New Linear Codes over $\mathbf{Z_{p^s}}$ 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 $\mathbf{Z_4}$ and $\mathbf{Z_{2^s}}$. We extend this technique to obtain new linear codes over $\mathbf{Z_{p^s}}$. 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^{sm}.**

I. Introduction

The use of the cocyclic map 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 $\mathbf{Z_4}$ and $\mathbf{Z_{2^s}}$. These cocyclic codes were found to be simplex codes of type α.

A natural extension of this research would be to find codes over Z_{p^s}. In this paper the trace map is used to define a cocycle and the cocyclic matrix obtained is found to give Butson Hadamard matrices of order p^{sm}. 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 Z_{p^s} is an additive sub group of $Z_{p^s}^n$. 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 $Z_{p^s}^n$ 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 $\{x_i, p^s - x_i\}$. The Hamming and Lee distance between $x, y \in Z_{p^s}^n$ 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 Z_{p^s} are denoted by $[n, k, d_L]$, where n is the length of the code, k is the p-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 $\varphi : G \times G \to C$ 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 $\omega = exp(\frac{2\pi i}{k})$ be the complex kth root of unity and $C_k = \{1, \omega, \omega^2, \ldots, \omega^{k-1}\}$ be the multiplicative group of all complex kth roots of unity. A square matrix $H = [h_{i,j}]$ 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 $E = [e_{i,j}]$, $e_{i,j} \in Z_k$, which is obtained from $H = [\omega^{e_{i,j}}] = [h_{i,j}]$ is called the exponent matrix associated with H.

A code C over 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 α and β over Z_4 and Z_{2^s} and in [6] Gupta et. al. constructed the senary simplex codes of type α, β and γ. A major distinguish characteristic of a simplex code of type α over either Z_4, Z_{2^s} or 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 Z_{p^s} with a similar type of generator matrix, but this is not a simplex code over Z_{p^s} for $p > 2$ and $s > 1$. However in the case of $s = 1$ this gives the usual simplex code over 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 $GR(p^s, m)$ and define the trace map over $GR(p^s, m)$. In Section III the trace map is used to define a cocycle over $GR(p^s, m)$ and this cocycle is then used to construct a Butson Hadamard matrix H of order p^{sm}. The rows of the exponent matrix of H form a $\left[p^{sm}, m, p^{s(m-1)}\left(\frac{p^{2s}-p^{2(s-1)}}{4}\right)\right]$ linear code over $\mathbf{Z_{p^s}}$.

II. Galois ring $\mathbf{GR(p^s, m)}$ and the Trace Map

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

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 $Z_{p^s}[x]/(h(x))$ and is denoted by $GR(p^s, m)$. 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. Consequently we say that ζ is a primitive element of $GR(p^s, m)$ and find that $GR(p^s, m) = Z_{p^s}[\zeta]$. Thus $GR(p^s, m) =< 1, \zeta, \zeta^2, \ldots, \zeta^{m-1} >$ and hence $|GR(p^s, m)| = p^{sm}$.

Every element $u \in GR(p^s, m)$ has a unique representation as $u = \sum_{i=0}^{s-1} p^i u_i$, 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 $GR(p^s, m)$ and the set $\mathcal{T}$ is called the Teichmuller set. Note that u is invertible if and only if $u_0 \neq 0$. Hence every non-invertible element of $GR(p^s, m)$ can be written as $u = \sum_{i=k}^{s-1} p^i u_i, \quad k = 1, 2, \ldots, s-1$. By using the p - adic representation of elements of $GR(p^s, m)$, the Frobenius automorphism f is defined in [7], [8], [9], etc. as

$$\begin{gathered} f : GR(p^s, m) \rightarrow GR(p^s, m) \\ f(u) = \sum_{i=0}^{s-1} p^i u_i^p. \end{gathered}$$

Note that when $s = 1$, f is the usual Frobenius automorphism for the Galois field $GF(p, m)$ (see [10]).

The relative trace map over $GR(p^s, m)$ is defined as

$$\begin{gathered} T : GR(p^s, m) \rightarrow Z_{p^s} \\ T(u) = u + f(u) + f^2(u) + \ldots + f^{m-1}(u). \end{gathered}$$

In addition to being a surjective linear transformation, the trace map also satisfies the following property:

Lemma 2.1: For any $b \in GR(p^s, m)$, as x ranges over $GR(p^s, m)$, $T(xb)$ takes elements in $D_k = \{p^k t \mid t = 0, 1, 2, \ldots, p^{s-k} - 1\}$ equally often, i.e., $p^{s(m-1)+k}$ times, where $k = 0, 1, 2, \ldots, s-1$.

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

$$\alpha : GR(p^s, m) \rightarrow V.$$

It is easy to see that α sets up a one to one correspondence between the elements of $GR(p^s, m)$ and the m - tuples of V over D_0. Thus as x ranges over $GR(p^s, m)$, each component $T(x\zeta^i)$, for $i = 0, 1, 2, \ldots, m-1$, must take each element of D_0 equally often, i.e., $\frac{p^{sm}}{p^s} = p^{s(m-1)}$ times. In general, for invertible element $b \in GR(p^s, m)$ (i.e., $b = \sum_{i=0}^{s-1} p^i u_i; \quad u_i \in \mathcal{T}$ and $u_0 \neq 0$), as x ranges over $GR(p^s, m)$, $T(xb)$ must also assume each element of D_0 equally often, i.e., $p^{s(m-1)}$ times. If b is not invertible then $b = \sum_{i=k}^{s-1} p^i u_i, \quad k = 1, 2, \ldots, s-1$. Now from the expansion of $T(xb)$ and induction on k, as x ranges over $GR(p^s, m)$, $T(xb)$ must takes each element of D_k equally often, i.e., $\frac{p^{sm}}{p^{s-k}} = p^{sm-(s-k)} = p^{s(m-1)+k}$ times. This complete the proof.

III. Cocyclic Butson Hadamard Matrices of order p^{sm} and Linear codes over $\mathbf{Z_{p^s}}$

Defining a cocycle using the trace map, we can obtain cocyclic Butson Hadamard matrices. It turns out that the exponent matrices of these Buston Hadamard matrices are linear codes which are similar in structure to the simplex codes of type α over Z_4, Z_{2^s} and Z_6 found by [2], [4], [6], but are not simplex codes in the case $p > 2$ and $s > 1$. The important thing to note is that the trace map has not been used in this manner before, that the trace map is not a cocycle and that the Butson Hadamard matrix is obtained using the cocycle.

Proposition 3.1: Let p be a prime, $p > 2$. Let $GR(p^s, m)$ be the Galois ring of characteristic p^s and C_{p^s} be the multiplicative group of all complex (p^s)th roots of unity.

(i) The set mapping

$$\begin{gathered} \varphi : GR(p^s, m) \times GR(p^s, m) \rightarrow C_{p^s} \\ \varphi(c_i, c_j) = (\omega)^{T(c_i c_j)} \end{gathered}$$

is a cocycle.

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

(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

$$[n, k, d_L, d_H] = \left[p^{sm}, m, p^{s(m-1)}\left(\frac{p^{2s} - p^{2(s-1)}}{4}\right), p^{sm-1}(p-1)\right].$$

Proof:

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

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

$$S = \sum_{\forall x \in GR(p^s, m)} \varphi(c_i, x)\overline{\varphi(x, c_j)}, \tag{1}$$

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

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

When $c_i = c_j$, $S = p_1^{sm}$. When $c_i \neq c_j$, from Lemma 2.1 and basic properties of the sum of the nth roots of unity, we have

$$\begin{aligned} S &= \sum_{\forall x \in GR(p^s, m)} \left(exp\left(\frac{2\pi i}{p^s}\right)\right)^{T(x(c_i - c_j))} && (3) \\ &= p^{s(m-1)+k} \sum_{t=0}^{p^{s-k}-1} \left(exp\left(\frac{2\pi i}{p^s}\right)\right)^{p^k t} && (4) \\ &= 0. && (5) \end{aligned}$$

(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

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

where $c_i \in GR(p^s, m)$. Since ζ^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_4, Z_{2^s} and Z_6.

Now taking all linear combinations of the rows of G_A we obtain

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

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 $x = (x_1, x_2, \ldots, x_{p^{sm}})$, where $x_i \in D_k$. From Lemma 2.1, each element in D_k will appear in x equally often, i.e., $p^{s(m-1)+k}$ times. Therefore the Lee weight of x is $W_L(x) = p^{s(m-1)} \left(\frac{p^{2s} - p^{2k}}{4} \right)$ and the Hamming weight is $W_H(x) = p^{s(m-1)+k} \left(p^{s-k} - 1 \right)$. The minimum Lee and Hamming weights of the codewords of A are obtained when $k = s - 1$. Thus min $W_L(x) = p^{s(m-1)} \left(\frac{p^{2s} - p^{2(s-1)}}{4} \right)$ and min $W_H(x) = p^{sm-1} (p - 1)$. Therefore the parameters of the code A are $[n, k, d_L, d_H] = \left[p^{sm}, m, p^{s(m-1)} \left(\frac{p^{2s} - p^{2(s-1)}}{4} \right), p^{sm-1} (p - 1) \right]$.

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

$$\varphi : GF(p, m) \times GF(p, m) \to C_p$$
$$\varphi(c_i, c_j) = (w)^{T(c_i c_j)}$$

is a cocycle and the matrix $H = M_\varphi = [\varphi(c_i, c_j)]_{\forall c_i, c_j \in GF(p,m)}$ is a Butson Hadamard matrix of order p^m.

(ii) Rows of the exponent matrix associated with M_φ, i.e., $A = [T(c_i c_j)]_{\forall c_i, c_j \in GF(p,m)}$, form a Z_p - linear code with parameters $[n, k, d_H] = [p^m, m, p^{m-1}(p-1)]$, where d_H is the minimum Hamming distance. Also every nonzero codeword has constant Hamming weight $W_H = p^{m-1}(p - 1)$ and constant Lee weight $W_L = \frac{p^{m-1}}{4}(p^2 - 1)$. Thus the code A is a simplex code over Z_p.

In the case $p = 2$, the cocylic 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., $A = [T(c_i c_j)]_{\forall c_i, c_j \in GF(2,m)}$, the exponent matrix associated with H) is a binary linear code with parameters $[n, k, d_L] = [2^m, m, 2^{m-1}]$.
In addition the rows of the matrix A^* obtained by deleting the all zero column of A form an Z_2 - simplex code $[2^m - 1, m, 2^{m-1}]$.

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^{sm}.

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 Boztaş for his helpful comments on this paper and especially for pointing out the relationship with Klappenecker and Roetteler's paper [3].

References

[1] A. Baliga, “New self-dual codes from cocyclic Hadamard matrices,” *J. Combin. Maths. Combin. Comput.*, vol. 28, pp. 7–14, 1998.

[2] N. Pinnawala and A. Rao, “Cocyclic simplex codes of type α over Z_4 and Z_{2^s},” *IEEE Trans. Inform. Theory*, vol. 50, no. 9, pp. 2165–2169, 2004.

[3] A. Klappenecker and M. Roetteler, “Constructions of mutually unbiased bases,” in *Proc. International Conf. Finite Fields and Apps. (Fq7, Lecture Notes in Comp. Sci., LNCS2948*. Springer, 2004, pp. 137–144.

[4] M. K. Gupta, “On some linear codes over z_{2^s},” Ph.D. dissertation, Department of Mathematics, Indian institute of technology, 1999.

[5] K. J. Horadam and A. A. I. Perera, “Codes from cocycles,” in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes; AAECC-12, Lecture Notes in Comp. Sci., LNCS 1255*. Springer-Verlag, Berlin, June 1997, pp. 151–163.

[6] M. K. Gupta, D. G. Glynn, and T. A. Gulliver, “On some quaternary self orthogonal codes,” in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes; AAECC-14, Lecture Notes in Comp. Sci., LNCS 2227*, S. Boztas and I. E. Shparlinski, Eds. Springer, 2001, pp. 112–121.

[7] J. T. Blackford and D. K. Ray-Chaudhuri, “A transform approach to permutation group of cyclic codes over galois rings,” *IEEE Trans. Inform. Theory*, vol. 46, no. 7, pp. 2350–2358, 2000.

[8] A. B. Calderbank and N. J. A. Sloane, “Modular and p - adic cyclic codes,” *Des. Codes Crypto*, vol. 6, pp. 21–35, 1995.

[9] Z. X. Wan, *Lectures on finite fields and Galois rings*. New Jersey: World Sciencetific, 2003.

[10] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge University press, 1997.