The main problem that should be the focus of further research is to prove that there are no nontrivial perfect codes in the Johnson scheme by using the concept of k-regular codes.

ACKNOWLEDGMENT

The authors would like to thank the two anonymous referees whose comments have amended this correspondence.

REFERENCES

[1] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1978.

[2] J. H. van Lint, "Nonexistence theorems for perfect error-correcting codes," in *Computers in Algebra and Number Theory, vol. IV, SIAM-AMS Proceedings*, 1971.

[3] A. Tietäväinen, "On the nonexistence of perfect codes over finite fields," *SIAM J. Appl. Math.*, vol. 24, pp. 88–96, 1973.

[4] V. A. Zinoviev and V. K. Leontiev, "The nonexistence of perfect codes over Galois fields," *Probl. Control and Inform. Theory*, vol. 2, pp. 123–132, 1973.

[5] M. R. Best, "Perfect codes hardly exist," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 349–351, May 1983.

[6] Q. A. Nguyen, L. Györfi, and J. L. Massey, "Constructions of binary constant-weight cyclic codes and cyclically permutable codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 940–949, May 1992.

[7] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, "A new table of constant-weight codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1334–1380, Nov. 1990.

[8] F. R. K. Chung, J. A. Salehi, and V. K. Wei, "Optical orthogonal codes: Design, analysis, and applications," *IEEE Trans. Inform. Theory*, vol. 35, pp. 595–604, May 1989.

[9] T. Etzion, "Constructions of error-correcting DC-free block codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 899–905, July 1990.

[10] H. C. A. van Tilborg and M. Blaum, "On error-correcting balanced codes," *IEEE Trans. Inform. Theory*, vol. 35, pp. 1091–1095, Sept. 1989.

[11] P. Delsarte, "An algebraic approach to association schemes of coding theory," *Philips J. Res.*, vol. 10, pp. 1–97, 1973.

[12] E. Biggs, "Perfect codes in graphs," *J. Combin. Theory Ser. B*, vol. 15, pp. 289–296, 1973.

[13] E. Bannai, "Codes in bi-partite distance-regular graphs," *J. London Math. Soc.*, vol. 2, pp. 197–202, 1977.

[14] P. Hammond, "On the nonexistence of perfect codes and nearly perfect codes," *Discr. Math.*, vol. 39, pp. 105–109, 1982.

[15] C. Roos, "A note on the existence of perfect constant weight codes," *Discr. Math.*, vol. 47, pp. 121–123, 1983.

[16] T. Etzion, "On the nonexistence of perfect codes in the Johnson scheme," *SIAM J. Discr. Math.*, vol. 9, no. 2, pp. 201–209, May 1996.

[17] ——, "On perfect codes in the Johnson scheme," *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, vol. 56, pp. 125–130, 2001.

[18] W. J. Martin, "Completely regular subsets," Ph.D. dissertation, Univ. Waterloo, Waterloo, ON, Canada, 1992.

[19] O. Shimabukuro, "On the nonexistence of perfect codes in $J(2w+p^2, w)$," *Ars Combinatoria*, to be published.

[20] R. Ahlswede, H. K. Aydinian, and L. H. Khachatrian, "On perfect codes and related concepts," *Des., Codes Cryptogr.*, vol. 22, no. 3, pp. 221–237, Jan. 2001.

[21] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*. Reading, MA: Addison-Wesley, 1994.

[22] N. J. Fine, "Binomial coefficients modulo a prime," *Amer. Math. Monthly*, vol. 54, pp. 589–592, 1947.

Cocyclic Simplex Codes of Type α Over $\boldsymbol{Z}_4$ and $\boldsymbol{Z}_{2^s}$

Nimalsiri Pinnawala and Asha Rao

Abstract—**Over the past decade, cocyles have been used to construct Hadamard and generalized Hadamard matrices. This, in turn, has led to the construction of codes—self-dual and others. Here we explore these ideas further to construct cocylic complex and Butson–Hadamard matrices, and subsequently we use the matrices to construct simplex codes of type α over $\boldsymbol{Z}_4$ and $\boldsymbol{Z}_{2^s}$, respectively.**

Index Terms—**Butson, cocycle, complex Hadamard, exponent, quaternary, self-orthogonal, simplex codes, trace.**

I. INTRODUCTION

Various authors [1], [2], [11], [12] have studied the construction of cocyclic Hadamard and cocyclic generalized Hadamard matrices and the use of these matrices in the construction of cocyclic codes. Here we extend these constructions to obtain cocyclic Butson and cocyclic complex Hadamard matrices. Simplex codes of type α were studied by Gupta [9], but no methods of constructions were given. We use the cocyclic complex and cocyclic Butson–Hadamard matrices to construct simplex codes of type α over $\boldsymbol{Z}_4$ and $\boldsymbol{Z}_{2^s}$, respectively. We assume that the reader is familiar with the basic facts of the theory of Hadamard matrices (see, for example, [15]) and of binary linear codes (see [13]).

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 $\psi: G \times G \rightarrow C$ which satisfies

$$\psi(a,b)\psi(ab,c) = \psi(a,bc)\psi(b,c), \qquad \forall a,b,c \in G.$$

A cocycle is *normalized* if $\psi(1,1) = 1$. A cocycle may be represented as a cocyclic matrix $M_\psi = [\psi(a,b)]_{a,b \in G}$ once an indexing of the elements of G has been chosen.

Let C_p be the multiplicative group of all complex pth roots of unity, $C_p = \{1, x, x^2, \dots, \ \ x^{p-1}\}$, where $x = \exp(2\pi i/p)$ and $p \geq 2$ is an integer. A square matrix $H = [h_{ij}]$ of order n with elements from C_p is called a Butson–Hadamard matrix $(BH(n,p))$ (see [5]) if and only if $HH^* = nI$, H^* being the conjugate transpose of H and I the identity matrix of order n. When $p = 2$ and $n = 1, 2$ or a multiple of 4, $BH(n,p)$ is a Hadamard matrix.

A complex Hadamard matrix H of order n is a matrix with entries from $\{1, i, -1, -i\}$ that satisfies $HH^* = nI$, where $i = \sqrt{-1}$ and H^* is the conjugate transpose of H. It is conjectured that a complex Hadamard matrix exists for every even order. In [15], it is shown that every complex Hadamard matrix has order 1 or divisible by 2. A complex Hadamard matrix is a special case of a Butson–Hadamard matrix $BH(n,p)$ for $p = 4$.

Let $H = [h_{i,j}]$ be a square matrix over C_p, where p is a fixed integer $p > 2$. The matrix $E = [e_{i,j}]$, $e_{i,j} \in \boldsymbol{Z}_p$, which is obtained from $H = [x^{e_{i,j}}] = [h_{i,j}]$, where $x = \exp(2\pi i/p)$, is called the *exponent matrix* associated with H. The elements of the exponent matrix E lie in the Galois ring GR$(p,1)$ (Galois field GF(p), for p prime), and its row vectors can be viewed as the codewords of a code over the integers modulo p.

Manuscript received December 10, 2003; revised May 5, 2004.

The authors are with the Department of Mathematics and Statistics, Royal Melbourne Institute of Technology, GPO Box 2476V, Melbourne, VIC 3001, Australia.

Communicated by C. Carlet, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2004.833354

In Section II, we introduce the main machinery of Galois rings for the study of $\boldsymbol{Z}_4$-codes and the trace map over GR $(4, m)$. In Section III, we define a cocycle for the construction of a complex Hadamard matrix and subsequently we use it for the construction of $\boldsymbol{Z}_4$-simplex codes of type α. We then extend these results to obtain cocyclic simplex codes over $\boldsymbol{Z}_{2^s}$. The Galois ring GR $(2^s, m)$ and the generalized trace map and codes over $\boldsymbol{Z}_{2^s}$ are studied in Section IV. In Section V, we define a cocycle over GR $(2^s, m)$ to construct Butson–Hadamard matrices and use these matrices to create $\boldsymbol{Z}_{2^s}$-simplex codes of type α.

II. The Galois Ring GR $(4, m)$, The Trace Map, and Codes Over $\boldsymbol{Z}_4$

Let $h(x)$ be a basic irreducible polynomial of degree m over $\boldsymbol{Z}_4$. Consider the residue class ring $\boldsymbol{Z}_4[x]/(h(x))$. The residue classes

$$a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} + (h(x))$$

where $a_0, a_1, \ldots, a_{m-1} \in \boldsymbol{Z}_4$, are all distinct elements of $\boldsymbol{Z}_4[x]/(h(x))$. Hence, $|\boldsymbol{Z}_4[x]/(h(x))| = 4^m$. The ring $\boldsymbol{Z}_4[x]/(h(x))$ is called the *Galois ring* of order 4^m and is denoted by GR $(4, m)$.

In the Galois ring GR $(4, m)$ there exists a nonzero element ζ of order $2^m - 1$ (take $\zeta = x + (h(x))$, for example), which is a root of a basic primitive polynomial $h(x)$ of degree m over $\boldsymbol{Z}_4$ and GR $(4, m) = \boldsymbol{Z}_4[\zeta]$. Moreover, $h(x)$ is the unique monic polynomial of degree $\leq m$ over $\boldsymbol{Z}_4$ having ζ as a root.

Let $\mathcal{T} = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{2^m-2}\}$ be the Teichmuller set; then any element $c \in$ GR $(4, m)$ can be written uniquely as $c = a + 2b$, where $a, b \in \mathcal{T}$. More details can be found in [16].

The Frobenius automorphism over the Galois ring GR $(4, m)$ is defined by

$$f : \text{GR}\,(4, m) \rightarrow \text{GR}\,(4, m), \quad c = a + 2b \rightarrow f(c) = a^2 + 2b^2$$

and the trace map over GR $(4, m)$ is defined by

$$\begin{aligned} &T : \text{GR}\,(4, m) \rightarrow \boldsymbol{Z}_4 \\ &T(c) = c + f(c) + f^2(c) + \cdots + f^{m-1}(c), \quad \text{for all } c \in \text{GR}\,(4^m). \end{aligned}$$

From the definition of f and T it is clear that T is a nontrivial linear transformation from GR $(4, m)$ to $\boldsymbol{Z}_4$.

Further, let $c \in$ GR $(4, m)$. Boztaş *et al.* [4] show that if c is invertible, then as x ranges over GR $(4, m)$, $T(cx)$ takes $0, 1, 2,$ and 3 equally often, i.e., 4^{m-1} times and if c is not invertible then as x ranges over GR $(4, m)$, $T(cx)$ takes 0 and 2 equally often, i.e., $2 \cdot 4^{m-1}$ times.

For a positive integer p, let $\boldsymbol{Z}_p$ be the set of integers modulo p, i.e., $\boldsymbol{Z}_p = \{0, 1, 2, \ldots, p-1\}$. The Lee weight of $a \in \boldsymbol{Z}_p$ is defined by $W_L(a) = \min\{a, p-a\}$. The *Lee weight* $W_L(\boldsymbol{x})$ of $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ in $\boldsymbol{Z}_p^n$ is defined to be the integral sum of the *Lee weight* of its components. The *Lee distance* between $\boldsymbol{x}, \boldsymbol{y} \in \boldsymbol{Z}_p^n$ is defined as

$$d_L(\boldsymbol{x}, \boldsymbol{y}) = W_L(\boldsymbol{x} - \boldsymbol{y}).$$

Let Z_4 be the ring of integers modulo 4 (i.e., $Z_4 = \{0, 1, 2, 3\}$), n be a positive integer, and Z_4^n be the set of n-tuples over Z_4. i.e.,

$$Z_4^n = \{\boldsymbol{x} = (x_1, x_2, \ldots, x_n) | x_i \in Z_4, \text{ for } i = 1, 2, \ldots, n\}.$$

A nonempty subset C of Z_4^n is called a Z_4-code (or a *quaternary code*). n is called the *length* of the code. n-tuples of C are called *codewords of* C. For all $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$ in Z_4^n, if the componentwise addition is defined as

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

then Z_4^n becomes an additive Abelian group of order 4^n. Any subgroup C of Z_4^n is called a quaternary linear code, or simply Z_4*-linear code.*

As pointed out by Hammons *et al.* [10], a $\boldsymbol{Z}_4$-linear code C containing some nonzero codewords is permutation equivalent to a $\boldsymbol{Z}_4$-linear code with a generator matrix of the form

$$G_C = \begin{bmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2D \end{bmatrix}$$

where I_{k_1} and I_{k_2} are the identity matrices of order k_1 and k_2, respectively, A and D are $\boldsymbol{Z}_2$-matrices, and B is a $\boldsymbol{Z}_4$-matrix. The code C is an Abelian group of type $4^{k_1} 2^{k_2}$ and it contains $2^{(2k_1+k_2)}$ codewords. Further, it is a free $\boldsymbol{Z}_4$-module if and only if $k_2 = 0$. Parameters of a Z_4-linear code C are denoted by $[n, k, d_L]$, where n is the length of the code, k is the 2-dimension of the code, and d_L is the minimum Lee distance of the code. For more information on the 2-dimension of a code see [9].

The Gray map is used to form binary codes from $\boldsymbol{Z}_4$-codes. Some well-known binary nonlinear codes are images under the Gray map of linear codes over $\boldsymbol{Z}_4$. The Gray map is usually denoted by ϕ, and defined as

$$\begin{aligned} \phi : \boldsymbol{Z}_4 &\rightarrow \boldsymbol{Z}_2^2 \\ 0 &\rightarrow 00 \\ 1 &\rightarrow 01 \\ 2 &\rightarrow 11 \\ 3 &\rightarrow 10. \end{aligned}$$

More details on $\boldsymbol{Z}_4$-codes can be found in [3], [10], [16], etc.

Let C be a $\boldsymbol{Z}_4$-linear code and d_H and d_L be the minimum Hamming distance and minimum Lee distance of C, respectively. In [14], Rains has shown that for any $\boldsymbol{Z}_4$-linear code C

$$d_H \geq \left\lceil \frac{d_L}{2} \right\rceil.$$

If $d_H = \lceil \frac{d_L}{2} \rceil$, then C is called a code of type α. Otherwise, it is said to be of type β.

Definition 2.1: $\boldsymbol{Z}_4$-simplex code of type $\boldsymbol{\alpha}$ [9].

Let G_m be an $m \times 4^m$ matrix over $\boldsymbol{Z}_4$ consisting of distinct columns. Inductively G_m can be written as

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

with $G_1 = [0123]$. The code generated by G_m, denoted by S_m^α, is called a $\boldsymbol{Z}_4$-simplex code of type α.

The Gray image of $\bar{S}_m^\alpha$ is nonlinear for all m, where $\bar{S}_m^\alpha$ is the punctured code of S_m^α obtained by deleting the zero coordinate [9].

III. Cocyclic Complex Hadamard Matrices and $\boldsymbol{Z}_4$-Simplex Codes of Type α

The key focus of this section is the construction of complex Hadamard matrices by using a cocycle and subsequently cocyclic $\boldsymbol{Z}_4$-simplex codes of type α.

Theorem 3.1: Let $h(x)$ be a basic irreducible polynomial of degree m over $\boldsymbol{Z}_4$ and GR $(4, m) = \boldsymbol{Z}_4[x]/(h(x))$. Let $C_4 = \{1, x, x^2, x^3\}$ be the multiplicative group of all complex 4th roots of unity and T be the trace map over GR $(4, m)$. Then

i) the function

$$\psi : \text{GR}\,(4, m) \times \text{GR}\,(4, m) \rightarrow C_4$$

given by

$$\psi(c_i, c_j) = (x)^{T(c_i c_j)}$$

is a cocycle;

ii) the matrix $H = [\psi(c_i, c_j)]_{c_i, c_j \in GR(4,m)}$ is a complex Hadamard matrix of order 4^m.

Proof:

i) From the definition of ψ and the properties of the trace map, it is obvious that ψ is a cocycle.

ii) For all $a, b \in \mathrm{GR}\,(4,m)$, consider the sum

$$S = \sum_{\forall h \in \mathrm{GR}\,(4,m)} \psi(a,h)\overline{\psi(b,h)}$$

where $\overline{\psi(b,h)}$ is the complex conjugate of $\psi(b,h)$. From the properties of the trace map

$$S = \sum_{\forall h \in \mathrm{GR}\,(4,m)} (x)^{T((a-b)h)}.$$

For $a = b, S = 4^m$, and for $a \neq b, S = 0$. Thus, H is a complex Hadamard matrix of order 4^m.

Theorem 3.2: The rows of the matrix $A = [T(c_i c_j)]$ (the exponent matrix associated with H in Theorem 3.1) form a quaternary linear code $[n, k, d_L] = [4^m, m, 4^m]$ and it is a $\boldsymbol{Z}_4$-simplex code of type α. Further A is a free $\boldsymbol{Z}_4$-module and a self-orthogonal code.

Proof: Consider the set $\mathcal{K} = \{1, \zeta, \zeta^2, \ldots, \zeta^{m-1}\}$, where ζ is a root of $h(x)$. It is clear that these elements are linearly independent m-tuples in $\mathrm{GR}\,(4,m)$ and are invertible. Further, we know that $\mathrm{GR}\,(4,m) = \langle 1, \zeta, \zeta^2, \ldots, \zeta^{m-1}\rangle$. Therefore, any element $c_i \in \mathrm{GR}\,(4,m)$ can be written uniquely as

$$c_i = a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{m-1}\zeta^{m-1}$$

where $a_j \in \boldsymbol{Z}_4, j = 0, 1, 2, \ldots, m-1$ and $i = 1, 2, \ldots, 4^m$.

Now consider the following matrix:

$$G_A = \begin{bmatrix} T(c_i), & i = 1, 2, \ldots, 4^m \\ T(\zeta c_i), & i = 1, 2, \ldots, 4^m \\ \vdots & \vdots \\ T(\zeta^{m-1} c_i), & i = 1, 2, \ldots, 4^m \end{bmatrix}_{m \times 4^m}.$$

Since $1, \zeta, \zeta^2, \ldots, \zeta^{m-1}$ are invertible, from the properties of the trace map, each row in G_A consists of $0, 1, 2, 3$ equally often (i.e., 4^{m-1} times). Further, the rows of the matrix G_A are linearly independent and G_A generates the matrix $A = [T(c_i c_j)]_{c_i, c_j \in \mathrm{GR}\,(4,m)}$. It is obvious that the minimum Lee distance of the code A is 4^m and hence A is a quaternary linear code with parameters $[n, k, d_L] = [4^m, m, 4^m]$. By deleting the all-zero column of A we get the linear quaternary code A^* with parameters $[4^m - 1, m, 4^m]$.

From Definition 2.1, the generator matrix G_A is equivalent to that of G_m, the generator matrix of a $\boldsymbol{Z}_4$-simplex code of type α. Therefore, the code A is a $\boldsymbol{Z}_4$-simplex code of type α.

G_A has no rows with only 0's and 2's. Therefore, it should be equivalent to a matrix of the form $G_A = [I_m \;\; A \;\; B]$, where A and B are $\boldsymbol{Z}_2$ and $\boldsymbol{Z}_4$ matrices, respectively. Thus, the code generated by the matrix G_A is a free $\boldsymbol{Z}_4$-module. In [8], it is shown that $\boldsymbol{Z}_4$-simplex codes S_m^α $(m \geq 2)$ are self-orthogonal and, hence, A is a self-orthogonal code.

Further, the binary image of A^*, which is obtained by deleting the all-zero column of A, is a nonlinear $\boldsymbol{Z}_2$-code $C = \phi(A^*)$ with parameters $(n, M, d_H) = (2 \cdot (4^m - 1), 4^m, 4^m)$.

Example 3.3: Consider the basic irreducible polynomial $h(x) = x^2 + x + 1$ over $\boldsymbol{Z}_4$. Define the Galois ring $\mathrm{GR}\,(4,2) = \boldsymbol{Z}_4[x]/(h(x))$. Let ζ be a root of $h(x)$. Since $m = 2$, the order of ζ is $2^2 - 1 = 3$. Therefore, $\zeta^0 = 1, \zeta^1 = \zeta, \zeta^2 = 3\zeta + 3$ and $\mathcal{T} = \{0, 1, \zeta, \zeta^2\}$. $\mathrm{GR}\,(4,2) = \{c = a + 2b \mid a, b \in \mathcal{T}\}$. Elements of this ring and value of each element under the trace map are given in the Table I.

Consider the set mapping

$$\psi : \mathrm{GR}\,(4,2) \times \mathrm{GR}\,(4,2) \to C_4, \qquad \psi(c_i, c_j) = (i)^{T(c_i c_j)}.$$

TABLE I
ELEMENTS OF GR (4, 2) AND THEIR VALUES UNDER THE TRACE MAP

Element	$c_i = a + 2b$	$T(c_i)$	$T(\zeta c_i)$
00	0	0	0
20	2	0	2
02	2ζ	2	2
22	$2\zeta^2$	2	0
10	1	2	3
30	$1+2$	2	1
12	$1+2\zeta$	0	1
32	$1+2\zeta^2$	0	3
01	ζ	3	3
21	$\zeta+2$	3	1
03	$\zeta+2\zeta$	1	1
23	$\zeta+2\zeta^2$	1	3
33	ζ^2	3	2
13	ζ^2+2	3	0
31	$\zeta^2+2\zeta$	1	0
11	$\zeta^2+2\zeta^2$	1	2

According to the proof of Theorem 3.1 i), ψ is a cocycle. The matrix

$$H = [\psi(c_i, c_j)]_{c_i, c_j \in \mathrm{GR}\,(4,2)}$$

is shown in Fig. 1.

By Theorem 3.1 ii), $HH^* = 4^2 I_{4^2 \times 4^2}$. i.e., H is a complex Hadamard matrix of order 4^2.

The matrix $A = [T(c_i c_j)]_{\forall\, c_i, c_j \in \mathrm{GR}\,(4,2)}$ (the exponent matrix associated with H) is shown in Fig. 2.

The rows of the matrix A can be considered as codewords over $\boldsymbol{Z}_4$. A generator matrix for this code is

$$G_A = \begin{bmatrix} T(c_i), & i = 1, 2, \ldots, 4^2 \\ T(\zeta c_i), & i = 1, 2, \ldots, 4^2 \end{bmatrix}_{2 \times 4^2}$$

i.e.,

$$G_A = \begin{bmatrix} 0 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 3 & 3 & 1 & 1 & 3 & 3 & 1 & 1 \\ 0 & 2 & 2 & 0 & 3 & 1 & 1 & 3 & 3 & 1 & 1 & 3 & 2 & 0 & 0 & 2 \end{bmatrix}.$$

Parameters of this $\boldsymbol{Z}_4$-linear code are $[4^2, 2, 4^2]$. By deleting the all-zero column of A we get A^*, a $\boldsymbol{Z}_4$-linear code with parameters $[4^2 - 1, 2, 4^2]$. It is clear that the generator matrix G_A is equivalent to the generator matrix G_2 of Definition 2.1 and, hence, A is a $\boldsymbol{Z}_4$-simplex code of type α.

The binary image of A^* is a nonlinear $\boldsymbol{Z}_2$-code $C = \phi(A^*)$ with parameters $(n, M, d_H) = (2 \cdot (4^2 - 1), 4^2, 4^2)$.

IV. Galois Ring GR $(2^s, m)$ and Codes Over $\boldsymbol{Z}_{2^s}$

Let $\boldsymbol{Z}_{2^s} = \{0, 1, 2, \ldots, 2^s - 1\}$ be the ring of integers modulo 2^s. Let $h(x)$ be an irreducible polynomial of degree m over $\boldsymbol{Z}_{2^s}$. Define the Galois ring $\mathrm{GR}\,(2^s, m) = \boldsymbol{Z}_{2^s}[x]/(h(x))$. Let $\zeta = x + (h(x))$. Then $h(\zeta) = 0$ and, hence, $\mathrm{GR}\,(2^s, m) = \boldsymbol{Z}_{2^s}[\zeta]$. Thus, we have $\mathrm{GR}\,(2^s, m) = \langle 1, \zeta, \zeta^2, \ldots, \zeta^{m-1}\rangle$ and $|\mathrm{GR}\,(2^s, m)| = 2^{sm}$.

Let $\mathcal{T} = \{0, 1, \zeta, \ldots, \zeta^{2^m - 2}\}$ be the Teichmuller set. Then any $u \in \mathrm{GR}\,(2^s, m)$ can be uniquely written as $u = \sum_{i=0}^{s-1} 2^i u_i$, where $u_i \in \mathcal{T}$. Further, u is invertible iff $u_0 \neq 0$.

Consider the Frobenius automorphism given in [7]

$$f : \mathrm{GR}\,(2^s, m) \to \mathrm{GR}\,(2^s, m)$$

$$f(u) = \sum_{i=0}^{s-1} 2^i u_i^2$$

and the trace map

$$T : \mathrm{GR}\,(2^s, m) \to \boldsymbol{Z}_{2^s}$$

$$T(u) = u + f(u) + f^2(u) + \cdots + f^{m-1}(u).$$

Since f is an automorphism, obviously T is a nontrivial linear transformation.

Also for any $b \in \mathrm{GR}\,(2^s, m)$, if b is invertible, then as x ranges over $\mathrm{GR}\,(2^s, m)$, $T(xb)$ takes each element of $\boldsymbol{Z}_{2^s}$ equally often, i.e.,

$$H = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -i & -i & i & i & -i & -i & i & i \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & i & i & -i & -i & i & i & -i & -i \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & i & i & -i & -i & -i & -i & i & i \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -i & -i & i & i & i & i & -i & -i \\
1 & -1 & -1 & 1 & -i & i & i & -i & -i & i & i & -i & -1 & 1 & 1 & -1 \\
1 & -1 & -1 & 1 & -i & i & i & -i & i & -i & -i & i & 1 & -1 & -1 & 1 \\
1 & -1 & -1 & 1 & i & -i & -i & i & i & -i & -i & i & -1 & 1 & 1 & -1 \\
1 & -1 & -1 & 1 & i & -i & -i & i & -i & i & i & -i & 1 & -1 & -1 & 1 \\
1 & -1 & 1 & -1 & -i & i & -i & i & -1 & 1 & -1 & 1 & -i & i & -i & i \\
1 & -1 & 1 & -1 & -i & i & -i & i & 1 & -1 & 1 & -1 & i & -i & i & -i \\
1 & -1 & 1 & -1 & i & -i & i & -i & 1 & -1 & 1 & -1 & -i & i & -i & i \\
1 & -1 & 1 & -1 & i & -i & i & -i & -1 & 1 & -1 & 1 & i & -i & i & -i
\end{bmatrix}$$

Fig. 1. Cocyclic matrix over GR $(4, 2)$ using the trace map.

$$A = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\
0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 \\
0 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 3 & 3 & 1 & 1 & 3 & 3 & 1 & 1 \\
0 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 1 & 1 & 3 & 3 & 1 & 1 & 3 & 3 \\
0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 1 & 1 & 3 & 3 & 3 & 3 & 1 & 1 \\
0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 3 & 3 & 1 & 1 & 1 & 1 & 3 & 3 \\
0 & 2 & 2 & 0 & 3 & 1 & 1 & 3 & 3 & 1 & 1 & 3 & 2 & 0 & 0 & 2 \\
0 & 2 & 2 & 0 & 3 & 1 & 1 & 3 & 1 & 3 & 3 & 1 & 0 & 2 & 2 & 0 \\
0 & 2 & 2 & 0 & 1 & 3 & 3 & 1 & 1 & 3 & 3 & 1 & 2 & 0 & 0 & 2 \\
0 & 2 & 2 & 0 & 1 & 3 & 3 & 1 & 3 & 1 & 1 & 3 & 0 & 2 & 2 & 0 \\
0 & 2 & 0 & 2 & 3 & 1 & 3 & 1 & 2 & 0 & 2 & 0 & 3 & 1 & 3 & 1 \\
0 & 2 & 0 & 2 & 3 & 1 & 3 & 1 & 0 & 2 & 0 & 2 & 1 & 3 & 1 & 3 \\
0 & 2 & 0 & 2 & 1 & 3 & 1 & 3 & 0 & 2 & 0 & 2 & 3 & 1 & 3 & 1 \\
0 & 2 & 0 & 2 & 1 & 3 & 1 & 3 & 2 & 0 & 2 & 0 & 1 & 3 & 1 & 3
\end{bmatrix}$$

Fig. 2. The exponent matrix associated with H.

2^{sm-s} times and if b is not invertible then, as x ranges over GR $(2^s, m)$, $T(xb)$ takes elements in

$$\{2^k t \mid t = 0, 1, 2, \dots, 2^{s-k} - 1,\ k = 1, 2, \dots, s-1\}$$

equally often, i.e., $2^{sm-(s-k)}$ times.

Moving on to codes over $\boldsymbol{Z}_{2^s}$, the generator matrix G of any linear code C of length n over $\boldsymbol{Z}_{2^s}$ is equivalent to

$$\begin{bmatrix}
I_{k_0} & A_{0,1} & A_{0,2} & \dots & \dots & A_{0,s-1} & A_{0,s} \\
0 & 2I_{k_1} & 2A_{1,2} & \dots & \dots & 2A_{1,s-1} & 2A_{1,s} \\
0 & 0 & 2^2 I_{k_2} & 2^2 A_{2,3} & \dots & 2^2 A_{2,s-1} & 2^2 A_{2,s} \\
\vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \dots & 2^{s-1} I_{k_{s-1}} & 2^{s-1} A_{s-1,s}
\end{bmatrix}.$$

Here the $A_{i,j}$ are matrices over $\boldsymbol{Z}_{2^s}$. Note that C is a free $\boldsymbol{Z}_{2^s}$-module if and only if $k_i = 0$ for all $i = 1, 2, \dots, s-1$([6]).

The Gray map can be generalized to construct binary codes from codes over Z_{2^s} [7].

Let s be any positive integer, u any element of Z_{2^s}, and $\sum_{i=1}^{s} 2^{i-1} u_i$ its binary expansion $(u_i = 0, 1)$. The image of u by the generalized Gray map is the following Boolean function on Z_2^{s-1}:

$$G(u) : (y_1, y_2, \dots, y_{s-1}) \to u_s + \sum_{i=1}^{s-1} u_i y_i$$

where $(y_1, y_2, \dots, y_{s-1}) \in Z_2^{s-1}$.

Definition 4.1: $\boldsymbol{Z}_{2^s}$-simplex code of type α [9].

Let G_m be an $m \times 2^{sm}$ matrix over $\boldsymbol{Z}_{2^s}$ defined inductively by the expressions at the bottom of the page.

The code generated by G_m is called the $\boldsymbol{Z}_{2^s}$-simplex code of type α and is denoted by S_m^α.

Let $\bar{C} = \overline{S_m^\alpha}$ be the punctured code of S_m^α, which is obtained by deleting the zero coordinate. The Gray image of $\bar{C}$ under the generalized Gray map of 2-basis is a $[2^{s-1}(2^{sm} - 1), sm, 2^{s(m+1)-2}]$ binary linear code.

V. Cocyclic Butson–Hadamard Matrices and $\boldsymbol{Z}_{2^s}$-Simplex Codes of Type α

Here we define a cocycle over the Galois ring GR $(2^s, m)$ and construct Butson–Hadamard matrices $H_{2^{sm}}$ of order 2^{sm}. The exponent matrix of $H_{2^{sm}}$ is a simplex code of type α over the integers modulo 2^s. The proofs of the following two theorems are very similar to those of Theorems 3.1 and 3.2.

Theorem 5.1: Let $C_{2^s} = \{1, x, x^2, \dots, x^{2^s - 1}\}$ be the set of all complex (2^s)th roots of unity and and GR $(2^s, m)$ be the Galois ring of order 2^{sm}. Consider the set mapping

$$\psi : \text{GR}\,(2^s, m) \times \text{GR}\,(2^s, m) \to C_{2^s}$$
$$\psi(a,b) = (x)^{T(ab)}.$$

Then

i) ψ is a cocycle,

ii) $M_\psi = [\psi(a,b)]_{\forall a,b \in \text{GR}\,(2^s,m)}$ is a Butson–Hadamard matrix of order 2^{sm}.

$$G_1 = [0, 1, 2, \dots, 2^s - 1]$$

$$G_m = \left[\begin{array}{c|c|c|c}
00\dots0 & 11\dots1 & \dots & (2^s-1)(2^s-1)\dots(2^s-1) \\
\hline
G_{m-1} & G_{m-1} & \dots & G_{m-1}
\end{array}\right].$$

Theorem 5.2: If $A = [T(ab)]_{\forall a,b \in \mathrm{GR}\,(2^s,m)}$ is the exponent matrix associated with M_ψ in Theorem 5.1, then the rows of A form a simplex code of type α over $\boldsymbol{Z}_{2^s}$.

VI. Conclusion

In this correspondence, we introduced a cocycle over the Galois ring $\mathrm{GR}\,(4,m)$ for the construction of complex Hadamard matrices and a cocycle over the Galois ring $\mathrm{GR}\,(2^s,m)$ for the construction of Butson–Hadamard matrices. Subsequently, we used these matrices for the construction of simplex codes of type α over $\boldsymbol{Z}_4$ and $\boldsymbol{Z}_{2^s}$, respectively.

References

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

[2] A. Baliga and K. J. Horadam, "Cocyclic Hadamard matrices over $\boldsymbol{Z}_t \times \boldsymbol{Z}_2^2$," *Australas. J. Combin.*, vol. 11, pp. 123–134, 1995.

[3] A. Bonnecaze and I. M. Duursma, "Translates of linear codes over Z_4," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1218–1230, July 1997.

[4] S. Boztaş, A. R. Hammons, and P. V. Kumar, "4-phase sequences with near-optimum correlation properties," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1101–1113, May 1992.

[5] A. T. Butson, "Generalized Hadamard matrices," *Proc. Amer. Math. Soc.*, vol. 13, pp. 894–898, 1962.

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

[7] C. Carlet, "$\boldsymbol{Z}_{2^k}$-linear code," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1543–1547, July 1998.

[8] D. G. Glynn, T. A. Gulliver, and M. K. Gupta, "On some quaternary self orthogonal codes," preprint.

[9] M. K. Gupta, "On some linear codes over $\boldsymbol{Z}_{2^s}$," Ph.D. dissertation, Indian Institute of Technology, Department of Mathematics, Kanpur, 1999.

[10] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $\boldsymbol{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 301–319, Mar. 1994.

[11] K. J. Horadam, "An introduction to cocyclic generalized Hadamard matrices," *Discr. Appl. Math.*, vol. 102, pp. 115–131, 2000.

[12] K. J. Horadam and P. Udaya, "Cocyclic Hadamard codes," *IEEE Trans. Inform. Theory*, vol. 46, pp. 1545–1550, July 2000.

[13] F. J. McWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[14] E. M. Rains, "Optimal self dual codes over $\boldsymbol{Z}_4$," *Discr. Math.*, vol. 203, pp. 215–228, 1999.

[15] W. D. Wallis, A. P. Street, and J. S. Wallis, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices (Lecture Notes in Mathematics)*. New York: Springer-Verlag, 1972, vol. 292.

[16] Z. X. Wan, *Quaternary Codes*. Lund, Sweden: Lund University, Chinese Academy of Sciences, 1997.

Code Construction on Fiber Products of Kummer Covers

Hiren Maharaj

***Abstract*—We show that Riemann–Roch spaces of divisors from fiber products of Kummer covers of the projective line, which are invariant with respect to the Galois group, decompose as a direct sum of Riemann–Roch spaces of divisors of the projective line. Consequently, one obtains explicit bases and good upper bounds for the minimum distance of the resulting Goppa codes. This correspondence is a generalization of the work of Xing.**

***Index Terms*—Algebraic-geometry codes, fiber products of Kummer covers, geometric Goppa codes.**

I. Introduction and Main Results

Motivated by applications in coding theory much work has been done, using a variety of techniques, on the construction of curves with many points over finite fields (see [4], [8]). Specifically, in [1]–[3], [5], [7] such curves are constructed using Kummer covers or fiber products of Kummer covers of the projective line. Recall that a collection of all functions defined on a curve, whose poles with pole order upper-bounded by a prescribed set of corresponding fixed integers (specified by a divisor) forms a vector space called a Riemann–Roch space. In this correspondence, it is shown how to obtain explicit bases for a large class of Riemann–Roch spaces from these curves by exhibiting the space as a direct sum of Riemann–Roch spaces of divisors of the projective line. In this section, we state the main results and the proofs are given in Section II. In order to illustrate the application of this work to code construction, in Section III we work two examples in detail. There we indicate how to derive upper bounds on the minimum distance of the corresponding Goppa codes.

Henceforth, we use the language of algebraic function fields (of a single variable) as in [6]. For example, we denote the set of places of a function field F by $\mathbb{P}(F)$. To state our first result, we need the following definition. Let F'/F be a finite extension of algebraic function fields. Any divisor of F' can be written in the form

$$G = \sum_{R \in \mathbb{P}(F)} \sum_{Q \in \mathbb{P}(F'), Q|R} a_Q Q$$

where the a_Q are integers such that $a_Q = 0$ for almost all $Q \in \mathbb{P}(F')$. We define the restriction of G to F, denoted $G|_F$, to be the following divisor of F:

$$G|_F := \sum_{R \in \mathbb{P}(F)} \min \left\{ \left\lfloor \frac{a_Q}{e(Q|R)} \right\rfloor : Q|R \right\} R.$$

Next we assume F'/F is a Kummer extension of degree $n > 1$ so that we can write $F' = F(y)$ where $y^n \in F$.

Theorem 2.2: Let G be a divisor of F' which is invariant with respect to $\mathrm{Gal}(F'/F)$. Then

$$\mathcal{L}(G) = \bigoplus_{i=0}^{n-1} \mathcal{L}\left((G + i(y))|_F \right) y^i.$$

Thus, $\mathcal{L}(G)$ can be decomposed as a direct sum of Riemann–Roch spaces of F. In the case that F is the rational function field, explicit

Manuscript received January 1, 2004; revised May 19, 2004. The material in this correspondence was presented in part at the Conference on Finite Fields and Applications, Oberwolfach, Germany, December 2003.

The author is with the Department of Mathematical Sciences, Clemson University, Clemson, SC, 29634 USA (e-mail: hmahara@clemson.edu).

Communicated by C. Carlet, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2004.833356