systematic code to q-ary systematic code. One simply needs to change $B = (C^T I_k)$ into $B = (-C^T I_k)$ and generalize Definition 4.1 to the following Definition 4.2, and then Theorems 4.1, 4.2, and 4.3 are also hold.

Definition 4.2: If the stabilizer and normalizer matrices of $\mathcal{Q} = [[n, k, d]]_q$ are $\mathfrak{S} = (I_{(n-k)}C \mid (I_{(n-k)}C)S)$ and

$$N(\mathfrak{S}) = \begin{pmatrix} I_n & S \\ 0_{k\times n} & B \end{pmatrix}$$

respectively, where S is symmetric and $B = (-C^T I_k)$, then $\mathcal{Q}$ is called a systematic quantum code, and its stabilizer matrix $\mathfrak{S}$ and normalizer matrix $N(\mathfrak{S})$ are called in standard form.

Remark 4.2: In [10], Tonchev proved that the subspaces generated by matrices of the form $(I_n \mid S)$ are maximum totally isotropic subspaces, where S is the adjacency matrix of an undirected graph. He also pointed out that the number of trace self-dual additive codes with generator matrix $\phi(I_n \mid S)$ is much smaller than the total number of trace self-dual additive codes. Our Theorem 4.3 shows that it suffices to study trace self-dual additive codes with generator matrix $\phi(I_n \mid S)$ for dealing with trace self-dual additive codes.

ACKNOWLEDGMENT

The authors would like to thank the anonymous referees for their valuable comments and suggestions, which help to improve this manuscript significantly. R. Li would like to thank Prof. S. Zhang and J. Zhang for their help in revising this correspondence.

REFERENCES

[1] A. Ashikhmin and E. Knill, "Nonbinary quantum stablizer codes," airXiv:quant-ph/0005008.
[2] J. Bierbrauer and Y. Edel, "Quantum twisted codes," *J. Comb. Designs*, vol. 8, pp. 174–188, 2000.
[3] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error-correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.
[4] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, Phys. Dept., California Inst. Technol., Los Angeles, CA, 1997, quant-ph/9707027.
[5] L. K. Hua and Z. Wan, *Classical Group (In Chinese)*. Shanghai, China: Shanghai Sci. Technol. Press, 1963.
[6] W. C. Huffman, "On the classification and enumeration of self-dual codes," *Finite Fields Appl.*, vol. 11, pp. 451–490, 2005.
[7] R. J. McEliece, *The Theory of Information and Coding*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2002.
[8] J. H. van Lint, *Introduction to Coding Theory*. New York: Springer-Verlag, 1982.
[9] E. M. Rains, "Nonbinary quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1827–1832, Sep. 1999.
[10] V. Tonchev, "Error-correcting codes from graphs," *Discrete Math.*, vol. 257, pp. 549–557, 2002.
[11] Z. Wan, *Geometry of Classical Groups Over Finite Fields*. Lund, Sweden: Student Literature, 1993.

On The Classification of Binary Optimal Self-Orthogonal Codes

Ruihu Li, Zongben Xu, and Xuejun Zhao

***Abstract*—The classification of binary $[n, k, d]$ codes with $d \geq s2^{k-1}$ and without zero coordinates is reduced to the classification of binary $[(2^k - 1)c(k, s, t) + t, k, d]$ code for $n = (2^k - 1)s + t$, $s \geq 1$ and $1 \leq t \leq 2^k - 2$, where $c(k, s, t) \leq \min\{s, t\}$ is a function of k, s, and t. Binary $[15s + t, 4]$ optimal self-orthogonal codes are characterized by systems of linear equations. Based on these two results, the complete classification of $[15s + t, 4]$ optimal self-orthogonal codes for $t \in \{1, 2, 6, 7, 8, 9, 13, 14\}$ and $s \geq 1$ is obtained, and the generator matrices and weight polynomials of these 4-dimensional optimal self-orthogonal codes are also given.**

***Index Terms*—Binary linear code, self-orthogonal code, optimal code.**

I. INTRODUCTION

Since the pioneer work of Pless in [6], people paid much attention on self-dual codes—a subclass of self-orthogonal codes (SO codes, for short), and a vast number of papers have been devoted to the study of self-dual codes, as shown in the excellent survey of [7] and [4] for an overview of these results and the references therein.

But, very little has previously been known about the minimum distance and number of general $[n, k]$ SO codes of rate less than $\frac{1}{2}$, except the binary $[2k + 1, k]$ SO codes for $k \leq 9$ in [6].

Recently, people begin to study general optimal $[n, k]$ SO codes of rate less than $\frac{1}{2}$ and use these optimal $[n, k]$ SO codes to study self-dual codes, see [1]. In [2] Bouykliev *et al.* studied the classification of optimal SO codes of length ≤ 29 and dimension less than 7 over F_3 and F_4. In [3] Bouykliev *et al.* studied the classification of binary optimal SO codes of length ≤ 40 and dimension less than 10, and gave complete classification of three-dimensional (3-D) optimal SO codes. However, their classification are based on two algorithms and no unified proofs for dimension greater than 4, and most of the generator matrices of their optimal SO codes of length ≥ 25 and dimension greater than 6 are not given.

In this correspondence, we discuss the classification of k-dimensional binary optimal SO codes. This correspondence is arranged as follows. First, we give some notations and make some preparation in this section. In Section II, we give the proof of our main result. In Section III, we give the relations of binary SO codes and some systems of linear equations, and explain how to determine the $[15s + t, 4]$ optimal SO codes. In Section IV, we give the classification of $[15s + t, 4]$ optimal SO codes for $t \in \{1, 2, 6, 7, 8, 9, 13, 14\}$ and $s \geq 1$.

Manuscript received April 16, 2007; revised November 22, 2007. This work is supported by Natural Science Foundation of China under Grants 60573040, 60575045, and 70531030, the National Basic Research Program of China (973 Program) under Grant 2007CB311002, the Postdoctoral Science Foundation of China under Grant 20060391009, and the Science Research Foundation of College of Science at AFE University.

R. Li is with the College of Science, Xi'an Jiaotong University, Shaanxi 710049, China, and the Department of Applied Mathematics and Physics, College of Science, Air Force Engineering University, Xi'an, Shaanxi 710051, China (e-mail: liruihu@yahoo.com.cn).

Z. Xu is with the College of Science, Xi'an Jiaotong University, Shaanxi 710049, China (e-mail: zbxu@mail.xjtu.edu.cn).

X. Zhao is with the Department of Applied Mathematics and Physics, College of Science, Air Force Engineering University, Xi'an, Shaanxi 710051, China (e-mail: zly419@163.com).

Communicated by G. Seroussi, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2008.926367

Let F_2^n be the n-dimensional row vector space over the binary field F_2. A binary linear $[n,k]$ code $\mathcal{C}$ is a k-dimensional subspace of F_2^n. The weight $w(x)$ of $x \in \mathcal{C}$ is the number of its nonzero coordinates. A code $\mathcal{C}$ is called *even* if the weights of $x \in \mathcal{C}$ are even and *odd* otherwise. Two binary codes $\mathcal{C}$ and $\mathcal{C}'$ are equivalent if one can be obtained from the other by permuting the coordinates. If two matrices G_1 and G_2 generate equivalent codes, we denote them as $G_1 \cong G_2$.

The dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ is defined as $\mathcal{C}^\perp = \{x \in F_2^n \mid x \cdot y = xy^T = \mathbf{0} \text{for all } \mathbf{y} \in \mathcal{C}\}$. A code $\mathcal{C}$ is *self-orthogonal* if $\mathcal{C} \subseteq \mathcal{C}^\perp$, and *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$. All SO codes are even, but an even code is not always self-orthogonal.

Definition 1.1: An $[n,k]$ SO code $\mathcal{C}$ is called optimal if it has the highest weight among all $[n,k]$ SO codes.

Let $N(n,k)$ be the number of nonequivalent optimal $[n,k]$ SO codes, and $N_0(n,k)$ and $N_1(n,k)$ be the number of nonequivalent optimal $[n,k]$ SO codes with zero coordinates and without zero coordinates, respectively. Then $N(n,k) = N_0(n,k) + N_1(n,k)$. If the minimum distance of an optimal $[n,k]$ SO code equal the minimum distance of an optimal $[n-1,k]$ SO code, then $N_0(n,k) = N(n-1,k)$, otherwise $N_0(n,k) = 0$. Thus, in the following we usually focus on optimal SO codes without zero coordinates.

We use G_k to denote the generator matrix of $[2^k-1,k]$ simplex code, and $\mathbf{1_n}=(1,1,\cdots,1)_{1\times n}$ and $\mathbf{0_n}=(0,0,\ldots,0)_{1\times n}$ to denote the all-ones vector and the zero vector of length n, respectively. And use $iG = (G,G,\cdots,G)$ to denote the juxtaposition of i copies of G for given matrix G.

Our main result of this correspondence is as follows.

Theorem 1.1: Suppose $k \geq 3$, $s \geq 1$, $1 \leq t \leq 2^k - 2$ and $n = (2^k-1)s+t$. Then, every $[n,k,d]$ binary code $\mathcal{C}$ with $d \geq s2^{k-1}$ and without zero coordinates is equivalent to a code with generator matrix $G = ((s-c(k,s,t))G_k \ H)$, where $c(k,s,t) \leq \min\{s,t\}$ is a function of k, s and t, and H has $(2^k-1)c(k,s,t)+t$ columns.

According to Theorem 1.1, the classification of $[n,k]$ optimal SO codes can be reduced to the classification of $[(2^k-1)c(k,s,t)+t,k]$ optimal SO codes.

II. Proof of Theorem 1.1

In order to prove Theorem 1.1, we need some preparation.

Let α_i be the k-dimensional binary column vector representation of i for $0 \leq i \leq 2^k-1$, i.e., $\alpha_0 = (0,0,\ldots,0)^T = \mathbf{0_k^T}$, $\alpha_1=(0,0,\ldots,1)^T$, $\cdots$, $\alpha_{2^k-1} = (1,1,\ldots,1)^T$. Then $G_k = (\alpha_1,\ldots,\alpha_{2^k-1})$ is a generator matrix of $[2^k-1,k]$ simplex code. Using the columns of G_k, we construct a $(2^k-1)\times(2^k-1)$ matrix D_k, where $D_k = (\frac{1}{2}(1-(-1)^{\alpha_i\cdot\alpha_j}))_{1\leq i,j\leq 2^k-1}$.

Let $1 \leq i,j,m \leq 2^k-1$. For each α_i, there are $2^{k-1}-1\alpha_m$'s such that $\alpha_i\cdot\alpha_m = 0$ and $2^{k-1}\alpha_m$'s such that $\alpha_i\cdot\alpha_m = 1$, and if $\alpha_i \neq \alpha_j$, there are $2^{k-2}-1\alpha_m$'s such that $\alpha_i\cdot\alpha_m = \alpha_j\cdot\alpha_m = 0$. Thus each row of D_k has weight 2^{k-1}, and the distance of any two different rows of D_k is 2^{k-1}. Hence, the rows of D_k are just the nonzero vectors of the $[2^k-1,k]$ simplex code generated by G_k.

Suppose G is a generator matrix of an $[n,k]$ code $\mathcal{C}$. If the columns of G have l_i copies of α_i for $0 \leq i \leq 2^k-1$, we denote G as $G = (l_0\alpha_0, l_1\alpha_1, \ldots, l_{2^k-1}\alpha_{2^k-1})$ for short, and call $L_{Gc} = (l_0, l_1, \ldots, l_{2^k-1})$ the *complete define vector* of G and $L_G = (l_1, l_2, \ldots, l_{2^k-1})$ the *define vector* of G. If the code generated by G without zero coordinates, then $L_{Gc} = L_G$. Let $Y^T = D_k L_G^T$, where $Y = (y_1, y_2, \ldots, y_{2^k-1})$. Then the nonzero weights of $\mathcal{C}$ are $y_1, y_2, \ldots, y_{2^k-1}$.

Lemma 2.1: If $k \geq 3$, then D_k is invertible over the rational field $\mathbb{Q}$, and $D_k^{-1} = -\frac{1}{2^{k-1}}((-1)^{\alpha_i\cdot\alpha_j}))_{1\leq i,j\leq 2^k-1}$. And each row (or column) of $2^{k-1}D_k^{-1}$ has 2^{k-1} 1's and $(2^{k-1}-1)-1$'s.

Proof: Let $E_k = -\frac{1}{2^{k-1}}((-1)^{\alpha_i\cdot\alpha_j}))_{1\leq i,j\leq 2^k-1}$, a_i be the ith row of D_k and b_m be the mth column of E_k. From the above discussion, it is easy to check that

$$\begin{aligned} a_i b_m &= -\frac{1}{2^k}\sum_j [1-(-1)^{\alpha_i\cdot\alpha_j}](-1)^{\alpha_j\cdot\alpha_m} \\ &= -\frac{1}{2^k}[\sum_j (-1)^{\alpha_j\cdot\alpha_m} - \sum_j (-1)^{\alpha_j\cdot(\alpha_i+\alpha_m)}] \\ &= -\frac{1}{2^k}[-1-(-1+2^k\delta_{i,m})] \\ &= \delta_{i,m}. \end{aligned}$$

Hence, the Lemma holds.

Proof of Theorem 1.1: Let $G = (l_1\alpha_1, \cdots, l_{2^k-1}\alpha_{2^k-1})$ be a generator matrix of $\mathcal{C}$. The nonzero weights $y_1, y_2, \ldots, y_{2^k-1}$ of $\mathcal{C}$ are given by

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{2^k-1} \end{pmatrix} = D_k \begin{pmatrix} l_1 \\ l_2 \\ \vdots \\ l_{2^k-1} \end{pmatrix}.$$

Let $z_i = y_i - s2^{k-1}$. Then

$$\begin{aligned} \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_{2^k-1} \end{pmatrix} &= D_k \begin{pmatrix} l_1 \\ l_2 \\ \vdots \\ l_{2^k-1} \end{pmatrix} - D_k \begin{pmatrix} s \\ s \\ \vdots \\ s \end{pmatrix} \\ &= D_k \begin{pmatrix} l_1 - s \\ l_2 - s \\ \vdots \\ l_{2^k-1} - s \end{pmatrix}. \end{aligned}$$

i.e.

$$\begin{pmatrix} l_1 - s \\ l_2 - s \\ \vdots \\ l_{2^k-1} - s \end{pmatrix} = D_k^{-1} \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_{2^k-1} \end{pmatrix}.$$

Since $z_i \geq 0$, we have

$$\begin{aligned} l_i - s &\geq -\frac{1}{2^{k-1}}(z_1 + z_2 + \ldots + z_{2^k-1}) \\ &= -\frac{1}{2^{k-1}}[(y_1 + y_2 + \ldots + y_{2^k-1}) - s2^{k-1}(2^k-1)] \\ &= -\frac{1}{2^{k-1}}[2^{k-1}((2^k-1)s+t) - s2^{k-1}(2^k-1)] \\ &= -t. \end{aligned}$$

Let $c(k,s,t) = -\min\{l_i - s \mid 1 \leq i \leq 2^k-1\}$. Then $c(k,s,t) \leq \min\{s,t\}$, and the conclusion follows.

Using Theorem 1.1, one can deduce the following corollary.

Corollary 2.2: If $k \geq 3$, every $[(2^k-1)s, k, s2^{k-1}]$ code is equivalent to the SO code with generator matrix sG_k.

III. Binary Self-Orthogonal Codes and Systems of Linear Equations

We will use systems of liner equations to characterize SO codes of given minimum distance, and explain how to determine the generator

matrices of all $[n, 4]$ optimal SO codes, where $n = 15s+t$, $s \geq 1$ and $1 \leq t \leq 14$. And, we will give a method of determining $c(4, s, t)$ at the end of this section.

Let $\mathcal{C} = [n, k+1, 2m]$ be a SO code. From the definition of equivalence of binary codes, we can assume that $\mathcal{C}$ has generator matrix G, where

$$G = \begin{pmatrix} \mathbf{1_{2m}} & \mathbf{0_{n-2m}} \\ X & Y \end{pmatrix}.$$

Lemma 3.1: Let $\mathcal{C} = [n, k+1, 2m]$ be a SO code with generator matrix G as above, and let the codes generated by $(X \quad Y)$, X and Y be $\mathcal{C}_0$, $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Then $\mathcal{C}_0$ is an $[n, k]$ SO code, $\mathcal{C}_1$ and $\mathcal{C}_2$ are even codes. And the following holds.

1) If $(u \mid v) \in \mathcal{C}_0$ with $u \in \mathcal{C}_1$ and $v \in \mathcal{C}_2$, then $w(u) \leq w(v)$.
2) $d(\mathcal{C}_1) \leq d(\mathcal{C}_2)$ and $d(\mathcal{C}_2) \geq 2\lceil \frac{m}{2} \rceil$.
3) $\mathcal{C}_2$ is an $[n-2m, k]$ code.

Proof: Since $\mathcal{C}$ is self-orthogonal, it is obviously that $\mathcal{C}_0$ is an $[n, k]$ SO code, $\mathcal{C}_1$ and $\mathcal{C}_2$ are even codes.

1) Let $(u \mid v) \in \mathcal{C}_0$ with $u \in \mathcal{C}_1$ and $v \in \mathcal{C}_2$, and $w(u) = 2a$ and $w(v) = 2b$. Then $w(u + \mathbf{1_{2m}} \mid v) = 2m - 2a + 2b \geq d(\mathcal{C}) = 2m$, thus $w(u) \leq w(v)$.
2) If $v_1 \in \mathcal{C}_2$ with $w(v_1) = d(\mathcal{C}_2)$, then there is a $u_1 \in \mathcal{C}_1$ such that $(u_1 \mid v_1) \in \mathcal{C}_0$, and $d(\mathcal{C}_1) \leq w(u_1) \leq w(v_1) = d(\mathcal{C}_2)$. Since $2d(\mathcal{C}_1) \geq w(u_1) + w(v_1) \geq d(\mathcal{C})$ and $d(\mathcal{C}_2)$ is even, thus we have $d(\mathcal{C}_2) \geq 2\lceil \frac{m}{2} \rceil$.

It is obviously that 3) also holds from the discussion of 1) and 2).

Using Lemma 3.1 and the Griesmer bound, one can deduce the following corollary easily.

Corollary 3.2: There are no $[15s+5, 4, 8s+2]$ and $[15s+12, 4, 8s+6]$ SO codes.

Now, we focus our discussion on $[n, 4]$ optimal SO codes without zero coordinates, where $n = 15s + t$ and $s, t \geq 1$, and let $\mathcal{C} = [n, 4, 2m]$ be such a code.

Let G be a generator matrix of $\mathcal{C}$, where G, X, Y as in Lemma 3.1. And, let $X = (l_0\alpha_0, l_1\alpha_1, \ldots, l_7\alpha_7)$ and $Y = (r_1\alpha_1, r_2\alpha_2, \ldots, r_7\alpha_7)$. Then, $L_0 = (l_0, l_1, \cdots, l_7)$ is the complete define vectors of X, $L = (l_1, l_2, \cdots, l_7)$ and $R = (r_1, r_2, \cdots, r_7)$ are the define vectors of X and Y, respectively. Since G can be completed determined by (L_0, R), we call (L_0, R) the *define vectors* of G. Let $W_X^T = D_3 L^T$ and $W_Y^T = D_3 R^T$, where $W_X = (x_1, x_2, \ldots, x_7)$ and $W_Y = (y_1, y_2, \ldots, y_7)$. Then, we change the problem of determine G into that of determine X and Y (or (L_0, R)).

Since $GL(3, 2)$ acts double transitively on $\{\alpha_1, \cdots, \alpha_7\}$, so, in the following, we can assume $r_1 \geq r_2 \geq r_i$, $i = 3, 4, \cdots, 7$, and $r_4 \geq r_j$, $j = 5, 6, 7$ as in [3].

Since $y_1 + y_2 + \cdots + y_7 = 4(n - 2m)$, we have the following system of linear equations:

$$\begin{cases} R^T = D_3^{-1} W_Y^T \\ y_i \equiv 0 (mod 2), i = 1, 2, \cdots, 7 \\ 2\lceil \frac{m}{2} \rceil \leq y_i \leq n - 2m \\ y_1 + y_2 + \cdots + y_7 = 4(n - 2m) \\ r_1 \geq r_2 \geq r_i, i = 3, 4, \cdots, 7 \\ r_4 \geq r_j, j = 5, 6, 7. \end{cases} \tag{1}$$

For each given $W_Y = (y_1, y_2, \cdots, y_7)$ satisfying $y_1 + y_2 + \cdots + y_7 = 4(n - d(\mathcal{C}))$, $y_i \equiv 0 (\mathrm{mod}\ 2)$ and $y_i \geq d(\mathcal{C}_2)$ for $1 \leq i \leq 7$, such Y exists if and only if (1) has nonnegative integer solutions. Thus, one can easily determine all the possible Y (or R) by the nonnegative integer solutions of (1).

Once R (or Y) satisfying (1) is given, from [3] and Lemma 3.1, we know that $r_i + l_i \equiv r_j + l_j (\mathrm{mod}\ 2)$, and $x_i \leq y_i$ for $1 \leq i \leq 7$. Thus, W_X and L_0 can be determined by the following system of linear equations (2):

$$\begin{cases} L^T = D^{-1} W_X^T \\ x_i \equiv 0 (\mathrm{mod}\ 2) \\ x_i + y_i \geq 2m, 1 \leq i \leq 7 \\ y_i - x_i \geq 0, 1 \leq i \leq 7 \\ r_i + l_i \equiv r_j + l_j (\mathrm{mod}\ 2), 1 \leq i, j \leq 7 \\ l_0 = 2m - (l_1 + \cdots + l_7). \end{cases} \tag{2}$$

Then, X exists if and only if (2) has nonnegative integer solutions. Thus, one can easily determine all the possible X by the nonnegative integer solutions of (2), and determine all the possible generator matrix G of $[n, 4, 2m]$ optimal SO codes at last.

For given $s \geq 1$ and $1 \leq t \leq 14$. Denote the set of all the generator matrix G (determined above) of $[15s + t, 4]$ optimal SO codes as $\mathcal{G}[15s + t, 4]$, and let $\mathcal{D}[15s + t, 4] = \{(L_0, R) \mid (L_0, R)$ is the define vectors of $G, G \in \mathcal{G}[15s + t, 4]\}$. Then $c(4, s, t) = -\min_{0 \leq i \leq 7, 1 \leq j \leq 7} \{l_i - s, r_j - s \mid (L_0, R) \in \mathcal{D}[15s + t, 4]\}$.

IV. Classification of Four-Dimensional (4-D) Optimal SO Codes

In this section, we will study the classification of optimal $[n, 4]$ SO codes for $n = 15s + t, s \geq 1$ and $t \in \{1, 2, 6, 7, 8, 9, 13, 14\}$. According to Corollary 2.2 and 3.2, and the relations among $N(n, k)$, $N_0(n, k)$, $N_1(n, k)$ and $N(n-1, k)$, we only need to give $N_1(n, 4)$.

To save space, we only explain our classification process for $[15s + 1, 4]$ OSO codes, other case can be deduced similarly. And, we use OSO codes to represent optimal SO codes without zero coordinates in this section.

Case 1: $n = 15s + 1, s \geq 1$.

A $[15s + 1, 4]$ OSO code has minimum distance $8s$. Using MATLAB [8] program, one can easily check that there are seven solutions satisfying (1) and (2), thus $\mathcal{D}[15s + 1, 4]$ has seven elements, denoted as $(L_{0i}, R_i) = (\boldsymbol{s1_8}, \boldsymbol{s1_7}) + (L'_{0i}, R'_i)$, $1 \leq i \leq 7$, where $L'_{01} = (-1, 1, 1, -1, 1, -1, -1, 1) = -L'_{02}$, $L'_{03} = \mathbf{0_8}$, $L'_{04} = (1, -1, -1, 1, 0, 0, 0, 0) = -L'_{05}$, $L'_{06} = -L'_{07} = (0, 0, 0, 0, 1, -1, -1, 1)$, $R'_i = (1, 1, -1, 1, -1, -1, 1)$ for $1 \leq i \leq 3$, and $R'_i = (1, 1, -1, 0, 0, 0, 0)$ for $4 \leq i \leq 7$. Thus $c(4, s, 1) = 1$. Accordingly, the generator matrices $G_{n(i)}$, $1 \leq i \leq 7$, of these 7 OSO codes are determined.

Let the define vectors of $H_{16,j}$ be $(L_{0,j}, R)$ and $G_{n,j} = ((s-1)G_4\ H_{16,j})$, $j = 1, 2$,where $L_{0,1} = (0, 2, 2, 0, 2, 0, 0, 2)$, $L_{0,2} = (1, 1, \ldots, 1)$, $R = (2, 2, 0, 2, 0, 0, 2)$. It is easy to check that $G_{n(i)} \cong G_{n,1}$ for $1 \leq i \leq 2$, and $G_{n(i)} \cong G_{n,2}$ for $3 \leq i \leq 7$. Thus, we have the following theorem.

Theorem 4.1: If $n = 15s + 1, s \geq 1$, then $N_1(n, k) = 2$. The two nonequivalent $[n, 4, 8s]$ OSO codes have generate matrices $G_{n,1}$ and $G_{n,2}$, their weight polynomials are $1 + 14y^{8s} + y^{8s+8}$ and $1 + 13y^{8s} + 2y^{8s+4}$, respectively.

Case 2: $n = 15s + 2, s \geq 1$.

Let the define vectors of $H_{17,i}$ be $(L_{0,i}, R_1)$ and $H_{32,i} = ((s-1)G_4\ H_{17,i})$ for $i = 1, 2$, where $L_{0,1}$ and $L_{0,2}$ as in **Case 1**, and $R_1 = (3, 1, \ldots, 1)$.

Let the define vectors of $H_{32,j}$ be $(L_{0,j}, R_j)$ for $3 \leq j \leq 9$, where $L_{0,3} = (2, 2, \ldots, 2) = L_{0,7}, L_{0,4} = (0, 3, 3, 2, 3, 2, 2, 1)$, $L_{0,5} = (0, 4, 3, 1, 3, 1, 2, 2), L_{0,6} = (0, 3, 3, 2, 3, 2, 3)$, $L_{0,8} = (3, 1, 1, 3, 1, 3, 3, 1)$, $L_{0,9} = (0, 4, 4, 0, 4, 0, 0, 4)$, $R_3 =$

$(4,4,0,2,2,2,2)$, $R_4=(3,3,2,3,2,2,1)$, $R_5=(4,3,1,3,1,2,2)$, $R_6=(3,3,2,3,2,3)$, $R_7=(4,4,0,4,0,0,4)=R_8=R_9$.

If $s\geq 2$, let $G_{n,l}=((s-2)G_4\ H_{32,l})$ for $1\leq l\leq 9$.

Theorem 4.2: Let $n=15s+2, s\geq 1$.

1) If $s=1$, then $N_1(17,4)=2$. The two $[17,4,8]$ OSO codes have generate matrices $H_{17,1}$ and $H_{17,2}$, and have weight polynomials $1+11y^8+4y^{12}$ and $1+7y^8+8y^{10}$, respectively.
2) If $s\geq 2$, then $N_1(n,4)=9$. The nine nonequivalent $[n,4,8s]$ OSO have generate matrices $G_{n,i}$, $1\leq i\leq 9$, their weight polynomials are $1+11y^{8s}+4y^{8s+4}$, $1+7y^{8s}+8y^{8s+2}$, $1+11y^{8s}+4y^{8s+4}$, $1+11y^{8s}+4y^{8s+4}$, $1+12y^{8s}+2y^{8s+4}+y^{8s+12}$, $1+12y^{8s}+2y^{8s+4}+y^{8s+12}$, $1+13y^{8s}+2y^{8s+8}$, $1+13y^{8s}+y^{8s+4}+y^{8s+12}$, $1+14y^{8s}+y^{8s+16}$, respectively.

Case 3: $n=15s+6, s\geq 1$.

Let the define vectors of H_{21} be $(L_{0,a}, R_a)$ and $H_{36,1}=(G_4\ H_{21})$, where $L_{0,a}=(1,2,2,1,2,1,1,0)$, $R_a=(2,2,1,2,1,1,2)$. Let the define vectors of $H_{36,2}$ be $(L_{0,b}, R_b)$, where $L_{0,b}=(3,2,2,3,2,3,3,0)$, $R_b=(3,3,2,3,2,2,3)$. For $s\geq 2$, let $G_{n,i}=((s-2)G_4\ H_{36,i})$, $1\leq i\leq 2$.

Theorem 4.3: Let $n=15s+6, s\geq 1$.

1) If $s=1$, then $N_1(n,4)=1$. The $[21,4,10]$ OSO code has generate matrix H_{21} and weight polynomial $1+8y^{10}+6y^{12}+y^{16}$.
2) If $s\geq 2$, then $N_1(n,4)=2$. The two nonequivalent $[n,4,8s+2]$ OSO codes have generate matrices $G_{n,1}$ and $G_{n,2}$, and their weight polynomials are $1+8y^{8s+2}+6y^{8s+4}+y^{8s+8}$ and $1+7y^{8s+2}+7y^{8s+4}+y^{8s+6}$, respectively.

Case 4: $n=15s+7, s\geq 1$.

Let the define vectors of $H_{22,i}$ be $(L_{01,i}, R_i)$ and $H_{37,i}=(G_4\ H_{22,i})$, $1\leq i\leq 6$, where $L_{01,1}=(1,2,2,1,2,1,1,0)$, $L_{01,2}=(0,3,3,0,3,0,0,1)$, $L_{01,3}=(1,2,2,1,1,0,0,3)$, $L_{01,4}=(2,1,1,2,2,1,1,0)$, $L_{01,5}=(2,0,2,2,2,2,0,0)$,$L_{01,6}=(1,2,1,2,1,2,1,0)$, $R_1=(3,3,0,3,0,0,3)=R_2$, $R_3=(3,3,0,2,1,1,2)=R_4$, $R_5=(2,2,2,2,2,2,0)$, $R_6=(3,2,1,2,1,2,1)$.

Let the define vectors of $H_{37,j}$ be $(L_{02,j}, R_j)$ for $7\leq j\leq 8$, where $L_{02,7}=(3,2,2,3,2,3,3,0)$, $L_{02,8}=(2,3,3,2,2,3,3,0)$, $R_7=(4,4,1,4,1,1,4)$, $R_8=(4,4,1,3,2,2,3)$.

Let the define vectors of $H_{52,l}$ be $(L_{03,l}, R_l)$ for $9\leq l\leq 12$, where $L_{03,9}=(5,2,2,5,2,5,5,0)$, $L_{03,10}=(4,3,3,4,2,5,5,0)$, $L_{03,11}=(3,4,3,4,3,4,5,0)$, $L_{03,12}=(2,4,4,4,4,4,4,0)$, $R_9=(5,5,2,5,2,2,5)$, $R_{10}=(5,5,2,4,3,3,4)$, $R_{11}=(5,4,3,4,3,4,3)$, $R_{12}=(4,4,4,4,4,4,2)$.

Let $H_{52,m}=(G_4\mid H_{37,m})$ for $1\leq m\leq 8$, and $G_{n,p}=((s-3)G_4\mid H_{52,p})$ for $s\geq 3$ and $1\leq p\leq 12$.

Theorem 4.4: Let $n=15s+7, s\geq 1$.

1) If $s=1$, then $N_1(22,4)=6$. The six nonequivalent $[22,4,10]$ OSO codes have generate matrix $H_{22,i}$, $1\leq i\leq 6$, and their weight polynomials $W_{22,i}$ are $1+7y^{10}+6y^{12}+y^{16}+y^{18}$, $1+7y^{10}+7y^{12}+y^{22}$, $1+6y^{10}+7y^{12}+y^{14}+y^{18}$, $1+6y^{10}+6y^{12}+2y^{14}+y^{16}$, $1+6y^{10}+6y^{12}+2y^{14}+y^{20}$, $1+5y^{10}+7y^{12}+3y^{14}$, respectively.
2) If $s=2$, then $N_1(37,4)=8$. The eight nonequivalent $[37,4,18]$ OSO codes have generate matrices $H_{37,j}, 1\leq j\leq 8$, their weight polynomials $W_{37,j}$ are $W_{37,i}=1+y^8(W_{22,i}-1)$ for $1\leq i\leq 6$, and $W_{37,7}=1+7y^{18}+6y^{20}+y^{22}+y^{28}$, $W_{37,8}=1+7y^{18}+5y^{20}+y^{22}+2y^{24}$, respectively.
3) If $s\geq 3$, then $N_1(n,4)=12$. The twelve nonequivalent $[n,4,8s+2]$ OSO codes have generate matrices $G_{n,l}$, $1\leq l\leq 12$, their weight polynomials $W_{n,l}$ are $W_{n,j}=1+y^{8(s-2)}(W_{37,j}-1)$ for $1\leq j\leq 8$, and $1+8y^{8s+2}+6y^{8s+4}+y^{8s+16}$, $1+8y^{8s+2}+5y^{8s+4}+y^{8s+8}+y^{8s+12}$, $1+8y^{8s+2}+4y^{8s+4}+3y^{8s+8}$, $1+8y^{8s+2}+4y^{8s+4}+3y^{8s+8}$, respectively.

Case 5: $n=15s+8, s\geq 1$.

Theorem 4.5: If $n=15s+8, s\geq 1$, then $N(n,4)=N_1(n,k)=1$. The only $[n,4,8s+4]$ OSO code is the juxtaposition of s-copies of simplex codes and the $[8,4,4]$ self-dual code, and has weight polynomial $1+14y^{8s+4}+y^{8s+8}$.

Case 6: $n=15s+9, s\geq 1$.

Let the define vectors of $H_{24,i}$ be $(L_{0i,c}, R_{i,c})$ and $G_{n,i}=(G_4\ H_{24,i})$, $1\leq i\leq 4$, where $L_{01,c}=(3,0,0,3,0,3,3,0)$, $L_{02,c}=(2,1,1,2,1,2,2,1)$, $L_{03,c}=(2,1,1,2,2,1,1,2)$, $L_{04,c}=(0,3,3,0,3,0,0,3)$, $R_{1,c}=R_{2,c}=R_{4,c}=(3,3,0,3,0,0,3)$, $R_{3,c}=(3,3,2,1,1,2)$.

Theorem 4.6: If $n=15s+9$ and $s\geq 1$, then $N_1(n,4)=4$. The four nonequivalent $[n,4,8s+4]$ OSO codes have generator matrices $G_{n,i}$, $1\leq i\leq 4$, and their weight polynomials are $1+14y^{8s+4}+y^{8s+16}$, $1+13y^{8s+4}+y^{8s+8}+y^{8s+12}$, $1+12y^{8s+4}+3y^{8s+8}$, and $1+12y^{8s+4}+3y^{8s+8}$, respectively.

Case 7: $n=15s+13, s\geq 1$.

Let the define vectors of H_{28} be $(L_{0,d}, R_d)$ and $G_n=((s-1)G_4\mid H_{28})$ for $s\geq 1$, where $L_{0,d}=(0,2,\ldots,2)$, $R_d=(2,\ldots,2)$.

Theorem 4.7: If $n=15s+13, s\geq 1$, then $N_1(n,k)=1$. The only $[n,4,8s+6]$ SO code has generator matrix G_n, and has weight polynomial $1+8y^{8s+6}+7y^{8s+8}$.

Case 8: $n=15s+14, s\geq 1$.

Let the define vectors of $H_{29,i}$ be $(L_{01,e}, R_{i,e})$ and $H_{44,i}=(G_4\ H_{29,i})$ for $1\leq i\leq 3$, where $L_{01,e}=(3,1,1,3,1,3,1,1)$, $L_{02,e}=(2,2,2,2,3,1,1,1)$, $L_{03,e}=(0,2,2,\ldots,2)$, $R_{1,e}=R_{3,e}=(3,3,1,3,1,1,3)$, $R_{2,e}=(3,3,1,2,2,2,2)$.

Let the define vectors of $H_{44,l}$ be $(L_{0l,e}, R_{l,e})$ for $4\leq l\leq 5$, where $L_{04,e}=(0,4,4,2,4,2,2,4)=(0,R_{4,e})$, $L_{05,e}=(0,4,4,2,3,3,3,3)=(0,R_{5,e})$. Let $G_{n,m}=((s-2)G_4\ H_{44,m})$ for $s\geq 2$ and $1\leq m\leq 5$.

Theorem 4.8: Let $n=15s+14, s\geq 1$ as follows.

1) If $s=1$, then $N_1(n,4)=3$, the three nonequivalent $[29,4,14]$ OSO codes have generate matrix $H_{29,1}$, $H_{29,2}$ and $H_{29,3}$, and their weight polynomials are $1+7y^{14}+7y^{16}+y^{22}$, $1+6y^{14}+7y^{16}+2y^{18}$, $1+7y^{14}+6y^{16}+y^{18}+y^{20}$, respectively.
2) If $s\geq 2$, then $N_1(n,4)=5$. The five nonequivalent $[n,4,8s+6]$ OSO codes have generator matrices $G_{n,i}$, $1\leq i\leq 5$, and their weight polynomials are $1+7y^{8s+6}+7y^{8s+8}+y^{8s+14}$, $1+6y^{8s+6}+7y^{8s+8}+2y^{8s+10}$, $1+7y^{8s+6}+6y^{8s+8}+y^{8s+10}+y^{8s+12}$, $1+8y^{8s+6}+6y^{8s+8}+y^{8s+16}$, $1+8y^{8s+6}+5y^{8s+8}+2y^{8s+12}$, respectively.

V. Conclusion

We have given the complete classification of $[15s+t,4]$ optimal SO codes for $s\geq 1$ and $t\in\{1,2,6,7,8,9,13,14\}$. Our classification results of optimal $[n,4]$ SO codes for $n\leq 40$ in Section IV are concordant with the results of [3]. For $t\in\{3,4,5,10,11,12\}$ and $s\geq 1$, the classification of $[15s+t,4]$ optimal SO codes can also be given as in Section IV, but a little complex and lengthy, we will discuss in another paper. The method we used in Section III can be generalized to $[n,k]$ optimal SO codes for $k\geq 4$.

ACKNOWLEDGMENT

The authors are very grateful to an anonymous referee for the proofs of Lemma 2.1 and Theorem 1.1 which simplifies the original proofs.

REFERENCES

[1] S. Bouyuklieva, "Some optimal self-orthogonal codes and self-dual codes," *Discr. Math.*, vol. 287, pp. 1–10, 2004.
[2] I. Bouyukliev and P. Ostergard, "Classification of self-orthogonal codes over F_3 and F_4," *SIAM J. Discr. Math.*, vol. 19, no. 2, pp. 363–370, 2005.
[3] I. Bouyukliev, S. Bouyuklieva, T. A. Gulliver, and P. Ostergard, *Classification of Optimal Binary Self-Orthogonal Codes.* [Online]. Available: http://users.tkk.fi/pat/patric-pub-html
[4] W. C. Huffman, "On the classification and enumeration of self-dual codes," *Finite Fields Appl.*, vol. 11, pp. 451–490, 2005.
[5] W. C. Huffman and V. Pless, *Fundmentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge University Press, 2003.
[6] V. Pless, "A classification of self-orthogonal codes over GF (2)," *Discr. Math.*, vol. 3, pp. 209–246, 1972.
[7] E. M. Rains and N. J. A. Sloane, "Self-Dual Codes," in *Handbook of Coding Theory*, W. C. Huffman and V. S. Pless, Eds. Amsterdam, The Netherlands: Elsevier, 1998, pp. 177–294.
[8] The MathWorks, MATLAB R2006a, Natick, MA, 2006.

The Icosian Code and the E_8 Lattice: A New 4×4 Space–Time Code With Nonvanishing Determinant

Jiaping Liu and A. Robert Calderbank, *Fellow, IEEE*

***Abstract*—This paper introduces a new rate-2, full-diversity space–time code for four transmit antennas and one receive antenna. The 4×4 codeword matrix consists of four 2×2 Alamouti blocks with entries from $Q(i, \sqrt{5})$, and these blocks can be viewed as quaternions which in turn represent rotations in R^3. The Alamouti blocks that appear in a codeword are drawn from the icosian ring consisting of all linear combinations of 120 basic rotations corresponding to symmetries of the icosahedron. This algebraic structure is different from the Golden code, but the complex entries are taken from a common underlying field. The minimum determinant is bounded below by a constant that is independent of the signal constellation, and the new code admits a simple decoding scheme that makes use of a geometric correspondence between the icosian ring and the E_8 lattice.**

***Index Terms*—Space–time codes, icosian ring, Gosset lattice E_8, reduced complexity decoding algorithms.**

I. INTRODUCTION

Space–time codes improve the reliability of communication systems over fading channels by correlating signals across different transmit antennas. Tarokh *et al.* [1] developed the following two design criteria for the high SNR regime.

- **Rank Criterion**: Maximize the minimum rank r of the difference $X_i - X_j$ over all distinct pairs of space–time codewords X_i, X_j; the space–time code achieves a *diversity gain* of r.
- **Determinant Criterion**: For a given diversity r, maximize the minimum product δ of the nonzero singular values of the difference $X_i - X_j$ over all distinct pairs of space–time codewords X_i, X_j; the product δ determines the *coding gain* of the space-time code.

The construction of space–time block codes that achieve particular rate–diversity tradeoffs is an area of intense research activity (see [2]–[9]), and many authors have used algebraic techniques to guarantee full diversity (see the monograph by Viterbo and Oggier [10] connecting algebraic number theory to code design for Rayleigh-fading channels). We will follow this approach to get full diversity, and in addition, we will use the algebraic techniques to introduce a geometric structure that simplifies decoding.

Conway and Sloane [12] connected the geometry of finite-dimensional lattices with signal constellation design for the additive white Gaussian noise channel. The lattice/coset framework provides solutions to the problem of addressing the signal constellation at the encoder and the problem of decoding the received vector to the closest lattice point at the decoder. We are able to simplify decoding of the new space–time block code by associating constituent Alamouti blocks with vectors in the Gosset lattice E_8 and then applying the E_8 decoding algorithms developed by Conway and Sloane.

The new code is described by a 4×4 matrix for four transmit antennas and one receive antenna for the implementation of its low-complexity decoding algorithm. It contains four 2×2 Alamouti blocks, each of which is the quaternionic form of an icosian. The algebraic structure of the code is similar to the Golden code [2] of Belfiore *et al.* in that algebraic conjugation interchanging $\sqrt{5}$ and $-\sqrt{5}$ appears as the isomorphism of the Galois extension $Q(i, \sqrt{5})/Q(i)$ used in the construction of the Golden code. The codeword matrix takes the form

$$X = \begin{bmatrix} A & B \\ \bar{B} \cdot K & \bar{A} \end{bmatrix}$$

where information symbols A and B are icosians in Alamouti blocks and $\bar{A}, \bar{B}$ are the algebraic conjugates of A, B. Moreover, a "magic K" which is also an Alamouti block of an icosian will be chosen to guarantee full diversity. A similar approach to increasing diversity by rotation is given by Jafarkhani for his quasi-orthogonal code design [5].

The correspondence is organized as follows. Section II introduces the icosian ring and derives some important properties. Section III gives the construction of the new 4×4 Space–Time Block Code (STBC) based on the icosian ring and establishes full diversity. Section IV develops a coherent decoding scheme with reduced complexity, using the correspondence of the icosian ring with the E_8 lattice. Simulation results are presented in Section V and conclusions are given in Section VI.

II. THE ICOSIAN RING AND THE LATTICE E_8

We assume a basic familiarity with quaternion algebra, including the classical two-to-one correspondence between unit quaternions and rotations in SO_3, and we refer readers interested in more details to Conway and Sloane [12, pp. 52–55].

Definition 1: The double cover $2I$ of the icosahedral group is a multiplicative group of order 120 consisting of the quaternions

$$(\pm 1, 0, 0, 0)^E, \frac{1}{2}(\pm 1, \pm 1, \pm 1, \pm 1)^E, \frac{1}{2}(0, \pm 1, \pm \sigma, \pm \tau)^E$$

where $(\alpha, \beta, \gamma, \delta)$ means $\alpha + \beta i + \gamma j + \delta k$, $\sigma = \frac{1-\sqrt{5}}{2}$, $\tau = \frac{1+\sqrt{5}}{2}$, and the superscript E means that all even permutations of the coordinates are permitted.

Manuscript received September 2, 2006; revised February 5, 2008. This work was supported in part by the National Science Foundation under Contract 1096066. The material in this correspondence was presented in part at the IEEE International Symposium on Information Theory, Seattle, WA, July 2006.

The authors are with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 (e-mail: jiapingl@princeton.edu; calderbk@princeton.edu).

Communicated by G. Seroussi, Associate Editor for Coding Theory.

Color versions of Figures 1–3 in this correspondence are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2008.926352