involve
a journal of mathematics

Some generalizations of the ASR search algorithm for quasitwisted codes

Nuh Aydin, Thomas H. Guidotti, Peihan Liu,
Armiya S. Shaikh and Robert O. VandenBerg

msp

2020 vol. 13, no. 1

INVOLVE 13:1 (2020)
dx.doi.org/10.2140/involve.2020.13.137

Some generalizations of the ASR search algorithm for quasitwisted codes

Nuh Aydin, Thomas H. Guidotti, Peihan Liu,
Armiya S. Shaikh and Robert O. VandenBerg

(Communicated by Kenneth S. Berenhaut)

One of the most important and challenging problems in coding theory is explicit construction of linear codes with the best possible parameters. It is well known that the class of quasitwisted (QT) codes is asymptotically good and contains many linear codes with best known parameters (BKLCs). A search algorithm (ASR) on QT codes has been particularly effective to construct such codes. Recently, the ASR algorithm was generalized based on the notion of code equivalence. In this work, we introduce a new generalization of the ASR algorithm to include a broader scope of QT codes. As a result of implementing this algorithm, we have found eight new linear codes over the field $\mathbb{F}_5$. Furthermore, we have found seven additional new codes from the standard constructions of puncturing, shortening or Construction X. We also introduce a new search algorithm that can be viewed as a further generalization of ASR into the class multitwisted (MT) codes. Using this method, we have found many codes with best known parameters with more direct and desirable constructions than what is currently available in the database of BKLCs.

1. Introduction

A linear code C of length n over a finite field $\mathbb{F}_q$ is a vector subspace of $\mathbb{F}_q^n$ with three basic parameters: the length n, the dimension k, and the minimum (Hamming) distance/weight d. Such a code is referred to as an $[n, k, d]_q$ code. Given an alphabet $\mathbb{F}_q$, a length n, and a dimension k, a key problem in coding theory is to construct a code with the highest possible minimum distance $d_q(n, k)$. There are theoretical upper bounds on $d_q(n, k)$, but upper bounds usually do not give a way of constructing codes and it is not guaranteed that they may be attained. Determining $d_q(n, k)$ with an explicit construction of a code attaining it is a challenging problem with many instances that are open. There are databases which keep records of the best known linear codes (BKLC), providing information about upper and lower

MSC2010: 94B15, 94B60.
Keywords: quasitwisted codes, multitwisted codes, best known linear codes, ASR search algorithm.

bounds, and their constructions. One of the databases is maintained by M. Grassl [2019] and another is available within the Magma software.[1] Both of these databases cover information about BKLCs over finite fields $\mathbb{F}_q$ for $q = 2, 3, 4, 5, 7, 8, 9$ up to a certain value of n for each alphabet.

Computers are very useful in searching for new codes with best possible parameters. The two main challenges in this search come from the fact that computing the minimum distance of a linear code is NP-hard [Vardy 1997] and the number of linear codes for a given length n and dimension k grows very fast. Therefore, exhaustive searches for arbitrary linear codes are not possible for all but small parameters. In order to combat these computational challenges, researchers choose to focus on certain classes of codes that have ample mathematical structure and are known to contain many good codes. One well-known example of such a class of codes is the class of quasitwisted (QT) codes, which are a generalization of cyclic, constacyclic, and quasicyclic (QC) codes. For the last several decades, hundreds of new linear codes have been found by computer searches from the class of QC and QT codes; see, e.g., [Chen 1994; Daskalov and Gulliver 2000; Gulliver and Bhargava 1996]. In particular, a specific search algorithm called ASR [Aydin et al. 2001] on 1-generator QT codes has been effective in discovering record-breaking codes; see, e.g., [Daskalov and Hristov 2003a; 2003b; 2004; Aydin and Siap 2002]. The ASR algorithm searches for QT codes with generator polynomials of the form

$$(g(x), f_2(x)g(x), f_3(x)g(x), \ldots, f_\ell(x)g(x)), \tag{1}$$

where ℓ is the number of blocks in the QT code and each $f_i(x) \in \mathbb{F}_q[x]$ has degree less than $k = m - \deg(g(x))$ and is relatively prime with $h(x)$, where $h(x)$ is the check polynomial of the constacyclic code generated by $g(x)$, that is, $x^m - a = g(x)h(x)$ [Aydin et al. 2001]. Such a code is a 1-generator QT code of index ℓ with parameters $[m\ell, k, \geq d\ell]$, if the constacyclic code generated by $g(x)$ has parameters $[m, k, d]$.

We have two main contributions to this research. Our first contribution is to generalize this search algorithm to generate 1-generator QT codes with generators of the form $(f_1(x)g_1(x), f_2(x)g_2(x), \ldots, f_\ell(x)g_\ell(x))$, where polynomials $g_i(x)$ generate nonequivalent constacyclic codes with length m and dimension k, and each of the scrambling polynomials $f_i(x)$ fulfills the conditions $\gcd(h_i(x), f_i(x)) = 1$ and $\deg(f_i(x)) < k$. If there are ℓ blocks and r generators for a specific m and k, then there are $\binom{\ell+r-1}{r-1}$ possible combinations of generator polynomials.[2] Meaning, for a given m, k, and ℓ we have $\binom{\ell+r-1}{r-1}$ different searches. This generalized search

[1] http://magma.maths.usyd.edu.au/magma/

[2] This follows from the following well-known formula from combinatorics: the number of distinct nonnegative integer-valued vectors $(x_1, x_2, \ldots, x_k)$ satisfying $x_1 + x_2 + \cdots + x_k = n$ is $\binom{n+k-1}{n}$, which is the same as $\binom{n+k-1}{k-1}$. In our situation, we take $k = r$ and $n = \ell$.

algorithm builds upon the work of previous researchers who generalized the search by partitioning generator polynomials using code equivalence [Aydin et al. 2019]. Our second contribution is to introduce a new search algorithm to find linear codes with generator matrices of the form $[I_k, C]$, where I_k is the $k \times k$ identity matrix over $\mathbb{F}_q$ and C is a circulant matrix corresponding to the generator of a constacyclic code of length $n-k$.

We first give some basic information on the structure of cyclic and QT codes, and the background of our generalized and new search methods. We then discuss some implementation details regarding both methods. Finally, we present new codes and their generators. We used Magma software along with C++ programs in executing our search algorithms.

2. Basic definitions

Cyclic codes are an important class of codes that connect coding theory to algebra [Prange 1957; 1958]. A cyclic code C is a linear code that is closed under the cyclic shift operation, meaning that if $c = (c_0, c_1, \ldots, c_{n-1})$ is a codeword then $\pi(c) = (c_{n-1}, c_0, \ldots, c_{n-2})$ must be as well. Representing a codeword $c = (c_0, c_1, \ldots, c_{n-1})$ as the polynomial $c(x) = c_o + c_1 x + \cdots + c_{n-1}x^{n-1}$ is the basis of the link between coding theory and algebra. It is well known that cyclic codes of length n over $\mathbb{F}_q$ are precisely ideals in the quotient ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$, which is a principal ideal ring. There is a one-to-one correspondence between divisors of $x^n - 1$ over $\mathbb{F}_q[x]$ and cyclic codes of length n over $\mathbb{F}_q$. Every cyclic code C has a unique standard generator polynomial $g(x)$ that divides $x^n - 1$. If we write $x^n - 1 = g(x)h(x)$ then the dimension of C is $\deg(h(x)) = n - \deg(g(x))$, and $h(x)$ is called the check polynomial of C.

An important generalization of cyclic codes is the class of constacyclic codes. A linear code C is called a constacyclic code if it is closed under the constacyclic shift operator π_a, where $a \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. This means if c is a codeword then so is $\pi_a(c) = (ac_{n-1}, c_0, \ldots, c_{n-2})$. Note that, the case $a = 1$ gives the cyclic codes. Similarly to cyclic codes, every constacyclic code C has a standard generator polynomial $g(x)$ that divides $x^n - a$. Any other generator of $C = \langle g(x)\rangle$ has the form $g(x)f(x)$, where $\gcd(g(x), h(x)) = 1$. Algebraically, constacyclic codes of length n over $\mathbb{F}_q$ with shift constant a are precisely the ideals in $\mathbb{F}_q[x]/\langle x^n - a\rangle$. Given a generator $p(x) = p_0 + p_1 x + \cdots + p_{n-1}x^{n-1}$ of a constacyclic code, it has a generator matrix of the form

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

Such a matrix is called an a-circulant matrix (also called a twistulant matrix). The special case $a = 1$ gives us the class of cyclic codes and its circulant matrices. We obtain quasicyclic (QC) and quasitwisted (QT) codes as further generalizations of cyclic and constacyclic codes.

A quasitwisted code is closed under a constacyclic shift by more than one position. A linear code C is said to be ℓ-QT (or a QT code of index ℓ) if for a positive integer ℓ, whenever $(c_0, c_1, \ldots, c_{n-1}) \in C$, then $(ac_{n-\ell}, \ldots, ac_{n-1}, c_0, c_1, \ldots, c_{n-\ell-1}) \in C$. If we take $a = 1$, then we have the class of QC codes. Thus the class of QT codes is a generalization of QC codes. A generator matrix of an r-generator QT code has the form

$$\begin{bmatrix} G_{11} & G_{12} & \cdots & G_{1l} \\ G_{21} & G_{22} & \cdots & G_{2l} \\ \vdots & \vdots & & \vdots \\ G_{r1} & G_{r2} & \cdots & G_{rl} \end{bmatrix},$$

where each G_{ij} is a circulant matrix corresponding to a constacyclic code [Aydin et al. 2001]. Thus we can think of QT codes as codes made up of "blocks" of constacyclic codes. Throughout this paper we will be working with 1-generator QT codes, that is, codes whose generator matrices have the form

$$[G_1 \;\; G_2 \;\; \cdots \;\; G_l].$$

A QT code of length $n = m\ell$ and index ℓ is an R-submodule of R^ℓ, where $R = \mathbb{F}_q[x]/\langle x^m - a\rangle$.

Multitwisted (MT) codes are a more recent generalization of QT codes [Aydin and Halilović 2017]. A linear code C is multitwisted if for any codeword

$$\vec{c} = (c_{1,0}, \ldots, c_{1,m_1-1}; c_{2,0}, \ldots, c_{2,m_2-1}; \cdots ; c_{\ell,0}, \ldots, c_{\ell,m_\ell-1}) \in C$$

its MT shift

$$(a_1 c_{1,m_1-1}, c_{1,0}, \ldots, c_{1,m_1-2}; a_2 c_{2,m_2-1}, c_{2,0}, \ldots, c_{2,m_2-2}; \cdots ; a_\ell c_{\ell,m_\ell-1}, \ldots, c_{\ell,m_\ell-2})$$

is also a codeword, where $a_1, a_2, \ldots, a_\ell \in \mathbb{F}_q^*$. Under the usual representation of a codeword $\vec{c}$ as the corresponding polynomial (in this case a tuple of polynomials) $C(x) = (c_1(x), c_2(x), \ldots, c_\ell(x))$, where $c_i(x) = c_{i,0} + c_{i,1}x + \cdots + c_{i,m_i-1}x^{m_i-1}$, we observe that the MT shift corresponds to the operation

$$xC(x) = (xc_1(x) \bmod x^{m_1} - a_1, \ldots, xc_l(x) \bmod x^{m_l} - a_l)$$

in the ring

$$V = \prod_{i=1}^{\ell} \mathbb{F}_q[x]/\langle x^{m_i} - a_i\rangle,$$

where $a_i \in \mathbb{F}_q^*$ and m_i are (possibly distinct) positive integers.

3. A new generalization of the ASR algorithm

Recently, a generalization of the ASR algorithm was introduced in [Aydin et al. 2019] that made the algorithm more comprehensive based on the notion of code equivalence. Given a block length m, dimension k, alphabet size q and shift constant $a \in \mathbb{F}_q^*$, the original ASR algorithm used a code of largest minimum weight among all constacyclic codes of length m and dimension k over $\mathbb{F}_q$ as the building block of a QT code with a generator of the form (1) (in the case of multiple such codes, one was arbitrarily chosen). Each such generator $g(x)$ is a divisor of $x^m - a$, with check polynomial $h(x)$, i.e., $x^m - a = g(x)h(x)$. The generalization introduced in [Aydin et al. 2019] first partitions all constacyclic codes of length m and dimension k over $\mathbb{F}_q$ into equivalence classes. It keeps the (standard) generator of one code for each equivalence class, and uses each one of these polynomials as the building block of a QT search. As a result of this more comprehensive approach, a number new codes were found in [Aydin et al. 2019] that would have been missed by the original algorithm.

Past researchers have written Magma code that outputs generator polynomials for all nonequivalent cyclic and constacyclic codes for a fixed n over a finite field $\mathbb{F}_q$ using cyclotomic cosets [Aydin et al. 2019]. Our first step in generalizing their search method was to take the list of nonequivalent generators and sort them by degree. The end result of the program is a set of text files each containing generator polynomials of a fixed degree.

In the past, researchers have automated the process of searching for new QT codes. They wrote C++ programs that take in the list of nonequivalent generator polynomials and generate Magma code in output files, and then they wrote a runner script that is able to run all of the Magma files simultaneously with one command. In order to consider all $\binom{\ell+r-1}{r-1}$ possible combinations of the distinct generator polynomials, we made significant changes to this program. To accomplish this we wrote a function that runs through each number $1, \ldots, (\ell+1)^r$ and converts it to a number base $\ell+1$. To give a concrete example, if we have $\ell = 2$ and $r = 6$, the decimal number 10 will be represented in base 3 as 000101. We interpret this number in base $\ell + 1$ as the number of times each of the r generators appear. In this instance, this means that g_4 and g_6 will appear as the generators of the QT code. In order for this number in base $\ell + 1$ to be a valid combination of generator polynomials, it is clear that the components must sum to the number of blocks. Further, this method avoids equivalent codes because each number in base $\ell+1$ represents a unique combination of the r generator polynomials.

Our further generalization of the algorithm in [Aydin et al. 2019] does not require the generator polynomial $g(x)$ in (1) to be the same. Instead, we consider QT codes with generators of the form

$$(f_1(x)g_1(x),\ f_2(x)g_2(x),\ \ldots,\ f_\ell(x)g_\ell(x)),$$

where each $g_i(x)$ is the standard generator of a constacyclic code of length m and dimension k, hence a divisor of $x^m - a$, for distinct equivalence classes. After storing the generator polynomials in an array, for each $g_i(x)$ we generate a random polynomial f_i over $\mathbb{F}_q$ of degree $< k$ such that $\gcd(f_i(x), h_i(x)) = 1$. For each fixed set of polynomials $(g_1(x), g_2(x), \ldots, g_\ell(x))$, we generate a large number of codes, where the $f_i(x)$ vary (generated by computer), with a generator of the form $(f_1(x)g_1(x), f_2(x)g_2(x), \ldots, f_\ell(x)g_\ell(x))$.

For such a code the dimension is equal to $m - \deg(\gcd(g_1(x), g_2(x), \ldots, g_\ell(x)))$. Since $\deg(\gcd(g_1(x), g_2(x), \ldots, g_\ell(x))) \leq \deg(g_1(x))$, it is often the case that $m - \deg(\gcd(g_1(x), g_2(x), \ldots, g_l(x))) > m - \deg(g_1(x))$. As such, truncating the generator matrix so that it has $m - \deg(g_1(x))$ rows often produces a code with higher minimum distance.

Note that when $g_1(x) = g_2(x) = \cdots = g_\ell(x) = g(x)$, we obtain the form of the generator given by the algorithm ASR that has been used in previous searches and produced a large number of record-breaking codes over many alphabets. Hence, our method is more general. In the implementation of the ASR algorithm, the polynomial $f_1(x)$ is often taken to be 1, meaning codes are obtained by generators of the form $(g(x), f_2(x)g(x), \ldots, f_\ell(x)g(x))$. We observe however that this may cause the search to miss some codes with potentially higher minimum distances. We illustrate this by a concrete example for $\ell = 2$.

Let S be the set of all polynomials of degree $< k$ over $\mathbb{F}_q$ that are relatively prime with the check polynomial $h(x)$. If $\ell = 2$ and $f_1(x) = 1$, then the size of the search space is $|S|$. If we do not make the simplification $f_1(x) = 1$, then the size of the search space is increased to $|S|^2$. The computational cost in the increased size of the search space comes with a benefit, however. Through exhaustive computer search, we found that it is not possible to obtain every code of the form $(g(x)f_1(x), g(x)f_2(x))$ (or its equivalent) as a code of the form $(g(x), g(x)p(x))$. In particular, we have found cases in which an identical $g(x)$ can generate a code with a higher minimum distance if the generator is in the form $(g(x)f_1(x), g(x)f_2(x))$ as opposed to the form $(g(x), g(x)p(x))$. One such example is over $\mathbb{F}_3$. If we take $g(x) = x^9 + x^7 + x + 1$, $n = 14$, $\ell = 2$, and $a = 1$, the QC code generated by $(g(x)f_1(x), g(x)f_2(x))$, where $f_1(x) = x^2 + 2x + 2$ and $f_2(x) = x^5 + 2x^3 + x + 1$ has minimum distance 16. On the other hand, the largest minimum distance of any QC code with a generator of the form $(g(x), f(x)g(x))$ is 14. Because of this oversight in the previous searches, we reran the usual ASR algorithm with $f_1(x)$ not fixed to 1. We obtained several new linear codes that are QC with this search. They are listed in Table 1 below.

In addition to trying cases where the degrees of the generator polynomials are equal, we also tried cases where the degrees are not equal. Say that we are working with $\ell = 2$ and we have $m - \deg(g_1(x)) = k_1$ and $m - \deg(g_2(x)) = k_2$, where

$k_1 < k_2$. In such a case it is clear that the left-hand block, corresponding to the $k_1 - 1$ constacyclic shifts of $g_1(x)$, will have fewer linearly independent rows than the right-hand block. In this case, without truncating we will have the dimension $m - \deg(\gcd(g_1(x), g_2(x)))$. In general this is greater than k_1 or k_2, so the first block will have a number of rows that are linearly dependent. As a result when we row reduce the generator matrix there will be extra rows of zeros, which is detrimental to the minimum distance of the code. In order to avoid this issue, we ran a search in which the blocks are truncated to $k = \min(k_1, k_2)$. With this method, we found codes whose minimum distances are within 2 units of the BKLCs.

4. A new search algorithm: ICY

It is well known that every linear code has an equivalent linear code with a generator matrix of the form $G = [I_k \mid A]$, where I_k is the $k \times k$ identity matrix and A is a $k \times n - k$ matrix. This is known as the standard form of G. Our new search method is motivated by this fact as well as the form of the generator matrices of 1-generator MT codes. It combines these two forms. Consider linear codes with generator matrices of the form $G = [I_k \mid C_p]$, where C_p is the circulant generator matrix of a constacyclic code of length $n - k$ and dimension k defined by a generator polynomial (not necessarily the standard generator polynomial) $p(x) = p_0 + p_1 x + \cdots + p_{n-k-1}x^{n-k-1}$,

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

where each row is the constacyclic shift of the row above it.

We can view such a code as a 1-generator MT code generated by $(1, p(x))$, where each component is a constacyclic code of length k and $n - k$ respectively. We modify the algorithm ASR to search for 1-generator MT codes with generators of the form $(1, g(x)f(x))$, where $g(x)$ is the standard generator of a constacyclic code of length $n - k$ with shift constant a, $x^m - a = g(x)h(x)$, and $f(x)$ is coprime with $h(x)$. We impose one further condition on $f(x)$. Since we fix k and n in advance, we know the minimum weight, d_{tar} of BKLC of length n and dimension k. In order for a code with generator of the form $(1, g(x)f(x))$ to have a greater minimum weight than the BKLC, it is necessary that the weight of the polynomial $f(x)g(x)$ be $\geq d_{\text{tar}}$. Without fulfilling this condition the resulting code would definitely have a minimum distance $\leq d_{\text{tar}}$. Our search uses the previous partition program from [Aydin et al. 2019] in Magma to find all nonequivalent generator polynomials (divisors of $x^m - a$) using cyclotomic cosets. Then, we

	$[n, k, d]_q$	α	polynomials
1	$[36, 14, 15]_5$	1	$g = [14014]$, $f_1 = [40041120014234]$, $f_2 = [41304123120031]$
2	$[42, 19, 15]_5$	1	$g = [111]$, $f_1 = [2103021100133]$, $f_2 = [404410144313]$
3	$[42, 13, 20]_5$	1	$g = [123333321]$, $f_1 = [2103021100133]$, $f_2 = [404410144313]$
4	$[56, 19, 23]_5$	1	$g = [1123421123]$, $f_1 = [2024244022144132123]$, $f_2 = [2141002343343311431]$
5	$[66, 16, 33]_5$	1	$g = [142141404012120124]$, $f_1 = [3442111233311333]$, $f_2 = [1313324003444113]$
6	$[66, 15, 34]_5$	1	$g = [13343231411141311121]$, $f_1 = [212410113224012]$, $f_2 = [230103303344443]$
7	$[76, 20, 35]_5$	1	$g = [1413203213422033444]$, $f_1 = [23433002000100243 41]$, $f_2 = [323403213212002334 21]$
8	$[76, 18, 37]_5$	1	$g = [1404121231343313110 11]$, $f_1 = [201430342434231303]$, $f_2 = [1234434132043004 24]$

Table 1. Record breaking QT codes.

run a C++ program that generates a search in Magma for each distinct generator polynomial along with a runner script.

We call this search method "ICY" from the form of the generator matrix $[I, C]$. The following result is a special case of Theorem 5.3 in [Aydin and Halilović 2017] and gives a lower bound on the minimum weight of codes generated by the ICY method.

Proposition 1. *Let $a \in \mathbb{F}_q^*$, $n \in \mathbb{Z}^+$, be such that $x^n - a = g(x)h(x)$, with $k = \deg(h(x))$. Let $C_2 = \langle g(x) \rangle$ be a constacyclic code with shift constant a and parameters $[n, k, d_2]$, with generator matrix G_2. Let $G = [I_k, G_2]$. Then the MT code generated by G has parameters $[n + k, k, d]$, where $d \geq d_2 + 1$.*

	$[n, k, d]_q$	method
1	$[41, 18, 15]_5$	shortening of $[42, 19, 15]_5$ by coordinate 1
2	$[55, 18, 23]_5$	shortening of $[56, 19, 23]_5$ by coordinate 1
3	$[65, 16, 32]_5$	puncturing of $[66, 16, 33]_5$ by coordinate 1
4	$[65, 15, 33]_5$	shortening of $[66, 16, 33]_5$ by coordinate 1
5	$[75, 20, 34]_5$	puncturing of $[76, 20, 35]_5$ by coordinate 1
6	$[75, 17, 37]_5$	shortening of $[76, 18, 37]_5$ by coordinate 1
7	$[80, 20, 37]_5$ ⋆	applying Construction X to $[76, 20, 34]_5$ and $[76, 18, 37]_5$ along with a $[4, 2, 3]$-code

Table 2. Additional new codes; the starred construction is due to Grassl [2019].

Using this method have found many codes with the same parameters as the BKLCs over $\mathbb{F}_2$ and $\mathbb{F}_5$. One such example is a code with parameters $[44, 14, 19]_5$ with shift constant $a = 2$,

$$g(x) = x^{16} + 4x^{15} + 4x^{14} + 3x^{13} + 3x^{12} + 2x^{11} + 2x^{10} + 2x^9 + 3x^8 + 2x^7 + 2x^6 + 2x^5 + 3x^4 + 3x^3 + 4x^2 + 4x + 1,$$

$$f(x) = 3x^{13} + 3x^{11} + 2x^{10} + 4x^9 + 2x^8 + 3x^6 + 4x^5 + 4x^4 + 4x^2 + 4x + 3.$$

The constacyclic code generated by $g(x)$ has parameters $[30, 14, 5]_5$, so the minimum distance of the resulting $[I, C]$ code is far greater than $d_2 + 1$. Furthermore, this code has a much simpler and more elegant construction than the current BKLC given in [Grassl 2019]. Moreover, according to the database of QC and QT codes, there does not exist a QT code with these parameters over $\mathbb{F}_5$. Although this code is MT, not QT, its structure is very close to the structure of a QT code. The fact that this code has the parameters of BKLC with a more desirable and simpler construction, as well as having better parameters than known QT codes makes it an excellent code. We have found a number of similar codes. They are listed in Table 3 below.

5. Multitwisted searches

Multitwisted (MT) codes [Aydin and Halilović 2017] are a recent generalization of QT codes, which also generalize previously introduced classes of double cyclic codes [Borges et al. 2018; Gao et al. 2016], QCT codes [Aydin et al. 2007], and GQC codes [Siap and Kulhan 2005]. We conducted a computer search based on Theorem 5.7 from [Aydin and Halilović 2017] and our earlier algorithms.

We fix n_2 and a_2 over a given finite field $\mathbb{F}_q$. Our cyclic partition program gives all nonequivalent generators $g(x)$ (divisors of $x^{n_2} - a_2$). Then we sort all polynomials by degree. Once we have all of the generators sorted by degree we loop through many values of $k = n_1$. We chose $10 \le n_1 \le n_2 - 5$. For each n_1 we

	$[n,k,d]_q$	ℓ	α	polynomials
1	$[49,19,12]_2$ ⋆	2	1	$g=[100100101101]$, $f=[1101101001010100101]$
2	$[50,20,12]_2$	2	1	$g=[11100011011]$, $f=[1101011111000111111]$
3	$[51,21,12]_2$ ⋆	2	1	$g=[1100001111]$, $f=[1011110001000111]$
4	$[52,22,12]_2$ ⋆	2	1	$g=[100000101]$, $f=[1000111111110110101]$
5	$[55,25,12]_2$ ⋆	2	1	$g=[11111]$, $f=[1101111101001001001011101]$
6	$[67,25,16]_2$ ⋆	2	1	$g=[111110011000100001]$, $f=[1110011111011010111011]$
7	$[68,26,16]_2$	2	1	$g=[110100001011101101]$, $f=[1100100101100111111010111]$
8	$[69,27,16]_2$ ⋆	2	1	$g=[1001011110111011]$, $f=[1110100010001000101011011 1]$
9	$[96,36,20]_2$ ⋆	2	1	$g=[1101001001001011110010101]$, $f=[1100001001111101000011101000011 0101]$
10	$[98,38,20]_2$ ⋆	2	1	$g=[1000011110100111111 0111]$, $f=[1000110000100000001010010111110001]$
11	$[109,47,20]_2$ ⋆	2	1	$g=[1011101000110101]$, $f=[1001110110111010101101000101000001 1100001]$
12	$[87,24,24]_2$ ⋆	2	1	$g=[1010001010010010000101011110000100001001]$, $f=[101011110010111001100 01]$
13	$[88,25,24]_2$ ⋆	2	1	$g=[1100101100000010110010100010111100110 11]$, $f=[1100001110000111101000001]$
14	$[45,18,16]_5$	2	2	$g=[1000000004]$, $f=[1330111202203403 41]$
15	$[44,14,19]_5$ ⋆	2	2	$g=[144332223223234 41]$, $f=[30324203440443]$

Table 3. Good codes from ICY method. Here the star denotes a code with better parameters than those in the online database of QT codes [Chen].

find all generator polynomials of degree $n_2 - n_1$ and create a search program for each. We also loop through all $a \in \mathbb{F}_q^*$ of distinct orders. We chose these bounds to limit the search space to a manageable size.

Our search produced a number of ties for BKLCs over $\mathbb{F}_5$ and $\mathbb{F}_2$. One such example is the code with parameters $[51, 17, 21]_5$, where

$$n_1 = 17, \quad n_2 = 34, \quad a_1 = 4, \quad a_2 = 1, \quad g(x) = x^{17} + 4,$$
$$\begin{aligned} f_1(x) = {} & 2x^{16} + 2x^{15} + 4x^{14} + 2x^{13} + 3x^{12} + 2x^{11} \\ & + 2x^{10} + 2x^9 + 2x^8 + 2x^7 + 3x^6 + 4x^5 + 2x^4 + 4x^3 + 2x^2 + 1, \\ f_2(x) = {} & x^{16} + 4x^{15} + x^{14} + 2x^{13} + 4x^{12} + 2x^{11} + 2x^{10} \\ & + 2x^9 + 2x^8 + x^7 + 2x^6 + 4x^5 + 3x^4 + 4x^3 + 2x^2 + x + 1. \end{aligned}$$

While our tie is an equally similar construction to the one recorded in the database [Grassl 2019], we have found a number of ties with simpler constructions. One such code has the parameters $[44, 16, 17]_5$, where

$$n_2 = 28, \quad n_1 = 16, \quad a_2 = 1, \quad a_1 = 1,$$
$$\begin{aligned} g(x) = {} & 2x^{27}+x^{26}+3x^{25}+3x^{24}+4x^{23}+2x^{21}+4x^{19}+3x^{18}+4x^{17}+4x^{16}+4x^{15} \\ & +3x^{14}+3x^{13}+3x^{12}+3x^{11}+3x^9+2x^8+3x^7+4x^6+3x^5+3x^4+3x^3+x^2+x, \\ f_1(x) = {} & 2x^{15}+2x^{14}+2x^{12}+2x^{11}+4x^{10}+3x^9+3x^8+3x^4+4x^3+x^2+4x+4, \\ f_2(x) = {} & 2x^{15}+4x^{14}+4x^{13}+2x^{12}+x^{11}+4x^{10}+3x^9+2x^7+x^6+x^4+2x^3+x^2+x. \end{aligned}$$

6. Computational results

First, we present our new record-breaking codes from the QT search in Table 1. We present the polynomials with the highest-degree coefficients on the left. Each of these codes has $\ell = 2$. Table 2 gives new codes obtained from these QT codes through the standard procedures of shortening and puncturing. Finally, in Table 3 we present codes that have the parameters of the BKLCs but with simpler and more desirable constructions obtained by the ICY method. Most of these codes have better parameters than the codes in the database of QC and QT codes [Chen]. Each such code is marked with a $\star$.

Acknowledgement

This work was supported by Kenyon Summer Science Scholars program.

References

[Aydin and Halilović 2017] N. Aydin and A. Halilović, "A generalization of quasi-twisted codes: multi-twisted codes", *Finite Fields Appl.* **45** (2017), 96–106. MR Zbl

[Aydin and Siap 2002] N. Aydin and I. Siap, "New quasi-cyclic codes over $\mathbb{F}_5$", *Appl. Math. Lett.* **15**:7 (2002), 833–836. MR Zbl

[Aydin et al. 2001] N. Aydin, I. Siap, and D. K. Ray-Chaudhuri, "The structure of 1-generator quasi-twisted codes and new linear codes", *Des. Codes Cryptogr.* **24**:3 (2001), 313–326. MR Zbl

[Aydin et al. 2007] N. Aydin, T. Asamov, and T. A. Gulliver, "Some open problems on quasi-twisted and related code constructions and good quaternary codes", pp. 856–860 in *Proceedings of the 2007 IEEE International Symposium on Information Theory* (Nice, France, 2007), IEEE, Piscataway, NJ, 2007.

[Aydin et al. 2019] 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.* **87**:10 (2019), 2199–2212. MR Zbl

[Borges et al. 2018] J. Borges, C. Fernández-Córdoba, and R. Ten-Valls, "$\mathbb{Z}_2$-double cyclic codes", *Des. Codes Cryptogr.* **86**:3 (2018), 463–479. MR Zbl

[Chen 1994] Z. Chen, "Six new binary quasi-cyclic codes", *IEEE Trans. Inform. Theory* **40**:5 (1994), 1666–1667. MR Zbl

[Chen] E. Chen, "Online database of quasi-twisted codes", website, http://www.tec.hkr.se/~chen/research/codes/.

[Daskalov and Gulliver 2000] R. N. Daskalov and T. A. Gulliver, "New quasi-twisted quaternary linear codes", *IEEE Trans. Inform. Theory* **46**:7 (2000), 2642–2643. MR Zbl

[Daskalov and Hristov 2003a] R. Daskalov and P. Hristov, "New binary one-generator quasi-cyclic codes", *IEEE Trans. Inform. Theory* **49**:11 (2003), 3001–3005. MR Zbl

[Daskalov and Hristov 2003b] R. Daskalov and P. Hristov, "New quasi-twisted degenerate ternary linear codes", *IEEE Trans. Inform. Theory* **49**:9 (2003), 2259–2263. MR Zbl

[Daskalov et al. 2004] R. Daskalov, P. Hristov, and E. Metodieva, "New minimum distance bounds for linear codes over GF(5)", *Discrete Math.* **275**:1-3 (2004), 97–110. MR Zbl

[Gao et al. 2016] J. Gao, M. Shi, T. Wu, and F.-W. Fu, "On double cyclic codes over $\mathbb{Z}_4$", *Finite Fields Appl.* **39** (2016), 233–250. MR Zbl

[Grassl 2019] M. Grassl, "Code tables: bounds on the parameters of various types of codes", website, 2019, http://www.codetables.de/.

[Gulliver and Bhargava 1996] T. A. Gulliver and V. K. Bhargava, "New good rate $(m-1)/pm$ ternary and quaternary quasi-cyclic codes", *Des. Codes Cryptogr.* **7**:3 (1996), 223–233. MR Zbl

[Prange 1957] E. Prange, "Cyclic error-correcting codes in two symbols", technical report TN-57-103, Air Force Cambridge Research Center, 1957.

[Prange 1958] E. Prange, "Some cyclic error-correcting codes with simple decoding algorithm", technical report TN-58-156, Air Force Cambridge Research Center, 1958.

[Siap and Kulhan 2005] I. Siap and N. Kulhan, "The structure of generalized quasi cyclic codes", *Appl. Math. E-Notes* **5** (2005), 24–30. MR Zbl

[Vardy 1997] A. Vardy, "The intractability of computing the minimum distance of a code", *IEEE Trans. Inform. Theory* **43**:6 (1997), 1757–1766. MR Zbl

Received: 2019-08-02 Revised: 2019-12-08 Accepted: 2019-12-27

aydinn@kenyon.edu *Kenyon College, Gambier, OH, United States*

guidotti1@kenyon.edu *Kenyon College, Gambier, OH, United States*

liu4@kenyon.edu *Kenyon College, Gambier, OH, United States*

shaikh1@kenyon.edu *Kenyon College, Gambier, OH, United States*

vandenberg1@kenyon.edu *Kenyon College, Gambier, OH, United States*

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2020 is US $205/year for the electronic version, and $275/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve
2020 vol. 13 no. 1

Structured sequences and matrix ranks 1
Charles Johnson, Yaoxian Qu, Duo Wang and John Wilkes

Analysis of steady states for classes of reaction-diffusion equations with hump-shaped density-dependent dispersal on the boundary 9
Quinn Morris, Jessica Nash and Catherine Payne

The L-move and Markov theorems for trivalent braids 21
Carmen Caprau, Gabriel Coloma and Marguerite Davis

Low stages of the Taylor tower for r-immersions 51
Bridget Schreiner, Franjo Šarčević and Ismar Volić

A new go-to sampler for Bayesian probit regression 77
Scott Simmons, Elizabeth J. McGuffey and Douglas VanDerwerken

Characterizing optimal point sets determining one distinct triangle 91
Hazel N. Brenner, James S. Depret-Guillaume, Eyvindur A. Palsson and Robert W. Stuckey

Solutions of periodic boundary value problems 99
R. Aadith, Paras Gupta and Jagan Mohan Jonnalagadda

A few more trees the chromatic symmetric function can distinguish 109
Jake Huryn and Sergei Chmutov

One-point hyperbolic-type metrics 117
Marina Borovikova, Zair Ibragimov, Miguel Jimenez Bravo and Alexandro Luna

Some generalizations of the ASR search algorithm for quasitwisted codes 137
Nuh Aydin, Thomas H. Guidotti, Peihan Liu, Armiya S. Shaikh and Robert O. VandenBerg

Continuous factorization of the identity matrix 149
Yuying Dai, Ankush Hore, Siqi Jiao, Tianxu Lan and Pavlos Motakis

Almost excellent unique factorization domains 165
Sarah M. Fleming and Susan Loepp