Designs, Codes and Cryptography, 24, 313–326, 2001

The Structure of 1-Generator Quasi-Twisted Codes and New Linear Codes

NUH AYDIN naydin@math.ohio-state.edu
Department of Mathematics, The Ohio State University

IRFAN SIAP isiap@sakarya.edu.tr
Department of Mathematics, Sakarya University

DIJEN K. RAY-CHAUDHURI dijen@math.ohio-state.edu
Department of Mathematics, The Ohio State University

Communicated by: J. D. Key

Received February 23, 2000; Revised December 15, 2000; Accepted December 21, 2000

Abstract. One of the most important problems of coding theory is to construct codes with best possible minimum distances. Recently, quasi-cyclic (QC) codes have been proven to contain many such codes. In this paper, we consider quasi-twisted (QT) codes, which are generalizations of QC codes, and their structural properties and obtain new codes which improve minimum distances of best known linear codes over the finite fields $GF(3)$ and $GF(5)$. Moreover, we give a BCH-type bound on minimum distance for QT codes and give a sufficient condition for a QT code to be equivalent to a QC code.

Keywords: quasi-twisted codes, new bounds, ternary codes

1. Introduction

The class of quasi-cyclic (QC) codes have been shown to be promising to solve one of the most important problems in coding theory: to construct codes with the best possible parameters. Therefore a larger class of linear codes, called quasi-twisted (QT) codes, deserves a careful study. We have investigated this class of codes very closely, determined some of their structural properties, and found a BCH-type bound on minimum distance, in the special case of 1-generator QT codes. Moreover, we have found sufficient conditions for a QT code to be equivalent to a QC code. Finally, we made use of these results to develop an efficient method to search for new linear QT codes over the fields $GF(3)$ and $GF(5)$ and we have been able to find many such codes.

Following the convention, a linear code C of length n, dimension k, and minimum distance d over F_q will be denoted by $[n, k, d]_q$. The following map is useful in defining some important classes of codes.

Let $n = lm$ where $l, m \in \mathbb{N}$, $a \in F_q^\times := F_q - \{0\}$ and

$$\mu_{a,l} : C \to V$$

$$\mu_{a,l}((c_0, \ldots, c_{n-1})) = (a \cdot c_{0-l}, \ldots, a \cdot c_{(l-1)-l}, c_{l-l}, \ldots, c_{n-l-1})$$

where the subscripts are taken modulo n.

Definition 1.1. A linear code C is called l-quasi-twisted (l-QT) if $\mu_{a,l}(C) = C$.

In words, a constacyclic shift of a codeword by l positions is still a codeword, where a constacyclic shift of a codeword $(c_0, \ldots, c_{n-1})$ is $(ac_{n-1}, c_0, \ldots, c_{n-2})$. Some of the most important classes of codes can be realized as special cases of QT codes. For example the case $a = 1$ gives quasi-cyclic codes, $l = 1$ gives constacyclic codes (also known as pseudocyclic codes), $l = 1$ and $a = 1$ yields cyclic codes.

Since a code C is l-QT if and only if it is (l, n)-QT (an immediate generalization of the corresponding fact for QC codes in [9]), where (l, n) denotes the greatest common divisor of n and l, we will assume, without loss of generality, that $l \mid n$, so that $n = ml$ for some integer m. Note that if $(l, n) = 1$, the code is constacyclic.

Recently, there has been much research on quasi-cyclic codes. Some of the important facts that have motivated the researchers are the following:

1. Quasi-cyclic codes meet a modified version of Gilbert Varshamov bound unlike many other classes of codes [21].
2. Some best quadratic residue codes and Pless symmetry codes are quasi-cyclic [24].
3. They enjoy a simpler algebraic structure compared to arbitrary linear codes (which makes the search process much simpler).
4. A large number of record breaking codes come from quasi-cyclic codes. Among these, there is a significant number of *optimal codes* (the best possible minimum distance that a code can achieve), etc.
5. They are natural generalizations of important class of cyclic codes.

Due to the facts mentioned above and many more, researchers worked on quasi-cyclic codes and have been able to discover new record breaking codes over finite fields of orders 2, 3, 5, 7, 8, and 9 which were quasi-cyclic. Most of the work can be found in [2, 5, 7–17, 19, 27] and [29]. Aside from [8] and [19], there has not been quite as much search on QT codes as on QC codes. Since the class of QT codes is larger, it would be no surprise to find "good" linear codes which are QT. That is part of the reason we search over QT codes. We first review constacyclic codes in the next section and then obtain structural properties of QT codes in the following sections. Finally, we present new codes and their generators together with (Hamming) weight enumerators.

2. Constacyclic Codes and a BCH Bound

Constacyclic codes have algebraic properties similar to cyclic codes [1, 20, 22]. For example they can also be specified through the roots of their generator polynomials. In studying cyclic codes the factorization of $x^n - 1$ was crucial. Now, we are interested in factorizing $x^n - a$ over F_q. Before looking at this factorization, we remark that in certain cases constacyclic codes are equivalent to cyclic codes.

Definition 2.1. [24] Let C_1 and C_2 be codes of length n over F_q. We say that C_1 and C_2 are equivalent if there are n permutations $\pi_0, \pi_1 \ldots, \pi_{n-1}$ of F_q and a permutation σ of n

coordinate positions such that

$$\text{If} \quad (c_0, \ldots, c_{n-1}) \in C_1 \quad \text{then} \quad \sigma(\pi_0(c_0), \ldots, \pi_{n-1}(c_{n-1})) \in C_2.$$

For linear codes only those π_i's which are the compositions of a scalar multiplication with a field automorphism are allowed. The scalar multiple may vary for each coordinate, but the field automorphism must be the same.

There are some important special cases: when all π_i's are identity permutations, we say that C_1 and C_2 are *permutation equivalent* and when each π_i is a multiplication by a non-zero scalar, C_1 and C_2 are said to be *scalar multiple equivalent* [26] or *monomially equivalent* [4] pp. 18. (For prime fields such as $GF(p)$ for a prime p, there are no non-trivial field automorphisms.) Monomially equivalent codes have the same weight enumerator, in particular they have the same minimum distance [4] pp. 18.

THEOREM 2.1. *Let C be a constacyclic code of length n, generated by $g(x) \mid (x^n - a)$ over F_q. The constacyclic code C_δ generated by the same polynomial over $K := F_q[\delta]$ (the smallest field containing F_q and δ), where δ is an nth root of $a \in F_q$, is equivalent to a cyclic code of the same length over K.*

Proof. First, we embed the field F_q in K by the inclusion map $\iota : F_q \hookrightarrow K$. The image $\iota(C)$ of C need not be an ideal in $\frac{K[x]}{\langle x^n - a\rangle}$ but it is contained in the ideal C_δ generated by $g(x)$ in $\frac{K[x]}{\langle x^n - a\rangle}$. Consider the map $\psi : K[x] \longmapsto \frac{K[x]}{\langle x^n - 1\rangle}$, where $\psi(p(x)) = \overline{p(x\delta)}$, for any $p(x) \in K[x]$, $\overline{p(x)}$ denotes $p(x) \bmod (x^n - 1)$ in $\frac{K[x]}{\langle x^n - 1\rangle}$. Then ψ is a ring homomorphism which is surjective because for any $\overline{p(x)} \in \frac{K[x]}{\langle x^n - 1\rangle}$, $p(x\delta^{-1})$ belongs to $K[x]$. Therefore, $|\frac{K[x]}{\mathrm{Ker}\psi}| = |\frac{K[x]}{\langle x^n - 1\rangle}|$.

Since $\psi(x^n - a) = \overline{(\delta x)^n - a} = \overline{a(x^n - 1)} = \bar{0}$, $x^n - a$ is in the kernel ($\mathrm{Ker}(\psi)$) of this homomorphism. But $\mathrm{Ker}(\psi)$ is an ideal, so $\langle x^n - a\rangle \subseteq \mathrm{Ker}(\psi)$. Hence $|\frac{K[x]}{\mathrm{Ker}\psi}| \leq |\frac{K[x]}{\langle x^n - a\rangle}|$. Also, $|\frac{K[x]}{\langle x^n - 1\rangle}| = |\frac{K[x]}{\langle x^n - a\rangle}|$. Therefore we obtain the following chain of inequalities.

$$\left|\frac{K[x]}{\langle x^n - 1\rangle}\right| = \left|\frac{K[x]}{\mathrm{Ker}\psi}\right| \leq \left|\frac{K[x]}{\langle x^n - a\rangle}\right| = \left|\frac{K[x]}{\langle x^n - 1\rangle}\right|$$

which implies that $|\frac{K[x]}{\mathrm{Ker}\psi}| = |\frac{K[x]}{\langle x^n - a\rangle}|$. Together with $\langle x^n - a\rangle \subseteq \mathrm{Ker}(\psi)$, we conclude that $\mathrm{Ker}(\psi) = \langle x^n - a\rangle$. Consequently, the rings $\frac{K[x]}{\langle x^n - a\rangle}$, $\frac{K[x]}{\langle x^n - 1\rangle}$ are isomorphic. Hence the ideals of these rings are in one-to-one correspondence given by ψ. This means that the equivalence is given by the permutations $\pi_i(\alpha) := \delta^i\alpha$, $\alpha \in K$, of K and σ, the identity permutation, in Definition 2.1 and in fact this is a scalar multiple equivalence. ∎

Remark 1. Note that we have the following relations between the quotient rings under consideration:

$$\frac{F_q[x]}{\langle x^n - a\rangle} \hookrightarrow \frac{K[x]}{\langle x^n - a\rangle} \cong \frac{K[x]}{\langle x^n - 1\rangle}.$$

Remark 2. The code C in the last theorem is actually *subfield-subcode* [24] of C_δ, which is the restriction of C_δ to F_q.

COROLLARY 2.1. *When F_q contains an nth root δ of a, a constacyclic code of length n over F_q is equivalent to a cyclic code of length n over F_q.*

The following lemma from finite field theory tells us exactly when an element $a \in F_q$ has an nth root in F_q (hence a sufficient condition for a constacyclic code to be equivalent to a cyclic code).

LEMMA 2.1. *[25] Let $a = \alpha^i$ where α is a primitive element of F_q. Then the equation $x^n = a$ has a solution in F_q if and only if $(n, q-1) \mid i$, where $(n, q-1)$ denotes the greatest common divisor of the integers n and $q-1$.*

2.1. Factorization of $x^n - a$ and a BCH Bound

We review factorization of the polynomial $x^n - a$ for the sake of completeness. This can be found in [20] for example. Let $a \in F_q^\times$ be such that it does not have an nth root in F_q. We also assume that $(n, q) = 1$ so that the polynomial $x^n - a$ does not have multiple roots. The roots of $x^n - a$ are $\delta, \delta\zeta, \delta\zeta^2, \ldots, \delta\zeta^{n-2}$ and $\delta\zeta^{n-1}$ where ζ is a primitive nth root of unity and $\delta^n = a$. Then ζ lies in F_{q^m} where $m = ord_n(q)$, the (multiplicative) order of q modulo n. Since $\delta^n = a$, $\delta^{nr} = a^r = 1$, where r is the order of a in the multiplicative group $F_q^\times$ which is equal to $\frac{q-1}{(i,q-1)}$, $a = \alpha^i$ and α is a primitive element of F_q. Hence δ is an nrth root of 1. Therefore, $\delta \in F_{q^s}$ where $s = ord_{nr}(q)$. Now, $q^s - 1 \equiv 0 \bmod nr$ so $q^s - 1 \equiv 0 \bmod n$. This implies that $m \mid s$. Consequently, $F_{q^m} \subseteq F_{q^s}$. Hence, the field F_{q^s} contains both ζ and δ and we may take $\delta = w^t$ and $\zeta = w^{rt}$ where w is a primitive element of F_{q^s} (therefore a primitive $(q^s - 1)$-st root of unity) and $q^s - 1 = ntr$, for some integer t. So $\zeta = \delta^r$, and $x^n - a$ factors as follows:

$$x^n - a = \prod_{i=0}^{n-1}(x - \delta\zeta^i) = \prod_{i=0}^{n-1}\left(x - w^{t(1+ir)}\right) = \prod_{i=0}^{n-1}(x - \delta^{1+ir}).$$

Each irreducible factor of $x^n - a$ corresponds to a cyclotomic coset modulo nr (*not* necessarily modulo n) i.e., the degree of each irreducible factor is the same as size of a cyclotomic coset modulo nr. Since all the roots of $x^n - a$ are nrth roots of unity, we have $(x^n - a) \mid (x^{nr} - 1)$, and $(x^{nr} - 1) \mid (x^{n(q-1)} - 1) \mid (x^{q^s - 1} - 1)$.

EXAMPLE 1. *Let $q = 5$ and $n = 6$ and let us consider the polynomial $x^6 - 3$ over F_5 (hence constacyclic codes of length 6 over F_5 with $a = 3$). A primitive element of F_5 is 2, $3 = 2^3$ in F_5, order of 3 in F_5 is 4 and $(n, q-1) = (6, 4) = 2 \not| 3$ so that there is no 6th root of 3 in F_5. According to the discussion above,*

$$x^6 - 3 = \prod_{i=0}^{5}(x - \delta^{4i+1}) = (x^2 + 3x + 3)(x^2 + 2x + 3)(x^2 + 3)$$

where δ is a primitive $6 \cdot 4 = 24$th root of unity. The powers of δ that appear in this factorization are 1, 5, 9, 13, 17, *and* 21, *and these are precisely union of three (the same as the number of irreducible factors over F_5) cyclotomic cosets* modulo 24: *$cl_1 = \{1, 5\}$,*

$cl_9 = \{9, 21\}$, and $cl_{13} = \{13, 17\}$. On the other hand, $x^{24} - 1$ and $x^6 - 1$ factor over F_5 as follows:

$$\begin{aligned} x^{24} - 1 &= (x^2 + 3x + 3)(x^2 + 2x + 3)(x^2 + 3)(x^2 + 4x + 1)(x^2 + x + 2) \\ &\quad (x^2 + 2x + 4)(x^2 + x + 1)(x^2 + 4x + 2)(x^2 + 3x + 4)(x^2 + 2) \\ &\quad (x + 3)(x + 4)(x + 2)(x + 1), \quad \text{and} \\ x^6 - 1 &= (x^2 + 4x + 1)(x^2 + x + 1)(x + 1)(x + 4). \end{aligned}$$

The factors of $x^6 - 1$ correspond to the following cyclotomic cosets modulo 24:

$$cl_0 = \{0\}, cl_4 = \{4, 20\}, cl_8 = \{8, 16\}, \quad \text{and} \quad cl_{12} = \{12\},$$

which are obtained by shifting the cosets corresponding to $x^6 - 3$ by 1.

Now, using Theorem 2.1 we give an alternative proof of the well-known BCH bound.

THEOREM 2.2 [22](BCH Bound for Constacyclic Codes). *Let C be a constacyclic code of length n over F_q and let the generator polynomial $g(x)$ have the elements $\{\delta\zeta^i : 1 \le i \le d - 1\}$, where ζ is a primitive nth root of unity and δ is an nth root of a, among its roots. Then the minimum distance of $C \ge d$.*

Proof. (We assume the setting and the notations of Theorem 2.1) $\{\delta\zeta, \delta\zeta^2, \ldots, \delta\zeta^{d-1}\} = \{\delta^{r+1}, \delta^{2r+1}, \ldots, \delta^{(d-1)r+1}\}$. Consider the constacyclic code C_δ of length n over K with generator polynomial $g(x) \mid (x^n - a)$ having these elements among its roots. The corresponding cyclic code $\psi(C_\delta)$ (over K) generated by $g(\delta x) \mid (x^n - 1)$ has the elements $\zeta, \zeta^2, \ldots, \zeta^{d-1}$ among its roots. By the classical BCH bound, the minimum distance of $\psi(C_\delta) \ge d$. Since C_δ and $\psi(C_\delta)$ are equivalent, $d(C_\delta) \ge d$ as well. Finally, C is a subfield-subcode of C_δ, and therefore has also minimum distance $\ge d$. ∎

As the following example shows, the BCH bound is sometimes very useful and sharp.

EXAMPLE 2. *We assume the notation of Theorem 2.1. Let $q = 3$ and $n = 28$ and consider constacyclic codes of length 28 over F_3 with $a = 2$. We remark that the condition $(n, q - 1) \nmid i$ implies that it suffices to consider only even lengths over F_3 (to possibly obtain constacyclic codes not equivalent to cyclic ones). We find that $r = 2$ and therefore $(x^{28} - 2) \mid (x^{56} - 1)$. The factorization of $x^{28} - 2$ over F_3 is as follows:*

$$\begin{aligned} x^{28} - 2 &= \prod_{i=0}^{27}(x - \delta\zeta^i) = \prod_{i=0}^{27}(x - \delta^{2i+1}) \\ &= (x^6 + 2x^4 + x^3 + x^2 + 2)(x^6 + 2x^5 + 2x + 2)(x^2 + x + 2) \\ &\quad \times (x^6 + x^5 + x + 2)(x^6 + 2x^4 + 2x^3 + x^2 + 2)(x^2 + 2x + 2) \end{aligned}$$

where δ is a primitive 56th root of 1 and $\zeta = \delta^2$ is a primitive 28th root of 1 over F_3. The exponents of δ in this factorization are exactly odd integers modulo 56 and they are partitioned into the following cyclotomic cosets:

$$\{1, 3, 9, 19, 25, 27\}, \quad \{5, 13, 15, 23, 39, 45\}, \quad \{7, 21\}, \quad \{11, 17, 33, 41, 43, 51\},$$
$$\{35, 49\}, \quad \text{and} \quad \{29, 31, 37, 47, 53, 55\}.$$

Let $g(x)$ be the polynomial of smallest degree which contains $\delta^i, i = 5, 11, 29,$ and 35 among its roots. Then

$$g(x) = x^{20} + 2x^{19} + x^{17} + 2x^{16} + 2x^{13} + 2x^{12} + 2x^{11} + x^{10} + x^9 + 2x^8 + x^7 + 2x^4 + 2x^3 + x + 1$$

and the elements $\delta\zeta^i, 14 \leq i \leq 27$ are among the zeros of $g(x)$. Therefore, by the BCH bound for constacyclic codes, the constacyclic code of length 28 generated by $g(x)$ has minimum distance at least 15 (and its dimension is 8). It turns out that these are the parameters of an optimal *linear code over F_3 of length 28 and dimension 8 [3].*

3. Structure of 1-Generator QT Codes

Let

$$G_0 = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{m-1} \\ ag_{m-1} & g_0 & g_1 & \cdots & g_{m-2} \\ ag_{m-2} & ag_{m-1} & g_0 & \cdots & g_{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ ag_1 & ag_2 & ag_3 & \cdots & g_0 \end{bmatrix}_{m\times m} . \tag{1}$$

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

It is shown in [29] that the generator matrices of QC codes can be transformed into blocks of circulant (twistulant with $a = 1$) matrices by suitable permutation of columns. We can adopt a similar proof for QT codes here: Let C be QT code over F_q. Let $c_1, c_2, \ldots, c_r$ be the rows of the generator matrix of C. Form another generator matrix for C by taking all possible $\mu_{a,l}(c_i)$ (l quasi-twisted shifts). Thus we form an $rm \times n$ generator matrix for C. Next permute the columns $C_1, C_2, \ldots, C_n$ of the generator matrix so that they appear in the order

$$C_1, C_{l+1}, \ldots, C_{(m-1)l+1}, C_2, C_{2+l}, \ldots, C_{(m-1)l+2}, \ldots, C_l, C_{2l}, \ldots, C_{ml}.$$

Then, the resulting matrix will be in the blocks of twistulant matrices. Therefore, generator matrices of an r-generator and 1-generator QT codes can be assumed to be in the following forms:

$$\begin{bmatrix} G_{11} & G_{12} & \ldots & G_{1l} \\ G_{21} & G_{22} & \ldots & G_{2l} \\ \vdots & \vdots & & \vdots \\ G_{r1} & G_{r2} & \ldots & G_{rl} \end{bmatrix}_{rm\times n}, \quad \text{and} \quad [\, G_1 \; G_2 \; \ldots \; G_l \,]_{m\times n},$$

respectively, where each G_{ij} (or G_k) is a twistulant matrix of the form (1).

Similar to quasi-cyclic case, 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 we restrict ourselves to

1-generator QT codes. 1-Generator QC codes and their structural properties have been studied in [27] and [6], respectively. Recently, in [23] the structure of r-generator QC codes has been investigated by use of Gröbner basis.

Let $1 \le i \le l$. For fixed i consider the following ith *projection map* on an l-QT code C of length $n = ml$:

$$\Pi_i : F_q^n \to F_q^m$$
$$\left(c_0, c_1, \ldots, c_{(ml-1)}\right) \to \left(c_{(i-1)m}, c_{(1+(i-1)m)}, \ldots, c_{(m-1+(i-1)m)}\right).$$

In view of the structure of QT codes described above, $\Pi_i(C)$ is a constacyclic code for all i. This will yield the following theorem.

THEOREM 3.1. *Let C be a 1-generator l-QT code over F_q of length $n = ml$. Then, a generator $\boldsymbol{g(x)} \in (F_q[x]/\langle x^m - a\rangle)^l$ of C has the following form*

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

where

$$g_i(x) \mid (x^m - a) \quad \text{and} \quad (f_i(x), (x^m - a)/g_i(x)) = 1 \quad \text{for all } 1 \le i \le l.$$

Proof. Since $\Pi_i(C)$ is a constacyclic code for every i we have the result. ∎

The following is the main theorem which plays an important role in our research.

THEOREM 3.2. *Let C be a 1-generator l-QT code of length $n = ml$ with a generator of the form:*

$$\boldsymbol{g(x)} = (f_1(x)g(x), f_2(x)g(x), \ldots, f_l(x)g(x)) \tag{2}$$

where $g(x) \mid (x^m - a)$, $g(x)$, $f_i(x) \in F_q[x]/\langle x^m - a\rangle$, and $(f_i(x), h(x)) = 1$, $h(x) = \frac{x^m - a}{g(x)}$ for all $1 \le i \le l$. Then $l \cdot (d+1) \le d(C)$, where $\{\delta\zeta^i : s \le i \le s + (d-1)\}$ are among the zeros of $g(x)$ for some integers s, d $(d > 0)$ and dimension of C is equal to $n - \deg(g(x))$.

Proof. Observe that $\Pi_i(C)$ is a constacyclic code generated by $f_i(x)g(x)$ for all $1 \le i \le l$. We have that one of the components becomes zero if and only if all the others do because $p(x)f_i(x)g(x) = 0$ if and only if $h(x) \mid (p(x)f_i(x))$ (if $p(x) \ne 0$), which implies that $h(x) \mid p(x)$ since $(f_i(x), h(x)) = 1$. So, $p(x)f_j(x)g(x) = 0$ for all j. Therefore if $\boldsymbol{c}$ is a nonzero codeword in C, then $\Pi_i(\boldsymbol{c}) \ne 0$ for all i. Since $\langle f_i(x)g(x)\rangle = \langle g(x)\rangle$, $\Pi_i(C)$ is a constacyclic code with generator polynomial $g(x)$, and every nonzero codeword has weight $>d$ (by BCH bound). Hence, a nonzero codeword in C has a weight larger than or equal to $l \cdot (d+1)$. Moreover, it can be shown, similar to the cyclic code case, that elements $\boldsymbol{g(x)}, x\boldsymbol{g(x)}, \ldots, x^{n-(\deg(g(x)-1)}\boldsymbol{g(x)}$ form a basis for the code. In fact, if a relation $\sum_{i=0}^{\deg g(x)-1} a_i x^i g(x) = \boldsymbol{0}$ with $a_i \in F_q$ exists (with m-dimensional vectors), then a similar relation $\sum_{i=0}^{\deg g(x)-1} a_i x^i \boldsymbol{g}(x) = \boldsymbol{0}$ holds in F_q^n. Also, if $\sum_i b_i x^i g(x) \ne \boldsymbol{0}$, then neither is $\sum_i b_i x^i \boldsymbol{g}(x) = \boldsymbol{0}$. ∎

THEOREM 3.3. *Let $a = \alpha^i$ where α is a primitive element of F_q. If $(m, q-1) \mid i$, a QT code of length $n = ml$ over F_q is equivalent to a QC code of length n over F_q.*

Proof. Let C be such a QT code with a generator matrix G of the form described in the beginning of the section. Then to each vertical block j, $1 \leq j \leq l$, of m columns of G apply the permutations π_i $1 \leq i \leq m$ in the proof of the Theorem 2.1. Then the resulting code is equivalent to a QC code. ■

We end this section with the remark that the results of [23] about 1-generator QC are special cases of the results in this section.

4. New Codes and Their Generator Matrices

4.1. The Search Method

Our method is based on the Theorem 3.2. We have restricted our search to 1-generator QT codes with generators of the form:

$$(g(x), f_2(x)g(x), \ldots, f_l(x)g(x)).$$

In order to refine the search we looked at cyclotomic cosets of appropriate modulus and formed generator polynomials having longest possible strings of consecutive integer powers of ζ among its zeros. After fixing $g(x)$ (hence determining the dimension of the code as well as the block length m), we searched over $f_i(x)$ (by the help of a computer). In most cases $l = 2$ or 3. When $l = 2$, we only search for one $f(x)$ with $\deg(f(x)) < m - \deg(g(x)$. In this case the search is exhaustive over the QT codes with the prescribed block length m and dimension, if the dimension is not too large. For an illustration of the method, we work the following example in detail.

EXAMPLE 3. *Let $q = 3$, $m = 40$ and $a = 2$ and consider constacyclic codes of length 40 over F_3. The order of 2* mod 3 *is 2 and $x^{40} - 2$ factors over F_3 as*

$$x^{40} - 2 = \prod_{i=0}^{39} (x - \delta^{2i+1}).$$

The exponents of δ (a primitive 80th root of 1) are odd integers mod 80 *which are partitioned into the following cyclotomic cosets* mod 80*:*

$$\{1, 3, 9, 27\}, \quad \{5, 15, 45, 55\}, \quad \{7, 21, 29, 63\}, \quad \{11, 19, 33, 57\},$$
$$\{13, 31, 37, 39\}, \quad \{17, 51, 59, 73\}, \quad \{23, 47, 61, 69\}, \quad \{25, 35, 65, 75\},$$
$$\{41, 43, 49, 69\}, \quad \text{and} \quad \{53, 71, 77, 79\}.$$

Let $h(x)$ be the polynomial corresponding to cyclotomic cosets containing 1, 7 and 25 and let

$$g(x) = \frac{x^{40} - 2}{h(x)} = x^{28} + 2x^{27} + 2x^{25} + x^{24} + 2x^{23} + x^{21} + 2x^{20} + x^{19} + x^{18} + 2x^{17} + 2x^{15} + x^{14} + x^{13} + 2x^{11} + x^8 + 2x^7 + 2x^5 + x^3 + x^2 + 2.$$

Then $g(x)$ has degree 28 and contains $\delta\zeta^i$, $18 \leq i \leq 30$ among its roots. Therefore, the constacyclic code of length 40 generated by $g(x)$ has dimension 12 and minimum

distance ≥ 14 *and a QT code of the form* (g, gf_1, gf_2) *with* $(f_i, \frac{x^{40}-2}{g}) = 1, i = 1, 2$ *has length 120, dimension 12 and minimum distance at least 42. Let* $f_1 = 2x^{10} + x^9 + x^8 + x^6 + 2x^4 + x^3 + 2x^2 + x + 1$, *and* $f_2 = x^{11} + 2x^{10} + x^9 + x^6 + x^2 + 2x$ *(these are two such polynomials). A computer search showed that the QT code with these generators has, in fact, minimum distance 66, 3 units larger than the previously best known linear code over* F_3 *with parameters [120,12,63].*
The weight enumerator of this code is as follows:

$0^1 66^{4480} 69^{14000} 72^{36080} 75^{75008} 78^{114160} 81^{119040} 84^{94160} 87^{49840} 90^{19552}\ 93^{4480} 96^{560} 99^{80}$.

4.2. Generators and Weight Enumerators

We conclude by giving the generator matrices and weight enumerators of the new codes. Since a generator matrix of a 1-generator QT code is determined by the first row alone (and the constant a), we only present the first row separating the blocks with a comma.

The first 15 codes in the following list are ternary QT with $a = 2$ except code number 14 which is QC with $a = 1$. The last 3 codes are QT over $GF(5)$ with $a = 4$.

1. A $[120, 12, 66]_3$ code:

(201102221002011202112102120210000000000,
22211201021202020101121011200112202002 20,
01220100112201001220021011220220011212 11).

The weight enumerator is given in the last example.

2. A $[160, 12, 90]_3$ code:

(201102221002011202112102120210000000000,
00201102111222110211011200101010020100 10,
02011210120122222020120202220011210101 20,
12122210110200121200011222200211221220 22).

The weight enumerator of this code is

$0^1 90^{3472} 93^{8080} 96^{22160} 99^{46400} 102^{73440} 105^{102320} 108^{107280}$
$111^{84080} 114^{49040} 117^{24720} 120^{7408} 123^{2160} 126^{800} 129^{80}$.

3. A $[164, 8, 102]_3$ code:

(100112121211002110220122101222111122202122121121101122012
01220021111111200100000 00, 00001110210121200010102011121102
22021201222120102020001111011021200001122220212112).

The weight enumerator of this code is

$0^1 102^{1312} 105^{1312} 108^{656} 111^{1312} 114^{1312} 120^{328} 123^{328}$.

4. A $[164, 10, 96]_3$ code:

(10212121212010110220111102101202121010111101101102121021021010222222222201000000000, 00002002120212102101110110101021220011022220021122212112221121022112100222210022221).

The weight enumerator of this code is

$0^1 96^{1476} 99^{3444} 102^{6068} 105^{7544} 108^{10496} 111^{10988} 114^{10496} 117^{4428} 120^{3608} 123^{500}$.

5. A $[56, 12, 27]_3$ code:

(12221001020011211000000000, 00000010102111112122012021011).

The weight enumerator of this code is

$0^1 27^{3136} 30^{23520} 33^{79072} 36^{167552} 39^{162960} 42^{78064} 45^{16016} 48^{1008} 51^{112}$.

6. A $[56, 16, 21]_3$ code:

(10111000221220101211220001 01, 11210211022210000000000000000).

The weight enumerator of this code is

$0^1 21^{400} 22^{560} 23^{1960} 24^{7056} 25^{13328} 26^{32592} 27^{100408} 28^{153056} 29^{290864} 30^{713552} 31^{870800} 32^{1366624} 33^{2744112} 34^{2690576} 35^{3381192} 36^{5419288} 37^{4274312} 38^{4269440} 39^{5416208} 40^{3342080} 41^{2616544} 42^{2571432} 43^{1216544} 44^{711816} 45^{522928} 46^{184016} 47^{81536} 48^{41608} 49^{9144} 50^{2016} 51^{504} 52^{168} 54^{56}$.

7. A $[68, 16, 30]_3$ code:

(00000000102011122122110101210121 12, 11112111202212221210000000000000000).

The weight enumerator of this code is

$0^1 30^{9520} 33^{111656} 36^{805664} 39^{3511248} 42^{8934996} 45^{13109040} 48^{10726932} 51^{4697304} 54^{1035572} 57^{100640} 60^{4012} 63^{136}$.

8. A $[182, 12, 105]_3$ code:

(01111010120210121222022120101102101000222022100111 12012021201121100001011001011111202100102, 11002111 11110001010021202021011200102012200202221212201212 02101012100122201210210000000000000).

The weight enumerator of this code is

$0^1 105^{3276} 108^{20020} 111^{22932} 114^{42588} 117^{78624} 120^{101556} 123^{111384} 126^{58968} 129^{52416} 132^{19656} 135^{20020}$.

9. A $[182, 14, 99]_3$ code:

(010202211222001001120122111000120222021202102122211121212002022122022102220121221011020021, 10122110002002220112120020212212020222222120221202112121011110110221120102201000000000000000).

The weight enumerator of this code is

$0^{1}99^{3984}102^{13842}105^{48174}108^{121746}111^{279462}114^{504714}117^{766464}120^{893830}123^{842354}126^{647810}129^{384764}132^{184604}135^{67246}138^{19478}141^{3812}144^{626}147^{58}$.

10. A $[82, 17, 36]_3$ code:

(11200111002202200111002110000000000000000, 01010010121021211001012012210001100111211).

The weight enumerator of this code is

$0^{1}36^{1640}37^{5084}38^{8528}39^{21648}40^{45346}41^{91186}42^{179088}43^{327344}44^{574902}45^{987526}46^{1574892}47^{2453522}48^{3547156}49^{4916802}50^{6489480}51^{8123330}52^{9741436}53^{11004892}54^{11797750}55^{12005866}56^{11598244}57^{10584888}58^{9134882}59^{7423706}60^{5705806}61^{4079664}62^{2765286}63^{1774562}64^{1055668}65^{574984}66^{297086}67^{143418}68^{65436}69^{25584}70^{9348}71^{3116}72^{656}73^{410}$.

11. A $[70, 17, 29]_3$ code:

(10202000021121112210000000000000000, 00000001121002222001021020021000021).

The weight enumerator of this code is

$0^{1}29^{2660}30^{3360}32^{39550}33^{45010}35^{392982}36^{384860}38^{2465680}39^{2029790}41^{9225160}42^{6328340}44^{20211310}45^{11746910}47^{26081230}48^{12452720}50^{18783100}51^{7363790}53^{7317520}54^{2318680}56^{1440410}57^{348740}59^{130200}60^{24220}62^{3640}63^{300}$.

12. A $[148, 18, 71]_3$ code:

(10022221021211002112111010211120101112112001121201222200100000000000000000, 00001002202121020212121210121011100001122010022200022021112110100120012111).

The weight enumerator of this code is

$0^{1}71^{740}72^{740}73^{1628}74^{3404}75^{7548}76^{17464}77^{31376}78^{56240}79^{94276}$

$80^{154068}81^{285492}82^{435860}83^{714988}84^{1108964}85^{1690752}86^{2427052}$
$87^{3522548}88^{4805264}89^{6549740}90^{8526280}91^{10881404}92^{13466668}$
$93^{16262388}94^{18963388}95^{21626648}96^{23739052}97^{25642036}98^{26680552}$
$99^{26948432}100^{26400832}101^{24953688}102^{23124408}103^{20656952}104^{17888612}$
$105^{14970200}106^{12037876}107^{9520248}108^{7219440}109^{5332588}110^{3767932}$
$111^{2562028}112^{1716948}113^{1092684}114^{658748}115^{395604}116^{231028}$
$117^{119436}118^{67192}119^{34336}120^{14208}121^{6068}122^{2516}123^{888}124^{592}125^{444}$.

13. A $[52, 13, 23]_3$ (quasi-cyclic with $a = 1$) code:

(0111001012112202001012000 0, 0010100112202101012112200 0).

The weight enumerator of this code is

$0^{1}23^{1612}24^{1690}26^{16538}27^{16900}29^{92976}30^{70122}32^{267436}33^{161980}35^{372008}$
$36^{177086}38^{240318}39^{85020}41^{65104}42^{17446}44^{6734}45^{1196}47^{156}$.

14. A $[52, 10, 26]_3$ code:

(1021000000000, 0000112100211, 1001211212020, 0102211111220).

The weight enumerator of this code is

$0^{1}26^{756}27^{650}29^{3588}30^{2860}32^{9204}33^{5590}35^{14352}36^{6838}38^{9048}$
$39^{2990}41^{2028}42^{728}44^{390}45^{26}$.

15. A $[84, 9, 54]_5$ code:

(1031242421301000000 00, 0000000143312323422 14,
1031022203202401424 11, 0004241234043100230 13).

The weight enumerator of this code is

$0^{1}54^{1344}55^{1932}56^{4212}57^{7140}58^{12348}59^{19068}60^{32004}$
$61^{53508}62^{75180}63^{96900}64^{130032}65^{163800}66^{196728}67^{216972}$
$68^{209580}69^{201432}70^{168468}71^{137760}72^{96180}73^{64512}74^{34188}$
$75^{17136}76^{7308}77^{3528}78^{1260}79^{420}80^{84}81^{84}84^{16}$.

16. A $[78, 10, 48]_5$ code:

(1334442013301030201230113143010000000 00,
0000022234042140042112101421021010210 34).

The weight enumerator of this code is

$0^{1}48^{1248}49^{2496}50^{3900}51^{9672}52^{21384}53^{38844}54^{81588}55^{121992}$
$56^{224016}57^{336336}58^{486408}59^{679380}60^{800020}61^{982488}62^{1084668}$
$63^{1114308}64^{1042080}65^{821496}66^{734604}67^{510900}68^{322296}69^{185328}$

$$70^{93600}71^{41964}72^{15912}73^{6084}74^{2028}75^{416}76^{156}78^{12}.$$

17. A $[42, 12, 21]_5$ code:

(11304403110000000000, 00001320131032233113 1).

The weight enumerator of this code is

$$0^{1}21^{2912}22^{11256}23^{32844}24^{107072}25^{308784}26^{801024}27^{1916068}$$
$$28^{4096932}29^{7859124}30^{13727196}31^{21197148}32^{29084328}33^{35393344}34^{37446276}$$
$$35^{34115088}36^{26615624}37^{17248056}38^{9098880}39^{3731028}40^{1109556}41^{215292}42^{22792}.$$

Remark. Using the extension theorem in [18] we can extend the codes 11, 13 and 14 to $[71, 17, 30]_3$, $[53, 13, 24]_3$ and $[53, 10, 27]_3$ codes respectively.

Acknowledgments

We would like to thank the anonymous referees for their useful comments and suggestions. In particular, for pointing out the reference [18] and the extensions mentioned above.

References

1. E. R. Berlekamp, *Algebraic Coding Theory,* McGraw-Hill, New York (1968).
2. V. K. Bhargava, G. E. Séguin and J. M. Stein, Some (mk, k) cyclic codes in quasi-cyclic form, *IEEE Trans. Inform. Theory,* Vol. 24, No. 5 (1978) pp. 630–632.
3. A. E. Brouwer, Linear code bound (server), Eindhoven University of Technology, The Netherlands, http://www.win.tue.nl/math/dw/personalpages/aeb/voorlincod.html.
4. A. E. Brouwer, Bound on the size of a linear code, *Handbook Of Coding Theory* (V. S. Pless and W. Huffman, eds.), Vol. 1, Elsevier, New York (1998).
5. Z. Chen, Six new binary quasi-cyclic codes, *IEEE Trans. Inform. Theory,* Vol. 40, No. 5 (1994) pp. 1666–1667.
6. J. Conan and G. E. Séguin, Structural properties and enumeration of quasi-cyclic codes, *Appl. Algebra Engrg. Comm. Comput.,* Vol. 4, No. 1 (1993) pp. 25–39.
7. R. N. Dasklov, T. A. Gulliver and E. Metodieva, New good quasi-cyclic ternary and quaternary linear codes, *IEEE Trans. Inform. Theory,* Vol. 43, No. 5 (1997) pp. 1647–1650.
8. R. N. Daskalov, T. Aaron Gulliver, and E. Metodieva, New ternary linear codes, *IEEE Trans. Inform. Theory,* Vol. 45, No 5 (1999) pp. 1687–1688.
9. P. P. Greenough and R. Hill, Optimal ternary quasi-cyclic codes, *Des. Codes Cryptogr.,* Vol. 2, No. 1 (1992) pp. 81–91.
10. T. A. Gulliver, New optimal ternary linear codes of dimension 6, *Ars. Combin.,* Vol. 40 (1995) pp. 97–108.
11. T. A. Gulliver and V. K. Bhargava, Some best rate 1/p quasi-cyclic codes over GF(5), *Inform. Theory Applic. II,* Springer-Verlag, Berlin, New York (1996) pp. 28–40.
12. T. A. Gulliver, and V. K. Bhargava, Two new rate 2/p binary quasi-cyclic codes, *IEEE Trans. Inform. Theory,* Vol. 40, No. 5 (1994) pp. 1667–1668.
13. T. A. Gulliver and V. K. Bhargava, Nine good rate $(m-1)/pm$ quasi-cyclic codes, *IEEE Trans. Inform. Theory,* Vol. 38, No 4 (1992) pp. 1366–1369.
14. T. A. Gulliver and V. K. Bhargava, Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes over GF(3) and GF(4), *IEEE Trans. Inform. Theory,* Vol. 38, No 4 (1992) pp. 1369–1374.

15. T. A. Gulliver and V. K. Bhargava, New good rate $(m-1)/pm$ ternary and quaternary quasi-cyclic codes, *Des. Codes Cryptogr.,* Vol. 7, No. 3 (1996) pp. 223–233.
16. T. A. Gulliver and P. R. J. Östergard, New binary linear codes, *Ars. Comb.,* Vol. 56 (2000) pp. 105–112.
17. T. A. Gulliver and P. R. J. Östergard, Improved bounds for ternary linear codes of dimension 7, *IEEE Trans. Inform. Theory,* Vol. 43, No. 4 (1997) pp. 1377–1381.
18. R. Hill, An extension theorem for linear codes, *Des. Codes Cryptogr.,* Vol. 17, No. 1–3 (1999) pp. 151–157.
19. R. Hill and P. P. Greenough, Optimal quasi-twisted codes, in *Proceedings of the Second International Workshop Algebraic and Combinatorial Coding Theory,* Voneshta Voda, Bulgaria, June (1992) pp. 92–97.
20. J. M. Jensen, Cyclic concatenated codes with constacyclic outer codes, *IEEE Trans. Inform. Theory,* Vol. 38, No. 3 (1992) pp. 950–959.
21. T. Kasami, A Gilbert-Varshamov bound for quasi-cyclic codes of rate $1/2$, *IEEE Trans. Inform. Theory,* Vol. 20 (1974) pp. 679.
22. A. Krishna and D. V. Sarwate, Pseudocyclic maximum-distance-separable codes, *IEEE Trans. Inform. Theory,* Vol. 36, No. 4 (1990) pp. 880–884.
23. K. Lally and P. Fitzpatrick, Construction and classification of quasi-cyclic codes, *WCC 99, Workshop on Coding and Cryptography* Paris (France), January (1999) pp. 11–14.
24. F. J. MacWilliams and N. J. A. Sloane, *The Theory Of Error Correcting Codes,* North Holland, New York (1977).
25. S. Roman, *Field Theory,* Springer-Verlag, New York (1995).
26. S. Roman, *Coding and Information Theory,* Springer-Verlag, New York (1992).
27. G. E. Séguin and G. Drolet, The theory of 1-generator quasi-cyclic codes, Manuscript, Dept. Elec. Comput. Eng., Royal Military College of Canada, Kingston, Ont. (1990).
28. S. E. Tavares, V. K. Bhargava and S. G. S. Shiva, Some rate $p/(p+1)$ quasi-cyclic codes, *IEEE Trans. Inform. Theory,* Vol. 20 (1974) pp. 133–135.
29. K. Thomas, Polynomial approach to quasi-cyclic codes, *Bul. Cal. Math. Soc.,* Vol. 69 (1977) pp. 51–59.
30. H. van Tilborg, On quasi-cyclic codes with rate 1/m, *IEEE Trans. Inform. Theory,* Vol. 24, No. 5 (1978) pp. 628–630.