Cover-Free Codes and Separating System Codes

A. G. D'yachkov, I.V. Vorobyev, N.A. Polyanskii and V.Yu. Shchukin
Lomonosov Moscow State University, Moscow, Russia
Email: agd-msu@yandex.ru, vorobyev.i.v@yandex.ru, nikitapolyansky@gmail.com, vpike@mail.ru

***Abstract*—We discover some important properties of cover-free (CF) codes, separating system (SS) codes and completely separating system (CSS) codes connected with the concept of constant weight CF codes. New upper and lower bounds on the rate of CF and SS codes based on the known results for CF and CSS codes are obtained. Tables of numerical values for the improved upper and lower bounds are presented.**

Keywords: Cover-free (CF) codes, separating system codes, completely separating system codes, fixed relative weight CF codes, bounds on the rate

I. Notations, Definitions and Results

Let N, t, s and L be integers, $1 \leqslant s < t$, $1 \leqslant L \leqslant t-s$, the symbol $\triangleq$ denotes equality by definition, $|A|$ – cardinality of the set A, and $[N] \triangleq \{1, 2, \ldots, N\}$ – the set of integers from 1 to N. The standard symbol $\lfloor a \rfloor$ ($\lceil a \rceil$) will be used to denote the largest (least) integer $\leqslant a$ ($\geqslant a$). Introduce a binary matrix $X \triangleq \|x_i(j)\|$, $x_i(j) = 0, 1$ with t columns (codewords) $\boldsymbol{x}(j) \triangleq (x_1(j), \ldots, x_N(j))$, $j \in [t]$, and N rows $\boldsymbol{x}_i \triangleq (x_i(1), \ldots, x_i(t))$, $i \in [N]$. Any such matrix is called a binary *code* X of *length* N and *size* t. The number of ones in column $\boldsymbol{x}(j)$, i.e., $|\boldsymbol{x}(j)| \triangleq \sum_{i=1}^{N} x_i(j)$, is called the *weight* of $\boldsymbol{x}(j)$, $j \in [t]$. Let Q, $0 < Q < 1$, be a fixed parameter. A code X of length N and size t is said to be the *constant weight* code of the *relative* weight Q if the weight $|\boldsymbol{x}(j)| \triangleq \lceil Q\,N \rceil$ for any $j \in [t]$.

A. Cover-Free and Separating Codes

Let $s \geqslant 1$ and $\ell \geqslant 1$ be positive integers such that $s+\ell \leqslant t$.

Definition 1.[1],[2]. A code X is called a *cover-free* (CF) (s, ℓ)*-code*, if for any two disjoint sets $\mathcal{S}$, $\mathcal{L} \subset [t]$, $|\mathcal{S}| = s$, $|\mathcal{L}| = \ell$, $\mathcal{S} \cap \mathcal{L} = \varnothing$, there exists a row $\boldsymbol{x}_i$, $i \in [N]$, such that

$$x_i(j) = 0 \quad \text{for } \forall\, j \in \mathcal{S}, \quad \text{and} \quad x_i(k) = 1 \quad \text{for } \forall\, k \in \mathcal{L}.$$

Taking into account the obvious symmetry over the parameters s and ℓ, we denote by $t_{cf}(N, s, \ell) = t_{cf}(N, \ell, s)$ the maximal size of CF (s, ℓ)-codes of length N, and by $N_{cf}(t, s, \ell) = N_{cf}(t, \ell, s)$, the minimal length of CF (s, ℓ)-codes of size t. Introduce the *rate* of CF (s, ℓ)-codes:

$$R_{cf}(s, \ell) = R_{cf}(\ell, s) \triangleq \overline{\lim_{N\to\infty}} \frac{\log_2 t_{cf}(N, s, \ell)}{N}$$

The best presently known upper and lower bounds on the rate $R_{cf}(s, \ell)$ of CF (s, ℓ)-codes were established in [4], [5]. If $\ell \geqslant 1$ is fixed and $s \to \infty$, then these bounds have the following asymptotic form:

$$R_{cf}(s, \ell) \geqslant \frac{(\ell+1)^{\ell+1}}{e^{\ell+1}} \frac{\log_2 s}{s^{\ell+1}} (1 + o(1)), \tag{1}$$

$$R_{cf}(s, \ell) \leqslant \frac{(\ell+1)^{\ell+1}}{2e^{\ell-1}} \frac{\log_2 s}{s^{\ell+1}} (1 + o(1)). \tag{2}$$

Definition 2.[6]. A code X is called a *separating system* (s, ℓ)*-code* or, briefly, SS (s, ℓ)*-code*, if for any two disjoint sets $\mathcal{S}$, $\mathcal{L} \subset [t]$, $|\mathcal{S}| = s$, $|\mathcal{L}| = \ell$, $\mathcal{S} \cap \mathcal{L} = \varnothing$, there exists a row $\boldsymbol{x}_i$, $i \in [N]$, such that

$$x_i(j) = 0 \quad \text{for } \forall\, j \in \mathcal{S}, \quad \text{and} \quad x_i(k) = 1 \quad \text{for } \forall\, k \in \mathcal{L},$$

or

$$x_i(j) = 1 \quad \text{for } \forall\, j \in \mathcal{S}, \quad \text{and} \quad x_i(k) = 0 \quad \text{for } \forall\, k \in \mathcal{L}.$$

Taking into account the evident symmetry over the parameters s and ℓ, denote by $t_{ss}(N, s, \ell) = t_{ss}(N, \ell, s)$ the maximum possible size of SS (s, ℓ)-codes of length N and denote by $N_{ss}(t, s, \ell) = N_{ss}(t, \ell, s)$ the minimum possible length of SS (s, ℓ)-code of size t. Introduce the *rate* of SS (s, ℓ)-codes:

$$R_{ss}(s, \ell) = R_{ss}(\ell, s) \triangleq \overline{\lim_{N\to\infty}} \frac{\log_2 t_{ss}(N, s, \ell)}{N} \tag{3}$$

Definition 3.[7]. Code X is called a *completely separating system* (s, ℓ)*-code* or, briefly, CSS (s, ℓ)*-code*, if for any two disjoint sets $\mathcal{S}$, $\mathcal{L} \subset [t]$, $|\mathcal{S}| = s$, $|\mathcal{L}| = \ell$, $\mathcal{S} \cap \mathcal{L} = \varnothing$, there exist two rows $\boldsymbol{x}_i$, $\boldsymbol{x}_j$, $i, j \in [N]$, such that

$$x_i(m) = 0 \quad \text{for } \forall\, m \in \mathcal{S}, \quad \text{and} \quad x_i(k) = 1 \quad \text{for } \forall\, k \in \mathcal{L},$$

and

$$x_j(m) = 1 \quad \text{for } \forall\, m \in \mathcal{S}, \quad \text{and} \quad x_j(k) = 0 \quad \text{for } \forall\, k \in \mathcal{L}.$$

Given the symmetry over s and ℓ, denote by $t_{css}(N, s, \ell) = t_{css}(N, \ell, s)$ the maximum size of CSS (s, ℓ)-codes of length N, and by $N_{css}(t, s, \ell) = N_{css}(t, \ell, s)$, the minimum length of CSS (s, ℓ) codes of size t. Introduce the *rate* of CSS (s, ℓ)-codes:

$$R_{css}(s, \ell) = R_{css}(\ell, s) \triangleq \overline{\lim_{N\to\infty}} \frac{\log_2 t_{css}(N, s, \ell)}{N} \tag{4}$$

Bounds on the rates (3)-(4) along with constructions of SS (s, ℓ)-codes and CSS (s, ℓ)-codes have been investigated in many papers. See, overviews [8], [9]. Note the evident

Proposition 1. [8], [9]. (Monotonicity properties). *For any $s \geqslant 1$ and $\ell \geqslant 1$, the rate $R_{cf}(s, s) = R_{css}(s, s)$ and the inequalities*

$$R_{ss}(s, l)/2 \leqslant R_{css}(s, l) \leqslant R_{cf}(s, l) \leqslant R_{ss}(s, l) \tag{5}$$

hold.

In Definitions 1-3, we follow the notations used in the survey [9]. The aim of our paper is presented in the Abstract.

B. Applications of Separating Codes

The most important applications of separating codes are connected with the automata synthesis (see [8],[10]), digital fingerprinting (see [11]-[13]), and constructions of hash functions [14].

C. Constant Weight CF (s,ℓ)-codes

Denote by $t_{cf}^{Q}(N,s,\ell) = t_{cf}^{1-Q}(N,\ell,s)$ the maximum possible size of constant weight CF (s,ℓ)-codes of length N and the relative weight Q. Denote by $N_{cf}^{Q}(t,s,\ell) = N_{cf}^{1-Q}(t,\ell,s)$ the minimum possible length of constant weight CF (s,ℓ)-codes of size t and the relative weight Q. Introduce the concept of *Q-rate* of CF (s,ℓ)-codes:

$$R_{cf}^{Q}(s,\ell) = R_{cf}^{Q}(\ell,s) \triangleq \overline{\lim_{N\to\infty}} \frac{\log_2 t_{cf}^{Q}(N,s,\ell)}{N} \qquad (6)$$

Proposition 2. *The Q-rate of CF (s,ℓ)-codes $R_{cf}^{Q}(s,\ell)$ and the rate $R_{cf}(s,\ell)$ of CF (s,ℓ)-codes satisfy the inequalities*:

$$R_{cf}^{Q}(s+1,\ell) \leqslant (1-Q)\cdot R_{cf}(s,\ell),$$
$$R_{cf}^{Q}(s,\ell+1) \leqslant Q\cdot R_{cf}(s,\ell). \qquad (7)$$

Proof. Consider an arbitrary constant weight CF $(s+1,\ell)$-code X of length N, size t and the relative weight Q. Fix an arbitrary column $\boldsymbol{x}(j)$. Delete the column $\boldsymbol{x}(j)$ and all $\lceil Q\,N\rceil$ rows having ones in $\boldsymbol{x}(j)$. It's easy to see that the obtained code X' is a CF (s,ℓ)-code of size $t-1$ and length $\leqslant (1-Q)N$. This yields

$$N_{cf}^{Q}(t,s+1,\ell)\cdot(1-Q) \geqslant N_{cf}(t-1,s,\ell).$$

Therefore, the rate definitions (3) and (6) lead to the first inequality in (7). The second inequality in (7) is established in the similar way. $\square$

Proposition 3. *The rate of SS (s,ℓ)-codes $R_{ss}(s,\ell)$ and the $1/2$-rate of CF (s,ℓ)-codes $R_{cf}^{1/2}(s,\ell)$ satisfy the inequality*

$$R_{ss}(s,\ell) \leqslant 2\cdot R_{cf}^{1/2}(s,\ell). \qquad (8)$$

Proof. Consider an arbitrary SS (s,ℓ)-code X of size t and length N. Construct the code $X' = (\boldsymbol{x}'(1),\boldsymbol{x}'(2),\ldots,\boldsymbol{x}'(t))$ of size t and length $2N$ as follows: $\boldsymbol{x}'(i) = \boldsymbol{x}(i)\&\overline{\boldsymbol{x}(i)}$, $i\in[t]$, where the symbol $\&$ denotes the concatenation of two vectors, and $\overline{\boldsymbol{x}(i)} \triangleq (\overline{x_1(i)},\overline{x_2(i)},\ldots,\overline{x_N(i)})$ denotes the opposite vector to $\boldsymbol{x}(i)$. One can easily see that the code X' is a constant weight CF (s,ℓ)-code of the relative weight $1/2$. Hence, the rate definitions (3) and (6) lead to (8). $\square$

Our new upper bounds on the rate of SS (s,ℓ)-codes are obtained with the help of the known upper bounds on the rate $R_{cf}(s,\ell)$ of CF (s,ℓ)-codes and the following

Theorem 1. *The rate $R_{ss}(s,\ell)$ of SS (s,ℓ)-codes and the rate $R_{cf}(s,\ell)$ of CF (s,ℓ)-codes satisfy inequalities*

$$R_{cf}(s,\ell) \leqslant R_{ss}(s,\ell) \leqslant R_{cf}(s-1,\ell), \quad \ell\geqslant 1,\ s\geqslant 2,$$
$$R_{cf}(s,\ell) \leqslant R_{ss}(s,\ell) \leqslant R_{cf}(s,\ell-1), \quad \ell\geqslant 2,\ s\geqslant 1. \qquad (9)$$

Proof of Theorem 1. The left-hand sides in (9) follow immediately from (5). To prove the right-hand sides of (9), we consequently apply (8) and (7) for $Q=1/2$. $\square$

In particular, Theorem 1 implies that the rate $R_{ss}(s,\ell)$ of SS (s,ℓ)-codes and the rate $R_{cf}(s,\ell)$ of CF (s,ℓ)-codes satisfy the same asymptotic inequalities (1)-(2).

D. Bounds of Theorem 1 for q-ary SS (s,ℓ)-codes

In this Sect., let $q\geqslant 2$ be a fixed integer and a code $X' \triangleq \|x_i'(j)\|$, $i\in[N]$, $j\in[t]$, $x_i'(j)\in[q]$ be a q-ary code of length N and size t. The following definition is the q-ary generalization of Definition 2.

Definition 2'. [6]. A q-ary code X' is called a *q-ary separating system (s,ℓ)-code* or, briefly, *q-ary* SS *(s,ℓ)-code*, if for any two disjoint sets $\mathcal{S},\mathcal{L}\subset[t]$, $|\mathcal{S}|=s$, $|\mathcal{L}|=\ell$, $\mathcal{S}\cap\mathcal{L}=\varnothing$, there exists an index $i\in[N]$, such that two q-ary coordinate sets

$$\{x_i'(j),\, j\in\mathcal{S}\}\subseteq[q] \quad\text{and}\quad \{x_i'(j),\, j\in\mathcal{L}\}\subseteq[q]$$

are disjoint as well, i.e., $\{x_i'(j),\, j\in\mathcal{S}\}\cap\{x_i'(j),\, j\in\mathcal{L}\}=\varnothing$. Taking into account the evident symmetry over the parameters s and ℓ, denote by $t_{ss}^{(q)}(N,s,\ell)=t_{ss}^{(q)}(N,\ell,s)$ the maximum possible size of q-ary SS (s,ℓ)-codes of length N. Introduce the *rate* of q-ary SS (s,ℓ)-codes:

$$R_{ss}^{(q)}(s,\ell) = R_{ss}^{(q)}(\ell,s) \triangleq \overline{\lim_{N\to\infty}} \frac{\log_q t_{ss}^{(q)}(N,s,\ell)}{N}. \qquad (10)$$

The q-ary extension of Theorem 1 is given by

Theorem 1'. *If $q\geqslant 3$, $s\geqslant\ell\geqslant 1$, $s\geqslant 2$, then the rate $R_{ss}^{(q)}(s,\ell)$ of SS (s,ℓ)-codes and the rate $R_{cf}(s,\ell)$ of binary CF (s,ℓ)-codes satisfy inequalities*

$$\frac{R_{cf}(s,\ell)}{\log_2 q} \leqslant R_{ss}^{(q)}(s,\ell) \leq \frac{C(\ell,q)\cdot R_{cf}(s-1,\ell)}{\log_2 q}, \qquad (11)$$

where

$$C(\ell,q) = \min\left(2^{q-1}-1, \sum_{k=1}^{\ell}\binom{q}{k}\right).$$

Theorem 1' and the asymptotic inequalities (1)-(2) imply that for any fixed q, $q\geqslant 3$, and any fixed ℓ, $\ell\geqslant 1$, the rate $R_{ss}^{(q)}(s,\ell)$ of q-ary SS (s,ℓ)-codes satisfies asymptotic $(s\to\infty)$ inequalities:

$$R_{ss}^{(q)}(s,\ell) \geqslant \frac{(\ell+1)^{\ell+1}}{e^{\ell+1}}\frac{\log_q s}{s^{\ell+1}}(1+o(1)), \qquad (12)$$

$$R_{ss}^{(q)}(s,\ell) \leqslant C(\ell,q)\frac{(\ell+1)^{\ell+1}}{2e^{\ell-1}}\frac{\log_q s}{s^{\ell+1}}(1+o(1)). \qquad (13)$$

Note that in the case $\ell=1$ and fixed $q\geqslant 3$, bounds (12)-(13) improve the previously known [9] lower and upper bounds on $R_{ss}^{(q)}(s,1)$ having orders $O(1/s^2)$ and $O(1/s)$, respectively.

Proof of Theorem 1'. Obviously, the maximum possible size $t_{ss}^{(q)}(N,s,\ell)$ of q-ary SS (s,ℓ)-codes of length N is the increasing function of the alphabet size $q\geqslant 2$. Therefore, the left-hand side of (11) immediately follows from the rate definition (10). To establish the right-hand side of (11), consider an arbitrary q-ary SS (s,ℓ)-code X' of size t and length N. For any superset $A=\{A_1,A_2,\dots,A_{|A|}\}$, $A_i\subset[q]$, introduce the $(0,1)$-binary $(N\cdot|A|)\times t$ matrix $X_A=X_A(X')$ obtained as follows. Each q-ary symbol x', $x'\in[q]$, in X' is replaced by the $(0,1)$-column of length $|A|$. This column has 1 at the i-th position if $x'\in A_i$ and 0, otherwise. Let D_1 be the set of all nonempty subsets of $[q]$ such that the cardinality of each subset $\leqslant\ell$ and D_2 be the set of all nonempty subsets of $[q]\backslash\{0\}$. One can easily check that the binary code X_{D_1} (X_{D_2}) is a binary SS (s,ℓ)-codes of size t and length $N\cdot\sum\limits_{k=1}^{\ell}\binom{q}{k}$ $\left(N\cdot\left[2^{q-1}-1\right]\right)$, hence the upper bound of Theorem 1 leads to the right-hand side of (11). $\square$

E. Recurrent Inequalities

The best known upper bounds [2]-[3] on the rate $R_{cf}(s,\ell)$ of CF (s,ℓ)-codes are based on the recurrent inequality [15]:

$$R_{cf}(s,\ell)\leqslant R_{cf}(s-u,\ell-v)\cdot\frac{u^u v^v}{(u+v)^{u+v}},$$
$$1\leqslant u\leqslant s-1,\quad 1\leqslant v\leqslant\ell-1. \tag{14}$$

and its improvement [16]:

$$R_{cf}(s,\ell)\leqslant\frac{R_{cf}(s-u,\ell-v)}{R_{cf}(s-u,\ell-v)+\frac{(u+v)^{u+v}}{u^u v^v}},$$
$$1\leqslant u\leqslant s-1,\quad 1\leqslant v\leqslant\ell-1. \tag{15}$$

The similar joint recurrent inequalities for the rates $R_{cf}(s,\ell)$, $R_{ss}(s,\ell)$ and $R_{css}(s,\ell)$ are formulated below in the form of Theorem 2 which will be established in Sect. II.

Theorem 2. 1) *For any* $u\in[s-1]$, $v\in[\ell-1]$, $u\neq v$,

$$R_{ss}(s,\ell)\leqslant R_{ss}(s-u,\ell-v)\cdot\max_{0\leqslant z\leqslant1}\{z^u(1-z)^v+(1-z)^u z^v\}. \tag{16}$$

2) *For any* $v\in[\ell-1]$,

$$R_{ss}(s,\ell)\leqslant R_{css}(s-v,\ell-v)\frac{1}{2^{2v-1}}. \tag{17}$$

3) *For any* $v\in[\ell-1]$ *and* $u=v+s-\ell$,

$$R_{ss}(s,\ell)\leqslant R_{css}(s-u,\ell-v)\cdot\max_{0\leqslant z\leqslant1}\{z^u(1-z)^v+(1-z)^u z^v\}. \tag{18}$$

4) *For any* $i\in[s-1]$,

$$R_{ss}(s,s)\leqslant\frac{R_{cf}(i,i)}{2^{2s-2i-1}}. \tag{19}$$

5) *For any* $v\in[\ell-1]$,

$$R_{cf}(s,\ell)\leqslant R_{css}(s-v,\ell-v)\frac{1}{2^{2v}}. \tag{20}$$

6) *For any* $v\in[\ell-1]$ *and* $u=v+s-\ell$,

$$R_{cf}(s,\ell)\leqslant R_{css}(s-u,\ell-v)\cdot\frac{u^u v^v}{(u+v)^{u+v}} \tag{21}$$

Note that the monotonicity inequality (5) and (21) imply a possibility to improve the recurrent inequalities (14)-(15). In Sect. I-F, we present detailed Tables of new upper bounds on the rates $R_{cf}(s,\ell)$, $R_{ss}(s,\ell)$ and $R_{css}(s,\ell)$ which follow from Theorems 1-2.

F. Tables of Upper Bounds

In Table I, we present the best known upper bounds [9] on the rate of CSS (s,ℓ)-codes. We use these values to improve upper bounds on the rates of CF (s,ℓ)-codes and SS (s,ℓ)-codes with the help of Theorem 2.

TABLE I
UPPER BOUNDS FOR COMPLETELY SEPARATING SYSTEM (s,ℓ)-CODES

s | ℓ	1	2	3	4	5
1	1	0.322	0.199	0.14	0.106
2	0.322	0.161	0.0662	0.0429	0.0286
3	0.199	0.0662	0.0353	0.0153	0.0101
4	0.14	0.0429	0.0153	0.00836	0.00370
5	0.106	0.0286	0.0101	0.00370	0.00204
6	0.083	0.0203	0.00669	0.00245	0.000911

In Table II, upper bounds on the rate of CF (s,ℓ)-codes are given.

TABLE II
UPPER BOUNDS FOR COVER-FREE (s,ℓ)-CODES

s | ℓ	1	2	3	4	5
1	1	0.322[1]	0.199[1]	0.14[1]	0.106[1]
2	0.322[1]	0.161[1]	0.0744[2]	0.0455[2]	0.0286[2]
3	0.199[1]	0.0744[2]	0.0353[3]	0.0165[4]	0.0107[4]
4	0.14[1]	0.0455[2]	0.0165[4]	0.00837[3]	0.00383[4]
5	0.106[1]	0.0286[2]	0.0107[4]	0.00383[4]	0.00204[3]
6	0.083[1]	0.0203[2]	0.00669[2]	0.00252[4]	0.000926[4]

[1] See [2]. [2] See [16]. [3] See [9]. [4] Claim 5 of Theorem 2.

In Table III, we provide new upper bounds for SS (s,ℓ)-code.

TABLE III
UPPER BOUNDS FOR SEPARATING SYSTEMS (s,ℓ)-CODES

s | ℓ	1	2	3	4	5
1	1	0.5[3]	0.322[1]	0.199[1]	0.14[1]
2	0.5[3]	0.283[3]	0.120[3]	0.0744[1]	0.0455[1]
3	0.322[1]	0.120[3]	0.0662[3]	0.0295[3]	0.0183[1]
4	0.199[1]	0.0744[1]	0.0295[3]	0.0163[3]	0.00728[3]
5	0.14[1]	0.0455[1]	0.0183[1]	0.00728[3]	0.00403[3]
6	0.106[1]	0.0286[1]	0.0109[1]	0.00441[2]	0.00181[3]

[1] Theorem 1. [2] Claim 3 of Theorem 2. [3] See [9].

Let us demonstrate how these values have been obtained. Consider, for instance, upper bound for SS $(4,6)$-code. Applying Claim 3 of Theorem 2 with $v=3$ and $u=1$, we obtain the following inequality

$$R_{ss}(4,6)\leqslant R_{css}(3,3)\max_{0\leqslant z\leqslant1}\{z(1-z)^3+(1-z)z^3\}.$$

The maximum value $\frac{1}{8}$ of $z(1-z)^3+(1-z)z^3$ is attained at $z=\frac{1}{2}$. Hence, the rate

$$R_{ss}(4,6)\leqslant\frac{R_{css}(3,3)}{8}\leqslant\frac{0.0353}{8}\approx0.00441.$$

It is clear that this bound is better than the previous one 0.00485634, computed by Theorem 5 in [9].

G. Tables of Lower Bounds

In Table IV, we remind the best known lower bounds on the rate of CF (s, ℓ)-codes [4], [5].

TABLE IV
LOWER BOUNDS FOR COVER-FREE (s, ℓ)-CODES

$s \mid \ell$	1	2	3	4	5
1	1	0.182	0.082	0.0566	0.042
2	0.182	0.0584	0.031	0.0185	0.012
3	0.082	0.031	0.00978	0.00553	0.00336
4	0.0566	0.0185	0.00553	0.00192	0.0011
5	0.042	0.012	0.00336	0.0011	0.000404
6	0.0325	0.00825	0.00215	0.000671	0.000234

With the help of these values and the inequality (5) we improve lower bounds for SS (s, ℓ)-codes, which are presented in Table V.

TABLE V
LOWER BOUNDS FOR SEPARATING SYSTEMS (s, ℓ)-CODES

$s \mid \ell$	1	2	3	4	5
1	1	0.2075^3	0.082^1	0.0566^1	0.042^1
2	0.2075^3	0.0642^2	0.031^1	0.0185^1	0.012^1
3	0.082^1	0.031^1	0.00978^1	0.00553^1	0.00336^1
4	0.0566^1	0.0185^1	0.00553^1	0.00192^1	0.0011^1
5	0.042^1	0.012^1	0.00336^1	0.0011^1	0.000404^1
6	0.0325^1	0.00825^1	0.00215^1	0.000671^1	0.000234^1

[1] See Theorem 1 and [5], [4]. [2] See [10]. [3] See [8], [17].

II. PROOF OF THEOREM 2

Denote by $\mathcal{P}_u(t)$ all u-subsets t-set, i.e.

$$\mathcal{P}_u(t) \triangleq \{P \subset [t] : \quad |P| = u\}.$$

Without loss of generality we suppose that $s \geqslant \ell$.

Proof of Claim 1. Let $\mathcal{U} \subset [t]$, $|\mathcal{U}| = u$, and $\mathcal{V} \subset [t]$, $|\mathcal{V}| = v$, $\mathcal{U} \cap \mathcal{V} = \varnothing$ be two disjoint subsets of t-set with cardinalities u and v respectively. Denote by X an arbitrary binary code of size t and length N. Define the set of rows $D_{u,v}(\mathcal{U}, \mathcal{V}, X) \subset [N]$, $0 \leqslant |D_{u,v}(\mathcal{U}, \mathcal{V}, X)| \leqslant N$, as the set of rows $\boldsymbol{x}_i$ of the code X such that one of the conditions

$$x_i(j) = 0 \text{ for any } j \in \mathcal{U} \quad \text{and} \quad x_i(k) = 1 \text{ for any } k \in \mathcal{V},$$

$$x_i(j) = 1 \text{ for any } j \in \mathcal{U} \quad \text{and} \quad x_i(k) = 0 \text{ for any } k \in \mathcal{V}$$

holds. Define the average number

$$\overline{D}_{u,v}(X) \triangleq \sum_{\substack{\mathcal{U} \in \mathcal{P}_u(t),\, \mathcal{V} \in \mathcal{P}_v(t), \\ \mathcal{U} \cap \mathcal{V} = \varnothing}} \frac{|D_{u,v}(\mathcal{U}, \mathcal{V}, X)|}{\binom{t}{u+v} \cdot \binom{u+v}{u}},$$

and

$$\overline{D}_{u,v}(t, N) = \max_X \overline{D}_{u,v}(X)$$

where the maximum is taken over all codes X of length N and size t.

Lemma 1. *The number $\overline{D}_{u,v}(t, N)$ satisfies the asymptotic inequality*

$$\varlimsup_{t \to \infty} \frac{\overline{D}_{u,v}(t, N)}{N} \leqslant \max_{0 \leqslant z \leqslant 1} \{z^u (1-z)^v + (1-z)^u z^v\}. \quad (22)$$

Proof of Lemma 1. Let $\mathcal{K} \subset [t]$, $|\mathcal{K}| = u + v$ and $i \in N$. Denote by $\boldsymbol{x}_i(K)$ the $1 \times (u+v)$ submatrix of X composed of elements of the i-th row and columns from the set $\mathcal{K}$. Define

$$I(X, \mathcal{K}, i) \triangleq \begin{cases} 1 & \text{if } \boldsymbol{x}_i(\mathcal{K}) \text{ contains either } u \text{ or } v \text{ zeroes}, \\ 0 & \text{otherwise.} \end{cases}$$

Denote by $M_{u,v}(X)$ the number of all possible $1 \times (u+v)$ submatrices of X with either u zeroes and v ones or v zeroes and u ones, i.e.

$$M_{u,v}(X) \triangleq \sum_{i \in N,\, \mathcal{K} \in \mathcal{P}_{u+v}(t)} I(X, \mathcal{K}, i).$$

Let a_i $(t - a_i\ )$ be equal to the number of zeroes (ones) in the i-th row of the code X. Then

$$M_{u,v}(X) = \sum_{i=1}^{N} \binom{a_i}{u} \cdot \binom{t - a_i}{v} + \sum_{i=1}^{N} \binom{a_i}{v} \cdot \binom{t - a_i}{u}.$$

On the other hand

$$M_{u,v}(X) = \overline{D}_{u,v}(X) \cdot \binom{t}{u+v} \binom{u+v}{u}.$$

These two equations lead to

$$\binom{t}{u+v} \binom{u+v}{u} \cdot \overline{D}_{u,v}(X) \leqslant$$

$$\leqslant N \cdot \max_{a \in [t]} \left\{ \binom{a}{u} \cdot \binom{t-a}{v} + \binom{a}{v} \cdot \binom{t-a}{u} \right\}.$$

If $t \to \infty$, then the passage to the limit yields (22). Lemma 1 is proved. $\square$

To complete the proof of Claim 1 we need

Lemma 2. *For any $u \in [s-1]$ and $v \in [\ell - 1]$, the minimum length of SS $(s-u, \ell-v)$-code of size t satisfies the inequality*

$$N_{ss}(t - (u+v), s-u, \ell-v) \leqslant \overline{D}_{u,v}(t, N). \quad (23)$$

Proof of Lemma 2. Let X be an arbitrary SS (s, ℓ)-code of size t and length N. Consider two disjoint sets $\mathcal{U} \subset [t]$, $|\mathcal{U}| = u$, $\mathcal{V} \subset [t]$, $|\mathcal{V}| = v$, $\mathcal{U} \cap \mathcal{V} = \varnothing$, such that $|D_{u,v}(\mathcal{U}, \mathcal{V}, X)| \geqslant \overline{D}_{u,v}(X)$. Obviously, we can find such sets, since the number $\overline{D}_{u,v}(X)$ is equal to the average value of $|D_{u,v}(\mathcal{U}, \mathcal{V}, X)|$ over all $\mathcal{U}$ and $\mathcal{V}$ by definition. Define the code X' of length $|D_{u,v}(\mathcal{U}, \mathcal{V}, X)|$ and size $t - (u+v)$ as the subcode of X composed of rows $D_{u,v}(\mathcal{U}, \mathcal{V}, X)$ and columns $[t] \setminus \{\mathcal{U} \cup \mathcal{V}\}$. Let us show that X' is an SS $(s-u, \ell-v)$-code. Indeed, fix any two sets $\mathcal{U}' \subset [t - (u+v)]$, $|\mathcal{U}'| = s - u$, and $\mathcal{V}' \subset [t - (u+v)]$, $|\mathcal{V}'| = \ell - v$, $\mathcal{U}' \cap \mathcal{V}' = \varnothing$. Then find the columns in X corresponding to $\mathcal{U}'$ and $\mathcal{V}'$. Denote these columns by $\hat{\mathcal{U}}'$ and $\hat{\mathcal{V}}'$ respectively. Note that these sets don't intersect $\mathcal{U}$ and $\mathcal{V}$ by construction of the code X'. Hence, for the SS (s,ℓ)-code X and sets $\hat{\mathcal{U}}'\cup\mathcal{U}$, $|\hat{\mathcal{U}}'\cup\mathcal{U}|=s$, and $\mathcal{V}\cup\hat{\mathcal{V}}'$, $|\mathcal{V}\cup\hat{\mathcal{V}}'|=\ell$, there exists a row $\boldsymbol{x}_i$ in X, such that either

$$x_i(j)=0 \text{ for } \forall\, j\in\hat{\mathcal{U}}'\cup\mathcal{U}, \text{ and } x_i(k)=1 \text{ for } \forall\, k\in\mathcal{V}\cup\hat{\mathcal{V}}',$$

$$x_i(j)=1 \text{ for } \forall\, j\in\hat{\mathcal{U}}'\cup\mathcal{U}, \text{ and } x_i(k)=0 \text{ for } \forall\, k\in\mathcal{V}\cup\hat{\mathcal{V}}'$$

holds. Note that this row belongs to the set $D_{u,v}(\mathcal{U},\mathcal{V},X)$. Therefore, the code X' is an SS $(s-u,\ell-v)$-code. Lemma 2 is proved. $\square$

For $N\triangleq N_{ss}(t,s,\ell)$, the inequality (23) of Lemma 2 can be written in the form:

$$\frac{N_{ss}(t-(u+v),s-u,\ell-v)}{N_{ss}(t,s,\ell)}\leqslant\frac{\overline{D}_{u,v}(t,N)}{N}, \qquad N=N_{ss}(t,s,\ell). \tag{24}$$

If $t\to\infty$, then in virtue of (22), the passage to the limit in (24) yields

$$\frac{R_{ss}(s,\ell)}{R_{ss}(s-u,\ell-v)}\leqslant$$

$$\leqslant\overline{\lim_{t\to\infty}}\,\frac{N_{ss}(t-(u+v),s-u,\ell-v)}{N_{ss}(t,s,\ell)}\leqslant$$

$$\leqslant\overline{\lim_{t\to\infty}}\,\frac{\overline{D}_{u,v}(t,N)}{N}\leqslant\max_{0\leqslant z\leqslant 1}\{z^u(1-z)^v+(1-z)^u z^v\}.$$

Claim 1 is proved completely. $\square$

Proof of Claim 2. The proof of Claim 2 is similar to the proof of Claim 1, but instead of Lemma 2 we need

Lemma 3. *For any $v\in[\ell-1]$ length of CSS $(s-v,\ell-v)$-code satisfies the inequality*

$$N_{css}(t-2v,s-v,\ell-v)\leqslant\overline{D}_{v,v}(t,N).$$

Proof of Lemma 3. Consider two sets $\mathcal{U}\subset[t]$, $|\mathcal{U}|=v$, and $\mathcal{V}\subset[t]$, $|\mathcal{V}|=v$, $\mathcal{U}\cap\mathcal{V}=\varnothing$, such that the inequality

$$|D_{v,v}(\mathcal{U},\mathcal{V},X)|\geqslant\overline{D}_{v,v}(X)$$

holds. Such two sets $\mathcal{U}$ and $\mathcal{V}$ do exist, since the value $\overline{D}_{v,v}(X)$ is equal to the average of $|D_{v,v}(\mathcal{U},\mathcal{V},X)|$ over all possible $\mathcal{U}$ and $\mathcal{V}$. Consider the subcode of X composed of columns corresponding to sets $\mathcal{U}$ and $\mathcal{V}$. Without loss of generality, we assume that each row from $D_{v,v}(\mathcal{U},\mathcal{V},X)$ has the following form

$$0\,0\ldots0\,1\,1\ldots1.$$

Define the code X' of length $|D_{v,v}(\mathcal{U},\mathcal{V},X)|$ and size $t-2v$ as the subcode of X composed of rows $D_{v,v}(\mathcal{U},\mathcal{V},X)$ and columns $[t]\setminus\{\mathcal{U}\cup\mathcal{V}\}$. Let us prove that X' is an CSS $(s-v,\ell-v)$-code. Indeed, fix any two sets $\mathcal{U}'\subset[t-2v]$, $|\mathcal{U}'|=s-v$, and $\mathcal{V}'\subset[t]$, $|\mathcal{V}'|=\ell-v$, $\mathcal{U}'\cap\mathcal{V}'=\varnothing$. Then find the columns in X corresponding to $\mathcal{U}'$ and $\mathcal{V}'$. Denote them by $\hat{\mathcal{U}}'$ and $\hat{\mathcal{V}}'$ respectively. These two sets don't intersect $\mathcal{U}$ and $\mathcal{V}$ by construction of X'. Hence for the SS (s,ℓ)-code X and sets $\hat{\mathcal{U}}'\cup\mathcal{U}$, $|\hat{\mathcal{U}}'\cup\mathcal{U}|=s$, and $\mathcal{V}\cup\hat{\mathcal{V}}'$, $|\mathcal{V}\cup\hat{\mathcal{V}}'|=\ell$, there exists a row $\boldsymbol{x}_i$ in X, such that

$$x_i(j)=0 \text{ for } \forall\, j\in\hat{\mathcal{U}}'\cup\mathcal{U}, \text{ and } x_i(k)=1 \text{ for } \forall\, k\in\mathcal{V}\cup\hat{\mathcal{V}}'.$$

For sets $\mathcal{U}\cup\hat{\mathcal{V}}'$ and $\mathcal{V}\cup\hat{\mathcal{U}}'$ we also can find such row. Note that these rows belong to $D_{v,v}(\mathcal{U},\mathcal{V},X)$. Therefore, the code X' is an CSS $(s-v,\ell-v)$-code.

Lemma 3 and Claim 2 are proved. $\square$

Proof of Claim 3. Taking into account the equality $s-u=l-v$, the proof of (18) is essentially the same as the proof of (17). $\square$

Proof of Claims 4-6. If we apply the second claim (17) to the particular case $v=s-i$, then the recurrent inequality (19) immediately follows from the evident property:

$$\max_{0\leqslant z\leqslant 1}\{z^v(1-z)^v\}=\frac{1}{2^{2s-2i}}.$$

The recurrent inequalities (20)-(21) can be easily obtained with the help of the same arguments that were used to establish the recurrent inequalities (17)-(18).

Theorem 2 is proved completely. $\square$

References

[1] Mitchell, C.J. and Piper, F.C., "Key Storage in Secure Networks", *Discrete Appl. Math.*, vol. 21, no. 3, pp. 215-228, 1988.

[2] D'yachkov A.G., Vilenkin P.A., Macula A.J., Torney D.C., "Families of Finite Sets in Which No Intersection of ℓ Sets Is Covered by the Union of s Others", *Journal of Combinatorial Theory*, Series A, vol. 99. pp. 195-218, 2002.

[3] D'yachkov A.G., Rykov V.V., Deppe C., Lebedev V.S. "Superimposed Codes and Threshold Group Testing", *Information Theory, Combinatorics, and Search Theory*, Lecture Notes in Computer Science, vol. 7777, pp. 509-533, 2013.

[4] D'yachkov A.G., Vorobyev I.V., Polyanskii N.A., Shchukin V.Yu., "Bounds on the Rate of Disjunctive Codes", *Problems of Information Transmission*, vol. 50, no. 1, pp. 27-56, 2014.

[5] D'yachkov A.G., Vorobyev I.V., Polyanskii N.A., Shchukin V.Yu., "Bounds on the Rate of Superimposed Codes", *2014 IEEE International Symposium on Information Theory*, pp. 2341-2345, Honolulu, HI USA, Jun.29-Jul.4, 2014.

[6] A. D. Friedman, R. L. Graham, and J. D. Ullman, "Universal single transition time asynchronous state assignments", *IEEE Trans. Comput.*, vol. 18, no. 6, pp. 541-547, 1969.

[7] Mago G. "Monotone Functions in Sequential Circuits", *IEEE Trans. Comput.*, v. 22, no. 10, pp. 928-933, 1973.

[8] Yu. L. Sagalovich, "Separating systems", *Problems of Information Transmission*, vol. 30, no. 2,pp. 105-123, 1994.

[9] G. D. Cohen and H. G. Schaathun, "Asymptotic overview on separating codes", *Tech. Report 248*, Department of Informatics, University of Bergen, Bergen, Norway, 2003.

[10] Yu. L. Sagalovich, "Completely Separating Systems", *Probl. Peredachi Inf.*, vol. 18, no. 2, pp. 74-82, 1982.

[11] Dan Boneh and James Shaw. "Collusion-secure fingerprinting for digital data", *IEEE Trans. Inform. Theory*, 44(5):1897-1905, 1998.

[12] J. N. Staddon, D. R. Stinson and R. Wei. "Combinatorial properties of frameproof and traceability codes", *IEEE Trans. Inform. Theory*, 47(3):1042-1049, 2001.

[13] A. Barg, G. R. Blakley, and G. A. Kabatiansky, Digital fingerprinting codes: Problem statements, constructions, identification of traitors, *IEEE Trans. Inf. Theory*, 49(4):852-865, 2003.

[14] D. R. Stinson, R. Wei, and K. Chen, On generalized separating hash families, *J. Combinat. Theory Ser. A*, vol. 115, no. 1, pp. 105-120, 2008.

[15] Engel, K., "Interval Packing and Covering in the Boolean Lattice", *Combin. Probab. Comput.*, vol. 5, no. 4, pp. 373-384, 1996.

[16] Lebedev, V.S., "Asymptotic Upper Bound for the Rate of (w, r) Cover-Free Codes", *Problems of Information Transmission*, vol. 39, no. 4, pp. 317-323, 2003.

[17] Gerard Cohen and Gilles Zemor, "Intersecting codes and independent families", *IEEE Trans. Inform. Theory*, 40:1872-1881, 1994.