Seventh International Workshop on Optimal Codes and Related Topics
September 6-12, 2013, Albena, Bulgaria *pp. 33-40*

On q-ary optimal equitable symbol weight codes[1]

L. A. Bassalygo `bass@iitp.ru`
V. A. Zinoviev `zinov@iitp.ru`
A.A. Kharkevich Institute for Problems of Information Transmission,
Russian Academy of Sciences, Moscow, RUSSIA

Dedicated to the memory of Professor Stefan Dodunekov

Abstract. Two new families of optimal equitable symbol weight q-ary codes are constructed.

1 Introduction

Denote by $Q = \{0, 1, \ldots, q-1\}$ an alphabet of size q and by Q^n the set of all words of length n over Q. Let $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ be an arbitrary word over Q. Denote by $\xi_a(\boldsymbol{x})$ the number of times the symbol $a \in Q$ occurs in $\boldsymbol{x}$, i.e.

$$\xi_a(\boldsymbol{x}) = |\{j : \, x_j = a, \; j = 1, 2, \ldots, n\}|.$$

Say that $\boldsymbol{x} \in Q^n$ has *equitable symbol weight* if $\xi_a(\boldsymbol{x}) \in \{\lfloor n/q \rfloor, \lceil n/q \rceil\}$ for every $a \in Q$.

Definition 1. *A code $C \subset Q^n$ we call* equitable symbol weight code*, if every its codeword has equitable symbol weight.*

Denote such q-ary equitable symbol weight codes of length n, cardinality M and with minimum distance d by $E(n, M, d; q)$. Equitable symbol weight codes were recently introduced in [1] for more precisely capture a code's performance against permanent narrowband noise in power line communication [2]. Several optimal infinite families of such codes were constructed in [1,3]. In particular, a family of optimal equitable symbol weight codes $E(n, M, d; q)$ was constructed in [3] with parameters

$$n = q^2 - 1, \;\; M = q^2, \;\; d = q(q-1), \tag{1}$$

for any $q = p^s$, where p is any odd prime number.

[1] This work has been partially supported by the Russian fund of fundamental researches (under the project No. 12 - 01 - 00905).

In this paper we construct, using the other approach, equitable symbol weight codes with parameters (1) for $q = p^s \geq 3$, where p is any prime number, i.e. including the case $p = 2$. Besides, a family of optimal equitable symbol weight q-ary codes is constructed with parameters

$$n, \;\; M = q(n-1), \;\; d = n(q-1)/q, \tag{2}$$

where n is such, that there exists a difference matrix of size $n \times n$ over the alphabet Q.

2 Main construction

It is well known (see, for example, [4,5] and references there) that optimal equidistant q-ary codes of length $q^2 - 1$, with minimum distance $q(q-1)$ and cardinality q^2 can be easily constructed for any prime power $q \geq 3$. These codes are not equitable symbol weight, but it is possible to reconstruct them such that they become equitable symbol weight codes without missing the property to be equidistant. To describe the construction of these codes we need a concept of a Latin square. A square matrix of size q over an alphabet Q is called a Latin square of order q, if every element occurs once in every row and in every column.

Let A be a matrix of size $q \times q$ of form

$$\begin{bmatrix} 0 & 0 & \ldots & 0 \\ 1 & 1 & \ldots & 1 \\ \cdot & \cdot & \ldots & \cdot \\ q-1 & q-1 & \ldots & q-1 \end{bmatrix},$$

and let $L_1, L_2, \ldots, L_{q-1}$ be a set of $q-1$ Latin squares of order q over Q with the following property: the pairwise distance between any two rows of different squares is equal to $q-1$ (it is clear that the pairwise distance between any two rows of one square is equal to q). The rows of the following matrix of size $q^2 \times (q^2-1)$ form an equidistant code with distance $d = q(q-1)$:

$$\begin{bmatrix} A & \cdots A & \boldsymbol{e}_0 & \boldsymbol{e}_1 \cdots & \boldsymbol{e}_{q-2} \\ L_1 & \cdots L_1 & \boldsymbol{e}_1 & \boldsymbol{e}_2 \cdots & \boldsymbol{e}_{q-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ L_{q-1} & \cdots L_{q-1} & \boldsymbol{e}_{q-1} & \boldsymbol{e}_0 \cdots & \boldsymbol{e}_{q-3} \end{bmatrix},$$

where $\boldsymbol{e}_i$ is the column-vector $(i \, i \, \ldots \, i)^t$. Under reconstruction of this matrix the last $q-1$ columns remain unchanged such that only the first $q(q-1)$ columns undergo to transformation. Denote by K the matrix of size $q^2 \times q(q-1)$, formed by the first these $q(q-1)$ columns. We suggest a such reconstruction of the matrix K, which keeps all pairwise distances between rows, but the matrix transforms to equitable symbol weight type, i.e. it contains every symbol in every row exactly $q-1$ times. It is enough, since in the last $q-1$ positions all elements are different in every row. The condition of equality of occurences of different elements is not satisfied in the first layer of the matrix K:

$$[\, A\; A\; \cdots\; A \,]$$

and we start reconstruction by adding to every row of matrix K the vector

$$\boldsymbol{a} = (\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_{q-1}),$$

where the vector $\boldsymbol{a}_j$ of length q is of the form $(0, j, j, \ldots, j)$. For this purpose we have to define the addition operation in the alphabet Q. Since q is a power of a prime number, to the every nonzero element $i \in Q$ set in correspondence the element α^{i-1}, where α is a primitive element of the Galois field $\mathbf{F}_q$, and to $0 \in Q$ set in correspondence the zero element of $\mathbf{F}_q$. Define the addition operation $\oplus$ in Q as follows: $i \oplus j = k$, where k is such that $\alpha^{i-1} + \alpha^{j-1} = \alpha^{k-1}$.

After adding of $\boldsymbol{a}$ to the first layer of the matrix K the resulting $q \times q(q-1)$ submatrix becomes of equitable symbol weight type. Further we will reconstruct every i-th layer of the matrix $K \oplus \boldsymbol{a}$ separately:

$$\left[\, L_i^{(1)}\; L_i^{(2)}\; \cdots\; L_i^{(q-1)} \,\right],$$

where $L_i^{(j)}$ is obtained from L_i by adding of vector $\boldsymbol{a}_j$ to the every row of matrix L_i.

The reconstruction would be concluded in permutation of rows in the every matrix $L_i^{(j)}$ independently. Evidently such permutation does not change the distance properties of the matrix K and by this way the every i-th, $i = 1, 2, \ldots, q-1$, layer we will transform to equitable symbol weight type.

Without loss of generality we assume that the first column of the matrix L_i and, therefore, the first column of all matrices $L_i^{(j)}$, $j = 1, 2, \ldots, q-1$, is of the form

$$\begin{bmatrix} 0 \\ 1 \\ \cdots \\ q-1 \end{bmatrix}.$$

In this case the k-th row of the every matrix $L_i^{(j)}$ contains the element k exactly two times and does not contain the element $k \oplus j$, and all other $q-2$ elements of Q occur exactly once. Similarly the ℓ-th column of the every matrix $L_i^{(j)}$ contains the element ℓ exactly two times and does not contain the element $k \ominus j$, and all other $q-2$ elements of Q occur exactly once.

Now set in correspondence to every matrix $L_i^{(j)}$ the integer matrix $B_i^{(j)} = [b_{k,\ell}^{(j)}]$ of size $q \times q$ over the numbers $0, 1, 2$ in the following way:

$$b_{k,\ell}^{(j)} = \begin{cases} 2, & \text{if} \quad k = \ell, \\ 0, & \text{if} \quad k \oplus j = \ell, \\ 1, & \text{in other cases} \end{cases}$$

To finish the proof we have to choose from the every matrix $B_i^{(j)}$, $j = 1, 2, \ldots, q-1$, one row $\boldsymbol{r}^{(j)}$ in such way that the usual sum (i.e. sum in $\mathbf{Z}$) of all these rows would be equal to $q-1$ for every position:

$$\boldsymbol{r}^{(1)} + \boldsymbol{r}^{(2)} + \cdots + \boldsymbol{r}^{(q-1)} = (q-1, q-1, \ldots, q-1). \tag{3}$$

This gives us one equal symbol weight row of length $q(q-1)$ and we will continue this procedure with the rest rows.

Now we explain how to make it. Taking the first arbitrary s_1-th row $\boldsymbol{r}_{s_1}^{(1)}$ from the first matrix $B_i^{(1)}$ (which contains the number 2 in s_1-th position), in the second matrix $B_i^{(2)}$ chose the row $\boldsymbol{r}_{s_2}^{(2)}$, which contains the number 0 in the position s_1, implying that $s_2 = s_1 \ominus 2$. Then the row s_2 contains the number 2 in s_2-th column, hence in the third matrix $B_i^{(3)}$ chose the row $\boldsymbol{r}_{s_3}^{(3)}$ with $s_3 = s_2 \ominus 3 = s_1 \ominus 2 \ominus 3$ and so on. Finally chose the row $\boldsymbol{r}_{s_{q-1}}^{(q-1)}$ in the matrix $B_i^{(q-1)}$ with

$$s_{q-1} = s_1 \ominus 2 \ominus 3 \cdots \ominus (q-1).$$

As we know the matrix $B_i^{(1)}$ contains in the s_1-th row the number 0 in the position $s_1 \oplus 1$. Since

$$s_1 \oplus 1 = s_1 \ominus 2 \ominus 3 \cdots \ominus (q-1),$$

the number 2 of the last row $\boldsymbol{r}_{s_{q-1}}^{(q-1)}$ occupies the same position as the number 0 of the first row $\boldsymbol{r}_{s_1}^{(1)}$. More short cycles are also possible, but it does not change the merits of the case. Thus the equality (3) is satisfied for any choice of the first row of the matrix $B_i^{(1)}$. Since the choice of the first row defines uniquely the choice of the other rows, this equality is valid for all rows of the i-th layer of the matrix K.

This completes the proof, since the given method does not depend on the index i. The fact that these codes are optimal directly follows from the well known Plotkin upper bound.

Therefore the following result takes place.

Theorem 1. *Let $q \geq 3$ be any prime power. Then there exists an optimal equitable symbol weight equidistant q-ary code $E(q^2-1, q^2, q(q-1); q)$.*

Note once more that for the case of odd q this result has been obtained in [3] using the other approach.

Consider an example of our construction for the case $q = 4$. Let $Q_4 = \{0, 1, 2, 3\}$, where $1 = \alpha^0$, $2 = \alpha$, $3 = \alpha^2$, and the element α is the primitive element of the field $\mathbf{F}_4$ such that $\alpha^2 = \alpha + 1$ (in this case the operation $\oplus$ coincides with addition operation in $\mathbf{F}_4$). Give the matrix C, formed by the words of equidistant $(5, 16, 4; 4)$ code, which can be presented as follows:

$$C = \left[\begin{array}{c|c} A & \boldsymbol{e}_0 \\ L_1 & \boldsymbol{e}_1 \\ L_2 & \boldsymbol{e}_2 \\ L_3 & \boldsymbol{e}_3 \end{array}\right],$$

where $\boldsymbol{e}_i = (i\,i\,i\,i)^t$, $i = 0, 1, 2, 3$, and the matrices A, L_1, L_2, L_3 are of the form:

$$A = \begin{bmatrix} 0000 \\ 1111 \\ 2222 \\ 3333 \end{bmatrix}, \quad L_1 = \begin{bmatrix} 0123 \\ 1032 \\ 2301 \\ 3210 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 0231 \\ 1320 \\ 2013 \\ 3102 \end{bmatrix}, \quad L_3 = \begin{bmatrix} 0312 \\ 1203 \\ 2130 \\ 3021 \end{bmatrix}.$$

Construct the equidistant $(15, 16, 12; 4)$ code E by repeting three times the given above code C and define the matrix K:

$$E = \left[\begin{array}{c|c|c|c} A & A & A & \boldsymbol{e}_0\ \boldsymbol{e}_1\ \boldsymbol{e}_2 \\ L_1 & L_1 & L_1 & \boldsymbol{e}_1\ \boldsymbol{e}_2\ \boldsymbol{e}_3 \\ L_2 & L_2 & L_2 & \boldsymbol{e}_2\ \boldsymbol{e}_3\ \boldsymbol{e}_0 \\ L_3 & L_3 & L_3 & \boldsymbol{e}_3\ \boldsymbol{e}_0\ \boldsymbol{e}_1 \end{array}\right], \quad K = \left[\begin{array}{c|c|c} A & A & A \\ L_1 & L_1 & L_1 \\ L_2 & L_2 & L_2 \\ L_3 & L_3 & L_3 \end{array}\right].$$

Add to all rows of K the following vector

$$\boldsymbol{a} = (0,\ 1,\ 1,\ 1, 0,\ 2,\ 2,\ 2,\ 0,\ 3,\ 3,\ 3).$$

Show how to reconstruct the first nontrivial layer of the matrix K:

$$\left[\begin{array}{c|c|c} L_1 & L_1 & L_1 \end{array}\right].$$

Adding to this layer of the vector $\boldsymbol{a}$, we obtain the following matrices $L_1^{(j)}$:

$$L_1^{(1)} = \begin{bmatrix} 0032 \\ 1123 \\ 2210 \\ 3301 \end{bmatrix}, \quad L_1^{(2)} = \begin{bmatrix} 0301 \\ 1210 \\ 2123 \\ 3032 \end{bmatrix}, \quad L_1^{(3)} = \begin{bmatrix} 0210 \\ 1301 \\ 2032 \\ 3123 \end{bmatrix}.$$

The corresponding matrices $B_1^{(j)}$ look as follows:

$$B_1^{(1)} = \begin{bmatrix} 2\,0\,1\,1 \\ 0\,2\,1\,1 \\ 1\,1\,2\,0 \\ 1\,1\,0\,2 \end{bmatrix}, \quad B_1^{(2)} = \begin{bmatrix} 2\,1\,0\,1 \\ 1\,2\,1\,0 \\ 0\,1\,2\,1 \\ 1\,0\,1\,2 \end{bmatrix}, \quad B_1^{(3)} = \begin{bmatrix} 2\,1\,1\,0 \\ 1\,2\,0\,1 \\ 1\,0\,2\,1 \\ 0\,1\,1\,2 \end{bmatrix}.$$

Chose the row $(2\,0\,1\,1)$ of the first matrix $B_1^{(1)}$. This choice uniquely implies the choice of the row $(0\,1\,2\,1)$ of the second matrix $B_1^{(2)}$ and the choice of the row $(1\,2\,0\,1)$ of the third matrix $B_1^{(3)}$. We see, that 2 in the third row of the matrix $B_1^{(3)}$ occupies the same position as 0 of the first row of the matrix $B_1^{(1)}$ such that

$$(2\,0\,1\,1) + (0\,1\,2\,1) + (1\,2\,0\,1) = (3\,3\,3\,3).$$

Then the choice of the first row $(0\,2\,1\,1)$ from $B_1^{(1)}$ implies the choice of $(1\,0\,1\,2)$ from $B_1^{(2)}$ and $(2\,1\,1\,0)$ from the third matrix. This gives

$$(0\,2\,1\,1) + (1\,0\,1\,2) + (2\,1\,1\,0) = (3\,3\,3\,3)$$

and so on. Continuing in this way we obtain the optimal equitable symbol weight equidistant 4-ary code $E(15, 16, 12; 4)$, whose all codewords look as follows:

0 1 1 1	0 2 2 2	0 3 3 3	0 1 2
1 0 0 0	1 3 3 3	1 2 2 2	0 1 2
2 3 3 3	2 0 0 0	2 1 1 1	0 1 2
3 2 2 2	3 1 1 1	3 0 0 0	0 1 2
0 0 3 2	2 1 2 3	1 3 0 1	1 2 3
1 1 2 3	3 0 3 2	0 2 1 0	1 2 3
2 2 1 0	0 3 0 1	3 1 2 3	1 2 3
3 3 0 1	1 2 1 0	2 0 3 2	1 2 3
0 3 2 0	2 2 3 1	1 0 1 3	2 3 0
1 2 3 1	3 3 2 0	0 1 0 2	2 3 0
2 1 0 2	0 0 1 3	3 2 3 1	2 3 0
3 0 1 3	1 1 0 2	2 3 2 0	2 3 0
0 2 0 3	2 3 1 2	1 1 3 0	3 0 1
1 3 1 2	3 2 0 3	0 0 2 1	3 0 1
2 0 2 1	0 1 3 0	3 3 1 2	3 0 1
3 1 3 0	1 0 2 1	2 2 0 3	3 0 1

3 Optimal $E(n, M, d; q)$ codes from difference matrices

For construction of codes with parameters (2) recall the definition of *difference matrix* $D(n, q)$ [6]. Assume that the alphabet Q is an additive abelian group with neutral element 0.

Definition 2. *Call the matrix $D(n, q)$ of size $n \times n$ over Q by the difference matrix, if the difference of any two its rows contains every symbol of the alphabet Q exactly n/q times.*

Theorem 2. *Let integer numbers $q \geq 2$ and n be such that there exists a difference matrix $D(n, q)$ over the alphabet Q. Then there exists an optimal equitable symbol weight q-ary code $E(n, M, d; q)$ with parameters n, $M = q(n-1)$, $d = (q-1)n/q$.*

Proof. Without loss of generality assume that the difference matrix $D(n, q)$ contains a zero word $(0, 0, \ldots, 0)$. Then clearly all other rows contain every symbol exactly n/q times. There are $n - 1$ such rows and the pairwise distance between any two different rows equals $(q-1)n/q$ according to definiton of a difference matrix. Adding all these rows with vectors of length n

$$(0, 0, \ldots, 0), \quad (1, 1, \ldots, 1), \quad \ldots, \quad (q-1, q-1, \ldots, q-1)$$

we obtain all together $q(n-1)$ vectors, which form our code (this construction was used in [7] for construction codes from simplices). It is easy to see that this code is equitable symbol weight with two pairwise distances $(q-1)n/q$ and n [4]. Since every codeword has the same weight $w = (q-1)n/q$, the number of codewords is less or equal to $A_q(n, d, w)$, i.e. maximal possible number of codewords of length n, distance d on sphere of radius w. Further

$$A_q(n, d, w) \leq q \times A_q(n-1, d, w)$$

and

$$A_q(n-1, (q-1)n/q, (q-1)n/q) \leq n-1,$$

where the last inequality follows from the following (Johnson type) bound for q-ary constant weight codes [8]:

$$A_q(n, d, w) \leq \frac{\left(1 - \frac{1}{q}\right) dn}{w^2 - \left(1 - \frac{1}{q}\right)(2w - d)n}.$$

Therefore the constructed code is optimal as equitable symbol weight code of length n with distance $d = (q-1)n/q$ (but it is not optimal as a code of length n even with the same two distances [4, 7]). □

References

[1] Y. M. Chee, H. Kiah, A. Ling, C. Wang, Optimal equitable symbol weight codes for power line communications, ISIT 2012, Proc. 2012 IEEE International Symposium on Information Theory, 2012, 671-675; extended variant in: arXiv:1304.0278v1 [math.CO] 1 Apr 2013.

[2] Y. M. Chee, H. Kiah, P. Purkayastha, C. Wang, Importance of symbol equity in coded modulation for power line communication, ISIT 2012, Proc. 2012 IEEE International Symposium on Information Theory, 2012, 666-670; extended variant in: arXiv:1301.2041v1 [cs.IT] 10 Jan 2013.

[3] D. Peipei, W. Jianmin, Y. Jianxing, Two series of equitable symbol weight codes meeting the Plotkin bound, Designs, Codes and Cryptography, 2013, to appear.

[4] N. V. Semakov, G. V. Zaitzev, V. A. Zinoviev, Class of naximal equidistant codes, *Problems of Information Transmission*, 1969, vol. 5, No. 2, 84-87.

[5] G. T. Bogdanova, V. A. Zinoviev, T. I. Todorov, On construction of q-ary equidistant codes, *Problems of Information Theory*, 2007, vol. 43, No. 4, 13-36.

[6] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, London: Cambridge University Press, 1986.

[7] L. A. Bassalygo, S. M. Dodunekov, V. A. Zinoviev, T. Helleseth, On Grey-Rankin bound for nonbinary codes, *Problems of Information Transmission*, 2006, vol. 42, No. 3, 37-44.

[8] L. A. Bassalygo, New upper bounds for error-correcting codes, *Problems of Information Transmission*, 1965, vol. 1, No. 1, 41-44.