Some results on self-orthogonal and self-dual codes

S. Georgiou, C. Koukouvinos
Department of Mathematics
National Technical University of Athens
Zografou 15773, Athens, Greece

and

J. Seberry
School of IT and Computer Science
University of Wollongong
Wollongong, NSW, 2522, Australia

Abstract

We use generator matrices G satisfying $GG^T = aI + bJ$ over $\mathbb{Z}_k$ to obtain linear self-orthogonal and self-dual codes. We give a new family of linear self-orthogonal codes over $GF(3)$ and $\mathbb{Z}_4$ and a new family of linear self-dual codes over $GF(3)$.

Key words and phrases: Self-orthogonal, self-dual, codes, construction, conference matrix, projective plane.
AMS Subject Classification: Primary 94B05, 94B25, Secondary 05B20.

1 Introduction

A linear code C of length n over $\mathbb{Z}_k$ (or a $\mathbb{Z}_k$-code of length n) is a $\mathbb{Z}_k$-submodule of $\mathbb{Z}_k^n$. If $k = p$ is prime then $\mathbb{Z}_p = GF(p)$ and a linear code of length n is a subspace of $GF(p)$. An element of C is called a codeword. We define the inner product on $\mathbb{Z}_k^n$ by $x \cdot y = x_1y_1 + \cdots + x_ny_n$, where $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$. The dual code $C^{\perp}$ of C is defined as $C^{\perp} = \{v \in \mathbb{Z}_k^n \mid v \cdot w = 0 \text{ for all } w \in C\}$. A code C is *self-dual* if $C = C^{\perp}$. The Hamming weight ($wt(c)$)of a codeword c is the number of non-zero components in the codeword. The *minimum weight* of a code C

is the smallest weight among all codeswords of C. The minimum distance of a linear code C is its minimum weight. We say that self-dual codes with the largest minimum weight among self-dual codes of that length are *optimal*. A linear code over $GF(p)$ of length n with k independed rows in its generator matrix will be denoted as $[n, k; p]$. Furthermore, if its minimum distance is d it will be denoted as $[n, k, d; p]$.

Two codes over $\mathbb{Z}_k$ are said to be *equivalent* if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates.

There has been a large amount of research recently devoted to self-orthogonal and self-dual codes over the ring $\mathbb{Z}_4$, [1, 3, 5, 7]. Patrick Solé's remark that the orthogonality of Hadamard matrices can naturally be interpreted as $\mathbb{Z}_4$-orthogonality was investigated in [4]. These self-orthogonal and self-dual codes over $\mathbb{Z}_4$ were obtained from equivalence classes of Hadamard matrices.

2 The constructions

We give a general theorem which will be used later in the paper.

Theorem 1 *Suppose A and B are two matrices of order n over $\mathbb{Z}_k$ satisfying*

$$AA^T + BB^T = sI + rJ$$

where $s \equiv r \equiv 0(mod\ k)$. Then

$$G = [A\ B]$$

generates a linear self-orthogonal code over $\mathbb{Z}_k$, of length $2n$ and with m, $m \leq \frac{n}{2}$ independed rows in its generator matrix. □

The next corollary is a generalization of a construction given by Georgiou and Koukouvinos [6].

Corollary 1 *Suppose A and B are two matrices of order n over $\mathbb{Z}_k$ satisfying*

$$AA^T = a_1 I + a_2 J \text{ and } BB^T = b_1 I + b_2 J$$

where $a_1 + b_1 \equiv a_2 + b_2 \equiv 0(mod\ k)$. Then

$$G = [A\ B]$$

generates a linear self-orthogonal code of length $2n$ and with m independed rows in its generator matrix, over $\mathbb{Z}_k$, $m \leq \frac{n}{2}$. □

Theorem 2 *Suppose A and B are two matrices of order n over $\mathbb{Z}_k$ satisfying*

$$AA^T = a_1 I + a_2 J \text{ and } BB^T = b_1 I + b_2 J$$

where $a_2 + b_2 \equiv 0(mod\ k)$ and $a_1 + b_1 + a \equiv 0(mod\ k)$ for some $a \in \mathbb{Z}_k$. Then

$$G_2 = \left[aI_{2n}, \begin{matrix} A & B \\ B^T & -A^T \end{matrix} \right]$$

generates a linear self-dual code of length $4n$ and with $2n$ independed rows in its generator matrix, over $\mathbb{Z}_k$. □

Example 1 (i) Set $A = B = circ(1,1,1,1,0)$. We have that $AA^T = BB^T = I + 3J$. Then

$$G_2 = \left[I_{2n} \begin{matrix} A & B \\ B^T & -A^T \end{matrix} \right]$$

generates an $[20, 10, 6; 3]$ extremal self-dual code with weight enumerator

$$W(z) = 1 + 120z^6 + 4260z^9 + 26280z^{12} + 25728z^{15} + 2560z^{18}.$$

(ii) Set $A = circ(-2,-2,0,-1,0)$ and $B = circ(-1,-1,-1,-1,1)$. We have that $AA^T = 5I + 4J$ and $BB^T = 4I + J$. Then

$$G_2 = \left[I \begin{matrix} A & B \\ B^T & -A^T \end{matrix} \right]$$

generates an $[20, 10, 8; 5]$ extremal self-dual code with weight enumerator

$$W(z) = 1 + 1280z^8 + 3200z^9 + 24848z^{10} + 58560z^{11} + 248480z^{12} + +464960z^{13} + 1175840z^{14} + 1568000z^{15} + 2267240z^{16} + +1896720z^{17} + 1398960z^{18} + 541760z^{19} + 115776z^{20}.$$

(ii) Set $A = circ(-2,-2,0,-1,0)$ and $B = circ(-1,-1,-1,-1,1)$. We have that $AA^T = 5I + 4J$ and $BB^T = 4I + J$. Then

$$G = [A\ B]$$

generates an $[10, 5, 4; 5]$ self-dual code with weight enumerator

$$W(z) = 1 + 40z^4 + 44z^5 + 220z^6 + 760z^7 + 940z^8 + 740z^9 + 380z^{10}.$$

For the SBIBDs we use in the remainder of this paper, we refer the reader to the book of Beth, Jungnickel and Lenz [2]. By $A = SBIBD(v, k, \lambda)$ we denote the $v \times v$ $(0,1)$ incidence matrix of the $SBIBD(v,k,\lambda)$.

Example 2

1. There exist A=SBIBD(31,10,3) and B=SBIBD(31,15,7), so $[A\ B]$ generates a linear self-orthogonal code of length 62 and with k_1 independed rows in its generator matrix, over $GF(5)$ with minimum distance d_1 as
$$AA^T = 7I + 3J \text{ and } BB^T = 8I + 7J.$$
2. There exist A=SBIBD(71,15,3) and B=SBIBD(71,21,6), so $[A\ B]$ generates a linear self-orthogonal code of length 142 and with k_2 independed rows in its generator matrix, over $GF(3)$ with minimum distance d_2 as
$$AA^T = 12I + 3J \text{ and } BB^T = 15I + 6J.$$
3. There exist A=SBIBD(133,33,8) and B=SBIBD(133,12,1), so $[A\ B]$ generates a linear self-orthogonal code of length 266 and with k_3 independed rows in its generator matrix, over $GF(3)$ with minimum distance d_3 as
$$AA^T = 25I + 8J \text{ and } BB^T = 11I + J.$$

□

In the next theorems we use specific families to find linear self-orthogonal codes. We combine skew-Hadamard matrices or conference matrices with incidence matrices of projective planes to construct some linear self-orthogonal codes over $\mathbb{Z}_k$.

Details on skew-Hadamard matrices and conference matrices required for the next theorem can be found in Seberry and Yamada [9]. Appropriate details of the incidence matrices of projective planes can be found in Ryser [8].

Theorem 3 *Let $p+1$ be the order of a skew-Hadamard matrix or a conference matrix. Suppose $p = q^2 + q + 1$ for some prime power q. Then there exists a self-orthogonal code over $\mathbb{Z}_k$ of length $2p$, with m independed rows in its generator matrix and minimum distance d whenever $p + q = (q+1)^2 \equiv 0 \ (\ mod\ k)$.*

Proof. Write the skew-Hadamard matrix $S+I$, minus its diagonal entries, or conference matrix as
$$\begin{bmatrix} 0 & e \\ \pm e^T & P \end{bmatrix}$$

where e is the $1 \times p$ matrix of ones. Then P is a $p \times p$ matrix satisfying

$$PP^T = pI - J.$$

Write Q for an incidence matrix of the projective plane over $GF(q)$. Then Q, of order $p = q^2 + q + 1$, is circulant and satisfies

$$QQ^T = qI + J.$$

Now $G_1 = [P\ Q]$ generates the required self-orthogonal code over $\mathbb{Z}_k$ of length $2p$ and with m, $m \leq p$ independed rows in its generator matrix as $G_1 G_1^T = (p+q)I = (q+1)^2 I \equiv 0$. □

Corollary 2 *Let $p+1$ be the order of a skew-Hadamard matrix or a conference matrix. Suppose $p = q^2 + q + 1$ for some prime power q, and $q \equiv 2 (mod\ 3)$. Then there exists a self-orthogonal $[2p, m, d]$ ternary code with $m \leq p - 1$. Note that $m = p$ iff $q \equiv 1$ (mod 3) and thus $G_1 = [P\ Q]$ is the generator matrix of a self-dual code.*

Proof. Use theorem 3. □

Example 3 *Let $q = 2$, $p = 7$, $P = circ(0,1,1,-1,1,-1,-1)$ and $Q = circ(1,1,0,1,0,0,0)$. We consider the matrix $[P\ Q]$ and we remove its first row. Then the derived matrix is the generator matrix of a $[14,6,6;3]$ code with weight enumerator*

$$W(z) = 1 + 84z^6 + 476z^9 + 168z^{12}.$$

Theorem 4 *The codes over $GF(3)$ and $\mathbb{Z}_4$ we obtain using G_1 are*

(i) $[2p, p, d]$ for $q \equiv 1 (mod\ 3)$

(ii) $[2p, p-1, d]$ for $q \equiv 0, 2 (mod\ 3)$ and $q \equiv 0, 1, 2, 3 (mod\ 4)$.

Proof. Consider the matrix P of order $p = q^2 + q + 1$. Now $PP^T = (q^2+q+1)I - J$ and det $PP^T \equiv 0 (mod\ 3)$ and $0 (mod\ 4)$. Now consider P' with one row of P removed. Then the matrix P' has size $(q^2+q) \times (q^2+q+1)$ and so $P'P'^T$ is of order $q^2 + q$ and has the following form:

$$P'P'^T = \begin{bmatrix} q^2+q & -1 & -1 & \cdots & -1 \\ -1 & q^2+q & -1 & \cdots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & -1 & \cdots & q^2+q \end{bmatrix}$$

and det $P'P'^T = (1)(q^2+q+1)^{q^2+q-1} \not\equiv 0$ for $q \equiv 0, 2(mod\ 3)$ and $q \equiv 0, 1, 2, 3(mod\ 4)$. Hence the rank of the matrix P' is $p-1$ for these cases.
Now the matrix Q satisfies $QQ^T = qI + J$ and det $QQ^T = (q+1)^2(q)^{q^2+q} \not\equiv 0(mod\ 3)$ for $q \equiv 1(mod\ 3)$. Hence the rank of the matrix Q is p for this case. □

Remark 1 We recall that a self-orthogonal code, C, of length $2p$, with p independed rows in its generator matrix and distance d_1 with $C^{\perp}$ a self-orthogonal code of length $2p$ and p independed rows in its generator matrix with distance d_2 we have that $C = C^T$ and so C is in fact self-dual.

Theorem 5 *Let $p+1$ be the order of a skew-Hadamard matrix or a conference matrix. Suppose $p = q^2+q+1$ for some prime power q. Then there exists a self-orthogonal $\mathbb{Z}_k$-code of length $2p$, with m independed rows in its generator matrix and minimum distance d, whenever $p+q \equiv 0(mod\ k)$.*

Proof. Construct the matrices P and Q as in the proof of theorem 3. Set

$$G_3 = \begin{bmatrix} P & Q \\ Q^T & -P^T \end{bmatrix}.$$

We have that

$$G_3G_3^T = \begin{bmatrix} P & Q \\ Q^T & -P^T \end{bmatrix} \begin{bmatrix} P^T & Q \\ Q^T & -P \end{bmatrix} = \begin{bmatrix} PP^T + QQ^T & PQ - QP \\ Q^TP^T - P^TQ^T & Q^TQ + P^TP \end{bmatrix}$$

If $PQ = QP$ (for example, this is true if P is circulant, in which case p is prime) then this matrix generates the required self-orthogonal code of length $2p$ with m independed rows in its generator matrix, as $G_3G_3^T = (q+1)^2 I_m \equiv 0(mod\ k)$.

□

Theorem 6 *Let $p+1$ be the order of a skew-Hadamard matrix or a conference matrix. Suppose $p = q^2+q+1$ for some prime power q. Then there exists a self-dual $\mathbb{Z}_k$-code of length $4p$, with $2p$ independed rows in its generator matrix and minimum distance d, whenever $p+q+a \equiv 0(mod\ k)$ for some $a \in \mathbb{Z}_k$.*

Proof. Construct the matrices P, Q and G_3 as in the proof of theorem 5. Set $G_4 = [I_{2p}\ G_3]$. If $PQ = QP$ (for example, this is true if P is circulant, in which case p is prime) then the matrix G_4 generates the required self-dual code of length $4p$ with $2p$ independed rows in its generator matrix, as $G_4G_4^T = (q+p+a)I_{2p}$.

□

We are able to use the considerable literature on the minimum distance of codes generated by skew-Hadamard matrices, $I+S$, minus its diagonal entries, to obtain lower bounds for the minimum distance of codes with generator matrix $[P\ Q]$, where P and Q are given in the proof of Theorem 3 via the following lemma:

Lemma 1 *Suppose A and B are two matrices of order n with elements from $\mathbb{Z}_k$ and $det(A) \neq 0$. We denote the minimum weights among all linear combinations of their rows (over $\mathbb{Z}_k$) by d_A and d_B respectively. Then the code, C, with generator matrix $[A\ B]$ has minimum Hamming distance $d_C \geq d_A + d_B$.*

Remark 2 There are many pairs (p,q) which satisfy the conditions of Theorem 3. The first few pairs are $(7,2), (13,3), (31,5), (73,8), (91,9)$, $(183,13)$, $(307,17)$, $(757,27), (1723,41)$.

Example 4

1. Let $q=3$, $p=13$, $P = circ(0,1,-1,1,1,-1,-1,-1,-1,1,1,-1,1)$ and $Q = circ(1,1,0,1,0,0,0,0,0,1,0,0,0)$. We consider the matrix $[P\ Q]$ and we remove its first row. Then the derived matrix is the generator matrix of a self-orthogonal $\mathbb{Z}_4$−code of length 26, with 12 independed rows in its generator matrix and minimum distance 8 with weight enumerator

$$\begin{aligned} W(z) &= 1+390z^8+1716z^{10}+40092z^{12}+17056z^{13}+226720z^{14}+ \\ &+422656z^{15}+541593z^{16}+2348320z^{17}+1012440z^{18}+ \\ &+4010240z^{19}+2425436z^{20}+2384096z^{21}+2247648z^{22}+ \\ &+559104z^{23}+472680z^{24}+56160z^{25}+10868z^{26}. \end{aligned}$$

2. Let $q=5$, $p=31$, $P = circ(0,-1,-1,1,-1,-1,1,-1,-1,-1,-1,1,1,1,-1,1,-1,1,-1,-1,-1,1,1,1,1,-1,1,1,-1,1,1)$ and $Q = circ(1,1,0,1,0,0,0,0,1,0,0,0,1,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0)$. We consider the matrix $[P\ Q]$ and we remove its first row. Then the derived matrix is the generator matrix of a self-orthogonal code over $GF(3)$ of length 62, with 30 independed rows in its generator matrix and minimum distance 12. Thus we can obtain a $[62, m, d; 3]$ code for all $m \leq 30$ and with $d(m) \geq 12$ by removing rows. □

References

[1] E. Bannai, S. T. Dougherty, M. Harada, and M. Oura, Type II codes, even unimodular lattices, and invariant rings, *IEEE Trans. Inform. Theory,* 45 (1999), 1194-1204.

[2] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, 1985.

[3] A. Bonnecaze, P. Solé, C. Bachoc and B. Mourrain, Type II codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory,* 43 (1997), 969-976.

[4] C. Charnes, Hadamard matrices, codes over the integers modulo 4 and their Gray images, in Proceedings of SETA'98 C. Ding, T. Helleseth and H. Niederreiter (Eds), *Discrete Mathematics and Theoretical Computer Science,* Springer-Verlag, Berlin, (1999), 171-183.

[5] J. H. Conway and N. J. A. Sloane, Self-dual codes over the integers modulo 4, *J. Combin. Theory Ser. A,* 62 (1993), 30-45.

[6] S. Georgiou and C. Koukouvinos, New self dual codes over $GF(5)$, in *Cryptography and Coding*, M. Walker (Ed.), Lecture Notes in Computer Science-, vol. 1746, Springer-Verlag, Heidelberg, 1999, 63-69.

[7] E. M. Rains and N. J. A. Sloane, Self-dual codes, in *Handbook of Coding Theory,* V. Pless and W. C. Huffman, (Eds.), Amsterdam, Elsevier, 1998.

[8] H. J. Ryser, *Combinatorial Mathematics*, The Carus Mathematical Monographs, No. 14, The Mathematical Association of America, 1965.

[9] J. Seberry, and M. Yamada, Hadamard matrices, sequences and block designs, *Contemporary Design Theory: A Collection of Surveys*, J.Dinitz and D.Stinson, (Eds.) J.Wiley, New York, (1992), 431- 560.

[10] V. Tonchev, Codes, in *CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz (Eds.), CRC Press, Boca Raton, Fla., (1996), 517-543.