Arkady G. D'yachkov, Vyacheslav V. Rykov

Optimal Superimposed Codes and Designs for Renyi's Search Model

Abstract– **We consider a class of superimposed codes [1, 2] for the search model of A. Renyi [3]. A lower bound on the code length is obtained and optimal superimposed codes are presented.**

1. Notations and definitions.

Let $1 \leq s < k < t$, $N > 1$ be integers and $X = \|x_i(u)\|$, $i = 1, 2, \ldots, N$, $u = 1, 2, \ldots, t$ be a binary $N \times t$–matrix (code) with columns (codewords) $\mathbf{x}(1), \mathbf{x}(2), \ldots, \mathbf{x}(t)$, where $\mathbf{x}(u) = (x_1(u), x_2(u), \ldots, x_N(u))$. We say that the binary column $\mathbf{x}$ *covers* the binary column $\mathbf{y}$ if the Boolean sum $\mathbf{x} \vee \mathbf{y} = \mathbf{x}$. The code X is called [1, 2] a *superimposed* (s,t)*-code* if the Boolean sum of any s-subset of columns of X covers those and only those columns of X which are the terms of the given Boolean sum. The code X is called [1, 2] a *superimposed* (s,t)*-design* if all Boolean sums composed of not more than s columns of X are distinct.

Let $\mathbf{x}_i = (x_i(1), x_i(2), \ldots, x_i(t))$, $i = 1, 2, \ldots, N$, be the i-th row of X and

$$|\mathbf{x}_i| = \sum_{u=1}^{t} x_i(u), \quad i = 1, 2, \ldots, N, \quad 0 \leq |\mathbf{x}_i| \leq t,$$

be the number of 1-entries (weight) in row $\mathbf{x}_i$.

Definition 1. An $N \times t$ matrix X is called a superimposed (s,t,k)-code (design) of *length* N*, size* t*, strength* s and *constraint* k if two conditions are fulfilled:

- code X is a superimposed (s,t)-code (design),
- for any $i = 1, 2, \ldots, N$, weight $|\mathbf{x}_i| \leq k$.

Remark 1. The consraint on the weight of rows $|\mathbf{x}_i| \leq k$, $i = 1, 2, \ldots, N$, was introduced by A. Renyi [3] and was studied by G. Katona [4] for the search designs.

2. Lower bound

Proposition 1. *Let $k \ge s \ge 2$. For any superimposed $(s-1,t,k)$-code $((s,t,k)-design)$ X of length N, the following inequality takes place*

$$N \ge \left\lceil \frac{st}{k} \right\rceil , \tag{1}$$

where $\lceil a \rceil$ denotes the least integer $\ge a$. In addition, if $t = kq,\ q = 2,3,\ldots$ and there exists superimposed $(s-1,kq,k)$-code $((s,kq,k)-design)$ X of length $N = sq$, then X is a constant weight code of weight s and for any $i = 1,2,\ldots,N$, the weight of row $|\mathbf{x}_i| = k$.

Proof. Consider an arbitrary superimposed $(s-1,t,k)$-code X of length N. Let $n, 0 \le n \le t$, be the number of codewords of X having a weight $\le s-1$. From definition of superimposed $(s-1,t)$-code it follows (see, [1]) that $n \le N$ and, for each codeword of weight $\le s-1$, there exists a row in which all the remaining elements, except for the element of this codeword, are 0's. We delete these n rows from X together with n codewords of weight $\le s-1$. Consider the remaining $(N-n)\times(t-n)$ matrix X'. Obviously, each column of X' has a weight $\ge s$ and each its row contains $\le k$ 1's. Hence,

$$s(t-n) \le k(N-n). \tag{2}$$

It follows $ts \le kN - n(k-s) \le kN$, provided that $k \ge s$. For superimposed $(s-1,t,k)$-code, inequality (1) is proved. Let $q = 2,3,\ldots$ be integer and $t = kq$. It is easy to see that both of inequalities (1) and (2) have signs of equality, iff superimposed $(s-1,kq,k)$-code X is a constant weight code of weight s and for any $i = 1,2,\ldots,N$, the weight of row $|\mathbf{x}_i| = k$. For superimposed $(s-1,t,k)$-code, Proposition 1 is proved.

It is known [2] that code X is superimposed (s,t,k)-design iff X is superimposed $(s-1,t,k)$-code and all $\binom{t}{s}$ Bolean sums composed of s columns of X are distinct. Hence, inequality (1) is true for superimposed (s,t,k)-design.
Proposition 1 is proved.

Denote by $N(s,t,k)$, $(\tilde{N}(s,t,k))$ the minimal possible length of superimposed (s,t,k)-code $((s,t,k)$-design). From Proposition 1 it follows that for $k \le s$,

$$N(s-1,t,k) = \tilde{N}(s,t,k) = t$$

and for $k \ge s+1$,

$$\tilde{N}(s,t,k) \ge N(s-1,t,k) \ge \left\lceil \frac{st}{k} \right\rceil .$$

3. Optimal parameters

Let $s \geq 2$ and $k \geq s+1$ be fixed integers. Denote by $q \geq 2$ an arbitrary integer. We shall consider the *optimal* superimposed $(s-1, kq, k)$-codes and *optimal* superimposed (s, kq, k)-designs of length $N = 2q$ whose parameters satisfy (1) with the sign of equality.

Remark 2. For the case $s = 2$, some constructions of superimposed $(2, kq, k)$-designs of length $N = 2q$ were obtained in [1, pp. 374-375]. By virtue of Proposition 1, they are optimal. We give here the parameters of these designs. *Let $s = 2$ and $k \geq 3$ be integers. The following statements are true:*

- *if $k-1$ is a prime power and $q = k^2 - k + 1$, then there exists an superiposed $(2, kq, k)$-design of length $N = 2q$,*
- *for pair $(k = 3,\ q = 5)$ and pair $(k = 7,\ q = 25)$, there exists an superimposed $(2, kq, k)$-design of length $N = 2q$.*

The aim of this paper – to prove Theorems 1–4.

Theorem 1. *Let $s = 2$ and $k \geq 3$ be integers. Then*

1) *for any integers $q \geq k \geq 3$ there exists an optimal superimposed $(1, kq, k)$-code of length $N = 2q$, i.e.,*

$$N(1, kq, k) = 2q, \quad q \geq k,$$

2) *for any integer $q \geq 2^k - 1$ there exists an optimal superimposed $(2, kq, k)$-design of length $N = 2q$, i.e.,*

$$\tilde{N}(2, kq, k) = 2q, \quad q \geq 2^k - 1.$$

Theorem 2. *Let $s \geq 3$, $k \geq s+1$ be fixed integers and $q = k^{s-1}$. Then there exists an optimal superimposed (s, kq, k)-design X of length $N = sq$, i.e,*

$$\tilde{N}(s, k^s, k) = sk^{s-1}.$$

Theorems 3 and 4 supplement Theorem 2 if $s = 3$.

Theorem 3. *Let $s = 3$ and $k = 4, 5, \ldots$ be a fixed integer. For any integer $q \geq k^2$, there exists an optimal superimposed $(2, kq, k)$-code X of length $N = 3q$, i.e,*

$$N(2, kq, k) = 3q, \quad q \geq k^2.$$

Theorem 4. *Let $s = 3$. The following two statements are true:*

1) *if* $k=4$, *then*

   – *for* $q=8,9,10,11,12$, *there exists an optimal superimposed* $(2,4q,4)$-*code of length* $N=3q$,

   – *for* $q=13,14,15$, *there exists an optimal superimposed* $(3,4q,4)$-*design of length* $N=3q$;

2) *if* $k=6$, *then for* $q=3i$, $i=6,7,\ldots,11$ *and for* $q=4j$, $j=7,8$, *there exists an optimal superimposed* $(2,6q,6)$-*code of length* $N=3q$.

To construct the optimal superimposed $(s-1,kq,k)$-codes and optimal superimposed (s,kq,k)-designs, we shall apply concatenated codes using a class of q-nary s-hashing codes [5] of size $t=kq$ and length s. The description of cascade construction, definitions, properties of s-hashing codes and the proof of Theorems 1 and 2 will be given in **Section 4**. Theorems 3 and 4 will be proved in **Section 5** using some characterization properties of 3-hashing q-nary codes.

4. Homogeneous q-nary codes

Let $q\ge s\ge 1$, $k\ge 2$, $k\le t\le kq$ be integers, $A_q=\{a_1,a_2,\ldots,a_q\}$ be an arbitrary q-nary alphabet and

$$B=\|b_j(u)\|,\ j=1,2,\ldots,s,\quad u=1,2,\ldots,t,$$

be $s\times t$ q-nary ($b_j(u)\in A_q$) matrix (code) with columns (codewords)

$$\mathbf{b}(u)=(b_1(u),b_2(u),\ldots,b_s(u)),\ u=1,2,\ldots,t,$$

and rows

$$\mathbf{b}_j=(b_j(1),b_j(2),\ldots,b_j(t)),\ j=1,2,\ldots,s,$$

Denote by $n_j(a)$, $a\in A_q$, $j=1,2,\ldots,s$– the number of a-entries in the j-th row $\mathbf{b}_j$. We suppose that for any $j=1,2,\ldots,s$ and any $a\in A_q$, the value $n_j(a)\le k$.

Definition 2.1. Let $t=kq$. Code B is called an (q,k,s)-*homogeneous* code if for any $j=1,2,\ldots,s$ and any $a\in A_q$, the number $n_j(a)=k$.

Let $n\le t$ be a fixed integer and $\mathbf{e}=(e_1,e_2,\ldots,e_n)$, $1\le e_1<e_2<\cdots<e_n\le t$ be an arbitrary n-subset of the set $[t]=\{1,2,\ldots,t\}$. For a given code B and any $j=1,2,\ldots,s$, denote by $\mathsf{A}_j(\mathbf{e},B)\subseteq A_q$ –the *set of*

all pairwise distinct elements of the sequence $b_j(e_1), b_j(e_2), \ldots, b_j(e_n)$. For its *cardinality* $|\mathsf{A}_j(\mathbf{e}, B)|$, we have

$$1 \le |\mathsf{A}_j(\mathbf{e}, B)| \le \min\{n,\, q\}.$$

Definition 2.2. Let $q \ge s \ge 2$. Code B is called an *s-hashing* code if for any s-subset

$$\mathbf{e} = (e_1, e_2, \ldots, e_s),\ 1 \le e_1 < e_2 < \cdots < e_s \le t,$$

of the set $[t]$, there exists $j = 1, 2, \ldots, s$, for which the elements of the j-th row $b_j(e_1), b_j(e_2)$,
$\ldots, b_j(e_s)$ *all differ*, i.e., the cardinality $|\mathsf{A}_j(\mathbf{e}, B)| = s$. In this case, we say that the j-th row of B is a *hashing* row for the corresponding codewords $\mathbf{b}(e_1), \mathbf{b}(e_2), \ldots, \mathbf{b}(e_s)$.

Definition 2.3. Let $s \ge 1,\ n \le s,\ m \le s$ be arbitrary integers. Code B is called an *s-separating* code if for any two distinct subsets

$$\mathbf{e} = (e_1, e_2, \ldots, e_n),\ 1 \le e_1 < e_2 < \cdots < e_n \le t,$$

$$\mathbf{e}' = (e'_1, e'_2, \ldots, e'_m),\ 1 \le e'_1 < e'_2 < \cdots e'_m \le t,$$

of the set $[t]$, there exists $j = 1, 2, \ldots, s$, for which the set $\mathsf{A}_j(\mathbf{e}, B) \ne \mathsf{A}_j(\mathbf{e}', B)$. In other words, for an arbitrary n-subset

$$\mathbf{e} = (e_1, e_2, \ldots, e_n),\ 1 \le e_1 < e_2 < \cdots < e_n \le t,\ n \le s,$$

of the set $[t]$, there exists the *possibility to identify* this n-subset $\mathbf{e} = (e_1, e_2, \ldots, e_n)$ (or the corresponding n-subset of codewords $\mathbf{b}(e_1),\ \mathbf{b}(e_2), \ldots, \mathbf{b}(e_n)$ of code B) on the basis of sets:

$$\mathsf{A}_1(\mathbf{e}, B), \mathsf{A}_2(\mathbf{e}, B), \ldots, \mathsf{A}_s(\mathbf{e}, B), \quad \mathsf{A}_j(\mathbf{e}, B) \subseteq A_q.$$

Let q-nary alphabet $A_q = [q] = \{1, 2, \ldots, q\}$. To illustrate definitions 2.1–2.3, we give several examples of hashing and separating codes.

Example 1. Let $k = q = 2, 3, \ldots$ be fixed integer. The evident $(k, k, 2)$-homogeneous 1-separating 2-hashing code B has the following $t = k^2$ columns (codewords):

$$\begin{array}{ccccccccccc} 111 & \ldots & 1 & 222 & \ldots & 2 & \ldots & kkk & \ldots & k \\ 123 & \ldots & k & 123 & \ldots & k & \ldots & 123 & \ldots & k. \end{array}$$

Example 2. For $k = 3,\ q = 7$, the $(7, 3, 2)$-homogeneous 2-separating code B has $kq = 21$ codewords:

$$\begin{array}{ccccccc} 111 & 222 & 333 & 444 & 555 & 666 & 777 \\ 124 & 235 & 346 & 457 & 156 & 267 & 137. \end{array}$$

Example 3. For $k = 3,\ q = 9$, the $(9, 3, 3)$-homogeneous 3-hashing (separating) code B has $kq = 27$ columns (codewords):

$$\begin{array}{ccc|ccc|ccc} 111 & 222 & 333 & 444 & 555 & 666 & 777 & 888 & 999 \\ 123 & 123 & 123 & 456 & 456 & 456 & 789 & 789 & 789 \\ 123 & 456 & 789 & 123 & 456 & 789 & 123 & 456 & 789 \end{array} \ .$$

Example 4. For $k = 4,\ q = 16$, the $(16, 4, 3)$-homogeneous 3-hashing (separating) code B has $kq = 64$ columns (codewords):

- the first 16 codewords take the form

$$\begin{array}{cccccccccc} 1111 & 2222 & 3 & 3 & 3 & 3 & 4 & 4 & 4 & 4 \\ 1234 & 1234 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 \\ 1234 & 5678 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16, \end{array}$$

- the construction of the last 48 codewords of B:
  - for $j = 1, 2$ and $u = 16m + l,\ m = 1, 2, 3,\ l = 1, 2, \ldots, 16$, the element
    $b_j(u) = b_j(16m + l) = b_j(l) + 4m$,
  - for $j = 3$ and $u = 16m + l,\ m = 1, 2, 3,\ l = 1, 2, \ldots, 16$, the element
    $b_3(u) = b_3(16m + l) = b_3(l) = l$.

The following two examples of (q, k)-homogeneous 3-hashing (but not 3-separating) codes will be used to prove Theorem 4 when $k = 4,\ q = 8$ and $k = 4,\ q = 9$.

Example 5. For $k = 4,\ q = 8$, the $(8, 4, 3)$-homogeneous 3-hashing code B has $qk = 32$ columns (codewords):

$$\begin{array}{cccccccc} 1111 & 2222 & 3333 & 4444 & 5555 & 6666 & 7777 & 8888 \\ 1234 & 1256 & 1357 & 1467 & 2358 & 2468 & 3478 & 5678 \\ 4321 & 6521 & 7531 & 8532 & 7641 & 8642 & 8743 & 8765 \end{array} \ .$$

Example 6. For $k = 4,\ q = 9$, the $(9,4,3)$-homogeneous 3-hashing code B has $qk = 36$ columns (codewords):

$$\begin{array}{ccccccccc}
1111 & 2222 & 3333 & 4444 & 5555 & 6666 & 7777 & 8888 & 9999 \\
1245 & 1346 & 2356 & 1278 & 1379 & 2389 & 4578 & 4679 & 5689 \\
5421 & 6431 & 6532 & 8721 & 9731 & 9832 & 8754 & 9764 & 9865
\end{array} .$$

Note that $t = kq = 36$ columns of B could be divided (in increasing order) into $q = 9$ groups of equal cardinality $k = 4$ and the following property is true: all columns, which belong to the same group, have the same sum of their second and third components and, for different groups, these sums are differ. Using this property, one can easy to check the 3-hash-property of code B.

Let q-nary alphabet $A_q = [q] = \{1, 2, \ldots, q\}$. For code B, we denote by

$$X_B = (\mathbf{x}(1), \mathbf{x}(2), \ldots, \mathbf{x}(t)), \quad t \geq k,$$

a binary $s \times t$ matrix (code), whose columns (codewords) have the form

$$\mathbf{x}(u) = (\mathbf{x}^1(u), \mathbf{x}^2(u), \ldots, \mathbf{x}^s(u)), \quad u = 1, 2, \ldots, t,$$

$$\mathbf{x}^j(u) = (x_1^j(u), x_2^j(u), \ldots, x_q^j(u)), \quad j = 1, 2, \ldots, s,$$

$$x_l^j(u) = \begin{cases} 1, & \text{if } l = b_j(u), \\ 0, & \text{if } l \neq b_j(u),\ l = 1, 2, \ldots, q. \end{cases}$$

In other words, a symbol $b \in [q]$ of q-nary matrix B is replaced by the binary q-sequence in which all elements are 0's, except for the element with number b. Obviously, each codeword $\mathbf{x}(u)$ of (code) X_B contains s 1's and $(sq - s)$ 0's and each row $\mathbf{x}_i$ of code X_B contains $\leq k$ 1's. For (q,k)-homogeneous code B, each row $\mathbf{x}_i$ of code X_B contains k 1's and $(kq - k)$ 0'. In addition, the stated below Proposition 2 follows easily by definitions 2.1–2.3 and Proposition 1.

Proposition 2. *Let $q > k \geq s + 1$. The following two statements are true.*

- *If B is an (q,k,s)-homogeneous s-hashing code, then X_B will be the optimal superimposed $(s-1, kq, k)$-code of length $N = sq$.*
- *If B is an (q,k,s)-homogeneous s-separating code, then X_B will be the optimal superimposed (s, kq, k)-design of length $N = sq$.*

Hence, to prove Theorems 1–4, it is sufficient to construct the corresponding (q, k, s)-homogeneous codes.

Proof of Theorem 1. Let $s = 2$, $q \geq k$, q-nary alphabet $A_q = [q] = \{1, 2, \ldots, q\}$ and $B = (\mathbf{b}(1), \mathbf{b}(2), \ldots, \mathbf{b}(kq))$ be an arbitrary q-nary 2-hashing code, i.e., B has pairwise distinct codewords $\mathbf{b}(u) = (b_1(u), b_2(u))$, $u = 1, 2, \ldots, kq$. Following [1], we introduce $q \times q$ *binary characteristic matrix* $C = \|c_i(j)\|$, $i = 1, 2, \ldots, q$, $j = 1, 2, \ldots, q$, where

$$c_i(j) = \begin{cases} 1, & \text{if there exists codeword } \mathbf{b}(u) = (i, j), \\ 0, & \text{otherwise.} \end{cases}$$

Example 2'. For $(7, 3, 2)$-homogeneous code B of **Example 2**, the characteristic (7×7) matrix C is the circulant matrix:

$$C = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Obviously, 2-hashing code B is $(q, k, 2)$-homogeneous code iff the *weight of each row* and the *weight of each column* of C are equal k. The evident sufficient condition of this property is the *circulant property* of characteristic matrix C:

- the first row $\mathbf{c}_1 = (c_1(1), c_1(2), \ldots, c_1(q))$ of circulant matrix C is an arbitrary binary sequence of length q and weight $k \leq q$,
- the m-th $m = 2, 3, \ldots, q$ row $\mathbf{c}_m = ((c_m(1), c_m(2), \ldots, c_m(q))$ of C is the *cyclic shift* of the $(m-1)$-th row, i.e.,

$$c_m(j) = \begin{cases} c_{m-1}(q), & \text{if } j = 1, \\ c_{m-1}(j-1), & \text{if } j = 2, 3, \ldots, q. \end{cases}$$

The first statement of Theorem 1 is proved.

To prove the second statement of Theorem 1, we apply the evident necessary and sufficient condition of 2-separating property which is given in [1]: *no two 1's in C must occupy the same pair of rows and columns as two other 1's; that is, no row of C can contain a pair of 1's in the same two positions as another row.*

It is easy to check that the circulant matrix C of **Example 2'** satisfies this condition. Let $q \geq 2^k$. As the simple generalization, we consider the circulant matrix C whose first row $\mathbf{c}_1 = (c_1(1), c_1(2), \ldots, c_1(q))$ is defined as follows

$$c_1(j) = \begin{cases} 1, & \text{if } j = 2^{n-1},\ n = 1, 2, \ldots, k, \\ 0, & \text{otherwise.} \end{cases}$$

Theorem 1 is proved.

The following Proposition 3 gives the recurrent construction method of $(s+1)$- separating codes with the help of s-separating codes.

Proposition 3. *If there exists an (q,k,s)-homogeneous s-separating code $B(q,k,s)$ with elements from $A_q = [q]$, then there exists the $(kq,k,s{+}1)$-homogeneous $(s{+}1)$-separating code $B(kq,k,s{+}1)$ with elements from $A_{kq} = [kq]$.*

Proof. Let

$$B(q,k,s) = \|b_j^s(u)\|,\ b_j^s(u) \in [q],\ j = 1, 2, \ldots, s,\ u = 1, 2, \ldots, kq$$

be an arbitrary (q,k,s)-homogeneous s-separating code. Consider the following two-step recurrent construction (cf. **Examples 3** and **4**) for $(kq,k,s+1)$-homogeneous code

$$B(kq,k,s{+}1) = \|b_j^{s+1}(u)\|,\ b_j^{s+1}(u) \in [kq],\ j = 1, 2, \ldots, s{+}1,\ u = 1, 2, \ldots, k^2 q.$$

- The first kq codewords of $B(kq,k,s+1)$ have the form

$$\begin{array}{cccc} b_1^s(1) & b_1^s(2) & \ldots & b_1^s(kq) \\ b_2^s(1) & b_2^s(2) & \ldots & b_2^s(kq) \\ \ldots & \ldots & \ldots & \ldots \\ b_s^s(1) & b_s^s(2) & \ldots & b_s^s(kq) \\ 1 & 2 & \ldots & kq, \end{array}$$

  i.e., for $u = 1, 2, \ldots, kq$, the element $b_j^{s+1}(u) = b_j^s(u)$, if $j = 1, 2, \ldots, s$, and $b_{s+1}^{s+1}(u) = u$.

- If the number $u = kqm + l,\ m = 1, 2, \ldots, k-1,\ l = 1, 2, \ldots, kq$, then
  - for $j = 1, 2, \ldots s$, the element $b_j^{s+1}(u) = b_j^{s+1}(kqm{+}l) = b_j^{s+1}(l) + qm$,
  - for $j = s+1$, the element $b_{s+1}^{s+1}(u) = b_{s+1}^{s+1}(kqm+l) = b_{s+1}^{s+1}(l) = l$.

Note that $t = k^2q$ codewords of $B(kq, k, s+1)$ (or the set $[k^2q]$) could be divided into k groups of the equal cardinality kq where the m-th group $G_m(q,k,s)$, $m = 1, 2, \ldots, k$, has the form

$$G_m(q,k,s) = \begin{pmatrix} b_1^s(1)+(m-1)q & b_1^s(2)+(m-1)q & \ldots & b_1^s(kq)+(m-1)q \\ b_2^s(1)+(m-1)q & b_2^s(2)+(m-1)q & \ldots & b_2^s(kq)+(m-1)q \\ \ldots & \ldots & \ldots & \ldots \\ b_s^s(1)+(m-1)q & b_s^s(2)+(m-1)q & \ldots & b_s^s(kq)+(m-1)q \\ 1 & 2 & \ldots & kq \end{pmatrix}.$$

Let

$$A_{kq}^{(m)} = \{(m-1)kq+1, (m-1)kq+2, \ldots, mkq\},\ |A_{kq}^{(m)}| = kq,\ \bigcup_{m=1}^{k} A_{kq}^{(m)} = [k^2q],$$

be the set of numbers of codewords which belong to $G_m(q,k,s)$. Consider the $s \times kq$ matrix $B_m(q,k,s)$ composed of the first s rows of $G_m(q,k,s)$, $m = 1, 2, \ldots, k$. Obviously, $B_m(q,k,s)$ is (q,k,s)-homogeneous code. In addition, all elements of $B_m(q,k,s)$ belong to the alphabet

$$A_q^{(m)} = \{(m-1)q+1, (m-1)q+2, \ldots, mq\},\ |A_q^{(m)}| = q,\ \bigcup_{m=1}^{k} A_q^{(m)} = [kq],$$

and, hence, they do not may occur in $B_n(q,k,s)$, if $n \neq m$, $n = 1, 2, \ldots, k$. On account the s-separating property of $B(q,k,s)$, it follows the s-separating property of $B_m(q,k,s)$, $m = 1, 2, \ldots, k$.

To prove the $(s+1)$-separating property of $B(kq, k, s+1)$, we consider an arbitrary $(s+1)$-subset of the set $[k^2q]$:

$$\mathbf{e} = (e_1, e_2, \ldots, \mathbf{e}_{s+1}),\ 1 \le e_1 < e_2 < \cdots < e_{s+1} \le k^2q.$$

Let

$$\mathsf{A}_1(\mathbf{e}, B), \mathsf{A}_2(\mathbf{e}, B), \ldots, \mathsf{A}_s(\mathbf{e}, B), \mathsf{A}_{s+1}(\mathbf{e}, B)$$

be the corresponding subsets of the set $[kq]$ and

$$\mathbf{e} = \sum_{m=1}^{k} \mathbf{e}_m, \quad \mathbf{e}_m = \mathbf{e} \bigcap A_{kq}^{(m)}.$$

The above-mentioned property of groups $G_m(q,k,s)$, $m = 1, 2, \ldots, k$ implies that for any $j = 1, 2, \ldots, s$ the set $\mathsf{A}_j(\mathbf{e}, B)$ could be written in the form

$$\mathsf{A}_j(\mathbf{e}, B) = \sum_{m=1}^{k} \mathsf{A}_j(\mathbf{e}_m, B),$$

where $\mathsf{A}_j(\mathbf{e}_m, B) \subseteq A_q^{(m)}$. Hence, for any fixed $j = 1, 2, \dots, s$, all nonempty sets $\mathsf{A}_j(\mathbf{e}_m, B)$, $m = 1, 2, \dots, k$, could be identified on the basis of the set $\mathsf{A}_j(\mathbf{e}, B)$.

We have two possibilities.

- There exists the unique value $m = 1, 2, \dots, k$ such that $\mathbf{e}_m = \mathbf{e}$, $|\mathbf{e}_m| = s + 1$. It follows that for any $j = 1, 2, \dots, s$,
  - the set $\mathsf{A}_j(\mathbf{e}_m, B) \neq \emptyset$,
  - for any $n \neq m$, the set $\mathsf{A}_j(\mathbf{e}_n, B) = \emptyset$. Hence, one can identify the set $\mathbf{e}$ on the basis of the set $\mathsf{A}_{s+1}(\mathbf{e}, B)$.
- For any $m = 1, 2, \dots, k$, the cardinality $|\mathbf{e}_m| \leq s$. Accounting the s-separating property of $B_m(q, k, s)$, the set $\mathbf{e}_m$ could be identified on the basis of s subsets $\mathsf{A}_j(\mathbf{e}_m, B)$, $j = 1, 2, \dots, s$. It follows the possibility to identify $\mathbf{e} = \sum_{m=1}^{k} \mathbf{e}_m$.

Proposition 3 is proved.

Proof of Theorem 2. Let an $(k, k, 2)$-homogeneous 1-separating 2-hashing code $B(k, k, 2)$ be the code from **Example 1**. Consider the corresponding $(k^2, k, 3)$-homogeneous code $B(k^2, k, 3)$ obtained from $B(k, k, 2)$ on the basis of Proposition 3. For $k = 3, 4$, constructions of $B(k^2, k, 3)$ are given in **Examples 3** and **4**. To prove Theorem 2, it is sufficient to establish the 3-separating property of code $B = B(k^2, k, 3)$ for $k = 4, 5, \dots$.

We shall use symbols which were introduced to prove Proposition 1. Note that $t = k^3$ codewords of B could be divided (in increasing order) into k groups $G_m(k, k, 2)$, $m = 1, 2, \dots, k$ of the equal cardinality k^2. Consider the $2 \times k^2$ matrix $B_m(k, k, 2)$ composed of the first 2 rows of $G_m(k, k, 2)$, $m = 1, 2, \dots, k$. Obviously, $B_m(k, k, 2)$ is the $(k, k, 2)$-homogeneous 1-separating code. In addition, all elements of $B_m(k, k, s)$ belong to the alphabet

$$A_k^{(m)} = \{(m-1)k + 1, (m-1)k + 2, \dots, mk\}, \ |A_k^{(m)}| = k, \ \bigcup_{m=1}^{k} A_k^{(m)} = [k^2],$$

and, hence, they do not may occur in $B_n(k, k, 2)$, if $n \neq m$, $n = 1, 2, \dots, k$.

Let $\mathbf{e} = (e_1, e_2, e_3)$, $1 \leq e_1 < e_2 < e_3 \leq k^3$ be an arbitrary fixed 3-subset of the set k^3 and $\mathbf{b}(e_1)$, $\mathbf{b}(e_2)$, $\mathbf{b}(e_3)$ be the corresponding triple of codewords of code B. ¿From the above-mentioned properties of $B_m(k, k, 2)$, $m = 1, 2, \dots, k$ it follows the possibility to identify (on the basis of sets $\mathsf{A}_1(\mathbf{e}, B)$ and $\mathsf{A}_2(\mathbf{e}, B)$) one of three cases.

- There are known three numbers $1 \le m_1 < m_2 < m_3 \le k$ such that the codeword $\mathbf{b}(e_i)$, $i = 1, 2, 3$ belongs to the group $G_{m_i}(k, k, 2)$. In this case, $\mathbf{b}(e_i)$ could be identified on the basis of 1-separating property of $B_{m_i}(k, k, 2)$.
- There is known the number $m = 1, 2, \dots, k$ such that all three codewords $\mathbf{b}(e_1)$, $\mathbf{b}(e_2)$, $\mathbf{b}(e_3)$ belong to the group $G_m(k, k, 2)$. In this case the triple $\mathbf{b}(e_1)$, $\mathbf{b}(e_2)$, $\mathbf{b}(e_3)$, could be identified on the basis of the set $\mathsf{A}_3(\mathbf{e}, B)$ whose cardinality $|\mathsf{A}_3(\mathbf{e}, B)| = 3$.
- There are known two numbers $1 \le m < n \le k$ such that (without loss of generality) codeword $\mathbf{b}(e_1)$ belongs to the group $G_m(k, k, 2)$ and two other codewords $\mathbf{b}(e_2)$ and $\mathbf{b}(e_3)$ belong to the group $G_n(k, k, 2)$. In this case, we have the following three-step identification:
  - the codeword $\mathbf{b}(e_1) = (b_1(e_1), b_2(e_1), b_3(e_1))$ is identified on the basis of 1-separating property of $B_m(k, k, 2)$,
  - the set $\{b_3(e_2), b_3(e_3)\}$ evidently identified on the basis of symbol $b_3(e_1)$ and the set $\mathsf{A}_3(\mathbf{e}, B)$,
  - codewords $\mathbf{b}(e_2)$ and $\mathbf{b}(e_3)$ are identified on the basis of the set $\{b_3(e_2), b_3(e_3)\}$.

Theorem 2 is proved.

5. Proof of theorems 3 and 4

Let $s = 3$, $q \ge k \ge 4$, q-nary alphabet $A_q = [q] = \{1, 2, \dots, q\}$ and $B = (\mathbf{b}(1), \mathbf{b}(2), \dots, \mathbf{b}(kq))$ be an arbitrary $(q, k, 3)$-homogeneous 3-hashing code, i.e., B has pairwise distinct codewords $\mathbf{b}(u) = (b_1(u), b_2(u), b_3(u))$, $u = 1, 2, \dots, kq$. By contradiction, it is easy to check the following property of these codes.

Lemma . *Let $a \in [q]$, $b \in [q]$, $a \ne b$ be arbitrary integers and $(q, k, 3)$-homogeneous 3-hashing code B contain codeword $\mathbf{b}(u) = (a, i, j)$. Then B does not contain codeword $\mathbf{b}(v) = (b, i, j)$.*

Hence, for $(q, k, 3)$-homogeneous 3-hashing code B, we can introduce $q \times q$ *characteristic matrix* $C = \|c_i(j)\|$, $i = 1, 2, \dots, q$, $j = 1, 2, \dots, q$ with elements from alphabet $A_{q+1} = \{*, [q]\} = \{*, 1, 2, \dots, q\}$, where

$$c_i(j) = \begin{cases} a, & \text{if there exists codeword } \mathbf{b}(u) = (a, i, j), \\ *, & \text{otherwise.} \end{cases}$$

We shall say that code B *is identified* by the (characteristic) matrix C.

Example 5'. The $(8,4,3)$-homogeneous code B of **Example 5**, is identified by (8×8) matrix

$$C = \begin{pmatrix} * & * & * & 1 & * & 2 & 3 & 5 \\ * & * & 1 & * & 2 & * & 4 & 6 \\ * & 1 & * & * & 3 & 4 & * & 7 \\ 1 & * & * & * & 5 & 6 & 7 & * \\ * & 2 & 3 & 4 & * & * & * & 8 \\ 2 & * & 5 & 6 & * & * & 8 & * \\ 3 & 5 & * & 7 & * & 8 & * & * \\ 4 & 6 & 7 & * & 8 & * & * & * \end{pmatrix}.$$

The characterization of $(q,k,3)$-homogeneous 3-hashing codes is given by Proposition 4.

Proposition 4. *The $(q,k,3)$-homogeneous code B is 3-hashing code iff its characteristic matrix C has the following properties:*

- *for any $a \in [q]$, the number of a-entries in C is equal k,*
- *for any $a \in [q]$ and any row (column) of C, the number of a-entries in the row (column) does not exceed 1,*
- *for any row (column) of C, the number of $*$-entries in the row (column) is equal $q-k$,*
- *if for $i \neq m$ and $j \neq n$, the element $c_i(j) = c_m(n) = a \neq *$, then $c_i(n) = c_m(j) = *$.*

Proof. The first three properties are equivalent to the homogeinity conditions. The necessity and sufficiency of the last property is proved *by contradiction*, because the condition

- $c_i(j) = c_m(n) = a \neq *,\ c_m(j) = b \neq *$

is equivalent to the condition

- there exist three codewords: $\mathbf{b}(u_1) = (a,i,j),\ \mathbf{b}(u_2) = (a,m,n),\ \mathbf{b}(u_3) = (b,m,j)$.

Proposition 4 is proved.

Proof of Theorem 3. Let $k = 3, 4, \ldots$ and $q \geq k^2$. Consider the following consruction of $(q, k, 3)$-homogeneous code $B = \|b_j(u)\|$ whose rows

$$\mathbf{b}_j = (b_j(1), b_j(2), \ldots, b_j(kq)), \ j = 1, 2, 3,$$

are defined as follows:

1. for $j = 1$, the first row
$$\mathbf{b}_1 = (\mathbf{b}_1^{(1)}, \mathbf{b}_1^{(2)}, \ldots, \mathbf{b}_1^{(q)}), \quad \mathbf{b}_1^{(m)} = \underbrace{(m, m, \ldots, m)}_{k}, \ m = 1, 2, \ldots, q;$$

2. for $j = 2$, the second row
$$\mathbf{b}_2 = (\mathbf{b}_2^{(1)}, \mathbf{b}_2^{(2)}, \ldots, \mathbf{b}_2^{(k)}), \quad \mathbf{b}_2^{(m)} = (1, 2, \ldots, q), \ m = 1, 2, \ldots, k;$$

3. for $j = 3$, the third row $\mathbf{b}_3 = (\mathbf{b}_3^{(1)}, \mathbf{b}_3^{(2)}, \ldots, \mathbf{b}_3^{(k)})$, where the subsequence $\mathbf{b}_3^{(m)}$ of length q is the $k(m-1)$-*step cyclic shift* of the sequence $(1, 2, \ldots, q)$:
$$\mathbf{b}_3^{(m)} = \begin{cases} (1, 2, \ldots, q), & \text{if } m = 1, \\ (k(m-1)+1, k(m-1)+2, \ldots, q-1, q, 1, 2, \ldots, k(m-1)), & \text{if } m = 2, 3, \ldots, k. \end{cases}$$

As an illustration, we yield the $(11, 3, 3)$-homogeneous code

$$B = \begin{pmatrix} 111 & 222 & 333 & 444 & 555 & 666 & 777 & 888 & 999 & aaa & bbb \\ 123 & 456 & 789 & ab1 & 234 & 567 & 89a & b12 & 345 & 678 & 9ab \\ 123 & 456 & 789 & ab4 & 567 & 89a & b12 & 378 & 9ab & 123 & 456 \end{pmatrix},$$

where, for convenience of notations, we put $a = 10$, $b = 11$.

If $q \geq k^2$, then this construction of $(q, k, 3)$-homogeneous code B has an evident property of *alphabet separation*, which could be formulated as follows. *Let the symbol $\oplus$ denote modulo kq addition and $u = 1, 2, \ldots, kq$ be an arbitrary fixed integer. Then the q-nary elements of k-subsequence*

$$b_3(u), b_3(u \oplus 1), b_3(u \oplus 2), \ldots, b_3(u \oplus (k-1))$$

do not may occur in the k-subsequence

$$b_3(u \oplus q), b_3(u \oplus (q+1)), b_3(u \oplus (q+2)), \ldots, b_3(u \oplus (q+k-1)).$$

By virtue of Proposition 4, it implies 3-hashing property of code B. Theorem 3 is proved.

Proposition 5. *If there exists $(q_1, k_1, 3)$-homogeneous 3-hashing code B_1 and there exists $(q_2, k_2, 3)$-homogeneous 3-hashing code B_2, then there exists $(q_1q_2, k_1k_2, 3)$-homogeneous 3 - hashing code B called a hash-product of codes B_1 and B_2.*

Proof. Let $v = 1, 2$ and

$$C^v = \|c_i^v(j)\|, \; i, j \in [q_v], \; c_i^v(j) \in \{*, \, [q_v]\},$$

be the characteristic matrix of code B_v. Denote by

$$C = C^1 \diamond C^2 = \|c_r(u)\|, \; r, u \in [q_1q_2], \; c_r(u) \in \{*, \, [q_1q_2]\}$$

the *characteristic matrix of hashing product.* Matrix C is defined as follows: for

$$r = q_2(i-1) + l, \; i \in [q_1], \, l \in [q_2], \quad u = q_2(j-1) + m, \; j \in [q_1], \, m \in [q_2],$$

the element

$$c_r(u) = \begin{cases} q_2(c_i^1(j) - 1) + c_l^2(m), & \text{if } c_i^1(j) \neq * \text{ and } c_l^2(m) \neq *, \\ *, & \text{otherwise.} \end{cases}$$

It is easy to check that the construction of C uses the method of separating alphabets which is similar to the method of Proposition 3. To explain this method we restrict ourselves by considering the following example.

Example 7. Let $k = 2, \; q = 3$, and two equivalent $(3, 2, 3)$-homogeneous 3-hashing codes B_1 and B_2 identified by matrices C_1 and C_2, where

$$C_1 = C_2 = \begin{pmatrix} * & 1 & 2 \\ 1 & * & 3 \\ 2 & 3 & * \end{pmatrix}.$$

Then the matrix

$$C = C_1 \diamond C_2 = \begin{pmatrix} * & * & * & * & 1 & 2 & * & 4 & 5 \\ * & * & * & 1 & * & 3 & 4 & * & 6 \\ * & * & * & 2 & 3 & * & 5 & 6 & * \\ * & 1 & 2 & * & * & * & * & 7 & 8 \\ 1 & * & 3 & * & * & * & 7 & * & 9 \\ 2 & 3 & * & * & * & * & 8 & 9 & * \\ * & 4 & 5 & * & 7 & 8 & * & * & * \\ 4 & * & 6 & 7 & * & 9 & * & * & * \\ 5 & 6 & * & 8 & 9 & * & * & * & * \end{pmatrix}$$

identifies $(9,4,3)$-homogeneous 3-hashing code B from **Example 6**. Proposition 5 is proved.

Consider an arbitrary $(q,k,3)$ -homogeneous 3-hashing code B. Let $(a.b,c)$, (i_1,i_2,i_3) and (j_1,j_2,j_3) be arbitrary ordered 3-subsets of $[q]$. One can easy understand that B is not 3-separating code iff B contains six code-words of the following form

$$\mathbf{b}(\mathbf{e_1}) = \begin{pmatrix} a \\ i_1 \\ j_1 \end{pmatrix}, \mathbf{b}(\mathbf{e_2}) = \begin{pmatrix} b \\ i_2 \\ j_2 \end{pmatrix}, \mathbf{b}(\mathbf{e_3}) = \begin{pmatrix} c \\ i_3 \\ j_3 \end{pmatrix},$$

$$\mathbf{b}(\mathbf{e'_1}) = \begin{pmatrix} a \\ i_2 \\ j_3 \end{pmatrix}, \mathbf{b}(\mathbf{e'_2}) = \begin{pmatrix} b \\ i_3 \\ j_1 \end{pmatrix}, \mathbf{b}(\mathbf{e'_3}) = \begin{pmatrix} c \\ i_1 \\ j_2 \end{pmatrix}.$$

Using the terminology of characteristic matrix C and its (3×3)-*submatrix*

$$\begin{pmatrix} c_{i_1}(j_1) & c_{i_1}(j_2) & c_{i_1}(j_3) \\ c_{i_2}(j_1) & c_{i_2}(j_2) & c_{i_2}(j_3) \\ c_{i_3}(j_1) & c_{i_3}(j_2) & c_{i_3}(j_3) \end{pmatrix},$$

this necessary and sufficient condition could be formulated as follows.

Proposition 6. *Let B be an arbitrary $(q,k,3)$ -homogeneous 3-hashing code with characteristic matrix C and a, b and c be arbitrary pairwise distinct elements of $[q]$. Then B is 3-separating code iff C does not contain any (3×3) submatrix of the form:*

$$\begin{pmatrix} * & a & c \\ a & * & b \\ c & b & * \end{pmatrix}, \begin{pmatrix} c & a & * \\ b & * & a \\ * & b & c \end{pmatrix}, \begin{pmatrix} * & c & a \\ a & b & * \\ c & * & b \end{pmatrix}, \begin{pmatrix} a & * & c \\ * & a & b \\ b & c & * \end{pmatrix}, \begin{pmatrix} a & c & * \\ * & b & a \\ b & * & c \end{pmatrix}, \begin{pmatrix} c & * & a \\ b & a & * \\ * & c & b \end{pmatrix}.$$

These matrices are the permutations of the same three columns.

Proof of Theorem 4. 1). With the help of Proposition 4, it is not difficult to check all assertions whose formulations are given in **Examples 8–12**.

Example 8. For $k=3$, $q=6$, the $(6,3,3)$-homogeneous 3-hashing code B is identified by matrix

$$C = \begin{pmatrix} * & * & 1 & 2 & 3 & * \\ * & 1 & * & 5 & * & 3 \\ 1 & * & * & * & 5 & 4 \\ * & 2 & 5 & * & * & 6 \\ 2 & * & 4 & * & 6 & * \\ 3 & 4 & * & 6 & * & * \end{pmatrix}.$$

Example 9. For $k = 3,\ q = 7$, the $(7, 3, 3)$-homogeneous 3-hashing code B is identified by matrix

$$C = \begin{pmatrix} * & * & 1 & 2 & 3 & * & * \\ * & 1 & * & 5 & 7 & * & * \\ 1 & * & * & * & * & 7 & 3 \\ * & 2 & * & * & * & 5 & 4 \\ 2 & * & 7 & * & * & * & 6 \\ * & 3 & * & 4 & * & 6 & * \\ 5 & * & 4 & * & 6 & * & * \end{pmatrix}.$$

Example 10. For $k = 3,\ q = 8$, the $(8, 3, 3)$-homogeneous 3-hashing code B is identified by matrix

$$C = \begin{pmatrix} * & * & 1 & * & * & 6 & 2 & 4 \\ * & 1 & * & * & 6 & * & * & 3 \\ 1 & * & * & * & * & 5 & * & 7 \\ * & * & * & * & 5 & * & 7 & * \\ * & 2 & 7 & 5 & * & * & * & * \\ 2 & * & * & 6 & * & * & * & 8 \\ * & 4 & * & 3 & * & * & 8 & * \\ 4 & * & 3 & * & * & 8 & * & * \end{pmatrix}.$$

Example 11. For $k = 4,\ q = 10$, the $(10, 4, 3)$-homogeneous 3-hashing code B is identified by

$$C = \begin{pmatrix} * & * & * & * & * & * & 1 & 2 & 5 & 6 \\ * & * & * & * & * & 1 & * & 3 & 4 & 8 \\ * & * & * & * & * & 2 & 3 & * & 7 & 9 \\ * & * & * & * & * & 5 & 4 & 7 & * & 10 \\ * & * & * & * & * & 6 & 8 & 9 & 10 & * \\ * & 1 & 2 & 3 & 4 & * & * & * & * & * \\ 1 & * & 5 & 6 & 7 & * & * & * & * & * \\ 2 & 5 & * & 8 & 9 & * & * & * & * & * \\ 3 & 6 & 8 & * & 10 & * & * & * & * & * \\ 4 & 7 & 9 & 10 & * & * & * & * & * & * \end{pmatrix}.$$

Example 12. For $k = 4,\ q = 11$, the $(11, 4, 3)$-homogeneous 3-hashing code B is identified by

$$C = \begin{pmatrix} * & * & * & * & * & 4 & * & 10 & 11 & 9 & * \\ * & * & * & * & * & * & 5 & 2 & 1 & * & 9 \\ * & * & * & * & * & * & 7 & 6 & * & 1 & 11 \\ * & * & * & * & * & * & 8 & * & 6 & 2 & 10 \\ * & * & * & * & * & 3 & * & 8 & 7 & 5 & * \\ 2 & * & * & * & 1 & * & 3 & * & * & * & 4 \\ * & 5 & 7 & 8 & * & 1 & * & * & * & * & * \\ 10 & 4 & 6 & * & 8 & * & * & * & * & * & * \\ 11 & 3 & * & 6 & 7 & * & * & * & * & * & * \\ 9 & * & 3 & 4 & 5 & * & * & * & * & * & * \\ * & 9 & 11 & 10 & * & 2 & * & * & * & * & * \end{pmatrix}.$$

By virtue of Proposition 2, **Examples 5–7** and **11–12** yield the first part of statement 1) of Theorem 4 for $q = 8, 9, 10, 11$. For the case $q = 12$, introduce the evident $(4, 2, 3)$-homogeneous 3-hashing code B with characteristic matrix

$$\begin{pmatrix} 1 & * & 2 & * \\ * & 1 & * & 2 \\ 3 & * & 4 & * \\ * & 3 & * & 4 \end{pmatrix}.$$

By virtue of Proposition 5, this $(4, 2, 3)$-homogeneous 3-hashing code and the $(3, 2, 3)$-homogeneous 3-hashing code of **Example 7** yield the $(12, 4, 3)$-homogeneous 3-hashing code. the first part of statement 1) is proved.

With the help of Propositions 4 and 6, it is not difficult to check all assertions whose formulations are given in **Examples 13–15**.

Example 13. For $k = 4,\ q = 13$, the $(13, 4, 3)$-homogeneous 3-*separating* code is identified by matrix

$$C = \begin{pmatrix}
\ast & \ast & \ast & \ast & \ast & \ast & 4 & 2 & 3 & \ast & 8 & \ast & \ast \\
\ast & \ast & \ast & \ast & \ast & \ast & \ast & 7 & 13 & 5 & 1 & \ast & \ast \\
\ast & \ast & \ast & \ast & \ast & \ast & \ast & 9 & 10 & \ast & \ast & 1 & 8 \\
\ast & \ast & \ast & \ast & \ast & \ast & 6 & 12 & 11 & \ast & \ast & 5 & \ast \\
\ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & 10 & 11 & 13 & 3 \\
\ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & 9 & 12 & 7 & 2 \\
1 & \ast & \ast & 13 & \ast & \ast & \ast & \ast & \ast & 6 & \ast & \ast & 4 \\
2 & 7 & 9 & 12 & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
3 & 6 & 11 & 10 & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
\ast & 5 & \ast & \ast & 11 & 9 & 13 & \ast & \ast & \ast & \ast & \ast & \ast \\
8 & 4 & \ast & \ast & 10 & 12 & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
\ast & \ast & 4 & 5 & 6 & 7 & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
\ast & \ast & 8 & \ast & 3 & 2 & 1 & \ast & \ast & \ast & \ast & \ast & \ast
\end{pmatrix}.$$

Example 14. For $k = 4,\ q = 14$, the $(14, 4, 3)$-homogeneous 3-*separating* code is identified by matrix

$$C = \begin{pmatrix}
\ast & \ast & \ast & \ast & \ast & \ast & \ast & 1 & 2 & 3 & 4 & \ast & \ast & \ast \\
\ast & \ast & \ast & \ast & \ast & \ast & \ast & 5 & 6 & 7 & 8 & \ast & \ast & \ast \\
\ast & \ast & \ast & \ast & \ast & \ast & \ast & 9 & 10 & 11 & 12 & \ast & \ast & \ast \\
\ast & \ast & \ast & \ast & \ast & \ast & \ast & 13 & \ast & \ast & \ast & 12 & 8 & 4 \\
\ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & 14 & \ast & \ast & 11 & 7 & 3 \\
\ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & 13 & \ast & 10 & 6 & 3 \\
\ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & 14 & 9 & 5 & 1 \\
1 & 5 & 9 & 13 & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
2 & 6 & 10 & \ast & 14 & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
3 & 7 & 11 & \ast & \ast & 13 & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
4 & 8 & 12 & \ast & \ast & \ast & 14 & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
\ast & \ast & \ast & 12 & 11 & 10 & 9 & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
\ast & \ast & \ast & 8 & 7 & 6 & 5 & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
\ast & \ast & \ast & 4 & 3 & 2 & 1 & \ast & \ast & \ast & \ast & \ast & \ast & \ast
\end{pmatrix}.$$

Example 15. For $k = 4,\ q = 15$, the $(15, 4, 3)$-homogeneous 3-separating code is identified by matrix

$$
C = \begin{pmatrix}
\ast & \ast & \ast & \ast & \ast & \ast & \ast & 4 & \ast & \ast & 2 & 3 & 8 & \ast & \ast \\
\ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & 5 & 1 & 13 & 7 & \ast & \ast & \ast \\
\ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & 9 & 10 & 14 & \ast & \ast & \ast & 3 \\
\ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & 11 & 12 & \ast & \ast & \ast & 7 & 8 \\
\ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & 15 & \ast & \ast & 14 & 13 & 2 \\
\ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & 15 & 10 & 12 & 1 & \ast \\
\ast & \ast & \ast & \ast & \ast & \ast & \ast & 6 & \ast & \ast & \ast & 9 & 11 & 5 & \ast \\
1 & \ast & \ast & \ast & \ast & \ast & 13 & \ast & 6 & \ast & \ast & \ast & \ast & \ast & 4 \\
\ast & 5 & 9 & 11 & \ast & \ast & \ast & 13 & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
\ast & 4 & 10 & 12 & 15 & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
2 & 6 & 14 & \ast & \ast & 15 & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
3 & 7 & \ast & \ast & \ast & 10 & 9 & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
8 & \ast & \ast & \ast & 14 & 12 & 11 & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
\ast & \ast & \ast & 6 & 7 & 4 & 5 & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
\ast & \ast & 3 & 8 & 2 & \ast & \ast & 1 & \ast & \ast & \ast & \ast & \ast & \ast & \ast
\end{pmatrix}.
$$

By virtue of Proposition 2, **Examples 13–15** yield the second part of statement 1) of Theorem 4 if $q = 13, 14, 15$.
Statement 1) is proved.

Let $q = 3i$, $i = 6, 7, \ldots, 11$. Applying Proposition 5 , we can construct the corresponding $(3i, 6, 3)$-homogeneous 3-hashing code as the hashing product of $(3, 2, 3)$- and $(i, 3, 3)$-homogeneous 3-hashing codes, whose parameters are given in **Examples 8–10** and in Theorem 3.

If $q = 4j$, $j = 7, 8$, then we can obtain the $(4j, 6, 3)$- homogeneous 3-hashing code as the hashing product of $(4, 2, 3)$- and $(4j, 3, 3)$-homogeneous 3-hashing codes from **Examples 9** and **10**.
Theorem 4 is proved.

References

[1] W.H. Kauts, R.C. Singleton, "Nonrandom Binary Superimposed Codes," *IEEE Trans. Inform. Theory*, vol. 10, no. 4, pp. 363-377, 1964.

[2] A.G. D'yachkov, V.V. Rykov, "A Survey of Superimposed Code Theory," *Problems of Control and Inform. Theory*, vol. 12, no. 4, pp. 229-242, 1983.

[3] A. Renyi, "On the Theory of Random Search," *Bull. Amer. Math. Sos.*, v. 71, no. 6, pp. 809-828, 1965.

[4] G. Katona, "On Separating System of a Finite Set," *J. Combin. Theory*, v. 1, no. 2, pp. 174-194, 1966.

[5] J. Korner, M. Lucertini, "Compressing inconsistent data," *IEEE Trans. Inform. Theory*, vol. 40, no. 3, pp. 706- 715, 1994.