# All $q$-ary equidistant 3-codes

Galina Bogdanova*
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
P.O.B. 323, 5000 V. Tarnovo, Bulgaria
galina@math.bas.bg

Gyula O.H. Katona†
Rényi Institute
Budapest, Hungary
ohkatona@renyi.hu

## 1 Introduction

The elements of $\{0, 1, \ldots, q-1\}^n$ are called $q$-ary *codewords of length $n$ over a $q$-element alphabet*. A code is a set of codewords. The Hamming-distance $d(c_1, c_2)$ of two codewords $c_1$ and $c_2$ is the number of positions where they differ. A code $\mathcal{C}$ is called *equidistant with distance $d$* if the Hamming-distance of any two codewords is exactly $d$. Another, shorter name is: $q$-ary equidistant d-code.

The binary case ($q = 2$) was studied in [6], [10], [8], [9], [7] and [13].

$q$-ary equidistant codes and their relationships to resolvable balanced incomplete block designs were considered in [11] and [12]. Paper [1] found the

*The work was partially supported by the Bulgarian National Science Fund, project number IO-03-02/2006.

†The work of the first author was supported by the Hungarian National Foundation for Scientific Research, grant number NK062321.

ternary ($q = 3$) equidistant codes for small values of $n(\leq 10)$ . The same was done for $q = 4, 5, 6$ in [2] and [3] [5].

[4] gives many interesting constructions and (among others) determines the largest size $|\mathcal{C}|$ of a $q$-ary equidistant code $\mathcal{C}$ of length $n$ with distance 3 for all $n$ and $q$. In the present paper we list all $q$-ary equidistant codes with distance 3.

The code consisting of a subset of codewords of an equidistant code is also an equidistant code. This is why it is sufficient to consider the maximal equidistant codes, that is, equidistant $d$-codes which cannot be enlarged by adding more codewords. The family of all maximal equidistant codes of length $n$ over a $q$-element alphabet with distance $d$ is denoted by $\mathcal{E}(n, q, d)$. If the code consists of $M$ codewords, we will say that it is an $(n, M, d)_q$ equidistant code. The goal of the present paper is to determine all the elements of $\mathcal{E}(n, q, 3)$.

Fix a permutation of the set $\{0, 1, \ldots, q-1\}$ and change the elements in the $i$th position of every codeword in a code. This operation does not change the Hamming-distance between the codewords, therefore it brings an equidistant code into an equidistant code. Fix one codeword in an equidistant code and make its first position 0 by the above operation. Repeat it with the second position, third position, and so on. Since the operations are performed independently in the distinct positions, the resulting equidistant code will have only 0s in each position of the fixed codeword. Therefore we may suppose that an equidistant code contains the codeword consisting of $n$ 0s. The set of these maximal equidistant codes is denoted by $\mathcal{E}_0(n, q, d)$. We will actually determine this family, the other maximal equidistant codes can be obtained by independently permuting the values in every position.

Notice that the application of the same permutation of the positions in all codewords does not change pairwise Hamming-distances, therefore an equidistant code becomes an equidistant code. Finally, adding new positions having the same value $i$ in every codeword results in an equidistant code. On the other hand if there are positions which have the same value in every codeword, the deletion of these positions also leads to an equidistant code. The codes obtainable from each other by these operations will be called *equivalent*. We will determine only one element in each such class of $\mathcal{E}_0(n, q, d)$.

Let $C = (c_0, c_1, \ldots, c_{M-1}) \in \mathcal{E}_0(n, q, d)$ be an equidistant code where $c_0$ is the zero sequence. Since $d(c_0, c_i) = d$ holds for all other codewords $c_i (0 < i)$, consequently the number of non-zero coordinates in $c_i(0 < i)$ is exactly $d$. Let $c = (a_1, a_2, \ldots, a_n)$ be a codeword with $d$ non-zero coordinates. Suppose that $a_{i_1}, a_{i_2}, \ldots, a_{i_d}$ are non-zero, ($i_1, i_2, \ldots i_d$ are distinct) but the other $a$s are 0. Associate the $d$-element set $F(c)$ with this codeword. It will be called the *support* of $c$. Observe, that $\mathcal{F}(c_i) = \mathcal{F}(c_j)$ might happen for $0 < i < j$.

$$\mathcal{F}(C) = \{F(c_1), F(c_2), \ldots, F(c_m)\}$$

is a family of $d$-element sets, where $m \leq M - 1$. The family $\mathcal{F}(C)$ is called the *support family* of the code $C$.

Let $[n] = \{1, 2, \ldots, n\}$, and let $\binom{[n]}{d}$ denote the family of all $d$-element subsets of $[n]$. Then $\mathcal{F}(C) \subset \binom{[n]}{d}$ holds. We say that a family $\mathcal{F}$ is $\ell$-*intersecting* if $F, G \in \mathcal{F}$ implies $|F \cap G| \geq \ell$. It is easy to see that if $C \in \mathcal{E}_0(n, q, d)$ holds then $\mathcal{F}(C)$ is $\lceil \frac{d}{2} \rceil$-intersecting. Observe, that $\mathcal{F}(C_1) = \mathcal{F}(C_2)$ might happen for distinct codes $C_1, C_2$.

The main idea of our approach is to study first the $\lceil \frac{d}{2} \rceil$ -intersecting families and to try to choose the appropriate coordinate-values to the non-zero positions after that.

## 2 $d = 3$

**Proposition 2.1** *The maximal 2-intersecting families in* $\binom{[n]}{3}$ *are*

$$\{\{1, 2, i\}(2 < i \leq n)\}, \tag{2.1}$$

$$\binom{[4]}{3} \tag{2.2}$$

*and the families obtained by permuting the set* $[n]$.

**Proof.** Suppose that $\mathcal{F}$ is a trivial 2-intersecting family, that is, every member $F \in \mathcal{F}$ contains (e.g.) 1 and 2. Since it is maximal it must contain all sets in (2.1).

Otherwise, there are no two elements which are contained in all the members of $\mathcal{F}$. Suppose that there is one such element, say 1. Deleting this element from all members of $\mathcal{F}$ a 1-intersecting family $\mathcal{F}' \subset \binom{[n-1]}{2}$ is obtained and there is no element which is contained in all of them. Let one member be e.g. $\{2,3\}$. Other members must intersect $\{2,3\}$, but not all of them in the same element. One member $F_1'$ contains 2, another one, $F_2'$ contains 3. However they must have a common element, say 4. Then $\{2,4\},\{3,4\} \in \mathcal{F}'$. There is no other 2-element set meeting all of $\{2,3\},\{2,4\},\{3,4\}$. We have $\mathcal{F} = \{1,2,3\},\{1,2,4\},\{1,3,4\}$, what is a subfamily of (2.2).

Finally, suppose that there is no element contained in all members of $\mathcal{F}$. Let two members be e.g. $F_1 = \{1,2,3\}, F_2 = \{1,2,4\}$. Since a further member intersects them in 2 elements, it cannot avoid both 1 and 2. However there is an $F_3$ avoiding 2, by the assumption of the case. Then $1 \in F_3$ and by the 2-intersecting property we have $F_3 = \{1,3,4\}$. Similarly, the set avoiding 1 must have the form $F_4 = \{2,3,4\}$. There is no more sets intersecting all of $F_1, F_2, F_3, F_4$ in 2 elements. This family is maximal and equal to (2.2). □

Now we are trying "to write in values into the sets $\in \mathcal{F}$". Let $C \in \mathcal{E}_0(n,q,3)$ be an equidistant code and $\mathcal{F}(C)$ the associated family. If $F \in \mathcal{F}$ then let $n(F)$ denote the number of codewords $c \in C$ such that $F(c) = F$. The *reduced version* of the codeword $c = (0,\ldots,a_{i_1},0,\ldots,0,a_{i_2},0,\ldots,0,a_{i_3},\ldots,0)$ is $(a_{i_1},a_{i_2},a_{i_3})$. Let $s(F)$ denote the set of reduced codewords such that $F(c) = F$. It is obvious that $s(F)$ consists of $n(F)$ sequences of length 3. Since the distances between any two codewords are 3, two elements of $s(F)$ must have Hamming distance 3, that is, no coordinates can be equal. Suppose now that $F_1, F_2 \in \mathcal{F}$ are distinct members. Then $|F_1 \cap F_2| = 2$ and the reduced versions of the codewords $c_1, c_2$ satisfying $F(c_1) = F_1, F(c_2) = F_2$ are equal in one of the positions in $F_1 \cap F_2$ and different in the other one.

**Lemma 2.2** *Let $C \in \mathcal{E}_0(n,q,3)$. If $F_1$ and $F_2$ are two distinct members of $\mathcal{F}(C)$ then $n(F_1), n(F_2) \leq 2$ holds.*

**Proof.** Suppose, in the contrary, that $n(F_1) \geq 3$ and $F(c_1) = F(c_2) = F(c_3) = F_1$. The reduced versions of $c_1, c_2$ and $c_3, (a_{11}a_{12},a_{13}),(a_{21},a_{22},a_{23}), (a_{31},a_{32},a_{33})$, have 3 distinct values in every position, that is, $a_{i1},a_{i2},a_{i3}$ are three distinct values $(i = 1,2,3)$. Let $F(c) = F_2$. Suppose that $F_1 \cap F_2$ is e.g. the first and second positions of the supports of both $c_1$ and $c$. The reduced version of $c, (a_1,a_2,a_3)$ has to be equal to the reduced versions of $c_1, c_2$ and $c_3$ in one of the positions in $F_1 \cap F_2$. But $a_1$ can be equal to only one of $a_{i1}$, say $a_{11}$. Similarly, $a_2$ is equal to, say $a_{22}$ (the equality $a_2 = a_{12}$ is forbidden!). Then $a_1 \neq a_{31}, a_2 \neq a_{32}$, implying that the Hamming distance of $c_1$ and $c$ is 4, a contradiction. □

**Corollary 2.3** *If $|\mathcal{F}(C)| > 1$ then $n(F) \leq 2$ holds for every $F \in \mathcal{F}$.*

□

**Theorem 2.4** *Every member of $\mathcal{E}_0(n, q, 3)$ is equivalent to one of the following three codes:*

$$\begin{gathered}(0,0,0,0,\dots,0)\\(1,1,1,0,\dots,0)\\(2,2,2,0,\dots,0)\\\vdots\\(q-1,q-1,q-1,0,\dots,0),\end{gathered}\tag{2.3}$$

$$\begin{gathered}(0,0,0,0,\dots,0)\\(1,1,1,0,\dots,0)\\(1,2,0,1,\dots,0)\\(1,3,0,0,1\dots,0)\\\vdots\\(1,q-1,0,0,\dots,1),\end{gathered}\tag{2.4}$$

$$\begin{gathered}(0,0,0,0,0,\dots,0)\\(1,1,1,0,0,\dots,0)\\(2,2,2,0,0,\dots,0)\\(1,2,0,1,0,\dots,0)\\(2,1,0,2,0,\dots,0)\\(1,0,2,2,0,\dots,0)\\(2,0,1,1,0,\dots,0)\\(0,1,2,1,0,\dots,0)\\(0,2,1,2,0,\dots,0).\end{gathered}\tag{2.5}$$

**Proof.** If $|\mathcal{F}(C)| = 1$, that is, $\mathcal{F} = \{F\}$ then $n(F) \le q$. The reduced codewords can be chosen to be $(i,i,i)$ for every $1 \le i < q$ and we have obtained one element of $\mathcal{E}_0(n,q,3)$, namely (2.3).

In the rest of the proof we can suppose that $|\mathcal{F}(C)| > 1$ holds and then Corollary 2.3 implies $n(F) \le 2$ for every $F \in \mathcal{F}$. Let $\mathcal{F}$ be first a subfamily of (2.1). Two subcases will be distinguished: 1.1. $n(F) = 1$ holds for every $F \in \mathcal{F}$, 1.2. $n(F) = 2$ holds for one of $F \in \mathcal{F}$.

*Case 1.1* It can be supposed that $F(c) = [3] \in \mathcal{F}$ holds for one of the codewords and that its reduced version is $(1,1,1)$ The other supports all contain $[2]$. If $c_1 \in C$ is another codeword, its reduced version must contain a 1 and a value different from 1, say 2, in the first two positions. Suppose, that the reduced version has the form $(1,2,i)$. Since this third position is in only one reduced version, it can be chosen to be 1. The reduced version is $(1,2,1)$. If $c_2 \in C$ is a third codeword, its reduced version has to contain such values in the first two positions which have a Hamming-distance 1 from both $(1,1)$ and $(1,2)$. If the reduced version of $c_2$ contains a value different from 1 in the first position, then it has to have a value equal to both 1 and 2 in the second position. This is impossible, therefore it must have a 1 in the first position, and a new value, say 3 in the second. The reduced version is $(1,3,1)$. Continuing in this way, (2.4) will be achieved.

*Case 1.2.* Suppose that $n([3]) = 2$. The reduced versions of the two codewords are $(1,1,1)$ and $(2,2,2)$. If the code contains one more codeword, say $c$, one can suppose that its support $F(c)$ satisfies $F(c) \cap [3] = \{1,2\}$, for instance $F(c) = \{1,2,4\}$. The reduced version must have a 1 and a 2 in the first two positions. Let it be $(1,2,1)$. Let, $F$ be another member of (2.1), say $\{1,2,5\}$. It is easy to see that codeword $c'$ can be found with $F(c') = F$ satisfying the conditions. That is no more members of (2.1) can be supports of codewords. The code what we have at the moment is equivalent to a subset of (2.5). Of course we can add the codeword $(2,1,0,2)$ to the previous 3 codewords preserving the property, but this extension is still equivalent to a subset of (2.5).

Finally suppose that the support family of the code is (2.2).

*Case 2.* In this case $n(F) \le 2$ holds for every $F \in \binom{[4]}{3}$. Construction (2.5) shows that one can choose two codewords for each such support in such a way that they (completed with the 0 codeword) form an equidistant code. Therefore this is largest possible element of $\mathcal{E}_0(n,q,3)$ in this case. We only have to show that (a) this construction is unique up to equivalence, (b) there are no "dead-ends", that is smaller maximal equidistant codes with supports from the family $\binom{[4]}{3}$. Observe that if only one or two members of $\binom{[4]}{3}$ are really supports then these cases were covered by our previous cases, therefore one can suppose that the number of supports is 3 or 4. If it is 3, we will suppose that they are $\{1,2,3\},\{1,2,4\},\{1,3,4\}$.

*Case 2.1.* Suppose that $n(F)=2$ holds for one of the sets, say, for $F=[3]$. Let the reduced versions of the two codewords with this support be $(1,1,1)$ and $(2,2,2)$. The values of the codeword with support $\{1,2,4\}$ must be 1 and 2 in some order in the first two positions, choose them in this order. The value in the 4th position can be chosen 1. Therefore the reduced codeword is $(1,2,1)$. A reduced codeword associated with the support $\{1,3,4\}$ must also have one 1 and one 2 in the first and third positions. If it is 1 in the first position, it must be 2 in the 4th position. The reduced codeword is $(1,2,2)$ otherwise $(2,1,1)$. In both cases the code is a subset of (2.5). If $\{2,3,4\}$ is also a support, the possible reduced codewords are $(1,2,1)$ or $(2,1,2)$, still in agreement with (2.5). If any of the support are used twice, the other codeword is uniquely determined. (Unless we have only 1's in the 4th position, then any value different from 1 is good, but we can choose 2.)

*Case 2.2.* $n(F)=1$ hold for 3 or 4 members of $\binom{[4]}{3}$. Starting with $(1,1,1)$ for the support $\{1,2,3\}$ and choosing the codeword following the rule with the smallest possible positive value we obtain a subset of the code (2.5), again. □

# References


[1] G.Bogdanova, Ternary Equidistant Codes and Maximum Clique Problem, in: *Proc. European Women in Mathematics Int. Workshop on Groups and Graphs*, Varna, Bulgaria. 31 August - 6 September, 2002, pp. 15-18.

[2] G. Bogdanova, T. Todorov, Bounds on the Size of Equidistant codes over Alphabet of Five and Six Elements, *Mathematica Balcanica, New Series*, **21**(2007) 131-140.

[3] G. Bogdanova, T. Todorov, Some bounds for equidistant codes, in: *International Workshop on Algebraic and Combinatorial Coding Theory*, Kranevo, Bulgaria, June, 2004, pp. 50-55.

[4] G.Bogdanova, V.Zinoviev, T.Todorov, On construction of q-ary equidistant codes, *Problems of Information Transmission* **43**(2007) 280-302.

[5] G.T.Bogdanova and T.A.Yorgova, Bounds for Ternary Equidistant Constant Weight Codes, in: *Mathematics and Education in mathematics* **31**, Borovec, April 3-6, 2002, pp. 131-135.

[6] M. Deza, Une propriete extremale des plans projectifs finis dans une classe de codes equidistants, *Discrete Math.* **6**(1973) 343-352.

[7] F.W.Fu, T.Klove, Y. Luo, V.K. Wei, On Equidistant Constant Weight Codes, *Discrete Applied Math.* **128**(2003) 157-164.

[8] J.I.Hall, Bounds for Equidistant Codes and Partual Projective Planes, *Discrete Math.* **17**(1977) 85-94.

[9] 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.

[10] van Lint J.H., A Theorem on Equidistant Codes, *Discrete Math.* **6**(1973) 353-358.

[11] N.V. Semakov, V.A. Zinoviev, Equidistant q-ary Codes with Maximal Distance and Resolvable Balanced Incomplete Block Designs, *Probl. Peredachi Inf.* **4**(1968) 3-8.

[12] N.V..Semakov N.V., V. A. Zinoviev V.A., G.V. Zaitsev, A Class of Maximal Equidistant Codes, *Probl. Peredachi Inf.* **5**(1969) 84-87.

[13] D.R.Stinson, G.H.J.van Rees, The Equivalence of Certain Equidistant Binary Codes and Symmetric BIBDs, *Combinatorica* **4**(1984) 357-362.