International Journal of Mathematics and
Computer Science, **17**(2022), no. 2, 923–930

On the construction of of q-ary constant-weight lexicodes

Galina Bogdanova[1], **Todor Todorov**[1,2]

[1]Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Sofia, 1040, Bulgaria

[2]Faculty of Mathematics and Informatics
St. Cyril and St. Methodius University of Veliko
Tarnovo, Bulgaria

email: galina@math.bas.bg, todor@math.bas.bg

(Received December 6, 2021)

Abstract

In this paper, we study the maximum number of codewords for equidistant codes with additional restriction to be constant-weight and lexicographic. We consider codes that are ternary, quaternary and over the alphabet with five elements. We use both computer and combinatorial methods.

These error-correcting codes are used for data security in a specialized scientific project with a specialized information system with security sensitive data.

1 Introduction

Let $Z_q(n, w)$ be the set of all vectors over Z_q with length n and Hamming weight w and let $(n, M, d)_q$ be an equidistant code or EC with length n, number of codewords M, and same Hamming distance d between distinct codewords. Denote by $B_q(n, d)$ the maximum number of codewords for such

Key words and phrases: Lexicographic codes, Equidistant codes, Constant-weight codes, Bounds of codes.
AMS (MOS) Subject Classifications: 68R05, 94B65.
ISSN 1814-0432, 2022, http://ijmcs.future-in-tech.net

code with other fixed parameters. Equidistant codes and their relation to other combinatorial structures were considered in [1], [2].

Let $(n, M, d, w)_q$ denote a constant-weight equidistant code or ECWC with length n, number of codewords M, same Hamming distance d between distinct codewords and same Hamming weight w for each codeword. We use the notation $B_q(n, d, w)$ for the maximum number of codewords for such code with other fixed parameters. Constant-weight codes were investigated in numerous scientific papers; for example, in [3], [4].

Let B be an ordered base $b_1, b_2, \ldots, b_n$ over Z_q^n and let $x = \lambda b_1 + \lambda b_2 + \cdots + \lambda b_n$ and $y = \mu b_1 + \mu b_2 + \cdots + \mu b_n$ be vectors in Z_q^n.

We say that x precedes y in lexicographical order if $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ precedes $(\mu_1, \mu_2, \ldots, \mu_n)$ in lexicographical order; i.e., $\lambda_1 \leq \mu_1, \lambda_2 \leq \mu_2, \lambda_n \leq \mu_n$.

Lexicographic codes with given parameters can be generated using the q-ary codewords with weight w. We add such vectors to the code if they comply to the distance restriction (to be on distance exactly d from other codewords) [5].

In this paper, we consider the maximum number of codewords for equidistant codes with additional restriction to be constant-weight and lexicographic.

The codes we consider are ternary, quaternary and over the alphabet with five elements.

We improve our search algorithms and recalculate bounds from previous results [8]. These codes are used for data security in the project Digital Accessibility for People with Special Needs: Methodology, Conceptual Models and Innovative EcoSystems. In this project, we design a specialized information system with security sensitive data using watermarking technologies in order to secure authorship of unique digital data. Our considered error-correcting codes are used as an additional technique before data are used for watermarking.

2 Preliminaries

In the following theorems we use combinatorial methods for equidistant and constant-weight codes construction.

Theorem 2.1. *[6]* $B_q(n, d) \leq \frac{dq}{dq - n(q-1)}$.

Theorem 2.2. *[4]* $$B_q(n, d) = 1 + B_q(n, d, d).$$

Theorem 2.3. *[7]* $$B_q(n, d) \leq (q-1)n + 1.$$

Theorem 2.4. $B_q(n,n,w) \leq q,$

$$B_q(n+1,d,w) \geq B_q(n,d,w), \qquad B_q(n+1,d,w+1) \geq B_q(n,d,w).$$

Theorem 2.5. (Trivial values) $B_3(n,d,w) = 1$ *if* $d > 2w$, $B_q(n,d,n) = B_{q-1}(n,d)$.

Theorem 2.6. (Johnson bounds for ECWC) *The maximum number of codewords in a q-ary ECWC satisfy the inequalities:*

$B_q(n,d,w) \leq \frac{n}{n-w} B_q(n-1,d,w)$, $B_q(n,d,w) \leq \frac{n(q-1)}{w} B_q(n-1,d,w-1)$.

Theorem 2.7. *[4] For* $k = 1,2,...,n$, *if* $P_k^2(w) > P_k(d) P_k(0)$, *then*

$$B_q(n,d,w) \leq \frac{P_k^2(0) - P_k(d) P_k(0)}{P_k^2(w) - P_k(d) P_k(0)}.$$

Here $P_k(x)$ is the Krawtchouk polynomial defined by

$$P_k(x) = \sum_{i=0}^{k} \binom{x}{i} \binom{n-x}{k} (q-1)^k.$$

Theorem 2.8. *If there exists an* $(n,M,d,w)_q$ *code, then there exists a* $(\lambda n, M, \lambda d, \lambda w)_q$ *code for all integers* $\lambda \geq 1$.

3 Algorithms for computer search

We use computer search algorithms to find values for lexicographic $B_q(n,d,w)$ for ECWC codes with given parameters. To achieve the goal, we consider a set of all possible codewords and join them to the code if they have weight w and comply to the distance restriction (to be on distance exactly d from other codewords). To improve our method, we use combinatorial observations from the previous section.

Also, we use a modification of lexicographic searching called search with seed where the starting set of vectors contains predefined codewords (seed) and is not empty.

Using this approach, the crucial part becomes the selection of proper seed. In our research, we apply two methods for seed selection. First, we use an exhaustive search and try with all possible subsets from restricted area of Z_q^n as a seed. Secondly, we use a randomly selected set as a seed.

We also perform a cyclic shift of the space in some cases (see Figure 1). In such a situation, we have two lexicographically ordered parts.

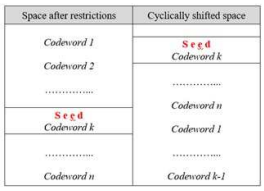

Figure 1: Cyclic shift of space

$(9,3,3,3)_4$ No seed
000000111
000000222
000000333

Figure 2: $(9, 3, 3, 3)_4$- No seed

As an example, consider searching of $(9, 8, 3, 3)_4$ lexicographic constant-weight equidistant code.

If we apply our search without a seed, the best code that we can obtain is with three codewords (see Figure 2).

However, if we use search with a seed, then we can obtain code with eight codewords (coincides with optimal code) (see Figure 3).

$(9,8,3,3)_4$ Seed 000001011
000001011
000000112
000000221
000001120
000001202
000002022
000002101
000002210

Figure 3: $(9, 8, 3, 3)_4$ - Seed 000001011

n	w	d							
		3	4	5	6	7	8	9	10
4	2	3	2						
	3	8	2						
5	2	3	2						
	3	8	5	2					
	4	8	5	2					
6	2	3	3						
	3	8	5	4	2				
	4	8	6	4	3				
	5	8	6	3	2				
7	2	3	3						
	3	8	7	4	2				
	4	8	7	7	3	2			
	5	8	6	6	3	2			
	6	8	6	7	2	2			
8	2	3	4						
	3	8	7	4	2				
	4	8	7	7	5	2	2		
	5	8	8	7	8	3	2		
	6	8	6	7	8	3	2		
	7	8	8	8	4	2	2		
9	2	3	4						
	3	8	7	4	3				
	4	8	7	7	9	3	2		
	5	8	8	7	9	5	3	2	
	6	8	8	7	11	6	3	3	
	7	8	8	8	12	5	3	2	
	8	8	8	8	9	3	2	2	
10	2	3	5						
	3	8	7	4	3				
	4	8	7	7	15	5	2		
	5	8	8	7	11	8	4	2	2
	6	8	8	7	14	8	5	3	2
	7	8	8	8	12	9	5	3	2
	8	8	8	8	12	10	5	2	2
	9	8	8	8	10	5	2	2	2

Table 1: Lexicographic $B_3(n, d, w)$

4 Algorithms for computer search

Results

In Tables 1, 2 and 3, we present results from a lexicographic search of constant-weight equidistant codes with different parameters over the alphabets with three four and five elements. We perform a lexicographic search with and without a seed. These algorithms are included in a developed specialized software which has various settings that could improve the setup of the seed that will be used in searching. These include selection of the size of the seed, a manual seed design and an automatic variation of possible seeds. The last option is very important if we want to find the code with maximum number of codewords for a given parameter. Also, the software package that we develop and use implements the algorithm for cyclic shift of space described in the previous section.

n	w	d							
		3	4	5	6	7	8	9	10
4	2	3	2						
	3	8	4						
	4	9	3						
5	2	3	2						
	3	8	10	2					
	4	9	15	3					
	5	9	6	3					
6	2	3	3						
	3	8	10	4	2				
	4	9	15	9	3				
	5	9	15	8	3				
	6	9	7	4	3				
7	2	3	3						
	3	8	10	7	2				
	4	9	15	9	5	2			
	5	9	15	9	7	3			
	6	9	15	9	7	3			
	7	9	8	7	3	3			
8	2	3	4						
	3	8	10	7	2				
	4	9	15	9	8	2	2		
	5	9	15	11	10	5	2		
	6	9	15	9	12	5	4		
	7	9	15	11	12	4	3		
	8	9	8	8	9	3	3		
9	2	3	4						
	3	8	10	7	3				
	4	9	15	9	9	3	2		
	5	9	15	11	10	9	3	2	
	6	9	15	11	12	11	5	3	
	7	9	15	11	12	11	5	3	
	8	9	15	11	12	11	4	3	
	9	9	8	8	12	6	3	3	
10	2	3	5						
	3	8	10	7	3				
	4	9	15	9	15	5	2		
	5	9	15	11	10	10	6	2	2
	6	9	15	11	14	11	10	5	2
	7	9	15	11	12	11	14	5	3
	8	9	15	11	12	11	15	5	3
	9	9	15	11	12	11	10	4	3
	10	9	8	8	9	10	6	3	3

Table 2: Lexicographic $B_4(n, d, w)$

n	w	d							
		3	4	5	6	7	8	9	10
4	2	3	2						
	3	8	4						
	4	9	4						
5	2	4	2						
	3	8	10	2					
	4	9	15	5					
	5	9	16	4					
6	2	3	3						
	3	8	10	4	2				
	4	9	15	9	3				
	5	9	16	24	4				
	6	9	16	9	4				
7	2	4	3						
	3	8	10	7	2				
	4	9	15	13	6	2			
	5	9	16	24	12	3			
	6	9	16	24	14	4			
	7	9	16	10	8	4			
8	2	4	4						
	3	8	10	7	2				
	4	9	15	13	9	2	2		
	5	9	16	24	9	6	2		
	6	9	16	24	12	7	4		
	7	9	16	24	10	4	4		
	8	9	16	10	12	5	4		
9	2	4	4						
	3	8	10	7	3				
	4	9	15	13	11	3	2		
	5	9	16	24	9	8	3	2	
	6	9	16	24	11	10	6	3	
	7	9	16	24	10	4	6	4	
	8	9	16	24	12	4	4	4	
	9	9	16	10	12	4	4	4	
10	2	4	5						
	3	8	10	7	3				
	4	9	15	13	15	5	2		
	5	9	16	24	9	9	6	2	2
	6	9	16	24	11	10	10	3	2
	7	9	16	24	10	4	9	6	3
	8	9	16	24	12	4	4	5	5
	9	9	16	24	12	4	4	4	4
	10	9	16	10	12	4	10	4	4

Table 3: Lexicographic $B_5(n, d, w)$

5 Conclusion

In this paper, we studied the maximum number of codewords for equidistant codes with additional restriction to be constant-weight and lexicographic. It is important to notice that in many cases, the bounds found with lexicographic methods are the same with the optimal codes with given parameters.

Acknowledgment. This research was funded by the National Science Fund of Bulgaria (scientific project Digital Accessibility for People with Special Needs: Methodology, Conceptual Models and Innovative EcoSystems), Grant Number KP-06-N42/4, 08.12.2020

References

[1] J. I. Hall, A. J. E. M. Jansen, A. W. J. Kolen, J. H. van Lint, Equidistant codes with distance 12, Discrete Math., **17,** (1977), 71–83.

[2] N. V. Semakov, V. A. Zinoviev, Equidistant q-ary codes with maximal distance and resolvable balanced incomplete block designs, Problemi peredachi Informatsii, **4,** no. 2, (1968), 3–10.

[3] E. Agrell, A. Vardy, K. Zeger, Upper bounds for constant-weight codes, IEEE Trans. Inform. Theory, **IT-46,** (2000), 2373–2395.

[4] F. W. Fu, T. Klove, Y. Luo, V. K. Wei, On equidistant Constant Weight codes. In proceedings WCC2001 Workshop on Coding and Cryptography, Paris, France, (2001), 225–232.

[5] J. H. Conway, Integral lexicographic codes, Discrete Math., **83,** (1990), 219–235.

[6] M. Plotkin, Binary codes with specified minimum distance, IRE Trans. Inform. Theory, **6,** (1960), 445–450.

[7] P. Delsarte, Bounds for unrestricted codes, by linear programming, Philips Res., Rep. 27, (1972), 47–64.

[8] T. Todorov, G. Bogdanova, T. Yorgova, Lexicographic Constant-Weight Equidistant Codes over the Alphabet of Three, Four and Five Elements, Intelligent Information Management, **2,** no. 3, (2010), 183–187.