J. Algebra Comb. Discrete Appl.
11(1) • 27–39

Received: 10 August 2022
Accepted: 5 December 2022

Journal of Algebra Combinatorics Discrete Structures and Applications

New results and bounds on codes over $GF(17)$

Research Article

Eric Zhi Chen, Nuh Aydin, Fredrik Jönsson, Kamilla Klonowska

Abstract: Determining the best possible values of the parameters of a linear code is one of the most fundamental and challenging problems in coding theory. There exist databases of best-known linear codes ($BKLC$) over small finite fields. In this work, we establish a database of $BKLCs$ over the field $GF(17)$ together with upper bounds on the minimum distances for lengths up to 150 and dimensions up to 6. In the process, we have found many new linear codes over $GF(17)$.

2020 MSC: 94B05, 94B65

Keywords: Quasi-cyclic codes, Quasi-twisted codes, Search algorithms for linear codes, Distance bounds, Lower bounds, Upper bounds, Optimal codes

1. Introduction

Let $[n, k, d]_q$ denote a linear code of length n, dimension k, and minimum distance (weight) d over the finite field $GF(q)$. A central and fundamental problem in coding theory is to find the optimal values of the parameters of a linear code and construct codes with these parameters [22]. The problem can be formulated in a few different ways. For example, we may wish to maximize the minimum distance d for the given block length n and dimension k; or minimize the block length n for the given dimension k and minimum distance d. Let $d_q(n, k)$ denote the largest value of d for which there exists an $[n, k, d]$ code over $GF(q)$, and let $n_q(k, d)$ denote the smallest value of n for which there exists an $[n, k, d]$ code over $GF(q)$. An $[n, k, d]$ code is called optimal (or length-optimal) if its block length n equals $n_q(k, d)$, and it is called distance-optimal if its minimum distance d equals to $d_q(n, k)$.

This optimization problem is very difficult. In general, it is only solved for the cases where either k or $n - k$ is small. Computers are often used in searching for codes with best parameters but there is an

Eric Zhi Chen (Corresponding Author); Department of Computer Science, Kristianstad University, Kristianstad, Sweden (email: eric.chen@hkr.se).
Nuh Aydin; Department of Mathematics, Kenyon College, Gambier, Ohio, USA (email: aydinn@kenyon.edu).
Fredrik Jönsson; Department of Computer Science, Kristianstad University, Kristianstad, Sweden (email: efredrik.jonsson@hkr.se).
Kamilla Klonowska; Department of Computer Science, Kristianstad University, Kristianstad, Sweden (email: kamilla.klonowska@hkr.se).

inherent difficulty: the number of linear codes is very large and computing the minimum distance of a linear code is computationally intractable [23]. 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. As a generalization to cyclic and constacyclic codes, quasi-cyclic (QC) and quasi-twisted (QT) codes are remarkable examples of such codes. They have been shown to contain many good linear codes. With the help of modern computers, many record-breaking QC and QT codes have been constructed. The reader is referred to [1] [2] [4] [8] [14] [15] [17] for a sample of publications that present new linear codes from QC or QT codes. Many more such papers are also available in the literature. However, the problem is still intractable as the dimension and the block length of the code get large.

Records of best-known linear codes ($BKLC$) are available. The online database of linear codes [16] over small fields is a well-known source for coding theorists. A similar database is included in Magma software as well [7]. The online database of QT codes contains best-known QC and QT codes [10]. These databases are updated as new codes are discovered. The two databases at [7] and [10] are for codes over finite fields of size up to 9. More recently, smaller databases for codes over $GF(11)$ and $GF(13)$ were introduced in [11] [12]. The main purpose of this paper is to introduce a database of $BKLCs$ together with upper bounds on minimum distances for codes over $GF(17)$.

Self-dual codes are another important class of codes in coding theory that have been studied extensively. In [6], self-dual codes over prime fields were presented, where self-dual codes with dimensions 2, 3 and 4 were classified, and a table self-dual codes over $GF(17)$ with largest minimum distances were presented for dimensions up to 12 [21]. A construction of sector-disk codes and MDS codes over $GF(17)$ to correct sector erasure errors were presented in [13]. QT codes over $GF(17)$ were studied in [19], and codes with dimension up to 5 were presented. These recent works on codes over $GF(17)$ motivate us to construct an initial database of $BKLCs$ over $GF(17)$ with upper bounds on minimum distances. Various computer search algorithms have been used to construct good QC and QT codes. A number of new codes have been found that improve the bounds on minimum distances compared to the codes in [19]. A table of lower and upper bounds on $d_{17}(n,k)$ is presented for block length $n \leq 150$, and dimension k up to 6. This is the first time such a table appears in the literature.

2. Quasi-twisted codes

A linear $[n,k,d]_q$ code is said to be α-constacyclic if there is a non-zero element α of $GF(q)$ such that for any codeword $(a_0, a_1, ..., a_{n-1})$, its constacyclic shift by one position, that is, $(\alpha a_{n-1}, a_0, ..., a_{n-2})$ is also a codeword [5]. Therefore, constacyclic codes are a generalization of cyclic codes, or a cyclic code is an α-constacyclic code with $\alpha = 1$. A constacyclic code can be defined by a generator polynomial. For a positive integer p, a code is said to be quasi-twisted (QT) of index p if a constacyclic shift of any codeword by p positions is still a codeword. Thus a constacyclic code is a QT code with $p = 1$, and a quasi-cyclic (QC) code is a QT code with $\alpha = 1$. The length n of a QT code is a multiple of p, i.e., $n = pm$ for some positive integer m.

Twistulant matrices (also called a constacyclic matrix) are basic components in a generator matrix for a QT code. An $n \times n$ α-constacyclic matrix is defined as

$$C = \begin{bmatrix} c_0 & c_1 & c_2 & \dots & c_{n-1} \\ \alpha c_{n-1} & c_0 & c_1 & \dots & c_{n-2} \\ \alpha c_{n-2} & \alpha c_{n-1} & c_0 & \dots & c_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha c_1 & \alpha c_2 & \alpha c_3 & \dots & c_0 \end{bmatrix} \tag{1}$$

and the algebra of $n \times n$ constacyclic matrices over $GF(q)$ is isomorphic to the algebra of the quotient ring $GF(q)\ [x]/(x^n - \alpha)$ if C is mapped onto the polynomial formed by the elements of its first row, $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x_{n-1}$, with the least significant coefficient on the left. The polynomial $c(x)$ is called the defining polynomial of the matrix C. A twistulant matrix is called a circulant matrix if $\alpha = 1$.

A generator matrix of a QT code can be transformed into rows of twistulant matrices by a suitable permutation of columns. Most research has been focused on 1-generator and 2-generator QT codes. The generator matrices for 1-generator and 2-generator QT codes consist of one row of twistulant matrices and two rows of twistulant matrices, respectively:

$$G = \begin{bmatrix} G_0 & G_1 & G_2 & \dots & G_{p-1} \end{bmatrix}, \quad (2)$$

$$G = \begin{bmatrix} G_{1,0} & G_{1,1} & G_{1,2} & \dots & G_{1,p-1} \\ G_{2,0} & G_{2,1} & G_{2,2} & \dots & G_{2,p-1} \end{bmatrix}, \quad (3)$$

where G_j and $G_{i,j}$ are twistulant matrices, for $j = 0, 1, 2, \dots, p-1$ and $i = 1$ and 2. Let $g_j(x)$ and $g_{i,j}(x)$ be the defining polynomials for the corresponding twistulant matrices G_j and $G_{i,j}$, respectively. Then, the defining polynomials $(g_0(x), g_1(x), g_2(x), \dots, g_{p-1}(x))$ and $(g_{1,0}(x), g_{1,1}(x), g_{1,2}(x), \dots, g_{1,p-1}(x); g_{2,0}(x), g_{2,1}(x), g_{2,2}(x), \dots, g_{2,p-1}(x))$ define, respectively, a 1-generator QT $[pm, k, d]$ code and 2-generator QT $[pm, k, d]$ code, where k, the dimension of the code, is the rank of the generator matrix G. In Magma algebra system [7], the number of generators is called the height. All the codes constructed in this paper have been checked with the Magma software.

3. Computer search algorithms and best-known QT $[pk, k]$ codes over $GF(17)$

As a generalization to cyclic codes and constacyclic codes, quasi-cyclic (QC) codes and quasi-twisted (QT) codes have been proven to contain many good codes. In fact, a lot of lower bounds on minimum distances have been established by computer construction of good QC and QT codes ([16] [10]). A widely applied method to find good QT codes is to start with the construction of the weight matrix [17]. By eliminating equivalent generator polynomials, and eliminating all redundant information polynomials, an $s \times s$ weight matrix W is computed, as given below, where $c_k(x)$ is the k-th generator polynomial, $i_j(x)$ is the j-th information polynomial, w_{jk} is the Hamming weight of $i_j(x)c_k(x) \mod (x^m - \alpha)$, m is the size of the twistulant matrix, and α is the shift constant. The size s of the weight matrix can be found in [19].

$$W = \begin{array}{c|cccccc} & c_1(x) & c_2(x) & \dots & c_k(x) & \dots & c_s(x) \\ \hline i_1(x) & w_{1,1} & w_{1,2} & \dots & w_{1,k} & \dots & w_{1,s} \\ i_2(x) & w_{2,1} & w_{2,2} & \dots & w_{2,k} & \dots & w_{2,s} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ i_j(x) & w_{j,1} & w_{j,2} & \dots & w_{j,k} & \dots & w_{j,s} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ i_s(x) & w_{s,1} & w_{s,2} & \dots & w_{s,k} & \dots & w_{s,s} \end{array} \quad (4)$$

To construct the best QT $[pm, k]$ code, it is necessary to examine all combinations of the generator polynomials and find p generator polynomials such that the set of columns maximizes the smallest row sum of the corresponding p columns. This problem can be formulated as a combinatorial optimization problem:

$$\max_S \min_{1 \le j \le s} \sum_{t \in S} w_{j,t} \quad (5)$$

where S is a multiset with p elements.

The search [17] [18] is initialized with an arbitrary $[pm, k]$ code (usually a good one) with p columns (or generator polynomials). To improve the code, a new column is found to replace one presently in the code so that the minimum distance is increased.

An iterative heuristic search algorithm was presented in [9]. Given an $s \times s$ weight matrix $W = (w_{ij})$, the iterative algorithm tries to find a sequence of good QT $[im, k]$ codes, $i = 1, 2, \ldots, t$, where $t \leq s$. The basic idea of the algorithm is to extend a QT $[(i-1)m, k]$ code by selecting one more column to get a good QT $[im, k]$ code, for $i = 2, 3, \ldots, t$. The algorithm is executed for a specified number of iterations. The algorithm records the best codes found so far, and stores them in files. When the algorithm stops, a summary of the codes obtained is presented. In this iterative search, a heuristic method is used to implement the selection.

The weight matrix is very important in the implementation of the algorithm. When the weight matrix becomes too big, it is difficult to store it in memory. For example, for $k = m = 6$, a weight table of $251542 \times 251542 = 63273377764$ entries is required to search for the QT codes over $GF(17)$. In [8], some specific sets of defining polynomials were used in the search to reduce the memory requirement and computation time. In this paper, a limited number of defining polynomials (less than 500) are randomly selected to reduce the size of the weight matrix in our search. The effectiveness of this iterative heuristic search algorithm is evident from the fact that a large number of new QT codes over $GF(17)$ for k up to 6 have been obtained.

A new attempt to limit the search is also made. For large code dimension k, and a given m, we first randomly choose 500 generator polynomials. Then we calculate the set of pairs (of generator polynomials) that defines non-equivalent $[2m, k]$ codes. To construct a good QT $[2tm, k]$ code, we select t pairs from the set that gives best minimum distance. This method has been used for $t = 1$ and 2, since it becomes time consuming when t is large. For example, for $k = m = 6$, we first get 100 random generator polynomials over $GF(17)$. Then we get 3369 pairs each of which defines a $[12, 6, 6]$ code, and the codes are non-equivalent. If we do not use only non-equivalent pairs, we need to investigate $100 * 99/2 = 4950$ pairs.

With the methods described above, lot of computer time has been used to construct good QT codes. Table 1 lists the best-known QT $[pk, k]$ codes over $GF(17)$ for k up to 6 and p up to 25. Most entries in the table with $k = 3$, 4, and 5, are from the results in [19]. The 22 entries labeled with superscript âĂIJeâĂİ are new codes found with the algorithm in this paper that improve the lower bounds on minimum distances, and the entries labeled with superscript âĂIJoâĂİ are optimal codes. All codes with $k = 6$ are newly constructed. It should be noted that most QT codes with $k = 3$ are optimal, since they reach the upper bound on the minimum distance.

Table 2 lists the new 1-generator QT $[pk, k]$ codes with k up to 5, that improve the previously known results. A total of 22 codes presented in [19] improve the minimum distance. Table 3 lists the new codes with $k = 6$. The defining polynomials are listed with the lowest degree coefficient on the left, and the finite field elements $0, 1, 2, \ldots, 9, 10, \ldots, 16$ of $GF(17)$ are denoted by $0, 1, 2, \ldots, 9, A, B, C, D, E, F$, and G, respectively. For example, $698DB$ corresponds to the polynomial $11x^4 + 13x^3 + 8x^2 + 9x + 6$.

4. Lower and upper bounds on minimum distances of linear codes over $GF(17)$

4.1. Lower bounds on minimum distance

Usually, the lower bounds on minimum distances are established by explicit construction of codes. Unfortunately, constructing good linear codes is a difficult task because computing the minimum distance of a linear code is computationally expensive [23] and the number of linear codes for a given length and dimension is very large. Hence, researchers focus on a special subclass of linear codes that are promising.

Table 1. Best-known QT $[pk, k]$ codes over $GF(17)$.

p \ k	3	4	5	6
2	4^o	5^o	6^o	7^o
3	7^o	9^o	10^o	13^o
4	10^o	13^o	15^e	17
5	13^o	16	19	22
6	16^o	20^o	23	28
7	18^o	23	28	32
8	21^o	27	32	37
9	24^o	30	37^e	43
10	26	34	41	48
11	29	38	46^e	53
12	32^o	41	51^e	59
13	35^o	45	54	64
14	38^o	49^e	59	69
15	41^{oe}	52	64^e	75
16	44^{oe}	56	68	80
17	46	60^e	72	86
18	49^o	64^e	78^e	92
19	52^o	67	81	96
20	55^{oe}	71^e	86	102
21	57^o	75^e	91^e	107
22	60^o	78	95	113
23	63^o	82^e	100^e	118
24	66^{oe}	86^e	105^e	125
25	69^{oe}	90^e	109	129

The class of QT codes is well known to be such a class. Many record-breaking linear codes have discovered from the class of QT codes in the past few decades. By following the approach given in [3] we have been able to compute all good constacyclic codes exhaustively for most lengths with dimensions up to 6. By applying the search algorithm outlined in the last section on the weight matrices, we have been able to construct many good QT codes. In the previous section, the improved and new 1-generator QT $[pk, k]$ codes with $m = k$ and $k = 3$, 4, 5, and 6, are presented. Table 4 lists new QT codes that are used to derive the lower bounds on the minimum distance. In the table, m is the size of the twistulant matrix, α is the shift constant.

Another method that is used to obtain new codes from existing codes is to apply the standard construction methods such as puncturing, shortening, and extending, to derive additional codes from known codes. With the codes constructed in [19], the new QT codes obtained in this paper, as well as the standard construction methods to derive new codes from existing ones, we have been able to create a comprehensive table (Table 5) of lower bounds on the minimum distances for linear codes over $GF(17)$ with dimensions up to 6, and block length up to 150.

4.2. Upper bounds on minimum distance

It is useful to know how good the constructed codes are, that is, to determine how close their minimum distances are to the theoretical upper bounds. Therefore, we also determined the upper bounds on the minimum distances by applying the standard bounds (such as Griesmer, Elias, Sphere Packing etc. [22]) and took the best result for each parameter set. For the range of the parameter sets under consideration ($n \leq 150$, $3 \leq k \leq 6$), the Griesmer bound turned out to be the best one in most cases, and in some cases the Levenshtein bound performed better. Griesmer bound is a bound on $n_q(k,d)$ [5], given by

$$n_q(k,d) \geq g_k(k,d) = \sum_{i=0}^{k-1} \lceil d/q^i \rceil, \tag{6}$$

where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x and it can also be used as an upper bound on $d_q(n,k)$. When a known bound on $n_q(k-1, \lceil d/q \rceil)$ is available, the Griesmer bound is also used in the following form:

$$n_q(k,d) \geq d + n_q(k-1, \lceil d/q \rceil). \tag{7}$$

This version is called one-step Griesmer bound. For $k \leq 2$, the Griesmer bound (and the Singleton bound) is met for all d and q with the trivial codes of $[n,1,n]$ and $[n,2,n-1]$. So it is only necessary to study codes with $k > 2$.

One of the most elementary bounds on the parameters of a linear code is the Singleton bound [22] which states: $n_q(k,d) \geq d + k - 1$, or equivalently, $d \leq n - k + 1$, giving an upper bound on $d_q(n,k)$. Codes that meet this bound with equality are called maximum distance separable (MDS). MDS codes exist for all values of $n \leq q + 1$. Thus, for $q = 17$, MDS codes exist for all lengths 18 or less.

By using the standard puncturing and shortening constructions, the following bounds are derived:

$$d_q(n+1,k) \leq d_q(n,k) + 1, \tag{8}$$

and

$$d_q(n+1,k+1) \leq d_q(n,k). \tag{9}$$

When a code with minimum distance equal to one of the upper bounds is obtained, an optimal code is found and there is no room for improvement in the table. When there is a gap between the minimum distance of a best-known code and the upper bound on the minimum distance, this is indicated in the table by listing both values.

4.3. Linear codes with dimension 3

There is a connection between $BKLCs$ and projective geometry. An (n,r)-arc in $PG(k-1,q)$ is a set of n points K with the property that every hyperplane is incident with at most r points of K and there is some hyperplane incident with exactly r points of K. It is known that there exists a projective $[n,3,d]_q$ code if and only if there exists an $(n,n-d)$-arc in $PG(2,q)$, and every $[n,k,d]_q$ Griesmer code with $d \leq q^{k-1}$ is projective [20]. Ball maintains an online table of bounds on the sizes of (n,r)-arcs in $PG(2,q)$ [4]. Therefore, the bounds on $k = 3$ can be derived from the bounds on the sizes of (n,r)-arcs in $PG(2,q)$, and by puncturing technique. It should be noted that most of the QC or QT codes with $k = 3$ constructed in this work meet the bounds.

5. Conclusion

As a result of extensive work on linear codes over $GF(17)$, many new QC or QT codes have been constructed in this work along with a number of codes that improve the parameters of previously best-known codes over $GF(17)$. Further, lower and upper bounds on codes with dimensions up to 6 and block lengths up to 150 have been tabulated.

References

[1] D. Akre, N. Aydin, M. Harrington, S. Pandey, New Binary and Ternary Quasi-Cyclic Codes with Good Properties, Computational and Applied Mathematics 42 (2023) 102.

[2] N. Aydin, I. Siap , DK. Ray-Chaudhuri, The structure of 1-generator quasi-twisted codes and new linear codes, Des. Codes Cryptogr. 24 (2001) 313–326.

[3] N. Aydin, J. Murphree, New Linear Codes from Constacyclic Codes, Journal of the Franklin Institute. 35(3) (2014) 1691–1699.

[4] Ball S. Table of bounds on three dimensional linear codes or (n, r)-arcs in $PG(2, q)$. [Online]. [cited 2022 3 30]. Available from: https://web.mat.upc.edu/simeon.michael.ball/codebounds.html.

[5] ER. Berlekamp, Algebraic Coding Theory Walnut Creek, Aegean Park Press (1984).

[6] K. Betsumiya, S. Georgiou, TA. Guilliver, M. Harada, C. Koukouvinos, On self-dual codes over some prime fields, Disc. Math. 262 (2003) 37–58.

[7] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (1997) 235–265.

[8] E. Z. Chen, Six new binary quasi-cyclic codes, IEEE Trans. Inform. Theory 40 (1994) 1666-âĂŞ1667.

[9] E. Z. Chen, A new iterative computer search algorithm for good quasi-twisted codes, Designs, Codes and Cryptography 76(2) (2015) 307–323.

[10] E. Z. Chen, Online Database of Quasi-Twisted Codes. [Online]. [cited 2022 03 30]. Available from: http://databases.cs.hkr.se/qtcodes/index.htm.

[11] E. Z. Chen, N. Aydin, A database of linear codes over F13 with minimum distance bounds and new quasi-twisted codes from a heuristic search algorithm, Journal of Algebra, Combinatorics, Discrete Structures and Applications 2(1) (2015) 1–16.

[12] EZ. Chen, N. Aydin, New quasi-twisted codes over F_{11}- minimum distance bounds and a new database, Journal of Information and Optimization Sciences 36 (2015) 129–157.

[13] J. Chen, K. W. Shum, Q. Yu, C. W. Sung, Sector-disk codes and partial MDS codes with up to three global parities. In 2015 IEEE International Symposium on Information Theory (ISIT) (2015) Hong Kong. 1876–1880.

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

[15] R. N. Daskalov, T. A. Gulliver, E. Metodieva, New ternary linear codes, IEEE Trans. Inform. Theory 45 (1999) 1687–1688.

[16] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes [Online] [cited 2022 03 30]. Available from: http://www.codetables.de.

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

[18] T. A. Gulliver, P. R. J., Ostergard, Improved bounds for ternary linear codes of dimension 7, IEEE Trans. Inform. Theory 43 (1997) 1377–1388.

[19] T. A. Gulliver, V. C. Venkaiah, Construction of quasi-twisted codes and enumeration of defining polynomials, J. Algebra Comb. Discrete Appl. 7 (2019) 3–20.

[20] R. Hill, Optimal linear codes Mitchell C, Oxford University Press (1992).

[21] I. S. Kotsireas, C. Koukouvinos, DE. Simos, MDS and near-MDS self-dual codes over large prime fields, Advances in Mathemtics of Communications 3(4) (2009) 349–361.

[22] FJ. MacWilliams, N. Sloane N, The Theory of Error-Correcting Codes. 2nd ed., North-holland Publishing Company (1978).

[23] A. Vardy, The intractability of computing the minimum distance of a code, IEEE Trans. Inform. Theory 43 (1997) 1757–1766.

Table 2. New improved QT $[pk, k]$ codes over $GF(17)$.

Code $[n, k, d]$	α	Defining polynomials
$[45, 3, 41]$	1	$241, 11, G11, 41, E41, B1, D1, F21, 461, 431, A31, 611, 711, F61, E31$
$[48, 3, 44]$	1	$19C, 381, E8, 75, 28C, 78E, E71, B1, AC6, E45, 731, G7, 471, 18D, 741, D81$
$[60, 3, 55]$	1	$1, 541, A81, 41, 521, E91, 81, G91, C51, D21, 4D1, E1, 561, 311, 831, E61, 711, C31, 911, C11$
$[72, 3, 66]$	1	$341, 541, G11, B81, 321, 71, 821, A21, C21, D21, G51, 231, 861, 831, 611, A31, F61, 811, 271, E31, F31, B11, A71, C71$
$[75, 3, 69]$	1	$C71, 1, G71, F21, 281, C81, A31, B31, 8C1, G31, 241, G1, 541, 311, 611, 811, B11, D11, E51, 461, 421, 521, B61, E61, D21$
$[56, 4, 49]$	1	$74B1, C5B, EBG1, CB3, 3D51, F1D, 98E1, 27A, B1C1, D58, E661, 331, A831, 7F7$
$[68, 4, 60]$	1	$41, C31, EC1, 8D1, GG1, GC11, 7F11, 6G11, 5421, 3D21, 4A31, F741, 5F41, F261, 2371, 2B81, EF91$
$[72, 4, 64]$	1	$311, 151, AD1, 6121, D121, 4321, B421, 4721, AD21, AC31, 5141, B241, 8341, 7451, F261, CA61, 5A71, BD71$
$[80, 4, 71]$	1	$9D21, FA1, CA3, E1B, 165D, 5G41, 5D7, 6C8, E465, 44D1, B1, D45, BF13, 6429, 59F1, ACG, 86BA, 6EGE, A152, 7261$
$[84, 4, 75]$	1	$51, 241, D41, 661, E61, 271, G71, 3211, F811, 5911, CB11, 5C11, 2F11, 3F21, B431, D831, CA31, ED31, CE31, 2F31, 4E41$
$[92, 4, 82]$	1	$G31, C51, 9611, AD11, E621, 3721, 6921, BD21, 5731, E831, FD31, DE31, C141, 5241, CA41, B851, 4G61, BA71, 8D71, A181, E381, FC81, 4G91$
$[96, 4, 86]$	1	$B1, 341, E41, 2D1, 6F1, 8411, 3611, 3911, DB11, 8D11, AE11, 6121, 2E21, G231, 4E41, B251, C851, B361, 5971, FD71, G281, A691, B1A1, A7B1$
$[100, 4, 90]$	3	$D4G9, BF91, C9A, A29, AA8, 9189, 100B, 1GC1, FDB, D58, 7D1E, F96B, 3GGA, ECG1, D25, 7161, DBE7, 0FC2, 3841, 131, 2C8C, FE72, 692A, E7C2, B9A1$
$[20, 5, 15]$	1	$43C31, 68611, FD151, F9G61$
$[45, 5, 37]$	1	$A36C8, C87B1, 5GG2, 21AE1, EDG11, A783, 2G534, GEB51, 3B1E1$
$[55, 5, 46]$	1	$A7F31, FA11, E5D21, 89EA1, C8G31, 4FE31, F8G11, FFA1, 89511, 3621, 4BA11$
$[60, 5, 51]$	1	$187D, 7131, BC6, 4G7A1, C6E6, 160E, A6BF1, A3751, B4CF1, BFBFE, 2A6B3, 648D1$
$[75, 5, 64]$	1	$187D, 7131, BC6, 60B35, 4CEB1, DFE, FG333, 64FE1, 6C7F, 2AAE2, F18A4, 64281, E0E52, 2G4C1, FC35$
$[90, 5, 78]$	1	$187D, 7131, BC6, G0126, CDD31, DDE2, B1G18, FBGB1, 57AF, 486CD, A6BB5, C4631, 3CE98, 65F21, 891B, F1FD4, 98653, C21F1$
$[105, 5, 91]$	1	$187D, 7131, BC6, B229E, 27EE1, 58DC, A2CAE, 8BBG2, ED121, 253FG, CC881, 415D1, 89FD7, E7C11, 2CB91, F82B3, D9D31, 42B5, 2G534, GEB51, 3B1E1$
$[115, 5, 100]$	1	$GC971, 1, B6F91, E5E31, 91C11, CF971, 9DF1, BC321, F961, 37B51, D2A41, G731, C8C71, 45E21, C2D21, 9EB1, FDE61, 74121, E981, 7E911, 58B31, DAE11, 2C91$
$[120, 5, 105]$	1	$CDAB9, F4C61, CF281, B229E, 27EE1, 58DC, D2988, 6GE31, 2849, A2CAE, 8BBG2, ED121, 187D, 7131, BC6, F1FD4, 98653, C21F1, F8D76, 82E71, 6405, C6GE6, 6F2D1, 4457$

Table 3. New QT $[pk, k]$ codes with $k = 6$ over $GF(17)$.

Code $[n, k, d]$	α	Defining polynomials
[12, 6, 7]	1	1, 4F6311
[18, 6, 13]	3	19C, 381, E8, 75, 28C, 78E, E71, B1, AC6, E45, 731, G7, 471, 18D, 741, D81
[24, 6, 17]	1	4D5721, B372B1, E9F41, G9E561
[30, 6, 22]	1	1, BAF51, C9F81, B372B1, 4G661, 69C51, EC4721B372B1, 4BG141, CBAD11, 74CB1, 59A421
[36, 6, 28]	3	DD8F39, 3118C1, E4296, 66ABE2, ED7D71, EG2F6
[42, 6, 32]	1	1, BAF51, C9F81, B372B1, 4G661, 69C51, EC4721
[48, 6, 37]	1	FB1811, GGA21, 51DD1, 4BG141, GE4E51, F8951, 4G661, 1
[54, 6, 43]	3	G6BE1, 65G211, 8DC611, E6BF11, 51DD1, 352E1, 1, 7D8F41, 932G11
[60, 6, 48]	1	1, FEA641, 7E241, C9F81, BCBA61, 65G211, G42811, 4A2B11, E14361, AAE511
[66, 6, 53]	1	FB1811, GGA21, 51DD1, 4BG141, GE4E51, F8951, 4G661, 1, G6BE1, D92121, F14A31
[72, 6, 59]	1	549641, 4BCG11, E14361, 6A2111, B7CA1, 8DC611, 43A111, ED61, FEA641, 38471, D1E641, 65D91
[78, 6, 64]	1	FD541, E6BF11, F89811, 65G211, 91111, GCG241, 29A511, E9F41, ED61, 2G4C31, 7E241, 5CFC31, 69C51
[84, 6, 69]	1	FB1811, GGA21, 51DD1, 4BG141, GE4E51, F8951, 4G661, 1, G6BE1, D92121, 4D5721, 549641, G7G621, F14A31
[90, 6, 75]	1	4EA791, 59A421, 352E1, E9F41, FEA641, 3E3E1, 4EDA21, BAF51, 932G11, E2E51, EC4721, GE4E51, FB1811, 37AB21, 43A111
[96, 6, 80]	1	1, BAF51, 549641, 297511, F4E571, 7E241, FB1811, 786F11, 4BCG11, 59A421, D78621, C1B611, 2DB911, GE4E51, 65D91, B372B1
[102, 6, 86]	1	EF5E1, 562211, CG4G11, B8921, 678E11, 8CDC71, 8GCF41, 7G4811, FDEE1, 5A8651, 6D7421, E79F11, 5C9721, 656F1, 6A7121, 4G2E11, 628C1
[108, 6, 92]	1	465841, G9596, C11C2, 0337F, 29F6D, B0A16, G0D39D, 18G237, BAGE6E, 495685, CE7121, 823F9, 334C6C, 149GGB, 7268E3, 888EF4, 6E0C71, G15D5
[114, 6, 96]	1	FB1811, GGA21, 51DD1, 4BG141, GE4E51, F8951, 4G661, 1, G6BE1, D92121, 4D5721, 549641, G7G621, F14A31, CBAD11, 37AB21, 4BCG11, ED61, D1E641
[120, 6, 102]	1	FB1811, GGA21, 51DD1, 4BG141, F8951, 854E21, CBAD11, B4F651, GE4E51, 786F11, 83181, BAF51, 297511, FD541, D78621, D92121, F54C1, F4E571, G42811, GCG241
[126, 6, 107]	1	FB1811, GGA21, 51DD1, 4BG141, GE4E51, F8951, 4G661, 1, G6BE1, D92121, 4D5721, 549641, G7G621, F14A31, CBAD11, 37AB21, 4BCG11, ED61, D1E641, 718D21, AEA11
[132, 6, 113]	1	G5GF11, F14A31, FEA641, 59A421, F74G21, 83181, 4G661, C1B611, 932G11, 65G211, 65D91, 5CFC31, B7CA1, 64CA21, 471721, F54C1, C9F81, B372B1, AAE511, CEAD41, 3E3E1, E14361
[138, 6, 118]	1	549431, B4F651, GE4E51, G7G621, 4G661, F4E571, E14361, 528231, 341, G52591, AAE511, 69C51, 4EA791, CBAD11, B372B1, 1, 8DC611, 2FC521, 2D2E41, 9G2121, 37AB21, E2E51, 7E241
[144, 6, 125]	1	22D5AC, B48AFD, 13979F, GBBB0C, G3FFB1, A9611, G3012F, BEAG4G, 2BE235, DFC842, 4C06E1, B6569, G1E24C, A6D5E1, 8B473G, GG32A2, 016DB1, 27D55, G27GDA, F6BE5D, BF62B2, GGB46B, 858531, 26BA1
[150, 6, 129]	1	58361, 2DB911, 4BG141, 7B5241, 43A111, B372B1, 91111, 455A1, GCG241, D1E641, 1, 854E21, 4EA791, 2FC521, 528231, 549431, FD541, G6BE1, 944211, 2G4C31, B7CA1, D78621, 38471, FB1811, B4F651

Table 4. New QT codes used to derive the lower bounds on minimum distances of codes $GF(17)$.

n	k	d	m	α	Defining polynomials
45	4	39	5	6	GEFC3, D1G99, E984F, 58631, A7A17, G97F1, 3D1C6, AE88F, 698DB
60	4	53	15	1	GBD37654EAC1, BDE4A2F6C746E1, DB1DCE83347FD11, 493FDGACG3EF231
72	4	64	12	1	1GD312136G1, DB2333791, 9E54EF61AB1, 5D6D9A5E4E1, 7FCC45F7AA1, C172ABGA491
87	4	78	29	3	G9CG307DB667B6ABB64A0E1581, 94A12G82AA8B9469D8914383ED81, 99G97181D6CF80AA94DF536F6731
100	4	90	20	3	DBCAA4F92AG9A9891, 911FD10GD580CB89B1, 7F3EDD9GC216GG5EBA1, 7D0311BF836EC411721, 2F6EBCE979872CAC2A21
116	4	105	29	1	G9CG307DB667B6ABB64A0E1581, 2F16526FFC5F86EBGA97EGC57B91, 77G9AA5E608D0BEBDF5D1EGB3G61, 6BDC6B4E9F3D45715FD683CB81311
126	4	114	18	3	BEEB91E878DEB7661, DDGB6F1701A191A01, 9778FDD7335G89D21, B92FBF7D8DD9E41, 8GCG68018271D3E1, CCD37F75BF2F8G9G1, 5D9BGC58F454A16831
145	4	132	29	1	G9CG307DB667B6ABB64A0E1581, F0GA53EG1613C69FG6E7ABGB4A1, 457E7C918ED4F8EB8C4625042D11, AGD5341CFBCE456999F9F62B3E41, 686E3341EE4E848E4EE1433E68611
150	4	136	15	1	891167EGFB2B01, 6EA732779E9D01, GBD37654EAC1, A75A827D6853G11, F89C1BGG4G8A91, 871D3FDC3DBE411, DD11F697F2FC91, A49C9C4848C901, 3GGBFG4452FEE1, B4B23E10EE9C61
20	5	15	5	1	43C31, 68611, FD151, F9G61
27	5	21	9	1	F90D8171, 3GD648C1, 793818E21
36	5	29	18	1	271841F54B9CE29C11, 2965B1DE2GC591G311
48	5	40	16	1	B7DA9E3522F0A91, 1E75GBGE656B701, 99D14E195B49121
60	5	51	15	1	17B81C736D1, 4C1G667E0A6E1, AAB634B7CF5F111, B26FA4B68FBDE31
68	5	58	17	1	34790EA844750451, 83537E8BFGED4GE11, 731CB5GDE15488A1, DE749129B61CD4B11
75	5	64	15	1	17B81C736D1, 64D0CFBEE3B051, F66G4C3F73EF31, 2F6A14A82EA8241, E2F0GCE435C521
90	5	78	18	1	17DB75AA57BD71, A3252E8GDD49659611, EF8F5FGCB24CF19B21, E89879A25C0G1FB51, 802DEGB107752321
102	5	89	17	1	15F1276721F51, E5CAD6DC3833B1311, A9D813CDC2EFA851, A6GE6D3AFE1274D11, DE4B503E987C5C11, G1846D6G521CA3F1
116	5	102	29	1	C575A902948B0EG8B942CF02E11, 751C3F07937168AC804BFB688B21, 7B7259CB6AEFA34EF6ABGBD1F4911, 89382966361622616366928398111
126	5	111	18	1	17DB75AA57BD71, FB53E6D61AC3GA4E11, F8B769DDE7GEC2F91, 914B8AFB5F5472551, EC5698A1E14671C71, 5ADE69FE7BCAGCGB1, C3AE1787395G4EB111
144	5	128	36	1	G0DC8C18DD59389DC48A66EA0BEBG3A1, 6G69BGEGGBDFDF871123GEDB7CCAE9A7B1, 6C698A6B9D5EBFFCA7ED9CD529FF12GC1B1, EDF2AC015CDF824F6710G1GF8FBDEBCC901

Table 4. Continued: New QT codes used to derive the lower bounds on minimum distances of codes $GF(17)$.

n	k	d	m	α	Defining polynomials
150	5	132	6	1	11, 4DA21, 46G261, C1D81, CGA611, 895A71, 738D1, CAE461, 374121, EF771, 89G361, 9G601, C76D31, G2311, E8291, CG8521, B1E821, C79261, F76F1, 23GG1, GE5821, 23F151, E65E1, 97361, 5CC511
26	6	19	13	1	G5B7A6C1, 792CF989F8521
36	6	28	6	3	DD8F39, 3118C1, E4296, 66ABE2, ED7D71, EG2F6
42	6	33	7	3	G4351C5, 67DAF83, 829FBBA, 5D5CG8A, C941A66, 126097A
52	6	42	26	3	G609F3C7C4BC3ADBD2E2CGD475, F4D9C9BGCEF495B65F461428A2
68	6	56	17	1	6D49AG2199CDF2E1, 234F862E413F2CA1, CF281B4B2FDDB981, 8B4C979DG197B5D1
78	6	65	26	3	B75A3098GDBC917F92F8DA151, E9B67EFBFAF548A1C584E94D11, G8DFB74B684A96D5D8GEE3631
85	6	71	17	1	GBDCA3E75461, 6D49AG2199CDF2E1, 977FC3FA249574811, F3E919C540F51CD1, CF2663BE89A624A1
98	6	83	7	3	G4351C5, 67DAF83, CGB0C7A, D225G62, 311D161, 54E683F, E5A6E8, DE48E5D, D21EEG, 1CD68GE, A5CC598, B568D61, 7EDEE5C, F826ABD
108	6	92	36	1	4GC02B6913905513FA89C761462FD61, G1B4C808A9E2DGG57332E61F936829D7E51, 31786G3428E1496805CG8ECD6GEF75CB341
117	6	100	13	1	GFBBD0046621, 668698C64AA, 77DB598B9BB, AC29ED193327, EC5D253B4B1, ACEDAFD529D3, FD5DGB2DG98E1, 8G8518A10E41, 6100G148E34B
130	6	112	13	3	96504890BB1, 466EFE92DB, 84FACA3F912F1, 3G897697CF531, B539GB979FD11, 7A08DC1F28A5, 1F3A82F6CFCE1, D94G99AAEE01, 38D7GFBF489C1, 564DG1F2C984
144	6	125	6	1	22D5AC, B48AFD, 13979F, GBBB0C, G3FFB1, A9611, G3012F, BEAG4G, 2BE235, DFC842, 4C06E1, B6569, G1E24C, A6D5E1, 8B473G, GG32A2, 016DB1, 27D55, G27GDA, F6BE5D, BF62B2, GGB46B, 858531, 26BA1
150	6	130	30	1	GC18DDGBE8BB632B92287BA62A9411, 68383E543A4A983F11D67G51B5BC11, F22D7A564DECAAFA9DC4535BCE3F1, 2793B5ADF99G21B2C2186B6DCAC21, F12585796GE8F8A088A15804GC201

Table 5. Lower and upper bounds on minimum distances of linear codes over $GF(17)$.

n	$k=3$	$k=4$	$k=5$	$k=6$	n	$k=3$	$k=4$	$k=5$	$k=6$
					76	70	67-69	64-68	63-67
					77	71	68-70	65-69	64-68
3	1				78	72	69-71	66-70	65-69 New
4	2	1			79	73 Be	70-72	67-71	65-70
5	3	2	1		80	73-74	71-73	68-72	66-71
6	4	3	2	1	81	74-75	72-74	69-73	67-72
7	5	4	3	2	82	75-76	73-75	70-74	68-73
8	6	5	4	3	83	76-77	74-76	71-75	69-74
9	7	6	5	4	84	77-78	75-77	72-76	70-75
10	8	7	6	5	85	78-79	76-78	73-77	71-76 New
11	9	8	7	6	86	79-80	77-78	74-78	71-77
12	10	9	8	7	87	80	78-79 New	75-78	72-78
13	11	10	9	8	88	81	78-80	76-79	73-78
14	12	11	10	9	89	82	79-81	77-80	74-79
15	13	12	11	10	90	83	80-82	78-81 New	75-80
16	14	13	12	11	91	84	81-83	78-82	76-81
17	15	14	13	12	92	85	82-84	79-83	77-82
18	16 Be	15 Be	14 Be	13 Be	93	86	83-85	80-84	78-83
19	16	15-16	14-15	13-14	94	87	84-86	81-85	79-84
20	17	16-17	15-16 New	13-15	95	88 Be	85-87	82-86	80-85
21	18	17	15-17	14-16	96	88-89	86-88	83-87	81-86
22	19	18	16-17	15-17	97	89-90	87-89	84-88	82-87
23	20	19	17-18	16-17	98	90-91	88-90	85-89	83-88 New
24	21	20 Gu	18-19	17-18	99	91-92	89-91	86-90	83-89
25	22	20-21	19-20	18-19	100	92-93	90-92 New	87-91	84-90
26	23	21-22	20-21	19-20 New	101	93-94	90-93	88-92	85-91
27	24	22-23	21-22 New	19-21	102	94-95	91-94	89-93 New	86-92
28	25 Ba	23-24	21-23	20-22	103	95-96	92-95	89-94	87-93
29	25-26	24-25	22-24	21-23	104	96	93-95	90-95	88-94
30	26-27	25-26	23-25	22-24	105	97	94-96	91-95	89-95
31	27-28	26-27	24-26	23-25	106	98	95-97	92-96	90-95
32	28-29	27-28 Gu	25-27	24-26	107	99	96-98	93-97	91-96
33	29-30	27-29	26-28	25-27	108	100	97-99	94-98	92-97 New
34	30	28-30	27-29	26-28	109	101	98-100	95-99	92-98
35	31	29-31	28-30	27-29	110	102	99-101	96-100	93-99
36	32	30-32	29-31 New	28-30 New	111	103	100-102	97-101	94-100
37	33	31-33	29-32	28-31	112	104	101-103	98-102	95-101

Table 5. Continued: Lower and upper bounds on minimum distances of linear codes over $GF(17)$.

n	$k=3$	$k=4$	$k=5$	$k=6$	n	$k=3$	$k=4$	$k=5$	$k=6$
38	34	32-33	30-33	29-32	113	105	102-104	99-103	96-102
39	35	33-34	31-33	30-33	114	106 Be	103-105	100-104	97-103
40	36	34-35	32-34	31-34	115	106-107	104-106	101-105	98-104
41	37	35-36	33-35	32-34	116	107-108	105-107 New	102-106 New	99-105
42	38	36-37	34-36	33-35 New	117	108-109	105-108	102-107	100-106 New
43	39	37-38	35-37	33-36	118	109-110	106-109	103-108	100-107
44	40	38-39	36-38	34-37	119	110-111	107-110	104-109	101-108
45	41	39-40 New	37-39	35-38	120	111-112	108-111	105-109	102-109
46	42	39-41	38-40	36-39	121	112	109-112	106-110	103-109
47	43	40-42	39-41	37-40	122	113	110-113	107-111	104-110
48	44 Ba	41-43	40-42 New	38-41	123	114	111-113	108-112	105-111
49	44-45	42-44	40-43	39-42	124	115	112-114	109-113	106-112
50	45-46	43-45	41-44	40-43	125	116	113-115	110-114	107-113
51	46-47	44-46	42-45	41-44	126	117	114-116 New	111-115	108-114
52	47-48	45-47	43-46	42-45 New	127	118	114-117	111-116	109-115
53	48	46-47	44-47	42-46	128	119	115-118	112-117	110-116
54	49	47-48	45-47	43-47	129	120	116-119	113-118	111-117
55	50	48-49	46-48	44-47	130	121	117-120	114-119	112-118 New
56	51	49-50	47-49	45-48	131	122	118-121	115-120	112-119
57	52	50-51	48-50	45-49	132	123	119-122	116-121	113-120
58	53	51-52	49-51	46-50	133	124	120-123	117-122	114-121
59	54	52-53	50-52	47-51	134	125	121-124	118-123	115-122
60	55	53-54 New	51-53 New	48-52	135	126	122-125	119-123	116-123
61	56 Be	53-55	51-54	49-53	136	127	123-126	120-124	117-123
62	56-57	54-56	52-55	50-54	137	128 Be	124-127	121-125	118-124
63	57-58	55-57	53-56	51-55	138	128	125-128	122-126	119-125
64	58-59	56-58	54-57	52-56	139	129	126-129	123-127	120-126
65	59-60	57-59	55-58	53-57	140	130	127-130	124-128	121-127
66	60-61	58-60	56-59	54-58	141	131	128-131	125-129	122-128
67	61-62	59-61	57-60	55-59	142	132	129-131	126-130	123-129
68	62-63	60-62	58-61 New	56-60 New	143	133	130-132	127-131	124-130
69	63-64	61-62	58-62	56-61	144	134	131-133	128-132 New	125-131 New
70	64	62-63	59-62	57-62	145	135	132-134 New	128-133	125-132
71	65	63-64	60-63	58-62	146	136	132-135	128-134	126-133
72	66	64-65 New	61-64	59-63	147	137	133-136	129-135	127-134
73	67	64-66	62-65	60-64	148	138	134-137	130-136	128-135
74	68	65-67	63-66	61-65	149	139	135-138	131-137	129-136
75	69	66-68	64-67 New	62-66	150	140 Be	136-139 New	132-137 New	130-137 New

- Ba - Simeon Ball [4]
- Be - Maximum distance separable code for $n < 19$ [5]
- New - new codes presented in this paper
- Gu - quasi-twisted code [19]
- Unmarked entries can be obtained by puncturing and extending techniques