Serdica J. Computing **3** (2009), 15–22

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

ON SOME OPTIMAL $(N, T, 1, 2)$ AND $(N, T, 1, 3)$ SUPERIMPOSED CODES*

Mladen D. Manev

Abstract. One of the main problems in the theory of superimposed codes is to find the minimum length N for which an (N, T, w, r) superimposed code exists for given values of T, w and r. Let $N(T, w, r)$ be the minimum length N for which an (N, T, w, r) superimposed code exists. The (N, T, w, r) superimposed code is called optimal when $N = N(T, w, r)$. The values of $N(T, 1, 2)$ are known for $T \leq 12$ and the values of $N(T, 1, 3)$ are known for $T \leq 20$. In this work the values of $N(T, 1, 2)$ for $13 \leq T \leq 20$ and the value of $N(21, 1, 3)$ are obtained. The optimal superimposed codes with parameters $(9, 10, 1, 2)$, $(10, 13, 1, 2)$, $(11, 14, 1, 2)$, $(11, 15, 1, 2)$, $(11, 16, 1, 2)$ and $(11, 17, 1, 2)$ are classified up to equivalence. The optimal $(N, T, 1, 3)$ superimposed codes for $T \leq 20$ are classified up to equivalence.

1. Introduction.

$(N, T, 1, r)$ superimposed codes were introduced by Kautz and Singleton [4]. A natural generalization of the $(N, T, 1, r)$ superimposed codes was made by Mitchell and Piper [7], who discuss the (N, T, w, r) superimposed codes in connection with cryptographic problems.

ACM Computing Classification System (1998): E.4.

Key words: superimposed codes, classification.

*Partially supported by the Technical University of Gabrovo under Grant C-801/2008.

Definition 1. *A binary $N \times T$ matrix C is called an (N, T, w, r) superimposed code (SIC) of length N and size T if for any pair of subsets $W, R \subset \{1, 2, \ldots, T\}$ such that $|W| = w$, $|R| = r$ and $W \cap R = \varnothing$, there exists a row $i \in \{1, 2, \ldots, N\}$ such that $c_{ij} = 1$ for all $j \in W$ and $c_{ij} = 0$ for all $j \in R$.*

There is a simple example of an (N, T, w, r) superimposed code. If we take a matrix whose rows are all possible binary vectors of weight w, then this matrix becomes an (N, T, w, r) superimposed code with $N = \binom{T}{w}$. We call this matrix the trivial superimposed code. The identity matrix is the trivial code for $w = 1$.

Let $N(T, w, r)$ be the minimum length N for which an (N, T, w, r) superimposed code exists. (N, T, w, r) superimposed codes with length $N = N(T, w, r)$ are called optimal.

Definition 2. *Two (N, T, w, r) superimposed codes are equivalent if one of them can be transformed into the other by a permutation of the rows and a permutation of the columns.*

Engel proved in [2] that the trivial code is optimal when $T \leq w + r + \frac{r}{w}$ and $w \leq r$. Therefore the identity matrix is an optimal $(T, T, 1, 2)$ superimposed code for $T \leq 5$ and an optimal $(T, T, 1, 3)$ superimposed code for $T \leq 7$. Kim and Lebedev [5] give the following values of $N(T, 1, 2)$ and $N(T, 1, 3)$:

T	5	6	7	8	9–12
$N(T,1,2)$	5	6	7	8	9

T	5	6	...	14	15	16–20
$N(T,1,3)$	5	6	...	14	15	16

Consequently the identity matrix is an optimal $(T, T, 1, 2)$ superimposed code for $T \leq 9$ and an optimal $(T, T, 1, 3)$ superimposed code for $T \leq 16$.

The number of nonequivalent classes of optimal $(N(T, 1, 2), T, 1, 2)$ superimposed codes for $T \leq 9$ is presented in [3]:

T	3	4	5	6	7	8	9
#	1	1	1	1	2	4	25

Kim, Lebedev and Oh proved the uniqueness of the $(9, 12, 1, 2)$ superimposed code in [6] and Oh proved the uniqueness of the $(9, 11, 1, 2)$ superimposed code in [8].

In this paper the values of $N(T, 1, 2)$ are obtained for $13 \leq T \leq 20$ and the optimal superimposed codes with parameters $(9, 10, 1, 2)$, $(10, 13, 1, 2)$,

$(11, 14, 1, 2)$, $(11, 15, 1, 2)$, $(11, 16, 1, 2)$, and $(11, 17, 1, 2)$ are classified up to equivalence. The optimal $(N, T, 1, 3)$ superimposed codes for $T \leq 20$ are classified up to equivalence and the value of $N(21, 1, 3)$ is obtained. The results have been obtained using the author's computer programs *Gen12SIC* and *Gen13SIC* for the generation of $(N, T, 1, 2)$ and $(N, T, 1, 3)$ superimposed codes, respectively, and the program *Q-extension* [1] for code equivalence testing.

2. Preliminaries.

Theorem 3. (Sperner's theorem [9]) *Let X be a finite set of N elements and let $\mathscr{F}$ be a family of different subsets of X such that every pair of members F_1 and F_2 of $\mathscr{F}$ $(F_1 \neq F_2)$ satisfies $F_1 \not\subset F_2$. Then $|\mathscr{F}| \leq \binom{N}{\lfloor N/2 \rfloor}$.*

It follows from Sperner's theorem that the maximum size T for which an $(N, T, 1, 1)$ superimposed code exists for fixed value of N is $\binom{N}{\lfloor N/2 \rfloor}$.

Definition 4. *The residual code $Res(C, x = v)$ of a superimposed code C with respect to value v in column x is a code obtained by taking all the rows in which C has value v in column x and deleting the x^{th} entry in the selected rows.*

We denote by S_x the characteristic set of column x and by L_p the characteristic set of row p. The following two lemmas are obvious:

Lemma 5. *Let C be an (N, T, w, r) superimposed code and x be a column of C. Then $Res(C, x = 0)$ is an $(N - |S_x|, T - 1, w, r - 1)$ superimposed code.*

Lemma 6. *Let C be an (N, T, w, r) superimposed code and x be a column of C. The matrix $C' = C \backslash \{x\}$ is an $(N, T - 1, w, r)$ superimposed code.*

The following lemma is a relation between the weights of columns and those of rows. We refer to [5] for a proof.

Lemma 7. *Suppose C is an $(N, T, 1, r)$ superimposed code and x is a column such that $|S_x| \leq r$. Then there exists a row p for which $c_{px} = 1$ and $|L_p| = 1$.*

The next lemma gives a relation between $N(T, 1, r)$ and $N(T - 1, 1, r)$.

Lemma 8. $N(T - 1, 1, r) \leq N(T, 1, r) \leq N(T - 1, 1, r) + 1$.

Proof. From Lemma 6, it follows that $N(T - 1, 1, r) \leq N(T, 1, r)$. Let C be an $(N - 1, T - 1, 1, r)$ superimposed code. The following matrix is an

$(N, T, 1, r)$ SIC:

$$\left(\begin{array}{c|c} 0 & \\ \vdots & C \\ 0 & \\ \hline 1 & 0\,0\ldots0\,0 \end{array}\right)$$

Therefore $N(T, 1, r) \leq N(T-1, 1, r) + 1$. □

3. Generation of $(N, T, 1, 2)$ superimposed codes. Let C be an $(N, T, 1, 2)$ superimposed code and x be a column of C. We may assume that the rows and the columns of C are sorted lexicographically. According to Lemma 5 $Res(C, x = 0)$ is an $(N - |S_x|, T - 1, 1, 1)$ superimposed code. Using Sperner's theorem, we obtain the following bounds for $|S_x|$:

$N \times T$	9×10	9×11	9×12	9×13	10×13	10×14
$\lvert S_x \rvert \leq$	4	4	3	3	4	4

$N \times T$	11×14	11×15	11×16	11×17	11×18
$\lvert S_x \rvert \leq$	5	5	5	4	4

We construct the matrix C column by column, using the $(N, T, 1, 2)$ superimposed code generation program *Gen12SIC* and *Q-extension* for code equivalence testing. At each step we check the conditions of the sorted rows property, the sorted columns property and the superimposed code property.

For example we describe how all inequivalent $(11, 14, 1, 2)$ superimposed codes have been constructed.

Let C be an $(11, 14, 1, 2)$ superimposed code and x be a column of C.

First, using the program *Gen12SIC*, we found all possibilities for the first 4 columns, which form an $(11, 4, 1, 2)$ superimposed code. We obtain 22651 superimposed codes. Using *Q-extension* we find that there are exactly 3743 inequivalent superimposed codes among them. Then we extend each of these codes by appending one column to be an $(11, 5, 1, 2)$ SIC. Using *Q-extension* we find that there are over 40000 inequivalent possibilities for the first 5 columns. Similarly we make an extension to an $(11, 6, 1, 2)$ and $(11, 7, 1, 2)$ SIC respectively. Thus we find that there are exactly 1552910 possibilities for the first 7 columns of the $(11, 14, 1, 2)$ superimposed code. We extend each of these codes to an $(11, 14, 1, 2)$ SIC with the program *Gen12SIC*. Using *Q-extension* we obtain finally 2705 inequivalent $(11, 14, 1, 2)$ superimposed codes.

Using the method described, the following number of inequivalent superimposed codes have been obtained:

$N\times T$	9×10	9×11	9×12	9×13	10×13	10×14
#	4	1	1	0	5	0

$N\times T$	11×14	11×15	11×16	11×17	11×18
#	2705	278	21	2	0

These results prove the validity of the following theorem:

Theorem 9.

$$N(13,1,2)=10,\quad N(14,1,2)=11,\quad N(15,1,2)=11,$$
$$N(16,1,2)=11,\quad N(17,1,2)=11.$$

There is no $(11,18,1,2)$ *superimposed code.*

Using the program *Gen12SIC* and *Q-extension* we constructed all inequivalent $(12,18,1,2)$, $(12,19,1,2)$, $(12,20,1,2)$ and $(12,21,1,2)$ superimposed codes for which all the columns are of weight 3. We found the following number of inequivalent $(12,18,1,2)$, $(12,19,1,2)$, $(12,20,1,2)$ and $(12,21,1,2)$ superimposed codes for which all the columns are of weight 3:

$N\times T$	12×18	12×19	12×20	12×21
#	9805	511	5	0

Therefore:

Theorem 10.

$$N(18,1,2)=N(19,1,2)=N(20,1,2)=12.$$

4. Generation of $(N,T,1,3)$ superimposed codes. Let C be an $(N,T,1,3)$ superimposed code and x be a column of C. We may assume that the rows and the columns of C are sorted lexicographically. According to Lemma 5 $Res(C,x=0)$ is an $(N-|S_x|,T-1,1,2)$ superimposed code. Using the values of $N(T,1,2)$ and the superimposed code property, we obtain the following exact values and bounds for $|S_x|$:

$N\times T$	4×4	5×5	6×6	7×7	8×8	9×9	10×10
$\lvert S_x\rvert$	1	1	1	1	1	1	1

$N\times T$	11×11	12×12	13×13	14×14	15×15	16×16
$\lvert S_x\rvert \leq$	2	3	4	4	4	5

$N\times T$	16×17	16×18	16×19	16×20	16×21
$\lvert S_x\rvert \leq$	5	5	4	4	4

It is obvious that the identity matrix is the unique $(T, T, 1, 3)$ superimposed code for $4 \leq T \leq 10$.

For $T = 11$ and $T = 12$ we construct the matrix C column by column, using the $(N, T, 1, 3)$ superimposed code generation program *Gen13SIC* and *Q-extension* for code equivalence testing. At each step we check the conditions of the sorted rows property, the sorted columns property and the superimposed code property.

For $13 \leq T \leq 15$ we consider the following two cases:

Case 1: All columns of C are of weight 4.

In this case we construct C using the programs *Gen13SIC* and *Q-extension.*

Case 2: There exists a column x for which $1 \leq |S_x| \leq 3$.

According to Lemma 7 there exists a row p of C for which $c_{px} = 1$ and $|L_p| = 1$. We can write C as follows, where x is the first column of C:

$$\left(\begin{array}{c|c} c_{11} & \\ \vdots & A \\ c_{N-1,1} & \\ \hline 1 & 0\,0\ldots0\,0 \end{array}\right)$$

The matrix A is an $(N-1, T-1, 1, 3)$ superimposed code. Using the classification of $(12, 12, 1, 3)$, $(13, 13, 1, 3)$ and $(14, 14, 1, 3)$ SIC respectively, we construct the whole matrix C.

For $T = 16$ we consider the following three cases:

Case 1: All columns of C are of weight 4.

In this case we construct C using the programs *Gen13SIC* and *Q-extension.*

Case 2: There exists a column x of C for which $|S_x| = 5$. We can write

C as follows, where x is the first column of C:

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

The matrix A is an $(11, 15, 1, 2)$ superimposed code. Using the classification of $(11, 15, 1, 2)$ SIC we tried to construct the whole matrix C, but we found that for each of the 278 possibilities for A the extension is impossible.

Case 3: There exists a column x for which $1 \leq |S_x| \leq 3$.

According to Lemma 7 there exists a row p of C for which $c_{px} = 1$ and $|L_p| = 1$. We can write C as follows, where x is the first column of C:

$$\left(\begin{array}{c|c} c_{11} & \\ \vdots & A \\ c_{N-1,1} & \\ \hline 1 & 0\,0\ldots0\,0 \end{array}\right)$$

The matrix A is an $(15, 15, 1, 3)$ superimposed code. Using the classification of $(15, 15, 1, 3)$ SIC we construct the whole matrix C.

For $17 \leq T \leq 20$ we extend each of the inequivalent $(16, 16, 1, 3)$, $(16, 17, 1, 3)$, $(16, 18, 1, 3)$ and $(16, 19, 1, 3)$ superimposed codes by appending one column to be $(16, 17, 1, 3)$, $(16, 18, 1, 3)$, $(16, 19, 1, 3)$ and $(16, 20, 1, 3)$ SIC, respectively.

The number of nonequivalent classes of optimal $(N(T, 1, 3), T, 1, 3)$ superimposed codes for $T \leq 20$ is presented in the following tables:

$N\times T$	4×4	5×5	6×6	7×7	8×8	9×9	10×10	11×11	12×12
#	1	1	1	1	1	1	1	1	1

$N\times T$	13×13	14×14	15×15	16×16	16×17	16×18	16×19	16×20
#	2	4	12	432	9	2	1	1

We tried to extend the unique $(16, 20, 1, 3)$ SIC by appending one column to be a $(16, 21, 1, 3)$ SIC. We found out that there is no $(16, 21, 1, 3)$ SIC. Using Lemma 8 we prove the following theorem:

Theorem 11. $N(21, 1, 3) = 17$.

Acknowledgement. I would like to thank the referees for their remarks, which helped for the improvement of the paper.

REFERENCES

[1] Bouyukliev I. What is Q-extension? *Serdica J. Computing*, **1**, No 2 (2007), 115–130.

[2] Engel K. Interval packing and covering in the Boolean lattice. *Combinatorics Prob. and Computing*, **5** (1996), 373–384.

[3] Kapralov S., M. Manev. The nonexistence of (19,10,2,2) superimposed codes. In: Proceedings of Fourth International Workshop on Optimal Codes and Related Topics, Pamporovo, Bulgaria, June 17–23, 2005, 196–200.

[4] Kautz W., R. Singleton. Nonrandom binary superimposed codes. *IEEE Trans. Inform. Theory*, **10** (1964), 363–377.

[5] Kim H., V. Lebedev. On optimal superimposed codes. *J. Combin. Designs*, **12** (2004), 79–91.

[6] Kim H., V. Lebedev, D. Oh. Some new results on superimposed codes. *J. Combin. Designs*, **13** (2005), 276–285.

[7] Mitchell C., F. Piper. Key storage in secure network. *Discrete Applied Mathematics*, **21** (1988), 215–228.

[8] Oh D. A classification of the structure of some Sperner families and superimposed codes. *Discrete Mathematics*, **306** (2006), 1722–1731.

[9] Sperner E. Ein Satz über Untermengen einer endlichen Menge. *Mathematische Zeitschrift*, **27** (1928), 544–548.

Mladen Manev
Department of Mathematics
Technical University of Gabrovo
5300 Gabrovo, Bulgaria
e-mail: `ml.manev@gmail.com`

Received November 2, 2008
Final Accepted February 18, 2009