Separable Codes for the Symmetric Multiple-Access Channel

Arkadii D'yachkov*, Nikita Polyanskii†,‡, Vladislav Shchukin†, Ilya Vorobyev§,¶
*Lomonosov Moscow State University, Moscow, Russia
†Institute for Information Transmission Problems, Moscow, Russia
‡Israel Institute of Technology, Haifa, Israel
§Skolkovo Institute of Science and Technology, Moscow, Russia
¶Moscow Institute of Physics and Technology, Moscow, Russia
agd-msu@yandex.ru, vorobyev.i.v@yandex.ru, nikitapolyansky@gmail.com, vpike@mail.ru

***Abstract*—A binary matrix is called an *s-separable code* for the *disjunctive multiple-access channel* (*$disj$-MAC*) if Boolean sums of sets of s columns are all distinct. The well-known issue of the combinatorial coding theory is to obtain upper and lower bounds on the rate of s-separable codes for the $disj$-MAC. In our paper, we generalize the problem and discuss upper and lower bounds on the rate of q-ary s-separable codes for models of noiseless *symmetric* MAC, i.e., at each time instant the output signal of MAC is a symmetric function of its s input signals.**

Keywords: Multiple-access channel (MAC), separable codes, random coding method, list-decoding.

I. Introduction

We study some combinatorial coding problems for the multiple access channel (MAC) that were motivated by two specific noiseless MAC models, corresponding to the transmission of q-ary symbols based on the frequency modulation method. Both models were suggested in the paper [1] and were called the s-user q-frequency MAC with (B–MAC) and without (A–MAC) intensity information. Using a well-known terminology [2] of the combinatorial coding theory, we describe the A–MAC coding problems along with the previously obtained results as follows.

Given arbitrary integers $2 \le s < t/2$, $q \ge 2$ and $N \ge 2$ introduce a code X consisting of t codewords of length N over a q-ary alphabet. The code X is called

- *s-separable* [2] code for the A–MAC if for any two distinct s-tuples of the codewords there exists a coordinate i, $1 \le i \le N$, in which *the union of s elements of the first s-tuple differs from the union of s elements of the second s-tuple*.
- *s-frameproof* code [2] if for any s-tuple of the codewords and every other codeword, there exists a coordinate i, $1 \le i \le N$, in which *the symbol of the other codeword doesn't belong to the union of s elements of the s-tuple*.
- *s-hash* code [3], [4] if $q \ge s$ and for every s-tuple of the codewords there exists a coordinate i, $1 \le i \le N$, in which they all are differ.
- *$(\le s)$-separable* [2] code for the A–MAC if for any k-tuple and any m-tuple, where $1 \le k, m \le s$, of the codewords there exists a coordinate i, $1 \le i \le N$, in which *the union of k elements of the k-tuple differs from the union of m elements of the m-tuple*.

If $t^{(A)}(s,q,N)$ denote the largest size of s-separable codes for the A–MAC, then the number

$$R^{(A)}(s,q) = \varlimsup_{N\to\infty} \frac{\ln\, t^{(A)}(s,q,N)}{N},$$

is said to be the rate of s-separable codes for the A–MAC. By the similar way we define the rate $R^{(hash)}(s,q)$ of s-hash codes, the rate $R^{(A)}(\le s,q)$ of $(\le s)$-separable codes and the rate $R^{(fp)}(s,q)$ of s-frameproof codes.

A. Related Work

The reference list from [2] contains the majority of significant papers which discuss non-asymptotic bounds on the rate $R^{(A)}(s,q)$ of s-separable codes and the rate $R^{(A)}(\le s,q)$ of $(\le s)$-separable codes along with applications of such codes for multimedia fingerprinting.

Recall the well-known properties

$$\begin{aligned} R^{(A)}(\le s,q) &\le \min\left\{R^{(fp)}(s-1,q),\, R^{(A)}(s,q)\right\},\\ R^{(fp)}(s,q) &\le R^{(A)}(\le s,q),\\ R^{(hash)}(s,q) &\le R^{(fp)}(s-1,q), \quad q \ge s \ge 2, \end{aligned} \tag{1}$$

and asymptotic (s-fixed, $q\to\infty$) lower and upper bounds

$$\begin{aligned} R^{(hash)}(s,q) &\ge \frac{\ln q}{s-1}\,(1+o(1)),\\ R^{(fp)}(s,q) &\le \frac{\ln q}{s}\,(1+o(1)). \end{aligned} \tag{2}$$

The first and second inequalities in (1) are the simple reformulations of the corresponding evident properties of binary superimposed codes [5], [6]. The third inequality in (1) as well as the asymptotic upper bound in (2) is given in [7]. The asymptotic lower bound in (2) is an obvious consequence of the random coding lower bound proved in [3], [4]. From (1) and (2) it follows the asymptotic (s-fixed, $q\to\infty$) equalities:

$$R^{(hash)}(s,q) \sim \frac{\ln q}{s-1}, \quad R^{(fp)}(s,q) \sim \frac{\ln q}{s}. \tag{3}$$

978-1-5386-4780-6/18/$31.00©2018 IEEE

Moreover, recent papers [2], [8] contains proofs of the asymptotic ($q \to \infty$) equalities:

$$R^{(A)}(\leq 2, q) \sim \frac{2 \ln q}{3}; \quad R^{(A)}(\leq s, q) \sim \frac{\ln q}{s-1}, \quad s \geq 3. \quad (4)$$

At present, in contrast to (3) and (4), the asymptotic behavior of the rate $R^{(A)}(s, q)$ of s-separable codes for the A–MAC is unknown. The aim of our paper is a further development and generalizations of the given open problem.

B. Outline

The paper is organized as follows. After introducing notations, in Section II, we give key definitions of MAC and a separable code for MAC. Section III describes five models of MACs which are important for applications. In Section IV we discuss the entropy upper bound on the rate of separable codes for any symmetric MAC and its known and new improvements. We present new asymptotic random coding bounds on the rate of separable codes for some MACs in Section V. Finally, in the last section, we derive a new combinatorial upper bound on the rate of s-separable codes which is based on the concept of list-decoding codes developed in [9].

In particular, as new results we claim the following:

$$\begin{aligned} &R^{(A)}(s, q) \geq \frac{2 \ln q}{s+1} (1 + o(1)), \ s \text{ is fixed}, q \to \infty, \\ &R^{(A)}(s, q) \leq \frac{2 \ln q}{s}, \quad s \geq 2, q \geq 2. \end{aligned} \quad (5)$$

In the given paper, we present only a brief survey of known and new results concerning the rate of separable codes for some MACs. Detailed proofs are available in an extended version of this paper [10].

II. Statement of Problem

A. Notations

Let q, N, t, s and L be integers, where $q \geq 2$, $N \geq 2$, $2 \leq s < t/2$, $1 \leq L \leq t - s$, symbol $\triangleq$ is the equality by definition, $\mathcal{A}_q \triangleq \{0, 1, \ldots, q-1\}$ – the standard q-ary alphabet, $[N] \triangleq \{1, 2, \ldots, N\}$ – the set of integers from 1 to N, $|A|$ – the size of the set A, $\lceil b \rceil$ – the least integer $\geq b$, $\lfloor b \rfloor$ – the largest integer $\leq b$. A q-ary $(N \times t)$-matrix $X = (x_i(j))$, $i \in [N]$, $j \in [t]$, $x_i(j) \in \mathcal{A}_q$, with t columns (*codewords*) $\boldsymbol{x}(j) \triangleq (x_1(j), \ldots, x_N(j)) \in \mathcal{A}_q^N$, $j \in [t]$, and N rows $\boldsymbol{x}_i \triangleq (x_i(1), x_i(2) \ldots, x_i(t)) \in \mathcal{A}_q^t$, $i \in [N]$, is called a *q-ary code of length N and size t*.

For a q-ary vector $\boldsymbol{x} = (x_1, \ldots, x_s) \triangleq x_1^s \in \mathcal{A}_q^s$, define the integer vector $(s_0, s_1, \ldots, s_{q-1})$ of length q, where $s_a = s_a(\boldsymbol{x})$, $0 \leq s_a \leq s$, $a \in \mathcal{A}_q$, is the number of positions i, $i \in [s]$, such that $x_i = a$. Obviously, $\sum_{a=0}^{q-1} s_a = s$. The vector $(s_0, \ldots, s_{q-1})$, is said to be a *composition* [1] of the q-ary vector $x_1^s = (x_1, \ldots, x_s) \in \mathcal{A}_q^s$ or, briefly,

$$comp\,(x_1^s) \triangleq (s_0, \ldots, s_{q-1}). \quad (6)$$

Let the standard symbol $\binom{[t]}{s}$ denote the set of all s-subsets of the set $[t]$. For any $\mathbf{e} = \{e_1, \ldots, e_s\} \in \binom{[t]}{s}$ called a *message of size* $|\mathbf{e}| \triangleq s$ and a code X, consider the non-ordered *s-collection* of codewords (subcode)

$$\boldsymbol{x}(\mathbf{e}) \triangleq \{\boldsymbol{x}(e_1), \ldots, \boldsymbol{x}(e_s)\}, \quad (7)$$

which can be interpreted as a subcode of X of size s.

[1] In the well-known book [11], the authors use the term *type*.

B. Symmetric Multiple-Access Channel

We use the terminology of the noiseless (deterministic) *multiple-access channel* (MAC), which has s inputs and one output [11]. Let all s input alphabets of MAC be the same and coincide with the alphabet $\mathcal{A}_q$. Denote by Z the finite output alphabet of size $|Z|$. Given s inputs $(x_1, \ldots, x_s) \in \mathcal{A}_q^s$ of MAC, the noiseless MAC is prescribed by the function

$$z = f(x_1, \ldots, x_s) \triangleq f(x_1^s), \quad z \in Z, \ x_1^s \in \mathcal{A}_q^s. \quad (8)$$

The deterministic model of MAC is called an f–MAC.

Definition 1. An f–MAC given by (8) is said to be the *symmetric* f–MAC if for any permutation $\pi \in S_s$, where S_s is the symmetric group on s elements, the following equality holds

$$f\,(x_1, \ldots, x_s) = f\left(x_{\pi(1)}, \ldots, x_{\pi(s)}\right). \quad (9)$$

Remark 1. Note that to specify a function $f = f(x_1, \ldots, x_s) = f(x_1^s)$ for the symmetric f–MAC it is necessary and sufficient to define f only on different compositions $(s_0, s_1, \ldots, s_q) = comp(x_1^s)$, $x_1^s \in \mathcal{A}_q^s$, or in other terms on multisets of cardinality s (s-collections) over A_q.

In what follows, we consider symmetric f–MACs only.

C. Separable Codes

For any message $\mathbf{e} \in \binom{[t]}{s}$ and code X, let $\boldsymbol{x}_i(\mathbf{e}) = \{x_i(e_1), \ldots, x_i(e_s)\}$, $i \in [N]$, be the s-collection of signals (7) at s symmetric f–MAC inputs at the i-th time unit. Then the signal z_i, $z_i \in Z$, $i \in [N]$, at the output of the symmetric f–MAC at the i-th time unit is

$$z_i = z_i^{(f)}(\mathbf{e}, X) \triangleq f(x_i(e_1), \ldots, x_i(e_s)) \in Z. \quad (10)$$

On the base of the code X and N signals

$$\boldsymbol{z}^{(f)}(\mathbf{e}, X) \triangleq (z_1^{(f)}(\mathbf{e}, X), \ldots, z_N^{(f)}(\mathbf{e}, X)) \in Z^N, \quad (11)$$

which are known at the output of MAC, an *observer* makes the *brute force* decision about the unknown message $\mathbf{e}$. To identify $\mathbf{e}$, a code X is assigned.

Definition 2. A q-ary code X is said to be a *s-separable* code of size t and length N for the f–MAC if all $\boldsymbol{z}^{(f)}(\mathbf{e}, X)$, $\mathbf{e} \in \binom{[t]}{s}$, are distinct.

The s-separable code allows to solve an identification problem of s active users, arising in some communication nets. A more detailed description of the problem can be found in [**?**].

Let $t^{(f)}(s, q, N)$ be the *maximal size* of s-separable q-ary codes of length N for the f–MAC. For fixed $s \geq 2$ and $q \geq 2$, the number

$$R^{(f)}(s, q) \triangleq \varlimsup_{N \to \infty} \frac{\ln\, t^{(f)}(s, q, N)}{N}, \quad (12)$$

is said to be a *rate* of s-separable q-ary codes for the f–MAC.

III. Examples of Symmetric f–MAC

A. A–MAC

The A–MAC is described by the function

$$z = f(x_1, \ldots, x_s) = \bigcup_{k=1}^{s} x_k \subseteq \mathcal{A}_q. \tag{13}$$

For instance, if $s = 4$ and $q = 3$, then

$$f(0,0,1,1) = \{0,1\}, \quad f(1,1,0,2) = \{0,1,2\}. \tag{14}$$

The cardinality $|Z|$ of output alphabet Z for the A–MAC is $|Z| = \sum_{k=1}^{\min(s,q)} \binom{q}{k}$. For $s \geq q$, we have $|Z| = 2^q - 1$.

B. B–MAC

The B–MAC known also as the compositional channel is described by the function

$$z = f(x_1^s) \triangleq comp(x_1^s), \quad x_1^s = (x_1, \ldots, x_s) \in \mathcal{A}_q^s, \tag{15}$$

where the compositional function $comp(x_1^s)$ is defined by (6). For instance, if $s = 4$ and $q = 3$, then

$$comp(0,0,1,1) = (2,2,0),\ comp(1,1,0,2) = (1,2,1).$$

The cardinality of the output alphabet for the B–MAC is $|Z| = \binom{q+s-1}{s}$, $s \geq 2$, $q \geq 2$. We acknowledge the paper [1], in which the significant applications of the B–MAC and the A–MAC were firstly developed. We also refer to [12]–[15], where the maximal output entropy [1], [11] of the A-MAC and the B-MAC was investigated in different asymptotic and non-asymptotic cases.

C. Erasure MAC

The q-ary, $q \geq 2$, f–MAC is said to be the *erasure* MAC (briefly, $eras$–MAC) if it has the $(q+1)$-ary output alphabet $Z \triangleq \{0, 1, \ldots, q-1, *\}$ and the output function $z = f(x_1^s)$ has the form:

$$z = f(x_1, \ldots, x_s) \triangleq \begin{cases} x, & \text{if } x_1 = \ldots = x_s = x,\ x \in \mathcal{A}_q, \\ *, & \text{otherwise.} \end{cases}$$

The $eras$-MAC model can be considered as an adequate description for the transmission of q-ary symbols based on the *frequency modulation* method.

D. Threshold MAC

The threshold f_ℓ–MAC (briefly, ℓ-thr–MAC) has the binary input (i.e., $q = 2$) and output alphabet $Z \triangleq \mathcal{A}_2 = \{0,1\}$, and

$$f_\ell = f_\ell(x_1, \ldots, x_s) \triangleq \begin{cases} 0, & \text{if } \sum_{i=1}^{s} x_i < \ell, \\ 1, & \text{otherwise,} \end{cases}$$

where terms of the sum are considered as $0, 1$ elements of ring $\mathbb{Z}$. Separable codes for the ℓ-thr–MAC are examples, which can be interpreted as *compressed genotyping* [16] models in molecular biology.

E. Disjunctive MAC

The disjunctive MAC (briefly, $disj$–MAC) has the binary input alphabet and the output alphabet $Z \triangleq \mathcal{A}_2 = \{0,1\}$, and

$$f(x_1, \ldots, x_s) \triangleq \begin{cases} 0, & \text{if } x_1 = \ldots = x_s = 0, \\ 1, & \text{otherwise.} \end{cases}$$

Notice that the $disj$–MAC is equivalent to the 1-thr–MAC. The $disj$-MAC model is interpreted as the transmission of binary symbols based on the *impulse modulation* method. In addition, the binary s-separable codes for the $disj$-MAC are closely connected with the *combinatorial search theory* [17] and the information-theoretic model called the *design of screening experiments* [18].

In what follows, we omit symbol $q = 2$ in notations if the corresponding channel is defined only for the binary case.

IV. Improvements of Entropy Bound

A. Entropy Upper Bound on $R^{(f)}(s,q)$

Let $\boldsymbol{p}$ be a fixed probability distribution on the alphabet $\mathcal{A}_q$ and the vector $\xi_1^s \triangleq \{\xi_1, \ldots, \xi_s\}$, $\xi_1^s \in \mathcal{A}_q^s$, is the s-collection of *independent* random variables having the same distribution, i.e., $\Pr\{\xi_k = a\} \triangleq \boldsymbol{p}(a)$, $k \in [s]$, $a \in \mathcal{A}_q$. Introduce the corresponding Shannon entropy of the output of the symmetric f–MAC, i.e,

$$H_{\boldsymbol{p}}^{(f)}(s,q) \triangleq \sum_{z \in Z} \Pr\{f(\xi_1^s) = z\} \cdot \log_q \frac{1}{\Pr\{f(\xi_1^s) = z\}}. \tag{16}$$

The following statement called the *entropy upper bound* is a conventional information-theoretic bound.

Proposition 1. *The rate $R^{(f)}(s,q)$ of s-separable q-ary codes for the symmetric f–MAC satisfies the inequality*

$$R^{(f)}(s,q) \leq C^{(f)}(s,q) \triangleq \frac{\max\limits_{\boldsymbol{p}} H_{\boldsymbol{p}}^{(f)}(s,q)}{s}. \tag{17}$$

Hereinafter, the value $C^{(f)}(s,q)$ is said to be a *capacity* of s-separable q-ary codes for the f–MAC.

B. Bounds on the Rate $R^{(disj)}(s)$ for the Disjunctive MAC

One can check that the capacity of s-separable binary codes for the $disj$–MAC is $C^{(disj)}(s) = \ln 2/s$ and the maximum in the right-hand side of (17) is attained at the distribution $\boldsymbol{p}$ with probabilities $\boldsymbol{p}(0) = 2^{-1/s}$ and $\boldsymbol{p}(1) = 1 - 2^{-1/s}$. The significant results relative to an improvement of the corresponding entropy bound (17), having the form $R^{(disj)}(s) \leq \ln 2/s$, were obtained in [19] for $s = 2$ and in [20] for $s \geq 11$. In addition, we refer to the best known asymptotic ($s \to \infty$) lower [18] and upper [20] bounds on the rate $R^{(disj)}(s)$:

$$\frac{2(\ln 2)^2}{s^2}(1 + o(1)) \leq R^{(disj)}(s) \leq \frac{4 \ln s}{s^2}(1 + o(1)).$$

C. Bounds on the Rate $R^{(eras)}(s,q)$ for the Erasure MAC

If $q=2$ and $s\to\infty$, then it is not difficult to establish [21] that the capacity of separable $(s,2)$-codes for the $eras$–MAC is $C^{(eras)}(s,2)\sim \ln 2/s$ and the maximum in the right-hand side of (17) is asymptotically attained at distribution $\boldsymbol{p}$ with $\boldsymbol{p}(1)\sim \ln 2/s$ or with $\boldsymbol{p}(0)\sim \ln 2/s$. In addition, we refer to the best known asymptotic ($s\to\infty$) lower [9] and upper [18] bounds on the rate $R^{(eras)}(s,2)$:

$$\frac{2(\ln 2)^2}{s^2}(1+o(1))\le R^{(eras)}(s,2)\le \frac{4\ln s}{s^2}(1+o(1)).$$

Open Problem. In the general case $s\ge 2$ and $q\ge 2$, we conjecture that the capacity $C^{(eras)}(s,q)$ of the $eras$–MAC does not depend on $q\ge 2$, i.e., $C^{(eras)}(s,q)=C^{(eras)}(s,2)$.

D. Bounds on the Rate $R^{(\ell-thr)}(s)$ for the Threshold MAC

The best known asymptotic ($\ell\ge 2$ is fixed and $s\to\infty$) lower and upper bounds on the rate $R^{(\ell-thr)}(s)$ were presented in [22], [23]:

$$\frac{\ell^\ell e^{-2\ell}}{(\ell-1)!2^{\ell+1}s^2}(1+o(1))\le R^{(\ell-thr)}(s)\le \frac{2\ell^2\ln s}{s^2}(1+o(1)).$$

E. Combinatorial Upper Bound for the Symmetric f–MAC

In the following theorem we establish a new combinatorial upper bound on the rate of s-separable q-ary codes for any symmetric f–MAC.

Theorem 1. [10]. *For any symmetric f–MAC and integers $s\ge 2$ and $q\ge 2$, the rate*

$$R^{(f)}(s,q)\overset{(a)}{\le} R^{(B)}(s,q)\le\begin{cases}\frac{s+1}{2s}\ln q, & \text{if } s \text{ is odd.}\\ \frac{s+2}{2(s+1)}\ln q, & \text{if } s \text{ is even.}\end{cases}$$

Observe that inequality (a) is evidently implied by Remark 1. If s is fixed and $q\to\infty$ one can check [10] that the capacity of s-separable q-ary codes for the B–MAC is $C^{(comp)}(s,q)\sim\ln q$. In other words, Theorem 1 improves the entropy upper bound (17) for the B–MAC.

V. Asymptotic Random Coding Bounds for the A–MAC and the B–MAC

In the following statements we prove asymptotic ($s\ge 2$ is fixed and $q\to\infty$) random coding lower bounds on the rate of s-separable q-ary codes for the A–MAC and the B–MAC.

Theorem 2. [10]. *If $s\ge 2$ is fixed and $q\to\infty$, then the rate $R^{(B)}(s,q)$ satisfies the asymptotic inequality*

$$R^{(B)}(s,q)\ge \frac{s}{2s-1}\ln q\,(1+o(1)).$$

Theorem 3. [10]. *If $s\ge 2$ is fixed and $q\to\infty$, then the rate $R^{(A)}(s,q)$ satisfies the asymptotic inequality*

$$R^{(A)}(s,q)\ge \frac{2}{s+1}\ln q\,(1+o(1)).$$

The asymptotic lower bound in Theorem 3 is proved with the help of a nontrivial improvement of the conventional random coding method [2]–[4].

VI. List Decoding Codes for the A–MAC

A. Notations and Definitions

For any s-collection $X=\{\boldsymbol{x}(1),\dots,\boldsymbol{x}(s)\}$ of columns $\boldsymbol{x}(j)\in\mathcal{A}_q^N$, $j\in[s]$, introduce its *union* $\langle\boldsymbol{x}(j),\,j\in[s]\rangle\triangleq \boldsymbol{z}^{(A)}(\mathbf{e},X)$, where $\mathbf{e}=\{1,\dots,s\}$ and vector $\boldsymbol{z}^{(A)}(\mathbf{e},X)$ is defined with the help of (11) and (13). We say that a column $\mathcal{Q}=(\mathcal{Q}_1,\dots,\mathcal{Q}_N)$, $\mathcal{Q}_i\subseteq\mathcal{A}_q$, $i\in[N]$, *covers* a column $\boldsymbol{x}=(x_1,\dots,x_N)\in\mathcal{A}_q^N$ if $x_i\in\mathcal{Q}_i$ for any $i\in[N]$.

Definition 3. [9]. Given integers $s\ge 1$ and $L\ge 1$ a q-ary code X is said to be a *list-decoding (s,L,q)-code* of size t and length N if for any s-collection of codewords $(\boldsymbol{x}(j_1),\dots,\boldsymbol{x}(j_s))$, its union $\langle\boldsymbol{x}(j_k),k\in[s]\rangle$ covers not more than $L-1$ other codewords of the code X.

In the case $s\ge 2$ and $L=1$, the list-decoding $(s,1,q)$-code (or s-frameproof code [2]) is an s-separable q-ary code for the A-MAC. Moreover, list-decoding $(s,1,q)$-code provides a simpler *factor* decoding algorithm, that picks the unknown message $\mathbf{e}=(e_1,\dots,e_s)\in\binom{[t]}{s}$ by searching all codewords of X covered by the output signal $\boldsymbol{z}^{(A)}(\mathbf{e},X)$. In the general case $L\ge 1$, the algorithm gives a subset of $[t]$ that contains s transmitted elements and not more than $L-1$ extra elements.

Let $t(s,L,q,N)$ be the *maximal possible size* of list-decoding (s,L,q)-codes of length N. For fixed $s\ge 2$, $L\ge 1$ and $q\ge 2$, define a *rate* of list-decoding (s,L,q)-codes:

$$R(s,L,q)\triangleq\varlimsup_{N\to\infty}\frac{\ln t(s,L,q,N)}{N}.$$

An important evident connection between s-separable q-ary codes for the A-MAC and list-decoding (s,L,q)-codes is formulated as

Proposition 2. *Any s-separable q-ary code for the A–MAC is a list-decoding $(s-1,2,q)$-code and, therefore, the rate $R^{(A)}(s,q)$ satisfies the inequality*

$$R^{(A)}(s,q)\le R(s-1,2,q),\quad s\ge 2,\quad q\ge 2. \tag{18}$$

Proposition 2 can be interpreted as a simple reformulation of the corresponding properties of binary list-decoding superimposed codes firstly introduced in [6]. A nontrivial recurrent inequality for the rate $R(s,L,q)$ of list-decoding (s,L,q)-codes is established by

Proposition 3. [10]. *For any integers $q'>q\ge 2$, $s\ge 2$ and $L\ge 1$ the following inequality holds:*

$$R(s,L,q)\ge\frac{R(s,L,q')}{\lceil q'/(q-1)\rceil}. \tag{19}$$

The inequality (19) is the base of the random coding bound presented in Theorem 4.

B. Lower Bound on the rate $R(s,L,q)$

In [9], the author established the random coding lower bound on the rate $R(s,L,q)$ of list-decoding (s,L,q)-codes which can be formulated as

Theorem 4. [10]. ***I.*** *For any fixed $q\ge 2$, $s\ge 2$ and $L\ge 1$ the following lower bound holds:*

$$R(s,L,q)\ge\underline{R}(s,L,q)\triangleq\max_{q'\ge q}\frac{-\ln P(q',s,L)}{(s+L-1)k(q,q')}, \tag{20}$$

where

$$P(q,s,L) \triangleq \sum_{m=1}^{\min\{q,s\}} \binom{q}{m} \left(\frac{m}{q}\right)^L \tag{21}$$

$$\times \sum_{k=0}^{m} (-1)^k \binom{m}{k} \left(\frac{m-k}{q}\right)^s, \tag{22}$$

$$k(q,q') \triangleq \begin{cases} 1, & \text{for} \quad q = q', \\ \lceil \frac{q'}{q-1} \rceil, & \text{otherwise}. \end{cases} \tag{23}$$

2. *For any fixed $q \geq 2$, $L \geq 1$ and $s \to \infty$*

$$\underline{R}(s,L,q) \geq \frac{L(q-1)(\ln 2)^2}{s^2}(1+o(1)). \tag{24}$$

3. *For any fixed $s \geq 2$, $L \geq 1$ and $q \to \infty$,*

$$\underline{R}(s,L,q) = \frac{L}{s+L-1} \ \ln q \ (1+o(1). \tag{25}$$

The lower bound $\underline{R}(s,L,q)$ defined by (20)-(23) improves the best previously known bounds presented in [21], [24], [25] in asymptotics (q is fixed, $s \to \infty$) and in a wide range of parameters (q,s,L) as well. Some numerical results and comparison of bounds are presented in Table I.

TABLE I
THE BEST KNOWN LOWER BOUNDS ON $R(s,L,q)$

s	2	3	4	5	6
$R(s,1,2) \geq$	$0.1438^{1,2,4}$	0.0554^{2}	0.0304^{2}	0.0194^{2}	0.0134^{2}
$R(s,2,2) \geq$	0.1703^{2}	0.0799^{2}	0.0474^{2}	0.0316^{2}	0.0226^{2}
$R(s,1,3) \geq$	$0.2939^{1,3,4}$	$0.1171^{1,4}$	0.0551^{1}	0.0360^{1}	0.0253^{1}
$R(s,2,3) \geq$	0.3662^{1}	0.1583^{1}	0.0864^{1}	0.0585^{1}	0.0425^{1}

[1] Theorem 4 [2] [9] [3] [24] [4] [25]

C. Upper Bound on the Rate $R(s,L,q)$

In [9], it was also conjectured that the lower bound (25) is tight. We prove the conjecture in the extended version of this paper [10].

Theorem 5. [10]. *For any $s \geq 2$, $L \geq 1$ and $q \geq 2$ the rate of list-decoding (s,L,q)-codes satisfies the inequality*

$$R(s,L,q) \leq \frac{L}{s+L-1} \ \ln q. \tag{26}$$

Theorem 5 and Proposition 2 lead to a corollary.

Corollary 1. *For any $s \geq 2$ and $q \geq 2$ the rate of s-separable q-ary codes for the A–MAC satisfies the inequality*

$$R^{(A)}(s,q) \leq \frac{2}{s} \ln q.$$

ACKNOWLEDGMENT

A. Dyachkov and V. Shchukin were supported in part by the Russian Foundation for Basic Research (RFBR) grant no. 16-01-00440-a. N. Polyanskii was supported in part by the Israel Science Foundation grant nos. 1162/15, 326/17 and RFBR under grant nos. 16-01-00440-a, 18-07-01427-a, 18-31-00310-mol_a. I. Vorobyev was supported in part by RFBR under grant nos. 16-01-00440-a, 18-07-01427-a, 18-31-00361-mol_a.

REFERENCES

[1] S. C. Chang and J. K. Wolf, "On the T-user M-frequency noiseless multiple-access channel with and without intensity information," *IEEE Trans. Inform. Theory*, vol. 27, no. 1, pp. 41–48, 1981.
[2] F. Gao and G. Ge, "New bounds on separable codes for multimedia fingerprinting," *IEEE Trans. Inform. Theory*, vol. 60, no. 9, pp. 5257–5262, 2014.
[3] M. L. Fredman and J. Komlós, "On the size of separating systems and families of perfect hash functions," *SIAM J. Algebraic Discrete Methods*, vol. 5, no. 1, pp. 61–68, 1984.
[4] J. Körner and K. Marton, "New bounds for perfect hashing via information theory," *European J. Combin.*, vol. 9, no. 6, pp. 523–530, 1988.
[5] W. Kautz and R. Singleton, "Nonrandom binary superimposed codes," *IEEE Trans. Inform. Theory*, vol. 10, no. 4, pp. 363–377, 1964.
[6] A. D'yachkov and V. Rykov, "A survey of superimposed code theory," *Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform.*, vol. 12, no. 4, pp. 229–242, 1983.
[7] L. Bassalygo, M. Burmester, A. Dyachkov, and G. Kabatianskii, "Hash codes," in *Proc. IEEE Int'l Symp. Inf. Theory (ISIT)*, pp. 174–174, 1997.
[8] S. R. Blackburn, "Probabilistic existence results for separable codes," *IEEE Trans. Inform. Theory*, vol. 61, no. 11, pp. 5822–5827, 2015.
[9] V. Y. Shchukin, "List decoding for a multiple access hyperchannel," *Probl. Inf. Trans.*, vol. 52, no. 4, pp. 329–343, 2016.
[10] A. G. Dyachkov, N. Polyanskii, V. Shchukin, and I. Vorobyev, "Separable codes for the symmetric multiple-access channel," *arXiv preprint arXiv:1701.06085*, 2017.
[11] I. Csiszar and J. Körner, *Information theory: coding theorems for discrete memoryless systems*. Cambridge University Press, 2011.
[12] L. A. Bassalygo and M. S. Pinsker, "Evaluation of the asymptotics of the summarized capacity of an m-frequency t-user noiseless multiple-access channel," *Probl. Inf. Trans.*, vol. 36, no. 2, pp. 91–97, 2000.
[13] L. Wilhelmsson and K. Zigangirov, "On the asymptotic capacity of a multiple-access channel," *Probl. Inf. Trans.*, vol. 33, no. 1, pp. 9–16, 1997.
[14] E. Egorova and V. Potapova, "Signature codes for a special class of multiple access channel," in *Problems of Redundancy in Information and Control Systems (REDUNDANCY), 2016 XV International Symposium*, pp. 38–42, IEEE, 2016.
[15] A. H. Vinck and K. J. Keuning, "On the capacity of the asynchronous t-user m-frequency noiseless multiple-access channel without intensity information," *IEEE Trans. Inform. Theory*, vol. 42, no. 6, pp. 2235–2238, 1996.
[16] Y. Erlich, A. Gordon, M. Brand, G. J. Hannon, and P. P. Mitra, "Compressed genotyping," *IEEE Trans. Inform. Theory*, vol. 56, no. 2, pp. 706–723, 2010.
[17] D.-Z. Du and F. K. Hwang, *Combinatorial group testing and its applications*, vol. 12 of *Series on Applied Mathematics*. World Scientific Publishing Co., Inc., River Edge, NJ, second ed., 2000.
[18] A. D'yachkov, *Lectures on Designing Screening Experiments*, vol. 10 of *Lect. Note Ser.* Pohang, Korea: Pohang Univ. of Science and Technology (POSTECH), 2003.
[19] D. Coppersmith and J. B. Shearer, "New bounds for union-free families of sets," *Electron. J. Combin.*, vol. 5, pp. Research Paper 39, 16, 1998.
[20] A. G. D'yachkov, I. V. Vorob'ev, N. A. Polyansky, and V. Y. Shchukin, "Bounds on the rate of disjunctive codes," *Probl. Inf. Transm.*, vol. 50, no. 1, pp. 27–56, 2014. Translation of Problemy Peredachi Informatsii **5**0 (2014), no. 1, 31–63.
[21] A. M. Rashad, "On symmetrical superimposed codes," *J. Inform. Process. Cybernet.*, vol. 25, no. 7, pp. 337–341, 1989.
[22] A. D'yachkov, V. Rykov, C. Deppe, and V. Lebedev, "Superimposed codes and threshold group testing," in *Information theory, combinatorics, and search theory*, vol. 7777 of *Lecture Notes in Comput. Sci.*, pp. 509–533, Springer, Heidelberg, 2013.
[23] A. De Bonis and U. Vaccaro, "Optimal algorithms for two group testing problems, and new bounds on generalized superimposed codes," *IEEE Trans. Inform. Theory*, vol. 52, no. 10, pp. 4673–4680, 2006.
[24] C. Shangguan, X. Wang, G. Ge, and Y. Miao, "New bounds for frame-proof codes," *IEEE Trans. Inform. Theory*, vol. 63, no. 11, pp. 7247–7252, 2017.
[25] D. R. Stinson, R. Wei, and K. Chen, "On generalized separating hash families," *J. Combin. Theory Ser. A*, vol. 115, no. 1, pp. 105–120, 2008.