МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2006
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2006
Proceedings of the Thirty Fifth Spring Conference of
the Union of Bulgarian Mathematicians
Borovets, April 5–8, 2006

THE UNIQUENESS OF THE OPTIMAL (20,10,2,2) SUPERIMPOSED CODE*

Stoyan N. Kapralov, Mladen D. Manev

The uniqueness (up to equivalence) of the optimal (20,10,2,2) superimposed code is proved.

1. Introduction.

Definition 1.1. *A binary $N \times T$ matrix $C = (c_{ij})$ is called an (N, T, w, r) superimposed code (SIC) if for any pair of subsets $W, R \subset \{1, ..., T\}$ such that $|W| = w$, $|R| = r$ and $W \bigcap R = \emptyset$, there exists a row $i \in \{1, \ldots, N\}$ such that $c_{ij} = 1$ for all $j \in W$ and $c_{ij} = 0$ for all $j \in R$.*

Let $N(T, w, r)$ be the minimum length N for which an (N, T, w, r) SIC exists, and let $T(N, w, r)$ be the maximum size T for which an (N, T, w, r) SIC exists. Superimposed (N, T, w, r) codes with length $N = N(T, w, r)$ or size $T = T(N, w, r)$ are called optimal.

The problem of determining the exact values of $N = N(T, w, r)$ and $T(N, w, r)$ is completely solved only for $w = r = 1$.

Theorem 1.2. (*Sperner Theorem*) [5] $T(N, 1, 1) = \binom{N}{\lfloor N/2 \rfloor}$.

In [1] the nonexistence of (19,10,2,2) superimposed code is proved. In [2] a construction of a (20,10,2,2) superimposed code is presented. Another construction of a (20,10,2,2) SIC is given in [3] but the constructed code turned out to be equivalent to the known one.

In the present paper we prove that there is a unique (20,10,2,2) superimposed code. The result is based on the classification (up to equivalence) of the residual (9,9,1,2) and (5,8,1,1) superimposed codes.

2. Preliminaries.

Definition 2.1. *Two (N, T, w, r) superimposed codes are called equivalent if anyone of them can be obtained from the other by a sequence of operations of the following types:*
(a) permutation of the rows;
(b) permutation of the columns;
(c) taking the complementary values of all the code entries.

*Partially supported by the Bulgarian National Science Fund (Project MM-1304/2003) and by Technical University of Gabrovo (Project III.1/2005).

Let C be a binary $N \times T$ matrix. Denote by $d(x,y)$ the Hamming distance between two columns x and y and let $d_2 = \min\{d(x,y) \mid x,y \in C,\ x \neq y\}$. Let $d(x,y,z) = d(x,y) + d(x,z) + d(y,z)$ and $d_3 = \min\{d(x,y,z) \mid x,y,z \in C,\ x \neq y, x \neq z, y \neq z\}$.

Lemma 2.2. *(Plotkin bound)* [4] $\binom{T}{2} d_2 \leq \sum_{x,y \in C,\ x \neq y} d(x,y) \leq N \left\lfloor \frac{T}{2} \right\rfloor \left\lfloor \frac{T+1}{2} \right\rfloor$.

Corrolary 2.3 $\binom{T}{3} d_3 \leq (T-2) N \left\lfloor \frac{T}{2} \right\rfloor \left\lfloor \frac{T+1}{2} \right\rfloor$.

Definition 2.4. *The residual code $Res(C, x = v)$ of a superimposed code C with respect to value v in the column x is a code obtained in the following way: take all the rows in which C has value v in column x, and delete the x-th entry in the selected rows.*

Denote by $Res(C, x = v_1, y = v_2)$ the code $Res(Res(C, x = v_1), y = v_2)$. Denote by S_x the characteristic set of the column x.

Lemma 2.5. *Suppose C is an (N, T, w, r) superimposed code and x and y are two different columns of C. Then*
(a) $Res(C, x = 1)$ is a $(|S_x|, T-1, w-1, r)$ superimposed code;
$Res(C, x = 0)$ is an $(N - |S_x|, T-1, w, r-1)$ superimposed code;
(b) $Res(C, x = 1, y = 0)$ is an $(N', T-2, w-1, r-1)$ superimposed code.

Lemma 2.6. *Suppose C is a $(20, 10, 2, 2)$ superimposed code. Then*
(a) $9 \leq |S_x| \leq 11$ for $x \in C$;
(b) $|S_x \bigcap \overline{S}_y| \geq 5$ for any two different columns $x, y \in C$;
(c) $d_2 = 10$.

Proof. (a) It is known that $N(9,1,2) = N(9,2,1) = 9$ [2]. Then the result follows from Lemma 2.5 (a).
(b) By Theorem 1.2 $N(8,1,1) = 5$ and the result follows from Lemma 2.5. (b).
(c) It follows from (b) that $d_2 \geq 10$. It follows from Corollary 2.3 that $d_3 \leq 33$. But d_3 is even, hence, $d_3 \leq 32$. If $d_2 \geq 11$, then $d_3 \geq 33$ – a contradiction. □

If C is a (20,10,2,2) superimposed code and x is a column of weight 9, then the residual code $Res(C, x = 1)$ is a (9,9,1,2) SIC. If C is a (20,10,2,2) superimposed code and x, y are two columns at distance 10, then the residual code $Res(C, x = 1, y = 0)$ is a (5,8,1,1) SIC.

Our approach to the construction of (20,10,2,2) codes consists in extending the residual (9,9,1,2) and (5,8,1,1) codes.

The (9,9,1,2) superimposed codes are classified in [3]. The non-equivalent (5,8,1,1) codes are enumerated in the next section.

3. Classification of $(5, T, 1, 1)$ SIC. It follows from the Sperner Theorem that $T(5,1,1) = 10$. The classification of $(5, T, 1, 1)$ SIC for $T = 8, 9, 10$ is presented in this section.

Let B_i be the number of the columns of weight i in a superimposed code C.

Lemmma 3.1. *If C is a (5,T,1,1) SIC with $T \geq 8$ then $B_1 = B_4 = 0$.*

Proof. If $wt(x) = 1$, then $Res(C, x = 0)$ is a $(4, T-1, 1, 1)$ SIC – a contradiction to the Sperner Theorem. □

Lemma 3.2. *If C is a $(5, T, 1, 1)$ SIC with $T \geq 8$, $B_2 \neq 0$, $B_3 \neq 0$ then $T = 8$.*

Proof. From Lemma 3.1 $B_2 + B_3 = T$. We may assume that $B_2 \geq B_3$ (if $B_2 < B_3$ we consider the complementary code).

Case 1: $B_3 = 1$. Let x be the column of weight 3, and $S_x = \{i_1, i_2, i_3\}$. Since C is (1,1) SIC, there is no column y with $S_y = \{i_1, i_2\}$, $S_y = \{i_1, i_3\}$ or $S_y = \{i_2, i_3\}$. Hence, there are at most $10 - 3 = 7$ possibilities for the columns of weight 2. Therefore, $B_2 \leq 7$ and $T = B_2 + B_3 \leq 7 + 1 = 8$. The corresponding (5,8,1,1) SIC is uniquely determined up to equivalence.

Case 2: $B_3 = 2$. Let $S_x = \{i_1, i_2, i_3\}$ and $S_y = \{j_1, j_2, j_3\}$. Then, the pairs $\{i_1, i_2\}$, $\{i_1, i_3\}$, $\{i_2, i_3\}$, $\{j_1, j_2\}$, $\{j_1, j_3\}$, $\{j_2, j_3\}$ are forbidden to be a characteristic set of a column of C. Since $|S_x \bigcap S_y| \leq 2$, there is at most one common pair between the first and the second triple of forbidden pairs. Consequently, $B_2 \leq 5$ and $T = B_2 + B_3 \leq 7$ – a contradiction.

Case 3: $B_3 = 3$. Let x,y and z be columns of weight 3. If there are 6 forbidden pairs from x,y (or x,z, or y,z), then $T = B_2 + B_3 \leq 4 + 3 = 7$ – a contradiction. If $|S_x \bigcap S_y| = |S_x \bigcap S_z| = |S_y \bigcap S_z| = 2$, then there are (up to equivalence) two possibilities for the columns of weight 3:

$$\begin{matrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix} \qquad\qquad \begin{matrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{matrix}$$

which have 7 and 6 forbidden pairs, respectively. Therefore, $T \leq 7$, a contradiction.

Case 4: $B_3 = 4$. There are at least 6 forbidden pairs, hence, $T \leq 8$. The only case for exactly 6 forbidden pairs is (up to equivalence):

$$\begin{matrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{matrix}$$

and the corresponding (5,8,1,1) SIC is uniquely determined up to equivalence.

Case 5: $B_3 \geq 5$. Then, by the similar reason as in Case 4, $B_2 \leq 4$ and therefore $B_2 < B_3$ – a contradiction. □

Theorem 3.3. (*a*) *There is a (5,10,1,1) SIC.*
(*b*) *There is a (5,9,1,1) SIC.*

Proof. (a) The code consists of all binary vectors of weight 2.

(b) The code is obtained from the (5,10,1,1) SIC by deleting an arbitrary column. □

Theorem 3.4. *There are exactly four non-equivalent (5,8,1,1) SIC.*

Proof. There are two non-equivalent (5,8,1,1) SIC with $B_3 > 0$ already mentioned in the proof of Lemma 3.2 cases 1 and 4.

Any (5,8,1,1) SIC with all the columns of weight 2 can be obtained by deleting two columns x and y of the (5,10,1,1) SIC. There are two non-equivalent possibilities: $|S_x \bigcap S_y| = 0$ or $|S_x \bigcap S_y| = 1$.

Thus any (5,8,1,1) SIC is equivalent to one of the codes $(A|B_i)$, $i = 1, 2, 3, 4$, where

$$A = \begin{matrix} 1\,1\,1\,1 \\ 1\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,1\,0 \\ 0\,0\,0\,1 \end{matrix} \quad B_1 = \begin{matrix} 0\,0\,0\,0 \\ 1\,1\,1\,0 \\ 1\,1\,0\,1 \\ 1\,0\,1\,1 \\ 0\,1\,1\,1 \end{matrix} \quad B_2 = \begin{matrix} 0\,0\,0\,0 \\ 1\,1\,0\,0 \\ 1\,0\,1\,0 \\ 1\,0\,0\,1 \\ 0\,1\,1\,1 \end{matrix} \quad B_3 = \begin{matrix} 0\,0\,0\,0 \\ 1\,1\,1\,0 \\ 1\,0\,0\,1 \\ 0\,1\,0\,1 \\ 0\,0\,1\,0 \end{matrix} \quad B_4 = \begin{matrix} 0\,0\,0\,0 \\ 1\,1\,0\,0 \\ 1\,0\,1\,0 \\ 0\,1\,0\,1 \\ 0\,0\,1\,1 \end{matrix}$$

□

4. The uniqueness of the $(20, 10, 2, 2)$ superimposed code.

Lemma 4.1. *If C is a (20,10,2,2) SIC and $|S_x \bigcap \overline{S}_y| = 5$ for some two columns x,y, then for any column z, $z \neq x$, $z \neq y$ the following condition holds:* $2 \leq |S_x \bigcap \overline{S}_y \bigcap S_z| \leq 3$.

Proof. The residual code $Res(C, x = 1, y = 0)$ is a (5,8,1,1) SIC, therefore, the weight of a column is either 2 or 3. □

Theorem 4.2. *Up to equivalence there is a unique $(20, 10, 2, 2)$ superimposed code.*

Proof.

Case 1. Suppose C is a (20,10,2,2) SIC with a column x of weight 9. If there is a column of weight 11, then we may consider the complementary code. The residual code $Res(C, x = 1)$ is a (9,9,1,2) SIC. There are exactly 25 non-equivalent (9,9,1,2) SIC [1]. We are looking for (20,10,2,2) SIC of the form

$$\left(\begin{array}{c|c} 1 & \\ \vdots & A \\ 1 & \\ \hline 0 & \\ \vdots & B \\ 0 & \end{array}\right),$$

where the matrix A is a (9,9,1,2) SIC, and the 11×9 matrix B has to be chosen in such a way that the whole matrix to be a (20,10,2,2) SIC. We may assume that the rows of B are sorted lexicographically. We construct the matrix B column by column, and at each step we check the conditions of Lemma 2.6, Lemma 4.1, the sorted rows property, and the superimposed code property.

It turns out that exactly one of the 25 (9,9,1,2) SIC can be extended to (20,10,2,2) SIC, and this extension can be done in a unique way.

Case 2. Suppose C is a (20,10,2,2) SIC with all columns of weight 10. Up to equivalence we may assume that the Hamming distance between first two columns is 10. Then the code is of the form

$$\left(\begin{array}{c|cc} 10 & & \\ \vdots & A & B_i \\ 10 & & \\ \hline 01 & & \\ \vdots & & \\ 01 & X & \\ 00 & & \\ \vdots & & \\ 00 & & \end{array}\right)$$

where the matrices A and B_i are as in Theorem 3.4, and the 15×8 matrix X has to be chosen in such a way that the whole matrix is a (20,10,2,2) SIC with all columns of weight 10.

We construct the matrix X column by column, keeping at each step properties similar to these in Case 1. However, it turns out, that at most 5 column could be chosen. Hence, there is no (20,10,2,2) superimposed code with columns of weight 10 only. □

REFERENCES

[1] S. Kapralov, M. Manev. The nonexistence of (19,10,2,2) superimposed codes, *Proc. Fourth Intern. Workshop on Optimal Codes and Related Topics*, Pamporovo, Bulgaria, June 17-23, 2005, 196–200.
[2] H.K. Kim, V.S.Lebedev. On optimal superimposed codes, *Journal of Combinatorial Designs*, 12, 2004, 79–91.
[3] M. Manev. A method of finding upper bounds for the length of optimal superimposed codes, *Proc. Intern. Conference UNITEX'2005*, Gabrovo, Bulgaria, November 24-25, 2005, III–361–364.
[4] M. Plotkin Binary codes with specified minimum distance, *IRE Trans. Inform. Theory*, 6, 1960, 445–450.
[5] E. Sperner. Ein Satz über Untermengen einer endlichen Menge, *Mathematische Zeitschrift*, 27, 1928, 544–548.

Stoyan Kapralov
Mladen Manev
Department of Mathematics
Technical University of Gabrovo
5300 Gabrovo, Bulgaria
e-mail: skapralov@tugab.bg
e-mail: manev@tugab.bg

ЕДИНСТВЕНОСТ НА ОПТИМАЛНИЯ (20,10,2,2) РАЗДЕЛЯЩ КОД

Стоян Н. Капралов, Младен Д. Манев

Доказано е, че с точност до еквивалентност оптималният (20,10,2,2) разделящ код е единствен.