Cocyclic Butson Hadamard matrices and Codes over $\mathbb{Z}_n$ via the Trace Map

N. Pinnawala and A. Rao

Abstract. Over the past couple of years trace maps over Galois fields and Galois rings have been used very successfully to construct cocyclic Hadamard, complex Hadamard and Butson Hadamard matrices and subsequently to generate simplex codes over $\mathbb{Z}_4, \mathbb{Z}_{2^s}$ and $\mathbb{Z}_p$ and new linear codes over $\mathbb{Z}_{p^s}$. Here we define a new map, the trace-like map and more generally the weighted-trace map and extend these techniques to construct cocyclic Butson Hadamard matrices of order n^m for all n and m and linear and non-linear codes over $\mathbb{Z}_n$.

1. Introduction

The cocyclic map has been used to construct Hadamard matrices (see [**2**]) and these Hadamard matrices were found to yield binary extremal self-dual codes [**1**]. 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 [**12**] the authors exploited this property to construct cocyclic Complex and Butson Hadamard matrices by defining the cocycle maps via the trace maps over Galois rings $GR(4, m)$ and $GR(2^e, m)$ respectively. In [**13**], this method was extended to construct some new linear codes over $\mathbb{Z}_{p^e}$ for prime $p > 2$ and positive integer e. A challenging open problem was the extension of this method to construct Butson Hadamard matrices of order n for any positive integer n. The prime factorization of n, i.e., $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ and the isomorphism $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \dots \times \mathbb{Z}_{p_k^{e_k}}$ paves the way to focus our attention on the ring $R(n, m) = GR(p_1^{e_1}, m) \times GR(p_2^{e_2}, m) \times \dots \times GR(p_k^{e_k}, m)$, where m is a positive integer. However there is no known map over this ring similar to the trace map over Galois rings and Galois fields. In this paper, we define a new map, the trace-like map, over the ring $R(n, m)$. A generalization of this map, called the weighted-trace map, is used in [**9**] for Fourier transforms. These maps satisfy fundamental properties parallel to the other trace maps, and can be used in a similar manner to the trace maps in [**12**] and [**13**] to first uniformly construct

2000 *Mathematics Subject Classification.* Primary 94B05; Secondary 11T71.
Key words and phrases. Cocycle, complex Hadamard, Butson, simplex codes, Trace, exponent.
The work of N. Pinnawala was carried out during his Ph.D. studies and was supported by a School of Mathematical and Geospatial Sciences Scholarship.

cocyclic Butson Hadamard matrices of any order n and then linear and non-linear codes over $\mathbb{Z}_n$.

A linear code $\mathcal{C}$ of length n over the integers modulo k (i.e., $\mathbb{Z}_k = \{0, 1, 2, \ldots, k-1\}$) is an additive subgroup of $\mathbb{Z}_k^n$. An element of $\mathcal{C}$ is called a codeword and a generator matrix of $\mathcal{C}$ is a matrix whose rows generate $\mathcal{C}$. 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 nonzero components 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.

A cocycle is a set mapping, $\varphi : G \times G \to C$, which satisfies

$$\varphi(a, b)\varphi(ab, c) = \varphi(b, c)\varphi(a, bc), \ \ \forall \ \ a, b, c \in G,$$

where G is a finite group and C is a finite abelian group. The matrix $M_\varphi = [\varphi(x, y)]_{x,y\in G}$ is called a cocyclic matrix.

Butson Hadamard matrices were first introduced by Butson in 1962 [**4**]. A square matrix H of order $n \geq 2$ all of whose elements are complex p^{th} roots of unity (p not necessarily a prime) is called a Butson Hadamard matrix, denoted by $BH(n, p)$, iff $HH^* = nI$, where H^* is the conjugate transpose of H and I is the identity matrix of order n. In 1979, Drake [**6**] introduced generalized Hadamard matrices. A square matrix $H = [h_{ij}]$ of order $n \geq 2$ over a group G is called a generalized Hadamard matrix $GH(n, G)$ if for $i \neq j$ the sequence $\{h_{ix}h_{jx}^{-1}\}$ with $1 \leq x \leq n$ contains every element of G equally often. For prime p the definition of a $BH(n, p)$ and a $GH(n, \mathbb{C}_p)$ are equivalent, where $\mathbb{C}_p$ denotes the multiplicative group of all complex p^{th} roots of unity. On the other hand, if $p = mt$, where m is a prime and $t > 1$, then there exists a Butson Hadamard matrix of order m over $\mathbb{C}_p$, but certainly no generalized Hadamard matrix of order m over $\mathbb{C}_p$ (Remark 1.3, [**6**]). The authors have been unable to find a reference for uniform construction of Butson Hadamard matrices. This paper provides such a uniform construction.

In Section 2 we study the Galois ring $GR(p^e, m)$ and the properties of the trace map over $GR(p^e, m)$. A cocycle over $GR(p^e, m)$ is defined and the cocyclic Butson Hadamard matrix of order p^{em} is constructed. This matrix is then used to construct linear codes over $\mathbb{Z}_{p^e}$. Section 3 details the ring $R(n, m) = GR(p_1^{e_1}, m) \times GR(p_2^{e_2}, m), n = p_1^{e_1}p_2^{e_2}$, and the properties of the trace-like map over $R(n, m)$. The trace-like map is then used to construct cocyclic Butson Hadamard matrices of order n^m and the exponent matrices are used to construct cocyclic codes over $\mathbb{Z}_n$. In addition, these results are easily extended to construct codes over $\mathbb{Z}_n$ for $n = p_1^{e_1}p_2^{e_2} \ldots p_k^{e_k}$. We also point out the relationship to the senary simplex codes of type α in [**8**]. In Section 4 the Hamming, Lee, Euclidean and Chinese Euclidean distances of these codes are calculated. A further generalization of the trace-like map, called the weighted-trace map (which first appeared in [**9**]) is studied in Section 5 and used to construct cocyclic Butson Hadamard matrices and consequently to construct non-linear codes over $\mathbb{Z}_n$. Finally, in Section 6, we summarize the results of this paper.

2. The Galois ring $GR(p^e, m)$, the trace map and cocyclic $\mathbb{Z}_{p^e}$ - linear codes

For the study of $\mathbb{Z}_{p^e}$-codes, we first need a brief review of the Galois ring of characteristic p^e and dimension m. For more details on Galois rings of this type, the reader is referred to [**11**] and [**14**]. Here we give in detail the results for primes $p > 2$, but the case $p = 2$ is similar and details can be found in [**12**].

Let $p > 2$ be a prime and e be a positive integer. The ring of integers modulo p^e is the set $\mathbb{Z}_{p^e} = \{0, 1, 2, \dots, p^e - 1\}$. 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 $GR(p^e, m) =< 1, \zeta, \zeta^2, \dots, \zeta^{m-1} >$ 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 $u_i \in \mathcal{T} = \{0, 1, \zeta, \zeta^2, \dots, \zeta^{p^m-2}\}$. This representation is called the p-adic representation of elements of $GR(p^e, m)$ and the set $\mathcal{T}$ is called the Teichmüller 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 $u = \sum_{i=k}^{e-1} p^i u_i, \quad k = 1, 2, \dots, e - 1$, and we can represent all the elements of $GR(p^e, m)$ in the form $u^{(k)} = \sum_{i=k}^{e-1} p^i u_i, \quad k = 0, 1, 2, \dots, e - 1$. Using the p-adic representation of the elements of $GR(p^e, m)$, the Frobenius automorphism f is defined in [**3**], [**5**] and [**14**] 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 $GF(p, m)$ (see [**10**]). The trace map over $GR(p^e, m)$ is then 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 f and Tr the trace map satisfies the following properties:

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 surjective.

In addition to these properties the trace map also satisfies the following property.

THEOREM 2.1. *[[**13**], Lemma 2.1] Given a Galois Ring $GR(p^e, m)$, let $D_k = \{p^k t \mid t = 0, 1, \dots, p^{e-k} - 1\} \subseteq \mathbb{Z}_{p^e}$ and $u^{(k)}$ be an element 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 $k = 0, 1, 2, \dots, e - 1$.*

We are now in a position to use the trace map to construct Butson Hadamard matrices and linear codes over $\mathbb{Z}_{p^e}$. Let $\omega = exp(\frac{2\pi\sqrt{-1}}{k})$ be the complex k^{th} root of unity and $\mathbb{C}_k$ be the multiplicative group of all complex k^{th} roots of unity. i.e., $\mathbb{C}_k = \{1, \omega, \omega^2, \dots, \omega^{k-1}\}$. It is well known that

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

Let $H = [h_{i,j}]$ be a square matrix over $\mathbb{C}_k$. 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 2.2. *[**13**], Proposition 3.1] Let p be a prime, $p > 2$. Let $GR(p^e, m)$ be the Galois ring of characteristic p^e and $\mathbb{C}_{p^e}$ be the multiplicative group of all complex p^e th roots of unity.*

i. *The set mapping*
$$\varphi : GR(p^e, m) \times GR(p^e, m) \to \mathbb{C}_{p^e}$$
$$\varphi(c_i, c_j) = (\omega)^{Tr(c_i c_j)}$$
is a cocycle.

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

iii. *The rows of the exponent matrix of M_φ (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 parameters $[n, k, d_L] =$ $\left[p^{em}, m, p^{e(m-1)} \left(\frac{p^{2e} - p^{2(e-1)}}{4}\right)\right]$.*

3. Ring $R(n, m)$ and cocyclic $\mathbb{Z}_n$-linear codes

Let $R(n, m)$ be the direct product of Galois rings. In this section we will look at the structure of the ring $R(n, m)$ and define a new map over $R(n, m)$ using the trace maps over the component Galois Rings. We call this map the trace-like map since it satisfies properties similar to that of the trace maps over Galois rings and Galois fields. We then use this map to construct cocyclic Butson Hadamard matrices of order n^m for all positive integers n and m.

In the first instance let us look at the case $n = p_1^{e_1} p_2^{e_2}$, where $p_1 \neq p_2 \geq 2$ are primes and e_1, e_2 are positive integers. 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, $\mathbb{Z}_n^m \cong (\mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}})^m$. For more details on these results see for example [**7**]. 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 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 $GR(p_2^{e_2}, m) =< 1, \zeta_2, \zeta_2^2, \ldots, \zeta_2^{m-1} >$ respectively. 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 $a \in GR(p_1^{e_1}, m)$ can be expressed as an m-tuple $a = (a_0, a_1, \ldots, a_{m-1})$ over $\mathbb{Z}_{p_1^{e_1}}$ while $b \in GR(p_2^{e_2}, m)$ as $b = (b_0, b_1, \ldots, b_{m-1})$ over $\mathbb{Z}_{p_2^{e_2}}$.

Now consider the direct product of the two Galois rings. 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 $c = (a, b)$, where $a \in GR(p_1^{e_1}, m)$ and $b \in GR(p_2^{e_2}, m)$ 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 $c = (c_0, c_1, \ldots, c_{m-1})$ over $\mathbb{Z}_n$, where $c_i = (a_i, b_i)\ \ i = 0, 1, 2, \ldots, m-1,\ a_i \in \mathbb{Z}_{p_1^{e_1}}$ and $b_i \in \mathbb{Z}_{p_2^{e_2}}$.

Let c, c' be elements in $R(n, m)$. It is easy to see that $R(n, m)$ is a ring under the addition $c + c' = ((c_0 + c_0'), (c_1 + c_1'), \ldots, (c_{m-1} + c_{m-1}')$ and the multiplication $cc' = (c_0 c_0', c_1 c_1', \ldots, c_{m-1} c_{m-1}')$. Also $|R(n, m)| = n^m = (p_1^{e_1} p_2^{e_2})^m = |GR(p_1^{e_1}, m)||GR(p_2^{e_2}, m)|$.

In this context, it is well known that:

$$\text{if } p \text{ is a prime and } a \text{ is any integer then } a^p \equiv a \pmod{p}. \tag{3.1}$$

The next result follows immediately from the Chinese remainder theorem.

Lemma 3.1. *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 $\alpha = (\alpha_1 p_2^{e_2} + \alpha_2 p_1^{e_1}) \bmod n$. Thus $\mathbb{Z}_n = \{(\alpha_1, \alpha_2) | \alpha_1 \in \mathbb{Z}_{p_1^{e_1}}, \alpha_2 \in \mathbb{Z}_{p_2^{e_2}}\}$.*

Theorem 3.2 (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. 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 any $c, c' \in R(n, m)$ 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

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

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

$$\begin{aligned} T(\alpha c) &= p_2^{e_2} Tr_1(\alpha c_1) + p_1^{e_1} Tr_2(\alpha c_2) \\ &= p_2^{e_2}(\alpha c_1 + \alpha^{p_1} g_1(c_1) + \ldots + \alpha^{p_1^{m-1}} g_1(c_1)) \\ &\quad + p_1^{e_1}(\alpha c_2 + \alpha^{p_2} g_2(c_2) + \ldots + \alpha^{p_2^{m-1}} g_2(c_2)) \\ &= p_2^{e_2} \alpha(Tr_1(c_1)) + p_1^{e_1} \alpha(Tr_2(c_2)) \qquad \text{from (3.1)} \\ &= \alpha T(c). \end{aligned}$$

Here g_1 and g_2 are the Frobenius automorphisms over $GR(p_1^{e_1}, m)$ and $GR(p_2^{e_2}, m)$ respectively.

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 $c = (c_1, c_2) \in R(n, m)$ and $T(c) = p_1^{e_1} Tr_2(c_2) + p_2^{e_2} Tr_1(c_1) = p_1^{e_1} + p_2^{e_2}$. 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. □

Since the trace-like map is a combination of the Galois ring traces, it is equi-distributed, just as the component trace maps are equi-distributed. We prove this in the next theorem.

THEOREM 3.3. *For any $c \in R(n,m)$, as x ranges over $R(n,m)$, $T(cx)$ takes each element in*

$$S_{i,j} = \left\{ p_1^i p_2^j t | t = 0, 1, 2, \ldots, \frac{n}{p_1^i p_2^j} - 1 \right\} \tag{3.2}$$

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

Proof: We first 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 $c = 0$, $T(cx) = 0$.

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

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

Here u_{1k} and u_{2k} are in the Teichmüller sets of the respective Galois rings. From Theorem 2.1, as x ranges over $R(n,m)$, since $T(cx) = p_2^{e_2} Tr_1(c_1x_1) + p_1^{e_1} Tr_2(c_2x_2)$, the two trace maps $Tr_1(c_1x_1)$ and $Tr_2(c_2x_2)$ will take values in the sets $D_i = \{p_1^i t_1 \mid 0 \le t_1 \le p_1^{e_1-i} - 1\}$ and $D_j = \{p_2^j t_2 \mid 0 \le t_2 \le p_2^{e_2-j} - 1\}$ respectively. Thus

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

Since the calculation are done modulo n, $\{(p_2^{e_2-j} t_1 + p_1^{e_1-i} t_2) \mid 0 \le t_1 \le p_1^{e_1-i} - 1, 0 \le t_2 \le p_2^{e_2-j} - 1\} \subseteq \mathbb{Z}_n$. From Lemma 3.1, $\{(p_2^{e_2-j} t_1 + p_1^{e_1-i} t_2) \mid 0 \le t_1 \le p_1^{e_1-i} - 1, 0 \le t_2 \le p_2^{e_2-j} - 1\} \cong \mathbb{Z}_{p_1^{e_1-i} p_2^{e_2-j}}$. Hence $T(cx) \in \{p_1^i p_2^j t \mid 0 \le t \le p_1^{e_1-i} p_2^{e_2-j} - 1\} = S_{i,j}$.

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 2.1, $Tr_2(c_2x_2) \in D_j$ (respectively $Tr_1(c_1x_1) \in D_i$) which implies $T(cx) \in \{p_1^{e_1} p_2^j t_2 \mid 0 \le s \le p_2^{e_2-j} - 1\} = S_{0,j}$ (respectively $T(cx) \in S_{i,0}$).

In addition $Tr_1(c_1x_1)$ (respectively $Tr_2(c_2x_2)$) takes each value in D_i (respectively D_j) equally often $p_1^{e_1(m-1)+i}$ (respectively $p_2^{e_2(m-1)+j}$). Hence $T(cx)$ will take each value 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 map over Galois fields and Galois rings, we call it the trace-like map.

EXAMPLE 3.4. Consider the ring $R(6,2) = GF(2,2) \times GF(3,2)$ and the irreducible polynomials $f(x) = x^2 + x + 1$ over $\mathbb{Z}_2$ and $g(x) = x^2 + x + 2$ over $\mathbb{Z}_3$. Thus $GF(2,2) = \mathbb{Z}_2[x]/(f(x))$ 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 $GF(3,2) = \mathbb{Z}_3[\zeta_2]$.

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

$$\begin{array}{lcl} f_1 : GF(2,2) \to GF(2,2) & \text{and} & f_2 : GF(3,2) \to GF(3,2) \\ f_1(c_1) = c_1^2 & & f_2(c_2) = c_2^3 \end{array}$$

respectively.

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

$$\begin{array}{lcl} Tr_1 : GF(2,2) \to \mathbb{Z}_2 & \text{and} & Tr_2 : GF(3,2) \to \mathbb{Z}_3 \\ Tr_1(c_1) = c_1 + f_1(c_1) & & Tr_2(c_2) = c_2 + f_2(c_2) \end{array}$$

respectively. Table 1 illustrates the values of the 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

TABLE 1. Trace map values over $GF(2,2)$ (left) and $GF(3,2)$ (right)

The trace-like map T over the ring $R(6,2)$ is defined as follows:

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

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). Table 2 illustrates the elements of $R(6,2)$ and the values of the trace-like map over $R(6,2)$.

We are now in a position to define a cocycle using the trace-like map.

THEOREM 3.5. *Let $\omega = exp\left(\frac{2\pi i}{n}\right)$ be a complex n^{th} root of unity, where $n = p_1^{e_1} p_2^{e_2}$ and $\mathbb{C}_n$ be the set of all complex n^{th} roots of unity.*

i. *The set mapping $\varphi : R(n,m) \times R(n,m) \to \mathbb{C}_n;\ \ \varphi(a,b) = \omega^{T(ab)}$ is a cocycle.*
ii. *The matrix $M_\varphi = [\varphi(a,b)]_{a,b \in R(n,m)}$ is a Butson Hadamard matrix of order n^m.*
iii. *The rows of the exponent matrix associated with M_φ, (i.e., $A = [T(ab)]$ for $a, b \in R(n,m)$), form a linear code over $\mathbb{Z}_n$ with parameters $[n,k] = [n^m, m]$. In the case $p_1 < p_2$ and $e_1 \leq e_2$, the minimum Hamming weight is given by $d_H = (n - p_1^{e_1} p_2^{e_2 - 1}) n^{m-1}$.*

Proof:

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

TABLE 2. Trace-like map values over R(6,2)

i. Let any $a,b,c\in R(n,m)$. 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 Proposition 2.4 [**2**].

ii. Let $M_\varphi=[\varphi(a,b)]_{a,b\in R(n,m)}$. To prove that $M_\varphi M_\varphi^*=n^mI$, consider the sum

$$S=\sum_{x\in R(n,m)}\varphi(a,x)\overline{\varphi(x,b)}, \tag{3.3}$$

where $\overline{\varphi(x,b)}$ is the complex conjugate of $\varphi(x,b)$. From the properties of the trace-like map (Theorem 3.2)

$$S=\sum_{x\in R(n,m)}\omega^{T(x(a-b))}. \tag{3.4}$$

When $a=b$, $S=n^m$.
When $a\neq b$, from Theorem 3.3 we have

$$S = p_1^i p_2^j n^{m-1} \sum_{t=0}^{\frac{n}{p_1^i p_2^j}-1} \omega^{p_1^i p_2^j t}, \tag{3.5}$$

where $0 \le i \le e_1 - 1$ and $0 \le j \le e_2 - 1$. From the equation (2.1) we have $S = 0$. Thus the matrix M_φ is a Butson Hadamard matrix of order n^m.

iii Let $B = [Tr_1(c_{1\alpha}c_{2\alpha})]$ for $c_{1\alpha}, c_{2\alpha} \in GR(p_1^{e_1}, m)$ and $D = [Tr_2(c_{1\beta}c_{2\beta})]$ for $c_{1\beta}, c_{2\beta} \in GR(p_2^{e_2}, m)$ be the codes over $\mathbb{Z}_{p_1^{e_1}}$ and $\mathbb{Z}_{p_2^{e_2}}$ respectively. Let G_B and G_D be the generator matrices of the codes B and D respectively.

Then a generator matrix for A is given by the $m \times n^m$ matrix:

$$G_A = p_2^{e_2}\left[p_2^{e_2 m} \text{ copies of } G_B\right] + p_1^{e_1}\left[p_1^{e_1 m} \text{ copies of } G_D\right], \tag{3.6}$$

i.e.,

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

where $l = 1, 2, \ldots, p_1^{e_1 m}$ and $t = 1, 2, \ldots, p_2^{e_2 m}$.

We need to show that the rows of G_A are linearly independent and generate A. This is easy to see since the k^{th} row of G_A, $0 \le k \le m-1$ can be written as

$$\vec{x}_k = p_2^{e_2}\left[Tr_1(\zeta_1^k c_{1l})\right] + p_1^{e_1}\left[Tr_2(\zeta_2^k c_{2t})\right], \tag{3.7}$$

where l ranges from 1 to $p_1^{e_1 m}$ and t ranges from 1 to $p_2^{e_2 m}$. Clearly the $\vec{x}_k$ are linearly independent n^m-tuples over $\mathbb{Z}_n$, since the ζ_i^k are linearly independent in $GR(p_i^{e_i}, m), i = 1, 2$, and the Tr_i are surjective and not identically zero.

In addition the code A can be generated by taking all the linear combinations of the rows of G_A. If we consider the rows of A as codewords over $\mathbb{Z}_n$ then from Theorem 3.3 the Hamming weight of each nonzero 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 $e_2 \ge e_1$, the minimum Hamming weight is given by $(n - p_2^{e_2} p_1^{e_1-1})n^{m-1}$. 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 $[n, k, d_H] = \left[n^m, m, (n - p_2^{e_2} p_1^{e_1-1})n^{m-1}\right]$. □

Example 3.6. 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 $R(6,2)$, Tr_1 be the trace map over $GF(2,2)$ and Tr_2 the trace map over $GF(3,2)$.

The code over $GF(2,2)$ obtained via the trace map Tr_1 is:

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

is the generator matrix. Whereas the code over $GF(3,2)$ obtained via the trace map Tr_2 is:

$$D = [Tr_2(a_2b_2)]_{a_2,b_2\in GF(3,2)} = \begin{bmatrix} 0&0&0&0&0&0&0&0&0\\ 0&2&2&0&2&1&1&0&1\\ 0&2&0&2&1&1&0&1&2\\ 0&0&2&1&1&0&1&2&2\\ 0&2&1&1&0&1&2&2&0\\ 0&1&1&0&1&2&2&0&2\\ 0&1&0&1&2&2&0&2&1\\ 0&0&1&2&2&0&2&1&1\\ 0&1&2&2&0&2&1&1&0 \end{bmatrix}$$

which has generator matrix:

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

$$\begin{aligned} G_A &= 3\,[\,9 \text{ copies of } G_B\,] + 2\,[4 \text{ copies of } G_D\,] \\ &= 3\left[\begin{array}{cccc|c|cccc} 0&0&1&1&\dots&0&0&1&1\\ 0&1&1&0&\dots&0&1&1&0 \end{array}\right] + 2\left[\begin{array}{ccccccccc|c} 0&2&2&0&2&1&1&0&1&\dots\\ 0&2&0&2&1&1&0&1&2&\dots \end{array}\right] \\ &= \begin{bmatrix} 0&4&1&3&4&2&5&3&2&\dots\\ 0&1&3&4&2&5&3&2&4&\dots \end{bmatrix} \end{aligned}$$

is a generator matrix for the code $A = [T(ab)]_{a,b\in R(6,2)}$ with parameters $[36, 2, 18]$ given in Figure 1 below.

It is relatively straight forward to extend these results to the case $n = \prod_{i=1}^{k} p_i^{e_i}$.

THEOREM 3.7. *Let Tr_i be the trace map over $GR(p_i^{e_i}, m)$, $i = 1, \dots, k$ as defined in section 2. 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 any $c, c^{'} \in R(n, m)$ 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
iv. For any $c \in R(n, m)$, as x ranges over $R(n, m)$, $T(cx)$ takes each element in

$$S_l = \left\{ \prod_{i=1}^{k} p_i^{l_i} t | t = 0, 1, 2, \dots, \frac{n}{\prod_{i=1}^{k} p_i^{l_i}} - 1 \right\} \tag{3.8}$$

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

THEOREM 3.8. *Let $\omega = exp\left(\frac{2\pi\sqrt{-1}}{n}\right)$ be the complex n^{th} root of unity, where $n = \prod_{i=1}^{k} p_i^{e_i}$, and $\mathbb{C}_n$ be the set of all complex nth root of unity.*

i *The set mapping*

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

FIGURE 1. Code $A = [T(ab)]_{a,b\in R(6,2)}$ with parameters $[36, 2, 18]$

$$
\begin{gathered}
\varphi : R(n,m) \times R(n,m) \to \mathbb{C}_n \\
\varphi(a,b) = \omega^{T(ab)}
\end{gathered}
$$

is a cocycle.

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

iii *The rows of the exponent matrix associated with M_φ (i.e., $A = [T(ab)]$ for $a, b \in R(n,m)$) form a linear code over $\mathbb{Z}_n$ with parameters $[n,k] = [n^m, m]$. In the case $p_1 < p_2 < \ldots < p_k$ and $e_1 \le e_2 \le \ldots \le e_k$, the minimum Hamming weight is given by $d_H(n - p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k - 1})n^{m-1}$.*

The generator matrix G_A of the code A is given by

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

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

Note that each row of G_A contains the elements of $\mathbb{Z}_n$ equally often n^{m-1} times.

In the case $n = 6$, the code obtained by the construction above can be shown to be the senary simplex code [**8**]. 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 a senary simplex code, because its codewords are equidistant with respect to the Chinese Euclidean distance. Thus we have shown the following:

Corollary 3.9. *In the case of $p_1 = 2, p_2 = 3, e_1 = e_2 = 1$, the generator matrix G_A 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.*

4. Lee, Euclidean and Chinese Euclidean Weights of the codewords of A

Let $n = \prod_{i=1}^{k} p_i^{e_i}$ and $A = [T(ab)]_{a,b \in R(n,m)}$ the code defined in Theorem 3.8,(iii). For $i = 1, 2, \ldots, k$, let $l = (l_1, l_2, \ldots, l_k)$, $0 \le l_i \le e_i$, $n_l = \prod_{i=1}^{k} p_i^{l_i}$ and $\bar{n_l} = n/n_l$.

From Theorem 3.7(vi), if $\mathbf{x}$ is a codeword in A, then the coordinates of $\mathbf{x}$ take values in $S_l = \{n_l t \mid t = 0, 1, 2, \ldots, \bar{n}_l - 1\}$ equally often $n_l n^{m-1}$ times.

Then depending upon the range of the l_i, the Lee ($W_L(\mathbf{x})$), Euclidean ($W_E(\mathbf{x})$) and the Chinese Euclidean ($W_{CE}(\mathbf{x})$) weights of $\mathbf{x}$ are as per the table below:

Case I: $p_1 = 2$, $p_i > 2$, $2 \le i \le k$					
Range of l_1	Range of l_i $2 \le l_i \le k$	n_l	$W_L(\mathbf{x})$	$W_E(\mathbf{x})$	$W_{CE}(\mathbf{x})$
$0 \le l_1 \le e_1 - 1$	$0 \le l_i \le e_i$	$2^{l_1} \prod_{i=2}^{k} p_i^{l_i}$	$\frac{1}{4} n^{m+1}$	$\frac{n^m(n^2+2n_l^2)}{12}$	$2n^m$
$l_1 = e_1$	$0 \le l_i \le e_i - 1$	$2^{e_1} \prod_{i=2}^{k} p_i^{l_i}$	$\frac{n^{m-1}(n^2-n_l^2)}{4}$	$\frac{n^m(n^2-n_l^2)}{12}$	
Case II: $p_i > 2$ $\forall i$					
$0 \le l_1 \le e_1$	$0 \le l_i \le e_i$	$\prod_{i=0}^{k} p_i^{l_i}$	$\frac{n^{m-1}(n^2-n_l^2)}{4}$	$\frac{n^m(n^2-n_l^2)}{12}$	$2n^m$

5. The Weighted-Trace map

So far we have studied the trace-like map and its fundamental properties parallel to the trace maps 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). It is fairly straight forward to extend this notion to the ring $R(d,n)$ constructed by taking the direct product of Galois rings and Galois fields of different degrees (say $m_1, m_2, \ldots, m_k$). Here $d = p_1^{e_1 m_1} p_2^{e_2 m_2} \ldots p_k^{e_k m_k}$ and $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$.

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., $R(d,n) = GR(p_1^{e_1}, m_1) \times GR(p_2^{e_2}, m_2) \times \ldots \times GR(p_k^{e_k}, m_k)$, where $d = p_1^{e_1 m_1} p_2^{e_2 m_2} \ldots p_k^{e_k m_k}$ and $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$. 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 5.1 (Weighted-trace map). [**9**] 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 3.2 we can prove that the weighted-trace map satisfies the following properties:

Theorem 5.2. *Let T_w be the weighted-trace map over the ring $R(d,n)$, where $d = p_1^{e_1 m_1} p_2^{e_2 m_2} \ldots p_k^{e_k m_k}$ and $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$. 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 3.3.

Theorem 5.3. *Let $c = (c_1, c_2) \in R(d,n)$ and T_w be the weighted-trace map over $R(d,n)$ as above. As x ranges over $R(d,n)$, $T_w(cx)$ takes each element in $S_l = \{\prod_{i=1}^k p_i^{l_i} t \mid t = 0, 1, 2, \ldots, \bar{n_l} - 1\}$ equally often i.e., dn_l/n times, where for $i = 1, 2, \ldots, k$, $l = (l_1, l_2, \ldots, l_k)$, $0 \le l_i \le e_i$, $n_l = \prod_{i=1}^k p_i^{l_i}$, and $\bar{n_l} = n/n_l$.*

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

THEOREM 5.4. *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 $\mathbb{C}_n$ be the multiplicative group of all complex n^{th} roots of unity and T_w be the weighted-trace map over the ring $R(d,n)$ as defined above. Then*
(i) The set mapping defined by

$$\varphi : R(d,n) \times R(d,n) \to \mathbb{C}_n$$
$$\varphi(a,b) = \omega_n^{T_w(ab)}$$

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 $w_H = d(p_1 - 1)/p_1)$ 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 similar to that of Theorem 3.5.
(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, N, is also $= \prod_{i=1}^{k} p_i^{e_i m_i} = d$. From Theorem 5.3 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 $w_H = d - p_k^{e_k m_k} \ldots p_2^{e_2 m_2} p_1^{e_1 m_1 - 1} = d(p_1 - 1)/p_1$. Thus A_w is a $(d, d, d(p_1 - 1)/p_1)$ code over $\mathbb{Z}_n$. $\square$
The next example illustrates this result.

EXAMPLE 5.5. 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

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

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 $c_2 \in GF(3,2)$.

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

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

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

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

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

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

6. Conclusion

In this paper we introduced a new map, the trace-like map and in general the weighted-trace map, to construct Butson Hadamard matrices and consequently to construct linear and non-linear cocyclic codes over $\mathbb{Z}_n$ for $n = p_1^{e_1}p_2^{e_2}$ and more generally for $n = p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}$.

References

1. A. Baliga, *New self-dual codes from cocyclic Hadamard matrices*, J. Combin. Maths. Combin. Comput. **28** (1998), 7–14.
2. A. Baliga and K. J. Horadam, *Cocyclic Hadamard matrices over $Z_t \times Z_2^2$*, Australas. J. Combin. **11** (1995), 123–134.
3. J. T. Blackford and D. K. Ray-Chaudhuri, *A transform approach to permutation group of cyclic codes over Galois rings*, IEEE Trans. Info. Theory **46** (2000), no. 7, 2350–2358.
4. A. T. Butson, *Generalised Hadamard matrices*, Proc. Amer. Math. Soc. **13** (1962), 894–898.
5. A. B. Calderbank and N. J. A. Sloane, *Modular and p - adic cyclic codes*, Designs Codes and Crypto **6** (1995), 21–35.
6. D. A. Drake, *Partial geometries and generalised Hadamard matrices*, Canad. J. Math. **31** (1979), 217–227.
7. A. J. Gareth and J. J. Mary, *Elementary number theory*, Springer-Verlag, 1998.
8. M. K. Gupta, D. G. Glynn, and T. A. Gulliver, *On some quaternary self orthogonal codes*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes; AAECC-14 (S. Boztas and I. E. Shparlinski, eds.), Lecture Notes in Computer Science LNCS 2227, Springer, 2001, pp. 112–121.

9. K. J. Horadam and A. Rao, *Fourier transforms from a generalised trace map*, 2006 IEEE International Symposium on Information Theory (Seattle, U.S.A.), July 2006, pp. 1080–1084.
10. R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University press, 1997.
11. B. McDonald, *Finite rings with identity*, Marcel Dekker, New York, 1974.
12. 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** (2004), no. 9, 2165–2169.
13. A. Rao and N. Pinnawala, *New linear codes over Z_{p^s} via the trace map*, 2005 IEEE International Symposium on Information Theory (Adelaide, Australia), 4-9 September 2005, pp. 124–126.
14. Z. X. Wan, *Lectures on finite fields and Galois rings*, World Scientific, New Jersey, 2003.

School of Mathematical and Geospatial Sciences,, RMIT University, GPO Box 2476V,, Melbourne VIC - 3001, Australia
E-mail address: nimalsiri.pinnawala@rmit.edu.au

School of Mathematical and Geospatial Sciences,, RMIT University, GPO Box 2476V,, Melbourne VIC - 3001, Australia
E-mail address: asha@rmit.edu.au