Optimality of the trivial (28,8,2,3) superimposed code

Mladen Manev
Department of Mathematics
Technical University of Gabrovo,
Gabrovo, Bulgaria

Introduction

Definition 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* $W, R \subset \{1, 2, \ldots, T\}$ *such that* $|W| = w$, $|R| = r$ *and* $W \cap R = \emptyset$ *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* $j \in R$*. We say also that* C *is a* (w, r) *superimposed code of length* N *and size* T*.*

Trivial (N, T, w, r) superimposed code

Introduction

Trivial (N, T, w, r) superimposed code

$$N = \binom{T}{w}$$

Introduction

Trivial (N, T, w, r) superimposed code

$$N = \binom{T}{w}$$

The rows are all possible binary vectors of weight w.

Example: The trivial $(15, 6, 2, 3)$ SIC

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

Introduction

$N(T, w, r)$ – the minimum length of an (N, T, w, r) superimposed code for given values of T, w and r.

$N(T, w, r)$ – the minimum length of an (N, T, w, r) superimposed code for given values of T, w and r.

The code is called optimal when $N = N(T, w, r)$.

Introduction

$N(T, w, r)$ – the minimum length of an (N, T, w, r) superimposed code for given values of T, w and r.

The code is called optimal when $N = N(T, w, r)$.

T	5	6	7	8	9	10
$N(T, 2, 3)$	10	15	21	$26 - 28$	$28 - 30$	30

Introduction

The first open case: $T = 8$

The first open case: $T = 8$

H. K. Kim, V. Lebedev, 2004: $24 \leqq N(8, 2, 3) \leqq 28$

Introduction

The first open case: $T = 8$

H. K. Kim, V. Lebedev, 2004: $24 \leqq N(8,2,3) \leqq 28$

S. Kapralov, M. Manev, 2006: $26 \leqq N(8,2,3) \leqq 28$

Introduction

The first open case: $T = 8$

H. K. Kim, V. Lebedev, 2004: $24 \leqq N(8, 2, 3) \leqq 28$

S. Kapralov, M. Manev, 2006: $26 \leqq N(8, 2, 3) \leqq 28$

In this paper: $N(8, 2, 3) = 28$

The first open case: $T = 8$

H. K. Kim, V. Lebedev, 2004: $24 \leqq N(8, 2, 3) \leqq 28$

S. Kapralov, M. Manev, 2006: $26 \leqq N(8, 2, 3) \leqq 28$

In this paper: $N(8, 2, 3) = 28$

The trivial $(28, 8, 2, 3)$ SIC is optimal.

Preliminaries

Definition 2 *Two* (N, T, w, r) *superimposed codes are equivalent if one of them can be transformed into the other by a series of operations of the following two types:*

Preliminaries

Definition 2 *Two* (N, T, w, r) *superimposed codes are equivalent if one of them can be transformed into the other by a series of operations of the following two types:*

- *permutation of the rows;*

Definition 2 *Two* (N, T, w, r) *superimposed codes are equivalent if one of them can be transformed into the other by a series of operations of the following two types:*

- *permutation of the rows;*
- *permutation of the columns.*

Preliminaries

Let C be a binary $N \times T$ matrix.

Preliminaries

Let C be a binary $N \times T$ matrix.

$d(x, y)$ – the Hamming distance between two columns x and y

Preliminaries

Let C be a binary $N \times T$ matrix.

$d(x, y)$ – the Hamming distance between two columns x and y

$d(x, y, z) = d(x, y) + d(x, z) + d(y, z)$

Preliminaries

Let C be a binary $N \times T$ matrix.

$d(x, y)$ – the Hamming distance between two columns x and y

$d(x, y, z) = d(x, y) + d(x, z) + d(y, z)$

$d(C) = \sum_{x,y \in C,\ x \neq y} d(x, y)$

Preliminaries

Let C be a binary $N \times T$ matrix.

$d(x, y)$ – the Hamming distance between two columns x and y

$d(x, y, z) = d(x, y) + d(x, z) + d(y, z)$

$d(C) = \sum_{x,y \in C,\ x \neq y} d(x, y)$

$d_2 = \min\{d(x, y) \mid x, y \in C,\ x \neq y\}$

Preliminaries

Let C be a binary $N \times T$ matrix.

$d(x, y)$ – the Hamming distance between two columns x and y

$d(x, y, z) = d(x, y) + d(x, z) + d(y, z)$

$d(C) = \sum_{x,y \in C,\ x \neq y} d(x, y)$

$d_2 = \min\{d(x, y) \mid x, y \in C,\ x \neq y\}$

$d_3 = \min\{d(x, y, z) \mid x, y, z \in C,\ x \neq y, x \neq z, y \neq z\}$

Preliminaries

Let C be a binary $N \times T$ matrix.

$d(x, y)$ – the Hamming distance between two columns x and y

$d(x, y, z) = d(x, y) + d(x, z) + d(y, z)$

$d(C) = \sum_{x,y \in C,\ x \neq y} d(x, y)$

$d_2 = \min\{d(x, y) \mid x, y \in C,\ x \neq y\}$

$d_3 = \min\{d(x, y, z) \mid x, y, z \in C,\ x \neq y, x \neq z, y \neq z\}$

$d(x, y, z)$ and d_3 are even numbers.

Preliminaries

Let C be a binary $N \times T$ matrix.

$d(x, y)$ – the Hamming distance between two columns x and y

$d(x, y, z) = d(x, y) + d(x, z) + d(y, z)$

$d(C) = \sum_{x,y \in C,\ x \neq y} d(x, y)$

$d_2 = \min\{d(x, y) \mid x, y \in C,\ x \neq y\}$

$d_3 = \min\{d(x, y, z) \mid x, y, z \in C,\ x \neq y, x \neq z, y \neq z\}$

$d(x, y, z)$ and d_3 are even numbers.

$3d_2 \leq d_3$

Lemma 4 *(Plotkin bound)*

$$\binom{T}{2} d_2 \leq d(C) \leq N \left\lfloor \frac{T}{2} \right\rfloor \left\lfloor \frac{T+1}{2} \right\rfloor .$$

Lemma 4 *(Plotkin bound)*

$$\binom{T}{2} d_2 \leq d(C) \leq N \left\lfloor \frac{T}{2} \right\rfloor \left\lfloor \frac{T+1}{2} \right\rfloor .$$

Corollary 5

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

Preliminaries

Definition 6 *Let* $x_1, x_2, ..., x_k$ *be different columns of the SIC* C. *The residual code* $Res(C, x_1 = v_1, x_2 = v_2, ..., x_k = v_k)$ *of* C *is the code obtained by taking all the rows in which* C *has value* v_i *in the column* x_i *for* $i = 1, 2, ..., k$ *and deleting the columns* $x_1, x_2, ..., x_k$ *in the selected rows.*

Preliminaries

Lemma 10 *(Kapralov, Manev, 2006)*
Any $(7, 6, 1, 2)$ *superimposed code is equivalent to one of the codes*

$$C_{1,2,\ldots,7} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ * & * & * & * & * & * \end{pmatrix} \quad C_8 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

The last row of $C_{1,2,\ldots,7}$ *is* 0000000, 0000001, 0000011, 0000111, 0001111, 0011111, 0111111 *or* 1111111 *respectively.*

The nonexistence of (27,8,2,3) SIC

Lemma 13 *Let C be a $(27, 8, 2, 3)$ superimposed code and x and y are two different columns of C. Then $Res(C, x = 0, y = 1)$ contains at most 5 rows of weight 0 or 1.*

The nonexistence of (27,8,2,3) SIC

Lemma 14 *Let C be a $(27, 8, 2, 3)$ superimposed code. Then $d_2 = 14$.*

Lemma 14 *Let C be a $(27, 8, 2, 3)$ superimposed code. Then $d_2 = 14$.*

Proof

The nonexistence of (27,8,2,3) SIC

Lemma 14 *Let C be a* $(27, 8, 2, 3)$ *superimposed code. Then* $d_2 = 14$.

Proof

x and y – columns of C at distance d_2

Lemma 14 *Let C be a* $(27, 8, 2, 3)$ *superimposed code. Then* $d_2 = 14$*.*

Proof

x and y – columns of C at distance d_2

Lemma 13 $\Rightarrow d_2 \geqq 14$

Lemma 14 *Let C be a $(27, 8, 2, 3)$ superimposed code. Then $d_2 = 14$.*

Proof

x and y – columns of C at distance d_2

Lemma 13 $\Rightarrow d_2 \geqq 14$

Lemma 4 $\Rightarrow d_2 \leqq 15$

Lemma 14 *Let C be a $(27, 8, 2, 3)$ superimposed code. Then $d_2 = 14$.*

Proof

x and y – columns of C at distance d_2

Lemma 13 $\Rightarrow d_2 \geqq 14$

Lemma 4 $\Rightarrow d_2 \leqq 15$

$Res(C, x = 0, y = 1)$ or $Res(C, x = 1, y = 0)$ is equivalent to the code

$$C_8 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Lemma 14 *Let C be a $(27, 8, 2, 3)$ superimposed code. Then $d_2 = 14$.*

Proof

x and y – columns of C at distance d_2

Lemma 13 $\Rightarrow d_2 \geqq 14$

Lemma 4 $\Rightarrow d_2 \leqq 15$

$Res(C, x = 0, y = 1)$ or $Res(C, x = 1, y = 0)$ is equivalent to the code

$$C_8 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$\Rightarrow d(C) \leqq 429$

Lemma 14 *Let C be a* $(27, 8, 2, 3)$ *superimposed code. Then* $d_2 = 14$*.*

Proof

x and y – columns of C at distance d_2

Lemma 13 $\Rightarrow d_2 \geqq 14$

Lemma 4 $\Rightarrow d_2 \leqq 15$

$Res(C, x = 0, y = 1)$ or $Res(C, x = 1, y = 0)$ is equivalent to the code

$$C_8 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$\Rightarrow d(C) \leqq 429$

Corollary 5 $\Rightarrow d_3 \leqq 45\frac{27}{28}$

Lemma 14 *Let C be a* $(27, 8, 2, 3)$ *superimposed code. Then* $d_2 = 14$*.*

Proof

x and y – columns of C at distance d_2

Lemma 13 $\Rightarrow d_2 \geqq 14$

Lemma 4 $\Rightarrow d_2 \leqq 15$

$Res(C, x = 0, y = 1)$ or $Res(C, x = 1, y = 0)$ is equivalent to the code

$$C_8 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$\Rightarrow d(C) \leqq 429$

Corollary 5 $\Rightarrow d_3 \leqq 45\frac{27}{28}$

d_3 is an even number $\Rightarrow d_3 \leqq 44$

Lemma 14 *Let C be a* $(27, 8, 2, 3)$ *superimposed code. Then* $d_2 = 14$.

Proof

x and y – columns of C at distance d_2

Lemma 13 $\Rightarrow d_2 \geqq 14$

Lemma 4 $\Rightarrow d_2 \leqq 15$

$Res(C, x = 0, y = 1)$ or $Res(C, x = 1, y = 0)$ is equivalent to the code

$$C_8 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$\Rightarrow d(C) \leqq 429$

Corollary 5 $\Rightarrow d_3 \leqq 45\frac{27}{28}$

d_3 is an even number $\Rightarrow d_3 \leqq 44 \Rightarrow d_2 = 14$

The nonexistence of (27,8,2,3) SIC

Theorem 15 *There is no* $(27, 8, 2, 3)$ *superimposed code.*

The nonexistence of (27,8,2,3) SIC

Theorem 15 *There is no* $(27, 8, 2, 3)$ *superimposed code.*

Proof

The nonexistence of (27,8,2,3) SIC

Theorem 15 *There is no* $(27, 8, 2, 3)$ *superimposed code.*

Proof

Let C be a (27,8,2,3) superimposed code.

The nonexistence of (27,8,2,3) SIC

Theorem 15 *There is no* $(27, 8, 2, 3)$ *superimposed code.*

Proof

Let C be a (27,8,2,3) superimposed code.

Lemma 14 $\Rightarrow$ there exist two columns x and y such that $d(x, y) = 14$.

Theorem 15 *There is no* $(27,8,2,3)$ *superimposed code.*

Proof

Let C be a (27,8,2,3) superimposed code.

Lemma 14 $\Rightarrow$ there exist two columns x and y such that $d(x,y) = 14$.

Lemma 10 and Lemma 13 $\Rightarrow$ $Res(C, x = 0, y = 1)$ and $Res(C, y = 0, x = 1)$ are equivalent to the code

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

The nonexistence of (27,8,2,3) SIC

x	y	
0	1	
⋮	⋮	$(7, 6, 1, 2)$ SIC
0	1	
1	0	
⋮	⋮	$(7, 6, 1, 2)$ SIC
1	0	
0	0	
⋮	⋮	M rows
0	0	
1	1	
⋮	⋮	$13 - M$ rows
1	1	

The nonexistence of (27,8,2,3) SIC

x y	
0 1 ⋮ ⋮ 0 1	$(7,6,1,2)$ SIC
1 0 ⋮ ⋮ 1 0	$(7,6,1,2)$ SIC
0 0 ⋮ ⋮ 0 0	M rows
1 1 ⋮ ⋮ 1 1	$13-M$ rows

30 inequivalent possibilities for the first 14 rows of C

The nonexistence of (27,8,2,3) SIC

x y	
0 1 ⋮ ⋮ 0 1	$(7,6,1,2)$ SIC
1 0 ⋮ ⋮ 1 0	$(7,6,1,2)$ SIC
0 0 ⋮ ⋮ 0 0	M rows
1 1 ⋮ ⋮ 1 1	$13 - M$ rows

30 inequivalent possibilities for the first 14 rows of C

$$7 \leqq M \leqq 12$$

The nonexistence of (27,8,2,3) SIC

We construct the missing parts column by column and at each step we check the conditions of:

The nonexistence of (27,8,2,3) SIC

We construct the missing parts column by column and at each step we check the conditions of:

- Lemma 14;

The nonexistence of (27,8,2,3) SIC

We construct the missing parts column by column and at each step we check the conditions of:

- Lemma 14;
- the superimposed code property;

The nonexistence of (27,8,2,3) SIC

We construct the missing parts column by column and at each step we check the conditions of:

- Lemma 14;
- the superimposed code property;
- the sorted last 13 rows property.

The nonexistence of (27,8,2,3) SIC

We construct the missing parts column by column and at each step we check the conditions of:

- Lemma 14;
- the superimposed code property;
- the sorted last 13 rows property.

It turned out that the extension to a $(27, 8, 2, 3)$ superimposed code is impossible.

The nonexistence of (27,8,2,3) SIC

We construct the missing parts column by column and at each step we check the conditions of:

- Lemma 14;
- the superimposed code property;
- the sorted last 13 rows property.

It turned out that the extension to a $(27, 8, 2, 3)$ superimposed code is impossible.
Therefore there is no $(27, 8, 2, 3)$ superimposed code.

The nonexistence of (27,8,2,3) SIC

We construct the missing parts column by column and at each step we check the conditions of:

- Lemma 14;
- the superimposed code property;
- the sorted last 13 rows property.

It turned out that the extension to a $(27, 8, 2, 3)$ superimposed code is impossible.
Therefore there is no $(27, 8, 2, 3)$ superimposed code.

Theorem 16 *The trivial $(28, 8, 2, 3)$ superimposed code is optimal.*