J. Algebra Comb. Discrete Appl.
6(1) • 13–20

Received: 21 November 2017
Accepted: 11 December 2018

Journal of Algebra Combinatorics Discrete Structures and Applications

New Linear Codes over $GF(3)$, $GF(11)$, and $GF(13)$*

Research Article

Nuh Aydin, Derek Foret

Abstract: Explicit construction of linear codes with best possible parameters is one of the major and challenging problems in coding theory. Cyclic codes and their various generalizations, such as quasi-twisted (QT) codes, are known to contain many codes with best known parameters. Despite the fact that these classes of codes have been extensively searched, we have been able to refine existing search algorithms to discover many new linear codes over the alphabets $\mathbb{F}_3$, $\mathbb{F}_{11}$, and $\mathbb{F}_{13}$ with better parameters. A total of 38 new linear codes over the three alphabets are presented.

2010 MSC: 94B15, 94B60

Keywords: Best known codes, Constacyclic codes, Quasi-cyclic codes, Quasi-twisted codes

1. Introduction

Let $\mathbb{F}_q$ denote the finite field with q elements (which is also denoted by $GF(q)$). A linear code C of length n over $\mathbb{F}_q$ is a vector subspace of $\mathbb{F}_q^n$. Over a given finite field $\mathbb{F}_q$, a linear code has three fundamental parameters: the length n, the dimension k, and the minimum (Hamming) distance d. A code with these parameters is denoted as an $[n, k, d]_q$-code. One of the main problems of coding theory is a discrete optimization problem: determine the optimal values of these parameters and construct codes whose parameters attain the optimal values. Over a given finite field $\mathbb{F}_q$ we can fix two of the parameters, and look for the optimal value of the remaining one. For example, $d_q[n, k]$ stands for the largest minimum distance of a linear code of length n and dimension k over $\mathbb{F}_q$. This optimization problem is very difficult. In general, it is only solved for the cases where either k or $n - k$ is small. There is a database of best known linear codes [14] over small finite fields which is a major source of reference for coding theory researchers.

While there exist theoretical upper bounds on the value of d for a given n and k, in general there do not exist explicit constructions for linear codes attaining these parameters. A code is called "good" if it has best known parameters; it is called "new" or "record-breaking" if its parameters are better than

* *This research was partially supported by Kenyon Summer Science Scholars program.*
Nuh Aydin (Corresponding Author), Derek Foret; Department of Mathematics, Kenyon College, United States (email: aydinn@kenyon.edu, foretd@kenyon.edu).

the currently best known codes; and called “optimal" if its parameters attain the equality in a theoretical bound. The good codes are also referred to as the best known linear codes (BKLCs). The database [14] of BKLC's includes the parameters of best known codes together with their constructions over finite fields up to size 9. Computer algebra system Magma also contains a similar database [8]. More recently, tables of best known codes over $GF(11)$ and $GF(13)$ have been published in [10] and [9].

The majority of the BKLCs do not attain the theoretical upper bounds on minimum distance. Therefore, it is still possible to improve the parameters of BKLCs. It should be noted however that it may not always be possible to attain the theoretical upper bound on the minimum distance for a given length and dimension.

Computers are often used in searching for codes with best parameters but there is an inherent difficulty: computing the minimum distance of a linear code is computationally intractable (NP-hard)[17]. Since it is not possible to conduct exhaustive searches for linear codes if the dimension is large, researchers often focus on promising subclasses of linear codes with rich mathematical structures. The class of cyclic codes and its various generalizations, such as constacyclic codes, quasi-cyclic (QC) codes, and quasi-twisted (QT) codes, lend themselves well to the problem of finding codes with good parameters. Many record-breaking codes have been obtained in the class of QC codes in the last few decades ([1–3, 5–7, 11–13, 15, 16]). These are the codes we consider in this paper. The search algorithm introduced in [6] has been highly effective and used in several subsequent works (e.g., [1–3, 5, 7, 12, 13]).

We begin by reviewing the structure of constacyclic and QT codes and then describe how we implemented an improved version of the search algorithm that was used in previous works to search for new linear codes. We conclude with a list of new record breaking codes over the fields $\mathbb{F}_3$, $\mathbb{F}_{11}$, and $\mathbb{F}_{13}$ with generators and other necessary information to construct them.

2. Constacyclic search method

A linear code C over $\mathbb{F}_q$ that is closed under a constacyclic shift is called a constacyclic code, that is, if $(c_0, c_1, \ldots, c_{n-1}) \in C$, then $(a \cdot c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$ as well. Here, $a \in \mathbb{F}_q^*$ is a non-zero field element, and it is called the shift constant. The important special case of cyclic codes are obtained when we take $a = 1$.

It is well known that constacyclic codes are ideals in $\mathbb{F}_q[x]/\langle x^n - a\rangle$ if we represent their elements as polynomials, and that each constacyclic code C contains at least one polynomial that generates it as an ideal. While generating polynomials are not unique, the monic generator polynomial of least degree is. This is what we call the generator polynomial $g(x)$ of C. It is also well known that $g(x)$ is the generator polynomial for a constacyclic code of length n with shift constant a if and only if $g(x)$ divides $x^n - a$, i.e. $x^n - a = g(x)h(x)$ for some $h(x) \in \mathbb{F}_q[x]/\langle x^n - a\rangle$. Hence, there is a one-to-one correspondence between the divisors of $x^n - a$ and the constacyclic codes of length n with shift constant a. The polynomial $h(x)$ is called the check polynomial of C. A constacyclic code is therefore uniquely determined by either its generator polynomial or its check polynomial. From the generator polynomial $g(x) = g_0 + g_1 x + \cdots + g_m x^m$ of a constacyclic code C we obtain its generator matrix as a circulant (twistulant) matrix

$$\begin{bmatrix} g_0 & g_1 & \cdots & g_m & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_m & 0 \cdots & 0 \\ \cdots & & & & & & \\ 0 & \ldots & 0 & g_0 & g_1 & \cdots & g_m \end{bmatrix}$$

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

Using the computational algebra system *Magma*, we are able to factor $x^n - a$ and compute the minimum distance d of all constacyclic codes generated by the divisors of $x^n - a$. We follow the method in [5] with a few variations to be more comprehensive in the constacyclic search, and the QT search that follows.

We first consider cyclic codes with length-dimension pairs for which lower bounds are available (found in either [14], [10], or [9]). We are then able to reduce the number of constacyclic codes to be examined by using the following theorems.

Theorem 2.1. *[6] Let $a \in \mathbb{F}_q$ where $a = \omega^i$ for some primitive element ω in $\mathbb{F}_q$. Then, a has an n-th root in $\mathbb{F}_q$ if and only if $\gcd(n, q-1)|i$.*

Theorem 2.2. *[6] If $\mathbb{F}_q$ contains an n-th root of a, then a constacyclic code with length n and shift constant a is equivalent to a cyclic code of length n.*

The above two theorems immediately lead to the following corollary:

Corollary 2.3. *Let ω be a primitive element of $\mathbb{F}_q$ and let $a = \omega^i$ for some positive integer i. If $\gcd(n, q-1)|i$ then a constacyclic code with length n and shift constant a is equivalent to a cyclic code of length n.*

Therefore, once we examine all cyclic codes of length n over $\mathbb{F}_q$, we do not need to examine constacyclic codes of length n for shift constant $a = \omega^i$ if $\gcd(n, q-1)|i$, as the resulting constacyclic code is equivalent to a cyclic code that we have already computed and equivalent codes have the same parameters. Of the remaining constacyclic codes with shift constant $a \neq 1$, some of them turn out to be equivalent to each other. The next theorem specifies which shift constants still need to be examined once all cyclic codes are computed.

Theorem 2.4. *[6] Let a, b have the same order in the multiplicative group $\mathbb{F}_q^*$ and let C_a be the constacyclic code $[n, k, d]_q$ with shift a. Then there exists a constacyclic code C_b that is equivalent to C_a.*

Given the theorem above, we classify the elements of $\mathbb{F}_q^*$ according to their multiplicative orders and examine only one constant from each class. The following table combines the results of Corollary 2.3 and Theorem 2.4 to show which constacyclic codes of length n and shift constant a still need to be checked after computing all cyclic codes. Any constacyclic code with parameters not found in the table would be equivalent to a cyclic or a constacyclic code.

Table 1. Constacyclic codes searched

q	$a \neq 0, 1$	n
3	2	all $n = 2m$
11	2	all $n = 2m$ or $n = 5m$
	3	all $n = 5m$
	10	all $n = 2m$
13	2	all $n = 2m$ or $n = 3m$
	3	all $n = 3m$
	4	all $n = 3m$ or $n = 4m$
	5	all $n = 2m$
	12	all $n = 4m$

Two parts of our search method that have the largest impact on the running time are the number factors of $x^n - a$ considered and the time to compute the minimum distance of each code generated by a divisor of $x^n - a$. When $x^n - a$ has many factors, we only consider a predetermined amount of factors of $x^n - a$ for each degree. We also allocate a maximum computation time for each minimum distance calculation and if the minimum distance is not computed within the time limit, then the computation is aborted. After these initial searches, our results are compiled into a master list which contains the best found minimum distance for each length and dimension pair, and the list is compared with the databases to identify any record-breaking codes. When there are multiple codes with the same highest minimum distance for a given length and dimension $[n, k]$, we just keep the generator polynomial of one of them. This master list also forms the basis of the next step in searching for new QT codes.

3. Quasi-twisted search method

Quasi-twisted (QT) codes are a generalization of constacyclic codes.

Definition 3.1. *Let π_a denote the constacyclic shift operator. A linear code C is said to be ℓ-***quasi-twisted** *(ℓ-QT) if it is invariant under π_a^ℓ, where ℓ is some positive integer which divides the length of the code. That is, if $(c_0, c_1, \ldots, c_{n-1}) \in C$, then $(ac_{n-\ell}, \ldots, ac_{n-1}, c_0, c_1, \ldots, c_{n-\ell-1}) \in C$ as well.*

The class of QT codes contains several other classes as special cases. When $a = 1$, we obtain the class of quasi-cyclic (QC) codes, when $\ell = 1$ the class of constacyclic codes, and when $a = \ell = 1$, the class of cyclic codes. Algebraically, a QT code of length $n = ml$ 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 obtained in 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 $G_{i,j}$ is a twistulant matrix. Such a code is called an r-generator QT code. Most of the work on QT codes is focused on the 1-generator case. We also consider 1-generator QT codes in the paper.

A method of constructing QT codes from constacyclic codes is based on the following theorem [6].

Theorem 3.2. *[3, 6] Let C be a 1-generator QT code of length $n = m\ell$ over $\mathbb{F}_q$ with a generator of the form*

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

where $x^m - a = g(x)h(x)$ and $(h(x), f_i(x)) = 1$ for all $i = 1, \ldots, \ell$. Then $\dim(C) = m - \deg(g(x))$, and $d(C) \geq \ell \cdot d$ where d is the minimum distance of the constacyclic code generated by $g(x)$.

Search methods based on this theorem have been implemented in a number of articles and many record-breaking codes have been obtained [1–3, 5, 7, 12, 13]. We continue this line of work by refining the search method even further. We build up QT codes from the best constacyclic codes obtained in the first stage. To do so, we take the generator polynomial $g(x)$ of one of the $[m, k, d]_q$ constacyclic codes and construct a QT code of index ℓ with generating polynomial of the form

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

so that $n = m\ell$, the length of the QT code, does not exceed the maximum lengths of codes found in the databases. Polynomials $f_i(x)$ that are relatively prime to the check polynomial $h(x) = (x^m - a)/g(x)$are randomly chosen from the elements of $\mathbb{F}_q[x]/\langle x^m - a\rangle$ with $\deg(f_i(x)) < \deg(h(x))$.

The generator polynomial of the best constacyclic code for every length/dimension pair that our constacyclic search found is used for as many values of ℓ as possible. Unlike in our constacyclic search, where one program examines numerous factors of $x^n - a$, our QT search programs examine only one factor of $x^m - a$ at a time; that is, the given generator polynomial $g(x)$. As the dimension of an ℓ-QT code in this method is $m - k$ where k is the degree of $g(x)$, each program only considers codes of one length-dimension pair at a time. Programs are run as long as possible and aborted after a certain period of time if they had not been completed. We used Magma software in the implementation of the search algorithms [8].

4. New codes

4.1. New constacyclic codes

The following are the parameters of new record breaking constacyclic codes. For each code we give its shift constant a, the parity check polynomial h, and w, the improvement on the minimum distance. The parity check polynomial is given in place of the generator polynomial $g(x)$ due to considerations of space. The coefficients of the parity check polynomial are listed in ascending order. Thus, the parity check polynomial for the first code in the table is $h(x) = 10 + x + 7x^2 + 9x^3 + 2x^4 + 4x^5 + 10x^6 + x^7$.

Table 2. Record-breaking $GF(11)$ and $GF(13)$ constacyclic codes

$[n, k, d]_q$	a	h	w
$[111, 7, 93]_{11}$	1	[10,1,7,9,2,4,10,1]	4
$[133, 7, 109]_{11}$	1	[10,9,4,6,5,7,2,1]	1
$[157, 6, 136]_{13}$	1	[1,0,7,12,7,0,1]	3
$[170, 5, 150]_{13}$	1	[1,2,5,5,2,1]	1
$[183, 6, 159]_{13}$	3	[9,6,5,10,11,2,1]	2
$[244, 6, 213]_{13}$	1	[5,7,12,5,12,2,1]	3

4.2. New quasi-twisted codes

The following are the parameters of new record breaking QT codes together with their generators. The shift constants a of the original constacyclic codes along with index ℓ are also given. Each ℓ-QT code is generated by a matrix of the form $[G_1, G_2, \ldots, G_\ell]$ where G_1 is the generator matrix of a constacyclic code with generator polynomial $g(x)$, and each one of the remaining G_i is a twistulant matrix defined by $g(x)f_i(x) \mod (x^n - a)$, where $f_i(x) \in \mathbb{F}_q[x]/\langle x^n - a\rangle$ is relatively prime with the check polynomial. To identify each new code, we have also given $g(x)$ (or $h(x)$ depending on space as above) as well as each $f_i(x)$. All of these codes have been included in the database [8].

We have special comments for 3 of the codes in the list. We found the code with parameters $[150, 22, 67]_3$ in the summer of 2015. Later we found a $[150, 22, 68]_3$ code using a more comprehensive search strategy in the summer of 2018 [4]. For the code with parameters $[105, 28, 37]$ over $\mathbb{F}_3$, an alternative construction that involves many steps is given in [14] [1]. Since our construction is more direct, hence preferable, we include this code in the list. The same is the case for the $[108, 19, 48]_3$-code in the list. It is possible that additional new codes might be obtained from these by applying the standard constructions such as extending, shortening, and puncturing.

[1] *The database contains a code with these parameters with the date of 2016-02-17. The construction given for this code is indirect and involves many steps. Obtaining this code directly as a QC code is preferable. Moreover, we found this code in the summer of 2015 but it was not reported until the spring of 2016.*

Table 3. Record-Breaking QT codes over $GF(3)$ and $GF(11)$.

$[n,k,d]_q$	α	ℓ	polynomials	
$[22,7,14]_{11}$	1	2	g	[1,7,6,7,1]
			f_1	[2,7,4,1,3,10]
$[44,5,35]_{11}$	1	4	g	[1,5,4,2,4,5,1]
			f_1	[9,1,1,4,8]
			f_2	[9,3,10,3,9]
			f_3	[7,6,0,8,3]
$[105,7,84]_{11}$	1	3	h	[7,0,2,7,9,2,10,1]
			f_1	[10,0,2,1,9,10,4]
			f_2	[4,9,2,9,1,7,1]
$[140,7,114]_{11}$	1	4	h	[7,0,2,7,9,2,10,1]
			f_1	[5,10,3,9,7,4,10]
			f_2	[6,10,6,3,2,6,1]
			f_3	[8,3,8,9,1,1,10]
$[180,7,149]_{11}$	1	3	h	[6,9,9,9,4,6,2,1]
			f_1	[4,9,8,5,0,5]
			f_2	[8,5,1,4,9,6,6]
$[222,7,187]_{11}$	1	2	h	[10,1,7,9,2,4,10,1]
			f_1	[0,5,9,7,7,0,9]
$[54,17,21]_3$	1	3	g	[11]
			f_1	[02100011120022022]
			f_2	[1120000001110211]
$[72,19,28]_3$	1	3	g	[211211]
			f_1	[2220112222001220221]
			f_2	[022010100001221121]
$[72,23,25]_3$	1	3	g	[11]
			f_1	[011222210121122102112222]
			f_2	[111001010101002210202221]
$[96,22,38]_3$	1	4	g	[121]
			f_1	[20000000002021010011122]
			f_2	[222012220001011221112]
			f_3	[121020102210122001022]
$[96,23,37]_3$	1	4	g	[11]
			f_1	[211200001222221120100221]
			f_2	[210112021002010222201222]
			f_3	[001202120000022012112 1]
$[108,23,43]_3$	1	4	g	[12021]
			f_1	[200111201022111202102221]
			f_2	[101002200021021211012201]
			f_3	[212012100110201122220 11]
$[60,21,21]_3$	1	2	g	[1201221021]
			f_1	[220221221121001220021]

$[60, 23, 19]_3$ 1 2 g [11122111]
f_1 [0020111110201210001122]

$[99, 25, 37]_3$ 1 3 g [112020201]
f_1 [22111001122202020011001102]
f_2 [02221121212102220021012221]

$[99, 26, 36]_3$ 1 3 g [21220011]
f_1 [21222102220010010101000122]
f_2 [10102010211100011100120 1]

$[70, 18, 28]_3$ 1 2 g [211210212200020101]
f_1 [2211102102202212]

$[70, 22, 25]_3$ 1 2 g [22012112222121]
f_1 [0212020110210011112001]

$*[150, 22, 67]_3$ 1 5 g [200201001]
f_1 [201010011201220212022]
f_2 [2011010222200200112]
f_3 [2100200100212110012201]
f_4 [0201221221220110212101]

$*[105, 28, 37]_3$ 1 3 g [20000001]
f_1 [022221201110020200110110102]
f_2 [110210000100020210120022121 2]

$*[108, 19, 48]_3$ 1 3 g [220121102102212011]
f_1 [0020100200212000022]
f_2 [110122020011221022]

$[111, 19, 50]_3$ 1 3 g [1020220100010220201]
f_1 [2221211012111220022]
f_2 [1001122120001122121]

$[156, 23, 70]_3$ 1 4 g [12112222110200211]
f_1 [1100212211111022021221]
f_2 [0110010122211021001021]
f_3 [0112201122001101102021 1]

$[80, 21, 31]_3$ 1 2 g [22001100011012102021]
f_1 [12021022220212212121]

$[200, 21, 98]_3$ 1 5 g [22001100011012102021]
f_1 [0200012220000112202]
f_2 [022200002211101112011]
f_3 [2200210100211211021 1]
f_4 [201000120020000002]

$[132, 22, 58]_3$ 1 3 g [1220020212021021120 1011]
f_1 [0000112102010210210212]
f_2 [0112112020201110011222]

$[176, 22, 84]_3$ 1 4 g [1220020212021021120 1011]
f_1 [2100210110120022211222]
f_2 [0001102221222001011022]
f_3 [0220001200100220201221]

$[104, 25, 41]_3$ 1 2 g [1110022112022011221200212111]
f_1 [0010001100101201212222201]

$[104, 28, 37]_3$ 1 2 g [20202100121210102212102 11]
f_1 [10010221022112101101021101 12]

$[112, 22, 48]_3$ 1 2 g [20202120101202010212102101201200011]
f_1 [02120121120101212200 02]

$[201, 22, 98]_3$ 1 3 g [22011021121002220111122112222011100212210220 11]
f_1 [00201211221221121022 2]
f_2 [01101002210112210011 22]

$[140, 26, 58]_3$ 1 2 g [12210221022002212111011202122221002102210221 1]
f_1 [02100102020020021100 2001]

References

[1] R. Ackerman, N. Aydin, New quinary linear codes from quasi–twisted codes and their duals, Appl. Math. Lett. 24(4) (2011) 512–515.
[2] N. Aydin, N. Connolly, J. Murphree, New binary linear codes from quasi–cyclic codes and an augmentation algorithm, Appl. Algebra Eng. Commun. Comput. 28(4) (2017) 339–350.
[3] N. Aydin, N. Connolly, M. Grassl, Some results on the structure of constacyclic codes and new linear codes over $GF(7)$ from quasi–twisted codes, Adv. Math. Commun. 11(1) (2017) 245–258.
[4] N. Aydin, J. Lambrinos, O. VandenBerg, On equivalence of cyclic codes, generalization of a quasi–twisted search algorithm, and new linear codes, in submission.
[5] N. Aydin, J. M. Murphree, New linear codes from constacyclic codes, J. Frankl. Inst. 351(3) (2014) 1691–1699.
[6] N. Aydin, I. Siap, D. K. Ray-Chaudhuri, The structure of 1–generator quasi–twisted codes and new linear codes, Des. Codes Cryptogr. 24(3) (2001) 313–326.
[7] N. Aydin, I. Siap, New quasi–cyclic codes over $\mathbb{F}_5$, Appl. Math. Lett. 15(7) (2002) 833–836.
[8] W. Bosma, J. J. Cannon, C. Playoust, The Magma algebra system I: The user language, J. Symbol. Comput. 24(3–4) (1997) 235–265.
[9] E. Z. Chen, N. Aydin, A database of linear codes over F_{13} with minimum distance bounds and new quasi–twisted codes from a heuristic search algorithm, J. Algebra Comb. Discrete Appl. 2(1) (2015) 1–16.
[10] E. Z. Chen, N. Aydin, New quasi-twisted codes over F_{11}–minimum distance bounds and a new database, J. Inform. Optim. Sci. 36(1–2) (2015) 129–157.
[11] E. Z. Chen, Six new binary quasi–cyclic codes, IEEE Trans. Inform. Theory 40(5) (1994) 1666–1667.
[12] R. Daskalov, P. Hristov, New binary one–generator quasi–cyclic codes, IEEE Trans. Inform. Theory 49(11) (2003) 3001–3005.
[13] R. Daskalov, P. Hristov, E. Metodieva, New minimum distance bounds for linear codes over GF(5), Discrete Math. 275(1-3) (2004) 97–110.
[14] M. Grassl, Code Tables: Bounds on the minimum distance of linear codes and quantum codes, online, http://www.codetables.de/
[15] T. A. Gulliver, V. K. Bhargava, New good rate $(m-1)/pm$ ternary and quaternary quasi–cyclic codes, Des. Codes Cryptogr. 7(3) (196) 223–233.
[16] I. Siap, N. Aydin, D. K. Ray–Chaudhuri, New ternary quasi–cyclic codes with better minimum distances, IEEE Trans. Inform. Theory 46(4) (2000) 1554–1558.
[17] A. Vardy, The intractability of computing the minimum distance of a code, IEEE Trans. Inform. Theory 43(6) (1997) 1757–1766.