On Some Quaternary Self-Orthogonal Codes*

David G. Glynn
School of Mathematical Sciences
The University of Adelaide, SA 5005 Australia
(previously Christchurch, New Zealand (Aotearoa))
Email: dglynn@mac.com, david.glynn@adelaide.edu.au

T. Aaron Gulliver
Department of Electrical & Computer Eng., University of Victoria,
P.O. Box 3055, STN CSC, Victoria, B.C., Canada V8W 3P6
Email: agullive@ece.uvic.ca

Manish K. Gupta
Department of Mathematics & Statistics, Queens University
99 University Ave, Kingston, ON K7L 3N6, Canada
Email: m.k.gupta@ieee.org

Abstract

This paper studies families of self-orthogonal codes over $\mathbb{Z}_4$. We show that the simplex codes (of Type α and Type β) are self-orthogonal. We answer the question of $\mathbb{Z}_4$-linearity for some codes obtained from projective planes of even order. A new family of self-orthogonal codes over $\mathbb{Z}_4$ is constructed via projective planes of odd order. Properties such as self-orthogonality, weight distribution, etc. are studied. Finally, some self-orthogonal codes constructed from twistulant matrices are presented.

*This work was supported by the Marsden fund of the Royal Society of New Zealand. The work of the third author was done when he was at the Department of Mathematics and Statistics, University of Canterbury, Christchurch, New Zealand.

1 Introduction

There has been considerable interest and research into codes over finite rings in recent years. In particular, codes over $\mathbb{Z}_4$ have been widely studied [2, 3, 9, 10, 11, 21, 26]. Self-orthogonal and self-dual codes have received much attention. An excellent survey of self-dual codes is given by Rains and Sloane [25]. In this paper we consider several families of self-orthogonal codes over $\mathbb{Z}_4$ and investigate their properties.

We give a simple characterization of self-orthogonal codes over $\mathbb{Z}_4$ and we show that $\mathbb{Z}_4$-simplex codes of Type α and Type β, namely S_k^α and S_k^β, are self-orthogonal. We also construct families of self-orthogonal and self-dual codes over $\mathbb{Z}_4$ via the projective planes of odd order. Section 2 contains some preliminaries and notation. The relationship between quaternary codes and projective planes is investigated in Section 3, while Section 4 considers projective planes and quantum codes. Finally, Section 5 presents some self-orthogonal codes constructed from twistulant matrices.

2 Preliminaries and Notation

A *linear code* C of length n over $\mathbb{Z}_4$ is an additive subgroup of $\mathbb{Z}_4^n$. An element of C is called a *codeword* and a *generator matrix* is a matrix whose rows generate C. The *Hamming weight* $w_H(x)$ of a vector $x = (x_1, x_2, \ldots, x_n)$ in $\mathbb{Z}_4^n$ is the number of components $x_i \neq 0$. The *Lee weight* $w_L(x)$ of a vector x is $\sum_{i=1}^{n} \min\{|x_i|, |4 - x_i|\}$. The *Euclidean weight* $w_E(x)$ of a vector x is $\sum_{i=1}^{n} \min\{x_i^2, (4 - x_i)^2\}$. The Euclidean weight is useful in connection with lattice constructions. The Hamming, Lee and Euclidean distances $d_H(x, y)$, $d_L(x, y)$ and $d_E(x, y)$ between two vectors x and y are $w_H(x-y)$, $w_L(x-y)$ and $w_E(x - y)$, respectively. The minimum Hamming, Lee and Euclidean weights, d_H, d_L and d_E, of C are the smallest Hamming, Lee and Euclidean weights respectively amongst all non-zero codewords of C.

The *Gray map* $\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ is the coordinate-wise extension of the function from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$ defined by $0 \to (0,0), 1 \to (1,0), 2 \to (1,1), 3 \to (0,1)$. The image $\phi(C)$, of a linear code C over $\mathbb{Z}_4$ of length n by the Gray map, is a (in general non-linear) binary code of length $2n$.

The *dual code* $C^\perp$ of C is defined as $\{x \in \mathbb{Z}_4^n \mid x \cdot y = 0, \forall\, y \in C\}$, where $x \cdot y$ is the standard inner product of x and y. C is *self-orthogonal* if $C \subseteq C^\perp$ and C is *self-dual* if $C = C^\perp$.

If C is a binary code, it is said to be *Type* II, or *doubly-even*, if all of the Hamming weights are divisible by four, and is said to be *Type* I otherwise.

Two codes 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. Codes differing by only a permutation of coordinates are called *permutation-equivalent*.

Any linear code C over $\mathbb{Z}_4$ is permutation-equivalent to a code with generator matrix G of the form

$$G = \begin{pmatrix} I_{k_0} & A & B_1 + 2B_2 \\ 0 & 2I_{k_1} & 2C \end{pmatrix}, \tag{1}$$

where A, B_1, B_2 and C are matrices with entries 0 or 1 and I_k is the identity matrix of order k. One can associate two binary linear codes with C, the *residue code* $C^{(1)} = \{\mathbf{c} \bmod 2 \mid \mathbf{c} \in C\}$ and the *torsion code* $C^{(2)} = \{\mathbf{c} \in \mathbb{Z}_2^n \mid 2\mathbf{c} \in C\}$. If $k_1 = 0$ then $C^{(1)} = C^{(2)}$. For details and further references see [25, 26]. The following theorem gives the relationships between these codes when they are self-orthogonal.

Theorem 1 *[25]*

1. *Let C be a linear self-orthogonal code over $\mathbb{Z}_4$ then its residue code $C^{(1)}$ is a self-orthogonal doubly-even binary code and $C^{(1)} \subseteq C^{(2)} \subseteq C^{(1)^\perp}$. If C is self-dual then $C^{(2)} = C^{(1)^\perp}$.*

2. *If C_A and C_B are binary codes with $C_A \subseteq C_B$ then there is a code C over $\mathbb{Z}_4$ with $C^{(1)} = C_A$ and $C^{(2)} = C_B$. If in addition C_A is self-orthogonal and doubly-even and $C_B \subseteq C_A^\perp$ then there is a self-orthogonal code C over $\mathbb{Z}_4$ with $C^{(1)} = C_A$ and $C^{(2)} = C_B$. Furthermore if $C_B = C_A^\perp$ then C is self-dual.*

A vector $\mathbf{v}$ is a 2-*linear combination* of the vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ if $\mathbf{v} = \lambda_1\mathbf{v}_1 + \ldots + \lambda_k\mathbf{v}_k$ with $\lambda_i \in \mathbb{Z}_2$ for $1 \le i \le k$. A subset $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ of C is called a 2-*basis* for C if

1. for each $i = 1, 2, \ldots, k-1$, $2\mathbf{v}_i$ is a 2−linear combination of $\mathbf{v}_{i+1}, \ldots, \mathbf{v}_k$ and $2\mathbf{v}_k = 0$, and

2. C is the 2-linear span of S and S is 2-linearly independent [3].

The number of elements in a 2-basis for C is called the *2-dimension* of C. It is easy to verify that the rows of the matrix

$$\mathcal{B} = \begin{pmatrix} I_{k_0} & A & B_1 + 2B_2 \\ 2I_{k_0} & 2A & 2B_1 \\ 0 & 2I_{k_1} & 2C \end{pmatrix}, \tag{2}$$

form a 2-basis for the code C generated by G given in (1).

A linear code C over $\mathbb{Z}_4$ (over $\mathbb{Z}_2$) of length n, 2-dimension k, minimum distances d_H, d_L and d_E is called an $[n, k, d_H, d_L, d_E]$ ($[n, k, d_H]$) or simply an $[n, k]$ code. C is called *$\mathbb{Z}_2$-linear* if $\phi(C)$ is a binary linear code. A binary code is said to be *$\mathbb{Z}_4$-linear* if it is equivalent to $\phi(C)$ for some linear code C over $\mathbb{Z}_4$. Necessary and sufficient conditions for $\mathbb{Z}_4$-linearity ($\mathbb{Z}_2$-linearity) are given by the following theorem.

Theorem 2 Hammons et al. *[21]*

1. *A binary linear code D of even length is $\mathbb{Z}_4$-linear if and only if its coordinates can be permuted so that*

$$\mathbf{u}, \mathbf{v} \in D \Rightarrow (\mathbf{u} + \sigma(\mathbf{u})) \star (\mathbf{v} + \sigma(\mathbf{v})) \in D, \tag{3}$$

   where σ is the (symplectic) swap map that interchanges the left and right halves of a vector, and $\star$ denotes the componentwise (or Hadamard) product of two vectors.

2. *For each $a \in \mathbb{Z}_4$, let $\bar{a}$ be the reduction of $a \pmod 2$ and let C be a linear code over $\mathbb{Z}_4$. Then C is $\mathbb{Z}_2$-linear if and only if $\mathbf{c} = (c_1, \ldots, c_n)$ and $\mathbf{c}' = (c_1', \ldots, c_n') \in C$ implies $2\bar{\mathbf{c}} \star \bar{\mathbf{c}}' = (2\bar{c_1}\bar{c_1}', \ldots, 2\bar{c_n}\bar{c_n}') \in C$.*

We now consider the above theorem, and explain the conditions and how they are connected. Recall that ϕ is the Gray map taking coordinates in $\mathbb{Z}_4$ to twice the number of coordinates in $\mathbb{Z}_2$. Thus, Condition 1 tells us when $D = \phi(C)$, given some pairing of the coordinates of D, while Condition 2 is the reverse of this. Both these conditions reduce to the fact that the set of vectors, under the Gray correspondence, are required to be closed under the two kinds of addition: in $\mathbb{Z}_4$ and in $\mathbb{Z}_2$. We can use the Gray map to keep track of which coordinates we are using: e.g. if $\mathbf{c}, \mathbf{c}' \in C$ (the quaternary code), then $\mathbf{c} + \mathbf{c}'$ denotes addition using $\mathbb{Z}_4$, while $\phi(\mathbf{c}) + \phi(\mathbf{c}')$ denotes addition in the binary code.

We can then say that the two conditions are merely two equivalent forms of the statement that the difference between the additions, $\phi(\mathbf{c} + \mathbf{c}') - (\phi(\mathbf{c}) + \phi(\mathbf{c}'))$, is in D, or using the map ϕ^{-1}, in C. Indeed, one can check that additions in C and in D give the same result on a particular position except when the coordinates of $\mathbf{c}$ and of $\mathbf{c}'$ are both units in that position (i.e. 1 or 3). In this case the difference in the $\mathbb{Z}_4$ and $\mathbb{Z}_2$ additions will be the element 2 of Z_4, or the element $\phi(2) = 11$. Now the mapping $\mathbf{u} \mapsto \mathbf{u} + \sigma(\mathbf{u})$ gives the vector of 11's corresponding to the units of $\mathbf{u}$, and the equivalent mapping in the Z_4 vector is $\mathbf{c} \mapsto 2\mathbf{c}$. The Hadamard product is needed because it gives the positions where both elements are units: if a 0 or 2 appears then multiplying by a further 2 gives 0. Finally, we note that for any vector $\mathbf{c}$ over $\mathbb{Z}_4$, the vector $2\mathbf{c} = 2\bar{\mathbf{c}}$, and also $2\bar{\mathbf{c}} \star \bar{\mathbf{c}}' = 2\mathbf{c} \star \mathbf{c}'$, and so the modulo 2 reductions of $\mathbf{c}$ and $\mathbf{c}'$ are not strictly necessary in Condition 2, although we have included it because it was in [21].

Quaternary simplex codes of type α and β have been studied in [3]. A type α simplex code S_k^α is a linear code over $\mathbb{Z}_4$ with parameters

$$[2^{2k}, 2k, 2^{2k-1}, 2^{2k}, 3 \cdot 2^{2k-1}],$$

and an inductive generator matrix given by

$$G_k^\alpha = \left[\begin{array}{c|c|c|c} 0\,0\cdots0 & 1\,1\cdots1 & 2\,2\cdots2 & 3\,3\cdots3 \\ \hline G_{k-1}^\alpha & G_{k-1}^\alpha & G_{k-1}^\alpha & G_{k-1}^\alpha \end{array}\right] \qquad (4)$$

with $G_1^\alpha = [0\ 1\ 2\ 3]$. A type β simplex code S_k^β is a punctured version of S_k^α with parameters $[2^{k-1}(2^k - 1), 2k, 2^{2(k-1)}, 2^{k-1}(2^k - 1), 2^k(3 \cdot 2^{k-2} - 1)]$, and an inductive generator matrix given by

$$G_2^\beta = \left[\begin{array}{c|c|c} 1\,1\,1\,1 & 0 & 2 \\ \hline 0\,1\,2\,3 & 1 & 1 \end{array}\right], \qquad (5)$$

and for $k > 2$

$$G_k^\beta = \left[\begin{array}{c|c|c} 1\,1\cdots1 & 0\,0\cdots0 & 2\,2\cdots2 \\ \hline G_{k-1}^\alpha & G_{k-1}^\beta & G_{k-1}^\beta \end{array}\right], \qquad (6)$$

where G_{k-1}^α is the generator matrix of S_{k-1}^α. For details the reader is referred to [3].

The following lemma gives a simple characterization of the self-orthogonality of codes over $\mathbb{Z}_4$.

Lemma 1 *A linear code C over $\mathbb{Z}_4$ is self-orthogonal if and only if given any generator matrix G of C*

1. *the number of units in each row of G is a multiple of 4 i.e., $\omega_1+\omega_3 \equiv 0 \pmod 4$, and*
2. *all pairs of G are orthogonal.*

Proof. The proof is simple and so is omitted. □

Remark 1 *The above lemma also holds when the generator matrix of the code C is in 2-basis form. One can give the characterization in terms of the Euclidean weights.*

The following theorem follows by induction on k and Lemma 1.

Theorem 3 *The simplex codes S_k^α ($k \geq 2$) and S_k^β ($k \geq 2$) are self-orthogonal.*

2.1 Quasi-Twisted Codes

The class of quasi-twisted (QT) codes was first introduced in [22] as a generalization of quasi-cyclic (QC) codes [17, 18]. A $\mathbb{Z}_4$ code is called quasi-twisted if the same negacyclic[1] shift of a codeword in p groups of size m always results in another codeword. Many QT codes can be constructed from $m \times m$ twistulant matrices (with a suitable permutation of coordinates). In this case, the generator matrix, G, can be represented as

$$G = [B_1, B_2, \ldots, B_p] \tag{7}$$

where the B_i are $m \times m$ *twistulant* matrices of the form

$$B = \begin{bmatrix} b_0 & b_1 & b_2 & \cdots & b_{m-2} & b_{m-1} \\ \eta b_{m-1} & b_0 & b_1 & \cdots & b_{m-3} & b_{m-2} \\ \eta b_{m-2} & \eta b_{m-1} & b_0 & b_{m-4} & \cdots & b_{m-3} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \eta b_1 & \eta b_2 & \eta b_3 & \cdots & \eta b_{m-1} & b_0 \end{bmatrix} \tag{8}$$

and $\eta = 1$ or 3. If $\eta = 1$, the code is QC. It has been shown that QT self-dual codes over $\mathbb{Z}_4$ exist only if $\eta = 3$ [19]. Thus in this paper we only consider this value of η.

[1] A negacyclic shift of an m-tuple $(x_0, x_1, \ldots, x_{m-1})$ is the m-tuple $(\eta x_{m-1}, x_0, \ldots, x_{m-2})$ where η is a unit in $\mathbb{Z}_4$, i.e., $\eta = 1$ or 3.

3 Projective Planes and Quaternary Codes

There have been various constructions of self-dual and self-orthogonal binary codes from projective planes of even order q [25]. These codes were useful in proving the non-existence of a projective plane of order 10. Recently codes over finite rings have been constructed from projective planes [11]. In [15], Glynn constructed binary codes from a projective plane of odd order. Dougherty has generalized this construction to construct self-dual codes over a finite field [8]. In this section, we shall associate a code over $\mathbb{Z}_4$ with any projective plane of odd order. We also consider the $\mathbb{Z}_4$-linearity of the codes obtained from the projective planes of even order.

Let π be a finite projective plane of order q. It is a symmetric $2-\left(q^2+q+1, q+1, 1\right)$ design. Thus, every pair of points is on a unique line and every line contains $q+1$ points. Let $\mathcal{P}$ and $\mathcal{L}$ denote the sets of points and lines, respectively, of π. Then $|\mathcal{P}| = |\mathcal{L}| = q^2+q+1$ and $|\mathcal{P} \cup \mathcal{L}| = 2(q^2+q+1)$.

3.1 Codes over $\mathbb{Z}_4$ from planes of even order

We first investigate the relationships between planes of even order and quaternary codes. If the order of the plane is $q \equiv 2 \pmod 4$, then the line/point[2] incidence matrix of π generates a binary code C_q with parameters $\left[q^2+q+1, \frac{(q^2+q+2)}{2}, q+1\right]$, which can be extended to a Type II binary self-dual code $\hat{C}_q$ if a column of all 1's is adjoined to the incidence matrix. For the other even values of q, when $q \equiv 0 \pmod 4$, the corresponding extended code $\hat{C}_q$ is not necessarily self-dual, but it is certainly self-orthogonal [1].

Example 1 *For $q=2$ this Type II code $\hat{C}_2$ is the $[8,4,4]$ extended Hamming code which is $\mathbb{Z}_4$-linear under the Gray map [21]. The corresponding code over $\mathbb{Z}_4$ is a $[4,4,2,4,4]$ Type α constant Lee weight code generated by the matrix*

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

The seven lines of the plane correspond to codewords of the $\mathbb{Z}_4$-code with a 2 or 3 in the fourth position (except for the word 2222), (see Figure 1). Label

[2]The rows correspond to the lines, and the columns to the points.

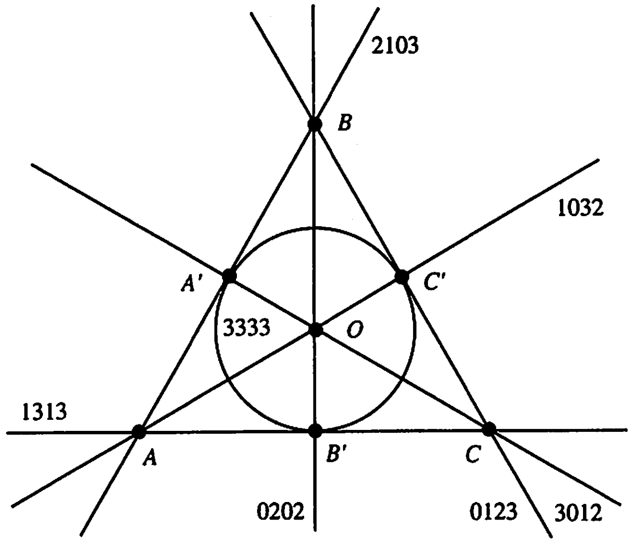

Figure 1: Representation of $PG(2,2)$ over $\mathbb{Z}_4$ with points and lines marked

the points $A, A', B, B', C, C', D, D'$, where $D = O$ and so $D' = O' = \infty$. The correspondence for the seven lines is then

$$
\begin{array}{lcl}
0202 & \leftrightarrow & \{B, B', O, \infty\} \\
0123 & \leftrightarrow & \{B, C, C', \infty\} \\
1032 & \leftrightarrow & \{A, C', O, \infty\} \\
2103 & \leftrightarrow & \{A, A', B, \infty\} \\
3333 & \leftrightarrow & \{A', B', C', \infty\} \\
1313 & \leftrightarrow & \{A, B', C, \infty\} \\
3012 & \leftrightarrow & \{A', C, O, \infty\}.
\end{array}
$$

In addition to $q = 2$ there are also unique (desarguesian) planes of orders $q = 4$ and $q = 8$, and the corresponding extended codes $\hat{C}_4$ and $\hat{C}_8$ have parameters $[22, 10, 6]$ and $[74, 28, 10]$, respectively. The dimensions of the codes are known for various kinds of planes. In particular, any desarguesian plane of even order $q = 2^h$ will give a self-orthogonal extended code $[q^2 + q + 2, 3^h + 1, q + 2]$. Note that the minimal words of weight $q + 2$ will correspond to lines if they contain the extended point ∞. Otherwise, they must be hyperovals of the plane. [3]

Motivated by the above example for $q = 2$, we define a code over $\mathbb{Z}_4$ from a projective plane π with the help of pairings of points in $\mathcal{P}$ as follows. We construct a generator matrix of a code $C(\pi, \mathcal{P}, \mathbb{Z}_4)$ with coordinates corresponding to pairs of points (P, P') in the plane and lines (l) corresponding to rows. The point O is paired with the point at infinity so that $\infty = O'$, and the extended vector corresponding to the lines has a 1 at the coordinate denoted ∞. The value on (P, P') is given by

$$\begin{cases} 0 & \text{if } P \text{ and } P' \notin l \\ 1 & \text{if } P \in l, P' \notin l \\ 2 & \text{if } P \in l, P' \in l \\ 3 & \text{if } P \notin l, P' \in l \end{cases}.$$

Note that each point P is paired with a unique point P' and the code $C(\pi, \mathcal{P}, \mathbb{Z}_4)$ has length $\frac{(q^2+q+2)}{2}$.

At this point the following question arises.

Question 1 *Which planes of order q have a partition into pairs of points such that $\hat{C}_q$ is $\mathbb{Z}_4$-linear, or equivalently, the code $C(\pi, \mathcal{P}, \mathbb{Z}_4)$ is $\mathbb{Z}_2$-linear?*

Remark 2 *We assume now that with the given pairing the inverse of the Gray map ϕ acting on $\hat{C}_q$ is a linear quaternary code $C(\pi, \mathcal{P}, \mathbb{Z}_4)$. Thus $\phi(C(\pi, \mathcal{P}, \mathbb{Z}_4))$ is equal to $\hat{C}_q$. The intention is to use Theorem 2 above to show that this can only happen when $q = 2$. From the discussion after Theorem 2, the question is the same as asking whether there can exist a certain pairing such that the extended code is closed under the two types of additions in $\mathbb{Z}_4$ and $\mathbb{Z}_2$.*

Note that the pairs are ordered, but equivalent codes are obtained by changing the ordering in any of the pairs, and so geometrically they are basically unordered pairs of points, forming a partition of the plane union with infinity.

Here we provide some answers to Question 1, but first present some preliminaries.

Definition 1 *Given a line $l \in \mathcal{L}$ of π let*

$$\gamma(l) := \{P, P' \mid P \in l \text{ and } P' \notin l\} \cup \{P, P' \mid P \notin l \text{ and } P' \in l\}.$$

[3] A hyperoval of a projective plane of even order q is a set of $q + 2$ points, no three collinear.

Note that $\{O, \infty\} \subseteq \gamma(l) \iff 0 \notin l$, because every line contains ∞.

Example 2 *In the case $q = 2$, the seven lines (as codewords) have the correspondence γ with the sets of points as follows:*

$$
\begin{array}{ccccc}
BB'O & \leftrightarrow & 0202 & \leftrightarrow & \emptyset \\
BCC' & \leftrightarrow & 0123 & \leftrightarrow & \{B, B', O, \infty\} \\
AC'O & \leftrightarrow & 1032 & \leftrightarrow & \{A, A', C, C'\} \\
AA'B & \leftrightarrow & 2103 & \leftrightarrow & \{B, B', O, \infty\} \\
A'B'C' & \leftrightarrow & 3333 & \leftrightarrow & \{A, A', B, B', C, C', O, \infty\} \\
AB'C & \leftrightarrow & 1313 & \leftrightarrow & \{A, A', B, B', C, C', O, \infty\} \\
A'CO & \leftrightarrow & 3012 & \leftrightarrow & \{A, A', C, C'\}.
\end{array}
$$

It is clear that the elements of $\gamma(l)$ correspond to the odd entries in the corresponding codeword over $\mathbb{Z}_4$. The above sets also correspond to vectors (or words) in $\mathbb{Z}_2^{q^2+q+2}$ in the natural way.

Using the conditions of Theorem 2 for distinct pairs of generators $C(\pi, \mathcal{P}, \mathbb{Z}_4)$ coming from two lines in $\mathcal{L}$, we obtain the following result.

Lemma 2 *For any two distinct lines l and m of π, the binary characteristic vector of $l{*}m := \gamma(l) \cap \gamma(m)$ is a codeword of $\hat{C}_q$, or equivalently, the function with value 2 on each pair in this set of points is a codeword of $C(\pi, \mathcal{P}, \mathbb{Z}_4)$.*

Now let l be a fixed line not passing through O, and X be any point of l. We consider the sum $S(l, X)$ (in $\hat{C}_q$, or modulo 2), of $l * m$, where m varies over the q lines of π passing through X, but not l. Then in $S(l, X)$ we have $\{0, \infty\}$ repeated $q - 1$ times, which is odd and so is equal to 1 mod 2. Further, every pair in $\gamma(l)$ that is not $(0, \infty)$ occurs precisely once in the sum.

Similarly, we consider any line l through O, and look at the sum $T(l)$ of $l * m$, where m is varied over all q lines through O, but not l. Then the sum modulo 2 is $\gamma(l)$. Hence the same result holds in the case of lines through O. This result can be obtained in a more direct way using Condition 1 of Theorem 2 when $\mathbf{u} = \mathbf{v}$ (because $(\mathbf{u} + \sigma(\mathbf{u})) \star (\mathbf{u} + \sigma(\mathbf{u})) = (\mathbf{u} + \sigma(\mathbf{u}))$.

Since we are assuming that Conditions 1 and 2 hold, and noting that $\hat{C}_q$ is closed under addition, we have shown the following.

Lemma 3 *For all lines $l \in \mathcal{L}$ the word corresponding to $\gamma(l)$ is a word in $\hat{C}_q$.*

Since $\hat{C}_q$ is self-orthogonal each codeword intersects any line (union ∞) in an even number of points. Thus it follows that for any line l not through O, the lines not through O intersect $\gamma^* := \gamma(l) \setminus \{0, \infty\}$ in an odd number of points, while the lines through O intersect it in an even number of points. Similarly, for any line l on O, the set of points $\gamma(l)$ has the property that any line intersects it in an even number of points. These conditions are quite strong and lead to severe restrictions on the types of pairings of the points of the plane that are possible.

Lemma 4 *Suppose now that l is a line of π not through O. Then l can contain at most one pair (P, P').*

This is because if it did contain such a pair, then $P \notin \gamma(l)$, and each of the $q-1$ lines through P, but not l or the line $P.O$, intersects $\gamma^*(l)$ in an odd number of points, i.e. at least one further point. But there are now at most $q-1$ points of $\gamma^*(l)$ not on l, and so there can be no further pairs on l, and also each line through P, or P', contains precisely one of these points of $\gamma^*(l)$.

Next, consider a line l of π containing O, and further, suppose that it contains a point of a pair of $\mathcal{P}$, but not both points of the pair. If that point is P, we consider the $q-1$ lines through P, but not the line PP' or l. Since P is in $\gamma(l)$ we see that each of these $q-1$ lines contains a further point of $\gamma(l)$, but since the number of these further points is bounded by $q-1$, there are no pairs of $\mathcal{P}$ completely contained in l, and $l \setminus \{O\} \subseteq \gamma(l)$. Thus we obtain the following lemma.

Lemma 5 *Any line through O is partitioned by pairs or contains no pairs.*

Note that for any line l on O containing no pairs, $\gamma(l) + l$ is a word of weight $q+2$ containing ∞ of $\hat{C}_q$, implying that the set of points $\{P' \mid P \in l\}$ is another line through O.

From Lemmas 4 and 5 we have the following.

Lemma 6 *There are two types of pairings $\mathcal{P}$ of the plane π that are possible:*

1. *all pairs lie on lines through O, or*

2. *all pairs lie on lines through O, except for two special lines a, b through O, for which the pairs have one point on a, and one point on b.*

Denote these pairings as Type T1 or Type T2, respectively. Considering a Type T1 pairing, we have the following.

Lemma 7 *For each line l not through O, $\gamma(l) = l \cup H(l) \cup \{\infty\}$, where $H(l)$ is a hyperoval containing O, but disjoint from l.*

Proof. $l \cup \{\infty\} \subset \gamma(l)$, but both $l \cup \{\infty\}$ and $\gamma(l)$ are words of $\hat{C}_q$. Thus $\gamma(l) \setminus (l \cup \{\infty\})$ is a word of $\hat{C}_q$ of minimal weight $q+2$, which must be a hyperoval since it doesn't contain ∞. □

Remark 3 *For any line l containing O for a Type T1 pairing, $\gamma(l)$ is the all-zero (or empty) codeword. If we dualize the Type T1 pairing to pairs of lines, we can use a construction of Glynn [16] to get a symmetric Hadamard matrix. In this case there are examples with any translation plane of even order which has a dual hyperoval that contains the translation line. There are connections also to Kantor's work, see [5, 24].*

Notwithstanding the above connections, we can now show that in only the case $q = 2$ can we get a Type T1 pairing that produces a $\mathbb{Z}_4$ code that is also $\mathbb{Z}_2$ linear. Returning to the condition that for any two lines l and m of π, $l * m$ is a word of $\hat{C}_q$, we first choose l to be any line not through O. Then choose m to be any line external to $H(l)$, but not l. This is possible if $q > 2$. Then we see that $l * m$ only contains 4 points: $X := l \cap m$, X', O, and $O' = \infty$. This cannot be a word of $\hat{C}_q$, unless $q = 2$. Similarly, in the case of a Type T2 pairing of points of the plane, we can show that the $\mathbb{Z}_4$ code is $\mathbb{Z}_2$ linear only in the case of $q = 2$. We provide only a brief outline of the proof since it is almost identical to the Type T1 case.

First we show that for all lines l not through O, $\gamma(l)$ is the sum modulo 2 of the line l, a hyperoval containing O, and the point ∞. There are q lines for which the hyperoval is a chord of its corresponding line, and $q^2 - q$ lines for which the hyperoval is external to its line. Now choose a hyperoval for which its line is external. If $q > 2$ there is another line m external to the hyperoval, and so $l * m$ has weight 4 in the $\mathbb{Z}_2$ code which is less than $q + 2$, a contradiction.

It is not known if Type T2 pairings can occur in projective planes of even orders more than 2. However, both types of pairings occur in a projective plane of order 2, so that the corresponding $\mathbb{Z}_4$ code is $\mathbb{Z}_2$ linear.

The main point of the above work is given in Theorem 4.

Theorem 4 *The only case in which the extended self-orthogonal binary code $\hat{C}_q$ is $\mathbb{Z}_4$-linear is when $q = 2$.*

3.2 Codes over $\mathbb{Z}_4$ from planes of odd order

Now we construct a code over $\mathbb{Z}_4$ from a projective plane π of odd order q. Recall that $\mathcal{P}$ and $\mathcal{L}$ denote the sets of points and lines, respectively, of π and $|\mathcal{P} \cup \mathcal{L}| = 2(q^2 + q + 1)$. Let δ be the map taking any point P to the set of lines not through P and let ∂ be the dual mapping taking a line to a set of points not on that line. δ extends to the linear coboundary map that takes any set of points S to the set of lines intersecting S in opposite parity to $|S|$, and ∂ similarly extends to the inverse map from sets of lines to sets of points. Note that $|S| \equiv |\delta S| \pmod 2$. There is a one-to one correspondence between the boolean algebra of all subsets of $\mathcal{P} \cup \mathcal{L}$ and the vector space $\mathbb{F}_2^{2(q^2+q+1)}$ [15]. For any two subsets E and F of $\mathcal{P} \cup \mathcal{L}$, the symmetric difference $E \Delta F$ corresponds to addition $E + F$ in $\mathbb{F}_2^{2(q^2+q+1)}$, and the size of any subset F of $\mathcal{P} \cup \mathcal{L}$ corresponds to the weight of a vector F.

With this correspondence in hand we can define the associated binary codes C_A and C_B. Let C_A be the set of all even sets of points of $\mathcal{P}$ together with the sets of lines that intersect these points an odd number of times. It was shown in [15] that C_A is a binary linear doubly-even self-orthogonal code with parameters $[2(q^2 + q + 1), q^2 + q, 2q + 2]$. Also $C_A^\perp$ is a code with parameters $[2(q^2 + q + 1), q^2 + q + 2, q + 2]$. Another binary code C_B was defined as a union of C_A with one of its cosets $C_A \cup (C_A + \mathcal{P} + \mathcal{L})$. It was shown that C_B is a binary linear self-dual code with parameters $[2(q^2 + q + 1), q^2 + q + 1, 2q]$. Thus, a main property of these codes is the following.

Proposition 1 *[15] $C_A \subset C_B \subset C_A^\perp$.*

In view of this and Condition 2 of Theorem 1, we get the following.

Theorem 5 *Let π be a projective plane of odd order q. Then there exists a self-orthogonal linear code $C_\pi(q)$ over $\mathbb{Z}_4$ with reduction code C_A, torsion code C_B, length $2(q^2 + q + 1)$, 2-dimension $2q^2 + 2q + 1$, and minimum Hamming weight $2q$.*

The remainder of this section considers further properties of the code $C_\pi(q)$. A generator matrix of the code C_B is $G(C_B) = [I_{q^2+q+1} \mid D]$, where

D is the complement of the incidence matrix of the projective plane with i^{th} row d_i for $1 \leq i \leq q^2+q+1$, and I_{q^2+q+1} is the identity matrix of order q^2+q+1. Then by Theorem 5, the generator matrix of the code $C_\pi(q)$ over $\mathbb{Z}_4$ is

$$\left[\begin{array}{cccc|c|c} 1 & 0 & \dots & 0 & 1 & d_1 + d_{q^2+q+1} \\ q+1 & 1 & \dots & 0 & 1 & d_2 + d_{q^2+q+1} \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots \\ q+1 & q+1 & \dots & 1 & 1 & d_{q^2+q} + d_{q^2+q+1} \\ 0 & 0 & \dots & 0 & 2 & 2d_{q^2+q+1} \end{array}\right]. \tag{9}$$

This code is self-orthogonal by construction.

Example 3 *For $q = 1$[4], C_B is a $[6,3,2]$ code with generator matrix $G_B = [I_3|D]$ where D is generated by the cyclic shifts of the vector* (100). *The weight distribution is $A(0) = 1, A(2) = 3, A(4) = 3$, and $A(6) = 1$. The code C_A is a $[6,2,4]$ optimal code with weight distribution $A(0) = 1$, and $A(4) = 3$. The code $C_\pi(1)$ is a $[6,5,2,4,4]$ Type α code with generator matrix*

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

The Hamming, Lee and Euclidean Weight distributions of this code are

i	$A_H(i)$	i	$A_L(i)$	i	$A_E(i)$
0	1	0	1	0	1
2	3	4	11	4	8
4	11	6	8	8	11
5	8	8	11	12	8
6	9	12	1	16	3
				24	1

Example 4 *For $q = 3$, C_B is a $[26,13,6]$ code with generator matrix $G_B = [I_{13}|D]$ where D is generated by the cyclic shifts of the vector* (0010111110111). *The weight distribution is $A(0) = 1, A(6) = 52, A(8) = 390, A(10) = 1313, A(12) = 2340, A(14) = 2340$,*

[4]Technically, there is no projective plane of order $q = 1$, because every line should have at least 3 points, but $q = 1$ denotes here the degenerate plane that is the triangle of 3 points.

$A(16) = 1313, A(18) = 390, A(20) = 52$, and $A(26) = 1$. The doubly-even subcode C_A of C_B is a $[26, 12, 8]$ optimal code with weight distribution $A(0) = 1, A(8) = 390, A(12) = 2340, A(16) = 1313$, and $A(20) = 52$.

$C_\pi(3)$ is a $[26, 25, 6, 8]$ code with generator matrix

$$\left[\begin{array}{c|c|c} 1000000000000 & 1 & 0111000011001 \\ 0100000000000 & 1 & 1100100010101 \\ 0010000000000 & 1 & 1001010010011 \\ 0001000000000 & 1 & 1011101010000 \\ 0000100000000 & 1 & 0010110110001 \\ 0000010000000 & 1 & 1110011000001 \\ 0000001000000 & 1 & 1000001111001 \\ 0000000100000 & 1 & 1011000100101 \\ 0000000010000 & 1 & 1010100001011 \\ 0000000001000 & 1 & 1010010011100 \\ 0000000000100 & 1 & 0010001010111 \\ 0000000000010 & 1 & 1110000110010 \\ 0000000000000 & 2 & 0202222202220 \end{array}\right].$$

The Hamming and Lee weight distributions are given by

i	$A_H(i)$	i	$A_L(i)$
0	1	0	1
6	52	8	312
8	702	12	3172
10	4433	14	29952
12	75660	16	94718
13	29952	18	868608
14	459420	20	1403753
15	868608	22	4722432
16	1085929	24	5477628
17	4642560	26	8353280
18	2009358	28	5477628
19	8087040	30	4722432
20	4868812	32	1403753
21	4722432	34	868608
22	4485000	36	94718
23	1134848	38	29952
24	948480	40	3172
25	109824	44	312
26	21321	52	1

We can modify the above construction to get an equivalent code over $\mathbb{Z}_4$ via a projective plane of odd order in a more natural way. Instead of (9), we take the generator matrix as

$$(10)\qquad \left[\begin{array}{cccc|c|c} 1 & 0 & \dots & 0 & 3 & d_1 + 3d_{q^2+q+1} \\ q+1 & 1 & \dots & 0 & 3 & d_2 + 3d_{q^2+q+1} \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots \\ q+1 & q+1 & \dots & 1 & 3 & d_{q^2+q} + 3d_{q^2+q+1} \\ 0 & 0 & \dots & 0 & 2 & 2d_{q^2+q+1} \end{array}\right].$$

Thus we have the following.

Proposition 2 *The code generated by (10) is a self-orthogonal code over $\mathbb{Z}_4$ for any odd q. Further it can be made into a self-dual code, which we denote by C_π', of length $n = 2(q^2+q+1)$ by deleting the last row and adding the two rows $22\dots2|2|0\dots0$ and $00\dots0|0|2\dots2$.*

Proof. A combination of the first q^2+q rows in (10) is dependent on the last three rows and since the last two rows are independent to the top rows, we delete the last row to yield a self-dual code over $\mathbb{Z}_4$ of length $n = 2(q^2+q+1)$.

□

Remark 4 *For $q = 1$, $C_{\pi}^{'}$ is the unique self-dual code of length 6 over $\mathbb{Z}_4$ [25].*

If $q \equiv 3 \pmod 4$ then the above code can be defined naturally in geometrical language from a projective plane π of odd order q as follows. Let P be a general point of π and δP denote its boundary. Then $C_\pi(q)$ is the set of all codewords $\sum_{P\in\pi} \alpha_P(P+\delta P)$ such that $\sum_{P\in\pi} \alpha_P \equiv 0 \pmod 4$. This can be made into a self-dual code by adding $\sum_{P\in\pi} 2P$ and $\sum_{L\in\pi} 2L$. The construction of the code $C_\pi(q)$ can also be generalized in the following way.

Lemma 8 *Let $G = [A|B]$ be the generator matrix of a self-orthogonal code over $\mathbb{Z}_4$ where the partition of G is compatible with a matrix X such that $XX^t = I$. Then the code generated by $G' = [A|BX]$ will also be a self-orthogonal code over $\mathbb{Z}_4$.*

Proof. It is straightforward to check that the matrix G' satisfies the required property.

□

Remark 5 *In Lemma 8, if we substitute $G = (10\cdots01)(10\cdots03)$, where the parenthesis denotes that all the cyclic shifts are taken, and $X = D$ is the complement of the incidence matrix of the projective plane, then we obtain $C_\pi(q)$. Note that*

$$DD^t = \begin{cases} 2J - I & \text{if } q \equiv 3 \pmod 4 \\ I & \text{if } q \equiv 1 \pmod 4 \end{cases}.$$

Similar results have been investigated recently in [12]. The next result shows that the code $C_\pi(q)$ is not $\mathbb{Z}_2$-linear i.e, its image under the Gray map is a non-linear binary code.

Theorem 6 *The Gray image of $C_\pi(q)$ is a $\left(4(q^2+q+1), 2^{2q^2+2q+1}, 2q+2\right)$ binary non-linear code.*

Proof. The result follows from Theorem 2. Let **u** and **v** be the first two rows of (9). If $\bar{x}$ denotes reduction modulo 2 of x, and $\star$ denotes component-wise multiplication, then $2\bar{\mathbf{u}}\star\bar{\mathbf{v}}$ is a vector of weight $q+1$. Since there is no vector of weight $q+1$ in C_B this vector does not belong to $C_\pi(q)$. □

4 Projective Planes and Quantum Codes

Any binary self-orthogonal code gives rise to a "binary" (a special class of "additive") quantum code via the CSS construction [7]. Thus the binary self-orthogonal codes from projective planes of odd order given in Section 3 will also provide classes of quantum codes. In this section, we list the parameters of such quantum codes. The necessary theorem is the following. See also [6].

Theorem 7 *Let C be an $[n,k,d]$ binary self-orthogonal code with dual $C^\perp$ having parameters $[n,n-k,d^\perp]$. Let $\{\mathbf{w_j} : 1 \le j \le 2^{n-2k}\}$ be a system of representatives of the cosets $C^\perp/C$. Then the 2^{n-2k} mutually orthogonal states*

$$|\psi_j\rangle = \frac{1}{\sqrt{|C|}}\sum_{\mathbf{c}\in C}|\mathbf{c}+w_j\rangle,$$

span a "binary" quantum code with parameters $[[n,n-2k]]$ of length n and dimension 2^{n-2k} and minimum weight d', where

$$d' = \min\left\{wt(\mathbf{c}) \mid \mathbf{c} \in C^\perp/C\right\} \ge d^\perp.$$

(If $k=0$ then $d'=d=d^\perp$.)

Applying the above theorem to code C_A will yield a $\left[[2(q^2+q+1), 2, q+2]\right]$ quantum code. This code encodes 2 qubits into $2(q^2+q+1)$ qubits. If we apply the above theorem to the code C_B we obtain a quantum code with parameters $\left[[2(q^2+q+1), 0, 2q]\right]$.

If $q \equiv 1 \pmod 4$, the binary self-dual code C_B can be extended to a unique doubly-even self-dual code C_D with parameters $\left[2(q^2+q+2), q^2+q+2, q+3\right]$ [15].

Applying the above theorem to C_D yields a binary (self-dual) quantum code with parameters $[[2(q^2+q+2),0,q+3]]$. If we compare it with the existing Tables [6], one finds that for $q=1$ we get an optimal quantum code.

If $q \equiv 3 \pmod 4$, the binary self-dual code C_B can be extended to a doubly-even self-dual code C_E with parameters $[2(q^2+q+4), q^2+q+4, 4]$ [15]. Applying the above theorem to C_E yields a binary (self-dual) quantum code with parameters $[[2(q^2+q+4),0,4]]$.

5 Self-Orthogonal Quasi-Twisted Codes

In this section, we present the results of a search for best self-orthogonal quasi-twisted codes. Because the Gray map connects the Lee weights of a $\mathbb{Z}_4$ code with the Hamming weights of a $\mathbb{Z}_2$ code, we consider here only best Lee weight codes. This search employed a stochastic optimization algorithm, tabu search [13, 14, 20]. This method has been shown to produce optimal or near-optimal solutions to difficult optimization problems with a reasonable amount of computational effort. For an extensive survey of optimization methods in coding theory, with an emphasis on stochastic procedures, see [23].

Tabu search is based on local search, which means that starting from an arbitrary initial solution, a series of solutions is obtained so that every new solution only differs slightly from the previous one. A potential new solution is called a *neighbor* of the old solution, and all neighbors of a given solution constitute the *neighborhood* of that solution. To evaluate the quality of solutions, a *cost function* is needed. Tabu search always proceeds to a best possible solution in the neighborhood of the current solution.

To ensure that the search does not loop on a subset of solutions, recent solutions are stored in a tabu list, and these are then not allowed for a certain period of time.

The search criterion used here was the minimum weight, and the cost function was chosen so as to maximize this weight, with the added condition that the resulting code be self-orthogonal. It was found that it is best to first find a code with a specified even minimum distance, then check for orthogonality.

Table 1 presents the minimum weights of the best codes obtained. Note that it was shown in [19] that self-dual QT codes exist only for lengths a multiple of 8 (m a multiple of 4). The first rows of the twistulant matrices of the QT codes listed in Table 1 are compiled in Tables 2 - 5. Since this is the first compiled table of $\mathbb{Z}_4$ codes (self-orthogonal or otherwise), it is not possible to compare these codes with previous results. However, using the Gray map, it is possible to compare these codes with the best binary linear codes [4] with even minimum distance. Of the 111 entries in Table 1, 54 or almost half attain the best known distance for the corresponding binary code. Hence it can be said that the class of self-orthogonal QT codes contains many good codes.

Acknowledgement. The authors would like to thank William M. Kantor for his useful communication [24].

References

[1] E. F. Assumus and J. D. Key, **Designs and Their Codes**, Cambridge University Press, 1992.

[2] 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), 1194–1205.

[3] M. C. Bhandari, M. K. Gupta and A. K. Lal *On $\mathbb{Z}_4$ simplex codes and their gray images.* Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-13, Lecture Notes in Computer Science **1719** (1999), 170–180.

[4] A.E. Brouwer, *Bounds on the size of linear codes* in V. S. Pless and W. C. Huffman (Eds.), **Handbook of Coding Theory**, North-Holland, New York, 1998.

[5] A. R. Calderbank, P. J. Cameron, W. M. Kantor and J. J. Seidel, $\mathbb{Z}_4$-*Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets.* Proc. Lond. Math. Soc. **75**, (1997) pp. 436–480.

[6] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane. *Quantum error correction via codes over $GF(4)$*. IEEE Trans. Inform. Theory **44**, (1998) pp. 1369-1387.

[7] A. R. Calderbank and P. Shor, *Good quantum error correcting codes exist.* Phys. Rev. A, **54** (1996), 1098–1105.

[8] S. T. Dougherty, *A new construction of self-dual codes from projective planes.* Australas. J. Combin. **31**, (2005), 337–348.

[9] S. T. Dougherty, T. A. Gulliver and M. Harada, *Type II codes over finite rings and even unimodular lattices.* J. Alg. Combin., **9** (1999), 233–250.

[10] S. T. Dougherty, M. Harada and P. Solé, *Shadow codes over* $\mathbb{Z}_4$. Finite Fields and Their Appl., **7**, No. 4, (2001), 507–529.

[11] S. T. Dougherty, M. Harada and P. Solé, *Self-dual codes over rings and the chinese remainder theorem.* Hokkaido Math. J., **28** (1999), 253–283.

[12] S. Georgiou, C. Koukouvinos. and J. Seberry, *Some results on self-orthogonal and self-dual codes.* Ars. Comb., **68** (2003) 97–104.

[13] F. Glover, *Tabu search—Part I.* ORSA J. Comput. **1** (1989) 190–206.

[14] F. Glover and M. Laguna, *Tabu Search.* Boston, MA: Kluwer, 1997.

[15] D. G. Glynn, *The construction of self-dual binary codes from projective planes of odd order.* Australas. J. Combin., **4** (1991), 277–284.

[16] D. G. Glynn, *Finite projective planes and related combinatorial systems.* **PhD Thesis**, Department of Mathematics, University of Adelaide, Australia. (1978)

[17] T.A. Gulliver and V.K. Bhargava, *Some best rate* $1/p$ *and rate* $(p-1)/p$ *systematic quasi-cyclic codes.* IEEE Trans. Inform. Theory, **37** (1991) 552–555.

[18] T.A. Gulliver and V.K. Bhargava, *Some best rate* $1/p$ *and* $(p-1)/p$ *quasi-cyclic codes over GF(3) and GF(4).* IEEE Trans. Inform. Theory, **38** (1992) 1369–1374.

[19] T.A. Gulliver and M. Harada, *Optimal double circulant* $\mathbb{Z}_4$*-codes.* Springer-Verlag Lecture Notes in Computer Science, **2227** (2001) 122–128.

[20] T.A. Gulliver and P.R.J. Östergård, *Improvements to the bounds on ternary linear codes of dimension 8 using tabu search. J. Heuristics* **7** (2001) 37–46.

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

[22] R. Hill and P.P. Greenough, *Optimal quasi-twisted codes.* Proc. *Int. Workshop Algebraic and Comb. Coding Theory*, Voneshta Voda, Bulgaria, (1992) 92–97.

[23] I.S. Honkala and P.R.J. Östergård, *Applications in code design* in *Local Search in Combinatorial Optimization*, E. Aarts and J.K. Lenstra, Eds., New York, NY: Wiley, 1997.

[24] W. M. Kantor, Personal communication, 4 March 2002.

[25] E. M. Rains and N. J. A. Sloane. *Self-Dual Codes* in V. Pless and W.C. Huffman (Eds.) **The Handbook of Coding Theory**. North-Holland, New York, 1998.

[26] Z. Wan. **Quaternary Codes**. World Scientific, Singapore, 1997.

Table 1: Maximum Minimum Lee Distances for Best Self-Orthogonal (pm, m) QC Codes over $\mathbb{Z}_4$

	p																
m	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	–	4	8	8	12	14	16	16	20	22	24	26	28	32	32	34	36
3	–	–	8	14	16	18	22	24	28	30	34	38	40	44	48	50	52
4	4	8	12	16	22	24	28	32	36	40	44	48	54	56	60	64	70
5	–	–	16	20	24	30	34	40	44	48	54	58	64	68	74	78	84
6	–	12	16	22	28	34	40	44	50	56	60	66	72	80	86	90	96
7	–	–	18	24	32	38	44	48	56	62	68	76	82	88	94	102	110
8	8	14	22	26	34	40	46	54	62	68	78	86	92	100	104	114	122

Table 2: First Rows of the Best Quaternary Self-Orthogonal QT Codes $m = 2, 3$

code	m	d	$b_i(x)$
(6,2)	2	4	1, 1, 13
(8,2)	2	8	1, 2, 12, 13
(10,2)	2	8	12, 2, 13, 2, 12
(12,2)	2	12	1, 13, 12, 12, 1, 11
(14,2)	2	14	12, 13, 1, 1, 12, 2, 11
(16,2)	2	16	1, 13, 1, 1, 12, 2, 12, 12
(18,2)	2	16	11, 1, 1, 1, 22, 13, 2, 22, 12
(20,2)	2	20	1, 1, 1, 12, 2, 12, 13, 12, 11, 11
(22,2)	2	22	1, 11, 13, 12, 12, 12, 1, 2, 2, 1, 11
(24,2)	2	24	11, 12, 1, 1, 1, 1, 12, 13, 22, 2, 2, 13
(26,2)	2	26	12, 1, 1, 1, 1, 11, 12, 12, 12, 11, 13, 2, 13
(28,2)	2	28	11, 1, 1, 12, 13, 13, 1, 22, 12, 12, 12, 12, 2, 11
(30,2)	2	30	12, 12, 12, 1, 1, 1, 1, 13, 13, 12, 2, 13, 2, 2, 11
(32,2)	2	32	11, 1, 1, 1, 1, 1, 11, 11, 13, 22, 12, 2, 2, 2, 12, 12
(34,2)	2	34	1, 1, 1, 1, 1, 12, 13, 11, 12, 11, 2, 12, 11, 12, 12, 2, 13
(36,2)	2	36	12, 12, 1, 1, 1, 1, 1, 1, 2, 12, 11, 11, 2, 13, 13, 11, 12, 22
(12,3)	3	8	1, 122, 21, 12
(15,3)	3	14	1, 122, 11, 12, 113
(18,3)	3	16	122, 123, 123, 113, 111, 122
(21,3)	3	18	1, 112, 123, 13, 122, 12, 111
(24,3)	3	22	1, 1, 113, 123, 112, 11, 112, 113
(27,3)	3	24	12, 111, 1, 1, 123, 112, 123, 11, 13
(30,3)	3	28	1, 1, 113, 11, 113, 122, 12, 11, 122, 12
(33,3)	3	30	12, 12, 12, 1, 11, 122, 11, 11, 113, 113, 111
(36,3)	3	34	1, 111, 123, 113, 1, 12, 122, 13, 12, 13, 11, 122
(39,3)	3	38	1, 123, 1, 11, 21, 123, 13, 12, 113, 111, 122, 2, 122
(42,3)	3	40	1, 21, 123, 12, 1, 12, 22, 21, 112, 2, 111, 11, 112, 113
(45,3)	3	44	122, 12, 21, 1, 1, 112, 11, 122, 11, 112, 113, 123, 2, 13, 113
(48,3)	3	48	112, 123, 112, 12, 1, 11, 21, 13, 111, 11, 21, 122, 12, 22, 113, 2
(51,3)	3	50	11, 12, 1, 12, 21, 112, 113, 12, 122, 13, 1, 122, 111, 113, 11, 21, 123
(54,3)	3	52	112, 1, 112, 111, 123, 113, 21, 21, 123, 12, 113, 12, 13, 11, 113, 122, 122, 122

Table 3: First Rows of the Best Quaternary Self-Orthogonal QT Codes $m = 4, 5$

code	m	d	$b_i(x)$
(8,4)	4	4	1, 133
(12,4)	4	8	1132, 123, 1213
(16,4)	4	12	112, 113, 102, 11
(20,4)	4	16	123, 122, 13, 11, 12
(24,4)	4	22	1132, 131, 122, 112, 1222, 1122
(28,4)	4	24	102, 111, 1, 12, 11, 1232, 1223
(32,4)	4	28	1223, 113, 121, 11, 133, 102, 1113, 1123
(36,4)	4	32	132, 11, 111, 133, 211, 122, 112, 202, 1222
(40,4)	4	36	122, 1113, 1, 1222, 211, 121, 111, 132, 113, 221
(44,4)	4	40	133, 212, 11, 1, 101, 112, 121, 123, 1112, 122, 221
(48,4)	4	44	211, 121, 1123, 122, 132, 113, 1222, 212, 131, 131, 123, 1
(52,4)	4	48	212, 12, 1232, 13, 131, 1212, 11, 221, 1132, 133, 1222, 1112, 22
(56,4)	4	54	113, 133, 1, 102, 131, 221, 1112, 1132, 122, 1213, 11, 21, 1222, 211
(60,4)	4	56	133, 102, 131, 1213, 1, 22, 1222, 21, 113, 132, 213, 1122, 211, 112, 1223
(64,4)	4	60	1113, 132, 1, 122, 111, 21, 133, 1222, 1112, 123, 102, 1, 12, 213, 1123, 1132
(68,4)	4	64	1113, 111; 12, 111, 2, 133, 1, 102, 123, 1223, 222, 1222, 121, 1132, 112, 132, 1223
(72,4)	4	70	1132, 1, 1222, 11, 1213, 221, 133, 122, 1112, 213, 212, 12, 1223, 1122, 1123, 211, 131, 112
(20,5)	5	16	1121, 2133, 11122, 1011
(25,5)	5	20	11, 133, 111, 1202, 11212
(30,5)	5	24	1113, 133, 131, 122, 1112, 11222
(35,5)	5	30	1021, 2221, 1321, 131, 1123, 11233, 1331
(40,5)	5	34	2212, 1323, 11112, 1223, 1122, 1232, 133, 12123
(45,5)	5	40	11312, 12223, 133, 1331, 1031, 1032, 1133, 11212, 2111
(50,5)	5	44	132, 11322, 1022, 1132, 1031, 1, 213, 1033, 2111, 11223
(55,5)	5	48	11113, 11112, 2021, 1202, 1132, 131, 1033, 122, 1322, 1031, 1102
(60,5)	5	54	11313, 11, 12, 2221, 101, 2021, 1211, 12122, 1221, 131, 111, 1123
(65,5)	5	58	2211, 1323, 211, 1132, 2122, 11322, 1311. 1123, 12223, 11223, 1202, 1212, 1332
(70,5)	5	64	1122, 1031, 111, 2132, 2112, 12223, 12222, 122, 21, 1111, 113, 12, 12313, 12123
(75,5)	5	68	2131, 132, 11, 1132, 2123, 201, 11223, 1011, 1033, 123, 11222, 12, 1131, 12122, 12213
(80,5)	5	74	11122, 1022, 12122, 1132, 1122, 12223, 11112, 12222, 12132, 1032, 1323, 11232, 2211, 1333, 11313, 12313
(85,5)	5	78	113, 201, 11223, 1031, 122, 1022, 1331, 21, 12222, 1302, 133, 11112, 11132, 11212, 1321, 2213, 2221
(90,5)	5	84	1211, 11313, 2221, 1132, 1221, 1323, 1, 2112, 11123, 12213, 1121, 211, 101, 12, 221, 131, 2212, 11112

Table 4: First Rows of the Best Quaternary Self-Orthogonal QT Codes $m = 6, 7$

code	m	d	$b_i(x)$
(18,6)	6	12	21, 111, 11321
(24,6)	6	16	21, 21313, 22213, 12
(30,6)	6	22	10323, 1333, 1, 102, 112122
(36,6)	6	28	1203, 121223, 112, 10321, 1, 13311
(42,6)	6	34	1131, 13333, 12333, 13022, 1323, 10112, 13302
(48,6)	6	40	20212, 12113, 1011, 1113, 21212, 1031, 13321, 1303
(54,6)	6	44	11212, 1301, 101, 2221, 20211, 11222, 11033, 1031, 11312
(60,6)	6	50	22113, 12, 13022, 2111, 10131, 21213, 121313, 13202, 10122, 1301
(66,6)	6	56	10213, 12022, 1223, 10121, 21133, 1031, 22211, 13111, 11013, 12211, 2013
(72,6)	6	60	111222, 11111, 1323, 12, 112322, 10121, 12322, 122232, 13, 112313, 22122, 13022
(78,6)	6	66	21113, 112223, 1, 201, 1101, 11322, 112323, 11031, 213, 21211, 1122, 121222, 13132
(84,6)	6	72	2, 1, 13, 112, 10213, 122232, 112233, 22111, 12012, 112133, 1131, 1213, 2103, 12121
(96,6)	6	86	2122, 2101, 2011, 10123, 10213, 112132, 21311, 12312, 21312, 121213, 1212, 113132, 122, 21221, 12313, 11131
(102,6)	6	90	213, 21313, 1, 10311, 12223, 122123, 21222, 21333, 22211, 10223, 1303, 13022, 10103, 1133, 11111, 2113, 133
(108,6)	6	96	12231, 11112, 2121, 133, 1, 113223, 21321, 12, 11131, 10211, 1332, 22113, 1002, 111332, 111313, 12312, 1303, 13221
(28,7)	7	18	12, 1123132, 13111, 103311
(35,7)	7	24	12122, 20111, 1, 1113111, 21033
(42,7)	7	32	1213, 2102, 113313, 111113, 210222, 10112
(49,7)	7	38	131132, 113032, 101312, 1231231, 1122122, 213133, 21212
(56,7)	7	44	211, 1212122, 113012, 210213, 1301, 1213212, 1132, 20123
(63,7)	7	48	102, 102212, 123231, 221123, 221222, 112213, 212113, 1123212, 123111
(70,7)	7	56	21112, 1, 113122, 1113131, 1011, 11212, 21012, 121131, 133211, 10121
(77,7)	7	62	21031, 10133, 20221, 12023, 22102, 1213, 101233, 1303, 133132, 11131, 102202
(84,7)	7	68	101021, 11, 122213, 202021, 1132312, 1131221, 130221, 11022, 1131321, 113132, 102133, 1022
(91,7)	7	76	10023, 213233, 13, 122202, 213211, 12022, 13122, 212231, 12103, 123212, 131133, 1123132, 202111
(98,7)	7	82	12132, 121312, 122313, 110131, 1113231, 1131221, 111213, 132212, 2132, 1132322, 112032, 1301, 121133, 1122211
(105,7)	7	88	13232, 211121, 131231, 13023, 1222312, 123222, 132113, 101201, 21103, 202112, 1112122, 110222, 222123, 12031, 103231
(112,7)	7	94	113, 1113, 10122, 123022, 112233, 111211, 13221, 21303, 102233, 10331 2, 1132132, 202222, 1111211, 12, 131133, 21
(119,7)	7	102	101333, 11223, 123, 13132, 112232, 10111, 120121, 1112222, 12211, 1213122, 13112, 1132131, 131323, 101322, 1111312, 132, 123233 321, 231311
(126,7)	7	110	103322, 11112, 111233, 2013, 101102, 1222, 1212221, 21132, 111012, 13022, 1323, 113133, 102012, 11231, 1232, 110122, 12201, 10133 12201, 20211

Table 5: First Rows of the Best Quaternary Self-Orthogonal QT Codes $m = 8$

code	m	d	$b_i(x)$
(16,8)	8	8	111, 1323123
(24,8)	8	14	12103, 11031, 213113
(32,8)	8	22	1121211, 1310231, 103021, 100213
(40,8)	8	26	12, 1, 2211212, 1313221, 11321312
(48,8)	8	34	221, 13333, 1201313, 1022311, 1323112, 210113
(56,8)	8	40	10231, 120132, 120301, 1102022, 110211, 1223222, 2021121
(64,8)	8	46	133, 1221023, 1111032, 202132, 213, 1311102, 1110122, 1223323
(72,8)	8	54	112, 101123, 110221, 1113122, 1111332, 1230232, 1311021, 13212, 1132323
(80,8)	8	62	121012, 1, 21312, 1033122, 221311, 11111212, 1133323, 11221221, 1012132, 1232331
(88,8)	8	68	1011, 11013, 1211023, 122031, 1131332, 1122231, 110233, 122022, 1103112, 121102, 12122212
(96,8)	8	78	132223, 1210223, 1012332, 130302, 10223, 12233, 103111, 1012333, 1023133, 201212, 1103232, 1312231
(104,8)	8	86	131111, 1212202, 102002, 212, 1302112, 123211, 132201, 1013322, 132032, 100231, 111311, 10112, 2021331
(112,8)	8	92	1020131, 12, 1122012, 2111213, 1133322, 2221332, 112302, 1222331, 1103121, 2211123, 202213, 132322, 1111333, 13212
(120,8)	8	100	10223, 11122131, 1221013, 11221312, 112102, 1113313, 2111, 1321112, 123332, 1321211, 12, 102303, 121333, 1101302, 210123
(128,8)	8	104	1233, 1213, 102002, 222221, 201232, 132301, 11322321, 1333321, 2123231, 1032312, 113212, 1330231, 2132221, 1332332 1112031, 1333322
(136,8)	8	114	1113102, 1012113, 1111311, 1101121, 2122211, 1203113, 1033131, 2111, 132032, 1212313, 1031323, 2113022, 211102, 130311 1223102, 1231031, 131231
(144,8)	8	122	2212131, 101232, 123, 110233, 12222221, 103012, 12203, 2102322, 103013, 1311232, 12222321, 1112023, 11232122, 1230221 11312311, 2131022, 113321, 1021132