Properties of Trace Maps and their Applications to Coding Theory

N. Pinnawala

Doctor of Philosophy

2007

RMIT

Properties of Trace Maps and their Applications to Coding Theory

A thesis submitted in fulfilment of the requirements

for the degree of
Doctor of Philosophy

Nimalsiri Pinnawala

B.Sc., M.App.Sc.

School of Mathematical and Geospatial Sciences

Science, Engineering and Technology Portfolio

RMIT University

August 2007

Declaration

I certify that except where due acknowledgement has been made, the work is that of the author alone; the work has not been submitted previously, in whole or in part, to qualify for any other academic award; the content of the thesis is the result of work which has been carried out since the official commencement date of the approved research program; and, any editorial work, paid or unpaid, carried out by a third party is acknowledged.

.....

Nimalsiri Pinnawala

.....

Acknowledgements

There are innumerable people who have assisted me during this research and thesis writing. I would like to express my appreciation to all of them.

My deepest appreciation goes to my senior supervisor, Dr Asha Rao, for her valuable guidance, continuous encouragement and generous assistance throughout the period of research and thesis writing. I extend my sincere thanks to my second supervisor, Dr Kristine Lally and also to Prof. Kathy Horadam, Assoc. Prof. Serdar Boztas and Prof. Aaron Gulliver for their valuable advices and support. I am grateful to the staff of the school of Mathematical and Geospatial Sciences for their help.

I offer my grateful thanks to my parents, brothers and sisters, wife Udishani and little son Dhanidu for their love, encouragement and blessings.

Lastly, but definitely not least, my grateful thanks to RMIT, School of Mathematical and Geospatial Sciences for providing a scholarship and tuition fee waiver giving me financial support.

Contents

Summary

In this thesis we study the application of the trace map over Galois fields and Galois rings in the construction of non-binary linear and non-linear codes and mutually unbiased bases. In Chapter 1 there are some preliminary results that will be used throughout the thesis.

Properties of the trace map over the Galois fields and Galois rings were used very successfully in this author's masters thesis [57](published in [58] and [65]) in the construction of cocyclic Hadamard, complex Hadamard and Butson Hadamard matrices and consequently to construct linear codes over $\mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}_{2^e}$ and $\mathbb{Z}_{p^e}$. These results provide motivation to extend this work to construct codes over $\mathbb{Z}_n$ for any positive integer n. The prime factorisation of n, i.e., $n = p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}$ and the isomorphism $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \ldots \times \mathbb{Z}_{p_k^{e_k}}$ paved the way to focus our attention on the ring $R(n,m) = GR(p_1^{e_1},m) \times GR(p_2^{e_2},m) \times \ldots \times GR(p_k^{e_k},m)$, where m is a positive integer. In Chapter 2 we define a new map over the ring $R(n,m) = GR(p_1^{e_1},m) \times GR(p_2^{e_2},m)$ by

$$T : R(n,m) \to \mathbb{Z}_n$$
$$T(c) = p_2^{e_2}Tr_1(c_1) + p_1^{e_1}Tr_2(c_2),$$

where Tr_1 and Tr_2 are the trace maps over the Galois rings $GR(p_1^{e_1},m)$ and $GR(p_2^{e_2},m)$ respectively. We study the fundamental properties of T and notice that these are very similar to that of the trace maps over Galois fields and Galois rings. As such this map is named the trace-like map over $R(n,m)$, and is used to construct cocyclic Butson Hadamard matrices H of order n^m. Then the exponent matrix A of H is a linear code over $\mathbb{Z}_n$ with the parameters $[n,k,d_H] = \left[n^m, m, (n - p_1^{e_1}p_2^{e_2-1})n^{m-1}\right]$. This construction is extended by using the trace-like map over the ring $R(n,m) = GR(p_1^{e_1},m) \times GR(p_2^{e_2},m) \times \ldots \times GR(p_k^{e_k},m)$. In the case of $n = 6$ we notice that the code A is a senary simplex code of type α that has been studied in [37].

A further generalisation of the trace-like map has been used in [45] and this map is called the weighted-trace map. We study the properties of the weighted-trace map over

the ring $R(d,n) = GR(p_1^{e_1}, m_1) \times GR(p_2^{e_2}, m_2) \ldots \times GR(p_k^{e_k}, m_k)$, defined by

$$\begin{aligned} T_w &: R(d,n) \to \mathbb{Z}_n \\ T_w(x) &= \sum_{i=1}^{k} \frac{n}{p_i^{e_i}} Tr_i(x_i), \end{aligned}$$

where $d = p_1^{e_1 m_1} p_2^{e_2 m_2} \ldots p_k^{e_k m_k}$ and $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$. T_w is used to construct cocyclic Butson Hadamard matrices H_w of order d. However the exponent matrix A_w of H_w does not form a linear code over $\mathbb{Z}_n$. It gives a non-linear code over $\mathbb{Z}_n$ with the parameters (d, N, w_H), where $d = \prod_{i=1}^{k} p_i^{e_i m_i}$ is the length of the code, $N = \prod_{i=1}^{k} p_i^{e_i m_i}$ is the number of codewords and $w_H = d - p_k^{e_k m_k} \ldots p_2^{e_2 m_2} p_1^{e_1 m_1 - 1}$ is the minimum Hamming weight provided that $p_1^{e_1} < p_2^{e_2} < \ldots < p_k^{e_k}$ and $m_1 < m_2 < \ldots < m_k$.

The trace map over the Galois field $GF(p,m)$ (respectively the Galois ring $GR(4,m)$) has also been used in [49] in the form of $Tr(ax^2 + bx)$ (respectively $Tr((a+2b)x)$) to construct mutually unbiased bases of odd (respectively even) prime power dimensions. This work is a motivation to use the weighted-trace map in a similar manner to construct mutually unbiased bases. In Chapter 3 we use the weighted-trace map T_w over the ring $R(d,n) = GF(p_1,e_1) \times GF(p_2,e_2) \times \ldots \times GF(p_k,e_k)$ in the form of $T_w(ax^2 + bx)$ to construct mutually unbiased bases of odd integer dimension $d = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$.

Since the trace map over the Galois field $GF(p,m)$ has been used in the form of $Tr(ax^2 + bx)$ to construct mutually unbiased bases, it is an interesting question to check whether the trace map can be used in similar manner to construct codes over $\mathbb{Z}_p$. In Chapter 4, for $a \in GF(p,2)$ we study the distribution of $Tr(ax^2)$ by changing x over $GF(p,2)$ and use this distribution to construct two-weight, self-orthogonal codes over $\mathbb{Z}_p$ with the parameters $[n,k,d_H] = [p^2, 2, (p-1)^2]$.

In Chapter 5 we use the trace map over $GF(p,2)$ in the form of $Tr(ax^\lambda)$, when $\lambda | (p+1)$, and construct two-weight, self-orthogonal codes over $\mathbb{Z}_p$ with the parameters $[n,k,d_H] = [p^2, 2, (p-(\lambda-1))(p-1)]$. In Chapter 6 the next case $\lambda | (p-1)$ is considered and we construct two-weight codes with the parameters $[n,k,d_H] = [p^2, 2, (p-1)^2]$ and constant-weight codes with the parameters $[n,k,d_H] = [p^2, 2, p(p-1)]$ for $\lambda >$ 2-even and $\lambda >$ 2-odd respectively.

Finally we conclude the thesis with some further research possibilities.

Chapter 1

Preliminaries

1.1 Introduction

Coding theory is an interesting subject to mathematicians as well as engineers because of its beautiful mathematical structures and applications to communications. Starting with group theory, together with field theory and ring theory, coding theory provides a framework for the construction of error-correcting codes, and encoding and decoding of these codes. In this chapter we include necessary information that will be used throughout the thesis.

Fundamental properties together with the distribution of the trace map values over the Galois field $GF(p, m)$ and Galois ring $GR(p^e, m)$ have been used to construct cocyclic Butson Hadamard matrices of order p^m and p^{em} and consequently to construct linear codes over $\mathbb{Z}_p$ and $\mathbb{Z}_{p^e}$ respectively in the master's thesis [57] of this author. These results have appeared in [58] and [65].

A challenging open problem was the extension of this construction for any integer n. By taking the advantage of $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ we tackle the problem by defining a new map, called the trace-like map, T over the ring $R(n, m) = GR(p_1^{e_1}, m) \times GR(p_2^{e_2}, m) \times \dots \times GR(p_k^{e_k}, m)$ in Chapter 2. For $a, x \in R(n, m)$ we study the distribution of $T(ax)$ and then use this property to construct cocyclic Butson Hadamard matrices of order n^m and then some linear codes over $\mathbb{Z}_n$. A further generalisation of T is studied and this map is called the weighted-trace map and denoted by T_w. In this case the ring

that we consider is $R(d,n) = GR(p_1^{e_1}, m_1) \times GR(p_2^{e_2}, m_2) \times \ldots \times GR(p_k^{e_k}, m_k)$, where $d = p_1^{e_1 m_1} p_2^{e_2 m_2} \ldots p_k^{e_k m_k}$ and $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$. The weighted-trace map T_w is used in Chapter 3 in the form of $T_w(ax^2 + bx)$ to construct mutually unbiased bases of odd integer dimension $d = p_1^{e_1 m_1} p_2^{e_2 m_2} \ldots p_k^{e_k m_k}$.

Once the argument ax is changed to ax^2 or ax^λ for elements in $GF(p,m)$, studying the distribution of the trace values is a difficult task. In this thesis we study the case $GF(p,2)$, for $p > 2$, and the distribution of $Tr(ax^2)$ and $Tr(ax^\lambda)$, where $\lambda|(p^2-1)$. In Chapter 4 we use the distribution of $Tr(ax^2)$ to construct two-weight, self-orthogonal codes over $\mathbb{Z}_p$ with the parameters $[p^2, 2, (p-1)^2]$. For $\lambda > 2$ such that $\lambda|(p+1)$, the distribution of $Tr(ax^\lambda)$ is used in Chapter 5 to construct two-weight, self-orthogonal codes over $\mathbb{Z}_p$ with the parameters $[p^2, 2, (p-(\lambda-1))(p-1)]$. The distribution of $Tr(ax^\lambda)$ for even $\lambda > 2$ such that $\lambda|(p-1)$ is used in Chapter 6 and we are able to construct two-weight codes over $\mathbb{Z}_p$ with the parameters $[p^2, 2, (p-1)^2]$ which are similar to those in Chapter 4 but not self-orthogonal. In the case of odd $\lambda > 2$ such that $\lambda|(p-1)$, the codes constructed by using the distribution of $Tr(ax^\lambda)$ are constant-weight codes over $\mathbb{Z}_p$ with the parameter $[p^2, 2, p(p-1)]$.

In Section 1.2 we state some basic results of error-correcting codes. Some basic definitions and results of cocycles and Hadamard matrices are given in Section 1.3. We devote Section 1.4 to the study of the fundamental properties of the trace maps over the Galois field $GF(p,m)$ and Galois ring $GR(p^e,m)$. Finally in Section 1.5 we briefly describe mutually unbiased bases.

1.2 Error-correcting codes

In this section we will study definitions and some basic results related to error-correcting codes.

Let B be a basis for the vector space V. The number of vectors in the basis B denoted by $|B| = k$ is called the dimension of V. If $\mathbb{F}$ is a field then $\mathbb{F}^n$ is an n-dimensional vector space over $\mathbb{F}$. Let $\mathbb{Z}_p^n$ be a vector space of dimension n over $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$, where p is a prime. Any subset C of N vectors of $\mathbb{Z}_p^n$ is called a code and its vectors are called

codewords. If C is a k-dimensional subspace of $\mathbb{Z}_p^n$ then C is called an $[n, k]$ linear code. The number of co-ordinates n of each codeword is called the length of the code and k is called the dimension of the code.

Definition 1.2.1 (Hamming weight). *Let $x \in \mathbb{Z}_p^n$. The number of non-zero components in x is called the Hamming weight of x and it is denoted by $W_H(x)$.*

Definition 1.2.2 (Hamming distance). *Let $x, y \in \mathbb{Z}_p^n$. The Hamming distance $d_H(x, y)$ between x and y is the number of co-ordinates in which they differ.*

It is clear that $d_H(x, y) = W_H(x - y)$. The minimum Hamming distance, d_H of a code C is the minimum of the Hamming distances of all distinct pairs of its codewords. The minimum Hamming distance of a linear code is the minimum Hamming weight of all non-zero codewords. A code with minimum Hamming distance d_H can correct up to $\lfloor \frac{d_H - 1}{2} \rfloor$ errors, where $\lfloor a \rfloor$ denotes the smallest integer not greater than a. Three other useful weights (distances) in coding theory are the Lee, Euclidean and Chinese Euclidean weights (distances) respectively. The Lee weight of $a \in \mathbb{Z}_p$ is given by $W_L(a) = \min\{a, p - a\}$. The Euclidean weight of $a \in \mathbb{Z}_p$ is given by $W_E(a) = (W_L(a))^2$. The Chinese Euclidean weight of $a \in \mathbb{Z}_p$ is given by $W_{CE}(a) = \left\{2 - 2\cos\left(\frac{2\pi a}{p}\right)\right\}$. The Lee (Euclidean, Chinese Euclidean) weight of a vector $x \in \mathbb{Z}_p^n$ is the sum of the Lee (Euclidean, Chinese Euclidean) weights of its components. The Lee, Euclidean and Chinese Euclidean distance between $x, y \in \mathbb{Z}_p^n$ are given by $d_L(x, y) = W_L(x - y)$, $d_E(x, y) = W_E(x - y)$ and $d_{CE}(x, y) = W_{CE}(x - y)$ respectively. The minimum Lee, Euclidean and Chinese Euclidean distance of a code C are defined by $d_L = \min\{d_L(x, y) | x, y \in C, x \neq y\}$, $d_E = \min\{d_E(x, y) | x, y \in C, x \neq y\}$ and $d_{CE} = \min\{d_{CE}(x, y) | x, y \in C, x \neq y\}$ respectively.

The standard inner product of $x, y \in \mathbb{Z}_p^n$ is defined by $x \cdot y = \sum_{i=1}^{n} x_i y_i$. The subset $C^{\perp} = \{x \in \mathbb{Z}_p^n | x \cdot y = 0, \forall\, y \in C\}$ is called the dual code of C.

Definition 1.2.3 (Self-orthogonal and self-dual codes). *A linear code C is called self-orthogonal if $C \subseteq C^{\perp}$ and if $C = C^{\perp}$ then it is called self-dual.*

If C is an $[n, k]$ linear code over $\mathbb{Z}_p$ then $C^{\perp}$ is an $[n, n - k]$ linear code. It is well known that linear self-dual codes over finite fields must have even length n and hence the

dimension $k = \frac{n}{2}$. However this is not true for codes over finite rings. In [62] self-dual codes of odd lengths over $\mathbb{Z}_4$ are constructed. More details on self-orthogonal and self-dual codes can be found in [3, 4, 5, 24, 38, 39, 59, 62, 63, 64, 72, 76] and the references therein.

Definition 1.2.4 (Hamming weight distribution). *Let $A_H(i)$ be the number of codewords of Hamming weight i of the code C. The list of numbers $\{A_H(0), A_H(1), \ldots, A_H(n)\}$ is called the Hamming weight distribution of C.*

Similar definitions are given for the Lee, Euclidean and Chinese Euclidean weight distribution. The polynomial

$$Ham_C(x, y) = \sum_{i=0}^{n} A_H(i) x^{n-i} y^i$$

is called the Hamming weight enumerator of C. This is the same as the polynomial

$$Ham_C(x, y) = \sum_{c \in C} x^{n - W_H(c)} y^{W_H(c)}.$$

If C is an $[n, k]$ linear code over $\mathbb{Z}_p$ with dual code $C^\perp$ then the MacWilliams Identity is given by $Ham_{C^\perp}(x, y) = \frac{1}{|C|} Ham_C(x + (p-1)y, x - y)$, where $|C| = p^k$. The complete weight enumerator (cwe) for a code C over $\mathbb{Z}_p$ is defined as

$$cwe_C(x_0, x_1, \ldots, x_m) \;=\; \sum_{c \in C} x_0^{w_0(c)} x_1^{w_1(c)} \ldots x_m^{w_m(c)},$$

where $m = p - 1,\ c = (c_1, c_2, \ldots, c_n) \in C,\ w_j(c) = |\{k : c_k = j\}|$.

Definition 1.2.5 (Constant-weight code). *If every non-zero codeword of a code has the same weight then the code is called a constant-weight code.*

The weight of a constant-weight code may be Hamming, Lee or Euclidean weight. It is known that constant Hamming weight codes exist for all dimensions over finite fields. They almost never exist over $\mathbb{Z}_n$ that are not fields. Constant Lee or Euclidean weight codes exist for any module over $\mathbb{Z}_{2^t}$. See [80] for more details. Binary constant-weight codes constitute an important class of error-correcting codes. A table of binary constant-weight codes of length $n \leq 28$ is given in [15] while that for $29 \leq n \leq 63$ is given in [68]. Ternary codes with constant Hamming weight have been studied in [56] which gives a table with bounds for the maximum cardinality $A_3(n, d, w)$. More details of constant-weight codes can also be found in [33, 53], etc. and the references therein.

Definition 1.2.6 (Simplex codes). *A linear code is called simplex if every pair of distinct codewords are the same distance apart.*

It is clear that linear constant-weight codes are linear simplex codes and vice versa since every pair of distinct codewords are the same distance apart [53].

Definition 1.2.7 (Equivalent codes). *Two codes C_1 and C_2 are said to be equivalent if one can be turned into the other by permuting the co-ordinate position of each codeword and by permuting the code symbols in each position of each codeword.*

Codes that differ only by a permutation are said to be permutation equivalent. Permutation equivalent codes have the same complete weight enumerators, but equivalent codes may have distinct complete weight enumerators. In the case of binary codes, two codes are equivalent, if they are permutation equivalent. Also codes with the same complete weight enumerators need not be equivalent. Reader may refer to [53, 75] for further details on weight distributions of codes.

Definition 1.2.8 (Cyclic code). *The linear code C of length n over $\mathbb{Z}_p$ is called a cyclic code if for each $c = (c_0, c_1, \ldots, c_{n-2}, c_{n-1}) \in C$, the codeword obtained by the cyclic shift of co-ordinates (i.e., $\overline{c} = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$) is also a codeword of C.*

Since C is invariant under this single right cyclic shift, by iteration it is invariant under any number of right cyclic shifts. Since a single left-cyclic shift is the same as $n-1$ right cyclic shifts, C is also invariant under a single left-cyclic shift. Hence C is invariant under all left-cyclic shifts. Therefore the linear code C is cyclic when it is invariant under all cyclic shifts.

When studying cyclic codes over $\mathbb{Z}_p$, it is convenient to represents the codewords in polynomial form $c(x) = c_0 + c_1x + \ldots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1} \in \mathbb{Z}_p[x]$ of degree at most $n-1$. With this convention, the shifted codeword $\overline{c}$ corresponds to the polynomial $\overline{c}(x) = c_{n-1}+c_0x+\ldots+c_{n-2}x^{n-1}$. Thus $\overline{c}(x) = xc(x)$ if $x^n = 1$. That is $\overline{c}(x) = xc(x) (\text{mod } x^n-1)$. For a detailed survey of cyclic codes see chapter 4 of [46].

Now we will move off from error-correcting codes to cocycles and Hadamard matrices as this is the other focus of this thesis.

1.3 Cocycles and Hadamard matrices

In this section first we will study the definitions of cocycle and Hadamard matrices and then include some known results.

Definition 1.3.1 (Cocycle). *Let G be a finite group and C be a finite abelian group. The set mapping $\varphi : G \times G \to C$ which satisfies*

$$\varphi(a,b)\varphi(ab,c) = \varphi(b,c)\varphi(a,bc), \ \ \forall \ \ a,b,c \in G \text{ is called a cocycle over } G.$$

For instance if $G = \mathbb{Z}_2^n$ and $C = \{\pm 1\}$ then $\varphi(u,v) = (-1)^{u \cdot v}$, for all $u, v \in G$, is a cocycle. A cocycle is normalised if $\varphi(1,1) = 1$. A cocycle is naturally displayed as a cocyclic matrix, i.e., a square matrix whose rows and columns are indexed by the elements of G under some fixed ordering, and whose entry in position (a,b) is $\varphi(a,b)$.

Definition 1.3.2 (Hadamard matrix). *A Hadamard matrix of order n is a square matrix $H = [h_{ij}]$ with entries $h_{ij} = \pm 1, \ \ 1 \leq i,j \leq n$, whose row vectors are pairwise orthogonal. In other words $HH^T = nI$, where H^T is the transpose of H and I is the identity matrix of order n.*

A Hadamard matrix must have order $1, 2$ or a multiple of 4. The Hadamard conjecture proposes that a Hadamard matrix exists for every $n \equiv 0 \pmod 4$.

Definition 1.3.3 (Generalised Hadamard matrix, [30]). *Let G be a group of finite order, $H = [h_{ij}]$ be a square matrix of order n, whose entries are elements of G. Then H is said to be a Generalised Hadamard matrix $GH(n,G)$ over G if*
(i) whenever $i \neq j$, the sequence $\{h_{ix}h_{jx}^{-1}\}$ with $1 \leq x \leq n$ contains every element of G equally often,
(ii) H^T has property (i).

A $GH(n,G)$ is normalised if the first row and first column consist entirely of the identity element of G. In the case of $G = \{\pm 1\}$ and $n \equiv 0 (\text{mod } 4)$, the generalised Hadamard matrix $GH(n,G)$ is a Hadamard matrix.

The next type of matrix is sometimes referred to as a generalised Hadamard matrix [78] and sometimes as a complex Hadamard matrix [25, 27]. However in this thesis we will refer to this as a Butson Hadamard matrix.

Definition 1.3.4 (Butson Hadamard matrix, [16]). *Let C_p be the multiplicative group of all complex p^{th} roots of unity. That is $C_p = \{1, x, x^2, \ldots, x^{p-1}\}$, where $x = exp(2\pi\sqrt{-1}/p)$. A square matrix $H = [h_{ij}]$ of order n with elements from C_p is a Butson Hadamard matrix if and only if $HH^* = nI$, where H^* denotes the conjugate transpose of H and I denotes the identity matrix of order n.*

A Butson Hadamard matrix is normally denoted by $BH(n, r)$. Note that r is not necessarily a prime number. When $r = 2$ and $n = 1, 2$ or a multiple of 4, $BH(n, r)$ is a Hadamard matrix. A generalised Hadamard matrix defined over the finite group C_r is a Butson Hadamard matrix. The following theorem gives us a nice relationship between generalised Hadamard matrices and Butson Hadamard matrices.

Theorem 1.3.5. *[Remarks 1.3, [30]]*
(i) In the definition of a $BH(n, r)$-matrix, the condition $HH^* = nI$ is equivalent to the requirement that $H^*H = nI$.
(ii) Every generalised Hadamard matrix over C_r (i.e., $GH(n, C_r)$) is a Butson Hadamard matrix (i.e., $BH(n, r)$) .
(iii) If r is a prime, every $BH(n, r)$-matrix over C_r (except for the matrix [1] of order 1) is a $GH(n, C_r)$-matrix .
(iv) If $r = pt$, where p is a prime and $t > 1$, then there exists a Butson Hadamard matrix of order p over C_r, but certainly no Generalised Hadamard matrix of order p over C_r.

The next theorem describes the existence of Butson Hadamard matrices and Generalised Hadamard matrices.

Theorem 1.3.6. *[Theorem 1, [27]]*
For primes $p > 2$, there exists a Butson Hadamard matrix $BH(n, p)$ over the cyclic group C_p if and only if there exists a generalised Hadamard matrix $GH(n, \mathbb{Z}_p)$ over the additive group $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$.

Definition 1.3.7 (Complex Hadamard matrix). *The matrix H of order n with entries from $\{1, i, -1, -i\}$ that satisfies $HH^* = nI$ is called a complex Hadamard matrix of order n, where $i = \sqrt{-1}$, H^* is the conjugate transpose of H and I is the identity matrix of order n.*

It is conjectured that a complex Hadamard matrix exists for every even order. In [74] it is shown that every complex Hadamard matrix has order 1 or divisible by 2. A complex Hadamard matrix is a special case of a Butson Hadamard matrix $BH(n,p)$ for $p = 4$. For the various type of constructions and further studies of complex Hadamard matrices reader can also refer to [26, 28, 48, 51, 54, 58, 67].

Definition 1.3.8 (Cocyclic Hadamard matrices). *Let φ be a cocycle over a finite group G and $M_\varphi = [\varphi(a,b)]_{a,b\in G}$. If M_φ is a Hadamard (Complex Hadamard, Butson Hadamard) matrix then M_φ is called a cocyclic Hadamard (Complex Hadamard, Butson Hadamard) matrix.*

Cocycles have been used to construct Hadamard matrices in [3, 6, 43]. In [57], cocycles are used to construct cocyclic complex Hadamard and cocyclic Butson Hadamard matrices. These results have appeared in [58, 65].

Definition 1.3.9 (Hadamard exponent matrix). *Let $H = [h_{i,j}]$ be a Butson Hadamard matrix (in [25, 27] this is referred to as a complex Hadamard matrix) over C_p, where p is a fixed prime, $p > 2$. The matrix $E = [e_{i,j}]$, $e_{i,j} \in \mathbb{Z}_p$, which is obtained from $H = [x^{e_{i,j}}] = [h_{i,j}]$, where $x = exp(2\pi\sqrt{-1}/p)$, is called the Hadamard exponent matrix associated with H.*

By deleting the all zero row and column of E, the remaining elements constitute a square sub-matrix E_p, called the core of H. The elements of the Hadamard exponent matrix E lie in the Galois field $GF(p)$, and its row vectors can be viewed as the codewords of a code over $\mathbb{Z}_p$.

We give the next definition as a generalisation of the definition of the Hadamard exponent matrix since we are going to use this in the thesis.

Definition 1.3.10 (Exponent matrix). *Let $H = [h_{i,j}]$ be a square matrix over $C_n = \{1, x, x^2, \ldots, x^{n-1}\}$, where n is a positive integer and $x = exp(2\pi\sqrt{-1}/n)$. The matrix $E = [e_{i,j}]$, $e_{i,j} \in \mathbb{Z}_n$, which is obtained from $H = [x^{e_{i,j}}] = [h_{i,j}]$ is called the exponent matrix associated with H.*

In the next section we will study the fundamental properties of the trace maps over Galois fields and Galois rings respectively.

1.4 The trace map and its fundamental properties

In this section first we will give a brief idea about the Galois field $GF(p,m)$ and basic properties of the trace map over $GF(p,m)$. Then the Galois ring $GR(p^e,m)$ and fundamental properties of the trace map over $GR(p^e,m)$ are studied.

Finite fields are used in most of the known constructions of codes and for encoding and decoding. Let p be a prime number and $\mathbb{Z}_p$ be the set of integers modulo p. This set forms a field of order p and it is also denoted by $GF(p)$. The elements of $GF(p)$ are $\{0,1,2,\ldots,p-1\}$ and all field arithmetic is carried out mod p. Suppose $f(x)$ is an irreducible polynomial of degree m over $\mathbb{Z}_p$. Then the set of all polynomials in x of degree $\leq m-1$ with coefficients from $\mathbb{Z}_p$, and calculations performed modulo $f(x)$, forms a field of order p^m. This is called a Galois field of order p^m and is denoted by $GF(p,m)$.

Definition 1.4.1 (Automorphism). *Let σ be a one to one mapping from $GF(p,m)$ onto itself. If for all $\alpha,\beta \in GF(p,m)$ and $a \in \mathbb{Z}_p$*
(i) $\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta)$,
(ii) $\sigma(\alpha\beta)=\sigma(\alpha)\sigma(\beta)$ and
(iii) $\sigma(a)=a$
then σ is called an automorphism of $GF(p,m)$ over $\mathbb{Z}_p$.

The set of all such automorphisms of $GF(p,m)$ over $\mathbb{Z}_p$ forms a group if we define the composition of σ and τ by $\tau\circ\sigma(\alpha)=\tau(\sigma(\alpha))$.

Theorem 1.4.2. *[Theorem 2.21, [52]]*
The distinct automorphisms of $GF(p,m)$ over $\mathbb{Z}_p$ are exactly the mappings $\sigma_0,\sigma_1,\ldots,\sigma_{m-1}$ defined by $\sigma_j(\alpha)=\alpha^{p^j}$, for all $\alpha \in GF(p,m)$ and $0 \leq j \leq m-1$.

The automorphism σ_1 of $GF(p,m)$ over $\mathbb{Z}_p$ which generates all automorphisms of $GF(p,m)$ over $\mathbb{Z}_p$ by Theorem 1.4.2 is called the Frobenius automorphism of $GF(p,m)$ over $\mathbb{Z}_p$.

Let f be the Frobenius automorphism of $GF(p,m)$ over $\mathbb{Z}_p$ defined as

$$f : GF(p,m) \to GF(p,m)$$
$$f(\alpha)=\alpha^p$$

and let Tr be the trace map defined as

$$Tr : GF(p, m) \to \mathbb{Z}_p$$
$$Tr(\alpha) = \alpha + f(\alpha) + f^2(\alpha) + \ldots + f^{m-1}(\alpha).$$

Theorem 1.4.3. *The trace map satisfies the following properties:*
For all $\alpha, \beta \in GF(p, m)$ and $a \in \mathbb{Z}_p$
(i) $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$.
(ii) $Tr(a\alpha) = aT(\alpha)$.
(iii) Tr is a linear transformation from $GF(p, m)$ onto $\mathbb{Z}_p$.
(iv) As α ranges over $GF(p, m)$, $Tr(\alpha)$ takes on each value in $\mathbb{Z}_p$ equally often, i.e., p^{m-1} times.

For a detailed proof of this theorem, see [52, 53].

Now we will study the Galois ring of characteristic p^e and dimension m and the properties of the trace map over the Galois ring. For more details on Galois rings of this type, the reader may refer to [55].

Definition 1.4.4 (Galois ring). *Let $p > 2$ be a prime and e be a positive integer. The ring of integers modulo p^e is the set $\mathbb{Z}_{p^e} = \{0, 1, 2, \ldots, p^e - 1\}$. Let $h(x) \in \mathbb{Z}_{p^e}[x]$ be a basic irreducible monic polynomial of degree m that divides $x^{p^m-1} - 1$. The Galois ring of characteristic p^e and dimension m is defined as the quotient ring $\mathbb{Z}_{p^e}[x]/(h(x))$ and is denoted by $GR(p^e, m)$.*

The element $\zeta = x + (h(x))$ is a root of $h(x)$ and consequently ζ is a primitive $(p^m - 1)^{th}$ root of unity. Therefore we say that ζ is a primitive element of $GR(p^e, m)$ and $GR(p^e, m) = \mathbb{Z}_{p^e}[\zeta]$. It follows that $GR(p^e, m) = < 1, \zeta, \zeta^2, \ldots, \zeta^{m-1} >$ and hence $|GR(p^e, m)| = p^{em}$. It is well known that each element $u \in GR(p^e, m)$ has a unique representation $u = \sum_{i=0}^{e-1} p^i u_i$, where $u_i \in \mathcal{T} = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{p^m-2}\}$. This representation is called the p-adic representation of elements of $GR(p^e, m)$ and the set $\mathcal{T}$ is called the Teichmuller set. Note that u is invertible if and only if $u_0 \neq 0$. Thus every non-invertible element of $GR(p^e, m)$ can be written as $u = \sum_{i=k}^{e-1} p^i u_i$, where $k \in \{1, 2, \ldots, e-1\}$. By using the p-adic representation of elements of $GR(p^e, m)$, the Frobenius automorphism f has been defined in [12, 18] as

$$f : GR(p^e, m) \to GR(p^e, m)$$
$$f(u) = \sum_{i=0}^{e-1} p^i u_i^p.$$

Note that when $e = 1$, f is the usual Frobenius automorphism for the Galois field $GF(p, m)$ [52]. The trace map over $GR(p^e, m)$ is defined by

$$Tr : GR(p^e, m) \to \mathbb{Z}_{p^e}$$
$$Tr(u) = u + f(u) + f^2(u) + \ldots + f^{m-1}(u).$$

From the definition of Tr the following properties are satisfied:

Theorem 1.4.5. *For any $u, v \in GR(p^e, m)$ and $\alpha \in \mathbb{Z}_{p^e}$*
(i) $Tr(u + v) = Tr(u) + Tr(v)$.
(ii) $Tr(\alpha u) = \alpha Tr(u)$.
(iii) Tr is nontrivial.

The trace map can be used to go down from a code defined over an extension field to a code defined over the ground field. Let $\mathbb{F}_q$ be the ground field of the extended field $\mathbb{F}_{q^r}$.

Definition 1.4.6 (Trace code). *Let C be an $\mathbb{F}_{q^r}$-linear code of length n and $Tr : \mathbb{F}_{q^r} \to \mathbb{F}_q$ be the trace map. The code $Tr(C)$, defined as the set of all vectors $(Tr(x_1), Tr(x_2), \ldots, Tr(x_n)) \in \mathbb{F}_{q^r}$, is called the trace code, where $(x_1, x_2, \ldots, x_n) \in C$.*

Another method of going down from a code defined over an extension field to a code defined over the ground field is the subfield code.

Definition 1.4.7 (Subfield code). *Let C be an $\mathbb{F}_{q^r}$-linear code of length n. The code $C_{\mathbb{F}_q}$, defined as $C_{\mathbb{F}_q} = C \cap \mathbb{F}_q^n$, is called the subfield code.*

It is well known that the trace codes and the subfield codes are linear codes over the ground field $\mathbb{F}_q$. There is a nice relationship between trace code and subfield code which is clarified by the following famous theorem due to Delsarte.

Theorem 1.4.8. *[Theorem 12.14, [11]] Let C be an $\mathbb{F}_{q^r}$-linear code of length n. Then $(Tr(C))^\perp = (C^\perp)_{\mathbb{F}_q}$.*

It is also known that the trivial bounds for the dimension of the trace code are $\dim(C) \leq \dim(Tr(C)) \leq r\dim(C)$. More details on trace codes can also be found in [22, 36, 41, 69, 70, 73].

As we are going to use the trace map to construct mutually unbiased bases, we will next study some basic theory of mutually unbiased bases.

1.5 Mutually Unbiased Bases (MUBs)

Let C^n be the complex vector space of dimension n. The inner product of $x, y \in C^n$, where $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$, is denoted by $< x, y >$ and defined by $< x, y > = \sum_{i=1}^{n} x_i \bar{y_i}$, where $\bar{y_i}$ is the complex conjugate of y_i. The norm of x is defined by $\parallel x \parallel = < x, x >^{\frac{1}{2}}$. Two vectors x and y in C^n are called orthogonal to each other if $< x, y > = 0$. Let B be a basis of the vector space C^n. B is called an orthogonal basis if for all $x, y \in B$, $< x, y > = 0$. An orthogonal basis B is called an orthonormal basis if for all $x \in B$, $\parallel x \parallel = 1$.

Definition 1.5.1 (Mutually unbiased bases). *Let B and $B^{'}$ be orthonormal bases of the vector space C^n. These bases are called Mutually Unbiased if and only if*
$| < b, b^{'} > | = \frac{1}{\sqrt{n}}$, $\forall\, b \in B$ *and* $b^{'} \in B^{'}$.

The idea of mutually unbiased bases (MUBs) appeared in the literature of quantum mechanics in 1960 in [66]. As they possess numerous applications in quantum information science, researchers have allocated more time to study the existence of MUBs and have introduced different types of construction methods. In [7] it has been proved that for any dimension n, the number of MUBs, denoted by $N(n)$, is at most $n + 1$ and when n is a prime power then $N(n) = n + 1$. Different construction methods have been used to construct MUBs. Authors in [49] have used the trace map over the Galois field of characteristic $p \geq 5$ very successfully in order to construct MUBs of odd prime power dimensions while the trace map over the Galois ring of characteristic 4 has been used to construct MUBs of even prime power dimensions. For a detailed survey of MUBs the reader may refer to [1, 2, 9, 20, 31, 32, 35, 50, 60, 61, 79] and the references therein.

Chapter 2

Cocyclic Codes over $\mathbb{Z}_n$

2.1 Introduction

The cocyclic map has been used to construct Hadamard matrices [6] and these Hadamard matrices were found to yield extremal binary self-dual codes [3]. The nature of the cocyclic map allowed for substantial cut-down in the computational time needed to generate the matrices and then the codes. In [58] Pinnawala and Rao exploited this property to construct cocyclic complex and Butson Hadamard matrices and consequently to construct simplex codes of type α over $\mathbb{Z}_4$ and $\mathbb{Z}_{2^e}$ by defining cocycle maps via the trace maps over Galois rings $GR(4,m)$ and $GR(2^e,m)$ respectively. In [65], the above authors extended this method to construct some new linear codes over $\mathbb{Z}_p$ and $\mathbb{Z}_{p^e}$ for prime $p > 2$ and positive integer e. A challenging open problem was the extension of this method to construct cocyclic Butson Hadamard matrices of order n for any positive integer n. Since $n = p_1^{e_1}p_2^{e_2}\ldots p_k^{e_k}$, where p_i are distinct primes and e_i are positive integers, $i = 1, 2, \ldots, k$, the motivation is to focus attention on the ring $R(n,m) = GR(p_1^{e_1},m) \times GR(p_2^{e_2},m) \times \ldots \times GR(p_k^{e_k},m)$. However there is no known map over this ring similar to the trace map over Galois rings and Galois fields. In this chapter we define a new map over the ring $R(n,m)$, which is called the trace-like map with fundamental properties parallel to the other trace maps.

In Section 2.2 we include some preliminaries that we need in this chapter and in Section 2.3 we study the basic results of the Galois ring $GR(p^e,m)$ and the properties of the trace

map over $GR(p^e, m)$. In Section 2.4 these properties are used to define a cocycle over $GR(p^e, m)$ and to construct a cocyclic Butson Hadamard matrix of order p^{em}. This matrix is then used to construct a linear code over $\mathbb{Z}_{p^e}$. These results are from [57] (published in [58]). Section 2.5 is devoted to the study of the ring $R(n, m) = GR(p_1^{e_1}, m) \times GR(p_2^{e_2}, m)$ and defining a new map called the trace-like map over $R(n, m)$. In Section 2.6, the fundamental properties of the trace-like map are used to construct Butson Hadamard matrices of order n^m. The exponent matrix associated with this Butson Hadamard matrix is then used to construct linear codes over $\mathbb{Z}_n$. In Section 2.7 we calculate the Lee, Euclidean and Chinese Euclidean weights of the codes that we construct in Section 2.6. In [37] Gupta et al. studied the senary simplex code of type α, β and γ and introduced a Chinese product type construction. In Section 2.8 we introduce the cocyclic senary simplex code of type α as a particular case of codes over $\mathbb{Z}_n$ for $n = 6$. Finally in section 2.9 we study a further generalisation of the trace-like map T, called the weighted-trace map, denoted by T_w.

2.2 Preliminaries

In this section we study the preliminary results that we need to use in other sections of this chapter.

A linear code C of length n over the integers modulo k (i.e., $\mathbb{Z}_k = \{0, 1, 2, \ldots, k-1\}$) is an additive sub group of $\mathbb{Z}_k^n$. An element of C is called a codeword and a generator matrix of C is a matrix whose rows generate C. The Hamming weight $W_H(x)$ of an n-tuple $x = (x_1, x_2, \ldots, x_n)$ in $\mathbb{Z}_k^n$ is the number of non-zero co-ordinates of x and the Lee weight $W_L(x)$ of x is $\sum_{i=1}^n \min\{x_i, k - x_i\}$. The Euclidean weight $W_E(x)$ of x is $\sum_{i=1}^n \min\{x_i^2, (k - x_i)^2\}$ and the Chinese Euclidean weight $W_{CH}(x)$ of x is $\sum_{i=1}^n \left\{2 - 2\cos\left(\frac{2\pi x_i}{k}\right)\right\}$. The Hamming, Lee, Euclidean and Chinese Euclidean distances between $x, y \in \mathbb{Z}_k^n$ are defined and denoted as $d_H(x, y) = W_H(x-y)$, $d_L(x, y) = W_L(x-y)$, $d_E(x, y) = W_E(x - y)$ and $d_{CE}(x, y) = W_{CE}(x - y)$ respectively.

Cocycles (see Definition 1.3.1) have been used in the construction of cocyclic matrices and consequently in the construction of error-correcting codes. In [44], Horadam and

Perera define a code over a ring R as a cocyclic code if it can be constructed using a cocycle or the rows of a cocyclic matrix or is equivalent to such a code.

Let $\omega = exp(\frac{2\pi\sqrt{-1}}{k})$ be the complex k^{th} root of unity and $C_k = \{1, \omega, \omega^2, \ldots, \omega^{k-1}\}$ be the multiplicative group of all complex k^{th} roots of unity.

A Butson Hadamard matrix (see Definition 1.3.4), is denoted by $B(n, k)$ and in the cases of $k = 2$ and $k = 4$, $B(n, k)$ provides Hadamard matrices (see Definition 1.3.2) and complex Hadamard matrices (see Definition 1.3.7) respectively. Several methods have been introduced to construct complex and Butson Hadamard matrices. In [54] Matsufuji and Suehiro use real valued bent functions and Cooke and Heng [27] use monic polynomials. To construct cocyclic Butson Hadmard matrices, we need the properties of the trace map over $GR(p^e, m)$, and we look at these in the next section.

2.3 Galois ring and the trace map

We defined the Galois ring in Definition 1.4.4, but we repeat it here for ease of reading.

Definition 2.3.1 (Galois ring). *Let $p > 2$ be a prime and e be a positive integer. The ring of integers modulo p^e is the set $\mathbb{Z}_{p^e} = \{0, 1, 2, \ldots, p^e - 1\}$. Let $h(x) \in \mathbb{Z}_{p^e}[x]$ be a basic monic irreducible polynomial of degree m that divides $x^{p^m-1} - 1$. The Galois ring of characteristic p^e and dimension m is defined as the quotient ring $\mathbb{Z}_{p^e}[x]/(h(x))$ and is denoted by $GR(p^e, m)$.*

The element $\zeta = x + (h(x))$ is a root of $h(x)$ and consequently ζ is a primitive $(p^m - 1)^{th}$ root of unity. Therefore we say that ζ is a primitive element of $GR(p^e, m)$ and $GR(p^e, m) = \mathbb{Z}_{p^e}[\zeta]$. Hence $GR(p^e, m) =< 1, \zeta, \zeta^2, \ldots, \zeta^{m-1} >$ and $|GR(p^e, m)| = p^{em}$. It is well known that each element $u \in GR(p^e, m)$ has a unique representation: $u = \sum_{i=0}^{e-1} p^i u_i$, where $u_i \in \mathcal{T} = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{p^m-2}\}$. This representation is called the p-adic representation of elements of $GR(p^e, m)$ and the set $\mathcal{T}$ is called the Teichmuller set. Note that u is invertible if and only if $u_0 \neq 0$. Thus every non-invertible element of $GR(p^e, m)$ can be written as $u = \sum_{i=k}^{e-1} p^i u_i$, where $k \in \{1, 2, \ldots, e-1\}$. We represent elements of $GR(p^e, m)$ by $u^{(k)} = \sum_{i=k}^{e-1} p^i u_i$, where $k \in \{0, 1, 2, \ldots, e-1\}$. By using the

p - adic representation of the elements of $GR(p^e, m)$, the Frobenius automorphism f has been defined in [12, 18, 77] as

$$f : GR(p^e, m) \to GR(p^e, m)$$
$$f(u) = \sum_{i=0}^{e-1} p^i u_i^p.$$

The following properties are satisfied by f:

Lemma 2.3.2. *For all $u, v \in GR(p^e, m)$ and $\alpha \in \mathbb{Z}_{p^e}$*
(i) $f(u+v) = f(u) + f(v)$.
(ii) $f(uv) = f(u)f(v)$.
(iii) $f(\alpha) = \alpha$.

Note that when $e = 1$, f is the usual Frobenius automorphism over the Galois field $GF(p, m)$ (see [52] for more details). The trace map over $GR(p^e, m)$ is defined by

$$Tr : GR(p^e, m) \to \mathbb{Z}_{p^e}$$
$$Tr(u) = u + f(u) + f^2(u) + \ldots + f^{m-1}(u).$$

The trace map satisfies the properties given in Theorem 1.4.5. In addition to these properties, the trace map also satisfies the following property:

Theorem 2.3.3. *[Lemma 2.1,[65]]*
Given a Galois ring $GR(p^e, m)$, let $D_k = \{p^k t \mid t = 0, 1, 2, \ldots, p^{e-k} - 1\} \subseteq \mathbb{Z}_{p^e}$ and $u^{(k)} \in GR(p^e, m)$, as defined above. As x ranges over $GR(p^e, m)$, $Tr(xu^{(k)})$ maps to each element in D_k equally often, i.e., $p^{e(m-1)+k}$ times, where $k = 0, 1, 2, \ldots, e-1$.

Proof:
For any $x \in GR(p^e, m)$, consider the m - tuple $V_x = (Tr(x), Tr(\zeta x), \ldots, Tr(\zeta^{m-1}x))$ over $\mathbb{Z}_{p^e} = D_0$. Let $V = \{V_x | x \in GR(p^e, m)\}$ and consider the following correspondence.

$$\alpha : GR(p^e, m) \to V.$$

It is easy to see that α sets up a one to one correspondence between the elements of $GR(p^e, m)$ and the m - tuples of V over $D_0 = \mathbb{Z}_{p^e}$. Thus as x ranges over $GR(p^e, m)$, each co-ordinate $Tr(x\zeta^i)$, for $i = 0, 1, 2, \ldots, m-1$, must take each element of D_0 equally

often, i.e., $\frac{p^{em}}{p^e} = p^{e(m-1)}$ times. In general, for any invertible element $u^{(k)} \in GR(p^e, m)$ (i.e., $u^{(k)} = u^{(0)} = \sum_{i=0}^{e-1} p^i u_i$; $u_i \in \mathcal{T}$ and $u_0 \neq 0$), as x ranges over $GR(p^e, m)$, $Tr(xu^{(0)})$ must also assume each element of D_0 equally often, i.e., $p^{e(m-1)}$ times.

If b is not invertible then $u^{(k)} = \sum_{i=k}^{e-1} p^i u_i$, where $k \in \{1, 2, \ldots, e-1\}$. Now from the expansion of $Tr(xu^{(k)})$ and induction on k, as x ranges over $GR(p^e, m)$, $Tr(xu^{(k)})$ must takes each element of D_k equally often, i.e., $\frac{p^{em}}{p^{e-k}} = p^{em-(e-k)} = p^{e(m-1)+k}$ times. □

Note that this proof is also clear from the multiplicative Cayley table of $\mathbb{Z}_{p^e}$. For more details on Galois rings of this type, the reader may refer to [55, 77] and the references therein. We are now in a position to use the trace map to construct cocyclic Butson Hadamard matrices of order p^{em} and codes over $\mathbb{Z}_{p^e}$.

2.4 Cocyclic Butson Hadamard matrices and linear codes via the trace map

In this section we will use the properties of the trace map over the Galois ring $GR(p^e, m)$ that we studied in Section 2.3 to construct cocyclic Butson Hadamard matrices and consequently to construct linear codes over $\mathbb{Z}_{p^e}$.

Let $\omega = exp(\frac{2\pi\sqrt{-1}}{k})$ be the complex k^{th} root of unity. Let C_k be the multiplicative group of all complex k^{th} roots of unity. i.e., $C_k = \{1, \omega, \omega^2, \ldots, \omega^{k-1}\}$. It is well know that

$$S = \sum_{j=0}^{k-1} \omega^j = 0 \tag{2.1}$$

Let $H = [h_{i,j}]$ be a square matrix over C_k. The matrix $E = [e_{i,j}]$, $e_{i,j} \in \mathbb{Z}_k$, which is obtained from $H = [\omega^{e_{i,j}}] = [h_{i,j}]$ is called the exponent matrix associated with H.

Theorem 2.4.1. *[Proposition 3.1, [65]]*
Let $p > 2$ be a prime and $GR(p^e, m)$ be the Galois ring of characteristic p^e and dimension m. Let C_{p^e} be the multiplicative group of all complex $(p^e)^{th}$ roots of unity.
(i) The set mapping

$$\varphi : GR(p^e, m) \times GR(p^e, m) \to C_{p^e}$$
$$\varphi(c_i, c_j) = (\omega)^{Tr(c_i c_j)}$$

is a cocycle.

(ii) The matrix $H = [\varphi(c_i, c_j)]_{c_i, c_j \in GR(p^e, m)}$ *is a Butson Hadamard matrix of order* p^{em}.

(iii) The rows of the exponent matrix of H *(i.e.,* $A = [Tr(c_i c_j)]_{c_i, c_j \in GR(p^e, m)}$*) form a linear code over* $\mathbb{Z}_{p^e}$ *with the parameters* $[n, k, d_L] = \left[p^{em}, m, p^{e(m-1)}\left(\frac{p^{2e}-p^{2(e-1)}}{4}\right)\right]$.

Proof:

(i) Let $a, b, c \in GR(p^e, m)$. Then

$$\begin{aligned}
\varphi(a, b) &= \omega^{Tr(ab)}. \\
\varphi(a + b, c) &= \omega^{Tr((a+b)c)} = \omega^{Tr(ac)+Tr(bc)}. \\
\varphi(b, c) &= \omega^{Tr(bc)}. \\
\varphi(a, b + c) &= \omega^{Tr(a(b+c))} = \omega^{Tr(ab)+Tr(ac)}.
\end{aligned}$$

From these equations we have

$$\varphi(a, b)\varphi(a + b, c) = \varphi(b, c)\varphi(a, b + c).$$

Thus φ is a cocycle.

(ii) $H = [\varphi(c_i, c_j)]_{c_i, c_j \in GR(p^e, m)}$. To prove that $HH^* = p^{em} I$, consider the sum

$$S = \sum_{x \in GR(p^e, m)} \varphi(c_i, x)\overline{\varphi(x, c_j)}, \tag{2.2}$$

where $\overline{\varphi(x, c_j)}$ is the complex conjugate of $\varphi(x, c_j)$. From the properties of the trace map we have

$$S = \sum_{x \in GR(p^e, m)} \left(exp\left(\frac{2\pi i}{p^e}\right)\right)^{Tr(x(c_i - c_j))}. \tag{2.3}$$

When $c_i = c_j$, it is clear that $S = p^{em}$. When $c_i \neq c_j$, from Theorem 2.3.3 and the equation 2.1 we have

$$\begin{aligned}
S &= \sum_{x \in GR(p^e, m)} \left(exp\left(\frac{2\pi i}{p^e}\right)\right)^{Tr(x(c_i - c_j))}. \\
&= p^{e(m-1)+k} \sum_{t=0}^{p^{e-k}-1} \left(exp\left(\frac{2\pi i}{p^e}\right)\right)^{p^k t} = 0.
\end{aligned} \tag{2.4}$$

Thus $HH^* = p^{em}I$.

(iii) Consider the exponent matrix A associated with H.

$$A = [Tr(c_i c_j)]_{c_i, c_j \in GR(p^e, m)}.$$

Since $Tr(c_i c_j) \in \mathbb{Z}_{p^e}$, we can consider the rows of A as codewords over $\mathbb{Z}_{p^e}$. Now consider the matrix

$$G_A = \begin{bmatrix} Tr(c_i), & i = 1, 2, \ldots, p^{em} \\ Tr(\zeta c_i), & i = 1, 2, \ldots, p^{em} \\ \vdots & \vdots \\ Tr(\zeta^{m-1} c_i), & i = 1, 2, \ldots, p^{em} \end{bmatrix}_{m \times p^{em}},$$

where $c_i \in GR(p^e, m)$. Since ζ^i are invertible in $GR(p^e, m)$, from Theorem 2.3.3, each row of G_A contains each element of $\mathbb{Z}_{p^e}$ equally often $p^{e(m-1)}$ times. We can also show that the rows of G_A are linearly independent. Writing all the linear combinations of rows of G_A, we obtain

$$A = [Tr(c_i c_j)]_{c_i, c_j \in GR(p^e, m)}.$$

Therefore G_A is a generator matrix for the code A and hence A is a linear code over $\mathbb{Z}_{p^e}$ with the dimension m. Let $x \in A$ be a non-zero codeword. Then x can be written as $x = (x_1, x_2, \ldots, x_{p^{em}})$, where $x_i \in D_k$ for $i = 1, 2, \ldots, p^{em}$. From Theorem 2.3.3, each element in D_k should appear in x equally often, i.e., $p^{e(m-1)+k}$ times. Therefore the Lee weight of x is $p^{e(m-1)}\left(\frac{p^{2e}-p^{2k}}{4}\right)$. The minimum Lee weight of the codewords in A is obtained when $k = e-1$. Thus $d_L = \min\ (Lee(x)) = p^{e(m-1)}\left(\frac{p^{2e}-p^{2(e-1)}}{4}\right)$ and hence the parameters of the code A are $[n, k, d_L] = \left[p^{em}, m, p^{e(m-1)}\left(\frac{p^{2e}-p^{2(e-1)}}{4}\right)\right]$. □

So far in this chapter we have used the trace map over the Galois ring $GR(p^e, m)$ to construct cocyclic Butson Hadamard matrices of order p^{em} and cocyclic linear codes over $\mathbb{Z}_{p^e}$. We now have enough basic information to study the ring $R(n, m) = GR(p_1^{e_1}, m) \times GR(p_2^{e_2}, m)$ and define the new map over $R(n, m)$, the trace-like map.

2.5 The direct product of Galois rings and the trace-like map

In this section first we will study the structure of the ring $R(n,m) = GR(p_1^{e_1},m) \times GR(p_2^{e_2},m)$, where $n = p_1^{e_1}p_2^{e_2}$. Then by using some number theory results, we define the trace-like map over the ring $R(n,m)$ and study its fundamental properties noticing that these are parallel to the properties of the trace maps over Galois fields and Galois rings.

Let $p_1 \neq p_2 \geq 2$ be primes and e_1, e_2 be positive integers. If $n = p_1^{e_1}p_2^{e_2}$, it is well known that $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}}$ and hence for any positive integer m, $\mathbb{Z}_n^m \cong \left(\mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}}\right)^m$. For more details on these results see for example [34]. Let $f_1(x)$ and $f_2(x)$ be basic monic irreducible polynomials of degree m over $\mathbb{Z}_{p_1^{e_1}}$ and $\mathbb{Z}_{p_2^{e_2}}$ respectively. As in Section 2.3 the Galois rings of characteristics $p_1^{e_1}$ and $p_2^{e_2}$ and common dimension m are defined as the quotient rings $\mathbb{Z}_{p_1^{e_1}}[x]/(f_1(x))$ and $\mathbb{Z}_{p_2^{e_2}}[x]/(f_2(x))$ respectively. These rings are denoted by $GR(p_1^{e_1},m)$ and $GR(p_2^{e_2},m)$. If ζ_1 and ζ_2 are defined to be $\zeta_1 = x + (f_1(x))$ and $\zeta_2 = x + (f_2(x))$, the two rings can then be expressed as $GR(p_1^{e_1},m) = < 1, \zeta_1, \zeta_1^2, \ldots, \zeta_1^{m-1} >$ and $GR(p_2^{e_2},m) = < 1, \zeta_2, \zeta_2^2, \ldots, \zeta_2^{m-1} >$. This tells us that $GR(p_1^{e_1},m) = \mathbb{Z}_{p_1^{e_1}}[\zeta_1]$ and $GR(p_2^{e_2},m) = \mathbb{Z}_{p_2^{e_2}}[\zeta_2]$. Hence any element $c_1 \in GR(p_1^{e_1},m)$ can be expressed as an m-tuple $c_1 = (a_0, a_1, \ldots, a_{m-1})$ over $\mathbb{Z}_{p_1^{e_1}}$ while $c_2 \in GR(p_2^{e_2},m)$ as $c_2 = (b_0, b_1, \ldots, b_{m-1})$ over $\mathbb{Z}_{p_2^{e_2}}$.

Now consider the direct product of the two Galois rings $GR(p_1^{e_1},m)$ and $GR(p_2^{e_2},m)$. Let $R(n,m) = GR(p_1^{e_1},m) \times GR(p_2^{e_2},m)$. Any element $c \in R(n,m)$ can be written as $c = (c_1, c_2)$, where $c_1 \in GR(p_1^{e_1},m)$ and $c_2 \in GR(p_2^{e_2},m)$ and further as
$c = ((a_0, a_1, \ldots, a_{m-1}), (b_0, b_1, \ldots, b_{m-1}))$. Since $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}}$, c can also be written as an m-tuple $c = (d_0, d_1, \ldots, d_{m-1})$ over $\mathbb{Z}_n$, where $d_i = (a_i, b_i)$. Here $a_i \in \mathbb{Z}_{p_1^{e_1}}$ and $b_i \in \mathbb{Z}_{p_2^{e_2}}$, where $i = 0, 1, 2, \ldots, m-1$.

Let $c, c' \in R(n,m)$. It is easy to see that $R(n,m)$ is a ring under the addition $c + c' = ((d_0 + d_0'), (d_1 + d_1'), \ldots, (d_{m-1} + d_{m-1}'))$ and the multiplication $cc' = (d_0 d_0', d_1 d_1', \ldots, d_{m-1} d_{m-1}')$. Also $|R(n,m)| = n^m = (p_1^{e_1}p_2^{e_2})^m = p_1^{e_1 m}p_2^{e_2 m} = |GR(p_1^{e_1},m)||GR(p_2^{e_2},m)|$.

To continue on, we need a couple of number theory results. The first one is well known.

Lemma 2.5.1. *[Corollary 4.4, [34]]*

If p is a prime and a is any integer then $a^p \equiv a(mod\, p)$.

The following result may also be a well known result, but ready reference seems hard to find. Therefore we state it giving the complete proof in order to apply the proof to some theorems that will appear later in this section.

Lemma 2.5.2. *Let $n = p_1^{e_1}p_2^{e_2}$. Then $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}}$ and given $\alpha \in \mathbb{Z}_n$ there exist $\alpha_1 \in \mathbb{Z}_{p_1^{e_1}}$ and $\alpha_2 \in \mathbb{Z}_{p_2^{e_2}}$ such that $\alpha = (\alpha_1 p_2^{e_2} + \alpha_2 p_1^{e_1})$ mod n. Thus $\mathbb{Z}_n = \left\{(\alpha_1, \alpha_2) | \alpha_1 \in \mathbb{Z}_{p_1^{e_1}}, \alpha_2 \in \mathbb{Z}_{p_2^{e_2}}\right\}$.*

Proof:
Since the $\gcd(p_1^{e_1}, p_2^{e_2}) = 1$ there exist $x, y \in \mathbb{Z}$ such that $xp_1^{e_1} + yp_2^{e_2} = 1$. Multiplying both sides of this equation by $\alpha \in \mathbb{Z}_n$ we have

$$\begin{aligned} \alpha &= (\alpha x p_1^{e_1} + \alpha y p_2^{e_2}) \bmod n. \\ \Rightarrow \alpha &= (\alpha x p_1^{e_1}) \bmod n + (\alpha y p_2^{e_2}) \bmod n. \end{aligned}$$

Suppose that $\alpha x p_1^{e_1} \equiv t_1 \bmod n$. This implies that $\alpha x p_1^{e_1} = nr + t_1$ which implies $p_1^{e_1} | (nr + t_1)$. Since $p_1^{e_1} | nr$ and hence $p_1^{e_1} | t_1$, we can write $t_1 = p_1^{e_1}\alpha_2$. Thus

$$\begin{aligned} \alpha x p_1^{e_1} &= p_1^{e_1} p_2^{e_2} r + p_1^{e_1}\alpha_2 \\ \Rightarrow \alpha x &= p_2^{e_2} r + \alpha_2 \\ \Rightarrow \alpha x &\equiv \alpha_2 \bmod p_2^{e_2} \end{aligned}$$

i.e., $\alpha_2 \in \mathbb{Z}_{p_2^{e_2}}$.

Similarly we can show that $\alpha y \equiv \alpha_1 \bmod p_1^{e_1}$. i.e., $\alpha_1 \in \mathbb{Z}_{p_1^{e_1}}$. Therefore there exist $\alpha_1 \in \mathbb{Z}_{p_1^{e_1}}$ and $\alpha_2 \in \mathbb{Z}_{p_2^{e_2}}$ such that $\alpha = (\alpha_1 p_2^{e_2} + \alpha_2 p_1^{e_1}) \bmod n$. Thus $\mathbb{Z}_n = \left\{(\alpha_1, \alpha_2) | \alpha_1 \in \mathbb{Z}_{p_1^{e_1}}, \alpha_2 \in \mathbb{Z}_{p_2^{e_2}}\right\}$. □

We are now in a position to define a new map and to prove its properties.

Theorem 2.5.3 (Trace-like map). *Let Tr_1 and Tr_2 be the trace maps over $GR(p_1^{e_1}, m)$ and $GR(p_2^{e_2}, m)$ respectively (see Section 2.3). For any $c = (c_1, c_2) \in R(n, m)$, the map T over $R(n, m)$ defined by*

$$T : R(n,m) \to \mathbb{Z}_n$$
$$T(c) = p_2^{e_2} Tr_1(c_1) + p_1^{e_1} Tr_2(c_2)$$

satisfies the following properties:

For $c, c' \in R(n,m)$ *and* $\alpha \in \mathbb{Z}_n$

(i) $T(c+c') = T(c) + T(c')$.

(ii) $T(\alpha c) = \alpha T(c)$.

(iii) T *is surjective.*

Proof:

(i) Let $c, c' \in R(n,m) = GR(p_1^{e_1}, m) \times GR(p_2^{e_2}, m)$. Then $c = (c_1, c_2)$ and $c' = (c_1', c_2')$, where $c_1, c_1' \in GR(p_1^{e_1}, m)$ and $c_2, c_2' \in GR(p_2^{e_2}, m)$. Since $c + c' = ((c_1 + c_1'), (c_2 + c_2'))$ we have

$$\begin{aligned} T(c+c') &= p_2^{e_2} Tr_1(c_1 + c_1') + p_1^{e_1} Tr_2(c_2 + c_2'). \\ &= p_2^{e_2} Tr_1(c_1) + p_2^{e_2} Tr_1(c_1') + p_1^{e_1} Tr_2(c_2) + p_1^{e_1} Tr_2(c_2') \text{(From Theorem 1.4.5)} \\ &= (p_2^{e_2} Tr_1(c_1) + p_1^{e_1} Tr_2(c_2)) + (p_2^{e_2} Tr_1(c_1') + p_1^{e_1} Tr_2(c_2')). \\ &= T(c) + T(c'). \end{aligned}$$

(ii) Let $\alpha \in \mathbb{Z}_n$ and $c \in R(n,m)$.

$$\begin{aligned} T(\alpha c) &= p_2^{e_2} Tr_1(\alpha c_1) + p_1^{e_1} Tr_2(\alpha c_2). \\ &= p_2^{e_2}(\alpha c_1 + \alpha^{p_1} f_1(c_1) + \ldots + \alpha^{p_1^{m-1}} f_1(c_1)) + p_1^{e_1}(\alpha c_2 + \alpha^{p_2} f_2(c_2) + \ldots + \alpha^{p_2^{m-1}} f_2(c_2)). \end{aligned}$$

Here f_1 and f_2 are the Frobenius automorphisms over $GR(p_1^{e_1}, m)$ and $GR(p_2^{e_2}, m)$ respectively. From Lemma 2.5.1 we know that if p is prime then for any integer a, $a^p \equiv a (\text{mod } p)$. Therefore we have

$$\begin{aligned} T(\alpha c) &= p_2^{e_2} \alpha(Tr_1(c_1)) + p_1^{e_1} \alpha(Tr_2(c_2)). \\ &= \alpha T(c). \end{aligned}$$

(iii) Since Tr_1 and Tr_2 are both surjective and not identically zero, there exist elements $c_1 \in GR(p_1^{e_1}, m)$ and $c_2 \in GR(p_2^{e_2}, m)$ such that $Tr_1(c_1) = 1$ and $Tr_2(c_2) = 1$. Then for $c = (c_1, c_2) \in R(n,m)$, $T(c) = p_1^{e_1} Tr_2(c_2) + p_2^{e_2} Tr_1(c_1) = p_1^{e_1} + p_2^{e_2}$. For all $\alpha \in \mathbb{Z}_n$ we have

proved in (ii) that $T(\alpha c) = \alpha T(c)$ and since $p_1^{e_1} + p_2^{e_2}$ is not a multiple of either p_1 or p_2, $T(\alpha c) = \alpha T(c)$ should represent every element in $\mathbb{Z}_n$ and hence T is surjective. □

The main purpose of this chapter is to apply the trace-like map to construct cocylic Butson Hadamard matrices of order n^m and consequently to construct linear codes over $\mathbb{Z}_n$ for $n = p_1^{e_1} p_2^{e_2}$. So we need to study the distribution of the trace-like map $T(cx)$ over $\mathbb{Z}_n$ as x ranges over $R(n,m)$, where $c \in R(n,m)$. The following theorem explains this distribution in detail for invertible and non-invertible elements $c \in R(n,m)$.

Theorem 2.5.4. *For any $c \in R(n,m)$ as x ranges over $R(n,m)$, $T(cx)$ takes each element in*

$$S_{i,j} = \left\{ p_1^i p_2^j t | t = 0, 1, 2, \ldots, \frac{n}{p_1^i p_2^j} - 1 \right\} \tag{2.5}$$

equally often, i.e., $p_1^i p_2^j n^{m-1}$ times, where $0 \leq i \leq e_1$ and $0 \leq j \leq e_2$.

Proof:

First of all we will prove that $T(cx) \in S_{i,j}$. Since $c, x \in R(n,m)$, $c = (c_1, c_2)$ and $x = (x_1, x_2)$, where $c_1, x_1 \in GR(p_1^{e_1}, m)$ and $c_2, x_2 \in GR(p_2^{e_2}, m)$. In the case of $c = 0$ it is clear that $T(cx) = 0$.

If $c \neq 0$ and both c_1 and c_2 are non-zero, then as they are elements of Galois rings, their p-adic representations are given by

$$\begin{aligned} c_1 &= u_1^{(i)} = \sum_{k=i}^{e_1-1} p_1^k u_{1k} : \ 0 \leq i \leq e_1 - 1, \ u_{1i} \neq 0 \text{ and} \\ c_2 &= u_2^{(j)} = \sum_{k=j}^{e_2-1} p_2^k u_{2k} : \ 0 \leq j \leq e_2 - 1, \ u_{2j} \neq 0 \end{aligned}$$

respectively. Here $u_{1k} \in \mathcal{T}_1$ and $u_{2k} \in \mathcal{T}_2$, where $\mathcal{T}_1$ and $\mathcal{T}_2$ are the Teichmuller sets of the Galois rings $GR(p_1^{e_1}, m)$ and $GR(p_2^{e_2}, m)$ respectively. From Theorem 2.3.3, as x ranges over $R(n,m)$, since $T(cx) = p_2^{e_2} Tr_1(c_1 x_1) + p_1^{e_1} Tr_2(c_2 x_2)$, the trace maps $Tr_1(c_1 x_1)$ and $Tr_2(c_2 x_2)$ will take values in the sets $D_i = \{p_1^i t_1 \mid t_1 = 0, 1, 2, \ldots, p_1^{e_1-i} - 1\}$ and $D_j = \{p_2^j t_2 \mid t_1 = 0, 1, 2, \ldots, p_2^{e_2-j} - 1\}$ respectively. Thus

$$\begin{aligned} T(cx) &\in \left\{ p_2^{e_2} p_1^i t_1 + p_1^{e_1} p_2^j t_2 | t_1 = 0, 1, 2, \ldots, p_1^{e_1-i} - 1, t_2 = 0, 1, 2, \ldots, p_2^{e_2-j} - 1 \right\} \\ &= \left\{ p_1^i p_2^j (p_2^{e_2-j} t_1 + p_1^{e_1-i} t_2) | t_1 = 0, 1, 2, \ldots, p_1^{e_1-i} - 1, t_2 = 0, 1, 2, \ldots, p_2^{e_2-j} - 1 \right\}. \end{aligned}$$

Since the calculations are done modulo n,
$\left\{(p_2^{e_2-j}t_1 + p_1^{e_1-i}t_2)|t_1 = 0, 1, 2, \ldots, p_1^{e_1-i} - 1, t_2 = 0, 1, 2, \ldots, p_2^{e_2-j} - 1\right\} \subseteq \mathbb{Z}_n$.
From Lemma 2.5.2,
$\left\{(p_2^{e_2-j}t_1 + p_1^{e_1-i}t_2)|t_1 = 0, 1, 2, \ldots, p_1^{e_1-i} - 1, t_2 = 0, 1, 2, \ldots, p_2^{e_2-j} - 1\right\} \cong \mathbb{Z}_{p_1^{e_1-i}p_2^{e_2-j}}$.
Hence $T(cx) \in \left\{p_1^i p_2^j t|t = 0, 1, 2 \ldots, p_1^{e_1-i}p_2^{e_2-j} - 1\right\} = S_{i,j}$.

If $c \neq 0$ and $c_1 = 0$ (or $c_2 = 0$) then $T(cx) = p_1^{e_1}Tr_2(c_2x_2)$ (respectively $T(cx) = p_2^{e_2}Tr_1(c_1x_1)$) and we are reduced to the Galois ring case. From Theorem 2.3.3,
$Tr_2(c_2x_2) \in D_j$ (respectively $Tr_1(c_1x_1) \in D_i$). This implies that
$T(cx) \in \left\{p_1^{e_1}p_2^j t|t = 0, 1, 2, \ldots, p_2^{e_2-j} - 1\right\} = S_{0,j}$
(respectively $T(cx) \in \left\{p_2^{e_2}p_1^i t|t = 0, 1, 2, \ldots, p_1^{e_1-i} - 1\right\} = S_{i,0}$).

Thus for all $c, x \in R(n, m)$, $T(cx) \in S_{i,j}$.

From Theorem 2.3.3, as x_1 ranges over $GR(p_1^{e_1}, m)$ (respectively as x_2 ranges over $GR(p_2^{e_2}, m)$) $Tr_1(c_1x_1)$ takes elements in D_i (respectively $Tr_2(c_2x_2)$ takes elements in D_j) equally often i.e., $p_1^{e_1(m-1)+i}$ (respectively i.e., $p_2^{e_2(m-1)+j}$) times. Hence as x ranges over $R(n, m)$, $T(cx)$ takes elements in $S_{i,j}$ equally often $p_1^{e_1(m-1)+i}p_2^{e_2(m-1)+j} = p_1^i p_2^j n^{m-1}$ times. □

Since the map T satisfies properties similar to those satisfied by the trace maps over the Galois fields and Galois rings, we call it the trace-like map.

As in Theorem 2.3.3, Theorem 2.5.4 is also clear from the multiplicative Cayley table of $\mathbb{Z}_n$.

Example 2.5.5. *Consider the ring $R(6, 2) = GF(2, 2) \times GF(3, 2)$. Consider the irreducible polynomials $f(x) = x^2 + x + 1$ over $\mathbb{Z}_2$ and $g(x) = x^2 + x + 2$ over $\mathbb{Z}_3$. Let $GF(2, 2) = \mathbb{Z}_2[x]/(f(x))$ and $GF(3, 2) = \mathbb{Z}_3[x]/(g(x))$. If $\zeta_1 = (f(x)) + x$ then $f(\zeta_1) = 0$ and hence $GF(2, 2) = \mathbb{Z}_2[\zeta_1]$. Similarly if $\zeta_2 = (g(x)) + x$ then $g(\zeta_2) = 0$ and hence $GF(3, 2) = \mathbb{Z}_3[\zeta_2]$.*

Frobenius automorphisms f_1 and f_2 over $GF(2, 2)$ and $GF(3, 2)$ are given by

$$f_1 : GF(2, 2) \to GF(2, 2)$$
$$f_1(c_1) = c_1^2$$
and

$$f_2 : GF(3,2) \to GF(3,2)$$
$$f_2(c_2) = c_2^3$$

respectively.

The trace maps Tr_1 *and* Tr_2 *over* $GF(2,2)$ *and* $GF(3,2)$ *are given by*

$$Tr_1 : GF(2,2) \to \mathbb{Z}_2$$
$$Tr_1(c_1) = c_1 + f_1(c_1)$$
$$\textit{and}$$
$$Tr_2 : GF(3,2) \to \mathbb{Z}_3$$
$$Tr_2(c_2) = c_2 + f_2(c_2)$$

respectively.

The following tables illustrate the values of trace maps.

Element	c_1	$Tr_1(c_1)$
$00 = 0 + 0$	0	0
$10 = 1 + 0$	1	0
$01 = 0 + \zeta_1$	ζ_1	1
$11 = 1 + \zeta_1$	ζ_1^2	1

Element	c_2	$Tr_2(c_2)$
$00 = 0 + 0$	0	0
$10 = 1 + 0$	1	2
$01 = 0 + \zeta_2$	ζ_2	2
$12 = 1 + 2\zeta_2$	ζ_2^2	0
$22 = 2 + 2\zeta_2$	ζ_2^3	2
$20 = 2 + 0$	ζ_2^4	1
$02 = 0 + 2\zeta_2$	ζ_2^5	1
$21 = 2 + \zeta_2$	ζ_2^6	0
$11 = 1 + \zeta_2$	ζ_2^7	1

Now define the trace-like map T *over the ring* $R(6,2)$ *as follows:*

$$T : R(6,2) \to \mathbb{Z}_6$$
$$T(c) = 3Tr_1(c_1) + 2Tr_2(c_2),$$

where $c_1 \in GF(2,2)$ *and* $c_2 \in GF(3,2)$.

Since $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, *elements of* $\mathbb{Z}_6$ *can be represented by* $0 = (0,0), 1 = (1,2), 2 = (0,1), 3 = (1,0), 4 = (0,2), 5 = (1,1)$.

The following table illustrates the elements of $R(6,2)$ *and values of the trace-like map over* $R(6,2)$.

c	$c = (c_1, c_2)$	$T(c)$	c	$c = (c_1, c_2)$	$T(c)$
00	$(00)(00) = ((00),(00))$	0	10	$(12)(00) = ((10),(20))$	2
01	$(00)(12) = ((01),(02))$	5	11	$(12)(12) = ((11),(22))$	1
02	$(00)(01) = ((00),(01))$	4	12	$(12)(01) = ((10),(21))$	0
03	$(00)(10) = ((01),(00))$	3	13	$(12)(10) = ((11),(20))$	5
04	$(00)(02) = ((00),(02))$	2	14	$(12)(02) = ((10),(22))$	4
05	$(00)(11) = ((01),(01))$	1	15	$(12)(11) = ((11),(21))$	3
20	$(01)(00) = ((00),(10))$	4	30	$(10)(00) = ((10),(00))$	0
21	$(01)(12) = ((01),(12))$	3	31	$(10)(12) = ((11),(02))$	5
22	$(01)(01) = ((00),(11))$	2	32	$(10)(01) = ((10),(01))$	4
23	$(01)(10) = ((01),(10))$	1	33	$(10)(10) = ((11),(00))$	3
24	$(01)(02) = ((00),(12))$	0	34	$(10)(02) = ((10),(02))$	2
25	$(01)(11) = ((01),(11))$	5	35	$(10)(11) = ((11),(01))$	1
40	$(02)(00) = ((00),(20))$	2	50	$(11)(00) = ((10),(10))$	4
41	$(02)(12) = ((01),(22))$	1	51	$(11)(12) = ((11),(12))$	3
42	$(02)(01) = ((00),(21))$	0	52	$(11)(01) = ((10),(11))$	2
43	$(02)(10) = ((01),(20))$	5	53	$(11)(10) = ((11),(10))$	1
44	$(02)(02) = ((00),(22))$	4	54	$(11)(02) = ((10),(12))$	0
45	$(02)(11) = ((01),(21))$	3	55	$(11)(11) = ((11),(11))$	5

We now use the basic properties of the trace-like map over $R(n,m)$ to construct cocyclic Butson Hadamard matrices of order n and linear codes over $\mathbb{Z}_n$.

2.6 Cocyclic Butsons Hadamard matrices and linear codes via the trace-like map

In this section we define a cocycle by using the trace-like map in order to construct cocyclic Butson Hadamard matrices of order n^m and consequently to construct linear codes over $\mathbb{Z}_n$.

The following lemma can be used as an alternate way to prove the part (i) of the next theorem.

Lemma 2.6.1. *[Proposition 2.4, [6]]*
Let α and β be cocycles over G and H respectively. Then $\gamma = \alpha \times \beta$ defined by

$$\alpha \times \beta((a,c)(b,d)) = \alpha(a,b)\beta(c,d), \quad a,b \in G \text{ and } c,d \in H$$

is a cocycle over $G \times H$.

Theorem 2.6.2. *Let $\omega = exp\left(\frac{2\pi\sqrt{-1}}{n}\right)$ be the complex n^{th} root of unity, where $n = p_1^{e_1}p_2^{e_2}$. Let C_n be the set of all complex n^{th} roots of unity. Then*
(i) The set mapping

$$\varphi : R(n,m) \times R(n,m) \to C_n$$
$$\varphi(a,b) = \omega^{T(ab)}$$

is a cocycle.
(ii) The matrix $H = [\varphi(a,b)]_{a,b \in R(n,m)}$ is a Butson Hadamard matrix of order n^m.
(iii) The rows of the exponent matrix associated with H (i.e., $A = [T(ab)]_{a,b \in R(n,m)}$) form a linear code over $\mathbb{Z}_n$ with the parameters $[n,k,d_H] = \left[n^m, m, (n - p_1^{e_1}p_2^{e_2-1})n^{m-1}\right]$, where $p_1 < p_2$ and $e_1 \leq e_2$.

Proof:
(i) Let $a,b,c \in R(n,m)$. Then

$$\begin{aligned}
\varphi(a,b) &= \omega^{T(ab)}. \\
\varphi(a+b,c) &= \omega^{T((a+b)c)} = \omega^{T(ac)+T(bc)}. \\
\varphi(b,c) &= \omega^{T(bc)}. \\
\varphi(a,b+c) &= \omega^{T(a(b+c))} = \omega^{T(ab)+T(ac)}.
\end{aligned}$$

From these equations we have

$$\varphi(a,b)\varphi(a+b,c) = \varphi(b,c)\varphi(a,b+c).$$

Thus φ is a cocycle. This proof also follows from Lemma 2.6.1: If α and β are the cocycles defined over $GR(p_1^{e_1}, m)$ and $GR(p_2^{e_2}, m)$ respectively as in Theorem 2.4.1.
that is

$$\alpha : GR(p_1^{e_1}, m) \times GR(p_1^{e_1}, m) \to C_{p_1^{e_1}}$$
$$\alpha(a_1, a_2) = \omega_1^{Tr_1(a_1 a_2)}$$

and

$$\beta : GR(p_2^{e_2}, m) \times GR(p_2^{e_2}, m) \to C_{p_2^{e_2}}$$
$$\beta(b_1, b_2) = \omega_2^{Tr_2(b_1 b_2)}.$$

Then

$$\begin{aligned}
\alpha \times \beta : R(n,m) \times R(n,m) &\to C_n \\
\alpha \times \beta((a_1,b_1),(a_2,b_2)) &= \omega_1^{Tr_1(a_1a_2)} \omega_2^{Tr_2(b_1b_2)} \\
&= e^{\left(\frac{2\pi\sqrt{-1}}{p_1^{e_1}} Tr_1(a_1a_2)\right)} e^{\left(\frac{2\pi\sqrt{-1}}{p_2^{e_2}} Tr_2(b_1b_2)\right)} \\
&= e^{\left(\frac{2\pi\sqrt{-1}}{p_1^{e_1}p_2^{e_2}} \left(p_2^{e_2} Tr_1(a_1a_2) + p_1^{e_1} Tr_2(b_1b_2)\right)\right)} \\
&= e^{\left(\frac{2\pi\sqrt{-1}}{n} \left(p_2^{e_2} Tr_1(a_1a_2) + p_1^{e_1} Tr_2(b_1b_2)\right)\right)} \\
&= \omega^{T(ab)}, \quad a = (a_1,b_1) \text{ and } b = (a_2,b_2) \\
&= \varphi(a,b).
\end{aligned}$$

Therefore φ is a cocycle.
(ii) Let $H = [\varphi(a,b)]_{a,b \in R(n,m)}$. To prove that $HH^* = n^m I$, consider the sum

$$S = \sum_{x \in R(n,m)} \varphi(a,x)\overline{\varphi(x,b)}, \tag{2.6}$$

where $\overline{\varphi(x,b)}$ is the complex conjugate of $\varphi(x,b)$. From the properties of the trace-like map that we studied in Theorem 2.5.3 we have

$$S = \sum_{x \in R(n,m)} \omega^{T(x(a-b))}. \tag{2.7}$$

When $a = b$ it is clear that $S = n^m$.

When $a \neq b$, from Theorem 2.5.4 we have

$$S = \sum_{x \in R(n,m)} \omega^{T(x(a-b))} = p_1^i p_2^j n^{m-1} \sum_{t=0}^{\frac{n}{p_1^i p_2^j}-1} \omega^{p_1^i p_2^j t}, \tag{2.8}$$

where $0 \leq i \leq e_1$ and $0 \leq j \leq e_2$. From equation (2.1) we have $S = 0$. Thus the matrix $H = [\varphi(a,b)]_{a,b \in R(n,m)}$ is a Butson Hadamard matrix of order n^m. Since we used a cocycle for this construction, H is a cocyclic Butson Hadamard matrix of order n^m.

(iii) Let $B = [Tr_1(c_{1\alpha}c_{2\alpha})]_{c_{1\alpha},c_{2\alpha} \in GR(p_1^{e_1},m)}$ and $D = [Tr_2(c_{1\beta}c_{2\beta})]_{c_{1\beta},c_{2\beta} \in GR(p_2^{e_2},m)}$ be the codes over $\mathbb{Z}_{p_1^{e_1}}$ and $\mathbb{Z}_{p_2^{e_2}}$ respectively that we studied in Theorem 2.4.1. Let G_B and G_D be the generator matrices of the codes B and D respectively and consider the $m \times n^m$ matrix G_A defined by

$$G_A = p_2^{e_2} \left[p_2^{e_2 m} \text{ copies of } G_B\right] + p_1^{e_1} \left[p_1^{e_1 m} \text{ copies of } G_D\right]. \tag{2.9}$$

i.e.,

$$G_A = p_2^{e_2} \begin{bmatrix} p_2^{e_2 m}\text{copies of } \{Tr_1(c_{1l})\} \\ p_2^{e_2 m}\text{copies of } \{Tr_1(\zeta_1 c_{1l})\} \\ \vdots \\ p_2^{e_2 m}\text{copies of } \{Tr_1(\zeta_1^{m-1} c_{1l})\} \end{bmatrix} + p_1^{e_1} \begin{bmatrix} p_1^{e_1 m}\text{copies of } \{Tr_2(c_{2t})\} \\ p_1^{e_1 m}\text{copies of } \{Tr_2(\zeta_2 c_{2t})\} \\ \vdots \\ p_1^{e_1 m}\text{copies of } \{Tr_2(\zeta_2^{m-1} c_{2t})\} \end{bmatrix}, \text{ where}$$

$l = 1, 2, \ldots, p_1^{e_1 m}$ and $t = 1, 2, \ldots, p_2^{e_2 m}$. Thus the k^{th} row of G_A can be written as

$$x_k = p_2^{e_2} \left[Tr_1(\zeta_1^k c_{1l})\right] + p_1^{e_1} \left[Tr_2(\zeta_2^k c_{2t})\right], \tag{2.10}$$

where $0 \leq k \leq m-1$. That is,

$$x_k = (x_{k1}, x_{k2}, \ldots, x_{ka}, \ldots, x_{kn^m}), \tag{2.11}$$

where $x_{ka} = p_2^{e_2} Tr_1(\zeta_1^k c_{1l}) + p_1^{e_1} Tr_2(\zeta_2^k c_{2t})$ for some l and t.

Now let $\alpha_0, \alpha_1, \ldots, \alpha_{m-1} \in \mathbb{Z}_n$. Suppose that $\alpha_0 x_0 + \alpha_1 x_1 + \ldots + \alpha_{m-1} x_{m-1} = \underline{0}$ for $\alpha_0, \alpha_1, \ldots, \alpha_{m-1} \in \mathbb{Z}_n$.

Then for all $a = 1, 2, \ldots, n^m$,

$$\begin{aligned}
\alpha_0 x_{0a} + \alpha_1 x_{1a} + \ldots + \alpha_{m-1} x_{(m-1)a} &= 0. \\
\Rightarrow \alpha_0 \left(p_2^{e_2} Tr_1(c_{1l}) + p_1^{e_1} Tr_2(c_{2t})\right) + & \\
\alpha_1 \left(p_2^{e_2} Tr_1(\zeta_1 c_{1l}) + p_1^{e_1} Tr_2(\zeta_2 c_{2t})\right) + & \\
\ldots + \alpha_{m-1} \left(p_2^{e_2} Tr_1(\zeta_1^{m-1} c_{1l}) + p_1^{e_1} Tr_2(\zeta_2^{m-1} c_{2t})\right) &= 0 \ \forall \ l, t. \\
\Rightarrow p_2^{e_2} Tr_1\left(c_{1l}\left(\alpha_0 + \alpha_1\zeta_1 + \ldots + \alpha_{m-1}\zeta_1^{m-1}\right)\right) + & \\
p_1^{e_1} Tr_2\left(c_{2t}\left(\alpha_0 + \alpha_1\zeta_2 + \ldots + \alpha_{m-1}\zeta_2^{m-1}\right)\right) &= 0 \ \forall \ l, t. \\
\Rightarrow p_2^{e_2} Tr_1(c_{1l} c_1^{'}) + p_1^{e_1} Tr_2(c_{2t} c_2^{'}) &= 0 \ \forall \ l, t. \qquad (2.12)
\end{aligned}$$

Here $c_1^{'} = \alpha_0 + \alpha_1\zeta_1 + \ldots + \alpha_{m-1}\zeta_1^{m-1}$ and $c_2^{'} = \alpha_0 + \alpha_1\zeta_2 + \ldots + \alpha_{m-1}\zeta_2^{m-1}$.

Equation (2.12) is true if and only if

$$Tr_1(c_{1l} c_1^{'}) = 0 = Tr_2(c_{2t} c_2^{'}) \ \forall \ l, t.$$

However $c_{1l} \neq 0$ for all l and $c_{2t} \neq 0$ for at least one t. Therefore $c_1^{'} = 0$ and $c_2^{'} = 0$. If $c_1^{'} = \alpha_0 + \alpha_1\zeta_1 + \ldots + \alpha_{m-1}\zeta_1^{m-1} = 0$ then $\alpha_k = 0$ for all $k = 0, 1, \ldots, m-1$, since ζ_1^k are linearly independent in $GR(p_1^{e_1}, m)$. Similarly if $c_2^{'} = \alpha_0 + \alpha_1\zeta_2 + \ldots + \alpha_{m-1}\zeta_2^{m-1} = 0$ then $\alpha_k = 0$ for all $k = 0, 1, \ldots, m-1$, since ζ_2^k are linearly independent in $GR(p_2^{e_2}, m)$. Therefore x_k are linearly independent n^m-tuples over $\mathbb{Z}_n$. Taking all the linear combinations of rows of G_A we can generate the matrix A. If we consider the rows of A as codewords over $\mathbb{Z}_n$ then from Theorem 2.5.4 the Hamming weight of each non-zero codeword is given by $(n - p_1^i p_2^j) n^{m-1}$, where $i = 0, 1, 2, \ldots, e_1$ and $j = 0, 1, 2, \ldots, e_2$. If $p_2 > p_1$ and $e_2 \geq e_1$, the minimum Hamming weight is $(n - p_2^{e_2} p_1^{e_1 - 1}) n^{m-1}$. Since A is a linear code the minimum Hamming distance $d_H = (n - p_2^{e_2} p_1^{e_1 - 1}) n^{m-1}$. Thus $[n, k, d_H] = \left[n^m, m, (n - p_2^{e_2} p_1^{e_1 - 1}) n^{m-1}\right]$. □

The next example illustrates this result.

Example 2.6.3. *In this example we illustrate the code constructed by using the trace-like map over $R(6,2) = GF(2,2) \times GF(3,2)$. Let T be the trace-like map over $R(6,2)$ and Tr_1 and Tr_2 be the trace maps over $GF(2,2)$ and $GF(3,2)$ respectively.*

Let

$$B = [Tr_1(a_1 b_1)]_{a_1, b_1 \in GF(2,2)} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

and

$$G_B = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

G_B *is a generator matrix of* B.

Let

$$D = [Tr_2(a_2 b_2)]_{a_2, b_2 \in GF(3,2)} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 0 & 2 & 1 & 1 & 0 & 1 \\ 0 & 2 & 0 & 2 & 1 & 1 & 0 & 1 & 2 \\ 0 & 0 & 2 & 1 & 1 & 0 & 1 & 2 & 2 \\ 0 & 2 & 1 & 1 & 0 & 1 & 2 & 2 & 0 \\ 0 & 1 & 1 & 0 & 1 & 2 & 2 & 0 & 2 \\ 0 & 1 & 0 & 1 & 2 & 2 & 0 & 2 & 1 \\ 0 & 0 & 1 & 2 & 2 & 0 & 2 & 1 & 1 \\ 0 & 1 & 2 & 2 & 0 & 2 & 1 & 1 & 0 \end{bmatrix}$$

and

$$G_D = \begin{bmatrix} 0 & 2 & 2 & 0 & 2 & 1 & 1 & 0 & 1 \\ 0 & 2 & 0 & 2 & 1 & 1 & 0 & 1 & 2 \end{bmatrix}.$$

G_D *is a generator matrix of* D.

Now consider the matrix

$$G_A = 3[9 \text{ copies of } G_B] + 2[4 \text{ copies of } G_D].$$

That is,

$$\begin{bmatrix} 0 & 4 & 1 & 3 & 4 & 2 & 5 & 3 & 2 & 0 & 1 & 1 & 0 & 4 & 5 & 5 & 0 & 2 & 3 & 1 & 4 & 0 & 1 & 5 & 2 & 0 & 5 & 3 & 4 & 4 & 3 & 1 & 2 & 2 & 3 & 5 \\ 0 & 1 & 3 & 4 & 2 & 5 & 3 & 2 & 4 & 3 & 1 & 0 & 4 & 5 & 5 & 0 & 2 & 1 & 3 & 4 & 0 & 1 & 5 & 2 & 0 & 5 & 1 & 0 & 4 & 3 & 1 & 2 & 2 & 3 & 5 & 4 \end{bmatrix}.$$

Taking all the linear combinations of these two codewords over $\mathbb{Z}_6$ we obtain:

$$\begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&4&1&3&4&2&5&3&2&0&1&1&0&4&5&5&0&2&3&1&4&0&1&5&2&0&5&3&4&4&3&1&2&2&3&5\\
0&2&2&0&2&4&4&0&4&0&2&2&0&2&4&4&0&4&0&2&2&0&2&4&4&0&4&0&2&2&0&2&4&4&0&4\\
0&0&3&3&0&0&3&3&0&0&3&3&0&0&3&3&0&0&3&3&0&0&3&3&0&0&3&3&0&0&3&3&0&0&3&3\\
0&4&4&0&4&2&2&0&2&0&4&4&0&4&2&2&0&2&0&4&4&0&4&2&2&0&2&0&4&4&0&4&2&2&0&2\\
0&2&5&3&2&4&1&3&4&0&5&5&0&2&1&1&0&4&3&5&2&0&5&1&4&0&1&3&2&2&3&5&4&4&3&1\\
0&1&3&4&2&5&3&2&4&3&1&0&4&5&5&0&2&1&3&4&0&1&5&2&0&5&1&0&4&3&1&2&2&3&5&4\\
0&2&0&2&4&4&0&4&2&0&2&0&2&4&4&0&4&2&0&2&0&2&4&4&0&4&2&0&2&0&2&4&4&0&4&2\\
0&3&3&0&0&3&3&0&0&3&3&0&0&3&3&0&0&3&3&0&0&3&3&0&0&3&3&0&0&3&3&0&0&3&3&0\\
0&4&0&4&2&2&0&2&4&0&4&0&4&2&2&0&2&4&0&4&0&4&2&2&0&2&4&0&4&0&4&2&2&0&2&4\\
0&5&3&2&4&1&3&4&2&3&5&0&2&1&1&0&4&5&3&2&0&5&1&4&0&1&5&0&2&3&5&4&4&3&1&2\\
0&5&4&1&0&1&2&5&0&3&2&1&4&3&4&5&2&3&0&5&4&1&0&1&2&5&0&3&2&1&4&3&4&5&2&3\\
0&0&1&5&2&0&5&1&4&0&3&1&2&2&3&5&4&4&3&3&4&2&5&3&2&4&1&3&0&4&5&5&0&2&1&1\\
0&1&4&3&4&5&2&3&2&3&4&1&0&1&2&5&0&5&0&1&4&3&4&5&2&3&2&3&4&1&0&1&2&5&0&5\\
0&2&1&1&0&4&5&5&0&0&5&1&4&0&1&5&2&0&3&5&4&4&3&1&2&2&3&3&2&4&1&3&4&2&5&3\\
0&3&4&5&2&3&2&1&4&3&0&1&2&5&0&5&4&1&0&3&4&5&2&3&2&1&4&3&0&1&2&5&0&5&4&1\\
0&3&5&4&4&3&1&2&2&3&3&2&4&1&3&4&2&5&3&0&2&1&1&0&4&5&5&0&0&5&1&4&0&1&5&2\\
0&1&0&1&2&5&0&5&4&3&4&3&4&5&2&3&2&1&0&1&0&1&2&5&0&5&4&3&4&3&4&5&2&3&2&1\\
0&5&1&4&0&1&5&2&0&3&5&4&4&3&1&2&2&3&3&2&4&1&3&4&2&5&3&0&2&1&1&0&4&5&5&0\\
0&3&2&1&4&3&4&5&2&3&0&5&4&1&0&1&2&5&0&3&2&1&4&3&4&5&2&3&0&5&4&1&0&1&2&5\\
0&4&2&2&0&2&4&4&0&0&4&2&2&0&2&4&4&0&0&4&2&2&0&2&4&4&0&0&4&2&2&0&2&4&4&0\\
0&5&5&0&2&1&1&0&4&3&5&2&0&5&1&4&0&1&3&2&2&3&5&4&4&3&1&0&2&5&3&2&4&1&3&4\\
0&0&2&4&4&0&4&2&2&0&0&2&4&4&0&4&2&2&0&0&2&4&4&0&4&2&2&0&0&2&4&4&0&4&2&2\\
0&1&5&2&0&5&1&4&0&3&1&2&2&3&5&4&4&3&3&4&2&5&3&2&4&1&3&0&4&5&5&0&2&1&1&0\\
0&2&3&5&4&4&3&1&2&0&5&3&2&4&1&3&4&2&3&5&0&2&1&1&0&4&5&3&2&0&5&1&4&0&1&5\\
0&3&0&3&0&3&0&3&0&3&0&3&0&3&0&3&0&3&0&3&0&3&0&3&0&3&0&3&0&3&0&3&0&3&0&3\\
0&4&3&1&2&2&3&5&4&0&1&3&4&2&5&3&2&4&3&1&0&4&5&5&0&2&1&3&4&0&1&5&2&0&5&1\\
0&5&0&5&4&1&0&1&2&3&2&3&2&1&4&3&4&5&0&5&0&5&4&1&0&1&2&3&2&3&2&1&4&3&4&5\\
0&0&4&2&2&0&2&4&4&0&0&4&2&2&0&2&4&4&0&0&4&2&2&0&2&4&4&0&0&4&2&2&0&2&4&4\\
0&1&1&0&4&5&5&0&2&3&1&4&0&1&5&2&0&5&3&4&4&3&1&2&2&3&5&0&4&1&3&4&2&5&3&2\\
0&2&4&4&0&4&2&2&0&0&2&4&4&0&4&2&2&0&0&2&4&4&0&4&2&2&0&0&2&4&4&0&4&2&2&0\\
0&3&1&2&2&3&5&4&4&3&3&4&2&5&3&2&4&1&3&0&4&5&5&0&2&1&1&0&0&1&5&2&0&5&1&4\\
0&4&5&5&0&2&1&1&0&0&1&5&2&0&5&1&4&0&3&1&2&2&3&5&4&4&3&3&4&2&5&3&2&4&1&3\\
0&5&2&3&2&1&4&3&4&3&2&5&0&5&4&1&0&1&0&5&2&3&2&1&4&3&4&3&2&5&0&5&4&1&0&1\\
0&0&5&1&4&0&1&5&2&0&3&5&4&4&3&1&2&2&3&3&2&4&1&3&4&2&5&3&0&2&1&1&0&4&5&5\\
0&1&2&5&0&5&4&1&0&3&4&5&2&3&2&1&4&3&0&1&2&5&0&5&4&1&0&3&4&5&2&3&2&1&4&3
\end{bmatrix}.$$

This is the code given by $A = [T(ab)]_{a,b \in R(6,2)}$. It is clear that the parameters of this code are $[36, 2, 18]$.

Thus far we have studied the trace-like map over $R(n, m)$ for $n = p_1^{e_1} p_2^{e_2}$. It is relatively straight forward to extend these results to the case $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$.

Theorem 2.6.4. *Let Tr_i be the trace map over $GR(p_i^{e_i}, m)$, where $i = 1, 2, \dots, k$, as defined in section 2.3. The mapping defined over $R(n, m)$ by*

$$T : R(n, m) \to \mathbb{Z}_n$$
$$T(c) = \sum_{i=1}^{k} \frac{n}{p_i^{e_i}} Tr_i(c_i)$$

satisfies the following properties.

For $c, c' \in R(n,m)$ and $\alpha \in \mathbb{Z}_n$:

(i) $T(c+c') = T(c) + T(c')$.

(ii) $T(\alpha c) = \alpha T(c)$.

(iii) T is surjective.

Proof is similar to that of Theorem 2.5.3.

As in Theorem 2.5.4, the next theorem describes the distribution of $T(cx)$.

Theorem 2.6.5. *For $c \in R(n,m)$, as x ranges over $R(n,m)$, $T(cx)$ takes each element in*

$$S_l = \left\{ \prod_{i=1}^{k} p_i^{l_i} t | t = 0, 1, 2, \ldots, \frac{n}{\prod_{i=1}^{k} p_i^{l_i}} - 1 \right\} \tag{2.13}$$

equally often i.e., $\prod_{i=1}^{k} p_i^{l_i} n^{m-1}$ times, where $l = (l_1, l_2, \ldots, l_k)$, $0 \leq l_i \leq e_i$ for $i = 1, 2, \ldots, k$.

Proof is similar to that of Theorem 2.5.4.

We use these properties of the trace-like map T over $R(n,m)$ to construct cocyclic Butson Hadamard matrices of order n^m for any n and consequently to construct cocyclic codes over $\mathbb{Z}_n$. The next theorem describes this construction.

Theorem 2.6.6. *Let $\omega = exp\left(\frac{2\pi\sqrt{-1}}{n}\right)$ be the complex n^{th} root of unity, where $n = \prod_{i=1}^{k} p_i^{e_i}$. Let C_n be the set of all complex n^{th} root of unity.*

(i) The set mapping

$$\varphi : R(n,m) \times R(n,m) \to C_n$$
$$\varphi(a,b) = \omega^{T(ab)}$$

is a cocycle.

(ii) The matrix $H = [\varphi(a,b)]_{a,b \in R(n,m)}$ is a Butson Hadamard matrix of order n^m.

(iii) The rows of the exponent matrix associated with H (i.e., $A = [T(ab)]_{a,b \in R(n,m)}$) form a linear code over $\mathbb{Z}_n$ with the parameters $[n,k,d_H] = \left[n^m, m, (n - p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k - 1}) n^{m-1}\right]$.

Proof is similar to that of Theorem 2.6.2. In this case the generator matrix G_A of the code A is

$$G_A = \sum_{i=1}^{k} \left(\frac{n}{p_i^{e_i}}\right) \left[\left(\frac{n}{p_i^{e_i}}\right)^m \text{ copies of } G_i \right],$$

where G_i is the generator matrix of the code $A_i = \left[Tr_i(cc')\right]_{c,c' \in GR(p_i^{e_i},m)}$.

We have now constructed codes over $\mathbb{Z}_n$ by using the trace-like map over $R(n,m)$ in the form of $T(ax)$. In the next section we calculate the Lee, Euclidean and Chinese Euclidean weights of these codes.

2.7 The Lee, Euclidean and Chinese Euclidean weights

In this section we first calculate the Lee, Euclidean and Chinese Euclidean weights of the codewords of $A = [T(ab)]_{a,b \in R(n,m)}$, where $n = p_1^{e_1} p_2^{e_2}$. Let x be any row of the matrix A. As in Theorem 2.5.4 x consists of elements from

$$S_{i,j} = \left\{ p_1^i p_2^j t | t = 0, 1, 2, \ldots, \frac{n}{p_1^i p_2^j} - 1 \right\}$$

equally often $p_1^i p_2^j n^{m-1}$ times, where $0 \leq i \leq e_1$ and $0 \leq j \leq e_2$.

Case I: $p_1 = 2$ and $p_2 > 2$

For $0 \leq i \leq e_1 - 1$ and $0 \leq j \leq e_2 - 1$ the Lee weight of x is given by

$$\begin{aligned} W_{L1}(x) &= n^{m-1} 2^i p_2^j \left(2 \left(2^i p_2^j \left(\sum_{t=0}^{\frac{n}{2p_2^j 2^i} - 1} t \right) \right) + \frac{n}{2} \right) \\ W_{L1}(x) &= n^{m-1} \left(\frac{n^2}{4} \right) = \frac{n^{m+1}}{4} \end{aligned}$$

and for $i = e_1$ and $0 \leq j \leq e_2 - 1$ it is given by

$$\begin{aligned} W_{L2}(x) &= n^{m-1} 2^{e_1} p_2^j \left(2 \left(2^{e_2} p_2^j \left(\sum_{t=0}^{\frac{\frac{n}{2^{e_1} p_2^j} - 1}{2}} t \right) \right) \right) \\ W_{L2}(x) &= \frac{n^{m-1}(n^2 - (2^{e_1} p_2^j)^2)}{4}. \end{aligned}$$

In this case the Euclidean weight of x is given by following formulae:

For $0 \leq i \leq e_1 - 1$ and $0 \leq j \leq e_2 - 1$

$$\begin{aligned} W_{E1}(x) &= n^{m-1} 2^i p_2^j \left(2 \left((2^i p_2^j)^2 \left(\sum_{t=0}^{\frac{n}{2p_2^j 2^i} - 1} (t)^2 \right) \right) + \left(\frac{n}{2} \right)^2 \right) \\ W_{E1}(x) &= n^{m-1} \left(\frac{n}{12} \left(n^2 - 3n 2^i p_2^j + 2 \left(p_2^j 2^i \right)^2 \right) + \frac{n^2 2^i p^j}{4} \right). \end{aligned}$$

For $i = e_1$ and $0 \leq j \leq e_2 - 1$

$$\begin{aligned} W_{E2}(x) &= n^{m-1} 2^{e_1} p_2^j \left(2 \left((2^{e_1} p_2^j)^2 \left(\sum_{t=0}^{\frac{\frac{n}{2^{e_1} p_2^j} - 1}{2}} (t)^2 \right) \right) \right) \\ W_{E2}(x) &= n^{m-1} \left(\frac{n}{12} \left(n^2 - \left(2^{e_1} p_2^j \right)^2 \right) \right). \end{aligned}$$

The Chinese Euclidean weight in this case is given by

$$\begin{aligned} W_{CE}(x) &= n^{m-1} 2^i p_2^j \left(\sum_{t=0}^{\frac{n}{2^i p_2^j} - 1} \left(2 - 2 \cos \left(\frac{2\pi t 2^i p_2^j}{n} \right) \right) \right) \\ W_{CE}(x) &= 2n^m. \end{aligned}$$

Case II: $p_1 \neq p_2 > 2$, $0 \leq i \leq e_1 - 1$ and $0 \leq j \leq e_2 - 1$.

In this case the Lee weight is given by

$$\begin{aligned} W_L(x) &= n^{m-1} p_1^i p_2^j \left(2 \left(p_1^i p_2^j \left(\sum_{t=0}^{\frac{\frac{n}{p_1^i p_2^j} - 1}{2}} t \right) \right) \right) \\ W_L(x) &= \frac{n^{m-1}(n^2 - (p_1^i p_2^j)^2)}{4}, \end{aligned}$$

the Euclidean weight is given by

$$\begin{aligned} W_E(x) &= n^{m-1} p_1^i p_2^j \left(2 \left((p_1^i p_2^j)^2 \left(\sum_{t=0}^{\frac{\frac{n}{p_1^i p_2^j} - 1}{2}} (t)^2 \right) \right) \right) \\ W_E(x) &= n^{m-1} \left(\frac{n}{12} \left(n^2 - \left(p_1^i p_2^j \right)^2 \right) \right) \end{aligned}$$

and the Chinese Euclidean weight is given by

$$\begin{aligned} W_{CE}(x) &= n^{m-1} p_1^i p_2^j \left(\sum_{t=0}^{\frac{n}{p_1^i p_2^j} - 1} \left(2 - 2 \cos \left(\frac{2\pi t p_1^i p_2^j}{n} \right) \right) \right) \\ W_{CE}(x) &= 2n^m. \end{aligned}$$

We can naturally extend the weights for the code $A = [T(ab)]_{a,b\in R(n,m)}$, where $n = \prod_{i=1}^{k} p_i^{e_i}$. Let x be any row of the matrix A. As in Theorem 2.6.5, x consists of elements from

$$S_l = \left\{ \prod_{i=1}^{k} p_i^{l_i} t | t = 0, 1, 2, \ldots, \frac{n}{\prod_{i=1}^{k} p_i^{l_i}} - 1 \right\}$$

equally often $\prod_{i=1}^{k} p_i^{l_i} n^{m-1}$ times, where $l = (l_1, l_2, \ldots, l_k)$, $0 \leq l_i \leq e_i$ for $i = 1, 2, \ldots, k$.

Case I: $p_1 = 2$ and $p_i > 2$ for $i = 2, 3, \ldots, k$.

For $0 \leq l_1 \leq e_1 - 1$ and $0 \leq l_i \leq e_i$, $i = 2, 3, \ldots, k$, the Lee weight of x is given by

$$\begin{aligned} W_{L1}(x) &= n^{m-1} 2^{l_1} \prod_{i=2}^{k} p_i^{l_i} \left(2 \left(2^{l_1} \prod_{i=2}^{k} p_i^{l_i} \left(\sum_{t=0}^{\frac{n}{2^{2l_1} \prod_{i=2}^{k} p_i^{l_i}} - 1} t \right) \right) + \frac{n}{2} \right) \\ W_{L1}(x) &= n^{m-1} \left(\frac{n^2}{4} \right) = \frac{n^{m+1}}{4} \end{aligned}$$

and for $l_1 = e_1$ and $0 \leq l_i \leq e_i - 1$, $i = 2, 3, \ldots, k$, it is given by

$$\begin{aligned} W_{L2}(x) &= n^{m-1} 2^{e_1} \prod_{i=2}^{k} p_i^{l_i} \left(2 \left(2^{e_1} \prod_{i=2}^{k} p_i^{l_i} \left(\sum_{t=0}^{\frac{\frac{n}{2^{e_1} \prod_{i=2}^{k} p_i^{l_i}}}{2} - 1} t \right) \right) \right) \\ W_{L2}(x) &= \frac{n^{m-1}(n^2 - (2^{e_1} \prod_{i=2}^{k} p_i^{l_i})^2)}{4}. \end{aligned}$$

In this case the Euclidean weight of x is given by following formulae.

For $0 \leq l_1 \leq e_1 - 1$ and $0 \leq l_i \leq e_i$, $i = 2, 3, \ldots, k$

$$\begin{aligned} W_{E1}(x) &= n^{m-1} 2^{l_1} \prod_{i=2}^{k} p_i^{l_i} \left(2 \left(\left(2^{l_1} \prod_{i=2}^{k} p_i^{l_i} \right)^2 \left(\sum_{t=0}^{\frac{n}{2^{2l_1} \prod_{i=2}^{k} p_i^{l_i}} - 1} (t)^2 \right) \right) + \left(\frac{n}{2} \right)^2 \right) \\ W_{E1}(x) &= n^{m-1} \left(\frac{n}{12} \left(n^2 - 3n 2^{l_1} \prod_{i=2}^{k} p_i^{l_i} + 2 \left(2^{l_1} \prod_{i=2}^{k} p_i^{l_i} \right)^2 \right) + \frac{n^2 2^{l_1} \prod_{i=2}^{k} p_i^{l_i}}{4} \right). \end{aligned}$$

and for $l_1 = e_1$ and $0 \leq l_i \leq e_i - 1$, $i = 2, 3, \ldots, k$

$$\begin{aligned} W_{E2}(x) &= n^{m-1} 2^{e_1} \prod_{i=2}^{k} p_i^{l_i} \left(2 \left(\left(2^{e_1} \prod_{i=2}^{k} p_i^{l_i} \right)^2 \left(\sum_{t=0}^{\frac{\frac{n}{2^{e_1} \prod_{i=2}^{k} p_i^{l_i}} - 1}{2}} (t)^2 \right) \right) \right) \\ W_{E2}(x) &= n^{m-1} \left(\frac{n}{12} \left(n^2 - \left(2^{e_1} \prod_{i=2}^{k} p_i^{l_i} \right)^2 \right) \right). \end{aligned}$$

The Chinese Euclidean weight in this case is given by

$$\begin{aligned} W_{CE}(x) &= n^{m-1} 2^{l_1} \prod_{i=2}^{k} p_i^{l_i} \left(\sum_{t=0}^{\frac{n}{2^{l_1} \prod_{i=2}^{k} p_i^{l_i}} - 1} \left(2 - 2 \cos \left(\frac{2\pi t 2^{l_1} \prod_{i=2}^{k} p_i^{l_i}}{n} \right) \right) \right) \\ W_{CE}(x) &= 2n^m. \end{aligned}$$

Case II: $p_1 \neq p_2 > 2$.

For $0 \leq l_i \leq e_i - 1$ and $i = 1, 2, \ldots, k$ the Lee weight is given by

$$\begin{aligned} W_L(x) &= n^{m-1} \prod_{i=1}^{k} p_i^{l_i} \left(2 \left(\prod_{i=1}^{k} p_i^{l_i} \left(\sum_{t=0}^{\frac{\frac{n}{\prod_{i=1}^{k} p_i^{l_i}} - 1}{2}} t \right) \right) \right) \\ W_L(x) &= \frac{n^{m-1} (n^2 - \left(\prod_{i=1}^{k} p_i^{l_i} \right)^2)}{4}, \end{aligned}$$

the Euclidean weight is given by

$$\begin{aligned} W_E(x) &= n^{m-1} \prod_{i=1}^{k} p_i^{l_i} \left(2 \left(\left(\prod_{i=1}^{k} p_i^{l_i} \right)^2 \left(\sum_{t=0}^{\frac{\frac{n}{\prod_{i=1}^{k} p_i^{l_i}} - 1}{2}} (t)^2 \right) \right) \right) \\ W_E(x) &= n^{m-1} \left(\frac{n}{12} \left(n^2 - \left(\prod_{i=1}^{k} p_i^{l_i} \right)^2 \right) \right) \end{aligned}$$

and the Chinese Euclidean weight is given by

$$\begin{aligned} W_{CE}(x) &= n^{m-1} \prod_{i=1}^{k} p_i^{l_i} \left(\sum_{t=0}^{\frac{n}{\prod_{i=1}^{k} p_i^{l_i}} - 1} \left(2 - 2 \cos \left(\frac{2\pi t \prod_{i=1}^{k} p_i^{l_i}}{n} \right) \right) \right) \\ W_{CE}(x) &= 2n^m. \end{aligned}$$

We now have enough information to classify the code that we have constructed by using the trace-like map over $R(n,m)$ in the case of $n=6$ as a simplex code of type α.

2.8 Cocyclic senary simplex codes of type α

In this section we point out the definition and basic properties of senary simplex codes of type α as studied by Gupta et al. [37]. Then we use the technique that we have introduced in section 2.6 to form cocyclic senary simplex codes of type α.

Definition 2.8.1. *[[37]] Let G_m^α be a $m \times 2^m 3^m$ matrix over $\mathbb{Z}_6$ consisting of all possible distinct columns. Inductively, G_m^α is written as*

$$G_m^\alpha = \left[\begin{array}{c|c|c|c|c|c} 00\ldots0 & 11\ldots1 & 22\ldots2 & 33\ldots3 & 44\ldots4 & 55\ldots5 \\ \hline G_{m-1} & G_{m-1} & G_{m-1} & G_{m-1} & G_{m-1} & G_{m-1} \end{array}\right]$$

with $G_1^\alpha = [012345]$. The code S_m^α generated by G_m^α is called the senary simplex code of type α.

The code S_m^α has the following Hamming, Lee, Euclidean and Chinese Euclidean weight distributions.

$A_H(0) = 1, \quad A_H(3\cdot 6^{m-1}) = 2^m - 1, \quad A_H(4\cdot 6^{m-1}) = 3^m - 1, \quad A_H(5\cdot 6^{m-1}) = (2^m-1)(3^m-1)$.

$A_L(0) = 1, \ A_L(8\cdot 6^{m-1}) = 3^m - 1, \ A_L(9\cdot 6^{m-1}) = 3^m(2^m-1)$.

$A_E(0) = 1, \quad A_E(27\cdot 6^{m-1}) = 2^m - 1, \quad A_E(16\cdot 6^{m-1}) = 3^m - 1, \quad A_H(19\cdot 6^{m-1}) = (2^m-1)(3^m-1)$.

$A_{CE}(0) = 1, \ A_E(2\cdot 6^m) = 3^m\cdot 2^m - 1$.

Here $A_H(i), \ A_L(i), \ A_E(i), \ A_{CE}(i)$ denotes the number of 6^m-tuples of Hamming, Lee, Euclidean and Chinese Euclidean weight i in S_m^α.

S_m^α is an equidistance code with respect to Chinese Euclidean distance. For more details of this code read [37].

In the case of $p_1 = 3, p_2 = 2, e_1 = e_2 = 1$, the generator matrix G_A in section 2.6 is permutation equivalent to G_m^α. Hence the code generated by G_A is a senary simplex code of type α and in particular this is a cocyclic senary simplex code of type α. See Example 2.6.3 for S_2^α. Types β and γ codes of this type follow from G_A as described in [37].

2.9 The Weighted-Trace map

Thus far in this chapter we have studied the trace-like map and its fundamental properties parallel to the trace map over Galois rings and Galois fields. The ring $R(n, m)$ was the direct product of Galois rings and Galois fields of the same degree (say m). This is a motivation to study the ring $R(d, n)$ that can be constructed by taking the direct product of Galois rings and Galois fields of different degrees (say $m_1, m_2, \ldots, m_k$), where $d = p_1^{e_1 m_1} p_2^{e_2 m_2} \ldots p_k^{e_k m_k}$ and $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$. In this section we study the structure of this ring and give the definition of the weighted-trace map T_w that first appeared in [45]. We study the the fundamental properties of T_w and notice that the weighted-trace map is a generalisation of the trace-like map. We use these properties to construct cocyclic Butson Hadamard matrices H_w of order d. However, unlike in Section 2.6, the exponent matrix A_w associated with H_w does not form a linear code over $\mathbb{Z}_n$. Experimental results shows that the code A_w is non-linear over $\mathbb{Z}_n$.

Let $GR(p_i^{e_i}, m_i)$ be the Galois ring of characteristic $p_i^{e_i}$ and degree m_i, where $i = 1, 2, \ldots, k$. Let $R(d, n)$ be the direct product of these rings. i.e., $R(d, n) = GR(p_1^{e_1}, m_1) \times GR(p_2^{e_2}, m_2) \ldots \times GR(p_k^{e_k}, m_k)$, where $d = p_1^{e_1 m_1} p_2^{e_2 m_2} \ldots p_k^{e_k m_k}$ and $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$. Any element $c \in R(d, n)$ can be written as $c = (c_1, c_2, \ldots, c_k)$, where $c_i \in GR(p_i^{e_i}, m_i)$, for $i = 1, 2, \ldots, k$. Since $GR(p_i^{e_i}, m_i) \cong \mathbb{Z}_{p_i^{e_i}}^{m_i}$ we can write c_i as an m_i - tuple over $\mathbb{Z}_{p_i^{e_i}}$. i.e., $c_i = (c_i^1, c_i^2, \ldots, c_i^{m_i})$, where $c_i^j \in \mathbb{Z}_{p_i^{e_i}}$, for $j = 1, 2, \ldots, m_i$. Let $M = \sum_{i=1}^{k} m_i$. We can now write the elements of $R(d, n)$ as M-tuples $c = ((c_1^1, c_1^2, \ldots, c_1^{m_1}), (c_2^1, c_2^2, \ldots, c_2^{m_2}), \ldots, (c_k^1, c_k^2, \ldots, c_k^{m_k}))$, where $c_i^j \in \mathbb{Z}_{p_i^{e_i}}$, for $j \in \{1, 2, \ldots, m_i\}$.

Let $c, c' \in R(d, n)$ and define the addition and multiplication of c, c' as follows:

$c + c' = (c_1 + c_1', c_2 + c_2', \ldots, c_k + c_k')$ and $cc' = (c_1 c_1', c_2 c_2', \ldots, c_k c_k')$.

It is easy to show that $R(d, n)$ is a ring under these binary operations and also that the number of elements of $R(d, n)$, denoted by d is given by $d = \prod_{i=1}^{k} p_i^{e_i m_i}$.
i.e., $d = \prod_{i=1}^{k} |GR(p_i^{e_i}, m_i)|$, where $|GR(p_i^{e_i}, m_i)|$ is the number of elements of $GR(p_i^{e_i}, m_i)$.

Definition 2.9.1 (Weighted-trace map). *Let Tr_i be the trace map over the Galois ring $GR(p_i^{e_i}, m_i)$, where $i = 1, 2, \ldots, k$. The weighted-trace map over the ring $R(d, n)$ is*

defined by

$$\begin{aligned} T_w &: R(d,n) \to \mathbb{Z}_n \\ T_w(x) &= \sum_{i=1}^{k} \frac{n}{p_i^{e_i}} Tr_i(x_i). \end{aligned}$$

As in Theorem 2.5.3 we can prove that the weighted-trace map satisfies the following properties:

Theorem 2.9.2. *Let T_w be the weighted-trace map over the ring $R(d,n)$, where $d = p_1^{e_1 m_1} p_2^{e_2 m_2} \dots p_k^{e_k m_k}$ and $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$. For $c, c' \in R(d,n)$ and $\alpha \in \mathbb{Z}_n$ the following properties are satisfied by T_w:*
(i) $T_w(c + c') = T_w(c) + T_w(c')$.
(ii) $T_w(\alpha c) = \alpha T_w(c)$.
(iii) T_w is surjective.

The weighted-trace map T_w also satisfies the following property which is very similar to that of the trace-like map in Theorem 2.6.5.

Theorem 2.9.3. *Let $c = (c_1, c_2) \in R(d,n)$ and T_w be the weighted-trace map over $R(d,n)$. As x ranges over $R(d,n)$, $T_w(cx)$ takes each element in $S_l = \{\prod_{i=1}^{k} p_i^{l_i} t | t = 0, 1, 2, \dots, \frac{n}{\prod_{i=1}^{k} p_i^{l_i}} - 1\}$ equally often i.e., $\prod_{i=1}^{k} p_i^{e_i(m_i-1)+l_i}$ times, where $l = (l_1, l_2, \dots, l_k)$, $0 \le l_i \le e_i$ for $i = 1, 2, \dots, k$.*

We can use T_w to construct Butson Hadamard matrices of order d and consequently to construct non-linear codes over $\mathbb{Z}_n$ as follows:

Theorem 2.9.4. *Let $n = \prod_{i=1}^{k} p_i^{e_i}$ and $\omega_n = e^{\frac{2\pi\sqrt{-1}}{n}}$ be the complex n^{th} root of unity. Let C_n be the multiplicative group of all complex n^{th} roots of unity and T_w be the weighted-trace map over the ring $R(d,n)$. Then*
(i) The set mapping defined by

$$\begin{aligned} \varphi : R(d,n) \times R(d,n) &\to C_n \\ \varphi(a,b) &= \omega_n^{T_w(ab)} \end{aligned}$$

is a cocycle.

(ii) Matrix $H_w = [\varphi(a,b)]_{a,b\in R(d,n)}$ *is a Butson Hadamard matrix of order* d.

(iii) The exponent matrix of H_w, *i.e.,* $A_w = [T_w(ab)]_{a,b\in R(d,n)}$ *forms a non-linear code over* $\mathbb{Z}_n$ *with the parameters* (d, N, w_H), *where* $d = \prod_{i=1}^{k} p_i^{e_i m_i}$ *is the length of the code,* $N = \prod_{i=1}^{k} p_i^{e_i m_i}$ *is the number of codewords and* $w_H = d - p_k^{e_k m_k} \dots p_2^{e_2 m_2} p_1^{e_1 m_1 - 1}$ *is the minimum Hamming weight provided that* $p_1^{e_1} < p_2^{e_2} < \ldots < p_k^{e_k}$ *and* $m_1 < m_2 < \ldots < m_k$.

Proof:

(i) and (ii) are the same as Theorem 2.6.2.

(iii) Since the number of elements in $R(d,n)$ is d, it is clear that the length of the code A_w is $d = \prod_{i=1}^{k} p_i^{e_i m_i}$ and the number of codewords in A_w is also $N = \prod_{i=1}^{k} p_i^{e_i m_i}$. From Theorem 2.9.3 it is clear that the Hamming weight of each codeword in A_w is given by $d - \prod_{i=1}^{k} p_i^{e_i(m_i-1)+l_i}$, where $0 \le l_i \le e_i$ for $i = 1, 2, \ldots, k$. When $p_1^{e_1} < p_2^{e_2} < \ldots < p_k^{e_k}$ and $m_1 < m_2 < \ldots < m_k$ the minimum Hamming weight of codewords in A_w is $w_H = d - p_k^{e_k m_k} \dots p_2^{e_2 m_2} p_1^{e_1 m_1 - 1}$. Thus A_w is a $(d, d, d - p_k^{e_k m_k} \dots p_2^{e_2 m_2} p_1^{e_1 m_1 - 1})$ code over $\mathbb{Z}_n$. □

The next example illustrates this result.

Example 2.9.5. *Consider the ring* $R(12,6) = GF(2,2) \times GF(3,1)$. *The trace maps* Tr_1 *and* Tr_2 *over* $GF(2,2)$ *and* $GF(3,1)$ *are given by*

$$Tr_1 : GF(2,2) \to \mathbb{Z}_2$$
$$Tr_1(c_1) = c_1 + c_1^2$$
and
$$Tr_2 : GF(3,1) \to \mathbb{Z}_3$$
$$Tr_2(c_2) = c_2$$

respectively.

The following tables illustrate the values of trace maps.

c_1	$Tr_1(c_1)$
00	0
10	0
01	1
11	1

c_2	$Tr_2(c_2)$
0	0
1	1
2	2

The weighted-trace map T_w *over the ring* $R(12,6)$ *is*

$$T_w : R(12,6) \to \mathbb{Z}_6$$
$$T_w(c) = 3Tr_1(c_1) + 2Tr_2(c_2),$$

where $c_1 \in GF(2,2)$ *and* $c_2 \in GF(3,1)$.

The elements of the ring $R(12,6)$ *and their weighted-trace values are given in the following table.*

c	$T_w(c)$
$(0,0),0$	*0*
$(0,0),1$	*2*
$(0,0),2$	*4*
$(1,0),0$	*0*
$(1,0),1$	*2*
$(1,0),2$	*4*
$(0,1),0$	*3*
$(0,1),1$	*5*
$(0,1),2$	*1*
$(1,1),0$	*3*
$(1,1),1$	*5*
$(1,1),2$	*1*

The code $A_w = [T_w(ax)]_{a,x\in R(12,6)}$ *is*

$$A_w = \left[\begin{array}{cccccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 2 & 4 & 0 & 2 & 4 & 0 & 2 & 4 & 0 & 2 & 4 \\
0 & 4 & 2 & 0 & 4 & 2 & 0 & 4 & 2 & 0 & 4 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 3 & 3 & 3 & 3 & 3 & 3 \\
0 & 2 & 4 & 0 & 2 & 4 & 3 & 5 & 1 & 3 & 5 & 1 \\
0 & 4 & 2 & 0 & 4 & 2 & 3 & 1 & 5 & 3 & 1 & 5 \\
0 & 0 & 0 & 3 & 3 & 3 & 3 & 3 & 3 & 0 & 0 & 0 \\
0 & 2 & 4 & 3 & 5 & 1 & 3 & 5 & 1 & 0 & 2 & 4 \\
0 & 4 & 2 & 3 & 1 & 5 & 3 & 1 & 5 & 0 & 4 & 2 \\
0 & 0 & 0 & 3 & 3 & 3 & 0 & 0 & 0 & 3 & 3 & 3 \\
0 & 2 & 4 & 3 & 5 & 1 & 0 & 2 & 4 & 3 & 5 & 1 \\
0 & 2 & 4 & 3 & 1 & 5 & 0 & 2 & 4 & 3 & 1 & 5
\end{array}\right]$$

and its parameters (d, N, w_H) *are* $(12, 12, 6)$

Clearly A_w is a non-linear codes since the sum of the 10^{th} and 12^{th} rows is not a codeword in A_w.

In this section we used the weighted-trace map T_w to construct cocyclic Butson Hadamard matrices and non-linear codes over $\mathbb{Z}_n$. In the next chapter we will use T_w to construct mutually unbiased bases of odd integer dimension $d = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$.

Chapter 3

Mutually Unbiased Bases (MUBs)

3.1 Introduction

Two orthonormal bases B and $B^{'}$ of the vector space $\mathbb{C}^d$ are called mutually unbiased if and only if $| < b, b^{'} > | = \frac{1}{\sqrt{d}}$, for all $b \in B$ and $b^{'} \in B^{'}$, where $\mathbb{C}$ is the complex number set. Recently researchers have focused their attention on construction of mutually unbiased bases (MUBs) in different dimensions. In [49] A. Klappenecker and M. Rotteler used the properties of trace maps over the Galois field $GF(p, m)$ and the Galois ring $GR(4, m)$ to construct MUBs of odd and even prime power dimensions respectively.

Let $N(d)$ denote the number of MUBs of $\mathbb{C}^d$. It is well know that the number of MUBs is at most $d + 1$ [7, 42, 81]. Sets attaining these bounds are extremely interesting because they allow quantum state tomography with projective measurements consisting of a minimal number of operators [47]. It is also known that $N(d) = d + 1$ if d is a prime power dimension [7, 47, 81]. The exact value of $N(d)$ is not known for non-prime dimension d. However in [49] it has been proved that if $d = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ then $N(d) \geq \min\{N(p_1^{e_1}), N(p_2^{e_2}), \dots, N(p_k^{e_k})\}$ and the case $d = 6$ is studied in [35]. In this chapter we use the weighted-trace map T_w that we studied in Section 2.9 to construct $\min\{N(p_1^{e_1}), N(p_2^{e_2}), \dots, N(p_k^{e_k})\} + 1$ MUBs of odd integer dimension d given by $d = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$. Lemma 3 in [49] gives a product construction of MUBs of odd integer dimension d, but it is clear that this is an elimination search. Our construction is very structured and points to possible future work in the area.

In Section 3.2 we study the basic theory of MUBs and give some known construction methods. Section 3.3 is devoted to the construction of MUBs of odd integer dimension d by using the weighted-trace map T_w and finally we give a couple of examples to illustrate the construction.

3.2 Preliminaries and known results

Let $\mathbb{C}^d$ be the complex vector space of dimension d. The inner product of $x, y \in \mathbb{C}^d$ is denoted by $< x, y >$ and is defined by $< x, y >= \sum_{i=1}^{d} x_i \bar{y}_i$, where $\bar{y}_i$ is the complex conjugate of y_i. The norm of x is defined by $\parallel x \parallel =< x, x >^{\frac{1}{2}}$. Two vectors x and y in $\mathbb{C}^d$ are said to be orthogonal to each other if $< x, y >= 0$. Let B be a basis of the vector space $\mathbb{C}^d$. B is called an orthogonal basis if for all $x, y \in B$, $< x, y >= 0$. An orthogonal basis B is called an orthonormal basis if for all $x \in B$, $\parallel x \parallel = 1$.

Definition 3.2.1 (Mutually unbiased bases). *Let B and $B^{'}$ be orthonormal bases of the vector space $\mathbb{C}^d$. These bases are called mutually unbiased if and only if $| < b, b^{'} > | = \frac{1}{\sqrt{d}}$ for all $b \in B$ and $b^{'} \in B^{'}$.*

We recall the definitions of trace maps over Galois fields and Galois rings to describe some known constructions of MUBs that use the trace map.

Let f be the Frobenius automorphism over the Galois field $GF(p, m)$ defined as

$$f : GF(p, m) \to GF(p, m)$$
$$f(x) = x^p$$

and Tr be the trace map defined as

$$Tr : GF(p, m) \to \mathbb{Z}_p$$
$$Tr(x) = x + f(x) + f^2(x) + \ldots + f^{m-1}(x).$$

The trace map Tr satisfies the properties given in Theorem 1.4.3. The following definition of an additive character of the additive group $GF(p, m)$ plays a major role in the next few theorems.

Definition 3.2.2 (Additive character). *Let* $\omega_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ *be the complex* p^{th} *root of unity. The function* χ_1 *defined by*

$$\chi_1(x) = \omega_p^{Tr(x)}, \forall x \in GF(p,m) \tag{3.1}$$

is an additive character of the additive group of $GF(p,m)$.

For $x, y \in GF(p,m)$, from Theorem 1.4.3, we have $Tr(x+y) = Tr(x) + Tr(y)$. Therefore it is easy to see that $\chi_1(x+y) = \chi_1(x)\chi_1(y)$. All additive characters of $GF(p,m)$ can be expressed in terms of χ_1. For more details on additive characters please read chapter 4 in [52].

Theorem 3.2.3. *[Theorem 5.7, [52]]*
Let $b \in GF(p,m)$. *For all* $x \in GF(p,m)$, *the function* χ_b *defined by* $\chi_b(x) = \chi_1(bx)$ *is an additive character of* $GF(p,m)$ *and every additive character of* $GF(p,m)$ *can be obtained in this way.*

Definition 3.2.4 (Weil sums). *Let* χ *be a nontrivial additive character of* $GF(p,m)$ *and let* f *be a polynomial of degree* n *over* $GF(p,m)$. *The sum*

$$\sum_{x \in GF(p,m)} \chi(f(x)) \tag{3.2}$$

is called the Weil sum.

Theorem 3.2.5. *[Theorem 5.38, [52]]*
Let f *be a polynomial of degree* $n \geq 1$ *over* $GF(p,m)$ *with* $gcd(n, p^m) = 1$ *and let* χ *be a nontrivial additive character of* $GF(p,m)$. *Then*

$$\left| \sum_{x \in GF(p,m)} \chi(f(x)) \right| \leq (n-1)\sqrt{p^m}. \tag{3.3}$$

The following lemma is a particular result from Theorem 3.2.5 that is in [49].

Lemma 3.2.6. *[Lemma 1, [49]]*
Let $GF(p,m)$ *be a Galois field of characteristic* p *and* χ *a nontrivial additive character of* $GF(p,m)$. *If* f *is a polynomial of degree* 2 *over* $GF(p,m)$ *then*

$$\left| \sum_{x \in GF(p,m)} \chi(f(x)) \right| = \sqrt{p^m}. \tag{3.4}$$

The following construction of MUBs of odd prime power dimensions is based on the trace map over the Galois field $GF(p,m)$.

Theorem 3.2.7. *[Theorem 2, [49]]*
Let $GF(p,m)$ be the Galois field of characteristic p and Tr be the trace map over $GF(p,m)$. For $a \in GF(p,m)$, let $B_a = \{v_{a,b} | b \in GF(p,m)\}$ be the set of vectors given by $v_{a,b} = \frac{1}{\sqrt{p^m}} \left(\omega_p^{Tr(ax^2+bx)}\right)_{x \in GF(p,m)}$, where $\omega_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ is the complex p^{th} root of unity. The standard basis of $\mathbb{C}^{p^m}$ and the sets B_a form an extremal set of p^m+1 MUBs of $\mathbb{C}^{p^m}$.

Proof:
For $a, c \in GF(p,m)$ let B_a and B_c be the sets of vectors defined above. Let $v_{a,b} \in B_a$ and $v_{c,d} \in B_c$. From the definition of the inner product of two vectors we have

$$\begin{aligned}
< v_{a,b}, v_{c,d} > &= \frac{1}{p^m} \sum_{x \in GF(p,m)} \omega_p^{Tr(ax^2+bx)} \overline{\omega_p^{Tr(cx^2+dx)}} \\
&= \frac{1}{p^m} \sum_{x \in GF(p,m)} (e^{\frac{2\pi i}{p}})^{Tr(ax^2+bx)} (e^{\frac{-2\pi i}{p}})^{Tr(cx^2+dx)} \\
&= \frac{1}{p^m} \sum_{x \in GF(p,m)} (e^{\frac{2\pi i}{p}})^{Tr(ax^2+bx)} (e^{\frac{2\pi i}{p}})^{-Tr(cx^2+dx)} \\
&= \frac{1}{p^m} \sum_{x \in GF(p,m)} (e^{\frac{2\pi i}{p}})^{Tr(ax^2+bx)-Tr(cx^2+dx)} \\
&= \frac{1}{p^m} \sum_{x \in GF(p,m)} \omega_p^{Tr((a-c)x^2+(b-d)x)}.
\end{aligned}$$

Thus

$$| < v_{a,b}, v_{c,d} > | = \left| \frac{1}{p^m} \sum_{x \in GF(p,m)} \omega_p^{Tr(a-c)x^2+(b-d)x} \right|. \tag{3.5}$$

Suppose that $a = c$, i.e., both vectors belong to the same basis. If $b = d$ then $| < v_{a,b}, v_{c,d} > | = 1$ and if $b \neq d$ then from equation (2.1) in Chapter 2 and the properties of the trace map given in Theorem 1.4.3 we have $| < v_{a,b}, v_{c,d} > | = 0$. Thus B_a is an orthonormal basis of the vector space $\mathbb{C}^{p^m}$. The coefficients of the vector $v_{a,b}$ are $\frac{1}{\sqrt{p^m}}$. Thus B_a is mutually unbiased with the standard basis of $\mathbb{C}^{p^m}$. On the other hand, if $a \neq c$ then from Lemma 3.2.6 we have $| < v_{a,b}, v_{c,d} > | = \frac{1}{\sqrt{p^m}}$. Thus the bases B_a and B_c are mutually unbiased. It is also clear that there are $p^m + 1$ MUBs. □

Authors in [49] also use the trace map over the Galois ring $GR(4,m)$ to construct MUBs of even prime power dimensions as follows.

Theorem 3.2.8. *[Theorem 3, [49]]*
Let $GR(4,m)$ be the Galois ring of characteristic 4, Tr be the trace map over $GR(4,m)$ and $\mathcal{T}$ be the Teichmuller set of $GR(4,m)$. For $a \in \mathcal{T}$, let $B_a = \{v_{a,b} \mid b \in \mathcal{T}\}$ be the set of vectors given by $v_{a,b} = \frac{1}{\sqrt{2^m}} \left(\omega_4^{Tr((a+2b)x)}\right)_{x\in\mathcal{T}}$, where $\omega_4 = e^{\frac{2\pi\sqrt{-1}}{4}}$ is the complex 4^{th} root of unity. The standard basis of $\mathbb{C}^{2^m}$ and the sets B_a form an extremal set of 2^m+1 MUBs of $\mathbb{C}^{2^m}$.

The following lemma gives the lower bound for number of MUBs when the dimension is a prime factorization.

Lemma 3.2.9. *[Lemma 3, [49]]*
Let $d = p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}$ be a factorization of d into distinct primes p_i. Then $N(d) \geq min\{N(p_1^{e_1}), N(p_2^{e_2}), \dots, N(p_r^{e_r})\}$.

Proof:
We denote the minimum by $m = \min_i N(p_i^{e_i})$. Choose m mutually unbiased bases $B_1^{(i)}, B_2^{(i)}, \dots, B_m^{(i)}$ of $\mathbb{C}^{p_i^{e_i}}$, for all i in the range $1 \leq i \leq r$. Then $\{B_k^{(1)} \bigotimes B_k^{(2)} \bigotimes \dots B_k^{(r)} : k = 1,2,\dots,m\}$ is a set of m MUBs of $\mathbb{C}^d$. □

In this section the trace map over the Galois field $GF(p,m)$ and the Galois ring $GR(4,m)$ have been used to construct MUBs of odd and even prime power dimensions respectively. This is a motivation to use the weighted-trace map T_w that we have studied in Section 2.9 to construct MUBs of odd integer dimensions $d = p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}$.

3.3 MUBs via the weighted-trace map for odd integer dimensions

So far we have studied the use of trace maps over the Galois field $GF(p,m)$ and the Galois ring $GR(4,m)$ to construct MUBs of odd and even prime power dimensions respectively.

When d is not a prime power then the exact value of $N(d)$, that is the number of MUBs of dimension d, is not yet known. As mentioned in [49] the problem of determining $N(d)$ is similar to the combinatorial problem of determining the number of mutually orthogonal Latin squares $M(d)$ of size $d \times d$. In [49] it is shown that for a given $d = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, a factorisation of d into distinct primes p_i, $N(d) \geq \min\{N(p_1^{e_1}), N(p_2^{e_2}), \dots, N(p_r^{e_r})\}$. Numerical evidence seems to suggest that considerably fewer MUBs might be possible if the dimension is not a prime power. In this section we construct sets of MUBs of odd dimension d by using the weighted-trace map T_w that we studied in Section 2.9. For a given $d = q_1 q_2 \dots q_r$, where $q_1 < q_2 < \dots < q_r$ are odd prime powers, we construct the set of $q_1 + 1$ MUBs of dimension d.

Let us recall the ring that we studied in Section 2.9. Let $n = p_1 p_2 \dots p_r$ and d be an odd integer such that $d = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r} = q_1 q_2 \dots q_r$, where $q_1 < q_2 < \dots < q_r$. Consider the ring $R(d, n) = GF(p_1, e_1) \times GF(p_2, e_2) \times \dots \times GF(p_r, e_r)$, where for $j = 1, 2, \dots, r$, $GF(p_j, e_j)$ is the Galois field of characteristic p_j. If $x, y \in R(d, n)$ then $x = (x_1, x_2, \dots, x_r)$ and $y = (y_1, y_2, \dots, y_r)$, where $x_j, y_j \in GF(p_j, e_j)$ for $j = 1, 2, \dots, r$. $R(d, n)$ is a ring under the addition and multiplication of x, y defined by

$$\begin{aligned} x + y &= (x_1 + y_1, x_2 + y_2, \dots, x_r + y_r) \text{ and} \\ xy &= (x_1 y_1, x_2 y_2, \dots, x_r y_r) \text{ respectively.} \end{aligned}$$

Let Tr_j be the trace map defined over the Galois field $GF(p_j, e_j)$. The weighted-trace map over the ring $R(d, n)$ is defined by

$$\begin{aligned} T_w : R(d, n) &\to \mathbb{Z}_n \\ T_w(x) &= \textstyle\sum_{j=1}^{r} \frac{n}{p_j} Tr_j(x_j). \end{aligned}$$

In Theorem 2.9.2 we have proved that the following basic properties are satisfied by the weighted-trace map. Let $x, y \in R(d, n)$ and $a \in \mathbb{Z}_n$. Then

(i) $T_w(x + y) = T_w(x) + T_w(y)$

(ii) $T_w(ax) = aT_w(x)$

(iii) T_w is surjective.

The main construction of this section is based on the weighted-trace map. Before we state the main theorem, we state and prove the following lemma that is mentioned in [71].

Lemma 3.3.1. *Let $R(d,n)$ be the ring defined above by using the direct product of Galois fields and T_w be the weighted-trace map over $R(d,n)$. Let Tr_j be the trace map over the Galois field $GF(p_j,e_j)$. If $\omega = e^{\frac{2\pi\sqrt{-1}}{n}}$ and $\omega_j = e^{\frac{2\pi\sqrt{-1}}{p_j}}$ then*

$$\sum_{x\in R(d,n)} \omega^{T_w(x)} = \prod_{j=1}^{r} \sum_{x_j\in GF(p_j,e_j)} \omega_j^{Tr_j(x_j)}. \tag{3.6}$$

Proof:

Since $x \in R(d,n)$ we have $x = (x_1, x_2, \ldots, x_r)$, where $x_j \in GF(p_j,e_j)$ for $j = 1,2,\ldots,r$. By the definition of the weighted-trace map we have

$$\begin{aligned}\sum_{x\in R(d,n)} \omega^{T_w(x)} &= \sum_{x\in R(d,n)} \omega^{\sum_{j=1}^{r}(\frac{n}{p_j}Tr_j(x_j))} \\ &= \sum_{x\in R(d,n)} \prod_{j=1}^{r} \omega_j^{Tr_j(x_j)}.\end{aligned}$$

Collecting all the like terms on the right hand side of the above equation we get

$$\sum_{x\in R(d,n)} \omega^{T_w(x)} = \prod_{j=1}^{r} \sum_{x_j\in GF(p_j,e_j)} \omega_j^{Tr_j(x_j)}.$$

□

We can now move into the major construction of this section which is the MUBs of odd integer dimension d. We state the following theorem in order to explain this construction by using the properties of the weighted-trace map over the ring $R(d,n)$ and the result in Lemma 3.3.1.

Theorem 3.3.2. *Let d be an odd integer such that $d = p_1^{e_1}p_2^{e_2}\ldots p_r^{e_r} = q_1q_2\ldots q_r$, where $q_1 < q_2 < \ldots < q_r$, $n = p_1p_2\ldots p_r$ and $q_i = p_i^{e_i}$. Let $R(d,n) = GF(p_1,e_1) \times GF(p_2,e_2) \times \ldots \times GF(p_r,e_r)$. Let Tr_j be the trace map over the Galois field $GF(p_j,e_j)$ for $j = 1,2,\ldots,r$ and T_w be the weighted-trace map over the ring $R(d,n)$. In addition let $\omega = e^{\frac{2\pi\sqrt{-1}}{n}}$ and $\omega_j = e^{\frac{2\pi\sqrt{-1}}{p_j}}$, for $j = 1,2,\ldots,r$. For $a \in R(d,n)$, consider the set of vectors $B_a = \{v_{a,b} | b \in R(d,n)\}$, where $v_{a,b} = \frac{1}{\sqrt{d}}\left(\omega^{T_w(ax^2+bx)}\right)_{x\in R(d,n)}$. Now choose a set $\{B_{a^{(1)}}, B_{a^{(2)}}, \ldots, B_{a^{(q_1)}}\}$ such that if $a^{(t)} = \left(a_1^{(t)}, a_2^{(t)}, \ldots, a_r^{(t)}\right)$ then for $t \neq k$, $1 \leq t,k \leq q_1$ and for all $1 \leq j \leq r$ the components $a_j^{(t)} \neq a_j^{(k)}$. Then the standard basis of $\mathbb{C}^d$ and the*

set $\{B_{a^{(1)}}, B_{a^{(2)}}, \ldots, B_{a^{(q_1)}}\}$ *form a set of* $q_1 + 1$ *MUBs of dimension* d. *Further there are* $q_1! \times \begin{pmatrix} q_2 \\ q_1 \end{pmatrix} \times \begin{pmatrix} q_3 \\ q_1 \end{pmatrix} \times \ldots \times \begin{pmatrix} q_r \\ q_1 \end{pmatrix}$ *such sets of MUBs.*

Proof:

For $a, b, \alpha, \beta \in R(d,n)$, let $v_{a,b} = \frac{1}{\sqrt{d}} \left(\omega^{T_w(ax^2+bx)}\right)_{x \in R(d,n)}$ and $v_{\alpha,\beta} = \frac{1}{\sqrt{d}} \left(\omega^{T_w(\alpha x^2+\beta x)}\right)_{x \in R(d,n)}$. By using the definition of inner product of two vectors and from the properties of the weighted-trace map we have

$$| < v_{a,b}, v_{\alpha,\beta} > | \;=\; \left| \frac{1}{d} \sum_{x \in R(d,n)} \omega^{T_w((a-\alpha)x^2+(b-\beta)x)} \right|.$$

We know that $a, b, \alpha, \beta, x \in R(d,n)$ are r-tuples that can be written as $a = (a_1, a_2, \ldots, a_r)$ and similarly b, α, β, x, where $a_j \in GF(p_j, e_j)$, $1 \leq j \leq r$. Now from Lemma 3.3.1 we have

$$| < v_{a,b}, v_{\alpha,\beta} > | \;=\; \left| \frac{1}{d} \prod_{j=1}^{r} \sum_{x_j \in GF(p_j,e_j)} \omega_j^{Tr_j((a_j-\alpha_j)x_j^2+(b_j-\beta_j)x_j)} \right|.$$

Let us consider the following two cases:

Case 1: Suppose $a = \alpha$, i.e., both vectors belong to the same basis. Then for all $1 \leq j \leq r$, $a_j = \alpha_j$. Hence

$$| < v_{a,b}, v_{\alpha,\beta} > | \;=\; \left| \frac{1}{d} \prod_{j=1}^{r} \sum_{x_j \in GF(p_j,e_j)} \omega_j^{Tr_j((b_j-\beta_j)x_j)} \right|.$$

If $b = \beta$ then $b_j = \beta_j$, for all $1 \leq j \leq r$. Hence

$$\begin{aligned} | < v_{a,b}, v_{\alpha,\beta} > | &= \left| \frac{1}{d} \prod_{j=1}^{r} q_j \right| \\ &= 1. \end{aligned}$$

If $b \neq \beta$ then $b_t \neq \beta_t$ for at least one t, where $1 \leq t \leq r$, and from the properties of the trace map over Galois fields, for these t we have

$$\sum_{x_t \in GF(p_t,e_t)} \omega_t^{Tr_t((b_t-\beta_t)x_t)} \;=\; 0.$$

Thus

$$\begin{aligned} |< v_{a,b}, v_{\alpha,\beta} >| &= \left| \frac{1}{d} \prod_{j=1, j\neq t}^{r} \sum_{x_j \in GF(p_j, e_j)} \omega_j^{Tr_j((b_j-\beta_j)x_j)} \cdot 0 \right| \\ &= 0. \end{aligned}$$

From the definition of orthonormal basis, this proves that B_a is an orthonormal basis of the vector space $\mathbb{C}^d$.

Case 2: Suppose $a \neq \alpha$. Then $a_j \neq \alpha_j$ for at least one j, where $1 \leq j \leq r$. From Lemma 3.2.6, for these j we have

$$\left| \sum_{x_j \in GF(p_j, e_j)} \omega_j^{Tr_j((a_j-\alpha_j)x_j^2+(b_j-\beta_j)x_j)} \right| = \sqrt{q_j}.$$

If $a_t = \alpha_t$ for some t, where $1 \leq t \leq r$, then for these t, we have

$$\left| \sum_{x_t \in GF(p_t, e_t)} \omega_t^{Tr_t((a_t-\alpha_t)x_t^2+(b_t-\beta_t)x_t)} \right| = \begin{cases} 0 & \text{when } b_t \neq \beta_t \\ q_t & \text{when } b_t = \beta_t. \end{cases}$$

Without loss of generality we can assume $a_t = \alpha_t$ for just one t. Then

$$|< v_{a,b}, v_{\alpha,\beta} >| = \left| \frac{1}{d} \prod_{j=1, j\neq t}^{r} \sum_{x_j \in GF(p_j, e_j)} \omega_j^{Tr_j((a_j-\alpha_j)x_j^2+(b_j-\beta_j)x_j)} \right| \times (0 \text{ or } q_t).$$

i.e.,

$$|< v_{a,b}, v_{\alpha,\beta} >| = 0$$

or

$$\begin{aligned} |< v_{a,b}, v_{\alpha,\beta} >| &= \frac{1}{d} \prod_{j=1, j\neq t}^{r} \sqrt{q_j} \times q_t \\ &= \frac{1}{\prod_{j=1, j\neq t}^{r} \sqrt{q_j}} \\ &\neq \frac{1}{\sqrt{d}}. \end{aligned}$$

Therefore if $a \neq \alpha$ and for all j, $a_j \neq \alpha_j$, then

$$|< v_{a,b}, v_{\alpha,\beta} >| = \frac{1}{\sqrt{d}}.$$

Thus for B_a and B_α to be mutually unbiased, it is necessary that a and α do not have any co-ordinates in common.

In addition to this the coefficients of the vector $v_{a,b}$ have absolute value $\frac{1}{\sqrt{d}}$, hence B_a is mutually unbiased with the standard basis of $\mathbb{C}^d$.

Finally, since the first component of a can be chosen in q_1 ways, the total number of MUBs together with the standard basis cannot exceed $q_1 + 1$. Since the j^{th} co-ordinate of a can be chosen in $\begin{pmatrix} q_j \\ q_1 \end{pmatrix}$ ways, there are $q_1! \times \begin{pmatrix} q_2 \\ q_1 \end{pmatrix} \times \begin{pmatrix} q_3 \\ q_1 \end{pmatrix} \times \ldots \times \begin{pmatrix} q_r \\ q_1 \end{pmatrix}$ such sets of MUBs. □

The next couple of examples illustrate this construction.

Example 3.3.3. *Let $R(15,15) = GF(3,1) \times GF(5,1)$. Let $T_w : R(15,15) \to \mathbb{Z}_{15}$ defined by $T_w(x) = 5Tr_1(x_1) + 3Tr_2(x_2)$ be the weighted-trace map over the ring $R(15,15)$, where Tr_1 and Tr_2 are trace maps over $GF(3,1)$ and $GF(5,1)$ respectively. We shall label the elements of $GF(3,1)$ and $GF(5,1)$ as follows:*

$GF(3,1) = \{0, 1, \alpha\} = \{0, 1, 2\}$.

$GF(5,1) = \{0, 1, \beta, \beta^2, \beta^3\} = \{0, 1, 2, 3, 4\}$.

The elements of $R(15,15)$ can be written as follows.

0=(0,0)	*1=(0,1)*	*2=(0,2)*	*3=(0,3)*	*4=(0,4)*
5=(1,0)	*6=(1,1)*	*7=(1,2)*	*8=(1,3)*	*9=(1,4)*
10=(2,0)	*11=(2,1)*	*12=(2,2)*	*13=(2,3)*	*14=(2,4)*

Consider the basis $B_a = \{V_{a,b} | b \in R(15,15)\}$, where $V_{a,b} = \left(\frac{1}{\sqrt{15}}\omega_{15}^{T_w(ax^2+bx)}\right)_{x \in R(15,15)}$. Here $\omega_{15} = e^{\frac{2\pi\sqrt{-1}}{15}}$ is the complex 15^{th} root of unity. It can be calculated that if $(a - a') \in R^*$ then $S = | < V_{a,b}, V_{a',b'} > | = | \sum_{x \in R(15,2)} \omega_{15}^{T_w(a-a')x^2+(b-b')x} | = \frac{1}{\sqrt{15}}$, where R^* is the set of invertible elements of $R(15,15)$.

Followings are the such sets of MUBs:

$\{B_0, B_6, B_{12}\}, \{B_0, B_6, B_{13}\}, \{B_0, B_6, B_{14}\}$
$\{B_0, B_7, B_{11}\}, \{B_0, B_7, B_{13}\}, \{B_0, B_7, B_{14}\}$
$\{B_0, B_8, B_{11}\}, \{B_0, B_8, B_{12}\}, \{B_0, B_8, B_{14}\}$
$\{B_0, B_9, B_{11}\}, \{B_0, B_9, B_{12}\}, \{B_0, B_9, B_{13}\}$

$\{B_1, B_5, B_{12}\}, \{B_1, B_5, B_{13}\}, \{B_1, B_5, B_{14}\}$
$\{B_1, B_7, B_{10}\}, \{B_1, B_7, B_{13}\}, \{B_1, B_7, B_{14}\}$
$\{B_1, B_8, B_{10}\}, \{B_1, B_8, B_{12}\}, \{B_1, B_8, B_{14}\}$
$\{B_1, B_9, B_{10}\}, \{B_1, B_9, B_{12}\}, \{B_1, B_9, B_{13}\}$

$\{B_2, B_5, B_{11}\}, \{B_2, B_5, B_{13}\}, \{B_2, B_5, B_{14}\}$
$\{B_2, B_6, B_{10}\}, \{B_2, B_6, B_{13}\}, \{B_2, B_6, B_{14}\}$
$\{B_2, B_8, B_{10}\}, \{B_2, B_8, B_{11}\}, \{B_2, B_8, B_{14}\}$
$\{B_2, B_9, B_{10}\}, \{B_2, B_9, B_{11}\}, \{B_2, B_9, B_{13}\}$

$\{B_3, B_5, B_{11}\}, \{B_3, B_5, B_{12}\}, \{B_3, B_5, B_{14}\}$
$\{B_3, B_6, B_{10}\}, \{B_3, B_6, B_{12}\}, \{B_3, B_6, B_{14}\}$
$\{B_3, B_7, B_{10}\}, \{B_3, B_7, B_{11}\}, \{B_3, B_7, B_{14}\}$
$\{B_3, B_9, B_{10}\}, \{B_3, B_9, B_{11}\}, \{B_3, B_9, B_{12}\}$

$\{B_4, B_5, B_{11}\}, \{B_4, B_5, B_{12}\}, \{B_4, B_5, B_{13}\}$
$\{B_4, B_6, B_{10}\}, \{B_4, B_6, B_{12}\}, \{B_4, B_6, B_{13}\}$
$\{B_4, B_7, B_{10}\}, \{B_4, B_7, B_{11}\}, \{B_4, B_7, B_{13}\}$
$\{B_4, B_8, B_{10}\}, \{B_4, B_8, B_{11}\}, \{B_4, B_8, B_{12}\}.$

It is clear that $N(15) = 3 = min\,\{3, 5\}$ *and together with the standard basis of* $\mathbb{C}^{15}$ *we can select 4 MUBs of* $\mathbb{C}^{15}$*. There are 60 such sets of MUBs given by*
$q_1! \times \begin{pmatrix} q_2 \\ q_1 \end{pmatrix} = 3! \times \begin{pmatrix} 5 \\ 3 \end{pmatrix}$.

Followings are the vectors of the set of MUBs $\{B_0, B_6, B_{12}\}$*:*

$B_0 =$

$\{(1,1,1,1,1,1,1,1,1,1,1,1,1,1,1),$

$(1,1,1,\omega_{15}^{3},\omega_{15}^{3},\omega_{15}^{3},\omega_{15}^{6},\omega_{15}^{6},\omega_{15}^{6},\omega_{15}^{9},\omega_{15}^{9},\omega_{15}^{9},\omega_{15}^{12},\omega_{15}^{12},\omega_{15}^{12}),$

$(1,1,1,\omega_{15}^{6},\omega_{15}^{6},\omega_{15}^{6},\omega_{15}^{12},\omega_{15}^{12},\omega_{15}^{12},\omega_{15}^{3},\omega_{15}^{3},\omega_{15}^{3},\omega_{15}^{9},\omega_{15}^{9},\omega_{15}^{9}),$

$(1,1,1,\omega_{15}^{9},\omega_{15}^{9},\omega_{15}^{9},\omega_{15}^{3},\omega_{15}^{3},\omega_{15}^{3},\omega_{15}^{12},\omega_{15}^{12},\omega_{15}^{12},\omega_{15}^{6},\omega_{15}^{6},\omega_{15}^{6}),$

$(1,1,1,\omega_{15}^{12},\omega_{15}^{12},\omega_{15}^{12},\omega_{15}^{9},\omega_{15}^{9},\omega_{15}^{9},\omega_{15}^{6},\omega_{15}^{6},\omega_{15}^{6},\omega_{15}^{3},\omega_{15}^{3},\omega_{15}^{3}),$

$(1,\omega_{15}^{5},\omega_{15}^{10},1,\omega_{15}^{5},\omega_{15}^{10},1,\omega_{15}^{5},\omega_{15}^{10},1,\omega_{15}^{5},\omega_{15}^{10},1,\omega_{15}^{5},\omega_{15}^{10}),$

$(1,\omega_{15}^{5},\omega_{15}^{10},\omega_{15}^{3},\omega_{15}^{8},\omega_{15}^{13},\omega_{15}^{6},\omega_{15}^{11},\omega_{15},\omega_{15}^{9},\omega_{15}^{14},\omega_{15}^{4},\omega_{15}^{12},\omega_{15}^{2},\omega_{15}^{7}),$

$(1,\omega_{15}^{5},\omega_{15}^{10},\omega_{15}^{6},\omega_{15}^{11},\omega_{15}^{1},\omega_{15}^{12},\omega_{15}^{2},\omega_{15}^{7},\omega_{15}^{3},\omega_{15}^{8},\omega_{15}^{13},\omega_{15}^{9},\omega_{15}^{14},\omega_{15}^{4}),$

$(1,\omega_{15}^{5},\omega_{15}^{10},\omega_{15}^{9},\omega_{15}^{14},\omega_{15}^{4},\omega_{15}^{3},\omega_{15}^{8},\omega_{15}^{13},\omega_{15}^{12},\omega_{15}^{2},\omega_{15}^{7},\omega_{15}^{6},\omega_{15}^{11},\omega_{15}),$

$(1,\omega_{15}^{5},\omega_{15}^{10},\omega_{15}^{12},\omega_{15}^{2},\omega_{15}^{7},\omega_{15}^{9},\omega_{15}^{14},\omega_{15}^{4},\omega_{15}^{6},\omega_{15}^{11},\omega_{15},\omega_{15}^{3},\omega_{15}^{8},\omega_{15}^{13}),$

$(1,\omega_{15}^{10},\omega_{15}^{5},1,\omega_{15}^{10},\omega_{15}^{5},1,\omega_{15}^{10},\omega_{15}^{5},1,\omega_{15}^{10},\omega_{15}^{5},1,\omega_{15}^{10},\omega_{15}^{5}),$

$(1,\omega_{15}^{10},\omega_{15}^{5},\omega_{15}^{3},\omega_{15}^{13},\omega_{15}^{8},\omega_{15}^{6},\omega_{15},\omega_{15}^{11},\omega_{15}^{9},\omega_{15}^{4},\omega_{15}^{14},\omega_{15}^{12},\omega_{15}^{7},\omega_{15}^{2}),$

$(1,\omega_{15}^{10},\omega_{15}^{5},\omega_{15}^{6},\omega_{15},\omega_{15}^{11},\omega_{15}^{12},\omega_{15}^{7},\omega_{15}^{2},\omega_{15}^{3},\omega_{15}^{13},\omega_{15}^{8},\omega_{15}^{9},\omega_{15}^{4},\omega_{15}^{14}),$

$(1,\omega_{15}^{10},\omega_{15}^{5},\omega_{15}^{9},\omega_{15}^{4},\omega_{15}^{14},\omega_{15}^{3},\omega_{15}^{13},\omega_{15}^{8},\omega_{15}^{12},\omega_{15}^{7},\omega_{15}^{2},\omega_{15}^{6},\omega_{15},\omega_{15}^{11}),$

$(1,\omega_{15}^{10},\omega_{15}^{5},\omega_{15}^{12},\omega_{15}^{7},\omega_{15}^{2},\omega_{15}^{9},\omega_{15}^{4},\omega_{15}^{14},\omega_{15}^{6},\omega_{15},\omega_{15}^{11},\omega_{15}^{3},\omega_{15}^{13},\omega_{15}^{8})\}.$

$B_6 =$

$\{(1,\omega_{15}^{5},\omega_{15}^{5},\omega_{15}^{3},\omega_{15}^{8},\omega_{15}^{8},\omega_{15}^{12},\omega_{15}^{2},\omega_{15}^{2},\omega_{15}^{12},\omega_{15}^{2},\omega_{15}^{2},\omega_{15}^{3},\omega_{15}^{8},\omega_{15}^{8}),$

$(1,\omega_{15}^{5},\omega_{15}^{5},\omega_{15}^{6},\omega_{15}^{11},\omega_{15}^{11},\omega_{15}^{3},\omega_{15}^{8},\omega_{15}^{8},\omega_{15}^{6},\omega_{15}^{11},\omega_{15}^{11},1,\omega_{15}^{5},\omega_{15}^{5}),$

$(1,\omega_{15}^{5},\omega_{15}^{5},\omega_{15}^{9},\omega_{15}^{14},\omega_{15}^{14},\omega_{15}^{9},\omega_{15}^{14},\omega_{15}^{14},1,\omega_{15}^{5},\omega_{15}^{5},\omega_{15}^{12},\omega_{15}^{2},\omega_{15}^{2}),$

$(1,\omega_{15}^{5},\omega_{15}^{5},\omega_{15}^{12},\omega_{15}^{2},\omega_{15}^{2},1,\omega_{15}^{5},\omega_{15}^{5},\omega_{15}^{9},\omega_{15}^{14},\omega_{15}^{14},\omega_{15}^{9},\omega_{15}^{14},\omega_{15}^{14}),$

$(1,\omega_{15}^{5},\omega_{15}^{5},1,\omega_{15}^{5},\omega_{15}^{5},\omega_{15}^{6},\omega_{15}^{11},\omega_{15}^{11},\omega_{15}^{3},\omega_{15}^{8},\omega_{15}^{8},\omega_{15}^{6},\omega_{15}^{11},\omega_{15}^{11}),$

$(1,\omega_{15}^{10},1,\omega_{15}^{3},\omega_{15}^{13},\omega_{15}^{3},\omega_{15}^{12},\omega_{15}^{7},\omega_{15}^{12},\omega_{15}^{12},\omega_{15}^{7},\omega_{15}^{12},\omega_{15}^{3},\omega_{15}^{13},\omega_{15}^{3}),$

$(1,\omega_{15}^{10},1,\omega_{15}^{6},\omega_{15},\omega_{15}^{6},\omega_{15}^{3},\omega_{15}^{13},\omega_{15}^{3},\omega_{15}^{6},\omega_{15},\omega_{15}^{6},1,\omega_{15}^{10},1),$

$(1,\omega_{15}^{10},1,\omega_{15}^{9},\omega_{15}^{4},\omega_{15}^{9},\omega_{15}^{9},\omega_{15}^{4},\omega_{15}^{9},1,\omega_{15}^{10},1,\omega_{15}^{12},\omega_{15}^{7},\omega_{15}^{12}),$

$(1,\omega_{15}^{10},1,\omega_{15}^{12},\omega_{15}^{7},\omega_{15}^{12},1,\omega_{15}^{10},1,\omega_{15}^{9},\omega_{15}^{4},\omega_{15}^{9},\omega_{15}^{9},\omega_{15}^{4},\omega_{15}^{9}),$

$(1,\omega_{15}^{10},1,1,\omega_{15}^{10},1,\omega_{15}^{6},\omega_{15},\omega_{15}^{6},\omega_{15}^{3},\omega_{15}^{13},\omega_{15}^{3},\omega_{15}^{6},\omega_{15},\omega_{15}^{6}),$

$(1,1,\omega_{15}^{10},\omega_{15}^{3},\omega_{15}^{3},\omega_{15}^{13},\omega_{15}^{12},\omega_{15}^{12},\omega_{15}^{7},\omega_{15}^{12},\omega_{15}^{12},\omega_{15}^{7},\omega_{15}^{3},\omega_{15}^{3},\omega_{15}^{13}),$

$(1, 1, \omega_{15}^{10}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}, 1, 1, \omega_{15}^{10}),$

$(1, 1, \omega_{15}^{10}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{4}, 1, 1, \omega_{15}^{10}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{7}),$

$(1, 1, \omega_{15}^{10}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{7}, 1, 1, \omega_{15}^{10}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{4}),$

$(1, 1, \omega_{15}^{10}, 1, 1, \omega_{15}^{10}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}\}.$

$B_{12} =$

$\{(1, \omega_{15}^{10}, \omega_{15}^{10}, \omega_{15}^{6}, \omega_{15}, \omega_{15}, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{4}, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{4}, \omega_{15}^{6}, \omega_{15}, \omega_{15}),$

$(1, \omega_{15}^{10}, \omega_{15}^{10}, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{4}, 1, \omega_{15}^{10}, \omega_{15}^{10}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{13}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{13}),$

$(1, \omega_{15}^{10}, \omega_{15}^{10}, \omega_{15}^{12}, \omega_{15}^{7}, \omega_{15}^{7}, \omega_{15}^{6}, \omega_{15}, \omega_{15}, \omega_{15}^{12}, \omega_{15}^{7}, \omega_{15}^{7}, 1, \omega_{15}^{10}, \omega_{15}^{10}),$

$(1, \omega_{15}^{10}, \omega_{15}^{10}, 1, \omega_{15}^{10}, \omega_{15}^{10}, \omega_{15}^{12}, \omega_{15}^{7}, \omega_{15}^{7}, \omega_{15}^{6}, \omega_{15}, \omega_{15}, \omega_{15}^{12}, \omega_{15}^{7}, \omega_{15}^{7}),$

$(1, \omega_{15}^{10}, \omega_{15}^{10}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{13}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{13}, 1, \omega_{15}^{10}, \omega_{15}^{10}, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{4}),$

$(1, 1, \omega_{15}^{5}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}^{11}),$

$(1, 1, \omega_{15}^{5}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{14}, 1, 1, \omega_{15}^{5}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{8}),$

$(1, 1, \omega_{15}^{5}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{2}, 1, 1, \omega_{15}^{5}),$

$(1, 1, \omega_{15}^{5}, 1, 1, \omega_{15}^{5}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{2}),$

$(1, 1, \omega_{15}^{5}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{8}, 1, 1, \omega_{15}^{5}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{14}),$

$(1, \omega_{15}^{5}, 1, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}^{6}, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{9}, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}^{6}),$

$(1, \omega_{15}^{5}, 1, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{9}, 1, \omega_{15}^{5}, 1, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{3}),$

$(1, \omega_{15}^{5}, 1, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{12}, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}^{6}, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{12}, 1, \omega_{15}^{5}, 1),$

$(1, \omega_{15}^{5}, 1, 1, \omega_{15}^{5}, 1, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{12}, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}^{6}, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{12}),$

$(1, \omega_{15}^{5}, 1, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{3}, 1, \omega_{15}^{5}, 1, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{9})\}.$

Followings are the vectors of the set of MUBs $\{B_0, B_6, B_{13}\}$*:*

$B_0 =$

$\{(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1),$

$(1, 1, 1, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{12}),$

$(1, 1, 1, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{9}),$

$(1, 1, 1, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}^{6}),$

$(1, 1, 1, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{3}),$

$(1, \omega_{15}^{5}, \omega_{15}^{10}, 1, \omega_{15}^{5}, \omega_{15}^{10}, 1, \omega_{15}^{5}, \omega_{15}^{10}, 1, \omega_{15}^{5}, \omega_{15}^{10}, 1, \omega_{15}^{5}, \omega_{15}^{10}),$

$(1, \omega_{15}^{5}, \omega_{15}^{10}, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{13}, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{4}, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{7}),$

$(1, \omega_{15}^{5}, \omega_{15}^{10}, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}^{1}, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{7}, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{13}, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{4}),$

$(1, \omega_{15}^{5}, \omega_{15}^{10}, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{4}, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{13}, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{7}, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}),$

$(1, \omega_{15}^{5}, \omega_{15}^{10}, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{7}, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{4}, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{13}),$

$(1, \omega_{15}^{10}, \omega_{15}^{5}, 1, \omega_{15}^{10}, \omega_{15}^{5}, 1, \omega_{15}^{10}, \omega_{15}^{5}, 1, \omega_{15}^{10}, \omega_{15}^{5}, 1, \omega_{15}^{10}, \omega_{15}^{5}),$

$(1, \omega_{15}^{10}, \omega_{15}^{5}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{8}, \omega_{15}^{6}, \omega_{15}, \omega_{15}^{11}, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{14}, \omega_{15}^{12}, \omega_{15}^{7}, \omega_{15}^{2}),$

$(1, \omega_{15}^{10}, \omega_{15}^{5}, \omega_{15}^{6}, \omega_{15}, \omega_{15}^{11}, \omega_{15}^{12}, \omega_{15}^{7}, \omega_{15}^{2}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{8}, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{14}),$

$(1, \omega_{15}^{10}, \omega_{15}^{5}, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{14}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{8}, \omega_{15}^{12}, \omega_{15}^{7}, \omega_{15}^{2}, \omega_{15}^{6}, \omega_{15}, \omega_{15}^{11}),$

$(1, \omega_{15}^{10}, \omega_{15}^{5}, \omega_{15}^{12}, \omega_{15}^{7}, \omega_{15}^{2}, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{14}, \omega_{15}^{6}, \omega_{15}, \omega_{15}^{11}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{8})\}.$

$B_6 =$

$\{(1, \omega_{15}^{5}, \omega_{15}^{5}, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{8}, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{2}, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{2}, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{8}),$

$(1, \omega_{15}^{5}, \omega_{15}^{5}, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}^{11}, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{8}, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}^{11}, 1, \omega_{15}^{5}, \omega_{15}^{5}),$

$(1, \omega_{15}^{5}, \omega_{15}^{5}, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{14}, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{14}, 1, \omega_{15}^{5}, \omega_{15}^{5}, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{2}),$

$(1, \omega_{15}^{5}, \omega_{15}^{5}, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{2}, 1, \omega_{15}^{5}, \omega_{15}^{5}, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{14}, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{14}),$

$(1, \omega_{15}^{5}, \omega_{15}^{5}, 1, \omega_{15}^{5}, \omega_{15}^{5}, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}^{11}, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{8}, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}^{11}),$

$(1, \omega_{15}^{10}, 1, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{3}, \omega_{15}^{12}, \omega_{15}^{7}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{7}, \omega_{15}^{12}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{3}),$

$(1, \omega_{15}^{10}, 1, \omega_{15}^{6}, \omega_{15}, \omega_{15}^{6}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{3}, \omega_{15}^{6}, \omega_{15}, \omega_{15}^{6}, 1, \omega_{15}^{10}, 1),$

$(1, \omega_{15}^{10}, 1, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{9}, 1, \omega_{15}^{10}, 1, \omega_{15}^{12}, \omega_{15}^{7}, \omega_{15}^{12}),$

$(1, \omega_{15}^{10}, 1, \omega_{15}^{12}, \omega_{15}^{7}, \omega_{15}^{12}, 1, \omega_{15}^{10}, 1, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{9}),$

$(1, \omega_{15}^{10}, 1, 1, \omega_{15}^{10}, 1, \omega_{15}^{6}, \omega_{15}, \omega_{15}^{6}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{3}, \omega_{15}^{6}, \omega_{15}, \omega_{15}^{6}),$

$(1, 1, \omega_{15}^{10}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{7}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{7}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{13}),$

$(1, 1, \omega_{15}^{10}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}, 1, 1, \omega_{15}^{10}),$

$(1, 1, \omega_{15}^{10}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{4}, 1, 1, \omega_{15}^{10}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{7}),$

$(1, 1, \omega_{15}^{10}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{7}, 1, 1, \omega_{15}^{10}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{4}),$

$(1, 1, \omega_{15}^{10}, 1, 1, \omega_{15}^{10}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}\}.$

$B_{13} =$

$\{(1, \omega_{15}^{10}, \omega_{15}^{10}, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{4}, \omega_{15}^{6}, \omega_{15}, \omega_{15}, \omega_{15}^{6}, \omega_{15}, \omega_{15}, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{4}),$

$(1, \omega_{15}^{10}, \omega_{15}^{10}, \omega_{15}^{12}, \omega_{15}^{7}, \omega_{15}^{7}, \omega_{15}^{12}, \omega_{15}^{7}, \omega_{15}^{7}, 1, \omega_{15}^{10}, \omega_{15}^{10}, \omega_{15}^{6}, \omega_{15}, \omega_{15})$,

$(1, \omega_{15}^{10}, \omega_{15}^{10}, 1, \omega_{15}^{10}, \omega_{15}^{10}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{13}, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{4}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{13})$,

$(1, \omega_{15}^{10}, \omega_{15}^{10}, \omega_{15}^{3}, \omega_{15}^{13}, \omega_{15}^{13}, \omega_{15}^{9}, \omega_{15}^{4}, \omega_{15}^{4}, \omega_{15}^{3}, \omega_{15}13, \omega_{15}13, 1, \omega_{15}^{10}, \omega_{15}^{10})$,

$(1, \omega_{15}^{10}, \omega_{15}^{10}, \omega_{15}^{6}, \omega_{15}, \omega_{15}, 1, \omega_{15}^{10}, \omega_{15}^{10}, \omega_{15}^{12}, \omega_{15}^{7}, \omega_{15}^{7}, \omega_{15}^{12}, \omega_{15}^{7}, \omega_{15}^{7})$,

$(1, 1, \omega_{15}^{5}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{14})$,

$(1, 1, \omega_{15}^{5}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{2}, 1, 1, \omega_{15}^{5}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}^{11})$,

$(1, 1, \omega_{15}^{5}, 1, 1, \omega_{15}^{5}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{8})$,

$(1, 1, \omega_{15}^{5}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{9}, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{3}, \omega_{15}^{3}, \omega_{15}^{8}, 1, 1, \omega_{15}^{5})$,

$(1, 1, \omega_{15}^{5}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{11}^{8}, 1, 1, \omega_{15}^{5}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{2})$,

$(1, \omega_{15}^{5}, 1, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{9}, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}^{6}, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}^{6}, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{9})$,

$(1, \omega_{15}^{5}, 1, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{12}, 1, \omega_{15}^{5}, 1, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}^{6})$,

$(1, \omega_{15}^{5}, 1, 1, \omega_{15}^{5}, 1, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{3}, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{9}, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{3})$,

$(1, \omega_{15}^{5}, 1, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{3}, \omega_{15}^{9}, \omega_{15}^{14}, \omega_{15}^{9}, \omega_{15}^{3}, \omega_{15}^{8}, \omega_{15}^{3}, 1, \omega_{15}^{5}, 1)$,

$(1, \omega_{15}^{5}, 1, \omega_{15}^{6}, \omega_{15}^{11}, \omega_{15}^{6}, 1, \omega_{15}^{5}, 1, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{12}, \omega_{15}^{12}, \omega_{15}^{2}, \omega_{15}^{12})\}$.

Example 3.3.4. *Let $R(45,15) = GF(5,1) \times GF(3,2)$. Let $T_w : R(45,15) \to \mathbb{Z}_{15}$ defined by $T_w(x) = 3Tr_1(x_1) + 5Tr_2(x_2)$ be the weighted-trace map over the ring $R(45,15)$, where Tr_1 and Tr_2 are trace maps over $GF(5,1)$ and $GF(3,2)$ respectively. We shall label the elements of $GF(5,1)$ and $GF(3,2)$ as follows:*

$GF(5,1) = \{0, 1, \alpha, \alpha^2, \alpha^3\} = \{0, 1, 2, 3, 4\}$

$GF(3,2) = \{0, 1, \beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6, \beta^7\} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

The elements of $R(45,15)$ can be written as follows:

0=(0,0)	1=(0,1)	2=(0,2)	3=(0,3)	4=(0,4)	5=(0,5)	6=(0,6)	7=(0,7)	8=(0,8)
9=(1,0)	10=(1,1)	11=(1,2)	12=(1,3)	13=(1,4)	14=(1,5)	15=(1,6)	16=(1,7)	17=(1,8)
18=(2,0)	19=(2,1)	20=(2,2)	21=(2,3)	22=(2,4)	23=(2,5)	24=(2,6)	25=(2,7)	26=(2,8)
27=(3,0)	28=(3,1)	29=(3,2)	30=(3,3)	31=(3,4)	32=(3,5)	33=(3,6)	34=(3,7)	35=(3,8)
36=(4,0)	37=(4,1)	38=(4,2)	39=(4,3)	40=(4,4)	41=(4,5)	42=(4,6)	43=(4,7)	44=(4,8)

Now consider the basis $B_a = \{V_{a,b} | b \in R(45,15)\}$, where $V_{a,b} = \left(\frac{1}{\sqrt{45}} \omega_{15}^{T_w(ax^2+bx)}\right)_{x \in R(45,15)}$. Here $\omega_{15} = e^{\frac{2\pi\sqrt{-1}}{15}}$ is the complex 15^{th} root of unity. It can be calculated that if $(a - a') \in R^*$ then $S = | < V_{a,b}, V_{a',b'} > | = | \sum_{x \in R(45,15)} \omega_{15}^{T_w(a-a')x^2+(b-b')x} | = \frac{1}{\sqrt{45}}$, where R^* is the set of invertible elements of $R(45,15)$.

For example $\{B_0, B_{10}, B_{20}, B_{30}, B_{40}\}$, $\{B_1, B_{11}, B_{21}, B_{31}, B_{41}\}$, $\{B_2, B_{12}, B_{22}, B_{32}, B_{42}\}$,$\{B_3, B_{13}, B_{23}, B_{33}, B_{43}\}$, *etc. are the sets of MUBs of* $\mathbb{C}^{45}$. *It is clear that* $N(45) = 5 = min\ \{5, 3^2\}$ *and together with the standard basis of* $\mathbb{C}^{45}$ *we can select 6 MUBs of* $\mathbb{C}^{45}$. *There are 15120 such sets of MUBs given by*

$$q_1! \times \begin{pmatrix} q_2 \\ q_1 \end{pmatrix} = 5! \times \begin{pmatrix} 9 \\ 5 \end{pmatrix}.$$

In this chapter we used trace maps over the Galois field $GF(p, m)$ and the Galois ring $GR(4, m)$ and the weighted-trace map T_w over the ring $R(d, n) = GF(p_1, e_1) \times GF(p_2, e_2) \times \ldots \times GF(p_k, e_k)$ in the form of $Tr(ax^2 + bx)$ and $T_w(ax^2 + bx)$ to construct MUBs. In the next chapter we will use the trace map over the Galois field $GF(p, 2)$ in the form of $Tr(ax^2)$ to construct two-weight, self-orthogonal codes over $\mathbb{Z}_p$.

Chapter 4

Two-Weight, Self-Orthogonal Codes from $\mathbf{Tr(ax^2)}$

4.1 Introduction

In Chapter 2 the trace map was used in the form of $Tr(ax)$ to construct linear and non-linear codes and in Chapter 3 in the form of $Tr(ax^2+bx)$ to construct mutually unbiased bases. The only difference between the use of the trace map in the constructions of codes and mutually unbiased bases was that the argument was a different one, i.e., ax and $ax^2 + bx$. Extending the code construction to include such different arguments was a challenging problem as the task of mapping the distribution of the trace values was not an easy one. Authors in [19] study the use of the trace map over $GF(p, m)$ in the form of $Tr(a\pi(x)+bx)$ to construct linear codes over $\mathbb{Z}_p$, where $\pi(x)$ is a perfect nonlinear mapping from $GF(p, m)$ to itself. They have not studied the distribution of $Tr(a\pi(x) + bx)$ and therefore they are unable to determine the exact value of the minimum distance of the codes. However in Theorem 10 in [19], the case $\pi(x) = x^2$ is studied and the minimum distance and all weights are determined without using the distribution of $Tr(ax^2 + bx)$. In our work we study the distribution of $Tr(ax^\lambda)$, $\lambda \geq 2$ over $GF(p, 2)$, which is a special case of $Tr(a\pi(x) + bx)$ and we construction 2-dimensional codes over $\mathbb{Z}_p$. These codes satisfy the Griesmer bound which is always the best bound for low-dimensional codes. In this chapter we study $\lambda = 2$ case and Chapters 5 and 6 are devoted to study $\lambda > 2$ cases.

In this chapter and the next couple of chapters we also construct cyclic codes with the length $p^2 - 1$ and the dimension 2. In [8] the trace map over $GF(p, m)$ is used in the form of $c(x) = (Tr(x), Tr(x\theta), Tr(x\theta^2), \ldots, Tr(x\theta^{n-1}))$ to construct irreducible cyclic codes over $\mathbb{Z}_p$, where $\theta = e^{\frac{2\pi i}{n}}$. The generating function given in Section 2 in [8] is used to determine the parameters of the codes. In the case of $m = 2$ the length and the dimension of the code are $p^2 - 1$ and 2 respectively, which are the same length and dimension of our cyclic codes. In our work we use the distribution of $Tr(ax^\lambda)$ for $\lambda \geq 2$ over $GF(p, 2)$ to determine the parameters of the codes which is different to the work that has been done in [8].

In Section 4.2 we give some preliminary information of two-weight codes and self-orthogonal codes together with some known results. The distribution of $Tr(ax^2)$ over $GF(p, 2)$ is studied in Section 4.3. In Section 4.4, we find that using the argument as above we can construct two-weight, self-orthogonal codes over $\mathbb{Z}_p$.

4.2 Preliminaries

In this section we include some preliminary results that will come in handy in latter sections of this chapter.

Let p be a prime and $\mathbb{Z}_p^n$ be the vector space of all n-tuples over the finite field $\mathbb{Z}_p$. If C is a k-dimensional subspace of $\mathbb{Z}_p^n$ then C is called an $[n, k]$ linear code over $\mathbb{Z}_p$. There are two most common ways of representing a linear code. One is with a generator matrix and the other one is with a parity check matrix. A generator matrix for C is any $n \times k$ matrix G whose rows form a basis for C. There are many generator matrices for a code and for any set of k linearly independent columns of a generator matrix G, the corresponding set of co-ordinates forms an information set for C. The remaining $r = n - k$ co-ordinates are termed a redundancy set and r is called the redundancy of C. If the first k co-ordinates form an information set, the code has a unique generator matrix of the form $[I_k|A]$. Since C is a subspace of $\mathbb{Z}_p^n$, it is the kernel of some linear transformation. In particular there is an $(n - k) \times n$ matrix H, called a parity check matrix for the code C. Now C can be defined by $C = \{x \in \mathbb{Z}_p^n \mid Hx^T = 0\}$. It is clear that the rows of H are also linearly

independent. It is well known that if the generator matrix of C is $G = [I_k|A_{k\times(n-k)}]$ then the parity check matrix of C is $H = [-A^T_{(n-k)\times k}|I_{n-k}]$. Thus C is contained in the kernel of the linear transformation $f : \mathbb{Z}_p^n \to \mathbb{Z}_p^{n-k}$ defined by $f(x) = Hx^T$. As H has rank $(n-k)$ this linear transformation has kernel of dimension k, which is also the dimension of C. $Kerf = \{x \in \mathbb{Z}_p^n | f(x) = 0\}$ and $C = \{x \in \mathbb{Z}_p^n | Hx^T = 0\}$. Thus $C = Kerf$.

The generator matrix G of an $[n, k]$ code C is simply a matrix whose rows are linearly independent and span the code. The rows of the parity check matrix H are independent. Hence H is the generator matrix of some code. This is called the dual or orthogonal code of C and is denoted by $C^\perp$. $C^\perp$ is an $[n, n-k]$ code. Alternately the dual code is defined by using the inner product of vectors. The inner product of $x = (x_1, x_2, \ldots x_n)$, $y = (y_1, y_2, \ldots y_n) \in \mathbb{Z}_p^n$ is defined by $x \cdot y = \sum_{i=1}^n x_i y_i$. Then $C^\perp$ can be defined by $C^\perp = \{x \in \mathbb{Z}_p^n | x \cdot c = 0 \ \ \forall c \in C\}$.

Definition 4.2.1 (Self-orthogonal and self-dual codes). *The code C is called self-orthogonal if $C \subseteq C^\perp$ and if $C = C^\perp$ then C is called self-dual.*

Since C is an $[n, k]$ linear code, $C^\perp$ is an $[n, n-k]$ linear code. If C is a self-dual code then $k = n - k$. Thus $k = \frac{n}{2}$ and $n = 2k$, i.e. if C is a self-dual code then the length of the code C is even and the dimension k is $\frac{n}{2}$.

An important invariant of a code is the minimum distance between codewords.

Definition 4.2.2 (Hamming distance). *The Hamming distance $d_H(x, y)$ between two vectors $x, y \in \mathbb{Z}_p^n$ is defined to be the number of co-ordinates in which x and y differ.*

The minimum distance of a code C is the smallest distance between distinct codewords, and is simply denoted by d. The higher the minimum distance, the greater the number of errors that can be corrected. The Hamming weight $w_H(x)$ of a vector $x \in \mathbb{Z}_p^n$ is the number of non-zero co-ordinates in x. If $x, y \in \mathbb{Z}_p^n$ then $d_H(x, y) = w_H(x - y)$. If C is a linear code the minimum distance d is the same as the minimum weight of the non-zero codewords of C. As a result of this the minimum distance of a linear code is also known as the minimum weight of the code. If the minimum distance d of an $[n, k]$ code is known then we denote the code C as an $[n, k, d]$ code.

The following lemma is a part of Theorem 1.4.3 in [46].

Lemma 4.2.3. *[Theorem 1.4.3, [46]]*
(i) If $x \in \mathbb{Z}_2^n$ *then* $w_H(x) \equiv x \cdot x \ (mod\, 2)$.
(ii) If $x \in \mathbb{Z}_3^n$ *then* $w_H(x) \equiv x \cdot x \ (mod\, 3)$.

Proof:
(i) Let n_1 be the number of 1's in $x \in \mathbb{Z}_2^n$. Then the Hamming weight of x is $w_H(x) = n_1$. Also $x \cdot x = \sum_{i=1}^{n} x_i^2 = n_1$. Thus $w_H(x) \equiv x \cdot x \pmod 2$.
(ii) Let n_1 and n_2 be the number of 1s and 2s in $x \in \mathbb{Z}_3^n$. Then the Hamming weight of x is $w_H(x) = n_1 + n_2$. Also $x \cdot x = \sum_{i=1}^{n} x_i^2 = n_1 + n_2 2^2$. Thus $w_H(x) \equiv x \cdot x \pmod 3$. □

Note that this result does not hold for $x \in \mathbb{Z}_p^n$ when $p > 3$. The reason is that when $x \in \mathbb{Z}_p^n$ the $w_H(x) = \sum_{i=1}^{p-1} n_i$, where n_i is the number of non-zero i's in x and $x \cdot x = \sum_{i=1}^{n} x_i^2 = n_1 + n_2 2^2 + n_3 3^2 + \ldots + n_{p-1}(p-1)^2$. This does not imply that $w_H(x) \equiv x \cdot x (\bmod p)$.

The following theorem can be used to check whether a given ternary code is self-orthogonal.

Theorem 4.2.4. *[Theorem 1.4.10, [46]]*
Let C *be an* $[n, k, d]$ *code over* $\mathbb{Z}_3$. C *is self-orthogonal if and only if the weight of every non-zero codeword is divisible by* 3.

Proof:
Suppose that C is a self-orthogonal code over $\mathbb{Z}_3$. Then $C \subseteq C^{\perp}$ and therefore for all $c \in C$, $c \cdot c = 0$. Since $w_H(c) = n_1 + n_2$ and from Lemma 4.2.3 we have $w_H(c) \equiv c \cdot c \pmod 3$. Thus $w_H(c) \equiv 0 \pmod 3$ and hence $3 | w_H(c)$.

Conversely suppose that the weight of every codeword is divisible by 3. For any $x, y \in C$ we need to prove that $x \cdot y = 0$. We can view the codewords x and y as follows:
There are a co-ordinates where x is non-zero and y is zero.
There are b co-ordinates where y is non-zero and x is zero.
There are c co-ordinates where both agree and are non-zero.
There are d co-ordinates where both disagree and are non-zero.
There are e co-ordinates where both are zero.

So $w_H(x+y) = a+b+c$ and $w_H(x-y) = a+b+d$. But $x \pm y \in C$ and hence $a+b+c \equiv a+b+d \equiv 0 \mod 3$. In particular $c \equiv d \mod 3$. Therefore $x \cdot y = c+2d \equiv 0 \mod 3$. Thus $C \subseteq C^{\perp}$ and hence C is self-orthogonal. □

This result cannot be applied to check the self-orthogonality of codes over $\mathbb{Z}_p$ for $p > 3$. Therefore we state the next theorem to overcome the problem of checking the self-orthogonality of codes over $\mathbb{Z}_p$ for $p > 3$.

Theorem 4.2.5. *[Proposition 1, [76]]*
Let p be an odd prime and C be a linear code over $\mathbb{Z}_p$. Then C is self-orthogonal if and only if $c \cdot c = 0,\ \forall\ c \in C$.

Proof:
Suppose that C is self-orthogonal. i.e. $C \subseteq C^{\perp} = \{x \in \mathbb{Z}_p^n : x \cdot c = 0,\ \forall\ c \in C\}$. Then $c \cdot c = 0,\ \forall\ c \in C$. Conversely suppose that $c \cdot c = 0,\ \forall\ c \in C$. For any $c, c^{'} \in C$, since C is linear, $c + c^{'} \in C$. Then
$c \cdot c = c^{'} \cdot c^{'} = (c + c^{'}) \cdot (c + c^{'}) = 0.$
$\Rightarrow c \cdot c + 2c \cdot c^{'} + c^{'} \cdot c^{'} = 0.$
$\Rightarrow 2c \cdot c^{'} = 0.$
Since p is odd we have $c \cdot c^{'} = 0$. Thus $C \subseteq C^{\perp}$. Therefore C is a self-orthogonal code over $\mathbb{Z}_p$. □

For a detailed survey of self-orthogonal codes, reader may refer to [14, 21, 37, 38, 76] and the references therein.

The weight enumerator of C is the polynomial $W_C(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$, where A_i is the number of codewords of weight i.

Definition 4.2.6 (Two-weight code). *A code is called a two-weight code if $|\{i | i \neq 0 \text{ and } A_i \neq 0\}| = 2$.*

More information of two-weight codes can be found in [10, 13, 17, 23, 29, 40] and the references therein. We note that the codes found in this chapter could be classed as trace codes, since they are found using a trace map. See [22, 36, 41, 69, 70, 73] for details on trace codes.

We now have some of the tools required to classify the codes constructed in this chapter. In the next section we study the distribution of the trace map over $GF(p,2)$, using the argument ax^2. In Section 4.4 we construct our codes and study their properties.

4.3 The distribution of $\mathbf{Tr(ax^2)}$ over $\mathbf{GF(p,2)}$

In this section we recall the definition of the trace map over the Galois field $GF(p,m)$ and state its fundamental properties. In particular we study the distribution of the trace values when the argument is ax^2 over $GF(p,2)$.

Let $p(x)$ be a primitive polynomial of degree m over $\mathbb{Z}_p$. The Galois field of characteristic p is defined as the quotient field $GF(p,m) = \mathbb{Z}_p[x]/(p(x))$. Let ζ be a root of $p(x)$ and therefore $GF(p,m) = \mathbb{Z}_p[\zeta]$. Any element in $GF(p,m)$ can be written as a polynomial of ζ over $\mathbb{Z}_p$ and further it is well known that $GF(p,m) = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{p^m-2}\}$

Definition 4.3.1 (Trace map). *Let $GF(p,m)$ be the Galois field of characteristic p. The trace map $Tr : GF(p,m) \to \mathbb{Z}_p$ is defined by $Tr(x) = x + x^p + x^{p^2} + \ldots + x^{p^{m-1}}$.*

The following theorem lists the fundamental properties of the trace map over the Galois field $GF(p,m)$.

Theorem 4.3.2. *The trace map satisfies the following properties:*
(i) $Tr(x+y) = Tr(x) + Tr(y), \ \forall\ x, y \in GF(p,m)$.
(ii) $Tr(ax) = aTr(x), \ \forall\ a \in \mathbb{Z}_p, \ x \in GF(p,m)$.
(iii) $Tr(x^p) = Tr(x), \ \forall\ x \in GF(p,m)$.
(iv) $Tr(a) = am, \ \forall\ a \in \mathbb{Z}_p$.
(v) $Tr(x) = 0$ if and only if $x = y^p - y$ for some $y \in GF(p,m)$.
(vi) As x ranges over $GF(p,m)$, $Tr(x)$ takes each element in $\mathbb{Z}_p$ equally often i.e., p^{m-1}-times.

Detailed proof of these properties can be found in [52, 53].

In order to study the distribution of the trace values when the argument is ax^2 over $GF(p,2)$, we first need to identify the elements of $GF(p,2)$ which have trace zero.

Theorem 4.3.3. *Let Tr be the trace map over $GF(p,2)$ defined by $Tr(x) = x + x^p$. Let $\zeta^t \in GF(p,2)^* = GF(p,2) \setminus \{0\}$, where $0 \leq t \leq p^2 - 2$.*
(i) If $Tr(\zeta^t) = 0$ then $Tr(\zeta^{t(2k+1)}) = 0$, for all $k = 0, 1, \ldots, p-2$.
(ii) $Tr(\zeta^{\frac{p+1}{2}}) = 0$.
(iii) For $0 \leq t < \frac{p+1}{2}$, $Tr(\zeta^t) \neq 0$.

Proof:
(i) From the definition of the trace map if $Tr(\zeta^t) = 0$ then

$$\begin{aligned} \zeta^t + \zeta^{tp} &= 0. \\ \Rightarrow \zeta^t &= -\zeta^{tp}. \\ \Rightarrow (\zeta^t)^{2k} &= (\zeta^{tp})^{2k}. \end{aligned}$$

Therefore

$$\begin{aligned} Tr(\zeta^{t(2k+1)}) &= \zeta^{t(2k+1)} + \zeta^{tp(2k+1)} \\ &= \zeta^t \zeta^{2tk} + \zeta^{2tkp} \zeta^{tp} \\ &= \zeta^t \zeta^{2tkp} + \zeta^{2tkp} \zeta^{tp} \\ &= \zeta^{2tkp}(\zeta^t + \zeta^{tp}) \\ &= \zeta^{2tkp}(0). \end{aligned}$$

Thus if $Tr(\zeta^t) = 0$ then $Tr(\zeta^{t(2k+1)}) = 0$. From part (vi) of Theorem 4.3.2 there are $p-1$ elements in $GF(p,2)^*$ such that $Tr(x) = 0$. Hence if $Tr(\zeta^t) = 0$ then $Tr(\zeta^{t(2k+1)}) = 0$, for all $k = 0, 1, 2, \ldots, p-2$.
(ii) By using the definition of the trace map we have

$$\begin{aligned} Tr(\zeta^{\frac{p+1}{2}}) &= \zeta^{\frac{p+1}{2}} + \left(\zeta^{\frac{p+1}{2}}\right)^p \\ &= \zeta^{\frac{p+1}{2}} \left(1 + \zeta^{\left(\frac{p+1}{2}\right)p - \left(\frac{p+1}{2}\right)}\right) \\ &= \zeta^{\frac{p+1}{2}} \left(1 + \zeta^{\left(\frac{p^2+p-p-1}{2}\right)}\right) \\ &= \zeta^{\frac{p+1}{2}} \left(1 + \zeta^{\left(\frac{p^2-1}{2}\right)}\right). \end{aligned}$$

Since ζ^{p^2-1} is the only element in $GF(p,2)^*$ such that $\zeta^{p^2-1}=1$, we have $\zeta^{\left(\frac{p^2-1}{2}\right)}=-1$. Therefore $Tr(\zeta^{\frac{p+1}{2}})=0$.

(iii) Let $Tr(\zeta^t)=0$ for some t, $0\leq t<\frac{p+1}{2}$. This implies that

$$\zeta^t+\zeta^{tp}=0.$$
$$\Rightarrow \zeta^t(1+\zeta^{(p-1)t})=0.$$
$$\Rightarrow \zeta^t=0 \text{ or } \zeta^{(p-1)t}=-1.$$

Since ζ is a primitive element of $GF(p,2)^*$, $\zeta^t\neq 0$ for any t. Thus $\zeta^{(p-1)t}=-1$ and $\zeta^{(p-1)2t}=1$. Since $\zeta^{p^2-1}=1$ and therefore $(p^2-1)|(p-1)2t$, i.e., $2(p-1)t=(p^2-1)m,\ \ m\in\mathbb{Z}^+$. This implies that $t=\frac{(p+1)}{2}m$, a contradiction to the assumption. Therefore $Tr(\zeta^t)\neq 0$, for any t, $0\leq t<\frac{p+1}{2}$ and the minimum value of t such that $Tr(\zeta^t)=0$ is $t=\frac{p+1}{2}$. □

Corollary 4.3.4. *For $x\in GF(p,2)^*$, $Tr(x)=0$ if and only if $x=\zeta^{\left(\frac{p+1}{2}\right)(2k+1)}=\zeta^{(p+1)k}\zeta^{\frac{(p+1)}{2}}$, where $k=0,1,2,\ldots,p-2$.*

The base field $GF(p,1)\cong\mathbb{Z}_p$ is a subfield of the extended field $GF(p,2)$. The next lemma gives us those indices t for which $\zeta^t\in GF(p,1)^*$.

Lemma 4.3.5. *Let $\zeta^t\in GF(p,2)^*$, for some t, $0\leq t\leq p^2-2$. If $\zeta^t\in GF(p,1)^*$ then $t=(p+1)k$, where $k=0,1,2,\ldots,p-2$.*

Proof:

Let $\zeta^t\in GF(p,2)^*$, for some t, $0\leq t\leq p^2-2$. Now $GF(p,1)\cong\mathbb{Z}_p$ is a subfield of $GF(p,2)$. Hence if $\zeta^t\in GF(p,1)^*\cong\mathbb{Z}_p\setminus\{0\}$ then $Tr(\zeta^t\zeta^{\frac{p+1}{2}})=\zeta^t Tr(\zeta^{\frac{p+1}{2}})=0$, from part (ii) of Theorem 4.3.2 and part (ii) of Theorem 4.3.3.

From Corollary 4.3.4, if $x\in GF(p,2)^*$ such that $Tr(x)=0$ then $x=\zeta^{\left(\frac{p+1}{2}\right)(2k+1)}=\zeta^{(p+1)k}\zeta^{\frac{(p+1)}{2}}$. Hence $\zeta^t\zeta^{\frac{p+1}{2}}=\zeta^{(p+1)k}\zeta^{\frac{(p+1)}{2}}\Rightarrow\zeta^t=\zeta^{(p+1)k}$, since $\zeta^{\frac{(p+1)}{2}}\neq 0$. Therefore if $\zeta^t\in GF(p,1)^*$ then $t=(p+1)k$, where $k=0,1,2,\ldots,p-2.$, i.e., ζ^t is an element of the subfield when $t=(p+1)k$, where $k=0,1,2,\ldots,p-2$. □

So far we have identified the elements $\zeta^t\in GF(p,2)^*$ which have trace 0 or are in the base

field $GF(p,1)^*$. For $a \in GF(p,2)$, we are now in a position to study the distribution of $Tr(ax^2)$, when x ranges over $GF(p,2)$. A useful tool in this study is to list the elements of $GF(p,2)^*$ in a two-dimensional array based on the powers of a chosen primitive element ζ.

Let ζ be a primitive element of $GF(p,2)$. Then $GF(p,2)^* = \{1, \zeta, \zeta^2, \ldots, \zeta^{p^2-2}\}$ and $\zeta^{p^2-1} = \zeta^0 = 1$. Also $\zeta^{\left(\frac{p+1}{2}\right)(2p-3)+\left(\frac{p+1}{2}\right)} = \zeta^{\frac{2p^2-3p+2p-3+p+1}{2}} = \zeta^{\frac{2(p^2-1)}{2}} = \zeta^{p^2-1} = 1$. The elements in $GF(p,2)^*$ can now be listed by means of a $(p-1) \times (p+1)$ matrix: $\left[\zeta^{\left(\frac{p+1}{2}\right)(2k+1)+d}\right]$, where $k = 0, 1, 2, \ldots, p-2$ ranges over the rows of the matrix creating $p-1$ rows and $d = 0, 1, 2, \ldots, p$ ranges over the columns of the matrix creating $p+1$ columns. This $(p-1) \times (p+1)$ matrix is given by

$$GF(p,2)^* = \begin{bmatrix} \zeta^{\left(\frac{p+1}{2}\right)} & \ldots & \zeta^{\left(\frac{p+1}{2}\right)+d} & \ldots & \zeta^{\left(\frac{p+1}{2}\right)+\left(\frac{p+1}{2}\right)} & \ldots & \zeta^{\left(\frac{p+1}{2}\right)+p} \\ \zeta^{\left(\frac{p+1}{2}\right)3} & \ldots & \zeta^{\left(\frac{p+1}{2}\right)3+d} & \ldots & \zeta^{\left(\frac{p+1}{2}\right)3+\left(\frac{p+1}{2}\right)} & \ldots & \zeta^{\left(\frac{p+1}{2}\right)3+p} \\ \vdots & \ldots & \vdots & \ldots & \vdots & \ldots & \vdots \\ \zeta^{\left(\frac{p+1}{2}\right)(2k+1)} & \ldots & \zeta^{\left(\frac{p+1}{2}\right)(2k+1)+d} & \ldots & \zeta^{\left(\frac{p+1}{2}\right)(2k+1)+\left(\frac{p+1}{2}\right)} & \ldots & \zeta^{\left(\frac{p+1}{2}\right)(2k+1)+p} \\ \vdots & \ldots & \vdots & \ldots & \vdots & \ldots & \vdots \\ \zeta^{\left(\frac{p+1}{2}\right)(2p-3)} & \ldots & \zeta^{\left(\frac{p+1}{2}\right)(2p-3)+d} & \ldots & \zeta^{p^2-1}=1 & \ldots & \zeta^{\left(\frac{p+1}{2}\right)(2p-3)+p} \end{bmatrix}_{(p-1)\times(p+1)}.$$

This arrangement of the elements of $GF(p,2)^*$ enables us to better understand the distribution of the values of the trace map. For ease of reading let a_k, where $k = 0, 1, 2, \ldots, p-2$, be a listing of the non-zero elements of the base field $GF(p,1)^*$.

Lemma 4.3.6. *The trace of elements of $GF(p,2)^*$ is distributed in the following manner:*
(i) The trace of each element in the first column of the matrix representation of $GF(p,2)^*$ is zero.
(ii) The trace of elements in every other column of the matrix representation of $GF(p,2)^*$ takes every element in $\mathbb{Z}_p \setminus \{0\}$ once only.

Proof:
(i) From Corollary 4.3.4, we know that $Tr(x) = 0$ if and only if $x = \zeta^{(\frac{p+1}{2})(2k+1)}$, where $k = 0, 1, 2, \ldots, p-2$. Therefore it is clear that the trace of the elements in the first column of the matrix representation of $GF(p,2)^*$ is zero, i.e., $Tr\left(\zeta^{\left(\frac{p+1}{2}\right)(2k+1)}\right) = 0, \forall\ k = 0, 1, 2, \ldots, p-2$.
(ii) The trace of elements in the d^{th} column ($d \neq 0$) of the matrix representation of

$GF(p,2)^*$ is given by

$$Tr(\zeta^{\left(\frac{p+1}{2}\right)(2k+1)+d}) \;=\; Tr(\zeta^{(p+1)k}\zeta^{\frac{p+1}{2}}\zeta^{d}).$$

From Lemma 4.3.5 we know that $\zeta^{(p+1)k} \in GF(p,1)^*$, where $k = 0, 1, 2, \ldots, p-2$. By using the notation $a_k = \zeta^{(p+1)k}$ we have

$$Tr(\zeta^{\left(\frac{p+1}{2}\right)(2k+1)+d}) \;=\; Tr(a_k\zeta^{\frac{p+2d+1}{2}}) \text{ (from Lemma 4.3.5).}$$

From part (ii) of Theorem 4.3.2 we have

$$Tr(\zeta^{\left(\frac{p+1}{2}\right)(2k+1)+d}) \;=\; a_k Tr(\zeta^{\frac{p+2d+1}{2}}).$$

From Corollary 4.3.4 again we know that for $x \in GF(p,2)^*$, $Tr(x) = 0$ if and only if $x = \zeta^{\left(\frac{p+1}{2}\right)(2k+1)}$, where $k = 0, 1, 2 \ldots, p-2$ and therefore $Tr(\zeta^{\frac{p+2d+1}{2}}) \neq 0$, for all $d = 1, 2 \ldots, p$. In addition a_k represents every element in $\mathbb{Z}_p \setminus \{0\}$ for $k = 0, 1, 2 \ldots, p-2$. Consequently the trace of the elements in the d^{th} column of the matrix representation of $GF(p,2)^*$ takes each element in $\mathbb{Z}_p \setminus \{0\}$ exactly once. □

The next example illustrates this result.

Example 4.3.7. *Consider the primitive polynomial $p(x) = x^2 + x + 2$ over $\mathbb{Z}_5$. The elements in $GF(5,2)^* = \{1, \zeta, \zeta^2, \ldots, \zeta^{23}\}$ and their trace values are given in the following table:*

Element x	$x = a_1\zeta + a_0$	$Tr(x)$	*Element* x	$x = a_1\zeta + a_0$	$Tr(x)$
1	$0\zeta + 1$	2	ζ^{12}	$0\zeta + 4$	3
ζ	$1\zeta + 0$	4	ζ^{13}	$4\zeta + 0$	1
ζ^2	$4\zeta + 3$	2	ζ^{14}	$1\zeta + 2$	3
ζ^3	$4\zeta + 2$	0	ζ^{15}	$1\zeta + 3$	0
ζ^4	$3\zeta + 2$	1	ζ^{16}	$2\zeta + 3$	4
ζ^5	$4\zeta + 4$	4	ζ^{17}	$1\zeta + 1$	1
ζ^6	$0\zeta + 2$	4	ζ^{18}	$0\zeta + 3$	1
ζ^7	$2\zeta + 0$	3	ζ^{19}	$3\zeta + 0$	2
ζ^8	$3\zeta + 1$	4	ζ^{20}	$2\zeta + 4$	1
ζ^9	$3\zeta + 4$	0	ζ^{21}	$2\zeta + 1$	0
ζ^{10}	$1\zeta + 4$	2	ζ^{22}	$4\zeta + 1$	3
ζ^{11}	$3\zeta + 3$	3	ζ^{23}	$2\zeta + 2$	2

The matrix representation of $GF(5,2)^*$ *is then:*

$$GF(5,2)^* = \begin{bmatrix} \zeta^3 & \zeta^4 & \zeta^5 & \zeta^6 & \zeta^7 & \zeta^8 \\ \zeta^9 & \zeta^{10} & \zeta^{11} & \zeta^{12} & \zeta^{13} & \zeta^{14} \\ \zeta^{15} & \zeta^{16} & \zeta^{17} & \zeta^{18} & \zeta^{19} & \zeta^{20} \\ \zeta^{21} & \zeta^{22} & \zeta^{23} & \zeta^{24} = 1 & \zeta^{25} = \zeta & \zeta^{26} = \zeta^2 \end{bmatrix}_{4\times 6}$$

and the corresponding trace matrix is:

$$Tr(GF(5,2)^*) = \begin{bmatrix} 0 & 1 & 4 & 4 & 3 & 4 \\ 0 & 2 & 3 & 3 & 1 & 3 \\ 0 & 4 & 1 & 1 & 2 & 1 \\ 0 & 3 & 2 & 2 & 4 & 2 \end{bmatrix}_{4\times 6}.$$

It is clear that the first column is an all zero column and all the other columns contain each element in $\mathbb{Z}_5 \setminus \{0\}$ *exactly once.*

We can now examine the trace distribution for the specific case considered in this chapter: $Tr(ax^2)$.

Theorem 4.3.8. *Let Tr be the trace map over $GF(p,2)$. As x ranges over $GF(p,2)^*$ and for $a \in GF(p,2)^*$, $Tr(ax^2)$ takes each element in $\mathbb{Z}_p \setminus \{0\}$ equally often either $p+1$ times or $p-1$ times.*

Proof:

Let $a \in GF(p,2)^*$ be an even (respectively odd) power of ζ and consider the set $\{Tr(ax^2) \mid x \in GF(p,2)^*\}$. This set can be written as two copies of the trace of the elements in the set $\{\zeta^{2h} \mid h = 0,1,2\ldots,\frac{p^2-3}{2}\}$ (respectively $\{\zeta^{2h+1} \mid h = 0,1,2\ldots,\frac{p^2-3}{2}\}$) or its cyclic shifts.

In the matrix representation of $GF(p,2)^*$ that we have studied in Lemma 4.3.6, we note that there are $\frac{p+1}{2}$ columns with odd powers of ζ and $\frac{p+1}{2}$ columns with even powers of ζ. (See example 4.3.7). We will label these columns as odd and even respectively. We call the matrix obtained by taking the trace of each element in the matrix representation of $GF(p,2)^*$ as the trace matrix of $GF(p,2)^*$. We consider the two cases, $p \equiv 1(\text{mod } 4)$ and $p \equiv 3(\text{mod } 4)$ respectively.

Case I. $p \equiv 1(\text{mod } 4)$:

In this case $\frac{p+1}{2}$ is odd. From Theorem 4.3.3 we know that $Tr(\zeta^{(\frac{p+1}{2})(2k+1)}) = 0$, for all $k = 0,1,2\ldots,p-2$. Hence the first odd column (which is the first column of the matrix representation of $GF(p,2)^*$) has trace zero. Therefore there are $\frac{p+1}{2} - 1 = \frac{p-1}{2}$ odd columns of the matrix representation of $GF(p,2)^*$ with non-zero trace. From Lemma 4.3.6, the trace of elements of each of these $\frac{p-1}{2}$ odd columns contain each element in $\mathbb{Z}_p \setminus \{0\}$ exactly once. Thus the trace of all the odd powers of ζ gives us each element in $\mathbb{Z}_p \setminus \{0\}$, $\frac{p-1}{2}$ times, and so the trace of all the even powers of ζ gives us each element in $\mathbb{Z}_p \setminus \{0\}$, $\frac{p+1}{2}$ times.

Thus if $a \in GF(p,2)^*$ is an odd power of ζ then, as x ranges over $GF(p,2)^*$, $Tr(ax^2)$ takes each element in $\mathbb{Z}_p \setminus \{0\}$ equally often $p-1$ times. If $a \in GF(p,2)^*$ is an even power of ζ then $Tr(ax^2)$ takes each element in $\mathbb{Z}_p \setminus \{0\}$ equally often $p+1$ times.

Case II. $p \equiv 3(\text{mod } 4)$:

Here $\frac{p+1}{2}$ is even. As in case I, $Tr(\zeta^{(\frac{p+1}{2})(2k+1)}) = 0$, for all $k = 0,1,2\ldots,p-2$ and the first even column of the matrix representation of $GF(p,2)^*$ has trace zero. Therefore there are other $\frac{p+1}{2} - 1 = \frac{p-1}{2}$ even columns in the matrix representation of $GF(p,2)^*$

with non-zero trace. Hence the trace of all the even powers of ζ gives us each element in $\mathbb{Z}_p \setminus \{0\}$, $\frac{p-1}{2}$ times. Consequently the trace of all the odd powers of ζ gives each element in $\mathbb{Z}_p \setminus \{0\}$, $\frac{p+1}{2}$ times.

Hence when $a \in GF(p,2)^*$ is an even power of ζ then, as x ranges over $GF(p,2)^*$, $Tr(ax^2)$ takes each element in $\mathbb{Z}_p \setminus \{0\}$ equally often $p-1$ times. If $a \in GF(p,2)^*$ is an odd power of ζ then as x ranges over $GF(p,2)^*$, $Tr(ax^2)$ takes each element in $\mathbb{Z}_p \setminus \{0\}$ equally often $p+1$ times. □

Examples 4.4.2 and 4.4.3 illustrate this result.

We now have enough information to apply the trace map over $GF(p,2)$ in the form of $Tr(ax^2)$ to construct two-weight, self-orthogonal codes.

4.4 Construction of two-weight, self-orthogonal codes

So far we have studied the distribution of $Tr(ax^2)$ by changing x over the Galois field $G(p,2)$. In this section we apply this result to construct cyclic, two-dimensional, two-weight, self-orthogonal codes over $\mathbb{Z}_p$. For more details of two-weight codes, the reader is referred to [17, 29, 40] and the references therein.

Theorem 4.4.1. *Let $GF(p,2)$ be the Galois field of characteristic $p \geq 3$ and Tr be the trace map over $GF(p,2)$. Consider the matrix $H_2 = [Tr(ax^2)]_{a,x \in GF(p,2)}$.*
(i) H_2 is a linear code over $\mathbb{Z}_p$ with the parameters $[n,k,d_H] = [p^2, 2, (p-1)^2]$, where d_H is the minimum Hamming distance.
(ii) H_2 is a two-weight code with Hamming weights p^2-1 and $(p-1)^2$.
(iii) The code obtained by deleting the first column of H_2, denoted by H_2^*, is a $[p^2-1, 2, (p-1)^2]$ code and the codewords of H_2^* are the left-cyclic shifts of the first two non-zero codewords of H_2^*.
(iv) For $p > 3$, H_2 is a self-orthogonal code.

Proof:
(i) Let ζ be a primitive element of $GF(p,2)$ and c_i be any element in $GF(p,2)$. Consider the matrix

$$G_{H_2}=\begin{bmatrix} Tr(c_i^2), & i=1,2,\ldots,p^2 \\ Tr(\zeta c_i^2), & i=1,2,\ldots,p^2 \end{bmatrix}_{2\times p^2}.$$

First we will show that the two rows of G_{H_2} are linearly independent. Let $\underline{x}=(Tr(c_i^2); i=1,2,\ldots,p^2)$ and $\underline{y}=(Tr(\zeta c_i^2); i=1,2,\ldots,p^2)$. For any $a_0,a_1\in\mathbb{Z}_p$ suppose that $a_0\underline{x}+a_1\underline{y}=\underline{0}$. i.e., for all $i=1,2,\ldots,p^2$, $a_0Tr(c_i^2)+a_1Tr(\zeta c_i^2)=0$. From the properties of the trace map, for all $i=1,2,\ldots,p^2$, $Tr((a_0+a_1\zeta)c_i^2)=0$. According to the distribution of the values of trace, $Tr((a_0+a_1\zeta)c_i^2)=0$ implies that $(a_0+a_1\zeta)c_i^2=0$, for all $i=1,2,\ldots,p^2$. However $c_i^2\neq 0$, for some i and hence $a_0+a_1\zeta=0$. Since 1 and ζ represent linearly independent 2-tuples over $\mathbb{Z}_p$, a_0 and a_1 should be 0. Therefore the two rows in G_{H_2} are linearly independent.

Next consider all linear combinations of the two rows in G_{H_2}. This gives us $a_0Tr(c_i^2)+a_1Tr(\zeta c_i^2)=Tr((a_0+a_1\zeta)c_i^2),\ \ i=1,2,\ldots,p^2$, which implies that the rows of the matrix H_2 are generated by the rows in G_{H_2}. Thus G_{H_2} is a generator matrix of H_2, the length n and the dimension k of the code H_2 are p^2 and 2 respectively, and hence H_2 is a linear code over $\mathbb{Z}_p$.

From Theorem 4.3.8 every non-zero row of H contains every non-zero element of $\mathbb{Z}_p$ equally often either $p+1$ times or $p-1$ times. Since there are $p-1$ non-zero elements in $\mathbb{Z}_p$, the minimum Hamming weight of H_2 is $(p-1)^2$. Therefore $H_2=[Tr(ax^2)]_{a,x\in GF(p,2)}$ is a linear code over $\mathbb{Z}_p$ with the parameters $[n,k,d_H]=[p^2,2,(p-1)^2]$.

(ii) Since every non-zero codeword of H_2 contains each element in $\mathbb{Z}_p\setminus\{0\}$ equally often either $p+1$ times or $p-1$ times, the codewords have Hamming weight either p^2-1 or $(p-1)^2$ and hence H_2 is a two-weight code over $\mathbb{Z}_p$.

(iii) Let H_2^* be obtained by deleting the first column of H_2:

$$H_2^*=\begin{bmatrix} Tr(0) & Tr(0) & \ldots & Tr(0) & Tr(0) & Tr(0) & \ldots & Tr(0) \\ Tr(1) & Tr(\zeta^2) & \ldots & Tr(\zeta^{2\frac{(p^2-3)}{2}}) & Tr(1) & Tr(\zeta^2) & \ldots & Tr(\zeta^{2\frac{(p^2-3)}{2}}) \\ Tr(\zeta) & Tr(\zeta^3) & \ldots & Tr(\zeta\zeta^{2\frac{(p^2-3)}{2}}) & Tr(\zeta) & Tr(\zeta^3) & \ldots & Tr(\zeta\zeta^{2\frac{(p^2-3)}{2}}) \\ Tr(\zeta^2) & Tr(\zeta^4) & \ldots & Tr(\zeta^2\zeta^{2\frac{(p^2-3)}{2}}) & Tr(\zeta^2) & Tr(\zeta^4) & \ldots & Tr(\zeta^2\zeta^{2\frac{(p^2-3)}{2}}) \\ Tr(\zeta^3) & Tr(\zeta^5) & \ldots & Tr(\zeta^3\zeta^{2\frac{(p^2-3)}{2}}) & Tr(\zeta^3) & Tr(\zeta^5) & \ldots & Tr(\zeta^3\zeta^{2\frac{(p^2-3)}{2}}) \\ \vdots & \vdots & \ldots & \vdots & \vdots & \vdots & \ldots & \vdots \\ Tr(\zeta^{p^2-2}) & Tr(\zeta^{p^2}) & \ldots & Tr(\zeta^{p^2-2}\zeta^{2\frac{(p^2-3)}{2}}) & Tr(\zeta^{p^2-2}) & Tr(\zeta^{p^2}) & \ldots & Tr(\zeta^{p^2-2}\zeta^{2\frac{(p^2-3)}{2}}) \end{bmatrix}_{p^2\times(p^2-1)}.$$

The first two non-initial rows generate this code and the next consecutive two rows are the left-cyclic shift by one element of the first two non-initial rows, and so on. The

parameters of H_2^* are $[p^2-1, 2, (p-1)^2]$. Indeed H_2^* is a cyclic code.

(iv) Let S be the dot product of every non-zero codeword of H_2 with itself. Again from Theorem 4.3.8 it is clear that every non-zero codeword of H_2^* contains each element in $\mathbb{Z}_p \setminus \{0\}$ equally often either $p+1$ times or $p-1$ times. Therefore either

$$\begin{aligned} S &= (p+1)\sum_{i=1}^{p-1} i^2 \\ &= \frac{p}{6}(p+1)(2p^2-3p+1) \end{aligned}$$

or

$$\begin{aligned} S &= (p-1)\sum_{i=1}^{p-1} i^2 \\ &= \frac{p}{6}(p-1)(2p^2-3p+1). \end{aligned}$$

If $p > 3$ we have $S \equiv 0 \bmod p$. From Theorem 4.2.5 we know that, for $p > 3$, a linear code is self-orthogonal if and only if the dot product of every codeword of the code with itself is zero. Therefore H_2 is a self-orthogonal code over $\mathbb{Z}_p$ for $p > 3$. □

The following two examples illustrate Theorem 4.3.8 and 4.4.1.

Example 4.4.2. *Consider the primitive polynomial $p(x) = x^2 + x + 2$ over $\mathbb{Z}_3$ and let ζ be a root of $p(x)$. The elements of $GF(3,2) = \mathbb{Z}_3[x]/(p(x)) = \mathbb{Z}_3[\zeta]$ can be written as $\{0, 1, \zeta, \zeta^2, \ldots, \zeta^7\}$. The following table provides the trace value of these elements and their squares.*

Element x	$x = a_1\zeta + a_0$	$Tr(x)$	x^2	$Tr(x^2)$
0	$0\zeta + 0$	0	0	0
1	$0\zeta + 1$	2	1	2
ζ	$1\zeta + 0$	2	ζ^2	0
ζ^2	$2\zeta + 1$	0	ζ^4	1
ζ^3	$2\zeta + 2$	2	ζ^6	0
ζ^4	$0\zeta + 2$	1	1	2
ζ^5	$2\zeta + 0$	1	ζ^2	0
ζ^6	$1\zeta + 2$	0	ζ^4	1
ζ^7	$1\zeta + 1$	1	ζ^6	0

Taking $a, x \in GF(3,2) = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^7\}$, *the* 9×9 *matrix* $A_2 = [(ax^2)]_{a,x \in GF(3,2)}$ *is given by*

$$A_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \zeta^0 & \zeta^2 & \zeta^4 & \zeta^6 & \zeta^0 & \zeta^2 & \zeta^4 & \zeta^6 \\ 0 & \zeta^1 & \zeta^3 & \zeta^5 & \zeta^7 & \zeta^1 & \zeta^3 & \zeta^5 & \zeta^7 \\ 0 & \zeta^2 & \zeta^4 & \zeta^6 & \zeta^0 & \zeta^2 & \zeta^4 & \zeta^6 & \zeta^0 \\ 0 & \zeta^3 & \zeta^5 & \zeta^7 & \zeta^1 & \zeta^3 & \zeta^5 & \zeta^7 & \zeta^1 \\ 0 & \zeta^4 & \zeta^6 & \zeta^0 & \zeta^2 & \zeta^4 & \zeta^6 & \zeta^0 & \zeta^2 \\ 0 & \zeta^5 & \zeta^7 & \zeta^1 & \zeta^3 & \zeta^5 & \zeta^7 & \zeta^1 & \zeta^3 \\ 0 & \zeta^6 & \zeta^0 & \zeta^2 & \zeta^4 & \zeta^6 & \zeta^0 & \zeta^2 & \zeta^4 \\ 0 & \zeta^7 & \zeta^1 & \zeta^3 & \zeta^5 & \zeta^7 & \zeta^1 & \zeta^3 & \zeta^5 \end{bmatrix}_{9 \times 9}$$

and the matrix $H_2 = [Tr(ax^2)]_{a,x \in GF(3,2)}$ *is given by*

$$H_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 2 & 0 & 1 & 0 \\ 0 & 2 & 2 & 1 & 1 & 2 & 2 & 1 & 1 \\ 0 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 2 \\ 0 & 2 & 1 & 1 & 2 & 2 & 1 & 1 & 2 \\ 0 & 1 & 0 & 2 & 0 & 1 & 0 & 2 & 0 \\ 0 & 1 & 1 & 2 & 2 & 1 & 1 & 2 & 2 \\ 0 & 0 & 2 & 0 & 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 2 & 2 & 1 & 1 & 2 & 2 & 1 \end{bmatrix}_{9 \times 9}.$$

A generator matrix for H_2 *is*

$$G_{H_2} = \begin{bmatrix} 0 & 2 & 0 & 1 & 0 & 2 & 0 & 1 & 0 \\ 0 & 2 & 2 & 1 & 1 & 2 & 2 & 1 & 1 \end{bmatrix}_{2 \times 9}.$$

By deleting the first column of H_2 *we obtain*

$$H_2^* = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 1 & 0 & 2 & 0 & 1 & 0 \\ 2 & 2 & 1 & 1 & 2 & 2 & 1 & 1 \\ 0 & 1 & 0 & 2 & 0 & 1 & 0 & 2 \\ 2 & 1 & 1 & 2 & 2 & 1 & 1 & 2 \\ 1 & 0 & 2 & 0 & 1 & 0 & 2 & 0 \\ 1 & 1 & 2 & 2 & 1 & 1 & 2 & 2 \\ 0 & 2 & 0 & 1 & 0 & 2 & 0 & 1 \\ 1 & 2 & 2 & 1 & 1 & 2 & 2 & 1 \end{bmatrix}_{9\times 8}.$$

H_2 is a linear code over $\mathbb{Z}_3$ with the parameters $[9, 2, 4]$. The Hamming weight of each non-zero codeword is either 4 or 8. Thus H_2 is a two-weight code. The punctured code H_2^*, obtained by deleting the first column of H_2 is an $[8, 2, 4]$ code over $\mathbb{Z}_3$ and codewords of H_2^* are the left-cyclic shifts of elements of the first two non-zero codewords of H_2^*. Indeed H_2^* is a cyclic code. The weight of each non-zero codeword is not divisible by 3 and from Theorem 4.2.4, H_2 is not a self-orthogonal code.

Example 4.4.3. *Consider the primitive polynomial $p(x) = x^2 + x + 2$ over $\mathbb{Z}_5$ and let ζ be a root of $p(x)$. Thus $\zeta^2 = 4\zeta + 3$ and the elements of $GF(5, 2) = \mathbb{Z}_5[x]/(p(x)) = \mathbb{Z}_5[\zeta]$ can be written as $\{0, 1, \zeta, \zeta^2, \ldots, \zeta^{23}\}$. The following table provides the trace value of these elements and their squares.*

Element x	$x = a_1\zeta + a_0$	$Tr(x)$	x^2	$Tr(x^2)$
0	$0\zeta + 0$	0	0	0
1	$0\zeta + 1$	2	1	2
ζ	$1\zeta + 0$	4	ζ^2	2
ζ^2	$4\zeta + 3$	2	ζ^4	1
ζ^3	$4\zeta + 2$	0	ζ^6	4
ζ^4	$3\zeta + 2$	1	ζ^8	4
ζ^5	$4\zeta + 4$	4	ζ^{10}	2
ζ^6	$0\zeta + 2$	4	ζ^{12}	3
ζ^7	$2\zeta + 0$	3	ζ^{14}	3
ζ^8	$3\zeta + 1$	4	ζ^{16}	4
ζ^9	$3\zeta + 4$	0	ζ^{18}	1
ζ^{10}	$1\zeta + 4$	2	ζ^{20}	1
ζ^{11}	$3\zeta + 3$	3	ζ^{22}	3
ζ^{12}	$0\zeta + 4$	3	1	2
ζ^{13}	$4\zeta + 0$	1	ζ^2	2
ζ^{14}	$1\zeta + 2$	3	ζ^4	1
ζ^{15}	$1\zeta + 3$	0	ζ^6	4
ζ^{16}	$2\zeta + 3$	4	ζ^8	4
ζ^{17}	$1\zeta + 1$	1	ζ^{10}	2
ζ^{18}	$0\zeta + 3$	1	ζ^{12}	3
ζ^{19}	$3\zeta + 0$	2	ζ^{14}	3
ζ^{20}	$2\zeta + 4$	1	ζ^{16}	4
ζ^{21}	$2\zeta + 1$	0	ζ^{18}	1
ζ^{22}	$4\zeta + 1$	3	ζ^{20}	1
ζ^{23}	$2\zeta + 2$	2	ζ^{22}	3

By selecting $a, x \in GF(5,2) = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{23}\}$, *the matrix* $A_2 = [(ax^2)]_{a,x \in GF(5,2)}$ *is given by*

$$A_2 = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & \zeta^{0} & \zeta^{2} & \zeta^{4} & \zeta^{6} & \zeta^{8} & \zeta^{10} & \zeta^{12} & \zeta^{14} & \zeta^{16} & \zeta^{18} & \zeta^{20} & \zeta^{22} & \zeta^{0} & \zeta^{2} & \zeta^{4} & \zeta^{6} & \zeta^{8} & \zeta^{10} & \dots & \zeta^{22} \\
0 & \zeta^{1} & \zeta^{3} & \zeta^{5} & \zeta^{7} & \zeta^{9} & \zeta^{11} & \zeta^{13} & \zeta^{15} & \zeta^{17} & \zeta^{19} & \zeta^{21} & \zeta^{23} & \zeta^{1} & \zeta^{3} & \zeta^{5} & \zeta^{7} & \zeta^{9} & \zeta^{11} & \dots & \zeta^{23} \\
0 & \zeta^{2} & \zeta^{4} & \zeta^{6} & \zeta^{8} & \zeta^{10} & \zeta^{12} & \zeta^{14} & \zeta^{16} & \zeta^{18} & \zeta^{20} & \zeta^{22} & \zeta^{0} & \zeta^{2} & \zeta^{4} & \zeta^{6} & \zeta^{8} & \zeta^{10} & \zeta^{12} & \dots & \zeta^{0} \\
0 & \zeta^{3} & \zeta^{5} & \zeta^{7} & \zeta^{9} & \zeta^{11} & \zeta^{13} & \zeta^{15} & \zeta^{17} & \zeta^{19} & \zeta^{21} & \zeta^{23} & \zeta^{1} & \zeta^{3} & \zeta^{5} & \zeta^{7} & \zeta^{9} & \zeta^{11} & \zeta^{13} & \dots & \zeta^{1} \\
0 & \zeta^{4} & \zeta^{6} & \zeta^{8} & \zeta^{10} & \zeta^{12} & \zeta^{14} & \zeta^{16} & \zeta^{18} & \zeta^{20} & \zeta^{22} & \zeta^{0} & \zeta^{2} & \zeta^{4} & \zeta^{6} & \zeta^{8} & \zeta^{10} & \zeta^{12} & \zeta^{14} & \dots & \zeta^{2} \\
0 & \zeta^{5} & \zeta^{7} & \zeta^{9} & \zeta^{11} & \zeta^{13} & \zeta^{15} & \zeta^{17} & \zeta^{19} & \zeta^{21} & \zeta^{23} & \zeta^{1} & \zeta^{3} & \zeta^{5} & \zeta^{7} & \zeta^{9} & \zeta^{11} & \zeta^{13} & \zeta^{15} & \dots & \zeta^{3} \\
0 & \zeta^{6} & \zeta^{8} & \zeta^{10} & \zeta^{12} & \zeta^{14} & \zeta^{16} & \zeta^{18} & \zeta^{20} & \zeta^{22} & \zeta^{0} & \zeta^{2} & \zeta^{4} & \zeta^{6} & \zeta^{8} & \zeta^{10} & \zeta^{12} & \zeta^{14} & \zeta^{16} & \dots & \zeta^{4} \\
0 & \zeta^{7} & \zeta^{9} & \zeta^{11} & \zeta^{13} & \zeta^{15} & \zeta^{17} & \zeta^{19} & \zeta^{21} & \zeta^{23} & \zeta^{1} & \zeta^{3} & \zeta^{5} & \zeta^{7} & \zeta^{9} & \zeta^{11} & \zeta^{13} & \zeta^{15} & \zeta^{17} & \dots & \zeta^{5} \\
0 & \zeta^{8} & \zeta^{10} & \zeta^{12} & \zeta^{14} & \zeta^{16} & \zeta^{18} & \zeta^{20} & \zeta^{22} & \zeta^{0} & \zeta^{2} & \zeta^{4} & \zeta^{6} & \zeta^{8} & \zeta^{10} & \zeta^{12} & \zeta^{14} & \zeta^{16} & \zeta^{18} & \dots & \zeta^{6} \\
0 & \zeta^{9} & \zeta^{11} & \zeta^{13} & \zeta^{15} & \zeta^{17} & \zeta^{19} & \zeta^{21} & \zeta^{23} & \zeta^{1} & \zeta^{3} & \zeta^{5} & \zeta^{7} & \zeta^{9} & \zeta^{11} & \zeta^{13} & \zeta^{15} & \zeta^{17} & \zeta^{19} & \dots & \zeta^{7} \\
0 & \zeta^{10} & \zeta^{12} & \zeta^{14} & \zeta^{16} & \zeta^{18} & \zeta^{20} & \zeta^{22} & \zeta^{0} & \zeta^{2} & \zeta^{4} & \zeta^{6} & \zeta^{8} & \zeta^{10} & \zeta^{12} & \zeta^{14} & \zeta^{16} & \zeta^{18} & \zeta^{20} & \dots & \zeta^{8} \\
0 & \zeta^{11} & \zeta^{13} & \zeta^{15} & \zeta^{17} & \zeta^{19} & \zeta^{21} & \zeta^{23} & \zeta^{1} & \zeta^{3} & \zeta^{5} & \zeta^{7} & \zeta^{9} & \zeta^{11} & \zeta^{13} & \zeta^{15} & \zeta^{17} & \zeta^{19} & \zeta^{21} & \dots & \zeta^{9} \\
0 & \zeta^{12} & \zeta^{14} & \zeta^{16} & \zeta^{18} & \zeta^{20} & \zeta^{22} & \zeta^{0} & \zeta^{2} & \zeta^{4} & \zeta^{6} & \zeta^{8} & \zeta^{10} & \zeta^{12} & \zeta^{14} & \zeta^{16} & \zeta^{18} & \zeta^{20} & \zeta^{22} & \dots & \zeta^{10} \\
0 & \zeta^{13} & \zeta^{15} & \zeta^{17} & \zeta^{19} & \zeta^{21} & \zeta^{23} & \zeta^{1} & \zeta^{3} & \zeta^{5} & \zeta^{7} & \zeta^{9} & \zeta^{11} & \zeta^{13} & \zeta^{15} & \zeta^{17} & \zeta^{19} & \zeta^{21} & \zeta^{23} & \dots & \zeta^{11} \\
0 & \zeta^{14} & \zeta^{16} & \zeta^{18} & \zeta^{20} & \zeta^{22} & \zeta^{0} & \zeta^{2} & \zeta^{4} & \zeta^{6} & \zeta^{8} & \zeta^{10} & \zeta^{12} & \zeta^{14} & \zeta^{16} & \zeta^{18} & \zeta^{20} & \zeta^{22} & \zeta^{0} & \dots & \zeta^{12} \\
0 & \zeta^{15} & \zeta^{17} & \zeta^{19} & \zeta^{21} & \zeta^{23} & \zeta^{1} & \zeta^{3} & \zeta^{5} & \zeta^{7} & \zeta^{9} & \zeta^{11} & \zeta^{13} & \zeta^{15} & \zeta^{17} & \zeta^{19} & \zeta^{21} & \zeta^{23} & \zeta^{1} & \dots & \zeta^{13} \\
0 & \zeta^{16} & \zeta^{18} & \zeta^{20} & \zeta^{22} & \zeta^{0} & \zeta^{2} & \zeta^{4} & \zeta^{6} & \zeta^{8} & \zeta^{10} & \zeta^{12} & \zeta^{14} & \zeta^{16} & \zeta^{18} & \zeta^{20} & \zeta^{22} & \zeta^{0} & \zeta^{2} & \dots & \zeta^{14} \\
0 & \zeta^{17} & \zeta^{19} & \zeta^{21} & \zeta^{23} & \zeta^{1} & \zeta^{3} & \zeta^{5} & \zeta^{7} & \zeta^{9} & \zeta^{11} & \zeta^{13} & \zeta^{15} & \zeta^{17} & \zeta^{19} & \zeta^{21} & \zeta^{23} & \zeta^{1} & \zeta^{3} & \dots & \zeta^{15} \\
0 & \zeta^{18} & \zeta^{20} & \zeta^{22} & \zeta^{0} & \zeta^{2} & \zeta^{4} & \zeta^{6} & \zeta^{8} & \zeta^{10} & \zeta^{12} & \zeta^{14} & \zeta^{16} & \zeta^{18} & \zeta^{20} & \zeta^{22} & \zeta^{0} & \zeta^{2} & \zeta^{4} & \dots & \zeta^{16} \\
0 & \zeta^{19} & \zeta^{21} & \zeta^{23} & \zeta^{1} & \zeta^{3} & \zeta^{5} & \zeta^{7} & \zeta^{9} & \zeta^{11} & \zeta^{13} & \zeta^{15} & \zeta^{17} & \zeta^{19} & \zeta^{21} & \zeta^{23} & \zeta^{1} & \zeta^{3} & \zeta^{5} & \dots & \zeta^{17} \\
0 & \zeta^{20} & \zeta^{22} & \zeta^{0} & \zeta^{2} & \zeta^{4} & \zeta^{6} & \zeta^{8} & \zeta^{10} & \zeta^{12} & \zeta^{14} & \zeta^{16} & \zeta^{18} & \zeta^{20} & \zeta^{22} & \zeta^{0} & \zeta^{2} & \zeta^{4} & \zeta^{6} & \dots & \zeta^{18} \\
0 & \zeta^{21} & \zeta^{23} & \zeta^{1} & \zeta^{3} & \zeta^{5} & \zeta^{7} & \zeta^{9} & \zeta^{11} & \zeta^{13} & \zeta^{15} & \zeta^{17} & \zeta^{19} & \zeta^{21} & \zeta^{23} & \zeta^{1} & \zeta^{3} & \zeta^{5} & \zeta^{7} & \dots & \zeta^{19} \\
0 & \zeta^{22} & \zeta^{0} & \zeta^{2} & \zeta^{4} & \zeta^{6} & \zeta^{8} & \zeta^{10} & \zeta^{12} & \zeta^{14} & \zeta^{16} & \zeta^{18} & \zeta^{20} & \zeta^{22} & \zeta^{0} & \zeta^{2} & \zeta^{4} & \zeta^{6} & \zeta^{8} & \dots & \zeta^{20} \\
0 & \zeta^{23} & \zeta^{1} & \zeta^{3} & \zeta^{5} & \zeta^{7} & \zeta^{9} & \zeta^{11} & \zeta^{13} & \zeta^{15} & \zeta^{17} & \zeta^{19} & \zeta^{21} & \zeta^{23} & \zeta^{1} & \zeta^{3} & \zeta^{5} & \zeta^{7} & \zeta^{9} & \dots & \zeta^{21}
\end{bmatrix}_{25\times 25}$$

and the matrix $H_2 = [Tr(ax^2)]_{a,x\in GF(5,2)}$ *is given by*

$$H_2=\begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3\\
0&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2\\
0&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2\\
0&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4\\
0&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2\\
0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0\\
0&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1\\
0&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4\\
0&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4\\
0&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3\\
0&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4\\
0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0\\
0&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2\\
0&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3\\
0&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3\\
0&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1\\
0&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3\\
0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0\\
0&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4\\
0&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1\\
0&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1\\
0&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2\\
0&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1\\
0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0
\end{bmatrix}_{25\times 25}.$$

The rows of H can be generated by

$$G_{H_2}=\begin{bmatrix}
0&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3\\
0&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2
\end{bmatrix}_{2\times 25}.$$

Therefore H_2 is a linear code over $\mathbb{Z}_5$ and its parameters are $[25, 2, 16]$. By deleting the

first column of the matrix H_2 we obtain:

$$H_2^* = \begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3\\
4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2\\
2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2\\
0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4\\
1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2\\
4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0\\
4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1\\
3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4\\
4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4\\
0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3\\
2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4\\
3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0\\
3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2\\
1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3\\
3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3\\
0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1\\
4&1&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3\\
1&2&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0\\
1&1&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4\\
2&0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1\\
1&3&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1\\
0&2&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2\\
3&2&2&1&4&4&2&3&3&4&1&1&3&2&2&1&4&4&2&3&3&4&1&1\\
2&4&0&4&3&0&3&1&0&1&2&0&2&4&0&4&3&0&3&1&0&1&2&0
\end{bmatrix}_{25\times 24}.$$

The punctured code H_2^*, obtained by deleting the first column of H_2 is a $[24, 2, 16]$ code over $\mathbb{Z}_5$ and codewords of H_2^* are the left-cyclic shifts of elements of the first two non-zero codewords of H_2^*. Indeed H_2^* is a cyclic code. The Hamming weight of each non-zero codeword of H_2 is either 16 or 24. Thus H_2 is a two-weight code. From part (iv) of

Theorem 4.4.1, H_2 is a self-orthogonal code.

Throughout this chapter we have studied the distribution of the trace map over $GF(p,2)$ in the form of $Tr(ax^2)$ and used it to construct two-dimensional, two-weight, self-orthogonal codes over $\mathbb{Z}_p$. The next question is whether we can apply the trace map over $GF(p,2)$ in the form of $Tr(ax^\lambda)$ for any $\lambda > 2$ integer. We devote the next two chapters to study this case.

Chapter 5

Two-Weight, Self-Orthogonal Codes from $\mathbf{Tr(ax^{\lambda})}$

5.1 Introduction

In Chapter 4 we studied the distribution of the trace map over the Galois field $GF(p,2)$ in the form of $Tr(ax^2)$ and constructed cyclic, two-weight, self-orthogonal codes over $\mathbb{Z}_p$ with the parameters $[p^2, 2, (p-1)^2]$. This is a motivation to examine the use of the trace map over the Galois field $GF(p,2)$ in the form of $Tr(ax^{\lambda})$ for $\lambda > 2$. Since $Tr(x) = Tr(x^p)$, we consider the values of λ in the range of $2 < \lambda < p$. In the case of $\lambda = 2$ in Chapter 4 we divided the elements of $GF(p,2)^*$ equally into two subsets to study the distribution of the trace values (see Theorem 4.3.8). Similarly, in this chapter, we will divide the elements of $GF(p,2)^*$ equally into λ subsets in order to study the distribution of trace values. Thus $\lambda | p^2 - 1$. i.e., $\lambda | (p+1)(p-1)$. Now since only 2 divides both $(p+1)$ and $(p-1)$, for $\lambda > 2$, we only consider the cases when $\lambda | (p+1)$ and $\lambda | (p-1)$. In this chapter we focus on $\lambda | (p+1)$. Since $(p-1)$ does not divide $(p+1)$, the range of λ now becomes $2 < \lambda < p-1$.

In Section 5.2 we study the distribution of $Tr(ax^{\lambda})$ for x and a in $GF(p,2)$. Subsequently we apply this distribution to construct codes over $\mathbb{Z}_p$ in Section 5.3 classifying them as cyclic, two-weight, self-orthogonal codes with the parameters
$[p^2, 2, (p-(\lambda-1))(p-1)]$.

5.2 The distribution of $\mathbf{Tr}(\mathbf{ax}^{\lambda})$

In this section we study the distribution of $Tr(ax^{\lambda})$ by changing x over the Galois field $GF(p,2)$ for $a \in GF(p,2)$.

Let us recall from Chapter 4 the Galois field $GF(p,2)$ and properties of the trace map. Let $p(x)$ be a primitive polynomial of degree 2 over $\mathbb{Z}_p$. The Galois field of characteristic p is defined as the quotient field $GF(p,2) = \mathbb{Z}_p[x]/(p(x))$. Let ζ be a root of $p(x)$ and therefore $GF(p,2) = \mathbb{Z}_p[\zeta]$. Thus any element in $GF(p,2)$ can be written as a polynomial of degree 1 in ζ over $\mathbb{Z}_p$ and further $GF(p,2) = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{p^2-2}\}$. The trace map $Tr : GF(p,2) \to \mathbb{Z}_p$ is defined by $Tr(x) = x + x^p$. From Corollary 4.3.4 we know that for $x \in GF(p,2)^*$, $Tr(x) = 0$ if and only if $x = \zeta^{\frac{p+1}{2}(2k+1)}$, where $k = 0, 1, 2 \ldots, p-2$. In this section, for $a \in GF(p,2)$, we study the distribution of $Tr(ax^{\lambda})$ by changing x over $GF(p,2)$.

The first step towards understanding the distribution of $Tr(ax^{\lambda})$ requires us to identify the position of the trace zero elements in $A^* = [ax^{\lambda}]_{a,x \in GF(p,2)^*}$. To do this, we first divide the elements of $GF(p,2)^*$ into equivalence classes modulo λ. Since the elements of $GF(p,2)^*$ can also be expressed as powers of ζ the primitive element, the best way is to define the disjoint sets $(i)_{\lambda}$ as follows:

Definition 5.2.1. $(i)_{\lambda} = \{\zeta^{\lambda h+i} \mid h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda} - 1\}$, *for* $i = 0, 1, 2, \ldots, \lambda - 1$.

Thus the $(i)_{\lambda}$ are the equivalence classes modulo λ and they partition $GF(p,2)^*$ into disjoint sets., i.e.,

$$GF(p,2)^* = \bigcup_{i=0}^{\lambda-1} (i)_{\lambda}. \tag{5.1}$$

The following lemma examines the pattern of elements in each row of the matrix $A^* = [ax^{\lambda}]_{a,x \in GF(p,2)^*}$ as a power of ζ.

Lemma 5.2.2. *Let* $2 < \lambda < p-1$ *be an integer such that* $\lambda | (p+1)$. *Let* $A^* = [ax^{\lambda}]_{a,x \in GF(p,2)^*}$ *and* ζ *be a primitive element of* $GF(p,2)$. *Let* $(i)_{\lambda} = \{\zeta^{\lambda h+i} \mid h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda} - 1\}$, *where* $i = 0, 1, 2, \ldots, \lambda - 1$. *Then*
(i) The first λ *rows of* A^* *are given by* λ *copies of* $(i)_{\lambda}$, *where* $i = 0, 1, 2, \ldots, \lambda - 1$.

(ii) The next λ rows of A^* are given by λ copies of one cyclic shift of $(i)_\lambda$, where $i = 0, 1, 2, \ldots, \lambda - 1$.

(iii) In this manner the last λ rows of A^* are given by λ copies of $\frac{p^2-1}{\lambda} - 1$ cyclic shifts of $(i)_\lambda$, where $i = 0, 1, 2, \ldots, \lambda - 1$.

Proof:

Consider the matrix $A^* = [ax^\lambda]_{a,x \in GF(p,2)^*}$, where $a, x \in GF(p,2)^* = \{1, \zeta, \zeta^2, \ldots, \zeta^{p^2-2}\}$. Let $a = \zeta^{t_0}$, for a fixed t_0, $0 \leq t_0 \leq p^2 - 2$ and $x = \zeta^t$, for all $0 \leq t \leq p^2 - 2$. Then any row in A^* can be written as $\{ax^\lambda\}_{t_0} = \{\zeta^{t_0+\lambda t} | 0 \leq t \leq p^2 - 2\}$. Since $(i)_\lambda = \{\zeta^{\lambda h+i} \mid h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda} - 1\}$, where $i = 0, 1, 2, \ldots, \lambda - 1$, it is clear that $|(i)_\lambda| = \frac{p^2-1}{\lambda}$ and $|\{ax^\lambda\}_{t_0}| = p^2 - 1$. Now $A^* = [\zeta^{t_0+\lambda t}]$, where t changes from 0 to $p^2 - 2$ giving $p^2 - 1$ columns and t_0 changes from 0 to $p^2 - 2$ giving $p^2 - 1$ rows.

(i) Let $t_0 = 0$ and $0 \leq t \leq p^2 - 2$. Then $\{ax^\lambda\}_0 = \{\zeta^{\lambda t} | t = 0, 1, 2, \ldots, p^2 - 2\}$. This is the first row of the matrix A^*. Now look at the set $(i)_\lambda = \{\zeta^{\lambda h+i} \mid h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda} - 1\}$, where $i = 0, 1, 2, \ldots, \lambda - 1$. Let $i = 0$ and then $(0)_\lambda = \{\zeta^{\lambda h} \mid h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda} - 1\}$. It is clear that $(0)_\lambda \subset \{ax^\lambda\}_0$. The last element in the set $(0)_\lambda$ is $\zeta^{\lambda(\frac{p^2-1}{\lambda}-1)} = \zeta^{p^2-\lambda-1}$. This is the $\left(\frac{p^2-1}{\lambda} - 1\right)^{th}$ element in the set $\{ax^\lambda\}_0$. The next element in $\{ax^\lambda\}_0$ is $\zeta^{\lambda\left(\frac{p^2-1}{\lambda}-1+1\right)} = \zeta^{p^2-1} = 1$. That means after the $\left(\frac{p^2-1}{\lambda} - 1\right)^{th}$ element in the set $\{ax^\lambda\}_0$, the elements of the set $(0)_\lambda$ will start to repeat. Since there are $p^2 - 1$ elements in $\{ax^\lambda\}_0$ we need λ copies of $(0)_\lambda$ to form the entire set $\{ax^\lambda\}_0$. i.e., the first row of the matrix A^*. We can continue the same process for $t_0 = 1, 2, \ldots, \lambda - 1$. In each case, the value of i is $i = 1, 2, \ldots, \lambda - 1$. This completes the creation of the first λ rows of the matrix A^*.

(ii) Now consider $t_0 = \lambda$. Then $a = \zeta^\lambda$ and the set

$$\begin{aligned} \{ax^\lambda\}_\lambda &= \{\zeta^{\lambda+\lambda t} = \zeta^{(t+1)\lambda} | t = 0, 1, 2, \ldots, p^2 - 2\} \\ &= \{\zeta^\lambda, \zeta^{2\lambda}, \ldots, \zeta^{(p^2-1)\lambda}\}. \end{aligned}$$

Also consider a one cyclic shift of each element in $(0)_\lambda$ to the left and label this as $L_1(0)_\lambda$. Then

$$\begin{aligned} L_1(0)_\lambda &= \{\zeta^{\lambda h} | h = 1, 2, \ldots, (\frac{p^2 - 1}{\lambda} - 1), 0\} \\ &= \{\zeta^\lambda, \zeta^{2\lambda}, \ldots, 1\}. \end{aligned}$$

It is clear that $L_1(0)_\lambda \subset \{ax^\lambda\}_\lambda$ and $\left(\frac{p^2-1}{\lambda}-1\right)^{th}$ element in the set $\{ax^\lambda\}_\lambda$ is $\zeta^{\lambda\left(\frac{p^2-1}{\lambda}-1+1\right)} = \zeta^{p^2-1} = 1$. This is the last element in the set $L_1(0)_\lambda$ and the next element in $\{ax^\lambda\}_\lambda$ will be ζ^λ. Thus the elements of the set $L_1(0)_\lambda$ will start to repeat in $\{ax^\lambda\}_\lambda$. Since $|L_1(0)_\lambda| = \frac{p^2-1}{\lambda}$ we need λ copies of $L_1(0)_\lambda$ to form the entire set $\{ax^\lambda\}_\lambda$. i.e., the $(\lambda+1)^{th}$ row of the matrix A^*. We can continue this process for $t_0 = \lambda+1, \lambda+2, \ldots, \lambda+\lambda-1$. In each case, the value of i is $i = 1, 2, \ldots, \lambda-1$ and relevant set can be denoted by $L_1(i)_\lambda$. This completes the creation of the second λ rows of the matrix A^*.

(iii) Now consider $t_0 = 2\lambda, 2\lambda+1, \ldots, 2\lambda+\lambda-1$. In each of these cases, the value of i is $i = 0, 1, 2, \ldots, \lambda-1$ and the relevant set should be labeled by $L_2(i)_\lambda$. This means we need to get two left-cyclic shifts of each element of $(i)_\lambda$. λ copies of each of these $L_2(i)_\lambda$ sets form the set $\{ax^\lambda\}_{t_0} = \{\zeta^{\lambda(2+t)+i} | t = 0, 1, 2, \ldots, p^2-2\}$. By continuing this process until it makes $\left(\frac{p^2-1}{\lambda}-1\right)$ left-cyclic shifts of elements in $(i)_\lambda$ for all $i = 0, 1, 2, \ldots, \lambda-1$, we can form all the rows of the matrix A^*. □

The following example illustrates this result.

Example 5.2.3. *Let $p = 5$ and $\lambda = 3$. Then $\lambda|(p+1)$ and the matrix $A_3^* = [ax^3]_{a,x\in GF(5,2)^*}$ is*

$$A_3^* = \begin{bmatrix}
1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \ldots & \zeta^{21} \\
\zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \ldots & \zeta^{22} \\
\zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \ldots & \zeta^{23} \\
\zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \ldots & \zeta^{21} & 1 \\
\zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \ldots & \zeta^{22} & \zeta \\
\zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \ldots & \zeta^{23} & \zeta^2 \\
\zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \ldots & \zeta^{21} & 1 & \zeta^3 \\
\zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \ldots & \zeta^{22} & \zeta & \zeta^4 \\
\zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \ldots & \zeta^{23} & \zeta^2 & \zeta^5 \\
\zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \ldots & \zeta^{21} & 1 & \zeta^3 & \zeta^6 \\
\zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \ldots & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 \\
\zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \ldots & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 \\
\zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \ldots & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 \\
\zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \ldots & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} \\
\zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \ldots & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} \\
\zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \ldots & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} \\
\zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \ldots & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} \\
\zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \ldots & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} \\
\zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \ldots & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} \\
\zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \ldots & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} \\
\zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \ldots & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} \\
\zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \ldots & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} \\
\zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \ldots & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} \\
\zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \ldots & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20}
\end{bmatrix}_{24\times 24}.$$

Elements in each row of $A_3^* = [ax^3]_{a,x \in GF(5,2)^*}$ *can be written by using 3 copies of* $(i)_3 = \{\zeta^{3h+i} \mid h = 0, 1, 2, \ldots, \frac{5^2-(3+1)}{3}\}$, *where* $i = 0, 1, 2$.

i.e.,

$(0)_3 = \{\zeta^{3h} \mid h = 0, 1, 2, \ldots, \frac{5^2-(3+1)}{3} = 7\}$.

$(1)_3 = \{\zeta^{3h+1} \mid h = 0, 1, 2, \ldots, \frac{5^2-(3+1)}{3} = 7\}$.

$(2)_3 = \{\zeta^{3h+2} \mid h = 0, 1, 2, \ldots, \frac{5^2-(3+1)}{3} = 7\}$.

i.e.,

$(0)_3 = \{1, \zeta^3, \zeta^6, \zeta^9, \zeta^{12}, \zeta^{15}, \zeta^{18}, \zeta^{21}\}$.

$(1)_3 = \{\zeta, \zeta^4, \zeta^7, \zeta^{10}, \zeta^{13}, \zeta^{16}, \zeta^{19}, \zeta^{22}\}$.

$(2)_3 = \{\zeta^2, \zeta^5, \zeta^8, \zeta^{11}, \zeta^{14}, \zeta^{17}, \zeta^{20}, \zeta^{23}\}$.

and 7 left-cyclic shifts of 3 copies of each of these three sets.

The main purpose of this section is studying the distribution of $\{Tr(ax^\lambda) \mid x \in GF(p,2)^*\}$ for $a \in GF(p,2)^*$. From Lemma 5.2.2 it is clear that for a fixed $a \in GF(p,2)^*$ the set $\{ax^\lambda \mid x \in GF(p,2)^*\}$ is equal to λ copies of $(i)_\lambda = \{\zeta^{\lambda h+i} \mid h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda}-1\}$ or cyclic shifts of λ copies of $(i)_\lambda$, where $i = 0, 1, 2, \ldots, \lambda - 1$. Therefore it is enough to study the trace values of elements in each set $(i)_\lambda$ for $i = 0, 1, 2 \ldots, \lambda - 1$. First we will find out the elements that have trace 0 and how they are distributed in the set $(i)_\lambda$.

Lemma 5.2.4. *Let* λ *be a positive integer. If* $\Psi_\lambda = \{ax^\lambda \mid Tr(ax^\lambda) = 0; a, x \in GF(p,2)^*\}$ *then* $\Psi_\lambda = \{\zeta^{\frac{(p+1)}{2}(2k+1)} \mid k = 0, 1, 2, \ldots, p-2\}$.

Proof:

Since $a, x \in GF(p,2)^*$, a and x can be written as $a = \zeta^{t_0}$ and $x = \zeta^{t_1}$, for some t_0 and t_1, where $0 \leq t_0, t_1 \leq p^2 - 2$. Now for any positive integer λ we have $ax^\lambda = \zeta^{t_0+\lambda t_1} = \zeta^t \in GF(p,2)^*$, for some $0 \leq t \leq p^2 - 2$. Therefore $\Psi_\lambda = \{\zeta^t \mid Tr(\zeta^t) = 0\}$. From Corollary 4.3.4 we know that for $x \in GF(p,2)^*$, $Tr(x) = 0$ if and only if $x = \zeta^{\left(\frac{p+1}{2}\right)(2k+1)}$, where $k = 0, 1, 2, \ldots, p-2$. In other words, $Tr(\zeta^t) = 0$ if and only if $t = \left(\frac{p+1}{2}\right)(2k+1)$, where $k = 0, 1, 2, \ldots, p-2$. Thus $\Psi_\lambda = \{\zeta^{\frac{(p+1)}{2}(2k+1)} \mid k = 0, 1, 2, \ldots, p-2\}$. □

Note that when we represent the elements in the set Ψ_λ as powers of ζ, the elements are independent from λ. Therefore from now on we use Ψ to represent the set Ψ_λ.

The following lemma describes the distribution of the elements of Ψ in the set $(i)_\lambda$.

Lemma 5.2.5. *Let $p > 3$ be a prime and λ be an integer such that $2 < \lambda < p-1$ and $\lambda|(p+1)$. Let $i = 0, 1, 2, \ldots, \lambda - 1$ and $(i)_\lambda = \left\{\zeta^{\lambda h+i} \mid h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda} - 1\right\}$. Let $\Psi = \{\zeta^{\frac{(p+1)}{2}(2k+1)} \mid k = 0, 1, 2, \ldots, (p-1)-1\}$.*
(i) If $\lambda = \frac{p+1}{2}$ then $\Psi \subset (0)_\lambda$.
(ii) If $\lambda = \frac{p+1}{2}$ and its prime factorisation is $\lambda = \lambda_1^{e_1}\lambda_2^{e_2}\ldots\lambda_u^{e_u}$ then for all $j = 1, 2, \ldots, u$, $\Psi \subset (0)_{\lambda_j}$ and $\Psi \subset (0)_{\lambda_j^{e_j}}$.
(iii) For $q > 1$, if $\lambda = 2q$ then $\Psi \subset (q)_{2q}$.

Proof:
(i) Consider the set $(0)_\lambda = \left\{\zeta^{\lambda h} \mid h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda} - 1\right\}$. If $\lambda = \frac{(p+1)}{2}$ then we have

$$\begin{aligned}
\frac{p^2-1}{\lambda} - 1 &= \frac{p^2 - (\frac{(p+1)}{2} + 1)}{\frac{(p+1)}{2}} \\
&= \frac{2p^2 - p - 3}{(p+1)} \\
&= \frac{(p+1)(2p-3)}{(p+1)} \\
&= (2p-3) \\
&= 2(p-1) - 1.
\end{aligned}$$

Hence for $\lambda = \frac{p+1}{2}$, the set $(0)_\lambda$ is $(0)_{\frac{(p+1)}{2}} = \left\{\zeta^{\frac{(p+1)}{2}h} \mid h = 0, 1, 2, \ldots, 2(p-1) - 1\right\}$.

It is clear that $(p-1)-1 < 2(p-1)-1$ and the highest power of ζ in Ψ is $\frac{p+1}{2}(2(p-1)-1)$. Thus it is clear that all the elements in Ψ are in the set $(0)_{\frac{p+1}{2}}$. Therefore for $\lambda = \frac{p+1}{2}$ we have $\Psi \subset (0)_\lambda$.
(ii) Let $\lambda = \frac{p+1}{2}$ and its prime factorisation be $\lambda = \lambda_1^{e_1}\lambda_2^{e_2}\ldots\lambda_u^{e_u}$. For each λ_j, where $j = 1, 2, \ldots, u$, we write
$(0)_{\lambda_j} = \left\{\zeta^{\lambda_j h} \mid h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda_j} - 1\right\}$. Since $\lambda_j|\lambda$, there exists $\alpha_j \in \mathbb{Z}^+$ such that

$$\begin{aligned}
\lambda &= \alpha_j\lambda_j. \\
\Rightarrow \frac{p+1}{2} &= \alpha_j\lambda_j. \\
\Rightarrow \lambda_j &= \frac{p+1}{2\alpha_j}.
\end{aligned}$$

Therefore $(0)_{\lambda_j} = (0)_{\frac{p+1}{2\alpha_j}} = \left\{\zeta^{\left(\frac{p+1}{2\alpha_j}\right)h} \mid h = 0, 1, 2, \ldots, \frac{p^2-1}{\frac{p+1}{2\alpha_j}} - 1\right\}$ and
$\frac{p^2-1}{\frac{p+1}{2\alpha_j}} - 1 = 2\alpha_j p - (1 + 2\alpha_j) = 2\alpha_j(p-1) - 1.$

Hence $(0)_{\lambda_j} = (0)_{\frac{p+1}{2\alpha_j}} = \left\{\zeta^{\left(\frac{p+1}{2\alpha_j}\right)h} \mid h = 0, 1, 2, \ldots, (2\alpha_j p - (1 + 2\alpha_j))\right\}$. It is also clear that, for all $\alpha_j \in \mathbb{Z}^+$, $(p-1) - 1 < 2\alpha_j(p-1) - 1$ and therefore all the elements in the set Ψ are entirely in the set $(0)_{\lambda_j} = (0)_{\frac{p+1}{2\alpha_j}} = \left\{\zeta^{\left(\frac{p+1}{2\alpha_j}\right)h} \mid h = 0, 1, 2, \ldots, 2\alpha_j(p-1) - 1\right\}$.
Thus for all $j = 1, 2, \ldots, u$, $\Psi \subset (0)_{\lambda_j}$. By using a similar argument, we can also prove that, for all $j = 1, 2, \ldots, u$, $\Psi \subset (0)_{\lambda_j^{e_j}}$.

(iii) For $q > 1$, let $\lambda = 2q$ and consider the set $(q)_{2q}$ given by
$(q)_\lambda = (q)_{2q} = \left\{\zeta^{2qh+q} = \zeta^{q(2h+1)} \mid h = 0, 1, 2, \ldots, \frac{p^2-1}{2q} - 1\right\}$.

Since $\lambda|(p+1)$, there exists $\mu \in \mathbb{Z}^+$ such that

$$\begin{aligned} p + 1 &= \lambda\mu. \\ \Rightarrow p + 1 &= 2q\mu. \\ \Rightarrow q &= \frac{p+1}{2\mu}. \end{aligned}$$

Therefore $(q)_\lambda = (q)_{\frac{p+1}{\mu}} = \left\{\zeta^{\left(\frac{p+1}{2\mu}\right)(2h+1)} \mid h = 0, 1, 2, \ldots, \frac{p^2-1}{\frac{p+1}{\mu}} - 1\right\}$ and
$\frac{p^2-1}{\frac{p+1}{\mu}} - 1 = \mu p - (1 + \mu) = \mu(p-1) - 1.$
Hence $(q)_\lambda = (q)_{\frac{p+1}{\mu}} = \left\{\zeta^{\left(\frac{p+1}{2\mu}\right)(2h+1)} \mid h = 0, 1, 2, \ldots, \mu(p-1) - 1\right\}$. It is also clear that $\frac{p+1}{2\mu} < \frac{p+1}{2}$ and $(p-1) - 1 < \mu(p-1) - 1$. Thus $\Psi \subset (q)_{2q}$. □

In Lemma 5.2.5 we have identified some values of λ such that $\Psi \subset (i)_\lambda$, where $i = 0, 1, 2, \ldots, \lambda - 1$. We noticed that if $\lambda = \frac{p+1}{2}$ then $\Psi \subset (0)_\lambda$ and if $\lambda = \frac{p+1}{2} = \lambda_1^{e_1}\lambda_2^{e_2}\ldots\lambda_u^{e_u}$ then, for all $j = 1, 2, \ldots, u$, $\Psi \subset (0)_{\lambda_j}$ and $\Psi \subset (0)_{\lambda_j^{e_j}}$. We can also show that, for $j = 1, 2, \ldots, u$, if θ is a product of any combination of λ_j and $\lambda_j^{e_j}$then $\Psi \subset (0)_\theta$. We also noticed that, for $q > 1$, if $\lambda = 2q$ then $\Psi \subset (q)_\lambda$. We now have to answer two more questions that arise from Lemma 5.2.5. Are there any other values of λ such that $\Psi \subset (q)_\lambda$ and in the case of $\lambda = 2q$, what are the relevant prime numbers such that $\lambda|(p+1)$? In order to answer these two questions we need to do a careful investigation of the indices of elements in the two sets Ψ and $(q)_\lambda$ respectively.

From Lemma 5.2.4 we know that $\Psi = \{\zeta^{\frac{(p+1)}{2}(2k+1)} | k = 0, 1, 2, \ldots, p-2\}$. Consider the set $(i)_\lambda = \{\zeta^{\lambda h+i} | h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda} - 1\}$. If Ψ is entirely in $(q)_\lambda$ for $q > 1$ then, for all $k = 0, 1, 2, \ldots, p-2$, there exists $\alpha_k \in \mathbb{Z}^+$ such that

$$\frac{(p+1)}{2}(2k+1) \;=\; \lambda\alpha_k + q, \text{ where } 0 \leq \alpha_k \leq \frac{p^2-1}{\lambda} - 1. \tag{5.2}$$

From (5.2), if $q \neq 0$ then we have
$(2p+2)k + (p-2q+1) = 2\lambda\alpha_k$.
Since $\alpha_k \in \mathbb{Z}^+$ and $\lambda|(p+1)$ both $(2p+2)$ and $(p-2q+1)$ should be divisible by 2λ. i.e., $\frac{2p+2}{2\lambda} = \beta$ and $\frac{p-2q+1}{2\lambda} = \gamma$, where $\beta, \gamma \in \mathbb{Z}^+$. This implies that $p = \lambda\beta - 1$ and $p = 2\lambda\gamma + 2q - 1$.
$\Rightarrow \lambda\beta - 1 = 2\lambda\gamma + 2q - 1$.
$\Rightarrow \beta = 2\gamma + \frac{2q}{\lambda}$.
Since $\beta \in \mathbb{Z}^+$ and $q < \lambda$ we have $\lambda = 2q$. Conversely if $\lambda = 2q$ then it is obvious that $q \neq 0$. Thus there are no other values of λ (except when $\lambda = 2q$) such that $\Psi \subset (q)_\lambda$.

The relevant primes for $\lambda = 2q$ are given by $p = 2\lambda\gamma + 2q - 1 = 4q\gamma + 2q - 1$. This implies $p \equiv (2q-1) \bmod (4q)$ or $p \equiv (\lambda - 1) \bmod (2\lambda)$. Since $2 < \lambda < p-1$, we have $1 < q < \frac{p-1}{2}$.

Example 5.2.6. *Let $q = 2$ then $\lambda = 4$ and $p \equiv 3(mod\ 8)$. This gives us $p = 11, 19, 43$, etc. For all these primes, the set $\Psi = \{ax^4 \mid Tr(ax^4) = 0,\ a, x \in GF(p,2)^*\} = \{\zeta^{\frac{(p+1)}{2}(2k+1)} \mid k = 0, 1, 2, \ldots, p-2\} \subset (2)_4 = \left\{\zeta^{4h+2} \mid h = 0, 1, 2, \ldots, \frac{p^2-1}{4} - 1\right\}$.*

Let $q = 3$ then $\lambda = 6$ and $p \equiv 5(mod\ 12)$. This gives $p = 17, 29, 41$, etc. For all these primes, the set $\Psi = \{ax^6 \mid Tr(ax^6) = 0,\ a, x \in GF(p,2)^*\} = \{\zeta^{\frac{(p+1)}{2}(2k+1)} \mid k = 0, 1, 2, \ldots, p-2\} \subset (3)_6 = \left\{\zeta^{6h+3} \mid h = 0, 1, 2, \ldots, \frac{p^2-1}{6} - 1\right\}$.

Let us consider the elements of $GF(11,2)^*$ that are in $(i)_4$, where $i = 0, 1, 2, 3$, to illustrate the case $q = 2$ and $\lambda = 4$ such that $\Psi \subset (2)_4$.
$(0)_4 = \{1, \zeta^4, \zeta^8, \zeta^{12}, \zeta^{16}, \zeta^{20}, \zeta^{24}, \zeta^{28}, \zeta^{32}, \zeta^{36}, \zeta^{40}, \zeta^{44}, \zeta^{48}, \zeta^{52}, \zeta^{56}, \ldots\}$.
$(1)_4 = \{\zeta, \zeta^5, \zeta^9, \zeta^{13}, \zeta^{17}, \zeta^{21}, \zeta^{25}, \zeta^{29}, \zeta^{33}, \zeta^{37}, \zeta^{41}, \zeta^{45}, \zeta^{49}, \zeta^{53}, \zeta^{57}, \ldots\}$.
$(2)_4 = \{\zeta^2, (\zeta^6), \zeta^{10}, \zeta^{14}, (\zeta^{18}), \zeta^{22}, \zeta^{26}, (\zeta^{30}), \zeta^{34}, \zeta^{38}, (\zeta^{42}), \zeta^{46}, \zeta^{50}, (\zeta^{54}), \zeta^{58}, \ldots\}$.
$(3)_4 = \{\zeta^3, \zeta^7, \zeta^{11}, \zeta^{15}, \zeta^{19}, \zeta^{23}, \zeta^{27}, \zeta^{31}, \zeta^{35}, \zeta^{39}, \zeta^{43}, \zeta^{47}, \zeta^{51}, \zeta^{55}, \zeta^{59}, \ldots\}$.

From Theorem 4.3.3 we know that $Tr(\zeta^{\frac{p+1}{2}(2k+1)}) = 0$*, for all* $k = 0, 1, 2, \ldots, p-2$*. In this example* $Tr(\zeta^{6(2k+1)}) = 0$*, for all* $k = 0, 1, 2, \ldots, 9$*. Thus*

$$\begin{aligned}\Psi &= \{\zeta^{6(2k+1)} | k = 0, 1, 2, \ldots, 9\} \\ &= \{\zeta^{4(3k+1)+2} | k = 0, 1, 2, \ldots, 9\} \\ &= \{\zeta^{4h+2} | h = (3k+1), k = 0, 1, 2, \ldots, 9\} \subset (2)_4.\end{aligned}$$

The elements of Ψ *are in parenthesis in* $(2)_4$*.*

Let us now recall the matrix representation of elements of $GF(p,2)^*$ that we studied in Lemma 4.3.6.

$$GF(p,2)^* = \begin{bmatrix} \zeta^{(\frac{p+1}{2})} & \ldots & \zeta^{(\frac{p+1}{2})+d} & \ldots & \zeta^{(\frac{p+1}{2})+(\frac{p+1}{2})} & \ldots & \zeta^{(\frac{p+1}{2})+p} \\ \zeta^{(\frac{p+1}{2})3} & \ldots & \zeta^{(\frac{p+1}{2})3+d} & \ldots & \zeta^{(\frac{p+1}{2})3+(\frac{p+1}{2})} & \ldots & \zeta^{(\frac{p+1}{2})3+p} \\ \vdots & \ldots & \vdots & \ldots & \vdots & \ldots & \vdots \\ \zeta^{(\frac{p+1}{2})(2k+1)} & \ldots & \zeta^{(\frac{p+1}{2})(2k+1)+d} & \ldots & \zeta^{(\frac{p+1}{2})(2k+1)+(\frac{p+1}{2})} & \ldots & \zeta^{(\frac{p+1}{2})(2k+1)+p} \\ \vdots & \ldots & \vdots & \ldots & \vdots & \ldots & \vdots \\ \zeta^{(\frac{p+1}{2})(2p-3)} & \ldots & \zeta^{(\frac{p+1}{2})(2p-3)+d} & \ldots & \zeta^{p^2-1}=1 & \ldots & \zeta^{(\frac{p+1}{2})(2p-3)+p} \end{bmatrix}_{(p-1)\times(p+1)},$$

where $d = 0, 1, 2, \ldots, p$ and $k = 0, 1, 2, \ldots, p-2$. Here we will label each column by using the first element of that column.

In the next three lemmas, we study, for different values of λ, the position of the elements of the set $(i)_\lambda = \{\zeta^{\lambda h+i} | h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda} - 1\}$ in the columns of the matrix representation of $GF(p,2)^*$.

Lemma 5.2.7. *Let* $p > 3$ *be a prime and* $2 < \lambda < p-1$ *such that* $\lambda | (p+1)$*. Let* $i = 0, 1, 2, \ldots, \lambda - 1$ *and for each* i*, the set* $(i)_\lambda = \{\zeta^{\lambda h+i} | h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda} - 1\}$*. If* $\lambda = \frac{p+1}{2}$ *then for a fixed* i*, the elements in the set* $(i)_\lambda$ *are completely listed in the columns indexed by* $\zeta^{\frac{p+1}{2}+\lambda l+i}$ *in the matrix representation of* $GF(p,2)^*$*, where* $l = 0, 1, \ldots, \frac{p+1}{\lambda} - 1$*.*

Proof:

If $\lambda = \frac{p+1}{2}$ then $(i)_\lambda = (i)_{\frac{p+1}{2}} = \{\zeta^{(\frac{p+1}{2})h+i} | h = 0, 1, 2, \ldots, 2p-3\}$. The set of elements of the column indexed by $\zeta^{\frac{p+1}{2}+\lambda l+i}$ in the matrix representation of $GF(p,2)^*$ (denoted by (l)) is given by $(l) = \{\zeta^{(\frac{p+1}{2})(2k+1)+(\frac{p+1}{2})l+i} | k = 0, 1, 2, \ldots, p-2\}$, where $l = 0, 1, \ldots, \frac{p+1}{\lambda} - 1$. Since $\lambda = \frac{p+1}{2}$ we have $l = 0, 1$ and hence

$(l = 0) = \{\zeta^{(\frac{p+1}{2})(2k+1)+i} | k = 0, 1, 2, \ldots, p-2\}$

and

$(l=1)=\{\zeta^{(\frac{p+1}{2})(2k+2)+i}|k=0,1,2,\ldots,p-2\}$ respectively.

We need to prove that $(i)_{\frac{p+1}{2}}=(l=0)\cup(l=1)$.

Let $x\in(i)_{\frac{p+1}{2}}$. Then $x=\zeta^{(\frac{p+1}{2})h+i}$ for some $h=0,1,2,\ldots,2p-3$. If h is odd then $x\in(l=0)$ and if h is even then $x\in(l=1)$. Therefore

$$(i)_{\frac{p+1}{2}}\subset(l=0)\cup(l=1). \tag{5.3}$$

Next let any element $x\in(l=0)\cup(l=1)$. If $x\in(l=0)$ then $x=\zeta^{(\frac{p+1}{2})(2k+1)+i}$ for some $k=0,1,2,\ldots,p-2$. We also have $0\leq k\leq p-2\Rightarrow 1\leq 2k+1\leq 2p-3$. Therefore $x\in(i)_{\frac{p+1}{2}}$.

If $x\in(l=1)$ then $x=\zeta^{(\frac{p+1}{2})(2k+2)+i}$ for some $k=0,1,2,\ldots,p-2$. It is clear that $x\in(i)_\lambda$ since these values of k correspond to the even h for $0\leq h\leq 2p-3$, except possibly for $k=p-2$. When $k=p-2$, $x=\zeta^{(\frac{p+1}{2})(2k+2)+i}=\zeta^{(\frac{p+1}{2})(2p-2)+i}=\zeta^i$, which is corresponds to $h=0$. Thus

$$(l=0)\cup(l=1)\subset(i)_{\frac{p+1}{2}}. \tag{5.4}$$

Now from equations (5.3) and (5.4) we have $(i)_{\frac{p+1}{2}}=(l=0)\cup(l=1)$. i.e., in the case of $\lambda=\frac{p+1}{2}$, the elements in the set $(i)_\lambda$ are completely listed in the columns indexed by $\zeta^{\frac{p+1}{2}+\lambda l+i}$ in the matrix representation of $GF(p,2)^*$, where $l=0,1,\ldots\frac{p+1}{\lambda}-1=0,1$. □

The next example illustrates this result.

Example 5.2.8. *Let $p=5$ and $\lambda=3$. Then $\lambda|(p+1)$ and the set $(i)_3=\{\zeta^{3h+i}\mid h=0,1,2,\ldots,\frac{5^2-1}{3}-1\}$, where $i=0,1,2$.*

i.e.,

$(0)_3=\{\zeta^{3h}\mid h=0,1,2,\ldots,\frac{5^2-1}{3}-1=7\}$.

$(1)_3=\{\zeta^{3h+1}\mid h=0,1,2,\ldots,\frac{5^2-1}{3}-1=7\}$.

$(2)_3=\{\zeta^{3h+2}\mid h=0,1,2,\ldots,\frac{5^2-1}{3}-1=7\}$.

i.e.,

$(0)_3=\{1,\zeta^3,\zeta^6,\zeta^9,\zeta^{12},\zeta^{15},\zeta^{18},\zeta^{21}\}$.

$(1)_3=\{\zeta,\zeta^4,\zeta^7,\zeta^{10},\zeta^{13},\zeta^{16},\zeta^{19},\zeta^{22}\}$.

$(2)_3 = \{\zeta^2, \zeta^5, \zeta^8, \zeta^{11}, \zeta^{14}, \zeta^{17}, \zeta^{20}, \zeta^{23}\}$.

The elements in the set $(i)_3$ *are from the columns indexed by* ζ^{3+i} *and* ζ^{6+i} *in the matrix representation of* $GF(5,2)^*$*, where* $i = 0, 1, 2$*. For example the elements of* $(0)_3$ *are in the columns indexed by* ζ^3 *and* ζ^6*.*

$$GF(5,2)^* = \begin{bmatrix} \zeta^3 & \zeta^4 & \zeta^5 & \zeta^6 & \zeta^7 & \zeta^8 \\ \zeta^9 & \zeta^{10} & \zeta^{11} & \zeta^{12} & \zeta^{13} & \zeta^{14} \\ \zeta^{15} & \zeta^{16} & \zeta^{17} & \zeta^{18} & \zeta^{19} & \zeta^{20} \\ \zeta^{21} & \zeta^{22} & \zeta^{23} & \zeta^{24}=1 & \zeta^{25}=\zeta & \zeta^{26}=\zeta^2 \end{bmatrix}_{4\times 6}.$$

In Lemma 5.2.7 we noticed that when $\lambda = \frac{p+1}{2}$, the elements in the set $(i)_\lambda$ are completely listed in columns indexed by $\zeta^{\frac{p+1}{2}+\lambda l+i}$ of the matrix representation of $GF(p,2)^*$, where $l = 0, 1$. Let us next look at the case $\lambda = \frac{p+1}{2}$ with a prime factorisation $\lambda_1^{e_1}\lambda_2^{e_2}\ldots\lambda_u^{e_u}$. The next lemma describes, for $j = 1, 2, \ldots, u$, the placement of the elements of the sets $(i)_{\lambda_j}$ and $(i)_{\lambda_j^{e_j}}$ in the columns of the matrix representation of $GF(p,2)^*$.

Lemma 5.2.9. *Let* $p > 3$ *be a prime and* $2 < \lambda < p-1$ *such that* $\lambda|(p+1)$*. Let* $i = 0, 1, 2, \ldots, \lambda - 1$ *and for each* i *the set* $(i)_\lambda = \{\zeta^{\lambda h+i} | h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda} - 1\}$*. If* $\lambda = \frac{p+1}{2}$ *and its prime factorisation is* $\lambda = \frac{p+1}{2} = \prod_{j=1}^{u} \lambda_j^{e_j}$ *then*

(i) for a fixed $i = 0, 1, 2, \ldots, \lambda_j - 1$*, the elements of the set* $(i)_{\lambda_j}$ *are completely listed in the columns indexed by* $\zeta^{\frac{p+1}{2}+\lambda_j l+i}$ *in the matrix representation of* $GF(p,2)^*$*, where* $l = 0, 1, \ldots, \frac{p+1}{\lambda_j} - 1$*.*

(ii) for a fixed $i = 0, 1, 2, \ldots, \lambda_j^{e_j} - 1$*, the elements of the set* $(i)_{\lambda_j^{e_j}}$ *are completely listed in the columns indexed by* $\zeta^{\frac{p+1}{2}+\lambda_j^{e_j} l+i}$ *in the matrix representation of* $GF(p,2)^*$*, where* $l = 0, 1, \ldots, \frac{p+1}{\lambda_j^{e_j}} - 1$*.*

Proof:

(i) If $\lambda = \frac{p+1}{2} = \lambda_1^{e_1}\lambda_2^{e_2}\ldots\lambda_u^{e_u}$ then $\lambda_j|\frac{p+1}{2}$, for all $j = 1, 2, \ldots, u$. i.e., there exist $\alpha_j \in \mathbb{Z}^+$ such that $\lambda_j = \frac{p+1}{2\alpha_j}$. Now for a fixed $i = 0, 1, 2, \ldots, \lambda_j - 1$, the set $(i)_{\lambda_j} = \{\zeta^{\lambda_j h+i} | h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda_j} - 1\}$ can be written as $(i)_{\lambda_j} = \{\zeta^{\lambda_j h+i} | h = 0, 1, 2, \ldots, (p-1)2\alpha_j - 1\}$. The values of h in $(i)_{\lambda_j}$ can be re-arranged as follows:

$(i)_{\lambda_j} = \{\zeta^{\lambda_j h+i} | h = \alpha_j, \alpha_j + 1, \ldots, (p-1)2\alpha_j - 1, 0, 1, 2, \ldots, \alpha_j - 1\}$. In addition to this, these values of h in $(i)_{\lambda_j}$ can be written in matrix form as follows:

$$h=\begin{bmatrix} \alpha_j & \alpha_j+1 & \alpha_j+2 & \dots & \alpha_j+\alpha_j-1 & \alpha_j+\alpha_j & \dots & \alpha_j+2\alpha_j-1 \\ 3\alpha_j & 3\alpha_j+1 & 3\alpha_j+2 & \dots & 3\alpha_j+\alpha_j-1 & 3\alpha_j+\alpha_j & \dots & 3\alpha_j+2\alpha_j-1 \\ 5\alpha_j & 5\alpha_j+1 & 5\alpha_j+2 & \dots & 5\alpha_j+\alpha_j-1 & 5\alpha_j+\alpha_j & \dots & 5\alpha_j+2\alpha_j-1 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ (2p-3)\alpha_j & (2p-3)\alpha_j+1 & (2p-3)\alpha_j+2 & \dots & (2p-3)\alpha_j+\alpha_j-1 & (2p-3)\alpha_j+\alpha_j & \dots & (2p-3)\alpha_j+2\alpha_j-1 \end{bmatrix}.$$

The following results hold:

$\lambda_j((2p-3)\alpha_j+\alpha_j-1) \equiv \lambda_j((p-1)2\alpha_j-1) \bmod (p^2-1)$.

$\lambda_j((2p-3)\alpha_j+\alpha_j) \equiv 0 \bmod (p^2-1)$.

$\lambda_j((2p-3)\alpha_j+2\alpha_j-1) \equiv \lambda_j(\alpha_j-1) \bmod (p^2-1)$.

The set of elements in the column indexed by $\zeta^{(\frac{p+1}{2})+\lambda_j l+i}$ in the matrix representation of $GF(p,2)^*$ is denoted by (l) and given by $(l) = \{\zeta^{(\frac{p+1}{2})(2k+1)+\lambda_j l+i} | k = 0,1,2,\dots,p-2\}$, where $l = 0,1,2,\dots,\frac{p+1}{\lambda_j}-1$. By using the substitution $\lambda_j = \frac{p+1}{2\alpha_j}$ we can re-write the elements of (l) as $(l) = \{\zeta^{\lambda_j(\alpha_j(2k+1)+l)+i} | k = 0,1,2,\dots,p-2\}$, where $l = 0,1,2,\dots,2\alpha_j-1$. It is clear that the number of elements of $(i)_{\lambda_j}$ is $(p-1)2\alpha_j$ and for $l = 0,1,2,\dots,2\alpha_j-1$, the sum of the number of elements in the sets (l) is also $(p-1)2\alpha_j$.

Now consider the set $(l=0) = \{\zeta^{\lambda_j(\alpha_j(2k+1))+i} | k = 0,1,2,\dots,p-2\}$. It is clear that these elements are in the set $(i)_{\lambda_j}$ and the corresponding values of h in $(i)_{\lambda_j}$ are in the first column of the matrix h above.

Next consider the set $(l=1) = \{\zeta^{\lambda_j(\alpha_j(2k+1)+1)+i} | k = 0,1,2,\dots,p-2\}$. It is clear that these elements are in the set $(i)_{\lambda_j}$ and the corresponding values of h in $(i)_{\lambda_j}$ are in the second column of the matrix h above.

Similarly we can show that the elements in the set $(l=2\alpha_j-1) = \{\zeta^{\lambda_j(\alpha_j(2k+1)+2\alpha_j-1)+i} |$ $k = 0,1,2,\dots,p-2\}$ are in the set $(i)_{\lambda_j}$ and the corresponding values of h in $(i)_{\lambda_j}$ are in the last column of the matrix h above.

Thus it is clear that

$$(i)_{\lambda_j} = \bigcup_{l=0}^{2\alpha_j-1} (l).$$

i.e., in the case of $\frac{p+1}{2} = \lambda_1^{e_1}\lambda_2^{e_2}\dots\lambda_u^{e_u}$, for a fixed $i = 0,1,2,\dots,\lambda_j-1$, the elements of $(i)_{\lambda_j}$ are completely listed in the columns indexed by $\zeta^{\frac{p+1}{2}+\lambda_j l+i}$ of the matrix representation of $GF(p,2)^*$, where $l = 0,1,2,\dots,\frac{p+1}{\lambda_j}-1$.

(ii) If $\lambda = \frac{p+1}{2} = \lambda_1^{e_1}\lambda_2^{e_2}\dots\lambda_u^{e_u}$ then $\lambda_j^{e_j} | \frac{p+1}{2}$, for all $j = 1,2,\dots,u$. i.e., there exists

$\beta_j \in \mathbb{Z}^+$ such that $\lambda_j^{e_j} = \frac{p+1}{2\beta_j}$. The rest of the proof is very similar to the proof of part (i). □

Note 5.2.10. *In Lemma 5.2.9, for $j = 1, 2, \ldots, u$, we identified the elements in the sets $(i)_{\lambda_j}$ and $(i)_{\lambda_j^{e_j}}$ from the columns in the matrix representation of $GF(p,2)^*$. Similarly, for $j = 1, 2, \ldots, u$, if θ is a product of any combination of λ_j and $\lambda_j^{e_j}$ we can identify the elements in the set $(i)_\theta$ from the columns in the matrix representation of $GF(p,2)^*$. In this case the elements of $(i)_\theta$ are completely listed in the columns indexed by $\zeta^{\frac{p+1}{2}+\theta l+i}$ in the matrix representation of $GF(p,2)^*$, where $l = 0, 1, 2, \ldots, \frac{p+1}{\theta} - 1$.*

Example 5.2.11. *Let $p = 11$ and $\lambda = \frac{p+1}{2} = 6 = 2 \times 3$. Then $6|(p+1)$, $2|(p+1)$ and $3|(p+1)$. The set $(i)_3 = \{\zeta^{3h+i} \mid h = 0, 1, 2, \ldots, \frac{11^2-(3+1)}{3}\}$, where $i = 0, 1, 2$.*

i.e.,

$(0)_3 = \{\zeta^{3h} \mid h = 0, 1, 2, \ldots, \frac{11^2-1}{3} - 1 = 39\}$.

$(1)_3 = \{\zeta^{3h+1} \mid h = 0, 1, 2, \ldots, \frac{11^2-1}{3} - 1 = 39\}$.

$(2)_3 = \{\zeta^{3h+2} \mid h = 0, 1, 2, \ldots, \frac{11^2-1}{3} - 1 = 39\}$.

i.e.,

$(0)_3 = \{1, \zeta^3, \zeta^6, \zeta^9, \zeta^{12}, \zeta^{15}, \zeta^{18}, \zeta^{21}, \zeta^{24}, \zeta^{27}, \zeta^{30}, \zeta^{33}, \zeta^{36}, \zeta^{39}, \zeta^{42}, \zeta^{45}, \zeta^{48}, \zeta^{51}, \zeta^{54}, \ldots\}$.

$(1)_3 = \{\zeta, \zeta^4, \zeta^7, \zeta^{10}, \zeta^{13}, \zeta^{16}, \zeta^{19}, \zeta^{22}, \zeta^{25}, \zeta^{28}, \zeta^{31}, \zeta^{34}, \zeta^{37}, \zeta^{40}, \zeta^{43}, \zeta^{46}, \zeta^{49}, \zeta^{52}, \zeta^{55}, \ldots\}$.

$(2)_3 = \{\zeta^2, \zeta^5, \zeta^8, \zeta^{11}, \zeta^{14}, \zeta^{17}, \zeta^{20}, \zeta^{23}, \zeta^{26}, \zeta^{29}, \zeta^{32}, \zeta^{35}, \zeta^{38}, \zeta^{41}, \zeta^{44}, \zeta^{47}, \zeta^{50}, \zeta^{53}, \zeta^{56}, \ldots\}$.

The elements of $(i)_3$ are completely listed in the columns indexed by ζ^{6+3l+i} in the matrix representation of $GF(11,2)^*$, where $l = 0, 1, 2, 3$ and $i = 0, 1, 2$. For example elements of $(0)_3$ are in the columns indexed by ζ^6, ζ^9, ζ^{12} and ζ^{15}.

$$GF(11,2)^*=\begin{bmatrix} \zeta^{6} & \zeta^{7} & \zeta^{8} & \zeta^{9} & \zeta^{10} & \zeta^{11} & \zeta^{12} & \zeta^{13} & \zeta^{14} & \zeta^{15} & \zeta^{16} & \zeta^{17} \\ \zeta^{18} & \zeta^{19} & \zeta^{20} & \zeta^{21} & \zeta^{22} & \zeta^{23} & \zeta^{24} & \zeta^{25} & \zeta^{26} & \zeta^{27} & \zeta^{28} & \zeta^{29} \\ \zeta^{30} & \zeta^{31} & \zeta^{32} & \zeta^{33} & \zeta^{34} & \zeta^{35} & \zeta^{36} & \zeta^{37} & \zeta^{38} & \zeta^{39} & \zeta^{40} & \zeta^{41} \\ \zeta^{42} & \zeta^{43} & \zeta^{44} & \zeta^{45} & \zeta^{46} & \zeta^{47} & \zeta^{48} & \zeta^{49} & \zeta^{50} & \zeta^{51} & \zeta^{52} & \zeta^{53} \\ \zeta^{54} & \zeta^{55} & \zeta^{56} & \zeta^{57} & \zeta^{58} & \zeta^{59} & \zeta^{60} & \zeta^{61} & \zeta^{62} & \zeta^{63} & \zeta^{64} & \zeta^{65} \\ \zeta^{66} & \zeta^{67} & \zeta^{68} & \zeta^{69} & \zeta^{70} & \zeta^{71} & \zeta^{72} & \zeta^{73} & \zeta^{74} & \zeta^{75} & \zeta^{76} & \zeta^{77} \\ \zeta^{78} & \zeta^{79} & \zeta^{80} & \zeta^{81} & \zeta^{82} & \zeta^{83} & \zeta^{84} & \zeta^{85} & \zeta^{86} & \zeta^{87} & \zeta^{88} & \zeta^{89} \\ \zeta^{90} & \zeta^{91} & \zeta^{92} & \zeta^{93} & \zeta^{94} & \zeta^{95} & \zeta^{96} & \zeta^{97} & \zeta^{98} & \zeta^{99} & \zeta^{100} & \zeta^{101} \\ \zeta^{102} & \zeta^{103} & \zeta^{104} & \zeta^{105} & \zeta^{106} & \zeta^{107} & \zeta^{108} & \zeta^{109} & \zeta^{110} & \zeta^{111} & \zeta^{112} & \zeta^{113} \\ \zeta^{114} & \zeta^{115} & \zeta^{116} & \zeta^{117} & \zeta^{118} & \zeta^{119} & 1 & \zeta & \zeta^{2} & \zeta^{3} & \zeta^{4} & \zeta^{5} \end{bmatrix}_{10\times 12}.$$

Thus far we have identified the positioning of the elements of $(i)_\lambda$ in the matrix representation of $GF(p,2)^*$ for $\lambda=\frac{p+1}{2}$, for the prime power factors of $\lambda=\frac{p+1}{2}$ and for the product of any combination of these factors. In the next lemma we will study the case $\lambda=2q$ for $1<q<\frac{p-1}{2}$ such that $p\equiv(2q-1)\text{mod}(4q)$.

Lemma 5.2.12. *Let $p>3$ be a prime such that, for $1<q<\frac{p-1}{2}$, $p\equiv(2q-1)(mod\ 4q)$ and $2<\lambda<p-1$ such that $\lambda|(p+1)$. Let $i=0,1,2,\ldots,\lambda-1$ and the set $(i)_\lambda=\{\zeta^{\lambda h+i}|h=0,1,2,\ldots,\frac{p^2-1}{\lambda}-1\}$. For $1<q<\frac{p-1}{2}$, if $\lambda=2q$ then for a fixed $i=0,1,2,\ldots,2q-1$ the elements of the set $(i)_{2q}$ are completely listed in the columns indexed by $\zeta^{\frac{p+1}{2}+2ql+q+i}$ in the matrix representation of $GF(p,2)^*$, where $l=0,1,2,\ldots,\frac{p+1}{2q}-1$.*

Proof:

Since $\lambda=2q$ and $\lambda|(p+1)$ we have $2q|(p+1)$ and hence there exists $\gamma\in\mathbb{Z}^+$ such that $\frac{p+1}{2q}=\gamma$. Since $p\equiv(2q-1)(\text{mod }4q)$ there exists $\rho\in\mathbb{Z}^+$ such that $\frac{p-(2q-1)}{4q}=\rho$. This implies that $\frac{p+1}{4q}-\frac{2q}{4q}=\frac{1}{2}\left(\frac{p+1}{2q}\right)-\frac{1}{2}$ is a positive integer. That is $\frac{\gamma-1}{2}$ is a positive integer and hence γ is an odd positive integer.

Now by using the substitution $\frac{p+1}{2q}=\gamma$ we can re-write the set $(i)_{2q}$ as

$$\begin{aligned}(i)_{2q} &= \{\zeta^{2qh+i}|h=0,1,2,\ldots,\frac{p^2-1}{2q}-1\}\\ &= \{\zeta^{2qh+i}|h=0,1,2,\ldots,\gamma(p-1)-1\}.\end{aligned}$$

Let (l) be the set of elements in the column labeled by $\zeta^{\frac{p+1}{2}+2ql+q+i}$ of the matrix representation of $GF(p,2)^*$, where $l=0,1,2,\ldots,\frac{p+1}{2q}-1$. Again by using the substitution

$\frac{p+1}{2q} = \gamma$ we can write the elements of the set (l) as

$$\begin{aligned}(l) &= \{\zeta^{\frac{p+1}{2}(2k+1)+2ql+q+i} | k = 0, 1, 2, \ldots, p-2\} \\ &= \{\zeta^{q\gamma(2k+1)+2ql+q+i} | k = 0, 1, 2, \ldots, p-2\},\end{aligned}$$

where $l = 0, 1, 2, \ldots, \gamma - 1$.

For $l = 0, 1, 2, \ldots, \gamma - 1$, it is clear that the number of elements of $(i)_{2q}$ and the sum of the number of elements of (l) are equal to $\gamma(p-1)$.

Re-writing the set $(i)_{2q}$:

$$\begin{aligned}(i)_{2q} &= \{\zeta^{2qh+i} | h = 0, 1, 2, \ldots, \gamma(p-1) - 1\} \\ &= \{\zeta^{2qh+i} | h = \frac{\gamma+1}{2}, \frac{\gamma+1}{2} + 1, \frac{\gamma+1}{2} + 2, \ldots, \gamma(p-1), 0, 1, 2, \ldots, \frac{\gamma-1}{2}\} \\ &= \{\zeta^{2qh+i} | h = \frac{\gamma+1}{2}, \frac{\gamma+3}{2}, \frac{\gamma+5}{2}, \ldots, \gamma(p-1), 0, 1, 2, \ldots, \frac{\gamma-1}{2}\}.\end{aligned}$$

As in Lemma 5.2.9, the values of h of $(i)_{2q}$ can be written in matrix form as follows:

$$h = \begin{bmatrix} \frac{\gamma+1}{2} & \frac{\gamma+3}{2} & \frac{\gamma+5}{2} & \ldots & \frac{\gamma+\gamma-2}{2} & \frac{\gamma+\gamma}{2} & \ldots & \frac{3\gamma-1}{2} \\ \frac{3\gamma+1}{2} & \frac{3\gamma+3}{2} & \frac{3\gamma+5}{2} & \ldots & \frac{3\gamma+\gamma-2}{2} & \frac{3\gamma+\gamma}{2} & \ldots & \frac{5\gamma-1}{2} \\ \frac{5\gamma+1}{2} & \frac{5\gamma+3}{2} & \frac{5\gamma+5}{2} & \ldots & \frac{5\gamma+\gamma-2}{2} & \frac{5\gamma+\gamma}{2} & \ldots & \frac{7\gamma-1}{2} \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots & \ldots & \vdots \\ \frac{(2p-3)\gamma+1}{2} & \frac{(2p-3)\gamma+3}{2} & \frac{(2p-3)\gamma+5}{2} & \ldots & \frac{(2p-3)\gamma+\gamma-2}{2} & \frac{(2p-3)\gamma+\gamma}{2} & \ldots & \frac{(2p-3)\gamma+2\gamma-1}{2} \end{bmatrix}.$$

The following results hold:

$2q\left(\frac{(2p-3)\gamma+\gamma-2}{2}\right) \equiv 2q(\gamma(p-1)-1) \bmod (p^2-1)$.

$2q\left(\frac{(2p-3)\gamma+\gamma}{2}\right) \equiv 0 \bmod (p^2-1)$.

$2q\left(\frac{(2p-3)\gamma+2\gamma-1}{2}\right) \equiv 2q\left(\frac{\gamma-1}{2}\right) \bmod (p^2-1)$.

Now consider the sets $(l) = \{\zeta^{q\gamma(2k+1)+2ql+q+i} | k = 0, 1, 2, \ldots, p-2\}$, for $l = 0, 1, 2, \ldots, \gamma-1$.

$$\begin{aligned}(0) &= \{\zeta^{q\gamma(2k+1)+q+i} | k = 0, 1, 2, \ldots, p-2\} \\ &= \{\zeta^{q(\gamma+1)+i}, \zeta^{q(3\gamma+1)+i}, \zeta^{q(5\gamma+1)+i}, \ldots, \zeta^{q((2p-3)\gamma+1)+i}\}.\end{aligned}$$

It is clear that the entire set (0) is in $(i)_{2q}$ and the corresponding values of h in $(i)_{2q}$ are in the first column of the matrix h above.

$$\begin{aligned}(1) &= \{\zeta^{q\gamma(2k+1)+2q+q+i} | k = 0, 1, 2, \ldots, p-2\} \\ &= \{\zeta^{q(\gamma+3)+i}, \zeta^{q(3\gamma+3)+i}, \zeta^{q(5\gamma+3)+i}, \ldots, \zeta^{q((2p-3)\gamma+3)+i}\}.\end{aligned}$$

It is clear that this entire set is in $(i)_{2q}$ and the corresponding h values in $(i)_{2q}$ are in the second column of the matrix h above.
Continuing in this manner we have

$$\begin{aligned}(\gamma-1) &= \{\zeta^{q\gamma(2k+1)+2q(\gamma-1)+q+i} | k=0,1,2,\ldots,p-2\} \\ &= \{\zeta^{q(3\gamma-1)+i}, \zeta^{q(5\gamma-1)+i}, \zeta^{q(7\gamma-1)+i}, \ldots, \zeta^{q((2p-3)\gamma+2\gamma-1)+i}\}\end{aligned}$$

and it is also clear that the entire set $(\gamma-1)$ is in $(i)_{2q}$ and the corresponding values of h in $(i)_{2q}$ are in the last column of the matrix h above.

Thus it is clear that

$$(i)_{2q} = \bigcup_{l=0}^{\gamma-1}(l).$$

i.e., in the case of $\lambda = 2q$, for a fixed $i = 0,1,2,\ldots,2q-1$, the elements in the set $(i)_{2q}$ are completely listed in $\zeta^{\frac{p+1}{2}+2ql+q+i}$ columns of the matrix representation of $GF(p,2)^*$, where $l = 0,1,2,\ldots,\frac{p+1}{2q}-1$. □

The following example illustrates this result.

Example 5.2.13. *Let $q=2$ and $p=11$. It is clear that $11 \equiv (2\times 2-1) mod (4\times 2)$. (i.e., $11 \equiv 3 (mod\ 8)$). Let $\lambda = 2q = 4$. Then $\lambda|(p+1)$. (i.e. $4|12$). The set $(i)_4 = \{\zeta^{4h+i} \mid h = 0,1,2,\ldots,\frac{11^2-(4+1)}{4}\}$, where $i=0,1,2,3$.*

i.e.,

$(0)_4 = \{\zeta^{4h} \mid h = 0,1,2,\ldots,\frac{11^2-1}{4}-1 = 29\}$.

$(1)_4 = \{\zeta^{4h+1} \mid h = 0,1,2,\ldots,\frac{11^2-1}{4}-1 = 29\}$.

$(2)_4 = \{\zeta^{4h+2} \mid h = 0,1,2,\ldots,\frac{11^2-1}{4}-1 = 29\}$.

$(3)_4 = \{\zeta^{4h+3} \mid h = 0,1,2,\ldots,\frac{11^2-1}{4}-1 = 29\}$.

i.e.,

$(0)_4 = \{1, \zeta^4, \zeta^8, \zeta^{12}, \zeta^{16}, \zeta^{20}, \zeta^{24}, \zeta^{28}, \zeta^{32}, \zeta^{36}, \zeta^{40}, \zeta^{44}, \zeta^{48}, \zeta^{52}, \zeta^{56}, \ldots\}$.

$(1)_4 = \{\zeta, \zeta^5, \zeta^9, \zeta^{13}, \zeta^{17}, \zeta^{21}, \zeta^{25}, \zeta^{29}, \zeta^{33}, \zeta^{37}, \zeta^{41}, \zeta^{45}, \zeta^{49}, \zeta^{53}, \zeta^{57}, \ldots\}$.

$(2)_4 = \{\zeta^2, \zeta^6, \zeta^{10}, \zeta^{14}, \zeta^{18}, \zeta^{22}, \zeta^{26}, \zeta^{30}, \zeta^{34}, \zeta^{38}, \zeta^{42}, \zeta^{46}, \zeta^{50}, \zeta^{54}, \zeta^{58}, \ldots\}$.

$(3)_4 = \{\zeta^3, \zeta^7, \zeta^{11}, \zeta^{15}, \zeta^{19}, \zeta^{23}, \zeta^{27}, \zeta^{31}, \zeta^{35}, \zeta^{39}, \zeta^{43}, \zeta^{47}, \zeta^{51}, \zeta^{55}, \zeta^{59}, \ldots\}$.

The elements of $(i)_4$ *are completely listed in the columns indexed by* $\zeta^{6+4l+2+i} = \zeta^{8+4l+i}$ *in the matrix representation of* $GF(11,2)^*$*, where* $l = 0, 1, 2$ *and* $i = 0, 1, 2, 3$*. For example the elements of* $(0)_4$ *are in the columns indexed by* ζ^8*,* ζ^{12} *and* ζ^{16}*.*

$$GF(11,2)^* = \begin{bmatrix} \zeta^6 & \zeta^7 & \zeta^8 & \zeta^9 & \zeta^{10} & \zeta^{11} & \zeta^{12} & \zeta^{13} & \zeta^{14} & \zeta^{15} & \zeta^{16} & \zeta^{17} \\ \zeta^{18} & \zeta^{19} & \zeta^{20} & \zeta^{21} & \zeta^{22} & \zeta^{23} & \zeta^{24} & \zeta^{25} & \zeta^{26} & \zeta^{27} & \zeta^{28} & \zeta^{29} \\ \zeta^{30} & \zeta^{31} & \zeta^{32} & \zeta^{33} & \zeta^{34} & \zeta^{35} & \zeta^{36} & \zeta^{37} & \zeta^{38} & \zeta^{39} & \zeta^{40} & \zeta^{41} \\ \zeta^{42} & \zeta^{43} & \zeta^{44} & \zeta^{45} & \zeta^{46} & \zeta^{47} & \zeta^{48} & \zeta^{49} & \zeta^{50} & \zeta^{51} & \zeta^{52} & \zeta^{53} \\ \zeta^{54} & \zeta^{55} & \zeta^{56} & \zeta^{57} & \zeta^{58} & \zeta^{59} & \zeta^{60} & \zeta^{61} & \zeta^{62} & \zeta^{63} & \zeta^{64} & \zeta^{65} \\ \zeta^{66} & \zeta^{67} & \zeta^{68} & \zeta^{69} & \zeta^{70} & \zeta^{71} & \zeta^{72} & \zeta^{73} & \zeta^{74} & \zeta^{75} & \zeta^{76} & \zeta^{77} \\ \zeta^{78} & \zeta^{79} & \zeta^{80} & \zeta^{81} & \zeta^{82} & \zeta^{83} & \zeta^{84} & \zeta^{85} & \zeta^{86} & \zeta^{87} & \zeta^{88} & \zeta^{89} \\ \zeta^{90} & \zeta^{91} & \zeta^{92} & \zeta^{93} & \zeta^{94} & \zeta^{95} & \zeta^{96} & \zeta^{97} & \zeta^{98} & \zeta^{99} & \zeta^{100} & \zeta^{101} \\ \zeta^{102} & \zeta^{103} & \zeta^{104} & \zeta^{105} & \zeta^{106} & \zeta^{107} & \zeta^{108} & \zeta^{109} & \zeta^{110} & \zeta^{111} & \zeta^{112} & \zeta^{113} \\ \zeta^{114} & \zeta^{115} & \zeta^{116} & \zeta^{117} & \zeta^{118} & \zeta^{119} & 1 & \zeta & \zeta^2 & \zeta^3 & \zeta^4 & \zeta^5 \end{bmatrix}_{10\times 12}.$$

By completing the proof of the previous few lemmas and giving suitable examples, we have studied a nice relationship between the elements in the columns of the matrix representation of $GF(p,2)^*$ and the elements of $(i)_\lambda = \{\zeta^{\lambda h+i} | h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda} - 1\}$, for various values of λ. We are now in a position to study the distribution of $Tr(ax^\lambda)$ for various values of λ, where $2 < \lambda < p-1$ such that $\lambda|(p+1)$.

Theorem 5.2.14. *Let* $p > 3$ *be a prime and* $2 < \lambda < p-1$ *such that* $\lambda|(p+1)$*. Let* Tr *be the trace map over* $GF(p,2)$ *and* $a \in GF(p,2)^*$*.*
(i) If $\lambda = \frac{p+1}{2}$ *then as* x *ranges over* $GF(p,2)^*$*,* $Tr(ax^\lambda)$ *takes each element in* $\mathbb{Z}_p \setminus \{0\}$ *equally often either* $p-(\lambda-1)$ *times or* $p+1$ *times.*
(ii) If $\lambda = \frac{p+1}{2} = \lambda_1^{e_1}\lambda_2^{e_2}\ldots\lambda_u^{e_u}$ *then*
(a) for each λ_j*,* $j = 1, 2, \ldots, u$*, as* x *ranges over* $GF(p,2)^*$*,* $Tr(ax^{\lambda_j})$ *takes each element in* $\mathbb{Z}_p \setminus \{0\}$ *equally often either* $p-(\lambda_j-1)$ *times or* $p+1$ *times.*
(b) for each λ_j*,* $j = 1, 2, \ldots, u$*, as* x *ranges over* $GF(p,2)^*$*,* $Tr(ax^{\lambda_j^{e_j}})$ *takes each element in* $\mathbb{Z}_p \setminus \{0\}$ *equally often either* $p-(\lambda_j^{e_j}-1)$ *times or* $p+1$ *times.*
(iii) For $1 < q < \frac{p-1}{2}$*, if* $p \equiv (2q-1) mod(4q)$ *and* $\lambda = 2q$ *then as* x *ranges over* $GF(p,2)^*$*,*

$Tr(ax^\lambda)$ takes each element in $\mathbb{Z}_p \setminus \{0\}$ equally often either $p-(2q-1)$ times or $p+1$ times.

Proof:

From Lemma 5.2.2 we know that for a fixed $a \in GF(p,2)^*$ and for all $x \in GF(p,2)^*$ the set $\{ax^\lambda\}$ is given by λ copies of $(i)_\lambda = \{\zeta^{\lambda h+i} | h = 0,1,2,\ldots,\frac{p^2-1}{\lambda}-1\}$ or λ copies of cyclic shifts of $(i)_\lambda$, where $2 < \lambda < p-1$ such that $\lambda|(p+1)$ and $i = 0,1,2,\ldots,\lambda-1$.

(i) If $\lambda = \frac{p+1}{2}$ then from part (i) of Lemma 5.2.7 we know that the elements in the set $(i)_\lambda$ are from the $\zeta^{\frac{p+1}{2}+\lambda l+i}$ columns of the matrix representation of $GF(p,2)^*$, where $l = 0,1$. From Lemma 4.3.6 we know that the trace of each element of the first column of the matrix representation of $GF(p,2)^*$ (i.e., the column indexed by $\zeta^{\frac{p+1}{2}}$) is 0 and each of the other columns take each element in $\mathbb{Z}_p \setminus \{0\}$ exactly once. Therefore the trace of the elements in $(i)_\lambda$ contains each element in $\mathbb{Z}_p \setminus \{0\}$ equally often either 1 time (when $i = 0$) or 2 times (when $i \neq 0$). Since $\{ax^\lambda\}$ contains λ copies of $(i)_\lambda$, the trace of elements of $\{ax^\lambda\}$ takes each element in $\mathbb{Z}_p \setminus \{0\}$ equally often either λ times or 2λ times. Since $\lambda = \frac{p+1}{2}$, as x ranges over $GF(p,2)^*$, $Tr(ax^\lambda)$ takes each element in $\mathbb{Z}_p \setminus \{0\}$ equally often either $\frac{p+1}{2}$ times (i.e., $p-(\lambda-1)$) or $(p+1)$ times.

(ii) (a) If $\lambda = \frac{p+1}{2} = \lambda_1^{e_1}\lambda_2^{e_2}\ldots\lambda_u^{e_u}$ then from part (i) of Lemma 5.2.9 we know that the elements of $(i)_{\lambda_j}$ are from $\zeta^{\frac{p+1}{2}+\lambda_j l+i}$ columns of the matrix representation of $GF(p,2)^*$, where $j = 1,2,\ldots,u$ and $l = 0,1,2,\ldots,\frac{p+1}{\lambda_j}-1$. Again from Lemma 4.3.6 we know that the trace of the elements in the first column of the matrix representation of $GF(p,2)^*$ (i.e., the column $\zeta^{\frac{p+1}{2}}$) is 0 and all the other columns take each element in $\mathbb{Z}_p \setminus \{0\}$ exactly once. Therefore the trace of the elements of $(i)_{\lambda_j}$ contains each element in $\mathbb{Z}_p \setminus \{0\}$ equally often either $\frac{p+1}{\lambda_j}-1$ times or $\frac{p+1}{\lambda_j}$ times. Since $\{ax^{\lambda_j}\}$ contains λ_j copies of $(i)_{\lambda_j}$, the trace of elements of $\{ax^{\lambda_j}\}$ takes each element in $\mathbb{Z}_p \setminus \{0\}$ equally often either $\lambda_j\left(\frac{p+1}{\lambda_j}-1\right)$ times or $\lambda_j\left(\frac{p+1}{\lambda_j}\right)$ times. Thus as x ranges over $GF(p,2)^*$, $Tr(ax^{\lambda_j})$ takes each element in $\mathbb{Z}_p \setminus \{0\}$ equally often either $(p-(\lambda_j-1))$ times (when $i = 0$) or $(p+1)$ times (when $i \neq 0$).

(b) Similarly, from part (ii) of Lemma 5.2.9, we can prove that as x ranges over $GF(p,2)^*$,

$Tr(ax^{\lambda_j^{e_j}})$ takes each element in $\mathbb{Z}_p \setminus \{0\}$ equally often either $(p-(\lambda_j^{e_j}-1))$ times (when $i=0$) or $(p+1)$ times (when $i \neq 0$).

(iii) For $1 < q < \frac{p-1}{2}$, if $p \equiv (2q-1)\text{mod}(4q)$ and $\lambda = 2q$ then from Lemma 5.2.12 we know that for $i = 0, 1, 2, \ldots, 2q-1$, the elements of $(i)_{2q}$ are completely from the $\zeta^{\frac{p+1}{2}+2ql+q+i}$ columns of the matrix representation of $GF(p,2)^*$, where $i = 0, 1, 2, \ldots, 2q-1$ and $l = 0, 1, 2, \ldots, \frac{p+1}{2q} - 1$. Again from Lemma 4.3.6 we know that the trace of the elements of the first column of the matrix representation of $GF(p,2)^*$ (i.e., the column $\zeta^{\frac{p+1}{2}}$) is 0 and all the other columns take each element in $\mathbb{Z}_p \setminus \{0\}$ exactly once. Therefore the trace of the elements of $(i)_{2q}$ contains each element in $\mathbb{Z}_p \setminus \{0\}$ equally often either $\frac{p+1}{2q} - 1$ times or $\frac{p+1}{2q}$ times. Since $\{ax^{2q}\}$ contains $2q$ copies of $(i)_{2q}$, the trace of elements of $\{ax^{2q}\}$ takes each element in $\mathbb{Z}_p \setminus \{0\}$ equally often either $2q\left(\frac{p+1}{2q} - 1\right)$ times (when $i = q$) or $2q\left(\frac{p+1}{2q}\right)$ times (when $i \neq q$). Thus as x ranges over $GF(p,2)^*$, $Tr(ax^{2q})$ takes each element in $\mathbb{Z}_p \setminus \{0\}$ equally often either $(p-(2q-1))$ times or $(p+1)$ times. □

So far we have studied, for different values of λ, the distribution of $Tr(ax^\lambda)$. We will apply this in the next section to construct two-weight, self-orthogonal codes over $\mathbb{Z}_p$.

5.3 Code construction from $\mathbf{Tr(ax^\lambda)}$

From Theorem 5.2.14 we studied, for various values of λ, as x ranges over $GF(p,2)$, the distribution of $Tr(ax^\lambda)$, for $a \in GF(p,2)$.We are now in a position to use this in the next theorem to construct two-dimensional, two-weight, self-orthogonal codes over $\mathbb{Z}_p$ for $p > 3$.

Theorem 5.3.1. *Let $p > 3$ be a prime and $2 < \lambda < p-1$ such that $\lambda|(p+1)$.*
(i) If $\lambda = \frac{p+1}{2}$ then the rows of the matrix $H_\lambda = [Tr(ax^\lambda)]_{a,x \in GF(p,2)}$ form a two-dimensional, two-weight, self-orthogonal code over $\mathbb{Z}_p$ with the parameters $[p^2, 2, (p-(\lambda-1))(p-1)]$.
(ii) If $\lambda = \frac{p+1}{2} = \lambda_1^{e_1}\lambda_2^{e_2}\ldots\lambda_u^{e_u}$ then
(a) the rows of the matrix $H_{\lambda_j} = [Tr(ax^{\lambda_j})]_{a,x \in GF(p,2)}$ form a two-dimensional, two-weight, self-orthogonal code over $\mathbb{Z}_p$ with the parameters $[p^2, 2, (p-(\lambda_j-1))(p-1)]$,

where $j = 1, 2, \ldots, u$.

(b) the rows of the matrix $H_{\lambda_j^{e_j}} = [Tr(ax^{\lambda_j^{e_j}})]_{a,x \in GF(p,2)}$ *form a two-dimensional, two-weight, self-orthogonal code over* $\mathbb{Z}_p$ *with the parameters* $[p^2, 2, (p - (\lambda_j^{e_j} - 1))(p - 1)]$ *, where* $j = 1, 2, \ldots, u$.

(iii) For $1 < q < \frac{p-1}{2}$*, if* $p \equiv (2q - 1)(mod 4q)$ *and* $\lambda = 2q$ *then the rows of the matrix* $H_\lambda = [Tr(ax^\lambda)]_{a,x \in GF(p,2)}$ *form a two-dimensional, two-weight, self-orthogonal code over* $\mathbb{Z}_p$ *with the parameters* $[p^2, 2, (p - (2q - 1))(p - 1)]$.

Proof:

Let

$$G_{H_\lambda} = \begin{bmatrix} Tr(c_i^\lambda), & i = 1, 2, \ldots, p^2 \\ Tr(\zeta c_i^\lambda), & i = 1, 2, \ldots, p^2 \end{bmatrix}_{2 \times p^2}.$$

Firstly the two rows of the matrix G_{H_λ} are linearly independent. Let any $a_0, a_1 \in \mathbb{Z}_p$ and suppose that, for all $i = 1, 2, \ldots, p^2$, $a_0 Tr(c_i^\lambda) + a_1 Tr(\zeta c_i^\lambda) = 0$. From the properties of the trace map of Theorem 4.3.2, for all $i = 1, 2, \ldots, p^2$, we have $Tr((a_0 + a_1\zeta)c_i^\lambda) = 0$. According to the distribution of the trace values over $\mathbb{Z}_p$ this implies that $(a_0 + a_1\zeta)c_i^\lambda = 0$, for all $i = 1, 2, \ldots, p^2$. However, $c_i^\lambda \neq 0$ for at least one $1 \leq i \leq p^2$ and hence $a_0 + a_1\zeta = 0$. Since 1 and ζ represent linearly independent 2-tuples over $\mathbb{Z}_p$, a_0 and a_1 should be 0. Therefore two rows in G_{H_λ} are linearly independent.

Now consider all the linear combinations of two rows of G_{H_λ}. For $i = 1, 2, \ldots, p^2$ these linear combinations are given by $a_0 Tr(c_i^\lambda) + a_1 Tr(\zeta c_i^\lambda) = Tr((a_0 + a_1\zeta)c_i^\lambda)$. This implies that the rows of the matrix H_λ can be generated by the rows of G_{H_λ}. Thus G_{H_λ} is a generator matrix of H_λ and therefore the length n and the dimension k of the code H_λ are p^2 and 2 respectively. Therefore H_λ is a two-dimensional linear code over $\mathbb{Z}_p$.

(i) From part (i) of Theorem 5.2.14, when $\lambda = \frac{p+1}{2}$, every non-zero row of the matrix $H_\lambda = [Tr(ax^\lambda)]_{a,x \in GF(p,2)}$ has every element in $\mathbb{Z}_p \setminus \{0\}$ equally often either $p - (\lambda - 1)$ times or $p + 1$ times. Since there are $p - 1$ elements in $\mathbb{Z}_p \setminus \{0\}$, the Hamming weights of the codewords of H_λ are $(p - (\lambda - 1))(p - 1)$ and $p^2 - 1$. Therefore H_λ is a two-weight code. The minimum Hamming weight of H_λ is $(p - (\lambda - 1))(p - 1)$. Therefore $H_\lambda = [Tr(ax^\lambda)]_{a,x \in GF(p,2)}$ is a $[p^2, 2, (p - (\frac{p+1}{2} - 1))(p - 1)]$ code over $\mathbb{Z}_p$.

(ii) (a) From part (ii) (a) of Theorem 5.2.14, when $\lambda = \frac{p+1}{2} = \lambda_1^{e_1}\lambda_2^{e_2}\ldots\lambda_u^{e_u}$, every non-zero row of $H_{\lambda_j} = [Tr(ax^{\lambda_j})]_{a,x\in GF(p,2)}$ has every element in $\mathbb{Z}_p \setminus \{0\}$ equally often either $p-(\lambda_j-1)$ times or $(p+1)$ times. Since there are $(p-1)$ elements in $\mathbb{Z}_p \setminus \{0\}$, the Hamming weights of codewords of H_{λ_j} are $(p-(\lambda_j-1))(p-1)$ and p^2-1. Therefore H_{λ_j} is a two-weight code. The minimum Hamming weight of codewords of H_{λ_j} is $(p-(\lambda_j-1))(p-1)$. Therefore $H_{\lambda_j} = [Tr(ax^{\lambda_j})]_{a,x\in GF(p,2)}$ is a $[p^2, 2, (p-(\lambda_j-1))(p-1)]$ code over $\mathbb{Z}_p$, where $j = 1, 2, \ldots, u$.
(b) Similarly from part (ii) (b) of Theorem 5.2.14 we can show that $H_{\lambda_j^{e_j}} = [Tr(ax^{\lambda_j^{e_j}})]_{a,x\in GF(p,2)}$ is a two-weight code with the parameters $[p^2, 2, (p-(\lambda_j^{e_j}-1))(p-1)]$ over $\mathbb{Z}_p$, where $j = 1, 2, \ldots, u$.

(iii) From part (iii) of Theorem 5.2.14, for $1 < q < \frac{p-1}{2}$, if $p \equiv (2q-1)\text{mod}(4q)$ and $\lambda = 2q$ then every non-zero row of $H_\lambda = [Tr(ax^\lambda)]_{a,x\in GF(p,2)}$ has every element in $\mathbb{Z}_p \setminus \{0\}$ equally often either $p-(2q-1)$ times or $(p+1)$ times. Since there are $(p-1)$ elements in $\mathbb{Z}_p \setminus \{0\}$, the Hamming weights of codewords of H_λ are $(p-(2q-1))(p-1)$ and (p^2-1). Therefore H_λ is a two-weight code. The minimum Hamming weight of codewords of H_λ is $(p-(2q-1))(p-1)$. Therefore $H_\lambda = [Tr(ax^\lambda)]_{a,x\in GF(p,2)}$ is a $[p^2, 2, (p-(2q-1))(p-1)]$ code over $\mathbb{Z}_p$.
Finally the dot product of each codeword of the above codes with itself is either

$$\begin{aligned} S &= (p+1)\sum_{i=1}^{p-1} i^2 \\ &= \frac{p}{6}(p+1)(2p^2-3p+1) \end{aligned}$$

or

$$\begin{aligned} S &= (p-(\lambda-1))\sum_{i=1}^{p-1} i^2 \\ &= \frac{p}{6}(p-(\lambda-1))(2p^2-3p+1). \end{aligned}$$

Since $p > 3$ we have $S \equiv 0 \bmod p$. From Theorem 4.2.5 we know that a linear code over $\mathbb{Z}_p$, for $p > 2$, is self-orthogonal if and only if the dot product of each codeword with itself

is zero. Therefore all the above codes are self-orthogonal codes over $\mathbb{Z}_p$ for $p > 3$. □

Corollary 5.3.2. *Let H_λ^* be the code that can be obtained by deleting the first column of the matrix H_λ of Theorem 5.3.1. H_λ^* is a $[p^2-1, 2, (p-(\lambda-1))(p-1)]$ code and the codewords of H_λ^* are the left-cyclic shifts of the first λ non-initial rows of H_λ^*.*

Proof:

Let $A_\lambda^* = [ax^\lambda]_{a,x\in GF(p,2)^*}$. From Lemma 5.2.2 we know that the first λ rows of A_λ^* are given by λ copies of $(i)_\lambda$, where $(i)_\lambda = \{\zeta^{\lambda h+i} \mid h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda}-1\}$ and $i = 0, 1, 2, \ldots, \lambda-1$. The next λ rows of A_λ^* are given by λ copies of one cyclic shift of $(i)_\lambda$ and in this manner the last λ rows of A_λ^* are given by λ copies of $\frac{p^2-1}{\lambda} - 1$ cyclic shifts of $(i)_\lambda$. Thus the codewords of H_λ^* that can be obtained by deleting the first column of the matrix $H_\lambda = [Tr(ax^\lambda)]_{a,x\in GF(p,2)}$ are the left-cyclic shifts of the first λ non-initial rows of H_λ^*. From Theorem 5.3.1 the parameters of H_λ^* are $[p^2-1, 2, (p-(\lambda-1))(p-1)]$. Indeed H_λ^* is a cyclic code. □

The following example illustrates the case $\lambda = \frac{p+1}{2}$ of Theorem 5.3.1.

Example 5.3.3. *Let $p = 5$ and $\lambda = 3$. Then $\lambda|(p+1)$ and $2 < \lambda < p-1$. Consider the primitive polynomial $p(x) = x^2 + x + 2$ over $\mathbb{Z}_5$ and let ζ be a root of $p(x)$. Then $\zeta^2 = 4\zeta + 3$ and the elements of $GF(5,2) = \mathbb{Z}_5[x]/(p(x)) = \mathbb{Z}_5[\zeta]$ can be written as $\{0, 1, \zeta, \zeta^2, \ldots, \zeta^{23}\}$. The following table provides us the trace values of these elements and the trace values of their third powers.*

Element x	$x = a_1\zeta + a_0$	$Tr(x)$	x^3	$Tr(x^3)$
0	$0\zeta + 0$	0	0	0
1	$0\zeta + 1$	2	1	2
ζ	$1\zeta + 0$	4	ζ^3	0
ζ^2	$4\zeta + 3$	2	ζ^6	4
ζ^3	$4\zeta + 2$	0	ζ^9	0
ζ^4	$3\zeta + 2$	1	ζ^{12}	3
ζ^5	$4\zeta + 4$	4	ζ^{15}	0
ζ^6	$0\zeta + 2$	4	ζ^{18}	1
ζ^7	$2\zeta + 0$	3	ζ^{21}	0
ζ^8	$3\zeta + 1$	4	1	2
ζ^9	$3\zeta + 4$	0	ζ^3	0
ζ^{10}	$1\zeta + 4$	2	ζ^6	4
ζ^{11}	$3\zeta + 3$	3	ζ^9	0
ζ^{12}	$0\zeta + 4$	3	ζ^{12}	3
ζ^{13}	$4\zeta + 0$	1	ζ^{15}	0
ζ^{14}	$1\zeta + 2$	3	ζ^{18}	1
ζ^{15}	$1\zeta + 3$	0	ζ^{21}	0
ζ^{16}	$2\zeta + 3$	4	1	2
ζ^{17}	$1\zeta + 1$	1	ζ^3	0
ζ^{18}	$0\zeta + 3$	1	ζ^6	4
ζ^{19}	$3\zeta + 0$	2	ζ^9	0
ζ^{20}	$2\zeta + 4$	1	ζ^{12}	3
ζ^{21}	$2\zeta + 1$	0	ζ^{15}	0
ζ^{22}	$4\zeta + 1$	3	ζ^{18}	1
ζ^{23}	$2\zeta + 2$	2	ζ^{21}	0

By taking $a, x \in GF(5,2) = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{23}\}$, *the matrix* $A_3 = [(ax^3)]_{a,x \in GF(5,2)}$ *is given by*

$$A_3 = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \dots & \zeta^{21} \\
0 & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \dots & \zeta^{22} \\
0 & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \dots & \zeta^{23} \\
0 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \dots & \zeta^{21} & 1 \\
0 & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \dots & \zeta^{22} & \zeta \\
0 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \dots & \zeta^{23} & \zeta^2 \\
0 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \dots & \zeta^{21} & 1 & \zeta^3 \\
0 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \dots & \zeta^{22} & \zeta & \zeta^4 \\
0 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \dots & \zeta^{23} & \zeta^2 & \zeta^5 \\
0 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \dots & \zeta^{21} & 1 & \zeta^3 & \zeta^6 \\
0 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \dots & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 \\
0 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \dots & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 \\
0 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \dots & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 \\
0 & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \dots & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} \\
0 & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \dots & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} \\
0 & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \dots & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} \\
0 & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \dots & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} \\
0 & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \dots & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} \\
0 & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \dots & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} \\
0 & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \dots & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} \\
0 & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \dots & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} \\
0 & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} & \zeta^{21} & 1 & \zeta^3 & \dots & \zeta^{21} & 1 & \zeta^3 & \zeta^6 & \zeta^9 & \zeta^{12} & \zeta^{15} & \zeta^{18} \\
0 & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} & \zeta^{22} & \zeta & \zeta^4 & \dots & \zeta^{22} & \zeta & \zeta^4 & \zeta^7 & \zeta^{10} & \zeta^{13} & \zeta^{16} & \zeta^{19} \\
0 & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20} & \zeta^{23} & \zeta^2 & \zeta^5 & \dots & \zeta^{23} & \zeta^2 & \zeta^5 & \zeta^8 & \zeta^{11} & \zeta^{14} & \zeta^{17} & \zeta^{20}
\end{bmatrix}_{25\times 25}.$$

The matrix $H_3 = [Tr(ax^3)]_{a,x\in GF(5,2)}$ *is given by*

$$H_3=\begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0\\
0&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3\\
0&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2\\
0&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2\\
0&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4\\
0&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2\\
0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0\\
0&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1\\
0&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4\\
0&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4\\
0&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3\\
0&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4\\
0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0\\
0&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2\\
0&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3\\
0&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3\\
0&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1\\
0&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3\\
0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0\\
0&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4\\
0&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1\\
0&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1\\
0&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2\\
0&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1
\end{bmatrix}_{25\times 25}.$$

The rows of H_3 can be generated by

$$G_{H_3}=\begin{bmatrix}
0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0\\
0&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3
\end{bmatrix}_{2\times 25}.$$

By deleting the first column of the matrix H_3 we obtain:

$$H_3^* = \begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0\\
4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3\\
2&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2\\
0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2\\
1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4\\
4&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2\\
4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0\\
3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1\\
4&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4\\
0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4\\
2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3\\
3&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4\\
3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0\\
1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2\\
3&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3\\
0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3\\
4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1\\
1&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3\\
1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0\\
2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4\\
1&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1\\
0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1&0&2&0&4&0&3&0&1\\
3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2&3&4&1&3&2&1&4&2\\
2&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1&2&2&4&4&3&3&1&1
\end{bmatrix}_{25\times 24}.$$

Therefore H_3 is a linear code over $\mathbb{Z}_5$ and its parameters are $[25, 2, 12]$. The punctured code H_3^*, obtained by deleting the first column of H_3 is a $[24, 2, 12]$ cyclic code over $\mathbb{Z}_5$. Indeed H_3^* is a cyclic code. The Hamming weight of each non-zero codeword of H_3 is either 12 or 24. Thus H_3 is a two-weight code. From Theorem 5.3.1, H_3 is a self-orthogonal code.

Throughout this chapter, for various values of $\lambda > 2$ such that $\lambda|(p+1)$, we have studied the use of the properties of the trace map over $GF(p,2)$ in the form of $Tr(ax^{\lambda})$ and used them to construct two-dimensional, two-weight, cyclic, self-orthogonal codes over $\mathbb{Z}_p$. The next question is whether we can apply the trace map over $GF(p,2)$ in similar manner for $\lambda|(p-1)$. We devote the next chapter to study this case.

Chapter 6

Two-Weight and Constant-Weight Codes from $\mathbf{Tr(ax^{\lambda})}$

6.1 Introduction

In Chapters 4 and 5 we have individually studied the use of the trace map over the Galois field $GF(p,2)$ in the from of $Tr(ax^2)$ and $Tr(ax^{\lambda})$ respectively. In Chapter 5 we have considered the case $\lambda|(p+1)$ and constructed two-weight, self-orthogonal codes over $\mathbb{Z}_p$ by using the trace map in the form of $Tr(ax^{\lambda})$. The main reason to consider the case $\lambda|(p+1)$ was that the number of invertible elements of the Galois field $GF(p,2)$, i.e., p^2-1, needed to be divisible by λ. Since $p^2-1=(p-1)(p+1)$, we need to also study the case when $\lambda|(p-1)$. Experimental results have provided us, when $\lambda > 2$ - even and $\lambda|(p-1)$, with the code $H_{\lambda}=[Tr(ax^{\lambda})]_{a,x\in GF(p,2)}$ a two-weight code over $\mathbb{Z}_p$ with the parameters $[p^2,2,(p-1)^2]$. These parameters are the same as that of the code $H_2=[Tr(ax^2)]_{a,x\in GF(p,2)}$ that we have constructed in Chapter 4. Experimental results have also provided us, when $\lambda > 2$-odd and $\lambda|(p-1)$, with the code $H_{\lambda}=[Tr(ax^{\lambda})]_{a,x\in GF(p,2)}$, a constant-weight code over $\mathbb{Z}_p$ with the parameters $[p^2,2,p(p-1)]$ and these parameters are the same as that of the code $H=[Tr(ax)]_{a,x\in GF(p,2)}$ that we have constructed in [65]. The equality of parameters with already constructed codes and the experimental results motivate us to study the case $\lambda|(p-1)$.

In Section 6.2 we study the case $\lambda > 2$-even such that $\lambda|(p-1)$ for both $p \equiv 1(\text{mod } 4)$

and $p \equiv 3(\text{mod } 4)$. We will prove that the code $H_\lambda = [Tr(ax^\lambda)]_{a,x \in GF(p,2)}$ is a two-weight code over $\mathbb{Z}_p$ with the parameters $[p^2, 2, (p-1)^2]$. Section 6.4 is devoted to the study of the case $\lambda >$ 2-odd such that $\lambda|(p-1)$ for both $p \equiv 1(\text{ mod } 4)$ and $p \equiv 3(\text{mod } 4)$. In this case we will prove that the code $H_\lambda = [Tr(ax^\lambda)]_{a,x \in GF(p,2)}$ is a constant-weight code over $\mathbb{Z}_p$ with the parameters $[p^2, 2, p(p-1)]$.

6.2 Two-weight codes from $\mathbf{Tr(ax^\lambda)}$ when $\lambda >$ 2-even

The codes that we constructed in Chapters 4 and 5 are totally dependent on the properties of the trace map over the Galois field $GF(p,2)$. In this section we recall Theorem 4.3.3 that was used to identify the elements of the Galois field that have trace zero. We know that these elements are $\Psi = \{\zeta^{\frac{(p+1)}{2}(2k+1)} | k = 0, 1, 2, \ldots, p-2\}$, where ζ is a primitive element of $GF(p,2)$. As usual first we need to study, for $a \in GF(p,2)$, the distribution of $Tr(ax^\lambda)$ by changing x over $GF(p,2)$. From Theorem 4.3.8 of Chapter 4, $Tr(ax^2)$ takes each element in $\mathbb{Z}_p \setminus \{0\}$ equally often either $p+1$ times or $p-1$ times and from Theorem 5.2.14 of Chapter 5, for different values of λ, $Tr(ax^\lambda)$ takes each element in $\mathbb{Z}_p \setminus \{0\}$ equally often either $p-(\lambda-1)$ times or $p+1$ times.

The next couple of lemmas study the distribution of elements of $\Psi = \{\zeta^{\frac{(p+1)}{2}(2k+1)} | k = 0, 1, 2, \ldots, p-2\}$ in each row of $A = [ax^\lambda]_{a,x \in GF(p,2)^*}$. Firstly we consider the case $\lambda >$ 2-even and $\lambda|(p-1)$ for $p \equiv 3(\text{mod } 4)$. We can readily check that the minimum value of such a prime p is 19.

Lemma 6.2.1. *Let $p \geq 19$ be a prime such that $p \equiv 3(mod\ 4)$ (i.e., $\frac{p+1}{2}$-even) and $\lambda >$ 2-even such that $\lambda|(p-1)$. Let $(i)_\lambda = \{\zeta^{\lambda h+i} | h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda} - 1\}$, where $i = 0, 1, 2, \ldots, \lambda-1$. Let $\Psi = \{\zeta^{\frac{(p+1)}{2}(2k+1)} | k = 0, 1, 2, \ldots, p-2\}$ and $(s) = \{\zeta^{(\frac{p+1}{2})(2s+1+\lambda j)} | j = 0, 1, 2, \ldots, \frac{2(p-1)}{\lambda} - 1\}$, where $0 \leq s \leq \frac{\lambda}{2} - 1$. Then*
(i) For all $s = 0, 1, 2, \ldots, \frac{\lambda}{2} - 1$, $(s) \subset \Psi$.
(ii) $\Psi = \dot{\bigcup}(s)$.
(iii) For each s, there exists an even i such that $(s) \subset (i)_\lambda$.

Proof:

From Lemma 5.2.4 the set Ψ gives the trace zero elements of $GF(p,2)^*$.

(i) Let any $\alpha \in (s)$. Then $\alpha = \zeta^{\frac{(p+1)}{2}(2s+1+\lambda j)}$. Since $\lambda > 2$ is even we have $2s+1+\lambda j$ is odd and therefore $2s+1+\lambda j$ can be written as $2k_1+1$ for $k_1 = s + \frac{\lambda}{2}j$. Thus $\alpha \in \Psi$ and hence $(s) \subset \Psi$.

(ii) Now let $\alpha \in \Psi$. Then $\alpha = \zeta^{\frac{(p+1)}{2}(2k+1)}$. Since $\lambda >$ 2-even $\Rightarrow \frac{\lambda}{2}$ is an integer. Since $0 \leq k \leq p-2$, by division algorithm we can write $k = \frac{\lambda}{2}j + s$ for some $j = 0, 1, 2, \ldots, \frac{2(p-1)}{\lambda} - 1$ and $s = 0, 1, 2, \ldots, \frac{\lambda}{2} - 1$. Therefore $\alpha \in (s)$ and since (s) are disjoint sets it is clear that $\Psi = \dot{\bigcup}(s)$.

(iii) Let $\alpha \in (s)$. Then $\alpha = \zeta^{\frac{(p+1)}{2}(2s+1+\lambda j)}$. To prove that $\zeta^{\frac{(p+1)}{2}(2s+1+\lambda j)} \in (i)_\lambda$ for all j, we need to prove that $\frac{p+1}{2}(2s+1+\lambda j) \equiv i (\text{mod } \lambda)$. That is we need to prove that $\frac{p+1}{2}(2s+1+\lambda j)$ is in the same equivalence class mod λ for all j. In another words we need to prove that $\left(\frac{p+1}{2}\right)(2s+1) + \left(\frac{p+1}{2}\right)\lambda j$ is in the same equivalence class mod λ for all j. Since $\left(\frac{p+1}{2}\right)\lambda j \equiv 0 (\text{mod } \lambda)$, we have $\left(\frac{p+1}{2}\right)(2s+1)$ is in the same equivalence class mod λ for all j. Therefore $\frac{p+1}{2}(2s+1+\lambda j)$ is in the same equivalence class mod λ for all j. i.e., in the equivalence class of $\frac{p+1}{2}(2s+1)$ when $j = 0$. Therefore $(s) \subset (i)_\lambda$ for $i \equiv \left(\frac{p+1}{2}\right)(2s+1)$ mod λ. Since λ and $\left(\frac{p+1}{2}\right)$ are even it is clear that i is even. □

Consider the following example to illustrate this result.

Example 6.2.2. *Let $p = 19$ and $\lambda = 6$. Then $\frac{p+1}{2} = 10$-even and $\lambda|(p-1)$. The sets $\Psi = \{\zeta^{10(2k+1)} | k = 0, 1, 2, \ldots, 17\}$, $(i)_6 = \{\zeta^{6h+i} | h = 0, 1, 2, \ldots, 59\}$ and $(s) = \{\zeta^{10(2s+1+6j)} | j = 0, 1, 2, 3, 4, 5\}$, where $i = 0, 1, 2, \ldots, 5$ and $s = 0, 1, 2$. Now look at the full set (s) for each s.*

$(0) = \{\zeta^{10}, \zeta^{70}, \zeta^{130}, \zeta^{190}, \zeta^{250}, \zeta^{310}\}$.

$(1) = \{\zeta^{30}, \zeta^{90}, \zeta^{150}, \zeta^{210}, \zeta^{270}, \zeta^{330}\}$.

$(2) = \{\zeta^{50}, \zeta^{110}, \zeta^{170}, \zeta^{230}, \zeta^{290}, \zeta^{350}\}$.

It is clear that all the elements of Ψ are in the above three sets.

Similarly consider the complete set of $(i)_6$ for $i = 0, 1, 2, 3, 4, 5$ given below.

$(0)_6 = \{1, \zeta^6, \zeta^{12}, \zeta^{18}, \zeta^{24}, \zeta^{30}, \zeta^{36}, \zeta^{42}, \zeta^{48}, \zeta^{54}, \zeta^{60}, \zeta^{66}, \zeta^{72}, \zeta^{78}, \zeta^{84}, \zeta^{90}, \zeta^{96}, \zeta^{102}, \zeta^{108}, \zeta^{114}, \ldots\}$.

$(1)_6 = \{\zeta, \zeta^7, \zeta^{13}, \zeta^{19}, \zeta^{25}, \zeta^{31}, \zeta^{37}, \zeta^{43}, \zeta^{49}, \zeta^{55}, \zeta^{61}, \zeta^{67}, \zeta^{73}, \zeta^{79}, \zeta^{85}, \zeta^{91}, \zeta^{97}, \zeta^{103}, \zeta^{109}, \zeta^{115}, \ldots\}$.

$(2)_6 = \{\zeta^2, \zeta^8, \zeta^{14}, \zeta^{20}, \zeta^{26}, \zeta^{32}, \zeta^{38}, \zeta^{44}, \zeta^{50}, \zeta^{56}, \zeta^{62}, \zeta^{68}, \zeta^{74}, \zeta^{80}, \zeta^{86}, \zeta^{92}, \zeta^{98}, \zeta^{104}, \zeta^{110}, \zeta^{116}, \ldots\}$.

$(3)_6 = \{\zeta^3, \zeta^8, \zeta^{15}, \zeta^{21}, \zeta^{27}, \zeta^{33}, \zeta^{39}, \zeta^{45}, \zeta^{51}, \zeta^{57}, \zeta^{63}, \zeta^{69}, \zeta^{75}, \zeta^{81}, \zeta^{87}, \zeta^{93}, \zeta^{99}, \zeta^{105}, \zeta^{111}, \zeta^{117}, \ldots\}$.

$(4)_6 = \{\zeta^4, \zeta^{10}, \zeta^{16}, \zeta^{22}, \zeta^{28}, \zeta^{34}, \zeta^{40}, \zeta^{46}, \zeta^{52}, \zeta^{58}, \zeta^{64}, \zeta^{70}, \zeta^{76}, \zeta^{82}, \zeta^{88}, \zeta^{94}, \zeta^{100}, \zeta^{106}, \zeta^{112}, \zeta^{118}, \ldots\}$.
$(5)_6 = \{\zeta^5, \zeta^{11}, \zeta^{17}, \zeta^{23}, \zeta^{29}, \zeta^{35}, \zeta^{41}, \zeta^{47}, \zeta^{53}, \zeta^{59}, \zeta^{65}, \zeta^{71}, \zeta^{77}, \zeta^{83}, \zeta^{89}, \zeta^{95}, \zeta^{101}, \zeta^{107}, \zeta^{113}, \zeta^{119}, \ldots\}$.

It is clear that the elements of the sets $(0), (1)$ *and* (2) *are completely listed in the sets* $(4)_6, (0)_6$ *and* $(2)_6$ *respectively. i.e., for each* $0 \leq s \leq 2$ *there exists an even* i, $0 \leq i \leq 5$ *such that* $(s) \subset (i)_\lambda$. *For example, when* $s = 0$, $\left(\frac{p+1}{2}\right)(2s+1) = \frac{p+1}{2} = 10 \equiv 4 (mod\ \lambda)$. *i.e.,* $(0) \subset (4)_6$.

We are now in a position to study the distribution of elements of $\Psi = \{\zeta^{(\frac{p+1}{2})(2k+1)} | k = 0, 1, 2, \ldots, p-2\}$ in each row of $A_\lambda = [ax^\lambda]_{a,x \in GF(p,2)^*}$. Let $a = \zeta^{t_0}$ and $x = \zeta^{t_1}$, where $0 \leq t_0, t_1 \leq p^2 - 1$. Then elements of any given row of A can be written as $\{\zeta^{t_0 + \lambda t_1} | t_1 = 0, 1, 2, \ldots, p^2 - 1\}$. Since λ is even, the powers of ζ in any given row of A are either odd or even. Therefore we label the rows of A as odd and even rows respectively.

Lemma 6.2.3. *Let* $p \geq 19$ *be a prime such that* $p \equiv 3 (mod\ 4)$ *(i.e.,*$\frac{p+1}{2}$*-even). Let* $\lambda > 2$*-even and* $\lambda | (p-1)$. *Let* $(i)_\lambda = \{\zeta^{\lambda h + i} | h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda} - 1\}$, *where* $i = 0, 1, 2, \ldots, \lambda - 1$, $\Psi = \{\zeta^{(\frac{p+1}{2})(2k+1)} | k = 0, 1, 2, \ldots, p-2\}$ *and* $A_\lambda = [ax^\lambda]_{a,x \in GF(p,2)^*}$. *Then every even row of* A_λ *has* $2(p-1)$ *elements from the set* Ψ *and no elements of* Ψ *occur in the odd rows of* A_λ.

Proof:

From Lemma 6.2.1 we know that the elements of Ψ are equally distributed over $(0)_\lambda, (2)_\lambda, (4)_\lambda, \ldots, (\lambda - 2)_\lambda$ giving $\frac{2(p-1)}{\lambda}$ elements per set. All the other sets $(i)_\lambda$ have no elements from the set Ψ. From Lemma 5.2.2 we know that each row of A_λ contains λ-copies of $(i)_\lambda$ or λ-copies of a cyclic shift of $(i)_\lambda$ for some $i = 0, 1, 2, \ldots, \lambda - 1$. Therefore each even row of A_λ contains $2(p-1)$ elements from the set Ψ and the odd rows of A_λ have no elements from Ψ. □

Thus far we have studied the distribution of elements of Ψ over the rows of $A_\lambda = [ax^\lambda]_{a,x \in GF(p,2)^*}$. In the next theorem we will apply this property to construct two-dimensional, two-weight codes over $\mathbb{Z}_p$.

Theorem 6.2.4. *Let* $p \geq 19$ *be a prime such that* $p \equiv 3 (mod\ 4)$*(i.e.,* $\frac{p+1}{2}$*-even). Let* $\lambda > 2$*-even and* $\lambda | (p-1)$. *Let* Tr *be the trace map over the Galois field* $GF(p, 2)$. *The*

code $H_\lambda = [Tr(ax^\lambda)]_{a,x\in GF(p,2)}$ *is a two-dimensional, two-weight code over* $\mathbb{Z}_p$ *with the parameters* $[p^2, 2, (p-1)^2]$.

Proof:

Consider the matrix

$$G_{H_\lambda} = \begin{bmatrix} Tr(c_i^\lambda), & i = 1, 2, \ldots, p^2 \\ Tr(\zeta c_i^\lambda), & i = 1, 2, \ldots, p^2 \end{bmatrix}_{2\times p^2},$$

where $c_i^\lambda \in GF(p,2)$ and ζ is a primitive element of $GF(p,2)$.

For any $a_0, a_1 \in \mathbb{Z}_p$, suppose that $a_0 Tr(c_i^\lambda) + a_1 Tr(\zeta c_i^\lambda) = 0$, for all $i = 1, 2, \ldots, p^2$. From the properties of the trace map, $\Rightarrow Tr((a_0 + a_1\zeta)c_i^\lambda) = 0$, for all $i = 1, 2, \ldots, p^2$. From the distribution of the trace values over $\mathbb{Z}_p$, this implies that $(a_0 + a_1\zeta)c_i^\lambda = 0$, for all $i = 1, 2, \ldots, p^2$. Since $c_i^\lambda \neq 0$, for at least one i, $i = 1, 2, \ldots, p^2$, we have $a_0 + a_1\zeta = 0$. Since 1 and ζ represent linearly independent 2-tuples over $\mathbb{Z}_p$, a_0 and a_1 should be 0. Therefore the rows of G_{H_λ} are linearly independent.

Now consider all the linear combinations of rows of G_{H_λ}. i.e., for all $i = 1, 2, \ldots, p^2$, we have $a_0 Tr(c_i^\lambda) + a_1 Tr(\zeta c_i^\lambda) = Tr((a_0 + a_1\zeta)c_i^\lambda)$. This implies that the rows of H can be generated by the rows of G_{H_λ}. Thus G_{H_λ} is a generator matrix of H_λ and therefore the length n and the dimension k of the code H_λ are p^2 and 2 respectively. Thus H_λ is a two-dimensional code.

From Lemma 6.2.3 every even row of $A_\lambda = [ax^\lambda]_{a,x\in GF(p.2)^*}$ contains $2(p-1)$ elements from Ψ and there are no elements from Ψ in the odd rows of A_λ. From Theorem 4.3.3 the trace of elements of Ψ is zero. Therefore when we take trace of the matrix A_λ, there will be $2(p-1)$ zeros in the even rows and no zeros in the odd rows. Hence in H_λ, the even rows will contain $2(p-1)+1$ zeros and the odd rows 1 zero. Thus the Hamming weight of non-zero codewords of H_λ is either $p^2 - 2(p-1) - 1 = p^2 - 2p + 1 = (p-1)^2$ or $p^2 - 1$. Thus H_λ is a two-weight code over $\mathbb{Z}_p$ and the minimum Hamming distance is $(p-1)^2$. Therefore the parameters of H_λ are $[p^2, 2, (p-1)^2]$. □

Thus far we have studied the case $\lambda >$ 2-even and $\lambda|(p-1)$ when $p \equiv 3 (\text{mod } 4)$ (i.e., $\frac{p+1}{2}$-even), constructing two-dimensional, two-weight codes over $\mathbb{Z}_p$ with the parameters $[p^2, 2, (p-1)^2]$. Next we will do a parallel construction when $p \equiv 1 (\text{mod } 4)$. (i.e., $\frac{p+1}{2}$-

odd). In this case we can readily check that the minimum value of such a prime p is 13.

Lemma 6.2.5. *Let $p \geq 13$ be a prime such that $p \equiv 1(mod\ 4)$ (i.e., $\frac{p+1}{2}$-odd) and $\lambda > 2$-even such that $\lambda|(p-1)$. Let $(i)_\lambda = \{\zeta^{\lambda h+i}|h = 0,1,2,\ldots,\frac{p^2-1}{\lambda}-1\}$, where $i = 0,1,2,\ldots,\lambda-1$. Let $\Psi = \{\zeta^{(\frac{p+1}{2})(2k+1)}|k = 0,1,2,\ldots,p-2\}$ and for $0 \leq s \leq \frac{\lambda}{2}-1$, let $(s) = \{\zeta^{\frac{p+1}{2}(2s+1+\lambda j)}|j = 0,1,2,\ldots,\frac{2(p-1)}{\lambda}-1\}$. Then*
(i) For all $s = 0,1,2,\ldots,\frac{\lambda}{2}-1$, $(s) \subset \Psi$.
(ii) $\Psi = \dot{\bigcup}(s)$.
(iii) For each s, there exists an odd i such that $(s) \subset (i)_\lambda$.

Proof of this lemma is very similar to that of Lemma 6.2.1. □

To illustrate this result, consider the following example.

Example 6.2.6. *Let $p = 13$. Then $\frac{p+1}{2} = 7$-odd and $p-1 = 12$. Let $\lambda = 6$. Then $\lambda|(p-1)$ and the sets $\Psi = \{\zeta^{7(2k+1)}|k = 0,1,2,\ldots,11\}$, $(i)_6 = \{\zeta^{6h+i}|h = 0,1,2,\ldots,27\}$ and $(s) = \{\zeta^{7(2s+1+6j)}|j = 0,1,2,3\}$, where $i = 0,1,2,3,4,5$ and $s = 0,1,2$. Now consider the complete set (s) for each s. i.e.,*
$(0) = \{\zeta^7, \zeta^{49}, \zeta^{91}, \zeta^{133}\}$.
$(1) = \{\zeta^{21}, \zeta^{63}, \zeta^{105}, \zeta^{147}\}$.
$(2) = \{\zeta^{35}, \zeta^{77}, \zeta^{119}, \zeta^{161}\}$.

It is clear that all the elements of Ψ are in the above three sets.

Similarly, for $i = 0,1,2,3,4,5$, consider the complete set $(i)_6$. i.e.,
$(0)_6 = \{1, \zeta^6, \zeta^{12}, \zeta^{18}, \zeta^{24}, \zeta^{30}, \zeta^{36}, \zeta^{42}, \zeta^{48}, \zeta^{54}, \zeta^{60}, \zeta^{66}, \zeta^{72}, \zeta^{78}, \zeta^{84}, \zeta^{90}, \zeta^{96}, \zeta^{102}, \zeta^{108}, \zeta^{114}, \ldots\}$.
$(1)_6 = \{\zeta, \zeta^7, \zeta^{13}, \zeta^{19}, \zeta^{25}, \zeta^{31}, \zeta^{37}, \zeta^{43}, \zeta^{49}, \zeta^{55}, \zeta^{61}, \zeta^{67}, \zeta^{73}, \zeta^{79}, \zeta^{85}, \zeta^{91}, \zeta^{97}, \zeta^{103}, \zeta^{109}, \zeta^{115}, \ldots\}$.
$(2)_6 = \{\zeta^2, \zeta^8, \zeta^{14}, \zeta^{20}, \zeta^{26}, \zeta^{32}, \zeta^{38}, \zeta^{44}, \zeta^{50}, \zeta^{56}, \zeta^{62}, \zeta^{68}, \zeta^{74}, \zeta^{80}, \zeta^{86}, \zeta^{92}, \zeta^{98}, \zeta^{104}, \zeta^{110}, \zeta^{116}, \ldots\}$.
$(3)_6 = \{\zeta^3, \zeta^8, \zeta^{15}, \zeta^{21}, \zeta^{27}, \zeta^{33}, \zeta^{39}, \zeta^{45}, \zeta^{51}, \zeta^{57}, \zeta^{63}, \zeta^{69}, \zeta^{75}, \zeta^{81}, \zeta^{87}, \zeta^{93}, \zeta^{99}, \zeta^{105}, \zeta^{111}, \zeta^{117}, \ldots\}$.
$(4)_6 = \{\zeta^4, \zeta^{10}, \zeta^{16}, \zeta^{22}, \zeta^{28}, \zeta^{34}, \zeta^{40}, \zeta^{46}, \zeta^{52}, \zeta^{58}, \zeta^{64}, \zeta^{70}, \zeta^{76}, \zeta^{82}, \zeta^{88}, \zeta^{94}, \zeta^{100}, \zeta^{106}, \zeta^{112}, \zeta^{118}, \ldots\}$.
$(5)_6 = \{\zeta^5, \zeta^{11}, \zeta^{17}, \zeta^{23}, \zeta^{29}, \zeta^{35}, \zeta^{41}, \zeta^{47}, \zeta^{53}, \zeta^{59}, \zeta^{65}, \zeta^{71}, \zeta^{77}, \zeta^{83}, \zeta^{89}, \zeta^{95}, \zeta^{101}, \zeta^{107}, \zeta^{113}, \zeta^{119}, \ldots\}$.

It is clear that the elements of the sets $(0), (1)$ and (2) are completely listed in the sets $(1)_6, (3)_6$ and $(5)_6$ respectively.

We now look at the distribution of the elements of $\Psi = \{\zeta^{(\frac{p+1}{2})(2k+1)} | k = 0, 1, 2, \ldots, p-2\}$ over the rows of the matrix $A_\lambda = [ax^\lambda]_{a,x \in GF(p,2)}$, for this case. We state the next lemma without giving the proof as it is similar to that of Lemma 6.2.3.

Lemma 6.2.7. *Let $p \geq 13$ be a prime such that $p \equiv 1 (mod\ 4)$ (i.e., $\frac{p+1}{2}$-odd). Let $\lambda > 2$-even such that $\lambda | (p-1)$. Let $\Psi = \{\zeta^{\frac{p+1}{2}(2k+1)} | k = 0, 1, 2, \ldots, p-2\}$ and $A_\lambda = [ax^\lambda]_{a,x \in GF(p,2)^*}$, where $GF(p,2)^* = \{1, \zeta, \zeta^2, \ldots, \zeta^{p^2-2}\}$. Then every odd row of A_λ has $2(p-1)$ elements from the set Ψ and no elements of Ψ occur in the even rows of A_λ.*

Now we know that the distribution of the elements of Ψ over the rows of A_λ. In the next theorem this property will be used to construct two-dimensional, two-weight codes over $\mathbb{Z}_p$. Again the proof of this theorem is very similar to that of Theorem 6.2.4 and is omitted.

Theorem 6.2.8. *Let $p \geq 13$ be a prime and $\frac{p+1}{2}$-odd. Let $\lambda > 2$-even and $\lambda | (p-1)$. Let Tr be the trace map over the Galois field $GF(p,2)$. The code $H_\lambda = [Tr(ax^\lambda)]_{a,x \in GF(p,2)}$ is a two-weight code over $\mathbb{Z}_p$ and its parameters are $[p^2, 2, (p-1)^2]$.*

Thus far we have constructed codes over $\mathbb{Z}_p$ by using the trace map over the Galois filed $GF(p,2)$ in the form of $Tr(ax^\lambda)$ for even $\lambda > 2$ such that $\lambda | (p-1)$. In the next section we compare this code with the code that we constructed in Chapter 4.

6.3 Comparison of H_λ with H_2

In Section 6.2 we constructed the code H_λ over $\mathbb{Z}_p$ by using the trace map over $GF(p,2)$ in the form of $Tr(ax^\lambda)$ when $\lambda > 2$-even. This code was classified as a two-weight code with the parameters $[p^2, 2, (p-1)^2]$ which are exactly the same as that of the code H_2 constructed in Chapter 4 using the trace map over $GF(p,2)$ in the form of $Tr(ax^2)$. The curiosity now is whether these two codes are equivalent to each other. In Chapter 4 we proved that the code $H_2 = [Tr(ax^2)]_{a,x \in GF(p,2)}$ is self-orthogonal, for $p > 3$ and experimental results show that the code $H_\lambda = [Tr(ax^\lambda)]_{a,x \in GF(p,2)}$ constructed in this section is not self-orthogonal. Therefore we can conclude that the codes constructed in

this section are not equivalent to those of in Chapter 4 even though they have the same parameters.

Consider the following examples.

Example 6.3.1. *Let $p = 13$ and $\lambda = 6$. Then $\lambda|(p-1)$. Now consider the primitive polynomial $p(x) = x^2 + x + 3$ over $\mathbb{Z}_{13}$ and let ζ be a root of $p(x)$. Then the elements of $GF(13,2) = \mathbb{Z}_{13}[x]/(p(x)) = \mathbb{Z}_{13}[\zeta]$ can be written as $\{0, 1, \zeta, \zeta^2, \ldots, \zeta^{167}\}$. The following matrix gives us the code $H_6 = [Tr(ax^6)]_{a,x \in GF(13,2)}$.*

$$
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\
0 & 2 & 9 & 5 & 2 & 10 & 1 & 6 & 3 & 7 & 1 & 3 & 2 & 8 & 9 & 11 & 4 & 8 & 11 & 3 & 12 & 7 & 10 & 6 & 12 & 10 & \ldots \\
0 & 12 & 0 & 12 & 4 & 9 & 7 & 7 & 5 & 0 & 5 & 6 & 7 & 4 & 4 & 1 & 0 & 1 & 9 & 4 & 6 & 6 & 8 & 0 & 8 & 7 & \ldots \\
0 & 10 & 8 & 4 & 5 & 10 & 4 & 7 & 2 & 12 & 6 & 1 & 2 & 6 & 4 & 3 & 5 & 9 & 8 & 3 & 9 & 6 & 11 & 1 & 7 & 12 & \ldots \\
0 & 5 & 5 & 11 & 0 & 11 & 8 & 5 & 1 & 1 & 10 & 0 & 10 & 12 & 1 & 8 & 8 & 2 & 0 & 2 & 5 & 8 & 12 & 12 & 3 & 0 & \ldots \\
0 & 1 & 5 & 7 & 3 & 8 & 10 & 7 & 8 & 1 & 4 & 11 & 12 & 2 & 4 & 12 & 8 & 6 & 10 & 5 & 3 & 6 & 5 & 12 & 9 & 2 & \ldots \\
0 & 2 & 11 & 10 & 10 & 9 & 0 & 9 & 3 & 10 & 2 & 2 & 7 & 0 & 7 & 11 & 2 & 3 & 3 & 4 & 0 & 4 & 10 & 3 & 11 & 11 & \ldots \\
0 & 9 & 5 & 2 & 10 & 1 & 6 & 3 & 7 & 1 & 3 & 2 & 8 & 9 & 11 & 4 & 8 & 11 & 3 & 12 & 7 & 10 & 6 & 12 & 10 & 11 & \ldots \\
0 & 0 & 12 & 4 & 9 & 7 & 7 & 5 & 0 & 5 & 6 & 7 & 4 & 4 & 1 & 0 & 1 & 9 & 4 & 6 & 6 & 8 & 0 & 8 & 7 & 11 & \ldots \\
0 & 8 & 4 & 5 & 10 & 4 & 7 & 2 & 12 & 6 & 1 & 2 & 6 & 4 & 3 & 5 & 9 & 8 & 3 & 9 & 6 & 11 & 1 & 7 & 12 & 11 & \ldots \\
0 & 5 & 11 & 0 & 11 & 8 & 5 & 1 & 1 & 10 & 0 & 10 & 12 & 1 & 8 & 8 & 2 & 0 & 2 & 5 & 8 & 12 & 12 & 3 & 0 & 3 & \ldots \\
0 & 5 & 7 & 3 & 8 & 10 & 7 & 8 & 1 & 4 & 11 & 12 & 2 & 4 & 12 & 8 & 6 & 10 & 5 & 3 & 6 & 5 & 12 & 9 & 2 & 1 & \ldots \\
0 & 11 & 10 & 10 & 9 & 0 & 9 & 3 & 10 & 2 & 2 & 7 & 0 & 7 & 11 & 2 & 3 & 3 & 4 & 0 & 4 & 10 & 3 & 11 & 11 & 6 & \ldots \\
0 & 5 & 2 & 10 & 1 & 6 & 3 & 7 & 1 & 3 & 2 & 8 & 9 & 11 & 4 & 8 & 11 & 3 & 12 & 7 & 10 & 6 & 12 & 10 & 11 & 5 & \ldots \\
0 & 12 & 4 & 9 & 7 & 7 & 5 & 0 & 5 & 6 & 7 & 4 & 4 & 1 & 0 & 1 & 9 & 4 & 6 & 6 & 8 & 0 & 8 & 7 & 11 & 5 & \ldots \\
0 & 4 & 5 & 10 & 4 & 7 & 2 & 12 & 6 & 1 & 2 & 6 & 4 & 3 & 5 & 9 & 8 & 3 & 9 & 6 & 11 & 1 & 7 & 12 & 11 & 7 & \ldots \\
0 & 11 & 0 & 11 & 8 & 5 & 1 & 1 & 10 & 0 & 10 & 12 & 1 & 8 & 8 & 2 & 0 & 2 & 5 & 8 & 12 & 12 & 3 & 0 & 3 & 1 & \ldots \\
0 & 7 & 3 & 8 & 10 & 7 & 8 & 1 & 4 & 11 & 12 & 2 & 4 & 12 & 8 & 6 & 10 & 5 & 3 & 6 & 5 & 12 & 9 & 2 & 1 & 11 & \ldots \\
0 & 10 & 10 & 9 & 0 & 9 & 3 & 10 & 2 & 2 & 7 & 0 & 7 & 11 & 2 & 3 & 3 & 4 & 0 & 4 & 10 & 3 & 11 & 11 & 6 & 0 & \ldots \\
0 & 2 & 10 & 1 & 6 & 3 & 7 & 1 & 3 & 2 & 8 & 9 & 11 & 4 & 8 & 11 & 3 & 12 & 7 & 10 & 6 & 12 & 10 & 11 & 5 & 4 & \ldots \\
0 & 4 & 9 & 7 & 7 & 5 & 0 & 5 & 6 & 7 & 4 & 4 & 1 & 0 & 1 & 9 & 4 & 6 & 6 & 8 & 0 & 8 & 7 & 11 & 5 & 4 & \ldots \\
0 & 5 & 10 & 4 & 7 & 2 & 12 & 6 & 1 & 2 & 6 & 4 & 3 & 5 & 9 & 8 & 3 & 9 & 6 & 11 & 1 & 7 & 12 & 11 & 7 & 9 & \ldots \\
0 & 0 & 11 & 8 & 5 & 1 & 1 & 10 & 0 & 10 & 12 & 1 & 8 & 8 & 2 & 0 & 2 & 5 & 8 & 12 & 12 & 3 & 0 & 3 & 1 & 12 & \ldots \\
0 & 3 & 8 & 10 & 7 & 8 & 1 & 4 & 11 & 12 & 2 & 4 & 12 & 8 & 6 & 10 & 5 & 3 & 6 & 5 & 12 & 9 & 2 & 1 & 11 & 9 & \ldots \\
0 & 10 & 9 & 0 & 9 & 3 & 10 & 2 & 2 & 7 & 0 & 7 & 11 & 2 & 3 & 3 & 4 & 0 & 4 & 10 & 3 & 11 & 11 & 6 & 0 & 6 & \ldots \\
0 & 10 & 1 & 6 & 3 & 7 & 1 & 3 & 2 & 8 & 9 & 11 & 4 & 8 & 11 & 3 & 12 & 7 & 10 & 6 & 12 & 10 & 11 & 5 & 4 & 2 & \ldots \\
0 & 9 & 7 & 7 & 5 & 0 & 5 & 6 & 7 & 4 & 4 & 1 & 0 & 1 & 9 & 4 & 6 & 6 & 8 & 0 & 8 & 7 & 11 & 5 & 4 & 12 & \ldots \\
0 & 10 & 4 & 7 & 2 & 12 & 6 & 1 & 2 & 6 & 4 & 3 & 5 & 9 & 8 & 3 & 9 & 6 & 11 & 1 & 7 & 12 & 11 & 7 & 9 & 10 & \ldots \\
0 & 11 & 8 & 5 & 1 & 1 & 10 & 0 & 10 & 12 & 1 & 8 & 8 & 2 & 0 & 2 & 5 & 8 & 12 & 12 & 3 & 0 & 3 & 1 & 12 & 5 & \ldots \\
0 & 8 & 10 & 7 & 8 & 1 & 4 & 11 & 12 & 2 & 4 & 12 & 8 & 6 & 10 & 5 & 3 & 6 & 5 & 12 & 9 & 2 & 1 & 11 & 9 & 1 & \ldots \\
0 & 9 & 0 & 9 & 3 & 10 & 2 & 2 & 7 & 0 & 7 & 11 & 2 & 3 & 3 & 4 & 0 & 4 & 10 & 3 & 11 & 11 & 6 & 0 & 6 & 2 & \ldots \\
0 & 1 & 6 & 3 & 7 & 1 & 3 & 2 & 8 & 9 & 11 & 4 & 8 & 11 & 3 & 12 & 7 & 10 & 6 & 12 & 10 & 11 & 5 & 4 & 2 & 9 & \ldots \\
0 & 7 & 7 & 5 & 0 & 5 & 6 & 7 & 4 & 4 & 1 & 0 & 1 & 9 & 4 & 6 & 6 & 8 & 0 & 8 & 7 & 11 & 5 & 4 & 12 & 0 & \ldots \\
0 & 4 & 7 & 2 & 12 & 6 & 1 & 2 & 6 & 4 & 3 & 5 & 9 & 8 & 3 & 9 & 6 & 11 & 1 & 7 & 12 & 11 & 7 & 9 & 10 & 8 & \ldots \\
0 & 8 & 5 & 1 & 1 & 10 & 0 & 10 & 12 & 1 & 8 & 8 & 2 & 0 & 2 & 5 & 8 & 12 & 12 & 3 & 0 & 3 & 1 & 12 & 5 & 5 & \ldots \\
0 & 10 & 7 & 8 & 1 & 4 & 11 & 12 & 2 & 4 & 12 & 8 & 6 & 10 & 5 & 3 & 6 & 5 & 12 & 9 & 2 & 1 & 11 & 9 & 1 & 5 & \ldots \\
0 & 0 & 9 & 3 & 10 & 2 & 2 & 7 & 0 & 7 & 11 & 2 & 3 & 3 & 4 & 0 & 4 & 10 & 3 & 11 & 11 & 6 & 0 & 6 & 2 & 11 & \ldots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{bmatrix}_{169 \times 169}
$$

Let H_6^* be the matrix obtained by deleting the first column of the matrix H_6. It is clear that each row of H_6^* can be formed by using 6 copies of the first 28 elements of each row. Clearly the matrix H_6 can be generated by using all linear combinations of the 2^{nd} and 3^{rd}

rows of H_6. Further H_6 is a two-weight code over $\mathbb{Z}_{13}$ with the parameters $[169, 2, 144]$ and the punctured code H_6^* is a $[168, 2, 144]$ code and its codewords are left-cyclic shifts of each of the first 6 non-zero codewords. Indeed H_6^* is a cyclic code. H_6 is not a self-orthogonal code.

Now we will compare the code $H_6 = [Tr(ax^6)]_{a,x\in GF(13,2)}$ with the code $H_2 = [Tr(ax^2)]_{a,x\in GF(13,2)}$ given in the next example.

Example 6.3.2. *Let $p = 13$ and consider the primitive polynomial $p(x) = x^2 + x + 3$ over $\mathbb{Z}_{13}$ and let ζ be a root of $p(x)$. Then the elements of $GF(13, 2) = \mathbb{Z}_{13}[x]/(p(x)) = \mathbb{Z}_{13}[\zeta]$ can be written as $\{0, 1, \zeta, \zeta^2, \ldots, \zeta^{167}\}$. The following matrix gives us the code $H_2 = [Tr(ax^2)]_{a,x\in GF(13,2)}$.*

$$
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\
0 & 2 & 10 & 1 & 9 & 8 & 5 & 5 & 4 & 7 & 2 & 5 & 3 & 10 & 10 & 8 & 1 & 4 & 10 & 6 & 7 & 7 & 3 & 2 & 8 & 7 & \ldots \\
0 & 12 & 5 & 2 & 0 & 5 & 11 & 12 & 11 & 10 & 4 & 0 & 10 & 9 & 11 & 9 & 7 & 8 & 0 & 7 & 5 & 9 & 5 & 1 & 3 & 0 & \ldots \\
0 & 10 & 1 & 9 & 8 & 5 & 5 & 4 & 7 & 2 & 5 & 3 & 10 & 10 & 8 & 1 & 4 & 10 & 6 & 7 & 7 & 3 & 2 & 8 & 7 & 12 & \ldots \\
0 & 5 & 2 & 0 & 5 & 11 & 12 & 11 & 10 & 4 & 0 & 10 & 9 & 11 & 9 & 7 & 8 & 0 & 7 & 5 & 9 & 5 & 1 & 3 & 0 & 1 & \ldots \\
0 & 1 & 9 & 8 & 5 & 5 & 4 & 7 & 2 & 5 & 3 & 10 & 10 & 8 & 1 & 4 & 10 & 6 & 7 & 7 & 3 & 2 & 8 & 7 & 12 & 1 & \ldots \\
0 & 2 & 0 & 5 & 11 & 12 & 11 & 10 & 4 & 0 & 10 & 9 & 11 & 9 & 7 & 8 & 0 & 7 & 5 & 9 & 5 & 1 & 3 & 0 & 1 & 10 & \ldots \\
0 & 9 & 8 & 5 & 5 & 4 & 7 & 2 & 5 & 3 & 10 & 10 & 8 & 1 & 4 & 10 & 6 & 7 & 7 & 3 & 2 & 8 & 7 & 12 & 1 & 1 & \ldots \\
0 & 0 & 5 & 11 & 12 & 11 & 10 & 4 & 0 & 10 & 9 & 11 & 9 & 7 & 8 & 0 & 7 & 5 & 9 & 5 & 1 & 3 & 0 & 1 & 10 & 5 & \ldots \\
0 & 8 & 5 & 5 & 4 & 7 & 2 & 5 & 3 & 10 & 10 & 8 & 1 & 4 & 10 & 6 & 7 & 7 & 3 & 2 & 8 & 7 & 12 & 1 & 1 & 6 & \ldots \\
0 & 5 & 11 & 12 & 11 & 10 & 4 & 0 & 10 & 9 & 11 & 9 & 7 & 8 & 0 & 7 & 5 & 9 & 5 & 1 & 3 & 0 & 1 & 10 & 5 & 10 & \ldots \\
0 & 5 & 5 & 4 & 7 & 2 & 5 & 3 & 10 & 10 & 8 & 1 & 4 & 10 & 6 & 7 & 7 & 3 & 2 & 8 & 7 & 12 & 1 & 1 & 6 & 4 & \ldots \\
0 & 11 & 12 & 11 & 10 & 4 & 0 & 10 & 9 & 11 & 9 & 7 & 8 & 0 & 7 & 5 & 9 & 5 & 1 & 3 & 0 & 1 & 10 & 5 & 10 & 2 & \ldots \\
0 & 5 & 4 & 7 & 2 & 5 & 3 & 10 & 10 & 8 & 1 & 4 & 10 & 6 & 7 & 7 & 3 & 2 & 8 & 7 & 12 & 1 & 1 & 6 & 4 & 3 & \ldots \\
0 & 12 & 11 & 10 & 4 & 0 & 10 & 9 & 11 & 9 & 7 & 8 & 0 & 7 & 5 & 9 & 5 & 1 & 3 & 0 & 1 & 10 & 5 & 10 & 2 & \ldots & \\
0 & 4 & 7 & 2 & 5 & 3 & 10 & 10 & 8 & 1 & 4 & 10 & 6 & 7 & 7 & 3 & 2 & 8 & 7 & 12 & 1 & 1 & 6 & 4 & 3 & 1 & \ldots \\
0 & 11 & 10 & 4 & 0 & 10 & 9 & 11 & 9 & 7 & 8 & 0 & 7 & 5 & 9 & 5 & 1 & 3 & 0 & 1 & 10 & 5 & 10 & 2 & 6 & 0 & \ldots \\
0 & 7 & 2 & 5 & 3 & 10 & 10 & 8 & 1 & 4 & 10 & 6 & 7 & 7 & 3 & 2 & 8 & 7 & 12 & 1 & 1 & 6 & 4 & 3 & 1 & 11 & \ldots \\
0 & 10 & 4 & 0 & 10 & 9 & 11 & 9 & 7 & 8 & 0 & 7 & 5 & 9 & 5 & 1 & 3 & 0 & 1 & 10 & 5 & 10 & 2 & 6 & 0 & 2 & \ldots \\
0 & 2 & 5 & 3 & 10 & 10 & 8 & 1 & 4 & 10 & 6 & 7 & 7 & 3 & 2 & 8 & 7 & 12 & 1 & 1 & 6 & 4 & 3 & 1 & 11 & 2 & \ldots \\
0 & 4 & 0 & 10 & 9 & 11 & 9 & 7 & 8 & 0 & 7 & 5 & 9 & 5 & 1 & 3 & 0 & 1 & 10 & 5 & 10 & 2 & 6 & 0 & 2 & 7 & \ldots \\
0 & 5 & 3 & 10 & 10 & 8 & 1 & 4 & 10 & 6 & 7 & 7 & 3 & 2 & 8 & 7 & 12 & 1 & 1 & 6 & 4 & 3 & 1 & 11 & 2 & 2 & \ldots \\
0 & 0 & 10 & 9 & 11 & 9 & 7 & 8 & 0 & 7 & 5 & 9 & 5 & 1 & 3 & 0 & 1 & 10 & 5 & 10 & 2 & 6 & 0 & 2 & 7 & 10 & \ldots \\
0 & 3 & 10 & 10 & 8 & 1 & 4 & 10 & 6 & 7 & 7 & 3 & 2 & 8 & 7 & 12 & 1 & 1 & 6 & 4 & 3 & 1 & 11 & 2 & 2 & 12 & \ldots \\
0 & 10 & 9 & 11 & 9 & 7 & 8 & 0 & 7 & 5 & 9 & 5 & 1 & 3 & 0 & 1 & 10 & 5 & 10 & 2 & 6 & 0 & 2 & 7 & 10 & 7 & \ldots \\
0 & 10 & 10 & 8 & 1 & 4 & 10 & 6 & 7 & 7 & 3 & 2 & 8 & 7 & 12 & 1 & 1 & 6 & 4 & 3 & 1 & 11 & 2 & 2 & 12 & 8 & \ldots \\
0 & 9 & 11 & 9 & 7 & 8 & 0 & 7 & 5 & 9 & 5 & 1 & 3 & 0 & 1 & 10 & 5 & 10 & 2 & 6 & 0 & 2 & 7 & 10 & 7 & 4 & \ldots \\
0 & 10 & 8 & 1 & 4 & 10 & 6 & 7 & 7 & 3 & 2 & 8 & 7 & 12 & 1 & 1 & 6 & 4 & 3 & 1 & 11 & 2 & 2 & 12 & 8 & 6 & \ldots \\
0 & 11 & 9 & 7 & 8 & 0 & 7 & 5 & 9 & 5 & 1 & 3 & 0 & 1 & 10 & 5 & 10 & 2 & 6 & 0 & 2 & 7 & 10 & 7 & 4 & 12 & \ldots \\
0 & 8 & 1 & 4 & 10 & 6 & 7 & 7 & 3 & 2 & 8 & 7 & 12 & 1 & 1 & 6 & 4 & 3 & 1 & 11 & 2 & 2 & 12 & 8 & 6 & 2 & \ldots \\
0 & 9 & 7 & 8 & 0 & 7 & 5 & 9 & 5 & 1 & 3 & 0 & 1 & 10 & 5 & 10 & 2 & 6 & 0 & 2 & 7 & 10 & 7 & 4 & 12 & 0 & \ldots \\
0 & 1 & 4 & 10 & 6 & 7 & 7 & 3 & 2 & 8 & 7 & 12 & 1 & 1 & 6 & 4 & 3 & 1 & 11 & 2 & 2 & 12 & 8 & 6 & 2 & 9 & \ldots \\
0 & 7 & 8 & 0 & 7 & 5 & 9 & 5 & 1 & 3 & 0 & 1 & 10 & 5 & 10 & 2 & 6 & 0 & 2 & 7 & 10 & 7 & 4 & 12 & 0 & 4 & \ldots \\
0 & 4 & 10 & 6 & 7 & 7 & 3 & 2 & 8 & 7 & 12 & 1 & 1 & 6 & 4 & 3 & 1 & 11 & 2 & 2 & 12 & 8 & 6 & 2 & 9 & 4 & \ldots \\
0 & 8 & 0 & 7 & 5 & 9 & 5 & 1 & 3 & 0 & 1 & 10 & 5 & 10 & 2 & 6 & 0 & 2 & 7 & 10 & 7 & 4 & 12 & 0 & 4 & 1 & \ldots \\
0 & 10 & 6 & 7 & 7 & 3 & 2 & 8 & 7 & 12 & 1 & 1 & 6 & 4 & 3 & 1 & 11 & 2 & 2 & 12 & 8 & 6 & 2 & 9 & 4 & 4 & \ldots \\
0 & 0 & 7 & 5 & 9 & 5 & 1 & 3 & 0 & 1 & 10 & 5 & 10 & 2 & 6 & 0 & 2 & 7 & 10 & 7 & 4 & 12 & 0 & 4 & 1 & 7 & \ldots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{bmatrix}_{169\times 169}
$$

Let H_2^* be the matrix obtained by deleting the first column of the matrix H_2. It is clear that each row of H_2^* can be formed by using 2 copies of the first 84 elements of each row. It is also clear that the matrix H_2 can be generated by using all linear combinations of the 2^{nd} and 3^{rd} rows of H_2. Further H_2 is a two-weight code over $\mathbb{Z}_{13}$ with the parameters $[169, 2, 144]$ and the punctured code H_2^* is a $[168, 2, 144]$ code and its codewords are left-cyclic shifts of each of the first 2 non-zero codewords. Indeed H_2^* is a cyclic code. H_2 is a self-orthogonal code, and consequently H_6 and H_2 are not equivalent codes.

Thus far we have considered the case $Tr(ax^\lambda)$ for even $\lambda > 2$ such that $\lambda|(p-1)$. In the next section we study the case odd $\lambda > 2$ such that $\lambda|(p-1)$.

6.4 Constant-weight codes from $\mathbf{Tr(ax^\lambda)}$ when $\lambda >$ 2-odd

In Section 6.2 we studied the codes constructed by using the trace map over the Galois field $GF(p, 2)$ in the form of $Tr(ax^\lambda)$, for $\lambda > 2$-even such that $\lambda|(p-1)$ when $p \equiv 1(\text{mod } 4)$ and $p \equiv 3(\text{mod } 4)$. Similarly in this section we consider the case $\lambda > 2$-odd such that $\lambda|(p-1)$ when $p \equiv 1(\text{mod } 4)$ and $p \equiv 3(\text{mod } 4)$. As usual, first we will study the distribution of trace zero elements which are in $\Psi = \{\zeta^{\frac{p+1}{2}(2k+1)} | k = 0, 1, 2, \ldots, p-2\}$ over the rows of $A = [ax^\lambda]_{a,x \in GF(p,2)^*}$. Then we will apply this result to construct codes over $\mathbb{Z}_p$ and we will prove that these codes are constant weight codes with the parameters $[p^2, 2, p(p-1)]$.

Lemma 6.4.1. *Let $p \geq 7$ be prime and $\lambda > 2$-odd such that $\lambda|(p-1)$. Let $(i)_\lambda = \{\zeta^{\lambda h+i} | h = 0, 1, 2, \ldots, \frac{p^2-1}{\lambda} - 1\}$, where $i = 0, 1, 2, \ldots, \lambda - 1$. Let $\Psi = \{\zeta^{\frac{p+1}{2}(2k+1)} | k = 0, 1, 2, \ldots, p-2\}$ and for $0 \leq s \leq \lambda - 1$ let $(s) = \{\zeta^{\frac{p+1}{2}(2s+1+2\lambda j)} | j = 0, 1, 2, \ldots, \frac{(p-1)}{\lambda} - 1\}$. Then*

(i) For all $s = 0, 1, 2, \ldots, \lambda - 1$, $(s) \subset \Psi$.

(ii) $\Psi = \dot{\bigcup}(s)$.

(ii) For each s, there exists an i such that $(s) \subset (i)_\lambda$

Proof:

Proof of part (i) and (ii) are very similar to that of Lemma 6.2.1

(iii) Let $\alpha \in (s)$. Then $\alpha = \zeta^{\frac{(p+1)}{2}(2s+1+2\lambda j)}$. To prove that $\zeta^{\frac{(p+1)}{2}(2s+1+2\lambda j)} \in (i)_\lambda$ for all j, we need to prove that $\frac{p+1}{2}(2s+1+2\lambda j) \equiv i(\text{mod } \lambda)$. That is we need to prove that $\frac{p+1}{2}(2s+1+2\lambda j)$ is in the same equivalence class mod λ for all j. In another words we need to prove that $\left(\frac{p+1}{2}\right)(2s+1) + \left(\frac{p+1}{2}\right)2\lambda j$ is in the same equivalence class mod λ for all j. Since $\left(\frac{p+1}{2}\right)2\lambda j \equiv 0(\text{mod } \lambda)$, we have $\left(\frac{p+1}{2}\right)(2s+1)$ is in the same equivalence class mod λ for all j. Therefore $\frac{p+1}{2}(2s+1+\lambda j)$ is in the same equivalence class mod λ for all j. i.e., in the equivalence class of $\frac{p+1}{2}(2s+1)$ when $j=0$. Therefore $(s) \subset (i)_\lambda$ for $i \equiv \left(\frac{p+1}{2}\right)(2s+1)$ mod λ. □

The next example illustrates this result.

Example 6.4.2. *Let $p = 11$. Then $\frac{p+1}{2} = 6$-even and $p-1 = 10$. Let $\lambda = 5$. Then $\lambda|(p-1)$ and the sets $\Psi = \{\zeta^{6(2k+1)}|k = 0,1,2,\ldots,9\}$, $(i)_5 = \{\zeta^{5h+i}|h = 0,1,2,\ldots,23\}$ and $(s) = \{\zeta^{6(2s+1+10j)}|j = 0,1\}$, where $i = 0,1,2,3,4$ and $s = 0,1,2,3,4$. For each s, the complete set (s) is given below.*

$(0) = \{\zeta^6, \zeta^{66}\}$.
$(1) = \{\zeta^{18}, \zeta^{78}\}$.
$(2) = \{\zeta^{30}, \zeta^{90}\}$.
$(3) = \{\zeta^{42}, \zeta^{102}\}$.
$(4) = \{\zeta^{54}, \zeta^{114}\}$.

It is clear that all the elements of Ψ are in the above five sets.

Similarly consider, for each i, the complete set $(i)_5$.

$(0)_5 = \{1, \zeta^5, \zeta^{10}, \zeta^{15}, \zeta^{20}, \zeta^{25}, \zeta^{30}, \zeta^{35}, \zeta^{40}, \zeta^{45}, \zeta^{50}, \zeta^{55}, \zeta^{60}, \zeta^{65}, \zeta^{70}, \zeta^{75}, \zeta^{80}, \zeta^{85}, \zeta^{90}, \zeta^{95}, \ldots\}$.
$(1)_5 = \{\zeta, \zeta^6, \zeta^{11}, \zeta^{16}, \zeta^{21}, \zeta^{26}, \zeta^{31}, \zeta^{36}, \zeta^{41}, \zeta^{46}, \zeta^{51}, \zeta^{56}, \zeta^{61}, \zeta^{66}, \zeta^{71}, \zeta^{76}, \zeta^{81}, \zeta^{86}, \zeta^{91}, \zeta^{96}, \ldots\}$.
$(2)_5 = \{\zeta^2, \zeta^7, \zeta^{12}, \zeta^{17}, \zeta^{22}, \zeta^{27}, \zeta^{32}, \zeta^{37}, \zeta^{42}, \zeta^{47}, \zeta^{52}, \zeta^{57}, \zeta^{62}, \zeta^{67}, \zeta^{72}, \zeta^{77}, \zeta^{82}, \zeta^{87}, \zeta^{92}, \zeta^{97}, \ldots\}$.
$(3)_5 = \{\zeta^3, \zeta^8, \zeta^{13}, \zeta^{18}, \zeta^{23}, \zeta^{28}, \zeta^{33}, \zeta^{38}, \zeta^{43}, \zeta^{48}, \zeta^{53}, \zeta^{58}, \zeta^{63}, \zeta^{68}, \zeta^{73}, \zeta^{78}, \zeta^{83}, \zeta^{88}, \zeta^{93}, \zeta^{98}, \ldots\}$.
$(4)_5 = \{\zeta^4, \zeta^9, \zeta^{14}, \zeta^{19}, \zeta^{24}, \zeta^{29}, \zeta^{34}, \zeta^{39}, \zeta^{44}, \zeta^{49}, \zeta^{54}, \zeta^{59}, \zeta^{64}, \zeta^{69}, \zeta^{74}, \zeta^{79}, \zeta^{84}, \zeta^{89}, \zeta^{94}, \zeta^{99}, \ldots\}$.

When $s = 0$, $\left(\frac{p+1}{2}\right)(2s+1) = 6 \equiv 1(mod\ 5)$. Therefore $(0) \subset (1)_5$.

When $s = 1$, $\left(\frac{p+1}{2}\right)(2s+1) = 18 \equiv 3(mod\ 5)$. Therefore $(1) \subset (3)_5$.

Similarly $(2) \subset (0)_5$,$(3) \subset (2)_5$ and $(4) \subset (4)_5$

We are now in a position to study the distribution of the trace zero elements $\Psi = \{\zeta^{\frac{p+1}{2}(2k+1)} | k = 0, 1, 2, \ldots, p-2\}$ over the rows of $A_\lambda = [ax^\lambda]_{a,x \in GF(p,2)^*}$.

Lemma 6.4.3. *Let $p \geq 7$ be prime and $\lambda >$ 2-odd such that $\lambda|(p-1)$. Let $\Psi = \{\zeta^{\frac{p+1}{2}(2k+1)} | k = 0, 1, 2, \ldots, p-2\}$ and $A_\lambda = [ax^\lambda]_{a,x \in GF(p,2)^*}$. Then each row of A_λ contains $(p-1)$ elements from Ψ.*

Proof:

From Lemma 6.4.1 we know that, for all $i = 0, 1, 2, \ldots \lambda - 1$, the elements of Ψ are equally distributed over $(i)_\lambda$ giving $\frac{(p-1)}{\lambda}$ elements per set. From Lemma 5.2.2 we also know that each row of A_λ contains λ-copies of $(i)_\lambda$ or λ-copies of a cyclic shift of $(i)_\lambda$ for some $i = 0, 1, 2, \ldots, \lambda - 1$. Therefore each row of the matrix A_λ contain $(p-1)$ elements from the set Ψ. □

Having studied the distribution of the elements of Ψ over the rows of A_λ, we now use this property to construct two-dimensional, constant-weight codes over $\mathbb{Z}_p$.

Theorem 6.4.4. *Let $p \geq 7$ be a prime such that $p \equiv 3 (mod\ 4)$ (i.e., $\frac{p+1}{2}$-even) and $\lambda >$ 2-odd such that $\lambda|(p-1)$. Let Tr be the trace map over the Galois field $GF(p,2)$. The code $H_\lambda = [Tr(ax^\lambda)]_{a,x \in GF(p,2)}$ is a constant-weight code over $\mathbb{Z}_p$ with the parameters $[p^2, 2, p(p-1)]$.*

Proof:

Consider that matrix

$$G_{H_\lambda} = \begin{bmatrix} Tr(c_i^\lambda), & i = 1, 2, \ldots, p^2 \\ Tr(\zeta c_i^\lambda), & i = 1, 2, \ldots, p^2 \end{bmatrix}_{2 \times p^2}.$$

Very similar to the proof of Theorem 6.2.4 we can show that the two rows of G_{H_λ} are linearly independent and hence G_{H_λ} is a generator matrix of H_λ. Therefore the length n and the dimension k of the code H_λ are p^2 and 2 respectively. Thus H_λ is a two-dimensional code.

From Lemma 6.4.3 we know that each row of the matrix $A_\lambda = [ax^\lambda]_{a,x \in GF(p,2)^*}$ contains $(p-1)$ elements which are from the set $\Psi = \{\zeta^{\frac{p+1}{2}(2k+1)} | k = 0, 1, 2, \ldots, p-2\}$.

From Theorem 4.3.3 we know that the trace of each of these elements is zero. Therefore there are $(p-1)+1 = p$ zeros in each row of the matrix H_λ and the Hamming weight of each codeword is $p^2 - p = p(p-1)$. Thus H_λ is a constant-weight code over $\mathbb{Z}_p$, the minimum Hamming distance between the codewords is $p(p-1)$, and the parameters of H_λ are $[p^2, 2, p(p-1)]$. □

Thus far in this section we have constructed codes over $\mathbb{Z}_p$ by using the trace map over the Galois filed $GF(p,2)$ in the form of $Tr(ax^\lambda)$ for odd $\lambda > 2$ such that $\lambda|(p-1)$. In the next section we compare this code with the code constructed in [65].

6.5 Comparison of $\mathbf{H}_\lambda$ with H

In the previous section we constructed the code H_λ over $\mathbb{Z}_p$ by using the trace map over $GF(p,2)$ in the form of $Tr(ax^\lambda)$ when $\lambda >$ 2-odd. We classified this code as a constant-weight code with the parameters $[p^2, 2, p(p-1)]$. In [65], the trace map over the Galois field $GF(p,m)$ was used in the form of $Tr(ax)$ to construct constant-weight codes with the parameters $[p^m, m, p^{m-1}(p-1)]$. In the case of $m = 2$, the code $H = [Tr(ax)]_{a,x\in GF(p,2)}$ has the parameters $[p^2, 2, p(p-1)]$ which are exactly the same as that of the codes constructed in the previous section. q-ary linear constant weight codes can be considered as simplex codes since every pair of distinct codewords are the same distance apart [53]. Therefore H and H_λ are simplex codes. Further every non-zero codeword of $H = [Tr(ax)]_{a,x\in GF(p,2)}$ contain each element of $\mathbb{Z}_p$ equally often p times and the dot product of every non-zero codeword of H is given by

$$\begin{aligned} S &= p\sum_{i=1}^{p-1} i^2 \\ &= \frac{p^2}{6}(2p^2 - 3p + 1). \end{aligned}$$

Since $p > 3$ we have $S \equiv 0 \bmod p$. From Theorem 4.2.5 a linear code over $\mathbb{Z}_p$, for $p > 2$, is self-orthogonal if and only if the dot product of each codeword with itself is zero. Therefore the above code $H = [Tr(ax)]_{a,x\in GF(p,2)}$ is a self-orthogonal code over $\mathbb{Z}_p$. As in Section 6.3 again the curiosity is whether these two codes are equivalent to each

other. Experimental results show that the code $H_\lambda = [Tr(ax^\lambda)]_{a,x\in GF(p,2)}$ constructed in this section is not a self-orthogonal code. The reason is that the non-zero elements of $\mathbb{Z}_p$ are not equally distributed over the rows of H_λ unlike in H (see examples 6.5.1 and 6.5.2). Therefore the code constructed in this section is not equivalent to those in [65] even though they have the same parameters.

Consider the following examples.

Example 6.5.1. *Let $p = 7$ and $\lambda = 3$. Then $\lambda|(p-1)$. Now consider the primitive polynomial $p(x) = x^2 + x + 3$ over $\mathbb{Z}_7$ and let ζ be a root of $p(x)$. Then $\zeta^2 = 6\zeta + 4$ and the elements of $GF(7,2) = \mathbb{Z}_7[x]/(p(x)) = \mathbb{Z}_7[\zeta]$ can be written as $\{0, 1, \zeta, \zeta^2, \ldots, \zeta^{47}\}$. The following matrix gives us the code $H_3 = [Tr(ax^3)]_{a,x\in GF(7,2)}$.*

$$H_3 = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\
0 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & \dots \\
0 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & \dots \\
0 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & \dots \\
0 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & \dots \\
0 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & \dots \\
0 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & \dots \\
0 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & \dots \\
0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & \dots \\
0 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & \dots \\
0 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & \dots \\
0 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & \dots \\
0 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & \dots \\
0 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & \dots \\
0 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & \dots \\
0 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & \dots \\
0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & \dots \\
0 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & \dots \\
0 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & \dots \\
0 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & \dots \\
0 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & \dots \\
0 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & \dots \\
0 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & \dots \\
0 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & \dots \\
0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & \dots \\
0 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & \dots \\
0 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & \dots \\
0 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & \dots \\
0 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & \dots \\
0 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & \dots \\
0 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & \dots \\
0 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & \dots \\
0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & \dots \\
0 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & \dots \\
0 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & \dots \\
0 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & \dots \\
0 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & \dots \\
0 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & \dots \\
0 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & \dots \\
0 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & \dots \\
0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & \dots \\
0 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & \dots \\
0 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & \dots \\
0 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & \dots \\
0 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & \dots \\
0 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & \dots \\
0 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & \dots \\
0 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & 2 & 3 & 5 & 1 & 6 & 0 & 6 & 6 & 5 & 4 & 2 & 6 & 1 & 0 & 1 & 1 & \dots \\
0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & 5 & 2 & 0 & 2 & 2 & 4 & 6 & 3 & 2 & 5 & 0 & 5 & 5 & 3 & 1 & 4 & \dots
\end{bmatrix}_{49\times 49}.$$

Let H_3^* be the matrix obtained by deleting the first column of the matrix H_3. It is clear that each row of H_3^* can be formed by using 3 *copies of the first* 16 *elements of each row. It is also clear that the matrix H_3 can be generated by using all linear combinations of the 2^{nd} and 3^{rd} rows of H_3. Further H_3 is a constant-weight code over $\mathbb{Z}_7$ with the parameters $[49, 2, 42]$ and the punctured code H_3^* is a $[48, 2, 42]$ code and its codewords are the left-cyclic shifts of elements of each of the first* 3 *non-zero rows of H_3^*. Indeed H_3^* is*

a cyclic code.

We now compare the code $H_3 = [Tr(ax^3)]_{a,x \in GF(7,2)}$ with the code $H = [Tr(ax)]_{a,x \in GF(7,2)}$ given in the next example.

Example 6.5.2. *Let $p = 7$ and consider the primitive polynomial $p(x) = x^2 + x + 3$ over $\mathbb{Z}_7$ and let ζ be a root of $p(x)$. Then $\zeta^2 = 6\zeta + 4$ and the elements of $GF(7,2) = \mathbb{Z}_7[x]/(p(x)) = \mathbb{Z}_7[\zeta]$ can be written as $\{0, 1, \zeta, \zeta^2, \ldots, \zeta^{47}\}$. The following matrix gives us the code $H = [Tr(ax)]_{a,x \in GF(7,2)}$.*

$$H = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\
0 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & \dots \\
0 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & \dots \\
0 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & \dots \\
0 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & \dots \\
0 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & \dots \\
0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & \dots \\
0 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & \dots \\
0 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & \dots \\
0 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & \dots \\
0 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & \dots \\
0 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & \dots \\
0 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & \dots \\
0 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & \dots \\
0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & \dots \\
0 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & \dots \\
0 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & \dots \\
0 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & \dots \\
0 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & \dots \\
0 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & \dots \\
0 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & \dots \\
0 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & \dots \\
0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & \dots \\
0 & 6 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & \dots \\
0 & 5 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & \dots \\
0 & 5 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & \dots \\
0 & 1 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & \dots \\
0 & 5 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & \dots \\
0 & 6 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & \dots \\
0 & 0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & \dots \\
0 & 3 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & \dots \\
0 & 4 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & \dots \\
0 & 1 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & \dots \\
0 & 1 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & \dots \\
0 & 3 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & \dots \\
0 & 1 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & \dots \\
0 & 4 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & \dots \\
0 & 0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & \dots \\
0 & 2 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & \dots \\
0 & 5 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & \dots \\
0 & 3 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & \dots \\
0 & 3 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & \dots \\
0 & 2 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & \dots \\
0 & 3 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & \dots \\
0 & 5 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & \dots \\
0 & 0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & \dots \\
0 & 6 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & \dots \\
0 & 1 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & \dots \\
0 & 2 & 2 & 6 & 2 & 1 & 0 & 4 & 3 & 6 & 6 & 4 & 6 & 3 & 0 & 5 & 2 & 4 & 4 & 5 & 4 & 2 & 0 & 1 & 6 & 5 & 5 & 1 & 5 & 6 & \dots
\end{bmatrix}_{49\times 49}.$$

The matrix H can be generated by using all linear combinations of the 2^{nd} and 3^{rd} rows of H. Further H is a constant-weight code over $\mathbb{Z}_7$ with the parameters $[49, 2, 42]$. Let H^* be the code obtained by deleting the first column of H. The punctured code H^* is a $[48, 2, 42]$ constant-weight, cyclic code over $\mathbb{Z}_7$.

Chapter 7

Conclusion

Throughout the thesis the major tool was the use of the trace maps Tr over the Galois field $GF(p,m)$ and Galois ring $GR(p_1^{e_1},m)$, the trace-like map T over the ring $R(n,m) = GR(p_1^{e_1},m) \times GR(p_2^{e_2},m) \times \ldots \times GR(p_k^{e_k},m)$ and more generally the weighted-trace map T_w over the ring $R(d,n) = GR(p_1^{e_1},m_1) \times GR(p_2^{e_2},m_2) \times \ldots \times GR(p_k^{e_k},m_k)$ to construct Cocyclic Butson Hadamard matrices, linear and non-linear codes. In Chapter 3 the weighted-trace map T_w over the ring $R(d,n) = GF(p_1,e_1) \times GF(p_2,e_2) \times \ldots \times GF(p_k,e_k)$ was used to construct mutually unbiased bases of odd integer dimension d. However we did not study the use of the weighted-trace map T_w over the ring $R(d,n) = GR(p_1^{e_1},m_1) \times GR(p_2^{e_2},m_2) \times \ldots \times GR(p_k^{e_k},m_k)$. This is a possible venue for research in mutually unbiased bases. In Chapters 4, 5 and 6 the trace map over the Galois field $GF(p,2)$ was used in the form of $Tr(ax^2)$ and $Tr(ax^\lambda)$ to construct two-weight and constant-weight codes over $\mathbb{Z}_p$. We noticed that these were two-dimensional codes. We may get higher dimensional two-weight and constant-weight codes if we use the trace map in the similar manner over the Galois field $GF(p,m)$. If we can finalise this research it may give further direction to carry out research by using the trace map over the Galois ring $GR(p^s,m)$ and more generally the weighted-trace map over the ring $R(d,n) = GR(p_1^{e_1},m_1) \times GR(p_2^{e_2},m_2) \times \ldots \times GR(p_k^{e_k},m_k)$.

Bibliography

[1] C. Archer. There is no generalisation of known formulas for mutually unbiased bases. *J. Math. Phys.*, 46(2):022106 1–11, 2005.

[2] M. Aschbacher, A. M. Childs, and P. Wocjan. The limitations of nice mutually unbiased bases. *J. Algebr. Comb.*, 25(2):111–123, 2007.

[3] A. Baliga. New self-dual codes from cocyclic Hadamard matrices. *J. Comb. Math. Comb. Comput.*, 28:7–14, 1998.

[4] A. Baliga. Extremal doubly-even self-dual cocyclic [40, 20] codes. In *2000 IEEE ISIT*, page 114, 2000.

[5] A. Baliga and J. J. Chua. Self-dual codes using image restoration techniques. In S. Boztas and I. E. Shparlinski, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes; AAECC-14,*, volume LNCS 2227 of *Lecture Notes in Computer Science*, pages 46–56. Springer, 2001.

[6] A. Baliga and K. J. Horadam. Cocyclic Hadamard matrices over $\mathbb{Z}_t \times \mathbb{Z}_{2^2}$. *Australas. J. Comb.*, 11:123–134, 1995.

[7] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan. A new proof for the existence of mutually unbiased bases. *arXiv:quant-ph/0103162 v3*, 2001.

[8] L. D. Baumert and R. J. McEliece. Weights of irreducible cyclic codes. *Inform. Control*, 20:158–175, 1972.

[9] I. Bengtsson and A. Ericsson. Mutually unbiased bases and the complementarity polytope. *Open Syst. Inf. Dyn.*, 12(2):107–120, 2005.

[10] J. Bierbrauer. A family of 2-weight codes related to BCH-codes. *J. Comb. Des.*, 5(5):391–399, 1997.

[11] J. Bierbrauer. *Introduction to coding theory.* Chapman and Hall/CRC, Florida, 2004.

[12] J. T. Blackford and D. K. Ray-Chaudhuri. A transform approach to permutation group of cyclic codes over Galois rings. *IEEE Trans. Inform. Theory*, 46(7):2350–2358, 2000.

[13] I. Bouyukliev, V. Fack, W. Willems, and J Winne. Projective two-weight codes with small parameters and their corresponding graphs. *Design Code. Cryptogra.*, 41(1):59–78, 2006.

[14] I. Bouyukliev and P. R. J. Ostergard. Classification of self-orthogonal codes over $\mathbb{F}_3$ and $\mathbb{F}_4^*$. *Discrete Math.*, 19(2):363–370, 2005.

[15] A. E. Brouwer, T. B. Shearer, N. J. A. Sloane, and W. D. Smith. A new table of constant-weight codes. *IEEE Trans. Inform. Theory*, 36(6):1334–1380, 1990.

[16] A. T. Butson. Generalised Hadamard matrices. *Proc. Amer. Math. Soc.*, 13:894–898, 1962.

[17] A. R. Calderbank and W. M. Kantor. The geometry of two-weight codes. *Bull. London Math. Soc.*, 1986, volume 18, pages 97-122,.

[18] A. R. Calderbank and N. J. A. Sloane. Modular and p-adic cyclic codes. *Design Code. Cryptogr.*, 6:21–35, 1995.

[19] C. Carlet and C. Ding. Linear codes from perfect nonlinear mappings and their secret sharing schemes. *IEEE Trans. Inform. Theory*, 51(6):2089–2102, 2005.

[20] S. Chaturvedi. Mutually unbiased bases. *Pramana J. Phys.*, 59(2):345–350, 2002.

[21] Z. Chen, P. Fan, and F. Jin. New results on self-orthogonal unequal error protection codes. *IEEE Trans. Inform. Theory*, 36(5):1141–1144, 1990.

[22] J. P. Cherdieu, D. J. Mercier, and T. Narayaninsamy. On the generalised weights of a class of trace codes. *Finite Fields Appl.*, 7:355–371, 2001.

[23] F. D. Clerck and M. Delanote. Two-weight codes, partial geometries and steiner systems. *Design Code. Cryptogr.*, 21:87–98, 2000.

[24] J. H. Conway and N. J. A. Sloane. A new upper bound on the minimal distance of self-dual codes. *IEEE Trans. Inform. Theory*, 36:1319–1333, 1990.

[25] C. H. Cooke and I. Heng. Error correcting codes associated with complex Hadamard matrices. *App. Math. Lett.*, 12(4):77–80, 1998.

[26] C. H. Cooke and I. Heng. On the non-existence of some generalised Hadamard matrices. *Australas. J. Combin.*, 19:137–148, 1999.

[27] C. H. Cooke and I. Heng. Polynomial construction of complex Hadamard matrices with cyclic core. *App. Math. Lett.*, 12:87–93, 1999.

[28] R. Craigen. Regular conference matrices and complex Hadamard matrices. *Utilitas Math.*, 45:65–69, 1994.

[29] R. Dodunekova and S. M. Dodunekov. Error detection with a class of q-ary two-weight codes. *IEEE ISIT*, pages 2232–2235, 2005.

[30] D. A. Drake. Partial λ geometries and generalised Hadamard matrices. *Canad. J. Math.*, 31:217–227, 1979.

[31] T. Durt. Derivation of an explicit expression for mutually unbiased bases in even and odd prime power dimensions. *arXiv:quant-ph/0409090 v2*, 2004.

[32] T. Durt. If $1 = 2 \oplus 3$, then $1 = 2 \odot 3$: Bell states, finite groups, and mutually unbiased bases, a unifying approach. *arXiv:quant-ph/0401037 v2*, 2004.

[33] F. W. Fu, A. J. H. Vinck, and S. Y. Shen. On the construction of constant-weight codes. *IEEE Trans. Inform. theory*, 44(1):328–333, 1998.

[34] A. J. Gareth and J. J. Mary. *Elementary number theory.* Springer-Verlag, Berlin Herdelberg, NewYork, 1998.

[35] M. Grassl. On SIC-POVMs and MUBs in dimension 6. *quant-ph/0406175 v1*, 2004.

[36] C. Guneri and F. Ozbudak. Improvements on generalised Hamming weight of some trace codes. *Design Code. Cryptogr.*, 39:215–231, 2006.

[37] M. K. Gupta, D. G. Glynn, and T. A. Gulliver. On some quaternary self-orthogonal codes. In S. Boztas and I. E. Shparlinski, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes; AAECC-14*, volume LNCS 2227 of *Lecture Notes in Computer Science*, pages 112–121. Springer, 2001.

[38] M. Harada and P. R. J. Ostergard. Self-dual and maximal self-orthogonal codes over $\mathbb{F}_7$. *Discrete Math.*, 256:471–477, 2002.

[39] M. Harada and V. D. Tonchev. Singly-even self-dual codes and Hadamard matrices. In G. Cohen, M. Guisti, and T. Mora, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes; AAECC-11,*, volume LNCS 948 of *Lecture Notes in Computer Science*, pages 279–284. Springer-Verlag, 1995.

[40] T. Helleseth. Some two-weight codes with composite parity-check polynomials. *IEEE Trans. Inform. Theory*, 22(5):631–632, 1976.

[41] T. Helleseth, P. V. Kumar, O. Moreno, and A. G. Shanbhag. Imporved estimates via exponential sums for the minimim distance of $\mathbb{Z}_4$-linear trace codes. *IEEE Trans. Inform. Theory*, 42(4):1212–1216, 1996.

[42] S. G. Hoggar. t-designs in projective spaces. *Eur. J. Combin.*, 3:233–254, 1982.

[43] K. J. Horadam and W. D. Launey. Generation of cocyclic Hadamard matrices. In A. van der Poorten W. Bosma, editor, *Computational Algebra and Number Theory*, chapter 20, pages 279–290. Kluwer Academic, Dordrecht, 1995.

[44] K. J. Horadam and A. A. I. Perera. Codes from cocycles. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes; AAECC-12,*, volume LNCS 1255

of *Lecture Notes in Computer Science*, pages 151–163. Springer-Verlag, Berlin, June 1997.

[45] K. J. Horadam and A. Rao. Fourier transforms from a weighted-trace map. In *2006 IEEE ISIT*, pages 1080–1084, Seattle, USA, 9-14 July 2006.

[46] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes.* Cambridge University Press, United Kingdom, 2003.

[47] I. D. Ivanovic. Geometrical description of quantal state determination. *J. Phys. A*, 14:3241–3245, 1981.

[48] H. Kharaghani and J. Seberry. Regular complex Hadamard matrices. *Congressus Numerantium*, 75:187–201, 1990.

[49] A. Klappenecker and M. Rotteler. Constructions of mutually unbiased bases. In *Proceedings International Conference on Finite Fields and Applications (Fq7)*, number LNCS 2948 in Lecture Notes in Computer Science, pages 137–144. Springer, 2004.

[50] A. Klappenecker and M. Rotteler. Mutually unbiased bases are complex projective 2-designs. *arXiv:quant-ph/0502031 v2*, 2005.

[51] W. D. Launey. On the asymptotic existence of partial complex Hadamard matrices and related combinatorial objects. *Discrete Appl. Math.*, 102:37–45, 2000.

[52] R. Lidl and H. Niederreiter. *Finite Fields.* Cambridge University Press, United Kingdom, 1997.

[53] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting codes.* North-Holland, Amsterdam, 1977.

[54] S. Matsufuji and N. Suehiro. Complex Hadamard matrices related to bent sequences. *IEEE Trans. Inform. Theory*, 42(2):637, 1996.

[55] B. McDonald. *Finite rings with identity.* Marcel Dekker, New York, 1974.

[56] P. R. J. Ostergard and M. Svanstrom. Ternary constant weight codes. *Electron. J. Comb.*, 9(R41):1–23, 2002.

[57] N. Pinnawala. Simplex and other cocyclic codes. Master's thesis, Department of Mathematics and Statistics, RMIT University, January 2004.

[58] N. Pinnawala and A. Rao. Cocyclic simplex codes of type α over $\mathbb{Z}_4$ and $\mathbb{Z}_{2^s}$. *IEEE Trans. Inform. Theory*, 50(9):2165–2169, 2004.

[59] N. Pinnawala, A. Rao, and T. A. Gulliver. Distribution of trace values and tow-weights, self-orthogonal codes over $GF(p, 2)$. *AAECC 17*.

[60] A. O. Pittenger and M. H. Rubin. Mutually unbiased bases, generalised spin matrices and separability. *arXiv:quant-ph/0308142 v2*, 2004.

[61] M. Planat and H. Rosu. Quantum phase uncertainty in mutually unbiased measurements and Gausss sums. *arXiv:quant-ph/0502167 v2*, 2005.

[62] V. Pless, P. Solé, and Z. Qian. Cyclic self-dual $\mathbb{Z}_4$-codes. *Finite Fields Appl.*, 3:48–69, 1997.

[63] E. M. Rains and N. J. A. Sloane. *Handbook of coding theory*. North Holland, New York, 1998.

[64] A. Rao. Shift-equivalence and cocyclic self-dual codes. *J. Comb. Math. Comb. Comput.*, 54:175–185, 2005.

[65] A. Rao and N. Pinnawala. New linear codes over $\mathbb{Z}_{p^s}$ via the trace map. In *2005 IEEE ISIT*, pages 124–126, Adelaide, Australia, 4-9 September 2005.

[66] J. Schwinger. Unitary operator bases. *Proc. Nat. Acad. Sci. U. S. A.*, 46:570–579, 1960.

[67] J. Seberry and X. M. Zhang. Some orthogonal designs and complex Hadamard matrices by using two Hadamard matrices. *Australas. J. Combin.*, 4:93–102, 1991.

[68] D. H. Smith, L. A. Hughes, and S. Perkins. A new table of constant weight codes of length greater than 28. *Electron. J. Comb.*, 13(A2):1–18, 2006.

[69] P. Sole and D. Zinoviev. Weighted degree trace codes for PAPR reduction. In T. Helleseth et al., editor, *Sequences and Their Applications*, volume 3486/2005, pages 406–413. Springer Berlin / Heidelberg, 2004.

[70] H. Stichtenoth and C. Voss. Generalised Hamming weight of trace codes. *IEEE Trans. Inform. Theory*, 40(2):554–558, 1994.

[71] F. Szechtman. Quadratic Gauss sums over finite commutative rings. *J. Number Theory*, 95(1):1–13, 2002.

[72] R. L. Townsend and E. J. Weldon. Self-orthogonal quasi-cyclic codes. *IEEE Trans. Inform. Theory*, 13(2):183–195, 1967.

[73] M. V. D. Vlugt. On the dimension of trace codes. *IEEE Trans. Inform. Theory*, 37(1):196–199, 1991.

[74] W. D. Wallis, A. P. Street, and J. S. Wallis. *Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices*. Number 292 in Lecture Notes in Math. Springer-Verlag, Berlin, 1972.

[75] Z. X. Wan. *Quaternary codes*. Chinese Academy of Sciences, China and Lund University, Sweden, 1997.

[76] Z. X. Wan. A characteristic property of self-orthogonal codes and its application to lattices. *Bull. Belg. Math. Soc.*, 5:477–482, 1998.

[77] Z. X. Wan. *Lectures on finite fields and Galois rings*. World Scientific, New Jersey, 2003.

[78] A. Winterhof. On the nonexistence of generalised Hadamard matrices. *J. Stat. Plan. Infer.*, 84:337–342, 2000.

[79] P. Wocjan and T. Beth. New construction of mutually unbiased bases in square dimensions. *arXiv:quant-ph/0407081 v1*, 2004.

[80] J. A. Wood. The structure of linear codes of constant weight. *Trans. AMS*, 354(3):1007–1026, 2000.

[81] W. K. Wootters and B. D. Fields. Optimal state-determination by mutually unbiased measurements. *Anal. Phys.*, 191:363–381, 1989.