ARTICLE IN PRESS

Available online at www.sciencedirect.com

ScienceDirect

Journal of the Franklin Institute ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Journal of The Franklin Institute

www.elsevier.com/locate/jfranklin

New linear codes from constacyclic codes

Nuh Aydin*, John M. Murphree

Department of Mathematics, Kenyon College, Gambier, OH 43022, USA

Received 6 August 2013; received in revised form 13 November 2013; accepted 28 November 2013

Abstract

One of the main challenges of coding theory is to construct linear codes with the best possible parameters. Various algebraic and combinatorial methods along with computer searches are used to construct codes with better parameters. Given the computational complexity of determining the minimum distance of a code, exhaustive searches are not feasible for all but small parameter sets. Therefore, codes with certain algebraic structures are preferred for both theoretical and practical reasons. In this work we focus on the class of constacyclic codes to first generate all constacyclic codes exhaustively over small finite fields of order up to 9 to create a database of best constacyclic codes. We will then use this database as a building block for a search algorithm for new quasi-twisted codes. Our search on constacyclic codes has revealed 16 new codes, i.e. codes with better parameters than currently best-known linear codes. Given that constacyclic codes are well known, this is a surprising result. Moreover, using the standard constructions of puncturing, shortening or extending a given code, we also derived 55 additional new codes from these constacyclic codes. Hence, we achieved improvements on 71 entries in the database of best-known codes. We use a search strategy that is comprehensive, i.e. it computes every constacyclic code for a given length and shift constant, and it avoids redundantly examining constacyclic codes that are equivalent to either cyclic codes or other constacyclic codes.

1. Introduction and motivation

A linear code C of length n over $\mathbb{F}_q$, the finite field with q elements, is a vector subspace of $\mathbb{F}_q^n$. A linear code of length n, dimension k, and minimum (Hamming) distance (weight) d is referred to as an $[n,k,d]_q$-code. One of the main problems in coding theory is to find the optimal values of these parameters and to construct codes that attain them. There are theoretical bounds on how

*Corresponding author.

E-mail addresses: aydinn@kenyon.edu, nuhaydin@gmail.com (N. Aydin), murphreejm@kenyon.edu (J.M. Murphree).

0016-0032/$32.00
http://dx.doi.org/10.1016/j.jfranklin.2013.11.019

Please cite this article as: N. Aydin, J.M. Murphree, New linear codes from constacyclic codes, Journal of the Franklin Institute. (2014), http://dx.doi.org/10.1016/j.jfranklin.2013.11.019

large these parameters could be. Most books on coding theory include these bounds (e.g. [21,22]). A code whose parameters attain the optimal values is called an optimal code. Often, a code whose parameters attain the best-known theoretical bounds is not known. In those cases we keep a record of the best-known codes, codes that have explicit constructions and have the best set of parameters among all known codes. There is an on-line table of best-known codes over small finite fields (fields of order up to 9) which is updated as new codes are discovered and reported [16]. The computer algebra system Magma [9,20] also has such a database. Generally, optimal values of the parameters are known only for the cases when k or $n-k$ is small and they constitute a small subset of all entries in the database. In most cases, there are gaps (i.e. potential improvements) on the tables. In fact, researchers continually update the bounds on the tables by constructing new codes that improve the records. Even still, the rate of discovery appears to be slow, considering the many gaps still present in the table. This is partially attributed to the fact that it gets more difficult to find new codes as these gaps narrow.

The main complication in constructing codes with best possible parameters is the computationally taxing process of finding the minimum distance of a linear code. It is well-known that almost all linear codes attain the Gilbert–Varshamov bound, one of the important bounds on the parameters of a code, a lower bound on the size of a linear code. So, if we had an efficient algorithm to compute the minimum distance of an arbitrary linear code, then randomized algorithms could be used to construct codes with optimal or near optimal parameters. However, it is proven in [27] that it is unlikely that such an algorithm exists: computing the minimum distance of an arbitrary linear code is NP-hard (and the corresponding decision problem is NP-complete).

Therefore, researchers focus on certain promising classes of codes with rich mathematical structure that contain codes with good parameters. The class of quasi-twisted (QT) codes (a generalization of quasi-cyclic codes) has been an excellent source for producing new codes. A large number of new codes have been obtained from this class in the last few decades by employing computer searches with various search strategies (e.g. [1,6,7,11–14,18,19,23–25]). One of the most fruitful search methods was introduced in [6] and was used in many subsequent works [12,14], not only for searching new codes over fields but over rings as well [5,3,4]. This method relies on existence of cyclic (in searching for QC codes) or constacyclic codes (in searching for QT codes) with good parameters (as large a minimum distance as possible). These codes are then used as building blocks for constructing QC or QT codes with potentially new parameters. Therefore, it is useful to have a database of best-known cyclic and constacyclic codes for small finite fields. Our work in this paper was originally motivated by this goal. While we constructed this database specifically to aid in this search method, a database of best-known constacyclic codes (which contain cyclic codes as a proper subclass) may be of interest to other researchers for additional purposes as well. We have started building this database and researchers who may be interested in accessing it can contact the authors. We will use this database to search for QT codes with new parameters in a subsequent work.

Since constacyclic codes have been known for a long time and have a mathematical structure that makes them convenient for computer searches, one would expect that best constacyclic codes have already been discovered. However, our search revealed 16 constacyclic codes that improve the parameters of best-known codes given in [16]. We were surprised to find these many new codes in the heavily studied class of constacyclic codes, and we suspect that our findings fill a gap.

There are many methods of constructing new codes in the literature, from relatively elementary search algorithms (e.g. [2,28]), to manipulation existent codes (e.g. [17]), and to more complicated methods that employ advanced tools in algebra or geometry (e.g. [15]). It is preferable however, whenever possible, to create codes with convenient algebraic structures through simple constructions. Since constacyclic codes are useful for both practical (shift registers to implement them) and theoretical reasons, the uncomplicated construction of constacyclic codes should make the results presented here more desirable, not less.

In the next section we review some of the basic properties of constacyclic codes. In Section 3, we describe our search strategy, and finally in Section 4 we present the new codes obtained from our search together with other codes that can be derived from the new constacyclic codes using some of the standard constructions.

2. Constacyclic codes

The class of constacyclic codes has been known for a long time [8]. Their algebraic structure is described in detail in [6]. Here, we review some of the basic facts about them that are more relevant to our search.

Definition 1. Let a be a non-zero constant in $\mathbb{F}_q$. A linear code C is called constacyclic if it is closed under the constacyclic shift, i.e. whenever $(c_0, c_1, \ldots, c_{n-1}) \in C$ then $(ac_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$ as well.

Note that when the constant in the definition, called the shift constant, is taken to be 1 then we obtain cyclic codes. Some of the most famous codes are instances of cyclic codes (hence of constacyclic codes). These include BCH codes, Reed–Solomon codes (used in compact discs), some Hamming codes, and quadratic residue codes.

We follow the usual convention of representing vectors as polynomials. With this representation, it is well known that every constacyclic code has a polynomial that generates it as an ideal. In general there are many generators for a given constacyclic code. However, if we consider the monic generator of least degree then it is unique. Such a polynomial is called the canonical generator, or simply the generator, of the code and it is a divisor of $x^n - a$. Therefore, there is a one-to-one correspondence between constacyclic codes of length n over $\mathbb{F}_q$ with shift constant a, and divisors of $x^n - a$.

Let C be a constacyclic code of length n over $\mathbb{F}_q$ with shift constant a and the generator $g(x)$. Then the dimension of C 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 $\mathbb{F}_q[x]/\langle x^n - a\rangle$. Either polynomial can be used to define a constacyclic code. The BCH bound, one of the most important facts about cyclic codes, has a version for constacyclic codes [6].

3. Search strategy

Since cyclic codes are a particularly important subclass of constacyclic codes, we first generated all cyclic codes and examined their parameters for each finite field $\mathbb{F}_q$, $q = 2, 3, 4, 5, 7, 8, 9$ and for all lengths for which records of best-known codes are available in [16]. This includes the case of repeated root cyclic codes [10,26] which is often excluded from consideration in the literature. Given n and k, there are many cyclic codes of length n and dimension k. For example, for $n = 164$, we see from the factorization of $x^{164} - 1$ that there are a total of $N = 2^{22} = 4,194,304$ cyclic codes over GF(3), and the number of cyclic codes of dimension $k=32$ is $\binom{20}{4}=4845$. Also note that a cyclic code may not exist for a given dimension depending on the degree of distribution of the factors. In this example, there are no cyclic codes of dimension $k=27$ (or for any odd dimension). For each dimension for which cyclic codes exist, we kept a record of the best cyclic code, a cyclic code with the highest minimum distance (in case there are more than one with the same highest distance we chose one of them arbitrarily).

Next, we considered each non-zero constant for a given field as a shift constant. It is important to note that it is not necessary to examine every constant or every length for a given constant. It is proven in [6] that when $\mathbb{F}_q$ contains an nth root of a, constacyclic codes of length n with shift constant a are equivalent to cyclic codes of length n over $\mathbb{F}_q$. Moreover, we know exactly when an element a has an nth root in $\mathbb{F}_q$ [6]. Combining these results with the proposition below allows us to reduce the size of the search space substantially to cover all remaining constacyclic codes once all cyclic codes are obtained. For example, once all cyclic codes are obtained over $\mathbb{F}_8$, it suffices to consider only one (any one) of the non-zero constants as the shift constant and only multiples of 7 as the length of the code.

Proposition 1. *Let $\alpha, \beta \in \mathbb{F}_q$ such that $|\alpha| = |\beta|$, where $|\alpha|$ denotes the order of α in the multiplicative group of non-zero elements $\mathbb{F}_q^{\times}$ of $\mathbb{F}_q$. Then α has an nth root in $\mathbb{F}_q$ if and only if β does.*

Proof. $\Rightarrow$: Suppose α has an nth root in $\mathbb{F}_q$ and let θ be a primitive element of $\mathbb{F}_q$. Then $\alpha = \theta^r$, and $\beta = \theta^s$ for some positive integers r, s. Since $|\alpha| = |\beta|$, we have $\gcd(q-1, r) = \gcd(q-1, s)$. Since α has an nth root in $\mathbb{F}_q$ we know $\gcd(q-1, n)|r$. To show that β has an nth root in $\mathbb{F}_q$, it suffices to show $\gcd(q-1, n)|s$. Let $d = \gcd(q-1, n)$. Then $d|q-1$, $d|n$ and $d|r$. Hence d is a common divisor of $q-1$ and r which implies $d|\gcd(q-1, r) = \gcd(q-1, s)$. It follows that $d|s$, meaning β has an nth root in $\mathbb{F}_q$. The other direction is proven similarly. □

The following table summarizes the shift constants and lengths to be examined for each finite field $q = 3, 4, 5, 7, 8, 9$ where α is a root of $x^2 + 2x + 2$.

q	$a \neq 0, 1$	n
3	2	All $n \ni 2\|n$
4	Any constant in field	All $n \ni 3\|n$
5	2	All $n \ni 2\|n$
	4	All $n \ni 4\|n$
7	2	All $n \ni 3\|n$
	3	All $n \ni 2\|n$ or $n \ni 3\|n$
	6	All $n \ni 2\|n$
8	Any constant in field	All $n \ni 7\|n$
9	α	All $n \ni 2\|n$
	α^2	All $n \ni 4\|n$
	α^4	All $n \ni 8\|n$

We employed some additional strategies to make our search more effective in Magma, the software we used. As we mentioned earlier, computing the minimum distance of a linear code is computationally intractable. Therefore, despite all the efforts to optimize the computation of the minimum distance in the case of cyclic codes, the MinimumDistance() function of Magma still takes very long time to complete for many lengths and dimensions. This becomes problematic when conducting a comprehensive search as a single minimum distance calculation may prevent the program from advancing to other codes which are computable in a short amount of time. To address this issue, we used the optional MaximumTime parameter for the MinimumDistance() function. This parameter allows us to restrict the time allotted to calculating the minimum distance of a single code to a certain specified time period. If this time limit was exceeded, the calculation was terminated. The program recorded basic information about such codes and progressed to the next code. Therefore, there are gaps in our database for some larger lengths and dimensions where it was not possible to compute minimum distances of constacyclic codes in a reasonable amount of time. It is an open problem to find a way to calculate the minimum distances of these discarded codes, thereby completing our table.

Another function we employed is the VerifyMinimumDistanceLowerBound() function. A code C, and value d, are passed to this function. This function is run until either d is found to be a lower bound of the minimum distance of C, or returns false if it is not [9]. This can be implemented to occasionally save time in the search process. For example, say C_1 is an $[n, k_1, d_1]$ code whose minimum distance has already been calculated and stored. If the program were to generate an $[n, k_2, d_2]$ code, C_2, such that $k_1 = k_2$, before calculating d_2, it would use VerifyMinimumDistanceLowerBound() with the argument $d_1 + 1$ to check that $d_1 + 1$ is a lower bound for the minimum weight of C_2. If $d_1 + 1$ is not a lower bound for the minimum distance of C_2, we know that $d_2 \leq d_1$. Thus, this code would be discarded. It is important to note, however, that this only occasionally accelerates the search process. It is possible that it will take a long time to verify that $d_1 + 1$ is a lower bound for the minimum distance of C_2 and, in this case, the function increases the computational time. Despite all the strategies employed, it was not possible to calculate the minimum distance of every code that is in the parameter range of the table [16]. For larger lengths, there are many codes whose minimum distances have not been computed. They are waiting for even more effective search algorithms.

We give an example to show what entries in our database look like. Consider the field $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ where α is a root of $x^2 + 2x + 2$. The table below contains a record of best constacyclic codes of length 30 with shift constant α. Note, w is the distance from the best-known linear code of a given n and k (Table 1).

As a result of our searches, we found that in 16 cases these best codes turned out to be new codes, i.e. each one has a minimum distance that is larger than the minimum distance of the best-known code given in [16], hence improving the lower bounds on the minimum distances of linear codes. We present all of these codes in the next section.

4. New codes

Here we list the parameters and generators of new codes. Note, in order to save space, either the generator polynomial or the parity check polynomial is given, whichever has the smaller degree (Table 2).

In addition to the new codes discovered using our search algorithm (given in the table above), we are able to generate 55 more new codes through the standard constructions of extending, puncturing or shortening a given code. Hence we achieved a total of 71 improvements on the table of best-known code [16]. Listed below are the additional new codes derived from the new constacyclic codes. We skip the details of the constructions for space consideration. For most of these codes, the way they are constructed (derivations from othercodes) can be obtained from [16].

Table 1
Constacyclic codes of length 30 in $GF(9)$ with shift constant α.

k	d	$g(x)$	w
2	27	$x^{28}+2x^{27}+\alpha x^{26}+\alpha^2x^{25}+\alpha^5x^{24}+\alpha^5x^{23}+\alpha^7x^{22}+\alpha^5x^{21}+2x^{20}+\alpha^3x^{18}+\alpha^7x^{17}+2x^{16}+\alpha^5x^{15}+x^{14}+x^{13}+\alpha^2x^{12}+x^{11}$ $+\alpha^7x^{10}+\alpha^6x^8+\alpha^2x^7+\alpha^7x^6+x^5+\alpha^3x^4+\alpha^3x^3+\alpha^5x^2+\alpha^3x+\alpha^2$	0
4	21	$x^{26}+\alpha^6x^{25}+\alpha x^{24}+\alpha^5x^{23}+2x^{22}+2x^{21}+\alpha x^{20}+\alpha^3x^{16}+\alpha x^{15}+2x^{14}+x^{13}+\alpha^7x^{12}+\alpha^7x^{11}+2x^{10}+\alpha^6x^6+2x^5+\alpha^7x^4+\alpha^3x^3+\alpha^2x^2+\alpha^2x+\alpha^7$	3
6	18	$x^{24}+\alpha^3x^{23}+x^{22}+\alpha^2x^{20}+\alpha^3x^{19}+2x^{18}+\alpha^7x^{17}+\alpha^7x^{16}+\alpha x^{15}+\alpha^2x^{13}+\alpha^3x^{12}+\alpha^5x^{11}+\alpha^2x^9+\alpha^3x^8+\alpha^6x^7+\alpha^6x^6+x^5+\alpha^2x^4+\alpha^6x^2+2x+2$	3
8	15	$x^{22}+\alpha^3x^{21}+\alpha x^{20}+\alpha^2x^{19}+\alpha^7x^{18}+x^{17}+\alpha^3x^{16}+\alpha^3x^{15}+\alpha^5x^{14}+\alpha^3x^{13}+2x^{12}+\alpha^6x^{11}+\alpha^7x^{10}+\alpha x^9+\alpha^6x^8+\alpha^7x^7+\alpha^2x^6+\alpha^2x^5+2x^4+\alpha^2x^3+2x^2+\alpha x+\alpha$	4
10	14	$x^{20}+\alpha^2x^{19}+x^{18}+\alpha^2x^{17}+\alpha^2x^{15}+x^{13}+\alpha x^{12}+\alpha^6x^{11}+\alpha^3x^{10}+\alpha x^9+\alpha^7x^8+\alpha x^7+\alpha x^5+\alpha^7x^3+x^2+\alpha^5x+\alpha^6$	3
12	10	$x^{18}+\alpha^2x^{17}+\alpha x^{16}+\alpha^3x^{15}+x^{14}+\alpha^6x^{13}+\alpha^7x^{12}+\alpha^3x^{11}+2x^{10}+\alpha^7x^8+\alpha x^7+x^6+\alpha^2x^5+\alpha^7x^4+\alpha^5x^3+\alpha^6x^2+\alpha^2x+\alpha^3$	5
14	9	$x^{16}+\alpha x^{15}+\alpha^7x^{14}+\alpha x^{13}+\alpha x^{12}+\alpha x^{11}+\alpha^6x^9+\alpha x^8+\alpha x^7+\alpha^2x^5+\alpha^5x^4+x^3+\alpha x^2+\alpha^6x+1$	4
16	9	$x^{14}+\alpha^2x^{13}+2x^{12}+\alpha^6x^{11}+\alpha^5x^{10}+\alpha^5x^9+\alpha^6x^8+\alpha x^7+\alpha x^6+\alpha^3x^5+\alpha^6x^4+\alpha^2x^3+\alpha^3x^2+2x+\alpha^5$	2
18	7	$x^{12}+x^{11}+x^{10}+\alpha^3x^9+x^7+\alpha^7x^6+\alpha^3x^5+2x^3+2x^2+\alpha^7x+\alpha^2$	2
20	6	$x^{10}+2x^9+\alpha^7x^8+\alpha^3x^7+\alpha x^6+\alpha^6x^5+2x^4+\alpha x^3+x^2+x+\alpha^7$	1
22	5	$x^8+2x^7+\alpha^3x^6+\alpha^7x^5+\alpha^3x^4+\alpha^2x^3+\alpha x^2+\alpha^5x+2$	1
24	3	$x^6+\alpha^7x^3+\alpha$	2
26	3	$x^4+\alpha x^3+\alpha^5x^2+2x+\alpha^6$	1
28	2	$x^2+\alpha^5x+\alpha^3$	0

Table 2
A table of new constacyclic codes.

q	n	$g(x)$ or $h(x)$	k	d	a
3	182	$h(x) = x^{22} + x^{21} + 2x^{20} + 2x^{19} + 2x^{17} + x^{13} + 2x^{11} + 2x^9 + x^8 + x^7 + x^4 + x^3 + 2x + 2$	22	86	1
3	182	$h(x) = x^{24} + x^{23} + x^{22} + x^{21} + 2x^{19} + 2x^{18} + 2x^{17} + x^{16} + 2x^{14} + 2x^{13} + 2x^{10} + 2x^8 + x^7 + x^6 + 2x^5 + x^3 + 2$	24	84	1
3	182	$h(x) = x^{25} + x^{24} + x^{23} + x^{21} + 2x^{19} + x^{18} + x^{17} + 2x^{15} + x^{13} + 2x^{11} + x^{10} + 2x^9 + 2x^8 + 2x^7 + x^6 + 2x^5 + 2x^3 + x + 2$	25	83	1
3	205	$h(x) = x^{17} + 2x^{15} + 2x^{14} + 2x^{13} + x^{10} + 2x^9 + 2x^8 + 2x^7 + x^4 + 2x^3 + 2x^2 + 2$	17	109	1
3	70	$x^{22} + x^{20} + 2x^{19} + x^{18} + x^{16} + 2x^{15} + x^{14} + 2x^{13} + x^{11} + x^9 + 2x^8 + x^5 + 2x^2 + 1$	48	10	2
3	146	$h(x) = x^{24} + x^{23} + 2x^{21} + 2x^{20} + 2x^{16} + 2x^{15} + x^{13} + x^{12} + 2x^{11} + x^9 + 2x^8 + 2x^4 + x^3 + 2x + 1$	24	66	2
3	146	$h(x) = x^{26} + x^{25} + x^{24} + 2x^{22} + 2x^{21} + 2x^{20} + 2x^{18} + 2x^{17} + 2x^{16} + x^{14} + x^{12} + 2x^{10} + x^9 + 2x^8 + 2x^6 + x^5 + 2x^4 + x^2 + 2x + 1$	26	62	2
5	78	$x^{26} + 4x^{25} + 2x^{24} + 2x^{22} + x^{21} + 3x^{19} + x^{17} + 4x^{16} + 2x^{15} + 2x^{14} + x^{13} + 3x^{12} + 3x^{10} + 3x^9 + 4x^8 + 3x^6 + 4x^5 + 3x^4 + 2x^3 + x + 2$	52	13	2
5	78	$x^{24} + 4x^{23} + 4x^{22} + x^{21} + x^{20} + x^{19} + 4x^{17} + 4x^{16} + 3x^{15} + 4x^{14} + x^{13} + 4x^{12} + x^{10} + x^9 + x^8 + 4x^7 + 3x^6 + 3x^4 + 4x^3 + 2x^2 + 1$	54	12	2
5	78	$x^{22} + x^{21} + 3x^{20} + 2x^{19} + 4x^{18} + 4x^{17} + x^{16} + 4x^{15} + 3x^{14} + x^{11} + x^{10} + x^8 + 4x^6 + 2x^5 + x^4 + 4x^3 + 4x^2 + 4x + 3$	56	11	2
5	78	$x^{18} + 4x^{17} + 4x^{15} + x^{1}4 + 4x^{12} + 2x^{11} + 4x^{10} + 4x^9 + 4x^8 + 3x^7 + 3x^6 + 4x^5 + 2x^4 + 2x^3 + 4x^2 + 2$	60	9	2
5	78	$x^{10} + x^9 + 3x^8 + 2x^7 + 4x^6 + 3x^5 + 2x^4 + x^3 + 2x^2 + 2$	68	6	2
7	48	$h(x) = x^{17} + 3x^{16} + 3x^{15} + 6x^{14} + 6x^{13} + 5x^{12} + x^{11} + 5x^{10} + 3x^8 + 2x^7 + 3x^6 + 2x^5 + 6x^4 + 3x^3 + 5x^2 + 2$	17	22	1
7	57	$x^{21} + 2x^{20} + 4x^{19} + 2x^{18} + 6x^{17} + x^{16} + 5x^{14} + 6x^{13} + 6x^{11} + 3x^9 + 6x^8 + 4x^6 + 4x^5 + 6x^4 + 5x + 4$	36	13	3
7	57	$x^{24} + 4x^{22} + 2x^{21} + 5x^{20} + 5x^{19} + 2x^{18} + x^{17} + 2x^{16} + x^{15} + 6x^{14} + x^{13} + 2x^{12} + 2x^{11} + 6x^{10} + x^9 + 4x^7 + 4x^6 + 3x^4 + x^3 + 3x^2 + 2$	33	15	3
9	58	$x^{28} + \alpha^6 x^{27} + \alpha^2 x^{26} + \alpha x^{25} + \alpha^7 x^{23} + \alpha^6 x^{21} + x^{20} + 2x^{18} + 2x^{17} + \alpha^5 x^{16} + \alpha^7 x^{15} + \alpha^2 x^{14} + x^{13} + \alpha^7 x^{12} + \alpha^7 x^{11} + x^{10} + \alpha^6 x^8 + \alpha^5 x^7 + x^5 + 2x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha^6$	30	18	α

Please cite this article as: N. Aydin, J.M. Murphree, New linear codes from constacyclic codes, Journal of the Franklin Institute. (2014), http://dx.doi.org/10.1016/j.jfranklin.2013.11.019

$[181,24,83]_3$, $[180,24,82]_3$, $[181,23,84]_3$, $[180,23,83]_3$, $[181,22,85]_3$, $[181,25,82]_3$, $[180,25,81]_3$, $[183,25,83]_3$, $[206,17,110]_3$, $[69,47,10]_3$, $[68,46,10]_3$, $[145,24,65]_3$, $[144,24,64]_3$, $[145,23,66]_3$, $[144,22,66]_3$, $[144,23,65]_3$, $[143,23,64]_3$, $[147,24,66]_3$, $[148,24,66]_3$, $[149,24,66]_3$, $[150,24,66]_3$, $[151,24,66]_3$, $[152,24,66]_3$, $[145,26,61]_3$, $[77,51,13]_5$, $[76,50,13]_5$, $[79,52,13]_5$, $[77,53,12]_5$, $[76,52,12]_5$, $[77,55,11]_5$, $[76,54,11]_5$, $[75,53,11]_5$, $[74,52,11]_5$, $[79,56,11]_5$, $[77,59,9]_5$, $[76,58,9]_5$, $[75,57,9]_5$, $[74,56,9]_5$, $[73,55,9]_5$, $[77,67,6]_5$, $[76,66,6]_5$, $[75,65,6]_5$, $[74,64,6]_5$, $[73,63,6]_5$, $[47,17,21]_7$, $[56,35,13]_7$, $[55,34,13]_7$, $[58,36,13]_7$, $[56,32,15]_7$, $[55,31,15]_7$, $[54,30,15]_7$, $[53,29,15]_7$, $[58,33,15]_7$, $[57,30,17]_9$, $[57,29,18]_9$.

References

[1] R. Ackerman, N. Aydin, New quinary linear codes from quasi-twisted codes and their duals, Appl. Math. Lett. 24 (2011) 512–515.

[2] T. Asamov, N. Aydin, A search algorithm for linear codes: progressive dimension growth, Des. Codes Cryptogr. 45 (2007) 213–217.

[3] N. Aydin, T.A. Gulliver, Some good cyclic and quasi-twisted Z4-linear codes, Ars Comb. XCIX (2011) 503–518.

[4] N. Aydin, S. Karadeniz, B. Yildiz, Some new binary quasi-cyclic codes from codes over the ring $F_2 + uF_2 + vF_2 + uvF_2$, Appl. Algebra Engrg. Comm. Comput. 24 (2013) 355–367.

[5] N. Aydin, D. Ray-Chaudhuri, Quasi-cyclic codes over Z4 and some new binary codes, IEEE Trans. Inf. Theory 48 (2002) 2065–2069.

[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 (2001) 313–326.

[7] N. Aydin, T. Asamov, T.A. Gulliver, Some open problems on quasi-twisted and related code constructions and good quaternary codes, in: Proceedings of IEEE International Symposium on Information Theory (ISIT 2007), pp. 856–860.

[8] E.R. Berlekamp, Algebraic Coding Theory, revised 1984 ed., Agean Park Press, 1984.

[9] W. Bosma, J. Cannon (Eds.), Discovering Mathematics with Magma: Reducing the Abstract to Concrete, Springer, Berlin, New York, 2006.

[10] G. Castagnoli, J.L. Massey, P.A. Schoeller, N. von Seemann, On repeated-root cyclic codes, IEEE Trans. Inf. Theory 37 (1991) 337–342.

[11] R. Daskalov, T.A. Gulliver, E. Metodieva, New good quasi-cyclic ternary and quaternary linear codes, IEEE Trans. Inf. Theory 43 (1997) 1647–1650.

[12] R. Daskalov, T.A. Gulliver, New quasi-twisted quaternary linear codes, IEEE Trans. Inf. Theory 46 (2000) 2642–2643.

[13] R. Daskalov, P. Hristov, New quasi-twisted degenerate ternary linear codes, IEEE Trans. Inf. Theory 49 (2003) 2259–2263.

[14] R. Daskalov, P. Hristov, New binary one-generator quasi-cyclic codes, IEEE Trans. Inf. Theory 49 (2003) 3001–3005.

[15] S. Fanali, M. Giulietti, One-point AG codes on the GK maximal curves, IEEE Trans. Inf. Theory 37 (2010) 202–210.

[16] M. Grassl, Bounds on the minimum distance of linear codes, available at ⟨http://www.codetables.de⟩.

[17] M. Grassl, G. White, New codes from chains of quasi-cyclic codes, in: Proceedings of IEEE International Symposium on Information Theory (ISIT 2005), pp. 2095–2099.

[18] P.P. Greenough, R. Hill, Optimal ternary quasi-cyclic codes, Des. Codes Cryptogr. 2 (1992) 81–91.

[19] T.A. Gulliver, V.K. Bhargava, Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes, IEEE Trans. Inf. Theory 37 (1991) 552–555.

[20] MAGMA computer algebra system web site available at ⟨http://magma.maths.usyd.edu.au/magma/MagmaInfo.html⟩.

[21] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error Correcting Codes, North Holland, Amsterdam, 1997.

[22] S. Roman, Coding and Information Theory, Springer-Verlag, New York, 1992.

Please cite this article as: N. Aydin, J.M. Murphree, New linear codes from constacyclic codes, Journal of the Franklin Institute. (2014), http://dx.doi.org/10.1016/j.jfranklin.2013.11.019

[23] I. Siap, N. Aydin, D.K. Ray-Chaudhuri, New ternary quasi-cyclic codes with better minimum distances, IEEE Trans. Inf. Theory 46 (2000) 1554–1558.
[24] I. Siap, New codes over GF(8), Ars Comb. 71 (2004) 239–247.
[25] I. Siap, N. Aydin, D. Ray-Chaudhuri, New 1-generator quasi-twisted codes over GF(5), in: Codes and Association Schemes, Piscataway, NJ, 1999; DIMACS Series in Discrete Mathematics and Theoretical Computer Science, American Mathematical Society, Providence, RI, 2001, pp. 265–275.
[26] J.H. van Lint, Repeated-root cyclic codes, IEEE Trans. Inf. Theory 37 (1991) 343–345.
[27] A. Vardy, The intractability of computing the minimum distance of a code, IEEE Trans. Inf. Theory 43 (1997) 1757–1766.
[28] J. Zwanzger, A heuristic algorithm for the construction of good linear codes, IEEE Trans. Inf. Theory 54 (2008) 2388–2392.

Please cite this article as: N. Aydin, J.M. Murphree, New linear codes from constacyclic codes, Journal of the Franklin Institute. (2014), http://dx.doi.org/10.1016/j.jfranklin.2013.11.019