Some Open Problems on Quasi-Twisted and Related Code Constructions and Good Quaternary Codes

Nuh Aydin and Tsvetan Asamov
Department of Mathematics
Kenyon College
Gambier, OH 43022
{aydinn,asamovt}@kenyon.edu

T. Aaron Gulliver
Dept. of Electrical & Computer Eng.
University of Victoria
Victoria, BC V8W 3P6 Canada
Email: agullive@ece.uvic.ca

***Abstract*— One of the most important and challenging problems in coding theory is to construct codes with the best possible parameters. Quasi-cyclic (QC) and the larger class of quasi-twisted (QT) codes have been proven to contain many good codes (with best-known parameters). In this paper, we review some open problems concerning these codes, introduce generalizations of QT codes, and suggest some constructions involving QT codes. We also present some new and good quaternary codes.**

Keywords: Quaternary codes, quasi-twisted codes, new bounds.

I. Introduction

Let F_q (or $GF(q)$) denote the finite field with q elements. A linear code over F_q of length n, dimension k and minimum Hamming distance d is said to be an $[n,k,d]_q$-code.

One of the main problems of coding theory is to find optimal values of the parameters n, k and d (for a given value of q) and to explicitly construct such codes. One version of the problem is to find the maximum value of d, given n and k. This value will be denoted by $d_q(n,k)$. There are various bounds on the parameters of a linear code (see for example [6]). Up-to-date tables of the best-known linear codes over F_q for $q = 2, 3, 4, 5, 7, 8$ and 9 up to certain lengths and dimensions are available at [5][1] and [12]. The computer algebra system MAGMA [4] also has such a database.

II. Quasi-Twisted Codes

The class of quasi-cyclic (QC) and the related class of quasi-twisted (QT) codes have been shown to be promising to solve the problem of determining $d_q(n,k)$. As a result, much research has focused on these two classes of codes. Aside from being a natural generalization of cyclic codes, some of the motivations to study these codes are as follows:

1) QC codes meet a modified version of Gilbert Varshamov bound, unlike many other classes of codes [15].
2) Some best quadratic residue codes and Pless symmetry codes are QC [16].
3) They enjoy a rich algebraic structure compared to arbitrary linear codes (which makes the search process much simpler).
4) A large number of best-known codes come from QC codes. Among these, there is a significant number of *optimal codes*.

As a result of searches for QC and QT codes, many new record breaking codes (codes with better parameters than the previously best-known codes), over finite fields of orders 2,3,5,7,8, and 9 have been discovered. Some of the recent work can be found in [2],[5]-[10], and [14].

This paper is organized as follows. We first summarize some of the basic facts concerning the structure of QT codes (a more detailed description can be found in [2]), and present some good and new QT codes over F_4. We state a long standing open problem that is connected to QT codes. We then introduce a generalization of QT codes, called QCT codes, and a similar open problem for that class. We also look at some constructions (variants of known constructions) and open problems related to QCT codes. New and good codes that we have found are also presented. By a "new code" we mean a code that has parameters better than a previously best-known code; and by a "good code" we mean a code that has the same parameters as a best-known code.

A. The Structure of 1-Generator QT Codes

A linear code is called $l-$QT if it is invariant under a constacyclic shift by l positions, where the constacyclic shift of a vector $(c_0, c_1, \ldots, c_{n-1}) \in F_q^n$ is $(a \cdot c_{n-1}, c_0, c_1, \ldots, c_{n-2})$, for some non-zero element $a \in F_q$. A linear code that is invariant under a constacyclic shift is called constacyclic. Therefore, constacyclic codes are a special case of QT codes corresponding to $l = 1$. (Note the similarity between the way QC and QT codes are generalizations of cyclic and constacyclic codes, respectively).

Algebraically, an l-QT code over F_q of length $n = ml$ can be viewed as an $F_q[x]/\langle x^m - a\rangle$ submodule of $(F_q[x]/\langle x^m - a\rangle)^l$. Then, an r-generator QT code is spanned by r elements of $(F_q[x]/\langle x^m - a\rangle)^l$. In this paper, as is the case in most of the literature, we restrict ourselves to 1-generator QT codes. An important result about 1-generator QT codes that has been used in some of the recent work is the following.

Theorem 2.1: [2] Let C be a 1-generator l-QT code of length $n = ml$ with a generator of the form:

$$\boldsymbol{g(x)} = (f_1(x)g(x), f_2(x)g(x), \ldots, f_l(x)g(x)) \qquad (1)$$

[1]After the submission of this manuscript, it has been announced that this online database is discontinued due to the existence of [12] which has more explicit information on constructions.

where $g(x)|(x^m - a), g(x), f_i(x) \in F_q[x]/\langle x^m - a\rangle$, and $(f_i(x), h(x)) = 1$, $h(x) = \frac{x^m-a}{g(x)}$ for all $1 \leq i \leq l$. Then $l \cdot d \leq d(C)$ (minimum distance of C), where d is the minimum distance of the constacyclic code generated by $g(x)$. Moreover, the dimension of C is equal to $n - \deg(g(x))$.

In terms of generator matrices, the QT codes can be characterized as follows. Let

$$G_0 = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{m-1} \\ ag_{m-1} & g_0 & g_1 & \cdots & g_{m-2} \\ \vdots & \vdots & \vdots & & \vdots \\ ag_1 & ag_2 & ag_3 & \cdots & g_0 \end{bmatrix}_{m \times m} \quad (2)$$

An $(m \times m)$ matrix of type G_0 is called a twistulant matrix of order m or simply a twistulant matrix.

It is shown in [2] that the generator matrices of QT codes can be transformed into blocks of twistulant matrices by a suitable permutation of columns. It is also shown that the generator matrix of a 1-generator QT code can be assumed to be in the form

$$\begin{bmatrix} G_1 & G_2 & \cdots & G_l \end{bmatrix}_{m \times n}$$

where each G_k is a twistulant matrix of the form (2).

B. New Codes and Their Generators

We searched for new QT codes over F_4. The field F_4 has elements $\{0, 1, a, b = a^2 = a+1\}$ where a is a root of x^2+x+1. Our method is based on Theorem 2.1. We have restricted our search to 1-generator QT codes with generators of the form: $(g(x), f_1(x)g(x), \ldots, f_{l-1}(x)g(x))$

We start by selecting a polynomial $g(x)$ that generates a constacyclic code with a large minimum distance. The choice of $g(x)$ determines the block length m, and the dimension of the code under consideration. Now choosing l determines the length and the dimension, and we can use the table of bounds [12] to obtain the currently best-known minimum distance. Then we search over the f_i's to improve the minimum distance.

Example 2.1:
Let $g(x) = \frac{x^{39}-a}{h(x)}$ where $h(x) = (x^6 + ax^5 + x^4 + ax^3 + x + a + 1)(x^6 + x^5 + ax^3 + x^2 + x + a + 1)$. Then $g(x)$ generates a quaternary constacyclic code with parameters $[39, 12, 18]$. According to [12], this is a best-known code. Searching over the codes with a generator of the form $(g(x), g(x)f_1(x))$, we find that if we choose $f_1 = 010b000a0bb1$ (here we just list the coefficients of the polynomial f_1 in increasing powers, thus f_1 is the polynomial $x + bx^3 + ax^7 + bx^9 + bx^{10} + x^{11}$ – we will use this notation in the sequel), then we obtain a $[78, 12, 44]$-code. This turns out to be a new code. The weight enumerator of this code is:
$0^1 44^{6786} 46^{24921} 48^{103194} 50^{321750} 52^{816075} 54^{1695096} 56^{2737215} 58^{3417453}$
$60^{3298464} 62^{2414529} 64^{1301391} 66^{491400} 68^{124371} 70^{21294} 72^{3159} 74^{117}$
where the bases are the weights and the exponents are the number of codewords of the given weight.

Using this procedure, we discovered the following constacyclic codes that are *optimal* (have the largest possible value of $d_q(n, k)$).
i) A $[11, 6, 5]$ code generated by $g(x) = a + x + x^2 + ax^3 + ax^4 + x^5$.
ii) A $[13, 6, 6]$ code generated by $g(x) = (x + a)(x^6 + x^5 + ax^3 + ax + 1)$
iii) A $[13, 7, 5]$ code generated by $g(x) = (x^6 + x^5 + ax^3 + ax + 1)$
iv) A $[19, 9, 8]$ code generated by
$g(x) = (x^9 + x^8 + bx^6 + x^5 + x^4 + ax^3 + x + 1)(x + a)$
v) A $[19, 10, 7]$ code generated by $g(x) = (x^9 + x^8 + bx^6 + x^5 + x^4 + ax^3 + x + 1)$
vi) A $[17, 8, 8]$ code generated by $g(x) = (x^4 + bx^3 + bx^2 + x + b)(x^4 + x^3 + ax^2 + ax + b)(x + b)$
vii) A $[17, 9, 7]$ code generated by $g(x) = (x^4 + bx^3 + bx^2 + x + b)(x^4 + x^3 + ax^2 + ax + b)$

New Quaternary Cyclic and Related Codes

We also discovered the following quaternary cyclic codes that are new:
i) A $[63, 35, 15]$ code generated by
$g = abbb0a001a101a0abba00a0b1aab1$ that divides $x^{63} - 1$.
ii) A $[63, 37, 14]$ code generated by
$g = a00100ba1ab100a0ab1ba011ab1$

Using standard construction techniques such as shortening and Construction X, we obtained 10 more new codes from the two cyclic codes above:

A) By shortening the first code we obtain the following new quaternary codes
iii) $[62, 36, 14]$ iv) [61,35,14] v) [60,34,14] vi) [59,33,14]
vii) [58,32,14] viii) [57,31,14]

B) By shortening the second code we obtain the following new quaternary codes
ix) [62,34,15] x) [61,33,15]

C) The following two codes are obtained by applying construction X.
xi) [64,36,15] code:
obtained by using [1, 1, 1] code, [63, 35, 15] cyclic code (found above), and [63, 36, 14] cyclic code (from [12])
xii) [66,37,15] code:
obtained by using [3, 3, 1] code, [63, 34, 15] cyclic code (from [12]), and [63, 37, 14] code (found above)

C. Generators of New and Good QT Codes

In this subsection, we present generators of the new and good quaternary codes. The weight enumerators were determined but will not be presented here. These are all 1-generator QT codes with a generator of the form described above and the constant involved is the field element a in F_4. All the computations were performed using the computer algebra software MAGMA.

New Quaternary QT Codes

i) A $[78, 12, 44]$ code: This is already given.
ii) A $[42, 9, 23]$ code generated by $(g(x), g(x)f_1(x))$ where, $g(x)h(x) = x^{21} - a$, $h(x) = (x^3 + bx^2 + x + a)(x^3 + ax^2 + ax + a)(x^3 + ax^2 + bx + a)$, $f_1 = 000aa00a1$

iii) A $[172, 7, 119]$ code generated by $(g(x), g(x)f_1(x), g(x)f_2(x), g(x)f_3(x))$ where $g(x)(x^7 + ax^6 + ax^5 + x^2 + x + a) = x^{43} - a$, $f_1 = 00101ba$, $f_2 = b10b$, and $f_3 = 0a1a01a$

iv) A $[215, 8, 147]$ code generated by $(g(x), g(x)f_1(x), g(x)f_2(x), g(x)f_3(x), g(x)f_4(x))$ where $g(x)(x^7 + ax^6 + ax^5 + x^2 + x + a)(x + a) = x^{43} - a$, $f_1 = 00aa10aa$, $f_2 = 1a011001$, $f_3 = 0a1b001$, and $f_4 = 0011010a1$

Good Quaternary QT Codes

i) A $[57, 10, 32]$ code generated by $(g(x), g(x)f_1(x), g(x)f_2(x))$ where $g(x) = (x^9 + x^8 + bx^6 + x^5 + x^4 + ax^3 + x + 1)$, $f_1 = 1bbab1bbab$, $f_2 = b10b001bb1$

ii) A $[172, 8, 117]$ code generated by $(g(x), g(x)f_1(x), g(x)f_2(x), g(x)f_3(x))$ where $g(x)(x^7 + ax^6 + ax^5 + x^2 + x + a)(x + a) = x^{43} - a$, $f_1 = 0aa1001a$, $f_2 = 00a0b101$, and $f_3 = 0aa10a01$

iii) A $[215, 7, 151]$ code generated by $(g(x), g(x)f_1(x), g(x)f_2(x), g(x)f_3(x), g(x)f_4(x))$ where $g(x)(x^7 + ax^6 + ax^5 + x^2 + x + a) = x^{43} - a$, $f_1 = a00aaab$, $f_2 = 1bb0001$, $f_3 = bb000b$, and $f_4 = 00a110b$.

D. QC Codes over $\mathbb{Z}_4$

Linear codes over the integers modulo 4, $\mathbb{Z}_4$ (also called quaternary codes), have also been studied extensively. In [3], QC and QT codes over $\mathbb{Z}_4$ are studied and a number of such codes whose Gray map images have better parameters than the corresponding binary linear codes are obtained. The search method used in [3] was similar to that described for F_4 above. Note the for $\mathbb{Z}_4$, the Lee weight is typically considered rather than the Hamming weight as with codes over fields. In [1], a number of new cyclic, QC, and QT $\mathbb{Z}_4$-codes are presented, including codes with Gray map images that are better than the best-known non-linear codes. Although the Gray map images of $\mathbb{Z}_4$-linear codes are most often non-linear, they are still better than arbitrary non-linear codes; for instance they are distance invariant.

In this work, we present two $\mathbb{Z}_4$-linear QCT codes, a generalization of QT codes defined in the next section, whose Gray map images have better parameters than the best-known QC and QT codes.

E. Open Problem I

The fact that a very large number of QC and QT codes of the form described above that have been discovered by computer search in recent years is intimately related to the following open problem stated in [16] (18.7, page 587):

Open Problem I: Let C be a cyclic (or constacyclic) code of length n. How should $a(x)$ be chosen so that the minimum distance of the code $\{|u(x)|a(x)u(x)(\mod x^n - 1)| : u(x) \in C\}$ is as large as possible? Is there a difference between the field version and the ring version of this problem?

The practical evidence from searches over 1-generator QC and QT codes shows that in many cases we do get very large minimum distances. However, to the best of our knowledge, no explanation has been provided for any specific properties of the polynomials that achieve these large minimum distances (one obvious restriction on $a(x)$ is that it be relatively prime to the canonical generator). Also, we have not noticed any explicit connection with good QT codes and this problem.

This problem can also be expressed in the following alternative, combinatorial way: Consider a 1-generator QT code C_T with a generator of the form (g, gf) where $x^m - a = gh$ and $(f, h) = 1$. Since g and fg generate the same cyclic or constacyclic code C, C_T is obtained from C by listing the codewords of C in a certain order, then listing them in another order and taking the juxtaposition. Each choice of f corresponds to an ordering of C. What would be a good ordering that would preserve the linearity of the code and give a large minimum distance?

III. A Generalization of QT Codes: QCT Codes

The purpose of this section is to introduce a generalization of QT codes (hence of QC codes as well), called QCT codes and investigate their structural properties.

Let $a_1, a_2, \ldots, a_l$ be non-zero constants (not necessarily distinct) in $\mathbb{F}_q$. A linear code of length $n = ml$ will be called a QCT code if it is invariant under the following shift:

$$(c_1, c_2, \ldots, c_{(m-1)l}, c_{(m-1)l+1}, \ldots, c_{ml}) \rightarrow$$
$$(a_1 c_{ml}, a_2 c_{ml-1}, \ldots, a_l c_{(m-1)l+1}, c_1, \ldots, c_{(m-1)l+1})$$

We remark that if all the constants are equal then we obtain a QT code, if they are all equal to 1 then we obtain a QC code. If $l = 1$ then we obtain constacyclic and cyclic codes as special cases.

As in the case of a QT code, it is easy to see that after a suitable permutation of the coordinate positions, a generator matrix of a QCT code can be put into blocks of twistulant matrices (each block involving a possibly different constant).

To illustrate this construction, we present two examples of QCT codes which are better than the best-known QC or QT codes over $\mathbb{Z}_4$.
i) A [6,2,6] code generated by

$$G = \left[\begin{array}{cc|cc|cc} 1 & 3 & 0 & 1 & 1 & 2 \\ 1 & 1 & 1 & 0 & 2 & 1 \end{array}\right]$$

This code has minimum Lee weight $d_L = 6$, while the best QC or QT code has $d_L = 5$ [1]. In addition, this code is *self-orthogonal*, and the best-known QT self-orthogonal code only

has $d_L = 4$ [11].
ii) An [8,4,6] code generated by

$$G = \left[\begin{array}{cccc|cccc} 0 & 0 & 1 & 2 & 0 & 1 & 1 & 1 \\ 2 & 0 & 0 & 1 & 3 & 0 & 1 & 1 \\ 1 & 2 & 0 & 0 & 3 & 3 & 0 & 1 \\ 0 & 1 & 2 & 0 & 3 & 3 & 3 & 0 \end{array}\right]$$

This is in fact a *self-dual* code, and the best QC or QT code has $d_L = 4$ [1],[11]. Note that the Gray map image of this code is the Nordstrom-Robinson code [16]. Thus this construction provides a new simple description of this code.

In addition to the codes above, many hundreds of quaternary (both over $\mathbb{Z}_4$ and F_4) QCT codes have been found which have the same parameters as the best-known codes.

A. Algebraic Properties

Now we like to investigate the algebraic structure of QCT codes. Let $a_i \in \mathbb{F}_q - \{0\}$, $R_i = \frac{\mathbb{F}_q[x]}{\langle x^m - a_i\rangle}$, $1 \le i \le l$ and $R = R_1 \times R_2 \times \cdots \times R_l$. A QCT code C, after a suitable permutation of coordinates, can be regarded as an $\mathbb{F}_q[x]$-module of R. We say that C is s-generated if it is generated by s elements. Since each block (of length m) of a QCT code is actually a constacyclic code, we have the following result.

Lemma 3.1: An s-generated QCT Code C has generators of the form $\{\mathbf{g_1}(x), \mathbf{g_2}(x), \ldots, \mathbf{g_s}(x)\}$ where

- $\mathbf{g_j}(x) = (g_{j1}(x), g_{j2}(x), \ldots, g_{jl}(x))$
- $g_{ji}(x) = f_{ji}(x)g_i(x)$ for some $g_i(x) \mid x^m - a_i$, $f_{ji}(x) \in R_i$ and $(f_{ji}, h_i) = 1$ where $x^m - a_i = g_i(x)h_i(x)$.

Again, we will focus on the 1-generator case. As a corollary we have that a 1-generator QCT code is generated by an element of the form

$$\mathbf{g}(x) = (f_1(x)g_1(x), f_2(x)g_2(x), \ldots, f_l(x)g_l(x))$$

where $f_i(x), g_i(x) \in R_i$ and $g_i(x) \mid (x^m - a_i)$. Moreover, we can show that f_i and g_i can be chosen so that $(f_i(x), h_i(x)) = 1$ where $h_i(x) = \frac{x^m - a_i}{g_i(x)}$. For two polynomials f and g we denote their greatest common divisor by (f, g) and their least common multiple by $[f, g]$.

Next we consider bounds on the parameters of a QCT code.

Theorem 3.1: Let C be a 1-generator QCT code generated by an element of the form described above.

1) $\dim(C) = \deg([h_1, h_2, \ldots, h_l])$
2) $d(C) \ge \min\{d_i : 1 \le i \le l\}$ where d_i is the minimum distance of the i-th constacyclic block and $d(C)$ is the minimum distance of C.

Proof: Let $h = [h_1, h_2, \ldots, h_l]$, then clearly, $h(x)\mathbf{g}(x) = 0$ which implies that $\dim(C) \le \deg(h)$. On the other hand, if $f(x)\mathbf{g}(x) = 0$ then $f(x)f_i(x)g_i(x) = 0$ in R_i, for $1 \le i \le l$. This implies that $h_i(x) \mid f(x)f_i(x)$. Since $(h_i(x), f_i(x)) = 1$, $h_i(x) \mid f(x)$ for $1 \le i \le l$. Hence $h(x) \mid f(x)$. This shows $\dim(C) \ge \deg(h)$ and the assertion on the dimension. The statement on the minimum distance is rather obvious. □

Example 3.1:
Let $q = 4$, $a_1 = 1, a_2 = a$, and $m = 11$. Let $g_1(x) = x^5 + ax^4 + x^3 + x^2 + bx + 1 \mid (x^{11} - 1)$ and $g_2(x) = x^5 + ax^4 + ax^3 + x^2 + x + a \mid (x^{11} - a)$. Then g_1 and g_2 generate cyclic and constacyclic (respectively) codes with parameters $[11, 6, 5]$. A code with these parameters is optimal [12]. Now we consider the QCT code generated by $\langle g1, g2\rangle$. In this case, $h_1 = \frac{x^{11}-1}{g_1}$ and $h_2 = \frac{x^{11}-a}{g_2}$ are relatively prime so that $[h_1, h_2] = h_1h_2$, hence the dimension is 12. The minimum distance of this QCT code is 5 which shows that the lower bound on the minimum distance is attained. Thus we obtain a quaternary $[22, 12, 5]$ code. According to [12], there exists a quaternary $[22, 12, 7]$ code.

Generalizing from this example, we can say more about the dimension and minimum distance of QCT codes in the special case when all the constants are distinct. If $a_1 \ne a_2$, then $x^m - a_1$ and $x^m - a_2$ are relatively prime. If $x^m - a_1 = g_1h_1$ and $x^m - a_2 = g_2h_2$ then $(h_1, h_2) = 1$ (as well as $(g_1, g_2) = 1$) so that $[h_1, h_2] = h_1h_2$. Then the QCT code C generated by $\mathbf{g} = \langle g1, g2\rangle$ has dimension $k_1 + k_2$ where k_1, k_2 are, respectively, the dimensions of the constacyclic codes generated by g_1 and g_2. We also claim that in this case the minimum distance is actually equal to $\min\{d_1, d_2\}$, where d_i is the minimum distance of the constacyclic code generated by g_i. To see this, consider $\{th_2\mathbf{g} = (th_2g_1, 0) : t \in \mathbb{F}_q[x], t \ne 0, \deg(t) < \deg(h_1)\}$. Since $\langle g_1\rangle = \langle h_2g_1\rangle$ (because $(h_1, h_2) = 1$), we see that there is a codeword of weight d_1 in C. Similarly, one can show that C contains a codeword of weight d_2. The same argument can be applied to any l when $a_1, a_2, \ldots, a_l$ are all distinct. This shows that the minimum distance of such a QCT code is not very high. However, there is a way to impose a restriction so that a better bound on the minimum distance is obtained.

Theorem 3.2: Let C be a 1-generator QCT code generated by, i.e., $\mathbb{F}_q$-span of $\mathbf{g}(x) = (f_1(x)g_1(x), f_2(x)g_2(x), \ldots, f_l(x)g_l(x))$ with the conditions on the f_i's and g_i's as described before. Let $h = \min\{\deg(h_i) : 1 \le i \le l\}$. Then the subcode C' generated by $\mathbf{g}(x), x\mathbf{g}(x), x^2\mathbf{g}(x), \ldots, x^{h-1}\mathbf{g}(x)$ has dimension h and minimum distance $\ge d_1 + d_2 + \cdots + d_l$ where d_i is the minimum distance of the code $\langle g_i\rangle$.

Example 3.2:
Let $q = 5, m = 13, l = 3, a_1 = 1, a_2 = 2, a_3 = 4$, $g_1 = (x^4 + x^3 + 4x^2 + x + 1)(x + 4)$, $g_2 = (x^4 + 4x^3 + 4x^2 + x + 1)(x + 3)$, $g_3 = (x^4 + 2x^3 + 2x^2 + 1)(x + 1)$ where $g_1 \mid (x^{13} - 1)$, $g_2 \mid (x^{13} - 2)$ and $g_3 \mid (x^{13} - 4)$ over $\mathbb{F}_5$. The constacyclic codes $\langle g_1\rangle$, $\langle g_2\rangle$ $\langle g_3\rangle$ all have parameters $[13, 8, 4]$. They are also optimal. The subcode of $\langle f_1g_1, f_2g_2, f_3g_3\rangle$ given in the last theorem has length 39, dimension 8 and minimum distance ≥ 12. However, when we choose $f_1 = x^7, f_2 = x^7 + 2x^6 + 2x^5$ and $f_3 = 3x^6 + x + 2$ the resulting code is a $[39, 8, 21]$ code. This example shows that the actual minimum distance in this construction may be significantly larger than the lower bound promised by the theorem. This code is not the best known code however, according to [12] there is a $[39, 8, 23]$ code.

B. Open Problem II

Open Problem II: Naturally, Open Problem 1 above can be stated for 1-generator QCT codes and their subclass described above.

IV. $|a+x|b+x|a+b+x|$ Construction and QT codes

Some well-known coding constructions can be applied to QCT codes to obtain new good codes. For example, construction X and related constructions have been applied to chains QC codes to find a large number of new codes in [13].

We also note that when we consider a QCT code C_T with a generator of the form (g_1, g_2) where $g_i | x^m - a_i$ and $a_1 \neq a_2$, C_T is equivalent to taking the direct sum of the two constacyclic codes with generator matrices G_1, G_2 resp. and therefore C_T has generator matrix $\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$.

One of the well-known constructions for new codes from existing codes is the $|a+x|b+x|a+b+x|$ construction [16] (18.7.4). If C_1 and C_2 are two linear codes with generator matrices G_1 of rank k_1, and G_2 of rank k_2 resp. then the code C obtained from this construction has generator matrix

$$\begin{pmatrix} G_1 & 0 & G_1 \\ 0 & G_1 & G_1 \\ G_2 & G_2 & G_2 \end{pmatrix}$$

and has dimension $2k_1 + k_2$. There is no simple formula known for the minimum distance. One of the most important applications of this constructing is the extended binary Golay code. Another open problem listed in [16] (18.7, page 588) is the following.

A. Open Problem III

Open Problem III: Are there other applications of this construction? Are there other constructions like this one which give good codes?

Inspired by this question, we propose to consider a related construction where the constituent matrices are twistulant. We consider linear codes with generator matrices of the form

$$\begin{pmatrix} G_1 & 0 & f_1G_1 \\ 0 & G_1 & f_2G_1 \\ G_2 & G_2 & G_2 \end{pmatrix}$$

where G_1 and G_2 are generator matrices of constacyclic codes, say with generator polynomials g_1 and g_2 (with possibly different constants). Here f_1G_1 denotes the twistulant matrix whose associated polynomial is f_1g_1.

We did a search over codes of this form and found the following good quaternary code. A $[51, 12, 24]$-code with a generator matrix of the above form where the component polynomials are as follows:

$g_1 = x^{13} + x^{12} + bx^{11} + x^9 + bx^8 + ax^7 + ax^6 + bx^5 + x^4 + bx^2 + x + 1$ dividing $x^{17} - 1$; $g_2 = x^{13} + x^{12} + bx^{11} + bx^{10} + bx^9 + ax^7 + x^6 + x^4 + ax^3 + bx^2 + ax + b$ dividing $x^{17} - a$; $f_1 = ax^2 + b$ and $f_2 = bx^3 + ax + a$.

V. Meta-QT Codes

Finally, we introduce a variant of the previous construction where generator matrices have the form

$$\begin{pmatrix} G_1 & f_1G_1 & f_2G_1 & 0 \\ 0 & G_1 & f_1G_1 & f_2G_1 \end{pmatrix}$$

or

$$\begin{pmatrix} G_1 & f_1G_1 & f_2G_1 & f_3G_1 & 0 \\ 0 & G_1 & f_1G_1 & f_2G_1 & f_3G_1 \end{pmatrix}$$

where the second row (of matrices) is a cyclic shift of the first row (of matrices). We can also have as many columns as desired. Again, each matrix is a twistulant matrix. We shall call such codes meta-QT codes. If g_1 generates an $[m, k, d]$ code then the code obtained with this construction will have length m times the number of vertical blocks and dimension $2k$. Again, there is no known simple formula for the minimum distance.

Searching over such codes, we obtain the following two good quaternary codes:

i) A [44,12,20] code with 4 block columns with $g = x^5 + ax^4 + ax^3 + x^2 + x + a$ that divides $x^{11} - a$, $f_1 = x^4 + x^2 + ax + 1$ and $f_2 = bx^4 + ax^3 + x^2 + ax + a$.

ii) A [55,12,27] code with the same g as in i), 5 block columns, $f_1 = ax^4 + bx^3 + x^2 + bx + 1$, $f_2 = bx^4 + ax^3 + ax^2 + a$ and $f_3 = x^5 + x^3 + ax^2 + ax$.

Acknowledgment

The authors would like to thank Markus Grassl for pointing out the extensions resulting in the new codes obtained using the two cyclic codes originally found.

References

[1] N. Aydin and T. A. Gulliver, "Some good cyclic and quasi-twisted $\mathbb{Z}_4$-linear codes," *Ars Comb.* (submitted).

[2] N. Aydin, I. Siap and D. K. Ray-Chaudhuri, "The structure of 1-generator quasi-twisted codes and new linear codes," *Des. Codes Cryptogr.*, vol. 24, no. 3, pp. 313-326, 2001.

[3] N. Aydin and D. Ray-Chaudhuri, "Quasi-cyclic codes over $\mathbb{Z}_4$ and some new binary codes," *IEEE Trans. Inform. Theory*, vol. 48, no. 7, pp. 2065–2069, 2002.

[4] W. Bosma, J. J. Cannon, and C. Playoust, "The Magma algebra system I: The user language," *J. Symbolic Comput.*, vol. 24, pp. 235–266, 1997.

[5] A. E. Brouwer, Linear code bounds [online server], http://www.win.tue.nl/ aeb/voorlincod.html.

[6] A. E. Brouwer, Bounds on the size of a linear code, in *Handbook Of Coding Theory*, V. S. Pless and W. C. Huffman Eds, pp. 295–461, Elsevier, New York, 1998.

[7] R. Daskalov, T. A. Gulliver and E. Metodieva, "New good quasi-cyclic ternary and quaternary linear codes," *IEEE Trans. Inform. Theory*, vol. 43, no. 5, pp. 1647–1650, 1997.

[8] R. Daskalov, T. A. Gulliver, and E. Metodieva, "New ternary linear codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 5, pp. 1687–1688, 1999.

[9] R. Daskalov and P. Hristov, "New quasi-twisted degenerate ternary linear codes," *IEEE Trans. Inform. Theory*, vol. 49, no. 9, pp. 2259–2263, 2003.

[10] R. Daskalov and P. Hristov, "New binary one-generator quasi-cyclic codes," *IEEE Trans. Inform. Theory*, vol. 49, no. 11, pp. 3001–3005, 2003.

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

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

[13] M. Grassl and G. White, "New codes from chains of quasi-cyclic codes," Proc. *IEEE Int. Symposium on Inform. Theory*, pp. 2095–2099, 2005.

[14] T. A. Gulliver and P. R. J. Östergård, "New binary linear codes," *Ars. Comb.*, vol. 56, pp. 105–112, 2000.

[15] T. Kasami, "A Gilbert-Varshamov bound for quasi-cyclic codes of rate $1/2$," *IEEE Trans. Inform. Theory*, vol. 20, pp. 679, 1974.

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

[17] I. Siap, N. Aydin, and D. K. Ray-Chaudhuri, "New ternary quasi-cyclic codes with better minimum distances," *IEEE Trans. Inform. Theory*, vol. 46, no. 4, pp. 1554–1558, 2000.