Some new Constructions of Optimal Superimposed Designs.

Sergey Yekhanin
* Moscow State University, Faculty of Mechanics and Mathematics
Department of Probability Theory, Moscow, 119899, Russia
Email: yekhanin@cityline.ru

Abstract– D'yachkov-Rykov in [1-2] presented optimal constructions of superimposed codes and designs. Their constructions are based on the q-ary codes, that were studied by Kautz-Singleton. This paper improves D'yachkov-Rykov's results concerning optimal superimposed designs.

1. Notations and Formulation of the Results.

Let $1 \leq s \leq t,\ 1 \leq k \leq t,\ N \geq 1$ 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) $\mathbf{x}(1), \mathbf{x}(2), \ldots, \mathbf{x}(t)$ and rows $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N$, where $\mathbf{x}(u) = (x_1(u), x_2(u), \ldots, x_N(u))$ and $x_i = (x_i(1), \ldots, x_i(t))$. Let $k = \max_i \sum\limits_{u=1}^{t} x_i(u)$ be the *maximal weight of rows.*

The code X is called a *superimposed* (s,t)-design if all the Boolean sums composed of not more than s columns are distinct.

Definition 1. An $(N \times t)$-matrix X is called a superimposed (s,t,k)-design of *length* N, *size* t, *strength* s and *constraint* k if code X is a superimposed (s,t)-design whose maximal row weight is equal to k.

By $N(s,t,k)$ we denote the minimal possible length of the superimposed (s,t,k)-design.

In [1] the following fact was proved:
For any $s \geq 3,\ k \geq s+1,\ q = k^{s-1}$ there is an optimal superimposed (s,kq,k)-design of length sq. The following theorem improves this result in case $s = 3$.

Theorem: Let $4 \leq k,\ q \geq k^2$ be integers. Then $N(s, kq, k) = 3q$.

Proof of the Theorem.

To prove the theorem we need the following notations and definitions.

Let $q \geq k \geq 4$, $t = kq$ be integers,

$A_q = [q] = \{1, \ldots, q\}$ be a q-nary alphabet,

Code $B =\| b_j(u) \|\ \ j = 1, 2, 3,\ u = 1, \ldots t$ be a q-nary $(3 \times t)$-matrix with elements $b_j(u)$ from A_q,

$\mathbf{b}(u) = (b_1(u), b_2(u), b_3(u))$, $u = 1, \ldots t$, be columns (codewords).

Definition 2. Code B is called an $(q,k,3)$-*homogeneous* code if for any $j = 1, 2, 3$ and any a from A_q, the number of a-entries in the $j-th$ row $\mathbf{b}_j$ is equal to k.

We call a homogeneous $(q,k,3)$-code B a 2-*disjunct* code if the Hamming distance of code $H(B) \geq 2$.

* This work was supported by the Russian Fundamental Research Foundation, Project 98-01-00241

Let $\mathbf{e} = (e_1, e_2, e_3)$ be an arbitrary 3-subset of set $[t] = \{1, \ldots t\}$. For a given code B and any $j = 1, 2, 3$, denote by $A_j(\mathbf{e}, B)$-the set of all pairwise distinct elements of the sequence $b_j(e_1), b_j(e_2), b_j(e_3)$.

Definition 3. Let $n \leq 3$ be arbitrary integer. 2-disjunct code B is called an 3-separable code if for an arbitrary n-subset $\mathbf{e} = (e_1, \ldots, e_n)$ of set $[t]$, there exists the possibility to identify this subset on the basis of sets:

$$A_1(\mathbf{e}, B),\ A_2(\mathbf{e}, B),\ A_3(\mathbf{e}, B)$$

Definition 4. Homogeneous code B is called a 3-*hash* if for an arbitrary 3-subset $\mathbf{e} = (e_1, e_2, e_3)$, of the set $[t]$, there exists a coordinate $j = 1, 2, 3$, such that all the elements $b_j(e_1), b_j(e_2), b_j(e_3)$ are all different.

Let a symbol b from $[q]$ of $(q, k, 3)$ separable code be replaced by the binary q-sequence in which all the elements are 0's, except the element with the number b. As a result we obtain a binary code X_B which is a superimposed design.

Consider an arbitrary $(q, k, 3)$ 2-disjunct code B. We introduce a characteristic $(q \times q)$-matrix C with the elements from alphabet $A_{q+1} = \{*, [q]\} = \{*, 1, 2, \ldots q\}$. Where

$$C_{ij} = \begin{cases} \text{a}, & \text{if in } X \text{ there is a codeword } (i, j, a); \\ *, & \text{otherwise.} \end{cases}$$

We say that matrix B is identified by the characteristic matrix C which will be called $C(q, k)$-matrix.

Matrix C is an $C(q, k)$-matrix if and only if C has the following properties:

1. For any x from $[q]$ there are exactly k pairs (i, j) such that $C_{ij} = x$. Hence, there are $q(q - k)$ $*$ in $C(q, k)$.

2. For any p, i, j from $[q]$ neither $C_{pi} = C_{pj} \neq *$ nor $C_{ip} = C_{jp} \neq *$ where $i \neq j$. Hence all the numbers in one column or row are distinct.

3. For any column (row) of C the number of $*$-entries s equal to k.

Denote by $C_{HS}(q, k)$-matrices of hash&separable code.

It is possible to prove that matrix C is $C_{HS}(q, k)$ if and only if C has the properties $1 - 3$ and the following 2 properties.

4. For any i, j, k, p from $[q]$ such that $C_{ij} = C_{kp} = a$ the $C_{ip} = C_{kj} = *$. Hence there are no submatrixes of the form of:

$$\begin{pmatrix} a & b \\ & a \end{pmatrix}$$

5. If $C_{iv} = C_{jp} = a$ and $C_{kv} = C_{jr} = b$ then $C_{ir} \neq C_{kp}$ Hence, in $C_{HS}(q, k)$ there are no submatrixes of the form of:

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

Lemma 1: Let $k \geq 4, c$ be integers. In case $c \geq k$ than there exists an $C_{HS}(ck, k)$.

Proof: By Q we denote a $((c + k) \times k)$-matrix whose elements are defined as follows:

$$Q_{ij} = \begin{cases} \text{(i-1)+j}, & \text{if } 1 \leq i \leq c; \\ \text{(i-c)+j}, & \text{if } c + 1 \leq i \leq c + k. \end{cases}$$

Let p be some integer $1 \leq p \leq c$. By B_k^p we denote a $(k \times k)$-matrix whose i^{th} row is the $(i+p)^{th}$ row of matrix Q.We construct

$$C(ck,k) = \begin{pmatrix} B_k^1 & & & \\ & B_k^2 & & \\ & & \ddots & \\ & & & B_k^c \end{pmatrix}$$

One can easily check that this matrix has all the properies $1-4$.

Lemma 2: Let $k \geq 4, q$ be integers. In case $q \geq k^2$ than there exists an $C_{HS}(q,k)$.

Proof: As $q \geq k^2$ $q = ck + r$ where $r \leq k$ and $c \geq r$. Here we explain an algorithm of constructing $C_{HS}(k,q)$.

Algorithm:

Step 1: According to the method explained in Lemma 2 we can simply construct a $C_{HS}(ck,k)$ where on the diagonal there are c squares-$(k \times k)$ We denote the first k of them as $A_1, A_2, \ldots, A_k$.

Step 2: (By this step we extend our alphabet with new numbers $ck+1, ck+2, \ldots, ck+r$). In every A_i r numbers $\{(i-1)k+1, (i-1)k+2, \ldots, (i-1)k+r\}$ (r first numbers) are changed to the numbers $ck+1, ck+2, \ldots, ck+r$.

Step 3: (By this step we change the size of the square).

We construct new squares D_i A_i $(1 \leq i \leq r)$. The size of the D_i will be $q+1$. On the diagonal positions we place $*$. On the sub-diagonal line (positions $C_{i(i-1)}$ where $2 \leq i \leq k+1$) the elements $i, k+i, \ldots, k(k-1)+i$ will be placed in some order. If in square A_i there also are elements from $\{i, k+i, \ldots, k(k-1)+i\}$ they will be placed at the positions symmetric to their equal on the sub-diagonal line. All the other elements from A_i will be transfered to D_i in arbitrary fixed order. There will be enough place as changing the size of the square we've added $2k+1$ new positions to it. And after that we've filled k positions with the numbers $i, k+i, \ldots, k(k-1)+i$ and $k+1$ with $*$.

Step 4: Changing the matrices A_i to D_i on the diagonal of $C_(ck,k)$ we get an $C(q,k)$.

One can easily check that all the properies $1-4$ are fulfilled. So Lemma 2 is proved.

To illustrate the algorithm the following example is given.

Example: Let $k = 3,\ q = 11\ \Rightarrow c = 3,\ r = 2$. Instead of 10 we write a, and instead of 11 we write b.

Step 1:

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

Step 2:

$$A_1 \Rightarrow \begin{pmatrix} a & b & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}, \quad A_2 \Rightarrow \begin{pmatrix} a & b & 6 \\ 7 & 8 & 9 \\ 1 & 2 & 3 \end{pmatrix}, \quad A_3 \Rightarrow \begin{pmatrix} a & b & 9 \\ 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}.$$

Step 3:

$$D_1 = \begin{pmatrix} * & a & b & 3 \\ 1 & * & 4 & 6 \\ 5 & 4 & * & 7 \\ 9 & 8 & 7 & * \end{pmatrix}, \quad D_2 = \begin{pmatrix} * & 2 & b & 8 \\ 2 & * & a & 3 \\ 7 & 5 & * & 9 \\ 6 & 1 & 9 & * \end{pmatrix}.$$

Step 4:

$$C(11,3) = \begin{pmatrix} * & a & b & 3 & * & * & * & * & * & * & * \\ 1 & * & 4 & 6 & * & * & * & * & * & * & * \\ 5 & 4 & * & 7 & * & * & * & * & * & * & * \\ 9 & 8 & 7 & * & * & * & * & * & * & * & * \\ * & * & * & * & * & 2 & b & 8 & * & * & * \\ * & * & * & * & 2 & * & a & 3 & * & * & * \\ * & * & * & * & 7 & 5 & * & 9 & * & * & * \\ * & * & * & * & 6 & 1 & 9 & * & * & * & * \\ * & * & * & * & * & * & * & * & a & b & 9 \\ * & * & * & * & * & * & * & * & 1 & 2 & 3 \\ * & * & * & * & * & * & * & * & 4 & 5 & 6 \end{pmatrix}.$$

From [1] it is known that $N(3, kq, k) \geq 3q$ where $q \geq k \geq 4$. Lemma 2 proves that for the case of $q \geq k^2$ there is a method of constructing designs of length $3q$. Hence, in this case $N(3, kq, k) = 3q$ and theorem is proved.

3. References

[1] A.G. D'yachkov, A.J. Macula, V.V. Rykov "On Optimal Parameters of a class of Superimposed Codes and Designs," *Proc. Int. Symp. on Information Theory*, Boston, USA, August 1998.

[2] A.G. D'yachkov, V.V. Rykov "Some Constructions of Optimal Superimposed Codes," *Conference on "Computer Science and Information Technologies",* Yerevan, Armenia, September 1997, pp. 242-245.