Laaksonen, Antti; Östergård, Patric R.J.

New lower bounds on q-ary error-correcting codes

Published in:
CRYPTOGRAPHY AND COMMUNICATIONS

DOI:
10.1007/s12095-018-0302-9

Published: 15/09/2019

Document Version
Peer reviewed version

Please cite the original version:
Laaksonen, A., & Östergård, P. R. J. (2019). New lower bounds on q-ary error-correcting codes. *CRYPTOGRAPHY AND COMMUNICATIONS*, *11*(5), 881-889. https://doi.org/10.1007/s12095-018-0302-9

Cryptography and Communications manuscript No.
(will be inserted by the editor)

New Lower Bounds on q-ary Error-Correcting Codes

Antti Laaksonen · Patric R. J. Östergård

Received: date / Accepted: date

Abstract Let $A_q(n, d)$ denote the maximum size of a q-ary code with length n and minimum distance d. For most values of n and d, only lower and upper bounds on $A_q(n, d)$ are known. In this paper new lower bounds on and updated tables of $A_q(n, d)$ for $q \in \{3, 4, 5\}$ are presented. The new bounds are obtained through an extensive computer search for codes with prescribed groups of automorphisms. Groups that act transitively on the (coordinate,value) pairs as well as groups with certain other closely related actions are considered.

Keywords automorphism groups, bounds on codes, error-correcting codes, transitive groups

1 Introduction

A q-ary code C of length n is a subset of Z_q^n where $Z_q = \{0, 1, \ldots, q-1\}$. Each element $c \in C$ is called a *codeword*, and Z_q is called the *alphabet* of C. The *size* of C is $|C|$, and the *minimum distance* of C is

$$\min_{a,b \in C, a \neq b} d_H(a, b)$$

where d_H denotes the Hamming distance. A q-ary code with length n, size M and minimum distance at least d is called an $(n, M, d)_q$ code.

Let $A_q(n, d)$ denote the maximum size of an $(n, M, d)_q$ code. As it is difficult to determine exact values of $A_q(n, d)$, an important problem in coding theory is to find lower and upper bounds on this function. While binary codes have

This work was supported in part by the Academy of Finland, Project #289002.

Department of Communications and Networking
Aalto University School of Electrical Engineering
P.O.Box 15400, 00076 Aalto, Finland
E-mail: antti.2.laaksonen@aalto.fi, E-mail: patric.ostergard@aalto.fi

received the most attention [1], also ternary [6], quaternary [4] and quinary [5] codes have been studied in this context.

Lower bounds on $A_q(n,d)$ can be determined by constructing codes: if there is an $(n,M,d)_q$ code, then $A_q(n,d) \geq M$. Computer search techniques are often used to find such codes. However, as the search space gets very large already for relatively small parameters, assumptions about the structure of the code are usually needed to make such a search efficient enough.

One way to limit the search space is to assume that the codes have *symmetries*. Two q-ary codes are said to be *equivalent* if there is a permutation of the coordinates and permutations of the coordinate values, individually for each coordinate, that map one code to the other. Such a mapping from a code to itself is called an *automorphism*. The automorphisms form a group under composition, the *automorphism group* of the code. A subgroup of the automorphism group is called a *group of automorphisms*.

The approach of searching for codes with prescribed groups of automorphisms has been used in several studies, including [9,12,25]. One challenge in such an approach is that of deciding the class of groups and actions to consider. In [16], binary codes are obtained by focusing on codes with a group of automorphisms that acts transitively on the (coordinate,value) pairs. This approach is here extended to ternary ($q = 3$), quaternary ($q = 4$) and quinary ($q = 5$) codes. Preliminary results of the current study can be found in [17].

The structure of the rest of the paper is as follows: In Section 2, we discuss the method used for constructing codes with prescribed groups of automorphisms and carrying out the computer search. Then, in Section 3, we present the new lower bounds and updated tables of $A_q(n,d)$ for $q = 3$, $n \leq 16$; $q = 4$, $n \leq 12$; and $q = 5$, $n \leq 11$.

2 Code Construction

To study codes with prescribed groups of automorphisms, it is convenient to consider codes in the framework of set systems and represent codewords as sets of integers in the following way. Let $[n] = \{1, 2, \ldots, n\}$. The representation of a q-ary codeword $c_1 c_2 \cdots c_n$ is a set

$$\{c_k n + k \mid k \in [n]\},$$

so that each codeword is an n-element subset of $[nq]$. Automorphisms can then be studied in the context of permutations acting on $[nq]$. Notice that not all permutations of $[nq]$ are allowed, but a group of permutations must have a block system

$$\{\{k, n+k, \ldots, (q-1)n+k\} \mid k \in [n]\}. \tag{1}$$

A *block system* for the action of a group G on a set is defined as a partition of the set (into subsets called *blocks*) that is G-invariant, that is, each element of G maps a block to some block.

Consider a prescribed group of automorphisms G for a q-ary code of length n. The *orbit* of a word w is

$$\{gw \mid g \in G\}.$$

A code with G as a group of automorphisms consists of a union of such orbits of codewords, that is, for each orbit of words, either all words or no words are in the code.

Example: Let us construct a ternary code of length 4 with

$$G = \langle (1\ 5\ 9)(2\ 6\ 10)(3\ 7\ 11)(4)(8)(12) \rangle$$

as a group of automorphisms. Consequently, whenever we include a codeword $c_1c_2c_3c_4$ in the code, we must also include all other codewords of the form $(c_1 + i)(c_2 + i)(c_3 + i)c_4$ where $i \in Z_3$ and addition is carried out modulo 3. For example, we may then create the (Hamming) code

$$C = \{0000, 1110, 2220, 0121, 1201, 2011, 0212, 1022, 2102\},$$

which consists of three orbits whose representatives are, for example, 0000, 0121 and 0212.

To prove that $A_q(n, d) \geq M$, it suffices to find a code with size at least M and minimum distance d. For a fixed group of automorphisms G, the problem of finding such a code can be transformed into the problem of finding a clique of weight at least M in the following graph [15, Sect. 9.3.2]: For each orbit where the distance between any two words is at least d, there is a vertex. The weight of such a vertex is the number of words in the orbit. There is further an edge between two vertices if the distance between any two words in the corresponding orbits is at least d.

For given parameters q and n, we now search for codes by prescribing a group of automorphisms G that acts transitively on $[qn]$, that is, the permutation group has degree qn. Transitive permutation groups have been classified [7,11] up to degree 47, so we may systematically consider all transitive groups of degree qn as long as $qn \leq 47$.

For a prescribed permutation group G, we first generate all block systems of G with block size q and for each such block system, we relabel the elements of $[qn]$ so that the blocks are of the form (1). Finally, we conduct a search for cliques of large weight in the graph defined earlier.

In addition to transitive group actions on all elements in $[qn]$, we consider the following four types of actions. We search for q-ary codes of length $n + 1$ such that G acts transitively on the (coordinate,value) pairs of n coordinates and fixes one coordinate and its values—in other words, we have a transitive action on a subset $[qn]$ of a set $[q(n+1)]$. We further search for q-ary codes of length nk using k copies of G that act transitively and simultaneously on the (coordinate,value) pairs of n coordinates each, and we also search for q-ary codes of length $nk+1$ by combining the two previous cases. Finally, we search

for q-ary codes of length n such that G acts transitively on (coordinate,value) pairs considering just $q-1$ of the coordinate values and fixing one coordinate value.

We use the *Cliquer* software [22] to find maximum-weight cliques in graphs. We restricted ourselves to graphs that contain at most 5000 vertices, because processing larger graphs would have been too slow. Each clique search was run for at most 1000 seconds; in most cases the maximum-weight clique was found in a couple of seconds.

3 New Lower Bounds

We study $A_3(n,d)$ for $n \leq 16$, $A_4(n,d)$ for $n \leq 12$ and $A_5(n,d)$ for $n \leq 11$. The current work led to 22 new lower bounds for those parameters, three of which—$A_3(14,4)$, $A_4(8,5)$ and $A_5(7,4)$—follow from other new bounds either through

$$A_q(n+1,d) \leq qA_q(n,d) \tag{2}$$

or

$$A_q(n+1,d+1) \leq A_q(n,d). \tag{3}$$

The new codes are listed in the Appendix and in the presentation [17] of preliminary results of the current study.

Tables 1, 2 and 3 contain the current best known lower and upper bound for $A_3(n,d)$, $A_4(n,d)$ and $A_5(n,d)$, respectively, in the above mentioned ranges (for $q=3$ we further have [6] $A_3(16,12)=9$, $A_3(15,12)=6$, $A_3(16,13)=4$ and $A_3(n,d)=3$ for $0 \leq n-d \leq 2$, $12 \leq d \leq 16$). The tables update earlier tables published in [6,27] for $q=3$, in [4] for $q=4$, and in [5] for $q=5$. The new lower bounds obtained in the current work are marked in boldface in the tables.

Acknowledgments

Electronic tables of bounds maintained by Andries Brouwer have been of great help to the authors.

References

1. Agrell, E., Vardy, A., Zeger, K.: A table of upper bounds for binary codes. IEEE Trans. Inform. Theory 47, 3004–3006 (2001)
2. Bellini, E., Guerrini, E., Sala, M.: Some bounds on the size of codes. IEEE Trans. Inform. Theory 60, 1475–1480 (2014)
3. Blokhuis, A., Brouwer, A. E.: Small additive quaternary codes. European J. Combin. 25, 161–167 (2004)
4. Bogdanova, G. T., Brouwer, A. E., Kapralov, S. N., Östergård, P. R. J.: Error-correcting codes over an alphabet of four elements. Des. Codes Cryptogr. 23, 333–342 (2001)
5. Bogdanova, G. T., Östergård, P. R. J.: Bounds on codes over an alphabet of five elements. Discrete Math. 240, 13–19 (2001)

Table 1: Bounds on $A_3(n,d)$ for $n \leq 16$, $d \leq 11$

$n\backslash d$	3	4	5	6	7	8	9	10	11
3	3								
4	9	3							
5	18	6	3						
6	38^{e}	18	4	3					
7	111^{e} 99	33^{f}	10	3	3				
8	333^{d} 252_{b}	99^{d}	27	9	3	3			
9	937 729	297^{d} 243	81	27	6	3	3		
10	2808^{g} 2187	891^{d} 729	243	81	14^{h}	6	3	3	
11	7029 6561	2561 1458	729	243	36^{i}	12	4	3	3
12	19683	6839^{j} 4374	1557^{j} 729	729	108^{d} 60_{b}	36	9	4	3
13	59049	19270^{j} **13122**	4078^{j} 2187	1449^{j} 729	324^{d} 162_{b}	95^{j} 54_{b}	27	6	3
14	153527 118098	54774^{j} **27702**$_{a}$	10624^{j} 6561	3660^{j} 2187	805^{j} 243	237 108_{b}	62^{j} 36_{b}	13^{k}_{c}	6
15	434815 354294	149585^{j} **83106**	29213^{j} **7812**	9904^{j} **3321**	2204^{j} 729	685^{j} 243	165^{j} 81	39^{d} 27	10
16	1240029^{l} 1062882	424001^{j} 216513	77217 19683	27356^{j} 6561	6235^{j} **1026**	1923^{j} **387**	451 243	114^{j} 54	29^{m} 18

Unmarked bounds are from Brouwer, Hämäläinen, Östergård, Sloane [6].
Lower bounds: a – (2), b – Discussions on *Foros de Free1X2.com* [8], c – Letourneau, Houghten [19]
Upper bounds: d – (2), e – Östergård [24], f – Östergård [23], g – Lang, Quistorff, Schneider [18], h – Kapralov [13], i – Letourneau, Houghten [19], j – Gijswijt, Schrijver, Tanaka [10], k – Kaski, Östergård [14], l – Bellini, Guerrini, Sala [2], m – Polak [26]

6. Brouwer, A. E., Hämäläinen, H. O., Östergård, P. R. J, Sloane, N. J. A.: Bounds on mixed binary/ternary codes. IEEE Trans. Inform. Theory 44, 140–161 (1998)
7. Cannon, J. J., Holt, D. F.: The transitive permutation groups of degree 32. Exp. Math. 17, 307–314 (2008)
8. Discussions on *Foros de Free1X2.com*, cited by Andries Brouwer at `https://www.win.tue.nl/~aeb/codes/ternary-1.html`
9. Elssel, K., Zimmermann, K.-H.: Two new nonlinear binary codes. IEEE Trans. Inform. Theory 51, 1189–1190 (2005)
10. Gijswijt, D., Schrijver, A., Tanaka, H.: New upper bounds for nonbinary codes based on the Terwilliger algebra and semidefinite programming. J. Combin. Theory Ser. A 113, 1719–1731 (2006)
11. Hulpke, A.: Constructing transitive permutation groups. J. Symbolic Comput. 39, 1–30 (2005)
12. Kaikkonen, M. K.: Codes from affine permutation groups. Des. Codes Cryptogr. 15, 183–186 (1998)
13. Kapralov, K. S.: The nonexistence of ternary (10,15,7) codes. In Proc. 7th International Workshop on Algebraic and Combinatorial Coding Theory, (ACCT'2000), Bansko, Bulgaria, 18–24 June, 2000, 189–192 (2000)

Table 2: Bounds on $A_4(n, d)$ for $n \leq 12$

$n \setminus d$	3	4	5	6	7	8	9	10	11	12
3	4									
4	16	4								
5	64	16	4							
6	176^{e} 164	64	9	4						
7	596^{e} 512	155^{e} 128	32	8	4					
8	2340 2048	611^{f} **352**	128 $\mathbf{76}_{a}$	32	5	4				
9	9344^{g} 8192	2314^{f} **1152**	512 256	120^{h} **76**	20 18	5	4			
10	30427 **24576**	8951^{f} **4192**	2045^{f} 1024	480^{d} 256	80 48_{a}	16	5	4		
11	109226 **77056**	30427 16384	6241 4096	1780^{f} 1024	320 128_{a}	60^{h} 48_{a}	12	4	4	
12	419430 262144	109226 65536	20852 8192	5864^{f} 4096	1167^{f} 256	240^{d} 128_{b}	48_{c}	9	4	4

Unmarked bounds are from Bogdanova, Brouwer, Kapralov, Östergård [4].
Lower bounds: a – (3), b – Blokhuis, Brouwer [3], c – Mackenzie, Seberry [21]
Upper bounds: d – (2), e – Litjens, Polak, Schrijver [20], f – Gijswijt, Schrijver, Tanaka [10], g – Lang, Quistorff, Schneider [18], h – Polak [26]

Table 3: Bounds on $A_5(n, d)$ for $n \leq 11$

$n \setminus d$	3	4	5	6	7	8	9	10	11
3	5								
4	25	5							
5	125	25	5						
6	625	125	25	5					
7	2291 1597	489^{d} $\mathbf{257}_{a}$	87^{d} **57**	15	5				
8	9672 7985	2291 **1225**	435^{c} **257**	65^{e} 50_{a}	10	5			
9	44642 31040	9672 **4375**	2152^{f} **857**	325^{c} **157**	50_{a}	10	5		
10	217013 125000	44642 **17500**	9559^{f} 3125	1625^{c} 625	250 125	50_{b}	7	5	
11	1085053^{g} 468750	217013 78125	44379^{f} 15625	8125^{c} 3125	1250 625	250 125	35 25	6	5

Unmarked bounds are from Bogdanova, Östergård [5].
Lower bounds: a – (3), b – Mackenzie, Seberry [21]
Upper bounds: c – (2), d – Litjens, Polak, Schrijver [20], e – Polak [26], f – Gijswijt, Schrijver, Tanaka [10], g – Lang, Quistorff, Schneider [18]

14. Kaski, P., Östergård, P. R. J.: There exists no (15,5,4) RBIBD. J. Combin. Des. 9, 227–232 (2001)
15. Kaski, P., Östergård, P. R. J.: Classification Algorithms for Codes and Designs, Springer, Berlin (2006)
16. Laaksonen, A., Östergård, P. R. J.: Constructing error-correcting binary codes using transitive permutation groups. Discrete Appl. Math. 233, 65–70 (2017)
17. Laaksonen, A., Östergård, P. R. J.: New lower bounds on error-correcting ternary, quaternary and quinary codes. In Coding Theory and Applications, Barbero, Á., Skachek, V., Ytrehus, Ø. (Editors), LNCS 10495, Springer, Cham, 228–237 (2017)
18. Lang, W., Quistorff, J., Schneider, E.: New results on integer programming for codes. Congr. Numer. 188, 97–107 (2007)
19. Letourneau, M. J., Houghten, S. K.: Optimal ternary (11,7) and (14,10) error-correcting codes. J. Combin. Math. Combin. Comput. 51, 159–164 (2004)
20. Litjens, B., Polak, S., Schrijver, A.: Semidefinite bounds for nonbinary codes based on quadruples. Des. Codes Cryptogr. 84, 87–100 (2016)
21. Mackenzie, C., Seberry, J.: Maximal q-ary codes and Plotkin's bound. Ars Combin. 26B, 37–50 (1988)
22. Niskanen, S., Östergård, P. R. J.: Cliquer User's Guide, Version 1.0, Communications Laboratory, Helsinki University of Technology, Espoo, Finland, Tech. Rep. T48 (2003)
23. Östergård, P. R. J.: On binary/ternary error-correcting codes with minimum distance 4. In Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Fossorier, M., Imai, H., Lin, S., Poli, A. (Editors), LNCS 1719, Springer, Berlin, 472–481 (1999)
24. Östergård, P. R. J.: Classification of binary/ternary one-error-correcting codes. Discrete Math. 223, 253–262 (2000)
25. Östergård, P. R. J.: Two new four-error-correcting binary codes. Des. Codes Cryptogr. 36, 327–329 (2005)
26. Polak, S. C.: New nonbinary code bounds based on divisibility arguments. Des. Codes Cryptogr. 86, 861–874 (2018)
27. Vaessens, R. J. M., Aarts, E. H. L., van Lint, J. H.: Genetic algorithms in coding theory – a table for $A_3(n, d)$. Discrete Appl. Math. 45, 71–87 (1993)

Appendix: Codes Attaining New Lower Bounds

Bound: $A_5(7, 5) \geq 57$
Generators of G:
(2 9)(3 17)(4 11)(5 26)(6 27)(7 21)(10 24)(12 19)(13 20)(14 28)(16 23)(18 25),
(1 3 5 14 23 25 27)(2 4 6 22 24 26 21)(7 16 18 20 8 10 12)
(9 11 13 15 17 19 28)(29 31 33 35 30 32 34)
Orbit representatives:
0304000, 4444444

Bound: $A_5(8, 5) \geq 257$
(1 14 9 6)(2 21 26 13)(3 8 19 24)(4 15)(5 10 29 18)(7 12)
(11 16 27 32)(17 30 25 22)(20 31)(23 28)(33 38)(34 37)(35 40)(36 39),
(1 28 17 4)(2 27)(3 26)(5 16 21 32)(6 7 14 15)(8 29 24 13)
(9 20 25 12)(10 19)(11 18)(22 31 30 23)(33 36)(34 35)(37 40)(38 39),
(1 32 25 16)(2 15 10 7)(3 14 27 30)(4 5)(6 19 22 11)(8 9 24 17)
(12 13)(18 31 26 23)(20 21)(28 29)(33 40)(34 39)(35 38)(36 37)
Orbit representatives:
21401000, 44444444

Bound: $A_5(9,5) \geq 857$
Generators of G:
(1 30 24 14)(2 35 25 36)(3 33 23 19)(4 13)(5 10 12 6)(7 9 11 8)
(15 32 28 21)(16 18 29 17)(20 26 34 27)(22 31)(37 39 42 41)(38 44 43 45),
(1 11 34)(2 7 28)(3 22 17)(4 8 30)(5 9 33)(6 32 27)(10 29 16)(12 31 35)
(13 26 21)(14 18 24)(15 23 36)(19 20 25)(37 38 43)(39 40 44)(41 45 42)
Orbit representatives:
114040000, 312431000, 221012000, 443423000, 334241100, 000322200, 224143300,
401410010, 024433010, 023240110, 031121110, 112402410, 444444444

Bound: $A_5(9,6) \geq 157$
Generators of G:
(1 3 2)(4 31 22)(5 32 23)(6 33 24)(7 35 18)(8 36 16)(9 34 17)
(10 30 20)(11 28 21)(12 29 19)(25 26 27)(37 39 38)(43 44 45),
(1 18 32 2 16 31 3 17 33)(4 21 26 6 19 27 5 20 25)(7 13 30 8 15 28 9 14 29)
(10 36 23 11 34 22 12 35 24)(37 45 41 38 43 40 39 44 42)
Orbit representatives:
111000000, 412423100, 144310210, 444444444