Distribution of trace values and two-weight, self-orthogonal codes over GF (p,2)

Pinnawala Ralalage, Nimalsiri; Rao, Asha; Gulliver, Aaron

Pinnawala Ralalage, N., Rao, A., & Gulliver, A. (2007). Distribution of trace values and two-weight, self-orthogonal codes over GF (p,2). Lecture Notes in Computer Science, 4851, 311–320. https://doi.org/10.1007/978-3-540-77224-8_36

Published Version: https://doi.org/10.1007/978-3-540-77224-8_36

Distribution of Trace values and Two-Weight, Self-Orthogonal Codes over $GF(p, 2)$

N. Pinnawala[1], A. Rao[1], and T.A. Gulliver[2]

[1] School of Mathematical and Geospatial Sciences, RMIT University, GPO Box 2476V, Melbourne, VIC - 3001, Australia.
[2] Department of Electrical and Computer Engineering, University of Victoria, P.O. Box 3055, STN CSC, Victoria, B.C., Canada V8W 3P6
nimalsiri.pinnawala@rmit.edu.au,asha@rmit.edu.au,agullive@engr.uvic.ca

Abstract. The uniform distribution of the trace map lends itself very well to the construction of binary and non-binary codes from Galois fields and Galois rings. In this paper we study the distribution of the trace map with the argument ax^2 over the Galois field $GF(p, 2)$. We then use this distribution to construct two-weight, self-orthogonal, trace codes.

Key words: Trace map, self-orthogonal, non-binary, two-weight, Galois fields

1 Introduction

In [11] and [12] the trace map over Galois field $GF(p, m)$ and ring $GR(p^s, m)$ was used to construct linear codes over $\mathbb{Z}_{2^s}$ and $\mathbb{Z}_{p^s}$, respectively. At that time the distribution of the trace map was very intriguing and the question arose of whether this trace distribution was as straightforward when the argument was changed. One encounter of a different argument was in the search for mutually unbiased bases which can enable a quantum cryptosystem in d-dimensions [4].

The authors were unable to find any information in the literature about such distribution of the trace map other than the fundamental properties. It does turn out that this work is not straightforward and this paper looks at the distribution of $Tr(ax^2)$ over $GF(p, 2)$ for odd primes p. The two-weight self-orthogonal codes generated using this distribution are a by-product.

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 $\mathbb{Z}_p$. The generator matrix G of an $[n, k]$ code C is simply a matrix whose rows are linearly independent and span the code. The inner product of $x = (x_1, x_2, \ldots x_n), \quad y = (y_1, y_2, \ldots y_n) \in \mathbb{Z}_p^n$ is defined by $x \cdot y = \sum_{i=1}^{n} x_i y_i$. Using the inner product, the dual code $C^\perp$ of C is defined by $C^\perp = \{x \in \mathbb{Z}_p^n | x \cdot c = 0 \ \ \forall c \in C\}$. The code C is called self-orthogonal if $C \subseteq C^\perp$.

Many authors look at self-orthogonal codes, for example, [2, 7, 8, 13]. Following are some preliminary results on self-orthogonal codes that are useful here:

Lemma 1 (Theorem 1.4.3, [10]). *(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 $w_H(x) \equiv x \cdot x \ (mod\ 3)$.*

Note that this result does not hold for $x \in \mathbb{Z}_p^n$ when $p > 3$, the reason being that when $x \in \mathbb{Z}_p^n$, $w_H(x) = \sum_{i=1}^{p-1} n_i$, 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 $w_H(x) \equiv x \cdot x \ (\text{mod } p)$. Lemma 1 does tell us whether a given ternary code is self-orthogonal.

Lemma 2 (Theorem 1.4.10, [10]). *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.*

Again this result cannot check the self-orthogonality of codes over $\mathbb{Z}_p$ for $p > 3$. For this we need the following result.

Lemma 3 (Proposition 1 [13]). *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 $c \cdot c = 0 \ \forall \ c \in C$.*

An important invariant of a code is the minimum distance between codewords. The Hamming distance $d_H(x, y)$ between two vectors $x, y \in \mathbb{Z}_p^n$ is defined to be the number of coordinates 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. If the minimum distance d of an $[n, k]$ code is known then C is an $[n, k, d]$ code.

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. A code is called a two-weight code if $|\{i | i \neq 0 \ \text{ and } \ A_i \neq 0\}| = 2$. More details on two-weight codes can be found in [3, 6, 9], etc. and the references therein.

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 $\mathbb{F}_{q^r}$. Let C be an $\mathbb{F}_{q^r}$-linear code of length n and $Tr : \mathbb{F}_{q^r} \rightarrow \mathbb{F}_q$ be the trace. The code $Tr(C)$, defined as the set of all $(Tr(x_1), Tr(x_2), \ldots, Tr(x_n))$, is called the trace code, where $(x_1, x_2, \ldots, x_n) \in C$. We note that the codes found in this paper could be classed as trace codes, since they are found using a trace map. See [1] for example for details on trace codes.

We now have some of the tools required to classify the codes found in this paper. In the next section we study the distribution of the trace map over $GF(p, 2)$, using the argument ax^2. In Section 3 we construct our codes and study their properties. In the final section, we give some conclusions and detail further work.

2 Distribution of the $Tr(ax^2)$ 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 to be 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 1. *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 $Tr(x) = x + x^p + x^{p^2} + \ldots + x^{p^{m-1}}$.*

Theorem 1. *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 p^{m-1}-times.

Since every non-zero element of $GF(p,2)$ can be written as a power of the primitive element ζ, we first identify the powers of ζ that have trace zero.

Lemma 4. *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 $0 \le t \le p^2 - 2$. Then*

i. $Tr(\zeta^{\frac{p+1}{2}}) = 0$.
ii. *For* $0 \le t < \frac{p+1}{2}$, $Tr(\zeta^t) \neq 0$.
iii. *If* $Tr(\zeta^t) = 0$ *then* $Tr(\zeta^{t(2k+1)}) = 0$, *where* $k = 0, 1, \ldots, p-2$.

Proof:

i. By using the definition of the trace map we have

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

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 $Tr(\zeta^{\frac{p+1}{2}}) = 0$.

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

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

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

iii. From the definition of the trace map if $Tr(\zeta^t) = 0$ then $\zeta^t + \zeta^{tp} = 0 \Rightarrow (\zeta^t)^{2k} = (\zeta^{tp})^{2k}$. Therefore $Tr(\zeta^{t(2k+1)}) = \zeta^{t(2k+1)} + \zeta^{tp(2k+1)} = \zeta^t \zeta^{2tk} + \zeta^{2tkp}\zeta^{tp} = \zeta^t \zeta^{2tkp} + \zeta^{2tkp}\zeta^{tp} = 0$. Thus if $Tr(\zeta^t) = 0$ then $Tr(\zeta^{t(2k+1)}) = 0$. From part (vi) of Theorem 1 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 $k = 0, 1, 2, \ldots, p-2$. □

Corollary 1. *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 5. *Let $\zeta^t \in GF(p,2)^*$, for some t, $0 \leq t \leq p^2-1$. If $\zeta^t \in GF(p,1)^*$ then $t = (p+1)k$.*

Proof: Let $\zeta^t \in GF(p,2)^*$, for some t, $0 \leq t \leq p^2-1$. 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 1 and part (i) of Lemma 4.

But from Corollary 1, 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 $t = (p+1)k, k = 0, 1, 2, \ldots, p-2$, i.e., ζ^t is an element of the subfield when $t = (p+1)k$, $k = 0, 1, 2, \ldots, p-2$. □

Thus far we have identified the elements $\zeta^t \in GF(p,2)^*$ which have trace 0 or are in the base field. We are now in a position to study the distribution of $Tr(ax^2)$, when both a and x range 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

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

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 $a_k, k = 0, 1, \ldots p-2$, be a listing of the non-zero elements of the base field.

Lemma 6. *The trace of the 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 the elements in every other column of the matrix representation of $GF(p,2)^*$ takes every element in $\mathbb{Z}_p\backslash\{0\}$ once only.

Proof:

i. From Corollary 1 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. From Lemma 5 the trace of the elements in the d^{th} column ($d \neq 0$) of the matrix is given by

$$\begin{aligned} Tr(\zeta^{\left(\frac{p+1}{2}\right)(2k+1)+d}) &= Tr(\zeta^{(p+1)k}\zeta^{\frac{p+1}{2}}\zeta^{d}) \\ &= Tr(a_k\zeta^{\frac{p+2d+1}{2}})(\text{ from Lemma 5}) \\ &= a_k Tr(\zeta^{\frac{p+2d+1}{2}})\ \ ; a_k \in GF(p,1)^* \equiv \mathbb{Z}_p\backslash\{0\} \end{aligned}$$

From Corollary 1 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 $d = 1,2,\ldots,p$, i.e., $Tr(\zeta^{\frac{p+2d+1}{2}})$ is fixed for each column. In addition, a_k represents every element in $\mathbb{Z}_p\backslash\{0\}$ 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 $\mathbb{Z}_p\backslash\{0\}$ exactly once. □

Example 1. 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:

x	$x = a_1\zeta + a_0$	$Tr(x)$	x	$x = a_1\zeta + a_0$	$Tr(x)$	x	$x = a_1\zeta + a_0$	$Tr(x)$
1	$0\zeta + 1$	2	ζ^8	$3\zeta + 1$	4	ζ^{16}	$2\zeta + 3$	4
ζ	$1\zeta + 0$	4	ζ^9	$3\zeta + 4$	0	ζ^{17}	$1\zeta + 1$	1
ζ^2	$4\zeta + 3$	2	ζ^{10}	$1\zeta + 4$	2	ζ^{18}	$0\zeta + 3$	1
ζ^3	$4\zeta + 2$	0	ζ^{11}	$3\zeta + 3$	3	ζ^{19}	$3\zeta + 0$	2
ζ^4	$3\zeta + 2$	1	ζ^{12}	$0\zeta + 4$	3	ζ^{20}	$2\zeta + 4$	1
ζ^5	$4\zeta + 4$	4	ζ^{13}	$4\zeta + 0$	1	ζ^{21}	$2\zeta + 1$	0
ζ^6	$0\zeta + 2$	4	ζ^{14}	$1\zeta + 2$	3	ζ^{22}	$4\zeta + 1$	3
ζ^7	$2\zeta + 0$	3	ζ^{15}	$1\zeta + 3$	0	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 every non-initial column contains each non-zero element of $\mathbb{Z}_5$ exactly once.

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

Theorem 2. *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 $\mathbb{Z}_p\backslash\{0\}$ equally often either $p+1$ times or $p-1$ times.*

In the matrix representation of $GF(p,2)^*$ (Lemma 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. 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 $GF(p,2)^*$.

Before we can prove Theorem 2, we need to work out some more details of the trace matrix. We consider the two cases, $p \equiv 1 \ (mod\ 4)$ and $p \equiv 3 \ (mod\ 4)$ separately.

Case I: $p \equiv 1 \ (mod\ 4)$ In this case $\frac{p+1}{2}$ is odd. From Lemma 4, $Tr(\zeta^{(\frac{p+1}{2})(2k+1)}) = 0$ 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 in the matrix representation of $GF(p,2)^*$ with non-zero trace.

From Lemma 6, the trace of the elements of each of these $\frac{p-1}{2}$ odd columns contain each element in $\mathbb{Z}_p\backslash\{0\}$ exactly once. Thus the trace of all the odd powers of ζ gives us each element in $\mathbb{Z}_p\backslash\{0\}$, $\frac{p-1}{2}$ times, and so the trace of all the even powers of ζ gives us each element in $\mathbb{Z}_p\backslash\{0\}$, $\frac{p+1}{2}$ times.

Case II: $p \equiv 3 \ (mod\ 4)$ 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 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 and 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 us each element in $\mathbb{Z}_p\backslash\{0\}$, $\frac{p+1}{2}$ times.

Proof of Theorem 2 Let $a \in GF(p,2)^*$ be an even (resp. 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 $\{\zeta^{2h} \mid h = 0, 1, 2, \ldots, \frac{p^2-3}{2}\}$ (resp. $\{\zeta^{2h+1} \mid h = 0, 1, 2, \ldots, \frac{p^2-3}{2}\}$) or its cyclic shifts.

Suppose $p \equiv 1 \ (mod\ 4)$. If $a \in GF(p,2)^*$ is an odd power of ζ then from Case I above, as x ranges over $GF(p,2)^*$, $Tr(ax^2)$ takes each element in $\mathbb{Z}_p\backslash\{0\}$ 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.

Similarly if $p \equiv 3 \ (mod\ 4)$, when $a \in GF(p,2)^*$ is an even power of ζ then from Case II above, as x ranges over $GF(p,2)^*$, $Tr(ax^2)$ takes each element in $\mathbb{Z}_p\backslash\{0\}$ equally often $p-1$ times and when $a \in GF(p,2)^*$ is an odd power of ζ, $Tr(ax^2)$ takes each element in $\mathbb{Z}_p\backslash\{0\}$ equally often $p+1$ times. (See Examples 2 and 3.) □

3 Two-weight Self-Orthogonal codes via $Tr(ax^2)$ over $GF(p,2)$

Thus far we have studied the distribution of $Tr(ax^2)$ for x ranging over the Galois field $GF(p,2)$. In this section we apply this result to construct cyclic, two-dimensional, two-weight, self-orthogonal codes over $\mathbb{Z}_p$.

Theorem 3 (Codes from $Tr(ax^2)$).
Let $GF(p,2)$ be the Galois Field of characteristic $p \geq 3$. Let Tr be the trace map over $GF(p,2)$. Consider the matrix $H = [Tr(ax^2)]_{a,x \in GF(p,2)}$.

i. H is a linear code over $\mathbb{Z}_p$ with parameters $[n,k,d_H] = [p^2, 2, (p-1)^2]$, where d_H is the minimum Hamming distance.
ii. H 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, denoted by H^*, is a cyclic code with parameters $[p^2-1, 2, (p-1)^2]$.
iv. For $p > 3$, H 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

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

The two rows of G_H are linearly independent: For $a_0, a_1 \in \mathbb{Z}_p$, and for all $i = 1,2,\ldots,p^2$, $a_0 Tr(c_i^2) + a_1 Tr(\zeta c_i^2) = 0 \Rightarrow a_0 + a_1\zeta = 0$ since $c_i^2 \neq 0$ for some i $\Rightarrow a_0 = a_1 = 0$ since 1 and ζ are linearly independent over $\mathbb{Z}_p$.
Now consider all linear combinations of the two rows in G_H. This gives us $a_0 Tr(c_i^2) + a_1 Tr(\zeta c_i^2) = Tr((a_0 + a_1\zeta)c_i^2)$, $i = 1,2,\ldots,p^2$. Thus G_H is a generator matrix for H, and consequently the length n and the dimension k of H are p^2 and 2, respectively, and H is a linear code.
Now from Theorem 2 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 is $(p-1)^2$.

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

iii. Let H^* be obtained by deleting the first column of H: $H^* =$

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

The second and third rows generate this code, the next consecutive two rows are the left cyclic shift by one element of the second and third rows, respectively, and so on. Thus H^* is a cyclic code.

iv. Let S be the dot product of every non-zero codeword of H with itself. Again from Theorem 2 every non-zero codeword of H contains each element in $\mathbb{Z}_p \backslash \{0\}$ equally often either $p+1$ times or $p-1$ times. Therefore either

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

or

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

If $p > 3$ we have $S \equiv 0 \bmod p$ and from Theorem 3 H is a self-orthogonal code over $\mathbb{Z}_p$ for $p > 3$. □

The following two examples illustrate Theorems 2 and 3.

Example 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 listed as $\{0, 1, \zeta, \zeta^2, \ldots, \zeta^7\}$. The following table provides the trace value of these elements and their squares.

x	$x = a_1\zeta + a_0$	$Tr(x)$	x^2	$Tr(x^2)$	x	$x = a_1\zeta + a_0$	$Tr(x)$	x^2	$Tr(x^2)$	x	$x = a_1\zeta + a_0$	$Tr(x)$	x^2	$Tr(x^2)$
0	$0\zeta+0$	0	0	0	ζ^2	$2\zeta+1$	0	ζ^4	1	ζ^5	$2\zeta+0$	1	ζ^2	0
1	$0\zeta+1$	2	1	2	ζ^3	$2\zeta+2$	2	ζ^6	0	ζ^6	$1\zeta+2$	0	ζ^4	1
ζ	$1\zeta+0$	2	ζ^2	0	ζ^4	$0\zeta+2$	1	1	2	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 matrices $A = [(ax^2)]_{a,x \in GF(3,2)}$ and $H = [Tr(ax^2)]_{a,x \in GF(3,2)}$ are given by

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \zeta^0 & \zeta^2 & \zeta^4 & \zeta^6 & \zeta^0 & \zeta^2 & \zeta^4 & \zeta^6 \\ 0 & \zeta^1 & \zeta^3 & \zeta^5 & \zeta^7 & \zeta^1 & \zeta^3 & \zeta^5 & \zeta^7 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \zeta^6 & \zeta^0 & \zeta^2 & \zeta^4 & \zeta^6 & \zeta^0 & \zeta^2 & \zeta^4 \\ 0 & \zeta^7 & \zeta^1 & \zeta^3 & \zeta^5 & \zeta^7 & \zeta^1 & \zeta^3 & \zeta^5 \end{bmatrix}, \quad H = \begin{bmatrix} 0&0&0&0&0&0&0&0&0 \\ 0&2&0&1&0&2&0&1&0 \\ 0&2&2&1&1&2&2&1&1 \\ \vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots \\ 0&0&2&0&1&0&2&0&1 \\ 0&1&2&2&1&1&2&2&1 \end{bmatrix}.$$

A generator matrix for H is

$$G_H = \begin{bmatrix} 0&2&0&1&0&2&0&1&0 \\ 0&2&2&1&1&2&2&1&1 \end{bmatrix}_{2\times 9} \text{ while } \quad H^* = \begin{bmatrix} 0&0&0&0&0&0&0&0 \\ 2&0&1&0&2&0&1&0 \\ 2&2&1&1&2&2&1&1 \\ \vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots \\ 0&2&0&1&0&2&0&1 \\ 1&2&2&1&1&2&2&1 \end{bmatrix}_{9\times 8} \text{ is obtained by deleting the first column of } H.$$

H is a linear code over $\mathbb{Z}_3$ with parameters $[9, 2, 4]$. The Hamming weight of each non-zero codeword is either 4 or 8. Thus H is a two-weight

code. The punctured code H^*, obtained by deleting the first column of H, is an $[8,2,4]$ cyclic code over $\mathbb{Z}_3$. The weight of each non-zero codeword is not divisible by 3 and from Theorem 2, H is not a self-orthogonal code.

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

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

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

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

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

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

The rows of H can be generated by

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

Therefore H is a linear code over $\mathbb{Z}_5$ and its parameters are $[25, 2, 16]$. The punctured code H^*, obtained by deleting the first column in H, is a $[24, 2, 16]$ cyclic code over $\mathbb{Z}_5$. The Hamming weight of each non-zero codeword of H is either 16 or 24. Thus H is a two-weight code. From part iv of Theorem 3, H is a self-orthogonal code.

4 Conclusions and Further Work

Even though much work has been done on the classification of nonbinary self-orthogonal codes ([2, 7, 5], these deal mostly with dimension 3 and larger. The codes we find here are 2-dimensional.

In this paper we studied the distribution of $Tr(ax^2)$ and used it to construct two-dimensional, two-weight, cyclic, self-orthogonal codes over $\mathbb{Z}_p$. The questions that arise are whether we can extend this construction to construct codes over $GF(p,2)$ using $Tr(ax^\lambda)$ for any integer $\lambda > 0$ and in general over $GF(p,m)$. We are currently doing this research.

References

1. J. Bierbrauer. *Introduction to Coding Theory*, volume 28 of *Discrete Mathematics and its Applications*. Chapman & Hall/CRC, New York, 2005.
2. I. Bouyukliev and P. R. J. Ostergard. Classification of self-orthogonal codes. *Discrete Math.*, 19(2):363–370, 2005.
3. A. R. Calderbank and W. M. Kantor. The geometry of two-weight codes. *Bull. London Maths. Soc.*, 18:97–122, 1986.
4. Nicolas J. Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin. Security of quantum key distribution using d-level systems. *Physical Review Letters*, 88(127902), March 2002.
5. Z. Chen, P. Fan, and F. Jin. New results on self-orthogonal unequal error protection codes. *IEEE Trans. Info. Theory*, 36(5):1141–1144, 1990.
6. R. Dodunekova and S. M. Dodunekov. Error detection with a class of q-ary two-weight codes. *IEEE Inform, Theory ISIT 2005 Proceedings*, pages 2232–2235, 2005.
7. 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.
8. M. Harada and P. R. J. Ostergard. Self- dual and maximal self-orthogonal codes over f_7. *Elsevier Disc. Math.*, 256:471–477, 2002.
9. T. Helleseth. Some two-weight codes with composite parity-check polynomials. *IEEE Trans. Inform. Theory*, 22(5):631–632, 1976.
10. W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, 2003.
11. N. Pinnawala and A. Rao. Cocyclic simplex codes of type α over $\mathbb{Z}_4$ and $\mathbb{Z}_{2^s}$. *IEEE Trans. Info. Theory*, 50(9):2165–2169, 2004.
12. A. Rao and N. Pinnawala. New linear codes over Z_{p^s} via the trace map. In *2005 IEEE International Symposium on Information Theory*, pages 124–126, Adelaide, Australia, 4-9 September 2005.
13. Z. X. Wan. A characteristic property of self-orthogonal codes and its application to lattices. *Bull. Belg. Maths. Soc*, 5:477–482, 1998.