New Linear Codes over $\mathbb{Z}_p^s$ via the Trace Map

Asha Rao* and Nimalsiri Pinnawala
*Formerly A. Baliga
School of Mathematical and Geospatial Sciences
RMIT University
GPO Box 2476V, Melbourne, VIC - 3001, Australia
Email: asha@rmit.edu.au, nimalsiri.pinnawala@rmit.edu.au

Abstract—The trace map has been used very successfully to generate cocyclic complex and Butson Hadamard matrices and simplex codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2^s$. We extend this technique to obtain new linear codes over $\mathbb{Z}_p^s$. It is worth nothing here that these codes are cocyclic but not simplex codes. Further we find that the construction method also gives Butson Hadamard matrices of order $p^m$.

I. INTRODUCTION

The use of the cocyclic maps to find codes was first done in [1]. The internal structure of the Hadamard matrices used to generate these codes came from the nature of the cocyclic map, which allowed for substantial cut-downs in the computational times required to generate the Hadamard matrices and then the codes. This property of cocycles was further exploited in [2] where the authors constructed cocyclic complex and Butson Hadamard matrices via the trace map. An interesting by-product of this was the uniform construction of cocyclic codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2^s$. These cocyclic codes were found to be simplex codes of type $\alpha$.

A natural extension of this research would be to find codes over $\mathbb{Z}_p$. In this paper the trace map is used to define a cocycle and the cocyclic codes obtained is found to give Butson Hadamard matrices of order $p^{m}$ in [3]. Klappenecker and Roetteler use the trace map in a similar manner to obtain $q + 1$ mutually unbiased bases, where $q$ is an odd prime power. The authors are not aware of the trace map being used before in this manner to find codes.

A linear code $C$ of length $n$ over $\mathbb{Z}_p$ is an additive sub group of $\mathbb{Z}_p^n$. 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 $x$ in $\mathbb{Z}_p^n$, is the number of nonzero components and the Lee weight $W_L(x)$ of $x = (x_1, x_2, \ldots, x_n)$ is $\sum_{i=1}^{n} \min \{x_i, p - x_i\}$. The Hamming and Lee distance between $x, y \in \mathbb{Z}_p^n$ are defined and denoted as $d_H(x, y) = W_H(x - y)$ and $d_L(x, y) = W_L(x - y)$ respectively. Parameters of a linear code over $\mathbb{Z}_p$ are denoted by $[n, k, d_L]$, where $n$ is the length of the code, $k$ is the dimension of the code (see [4]) and $d_L$ is the minimum Lee distance of the code.

If $G$ is a finite group (written multiplicatively with identity 1) and $C$ is an abelian group, a cocycle (over $G$) is a set mapping $\varphi : G \times G \rightarrow C$ which satisfies $\varphi(a, b)\varphi(ab, c) = \varphi(a, bc)\varphi(b, c)$, $\forall a, b, c \in G$. A cocycle is normalized if $\varphi(1, 1) = 1$. A cocycle may be represented as a cocyclic matrix $M_\varphi = [\varphi(a, b)]_{a,b\in G}$ once an indexing of the elements of $G$ has been chosen. In [5], Horadam and Perera define a code over a ring $R$ as a cocyclic code if it can be constructed by using a cocycle or the rows of a cocyclic matrix or is equivalent to such a code.

Let $\omega = \exp\left(\frac{2\pi i}{k}\right)$ 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 square matrix $H = [h_{ij}]$ of order $n$ with elements from $C_k$ is called a Butson Hadamard matrix if and only if $HH^* = nI$, where $H^*$ is the conjugate transpose of $H$. A Butson Hadamard matrix is denoted by $B(n, k)$ and in the case $k = 2$ and $k = 4$, $B(n, k)$ is a Hadamard and a complex Hadamard matrix respectively. The matrix $E = [e_{ij}]$, $e_{ij} \in \mathbb{Z}_k$, which is obtained from $H = [\omega^{e_{ij}}]$ is called the exponent matrix associated with $H$.

A code $C$ over $\mathbb{Z}_p$, $p$-prime, is called a simplex code if every pair of codewords are the same Hamming distance apart. In [4] Gupta introduced the simplex code of type $\alpha$ and $\beta$ over $\mathbb{Z}_4$ and $\mathbb{Z}_2^s$, and in [6] Gupta et. al. constructed the senary simplex codes of type $\alpha, \beta$, and $\gamma$. A major distinguish characteristic of a simplex code of type $\alpha$ over either $\mathbb{Z}_4$, $\mathbb{Z}_2^s$, or $\mathbb{Z}_6$ is that each row of its generator matrix contains every element of the alphabet equally often (see [4], [6], etc.). We construct a code over $\mathbb{Z}_p^s$ with a similar type of generator matrix, but this is not a simplex code over $\mathbb{Z}_p$, for $p > 2$ and $s > 1$. However in the case of $s = 1$ this gives the usual simplex code over $\mathbb{Z}_p$ and when $p = 2$ and $s = 1$, we get the binary simplex code.

In Section II of this paper we outline the theory of the Galois ring $GR(p^m, m)$ and define the trace map over $GR(p^m, m)$. In Section III the trace map is used to define a cocycle over $GR(p^m, m)$ and this cocycle is then used to construct a Butson Hadamard matrix $H$ of order $p^{m}$. The rows of the exponent matrix of $H$ form a $\left[p^{sm}, m, p^{(m-1)}\left(\frac{p^s-1}{4}\right)\right]$ linear code over $\mathbb{Z}_p$.

II. GALOIS RING $GR(p^m, m)$ AND THE TRACE MAP

To be able to define the cocycle, we first need to look at the definition of a Galois ring $GR(p^m, m)$.

Let $p > 2$ be a prime and $s$ a positive integer. The ring of integers modulo $p^s$ is the set $Z_{p^s} = \{0, 1, 2, \ldots, p^s - 1\}$.

Let $h(x) \in Z_{p^s}[x]$ be a monic basic irreducible polynomial of degree $m$ that divides $(x^{p^m - 1} - 1)$. The Galois ring of characteristic $p^s$ and dimension $m$ is defined to be the quotient ring $\left[Z_{p^s} [x]/\langle h(x) \rangle\right]_m$.

The trace map is defined by $tr : Z_{p^s} [x]/\langle h(x) \rangle \rightarrow Z_{p^s}$ for $\phi(x) \in Z_{p^s} [x]/\langle h(x) \rangle$ as $\phi(x) \rightarrow tr(\phi(x))$.
Let $\varphi : GR(p^s, m) \times GR(p^s, m) \rightarrow C_{p^s}$

$$\varphi(c_i, c_j) = (\omega)^{T(c_i, c_j)}$$

is a cocycle.

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

Proof:

(i) This is easy to show using the properties of the trace map.

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

$$S = \sum_{x \in GR(p^s, m)} \varphi(c_i, x)\bar{\varphi}(x, c_j)$$

(1)

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

$$S = \sum_{x \in GR(p^s, m)} \left(\exp\left(\frac{2\pi i}{p^s}\right)\right)^{T(x(c_i, c_j))}$$

(2)

When $c_i = c_j$, $S = p^m$. When $c_i \neq c_j$, from Lemma 2.1 and basic properties of the sum of the $n$th roots of unity, we have

$$S = \sum_{x \in GR(p^s, m)} \left(\exp\left(\frac{2\pi i}{p^s}\right)\right)^{T(x(c_i, c_j))}$$

(3)

$$p^{(m-1)+k} \sum_{t=0}^{p^{k-1}} \left(\exp\left(\frac{2\pi i}{p^s}\right)\right)^{p^k t}$$

(4)

$$= 0.$$  

(5)

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

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

Since $T(c_i, c_j) \in Z_{p^s}$, we can consider the rows of $A$ as codewords over $Z_{p^s}$. Now consider the matrix

$$G_A = \begin{bmatrix} 
T(c_i), & i = 1, 2, \ldots, p^m \\
T(\zeta c_i), & i = 1, 2, \ldots, p^m \\
\vdots & \vdots \\
T(\zeta^{m-1} c_i), & i = 1, 2, \ldots, p^m
\end{bmatrix}_{m \times p^m}$$
where \( c_i \in GR(p^s, m) \). Since \( \zeta^i \) are invertible in \( GR(p^s, m) \) and from Lemma 2.1, each row of \( G_A \) contains each element of \( Z_{p^s} \) equally often, i.e., \( p^{s(m-1)} \) times. Further the rows of \( G_A \) are linearly independent. Therefore the code generated by \( G_A \) is a linear code over \( Z_{p^s} \). In addition the structure of \( G_A \) is very similar to the generator matrices of the simplex codes in \([2],[4],[6]\) over \( Z_2, Z_2^2 \) and \( Z_6 \).

Now taking all linear combinations of the rows of \( G_A \) we obtain
\[
A = [ T(c_i c_j) ]_{i,j \in  G(p^s, m)}.
\]

Therefore \( G_A \) is a generator matrix of the code \( A \) and hence \( A \) is a linear code over \( Z_{p^s} \) with the \( p \)-dimension \( k = m \). Let \( x \) be any nonzero codeword in \( A \). Then \( x \) can be written as \( x = (x_1, x_2, \ldots, x_{p^s m}) \), where \( x_i \in D_k \). From Lemma 2.1, each element of \( D_k \) will appear in \( x \) equally often, i.e., \( p^{s(m-1)+k} \) times. Therefore the Lee weight of \( x \) is \( W_L(x) = p^{s(m-1)} \left( \frac{p^s - 2}{p^s - 1} \right) \) and the Hamming weight is \( W_H(x) = p^{s(m-1)+k} (p^s - k - 1) \). The minimum Lee and Hamming weights of the codewords of \( A \) are obtained when \( k = s - 1 \). Thus \( W_L(x) = p^{s(m-1)} \left( \frac{p^s - 2}{p^s - 1} \right) \) and \( W_H(x) = p^{s(m-1)} (p - 1) \).

Therefore the parameters of the code \( A \) are \([n, k, d_L, d_H] = [p^m, m, p^{s(m-1)} \left( \frac{p^s - 2}{p^s - 1} \right), p^{s(m-1)} (p - 1)]\).

Note that the code \( A \) is not equidistance with respect to either the Lee or Hamming distances. Therefore this is not a simplex code over \( Z_{p^s} \).

When \( p > 2 \) and \( s = 1 \), then \( GF(p, m) \) is the Galois field of order \( p^m \). Hence

(i) The map defined by
\[
\varphi : GF(p, m) \times GF(p, m) \to C_p
\]
\[
\varphi(c_1, c_2) = (w)T(c_1c_2)
\]
is a cocycle and the matrix \( H = M_{\varphi} = [\varphi(c_1 c_2)]_{c_1, c_2 \in GF(p, m)} \) is a Butson Hadamard matrix of order \( p^m \).

(ii) Rows of the exponent matrix associated with \( M_{\varphi} \), i.e., \( A = [ T(c_i c_j) ]_{c_i, c_j \in GF(p, m)} \), form a \( Z_{p^s} \) - linear code with parameters \([n, k, d_H] = [p^m, m, p^{s(m-1)} (p - 1)]\), where \( d_H \) is the minimum Hamming distance. Also every nonzero codeword has constant Hamming weight \( W_H = p^{s(m-1)} (p - 1) \) and constant Lee weight \( W_L = \frac{p^{s(m-1)} (p - 1)}{(p^s - 1)} \). Thus the code \( A \) is a simplex code over \( Z_{p^s} \).

In the case \( p = 2 \), the cocyclic matrix obtained is a Hadamard matrix and the rows of the matrix \( A \) obtained by substituting the entries of \( H \) which are 1 by 0 and -1 by 1 (i.e., \( A = [ T(c_i c_j) ]_{c_i, c_j \in GF(2, m)} \)) the exponent matrix associated with \( H \) is a binary linear code with parameters \([n, k, d_L] = [2^m - 1, m, 2^{m-1}]\).

In addition the rows of the matrix \( A^* \) obtained by deleting the all zero column of \( A \) form an \( Z_2 \) - simplex code \([2^{m-1} - 1, m, 2^{m-1}]\).

It is important to note here that the Hadamard matrix obtained by the above construction is of Paley type.

IV. CONCLUSION

Here the trace map was used to define a cocycle and the cocyclic matrix obtained is found to give Butson Hadamard matrices of order \( p^m \).

A natural extension of this work would be to generate cocyclic codes over \( Z_n \) for any positive integer \( n \). This is currently under investigation.

ACKNOWLEDGMENT

The authors would like to thank Serdar Boztas for his helpful comments on this paper and especially for pointing out the relationship with Klappenecker and Roetteler’s paper [3].

REFERENCES


