an optimal matrix M for S should have either characteristic polynomial $\phi_M(x) = (x-\alpha)^2(x-\beta)$, as in case 1, or $\phi_M(x) = q(x)(x-\beta)$, where $q(x)$ is a quadratic irreducible polynomial, as in case 2. This is the reason why Algorithm 4.4.2 examines all 3×3 matrices of the form $\begin{pmatrix} C_P^{t_1} & 0 \\ 0 & g^{t_2} \end{pmatrix}$ and $\begin{pmatrix} g^{t_1} & 1 & 0 \\ 0 & g^{t_1} & 0 \\ 0 & 0 & g^{t_2} \end{pmatrix}$ and selects the one which minimizes $\eta_{m_S}(t_1, t_2)$.

Algorithm 4.4.2

Inputs: *prime p, primitive polynomial $P(x) = x^2 + ax + b$ over Z_p,*
$P_1(x) = x - \lambda_1$, $P_2(x) = x - \lambda_2$, *where* $0 \neq \lambda_1 \neq \lambda_2 \neq 0$

Output: (t_1, t_2, TAG) *such that* $\eta_{m_S}(t_1, t_2)$ *is minimal.*
if $TAG = 1$, *the optimal* M *is of the form* $\begin{pmatrix} C_P^{t_1} & 0 \\ 0 & g^{t_2} \end{pmatrix}$
if $TAG \neq 1$, *the optimal* M *is of the form* $\begin{pmatrix} g^{t_1} & 1 & 0 \\ 0 & g^{t_1} & 0 \\ 0 & 0 & g^{t_2} \end{pmatrix}$

1. *compute:* $Ind_{C_P}(\lambda_1 I_2), Ind_g(\lambda_2)$, *where* $g = P(0)$
2. *compute:* k_{P_1}, k_{P_2}
3. *compute:* e_1, e_2
4. *compute:* $\mu_{P_1}, \mu_{P_2}, \mu_{P_1,P_2}$
5. *Initialize:* $t_1, t_2, t_{1,0}, t_{2,0}$ *to* p^2
6. *Initialize:* $\eta_{P_1}, \eta_{P_2}, \eta_{P_1,P_2}, \eta_{m_S}$ *to* p^3
7. *Initialize:* $\eta_{P_1,0}, \eta_{P_2,0}, \eta_{P_1,P_2,0}, \eta_{m_S,0}$ *to* p^3
8. **for**$(t_1' = 1$ *to* $t_1' = p^2 - 1)$ **do**
   compute: η'_{P_1}
   if$(t_1' < p)$ *compute:* $\eta''_{P_1,0}$
   for$(t_2' = 1$ *to* $t_2' = p - 1)$ **do**
      compute: $\eta'_{P_2}, \eta'_{P_1,P_2}$
      $\eta'_{m_S} \leftarrow \eta'_{P_1} + \eta'_{P_2} + \eta'_{P_1,P_2}$
      if$(t_2' < p)$

compute: $\eta''_{P_2}, \eta''_{P_1,P_2,1}$

$\eta''_{m_S} \leftarrow 2\eta''_{P_1,0} + \eta''_{P_2} + 2\eta''_{P_1,P_2,1}$

if$(\eta''_{m_S} < \eta_{m_S,0})$

$(\eta_{P_1,0}, \eta_{P_2,0}, \eta_{P_1,P_2,0}, \eta_{m_S,0}) \leftarrow (\eta''_{P_1,0}, \eta''_{P_2}, \eta''_{P_1,P_2,1}, \eta''_{m_S})$

$(t_{1,0}, t_{2,0}) \leftarrow (t'_1, t'_2)$

if$(\eta'_{m_S} < \eta_{m_S})$

$(\eta_{P_1}, \eta_{P_2}, \eta_{P_1,P_2}, \eta_{m_S}) \leftarrow (\eta'_{P_1}, \eta'_{P_2}, \eta'_{P_1,P_2}, \eta'_{m_S})$

$(t_1, t_2) \leftarrow (t'_1, t'_2)$

if $(\eta_{m_S} \leq \eta_{m_S,0})$

return $(t_1, t_2, 1)$

else

return $(t_{1,0}, t_{2,0}, 0)$

Given a matrix S as described in this section, Theorem 4.4.7 shows how to compute an optimal matrix M.

Theorem 4.4.7 *Let $S \in \mathcal{M}_3$ be nonsingular with $\phi_S(x) = P_1(x)^2 P_2(x)$ and $m_S(x) = P_1(x)P_2(x)$, where $P_1(x) = x - \lambda_1$ and $P_2(x) = x - \lambda_2$. Let (t_1, t_2, TAG) be such that $\eta_{m_S}(t_1, t_2)$ is minimal. Let $P(x) = x^2 + ax + b$ be a primitive polynomial, C_P be the companion matrix of $P(x)$, and A be a nonsingular matrix such that $A^{-1}SA = diag(\lambda_1, \lambda_1, \lambda_2)$. Also, let $k_{q_{1,0}} = \frac{p-1}{\gcd(p-1,t_1)}$, $k_{q_1} = \frac{p^2-1}{\gcd(p^2-1,t_1)}$, $k_{q_2} = \frac{p-1}{\gcd(p-1,t_2)}$, $e_i = \frac{lcm(Ind_{g(\lambda_1)}, Ind_{g(\lambda_2)})}{Ind_{g(\lambda_i)}}$, $i = 1, 2$. Then, if $TAG = 1$, the optimal matrix for S is $M = A \begin{pmatrix} C_P^{t_1} & 0 \\ 0 & g^{t_2} \end{pmatrix} A^{-1}$ and the MS–orbit structure is*

$$1 + \eta_{P_1}[i_{P_1}] + \eta_{P_2}[i_{P_2}] + \eta_{P_1}[i_{P_1,P_2}];$$

otherwise, $TAG \neq 1$, the optimal matrix for S is $M = A \begin{pmatrix} g^{t_1} & 1 & 0 \\ 0 & g^{t_1} & 0 \\ 0 & 0 & g^{t_2} \end{pmatrix} A^{-1}$ and

the MS–orbit structure is

$$1 + \eta_{P_1,0}[i_{P_1,0}] + \eta_{P_1,0}[p \cdot i_{P_1,0}] + \eta_{P_1,P_2,1}[i_{P_1,P_2,1}] + \eta_{P_1,P_2,1}[p \cdot i_{P_1,P_2,1}] + \eta_{P_2}[i_{P_2}],$$

where

$$\begin{array}{llll}
i_{P_1,0} = \frac{k_{q_{1,0}}}{\gcd(k_{P_1},k_{q_{1,0}})}, & & \eta_{P_1,0} = \frac{p-1}{k_{P_1}\cdot i_{P_1,0}}, \\
i_{P_2} = \frac{k_{q_2}}{\gcd(k_{P_1},k_{q_2})}, & & \eta_{P_2} = \frac{p-1}{k_{P_2}\cdot i_{P_2}}, \\
i_{P_1} = \frac{k_{q_1}}{\gcd(k_{P_1},k_{q_1})}, & & \eta_{P_1} = \frac{p^2-1}{k_{P_1}\cdot i_{P_1}}, \\
i_{P_1,P_2} = \frac{p^2-1}{\gcd(e_1t_1-(p+1)e_2t_2,\gcd(k_{P_1}\eta_{P_1},(p+1)k_{P_2}\eta_{P_2}))}, & & \eta_{P_1,P_2} = \frac{(p+1)(p-1)^2}{lcm(k_{P_1},k_{P_2})i_{P_1,P_2}}, \\
i_{P_1,P_2,1} = \frac{p-1}{\gcd(e_1t_1-e_2t_2,\gcd(k_{P_1}\eta_{P_1,0},(p+1)k_{P_2}\eta_{P_2}))}, & & \eta_{P_1,P_2,1} = \frac{(p-1)^2}{lcm(k_{P_1},k_{P_2})i_{P_1,P_2,1}}.
\end{array}$$

Proof
Let $S \in \mathcal{M}_3$ be nonsingular with $m_S(x) = P_1^2(x)P_2(x)$ and $\phi_S(x) = P_1^3(x)P_2(x)$, where $P_1(x) = x - \lambda_1$ and $P_2(x) = x - \lambda_2$. Let $M \in \mathcal{N}(S)$ be nonsingular. By Lemma 2.2.6, $\phi_M(x) = -q(x)(x - \beta)$ for some quadratic polynomial $q(x)$ and some nonzero $\beta \in Z_p$.

It was already shown in Theorem 4.4.6 that if $m_M(x) = (x - \alpha_1)(x - \alpha_2)(x - \beta)$ $\alpha_1 \neq -\alpha_2$, or $m_M(x) = (x - \alpha)(x - \beta)$, then M cannot be optimal for S. We can see that $q(x)$ is quadratic and irreducible or $q(x) = (x - \alpha)^2$, for some $\alpha \neq 0$.

Let $P(x) = x^2 + ax + b$ be a primitive polynomial over Z_p. In order to consider all possible matrices M with $\phi_M(x) = -q(x)(x - \beta)$ where $q(x)$ is quadratic irreducible, it is only necessary to consider all powers of any 2×2 maximal matrix. In particular, Algorithm 4.4.2 considers all powers of C_P, the companion matrix of $P(x)$.

Let (t_1, t_2, TAG) be the output of Algorithm 4.4.2 in the inputs $P(x)$, $x - \lambda_1$, and $x - \lambda_2$. Clearly this algorithm examines all matrices of the form

$$\begin{pmatrix} C_P^{t_1} & 0 \\ 0 & g^{t_2} \end{pmatrix} \text{ and } \begin{pmatrix} g^{t_1} & 1 & 0 \\ 0 & g^{t_1} & 0 \\ 0 & 0 & g^{t_2} \end{pmatrix},$$

and selects the one that is optimal for

$$\begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{pmatrix}.$$

Now, let A be the matrix of Lemma 2.2.5 for which $A^{-1}SA = \mathrm{diag}(\lambda_1, \lambda_1, \lambda_2)$. If $TAG = 1$, then an optimal matrix for S is

$$M = A \begin{pmatrix} C_P^{t_1} & 0 \\ 0 & g^{t_2} \end{pmatrix} A^{-1};$$

otherwise

$$M = A \begin{pmatrix} g^{t_1} & 1 & 0 \\ 0 & g^{t_1} & 0 \\ 0 & 0 & g^{t_2} \end{pmatrix} A^{-1}.\diamondsuit$$

4.4.4 Optimal three dimensional matrices for case V

In this section we compute an optimal matrix M when the nonsingular 3×3 matrix S over Z_p has minimal polynomial $m_S(x) = (x - \lambda)^3$. Theorem 4.4.8 gives a direct formula to compute such an M.

The following lemma states that the number of MS–orbits is not less than 3, for any matrix M that commutes with S.

Lemma 4.4.1 *Let $S \in \mathcal{M}_3$ be nonsingular with $m_S(x) = P(x)^3$, where $P(x) = x - \lambda$, and let $M \in \mathcal{N}(S)$ be nonsingular. Then, the number of nontrivial MS–orbits, η_{m_S}, is not less than* 3.

Proof
Recall that

$$\begin{aligned} U_P &= \{\mathbf{x} \in Z_p^3 | P(S)\,\mathbf{x} = \mathbf{0}\}, \\ U_{P^2} &= \{\mathbf{x} \in Z_p^3 | P(S)^2\mathbf{x} = \mathbf{0}\}, \\ U_{P^3} &= \{\mathbf{x} \in Z_p^3 | P(S)^3\mathbf{x} = \mathbf{0}\}. \end{aligned}$$

By Theorem 3.1.4, $U_{P,1} = U_P$, $U_{P^2,P} = U_{P^2} - U_P$, and $U_{P^3,P^2} = U_{P^3} - U_{P^2}$ are all S–invariant sets. This is also true for any polynomial combination of S. Thus, since M commutes with S if and only if there is a polynomial $Q(x)$ such that $M = Q(S)$ (Theorem 2.2.6), then it is true that the three sets $U_{P,1}$, $U_{P^2,P}$, and U_{P^3,P^2} are all M–invariant.$\diamondsuit$

Next theorem shows that this case is one in which the M–method is definitely much better than the generator method of Auslander.

Theorem 4.4.8 *Let $S \in \mathcal{M}_3$ be nonsingular with $m_S(x) = P(x)^3$, where $P(x) = x - \lambda$. Let k_P be the order of $P(x)$ and $\mu_P = \frac{p-1}{k_P}$. Then, an optimal matrix M for S is $M = (S - \lambda I_3)^2 + gI_3$, where g is a primitive of Z_p^*, and the MS–orbit structure is $1 + 2[\mu_P] + 1[p \cdot \mu_P]$*

Proof
Recall that

$$\begin{aligned} U_P &= \{\mathbf{x} \in Z_p^3 | P(S)\,\mathbf{x} = \mathbf{0}\}, \\ U_{P^2} &= \{\mathbf{x} \in Z_p^3 | P(S)^2\mathbf{x} = \mathbf{0}\}, \\ U_{P^3} &= \{\mathbf{x} \in Z_p^3 | P(S)^3\mathbf{x} = \mathbf{0}\}. \end{aligned}$$

Also, define $U_{P^r,P^{r-1}} = U_{P^r} - U_{P^{r-1}}$, $r = 1, 2, 3$. Our proof will show that matrix M so defined will yield a single MS–orbit in each $\mathcal{O}_{P^r,P^{r-1}}$, $r = 1, 2, 3$.

First, note that by Theorem 3.1.4, the number of nontrivial S–orbits in $U_{P,1}$, $U_{P^2,P}$, and U_{P^3,P^2} is μ_P, μ_P, and $p \cdot \mu_P$, respectively.

It is straightforward to see that $M = (S - \lambda I_3)^2 + gI_3$ commutes with S. Let A be a matrix for which $A^{-1}SA = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix}$ and see that

$$\begin{aligned} A^{-1}MA &= A^{-1}((S - \lambda I_3)^2 + gI_3)A \\ &= (\begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix} - \lambda I_3)^2 + gI_3 \\ &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}^2 + gI_3 \\ &= \begin{pmatrix} g & 0 & 1 \\ 0 & g & 0 \\ 0 & 0 & g \end{pmatrix}. \end{aligned}$$

Thus, $S^j = M^i \bmod p$ is equivalent to

$$\begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix}^j = \begin{pmatrix} g & 0 & 1 \\ 0 & g & 0 \\ 0 & 0 & g \end{pmatrix}^i \pmod p$$

if and only if

$$\begin{pmatrix} \lambda^j & j\lambda^{j-1} & \frac{j(j-1)}{2}\lambda^{j-2} \\ 0 & \lambda^j & j\lambda^{j-1} \\ 0 & 0 & \lambda^j \end{pmatrix} = \begin{pmatrix} g^i & 0 & ig^{i-1} \\ 0 & g^i & 0 \\ 0 & 0 & g^i \end{pmatrix} \pmod p$$

if and only if

$$\lambda^j = g^i \tag{4.37}$$

$$j\lambda^{j-1} = 0 \pmod p \tag{4.38}$$

$$\frac{j(j-1)}{2}\lambda^{j-2} = ig^{i-1} \tag{4.39}$$

The smallest positive integer $i_{P,1}$ that solves (4.37), for some j_1, is the length of the MS–orbits in $\mathcal{O}_{P,1}$. By Theorem 2.3.16, $i_{P,1} = \frac{p-1}{\gcd(k_P, p-1)} = \mu_P$. Hence, the number of MS–orbits in $\mathcal{O}_{P,1}$ is $\eta_{P,1} = \frac{\mu_P}{\mu_P} = 1$.

On the other hand, since $U_{P,1} \subset U_{P^2,P}$, $i_{P^2,P}$ must be a multiple of $i_{P,1} = \mu_P$. Thus, $i_{P^2,P} = \mu_P t$ for some positive integer t. However, $i_{P^2,P} | \mu_P$, which says that $i_{P^2,P} = \mu_P$. Thus, the number of nontrivial MS–orbits in $\mathcal{O}_{P^2,P}$ is $\eta_{P^2,P} = \frac{\mu_P}{\mu_P} = 1$.

The smallest positive integer i_{P^3,P^2} that solves (4.39), for some j_3, is the length of the MS–orbits in $\mathcal{O}_{P^3,P^2}$. Now, from equation (4.38), $j_3 = 0 \bmod p$. Thus, replacing j_3 by $0 \bmod p$ in (4.39), we endup with

$$i_{P^3,P^2} g^{i_{P^3,P^2}-1} = 0 \pmod{p}.$$

Thus, $i_{P^3,P^2} = 0 \bmod p$. But, since i_{P^3,P^2} is a positive multiple of $i_{P^2,P}$, it must happen that $i_{P^3,P^2} = p \cdot \mu_P$. Hence, the number of MS–orbits in $\mathcal{O}_{P^3,P^2}$ is

$$\eta_{P^3,P^2} = \frac{p \cdot \mu_P}{i^3_P, P^2} = \frac{p \cdot \mu_P}{p \cdot \mu_P} = 1.$$

Therefore, the MS–orbit structure is

$$1 + 1[\mu_P] + 1[\mu_P] + 1[p \cdot \mu_P] = 1 + 2[\mu_P] + 1[p \cdot \mu_P].\diamondsuit$$

Theorem 4.4.9 computes the MS–orbit structure when we assume that M is the scalar matrix gI_3.

Theorem 4.4.9 *Let $S \in \mathcal{M}_3$ be nonsingular with $m_S(x) = P(x)^3$, where $P(x) = x - \lambda$, k_P be the order of $P(x)$, $\mu_P = \frac{p-1}{k_P}$. Also, let $M = gI_3$, g a generator of Z_p^*. Then, the MS–orbit structure is $1 + (p+2)[\mu_P]$.*

Proof

Let A be a matrix for which $A^{-1}SA = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix}$. Hence, the smallest positive integer i that solves $S^j = M^i$, for some j, is equivalent to $A^{-1}S^jA = A^{-1}(gI_3)^iA = g^iI_3$. if and only if

$$\begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix}^j = g^iI_3 \pmod{p}$$

if and only if

$$\begin{aligned} \lambda^j &= g^i && (4.40)\\ j\lambda^{j-1} &= 0 \pmod p && (4.41)\\ \frac{j(j-1)}{2}\lambda^{j-2} &= 0 && (4.42) \end{aligned}$$

The smallest positive integer $i_{P,1}$ that solves (4.40), for some j_1, is $i_{P,1} = \mu_P$. This is the length of the MS–orbits in $\mathcal{O}_{P,1}$. Hence, the number of MS–orbits in $\mathcal{O}_{P,1}$ is $\eta_{P,1} = \frac{\mu_P}{i_{P,1}} = 1$. Furthermore, it is straightforward to see that $i = \mu_P$ is the smallest positive value that simultaneously solves equations (4.40) – (4.42). Thus, the number of MS–orbits in $\mathcal{O}_{P^2,P}$ and $\mathcal{O}_{P^3,P^2}$ is $\eta_{P^2,P} = \frac{\mu_P}{\mu_P} = 1$, and $\eta_{P^3,P^2} = \frac{p\cdot\mu_P}{\mu_P} = p$, respectively. Therefore, the MS–orbit structure is

$$1 + 1[\mu_P] + 1[\mu_P] + p[\mu_P] = 1 + (p+2)[\mu_P].\diamondsuit$$

Example 4.4.4 *Let* $S = \begin{pmatrix} -1 & 1 & 1 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix}$ *be defined over* Z_p. *The minimal polynomial of* S *is* $m_S(x) = P(x)^3$, *where* $P(x) = x+1$. *The order of* $P(x)$ *is* $k_P = 2$ *for any prime* p. *Thus,* $\mu_P = \frac{p-1}{2}$. *By Theorem 4.4.8, an optimal matrix for* S *is*

$$M = (S + I_3)^2 + gI_3 = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}^2 + gI_3 = \begin{pmatrix} g & 0 & 1 \\ 0 & g & 0 \\ 0 & 0 & g \end{pmatrix}$$

and the optimal MS*–orbit structure is*

$$1 + 2[\frac{p-1}{2}] + 1[\frac{p(p-1)}{2}].$$

Table 4.4.2 *shows matrices* M *together with the* MS*–orbit structure when we apply Theorems* 4.4.8 *and* 4.4.9 *for primes* p *between* 809 *and* 859 *for matrices* S *as in Example* 4.4.4. *As expected, the optimal number of* MS*–orbits remains constant while the number of* MS*–orbits computed through a scalar matrix grows linearly with prime* p.

p	*optimal* M	*MS–orbit structure*	η_{mS}	*gS–orbit structure*	η_{mS}
809	$\begin{pmatrix} 3 & 0 & 1 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$	$1+2[404]+1[326836]$	3	$1+811[404]$	811
811	$\begin{pmatrix} 3 & 0 & 1 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$	$1+2[405]+1[328455]$	3	$1+813[405]$	813
821	$\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$	$1+2[410]+1[336610]$	3	$1+823[410]$	823
823	$\begin{pmatrix} 3 & 0 & 1 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$	$1+2[411]+1[338253]$	3	$1+825[411]$	825
827	$\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$	$1+2[413]+1[341551]$	3	$1+829[413]$	829
829	$\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$	$1+2[414]+1[343206]$	3	$1+831[414]$	831
839	$\begin{pmatrix} 11 & 0 & 1 \\ 0 & 11 & 0 \\ 0 & 0 & 11 \end{pmatrix}$	$1+2[419]+1[351541]$	3	$1+841[419]$	841
853	$\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$	$1+2[426]+1[363378]$	3	$1+855[426]$	855
857	$\begin{pmatrix} 3 & 0 & 1 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$	$1+2[428]+1[366796]$	3	$1+859[428]$	859
859	$\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$	$1+2[429]+1[368511]$	3	$1+861[429]$	861

Table 4.4.2 : *A family of matrices S for which an optimal M is not gI_2.*

4.4.5 Optimal three dimensional matrices for case VI

Let S be a 3×3 matrix with $m_S(x)=(x-\lambda_1)^2(x-\lambda_2)$, where λ_1 and λ_2 are distinct nonzero eigenvalues of S. Theorem 4.4.10 shows a procedure to compute an optimal

matrix M for this S. It is worth noting that this case reduces to the two dimensional case with two distinct eigenvalues (section 4.3.3).

Theorem 4.4.10 *Let $S \in \mathcal{M}_3$ be nonsingular with $m_S(x) = P_1(x)^2 P_2(x)$, where $P_1(x) = x - \lambda_1$, $P_2(x) = x - \lambda_2$, $\lambda_1 \neq \lambda_2$. Also, let (t_1, t_2) be such that $\eta_{P_1 P_2}$ is minimal, $q_1(x) = x - g^{t_1}$, $q_2(x) = x - g^{t_2}$, k_{P_t}, k_{q_t} be the orders of $P_t(x)$ and $q_t(x)$, respectively, for $t = 1, 2$. Then, an optimal matrix M for S is*

$$M = c_2 S^2 + c_1 S + c_0 I_3$$

and the MS–orbit structure is

$$1 + 2\eta_{P_1}[i_{P_1}] + 2\eta_{P_1,P_2}[i_{P_1,P_2}] + \eta_{P_2}[i_{P_2}],$$

where

$$\begin{aligned}
c_2 &= (g^{t_2} - g^{t_1})(\lambda_2 - \lambda_1)^{-2}, \\
c_1 &= -2c_2\lambda_1, \\
c_0 &= g^{t_1} - (c_2\lambda_1^2 + c_1\lambda_1), \\
i_{P_1} &= \tfrac{k_{q_1}}{\gcd(k_{P_1}, k_{q_1})}, \\
\eta_{P_1} &= \tfrac{p-1}{k_{P_1} i_{P_1}}, \\
i_{P_2} &= \tfrac{k_{q_2}}{\gcd(k_{P_2}, k_{q_2})}, \\
\eta_{P_2} &= \tfrac{p-1}{k_{P_2} i_{P_2}}, \\
i_{P_1,P_2} &= \tfrac{p-1}{\gcd(e_1 t_1 - e_2 t_2, \gcd(k_{P_1}\eta_{P_1}, k_{P_2}\eta_{P_2}))}, \\
\eta_{P_1,P_2} &= \tfrac{(p-1)^2}{lcm(k_{P_1}, k_{P_2}) i_{P_1,P_2}}, \\
e_t &= \tfrac{lcm(Ind_g(\lambda_1), Ind_g(\lambda_2))}{Ind_g(\lambda_t)}, \ t = 1, 2.
\end{aligned}$$

Proof

Let A be a nonsingular matrix for which $A^{-1}SA = S' = \begin{pmatrix} \lambda_1 & 1 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{pmatrix}$. Also, let $M \in \mathcal{N}(S)$ be nonsingular. By Theorem 2.2.6, $M = Q(S)$ for some polynomial $Q(x) = c_2 x^2 + c_1 x + c_0$. Thus,

$$A^{-1}MA = A^{-1}Q(S)A = Q(A^{-1}SA) = Q(S') = \begin{pmatrix} Q(\lambda_1) & Q'(\lambda_1) & 0 \\ 0 & Q(\lambda_1) & 0 \\ 0 & 0 & Q(\lambda_2) \end{pmatrix},$$

where $Q'(\lambda_1) = 2c_2\lambda_1 + c_1$. Hence, M is similar either to

(I) $M_1' = \begin{pmatrix} \beta_1 & 0 & 0 \\ 0 & \beta_1 & 0 \\ 0 & 0 & \beta_2 \end{pmatrix}$, if $Q'(\lambda_1) = 0$, where $\beta_t = Q(\lambda_t)$, $t = 1, 2$. Or

(II) $M_2' = \begin{pmatrix} \beta_1 & 1 & 0 \\ 0 & \beta_1 & 0 \\ 0 & 0 & \beta_2 \end{pmatrix}$, if $Q'(\lambda_1) \neq 0$, where $\beta_t = Q(\lambda_t)Q'(\lambda_1)^{-1}$, $t = 1, 2$.

Note that both M_1' and M_2' commute with S'. Our aim is to show that no matter which of these matrices we choose, they yield the same MS–orbit structure.

Define,

$$\begin{aligned} V_{P_1} &= \{\mathbf{x} \in Z_p^3 | P_1(S)\mathbf{x} = \mathbf{0}\}, \\ V_{P_1^2} &= \{\mathbf{x} \in Z_p^3 | P_1(S)^2\mathbf{x} = \mathbf{0}\}, \\ V_{P_2} &= \{\mathbf{x} \in Z_p^3 | P_2(S)\mathbf{x} = \mathbf{0}\}, \\ V_{P_1^2,P_2} &= V_{P_1^2P_2} - V_{P_1} \cup V_{P_2}. \end{aligned}$$

Also, define

$$\begin{aligned} V_{P_1^2,P_1} &= V_{P_1^2} - V_{P_1}, \\ V_{(P_1^2,P_1),P_2} &= \{\mathbf{x}+\mathbf{y} | \mathbf{x} \in V_{P_1^2,P_1} \text{ and } \mathbf{y} \neq \mathbf{0} \in V_{P_2}\}, \\ V_{P_1,P_2} &= \{\mathbf{x}+\mathbf{y} | \mathbf{x} \neq \mathbf{0} \in V_{P_1} \text{ and } \mathbf{y} \neq \mathbf{0} \in V_{P_2}\}, \end{aligned}$$

Observe that $V_{P_1^2,P_2} = V_{(P_1^2,P_1),P_2} \cup V_{P_1,P_2}$. Thus,

$$Z_p^3 = V_{P_1} \cup V_{P_1^2,P_1} \cup V_{P_2} \cup V_{P_1,P_2} \cup V_{(P_1^2,P_1),P_2}.$$

By Theorems 3.1.4 and 3.1.5, the S–orbit structure is

$$1 + \mu_{P_1}(k_{P_1}) + \mu_{P_1}(p \cdot k_{P_1}) + \mu_{P_2}(k_{P_2}) + \mu_{P_1,P_2}(k_{P_1,P_2}) + \mu_{P_1,P_2}(p \cdot k_{P_1,P_2}),$$

where $\mu_{P_1} = \frac{p-1}{k_{P_1}}$, $\mu_{P_2} = \frac{p-1}{k_{P_2}}$, $\mu_{P_1,P_2} = \mu_{P_1}\mu_{P_2}\gcd(k_{P_1}, k_{P_2})$, and $k_{P_1,P_2} = \mathrm{lcm}(k_{P_1}, k_{P_2})$.

Each set V_{P_1}, $V_{P_1^2,P_1}$, V_{P_2}, V_{P_1,P_2}, and $V_{(P_1^2,P_1),P_2}$ is M–invariant since M is a polynomial combination of S. First, let $\mathbf{x} \in V_{P_1}$. Thus, $P_1(S)M\mathbf{x} = MP_1(S)\mathbf{x} = \mathbf{0}$. Then, $M\mathbf{x} \in V_{P_1}$. Similarly for V_{P_2}. Now, let $\mathbf{x} \in V_{P_1^2,P_1}$. Thus, $P_1(S)^2M\mathbf{x} = MP_1(S)^2\mathbf{x} = \mathbf{0}$. Then, $M\mathbf{x} \in V_{P_1^2,P_1}$. Let, $\mathbf{x} \in V_{P_1,P_2}$. Then, $\mathbf{x} = \mathbf{x_1} + \mathbf{x_2}$ for some $\mathbf{x_1} \neq \mathbf{0} \in V_{P_1}$ and some $\mathbf{x_2} \neq \mathbf{0} \in V_{P_2}$. We already know that $M\mathbf{x_1} \in V_{P_1}$ and that $M\mathbf{x_2} \in V_{P_2}$. Hence, $M\mathbf{x_1} + M\mathbf{x_2} = M(\mathbf{x_1} + \mathbf{x_2}) = M\mathbf{x} \in V_{P_1,P_2}$. Similarly for $V_{(P_1^2,P_1),P_2}$.

Therefore, the set of MS–orbits is

$$\mathcal{O}_{m_S} = \mathcal{O}_{P_1} \cup \mathcal{O}_{P_1^2,P_1} \cup \mathcal{O}_{P_2} \cup \mathcal{O}_{P_1,P_2} \cup \mathcal{O}_{(P_1^2,P_1),P_2}.$$

Case (I), assume M to be similar to the matrix $\begin{pmatrix} \beta_1 & 0 & 0 \\ 0 & \beta_1 & 0 \\ 0 & 0 & \beta_2 \end{pmatrix}$. Thus, $S^j = M^i$ is equivalent to

$$\begin{pmatrix} \lambda_1 & 1 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{pmatrix}^j = \begin{pmatrix} \beta_1 & 0 & 0 \\ 0 & \beta_1 & 0 \\ 0 & 0 & \beta_2 \end{pmatrix}^i \pmod p \tag{4.43}$$

if and only if

$$\lambda_1^j = \beta_1^i \tag{4.44}$$
$$j\lambda_1^{j-1} = 0 \tag{4.45}$$
$$\lambda_2^j = \beta_2^i \tag{4.46}$$

The length of the MS–orbits in $\mathcal{O}_{P_t}$, $t = 1, 2$, is the smallest positive integer i_{P_t} that solves equations (4.44) and (4.46), for some j_t, respectively. By Theorem 2.3.16, $i_{P_t} = \frac{k_{q_t}}{\gcd(k_{P_t}, k_{q_t})}$, and the number of MS–orbits in $\mathcal{O}_{P_t}$ is $\eta_{P_t} = \frac{\mu_{P_t}}{i_{P_t}} = \frac{p-1}{k_{P_t} i_{P_t}}$.

The smallest positive integer $i_{P_1^2,P_1}$ that simultaneously solves equations (4.44) and (4.45) for some j, is the length of the MS–orbits in $\mathcal{O}_{P_1^2,P_1}$. Observe that equation (4.45) holds for any integer $i_{P_1^2,P_1}$. Thus, $i_{P_1^2,P_1} = i_{P_1}$. Hence, $\eta_{P_1^2,P_1} = \frac{\mu_{P_t}}{i_{P_t}} = \eta_{P_1}$.

The smallest positive integer i_{P_1,P_2} that simultaneously solves equations (4.44) and (4.46) is the length of the MS–orbits in $\mathcal{O}_{P_1,P_2}$. By Theorem 2.3.15,

$$i_{P_1,P_2} = \frac{p-1}{\gcd(e_1 \mathrm{Ind}_g(\beta_1) - e_2 \mathrm{Ind}_g(\beta_2), \gcd(k_{P_1}\eta_{P_1}, k_{P_2}\eta_{P_2}))},$$

and the number of MS–orbits in $\mathcal{O}_{P_1,P_2}$ is $\eta_{P_1,P_2} = \frac{\mu_{P_1,P_2}}{i_{P_1,P_2}} = \frac{(p-1)^2}{\mathrm{lcm}(k_{P_1},k_{P_2}) i_{P_1,P_2}}$.

The smallest positive integer $i_{(P_1^2,P_1),P_2}$ that simultaneously solves equations (4.44) – (4.46), for some j, is the length of the MS–orbits in $\mathcal{O}_{(P_1^2,P_1),P_2}$. Note that equation (4.45) holds for any value of i. Therefore, $i_{(P_1^2,P_1),P_2} = i_{P_1,P_2}$ and $\eta_{(P_1^2,P_1),P_2} = \frac{\mu_{P_1,P_2}}{i_{P_1,P_2}} = \eta_{P_1,P_2}$. Thus, for case (I), the MS–orbit structure is

$$1 + 2\eta_{P_1}[i_{P_1}] + 2\eta_{P_1,P_2}[i_{P_1,P_2}] + \eta_{P_2}[i_{P_2}].$$

For case (II), we assume M is similar to $\begin{pmatrix} \beta_1 & 1 & 0 \\ 0 & \beta_1 & 0 \\ 0 & 0 & \beta_2 \end{pmatrix}$. Thus, $S^j = M^i$ is equivalent to

$$\begin{pmatrix} \lambda_1 & 1 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{pmatrix}^j = \begin{pmatrix} \beta_1 & 1 & 0 \\ 0 & \beta_1 & 0 \\ 0 & 0 & \beta_2 \end{pmatrix}^i \pmod p \tag{4.47}$$

if and only if

$$\begin{aligned} \lambda_1^j &= \beta_1^i && (4.48)\\ j\lambda_1^{j-1} &= i\beta_1^{i-1} && (4.49)\\ \lambda_2^j &= \beta_2^i && (4.50) \end{aligned}$$

if and only if

$$\begin{aligned} \lambda_1^j &= \beta_1^i && (4.51)\\ j\beta &= i\lambda_1 && (4.52)\\ \lambda_2^j &= \beta_2^i && (4.53) \end{aligned}$$

As before, observe that equation (4.52) holds for any integer i. Therefore, the MS–orbit structure is the same as in case (I).

Finally, we want to find a matrix M (i.e., a polynomial $Q(x) = c_2x^2 + c_1x + c_0$ such that $M = Q(S)$) that minimizes

$$\eta_{m_S} = 2\eta_{P_1} + 2\eta_{P_1,P_2} + \eta_{P_2}.$$

We apply Algorithm 4.3.1 on the input $\lambda_1,\ \lambda_2,\ p$ and get a pair (t_1, t_2) that minimizes $\eta_{P_1P_2} = \eta_{P_1} + \eta_{P_1,P_2} + \eta_{P_2}$. Which yield matrix $M' = \begin{pmatrix} g^{t_1} & 0 & 0 \\ 0 & g^{t_1} & 0 \\ 0 & 0 & g^{t_2} \end{pmatrix}$. Thus,

$$\begin{aligned} Q(\lambda_1) &= g^{t_1}\\ Q(\lambda_2) &= g^{t_2}\\ Q'(\lambda_1) &= 0 \end{aligned}$$

if and only if

$$\begin{aligned} c_2\lambda_1^2 + c_1\lambda_1 + c_0 &= g^{t_1}\\ c_2\lambda_2^2 + c_1\lambda_2 + c_0 &= g^{t_2}\\ 2c_2\lambda_1 + c_1 &= 0 \end{aligned}$$

if and only if

$$\begin{aligned} c_2(\lambda_2^2 - \lambda_1^2) + c_1(\lambda_2 - \lambda_1) &= g^{t_2} - g^{t_1}\\ c_1 &= -2c_2\lambda_1 \end{aligned}$$

if and only if

$$c_2(\lambda_2 + \lambda_1^2) - 2c_2\lambda_1 = (g^{t_2} - g^{t_1})(\lambda_2 - \lambda_1)^{-1}$$

if and only if

$$\begin{aligned} c_2 &= (g^{t_2} - g^{t_1})(\lambda_2 - \lambda_1)^{-2} \\ c_1 &= -2c_2\lambda_1 \\ c_0 &= g^{t_1} - (c_2\lambda_1^2 + c_1\lambda_1).\diamondsuit \end{aligned}$$

4.4.6 Optimal three dimensional matrices for case VII

Let S be a nonsingular 3×3 matrix over Z_p with characteristic and minimal polynomials $\phi_S(x) = (x-\lambda)^3$ and $m_S(x) = (x-\lambda)^2$, respectively. Theorem 4.4.12 gives a direct formula to compute an optimal matrix M for S.

Let $S = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}$, $\lambda \neq 0$. Then, S decomposes $V = Z_p^3$ as a direct sum of two S–invariant subspaces U and W, where

$$\begin{aligned} U &= \{(u,v,0)^T | u,v \in Z_p\} \text{ and} \\ W &= \{(0,0,w)^T | u \in Z_p\}. \end{aligned}$$

An useful decomposition of U is

$$U = (U - U') \cup U',$$

where $U' = \{(u,0,0)^T | u \in Z_p\}$. Let k_P be the order of $P(x) = x - \lambda$ and $\mu_P = \frac{p-1}{k_P}$. By Theorem 3.1.4, there are two types of S–orbits in U; μ_P of length $p \cdot k_P$ in $U - U'$, and μ_P of length k_P in U'. Also, there are μ_P S–orbits of length k_P in W. Thus, by Theorem 3.1.5, the S–orbit structure is

$$\begin{aligned} & (1 + \mu_P(k_P) + \mu_P(kp))(1 + \mu_P(k_P)) \\ = \; & 1 + \mu_P(k_P) + \mu_P(p \cdot k_P) + \mu_P(k_P) + \mu^2 k_P(k_P) + \mu_P^2 k_P(p \cdot k_P) \\ = \; & 1 + \mu_P(k_P) + (\mu_P + \mu_P^2 k_P)(k_P) + (\mu_P + \mu_P^2 k_P)(p \cdot k_P) \\ = \; & 1 + \mu_P(k_P) + \mu(1 + \mu_P k_P)(k_P) + \mu_P(1 + \mu_P k_P)(p \cdot k_P) \\ = \; & 1 + \mu_P(k_P) + \mu_P(1 + p - 1)(k_P) + \mu_P(1 + p - 1)(p \cdot k_P) \\ = \; & 1 + \mu_P(k_P) + p\mu_P(k_P) + p\mu_P(p \cdot k_P) \end{aligned}$$

Lemma 4.4.2 *Let $S \in \mathcal{M}_3$ be nonsingular with $\phi_S(x) = -P^3(x)$ and $m_S(x) = P^2(x)$, where $P(x) = x - \lambda$. $M = gI_3$, k_P is the order of $P(x)$, $\mu_P = \frac{p-1}{k_P}$, and g a primitive of Z_p. Then, the MS–orbit structure is*

$$1 + (2p+1)[\mu_P].$$

Proof
$S^j = M^i$ is equivalent to

$$\begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}^j = \begin{pmatrix} g & 0 & 0 \\ 0 & g & 0 \\ 0 & 0 & g \end{pmatrix}^i$$

if and only if

$$\begin{aligned} \lambda^j &= g^i \\ j\lambda^{j-1} &= 0 \end{aligned}$$

The smallest positive i solving last system is $i = \mu_P$. Thus, since all the MS–orbits are of length $i = \mu_P$, the MS–orbit structure is

$$\begin{aligned} & 1 + \frac{\mu_P}{i}[i] + \frac{p\mu_P}{i}[i] + \frac{p\mu_P}{i}[i] \\ = \; & 1 + \frac{\mu_P}{\mu_P}[\mu_P] + \frac{p\mu_P}{\mu_P}[\mu] + \frac{p\mu_P}{\mu_P}[\mu_P] \\ = \; & 1 + 1[\mu_P] + p[\mu_P] + p[\mu_P] \\ = \; & 1 + (2p+1)[\mu_P].\diamondsuit \end{aligned}$$

Let us define

$$\begin{aligned} V_1 &= \{\mathbf{x} + \mathbf{y} | \mathbf{x} \in U - U' \text{ and } \mathbf{y} \neq \mathbf{0} \in W\}, \text{ and} \\ V_2 &= \{\mathbf{x} + \mathbf{y} | \mathbf{x} \in U' \text{ and } \mathbf{y} \neq \mathbf{0} \in W\}. \end{aligned}$$

We can show that

$$V = U' \cup V_1 \cup V_2.$$

The number of S–orbits in U', V_1, and V_2, is μ_P, $p\mu_P$, and $p\mu_P$, respectively.

Let $S = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}$ and $M \in \mathcal{M}_3$ be nonsingular. Then, by direct calculation we can show that $M \in \mathcal{N}(S)$ if and only if $M = \begin{pmatrix} a & b & c \\ 0 & a & 0 \\ 0 & d & e \end{pmatrix}$, for some $a \neq 0, b, c, d, e \neq 0 \in Z_p$.

Remark 4.4.2 *U' is M–invariant. Let $\mathbf{x} \in U'$. Thus, $M\mathbf{x} = (u, 0, 0)^T$, for some $u \in Z_p$. Then $M\mathbf{x} \in U'$.*

Remark 4.4.3 *$(U - U') \cup V_1$ is M–invariant. Let $\mathbf{y} \in (U - U') \cup V_1$. Thus, $\mathbf{y} = (u, v, w)^T$, $v \neq 0$. Hence, $M\mathbf{y} = (au + bv + cw, av, dv + ew)^T$. Thus, since $av \neq 0$, $M\mathbf{y} \notin U' \cup W \cup V_2$. Therefore, $M\mathbf{y} \in (U - U') \cup V_1$.*

Remark 4.4.4 *$W \cup V_2$ is M–invariant. A similar argument as in 4.4.3, can be used to prove it.*

By Remarks 4.4.2, 4.4.3, and 4.4.4, the number of nontrivial MS–orbits is at least three.

The following Theorem shows that if we choose $M = \begin{pmatrix} g & 0 & 1 \\ 0 & g & 0 \\ 0 & 1 & g \end{pmatrix}$, we indeed endup with a single MS–orbit in each U', V_1, and V_2, whose lengths are μ_P, $p\mu_P$, and $p\mu_P$, respectively.

Theorem 4.4.11 *Let $S = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}$, $\lambda \neq 0 \in Z_p$, and g be a generator of Z_p^*. Then, an optimal matrix for S is $M = \begin{pmatrix} g & 0 & 1 \\ 0 & g & 0 \\ 0 & 1 & g \end{pmatrix}$ and its MS–orbit structure is*

$$1 + 1[\mu_P] + 2[p\mu_P].$$

Proof

Let $\mathbf{x_1} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\mathbf{x_2} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$, and $\mathbf{x_3} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. Note that $\mathbf{x_1} \in U'$, $\mathbf{x_2} \in V_1$, and that $\mathbf{x_3} \in W$.

It is easy to see that the smallest i_1 that solves $S^{j_1'}\mathbf{x}_1 = M^{i_1'}\mathbf{x}_1$, for some j_1, is $i_1' = \mu_P$. Which means that the number of nontrivial MS–orbits in U' is $\eta_P' = \frac{\mu_P}{\mu_P} = 1$.

On the other hand, let i_2 be the length of $O_{MS}(\mathbf{x_2})$. Thus, i_2 is the smallest positive integer for which $S^{j_2}\mathbf{x}_2 = M^{i_2}\mathbf{x}_2$, for some j_2. Whence, $S^{j_2}\mathbf{x}_2 = M^{i_2}\mathbf{x}_2$ if and only if

$$\begin{pmatrix} \lambda^{j_2} & j\lambda^{j_2-1} & 0 \\ 0 & \lambda^{j_2} & 0 \\ 0 & 0 & \lambda^{j_2} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} g^{i_2} & \frac{i_2(i_2-1)}{2} g^{i_2-1} & i_2 g^{i_2-2} \\ 0 & g^{i_2} & 0 \\ 0 & i_2 g^{i_2-2} & g^{i_2} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \tag{4.54}$$

if and only if

$$\begin{aligned} j_2\lambda^{j_2-1} &= \frac{i_2(i_2-1)}{2}g^{i_2-1} && (4.55)\\ \lambda^{j_2} &= g^{i_2} && (4.56)\\ \lambda^{j_2} &= ig^{i_2-2}+g^{i_2} && (4.57)\end{aligned}$$

if and only if

$$\begin{aligned} j_2\lambda^{-1} &= \frac{i_2(i_2-1)}{2}g^{-1} && (4.58)\\ \lambda^{j_2} &= g^{i_2} && (4.59)\\ 0 &= ig^{i_2-2} && (4.60)\end{aligned}$$

if and only if

$$\begin{aligned} j_2\lambda^{-1} &= \frac{i_2(i_2-1)}{2}g^{-1} && (4.61)\\ \lambda^{j_2} &= g^{i_2} && (4.62)\\ 0 &= i_2. && (4.63)\end{aligned}$$

By Theorem 2.3.16, the smallest positive integer i_2 that solves (4.62), for some j_2, is

$$i_2 = \frac{\mu_P}{\gcd(\mu_P, 1)} = \mu_P.$$

On the other hand, from equation (4.62), $i_2 = 0 \bmod p$ implies that i_2 is a multiple of p. Hence, the smallest i_2 that simultaneously solves (4.61), (4.62), and (4.63) is a multiple of $\text{lcm}(\mu_P, p) = p \cdot \mu_P$. But, this i_2 must be smaller or equal to the number of S–orbits in V_1, which is $p \cdot \mu_P$. Therefore, $i_2 = p \cdot \mu_P$. Thus, the number of MS–orbits in V_1 is $\eta_P = \frac{p\cdot\mu_P}{p\cdot\mu_P} = 1$.

Finally, let i_3 be the length of $O_{MS}(\mathbf{x_3})$. The same type of argument used for i_2, shows that $i_3 = p \cdot \mu_P$. Thus, the number of MS–orbits in V_2 is $\eta''_P = \frac{p\cdot\mu_P}{p\cdot\mu_P} = 1$. Hence, the MS–orbit structure is

$$\begin{aligned} & 1 + \eta_P[i_P] + \eta'_P[i'_P] + \eta''_P[i''_P] \\ = \;& 1 + 1[\mu_P] + 1[p\cdot\mu_P] + 1[p\cdot\mu_P] \\ = \;& 1 + 1[\mu_P] + 2[p\cdot\mu_P].\diamondsuit \end{aligned}$$

Theorem 4.4.12 *Let $S \in \mathcal{M}_3$ be nonsingular with $\phi_S(x) = P(x)^3$ and $m_S(x) = P(x)^2$, wher $P(x) = x - \lambda$. Also, let k_P be the order of $P(x)$, $\mu_P = \frac{p-1}{k_P}$, g be a*

generator of Z_p^*, *and* A *be a nonsingular matrix for which* $A^{-1}SA = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}$.

Then, an optimal matrix M *for* S *is*

$$M = A \begin{pmatrix} g & 0 & 1 \\ 0 & g & 0 \\ 0 & 1 & g \end{pmatrix} A^{-1},$$

and the optimal MS*–orbit structure is*

$$1 + 1[\mu_P] + 2[p \cdot \mu_P].$$

Proof

Let $S' = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}$ and $M' = \begin{pmatrix} g & 0 & 1 \\ 0 & g & 0 \\ 0 & 1 & g \end{pmatrix}$. Observe that $M'S' = S'M'$. Hence,

$$\begin{aligned} SM &= (AS'A^{-1})AM'A^{-1} \\ &= AS'M'A^{-1} \\ &= AM'S'A^{-1} \\ &= AM'A^{-1}AS'A^{-1} \\ &= MS. \end{aligned}$$

By Theorem 4.4.11, M' is optimal for S' and since similarity preserves MS–orbit structures, then $M = AM'A^{-1}$ is optimal for $S = AS'A^{-1}$ with MS–orbit structure $1 + 1[\mu_P] + 2[p \cdot \mu_P]$.$\diamondsuit$

Note that the cost of computing A and its inverse is $O(p^3)$ time in the worse case.

Example 4.4.5 *Let* $S = \begin{pmatrix} 11 & 2 & 0 \\ 2 & 10 & 0 \\ 12 & 14 & 2 \end{pmatrix}$ *be defined over* Z_{17} *and let us find an optimal matrix* M *for* S. *First, see that the characteristic polynomial of* S *is* $\phi_S(x) = P(x)^3$, *where* $P(x) = x - 2$, *and that* $P(S)^2 = 0$, *but* $P(S) \neq 0$. *Thus,* $m_S(x) = P(x)^2$. *Let* $S' = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$. *By Theorem 4.4.11, an optimal matrix for* S' *is*

$M' = \begin{pmatrix} 3 & 0 & 1 \\ 0 & 3 & 0 \\ 0 & 1 & 3 \end{pmatrix}$. *It remains to compute* A. *Let*

$$\begin{aligned} N(S-2I_3) &= \{\mathbf{x} \in Z_{17}^3 | (S-2I_3)\mathbf{x} = \mathbf{0}\} \\ &= \{\mathbf{x} \in Z_{17}^3 | \begin{pmatrix} 9 & 2 & 0 \\ 2 & 8 & 0 \\ 12 & 14 & 0 \end{pmatrix} \mathbf{x} = \mathbf{0}\} \\ &= \{\mathbf{x} \in Z_{17}^3 | \begin{pmatrix} 9 & 2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \mathbf{x} = \mathbf{0}\}, \end{aligned}$$

since the last two rows of $S - 2I_3$ *are simply multiples of the first one. Hence,*

$$\begin{aligned} N(S-2I_3) &= \{ \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} | 9x_0 + 2x_1 = 0\} \\ &= \{ \begin{pmatrix} x_0 \\ 4x_0 \\ x_1 \end{pmatrix} | x_0, x_1 \in Z_{13}\}. \end{aligned}$$

Let $\mathbf{x_1} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ *and see that* $\mathbf{x_1} \notin N(S-2I_3)$. *Thus,* $(S-2I_3)\mathbf{x_1} = \begin{pmatrix} 2 \\ 8 \\ 14 \end{pmatrix}$. *Now, let* $\mathbf{x_2} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \in N(S-2I_3)$ *and observe that* $\mathbf{x_2}$ *is linearly independent with* $(S-2I_3)\mathbf{x_1}$. *Then, applying Lemma 2.2.7, matrix* $A = \begin{pmatrix} 2 & 0 & 0 \\ 8 & 1 & 0 \\ 14 & 0 & 1 \end{pmatrix}$. *The characteristic polynomial of* A *is* $\phi_A(x) = -x^3 + 4x^2 + 12x + 2$. *Thus, using the fact that* $\phi_A(A) = 0$, $A^{-1} = 9(A^2 + 13A + 5I_3) = \begin{pmatrix} 9 & 0 & 0 \\ 13 & 1 & 0 \\ 10 & 0 & 1 \end{pmatrix}$.

Therefore, an optimal matrix for S is

$$M = \begin{pmatrix} 2 & 0 & 0 \\ 8 & 1 & 0 \\ 14 & 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 0 & 1 \\ 0 & 3 & 0 \\ 0 & 1 & 3 \end{pmatrix} \begin{pmatrix} 9 & 0 & 0 \\ 13 & 1 & 0 \\ 10 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 0 & 2 \\ 12 & 3 & 8 \\ 0 & 1 & 0 \end{pmatrix}.$$

The order of $P(x)$ is $k_P = 8$. Thus, $\mu_P = \frac{p-1}{k_P} = 2$. Therefore, the optimal MS–orbit structure is

$$1 + 1[2] + 2[34].$$

4.4.7 Optimal three dimensional matrices for case $VIII$

In this section we find an optimal matrix M for a 3×3 nonsingular matrix S over Z_p with three distinct eigenvalues. Algorithm 4.4.3 and Theorem 4.4.14 outline the steps to compute such an optimal matrix M.

Theorem 4.4.13 *Let $S \in \mathcal{M}_3$ be nonsingular with three distinct eigenvalues λ_1, λ_2, and λ_3 and $m_S(x) = P_1(x)P_2(x)P_3(x)$, where for $t = 1, 2, 3$, $P_t(x) = x - \lambda_t$, $e_{tu} = \frac{lcm(Ind_g(\lambda_t), Ind_g(\lambda_u))}{Ind_g(\lambda_t)}$, $t \neq u$, $t, u = 1, 2, 3$, and g a generator of Z_p^*. Then for any nonsingular $M \in \mathcal{N}(S)$, $\phi_M(x) = q_1(x)q_2(x)q_3(x)$, where for $t = 1, 2, 3$ $q_t(x) = x - \beta_t$ and the MS–orbit structure induced by M is given by*

$$1 + \eta_{P_1}[i_{P_1}] + \sum \mathcal{O}_{P_2P_3} + \sum \mathcal{O}_{P_1,P_2P_3},$$

where k_{P_t}, k_{q_t} are the orders of P_t, q_t, respectively, and for $t \neq u$, $t, u = 1, 2, 3$

$$\begin{aligned}
\textstyle\sum \mathcal{O}_{P_2P_3} &= \eta_{P_2}[i_{P_2}] + \eta_{P_3}[i_{P_3}] + \eta_{P_2,P_3}[i_{P_2,P_3}], \\
\textstyle\sum \mathcal{O}_{P_1,P_2P_3} &= \eta_{P_1,P_3}[i_{P_1,P_3}] + \eta_{P_1,P_2}[i_{P_1,P_2}] + \eta_{P_1,P_2,P_3}[i_{P_1,P_2,P_3}], \\
i_{P_t} &= \tfrac{k_{q_t}}{\gcd(k_{P_t}, k_{q_t})}, \\
\eta_{P_t} &= \tfrac{p-1}{lcm(k_{P_t}, k_{q_t})}, \\
i_{P_t,P_u} &= \tfrac{p-1}{\gcd(e_{tu}Ind_{g(\beta_t)} - e_{ut}Ind_{g(\beta_u)}, \gcd(k_{P_t}\eta_{P_t}, k_{P_u}\eta_{P_u}))}, \\
\eta_{P_t,P_u} &= \tfrac{(p-1)^2}{lcm(k_{P_t}, k_{P_u})i_{P_t,P_u}}, \\
i_{P_1,P_2,P_3} &= lcm(i_{P_1,P_2}, i_{P_1,P_3}, i_{P_2,P_3}), \\
\eta_{P_1,P_2,P_3} &= \tfrac{(p-1)^3}{lcm(k_{P_1}, k_{P_2}, k_{P_3})i_{P_1,P_2,P_3}}.
\end{aligned}$$

Proof
Let S be a nonsingular 3×3 matrix over Z_p with three distinct eigenvalues and $m_{S(x)} = P_1(x)P_2(x)P_3(x)$, where $P_t(x) = x - \lambda_t$. Let k_{P_t} be the order of P_t and define $k_{P_t,P_u} = \text{lcm}(k_{P_t}, k_{P_u})$, $k_{P_1,P_2,P_3} = \text{lcm}(k_{P_1}, k_{P_2,P_3})$, $\mu_{P_t} = \frac{p-1}{k_{P_t}}$, $\mu_{P_t,P_u} = \mu_{P_t}\mu_{P_u}\gcd(k_{P_t}, k_{P_u})$, $\mu_{P_1,P_2,P_3} = \mu_{P_1}\mu_{P_2,P_3}\gcd(k_{P_1}, k_{P_2,P_3}))$, and $e_{tu} = \frac{\text{lcm}(Ind_g(\lambda_t), Ind_g(\lambda_u))}{Ind_g(\lambda_t)}$, $t \neq u$, $t, u = 1, 2, 3$, g a generator of Z_p^*. Also, let

$$\begin{aligned}
V_{P_t} &= \{\mathbf{x} \in Z_p^3 | P_t(S)\mathbf{x} = \mathbf{0}\},\\
V_{P_tP_u} &= \{\mathbf{x} \in Z_p^3 | P_t(S)P_u(S)\mathbf{x} = \mathbf{0}\},\\
V_{P_t,P_u} &= V_{P_tP_u} - V_{P_t} \cup V_{P_u},\\
V_{P_1,P_2P_3} &= V_{P_1P_2P_3} - V_{P_1} \cup V_{P_2P_3},\\
V_{P_1,P_2,P_3} &= V_{P_1P_2P_3} - \cup_{t=1}^{3} V_{P_t} \cup V_{P_1,P_2} \cup V_{P_1,P_3} \cup V_{P_2,P_3}.
\end{aligned}$$

Observe that

$$Z_p^3 = V_{P_1} \cup V_{P_2P_3} \cup V_{P_1,P_2P_3},$$

hence the S–orbit structure is the formal sum of S–orbits in V_{P_1}, $V_{P_2P_3}$, and V_{P_1,P_2P_3}. Let $\sum O_T$ be the formal sum of S–orbits in V_T. Thus, the formal sum of S–orbits in Z_p^3 can be expressed as

$$1 + \sum O_{P_1} + \sum O_{P_2P_3} + \sum O_{P_1,P_2P_3},$$

where, by Theorem 3.1.3,

$$\begin{aligned}
\sum O_{P_1} &= \mu_{P_1}(k_{P_1}),\\
\sum O_{P_2P_3} &= (1 + \mu_{P_1}(k_{P_1}))(1 + \mu_{P_2}(k_{P_2}))\\
&= \mu_{P_2}(k_{P_2}) + \mu_{P_3}(k_{P_3}) + \mu_{P_2,P_3}(k_{P_2,P_3}),\\
\sum O_{P_1,P_2P_3} &= \mu_{P_1,P_2}(k_{P_1,P_2}) + \mu_{P_1,P_3}(k_{P_1,P_3}) + \mu_{P_1,P_2,P_3}(k_{P_1,P_2,P_3}).
\end{aligned}$$

Let M be any nonsingular matrix that commutes with S. Thus, by Corollary 2.2.7, $M = Q(S)$, for some quadratic polynomial $Q(x)$. Let A be the nonsingular matrix for which

$$A^{-1}SA = \text{diag}(\lambda_1, \lambda_2, \lambda_3).$$

Thus,

$$A^{-1}MA = A^{-1}Q(S)A = Q(A^{-1}SA) = \text{diag}(Q(\lambda_1), Q(\lambda_2), Q(\lambda_3)).$$

Let $\beta_t = Q(\lambda_t)$. Hence, $\phi_M(x) = q_1(x)q_2(x)q_3(x)$, where $q_t(x) = x - \beta_t$. Also, let k_{q_t} be the order of q_t. It is straightforward to see that V_{P_1}, $V_{P_2P_3}$ as well as V_{P_1,P_2P_3} are M–invariant sets. Thus, the formal sum of MS–orbits in Z_p^3 can be expressed as

$$\mathcal{O}_{m_S} = 1 + \sum \mathcal{O}_{P_1} + \sum \mathcal{O}_{P_2P_3} + \sum \mathcal{O}_{P_1,P_2P_3}.$$

Furthermore,

$$\begin{aligned}\mathcal{O}_{P_2P_3} &= \mathcal{O}_{P_2} \cup \mathcal{O}_{P_3} \cup \mathcal{O}_{P_2,P_3},\\ \mathcal{O}_{P_1,P_2P_3} &= \mathcal{O}_{P_1,P_2} \cup \mathcal{O}_{P_1,P_3} \cup \mathcal{O}_{P_1,P_2,P_3}.\end{aligned}$$

Whence,

$$\begin{aligned}\sum \mathcal{O}_{P_2P_3} &= \sum \mathcal{O}_{P_2} + \sum \mathcal{O}_{P_3} + \sum \mathcal{O}_{P_2,P_3},\\ \sum \mathcal{O}_{P_1,P_2P_3} &= \sum \mathcal{O}_{P_1,P_2} + \sum \mathcal{O}_{P_1,P_3} + \sum \mathcal{O}_{P_1,P_2,P_3}.\end{aligned}$$

On the one hand, since $P_t(x)$ is irreducible, the MS–orbit structure in $\mathcal{O}_{P_t}$ is $\eta_{P_t}[i_{P_t}]$, where i_{P_t} is the smallest positive integer that solves $\lambda_t^{j_t} = \beta_t^{i_{P_t}} \pmod p$, for some integer j_t. By Theorem 2.3.16, $i_{P_t} = \frac{k_{q_t}}{\gcd(k_{P_t},k_{q_t})}$ and $\eta_{P_t} = \frac{\mu_{P_t}}{i_{P_t}} = \frac{p-1}{\mathrm{lcm}(k_{P_t},k_{q_t})i_{P_t}}$.

On the other hand, the smallest positive integer i_{P_t,P_u} that simultaneously solves

$$\lambda_t^{j_{P_t,P_u}} = \beta_t^{i_{P_t,P_u}} \pmod p \tag{4.64}$$
$$\lambda_u^{j_{P_t,P_u}} = \beta_u^{i_{P_t,P_u}} \pmod p \tag{4.65}$$

for some j_{P_t,P_u} is the length of the MS–orbits in $\mathcal{O}_{P_t,P_u}$. By Theorem 2.3.18,

$$i_{P_t,P_u} = \frac{p-1}{\gcd(e_{tu}\mathrm{Ind}_g(\beta_t) - e_{ut}\mathrm{Ind}_g(\beta_u), \gcd(k_{P_t}\eta_{P_t}, k_{P_u}\eta_{P_u}))}.$$

The number of MS–orbits in $\mathcal{O}_{P_t,P_u}$ is

$$\eta_{P_t,P_u} = \frac{\mu_{P_t,P_u}}{i_{P_t,P_u}} = \frac{\mu_{P_t}\mu_{P_u}\gcd(k_{P_t},k_{P_u})}{i_{P_t,P_u}} = \frac{(p-1)^2}{\mathrm{lcm}(k_{P_t},k_{P_u})i_{P_t,P_u}}.$$

Finally, the smallest positive integer i_{P_1,P_2,P_3} that simultaneously solves

$$\lambda_1^{j_{P_1,P_2,P_3}} = \beta_1^{i_{P_1,P_2,P_3}} \pmod p \tag{4.66}$$
$$\lambda_2^{j_{P_1,P_2,P_3}} = \beta_2^{i_{P_1,P_2,P_3}} \pmod p \tag{4.67}$$
$$\lambda_3^{j_{P_1,P_2,P_3}} = \beta_3^{i_{P_1,P_2,P_3}} \pmod p, \tag{4.68}$$

for some j_{P_1,P_2,P_3} is the length of the MS–orbits in $\mathcal{O}_{P_1,P_2,P_3}$. That is, the pair $(i_{P_1,P_2,P_3}, j_{P_1,P_2,P_3})$ must satisfy the following three pair of congruences

$$\lambda_1^{j_{P_1,P_2,P_3}} = \beta_1^{i_{P_1,P_2,P_3}} \pmod p \tag{4.69}$$
$$\lambda_2^{j_{P_1,P_2,P_3}} = \beta_2^{i_{P_1,P_2,P_3}} \pmod p \tag{4.70}$$

$$\lambda_1^{j_{P_1,P_2,P_3}} = \beta_1^{i_{P_1,P_2,P_3}} \pmod p \tag{4.71}$$
$$\lambda_3^{j_{P_1,P_2,P_3}} = \beta_3^{i_{P_1,P_2,P_3}} \pmod p, \tag{4.72}$$

$$\lambda_2^{j_{P_1,P_2,P_3}} = \beta_2^{i_{P_1,P_2,P_3}} \pmod p \tag{4.73}$$
$$\lambda_3^{j_{P_1,P_2,P_3}} = \beta_3^{i_{P_1,P_2,P_3}}. \pmod p \tag{4.74}$$

That is,

$$i_{P_1,P_2,P_3} = i_{P_1,P_2} t_1 \tag{4.75}$$
$$i_{P_1,P_2,P_3} = i_{P_1,P_3} t_2 \tag{4.76}$$
$$i_{P_1,P_2,P_3} = i_{P_2,P_3} t_3, \tag{4.77}$$

for some positive integers t_1, t_2, and t_3. Then,

$$i_{P_1,P_2,P_3} = \mathrm{lcm}(i_{P_1,P_2}, i_{P_1,P_3}, i_{P_2,P_3}) t_4 \text{ for some positive integer } t_4.$$

It is easy to see that $i_{P_1,P_2,P_3} = \mathrm{lcm}(i_{P_1,P_2}, i_{P_1,P_3}, i_{P_2,P_3})$ is the smallest positive integer fulfilling (4.66) – (4.77). The number of MS–orbits in $\mathcal{O}_{P_1,P_2,P_3}$ is

$$\eta_{P_1,P_2,P_3} = \frac{\mu_{P_1,P_2,P_3}}{i_{P_1,P_2,P_3}} = \frac{\mu_{P_1}\mu_{P_2,P_3}\gcd(k_{P_1}, k_{P_2,P_3})}{i_{P_1,P_2,P_3}} = \frac{(p-1)^3}{\mathrm{lcm}(k_{P_1}, k_{P_2}, k_{P_3}) i_{P_t,P_u}}. \diamondsuit$$

Example 4.4.6 *Assume matrix* $S = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 7 \end{pmatrix}$ *is defined over* Z_{13}. *We want to find another matrix* $M = \begin{pmatrix} \beta_1 & 0 & 0 \\ 0 & \beta_2 & 0 \\ 0 & 0 & \beta_3 \end{pmatrix}$,

$\lambda_1 = 2$, $\lambda_2 = 6$, $\lambda_3 = 7$. *In this case,* λ_i, $i = 1, 2, 3$, *are generators of* Z_{13}. *Hence,* $k_1 = k_2 = k_3 = 12$.

Recall that by Corollary 2.2.7, given S with three distinct eigenvalues, any matrix M that commutes with S can be written as $A \begin{pmatrix} \beta_1 & 0 & 0 \\ 0 & \beta_2 & 0 \\ 0 & 0 & \beta_3 \end{pmatrix} A^{-1}$ for some nonsingular matrix A, where g is a generator of Z_p^* and $\beta_i = g^{t_i}$ for some integer t_i. Hence, η_{m_S} depends on t_1, t_2, and t_3, and for this reason we denote η_{m_S} by $\eta_{m_S}(t_1, t_2, t_3)$.

Given three distinct nonzero values λ_1, λ_2, and λ_3 from Z_p, p prime, Algorithm 4.4.3 examines all possible triplets $(t_1', t_2', t_3') \in Z_p^* \times Z_p^* \times Z_p^*$ and returns a triplet (t_1, t_2, t_3) for which $\eta_{m_S}(t_1, t_2, t_3)$ is minimal, where $m_S(x) = P_1(x)P_2(x)P_3(x)$ and $P_i(x) = x - \lambda_i$, $i = 1, 2, 3$.

Algorithm 4.4.3

Inputs: $(\lambda_1, \lambda_2, \lambda_3)$, *prime* p.

Output: (t_1, t_2, t_3) *such that* $\eta_{m_S}(t_1, t_2, t_3)$ *is minimal.*

Assumption: *Precomputed log and antilog tables with respect to a primitive element* $g \in Z_p$ *are available.*

compute: $k_1, k_2, k_3, k_{1,2}, k_{1,3}, k_{2,3}, k_{1,2,3}$

compute: $e_{12}, e_{21}, e_{13}, e_{31}, e_{23}, e_{32}$

compute: $\mu_1, \mu_2, \mu_3, \mu_{1,2}, \mu_{1,3}, \mu_{2,3}, \mu_{1,2,3}$

initialize: t_1, t_2, t_3 *to* $p-1$

initialize: $\eta_1, \eta_2, \eta_3, \eta_{1,2}, \eta_{1,3}, \eta_{2,3}, \eta_{1,2,3}, \eta$ *to* p^3

for$(t_1' = 1$ *to* $t_1' = p-1)$ **do**

  compute: η_1'

  for$(t_2' = 1$ *to* $t_2' = p-1)$ **do**

    compute: η_2', $i_{1,2}'$, $\eta_{1,2}'$

    for$(t_3' = 1$ *to* $t_3' = p-1)$ **do**

      compute: η_3', $i_{1,3}'$, $i_{2,3}'$, $\eta_{2,3}'$, $\eta_{2,3}'$,$i_{1,2,3}'$, $\eta_{1,2,3}'$

      $\eta' \leftarrow \eta_1' + \eta_2' + \eta_3' + \eta_{1,2}' + \eta_{1,3}' + \eta_{2,3}' + \eta_{1,2,3}'$

      if$(\eta' < \eta)$

        $(t_1, t_2, t_3) \leftarrow (t_1', t_2', t_3')$

        $(\eta_1, \eta_2, \eta_3, \eta_{1,2}, \eta_{1,3}, \eta_{2,3}, \eta_{1,2,3}) \leftarrow (\eta_1', \eta_2', \eta_3', \eta_{1,2}', \eta_{1,3}', \eta_{2,3}', \eta_{1,2,3}')$

return (t_1, t_2, t_3)

The complexity of Algorithm 4.4.3 is as follows. There are three nested **for** loops and several *greatest common divisor* mod p operations inside them, which can be computed in $\log(p)$ arithmetic operations. Hence, the complexity of the overall algorithm is $O(p^3 \log(p))$.

Theorem 4.4.14 *Let* S *be a nonsingular matrix over* Z_p *with three distinct eigenvalues and* $m_S(x) = P_1(x)P_2(x)P_3(x)$, *where* $P_i(x) = x - \lambda_i$, $i = 1, 2, 3$. *Let* (t_1, t_2, t_3)

be a triplet for which $\eta_{m_S}(t_1, t_2, t_3)$ *is minimal. Also, let*

$$\begin{aligned}
d_1 &= \lambda_2 - \lambda_3, \\
d_2 &= \lambda_3 - \lambda_1, \\
d_3 &= \lambda_1 - \lambda_2, \\
d &= (-(\lambda_2 d_2(\lambda_1 + \lambda_3) + \lambda_1 d_1(\lambda_2 + \lambda_3) + \lambda_3 d_3(\lambda_1 + \lambda_2)))^{-1}, \\
c_2 &= d(d_1 g^{t_1} + d_2 g^{t_2} + d_3 g^{t_3}), \\
c_1 &= d(-d_1(\lambda_2 + \lambda_3) g^{t_1} + d_2(\lambda_1 + \lambda_3) g^{t_2} - d_3(\lambda_1 + \lambda_2) g^{t_3}), \\
c_0 &= g^{t_3} - (c_2 \lambda_3^2 + c_1 \lambda_3).
\end{aligned}$$

Then, an optimal matrix for S *is*

$$M = c_2 S^2 + c_1 S + c_0 I_3.$$

Proof
Let $S' = \text{diag}(\lambda_1, \lambda_2, \lambda_3)$. It is clear that $M' = \text{diag}(g^{t_1}, g^{t_2}, g^{t_3})$ is optimal for S' since Algorithm 4.4.3 examines all possible triplets (t_1, t_2, t_3) from $Z_p^* \times Z_p^* \times Z_p^*$ and selects one that minimizes η_{m_S}.

On the other hand, let A be a nonsingular matrix for which $A^{-1}SA = S'$. Let $M = AM'A^{-1}$. It is clear that M and S commute. Now, by Corollary 2.2.7, there exists a polynomial $Q(x) = c_2 x^2 + c_1 x + c_0$, such that $M = Q(S)$. Thus,

$$M' = A^{-1} Q(S) A = Q(A^{-1} S A) = Q(S').$$

Hence,

$$\begin{aligned}
g^{t_1} &= c_2 \lambda_1^2 + c_1 \lambda_1 + c_0, \\
g^{t_2} &= c_2 \lambda_2^2 + c_1 \lambda_2 + c_0, \\
g^{t_3} &= c_2 \lambda_3^2 + c_1 \lambda_3 + c_0,
\end{aligned}$$

which is equivalent to

$$\begin{pmatrix} \lambda_1^2 & \lambda_1 & 1 \\ \lambda_2^2 & \lambda_2 & 1 \\ \lambda_3^2 & \lambda_3 & 1 \end{pmatrix} \begin{pmatrix} c_2 \\ c_1 \\ c_0 \end{pmatrix} = \begin{pmatrix} g^{t_1} \\ g^{t_2} \\ g^{t_3} \end{pmatrix} \tag{4.78}$$

System (4.78) has a unique solution since we can show that the columns of the underlying matrix, say $\mathbf{V}$ known as a Vandermonde matrix, are linearly independent.

The inverse of $\mathbf{V}$ is

$$\mathbf{V}^{-1} = d \begin{pmatrix} d_1 & d_2 & d_3 \\ -d_1(\lambda_2+\lambda_3) & d_2(\lambda_1+\lambda_3) & -d_3(\lambda_1+\lambda_2) \\ -d_2\lambda_2(\lambda_1+\lambda_3) & -d_1\lambda_1(\lambda_2+\lambda_3) & -d_3\lambda_3(\lambda_1+\lambda_2)), \end{pmatrix} \tag{4.79}$$

where

$$d = \det(\mathbf{V})^{-1} = (-(\lambda_2 d_2(\lambda_1+\lambda_3) + \lambda_1 d_1(\lambda_2+\lambda_3) + \lambda_3 d_3(\lambda_1+\lambda_2)))^{-1}.$$

Finally,

$$\begin{pmatrix} c_2 \\ c_1 \\ c_0 \end{pmatrix} = \mathbf{V}^{-1} \begin{pmatrix} g^{t_1} \\ g^{t_2} \\ g^{t_3} \end{pmatrix} .\diamondsuit \tag{4.80}$$

4.4.8 General algorithm for computing three–dimensional optimal matrices

We summarize the results for, given a nonsingular matrix S, choosing an optimal matrix M in the three–dimensional cases in the following

Algorithm 4.4.4

Inputs: *prime p, nonsingular 3×3 matrix S over Z_p, primitive polynomials $P(x) = x^3 + ax^2 + bx + c$, $R(x) = x^2 + a_R x + g$.*

Output: *optimal matrix M*

1. *compute $\phi_S(x)$;*

2. *compute the roots of $\phi_S(x)$;*

3. *compute $m_S(x)$;*

I. **if** *$\phi_S(x)$ is irreducible,*

   1 *compute c_0, c_1, c_2 such that $P(c_2S^2+c_1S+c_0I_3) = \mathbf{0}$, the 3×3 zero matrix;*

   2 *set $M = c_2S^2 + c_1S + c_0I_3$.*

II. **if** *$\phi_S(x) = P_1(x)(x-\lambda)$, where $P_1(x) = x^2+d_1x+f_1$ is quadratic and irreducible,*

1 *compute* (t_1, t_2) *such that* $\eta_{m_S}(t_1, t_2)$ *is minimal;*

2 *compute* $N = eC_{P_1} + fI_2$, *where* $e^2 = \frac{a_R^2 - 4b_R}{d_1^2 - 4f_1}$, $f = 2^{-1}(ed_1 - a_R)$;

3 *compute* $N^{t_1} = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}$;

4 *compute*

$$\begin{aligned} c_2 &= (f_1^{-1}\lambda u_{12} + g^{t_2} - u_{11})P_1(\lambda)^{-1}, \\ c_1 &= d_1 c_2 - f_1^{-1} u_{12}, \\ c_0 &= u_{11} + c_2 f_1; \end{aligned}$$

5 *set* $M = c_2 S^2 + c_1 S + c_0 I_3$.

III. **if** $m_S(x) = x - \lambda$, *set* $M = \begin{pmatrix} 0 & 0 & -c \\ 1 & 0 & -b \\ 0 & 1 & -a \end{pmatrix}$.

IV. **if** $\phi_S(x) = P_1(x)^2 P_2(x)$ *and* $m_S(x) = P_1(x)P_2(x)$, *where* $P_1(x) = x - \lambda_1$, $P_2(x) = x - \lambda_2$, $\lambda_1 \neq \lambda_2$,

1 *compute* A *such that* $A^{-1}SA = diag(\lambda_1, \lambda_1, \lambda_2)$;

2 *compute* (t_1, t_2, TAG) *such that* η_{m_S} *is minimal;*

3.1 **if** $(TAG = 1)$ *set* $N = C_R^{t_1}$;

3.2 **else** *set* $N = diag(g^{t_1}, g^{t_1})$;

4 *set* $M = A^{-1} \begin{pmatrix} N & 0 \\ 0 & g^{t_2} \end{pmatrix} A$.

V. **if** $m_S(x) = (x - \lambda)^3$, *then set* $M = (S - \lambda I_3)^2 + gI_3$.

VI. If $m_S(x) = P_1(x)^2 P_2(x)$, *where* $P_1(x) = x - \lambda_1$, $P_2(x) = x - \lambda_2$, $\lambda_1 \neq \lambda_2$,

1 *compute* (t_1, t_2) *such that* $\eta_{P_1 P_2}$ *is minimal;*

2 *compute*

$$\begin{aligned} c_2 &= (g^{t_2} - g^{t_1})(\lambda_2 - \lambda_1)^{-2}, \\ c_1 &= -2c_2\lambda_1, \\ c_0 &= g^{t_1} - (c_2\lambda_1^2 + c_1\lambda_1); \end{aligned}$$

3 *set* $M = c_2S^2 + c_1S + c_0I_3$.

VII. **if** $\phi_S(x) = P_1(x)^3$ *and* $m_S(x) = P_1(x)^2$, *where* $P_1(x) = x - \lambda$,

1 *compute* A *such that* $A^{-1}SA = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}$;

2 *set* $M = A^{-1} \begin{pmatrix} g & 0 & 1 \\ 0 & g & 0 \\ 0 & 1 & g \end{pmatrix} A$.

VIII. **if** $m_S(x) = P_1(x)P_2(x)P_3(x)$, *where for* $i = 1, 2, 3$, $P_i(x) = x - \lambda_i$, $\lambda_i \neq \lambda_j$, $i \neq j$,

1 *compute* (t_1, t_2, t_3) *such that* $\eta_{m_S}(t_1, t_2, t_3)$ *is minimal;*

2 *compute*

$$\begin{aligned} d_1 &= \lambda_2 - \lambda_3, \quad d_2 = \lambda_3 - \lambda_1, \quad d_3 = \lambda_1 - \lambda_2, \\ d &= (-(\lambda_2 d_2(\lambda_1 + \lambda_3) + \lambda_1 d_1(\lambda_2 + \lambda_3) + \lambda_3 d_3(\lambda_1 + \lambda_2)))^{-1}, \\ c_2 &= d(d_1 g^{t_1} + d_2 g^{t_2} + d_3 g^{t_3}), \\ c_1 &= d(-d_1(\lambda_2 + \lambda_3)g^{t_1} + d_2(\lambda_1 + \lambda_3)g^{t_2} - d_3(\lambda_1 + \lambda_2)g^{t_3}), \\ c_0 &= g^{t_3} - (c_2\lambda_3^2 + c_1\lambda_3); \end{aligned}$$

3 *set* $M = c_2S^2 + c_1S + c_0I_3$.

end

Chapter 5

A Solution to reverse engineering genetic networks

We are in the genome era. After decoding the human genome, the next stumbling block is to understand the function of genes and how they interact with each other, so that drugs can be created to cure diseases. Researchers in the area have proposed Boolean networks to describe the logic of the genes, in a manner similar to the way boolean functions describe the logic of computers. But it is useful to generalize the Boolean model to finite field models and thus take advantage of a number of efficient algorithms that have recently been developed for applications in error–correcting codes and public–key cryptography.

The reverse engineering problem can be described roughly as follows: Given a set of biological measurements, determine the function that fits the data. Laubenbacher *et al* [23], [24] and Green [16] have addressed the reverse engineering problem for genetic networks using multivariable polynomials over finite fields and Groebner bases.

In this chapter we consider another approach which can be computationally very efficient. We consider a "lifting" method, described in more detail in section ??, that consists of lifting a multivariable polynomial to a univariable polynomial over a large finite field. There are very efficient algorithms available for the univariable case.

In section 5.1 we review the multivariable and single variable models for genetic networks introduced in section 3.3 and discuss their relationship between them in section 5.2. In section 5.3 we define the reverse engineering problem. In section 5.4

we discuss methods for fast arithmetic over finite fields and in section 5.5 we give a parallel solution to reverse engineering genetic networks.

5.1 Boolean and finite field genetic networks

Various researchers have described genetic regulatory networks using Boolean variables to represent gene expression levels or stimuli. For example, Ideker *et al* [22] give the following definition:

Definition 5.1.1 *A* **Boolean genetic network** *(BGN) consists of a directed graph G having n, numbered nodes $0, 1, \ldots, n-1$, such that for each node i there is an associated n–ary Boolean function f_i. We denote such a BGN by $(G, \{f_0, f_1, \ldots, f_{n-1}\})$.*

An expression matrix is a set of measurements (such as those which result from microarray experiments) made by disrupting or overexpressing especific genes from a genetic network. From this expression data, the challenge is to reconstruct or reverse engineer the genetic network.

In the Boolean model, either a gene can affect another gene or not. An alternative model that has been studied by several researchers [23], [27] is the finite field genetic network. In this model, one is able to capture graded differences in gene expression. Another advantage of the finite field model is that, as noted in section 3.3.2, it can be considered as a generalization of the Boolean model since each Boolean operation can be expressed in terms of the sum and product in Z_2. In particular,

$$x \cap y = x \cdot y \tag{5.1}$$
$$x \cup y = x + y + x \cdot y \tag{5.2}$$
$$\tilde{x} = x + 1 \tag{5.3}$$

It is thus natural to generalize the Boolean model as follows.

Definition 5.1.2 *A* **multivariable finite field genetic network** *(MFFGN) is a finite dynamical system $(GF(q)^n, f, GF(q))$, where functions f_i are defined by $f_i : GF(q)^n \to GF(q)$, $i = 0, 1, \ldots, n-1$. The function $f : GF(q)^n \to GF(q)^n$ is defined by*

$$f(x_0, x_1, \cdots, x_{n-1}) = (f_0(x_0, \cdots, x_{n-1}), \cdots, f_{n-1}(x_0, x_1, \cdots, x_{n-1})).$$

Each f_i can be expressed as a polynomial in n variables. For this reason, we refer to a network of the type defined above as a *multivariable finite field genetic network* ("MFFGN").

Clearly, every BGN is also a MFFGN over $GF(2)$. Each of the f_i can be expressed as a polynomial over $GF(2)$ by replacing each Boolean operation by one of the expressions given in equations (5.1) – (5.3).

Another approach taken by Moreno *et al* is to replace the n functions f_i defined on $GF(q)$ by a single function f that maps $GF(q^n)$ to $GF(q^n)$.

Definition 5.1.3 *A* **univariable finite field genetic network** *(UFFGN) is a finite dynamical system* $(GF(q^n), g, GF(q))$, *where* $GF(q^n)$ *is represented by the vector space* $\{a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0\}$ *and* α *is a zero of an irreducible polynomial over* $GF(q)$.

5.2 Equivalence of the multivariable and single variable models

The two types of models given in the previous section can be viewed in some sense as equivalent. In order to make this idea more precise, we first note that for any zero α of an irreducible polynomial of degree n over $GF(q)$, there is a natural correspondence between $GF(q)^n$ and $GF(q^n)$ given by

$$\varphi_\alpha(x_0, x_1, \cdots, x_{n-1}) = x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1}.$$

Definition 5.2.1 *We say that a MFFGN* $M = (GF(q)^n, f, GF(q))$ *is* **isomorphic** *to a UFFGN* $U = (GF(q^n), g, GF(q))$, *if there exists* $\alpha \in GF(q^n)$ *such that for all* $(x_0, x_1, \cdots, x_{n-1}) \in GF(q)^n$,

$$\varphi_\alpha(f(x_0, x_1, \cdots, x_{n-1})) = g(\varphi_\alpha(x_0, x_1, \cdots, x_{n-1})).$$

Given a MFFGN $M = (GF(q)^n, f, GF(q))$, it is easily seen that there is an isomorphic UFFGN $U = (GF(q^n), g, GF(q))$ since we need only to define

$$g(x_0, x_1, \cdots, x_{n-1}) = \varphi_\alpha(f(x_0, x_1, \cdots, x_{n-1}))$$

for all $(x_0, x_1, \cdots, x_{n-1})$. Thus,

Theorem 5.2.1 *For every MFFGN $M = (GF(q)^n, f, GF(q))$ there is an UFFGN $U = (GF(q^n), g, GF(q))$ that is isomorphic to M.*

Since every function defined on a finite field $GF(q)$ can be expressed as a univariant polynomial over $GF(q)$, it is natural to ask how one can determine the polynomial corresponding to the function g of Theorem 5.2.1. The answer is given by the discrete Fourier transform over $GF(q)$, which we now define.

Let ω be a primitive root in $GF(q)$, i.e., ω is a generator of the multiplicative cyclic group of $GF(q) - \{0\}$. A *discrete Fourier transform* ("DFT") over $GF(q)$ is a linear transformation on the vector space $\{(a_0, a_1, \cdots, a_{q-2}) | a_i \in GF(q)\}$ defined by the matrix

$$F_{q,\omega} = [\omega^{ij}], \quad i, j = 0, 1, \cdots, q-2 \tag{5.4}$$

Corollary 5.2.1 *Let $B_0 = \varphi(f(0, 0, \cdots, 0))$ and for each $i = 1, 2, \cdots, q^n - 1$, let $B_i = \varphi_\alpha(f(a_{n-1,i} \cdots, a_{0,i}))$ where $\alpha \in GF(q^n)$ is a root of an irreducible polynomial over $GF(q)$ and where $a_{n-1,i}\alpha^{n-1} + \cdots + a_{1,i} + a_{0,i} = \alpha^{i-1}$. Then g is given by the polynomial*

$$A_{q^n-1}x^{q^n-1} + A_{q^n-2}x^{q^n-2} + \cdots A_2x^2 + A_1x + A_0 \tag{5.5}$$

where $A_0 = B_0$ and

$$\begin{bmatrix} A_{q^n-1} \\ A_{q^n-2} \\ \vdots \\ A_1 \end{bmatrix} = F^{-1}_{q^n,\alpha} \begin{bmatrix} B_1 - A_0 \\ B_2 - A_0 \\ \vdots \\ B_{q^n-1} - A_0 \end{bmatrix} \tag{5.6}$$

Example 5.2.1 *Recall the MFFGN equivalent of Ideker's Boolean network given in Example 3.3.1:*

$$f_0(x_0, x_1, x_2, x_3) \;\; = \;\; 1,$$

$$
\begin{aligned}
f_1(x_0, x_1, x_2, x_3) &= 1, \\
f_2(x_0, x_1, x_2, x_3) &= x_0 \cap x_1, \\
f_3(x_0, x_1, x_2, x_3) &= x_1 \cap \tilde{x}_2.
\end{aligned}
$$

To compute an equivalent UFFGN over $GF(2^4)$*, take* $P(x) = x^4 + x + 1$ *to be the irreducible polynomial over* $GF(2)$.

In order to carry out the necessary computations, it is convenient to construct a table of α^i, $i = 0, 1, 2, \cdots, 2^4 - 2 = 14$, *in terms of polynomials* $a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0$.

i	a_3	a_2	a_1	a_0
0	0	0	0	1
1	0	0	1	0
2	0	1	0	0
3	1	0	0	0
4	0	0	1	1
5	0	1	1	0
6	1	1	0	0
7	1	0	1	1
8	0	1	0	1
9	1	0	1	0
10	0	1	1	1
11	1	1	1	0
12	1	1	1	1
13	1	1	0	1
14	1	0	0	1

Table 5.2.1 : α^i *in* $GF(2^4)$ *in terms of* $a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0$

Such a table can also be regarded as a table for φ where images are expressed as powers of α.

Now we have

$$\begin{aligned} B_0 &= \varphi(f(0,0,\cdots,0)) \qquad (5.7)\\ &= \varphi(f_0(0,0,0,0), f_1(0,0,0,0), f_2(0,0,0,0), f_3(0,0,0,0)) \\ &= \varphi(1,1,0,0) \\ &= \alpha^6 \\ B_1 &= \varphi(f(0,0,0,1)) = \varphi(1,1,0,0) = \alpha^6 \qquad (5.8)\\ B_2 &= \varphi(f(0,0,1,0)) = \varphi(1,1,0,0) = \alpha^6 \qquad (5.9) \end{aligned}$$

Similarly, we have $B_3 = \alpha^{13}$, $B_4 = \alpha^6$, $B_5 = \alpha^6$, $B_6 = \alpha^6$, $B_7 = \alpha^{12}$, $B_8 = \alpha^6$, $B_9 = \alpha^{13}$, $B_{10} = \alpha^6$, $B_{11} = \alpha^6$, $B_{12} = \alpha^{11}$, $B_{13} = \alpha^{12}$, $B_{14} = \alpha^{12}, B_{15} = \alpha^6$. *Thus,*

$$[A_{15}, A_{14}, A_{13}, \cdots, A_1]^T = F_{16,\alpha}[0,0,1,0,0,0,\alpha^4,0,1,0,0,\alpha,\alpha,\alpha^4,0]^T \qquad (5.10)$$

and so M is isomorphic to the UFFGN

$$U = (G, \alpha^3x^{12} + \alpha^8x^{10} + \alpha^{13}x^9 + \alpha^6x^8 + \alpha^6x^6 + \alpha^2x^5 + \alpha^{10}x^4 + \alpha^{14}x^3 + \alpha^3x^2 + \alpha x + \alpha^6, GF(2^4)).$$

In this example, we have computed the Fourier transform from its definition, which, in general, would require time $O(q^{2n})$ for the conversion of an MFFGN to an UFFGN. If instead we use a fast Fourier transform, the time can be reduced to $O(nq^n)$.

It is easy to prove the converse of Theorem 5.2.1.

Theorem 5.2.2 *For every UFFGN $U = (GF(q^n), g, GF(q))$, there is an equivalent MFFGN, $M = (GF(q)^n, f, GF(q))$.*

Proof
The functions f_i are defined by

$$[f_0(x_0, x_1, \cdots, x_{n-1}), \cdots, f_{n-1}(x_0, \cdots, x_1)]^T = \varphi_\alpha^{-1}(g(\varphi_\alpha(x_0, x_1, \cdots, x_{n-1})) \quad (5.11)$$

It follows from (5.2.1) that

$$\begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_{q^n-1} \end{bmatrix} = F_{q^n,\alpha} \begin{bmatrix} A_{p^n-1} \\ \vdots \\ A_1 \end{bmatrix} + \begin{bmatrix} A_0 \\ \vdots \\ A_0 \end{bmatrix} \quad (5.12)$$

and the values of the f_i can be calculated by applying this DFT and then calculating $f(a_{n-1,i}, \cdots, a_{0,i}) = \varphi_\alpha^{-1}(B_i)$.

In order to express each f_i algebraically we can express $g(\varphi_\alpha(x_0, \cdots, x_{n-1}))$ as a polynomial in α. Then the coefficient of each α^i is the value of $f_i(x_0, \cdots, x_{n-1})$.$\diamondsuit$

Example 5.2.2 *Let* $U = (G(3)^3, g = \alpha^{11}x^2 + \alpha^{18}x + \alpha^{11}, GF(3))$, *where* $\alpha \in GF(3^3)$ *is a root of* $x^3 + 2x + 1$. *Then*

$$\begin{aligned} g(\varphi_\alpha(x_2, x_1, x_0)) &= \alpha^{11}(x_0\alpha^2 + x_1\alpha + x_0)^2 + \alpha^{18}(x_2\alpha^2 + x_1\alpha + x_0) + \alpha^{11} \\ &= x_2^2\alpha^{15} + 2x_1x_2\alpha^{14} + (x_1^2 + 2x_0x_2)\alpha^{13} + 2x_0x_1\alpha^{12} + x_0^2\alpha^{11} + \\ &\quad x_2\alpha^{20} + x_1\alpha^{19} + x_0\alpha^{18} + \alpha^{11} \\ &= (2x_2^2 + 2x_0x_1 + x_0^2 + 2x_2 + 2x_1 + x_0 + 1)\alpha^2 + \\ &\quad (x_1x_2 + x_0^2 + x_2 + 2x_1 + 2x_0 + 1)\alpha + \\ &\quad 2x_1^2 + x_0x_2 + x_0x_1 + 2x_0^2 + x_2 + 2x_1 + x_0 + 2 \end{aligned}$$

Hence

$$\begin{aligned} f_1(x_2, x_1, x_0) &= 2x_2^2 + 2x_0x_1 + x_0^2 + 2x_2 + 2x_1 + x_0 + 1 \\ f_2(x_2, x_1, x_0) &= x_1x_2 + x_0^2 + x_2 + 2x_1 + 2x_0 + 1 \\ f_3(x_2, x_1, x_0) &= 2x_1^2 + x_0x_2 + x_0x_1 + 2x_0^2 + x_2 + 2x_1 + x_0 + 2. \end{aligned}$$

5.3 Reverse engineering

Given specific experimental data, how do we fit it to a specific model (either MFFGN or UFFGN)? This is known as the reverse engineering problem. More precisely, borrowing from Laubenbacher [23], we define this problem as follows: Given a time series $s_1, s_2, \cdots, s_k$ of measurements of gene expressions and a set of conditions χ, find all functions f - either $f : GF(q)^n \to GF(q)^n$, i.e., a set of functions f_i, $i = 0, 1, \cdots, n-1$ such that each $f_i : GF(q)^n \to GF(q)$, or $f : GF(q^n) \to GF(q^n)$ - with the property that $s_{i+1} = f(s_i)$, where $s_i = (a_0, a_1, \cdots, a_{n-1})$, and which satisfy the conditions in χ. Determining an $f : GF(q^n) \to GF(q^n)$, i.e., an UFFGN, gives global information about the network, whereas determining a set of functions $f_i : GF(q)^n \to GF(q)$, i.e., an MFFGN, gives local information at each node of the network.

If $k = q^n - 1$, then we already know how to determine the above f, i.e., by a DFT. If $k < p^n - 1$, we can use interpolation for either type of model. This gives

$$f_i(x_0, x_1, \cdots, x_{n-1}) = f_i'(x_0, x_1, \cdots, x_{n-1}) + h_i(x_0, x_1, \cdots, x_{n-1}), \quad i = 0, 1, \cdots, n-1$$

in the MFFGN case and

$$g(x) = g'(x) + h(x),$$

in the UFFGN case, where f_i', $i = 0, 1, \cdots, n-1$ and $g\prime$ are polynomials that interpolate the given k points and where the h_i and h are polynomials that vanish on the interpolated points.

The interpolation described by Laubenbacher [23] for the MFFGN case is essentially Lagrange interpolation. The computational complexity for Lagrange interpolation is $O(k^2)$, where k is the number of interpolated points and thus, the total time to interpolate at each of the n nodes is $O(nk^2)$.

In the UFFGN case it is necessary to interpolate only once. Furthermore, other interpolation methods are more efficient than Lagrange. For example, the time required to interpolate k points with Lipson's [26] method is $O(k\ log^2\ k)$. Another advantage of Lipson's algorithm is that it can be parallelized, which is very useful for very large genetic networks [5].

5.4 Fast finite field arithmetic

In order to adapt either Lagrange or Lipson interpolation to finite fields, we need efficient algorithms for finite field arithmetic of polynomials over arbitrary finite fields. In the last few years there has been considerable progress in developing just such

algorithms, particularly for applications in cryptography [38, 39, 18, 17, 41].

We assume that the coefficients of all polynomials over $GF(p^m)$ are written in the form α^i where α is a generator of the multiplicative cyclic group of $GF(p^m)$. The addition of two such polynomials then requires us to determine for a given a and b a number c such that $\alpha^c = \alpha^a + \alpha^b$. For the multiplication of two such polynomials we need to both add and multiply powers of α. This latter operation can be effected by simply adding the exponents modulo $p^m - 1$.

To add powers of α we use a table of Zech logarithms (also known as Jacobi logarithms). Every element of $GF(p^m)$ can be written in the form $1 + \alpha^i = \alpha^{z(i)}$ for some $z(i)$, $0 \leq z(i) \leq p^m - 1$. We note that $\alpha^a + \alpha^b = \alpha^a(1 + \alpha^{(b-a) \bmod p^m - 1})$. Hence, to add two powers of α we need only to compute a Zech log and add exponents. It is useful to also note that, if p is odd, $-1 = \alpha^{(p^m-1)/2}$ and so $\alpha^a - \alpha^b$ can be computed by $\alpha^a + \alpha^{(p^m-1)/2} \cdot \alpha^b = \alpha^a + \alpha^{((p^m-1)/2+b) \bmod p^m-1}$.

To construct a table of Zech logs, we first determine a primitive element α so that each field element x can be expressed as $x = \alpha^i$. We then construct an auxiliary table $A[i]$, $i = 1, 2, \cdots, p^m - 1$ such that each $A[i] = \alpha^i$. The table $Z[i]$ of Zech logs is then constructed by setting each $Z[i] = j$ where j is the index for which $A[j] = A[i] + 1$.

The following table gives the Zech logs for $GF(2^3)$ using the primitive polynomial $x^3 + x + 1$.

i	1	2	3	4	5	6	7	8	9	10	11	12	13
$z(i)$	9	21	1	18	17	11	4	15	3	6	10	2	$*$

i	14	15	16	17	18	19	20	21	22	23	24	25	26
$z(i)$	16	25	22	20	7	23	5	12	14	24	19	8	13

Table 5.4.1 : Zech Logs for $GF(3^3)$.

5.5 Solution to the reverse engineering problem for genetic networks

Given a time series $s_1, s_2, \cdots, s_k$ of measurements of gene expressions and a set of conditions χ, we want to find all functions $f : GF(q^n) \to GF(q^n)$ with the property that $s_{i+1} = f(s_i)$, where $s_i = (a_0, a_1, \cdots, a_{n-1})$, and which satisfy the conditions in χ. In order to do this we want to determine a polynomial $f'(x)$ that interpolates the given k points and such that $f(x) = f'(x) + h(x)$, where $h(x)$ is determined by the

conditions in χ.

An efficient algorithm for interpolation and one which can readily be parallelized is Lipson's algorithm [26]. This algorithm is based on the Chinese remainder theorem for polynomials, which says that given a set of n pairwise relatively prime polynomials

$$p_0(x),\ p_1(x),\ \ldots,\ p_{n-1}(x)$$

and a set of residues

$$f_0(x),\ f_1(x),\ \ldots,\ f_{n-1}(x),$$

there exists a unique polynomial $f(x)$ of degree less than the degree of

$$P(x) = p_0(x)p_1(x)\cdots p_{n-1}(x)$$

which solves the set of congruences

$$f(x) = f_i(x) \mod p_i(x),\ i = 0, 1, \cdots, n-1$$

Polynomial $f(x)$ is given by:

$$f(x) = \sum_{i=0}^{n-1} \epsilon_i d_i f_i \mod P(x),$$

where $\epsilon_i = P'(x_i)$ (i.e., ϵ_i is the formal derivative of $P(x)$ evaluated at $x = x_i$.)

In the special case of polynomial interpolation, the polynomials $p_i(x)$ are of the form $p_i(x) = x - x_i$, which are relatively prime since the x_i are distinct.

The sequential interpolation algorithm of Lipson can be depicted as follows:

Algorithm 5.5.1 (Lipson)

Input: $\{(x_0, y_0), (x_1, y_1), \ldots, (x_{k-1}, y_{k-1})\}$, $k = 2^t$.

Output: *Interpolating polynomial* $f(x)$, $0 \leq deg(f(x)) < k$, *such that* $f(x_i) = y_i$.

1. *Compute* $q_{i,j} = \prod_{m=i}^{i+2^j-1} p_m(x)$, $0 \leq j < t$, i *a multiple of* 2^j *and* $0 \leq i < k$.

2. *Compute* $d_i = (P'(x_i))^{-1}$, *where* P' *is the derivative of*
   $P(x) = q_{0,t} = (x - x_0)(x - x_1)\cdots(x - x_{n-1})$.

3. *Compute* $S_{i,0} = d_i \cdot y_i$, *for* $0 \leq i < k$ *and* i *a multiple of* 2^j *and*

$S_{i,j} = S_{i,j-1} \cdot q_{i+2^{j-1},j-1} + S_{i+2^{j-1},j-1} \cdot q_{i,j-1}$ *for* $0 < j < t$.

It is easily shown that the arithmetic complexity of the above Algorithm 5.5.1 is $O(k\ log^2 k)$, which is superior to the $O(k^2)$ interpolation of Lagrange.

Let us examine the possibility of parallelizing Lipson's algorithm. We first note that $q_{i,j}$ and $S_{i,j}$ can be defined recursively:

$$q_{i,j} = q_{i,j-1} \cdot q_{i+2^{j-1},j-1} \tag{5.13}$$

(5.14)

$$S_{i,j} = S_{i,j-1} \cdot q_{i+2^{j-1},j-1} + S_{i+2^{j-1},j-1} \cdot q_{i,j-1} \tag{5.15}$$

Thus, each of the $q_{i,j}$ and $S_{i,j}$ from (5.13) and (5.15) can be computed in parallel. The $S_{i,j}$ depend on the $q_{i,j}$ and in fact, the initial values $S_{i,0}$ depend on the values of $d_i = (P'(x_i))^{-1}$, which in turn depend on the last computed value of $q_{i,j}$, i.e., $q_{0,t}$. We note that

$$P'(x_i) = \prod_{0 \leq j \neq i \leq n-1} (x_i - x_j)$$

and so the d_i can be computed independently of $P(x)$ at no extra cost. We thus have the following parallel version of Lipson's algorithm:

Algorithm 5.5.2 (Parallel Lipson)

Input: $\{(x_0, y_0), (x_1, y_1), \ldots, (x_{k-1}, y_{k-1})\}$, $k = 2^t$.

Output: *Interpolating polynomial* $f(x)$, $0 \leq deg(f(x)) < k$, *such that* $f(x_i) = y_i$.

for *(*$i = 0$ *to* $i = n$*)* **do in parallel**

$d_i = \prod_{0 \leq j \neq i \leq n-1}(x_i - x_j)$;

$S_{i,0} = d_i \cdot y_i$;

$q_{i,0} = x - x_i$;

for *(*$j = 1$ *to* $j = t - 1$*)* **do**

for *(*$i = 0$ *to* $i = k - 1$ *step* 2^j*)* **do in parallel**

$S_{i,j} = S_{i,j-1} \cdot q_{i+2^{j-1},j-1} + S_{i+2^{j-1},j-1} \cdot q_{i,j-1}$

$q_{i,j} = q_{i,j-1} \cdot q_{i+2^{j-1},j-1}$;

The entire computation carried out by Algorithm 5.5.2 can be represented by a complete binary tree with height $\log k$. Load balancing is achieved by assigning a processor to every node. The only communications necessary are between parent nodes and their children.

We have implemented this algorithm in C/openMP on an SGI 3000 with 32 processors.

Example 5.5.1 *Let* $\{(\alpha, \alpha^{16}), (\alpha^{16}, \alpha^{22}), (\alpha^{22}, \alpha^{15}),$ $(\alpha^{15}, \alpha^2)\}$ *be a set of four points in* $GF(3^3) \times GF(3^3)$*, where* α *is a primitive element of* $GF(3^3)$*. Find a polynomial* $f(x)$ *of degree at most 3 that interpolates this set of points using Algorithm 5.5.2.*

- *First, compute the* d_i*,* $S_{i,0}$*, and* $q_{i,0}$*.*

$$
\begin{aligned}
d_0 &= [(x_0 - x_1)(x_0 - x_2)(x_0 - x_3)]^{-1} \\
&= [(\alpha - \alpha^{16})(\alpha - \alpha^{22})(\alpha - \alpha^{15})]^{-1} \\
&= (\alpha^{22}\alpha^{16}\alpha^{10})^{-1} \\
&= (\alpha^{22})^{-1} \\
&= \alpha^4 \\
S_{0,0} &= \alpha^4\alpha^{16} \\
&= \alpha^{20} \\
q_{0,0} &= x - \alpha \\
d_1 &= [(x_1 - x_0)(x_1 - x_2)(x_1 - x_3)]^{-1} \\
&= [(\alpha^{16} - \alpha)(\alpha^{16} - \alpha^{22})(\alpha^{16} - \alpha^{15})]^{-1} \\
&= (\alpha^9\alpha^{13}\alpha^{18})^{-1}
\end{aligned}
$$

$$
\begin{aligned}
&= (\alpha^{14})^{-1} \\
&= \alpha^{12} \\
S_{1,0} &= \alpha^{12}\alpha^{22} \\
&= \alpha^{8} \\
q_{1,0} &= x - \alpha^{16} \\
d_2 &= [(x_2 - x_0)(x_2 - x_1)(x_2 - x_3)]^{-1} \\
&= [(\alpha^{22} - \alpha)(\alpha^{22} - \alpha^{16})(\alpha^{22} - \alpha^{15})]^{-1} \\
&= (\alpha^{3}\alpha^{26}\alpha^{7})^{-1} \\
&= (\alpha^{10})^{-1} = \alpha^{16} \\
S_{2,0} &= \alpha^{16}\alpha^{15} \\
&= \alpha^{5} \\
q_{2,0} &= x - \alpha^{22} \\
d_3 &= [(x_3 - x_0)(x_3 - x_1)(x_3 - x_2)]^{-1} \\
&= [(\alpha^{15} - \alpha)(\alpha^{15} - \alpha^{16})(\alpha^{15} - \alpha^{2}]^{-1} \\
&= (\alpha^{23}\alpha^{5}\alpha^{20})^{-1} \\
&= (\alpha^{22})^{-1} = \alpha^{4} \\
S_{3,0} &= \alpha^{4}\alpha^{2} \\
&= \alpha^{6} \\
q_{3,0} &= x - \alpha^{15}
\end{aligned}
$$

- *Second, compute the* $S_{i,1}$ *and* $q_{i,1}$

$$
\begin{aligned}
S_{0,1} &= S_{0,0} * q_{1,0} + S_{1,0} * q_{0,0} \\
&= \alpha^{20} * (x - \alpha^{16}) + \alpha^{8}(x - \alpha) \\
&= \alpha^{10}x + \alpha^{5}
\end{aligned}
$$

$$
\begin{aligned}
S_{2,1} &= S_{2,0} * q_{3,0} + S_{3,0} * q_{2,0} \\
&= \alpha^5 * (x - \alpha^{15}) + \alpha^6 * (x - \alpha^{22}) \\
&= \alpha^{14} x + \alpha^{22} \\
q_{0,1} &= q_{0,0} * q_{1,0} \\
&= (x - \alpha)(x - \alpha^{16}) \\
&= x^2 + \alpha^{13} x + \alpha^{17} \\
q_{2,1} &= q_{2,0} * q_{3,0} \\
&= (x - \alpha^{22})(x - \alpha^{15}) \\
&= x^2 + \alpha^6 x + \alpha^{11}
\end{aligned}
$$

- *Third, compute* $S_{0,2}$

$$
\begin{aligned}
S_{0,2} &= S_{0,1} * q_{2,1} + S_{2,1} * q_{0,1} \\
&= (\alpha^{10} x + \alpha^5) * (x^2 + \alpha^6 x + \alpha^{11}) + (\alpha^{14} x + \alpha^{22}) * (x^2 + \alpha^{13} x + \alpha^{17}) \\
&= \alpha^2 x^3 + \alpha^8 x^2 + \alpha^2 x + \alpha^{14}
\end{aligned}
$$

Finally, the third–degree polynomial over $GF(3^3)$ *that interpolates the four given points is*

$$f(x) = \alpha^2 x^3 + \alpha^8 x^2 + \alpha^2 x + \alpha^{14}.$$

5.5.1 Composite finite field arithmetic

The log table method for carring out arithmetic in $GF(2^m)$ is very efficient for small values of m. In fact, experiments have shown that m must be smaller than half the word size of the underlying architecture [13]. To overcome this limitation we approach the problem through *composite finite field arithmetic*, which is based on the following theorem [27].

Theorem 5.5.1 *For any fixed basis $\alpha_1, \alpha_2, \ldots, \alpha_n$ for $GF(q)^n$ there is a natural one–one correspondence between $GF(q)^n$ and $GF(q^n)$.*

For large composite m, say $m = rs$, we have that $GF(2^m)$ can be taken to be a finite extension of the smaller Galois field $GF(2^r)$ and we choose an irreducible polynomial of degree s over the "ground" field $GF(2^r)$. The numbers r and s should be chosen to both localize memory access for table lookup in the ground field as well as speeding up the mod reduction following the operation of polynomial multiplication. In particular, if $p(x)$ is an irreducible polynomial of degree r over $GF(q)$ then it remains irreducible over $GF(q^s)$ if and only if r and s are relatively prime [25].

Example 5.5.2 (Composite field multiplication for $GF(2^3)^4$) *Let α be a root of the irreducible polynomial $q(t) = t^3 + t + 1$ over $GF(2)$. Moreover, $q(t)$ is is primitive over $GF(2)$.*

i	α^i	$z(i)$
0	001	$*$
1	010	3
2	100	6
3	011	1
4	110	5
5	111	4
6	101	2

Table 5.5.1 : *α^i in $GF(2^3)$ in terms of $a_2\alpha^2 + a_1\alpha + a_0$*

The elements of $GF(2^3)^4$ can be regarded as polynomials of the form

$$\beta_3 t^3 + \beta_2 t^2 + \beta_1 t + \beta_0,$$

where $\beta_i \in GF(2^3)$. The polynomial $p(t) = t^4 + t + 1$ is irreducible over $GF(2)$, hence it is also irreducible over $GF(2^3)^4$. Let $f_1(t) = \alpha t^3 + \alpha^4 t + \alpha^6$ and $f_2(t) = \alpha^3 t^3 + \alpha^2 t^2 + \alpha t + 1$. We want to perform the multiplication of f_1 and f_2 mod $p(t)$.

			α	0	α^4	α^6
			α^3	α^2	α	α^0
			α	0	α^4	α^6
		α^2	0	α^5	α^7	
	α^3	0	α^6	α^8		
α^4	0	α^0	α^2			
α^4	α^3	α^6	α^3	α^6	α^5	α^6
α^4	0	0	α^4	α^4	0	0
0	α^3	0	0	α^3	α^3	0
0	0	α^6	0	0	α^6	α^6
0	0	0	α^6	0	α^0	0

Hence,

$$\begin{aligned} f_1(t) * f_2(t) \ mod\ p(t) &= \alpha^6 t^3 + t \\ &= (101)t^3 + (000)t^2 + (001)t + (000), \end{aligned}$$

which is equivalent to 101000001000 *as a string of bits.*

Chapter 6

Some ethical concerns

Ethics consists of rules and standards that govern the conduct of a person or the members of a profession [45]. We apply ethics to different activities. These include our dealings with each other, with animals, the environment and scientific research. They should govern our interactions not only in conducting research but also in commerce, employment and politics. Ethics serves to identify desirable acceptable conduct, correct unacceptable conduct, and provides reasons for moral judgments. Projects without scientific merit waste resources and needlessly subject participants to risks. Accordingly, an essential condition of the ethical validity of research consists of determining that the scientific quality of the research as well as the skill and experience of the researchers guarantees achieving the objectives of the project.

6.1 Ethics in research

6.1.1 Scientific integrity and misconduct

Ethical scientific research requires integrity, an essential component of which is honesty. Integrity can be defined as freedom from corrupting influences or motives [45]. Integrity is vital to the scientific process while honesty is a necessary condition to truthful research. Dishonesty in science can take several forms. It is important to distinguish error and intentional dishonesty which is also called misconduct. Misconduct in science takes several forms including fabrication (making up data or results), plagiarism (using another's idea or research without appropriate credit), falsification (manipulating the data to make it appear more convincing), or selectively choosing only the data that fits the researchers preconceptions. Misconduct does not include honest errors or differences on interpretation of data.

6.1.2 Conflict of interest – responsible conduct in research

"A person has a conflict of interest if (a) he/she is an a relationship with another requiring him/her to exercise judgment in that other's service and (b) he/she has an interest tending to interfere with the proper exercise of judgment" [10]. In addition, you should be objective in research and researchers should be independent and impartial in their investigation. Research should not be determined, influenced or biased by the researcher or by a competing external interest.

6.1.3 Allocation of credits/recognition

Intellectual property refers to creations of the mind: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce [46]. Intellectual property can be divided into two categories. The first one, industrial property, includes trade marks, patents, etc. Copyright is a second category that includes literary works such as computer programs, newspapers, compositions, etc.

Along these lines recognition or allocation of credit is crucial to sound scientific research. We can credit others in scientific research through acknowledgment, citation and inclusion in a list of authors. In particular, citation explicitly acknowledges the work of other scientists and its influence on ones own results. It is important to recognize the work done by others, this will help to validate research.

6.2 Integrating ethics into this research project

6.2.1 Validating as ethical research

When selecting a research problem, it is important to focus on an unsolved, open problem. In addition, the research and its result must demonstrate scientific merit. Research requires activities such as clarifying, defining and understanding the problem. Ways to do this include numerical simulations, examples and counter examples. Once the problem is understood, an appropriate theoretical formulation is proposed that includes assumptions alongside the conditions in which a solution will be sought. The next step consists of a meticulous revision of relevant literature that includes recent articles, books, previous researches etc. After this literature review, credit or recognition is assigned to the appropriate scientists and researchers.

An important component in this project consists of the design of algorithms that can be used in software production. In this work, all the proposed algorithms are

sustained by theorems accompanied by their proofs. In those cases where we do not have rigorous proofs for the results, we make conjectures which are based on the numerical experiment we performed. Conjectures are labeled as such and carefully distinguished from rigorously proven theorems.

It is also important to acknowledge the sponsorship given by any institution committed to the developing and divulging of science. In this work we give explicit acknowledgement to PRECISE, National Science Foundation (NSF) and Alliance for Graduate Education and the Professoriate (AGEP).

6.2.2 Potential application in bioinformatics

The reverse engineering problem in bioinformatics is related to several ethical issues that have positive societal impacts. For instance, to reverse engineer a genetic network, biologists need to experiment with living organisms. This is a controversial issue that deserves careful attention. The mathematical models proposed in this research are intended to represent real life phenomena. Thus, having an appropriate model for the reverse engineering problem in bioinformatics will help biologists to reduce the use of living organisms in biological research. Also, this will help to decrease the cost of technological resources used to carry out the given experiments.

With the investigation that has been made, we hope that the results are useful to understand better the phenomena that are under study. In particular, we hope that results of reverse engineering for MS–orbits could be applied for the code production to compute symmetric FFTs. Also, we recommend that this knowledge and code be made available to the scientific community as well as the community in general. Additionally, the algorithms that we have developed to compute on large finite fields promise to be a useful tool in the study of finite dynamical systems.

Chapter 7

Summary and future work

We have completely solved the MS–orbits problem for the two and three dimensional cases, thus providing the theory for optimizing the computation of prime edge–length symmetric FFTs. For these cases, given a nonsingular matrix S over Z_p, p prime, we propose, as opposed to exhaustive searchs which yield $O(p^6)$ and $O(p^{12})$ algorithms, more efficient $O(p^2 \log p)$ and $O(p^3 \log p)$ algorithms to compute matrices M that minimize the number of cyclic convolutions (i.e., minimize the number of MS–orbits), respectively. For n dimensions, we characterize those important cases where there is only a single cyclic convolution, called the M–minimal case, and provide a general procedure to compute a maximal matrix which gives one nontrivial MS–orbit. Also, for the n dimensional cases, we propose a general procedure to compute the optimal matrix M when the characteristic polynomial of the nonsingular matrix S factors as the product of two distinct irreducible polynomials.

On the other hand, we have studied and compared two finite field models for genetic networks and provided algorithms for converting one model into the other via a discrete Fourier transform. We have developed efficient methods for performing arithmetic over finite fields and proposed a new efficient parallel algorithm based on the Chinese remindering theorem to interpolate over finite fields and have C/openMP implementations of these methods. These methods and their implementations provide valuable tools to reverse engineering large finite field genetic networks.

This work has also led to an important result that is interesting in its own right: if S is a nonsingular matrix with irreducible characteristic polynomial, then the set of all matrices that commute with S constitute a finite field.

In future work we plan to extend and enhance our results in both applications.

Regarding the application to the computation of symmetric FFTs with prime edge–length, we plan to extend the two and three dimensional cases to n dimensions and simplify the MS–orbits theory. With regard to the application to reverse engineering finite field genetic networks, we plan to extend our single variable parallel interpolating algorithm to the multivariable finite field model.

Bibliography

[1] A. V. Aho, J. E. Hopcroft, J. D. Ullman. *The Design and Analysis of Computer Algorithms.* Addison–Wesley Publishing Company, Reading, 1975.

[2] T. Akutsu, S. Kuahara, O. Maruyama, S. Miyano. *Identification of Gene Regulatory Networks by Strategic Gene Disruptions and Gene Overexpressions.* Proceedings of the 9th ACM–SIAM Symposium on Discrete Algorithms. H. Karloff, ACM Press. 1998.

[3] L. Auslander, M. Shenefelt. *Fourier Transforms that Respect Crystallographic Symmetries.* IBM J. Res. and Dev. Vol. 31, pp 213–223, 1987.

[4] E. R. Berlekamp. *Algebraic Coding Theory.* Revised 1984 edition. Aegean Park Press, 1984.

[5] D. Bollman, E. Orozco, O. Moreno. *A Parallel Solution to Reverse Engineering Genetic Networks.* M. L. Gavrilova, O. Gervasi, V. Kumar, A. Laganá, Y. Mun, K. J. Tan (eds.) Lecture Notes in Computer Science, Springer–Verlag, Part III. 3045 pp 490–497, 2004.

[6] R. Chandra, L. Dagum, D. Kohr, D. Maydan, J. McDonald, R. Menon. *Parallel Programming in OpenMP.* Morgan Kaufmann Publishers, 2001.

[7] T. Chen, H. L. He, G. M. Church. *Modeling Gene Expression with Differential Equations.* Pacific Symposium Biocomputing '99, pp 29–40, 1999.

[8] T. H. Cormen, C. E. Leiserson, R. L. Rivest, C. Stein. *Introduction to Algorithms.* Second edition. The MIT Press, Cambridge, Massachusetts, 2001.

[9] D. Cox, J. Little, D. O'Shea. *Ideals, Varieties, and Algorithms. An Introduction to Algebraic Geometry and Commutative Algebra.* Second edition. Springer–verlag, 1997.

[10] M. Davis. *Conflict of Interest.* Business and Professional Ethics Journal. Vol. 1 No. 4, pp 21, 1982.

[11] E. DeWin, A. Bosselaers, S. Vandenberghe, P. DeGersem, J. Vandewalle.*A fast software implementation for arithmetic operations in* $GF(2^n)$. K. Kim, T. Matsumoto (eds.) Advances in Cryptology - ASIACRYPT 96, Lecture Notes in Computer Science, 1163, pp 65–76, Springer–Verlag, 1999.

[12] B. Elspas. *The Theory of Autonomous Linear Sequential Networks, Linear Sequential Switching Circuits.* (eds.) W. Kautz, Holden-Day Inc., pp 21–61 1965.

[13] E. Ferrer, E. Orozco. *Fast Arithmetic in Large Finite Fields.* SIDIM XX, UPR–Mayaguez, Mayaguez, P.R. Feb 25–26, 2005.

[14] S. H. Friedberg, A. J. Insel, L. E. Spence. *Linear Algebra.* Prentice–Hall, Inc., Englewood Cliffs, New Jersey. 1979.

[15] R. Gilmer. *Finite Rings Having Cyclic Multiplicative Group of Units.* American Journal of Mathematics, Vol. 85, pp 447–452, 1963.

[16] E. L. Green. *On polynomial solutions to reverse engineering problems.* preprint.

[17] J. Guajardo, C. Paar. *Efficient algorithms for elliptic curve cryptosystems.* B. S. Kaliski Jr., (eds.) Advances in Cryptology – CRYPTO 97. Lecture Notes in Computer Science, 1294, pp 342–356, Springer–Verlag, 1997.

[18] M. A. Hasan. *Look–up table–based large finite field multiplication in memory constrained cryptosystems.* IEEE Trans. Computing, Vol. 49, No.7, pp 749–758, 2000.

[19] I. N. Herstein. *Topics in Algebra.* Second edition. John Wiley & Sons, New York. 1975.

[20] K. Hoffman, R. Kunze. *Linear Algebra.* Second edition. Prentice–Hall, Inc., Englewood Cliffs, New Jersey. 1971.

[21] R. A. Horn, C. R. Johnson. *Matrix Analysis.* Cambridge University Press. 1999.

[22] T. E. Ideker, V. Thorsson, R. M. Karp. *Discovery of regulatory interactions through perturbation, Inference and experimental design.* Pacific Symposium on Biocomputing, No. 5, pp 302–313, 2000.

[23] R. Laubenbacher, B. Stigler. *Dynamic networks.* Adv. in Appl. Math. Vol.26, pp. 237–251, 2001.

[24] R. Laubenbacher, B. Stigler. *Biochemical networks.* preprint.

[25] R. Lidl, H. Niederreiter. *Finite Fields.* Encyclopedia of Mathematics and its Applications, Vol. 20. 2nd ed. Cambridge University Press. 1997.

[26] J. Lipson. *Chinese remaindering and interpolation algorithms.* Proc. 2nd Symposium in Symbolic and Algebraic Manipulation, pp 372–391, 1971.

[27] O. Moreno, D. Bollman, and M. Aviño: *Finite dynamical systems, linear automata, and finite fields.* 2002 WSEAS Int. Conf. on System Science, Applied Mathematics & Computer Science and Power Engineering Systems, pp 1481–1483. Also to appear in the International Journal for Computer Research.

[28] N. H. McCoy. *Rings and Ideals.* The Carus Mathematical Monographs. The Mathematical Association of America. 1956.

[29] I. Niven, H. S. Zuckerman, H. L. Montgomery. *An Introduction to the Theory of Numbers.* Fith edition, John Wiley & Sons, Inc. 1991.

[30] E. Orozco, J. Seguel, D. Bollman. *A New Prime Edge–Length Crystallographic FFT.* SIDIM XVII. San German, P.R. Feb 2002.

[31] E. Orozco, D. Bollman, O. Moreno. *A Parallel Algorithmic Approach to the Reverse Engineering Problem.* 1st IMS–ISBA Statistical Meeting, Workshop: Bioinformatics and Biostatistics: Current Problems and Solutions. San Juan, P.R. July 27, 2003.

[32] E. Orozco, D. Bollman, O. Moreno. *Reverse Engineering of Genetic Networks.* Richard Tapia Celebration of Diversity in Computing Conference, Atlanta, GA. Oct 2003.

[33] E. Orozco, D. Bollman. *Optimizing Symmetric FFTs with Prime Edge–Length.* M. L. Gavrilova, O. Gervasi, V. Kumar, A. Laganá, Y. Mun, K. J. Tan (eds.) Lecture Notes in Computer Science, Springer–Verlag, Part III. 3045 pp 749–757, 2004.

[34] E. Orozco, D. Bollman. *Finite Field Models for Genetic Networks.* SIDIM XX, UPR–Mayaguez, Mayaguez, P.R. Feb 25–26, 2005.

[35] E. Orozco, D. Bollman, J. Seguel, O. Moreno. *Organizing Crystallographic Data.* Poster presentation. 1st Conference in Protein Structure, Function and Dynamics. Ponce, P.R. Feb 7–9, 2003.

[36] H. Ortiz, M.A. Aviño, S. Peña, R. Laubenbacher, O. Moreno. *Finite Fields are Better Boolean.* Proc. of the Seventh Annual International Conference on Research in Computational Molecular Biology (RECOMB), Vol. 2003 pp 162, 2003.

[37] S. Roman. *Advanced Linear Algebra.* Advanced Texts in Mathematics, Springer–Verlag, New York. 1991.

[38] E. Savas, C. K. Koc. *Efficient methods for composite field arithmetic.* Technical Report, Oregon State University, 1999.

[39] E. Savas, A. F. Tenca, M. E. Ciftcibasi, C. K. Koc *Novel Multiplier Architectures for $GF(p)$ and $GF(2^n)$.* IEE Proceedings – Computer and Digital Techniques, Vol. 151 (2), pp 147–160, March 2004.

[40] I. Shmulevich, E. R. Dougherty, S. Kim, W. Zhang. *Probabilistic Boolean Networks: a rule–based uncertainty model for gene regulatory networks.* Bioinformatics, Vol. 18 No 2, pp 261–274, 2002.

[41] B. Sunar, E. Savas, and C. K. Koc. *Constructing Field Representations for efficient conversion.* to appear in IEEE Transactions on Computers.

[42] J. Seguel, D. Bollman, E. Orozco. *A New Prime Edge–Length Crystallographic FFT.* In: P. Sloot, C. Tan, J. Dongarra, A. Hoekstra (eds.) Lecture Notes in Computer Science, Springer–Verlag, Part II. 2330 pp 548–557, 2002.

[43] J. Seguel. *Design and Implementation of a Parallel Prime Edge-Length Symmetric FFT.* In: V. Kumar et al (eds.) Lecture Notes in Computer Science, Springer–Verlag, 2667 pp 1025–1034, 2003.

[44] J. Seguel, D. Burbano. *A Scalable Crystallographic FFT.* In: J. Dongarra, D. Laforenza, S. Orlando (eds.) Euro PVM/MPI 2003, Lecture Notes in Computer Science, 2840 pp 134–141, 2002.

[45] The American Heritage Dictionary of the English Language, Fourth Edition Copyright 2000 by Houghton Mifflin Company.

[46] *WIPO Guide to Intellectual Property Worldwide.* Second edition, Publication 479(E).