# Some Good Cyclic and Quasi-Twisted $\mathbb{Z}_4$-Linear Codes

Nuh Aydin
Department of Mathematics, Kenyon College
Gambier, OH 43022
E-mail: aydinn@kenyon.edu

T. Aaron Gulliver
Department of Electrical and Computer Engineering,
University of Victoria, Victoria, BC Canada V8W 3P6
E-mail: agullive@ece.uvic.ca

**Abstract**

For over a decade, there has been considerable research on codes over $\mathbb{Z}_4$ and other rings. In spite of this, no tables or databases exist for codes over $\mathbb{Z}_4$, as is the case with codes over finite fields. The purpose of this work is to contribute to the creation of such a database. We consider cyclic, negacyclic and quasi-twisted (QT) codes over $\mathbb{Z}_4$. Some of these codes have binary images with better parameters than the best-known binary linear codes. We call such codes "good codes". Among these are two codes which improve the bounds on the best-known binary non-linear codes. Tables of best cyclic and QT codes over $\mathbb{Z}_4$ are presented.

**Keywords:** Codes over $\mathbb{Z}_4$, cyclic codes, quasi-cyclic codes, best-known codes.

## 1 Introduction

The study of linear codes over finite fields has provided many useful results in coding theory. After the discovery of good binary non-linear codes from codes over $\mathbb{Z}_4$, the ring of integers modulo 4, [24], [29], [30], there has been significant investigation into this class of codes. Despite this extensive research, there have been few new binary codes discovered by this approach. A solitary example is the new binary non-linear code given in [7] obtained from an extended cyclic code over $\mathbb{Z}_4$.

To date, much of the research attention has focussed on self-orthogonal and self-dual codes over $\mathbb{Z}_4$. Self-dual codes over $\mathbb{Z}_4$ of length up to 9 are classified in [8], and this is extended to length 15 in [12] (16 for Type II codes in [31]). Rains has classified optimal self-dual codes over $\mathbb{Z}_4$ in [33]. A large number of self-orthogonal quasi-twisted (QT) $\mathbb{Z}_4$ codes have also been constructed [15]. An excellent survey of self-dual codes is given by Rains and Sloane [34].

It is well known that the class of QT codes (which includes quasi-cyclic (QC) codes), contains many good codes. A very large number of new linear codes over finite fields have been discovered within these two classes [1], [9], [10], [17], [18], [19], [20], [21], [22], [37]. There exist tables/databases of best-known codes over small fields available online [6][1] and [16]. The computer algebra system MAGMA [5] has such a database too. A table of best-known binary non-linear codes is also available [27].

QC and QT codes over $\mathbb{Z}_4$ were first studied in [2] and a number of binary codes with parameters better than comparable linear codes were obtained via the standard Gray map. The binary image of one of the codes in [2] gives a new non-linear binary code, which has parameters $(92, 2^{34}, 28)$. We would like to remark that the table [27] is not as comprehensive as the tables for linear codes over fields; it does not go beyond minimum distance 29. Many of the binary images of $\mathbb{Z}_4$ linear codes are non-linear, and it is often not possible to compare such a code with a best-known non-linear binary code. In these cases, one can do the next best thing: compare the parameters with a best-known binary linear code. It should also be noted that although the Gray images of $\mathbb{Z}_4$-linear codes are not necessarily binary-linear, they are still distance invariant, a property that linear codes possess but arbitrary non-linear codes do not (necessarily).

This work begins the development of a database of best-known linear codes over $\mathbb{Z}_4$. In the light of the results of previous investigations over fields and $\mathbb{Z}_4$, our approach begins with cyclic and QT codes. We have investigated cyclic codes over $\mathbb{Z}_4$ and obtained a table of best-known cyclic codes (up to certain lengths and dimensions). This includes a number of codes that have better parameters than comparable binary linear codes. We call such codes "good codes". Of these, two lead to improvements in the distance bounds on binary non-linear codes in [27]. We have also searched for good QT codes over $\mathbb{Z}_4$ and

[1]After the submission of this manuscript, it was announced that this online database is discontinued due to the existence of [16] which has more explicit information on constructions

discovered a number of such codes.

## 2 Preliminaries

A *code* $C$ of length $n$ over $\mathbb{Z}_4$ is a subset of $\mathbb{Z}_4^n$. $C$ is a *linear code* over $\mathbb{Z}_4$ if it is an additive subgroup of $\mathbb{Z}_4^n$, hence a submodule of $\mathbb{Z}_4^n$. We represent the elements of $\mathbb{Z}_4$ by $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. In this paper we will consider only linear codes over $\mathbb{Z}_4$. 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 Hamming and Lee distances $d_H(x, y)$ and $d_L(x, y)$ between two vectors $x$ and $y$ are $w_H(x - y)$ and $w_L(x - y)$, respectively. The minimum Hamming and Lee weights, $d_H$ and $d_L$, of $C$ are the smallest Hamming and Lee 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 Gray map is an isometry from $(\mathbb{Z}_4^n, w_L)$ to $(\mathbb{Z}_2^{2n}, w_H)$. Therefore, the minimum Hamming weight of $\phi(C)$ is equal to the minimum Lee weight of $C$.

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 $C = C^\perp$.

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

$$G = \begin{bmatrix} I_{k_1} & A_1 & B_1 + 2B_2 \\ 0 & 2I_{k_2} & 2A_2 \end{bmatrix}, \tag{1}$$

where $A_1, A_2, B_1$, and $B_2$ are matrices with entries 0 or 1 and $I_k$ is the identity matrix of order $k$. Such a code has size $4^{k_1}2^{k_2}$. The code is a free module if and only if $k_2 = 0$. If $C$ has length $n$ and minimum Lee weight $d_L$, the code is referred to as an $[n, 4^{k_1}2^{k_2}, d_L]$-code.

The minimum weights of optimal linear $\mathbb{Z}_4$ codes up to length $n = 7$ are given in [11], and rate 1/2 codes over $\mathbb{Z}_4$ up to length $n = 8$ have been classified in [23].

# 3 The Structure of Cyclic Codes over $\mathbb{Z}_4$

## 3.1 Cyclic and Negacyclic Codes of Odd Length

A cyclic (negacyclic) code over $\mathbb{Z}_4$ is a $\mathbb{Z}_4$-linear code which is invariant under cyclic (negacyclic)[2] shifts. Similar to the case of finite fields, cyclic (negacyclic) codes over $\mathbb{Z}_4$ of length $n$ are ideals in the ring $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$ $\left(\frac{\mathbb{Z}_4[x]}{\langle x^n+1\rangle}\right)$, under the usual identification of vectors with polynomials. Although algebraically cyclic (negacyclic) codes have the same structure over fields and over $\mathbb{Z}_4$ (ideals in a factor ring), the fact that $\mathbb{Z}_4[x]$ is not a unique factorization domain makes it more challenging to find all cyclic codes over $\mathbb{Z}_4$. For instance, computer algebra systems (such as Magma and Maple), cannot provide factorizations of $x^n - 1$ or $x^n + 1$. There are some theoretical results to help with the search, but we do not have complete answers in all cases. One needs to use theoretical results to facilitate practical implementation of computer searches. Therefore, it is appropriate to recall relevant results from the literature on cyclic and negacyclic codes in this section. The easiest case to consider is cyclic codes of odd length over $\mathbb{Z}_4$. Some of the most important facts about ideals of the relevant ring and the factorization of $x^n - 1$ are summarized below, and they can be found in [32], [38] or [39].

For an odd positive integer $n$, $x^n - 1$ can be factored into a product of finitely many pairwise coprime basic irreducible polynomials over $\mathbb{Z}_4$. Also, this factorization is unique up to ordering of the factors [32, 39]. In fact, we have the following: if $f_2(x)|(x^n - 1)$ in $\mathbb{Z}_2[x]$ then there is a unique, monic polynomial $f(x) \in \mathbb{Z}_4[x]$ such that $f(x)|(x^n - 1)$ in $\mathbb{Z}_4[x]$ and $\overline{f(x)} = f_2(x)$, where $\overline{f(x)}$ denotes the reduction of $f(x)$ modulo 2 [39]. The polynomial $f(x)$ is called the Hensel lift of $f_2(x)$. There are well-known methods of finding this polynomial, such as Graeffe's method [24]. Therefore, there is a one-to-one correspondence between irreducible factors of $x^n - 1$ over $\mathbb{Z}_2$ and irreducible factors of $x^n - 1$ over $\mathbb{Z}_4$.

[2] A negacyclic shift of an $m$-tuple $(x_0, x_1, \ldots, x_{m-1})$ over $\mathbb{Z}_4$ is the $m$-tuple $(\alpha x_{m-1}, x_0, \ldots, x_{m-2})$ where $\alpha = 3 = -1$

Once the factorization of $x^n - 1$ over $\mathbb{Z}_4$ is obtained, the ideals of $R := \frac{\mathbb{Z}_4[x]}{\langle x^n - 1 \rangle}$ can be determined. For an odd positive integer $n$, any ideal $I$ of the ring $R$ has a generator of the form a $I = \langle f(x)h(x), 2f(x)g(x) \rangle$ where $f(x)g(x)h(x) = x^n - 1$ [32, 39]. Moreover, $|I| = 4^{\deg g(x)} 2^{\deg h(x)}$. It follows that the number of cyclic codes of length $n$ is $3^r$, where $r$ is the number of irreducible factors of $x^n - 1$ [32].

Finally, it can be shown that any ideal of $R$, for an odd $n$, is a principle ideal, with a generator of the form $p(x) = f(x)h(x) + 2f(x)$ (or equivalently $p(x) = f(x)h(x) + 2f(x)g(x)$) where $f(x), g(x), h(x)$ are as above [32, 39].

**Remark 1** When $x^n - 1$ has $r$ irreducible factors over a field, the total number of cyclic codes is $2^r$. We have a larger number over $\mathbb{Z}_4$ due to the existence of non-free codes (over a field all codes are free).

**Remark 2** The generator polynomial $p(x)$ of an ideal of $R$ described above does not necessarily divide $x^n - 1$. For example, let $n = 3, f(x) = 1$, and $h(x) = x - 1$, then $p(x) = x + 1$ and $p(x) \not| (x^3 - 1)$. When $h(x) = 1$, $p(x) = 3f(x) = -f(x)$ does divide $x^n - 1$. It is shown in [2] that the cyclic code generated by $p(x)$ is a free module if and only if $p(x)$ divides $x^n - 1$.

Making use of the structures of cyclic codes of odd length and the results from [32, 39] quoted above, we have conducted exhaustive computer searches over $\mathbb{Z}_4$-cyclic codes (up to certain lengths and sizes). We have determined the cyclic codes with best minimum Lee weights for each length and size. The binary images of many of these cyclic codes have the same parameters as the best-known binary linear codes, and some lead to good non-linear codes, which are listed in Table 1.

**Remark 3** It is well-known that negacyclic codes of odd length over $\mathbb{Z}_4$ are equivalent to cyclic codes of the same length. Therefore, there is no need to consider negacyclic codes of odd length as far as code parameters are concerned. When $n$ is odd, $x^n + 1$ has a unique factorization over $\mathbb{Z}_4$ and it is obtained from the factorization of $x^n - 1$ by the simple transformation (a ring isomorphism) $x \to -x$ [2].

## 3.2 Cyclic and Negacyclic Codes of Even Length

When $n$ is even $x^n - 1$ (or $x^n + 1$) does not have a unique factorization and the structures of cyclic and negacyclic codes of even length over $\mathbb{Z}_4$ are more

complicated. There are some results in this area but we do not have complete answers for all cases. Cyclic codes of oddly even length (length $N = 2n$, where $n$ is odd) are studied in [3]. It is shown that although the number of cyclic codes of oddly even length $N = 2n$ is much larger than the number of cyclic codes of odd length $n$ (for example, there are 27 cyclic codes of length 7, while the number of cyclic codes of length 14 is 1183), many of these codes have poor minimum distances. One subclass of such codes, called minimal codes, is identified in [3] as being promising in terms of having large minimum distances. These codes have generators of the form $f(x^2)\overline{f_s(x)}$ where $x^n - 1 = f(x)f_s(x)$ (over $\mathbb{Z}_4[x]$), and $\overline{f_s(x)} = f_s(x) + 2g(x)$, $\deg(g(x)) < \deg(f_s(x))$. Several examples of minimal codes of short length in this class are presented in [3] that have binary images with the same parameters as the best-known binary linear codes. It was given as an open problem to determine whether there are codes in this class with good binary images. We investigated this problem, searching for new codes in this class. We have found a number of additional codes with the same parameters as the best-known binary codes and one code with a better minimum distance. This code has $\mathbb{Z}_4$ parameters $[30, 4^4, 28]$ and generator $g = 3x^{26} + 3x^{25} + x^{24} + x^{23} + 3x^{21} + 2x^{20} + x^{19} + 3x^{18} + 2x^{16} + x^{15} + 2x^{13} + 2x^{12} + 3x^{11} + 3x^{10} + 3x^9 + x^8 + 3x^6 + 3x^4 + x^3 + 2x^2 + 2x + 3$ obtained from $f(x^2) = x^{22} + x^{20} + 3x^{18} + x^{16} + 2x^{14} + 3x^{12} + x^8 + 3x^6 + 2x^4 + 3$ and $\overline{f_s(x)} = 3x^4 + 3x^3 + 2x^2 + 2x + 1$. (We later give a QT code with the same parameters.)

Recall that a negacyclic code of odd length over $\mathbb{Z}_4$ is equivalent to a cyclic code of the same length under the ring isomorphism $x \to -x$. Negacyclic codes of even length over $\mathbb{Z}_4$ are studied in [4], where it is shown that a negacyclic code of even length $N = 2^a n$, $n$ odd, has a generator of the form $\prod_{i=0}^{2^{a+1}+1} [g_i(x)]^i$ (product taken in $\mathbb{Z}_4[x]$ modulo $x^N + 1$) where the $g_i(x)$'s are monic co-prime divisors of $x^n - 1$ in $\mathbb{Z}_4[x]$. It follows that the number of negacyclic codes of length $N$ is $(2^{a+1} + 1)^r$, where $r$ is the number of irreducible factors of $x^n - 1$. This enables us to systematically generate all negacyclic codes of even length. We have found a number of such codes with binary images that have the same parameters as the best-known binary linear codes.

## 3.3 New Cyclic Codes

In this section, we present the results of the search over cyclic codes. Table 1 gives the generators and parameters of the cyclic $\mathbb{Z}_4$ codes whose Gray images have better minimum distances than the comparable binary linear codes. The first three columns give the $\mathbb{Z}_4$ parameters, corresponding binary parameters, and minimum distance of the best-known binary linear code with the same parameters, respectively. The generator of the $\mathbb{Z}_4$ code is given in the last column. All the binary images are non-linear. The first 11 codes have parameters that fall into the table [27]. Of these, codes 1-9 have the same parameters as the best-known binary nonlinear codes. Note however that although they have additional structure, the $[47, 4^{23}, 18]$ and $[47, 4^{24}, 16]$ codes improve the bounds in the table of best-known nonlinear codes [27]. Their binary images have parameters $(94, 2^{46}, 18)$ and $(94, 2^{48}, 16)$, respectively. In the notation of [27], $A(93, 15)$ is improved from $9 \cdot 2^{44}$ to $2^{48} = 16 \cdot 2^{44}$, and $A(93, 17)$ is improved from $11 \cdot 2^{42}$ to $2^{46} = 16 \cdot 2^{42}$.

For the generators of these codes, we list the coefficients of the generator polynomials in increasing powers. For example, the generator $g(x) = 3x^6 + 2x^4 + 2x^3 + 3x^2 + 3x + 3$ of the $[31, 4^{25}, 6]$ cyclic code in the table is listed as 3332203. The parameters of other cyclic and negacyclic codes are available from the authors.

We summarize the results that lead to improvements in the table of best-known binary codes [27] in the following theorem.

**Theorem 3.1.** *Let $A(n, d)$ be the size of the largest binary code of length $n$ and minimum distance $d$. Then, $A(93, 15) \geq 2^{48}$ and $A(93, 17) \geq 2^{46}$.*

Table 1: Parameters and Generators of the Good Cyclic $Z_4$-codes

| $Z_4$ | Binary | $d$ | Generators |
|---|---|---|---|
| $[31,4^5,28]$ | $(62,2^{10},28)$ | 26 | 32103112330221313203323003 |
| $[31,4^6,26]$ | $(62,2^{12},26)$ | 24 | 31013223133032012103332201 |
| $[31,4^{15},14]$ | $(62,2^{30},14)$ | 12 | 30032012302211013 |
| $[31,4^{25},6]$ | $(62,2^{50},6)$ | 5 | 3332203 |
| $[31,4^52^1,26]$ | $(62,2^{11},26)$ | 25 | 30303310132003331120312322l |
| $[31,4^52^5,24]$ | $(62,2^{15},24)$ | 23 | 31021021333123132221032312l |
| $[31,4^62^5,22]$ | $(62,2^{17},22)$ | 21 | 10021132301023231310013031 |
| $[31,4^{15}2^5,12]$ | $(62,2^{35},12)$ | 11 | 32120011332133111 |
| $[31,4^{20}2^5,8]$ | $(62,2^{45},8)$ | 7 | 111310232321 |
| *$[47,4^{23},18]$ | $(94,2^{48},18)$ | 16 | 31223012232013033201102O3 |
| *$[47,4^{24},16]$ | $(94,2^{48},16)$ | 15 | 10201102013323301332ll33 |
| $[63,4^52^9,48]$ | $(126,2^{21},48)$ | 47 | 13122023023222112112032312303130333100310O<br>2121230213113321 |
| $[89,4^{12}2^{11},54]$ | $(178,2^{35},54)$ | 53 | 12231000021212233011002300110101303220l0<br>21313120300022003222023232301112000111 |
| $[89,4^{11}2^{12},56]$ | $(178,2^{34},56)$ | 54 | 33331102022110123001033133000031323220032<br>32201303223012100132311331223203302O1 |
| $[89,4^{22}2^1,48]$ | $(178,2^{45},48)$ | 46 | 10330202313233332031023121233213012<br>23320322202100130132110321310021 |

*These codes lead to improvements in the database of binary non-linear codes.

# 4 Quasi-Twisted Codes over $\mathbb{Z}_4$

## 4.1 Basic Facts

Next, we consider new $\mathbb{Z}_4$ codes in the class of quasi-twisted (QT) codes. The class of quasi-twisted codes over fields was first introduced in [25] as a generalization of quasi-cyclic (QC) codes [18], [19]. More recently, QT codes over $\mathbb{Z}_4$ and other rings have been considered. QT codes over $\mathbb{Z}_4$ was first considered in [2]. A $\mathbb{Z}_4$ code is called quasi-twisted if the same negacyclic shift of a codeword in $p$ groups of size $m$ always results in another codeword. Algebraically, QT codes are submodules of $R^p$ where $R := \frac{\mathbb{Z}_4[x]}{\langle x^m - \alpha \rangle}$ where $\alpha = 1$ or 3. Many QT codes can be constructed from $m \times m$ twistulant matrices (with a suitable permutation of coordinates). In the case of a 1-generator QT code, the generator matrix, $G$, can be represented as

$$G = [B_1, B_2, \ldots, B_p] \tag{2}$$

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

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

and $\alpha = 1$ or 3. If $\alpha = 1$, the code is QC.

The algebra of $m \times m$ twistulant matrices over $\mathbb{Z}_4$ is isomorphic to the algebra of polynomials in the ring $\mathbb{Z}_4[x]/\langle x^m - \alpha \rangle$ if $B$ is mapped onto the polynomial, $b(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{m-1} x^{m-1}$, formed from the entries in the first row of $B$ [28]. The $b_i(x)$ associated with a QT code are called the *defining polynomials* [17].

If the defining polynomials $b_i(x)$ contain a common factor which is also a factor of $x^m - \alpha$, then the QT code is called *degenerate* [17]. Define the *order* of this QT code as [36]

$$h(x) = \frac{x^m - \alpha}{\gcd\{x^m - \alpha, b_0(x), b_1(x), \cdots, b_{p-1}(x)\}}. \tag{4}$$

The dimension of the QT code, $k$, is equal to the degree of $h(x)$. If $h(x)$ has degree $m$, the dimension of the code is $m$, and (2) is a generator matrix. If $\deg(h(x)) = k < m$, a generator matrix for the code can be constructed by deleting $m - k$ rows of (2).

## 4.2 New Quasi-Twisted Codes

We now describe our search method for quasi-twisted codes, and present the results obtained. First, a representative set of defining polynomials is required. Consider the set, $A$, of polynomials of degree $m-1$ or less, with $|A| = 4^m$ elements. Two polynomials, $b_j(x)$ and $b_i(x)$ belong to the same equivalence class if

$$b_j(x) = ax^l b_i(x) \bmod (x^m - \alpha),$$

for some integer $l$ and scalar $a = 1$ or 3. This means that two polynomials are in the same class if one can be obtained from the other by a constacyclic shift, by multiplying by a nonzero scalar, or both. Only one polynomial from each class need be considered when constructing QT codes since polynomials from the same class produce equivalent codes [17]. This equivalence relation is induced by the action of a finite group on the set of $m$-tuples over $\mathbb{Z}_4$, where the group is generated by the transformation $(x_0, x_1, \ldots, x_{m-1}) \rightarrow (\alpha \cdot x_{m-1}, x_0, \ldots, x_{m-2})$. Distinct equivalence classes correspond to distinct orbits under the action of this group and so can be enumerated using Burnside's Lemma [35] (p. 294).

The search for a QC code was initialized by randomly choosing $p$ defining polynomials. The search employs a stochastic optimization algorithm, tabu search [13], [14], [22]. 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 [26].

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. In the context of our search, this means replacing a defining polynomial in the current solution with a new 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. Thus a new solution

Table 2: Maximum Minimum Lee Distances for Best $(pm, m)$ QC and QT 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 | 5 | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 | 28 | 32 | 33 | 36 | 38 |
| 3 | 4 | 7 | 10 | 14 | 16 | 20 | 24 | 26 | 29 | 32 | 34 | 38 | 40 | 44 | 48 | 50 | 53 |
| 4 | 4 | 8 | 12 | 16 | 22 | 24 | 28 | 32 | 36 | 41 | 46 | 49 | 54 | 58 | 64 | 66 | 70 |
| 5 | 6 | 10 | 16 | 20 | 26 | 30 | 34 | 40 | 46 | 50 | 55 | 60 | 64 | 69 | 74 | 80 | 84 |
| 6 | 6 | 12 | 17 | 24 | 28 | 34 | 40 | 46 | 52 | 58 | 64 | 68 | 74 | 80 | 86 | 92 | 97 |
| 7 | 8 | 13 | 20 | 26 | 32 | 40 | 46 | 52 | 58 | 64 | 72 | 77 | 84 | 90 | 96 | 103 | 110 |
| 8 | 8 | 14 | 22 | 28 | 36 | 42 | 49 | 56 | 64 | 72 | 78 | 86 | 92 | 100 | 108 | 114 | 122 |

is kept if the minimum weight of the code increases. To avoid local minima, the search is restarted at a new arbitrary solution after a specified number of iterations.

Tables 2 and 3 present the minimum weights of the best rate $1/mp$ and rate $1/(m-1)p$ codes, respectively, that were obtained. By best, we mean that this code has the highest weight of any known QT code with the same parameters. Since this is the first compiled table of $\mathbb{Z}_4$ codes, 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-known binary linear codes [27]. Of the 238 entries in Tables 2 and 3, 129 attain or exceed the best known distance for the corresponding binary code. The first rows of the twistulant matrices of the QT codes listed in these tables that exceed the minimum distances of the best linear codes are given in Table 4, where $d$ denotes the minimum Hamming distance of the corresponding best-known binary linear code, and the first column gives the $\mathbb{Z}_4$ code parameters. The first rows of the other codes are available from the authors.

Table 3: Maximum Minimum Lee Distances for Best $(pm, m-1)$ QC and QT Codes over $\mathbb{Z}_4$

| | $p$ | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $m$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 3 | 6 | 8 | 12 | 16 | 18 | 22 | 24 | 28 | 32 | 34 | 38 | 40 | 44 | 48 | 50 | 54 | 56 |
| 4 | 6 | 10 | 16 | 18 | 22 | 26 | 32 | 34 | 38 | 42 | 48 | 50 | 56 | 60 | 64 | 66 | 72 |
| 5 | 8 | 12 | 16 | 22 | 28 | 32 | 36 | 42 | 48 | 52 | 56 | 64 | 66 | 72 | 76 | 82 | 88 |
| 6 | 8 | 12 | 18 | 24 | 32 | 36 | 44 | 48 | 54 | 60 | 66 | 72 | 78 | 84 | 88 | 96 | 102 |
| 7 | 8 | 14 | 22 | 28 | 34 | 42 | 48 | 56 | 62 | 66 | 74 | 82 | 88 | 94 | 102 | 108 | 114 |
| 8 | 8 | 16 | 24 | 30 | 38 | 42 | 52 | 58 | 64 | 74 | 82 | 88 | 96 | 104 | 112 | 120 | 128 |
| 9 | 10 | 16 | 24 | 30 | 38 | 48 | 56 | 62 | 72 | 82 | 90 | 98 | 104 | 112 | 120 | 130 | 140 |

Table 4: Parameters and First Rows of the Good QT $\mathbb{Z}_4$ Codes

| $\mathbb{Z}_4$ | $m$ | $\alpha$ | $b_i(x)$ |
|---|---|---|---|
| $[30, 4^4, 28]$ | 5 | 1 | 3131,301,31332,2231,3302,2123 |
| $[30, 4^5, 26]$ | 5 | 1 | 2112,1333,1033,221,133,2123 |
| $[28, 4^6, 22]$ | 7 | 1 | 331311,301,310332,3311,323323 |
| $[49, 4^6, 42]$ | 7 | 1 | 3223222,331311,330321,21302,322221,3311,312033 |
| $[56, 4^7, 46]$ | 7 | 1 | 131213,102021,22221,12123,123323,13212,131111,132231 |
| $[66, 4^6, 58]$ | 6 | 3 | 1303,111211,111132,122131,11,102,21213,10212,2111,10321,2201 |

# References


[1] N. Aydin, I. Siap, and D. K. Ray-Chaudhuri, The structure of 1-generator quasi-twisted codes and new linear codes, *Des., Codes Cryptogr.*, **24** (2001) 313–326.

[2] N. Aydin and D. K. Ray-Chaudhuri, Quasi-cyclic codes over $\mathbb{Z}_4$ and some new binary codes, *IEEE Trans. Inform. Theory*, **48** (2002) 2065–2069.

[3] T. Blackford, Cyclic codes over $\mathbb{Z}_4$ of oddly even length, *Disc. Appl. Math.*, **128** (2003) 27–46.

[4] T. Blackford, Negacyclic codes over $\mathbb{Z}_4$ of even length, *IEEE Trans. Inform. Theory*, **49** (2003) 1417–1424.

[5] W. Bosma, J. J. Cannon, and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Computation*, **24** (1997) 235–266.

[6] A. E. Brouwer, Bounds on the minimum distance of linear codes [online server], http://www.win.tue.nl/~aeb/voorlincod.html.

[7] A. R. Calderbank and G. McGuire, Construction of a $(64, 2^{37}, 12)$ code via Galois rings, *Des., Codes Cryptogr.*, **10** (1997) 157–165.

[8] J.H. Conway and N. J. A. Sloane, Self-dual codes over the integers modulo 4, *J. Combin. Theory, Ser. A*, **62** (1993) 31–45.

[9] R. Daskalov, T. A. Gulliver, and E. Metodieva, New good quasi-cyclic ternary and quaternary linear codes, *IEEE Trans. Inform. Theory*, **43** (1997) 1647–1650.

[10] R. Daskalov, T. A. Gulliver, and E. Metodieva, New ternary linear codes, *IEEE Trans. Inform. Theory*, **45** (1999) 1687–1688.

[11] S. T. Dougherty, T. A. Gulliver, Y. H. Park, and J. N. C. Wong, Optimal linear codes over $Z_m$, *J. Korean Math. Society*, (to appear).

[12] J. Fields, P. Gaborit, J. Leon, and V. Pless, All self-dual $\mathbb{Z}_4$ codes of length 15 or less are known, *IEEE Trans. Inform. Theory*, **44** (1998) 1222–1228.

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

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

[15] D. G. Glynn, T. A. Gulliver, and M. K. Gupta, On some quaternary self-orthogonal codes, *ARS Comb.*, (to appear).

[16] M. Grassl, Table of bounds on linear codes [online server], http://www.codetables.de.

[17] P. P. Greenough and R. Hill, Optimal ternary quasi-cyclic codes, *Des., Codes Cryptogr.*, **2** (1992) 81–91.

[18] 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.

[19] 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.

[20] T. A. Gulliver, J.-L. Kim, and Y. Lee, New MDS or near-MDS self-dual codes, *J. Combin. Theory, Ser. A*, (submitted).

[21] T. A. Gulliver and P. R. J. Östergård, New binary linear codes, *Ars. Comb.*, **56** (2000) 105–112.

[22] 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.

[23] T. A. Gulliver and J. N. C. Wong, Classification of optimal linear $\mathbb{Z}_4$ rate 1/2 codes of length $\leq 8$, *ARS Comb.*, (to appear).

[24] A. R. Hammons, Jr., 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.

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

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

[27] S. Litsyn, Table of non-linear binary codes [online], http://www.eng.tau.ac.il/~litysn/tableand/index.html.

[28] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North Holland, New York, 1977.

[29] A. A. Nechaev, Trace-function in Galois rings and noise-stable codes, Proc. *5th All-Union Symposium on the Theory of Rings, Algebras and Modules*, (1982) 97.

[30] A. A. Nechaev, Kerdock code in cyclic form, *Disc. Math. (USSR)*, **1** (1989) 123–139 (in Russian). English translation: *Disc. Math. and Appl.*, **1** (1991) 364–384.

[31] V. S. Pless, J. S. Leon, and J. Fields, All $\mathbb{Z}_4$ codes of Type II and length 16 are known, *J. Combin. Theory, Ser. A* **78** (1997) 32–50.

[32] V. S. Pless and Z. Qian, Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory*, **42** (1996) 1594–1600.

[33] E. M. Rains, Optimal self-dual codes over $\mathbb{Z}_4$, *Disc. Math.*, **203** (1999) 215–228.

[34] 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.

[35] F.S. Roberts, *Applied Combinatorics*, Englewood Cliffs, NJ: Prentice-Hall, 1984.

[36] G. E. Séguin and G. Drolet, *The Theory of 1-generator Quasi-Cyclic Codes*, Technical Report, Royal Military College of Canada, Kingston, ON, 1991.

[37] I. Siap, N. Aydin, and D. K. Ray-Chaudhuri, New ternary quasi-cyclic codes with better minimum distances, *IEEE Trans. Inform. Theory*, **46** (2000) 1554–1558.

[38] J. H. van Lint, *Introduction to Coding Theory*, Springer, New York, 1999.

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