A Generalization of the ASR Search Algorithm to 2-Generator Quasi-Twisted Codes

1st Saurav R. Pandey
Department of Mathematics and Statistics
Kenyon College
Gambier, Ohio, USA
pandey1@kenyon.edu

2nd Nuh Aydin
Department of Mathematics and Statistics
Kenyon College
Gambier, Ohio, USA
aydinn@kenyon.edu

3rd Matthew J. Harrington
Department of Mathematics and Statistics
Kenyon College
Gambier, Ohio, USA
harrington1@kenyon.edu

4th Dev Akre
Department of Mathematics and Statistics
Kenyon College
Gambier, Ohio, USA
akre1@kenyon.edu

***Abstract*—One of the central problems in coding theory is to construct codes with best possible parameters and properties. A special class of codes called quasi-twisted (QT) codes is well-known to produce codes with good parameters. Most of the work on QT codes has been over the 1-generator case. In this work, we focus on 2-generator QT codes and generalize the ASR algorithm that has been very effective to produce new linear codes from 1-generator QT codes. As a result of implementing the generalized algorithm, we have found 103 2-generator QT codes that are new among the class of QT codes. Additionally, most of these codes possess the following additional properties: a) they have the same parameters as best known linear codes, and b) many of them have additional desired properties such as being LCD and dual-containing. Further, we have also found a binary 2-generator QT code that is new (record breaking) among all binary linear codes [1] and its extension yields another record breaking binary linear code.**

***Index Terms*—new quasi-twisted codes, best known codes, LCD codes, dual-containing codes, 2-generator quasi-twisted codes**

I. Introduction and Motivation

Constructing codes with best possible parameters is one of the central and challenging problems in coding theory. Every linear code has three fundamental parameters: the length (n), the dimension (k), and the minimum (Hamming) distance d. Such a code over the finite field $\mathbb{F}_q$ is referred to as an $[n,k,d]_q$-code.

Thus, we have an optimization problem where we want to determine the optimal value of the third parameter of a linear code given the values of the other two. For instance, fixing n and k, we look for the largest possible value of d, denoted $d_q[n,k]$. The online database ([1]) gives known information about $d_q[n,k]$ for $q \leq 9$ and for code lengths up to 256 (a different upper bound for n for each field).

However, this optimization problem is computationally taxing even with the help of modern computers. First, computing the minimum distance of an arbitrary linear code is NP-hard, and it becomes infeasible for large dimensions [18]. Second, for a given length, dimension, and finite field $\mathbb{F}_q$, the number of linear codes is large and grows very quickly. For these reasons, it becomes computationally infeasible to conduct comprehensive searches over arbitrary linear codes. As can be observed from the database [1], in most cases, optimal codes are not known. In general, this optimization problem is solved when either k or $n-k$ is relatively small.

A promising class of codes called quasi-twisted (QT) codes has been extremely fruitful in producing codes with good parameters. The search algorithm ASR, first introduced in [2] for 1-generator QT codes, has been particularly effective. The ASR algorithm and its generalization [3] have been used in many subsequent works (e.g., [4]–[7]) and produced many record breaking codes. Most of the research in the literature on QT codes has been on the special case of 1-generator codes with only a few exceptions on multi-generator codes (e.g., [8], [9]). The main goal of this work is to generalize the ASR algorithm to 2-generator QT codes and test its effectiveness.

II. Basic Definitions and Preliminaries

Cyclic codes have a prominent place in coding theory for both theoretical and practical reasons. Some of the most important classes of codes such as binary Hamming Codes, BCH codes, Reed-Solomon codes, and quadratic residue codes are either cyclic or equivalent to cyclic codes. Theoretically, they establish a key link between coding theory and algebra via the correspondence that maps an arbitrary vector $(c_0, c_1, \ldots, c_{n-1})$ in $\mathbb{F}_q^n$ to the polynomial $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ of degree less than n. Based on this vector space isomorphism, we use vectors and polynomials interchangeably.

Definition II.1. *A linear code C is called cyclic if it is closed under the cyclic shift operator π, i.e., whenever $c = (c_0, c_1, ..., c_{n-1})$ is a codeword of C, then so is $\pi(c) = (c_{n-1}, c_0, ..., c_{n-2})$.*

Constacyclic codes are generalizations of cyclic codes.

Definition II.2. *Let a be a non-zero constant in $\mathbb{F}_q$. A linear code C is called constacyclic (CC) if it is closed under the constacyclic shift operator, i.e., whenever $c = (c_0, c_1, ..., c_{n-1})$ is a codeword of C, then so is $\pi_a(c) = (ac_{n-1}, c_0, ..., c_{n-2})$.*

It is well known that the CC shift corresponds to multiplication by $x \mod x^n - a$ and constacyclic codes are ideals in the quotient ring $\mathbb{F}_q[x]/\langle x^n - a\rangle$. Note that when the constant a in the above definition, called the shift constant, is taken to be 1, we obtain cyclic codes as a special case. Similarly to a cyclic code, a CC code C of length n over $\mathbb{F}_q$ with shift constant a has a generator $g(x)$ that must divide $x^n - a$. Such a non-zero, monic polynomial of smallest degree is unique and it is called the (standard) generator of C. A CC code C is a principal ideal generated by $g(x)$, denoted $C = \langle g(x)\rangle$. Therefore, there is a one-to-one correspondence between CC codes of length n with shift constant a over $\mathbb{F}_q$ and the divisors of $x^n - a$. The dimension of $C = \langle g(x)\rangle$ is $k = n - \deg(g(x))$ with a basis $\{g(x), xg(x), \ldots, x^{k-1}g(x)\}$. The polynomial $h(x) = (x^n - a)/g(x)$ is called the check polynomial for C. The check polynomial has the property that a word $v(x)$ is in C if and only if $h(x)v(x) = 0$ in $\mathbb{F}_q[x]/\langle x^n - a\rangle$. A CC code $C = \langle g(x)\rangle$ has many generators and any generator is of the form $g(x)f(x)$ where $\gcd(f(x), h(x)) = 1$. From the generator polynomial $g(x) = g_0 + g_1 x + \cdots + g_m x^m$ of a CC code C we obtain its generator matrix as an a-circulant (twistulant) matrix:

$$Circ(g) = \begin{bmatrix} g_0 & g_1 & \cdots & g_m & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_m & 0\cdots & 0 \\ \cdots & & & & & & \\ 0 & \ldots & 0 & g_0 & g_1 & \cdots & g_m \end{bmatrix}$$

where each row is the cyclic (CC) shift of the row above.

A. Quasi-Cyclic (QC) and Quasi-Twisted (QT) codes.

Quasi-cyclic (QC) and quasi-twisted (QT) codes are generalizations of cyclic and CC codes where the shift can occur by ℓ positions for any $\ell \geq 1$. A linear code C is said to be ℓ-quasi-cyclic if for a positive integer ℓ, whenever $c = (c_0, c_1, ..., c_{n-1})$ is a codeword, $(c_{n-\ell}, ..., c_{n-1}, c_0, c_1, ...c_{n-\ell-1})$ is also a codeword. Similarly, a linear code C is said to be ℓ-quasi-twisted if it has the property that for a positive integer ℓ that divides n, if $c = (c_0, c_1, ..., c_{n-1})$ is a codeword, then so is $(ac_{n-\ell}, ..., ac_{n-1}, c_0, c_1, ...c_{n-\ell-1})$. Such a code C is called a QT code of index ℓ, or an ℓ-QT code. If $\gcd(\ell, n) = 1$, then a QT code is CC so WLOG, we assume that ℓ is a divisor of n. Hence we assume $n = m \cdot \ell$. It is also shown in [20] that in some cases a QT code is equivalent to a CC code. Algebraically a QT code of length $n = m\cdot\ell$ is an R-submodule of R^ℓ where $R = \mathbb{F}_q[x]/\langle x^m - a\rangle$. A generator matrix of a QT code can be put into the form

$$\begin{bmatrix} G_{1,1} & G_{1,2} & \ldots & G_{1,\ell} \\ G_{2,1} & G_{2,2} & \ldots & G_{2,\ell} \\ \vdots & \vdots & \ddots & \vdots \\ G_{r,1} & G_{r,2} & \ldots & G_{r,\ell} \end{bmatrix}$$

where each $G_{i,j} = Circ(g_{i,j})$ is a twistulant matrix defined by some polynomial $g_{i,j}(x)$. Such a code is called an r-generator QT code. Most of the work on QT codes in the literature is focused on the 1-generator case. In this work, we consider 2-generator QT codes.

III. 2-Gen QT Codes

A generator of a 2-generator QT code of index ℓ has the following form

$$\mathbf{g(x)} = \begin{bmatrix} g_{11}(x), g_{12}(x), \cdots, g_{1\ell}(x) \\ g_{21}(x), g_{22}(x), \cdots, g_{2\ell}(x) \end{bmatrix}$$

with the corresponding generator matrix

$$G = \begin{bmatrix} Circ(g_{11}(x)) & Circ(g_{12}(x)) & \cdots & Circ(g_{1\ell}(x)) \\ Circ(g_{21}(x)) & Circ(g_{22}(x)) & \cdots & Circ(g_{2\ell}(x)) \end{bmatrix}.$$

Our goal is to generalize the ASR algorithm that has been very effective to produce new linear codes, to the 2-generator case. The ASR algorithm was based on the following theorem.

Theorem III.1. *[2] Let C be a 1-generator ℓ-QT code over $\mathbb{F}_q$ of length $n = m\ell$ and shift constant a with the generator of the form:*

$$(f_1(x)g(x), f_2(x)g(x), ..., f_\ell(x)g(x)),$$

where $x^m - a = g(x)h(x)$ and for all $i = 1, ..., \ell$, $gcd(h(x), f_i(x)) = 1$. Then, C is an $[n, k, d']_q$-code where $dim(C) = m - deg(g(x))$, and $d' \geq \ell \cdot d$, where d is the minimum distance of the constacyclic code C_g of length m generated by $g(x)$.

In the original implementation of the ASR algorithm, the first step was to compute all CC codes of length m. When there are multiple codes of a given dimension k, a code with highest minimum distance was chosen, say with generator $g(x)$. Then a search for QT codes is set up so that many generators of the form given in the theorem above are considered for the same $g(x)$ but with different $f_i(x)$'s that satisfy the gcd condition. Later, the ASR algorithm was generalized in [3]. In the more generalized version, all constacyclic codes for a given length and dimension are partitioned into equivalence classes based on code equivalence and one generator polynomial from each equivalence class is used to set up a QT search. The general algorithm uses more generator polynomials $g(x)$, hence it is more comprehensive. In fact, it is shown in [3] that record breaking codes were obtained with the more general algorithm, that would have been missed by the original algorithm because they came from generators of CC codes that did not have the highest minimum distances.

Notion of equivalent codes was fundamental to the generalization in [3]. Codes that are equivalent share the same parameters and weight distributions, so it is sufficient to pick only one code from each equivalence class. Two linear codes are called equivalent to each other if one is obtained from the other by using any combination of the following operations:

1) Permutation of the coordinates.
2) Multiplication of elements in a fixed position by a non-zero scalar in $\mathbb{F}_q$.

3) Applying an automorphism of $\mathbb{F}_q$ to each component of the vectors.

When only the first transformation (permutation) is used, the resulting codes are said to be permutation equivalent, which is an important special case. In a recent work, an efficient algorithm to check equivalence of cyclic codes was given [12]. More recently, it has been generalized to CC codes [13]. We made use of this algorithm in our search.

We begin the ASR search algorithm for 2-generator QT codes by taking a generator $g(x)$ of a CC code over $\mathbb{F}_q$ with length m. Then, we construct the generator of an ℓ-QT code as in the 1-generator case of ASR.

$$(f_1(x)g(x), f_2(x)g(x), ..., f_\ell(x)g(x)),$$

where all $f_i(x)$ are chosen arbitrarily from $\mathbb{F}_q[x]/\langle x^m - 1\rangle$ such that they are relatively prime to $h(x)$, the check polynomial of the CC code generated by $g(x)$, and $\deg(f_i(x)) < \deg(h(x))$. The second block has a similar structure but we take one component 0. This is to ensure that the dimension of the QT code is $k_1 + k_2$. The following theorem gives more specifics about the form of a generator for a 2-generator QT code we considered.

Theorem III.2. *Let g be the standard generator of a CC code C_g of length m over $\mathbb{F}_q$, i.e., $x^m - a = gh_1$. Let p be a polynomial over $\mathbb{F}_q$ that divides h_1. Let $h_2 = \frac{(x^m-a)}{p\cdot g}$. Let C be a 2-generator QT code with a generator of the form*

$$\mathbf{g}(\mathbf{x}) = \begin{bmatrix} gf_{11} & gf_{12} & \cdots & gf_{1\ell} \\ 0 & pgf_{22} & \cdots & pgf_{2\ell} \end{bmatrix}$$

where $\gcd(f_{1j}, h_1) = 1$ and $\gcd(f_{2j}, h_2) = 1$. Let $k_1 = m - deg(g)$ and let $k_2 = m - deg(p \cdot g)$. Then, the dimension of the QT code generated by $\mathbf{g}(\mathbf{x})$ is $k = k_1 + k_2$ and $d(C) \geq d$ where d is the minimum distance of the CC code generated by g.

Proof. Let G be the matrix

$$\begin{bmatrix} Circ(gf_{11}(x)) & Circ(gf_{12}(x)) & \cdots & Circ(gf_{1\ell}(x)) \\ 0 & Circ(pgf_{22}(x)) & \cdots & Circ(pgf_{2\ell}(x)) \end{bmatrix}$$

which is a generator matrix of C and consider $Circ(gf_{11}(x))$ on the first row of G and the $k \times m$ zero matrix on the second row of G. Any codeword $c \in C$ is a linear combination of the rows $\{r_1, r_2, \ldots, r_{k_1+k_2}\}$ of G. Thus, $c = a_1 \cdot r_1 + a_2 \cdot r_2 + \ldots + a_{k_1} \cdot r_{k_1} + b_1 \cdot r_{k_1+1} + \ldots + b_{k_2} \cdot r_{k_1+k_2}$ for some $a_i \in \mathbb{F}_q$. Consider the first m coordinates of c. As the first m coordinates of r_i's are zeroes for $i = k_1+1, k_1+2, \ldots, k_1+k_2$, they are determined by rows r_j, $j = 1, 2, \ldots, k_1$. Thus, when considering the first m coordinates of a codeword, we only need to consider gf_{11} and $Circ(gf_{11}(x))$.

Let $gf_{11} = p_0+p_1x+\cdots+p_{m-1}x^{m-1}$ and let its twistulant matrix be $Circ(gf_{11}(x))$, represented by the following matrix:

$$\begin{bmatrix} p_0 & p_1 & p_2 & \cdots & p_{m-1} \\ ap_{m-1} & p_0 & p_1 & \cdots & p_{m-2} \\ ap_{m-2} & ap_{m-1} & p_0 & \cdots & p_{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ ap_{m-k+1} & ap_{m-k+2} & ap_{m-k+2} & \cdots & p_{m-k} \end{bmatrix}.$$

Note that the k_1 rows of $Circ(gf_{11})$ are linearly independent. Now let $c = \vec{0} \in C$. In particular, the first m coordinates of c are zero. Since the rows of $Circ(gf_{11})$ are linearly independent, it follows that for all $j = 1, 2, \ldots, k_1$, $a_j = 0$. Thus, $c = \vec{0} = b_1 \cdot r_{k_1+1} + \ldots + b_{k_2} \cdot r_{k_1+k_2}$. Now, since the rows of the matrices $Circ(pgf_{22}(x)), \cdots, Circ(pgf_{2\ell}(x))$ are linearly independent, $b_i = 0$ for all $i = 1, 2, \ldots, k_2$. Hence the rows of G are linearly independent, and $\dim(C) = k = k_1 + k_2$.

To show that $d' \geq d$, consider an arbitrary codeword $c \in C$ such that $c = r(gf_{11}, gf_{12}, \ldots, gf_{1\ell}) + t(pgf_{22}, \ldots, pgf_{2\ell}) = (rgf_{11}, g(rf_{12} + tf_{22}), \ldots, g(rf_{1\ell} + tf_{2\ell})$ for some polynomials $r, t \in \mathbb{F}[x]/\langle x^n - a\rangle$. Since c is non-zero, at least one block of it must be non-zero. Since each block is a CC code of minimum weight d, minimum weight of c is at least d. ☐

We have some important remarks about this theorem.

Remark 1. 1) *If the first (or some other) block of the second row of the generator is not 0 then the dimension of the QT code may be less than $k_1 + k_2$.*

2) *The lower bound on the minimum distance cannot be improved as there are cases where the lower bound is attained with equality. Consider, for example, a 2-generator QT code C as in Theorem 3.2 such that $p = 1$, and $f_{1i} = f_{2i}$ for $i = 2, 3, \ldots, \ell$. Let $r = -t$, and consider the codeword $c = r(gf_{11}, gf_{12}, \ldots, gf_{1\ell}) + t(0, pgf_{22}, \ldots, pgf_{2\ell})$. Then $c = (rf_{11}g, 0, 0, \ldots, 0)$. It follows that the weight of c is the weight of the CC code generated by $rf_{11}g$, which is d.*

3) *Even though the lower bound in the theorem cannot be improved and it is much smaller than the 1-generator case, the actual minimum distance of C is often much larger.*

4) *In the special case when $p = 1$, we have $k_1 = m - deg(g)$ and $k_2 = m - deg(1 \cdot g) = m - deg(g)$. Thus, $k_1 = k_2$, and $dim(C) = k_1 + k_2 = k_1 + k_1 = 2k_1$.*

IV. Search Methods

We developed and implemented a search algorithm based on Theorem 3.2 as a well as a variation of it. We consider this method a generalization the ASR algorithm. Our search yielded many new QT codes some of them with additional desirable properties such as being linear-complimentary dual (LCD), dual-containing, or reversible. Our search is set up the same way as the generalized ASR algorithm. Hence, we start with computing all CC codes of length m, partitioning them into equivalence classes using the algorithm in [13], and picking one generator from each equivalence class. We describe some special cases of the search below.

A. Case when $p = 1$

Let g be the standard generator of a CC code C_g of length m and dim k, i.e., $x^m - a = gh$ with $k = \deg(h) = m - \deg(g)$. Let C be a 2-generator QT code with a generator of the form

$$\begin{bmatrix} gf_{11} & gf_{12} & \cdots & gf_{1\ell} \\ 0 & gf_{22} & \cdots & gf_{2\ell} \end{bmatrix}$$

where $deg(g) \geq 0$ and $\gcd(f_{ij}, h) = 1$.

B. $g_1 = 1$ and high degree g_2

Let $g_1 = 1$ and let g_2 be the standard generator of a CC code C_g of length m and dim k, i.e. $x^m - a = g_2 h$ with $k = \deg(h) = m - \deg(g_2)$. Let C be a 2-generator QT code with a generator matrix G of the form

$$\begin{bmatrix} f_{11} & f_{12} & \cdots & f_{1\ell} \\ 0 & g_2 f_{22} & \cdots & g_2 f_{2\ell} \end{bmatrix}$$

where $\deg(g_2)$ starts from the highest possible value and decreases subsequently and $\gcd(f_{2j}, h) = 1$.

The following method is not directly related to Theorem III.2 but we have found some good 2-generator QT codes from it.

C. The second block is a CC shift of the first

Let g be the standard generator of a CC code C_g of length m and dim k, i.e. $x^m - a = gh$ with $k = \deg(h) = m - \deg(g)$. Consider a 2-generator QT code with a gen G of the form

$$\begin{bmatrix} gf_{11} & gf_{12} & \cdots & gf_{1(\ell-1)} & gf_{1\ell} \\ xgf_{1\ell} & gf_{11} & gf_{12} & \cdots & gf_{1(\ell-1)} \end{bmatrix}$$

where $deg(g) \leq 2$ and $\gcd(f_{ij}, h) = 1$. This form of the generator is different from the one given in Theorem III.2 but we found it promising. This also suggests that there may be other useful forms for 2-generator QT codes to explore.

V. The New Codes

Implementing the above search methods, we have obtained many new QT codes over $\mathbb{F}_q$, for $q = 2, 3, 4, 5$ and 7 that have the following characteristics:

1) All of these codes are new among the class of QT codes according to the database [10].
2) All of these codes have the the same parameters as BKLCs in [1].
3) In many cases, the BKLCs in the database ([1]) have indirect, multi-step constructions so it is more efficient and desirable to obtain them in the form of QT codes instead. Many of our codes possess this characteristic.
4) A number of our codes have additional desirable properties such as being dual-containing and linear complementary dual (LCD).

TABLE I
New QT Codes with $g = g_1 = g_2$ that are LCD

$[n,k,d]_q$	a, g	$[[f_{11}],...,[f_{1\ell}]],[[f_{21}],...,[f_{2\ell}]]$
$[39, 24, 6]_2$	[11]	[[010010111011], [011000110001], [111011011011]], [[0], [010101110011], [0001011001]]
$[51, 32, 8]_2$	[11]	[[10000101111101], [0111010011000001], [0111000011001101]], [[0], [1101101011010011], [1110001100110101]]
$[87, 56, 10]_2$	[11]	[[00110000011000000101101111001], [1111011111010011011000101101], [0001110001011001111111011111]], [[0], [11100010011101010001010011], [0000110101001001100010110001]]
$[105, 40, 22]_2$	[11]	[[01010101001100101011], [0100110100111010010 1], [11110100001001011], [000011001001010 1111], [1110001000000000100101]], [[0], [00100101110101111001], [1101100001100001], [00110001110101001011], [10000100011011101]]
$[57, 36, 8]_2$	[11]	[[0001010111001110 01], [111010000110111011], [110000101011101 01]], [[0], [01011101101001100 1], [10100010010111111 1]]
$[95, 36, 20]_2$	[11]	[[0111000100000111 1], [010100101011100001], [010111110011000111], [000110110001101011], [00000000000000100001]], [[0], [10101010110101 11], [00001010110111101], [101000000111000101], [10100111110011]]
$[93, 60, 10]_2$	[11]	[[0000101010100100100111100110 01], [000001100100000000100010111001], [11000111011001111111100101]], [[0], [000101000101010010010100011 11], [11111111100010100101001011]]
$[63, 40, 8]_2$	[11]	[[1001010101011001001], [00001011110001010101], [01111001100000111101]], [[0], [0111110110101001100 1], [00100110100011110001]]
$[36, 24, 6]_3$	2, [1]	[[001021111101], [200120211122], [02102100121]], [[0], [012010101221], [110200002221]]

The following tables list the parameters, properties, and generators of these new QT codes. For clarification, g_1 represents the generator polynomial of the main CC code for the first block and g_2 represents the generator polynomial of the main CC code for the second block of the 2-generator QT code. All polynomials are listed by their coefficients for a compact representation. For example, consider the $[39, 24, 6]_2$ code in Table 1 below whose f_{11} is $x^{11}+x^{10}+x^8+x^7+x^6+x^4+x$. Its coefficients are 010010111011 in increasing powers of x from left to right. The block length of a CC code used to generate the QT code, can be inferred from the data. For example, consider the $[39, 24, 6]_2$ code below. Observe that we have $[f_{11}]$,$[f_{12}]$, and $[f_{13}]$ in the last column for $[[f_{11}], \ldots, [f_{1\ell}]]$, which means the index (ℓ) is 3. This implies that the length of the CC code used is $m = \frac{n}{\ell} = \frac{39}{3} = 13$. Also, in the tables below, we indicate the shift constant a of the field only if it is different from 1.

In Table 2 below, we have codes with generators of the form $g_1 = 1$ and $g_2 = pg_1 = p$. So we simply give g_2. The remaining codes are available on pages 8 and 9 in [14], as well as on this page [19] to save space here. They are in the same format as the codes in Tables 1 and 2.

In addition to the additional properties that they posses, many of our new QT codes are better than the BKLCs currently listed in the database [1] for the reason that their constructions are far simpler. A QT code is more desirable than an arbitrary linear code for many reasons. It has a well understood algebraic structure and its generator matrix is

TABLE II
NEW QT CODES WITH $g_1 = 1$ THAT ARE LCD

$[n,k,d]_q$	a, g_2	$[[f_{11}], ..., [f_{1\ell}]], [[f_{21}], ..., [f_{2\ell}]]$
$[12,8,4]_5$	2, [42411]	[[103212], [201242]], [[0], [32]]
$[14,8,5]_5$	[1111111]	[[0213422], [104033]], [[0], [1]]
$[30,16,9]_5$	2, [40101]	[[142420004], [0234333133], [4302024312]], [[0], [013143], [432312]]
$[6,3,4]_5$	[11]	[[4], [21], [21]], [[0], [1], [4]]
$[18,10,6]_5$	2, [211]	[[343214], [320101], [121443]], [[0], [1023], [3014]]
$[45,17,17]_5$	[41]	[[411224401], [143434113], [1103241], [432004303], [202004042]], [[0], [24324023], [041344], [000422], [21112231]]
$[6,4,3]_5$	[111]	[[422], [321]], [[0], [4]]
$[18,8,8]_5$	2, [42411]	[[322144], [24241], [000442]], [[0], [31], [11]]
$[33,12,14]_5$	[11111111111]	[[23232410113], [0340212001], [02404034121]], [[0], [4], [4]]
$[38,20,11]_5$	[1111111111111111111]	[[43320011101304443], [1300410301141140302]], [[0], [1]]
$[12,8,4]_5$	2, [42411]	[[13333], [24401]], [[0], [04]]
$[21,8,10]_5$	[1111111]	[[2244002], [2443132], [3033314]], [[0], [1], [1]]
$[12,3,8]_5$	[11]	[[01], [02], [1], [31], [34], [34]], [[0], [4], [4], [3], [2], [3]]
$[27,10,12]_5$	[111111111]	[[34310241], [23310221], [434403341]], [[0], [3], [1]]
$[30,8,16]_5$	2, [42411]	[[133114], [432411], [243314], [314243], [32331]], [[0], [12], [34], [31], [43]]
$[18,4,12]_5$	[111]	[[232], [03], [342], [301], [031], [4]], [[0], [3], [2], [1], [2], [1]]
$[14,3,10]_5$	[11]	[[04], [24], [13], [1], [2], [04], [43]], [[0], [4], [2], [1], [4], [2], [4]]
$[28,8,15]_5$	[1111111]	[[1213104], [2141001], [1221304], [001221]], [[0], [2], [3], [4]]
$[18,3,13]_5$	[11]	[[4], [42], [24], [04], [12], [3], [12], [31], [01]], [[0], [4], [1], [4], [1], [4], [2], [2], [2]]
$[34,18,10]_5$	[11111111111111111]	[[0212240132442241], [20133301213221021]], [[0], [1]]
$[42,16,16]_5$	2, [4030102040301]	[[4232404223213], [30433103243322], [34024230010143]], [[0], [02], [31]]
$[6,4,3]_7$	[111]	[[332], [456]], [[0], [6]]
$[9,4,5]_7$	[111]	[[332], [456], [613]], [[0], [6], [3]]
$[6,3,4]_7$	[11]	[[42], [05], [15]], [[0], [6], [2]]
$[10,6,4]_7$	[11111]	[[10642], [20425]], [[0], [3]]
$[12,6,6]_7$	6, [141]	[[6265], [6536], [6441]], [[0], [3], [32]]
$[10,3,7]_7$	[11]	[[04], [13], [06], [04], [23]], [[0], [1], [1], [6], [5]]
$[15,6,8]_7$	[11111]	[[11545], [332], [30203]], [[0], [4], [3]]
$[16,6,9]_7$	6, [141]	[[1065], [0533], [1526], [0556]], [[0], [51], [41], [14]]

determined solely by its two rows. In comparison, the BKLCs in [1] with the same parameters often have complicated constructions. For example, we found a $[30, 16, 9]_5$ code that has the same parameters as the comparable BKLC, as well as being LCD. Since it is a QT code, it has a single step construction. The code in the database [1] on the other hand has a 6-step construction to achieve the same parameters and lacks any additional properties. So, in many cases the QC codes we have found have better structures with more desirable properties and with the same parameters as BKLCs.

The codes that have additional properties are given in the tables above. The new codes that are not listed in the tables above are enumerated below. To save space, we do not write down their generators, which are readily available from the authors. Moreover, these codes have been already added to the database along with their generators [10].

$[90,65,8]_2$	$[18,14,3]_4$	$[75,50,8]_2$
$[48,25,10]_2$	$[16,6,8]_4$	$[78,52,8]_2$
$[111,38,24]_2$	$[21,11,7]_4$	$[44,24,11]_5$
$[92,47,14]_2$	$[10,7,3]_5$	$[45,10,24]_5$
$[84,43,14]_2$	$[16,6,8]_5$	$[15,6,8]_5$
$[54,34,8]_2$	$[10,6,4]_5$	$[45,16,18]_5$
$[45,28,8]_2$	$[8,3,5]_5$	$[39,14,16]_5$
$[90,58,10]_2$	$[36,14,14]_5$	$[20,6,12]_7$
$[30,23,4]_3$	$[9,4,5]_5$	$[16,10,5]_7$
$[26,22,3]_3$	$[55,17,23]_5$	$[35,8,21]_7$
$[33,22,6]_3$	$[33,17,10]_5$	$[14,8,6]_7$
$[45,30,7]_3$	$[38,28,6]_5$	$[18,10,7]_7$
$[12,4,7]_4$	$[45,30,6]_2$	
$[26,20,4]_4$	$[102,68,10]_2$	

VI. NEW RECORD BREAKING BINARY LINEAR CODES

Using the search method described in section 4.2, we were able to obtain a record-breaking 2-generator binary QT code with a minimum distance higher than the BKLC of the same length and dimension over $GF(2)$ given in [1]. Using a compact representation similar to the codes given in the earlier tables, the generators of this $[111, 38, 25]_2$-code are as follows:

$g_1 = 1$

$g_2 = [11111111111111111111111111111111111111]$

$f_{11} = [00111111111100011001101111111000010011]$

$f_{12} = [011110110111110011011010101100100111]$

$f_{13} = [1111100000100000001010001010111000101]$

$f_{21} = 0, \qquad f_{22} = 1 \qquad f_{23} = 1$

Moreover, applying the standard method of extending this code, we obtain another record-breaking linear code with parameters $[112, 38, 26]_2$.

REFERENCES

[1] M. Grassl, Code Tables: Bounds on the parameters of of codes, online,http://www.codetables.de/

[2] N. Aydin, I. Siap, and D. Ray-Chaudhuri, ”The structure of 1-generator quasi-twisted codes and new linear codes,” Des. Codes, Cryptogr. , vol. 24, 2001, pp. 313-326.

[3] N. Aydin, J. Lambrinos, and O. VandenBerg, “On equivalence of cyclic codes, generalization of a quasi-twisted search algorithm, and new linear codes,” Des. Codes, Cryptogr., vol. 87, no. 10, 2019, pp. 2199–2212.

[4] N. Aydin and I. Siap, “New quasi-cyclic codes over $\mathbb{F}_5$,” Appl. Math. Lett., vol. 15, no. 7, 2002, pp. 833–836.

[5] R. Daskalov and P. Hristov, “New quasi-twisted degenerate ternary linear codes,” IEEE Trans. Inf. Theory, vol. 49, no. 9, 2008, pp. 2259–2263.

[6] R. Ackerman and N. Aydin, “New quinary linear codes from quasi-twisted codes and their duals,” Appl. Math. Lett., vol. 24, no. 4, 2011, pp. 512–515.

[7] R. Daskalov, and P. Hristov, “Some new quasi-twisted ternary linear codes,” J. Algebra Comb. Discrete Struct. Appl., vol. 2, no. 3, 2015.

[8] T. A. Gulliver, and V. K. Bhargava, “Two new rate $2/p$ binary quasi-cyclic codes,” IEEE Trans. Inf. Theory, vol. 40, no. 5, 1994, pp. 1667–1668.

[9] E. Z. Chen, “An explicit construction of 2-generator quasi-twisted codes,” IEEE Trans. Inf. Theory, vol. 54, no. 12, 2008, pp. 5770–5773.

[10] E. Z. Chen, Quasi-Cyclic Codes: Bounds on the parameters of of QC codes, online, http://www.tec.hkr.se/~chen/research/codes/qc.htm

[11] Magma computer algebra system, online, http://magma.maths.usyd.edu.au/

[12] N. Aydin, and R. O. VandenBerg, “A new algorithm for equivalence of cyclic codes and its applications,” Appl. Algebra Eng. Commun., 2021, https://doi.org/10.1007/s00200-021-00525-4

[13] D. Akre, N. Aydin, M. J. Harrington, and S. R. Pandey, “A generalization of cyclic code equivalence algorithm to constacyclic codes,” arxiv preprint, https://arxiv.org/abs/2108.08619, 2021.

[14] D. Akre, N. Aydin, M. J. Harrington, and S. R. Pandey, “A Generalization of the ASR Search Algorithm to 2-Generator Quasi-Twisted Codes,” arxiv preprint, https://arxiv.org/abs/2108.10316, 2021.

[15] R. Daskalov, and P. Hristov, “Some new ternary linear codes,” J. Algebra Comb. Discrete Struct. Appl., 2017, pp. 227–227.

[16] N. Aydin, T. H. Guidotti, P. Liu, A. S. Shaikh, and R. O. VandenBerg, “Some generalizations of the ASR search algorithm for quasi-twisted codes,” Involve, vol. 13, no. 1, 2020, pp. 137–148.

[17] N. Aydin, N. Connolly, and M. Grassl, “Some results on the structure of constacyclic codes and new linear codes over GF(7) from quasi-twisted codes,” Adv. Math. Commun., vol. 11, no. 1, 2017, pp. 245–258.

[18] A. Vardy, “The intractability of computing the minimum distance of a code,” IEEE Trans. Inf. Theory, vol. 43, no. 6, 1997, pp. 1757–1766.

[19] D. Akre, N. Aydin, M. J. Harrington, and S. R. Pandey, Tables of new QT codes continued, online, https://www2.kenyon.edu/Depts/Math/Aydin/ExtraCodeTables.pdf, 2021.

[20] M. Shi, and Z. Yiping, “Quasi-twisted codes with constacyclic constituent codes,” Finite Fields Appl. vol.39, pp. 159-178, May 2016.