Separable Codes for the Symmetric Multiple-Access Channel

Arkadii D'yachkov, Nikita Polyanskii, Vladislav Shchukin, and Ilya Vorobyev

***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 the 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.**

***Index Terms*— 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 (the B–MAC) and without (the A–MAC) intensity information. Using a well-known terminology [2] of the combinatorial coding theory, we describe the A–MAC and the B–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* [3] 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 the s elements of the first s-tuple differs from the union of the s elements of the second s-tuple*.
- s-*separable* [4] code for the B–MAC if for any two distinct s-tuples of the codewords there exists a coordinate i, $1 \le i \le N$, in which *the type (or the composition) of the first s-tuple differs from the type of the second s-tuple*.
- $(\le s)$-*separable* [3] 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 the k elements of the k-tuple differs from the union of the m elements of the m-tuple*.
- s-*frameproof* code [5] 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 the s elements of the s-tuple*.
- s-*hash* code [6], [7] 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 are all different.

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

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

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

Multimedia fingerprinting is a technique to trace the sources of pirate copies of copyrighted multimedia contents. Separable codes for the A–MAC were introduced in [3] as an efficient tool to construct codes for multimedia fingerprinting in the context of "averaging attack". Due to its importance, constructions, applications and bounds on the rate of separable codes were further investigated and discussed in papers [8]–[11].

Other security models and applications related to separable codes have been considered, and various classes of codes were defined in the literature. We only mention the most significant one and refer the reader to [5], where the problem of preventing an adversary from framing an innocent user was addressed, and the definition of frameproof codes was given. The latter were studied extensively in [3] and [12]–[17].

One important concept, which generalizes the definition of frameproof codes, is called (s, s')-separating codes [14], [18]

Manuscript received August 24, 2017; revised August 1, 2018; accepted December 23, 2018. A. D'yachkov, V. Shchukin, and I. Vorobyev were supported by the Russian Foundation for Basic Research under Grant 16-01-00440 a. N. Polyanskii was supported in part by the Russian Foundation for Basic Research under Grant 16-01-00440-a and in part by the Israel Science Foundation under Grant 1162/15 and Grant 326/17.

A. D'yachkov is with the Department of Probability Theory, Faculty of Mechanics and Mathematics, Lomonosov Moscow State University, 119991 Moscow, Russia (e-mail: agd-msu@yandex.ru).

N. Polyanskii is with the Skolkovo Institute of Science and Technology, 121205 Moscow, Russia, and also with the Israel Institute of Technology, Haifa 32000, Israel (e-mail: nikitapolyansky@gmail.com).

V. Shchukin is with the Institute for Information Transmission Problems, 127051 Moscow, Russia (e-mail: vpike@mail.ru).

I. Vorobyev is with the Skolkovo Institute of Science and Technology, 121205 Moscow, Russia, and also with the Moscow Institute of Physics and Technology, 141701 Dolgoprudny, Russia (e-mail: vorobyev.i.v@yandex.ru).

Communicated by A. G. Dimakis, Associate Editor for Coding Techniques.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2019.2893234

not to be confused with the definition of s-separable codes. For this kind of codes, we require the property that for any disjoint s-tuple and s'-tuple of codewords, there exists a coordinate, in which the symbols of the s-tuple are disjoint with the symbols of the s'-tuple. The most fundamental applications of (s, s')-separating codes (with $s \neq s' \geq 2$) are connected with automata synthesis [19], a key distribution problem in cryptography [20] and a problem in molecular biology [21].

Finally, hash codes have undergone study due to their applications in information retrieval, cryptography and algorithms. Different problems on hash codes were considered and developed in [6], [7], [22], and [23].

Recall the well-known results emphasizing the connection between separable codes, hash codes and frameproof codes, namely: the inequalities

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

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

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

The first and the second inequalities in (1) are simple reformulations of the corresponding evident properties of binary superimposed codes [24], [25]. The third inequality in (1) is trivially implied from the definitions. The upper bound for frameproof codes in (2) is given in [26] and is based on the same idea as an upper bound for hash codes [23], [27]. The asymptotic lower bound in (2) is an obvious corollary of the random coding lower bound proved in [6] and [28]. From (1) and (2) it follows the asymptotic (s-fixed and $q \to \infty$) equalities:

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

Moreover, recent papers [9], [10] contain proofs of the asymptotic (s-fixed and $q \to \infty$) equalities:

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

Unlike (3) and (4), the similar asymptotic behavior of the rates $R^{(A)}(s, q)$ and $R^{(B)}(s, q)$ of s-separable codes for the A–MAC and the B–MAC is unknown at present. The aim of our paper is a further development and generalization of the given open problems.

B. Outline

The remainder of the paper is organized as follows. After introducing notations, in Section II, we give a general definition of the noiseless symmetric MAC (the f-MAC) along with the corresponding definition of an s-separable code for the f-MAC, and describe five models of the f-MACs, which are important for applications. In Section III, we speculate about an information-theoretic upper bound, called an *entropy* bound, on the rate of s-separable codes for the f-MAC and discuss the known and new improvements of the entropy bound. In particular, a combinatorial upper bound on $R^{(B)}(s, q)$ is given by Theorem 1. In Section IV, new asymptotic (s-fixed, $q \to \infty$) random coding lower bounds on the rates $R^{(A)}(s, q)$ and $R^{(B)}(s, q)$ are presented by Theorem 2 and Theorem 3, respectively. In Section V, we introduce the concept of list-decoding codes for the A–MAC and obtain an upper bound on the rate of these codes, matching with the known lower bound for very large alphabet size q. Based on a simple connection between list-decoding codes and s-separable codes, we also derive an upper bound on $R^{(A)}(s, q)$, given by Theorem 6. Finally, in the Appendix, we introduce the Shannon concept of an error probability for the f-MAC and investigate the logarithmic asymptotics of the standard random coding upper bounds on the error probability. The obtained results lead us to some non-asymptotic random coding lower bounds on the rate of s-separable codes for the symmetric f–MAC.

In particular, as new results we claim the following.

Theorem 1: For any $s \geq 2$ and $q \geq 2$, the rate of s-separable q-ary codes for the B–MAC satisfies the inequality

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

Theorem 2: If $s \geq 2$ is fixed and $q \to \infty$, then the rate $R^{(B)}(s, q)$ satisfies the asymptotic inequality

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

Theorem 3: If $s \geq 2$ is fixed and $q \to \infty$, then the rate $R^{(A)}(s, q)$ satisfies the asymptotic inequality

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

Theorem 6: For any $s \geq 2$ and $q \geq 2$, the rate of s-separable q-ary codes for the A–MAC satisfies the inequality

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

II. Statement of the Problem

A. Notations

Let q, N, t, s and L be integers, where $q \geq 2$, $N \geq 2$, $2 \leq s < t/2$, $1 \leq L \leq t - s$. Let symbol $\triangleq$ denote equality by definition, $\mathcal{A}_q \triangleq \{0, 1, \ldots, q-1\}$ be the standard q-ary alphabet, $[N] \triangleq \{1, 2, \ldots, N\}$ be the set of integers from 1 to N, $|A|$ be the size of the set A, $[b]^+ \triangleq \max\{0; b\}$ be the positive part of 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*) $\boldsymbol{x}(j) \triangleq (x_1(j), \ldots, x_N(j))$, $j \in [t]$, and N rows $\boldsymbol{x}_i \triangleq (x_i(1), \ldots, x_i(t))$, $i \in [N]$, is called a *q-ary code of length N and size t.*

For any fixed q-ary vector $\boldsymbol{x} = (x_1, \ldots, x_s) \triangleq x_1^s \in \mathcal{A}_q^s$, define the integer vector $\left(s_0, s_1, \ldots, s_{q-1}\right)$ 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

$\left(s_0, \ldots, s_{q-1}\right)$ is said to be a *type* (or, *composition*) of the q-ary vector $x_1^s \in \mathcal{A}_q^s$ or, briefly,

$$T\left(x_1^s\right) \triangleq \left(s_0, \ldots, s_{q-1}\right). \tag{5}$$

Introduce the standard symbols 2^Y and $\binom{[t]}{s}$ to denote the set of all subsets of a set Y and the set of all subsets of size s of the set $[t]$. By definition, the union $U(x_1^s)$ of the q-ary vector $x_1^s \in \mathcal{A}_q^s$ is

$$U(x_1^s) \triangleq \bigcup_{i\in[s]} x_i \in 2^{\mathcal{A}_q}. \tag{6}$$

For any $\mathbf{e} = \{e_1, \ldots, e_s\} \in \binom{[t]}{s}$, called a *message*, and a code X, consider the non-ordered s-collection of codewords

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

We say that $\boldsymbol{x}(\mathbf{e})$ *encodes* the message $\mathbf{e}$.

B. The Symmetric Multiple-Access Channel

We use the terminology of the noiseless (deterministic) *multiple-access channel* (MAC), which has s inputs and one output [2]. Let all s input alphabets of MAC be the same and coincide with the alphabet $\mathcal{A}_q = \{0, 1, \ldots, q-1\}$. 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

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

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

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

Remark 1: Note that to determine 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 $(s_0, s_1, \ldots, s_{q-1}) = T(x_1^s)$, $x_1^s \in \mathcal{A}_q^s$, or, in other terms, on multisets of cardinality s (s-collections) over $\mathcal{A}_q$.

In what follows, we consider the symmetric f–MAC only.

C. Separable Codes

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

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

On the base of the code X and N signals

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

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.

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 $s \ge 2$ and $q \ge 2$, the number

$$R^{(f)}(s, q) \triangleq \overline{\lim_{N\to\infty}} \frac{\ln t^{(f)}(s, q, N)}{N}, \tag{9}$$

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

D. Examples of the Symmetric f-MAC

1) The A–MAC: The A–MAC is described by the function

$$z = f(x_1^s) \triangleq U(x_1^s) \subseteq \mathcal{A}_q,$$

where the union function $U(x_1^s)$ of a vector x_1^s is given in (6). For instance, if $s = 4$ and $q = 3$, then

$$U(0, 0, 1, 1) = \{0, 1\}, \quad U(1, 1, 0, 2) = \{0, 1, 2\}.$$

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

2) The B–MAC: The B–MAC known also as the *compositional* channel is described by the function

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

where the type function $T(x_1^s)$ of a vector x_1^s is defined by (5). For instance, if $s = 4$ and $q = 3$, then

$$T(0, 0, 1, 1) = (2, 2, 0), \quad T(1, 1, 0, 2) = (1, 2, 1).$$

The cardinality of the output alphabet for the B–MAC is $|Z| = \binom{q+s-1}{s}$, $s \ge 2$, $q \ge 2$. We acknowledge the paper [1], in which the significant applications of the B–MAC and the A–MAC were firstly developed.

3) The Erasure MAC: A q-ary 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.

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

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

where terms of the sum are considered as 0 and 1 elements of the ring of integers $\mathbb{Z}$. Separable codes for the ℓ-*thr*–MAC are connected with some *compressed genotyping* [29] models arising in the molecular biology.

5) The 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

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

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* [30] and the information-theoretic model called the *design of screening experiments* [31].

III. Improvements of the Entropy Bound

In this section, we first give a general statement called the entropy bound on the rate of separable codes for any symmetric MAC. For an asymptotic regime $s \to \infty$, we recall the best known bounds on the rate of separable codes for the disjunctive, the erasure, the threshold, the A and the B MACs in Sections III-B-III-F, respectively. Finally, in Section III-G, we present Theorem 1, a novel upper bound, which holds for any symmetric MAC and improves the entropy bound.

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

Let $\boldsymbol{p} \triangleq \{p(a), a \in \mathcal{A}_q\}$, where $0 \le p(a) \le 1, a \in \mathcal{A}_q$, and $\sum_{a \in \mathcal{A}_q} p(a) = 1$, be a fixed probability distribution on the q-ary alphabet $\mathcal{A}_q$, and a multinomial random vector $\xi_1^s \triangleq (\xi_1, \ldots, \xi_s) \in \mathcal{A}_q^s$ is the collection of s *independent* random variables having the same distribution $\boldsymbol{p}$, i.e., $\Pr\{\xi_k = a\} \triangleq p(a), k \in [s], a \in \mathcal{A}_q$. If the random vector ξ_1^s is interpreted as s signals at s *independent* inputs of the symmetric f–MAC, then the output Shannon entropy $H_{\boldsymbol{p}}^{(f)}(s, q)$ is defined [2] as

$$H_{\boldsymbol{p}}^{(f)}(s, q) \triangleq \sum_{z \in Z} \Pr\{f\left(\xi_1^s\right) = z\} \cdot \ln \frac{1}{\Pr\{f\left(\xi_1^s\right) = z\}},$$

$$\Pr\{\xi_1^s = a_1^s\} \triangleq \prod_{k=1}^{s} \Pr\{\xi_k = a_k\} \triangleq \prod_{k=1}^{s} p(a_k). \tag{10}$$

Remark 2: Remark 1 and the well-known maximization property [2] of the Shannon entropy imply that for any symmetric f-MAC and any probability distribution $\boldsymbol{p}$, the entropy function $H_{\boldsymbol{p}}^{(f)}(s, q)$ satisfies the inequalities

$$H_{\boldsymbol{p}}^{(f)}(s, q) \le H_{\boldsymbol{p}}^{(B)}(s, q) \le \ln \binom{s+q-1}{q}, \tag{11}$$

where we took into account that for the B-MAC, the output alphabet size $|Z| = \binom{s+q-1}{q}$.

Proposition 1 [32]–[34]: The rate of s-separable q-ary codes for the symmetric f–MAC satisfies the inequality

$$R^{(f)}(s, q) \le \overline{C}^{(f)}(s, q) \triangleq \frac{\max\limits_{\boldsymbol{p}} H_{\boldsymbol{p}}^{(f)}(s, q)}{s}. \tag{12}$$

The foregoing statement is based on the subadditive property [2] of the Shannon entropy and, hereinafter, the function $\overline{C}^{(f)}(s, q)$ defined by (10) and (12) is said to be an *entropy bound* for the f–MAC.

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

One can check [33] that the entropy bound of the $disj$–MAC is $\overline{C}^{(disj)}(s, 2) = \ln 2/s$ and the maximum in the right-hand side of (12) is attained at the distribution $\boldsymbol{p}$ with probabilities $p(0) = 2^{-1/s}$ and $p(1) = 1 - 2^{-1/s}$. Some significant results, improving the entropy bound $R^{(disj)}(s, 2) \le \ln 2/s$, were obtained in [35] for $s = 2$ and in [36] for $s \ge 11$. In addition, we refer to the best known asymptotic ($s \to \infty$) lower [31] and upper [36] bounds on the rate $R^{(disj)}(s)$:

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

where the lower bound is based on Proposition 5 formulated in the Appendix.

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 [37] that the entropy bound of the $eras$–MAC is $\overline{C}^{(eras)}(s, 2) \sim \ln 2/s$ and the maximum in the right-hand side of (12) is asymptotically attained at distribution $\boldsymbol{p}$ with $p(1) \sim \ln 2/s$ or with $p(0) \sim \ln 2/s$. In addition, we mention the best known asymptotic ($s \to \infty$) lower [38] and upper [31] 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: We conjecture that the enropy bound of the $eras$–MAC does not depend on $q \ge 2$, i.e.,

$$\overline{C}^{(eras)}(s, q) = \overline{C}^{(eras)}(s, 2), \quad s \ge 2, \; q \ge 2.$$

D. Bounds on the Rate $R^{(\ell\text{-}thr)}(s)$ 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 [39] and [40]:

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

E. Bounds on the Rate $R^{(A)}(s, q)$ for the A–MAC

For fixed q and $s \to \infty$, the best known upper bounds on the rate $R^{(A)}(s, q)$ are based on the upper bound for $R^{(disj)}(s, 2)$ and improve the entropy bound. The asymptotic ($s \to \infty$) lower and upper bounds were established in [38]

$$\frac{(q-1)}{s^2 \log_2^2 e}(1 + o(1)) \le R^{(A)}(s, q) \le \frac{4(q-1) \ln s}{s^2}(1 + o(1)).$$

F. Bounds on the Rate $R^{(B)}(s, q)$ for the B–MAC

For fixed q and $s \to \infty$, the best known lower and upper bounds on the rate $R^{(B)}(s, q)$ were given in [32] and [41] (case $q = 2$) and in [1] and [4] (case $q > 2$)

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

G. Combinatorial Upper Bound for the Symmetric MAC

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

Theorem 1: For any symmetric f–MAC and $s \ge 2$, $q \ge 2$, the rate satisfies the inequality

$$R^{(f)}(s,q) \overset{(a)}{\le} R^{(B)}(s,q)$$
$$\le \overline{R}^{(B)}(s,q) \triangleq \begin{cases} \frac{s+1}{2s}\ln q, & \text{if } s \text{ is odd}, \\ \frac{s+2}{2(s+1)}\ln q, & \text{if } s \text{ is even}. \end{cases} \qquad (13)$$

The inequality (a) is evidently implied by Remark 1 because any s-separable code for the given symmetric f–MAC is an s-separable code for the B–MAC as well. For the B–MAC, the maximization problem in the right-hand side of (12) was firstly solved in [42]. Mateev [42] proved that the maximum is attained at the uniform distribution $p(a) = 1/q, a \in \mathcal{A}_q$, and the entropy bound $\overline{C}^{(B)}(s,q)$ is

$$\overline{C}^{(B)}(s,q) = \frac{1}{s}\sum_{\sum s_i = s} \frac{s!}{s_0!\dots s_{q-1}!}\frac{1}{q^s}\ln\left(\frac{s_0!\dots s_{q-1}!}{s!/q^s}\right).$$

Applying the foregoing formula, one can easily check that for any $s \ge 2$ and $q \ge 2$,

$$\overline{C}^{(B)}(s,q) \ge \frac{1}{s}(\ln q^s - \ln s!) = \ln q - \frac{\ln s!}{s}. \qquad (14)$$

Observe that the general bound (11) yields the upper bound

$$\overline{C}^{(B)}(s,q) \le \frac{1}{s}\ln\binom{s+q-1}{s} < \ln(q+s-1) \qquad (15)$$

From Theorem 1 and inequalities (14)-(15), it follows

Corollary 1: If $s \ge 2$ is fixed and $q \to \infty$, then the entropy bound for the B-MAC $\overline{C}^{(B)}(s,q) \sim \ln q$, i.e., the upper bound $\overline{R}^{(B)}(s,q)$ defined in the left-hand side of (13) asymptotically improves the entropy bound $\overline{C}^{(B)}(s,q)$. In addition, for any $s \ge 2$ and $q > (s!)^{2/(s-1)}$, the rate $R^{(B)}(s,q)$ of s-separable codes for the B-MAC satisfies the strict inequality $R^{(B)}(s,q) < \overline{C}^{(B)}(s,q)$.

Remark 3: If $s \ge 2$ is fixed and $q \to \infty$, then we do not know any asymptotic results about the entropy bound $\overline{C}^{(A)}(s,q)$ for the A-MAC which are similar to the results described in Corollary 1 for the B-MAC.

Proof of Theorem 1: Fix an arbitrary q-ary $(N\times t)$-code X. For any α, $0 < \alpha < 1$, without loss of generality, we may assume that all codewords from X are distinct and the length N can be represented as a sum of two integers αN and $(1-\alpha)N$. Given X, introduce the bipartite graph

$$G = G(X) = (V,E) \triangleq (V_1 \cup V_2, E),$$
$$|V_1| = q^{\alpha N}, \quad |V_2| = q^{(1-\alpha)N},$$

defined as follows. Let the vertices in V_1 and V_2 correspond to distinct q-ary vectors of length αN and $(1-\alpha)N$, respectively. Two vertices $v_1 \in V_1$ and $v_2 \in V_2$ are connected with an edge if and only if the code X contains a codeword of length $N = \alpha N + (1-\alpha)N$ which is the concatenation of two q-ary vectors corresponding to v_1 and v_2. Thus, we obtain the graph $G(X)$ having $|V| = q^{(1-\alpha)N} + q^{\alpha N}$ vertices and t edges, identified by the indexes $[t]$ of the code X. In addition, any message $\mathbf{e} \in \binom{[t]}{s}$ is interpreted as a non-ordered s-collection of edges.

Let X be a q-ary s-separable code for the B-MAC. Now we shall prove that there is no short cycle in $G(X)$. Suppose, seeking a contradiction, that there exists a simple cycle $C_{2\ell}$ of length $2\ell \le 2s$ in $G(X)$. Enumerate edges in $C_{2\ell}$ by $e_1,\dots,e_{2\ell}$, where e_i and e_{i+1} are adjacent for any $i \in [2\ell - 1]$ (e_1 and $e_{2\ell}$ are also adjacent). Define the set E_1 as $\{e_1, e_3, \dots, e_{2\ell-1}\}$, and let E_2 be the remaining edges of the cycle. Consider an arbitrary subset $\mathcal{S} \subset [t] \setminus \{E_1 \cup E_2\}$ of the size $|\mathcal{S}| = s - \ell$ and define two messages $\mathbf{e}_i \triangleq E_i \cup \mathcal{S} \in \binom{[t]}{s}$, $i = 1,2$. It is easy to check that outputs of the B-MAC for these messages are the same, i.e., $z^{(B)}(\mathbf{e}_1, X) = z^{(B)}(\mathbf{e}_2, X)$. This contradicts to Definition 2.

It is known (e.g., see [43]) that if a bipartite graph with two parts of sizes n and m does not contain any simple cycle of length $\le 2s$, then the number t of its edges is

$$t \le \begin{cases} (2s-3)\left((mn)^{\frac{s+1}{2s}} + m + n\right), & \text{if } s \text{ is odd}, \\ (2s-3)\left(m^{\frac{s+2}{2s}}n^{1/2} + m + n\right), & \text{if } s \text{ is even}. \end{cases}$$

For odd s, we obtain

$$t \le (2s-3)\left[q^{N\frac{s+1}{2s}} + q^{\alpha N} + q^{(1-\alpha)N}\right]$$
$$\le 3(2s-3)q^{N\max\left\{\frac{s+1}{2s},\alpha,(1-\alpha)\right\}}.$$

Taking $\alpha = 1/2$, we derive

$$t \le 3(2s-3)q^{\frac{s+1}{2s}N},$$

and the rate is upper bounded as in (13). Applying the second inequality for even s, we have

$$t \le (2s-3)\left[q^{\frac{N}{2}(1+\frac{2\alpha}{s})} + q^{\alpha N} + q^{(1-\alpha)N}\right]$$
$$\le 3(2s-3)q^{N\max\left\{\frac{s+2\alpha}{2s},\alpha,1-\alpha\right\}}.$$

Taking α as a root of the equality $\frac{s+2\alpha}{2s} = 1-\alpha$, i.e., $\alpha = \frac{s}{2(s+1)}$, we obtain

$$t \le 3(2s-3)q^{\frac{s+2}{2(s+1)}N},$$

i.e., the rate satisfies (13). □

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

In this section, we apply the random coding method to construct the asymptotic (s-fixed, $q \to \infty$) lower bounds on the rate of s-separable q-ary codes for the A–MAC and the B–MAC.

Before deriving the bounds, let us introduce some auxiliary notations. Notation $2^{(\mathcal{A}_q,N)}$ stands for the Cartesian product of N copies of $2^{\mathcal{A}_q}$, where $2^{\mathcal{A}_q}$ is the set of all subsets of $\mathcal{A}_q$. For a collection of codewords $V = \{\boldsymbol{x}(i_1),\dots,\boldsymbol{x}(i_s)\} \subset \mathcal{A}_q^N$, by $T(V)$ we abbreviate the q-ary $(N\times q)$ matrix

$$T(V) \triangleq (T(x_1(i_1),\dots,x_1(i_s)),\dots,T(x_N(i_1),\dots,x_N(i_s)))^T, \qquad (16)$$

and we define the vector $U(V)$ from $2^{(\mathcal{A}_q,N)}$ as follows

$$U(V) \triangleq (U(x_1(i_1),\dots,x_1(i_s)),\dots,U(x_N(i_1),\dots,x_N(i_s)))^T. \tag{17}$$

A. Random Coding Lower Bound on $R^{(B)}(s,q)$

An asymptotic ($q \to \infty$) random coding lower bound on the rate of s-separable q-ary codes for the B–MAC is given by

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

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

Proof of Theorem 2: Consider the ensemble of matrices $X = (x_i(j))$, where entries $x_i(j)$, $i \in [N]$, $j \in [t]$, are chosen independently and uniformly at random from the alphabet $\mathcal{A}_q$. Define a *bad* event B_j: "there exist two distinct messages $\mathbf{e} \neq \hat{\mathbf{e}}$ from $\binom{[t]}{s}$ so that $j \in \mathbf{e}$, $j \notin \hat{\mathbf{e}}$ and $T(\boldsymbol{x}(\mathbf{e})) = T(\boldsymbol{x}(\hat{\mathbf{e}}))$", where the matrix $T(\cdot)$ is defined by (16). To establish the existence of an s-separable q-ary code for the B–MAC, we shall upper bound the probability of the bad event by

$$\begin{aligned}
\Pr\{B_j\} &= \Pr\left\{ \bigcup_{\substack{\mathbf{e},\hat{\mathbf{e}}\in\binom{[t]}{s} \\ j\in\mathbf{e},\, j\notin\hat{\mathbf{e}}}} T(\boldsymbol{x}(\mathbf{e})) = T(\boldsymbol{x}(\hat{\mathbf{e}})) \right\} \\
&\overset{(a)}{\le} s \max_{m\in[s]} \Pr\left\{ \bigcup_{\substack{\mathbf{e},\hat{\mathbf{e}}\in\binom{[t]}{s},\, j\in\mathbf{e} \\ |\mathbf{e}\cap\hat{\mathbf{e}}|=s-m,\, j\notin\hat{\mathbf{e}}}} T(\boldsymbol{x}(\mathbf{e})) = T(\boldsymbol{x}(\hat{\mathbf{e}})) \right\} \\
&\overset{(b)}{=} s \max_{m\in[s]} \Pr\left\{ \bigcup_{\substack{\mathbf{e},\hat{\mathbf{e}}\in\binom{[t]}{m},\, j\in\mathbf{e} \\ \mathbf{e}\cap\hat{\mathbf{e}}=\emptyset}} T(\boldsymbol{x}(\mathbf{e})) = T(\boldsymbol{x}(\hat{\mathbf{e}})) \right\} \\
&\overset{(c)}{\le} s \max_{m\in[s]} t^{2m-1} \Pr\left\{ \begin{array}{c} T(\boldsymbol{x}(\mathbf{e})) = T(\boldsymbol{x}(\hat{\mathbf{e}})) \\ \text{for some } \mathbf{e},\hat{\mathbf{e}}\in\binom{[t]}{m} \\ \mathbf{e}\cap\hat{\mathbf{e}}=\emptyset \end{array} \right\} \\
&\overset{(d)}{=} s \max_{m\in[s]} t^{2m-1} \left(\Pr\{T(u_1^m) = T(v_1^m)\}\right)^N,
\end{aligned}$$

where inequality (a) is implied by

$$\Pr\left\{\bigcup_{m=1}^{s} C_i\right\} \le s \max_{m\in[s]} \Pr\{C_i\},$$

equality (b) is followed by the fact

$$T(V_1) = T(V_2) \iff T(V_1 \setminus V_2) = T(V_2 \setminus V_1),$$

inequality (c) is an evident consequence of the union bound since the number of ways to choose a pair $\mathbf{e}, \hat{\mathbf{e}}$ with the property required is $\binom{t}{2m-1}\binom{2m-1}{m-1} \le t^{2m-1}$, and $\{u_i, v_i\}|_{i=1}^m$ in the last equality (d) are independent random variables having the uniform distribution on the set $\mathcal{A}_q$. Let us estimate the probability that two random m-tuples have the same type

$$\begin{aligned}
\Pr\left\{T\left(u_1^m\right) = T\left(v_1^m\right)\right\} &= \Pr\left\{ \bigcup_{\pi\in S_m} \left[\bigcap_{k=1}^{m} \left(u_k = v_{\pi(i)}\right) \right] \right\} \\
&\le m! \cdot \Pr\left\{ \bigcap_{k=1}^{m} \left(u_k = v_{\pi(k)}\right) \right\} = \frac{m!}{q^m}.
\end{aligned}$$

Therefore,

$$\Pr\{B_j\} \le s \max_{m\in[s]} t^{2m-1}(m!/q^m)^N.$$

Since $\Pr\{B_j\}$ does not depend on $j \in [t]$, we deduce that if the upper bound given above is less than $1/2$, then there exists an s-separable q-ary code for the B–MAC of size $t/2$ and length N. Thus, the lower bound on $R^{(B)}(s,q)$ is as follows

$$R^{(B)}(s,q) \ge \min_{m\in[s]} \frac{m\ln q - \ln m!}{2m-1}.$$

This leads to the statement of Theorem 2. □

B. Random Coding Lower Bound on $R^{(A)}(s,q)$

Now we establish an asymptotic random coding lower bound on the rate of s-separable q-ary codes for the A–MAC which is presented by

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

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

Proof of Theorem 3: Consider the ensemble of matrices $X = (x_i(j))$, where entries $x_i(j)$, $i \in [N]$, $j \in [t]$, are chosen independently and uniformly at random from the alphabet $\mathcal{A}_q$. Define a *bad* event A_j: "there exist two distinct messages $\mathbf{e} \neq \hat{\mathbf{e}}$ from $\binom{[t]}{s}$ so that $j \in \mathbf{e}$, $j \notin \hat{\mathbf{e}}$ and $U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}}))$", where the vector $U(\cdot) \in 2^{(\mathcal{A}_q,N)}$ is defined by (17). To establish the existence of an s-separable q-ary code for the A–MAC, we shall upper bound the probability of the bad event by

$$\begin{aligned}
\Pr\{A_j\} &= \Pr\left\{ \bigcup_{\substack{\mathbf{e},\hat{\mathbf{e}}\in\binom{[t]}{s} \\ j\in\mathbf{e},\, j\notin\hat{\mathbf{e}}}} U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}})) \right\} \\
&\overset{(a)}{\le} s \max_{m\in[s]} \Pr\left\{ \bigcup_{\substack{\mathbf{e},\hat{\mathbf{e}}\in\binom{[t]}{s},\, j\in\mathbf{e} \\ |\mathbf{e}\cap\hat{\mathbf{e}}|=s-m,\, j\notin\hat{\mathbf{e}}}} U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}})) \right\} \\
&\overset{(b)}{\le} s \max\left(\Pr\{C_1\},\ \max_{m\in\{2,\dots,s\}} t^{s+m-1}\Pr\{P_m\} \right),
\end{aligned}$$

where C_m and P_m are defined as follows

$$C_m \triangleq \left\{ \bigcup_{\substack{\mathbf{e},\hat{\mathbf{e}}\in\binom{[t]}{s},\, j\in\mathbf{e} \\ |\mathbf{e}\cap\hat{\mathbf{e}}|=s-m,\, j\notin\hat{\mathbf{e}}}} U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}})) \right\},$$

$$P_m \triangleq \left\{ \underset{\substack{\text{for some } \mathbf{e},\hat{\mathbf{e}}\in\binom{[t]}{s} \\ |\mathbf{e}\cap\hat{\mathbf{e}}|=s-m}}{U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}}))} \right\}.$$

Inequality (a) is implied by the evident inequality

$$\Pr\left\{\bigcup_{m=1}^{s} C_m\right\} \le s \max_{m\in[s]} \Pr\{C_m\},$$

inequality (b) is followed by

$$\max_{m\in[s]} \Pr\{C_m\} = \max\left(\Pr\{C_1\}, \max_{m\in\{2,\ldots,s\}} \Pr\{C_m\}\right)$$

and the union bound, which was applied for the cases $m \ge 2$. Now let us further estimate $\Pr\{P_m\}$ by

$$\Pr\{P_m\} = \prod_{i=1}^{N} \Pr\left\{ \underset{\substack{\text{for some } \mathbf{e},\hat{\mathbf{e}}\in\binom{[t]}{s} \\ |\mathbf{e}\cap\hat{\mathbf{e}}|=s-m}}{\bigcup_{k=1}^{s} x_i(e_k) = \bigcup_{j=1}^{s} x_i(\hat{e}_j)} \right\} \overset{(c)}{\le} \frac{s^{mN}}{q^{mN}}. \quad (18)$$

To prove (c) in the last inequality, we employ the following fact. Suppose $\xi_1, \ldots, \xi_{m+s}$ are independent random variables distributed uniformly over $\mathcal{A}_q$. Then

$$\Pr\left\{\bigcup_{k=1}^{s} \xi_k = \bigcup_{j=m+1}^{m+s} \xi_j\right\} \le \Pr\left\{\bigcup_{k=1}^{m} \xi_k \subset \bigcup_{i=m+1}^{m+s} \xi_i\right\}$$
$$\le \left(\Pr\left\{\xi_1 \in \bigcup_{i=m+1}^{m+s} \xi_i\right\}\right)^m \le \frac{s^m}{q^m}.$$

As for $\Pr\{C_1\}$, we obtain its upper bound in a different way. Let E_j consist of all possible pairs $(\mathbf{e}, \hat{\mathbf{e}})$ so that $\mathbf{e}, \hat{\mathbf{e}} \in \binom{[t]}{s}$, $j \in \mathbf{e}$, $j \notin \hat{\mathbf{e}}$ and $|\mathbf{e} \cap \hat{\mathbf{e}}| = s-1$. Since $|\mathbf{e} \cap \hat{\mathbf{e}}| = s-1$, there exists $\hat{j} \in [t]$ such that $\mathbf{e} = \{j\} \cup \{\mathbf{e} \cap \hat{\mathbf{e}}\}$ and $\hat{\mathbf{e}} = \{\hat{j}\} \cup \{\mathbf{e} \cap \hat{\mathbf{e}}\}$. For a real parameter a, $0 < a < 1$, we represent the event $\{U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}}))\}$ as a disjoint union of two events. For the first one, we additionally require the Hamming distance $d_H(\cdot)$ between $\boldsymbol{x}(j)$ and $\boldsymbol{x}(\hat{j})$ to be at least aN, i.e., $A_j(\mathbf{e}, \hat{\mathbf{e}}, \ge a) \triangleq \{U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}})), d_H(\boldsymbol{x}(j), \boldsymbol{x}(\hat{j})) \ge aN\}$. The remaining one is $A_j(\mathbf{e}, \hat{\mathbf{e}}, < a) \triangleq \{U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}})), d_H(\boldsymbol{x}(j), \boldsymbol{x}(\hat{j})) < aN\}$. Then we deal with each event individually. More concretely, $\Pr\{C_1\}$ is upper bounded by

$$\Pr\left\{\bigcup_{(\mathbf{e},\hat{\mathbf{e}})\in E_j} A_j(\mathbf{e}, \hat{\mathbf{e}}, \ge a)\right\} + \Pr\left\{\bigcup_{(\mathbf{e},\hat{\mathbf{e}})\in E_j} A_j(\mathbf{e}, \hat{\mathbf{e}}, < a)\right\}$$
$$\le t^s \Pr\left\{\underset{\text{for some } (\mathbf{e},\hat{\mathbf{e}})\in E_j}{A_j(\mathbf{e}, \hat{\mathbf{e}}, \ge a)}\right\} + t \Pr\{d_H(\boldsymbol{x}(j), \boldsymbol{x}(\hat{j})) < aN\},$$

where the inequality is implied by the union bound, and $\hat{j} \in [t]$, $\hat{j} \neq j$. For simplicity of notation let us assume that aN is an integer. Let us estimate the probability that two random q-ary vectors of length N have the Hamming distance at most aN

$$\Pr\{d_H(\boldsymbol{x}(j), \boldsymbol{x}(\hat{j})) < aN\}$$
$$= \sum_{i=0}^{aN-1} \Pr\{d_H(\boldsymbol{x}(j), \boldsymbol{x}(\hat{j})) = i\}$$
$$= \sum_{i=N-aN+1}^{N} \binom{N}{i} \left(\frac{1}{q}\right)^i \left(1 - \frac{1}{q}\right)^{N-i} < \frac{2^N}{q^{(1-a)N}}.$$

Now, for any $(\mathbf{e}, \hat{\mathbf{e}}) \in E_j$, we proceed with the event $A_j(\mathbf{e}, \hat{\mathbf{e}}, \ge a) = \{U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}})), d_H(\boldsymbol{x}(j), \boldsymbol{x}(\hat{j})) \ge aN\}$ as follows

$$\Pr\{A_j(\mathbf{e}, \hat{\mathbf{e}}, \ge a)\}$$
$$\overset{(d)}{=} \sum_{i=aN}^{N} \Pr\left\{U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}})) \middle| d_H(\boldsymbol{x}(j), \boldsymbol{x}(\hat{j})) = i\right\}$$
$$\times \Pr\left\{d_H(\boldsymbol{x}(j), \boldsymbol{x}(\hat{j})) = i\right\}$$
$$\overset{(e)}{\le} \sum_{i=0}^{N-aN} \binom{N}{i} \left(\frac{1}{q}\right)^i \left(1 - \frac{1}{q}\right)^{N-i}$$
$$\times \left(\frac{(s-1)^2}{q^2}\right)^{N-i} < \frac{\left(2s^2\right)^N}{q^{(1+a)N}}.$$

Equality (d) is derived by the law of total probability. To prove (e) in the last inequality, we use the following fact. Suppose $\xi_1, \ldots, \xi_{s+1}$ are independent random variables distributed uniformly over $\mathcal{A}_q$. Then

$$\Pr\left\{\bigcup_{k=1}^{s} \xi_k = \bigcup_{j=2}^{s+1} \xi_j, \xi_1 \neq \xi_{s+1}\right\}$$
$$\le \Pr\left\{\xi_1 \in \bigcup_{j=2}^{s} \xi_j, \xi_{s+1} \in \bigcup_{j=2}^{s} \xi_j\right\} \le \frac{(s-1)^2}{q^2}.$$

Therefore, we get

$$\Pr\{C_1\} \le \min_{0<a<1} \left(t^s \frac{\left(2s^2\right)^N}{q^{(1+a)N}} + t \frac{2^N}{q^{(1-a)N}}\right)$$
$$\le 2 \min_{0<a<1} \left(\max\left(\frac{t^s \left(2s^2\right)^N}{q^{(1+a)N}}, \frac{t\, 2^N}{q^{(1-a)N}}\right)\right).$$

Finally, summarizing the above arguments, we obtain

$$\Pr\{A_j\} \le 2s \max\left(\max_{m\in\{2,\ldots,s\}} \frac{t^{s+m-1} s^{mN}}{q^{mN}},\right.$$
$$\left.\min_{0<a<1} \left(\max\left(\frac{t^s \left(2s^2\right)^N}{q^{(1+a)N}}, \frac{t\, 2^N}{q^{(1-a)N}}\right)\right)\right).$$

Since $\Pr\{A_j\}$ does not depend on $j \in [t]$, we deduce that if the upper bound given above is less than $1/2$, then there exists an s-separable q-ary code for the A–MAC of size $t/2$

and length N. Thus, the asymptotic ($q \to \infty$) lower bound on $R^{(A)}(s, q)$ is as follows

$$R^{(A)}(s, q) \geq \min\left(\frac{2}{s+1}; \max_{0<a<1}\left(\min\left(\frac{1+a}{s}; 1-a\right)\right)\right)$$

$$\times \ln q(1+o(1)) = \frac{2}{s+1}\ln q(1+o(1)). \quad \square$$

Remark 4: It is worth noticing that if we upper bound $\Pr\{C_1\}$ like we estimate $\Pr\{P_m\}$ in (18), then we would get only $R^{(A)}(s, q) \geq \frac{1}{s}\ln q(1+o(1))$ as $q \to \infty$.

V. List Decoding Codes for the A–MAC

After giving definitions and notations, in Section V-A, we derive several useful properties establishing a connection between list-decoding codes for the A–MAC and separable codes for the A–MAC and a relation between list decoding codes over alphabets of different sizes. We recall the best known lower bounds on the rate of list-decoding codes in Section V-B. Finally, we present a new combinatorial upper bound on the rate of list-decoding codes in Section V-C, which also leads to an upper bound on the rate of separable codes for the A–MAC.

A. Notations and Definitions

Recall that $2^{(\mathcal{A}_q, N)}$ stands for the Cartesian product of N copies of $2^{\mathcal{A}_q}$, where $2^{\mathcal{A}_q}$ is the set of all subsets of $\mathcal{A}_q$. A vector $\mathcal{Q} = (\mathcal{Q}_1, \ldots, \mathcal{Q}_N)^T \in 2^{(\mathcal{A}_q, N)}$ is said to *cover* a column $\boldsymbol{x} = (x_1, \ldots, x_N)^T \in \mathcal{A}_q^N$ if $x_i \in \mathcal{Q}_i$ for all $i \in [N]$.

Definition 3 [38]: Given integers $s \geq 1$ and $L \geq 1$, a q-ary code X of size t and length N is said to be a *list-decoding* (s, L, q)*-code* of size t and length N if, for any s-collection of codewords $\{\boldsymbol{x}(j_1), \ldots, \boldsymbol{x}(j_s)\}$, the vector $U(\boldsymbol{x}(j_1), \ldots, \boldsymbol{x}(j_s))$, defined by (17), covers not more than $L-1$ other codewords of the code X.

In the case $s \geq 2$ and $L = 1$, the list-decoding $(s, 1, q)$-code (or s-frameproof code [9]) is an ($\leq s$)-separable q-ary code for the A–MAC. Moreover, list-decoding $(s, 1, q)$-code provides a simple *factor* decoding algorithm, that picks the unknown message $\mathbf{e} = (e_1, \ldots, e_s) \in \binom{[t]}{s}$ by searching all codewords of X covered by the output signal

$$\boldsymbol{z}^{(A)}(\mathbf{e}, X) = U(\boldsymbol{x}(e_1), \ldots, \boldsymbol{x}(e_s))$$

$$= \left(\bigcup_{m=1}^{s} x_1(e_m), \ldots, \bigcup_{m=1}^{s} x_N(e_m)\right)^T.$$

In the general case $L \geq 1$, the algorithm provides a subset of $[t]$ that contains s elements of the message $\mathbf{e}$ and at most $L-1$ 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 $s \geq 2$, $L \geq 1$ and $q \geq 2$, define a *rate* of list-decoding (s, L, q)-codes:

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

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 of s-separable q-ary code for the A–MAC satisfies the inequality

$$R^{(A)}(s, q) \leq R(s-1, 2, q), \quad s \geq 2,\ q \geq 2.$$

Proposition 2 can be seen as a simple reformulation of the corresponding properties of binary list-decoding superimposed codes firstly introduced in [25]. A nontrivial recurrent inequality for the rate $R(s, L, q)$ of list-decoding (s, L, q)-codes is established by

Proposition 3: For any integers $q' > q \geq 2$, $s \geq 2$ and $L \geq 1$ the following inequality holds:

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

Proof of Proposition 3: Assume that there exists a list-decoding (s, L, q')-code X' of length N and size t. Let $l \triangleq \lceil q'/(q-1)\rceil$. Consider a q-ary code C of length l and size $l(q-1) \geq q'$, which is composed from all possible codewords with one nonzero symbol:

$$\begin{vmatrix}
1 & 0 & \ldots & 0 & \ldots & q-1 & 0 & \ldots & 0\\
0 & 1 & \ldots & 0 & \ldots & 0 & q-1 & \ldots & 0\\
\vdots & \vdots & \ddots & \vdots & \ldots & \vdots & \vdots & \ddots & \vdots\\
0 & 0 & \ldots & 1 & \ldots & 0 & 0 & \ldots & q-1
\end{vmatrix}$$

Let us consider an injective map $\phi : \mathcal{A}_{q'} \to C$ such that $\phi(i)$ is the $(i+1)$th codeword of C. To construct a q-ary code X of length lN and size t, we replace each symbol $a \in \mathcal{A}_{q'}$ in all codewords in X' by q-ary codeword $\phi(a)$. One can easily check that the code X is a list-decoding (s, L, q)-code. $\square$

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

In [38], applying Proposition 3 and random coding arguments, the author established the lower bound on the rate of list-decoding (s, L, q)-codes which can be formulated as

Theorem 4 [38, Th. 2]:

1. *For any fixed $q \geq 2$, $s \geq 2$ and $L \geq 1$ the following lower bound holds:*

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

where

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

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

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

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

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

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

$$\underline{R}(s, L, q) = \frac{L}{s+L-1}\ln q(1+o(1). \qquad (19)$$

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} [38] ^{3} [12] ^{4} [22]

The lower bound $\underline{R}(s, L, q)$ defined by Theorem 4 improves the best previously known bounds presented in [12], [22], and [37] in asymptotics (q is fixed, $s \to \infty$) and in a wide range of parameters (q, s, L) as well. Some numerical results and a comparison of bounds are presented in Table I.

C. Upper Bounds on the Rates $R(s, L, q)$ and $R^{(A)}(s, q)$

It was also conjectured in [38] that the lower bound (19) is tight. We prove the conjecture in

Theorem 5: For any $s \geq 2$, $L \geq 1$ and $q \geq 2$ the rate $R(s, L, q)$ of list-decoding (s, L, q)-codes satisfies the inequality

$$R(s, L, q) \leq \frac{L}{s + L - 1} \ln q. \tag{20}$$

Proposition 2 and Theorem 5 for $L = 2$ lead to the upper bound on the rate $R^{(A)}(s, q)$ which was announced in Section I-B as

Theorem 6: For any $s \geq 2$ and $q \geq 2$, the rate of s-separable q-ary codes $R^{(A)}(s, q)$ satisfies the inequality

$$R^{(A)}(s, q) \leq R(s - 1, 2, q) \leq \frac{2}{s} \ln q.$$

Proof of Theorem 5: Consider an arbitrary code X of length N and size t. For a convenience of the proof, we will use indexes j (i) of codewords (rows) which can exceed t (N), assuming that the indexes are cyclically ordered, i.e.,

$$x_n(j) = x_{n'}(j') \quad \text{for } n - n' \equiv 0 \bmod N,$$
$$j - j' \equiv 0 \bmod t. \tag{21}$$

For a codeword $\boldsymbol{x}(j) \in \mathcal{A}_q^N$, $j \in [t]$, we abbreviate a *projection* of the codeword $\boldsymbol{x}(j)$ *on the coordinates* $n, n+1, \ldots, n+L-1$ by

$$\boldsymbol{x}_n^{n+L-1}(j) \triangleq (x_n(j), \ldots, x_{n+L-1}(j)) \in \mathcal{A}_q^L.$$

A codeword $\boldsymbol{x}(j)$, $j \in [t]$, is said to be *L-rare* in X if there exists a row index $n \in [N]$ such that the number of codeword indexes $j' \in [t]$, $j' \neq j$, with the same projection $\boldsymbol{x}_n^{n+L-1}(j') = \boldsymbol{x}_n^{n+L-1}(j)$ is at most $L - 1$. Let $r = r_L(X)$ be the number of codewords which are L-rare in X. For each L-rare codeword $\boldsymbol{x}(j)$, we can choose a row index $n \in [N]$, a q-ary sequence $(a_1, \ldots, a_L) \in \mathcal{A}_q^L$ and an ordinal number (from 1 to L) of the $\boldsymbol{x}(j)$ among all $\leq L$ codewords $\boldsymbol{x}(j')$, $j' \in [t]$, for which $\boldsymbol{x}_n^{n+L-1}(j') = \boldsymbol{x}_n^{n+L-1}(j) = (a_1, \ldots, a_L)$. This correspondence is injective. Therefore, the following claim holds.

Lemma 1: For any code X of length N, the number of its L-rare codewords satisfies the inequality

$$r = r_L(X) \leq N\, L\, q^L. \tag{22}$$

Now we formulate another auxiliary statement.

Lemma 2: If a q-ary code X of length N has size

$$t > N\, L\, q^L \sum_{k=0}^{L-1} k!, \tag{23}$$

then there exists an ordered set of codewords $\mathcal{L}_s = (\boldsymbol{x}(j_1), \ldots, \boldsymbol{x}(j_L))$ such that there is no L-rare codeword in $\mathcal{L}_s$. In addition, for any $k \in [L-1]$, the projections of $\boldsymbol{x}(j_k)$ and $\boldsymbol{x}(j_{k+1})$ on the coordinates $1 + k(s-1), 2 + k(s-1), \ldots, L + k(s-1)$ are the same, i.e.,

$$\boldsymbol{x}_{1+k(s-1)}^{L+k(s-1)}(j_k) = \boldsymbol{x}_{1+k(s-1)}^{L+k(s-1)}(j_{k+1}), \quad k \in [L-1]. \tag{24}$$

Proof of Lemma 2: For any $j_1 \in [t]$, we shall try to construct a sequence $\mathcal{L}(j_1) = (\boldsymbol{x}(j_1), \boldsymbol{x}(j_2), \ldots, \boldsymbol{x}(j_L))$ of L codewords by the following rules. The first element of the sequence $\mathcal{L}(j_1)$ is $\boldsymbol{x}(j_1)$. Let a sequence $(\boldsymbol{x}(j_1), \boldsymbol{x}(j_2), \ldots, \boldsymbol{x}(j_k))$ of length k, $1 \leq k \leq L$, be already constructed. If the last codeword $\boldsymbol{x}(j_k)$ is L-rare in X, then the process ends with a failure. If $k = L$ and $\boldsymbol{x}(j_L)$ is not L-rare in X, then the process successfully ends. Otherwise, for $k \leq L - 1$, we consider L indexes from $1 + k(s-1)$ to $L + k(s-1)$. Since the codeword $\boldsymbol{x}(j_k)$ is not L-rare in X, we can find at least L other codewords with the same projection on the coordinates from $1 + k(s-1)$ to $L + k(s-1)$. Among them there are at most $k - 1$ codewords that could be already included in the sequence $\mathcal{L}(j_1)$ at the previous $k - 1$ steps. Therefore, there exists a codeword which has not been used. Among all such unused codewords we uniquely choose the codeword $\boldsymbol{x}(j_{k+1})$ with the cyclically smallest index j_{k+1} so that $j_{k+1} > j_k$ as the $(k+1)$th element of $\mathcal{L}(j_1)$.

Example 1: Let $t = 4$ and indexes $j_1 = 2$ and $j_2 = 5$ are already used in constructing the sequence, i.e., the first two element of the sequence $\mathcal{L}(j_1)$ are $(\boldsymbol{x}(2), \boldsymbol{x}(5))$. Recall that the indexes $1, 5, 9, \ldots$ correspond to the codeword index 1 as they have the same residue modulo $t = 4$. Let codewords with indexes 3 $(7, 11, \ldots)$ and 4 $(8, 12, \ldots)$ be candidates to be the codeword at the third step. Then 7, corresponding to 3, is the cyclically smallest index so that $7 > 5$, and at the third stage we build the sequence $(\boldsymbol{x}(2), \boldsymbol{x}(5), \boldsymbol{x}(7))$.

Let us prove that there exists a codeword $\boldsymbol{x}(j_1)$ for which the described process successfully ends, i.e., as a result, we obtain a sequence $\mathcal{L}_s := \mathcal{L}(j_1)$ without L-rare codewords. The process ends with a failure if and only if the codeword $\boldsymbol{x}(j_{k+1})$ is L-rare at some step $k \in [L-1]$. Fix an arbitrary L-rare codeword $\boldsymbol{x}(j)$. Given $k \in L$, let j_1 be some element of $[t]$ so that we add $\boldsymbol{x}(j_k) = \boldsymbol{x}(j)$ in the sequence $\mathcal{L}(j_1)$ at the kth step. By construction of the sequence $\mathcal{L}(j_1)$ we know that the codeword $\boldsymbol{x}(j_k)$ coincides with the codeword $\boldsymbol{x}(j_{k-1})$ on the L coordinates:

$$1 + (k-1)(s-1), 2 + (k-1)(s-1), \ldots,$$
$$(L-1) + (k-1)(s-1), \quad L + (k-1)(s-1), \tag{25}$$

and has the cyclically smallest index $j_k > j_{k-1}$ among all codeword indexes, except possibly representative indexes from $\{j_1, \ldots, j_{k-2}\}$. Hence, the codeword $\boldsymbol{x}(j_{k-1})$ is the first codeword before $\boldsymbol{x}(j_k)$, except $\boldsymbol{x}(j_1), \ldots \boldsymbol{x}(j_{k-2})$, which has the same symbols as $\boldsymbol{x}(j_k)$ on the L coordinates (25). The number of codewords among $\boldsymbol{x}(j_1), \dots, \boldsymbol{x}(j_{k-2})$, which have the same symbols as $\boldsymbol{x}(j_k)$ and $\boldsymbol{x}(j_{k-1})$ on the L coordinates (25) is from 0 to $k-2$. Therefore, for fixed codeword $\boldsymbol{x}(j)$ and position $k \in [L]$, there exist at most $k-1$ possible options for $\boldsymbol{x}(j_{k-1})$. Thus, any L-rare codeword $\boldsymbol{x}(j)$, uniquely chosen as the codeword $\boldsymbol{x}(j_k)$ in the sequence $\mathcal{L}_s(j_1)$, spoils at most $(k-1)!$ of starting codewords $\boldsymbol{x}(j_1)$. In virtue of condition (23) and upper bound (22) from Lemma 1, the code size $t > r_L(X) \cdot \sum_{k=0}^{L-1} k!$. Therefore, there exists a starting codeword $\boldsymbol{x}(j_1)$, such that the sequence $\mathcal{L}(j_1)$ will be successfully constructed. □

Lemma 3: For any list-decoding (s, L, q)-code X of length $N = s + L - 1$, the size t of the code X is upper bounded as follows

$$t \le (s + L - 1)Lq^L \sum_{k=0}^{L-1} k!. \tag{26}$$

Proof of Lemma 3: Consider an arbitrary list-decoding (s, L, q)-code X of the length $N = s + L - 1$. We prove the claim of this lemma by contradiction. Assume that $t > (s + L - 1)Lq^L \sum_{k=0}^{L-1} k!$. In virtue of Lemma 2, we can construct the sequence $\mathcal{L}_s = (\boldsymbol{x}(j_1), \dots, \boldsymbol{x}(j_L))$ so that there is no L-rare codeword in $\mathcal{L}_s$, and the property (24) holds. Let $J = \{j_1, \dots, j_L\}$ be the set of codeword indexes. Without loss of generality, we may assume the sequence $(j_1, j_2, \dots, j_L)$ is lexicographically ordered or $j_k < j_{k+1}$ for $k \in [L-1]$, since, otherwise, we can take (21) j_{k+1} as $j_{k+1} + t\lceil j_k/t \rceil$.

Now we shall find an s-collection $I = \{i_1, \dots, i_s\} \subset [t] \setminus J$ consisting of codeword indexes such that $U(\boldsymbol{x}(i_1), \dots, \boldsymbol{x}(i_s))$ covers L codewords $\{x(j),\, j \in J\}$. Recall that by covering we mean that, for any pair (j, n), $j \in J$, $n \in [N]$, there exists $i \in I$ so that the symbol $x_n(j) = x_n(i)$. Define a lexicographically ordered sequence $\mathcal{P}$ of pairs so that the first $s+L-1$ pairs are from $(j_1, 1)$ to $(j_1, s+L-1)$, and the following $(s-1)(L-1)$ pairs are of the form (j_k, n), where n runs over all row indexes from $L + 1 + (k-1)(s-1)$ to $L + k(s-1)$, i.e.,

$$\begin{aligned}
\mathcal{P} \triangleq ((j_1, 1), &(j_1, 2), \dots, (j_1, L + s - 1),\\
&(j_2, L + 1 + (s-1)), \dots, (j_2, L + 2(s-1)), \dots,\\
&(j_L, L + 1 + (L-1)(s-1)), \dots, (j_L, sL)).
\end{aligned}$$

From (24) it follows that if, for any pair (j, n) in $\mathcal{P}$, there exists $i \in I$ so that the symbol $x_n(j) = x_n(i)$, then the s-collection I is a required one. It remains to find an appropriate I. Notice that the length of $\mathcal{P}$ is sL, and the second number in pairs goes from 1 to sL. Divide the sequence $\mathcal{P}$ into s subsequences of length L so that $\mathcal{P} = (\mathcal{P}_1, \dots, \mathcal{P}_s)$. Let

$$\mathcal{P}_k \triangleq ((j_{k_1}, (k-1)L+1), (j_{k_2}, (k-1)L+2), \dots, (j_{k_L}, kL)).$$

It is easy to check that the projection $\boldsymbol{x}(j_{k_L})$ (the codeword index is the same as the first number in the last pair of $\mathcal{P}_k$) on the coordinates $(k-1)L + 1, (k-1)L + 2, \dots, kL$ is

$$\begin{aligned}
&\boldsymbol{x}_{(k-1)L+1}^{kL}(j_{k_L})\\
&\qquad = \left(x_{(k-1)L+1}(j_{k_1}), x_{(k-1)L+2}(j_{k_2}), \dots, x_{kL}(j_{k_L})\right).
\end{aligned}$$

From Lemma 2, it follows that the codeword $\boldsymbol{x}(j_{k_L})$ is not L-rare. Therefore, we can find an index i_k, $i_k \notin J$, and the corresponding codeword $\boldsymbol{x}(i_k)$ such that the projections of $\boldsymbol{x}(i_k)$ and $\boldsymbol{x}(j_{k_L})$ on the coordinates $(k-1)L+1, (k-1)L+2, \dots, kL$ are the same, i.e.,

$$\boldsymbol{x}_{(k-1)L+1}^{kL}(i_k) = \boldsymbol{x}_{(k-1)L+1}^{kL}(j_{k_L}). \tag{27}$$

Since there are s subsequences $\mathcal{P}_k$, which form $\mathcal{P}$, we can find at most s different i_k so that $U(\boldsymbol{x}(i_1), \dots, \boldsymbol{x}(i_s))$ covers L codewords $\{\boldsymbol{x}(j),\, j \in J\}$. This contradiction completes the proof of Lemma 3. □

Lemma 2 and Lemma 3 are intuitively illustrated by the following example.

Example 2: Let $L = 4$, $s = 2$ and $N = L + s - 1 = 5$. Then four q-ary codewords $\boldsymbol{x}(j_k), \boldsymbol{x}(j_k) \in \mathcal{A}_q^5$, $k \in \{1, 2, 3, 4\}$, satisfying the equalities (24) can be written in the form:

$$\begin{aligned}
\boldsymbol{x}(j_1) &= (x_1(j_1), x_2(j_1), x_3(j_1), x_4(j_1), x_5(j_1)),\\
\boldsymbol{x}(j_2) &= (y_2, x_2(j_1), x_3(j_1), x_4(j_1), x_5(j_1)),\\
\boldsymbol{x}(j_3) &= (y_2, y_3, x_3(j_1), x_4(j_1), x_5(j_1)),\\
\boldsymbol{x}(j_4) &= (y_2, y_3, y_4, x_4(j_1), x_5(j_1)).
\end{aligned}$$

These codewords are covered by $U(\boldsymbol{x}(i_1), \boldsymbol{x}(i_2))$, where two q-ary codewords $\boldsymbol{x}(i_1), \boldsymbol{x}(i_2) \in \mathcal{A}_q^5$ are based on the property (27) and can be written in the form:

$$\begin{aligned}
\boldsymbol{x}(i_1) &= (x_1(j_1), x_2(j_1), x_3(j_1), x_4(j_1), a_1),\\
\boldsymbol{x}(i_2) &= (y_2, y_3, y_4, a_2\ x_5(j_1)).
\end{aligned}$$

To complete the proof of Theorem 5, consider an arbitrary list-decoding (s, L, q)-code X of length N, $N > s+L-1$, and size t. Divide each codeword of the code X into $s+L-1$ parts of sizes n_i, where $\left\lfloor \frac{N}{s+L-1} \right\rfloor \le n_i \le \left\lceil \frac{N}{s+L-1} \right\rceil$, $i \in [s+L-1]$. The number of different parts is upper bounded by $q^{\left\lfloor \frac{N}{s+L-1} \right\rfloor} + q^{\left\lceil \frac{N}{s+L-1} \right\rceil}$. Replace each part of each codeword with a unique symbol from the Q-ary alphabet of the size $Q \triangleq 2q^{\left\lceil \frac{N}{s+L-1} \right\rceil}$. It is easy to see that the code X', obtained after replacements, is a Q-ary list-decoding (s, L, Q)-code of length $N = s+L-1$ and size t. Thus, the inequality (26) of Lemma 3 implies that the size

$$t \le (s + L - 1)L \sum_{n=0}^{L-1} n! 2^L q^{L\left\lceil \frac{N}{s+L-1} \right\rceil}.$$

This upper bound immediately yields (20). □

Appendix

A. Notations and Definitions

Given the symmetric f–MAC and a q-ary code X, a message $\mathbf{e} \in \binom{[t]}{s}$ is said to be *bad* for the code X, if there exists a message $\mathbf{e}' \neq \mathbf{e}$ such that $z^{(f)}(\mathbf{e}', X) = z^{(f)}(\mathbf{e}, X)$. If the unknown message $\mathbf{e}$ is interpreted as the random vector taking equiprobable values in the set $\binom{[t]}{s}$, then the *relative number* of "bad" messages among all $\binom{t}{s} = |\binom{[t]}{s}|$ messages can be considered as the *error probability* $\epsilon^{(f)}(X, s)$ of the code X for the *brute force* decoding.

Definition 4 [33], [34], [44]: Fix a parameter $R > 0$. Define the *error probability* for the symmetric f-MAC:

$$\epsilon^{(f)}(s, q, R, N) \triangleq \min_{X: t=\lfloor \exp\{RN\}\rfloor} \epsilon^{(f)}(X, s), \tag{28}$$

where the minimum is taken over all q-ary codes of length N and size $t = \lfloor \exp\{RN\}\rfloor$. If the parameter $R > R^{(f)}(s, q)$, where the rate of s-separable codes $R^{(f)}(s, q)$ for the f-MAC is defined by (9), then the function

$$E^{(f)}(s, q, R) \triangleq \overline{\lim_{N\to\infty}} \frac{-\ln \epsilon^{(f)}(s, q, R, N)}{N} \tag{29}$$

is called the *error exponent* for the f-MAC. The quantity

$$C^{(f)}(s, q) \triangleq \sup\left\{R : E^{(f)}(s, q, R) > 0\right\} \tag{30}$$

is said to be the *capacity* of the f-MAC for the *exponentially decreasing* error probability. Using the Shannon terminology [2], the rate of s-separable codes $R^{(f)}(s, q)$ can be also called the *zero error capacity* of the f-MAC.

It is known [33], [34], [44] that for any symmetric f–MAC the value $C^{(f)}(s, q)$ defined by (28)-(30) does not exceed the entropy bound $\overline{C}^{(f)}(s, q)$ introduced in Proposition 1, i.e.,

$$C^{(f)}(s, q) \le \overline{C}^{(f)}(s, q) = \frac{\max_{\boldsymbol{p}} H_{\boldsymbol{p}}^{(f)}(s, q)}{s}, \tag{31}$$

where $H_{\boldsymbol{p}}^{(f)}(s, q)$ is the Shannon entropy (10) of the output of the f–MAC for the given input probability distribution $\boldsymbol{p}$.

B. Random Coding Error Exponent for the f-MAC

Let the symbol $\mathcal{P}_N^{(f)}\left(s, t, (N_0, \ldots, N_{q-1})\right)$ denote the *average value* of error probability $\epsilon^{(f)}(X, s)$ over the *fixed composition ensemble* (briefly, FC-ensemble) of t independent q-ary codewords $\boldsymbol{x}(j)$ with the same type $T(\boldsymbol{x}(j)) = (N_0, \ldots, N_{q-1})$, $j \in [t]$. By a similar symbol $\mathcal{P}_N^{(f)}(s, t, \boldsymbol{p})$ we will denote the *average value* of error probability $\epsilon^{(f)}(X, s)$ over the *completely randomized ensemble* (briefly, CR-ensemble) of q-ary codes $X = \|x_i(j)\|$ with independent components $x_i(j)$ having the same distribution $\boldsymbol{p}$, i.e., the probability $\Pr\{x_i(j) = a\} \triangleq p(a)$, $i \in [N]$, $j \in [t]$, $a \in \mathcal{A}_q$.

Let $s \ge 2$, $q \ge 2$, $R > 0$ be fixed and the entropy $H_{\boldsymbol{p}}^{(f)}(s, q)$ of a fixed distribution $\boldsymbol{p}$ be defined by (10). If code parameters $N, t \to \infty$ such that

$$\frac{\ln t}{N} \sim R, \quad \frac{N_x}{N} \sim p(x), \ x \in \mathcal{A}_q, \tag{32}$$

then from the standard random coding arguments [2] it follows that the error exponent $E^{(f)}(s, q, R)$ of the f-MAC, defined by (28)-(29) satisfies two random coding bounds:

$$E^{(f)}(s, q, R) \ge \overline{\lim_{N\to\infty}} \frac{-\ln \mathcal{P}_N^{(f)}\left(s, t, (N_0, .., N_{q-1})\right)}{N}, \tag{33}$$

$$E^{(f)}(s, q, R) \ge \overline{\lim_{N\to\infty}} \frac{-\ln \mathcal{P}_N^{(f)}(s, t, \boldsymbol{p})}{N}. \tag{34}$$

To formulate the results about the logarithmic asymptotic behavior of probabilities $\mathcal{P}_N^{(f)}\left(s, t, (N_0, .., N_{q-1})\right)$ and $\mathcal{P}_N^{(f)}(s, t, \boldsymbol{p})$, we need the following auxiliary notations [31]. Let a symmetric f–MAC be represented as the conditional probability $\tau^{(f)}(z|x_1^s)$, that is

$$\tau^{(f)}(z|x_1^s) \triangleq \begin{cases} 1, & z = f(x_1^s), \\ 0, & z \ne f(x_1^s), \end{cases}$$

and the symbol

$$\tau \triangleq \left\{\tau(x_1^s, z) : \tau(x_1^s, z) \ge 0, \sum_{x_1^s, z} \tau(x_1^s, z) = 1\right\} \tag{35}$$

denotes a probability distribution on the Cartesian product $\mathcal{A}_q^s \times Z$. Using the standard symbols for the conditional probabilities of the distribution τ, we abbreviate by

$$\{\tau\}^{(f)} \triangleq \left\{\tau : \tau^{(f)}(z|x_1^s) = 0 \Rightarrow \tau(z|x_1^s) = 0\right\} \tag{36}$$

the subset of probability distributions τ (35) such that the conditional probability $\tau(z|x_1^s) = 0$ is implied by $\tau^{(f)}(z|x_1^s) = 0$.

Introduce the $\cup$-convex information-theoretic functions of the argument $\tau \in \{\tau\}^{(f)}$:

$$\mathcal{H}^{(f)}(\boldsymbol{p}, \tau) \triangleq \sum_{x_1^s \cdot z} \tau(x_1^s, z) \ln \frac{\tau(x_1^s, z)}{\tau^{(f)}(z|x_1^s) \cdot \prod_{k=1}^{s} p(x_k)},$$

$$I_m(\boldsymbol{p}, \tau) \triangleq \sum_{x_1^s \cdot z} \tau(x_1^s, z) \ln \frac{\tau(x_1^m|x_{m+1}^s, z)}{\prod_{k=1}^{m} p(x_k)}, \quad m \in [s]. \tag{37}$$

From (10), it follows that the distribution

$$\tau_{\boldsymbol{p}}^{(f)} \triangleq \left\{\tau^{(f)}(z|x_1^s) \cdot \prod_{k=1}^{s} p(x_k), x_1^s \in \mathcal{A}_q^s, z \in Z\right\} \in \{\tau\}^{(f)}$$

and the functions (37) satisfy the equalities

$$\mathcal{H}^{(f)}\left(\boldsymbol{p}, \tau_{\boldsymbol{p}}^{(f)}\right) = 0, \quad I_s\left(\boldsymbol{p}, \tau_{\boldsymbol{p}}^{(f)}\right) = H_{\boldsymbol{p}}^{(f)}(s, q).$$

Proposition 4 [31], [34]: Let $s \ge 2$, $q \ge 2$, $R > 0$ be fixed and the entropy $H_{\boldsymbol{p}}^{(f)}(s, q)$ of a fixed distribution $\boldsymbol{p}$ be defined by (10). *If the asymptotic conditions* (32) *are fulfilled, then for the FC-ensemble, there exists*

$$\lim_{N\to\infty} \frac{-\ln \mathcal{P}_N^{(f)}\left(s, t, (N_0, .., N_{q-1})\right)}{N} \triangleq E_{FC}^{(f)}(s, q, R, \boldsymbol{p}) > 0, \quad 0 < R < \frac{H_{\boldsymbol{p}}^{(f)}(s, q)}{s}, \tag{38}$$

and for the CR-ensemble, there exists

$$\lim_{N\to\infty} \frac{-\ln \mathcal{P}_N^{(f)}(s, t, \boldsymbol{p})}{N} \triangleq E_{CR}^{(f)}(s, q, R, \boldsymbol{p}) > 0, \quad 0 < R < \frac{H_{\boldsymbol{p}}^{(f)}(s, q)}{s}. \tag{39}$$

For any fixed $\boldsymbol{p}$, the positive monotonically decreasing functions $E_{FC}^{(f)}(s, q, R, \boldsymbol{p})$ and $E_{CR}^{(f)}(s, q, R, \boldsymbol{p})$ are $\cup$-convex functions of the parameter $R > 0$ of the following form:

$$E_{FC}^{(f)}(s, q, R, \boldsymbol{p}) \triangleq \min_{m\in[s]} E_{FC}^{(f)}(s, q, R, \boldsymbol{p}, m),$$

$$E_{FC}^{(f)}(s, q, R, \boldsymbol{p}, m) \triangleq \min_{\{\tau\}^{(f)}(\boldsymbol{p})} \left\{\mathcal{H}^{(f)}(\boldsymbol{p}, \tau) + [I_m(\boldsymbol{p}, \tau) - mR]^+\right\}, \tag{40}$$

and

$$E_{CR}^{(f)}(s,q,R,\boldsymbol{p}) \triangleq \min_{m\in[s]} E_{CR}^{(f)}(s,q,R,\boldsymbol{p},m),$$
$$E_{CR}^{(f)}(s,q,R,\boldsymbol{p},m) \triangleq \min_{\{\tau\}^{(f)}} \left\{\mathcal{H}^{(f)}(\boldsymbol{p},\tau)+[I_m(\boldsymbol{p},\tau)-mR]^{+}\right\}. \tag{41}$$

The minimum in (40) *is taken over the subset* $\{\tau\}^{(f)}(\boldsymbol{p})$ *of distributions* $\{\tau\}^{(f)}$ (36) *for which the marginal probabilities* $\tau(x_k)$ *are fixed and coincide with* $p(x_k)$, $k\in[s]$, *i.e.,* $\{\tau\}^{(f)}(\boldsymbol{p})$ *is defined as*

$$\left\{\tau\in\{\tau\}^{(f)}: \sum_{x_1^{k-1}}\sum_{x_{k+1}^{s}}\sum_{z}\tau(x_1^s,z)=p(x_k),\, k\in[s]\right\}. \tag{42}$$

The minimum in (41) *is taken over the set of all distributions* (36).

Remark 5: Proposition 4 and the properties of the *random error exponents* (38) and (39) were formulated and proved in the papers [31] and [34] for the particular binary case $q=2$ only. In the general case $q\ge 2$, we omit the proofs because one can check that the given results are based on the same methods developed in [31] and [34]. Here we only note that for the symmetric f-MAC, definitions (40)-(42) lead to the inequality

$$E_{CR}^{(f)}(s,q,R,\boldsymbol{p}) \le E_{FC}^{(f)}(s,q,R,\boldsymbol{p}), \quad 0<R<\frac{H_{\boldsymbol{p}}^{(f)}(s,q)}{s}.$$

Random coding bounds (33)-(34) and Proposition 4 imply that the error exponent $E^{(f)}(s,q,R)$ defined by (28)-(29) is

$$E^{(f)}(s,q,R) \ge \max_{\boldsymbol{p}} E_{FC}^{(f)}(s,q,R,\boldsymbol{p}) > 0$$
$$0<R<\overline{C}^{(f)}(s,q)=\frac{\max_{\boldsymbol{p}} H_{\boldsymbol{p}}^{(f)}(s,q)}{s} \tag{43}$$

and, obviously, the inequality (43) means that for the capacity $C^{(f)}(s,q)$ of the f-MAC, defined by (28)-(30), the lower bound

$$C^{(f)}(s,q) \ge \overline{C}^{(f)}(s,q)=\frac{\max_{\boldsymbol{p}} H_{\boldsymbol{p}}^{(f)}(s,q)}{s}, \tag{44}$$

holds. The inequalities (31) and (44) lead to

Corollary 2: The capacity $C^{(f)}(s,q)$ of the f-MAC for the exponentially decreasing error probability coincides with the entropy bound $\overline{C}^{(f)}(s,q)$, i.e.,

$$C^{(f)}(s,q) = \overline{C}^{(f)}(s,q)=\frac{\max_{\boldsymbol{p}} H_{\boldsymbol{p}}^{(f)}(s,q)}{s}, \tag{45}$$

and the number defined by the right-hand side (45) can be considered as the Shannon capacity of the symmetric f-MAC [44].

The following statement called the random coding lower bound on the rate $R^{(f)}(s,q)$ of s-separable q-ary codes for the symmetric f-MAC can be obtained as a consequence of Proposition 4.

Proposition 5 [31]: The rate $R^{(f)}(s,q)$ *of* s*-separable* q*-ary codes for the symmetric* f*-MAC satisfies the inequality*

$$R^{(f)}(s,q) \ge \underline{R}^{(f)}(s,q), \quad s\ge 2,\ q\ge 2,$$

where for any fixed distribution $\boldsymbol{p}$ *the lower bound* $\underline{R}^{(f)}(s,q)$ *can be represented in the form*

$$\underline{R}^{(f)}(s,q) \triangleq \min_{m\in[s]} \frac{E_{FC}^{(f)}(s,q,0,\boldsymbol{p},m)}{s+m-1}$$
$$= \min_{m\in[s]} \frac{\min_{\{\tau\}^{(f)}(\boldsymbol{p})}\left\{\mathcal{H}^{(f)}(\boldsymbol{p},\tau)+I_m(\boldsymbol{p},\tau)\right\}}{s+m-1}$$

or in the form

$$\underline{R}^{(f)}(s,q) \triangleq \min_{m\in[s]} \frac{E_{CR}^{(f)}(s,q,0,\boldsymbol{p},m)}{s+m-1}$$
$$= \min_{m\in[s]} \frac{\min_{\{\tau\}^{(f)}}\left\{\mathcal{H}^{(f)}(\boldsymbol{p},\tau)+I_m(\boldsymbol{p},\tau)\right\}}{s+m-1}.$$

In paper [31], Proposition 5 was proved for the particular case of the B-MAC with binary ($q=2$) alphabet only. For an arbitrary symmetric f-MAC, one can use the same arguments. The asymptotic lower bound on the rate $R^{(disj)}(s)$ for the disjunctive MAC formulated in Sect. III-B was actually obtained in [31] as a nontrivial consequence of Proposition 5.

Acknowledgements

The authors would like to thank the anonymous reviewers for their many comments and suggestions which improved both the exposition of the paper and the clarity of the proofs.

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. Inf. Theory*, vol. IT-27, no. 1, pp. 41–48, Jan. 1981, doi: 10.1109/TIT.1981.1056304.

[2] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[3] M. Cheng and Y. Miao, "On anti-collusion codes and detection algorithms for multimedia fingerprinting," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4843–4851, Jul. 2011.

[4] E. Egorova and V. Potapova, "Signature codes for a special class of multiple access channel," in *Proc. XV Int. Symp. Problems Redundancy Inf. Control Syst. (REDUNDANCY)*, Sep. 2016, pp. 38–42.

[5] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inf. Theory*, vol. 44, no. 5, pp. 1897–1905, Sep. 1998.

[6] M. L. Fredman and J. Komlós, "On the size of separating systems and families of perfect hash functions," *SIAM J. Algebr. Discrete Methods*, vol. 5, no. 1, pp. 61–68, 1984, doi: 10.1137/0605009.

[7] K. Mehlhorn, *Sorting and Searching* (Data Structures and Algorithms), vol. 1. Berlin, Germany: Springer, 1984.

[8] M. Cheng, L. Ji, and Y. Miao, "Separable codes," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1791–1803, Mar. 2012.

[9] F. Gao and G. Ge, "New bounds on separable codes for multimedia fingerprinting," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5257–5262, Sep. 2014, doi: 10.1109/TIT.2014.2331989.

[10] S. R. Blackburn, "Probabilistic existence results for separable codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 5822–5827, Nov. 2015, doi: 10.1109/TIT.2015.2473848.

[11] E. Egorova, M. Fernandez, G. Kabatiansky, and M. H. Lee, "Signature codes for the A-channel and collusion-secure multimedia fingerprinting codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 3043–3047.

[12] C. Shangguan, X. Wang, G. Ge, and Y. Miao, "New bounds for frameproof codes," *IEEE Trans. Inf. Theory*, vol. 63, no. 11, pp. 7247–7252, Nov. 2017, doi: 10.1109/TIT.2017.2745619.

[13] J. N. Staddon, D. R. Stinson, and R. Wei, "Combinatorial properties of frameproof and traceability codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 1042–1049, Mar. 2001.

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

[15] M. S. Pinsker and Y. L. Sagalovich, "Lower bound on the cardinality of code of automata's states," *Problems Inf. Transmiss.*, vol. 8, no. 3, pp. 59–66, 1972.

[16] Y. Sagalovich, "Fully separated systems," *Problems Inf. Transmiss.*, vol. 18, no. 2, pp. 74–82, 1982.

[17] A. G. D'yachkov, I. V. Vorobyev, N. A. Polyanskii, and V. Y. Shchukin, "Cover-free codes and separating system codes," *Des., Codes Cryptogr.*, vol. 82, nos. 1–2, pp. 197–209, 2017.

[18] Y. L. Sagalovich, "A method for increasing the reliability of finite automata," *Problemy Peredachi Informatsii*, vol. 1, no. 2, pp. 27–35, 1965.

[19] Y. L. Sagalovich, "Separating systems," *Problems Inf. Transmiss.*, vol. 30, no. 2, pp. 105–123, 1994.

[20] C. J. Mitchell and F. C. Piper, "Key storage in secure networks," *Discrete Appl. Math.*, vol. 21, no. 3, pp. 215–228, 1988.

[21] A. G. D'yachkov, A. J. Macula, and V. V. Rykov, "New applications and results of superimposed code theory arising from the potentialities of molecular biology," in *Numbers, Information and Complexity*. Dordrecht, The Netherlands: Kluwer Academic, 2000, pp. 265–282.

[22] D. R. Stinson, R. Wei, and K. Chen, "On generalized separating hash families," *J. Combinat. Theory A*, vol. 115, no. 1, pp. 105–120, 2008, doi: 10.1016/j.jcta.2007.04.005.

[23] L. A. Bassalygo, M. Burmester, A. Dyachkov, and G. Kabatianski, "Hash codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Aug. 1997, p. 174.

[24] W. Kautz and R. Singleton, "Nonrandom binary superimposed codes," *IEEE Trans. Inf. Theory*, vol. IT-10, no. 4, pp. 363–377, Oct. 1964.

[25] A. G. D'yachkov and V. V. Rykov, "A survey of superimposed code theory," *Problems Control Inf. Theory*, vol. 12, no. 4, pp. 229–242, 1983.

[26] S. R. Blackburn, "Frameproof codes," *SIAM J. Discrete Math.*, vol. 16, no. 3, pp. 499–510, 2003.

[27] A. G. D'yachkov, "An upper bound for hash codes," in *Proc. Conf. Comput. Sci. Inf. Technol.*, 1997, pp. 219–221.

[28] J. Körner and K. Marton, "New bounds for perfect hashing via information theory," *Eur. J. Combinatorics*, vol. 9, no. 6, pp. 523–530, 1988, doi: 10.1016/S0195-6698(88)80048-9.

[29] Y. Erlich, A. Gordon, M. Brand, G. J. Hannon, and P. P. Mitra, "Compressed genotyping," *IEEE Trans. Inf. Theory*, vol. 56, no. 2, pp. 706–723, Feb. 2010, doi: 10.1109/TIT.2009.2037043.

[30] D.-Z. Du and F. K. Hwang, *Combinatorial Group Testing and Its Applications* (Series on Applied Mathematics), vol. 12, 2nd ed. River Edge, NJ, USA: World Scientific Publishing, 2000.

[31] A. G. D'yachkov. (2003). "Lectures on designing screening experiments." [Online]. Available: https://arxiv.org/abs/1401.7505

[32] A. G. D'yachkov, "On a search model of false coins," in *Topics in Information Theory (Colloquia Mathematica Societatis Janos Bolyai)*, vol. 16. Amsterdam, The Netherlands: North Holland, 1977, pp. 163–170.

[33] M. B. Malyutov, "The separating property of random matrices," *Math. Notes Acad. Sci. USSR*, vol. 23, no. 1, pp. 84–91, 1978.

[34] A. G. D'yachkov and A. Rashad, "Universal decoding for random design of screening experiments," *Microelectron. Rel.*, vol. 29, no. 6, pp. 965–971, 1989.

[35] D. Coppersmith and J. B. Shearer, "New bounds for union-free families of sets," *Electron. J. Combinatorics*, vol. 5, no. 1, p. 39, 1998. [Online]. Available: http://www.combinatorics.org/Volume 5/Abstracts/v5i1r39.html

[36] A. G. D'yachkov, I. V. Vorob'ev, N. A. Polyansky, and V. Y. Shchukin, "Bounds on the rate of disjunctive codes," *Problems Inf. Transmiss.*, vol. 50, no. 1, pp. 27–56, 2014, doi: 10.1134/S0032946014010037.

[37] A. M. Rashad, "On symmetrical superimposed codes," *J. Inf. Process. Cybern.*, vol. 25, no. 7, pp. 337–341, 1989.

[38] V. Y. Shchukin, "List decoding for a multiple access hyperchannel," *Problems Inf. Transmiss.*, vol. 52, no. 4, pp. 329–343, 2016.

[39] A. D'yachkov, V. Rykov, C. Deppe, and V. Lebedev, "Superimposed codes and threshold group testing," in *Information Theory, Combinatorics, and Search Theory* (Lecture Notes in Computer Science), vol. 7777. Berlin, Germany: Springer, 2013, pp. 509–533, doi: 10.1007/978-3-642-36899-8_25.

[40] A. D. Bonis and U. Vaccaro, "Optimal algorithms for two group testing problems, and new bounds on generalized superimposed codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4673–4680, Oct. 2006, doi: 10.1109/TIT.2006.881740.

[41] A. G. D'yachkov and V. V. Rykov, "On a coding model for a multiple-access adder channel," *Problemy Peredachi Informatsii*, vol. 17, no. 2, pp. 26–38, 1981.

[42] P. Mateev, "On the entropy of the multinomial distribution," *Theory Probab. Appl.*, vol. 23, no. 1, pp. 188–190, 1978.

[43] A. Naor and J. Verstraëte, "A note on bipartite graphs without $2k$-cycles," *Combinatorics, Probab. Comput.*, vol. 14, nos. 5–6, pp. 845–849, 2005, doi: 10.1017/S0963548305007029.

[44] M. B. Malyutov and P. S. Mateev, "Planning of screening experiments for a nonsymmetric response function," *Math. Notes Acad. Sci. USSR*, vol. 27, no. 1, pp. 57–68, 1980.

Arkadii D'yachkov was born in Russia in 1944. He received the Ph.D degree in Mathematics from the Institute for Information Transmission Problems, Moscow, Russia, in 1971 and the Doctor of Sciences degree in Mathematics from the Lomonosov Moscow State University, Moscow, Russia, in 1985. In 1972 he joined the Faculty of Mechanics and Mathematics, the Lomonosov Moscow State University, where he is currently a Full Professor at the Department of Probability Theory. His research interests include information theory, combinatorial coding theory, probability theory and statistics.

Nikita Polyanskii was born in Russia in 1991. He received the M.Sc. degree in Mathematics and the Ph.D. degree in Mathematics from the Lomonosov Moscow State University, Moscow, Russia, in 2013 and 2016, respectively. During 2015–2017 he was a researcher at the Institute for Information Transmission Problems, Moscow, Russia, and a senior engineer at Huawei Technologies, Moscow, Russia. Since 2017 Nikita has been a postdoctoral researcher in the Department of Mathematics, Technion–Israel Institute of Technology, Haifa, Israel. Since 2018 he has been a research scientist in the Center for Computational and Data-Intensive Science and Engineering, Skolkovo Institute of Science and Technology, Moscow, Russia. His research interests include coding theory and its applications to communications, group testing, storage systems, and combinatorics.

Vladislav Shchukin received the M.Sc. degree in Mathematics and the Ph.D. degree in Mathematics from the Lomonosov Moscow State University in 2013 and 2017, respectively. Since 2015 he has been a researcher at the Institute for Information Transmission Problems, Moscow. Since 2018 Vladislav has been a senior engineer at Huawei Technologies R&D department in Moscow. His research interests include coding theory, information theory, combinatorics and algorithms.

Ilya Vorobyev received the M.Sc. degree in Mathematics and the Ph.D. degree in Mathematics from the Lomonosov Moscow State University in 2013 and 2017, respectively. In 2015–2017 he worked as a research engineer at Huawei R&D department in Moscow. He also was a researcher at the Institute for Information Transmission Problems, Moscow, in 2015–2017. Since 2017 Ilya has been a senior researcher in the Advanced Combinatorics and Complex Networks Lab, Moscow Institute of Physics and Technology. Since 2018 he has been a research scientist in the Center for Computational and Data-Intensive Science and Engineering, Skolkovo Institute of Science and Technology. His research interests include extremal combinatorics and coding theory.

Separable Codes for the Symmetric Multiple-Access Channel

Arkadii D'yachkov, Nikita Polyanskii, Vladislav Shchukin, and Ilya Vorobyev

***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 the 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.**

***Index Terms*— 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 (the B–MAC) and without (the A–MAC) intensity information. Using a well-known terminology [2] of the combinatorial coding theory, we describe the A–MAC and the B–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* [3] 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 the s elements of the first s-tuple differs from the union of the s elements of the second s-tuple*.
- s-*separable* [4] code for the B–MAC if for any two distinct s-tuples of the codewords there exists a coordinate i, $1 \le i \le N$, in which *the type (or the composition) of the first s-tuple differs from the type of the second s-tuple*.
- $(\le s)$-*separable* [3] 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 the k elements of the k-tuple differs from the union of the m elements of the m-tuple*.
- s-*frameproof* code [5] 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 the s elements of the s-tuple*.
- s-*hash* code [6], [7] 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 are all different.

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

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

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

Multimedia fingerprinting is a technique to trace the sources of pirate copies of copyrighted multimedia contents. Separable codes for the A–MAC were introduced in [3] as an efficient tool to construct codes for multimedia fingerprinting in the context of "averaging attack". Due to its importance, constructions, applications and bounds on the rate of separable codes were further investigated and discussed in papers [8]–[11].

Other security models and applications related to separable codes have been considered, and various classes of codes were defined in the literature. We only mention the most significant one and refer the reader to [5], where the problem of preventing an adversary from framing an innocent user was addressed, and the definition of frameproof codes was given. The latter were studied extensively in [3] and [12]–[17].

One important concept, which generalizes the definition of frameproof codes, is called (s, s')-separating codes [14], [18]

Manuscript received August 24, 2017; revised August 1, 2018; accepted December 23, 2018. A. D'yachkov, V. Shchukin, and I. Vorobyev were supported by the Russian Foundation for Basic Research under Grant 16-01-00440 a. N. Polyanskii was supported in part by the Russian Foundation for Basic Research under Grant 16-01-00440-a and in part by the Israel Science Foundation under Grant 1162/15 and Grant 326/17.

A. D'yachkov is with the Department of Probability Theory, Faculty of Mechanics and Mathematics, Lomonosov Moscow State University, 119991 Moscow, Russia (e-mail: agd-msu@yandex.ru).

N. Polyanskii is with the Skolkovo Institute of Science and Technology, 121205 Moscow, Russia, and also with the Israel Institute of Technology, Haifa 32000, Israel (e-mail: nikitapolyansky@gmail.com).

V. Shchukin is with the Institute for Information Transmission Problems, 127051 Moscow, Russia (e-mail: vpike@mail.ru).

I. Vorobyev is with the Skolkovo Institute of Science and Technology, 121205 Moscow, Russia, and also with the Moscow Institute of Physics and Technology, 141701 Dolgoprudny, Russia (e-mail: vorobyev.i.v@yandex.ru).

Communicated by A. G. Dimakis, Associate Editor for Coding Techniques.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2019.2893234

not to be confused with the definition of s-separable codes. For this kind of codes, we require the property that for any disjoint s-tuple and s'-tuple of codewords, there exists a coordinate, in which the symbols of the s-tuple are disjoint with the symbols of the s'-tuple. The most fundamental applications of (s, s')-separating codes (with $s \neq s' \geq 2$) are connected with automata synthesis [19], a key distribution problem in cryptography [20] and a problem in molecular biology [21].

Finally, hash codes have undergone study due to their applications in information retrieval, cryptography and algorithms. Different problems on hash codes were considered and developed in [6], [7], [22], and [23].

Recall the well-known results emphasizing the connection between separable codes, hash codes and frameproof codes, namely: the inequalities

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

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

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

The first and the second inequalities in (1) are simple reformulations of the corresponding evident properties of binary superimposed codes [24], [25]. The third inequality in (1) is trivially implied from the definitions. The upper bound for frameproof codes in (2) is given in [26] and is based on the same idea as an upper bound for hash codes [23], [27]. The asymptotic lower bound in (2) is an obvious corollary of the random coding lower bound proved in [6] and [28]. From (1) and (2) it follows the asymptotic (s-fixed and $q \to \infty$) equalities:

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

Moreover, recent papers [9], [10] contain proofs of the asymptotic (s-fixed and $q \to \infty$) equalities:

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

Unlike (3) and (4), the similar asymptotic behavior of the rates $R^{(A)}(s, q)$ and $R^{(B)}(s, q)$ of s-separable codes for the A–MAC and the B–MAC is unknown at present. The aim of our paper is a further development and generalization of the given open problems.

B. Outline

The remainder of the paper is organized as follows. After introducing notations, in Section II, we give a general definition of the noiseless symmetric MAC (the f-MAC) along with the corresponding definition of an s-separable code for the f-MAC, and describe five models of the f-MACs, which are important for applications. In Section III, we speculate about an information-theoretic upper bound, called an *entropy* bound, on the rate of s-separable codes for the f-MAC and discuss the known and new improvements of the entropy bound. In particular, a combinatorial upper bound on $R^{(B)}(s, q)$ is given by Theorem 1. In Section IV, new asymptotic (s-fixed, $q \to \infty$) random coding lower bounds on the rates $R^{(A)}(s, q)$ and $R^{(B)}(s, q)$ are presented by Theorem 2 and Theorem 3, respectively. In Section V, we introduce the concept of list-decoding codes for the A–MAC and obtain an upper bound on the rate of these codes, matching with the known lower bound for very large alphabet size q. Based on a simple connection between list-decoding codes and s-separable codes, we also derive an upper bound on $R^{(A)}(s, q)$, given by Theorem 6. Finally, in the Appendix, we introduce the Shannon concept of an error probability for the f-MAC and investigate the logarithmic asymptotics of the standard random coding upper bounds on the error probability. The obtained results lead us to some non-asymptotic random coding lower bounds on the rate of s-separable codes for the symmetric f–MAC.

In particular, as new results we claim the following.

Theorem 1: For any $s \geq 2$ and $q \geq 2$, the rate of s-separable q-ary codes for the B–MAC satisfies the inequality

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

Theorem 2: If $s \geq 2$ is fixed and $q \to \infty$, then the rate $R^{(B)}(s, q)$ satisfies the asymptotic inequality

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

Theorem 3: If $s \geq 2$ is fixed and $q \to \infty$, then the rate $R^{(A)}(s, q)$ satisfies the asymptotic inequality

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

Theorem 6: For any $s \geq 2$ and $q \geq 2$, the rate of s-separable q-ary codes for the A–MAC satisfies the inequality

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

II. Statement of the Problem

A. Notations

Let q, N, t, s and L be integers, where $q \geq 2$, $N \geq 2$, $2 \leq s < t/2$, $1 \leq L \leq t - s$. Let symbol $\triangleq$ denote equality by definition, $\mathcal{A}_q \triangleq \{0, 1, \ldots, q-1\}$ be the standard q-ary alphabet, $[N] \triangleq \{1, 2, \ldots, N\}$ be the set of integers from 1 to N, $|A|$ be the size of the set A, $[b]^+ \triangleq \max\{0; b\}$ be the positive part of 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*) $\boldsymbol{x}(j) \triangleq (x_1(j), \ldots, x_N(j))$, $j \in [t]$, and N rows $\boldsymbol{x}_i \triangleq (x_i(1), \ldots, x_i(t))$, $i \in [N]$, is called a *q-ary code of length N and size t*.

For any fixed q-ary vector $\boldsymbol{x} = (x_1, \ldots, x_s) \triangleq x_1^s \in \mathcal{A}_q^s$, define the integer vector $\left(s_0, s_1, \ldots, s_{q-1}\right)$ 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

$\left(s_0, \ldots, s_{q-1}\right)$ is said to be a *type* (or, *composition*) of the q-ary vector $x_1^s \in \mathcal{A}_q^s$ or, briefly,

$$T\left(x_1^s\right) \triangleq \left(s_0, \ldots, s_{q-1}\right). \tag{5}$$

Introduce the standard symbols 2^Y and $\binom{[t]}{s}$ to denote the set of all subsets of a set Y and the set of all subsets of size s of the set $[t]$. By definition, the union $U(x_1^s)$ of the q-ary vector $x_1^s \in \mathcal{A}_q^s$ is

$$U(x_1^s) \triangleq \bigcup_{i\in[s]} x_i \in 2^{\mathcal{A}_q}. \tag{6}$$

For any $\mathbf{e} = \{e_1, \ldots, e_s\} \in \binom{[t]}{s}$, called a *message*, and a code X, consider the non-ordered s-collection of codewords

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

We say that $\boldsymbol{x}(\mathbf{e})$ *encodes* the message $\mathbf{e}$.

B. The Symmetric Multiple-Access Channel

We use the terminology of the noiseless (deterministic) *multiple-access channel* (MAC), which has s inputs and one output [2]. Let all s input alphabets of MAC be the same and coincide with the alphabet $\mathcal{A}_q = \{0, 1, \ldots, q-1\}$. 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

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

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

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

Remark 1: Note that to determine 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 $(s_0, s_1, \ldots, s_{q-1}) = T(x_1^s)$, $x_1^s \in \mathcal{A}_q^s$, or, in other terms, on multisets of cardinality s (s-collections) over $\mathcal{A}_q$.

In what follows, we consider the symmetric f–MAC only.

C. Separable Codes

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

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

On the base of the code X and N signals

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

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.

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

$$R^{(f)}(s, q) \triangleq \overline{\lim_{N\to\infty}} \frac{\ln t^{(f)}(s, q, N)}{N}, \tag{9}$$

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

D. Examples of the Symmetric f-MAC

1) The A–MAC: The A–MAC is described by the function

$$z = f(x_1^s) \triangleq U(x_1^s) \subseteq \mathcal{A}_q,$$

where the union function $U(x_1^s)$ of a vector x_1^s is given in (6). For instance, if $s = 4$ and $q = 3$, then

$$U(0, 0, 1, 1) = \{0, 1\}, \quad U(1, 1, 0, 2) = \{0, 1, 2\}.$$

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 $|Z| = 2^q - 1$.

2) The B–MAC: The B–MAC known also as the *compositional* channel is described by the function

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

where the type function $T(x_1^s)$ of a vector x_1^s is defined by (5). For instance, if $s = 4$ and $q = 3$, then

$$T(0, 0, 1, 1) = (2, 2, 0), \quad T(1, 1, 0, 2) = (1, 2, 1).$$

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.

3) The Erasure MAC: A q-ary 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.

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

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

where terms of the sum are considered as 0 and 1 elements of the ring of integers $\mathbb{Z}$. Separable codes for the ℓ-*thr*–MAC are connected with some *compressed genotyping* [29] models arising in the molecular biology.

5) The 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

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

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* [30] and the information-theoretic model called the *design of screening experiments* [31].

III. Improvements of the Entropy Bound

In this section, we first give a general statement called the entropy bound on the rate of separable codes for any symmetric MAC. For an asymptotic regime $s \to \infty$, we recall the best known bounds on the rate of separable codes for the disjunctive, the erasure, the threshold, the A and the B MACs in Sections III-B-III-F, respectively. Finally, in Section III-G, we present Theorem 1, a novel upper bound, which holds for any symmetric MAC and improves the entropy bound.

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

Let $\boldsymbol{p} \triangleq \{p(a), a \in \mathcal{A}_q\}$, where $0 \le p(a) \le 1, a \in \mathcal{A}_q$, and $\sum_{a \in \mathcal{A}_q} p(a) = 1$, be a fixed probability distribution on the q-ary alphabet $\mathcal{A}_q$, and a multinomial random vector $\xi_1^s \triangleq (\xi_1, \ldots, \xi_s) \in \mathcal{A}_q^s$ is the collection of s *independent* random variables having the same distribution $\boldsymbol{p}$, i.e., $\Pr\{\xi_k = a\} \triangleq p(a), k \in [s], a \in \mathcal{A}_q$. If the random vector ξ_1^s is interpreted as s signals at s *independent* inputs of the symmetric f–MAC, then the output Shannon entropy $H_{\boldsymbol{p}}^{(f)}(s, q)$ is defined [2] as

$$H_{\boldsymbol{p}}^{(f)}(s, q) \triangleq \sum_{z \in Z} \Pr\{f\left(\xi_1^s\right) = z\} \cdot \ln \frac{1}{\Pr\{f\left(\xi_1^s\right) = z\}},$$

$$\Pr\{\xi_1^s = a_1^s\} \triangleq \prod_{k=1}^{s} \Pr\{\xi_k = a_k\} \triangleq \prod_{k=1}^{s} p(a_k). \qquad (10)$$

Remark 2: Remark 1 and the well-known maximization property [2] of the Shannon entropy imply that for any symmetric f-MAC and any probability distribution $\boldsymbol{p}$, the entropy function $H_{\boldsymbol{p}}^{(f)}(s, q)$ satisfies the inequalities

$$H_{\boldsymbol{p}}^{(f)}(s, q) \le H_{\boldsymbol{p}}^{(B)}(s, q) \le \ln \binom{s+q-1}{q}, \qquad (11)$$

where we took into account that for the B-MAC, the output alphabet size $|Z| = \binom{s+q-1}{q}$.

Proposition 1 [32]–[34]: The rate of s-separable q-ary codes for the symmetric f–MAC satisfies the inequality

$$R^{(f)}(s, q) \le \overline{C}^{(f)}(s, q) \triangleq \frac{\max_{\boldsymbol{p}} H_{\boldsymbol{p}}^{(f)}(s, q)}{s}. \qquad (12)$$

The foregoing statement is based on the subadditive property [2] of the Shannon entropy and, hereinafter, the function $\overline{C}^{(f)}(s, q)$ defined by (10) and (12) is said to be an *entropy bound* for the f–MAC.

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

One can check [33] that the entropy bound of the $disj$–MAC is $\overline{C}^{(disj)}(s, 2) = \ln 2/s$ and the maximum in the right-hand side of (12) is attained at the distribution $\boldsymbol{p}$ with probabilities $p(0) = 2^{-1/s}$ and $p(1) = 1 - 2^{-1/s}$. Some significant results, improving the entropy bound $R^{(disj)}(s, 2) \le \ln 2/s$, were obtained in [35] for $s = 2$ and in [36] for $s \ge 11$. In addition, we refer to the best known asymptotic ($s \to \infty$) lower [31] and upper [36] bounds on the rate $R^{(disj)}(s)$:

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

where the lower bound is based on Proposition 5 formulated in the Appendix.

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 [37] that the entropy bound of the $eras$–MAC is $\overline{C}^{(eras)}(s, 2) \sim \ln 2/s$ and the maximum in the right-hand side of (12) is asymptotically attained at distribution $\boldsymbol{p}$ with $p(1) \sim \ln 2/s$ or with $p(0) \sim \ln 2/s$. In addition, we mention the best known asymptotic ($s \to \infty$) lower [38] and upper [31] 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: We conjecture that the enropy bound of the $eras$–MAC does not depend on $q \ge 2$, i.e.,

$$\overline{C}^{(eras)}(s, q) = \overline{C}^{(eras)}(s, 2), \quad s \ge 2, \ q \ge 2.$$

D. Bounds on the Rate $R^{(\ell\text{-}thr)}(s)$ 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 [39] and [40]:

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

E. Bounds on the Rate $R^{(A)}(s, q)$ for the A–MAC

For fixed q and $s \to \infty$, the best known upper bounds on the rate $R^{(A)}(s, q)$ are based on the upper bound for $R^{(disj)}(s, 2)$ and improve the entropy bound. The asymptotic ($s \to \infty$) lower and upper bounds were established in [38]

$$\frac{(q-1)}{s^2 \log_2^2 e}(1 + o(1)) \le R^{(A)}(s, q) \le \frac{4(q-1) \ln s}{s^2}(1 + o(1)).$$

F. Bounds on the Rate $R^{(B)}(s, q)$ for the B–MAC

For fixed q and $s \to \infty$, the best known lower and upper bounds on the rate $R^{(B)}(s, q)$ were given in [32] and [41] (case $q = 2$) and in [1] and [4] (case $q > 2$)

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

G. Combinatorial Upper Bound for the Symmetric MAC

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

Theorem 1: For any symmetric f–MAC and $s \ge 2$, $q \ge 2$, the rate satisfies the inequality

$$R^{(f)}(s,q) \overset{(a)}{\le} R^{(B)}(s,q)$$
$$\le \overline{R}^{(B)}(s,q) \triangleq \begin{cases} \frac{s+1}{2s}\ln q, & \text{if } s \text{ is odd},\\ \frac{s+2}{2(s+1)}\ln q, & \text{if } s \text{ is even}. \end{cases} \tag{13}$$

The inequality (a) is evidently implied by Remark 1 because any s-separable code for the given symmetric f–MAC is an s-separable code for the B–MAC as well. For the B–MAC, the maximization problem in the right-hand side of (12) was firstly solved in [42]. Mateev [42] proved that the maximum is attained at the uniform distribution $p(a) = 1/q, a \in \mathcal{A}_q$, and the entropy bound $\overline{C}^{(B)}(s,q)$ is

$$\overline{C}^{(B)}(s,q) = \frac{1}{s}\sum_{\sum s_i = s} \frac{s!}{s_0!\dots s_{q-1}!}\frac{1}{q^s}\ln\left(\frac{s_0!\dots s_{q-1}!}{s!/q^s}\right).$$

Applying the foregoing formula, one can easily check that for any $s \ge 2$ and $q \ge 2$,

$$\overline{C}^{(B)}(s,q) \ge \frac{1}{s}(\ln q^s - \ln s!) = \ln q - \frac{\ln s!}{s}. \tag{14}$$

Observe that the general bound (11) yields the upper bound

$$\overline{C}^{(B)}(s,q) \le \frac{1}{s}\ln\binom{s+q-1}{s} < \ln(q+s-1) \tag{15}$$

From Theorem 1 and inequalities (14)-(15), it follows

Corollary 1: If $s \ge 2$ is fixed and $q \to \infty$, then the entropy bound for the B-MAC $\overline{C}^{(B)}(s,q) \sim \ln q$, i.e., the upper bound $\overline{R}^{(B)}(s,q)$ defined in the left-hand side of (13) asymptotically improves the entropy bound $\overline{C}^{(B)}(s,q)$. In addition, for any $s \ge 2$ and $q > (s!)^{2/(s-1)}$, the rate $R^{(B)}(s,q)$ of s-separable codes for the B-MAC satisfies the strict inequality $R^{(B)}(s,q) < \overline{C}^{(B)}(s,q)$.

Remark 3: If $s \ge 2$ is fixed and $q \to \infty$, then we do not know any asymptotic results about the entropy bound $\overline{C}^{(A)}(s,q)$ for the A-MAC which are similar to the results described in Corollary 1 for the B-MAC.

Proof of Theorem 1: Fix an arbitrary q-ary $(N \times t)$-code X. For any α, $0 < \alpha < 1$, without loss of generality, we may assume that all codewords from X are distinct and the length N can be represented as a sum of two integers αN and $(1-\alpha)N$. Given X, introduce the bipartite graph

$$G = G(X) = (V,E) \triangleq (V_1 \cup V_2, E),$$
$$|V_1| = q^{\alpha N}, \quad |V_2| = q^{(1-\alpha)N},$$

defined as follows. Let the vertices in V_1 and V_2 correspond to distinct q-ary vectors of length αN and $(1-\alpha)N$, respectively. Two vertices $v_1 \in V_1$ and $v_2 \in V_2$ are connected with an edge if and only if the code X contains a codeword of length $N = \alpha N + (1-\alpha)N$ which is the concatenation of two q-ary vectors corresponding to v_1 and v_2. Thus, we obtain the graph $G(X)$ having $|V| = q^{(1-\alpha)N} + q^{\alpha N}$ vertices and t edges, identified by the indexes $[t]$ of the code X. In addition, any message $\mathbf{e} \in \binom{[t]}{s}$ is interpreted as a non-ordered s-collection of edges.

Let X be a q-ary s-separable code for the B-MAC. Now we shall prove that there is no short cycle in $G(X)$. Suppose, seeking a contradiction, that there exists a simple cycle $C_{2\ell}$ of length $2\ell \le 2s$ in $G(X)$. Enumerate edges in $C_{2\ell}$ by $e_1, \dots, e_{2\ell}$, where e_i and e_{i+1} are adjacent for any $i \in [2\ell - 1]$ (e_1 and $e_{2\ell}$ are also adjacent). Define the set E_1 as $\{e_1, e_3, \dots, e_{2\ell-1}\}$, and let E_2 be the remaining edges of the cycle. Consider an arbitrary subset $\mathcal{S} \subset [t] \setminus \{E_1 \cup E_2\}$ of the size $|\mathcal{S}| = s - \ell$ and define two messages $\mathbf{e}_i \triangleq E_i \cup \mathcal{S} \in \binom{[t]}{s}$, $i = 1, 2$. It is easy to check that outputs of the B-MAC for these messages are the same, i.e., $z^{(B)}(\mathbf{e}_1, X) = z^{(B)}(\mathbf{e}_2, X)$. This contradicts to Definition 2.

It is known (e.g., see [43]) that if a bipartite graph with two parts of sizes n and m does not contain any simple cycle of length $\le 2s$, then the number t of its edges is

$$t \le \begin{cases} (2s-3)\left((mn)^{\frac{s+1}{2s}} + m + n\right), & \text{if } s \text{ is odd},\\ (2s-3)\left(m^{\frac{s+2}{2s}} n^{1/2} + m + n\right), & \text{if } s \text{ is even}. \end{cases}$$

For odd s, we obtain

$$t \le (2s-3)\left[q^{N\frac{s+1}{2s}} + q^{\alpha N} + q^{(1-\alpha)N}\right]$$
$$\le 3(2s-3)q^{N\max\left\{\frac{s+1}{2s},\alpha,(1-\alpha)\right\}}.$$

Taking $\alpha = 1/2$, we derive

$$t \le 3(2s-3)q^{\frac{s+1}{2s}N},$$

and the rate is upper bounded as in (13). Applying the second inequality for even s, we have

$$t \le (2s-3)\left[q^{\frac{N}{2}(1+\frac{2\alpha}{s})} + q^{\alpha N} + q^{(1-\alpha)N}\right]$$
$$\le 3(2s-3)q^{N\max\left\{\frac{s+2\alpha}{2s},\alpha,1-\alpha\right\}}.$$

Taking α as a root of the equality $\frac{s+2\alpha}{2s} = 1-\alpha$, i.e., $\alpha = \frac{s}{2(s+1)}$, we obtain

$$t \le 3(2s-3)q^{\frac{s+2}{2(s+1)}N},$$

i.e., the rate satisfies (13). □

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

In this section, we apply the random coding method to construct the asymptotic (s-fixed, $q \to \infty$) lower bounds on the rate of s-separable q-ary codes for the A–MAC and the B–MAC.

Before deriving the bounds, let us introduce some auxiliary notations. Notation $2^{(\mathcal{A}_q,N)}$ stands for the Cartesian product of N copies of $2^{\mathcal{A}_q}$, where $2^{\mathcal{A}_q}$ is the set of all subsets of $\mathcal{A}_q$. For a collection of codewords $V = \{\boldsymbol{x}(i_1), \dots, \boldsymbol{x}(i_s)\} \subset \mathcal{A}_q^N$, by $T(V)$ we abbreviate the q-ary $(N \times q)$ matrix

$$T(V) \triangleq (T(x_1(i_1), \dots, x_1(i_s)), \dots, T(x_N(i_1), \dots, x_N(i_s)))^T, \tag{16}$$

and we define the vector $U(V)$ from $2^{(\mathcal{A}_q, N)}$ as follows

$$U(V) \triangleq (U(x_1(i_1), \dots, x_1(i_s)), \dots, U(x_N(i_1), \dots, x_N(i_s)))^T. \tag{17}$$

A. Random Coding Lower Bound on $R^{(B)}(s, q)$

An asymptotic ($q \to \infty$) random coding lower bound on the rate of s-separable q-ary codes for the B–MAC is given by

Theorem 2: If $s \geq 2$ is fixed and $q \to \infty$, then the rate $R^{(B)}(s, q)$ satisfies the asymptotic inequality

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

Proof of Theorem 2: Consider the ensemble of matrices $X = (x_i(j))$, where entries $x_i(j)$, $i \in [N]$, $j \in [t]$, are chosen independently and uniformly at random from the alphabet $\mathcal{A}_q$. Define a *bad* event B_j: "there exist two distinct messages $\mathbf{e} \neq \hat{\mathbf{e}}$ from $\binom{[t]}{s}$ so that $j \in \mathbf{e}$, $j \notin \hat{\mathbf{e}}$ and $T(\boldsymbol{x}(\mathbf{e})) = T(\boldsymbol{x}(\hat{\mathbf{e}}))$", where the matrix $T(\cdot)$ is defined by (16). To establish the existence of an s-separable q-ary code for the B–MAC, we shall upper bound the probability of the bad event by

$$\begin{aligned}
\Pr\{B_j\} &= \Pr\left\{ \bigcup_{\substack{\mathbf{e}, \hat{\mathbf{e}} \in \binom{[t]}{s} \\ j \in \mathbf{e}, j \notin \hat{\mathbf{e}}}} T(\boldsymbol{x}(\mathbf{e})) = T(\boldsymbol{x}(\hat{\mathbf{e}})) \right\} \\
&\overset{(a)}{\leq} s \max_{m \in [s]} \Pr\left\{ \bigcup_{\substack{\mathbf{e}, \hat{\mathbf{e}} \in \binom{[t]}{s}, j \in \mathbf{e} \\ |\mathbf{e} \cap \hat{\mathbf{e}}| = s-m, j \notin \hat{\mathbf{e}}}} T(\boldsymbol{x}(\mathbf{e})) = T(\boldsymbol{x}(\hat{\mathbf{e}})) \right\} \\
&\overset{(b)}{=} s \max_{m \in [s]} \Pr\left\{ \bigcup_{\substack{\mathbf{e}, \hat{\mathbf{e}} \in \binom{[t]}{m}, j \in \mathbf{e} \\ \mathbf{e} \cap \hat{\mathbf{e}} = \emptyset}} T(\boldsymbol{x}(\mathbf{e})) = T(\boldsymbol{x}(\hat{\mathbf{e}})) \right\} \\
&\overset{(c)}{\leq} s \max_{m \in [s]} t^{2m-1} \Pr\left\{ \substack{T(\boldsymbol{x}(\mathbf{e})) = T(\boldsymbol{x}(\hat{\mathbf{e}})) \\ \text{for some } \mathbf{e}, \hat{\mathbf{e}} \in \binom{[t]}{m} \\ \mathbf{e} \cap \hat{\mathbf{e}} = \emptyset} \right\} \\
&\overset{(d)}{=} s \max_{m \in [s]} t^{2m-1} \left(\Pr\{T(u_1^m) = T(v_1^m)\}\right)^N,
\end{aligned}$$

where inequality (a) is implied by

$$\Pr\left\{ \bigcup_{m=1}^{s} C_i \right\} \leq s \max_{m \in [s]} \Pr\{C_i\},$$

equality (b) is followed by the fact

$$T(V_1) = T(V_2) \iff T(V_1 \setminus V_2) = T(V_2 \setminus V_1),$$

inequality (c) is an evident consequence of the union bound since the number of ways to choose a pair $\mathbf{e}, \hat{\mathbf{e}}$ with the property required is $\binom{t}{2m-1}\binom{2m-1}{m-1} \leq t^{2m-1}$, and $\{u_i, v_i\}|_{i=1}^m$ in the last equality (d) are independent random variables having the uniform distribution on the set $\mathcal{A}_q$. Let us estimate the probability that two random m-tuples have the same type

$$\begin{aligned}
\Pr\left\{T\left(u_1^m\right) = T\left(v_1^m\right)\right\} &= \Pr\left\{ \bigcup_{\pi \in S_m} \left[\bigcap_{k=1}^{m} \left(u_k = v_{\pi(i)}\right) \right] \right\} \\
&\leq m! \cdot \Pr\left\{ \bigcap_{k=1}^{m} \left(u_k = v_{\pi(k)}\right) \right\} = \frac{m!}{q^m}.
\end{aligned}$$

Therefore,

$$\Pr\{B_j\} \leq s \max_{m \in [s]} t^{2m-1} (m!/q^m)^N.$$

Since $\Pr\{B_j\}$ does not depend on $j \in [t]$, we deduce that if the upper bound given above is less than $1/2$, then there exists an s-separable q-ary code for the B–MAC of size $t/2$ and length N. Thus, the lower bound on $R^{(B)}(s, q)$ is as follows

$$R^{(B)}(s, q) \geq \min_{m \in [s]} \frac{m \ln q - \ln m!}{2m - 1}.$$

This leads to the statement of Theorem 2. □

B. Random Coding Lower Bound on $R^{(A)}(s, q)$

Now we establish an asymptotic random coding lower bound on the rate of s-separable q-ary codes for the A–MAC which is presented by

Theorem 3: If $s \geq 2$ is fixed and $q \to \infty$, then the rate $R^{(A)}(s, q)$ satisfies the asymptotic inequality

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

Proof of Theorem 3: Consider the ensemble of matrices $X = (x_i(j))$, where entries $x_i(j)$, $i \in [N]$, $j \in [t]$, are chosen independently and uniformly at random from the alphabet $\mathcal{A}_q$. Define a *bad* event A_j: "there exist two distinct messages $\mathbf{e} \neq \hat{\mathbf{e}}$ from $\binom{[t]}{s}$ so that $j \in \mathbf{e}$, $j \notin \hat{\mathbf{e}}$ and $U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}}))$", where the vector $U(\cdot) \in 2^{(\mathcal{A}_q, N)}$ is defined by (17). To establish the existence of an s-separable q-ary code for the A–MAC, we shall upper bound the probability of the bad event by

$$\begin{aligned}
\Pr\{A_j\} &= \Pr\left\{ \bigcup_{\substack{\mathbf{e}, \hat{\mathbf{e}} \in \binom{[t]}{s} \\ j \in \mathbf{e}, j \notin \hat{\mathbf{e}}}} U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}})) \right\} \\
&\overset{(a)}{\leq} s \max_{m \in [s]} \Pr\left\{ \bigcup_{\substack{\mathbf{e}, \hat{\mathbf{e}} \in \binom{[t]}{s}, j \in \mathbf{e} \\ |\mathbf{e} \cap \hat{\mathbf{e}}| = s-m, j \notin \hat{\mathbf{e}}}} U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}})) \right\} \\
&\overset{(b)}{\leq} s \max\left(\Pr\{C_1\}, \max_{m \in \{2, \dots, s\}} t^{s+m-1} \Pr\{P_m\} \right),
\end{aligned}$$

where C_m and P_m are defined as follows

$$C_m \triangleq \left\{ \bigcup_{\substack{\mathbf{e},\hat{\mathbf{e}}\in\binom{[t]}{s},\, j\in\mathbf{e}\\ |\mathbf{e}\cap\hat{\mathbf{e}}|=s-m,\, j\notin\hat{\mathbf{e}}}} U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}})) \right\},$$

$$P_m \triangleq \left\{ \underset{\substack{\text{for some } \mathbf{e},\hat{\mathbf{e}}\in\binom{[t]}{s}\\ |\mathbf{e}\cap\hat{\mathbf{e}}|=s-m}}{U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}}))} \right\}.$$

Inequality (a) is implied by the evident inequality

$$\Pr\left\{\bigcup_{m=1}^{s} C_m\right\} \le s \max_{m\in[s]} \Pr\{C_m\},$$

inequality (b) is followed by

$$\max_{m\in[s]} \Pr\{C_m\} = \max\left(\Pr\{C_1\}, \max_{m\in\{2,\ldots,s\}} \Pr\{C_m\}\right)$$

and the union bound, which was applied for the cases $m \ge 2$. Now let us further estimate $\Pr\{P_m\}$ by

$$\Pr\{P_m\} = \prod_{i=1}^{N} \Pr\left\{ \underset{\substack{\text{for some } \mathbf{e},\hat{\mathbf{e}}\in\binom{[t]}{s}\\ |\mathbf{e}\cap\hat{\mathbf{e}}|=s-m}}{\bigcup_{k=1}^{s} x_i(e_k) = \bigcup_{j=1}^{s} x_i(\hat{e}_j)} \right\} \overset{(c)}{\le} \frac{s^{mN}}{q^{mN}}. \quad (18)$$

To prove (c) in the last inequality, we employ the following fact. Suppose $\xi_1, \ldots, \xi_{m+s}$ are independent random variables distributed uniformly over $\mathcal{A}_q$. Then

$$\Pr\left\{\bigcup_{k=1}^{s} \xi_k = \bigcup_{j=m+1}^{m+s} \xi_j\right\} \le \Pr\left\{\bigcup_{k=1}^{m} \xi_k \subset \bigcup_{i=m+1}^{m+s} \xi_i\right\}$$
$$\le \left(\Pr\left\{\xi_1 \in \bigcup_{i=m+1}^{m+s} \xi_i\right\}\right)^m \le \frac{s^m}{q^m}.$$

As for $\Pr\{C_1\}$, we obtain its upper bound in a different way. Let E_j consist of all possible pairs $(\mathbf{e}, \hat{\mathbf{e}})$ so that $\mathbf{e}, \hat{\mathbf{e}} \in \binom{[t]}{s}$, $j \in \mathbf{e}$, $j \notin \hat{\mathbf{e}}$ and $|\mathbf{e} \cap \hat{\mathbf{e}}| = s-1$. Since $|\mathbf{e} \cap \hat{\mathbf{e}}| = s-1$, there exists $\hat{j} \in [t]$ such that $\mathbf{e} = \{j\} \cup \{\mathbf{e} \cap \hat{\mathbf{e}}\}$ and $\hat{\mathbf{e}} = \{\hat{j}\} \cup \{\mathbf{e} \cap \hat{\mathbf{e}}\}$. For a real parameter a, $0 < a < 1$, we represent the event $\{U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}}))\}$ as a disjoint union of two events. For the first one, we additionally require the Hamming distance $d_H(\cdot)$ between $\boldsymbol{x}(j)$ and $\boldsymbol{x}(\hat{j})$ to be at least aN, i.e., $A_j(\mathbf{e}, \hat{\mathbf{e}}, \ge a) \triangleq \{U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}})), d_H(\boldsymbol{x}(j), \boldsymbol{x}(\hat{j})) \ge aN\}$. The remaining one is $A_j(\mathbf{e}, \hat{\mathbf{e}}, < a) \triangleq \{U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}})), d_H(\boldsymbol{x}(j), \boldsymbol{x}(\hat{j})) < aN\}$. Then we deal with each event individually. More concretely, $\Pr\{C_1\}$ is upper bounded by

$$\Pr\left\{\bigcup_{(\mathbf{e},\hat{\mathbf{e}})\in E_j} A_j(\mathbf{e}, \hat{\mathbf{e}}, \ge a)\right\} + \Pr\left\{\bigcup_{(\mathbf{e},\hat{\mathbf{e}})\in E_j} A_j(\mathbf{e}, \hat{\mathbf{e}}, < a)\right\}$$
$$\le t^s \Pr\left\{\underset{\text{for some } (\mathbf{e},\hat{\mathbf{e}})\in E_j}{A_j(\mathbf{e}, \hat{\mathbf{e}}, \ge a)}\right\} + t \Pr\{d_H(\boldsymbol{x}(j), \boldsymbol{x}(\hat{j})) < aN\},$$

where the inequality is implied by the union bound, and $\hat{j} \in [t]$, $\hat{j} \ne j$. For simplicity of notation let us assume that aN is an integer. Let us estimate the probability that two random q-ary vectors of length N have the Hamming distance at most aN

$$\Pr\{d_H(\boldsymbol{x}(j), \boldsymbol{x}(\hat{j})) < aN\}$$
$$= \sum_{i=0}^{aN-1} \Pr\{d_H(\boldsymbol{x}(j), \boldsymbol{x}(\hat{j})) = i\}$$
$$= \sum_{i=N-aN+1}^{N} \binom{N}{i} \left(\frac{1}{q}\right)^i \left(1 - \frac{1}{q}\right)^{N-i} < \frac{2^N}{q^{(1-a)N}}.$$

Now, for any $(\mathbf{e}, \hat{\mathbf{e}}) \in E_j$, we proceed with the event $A_j(\mathbf{e}, \hat{\mathbf{e}}, \ge a) = \{U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}})), d_H(\boldsymbol{x}(j), \boldsymbol{x}(\hat{j})) \ge aN\}$ as follows

$$\Pr\{A_j(\mathbf{e}, \hat{\mathbf{e}}, \ge a)\}$$
$$\overset{(d)}{=} \sum_{i=aN}^{N} \Pr\left\{U(\boldsymbol{x}(\mathbf{e})) = U(\boldsymbol{x}(\hat{\mathbf{e}})) \middle| d_H(\boldsymbol{x}(j), \boldsymbol{x}(\hat{j})) = i\right\}$$
$$\times \Pr\left\{d_H(\boldsymbol{x}(j), \boldsymbol{x}(\hat{j})) = i\right\}$$
$$\overset{(e)}{\le} \sum_{i=0}^{N-aN} \binom{N}{i} \left(\frac{1}{q}\right)^i \left(1 - \frac{1}{q}\right)^{N-i}$$
$$\times \left(\frac{(s-1)^2}{q^2}\right)^{N-i} < \frac{\left(2s^2\right)^N}{q^{(1+a)N}}.$$

Equality (d) is derived by the law of total probability. To prove (e) in the last inequality, we use the following fact. Suppose $\xi_1, \ldots, \xi_{s+1}$ are independent random variables distributed uniformly over $\mathcal{A}_q$. Then

$$\Pr\left\{\bigcup_{k=1}^{s} \xi_k = \bigcup_{j=2}^{s+1} \xi_j, \xi_1 \ne \xi_{s+1}\right\}$$
$$\le \Pr\left\{\xi_1 \in \bigcup_{j=2}^{s} \xi_j, \xi_{s+1} \in \bigcup_{j=2}^{s} \xi_j\right\} \le \frac{(s-1)^2}{q^2}.$$

Therefore, we get

$$\Pr\{C_1\} \le \min_{0<a<1}\left(t^s \frac{\left(2s^2\right)^N}{q^{(1+a)N}} + t \frac{2^N}{q^{(1-a)N}}\right)$$
$$\le 2 \min_{0<a<1}\left(\max\left(\frac{t^s \left(2s^2\right)^N}{q^{(1+a)N}}, \frac{t\, 2^N}{q^{(1-a)N}}\right)\right).$$

Finally, summarizing the above arguments, we obtain

$$\Pr\{A_j\} \le 2s \max\left(\max_{m\in\{2,\ldots,s\}} \frac{t^{s+m-1} s^{mN}}{q^{mN}},\right.$$
$$\left.\min_{0<a<1}\left(\max\left(\frac{t^s \left(2s^2\right)^N}{q^{(1+a)N}}, \frac{t\, 2^N}{q^{(1-a)N}}\right)\right)\right).$$

Since $\Pr\{A_j\}$ does not depend on $j \in [t]$, we deduce that if the upper bound given above is less than $1/2$, then there exists an s-separable q-ary code for the A–MAC of size $t/2$

and length N. Thus, the asymptotic ($q \to \infty$) lower bound on $R^{(A)}(s,q)$ is as follows

$$R^{(A)}(s,q) \ge \min\left(\frac{2}{s+1}; \max_{0<a<1}\left(\min\left(\frac{1+a}{s}; 1-a\right)\right)\right)$$
$$\times \ln q(1+o(1)) = \frac{2}{s+1}\ln q(1+o(1)). \quad \square$$

Remark 4: It is worth noticing that if we upper bound $\Pr\{C_1\}$ like we estimate $\Pr\{P_m\}$ in (18), then we would get only $R^{(A)}(s,q) \ge \frac{1}{s}\ln q(1+o(1))$ as $q \to \infty$.

V. List Decoding Codes for the A–MAC

After giving definitions and notations, in Section V-A, we derive several useful properties establishing a connection between list-decoding codes for the A–MAC and separable codes for the A–MAC and a relation between list decoding codes over alphabets of different sizes. We recall the best known lower bounds on the rate of list-decoding codes in Section V-B. Finally, we present a new combinatorial upper bound on the rate of list-decoding codes in Section V-C, which also leads to an upper bound on the rate of separable codes for the A–MAC.

A. Notations and Definitions

Recall that $2^{(\mathcal{A}_q,N)}$ stands for the Cartesian product of N copies of $2^{\mathcal{A}_q}$, where $2^{\mathcal{A}_q}$ is the set of all subsets of $\mathcal{A}_q$. A vector $\mathcal{Q} = (\mathcal{Q}_1,\dots,\mathcal{Q}_N)^T \in 2^{(\mathcal{A}_q,N)}$ is said to *cover* a column $\boldsymbol{x} = (x_1,\dots,x_N)^T \in \mathcal{A}_q^N$ if $x_i \in \mathcal{Q}_i$ for all $i \in [N]$.

Definition 3 [38]: Given integers $s \ge 1$ and $L \ge 1$, a q-ary code X of size t and length N is said to be a *list-decoding* (s,L,q)*-code* of size t and length N if, for any s-collection of codewords $\{\boldsymbol{x}(j_1),\dots,\boldsymbol{x}(j_s)\}$, the vector $U(\boldsymbol{x}(j_1),\dots,\boldsymbol{x}(j_s))$, defined by (17), 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 [9]) is an $(\le s)$-separable q-ary code for the A–MAC. Moreover, list-decoding $(s,1,q)$-code provides a simple *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

$$\boldsymbol{z}^{(A)}(\mathbf{e},X) = U(\boldsymbol{x}(e_1),\dots,\boldsymbol{x}(e_s))$$
$$= \left(\bigcup_{m=1}^{s} x_1(e_m),\dots,\bigcup_{m=1}^{s} x_N(e_m)\right)^T.$$

In the general case $L \ge 1$, the algorithm provides a subset of $[t]$ that contains s elements of the message $\mathbf{e}$ and at most $L-1$ 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 of s-separable q-ary code for the A–MAC satisfies the inequality

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

Proposition 2 can be seen as a simple reformulation of the corresponding properties of binary list-decoding superimposed codes firstly introduced in [25]. A nontrivial recurrent inequality for the rate $R(s,L,q)$ of list-decoding (s,L,q)-codes is established by

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

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

Proof of Proposition 3: Assume that there exists a list-decoding (s,L,q')-code X' of length N and size t. Let $l \triangleq \lceil q'/(q-1)\rceil$. Consider a q-ary code C of length l and size $l(q-1) \ge q'$, which is composed from all possible codewords with one nonzero symbol:

$$\begin{vmatrix} 1 & 0 & \dots & 0 & \dots & q-1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 & q-1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \dots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & \dots & 0 & 0 & \dots & q-1 \end{vmatrix}$$

Let us consider an injective map $\phi : \mathcal{A}_{q'} \to C$ such that $\phi(i)$ is the $(i+1)$th codeword of C. To construct a q-ary code X of length lN and size t, we replace each symbol $a \in \mathcal{A}_{q'}$ in all codewords in X' by q-ary codeword $\phi(a)$. One can easily check that the code X is a list-decoding (s,L,q)-code. $\square$

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

In [38], applying Proposition 3 and random coding arguments, the author established the lower bound on the rate of list-decoding (s,L,q)-codes which can be formulated as

Theorem 4 [38, Th. 2]:

1. *For any fixed $q \ge 2$, $s \ge 2$ and $L \ge 1$ the following lower bound holds:*

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

where

$$P(q,s,L) \triangleq \sum_{m=1}^{\min(q,s)} \binom{q}{m}\left(\frac{m}{q}\right)^L$$
$$\times \sum_{k=0}^{m} (-1)^k \binom{m}{k}\left(\frac{m-k}{q}\right)^s,$$

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

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

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

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

$$\underline{R}(s,L,q) = \frac{L}{s+L-1}\ln q(1+o(1). \qquad (19)$$

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} [38] ^{3} [12] ^{4} [22]

The lower bound $\underline{R}(s, L, q)$ defined by Theorem 4 improves the best previously known bounds presented in [12], [22], and [37] in asymptotics (q is fixed, $s \to \infty$) and in a wide range of parameters (q, s, L) as well. Some numerical results and a comparison of bounds are presented in Table I.

C. Upper Bounds on the Rates R(s, L, q) and $R^{(A)}$(s, q)

It was also conjectured in [38] that the lower bound (19) is tight. We prove the conjecture in

Theorem 5: For any $s \geq 2$, $L \geq 1$ and $q \geq 2$ the rate $R(s, L, q)$ of list-decoding (s, L, q)-codes satisfies the inequality

$$R(s, L, q) \leq \frac{L}{s + L - 1} \ln q. \tag{20}$$

Proposition 2 and Theorem 5 for $L = 2$ lead to the upper bound on the rate $R^{(A)}(s, q)$ which was announced in Section I-B as

Theorem 6: For any $s \geq 2$ and $q \geq 2$, the rate of s-separable q-ary codes $R^{(A)}(s, q)$ satisfies the inequality

$$R^{(A)}(s, q) \leq R(s-1, 2, q) \leq \frac{2}{s} \ln q.$$

Proof of Theorem 5: Consider an arbitrary code X of length N and size t. For a convenience of the proof, we will use indexes j (i) of codewords (rows) which can exceed t (N), assuming that the indexes are cyclically ordered, i.e.,

$$x_n(j) = x_{n'}(j') \quad \text{for } n - n' \equiv 0 \bmod N, \qquad j - j' \equiv 0 \bmod t. \tag{21}$$

For a codeword $\boldsymbol{x}(j) \in \mathcal{A}_q^N$, $j \in [t]$, we abbreviate a *projection* of the codeword $\boldsymbol{x}(j)$ *on the coordinates* $n, n+1, \ldots, n+L-1$ by

$$\boldsymbol{x}_n^{n+L-1}(j) \triangleq (x_n(j), \ldots, x_{n+L-1}(j)) \in \mathcal{A}_q^L.$$

A codeword $\boldsymbol{x}(j)$, $j \in [t]$, is said to be *L-rare* in X if there exists a row index $n \in [N]$ such that the number of codeword indexes $j' \in [t]$, $j' \neq j$, with the same projection $\boldsymbol{x}_n^{n+L-1}(j') = \boldsymbol{x}_n^{n+L-1}(j)$ is at most $L-1$. Let $r = r_L(X)$ be the number of codewords which are L-rare in X. For each L-rare codeword $\boldsymbol{x}(j)$, we can choose a row index $n \in [N]$, a q-ary sequence $(a_1, \ldots, a_L) \in \mathcal{A}_q^L$ and an ordinal number (from 1 to L) of the $\boldsymbol{x}(j)$ among all $\leq L$ codewords $\boldsymbol{x}(j')$, $j' \in [t]$, for which $\boldsymbol{x}_n^{n+L-1}(j') = \boldsymbol{x}_n^{n+L-1}(j) = (a_1, \ldots, a_L)$. This correspondence is injective. Therefore, the following claim holds.

Lemma 1: For any code X of length N, the number of its L-rare codewords satisfies the inequality

$$r = r_L(X) \leq N\, L\, q^L. \tag{22}$$

Now we formulate another auxiliary statement.

Lemma 2: If a q-ary code X of length N has size

$$t > N\, L\, q^L \sum_{k=0}^{L-1} k!, \tag{23}$$

then there exists an ordered set of codewords $\mathcal{L}_s = (\boldsymbol{x}(j_1), \ldots, \boldsymbol{x}(j_L))$ such that there is no L-rare codeword in $\mathcal{L}_s$. In addition, for any $k \in [L-1]$, the projections of $\boldsymbol{x}(j_k)$ and $\boldsymbol{x}(j_{k+1})$ on the coordinates $1 + k(s-1), 2 + k(s-1), \ldots, L + k(s-1)$ are the same, i.e.,

$$\boldsymbol{x}_{1+k(s-1)}^{L+k(s-1)}(j_k) = \boldsymbol{x}_{1+k(s-1)}^{L+k(s-1)}(j_{k+1}), \quad k \in [L-1]. \tag{24}$$

Proof of Lemma 2: For any $j_1 \in [t]$, we shall try to construct a sequence $\mathcal{L}(j_1) = (\boldsymbol{x}(j_1), \boldsymbol{x}(j_2), \ldots, \boldsymbol{x}(j_L))$ of L codewords by the following rules. The first element of the sequence $\mathcal{L}(j_1)$ is $\boldsymbol{x}(j_1)$. Let a sequence $(\boldsymbol{x}(j_1), \boldsymbol{x}(j_2), \ldots, \boldsymbol{x}(j_k))$ of length k, $1 \leq k \leq L$, be already constructed. If the last codeword $\boldsymbol{x}(j_k)$ is L-rare in X, then the process ends with a failure. If $k = L$ and $\boldsymbol{x}(j_L)$ is not L-rare in X, then the process successfully ends. Otherwise, for $k \leq L-1$, we consider L indexes from $1 + k(s-1)$ to $L + k(s-1)$. Since the codeword $\boldsymbol{x}(j_k)$ is not L-rare in X, we can find at least L other codewords with the same projection on the coordinates from $1 + k(s-1)$ to $L + k(s-1)$. Among them there are at most $k-1$ codewords that could be already included in the sequence $\mathcal{L}(j_1)$ at the previous $k-1$ steps. Therefore, there exists a codeword which has not been used. Among all such unused codewords we uniquely choose the codeword $\boldsymbol{x}(j_{k+1})$ with the cyclically smallest index j_{k+1} so that $j_{k+1} > j_k$ as the $(k+1)$th element of $\mathcal{L}(j_1)$.

Example 1: Let $t = 4$ and indexes $j_1 = 2$ and $j_2 = 5$ are already used in constructing the sequence, i.e., the first two element of the sequence $\mathcal{L}(j_1)$ are $(\boldsymbol{x}(2), \boldsymbol{x}(5))$. Recall that the indexes $1, 5, 9, \ldots$ correspond to the codeword index 1 as they have the same residue modulo $t = 4$. Let codewords with indexes $3\,(7, 11, \ldots)$ and $4\,(8, 12, \ldots)$ be candidates to be the codeword at the third step. Then 7, corresponding to 3, is the cyclically smallest index so that $7 > 5$, and at the third stage we build the sequence $(\boldsymbol{x}(2), \boldsymbol{x}(5), \boldsymbol{x}(7))$.

Let us prove that there exists a codeword $\boldsymbol{x}(j_1)$ for which the described process successfully ends, i.e., as a result, we obtain a sequence $\mathcal{L}_s := \mathcal{L}(j_1)$ without L-rare codewords. The process ends with a failure if and only if the codeword $\boldsymbol{x}(j_{k+1})$ is L-rare at some step $k \in [L-1]$. Fix an arbitrary L-rare codeword $\boldsymbol{x}(j)$. Given $k \in L$, let j_1 be some element of $[t]$ so that we add $\boldsymbol{x}(j_k) = \boldsymbol{x}(j)$ in the sequence $\mathcal{L}(j_1)$ at the kth step. By construction of the sequence $\mathcal{L}(j_1)$ we know that the codeword $\boldsymbol{x}(j_k)$ coincides with the codeword $\boldsymbol{x}(j_{k-1})$ on the L coordinates:

$$1 + (k-1)(s-1), 2 + (k-1)(s-1), \ldots, \qquad (L-1) + (k-1)(s-1), \quad L + (k-1)(s-1), \tag{25}$$

and has the cyclically smallest index $j_k > j_{k-1}$ among all codeword indexes, except possibly representative indexes from $\{j_1, \ldots, j_{k-2}\}$. Hence, the codeword $\boldsymbol{x}(j_{k-1})$ is the first codeword before $\boldsymbol{x}(j_k)$, except $\boldsymbol{x}(j_1), \ldots \boldsymbol{x}(j_{k-2})$, which has the same symbols as $\boldsymbol{x}(j_k)$ on the L coordinates (25). The number of codewords among $\boldsymbol{x}(j_1), \ldots, \boldsymbol{x}(j_{k-2})$, which have the same symbols as $\boldsymbol{x}(j_k)$ and $\boldsymbol{x}(j_{k-1})$ on the L coordinates (25) is from 0 to $k-2$. Therefore, for fixed codeword $\boldsymbol{x}(j)$ and position $k \in [L]$, there exist at most $k-1$ possible options for $\boldsymbol{x}(j_{k-1})$. Thus, any L-rare codeword $\boldsymbol{x}(j)$, uniquely chosen as the codeword $\boldsymbol{x}(j_k)$ in the sequence $\mathcal{L}_s(j_1)$, spoils at most $(k-1)!$ of starting codewords $\boldsymbol{x}(j_1)$. In virtue of condition (23) and upper bound (22) from Lemma 1, the code size $t > r_L(X) \cdot \sum_{k=0}^{L-1} k!$. Therefore, there exists a starting codeword $\boldsymbol{x}(j_1)$, such that the sequence $\mathcal{L}(j_1)$ will be successfully constructed. □

Lemma 3: For any list-decoding (s, L, q)-code X of length $N = s + L - 1$, the size t of the code X is upper bounded as follows

$$t \le (s + L - 1)Lq^L \sum_{k=0}^{L-1} k!. \tag{26}$$

Proof of Lemma 3: Consider an arbitrary list-decoding (s, L, q)-code X of the length $N = s + L - 1$. We prove the claim of this lemma by contradiction. Assume that $t > (s + L - 1)Lq^L \sum_{k=0}^{L-1} k!$. In virtue of Lemma 2, we can construct the sequence $\mathcal{L}_s = (\boldsymbol{x}(j_1), \ldots, \boldsymbol{x}(j_L))$ so that there is no L-rare codeword in $\mathcal{L}_s$, and the property (24) holds. Let $J = \{j_1, \ldots, j_L\}$ be the set of codeword indexes. Without loss of generality, we may assume the sequence $(j_1, j_2, \ldots, j_L)$ is lexicographically ordered or $j_k < j_{k+1}$ for $k \in [L-1]$, since, otherwise, we can take (21) j_{k+1} as $j_{k+1} + t\lceil j_k/t \rceil$.

Now we shall find an s-collection $I = \{i_1, \ldots, i_s\} \subset [t] \setminus J$ consisting of codeword indexes such that $U(\boldsymbol{x}(i_1), \ldots, \boldsymbol{x}(i_s))$ covers L codewords $\{x(j), j \in J\}$. Recall that by covering we mean that, for any pair (j, n), $j \in J$, $n \in [N]$, there exists $i \in I$ so that the symbol $x_n(j) = x_n(i)$. Define a lexicographically ordered sequence $\mathcal{P}$ of pairs so that the first $s+L-1$ pairs are from $(j_1, 1)$ to $(j_1, s+L-1)$, and the following $(s-1)(L-1)$ pairs are of the form (j_k, n), where n runs over all row indexes from $L + 1 + (k-1)(s-1)$ to $L + k(s-1)$, i.e.,

$$\begin{aligned} \mathcal{P} \triangleq ((j_1, 1), (j_1, 2), \ldots, (j_1, L + s - 1),\\ (j_2, L + 1 + (s-1)), \ldots, (j_2, L + 2(s-1)), \ldots,\\ (j_L, L + 1 + (L-1)(s-1)), \ldots, (j_L, sL)). \end{aligned}$$

From (24) it follows that if, for any pair (j, n) in $\mathcal{P}$, there exists $i \in I$ so that the symbol $x_n(j) = x_n(i)$, then the s-collection I is a required one. It remains to find an appropriate I. Notice that the length of $\mathcal{P}$ is sL, and the second number in pairs goes from 1 to sL. Divide the sequence $\mathcal{P}$ into s subsequences of length L so that $\mathcal{P} = (\mathcal{P}_1, \ldots, \mathcal{P}_s)$. Let

$$\mathcal{P}_k \triangleq ((j_{k_1}, (k-1)L+1), (j_{k_2}, (k-1)L+2), \ldots, (j_{k_L}, kL)).$$

It is easy to check that the projection $\boldsymbol{x}(j_{k_L})$ (the codeword index is the same as the first number in the last pair of $\mathcal{P}_k$) on the coordinates $(k-1)L + 1, (k-1)L + 2, \ldots, kL$ is

$$\begin{aligned} &\boldsymbol{x}^{kL}_{(k-1)L+1}(j_{k_L})\\ &\quad = \left(x_{(k-1)L+1}(j_{k_1}), x_{(k-1)L+2}(j_{k_2}), \ldots, x_{kL}(j_{k_L})\right). \end{aligned}$$

From Lemma 2, it follows that the codeword $\boldsymbol{x}(j_{k_L})$ is not L-rare. Therefore, we can find an index i_k, $i_k \notin J$, and the corresponding codeword $\boldsymbol{x}(i_k)$ such that the projections of $\boldsymbol{x}(i_k)$ and $\boldsymbol{x}(j_{k_L})$ on the coordinates $(k-1)L+1, (k-1)L+2, \ldots, kL$ are the same, i.e.,

$$\boldsymbol{x}^{kL}_{(k-1)L+1}(i_k) = \boldsymbol{x}^{kL}_{(k-1)L+1}(j_{k_L}). \tag{27}$$

Since there are s subsequences $\mathcal{P}_k$, which form $\mathcal{P}$, we can find at most s different i_k so that $U(\boldsymbol{x}(i_1), \ldots, \boldsymbol{x}(i_s))$ covers L codewords $\{\boldsymbol{x}(j), j \in J\}$. This contradiction completes the proof of Lemma 3. □

Lemma 2 and Lemma 3 are intuitively illustrated by the following example.

Example 2: Let $L = 4$, $s = 2$ and $N = L + s - 1 = 5$. Then four q-ary codewords $\boldsymbol{x}(j_k), \boldsymbol{x}(j_k) \in \mathcal{A}_q^5$, $k \in \{1, 2, 3, 4\}$, satisfying the equalities (24) can be written in the form:

$$\begin{aligned} \boldsymbol{x}(j_1) &= (x_1(j_1), x_2(j_1), x_3(j_1), x_4(j_1), x_5(j_1)),\\ \boldsymbol{x}(j_2) &= (y_2, x_2(j_1), x_3(j_1), x_4(j_1), x_5(j_1)),\\ \boldsymbol{x}(j_3) &= (y_2, y_3, x_3(j_1), x_4(j_1), x_5(j_1)),\\ \boldsymbol{x}(j_4) &= (y_2, y_3, y_4, x_4(j_1), x_5(j_1)). \end{aligned}$$

These codewords are covered by $U(\boldsymbol{x}(i_1), \boldsymbol{x}(i_2))$, where two q-ary codewords $\boldsymbol{x}(i_1), \boldsymbol{x}(i_2) \in \mathcal{A}_q^5$ are based on the property (27) and can be written in the form:

$$\begin{aligned} \boldsymbol{x}(i_1) &= (x_1(j_1), x_2(j_1), x_3(j_1), x_4(j_1), a_1),\\ \boldsymbol{x}(i_2) &= (y_2, y_3, y_4, a_2\ x_5(j_1)). \end{aligned}$$

To complete the proof of Theorem 5, consider an arbitrary list-decoding (s, L, q)-code X of length N, $N > s+L-1$, and size t. Divide each codeword of the code X into $s+L-1$ parts of sizes n_i, where $\left\lfloor \frac{N}{s+L-1} \right\rfloor \le n_i \le \left\lceil \frac{N}{s+L-1} \right\rceil$, $i \in [s+L-1]$. The number of different parts is upper bounded by $q^{\left\lfloor \frac{N}{s+L-1} \right\rfloor} + q^{\left\lceil \frac{N}{s+L-1} \right\rceil}$. Replace each part of each codeword with a unique symbol from the Q-ary alphabet of the size $Q \triangleq 2q^{\left\lceil \frac{N}{s+L-1} \right\rceil}$. It is easy to see that the code X', obtained after replacements, is a Q-ary list-decoding (s, L, Q)-code of length $N = s+L-1$ and size t. Thus, the inequality (26) of Lemma 3 implies that the size

$$t \le (s + L - 1)L \sum_{n=0}^{L-1} n! 2^L q^{L\left\lceil \frac{N}{s+L-1} \right\rceil}.$$

This upper bound immediately yields (20). □

Appendix

A. Notations and Definitions

Given the symmetric f–MAC and a q-ary code X, a message $\mathbf{e} \in \binom{[t]}{s}$ is said to be *bad* for the code X, if there exists a message $\mathbf{e}' \neq \mathbf{e}$ such that $z^{(f)}(\mathbf{e}', X) = z^{(f)}(\mathbf{e}, X)$. If the unknown message $\mathbf{e}$ is interpreted as the random vector taking equiprobable values in the set $\binom{[t]}{s}$, then the *relative number* of "bad" messages among all $\binom{t}{s} = |\binom{[t]}{s}|$ messages can be considered as the *error probability* $\epsilon^{(f)}(X, s)$ of the code X for the *brute force* decoding.

Definition 4 [33], [34], [44]: Fix a parameter $R > 0$. Define the *error probability* for the symmetric f-MAC:

$$\epsilon^{(f)}(s, q, R, N) \triangleq \min_{X: t=\lfloor \exp\{RN\} \rfloor} \epsilon^{(f)}(X, s), \tag{28}$$

where the minimum is taken over all q-ary codes of length N and size $t = \lfloor \exp\{RN\} \rfloor$. If the parameter $R > R^{(f)}(s, q)$, where the rate of s-separable codes $R^{(f)}(s, q)$ for the f-MAC is defined by (9), then the function

$$E^{(f)}(s, q, R) \triangleq \overline{\lim_{N\to\infty}} \frac{-\ln \epsilon^{(f)}(s, q, R, N)}{N} \tag{29}$$

is called the *error exponent* for the f-MAC. The quantity

$$C^{(f)}(s, q) \triangleq \sup \left\{ R : E^{(f)}(s, q, R) > 0 \right\} \tag{30}$$

is said to be the *capacity* of the f-MAC for the *exponentially decreasing* error probability. Using the Shannon terminology [2], the rate of s-separable codes $R^{(f)}(s, q)$ can be also called the *zero error capacity* of the f-MAC.

It is known [33], [34], [44] that for any symmetric f–MAC the value $C^{(f)}(s, q)$ defined by (28)-(30) does not exceed the entropy bound $\overline{C}^{(f)}(s, q)$ introduced in Proposition 1, i.e.,

$$C^{(f)}(s, q) \le \overline{C}^{(f)}(s, q) = \frac{\max\limits_{\boldsymbol{p}} H_{\boldsymbol{p}}^{(f)}(s, q)}{s}, \tag{31}$$

where $H_{\boldsymbol{p}}^{(f)}(s, q)$ is the Shannon entropy (10) of the output of the f–MAC for the given input probability distribution $\boldsymbol{p}$.

B. Random Coding Error Exponent for the f-MAC

Let the symbol $\mathcal{P}_N^{(f)}\left(s, t, (N_0, \ldots, N_{q-1})\right)$ denote the *average value* of error probability $\epsilon^{(f)}(X, s)$ over the *fixed composition ensemble* (briefly, FC-ensemble) of t independent q-ary codewords $\boldsymbol{x}(j)$ with the same type $T(\boldsymbol{x}(j)) = (N_0, \ldots, N_{q-1})$, $j \in [t]$. By a similar symbol $\mathcal{P}_N^{(f)}(s, t, \boldsymbol{p})$ we will denote the *average value* of error probability $\epsilon^{(f)}(X, s)$ over the *completely randomized ensemble* (briefly, CR-ensemble) of q-ary codes $X = \|x_i(j)\|$ with independent components $x_i(j)$ having the same distribution $\boldsymbol{p}$, i.e., the probability $\Pr\{x_i(j) = a\} \triangleq p(a)$, $i \in [N]$, $j \in [t]$, $a \in \mathcal{A}_q$.

Let $s \ge 2$, $q \ge 2$, $R > 0$ be fixed and the entropy $H_{\boldsymbol{p}}^{(f)}(s, q)$ of a fixed distribution $\boldsymbol{p}$ be defined by (10). If code parameters $N, t \to \infty$ such that

$$\frac{\ln t}{N} \sim R, \quad \frac{N_x}{N} \sim p(x), \; x \in \mathcal{A}_q, \tag{32}$$

then from the standard random coding arguments [2] it follows that the error exponent $E^{(f)}(s, q, R)$ of the f-MAC, defined by (28)-(29) satisfies two random coding bounds:

$$E^{(f)}(s, q, R) \ge \overline{\lim_{N\to\infty}} \frac{-\ln \mathcal{P}_N^{(f)}\left(s, t, (N_0, ., N_{q-1})\right)}{N}, \tag{33}$$

$$E^{(f)}(s, q, R) \ge \overline{\lim_{N\to\infty}} \frac{-\ln \mathcal{P}_N^{(f)}(s, t, \boldsymbol{p})}{N}. \tag{34}$$

To formulate the results about the logarithmic asymptotic behavior of probabilities $\mathcal{P}_N^{(f)}\left(s, t, (N_0, ., N_{q-1})\right)$ and $\mathcal{P}_N^{(f)}(s, t, \boldsymbol{p})$, we need the following auxiliary notations [31]. Let a symmetric f–MAC be represented as the conditional probability $\tau^{(f)}(z|x_1^s)$, that is

$$\tau^{(f)}(z|x_1^s) \triangleq \begin{cases} 1, & z = f(x_1^s), \\ 0, & z \ne f(x_1^s), \end{cases}$$

and the symbol

$$\tau \triangleq \left\{ \tau(x_1^s, z) : \tau(x_1^s, z) \ge 0, \sum_{x_1^s, z} \tau(x_1^s, z) = 1 \right\} \tag{35}$$

denotes a probability distribution on the Cartesian product $\mathcal{A}_q^s \times Z$. Using the standard symbols for the conditional probabilities of the distribution τ, we abbreviate by

$$\{\tau\}^{(f)} \triangleq \left\{ \tau : \tau^{(f)}(z|x_1^s) = 0 \Rightarrow \tau(z|x_1^s) = 0 \right\} \tag{36}$$

the subset of probability distributions τ (35) such that the conditional probability $\tau(z|x_1^s) = 0$ is implied by $\tau^{(f)}(z|x_1^s) = 0$.

Introduce the $\cup$-convex information-theoretic functions of the argument $\tau \in \{\tau\}^{(f)}$:

$$\mathcal{H}^{(f)}(\boldsymbol{p}, \tau) \triangleq \sum_{x_1^s \cdot z} \tau(x_1^s, z) \ln \frac{\tau(x_1^s, z)}{\tau^{(f)}(z|x_1^s) \cdot \prod\limits_{k=1}^{s} p(x_k)},$$

$$I_m(\boldsymbol{p}, \tau) \triangleq \sum_{x_1^s \cdot z} \tau(x_1^s, z) \ln \frac{\tau(x_1^m | x_{m+1}^s, z)}{\prod\limits_{k=1}^{m} p(x_k)}, \quad m \in [s]. \tag{37}$$

From (10), it follows that the distribution

$$\tau_{\boldsymbol{p}}^{(f)} \triangleq \left\{ \tau^{(f)}(z|x_1^s) \cdot \prod_{k=1}^{s} p(x_k), x_1^s \in \mathcal{A}_q^s, z \in Z \right\} \in \{\tau\}^{(f)}$$

and the functions (37) satisfy the equalities

$$\mathcal{H}^{(f)}\left(\boldsymbol{p}, \tau_{\boldsymbol{p}}^{(f)}\right) = 0, \quad I_s\left(\boldsymbol{p}, \tau_{\boldsymbol{p}}^{(f)}\right) = H_{\boldsymbol{p}}^{(f)}(s, q).$$

Proposition 4 [31], [34]: Let $s \ge 2$, $q \ge 2$, $R > 0$ be fixed and the entropy $H_{\boldsymbol{p}}^{(f)}(s, q)$ of a fixed distribution $\boldsymbol{p}$ be defined by (10). *If the asymptotic conditions* (32) *are fulfilled, then for the FC-ensemble, there exists*

$$\lim_{N\to\infty} \frac{-\ln \mathcal{P}_N^{(f)}\left(s, t, (N_0, ., N_{q-1})\right)}{N}$$

$$\triangleq E_{FC}^{(f)}(s, q, R, \boldsymbol{p}) > 0, \quad 0 < R < \frac{H_{\boldsymbol{p}}^{(f)}(s, q)}{s}, \tag{38}$$

and for the CR-ensemble, there exists

$$\lim_{N\to\infty} \frac{-\ln \mathcal{P}_N^{(f)}(s, t, \boldsymbol{p})}{N} \triangleq E_{CR}^{(f)}(s, q, R, \boldsymbol{p}) > 0,$$

$$0 < R < \frac{H_{\boldsymbol{p}}^{(f)}(s, q)}{s}. \tag{39}$$

For any fixed $\boldsymbol{p}$, the positive monotonically decreasing functions $E_{FC}^{(f)}(s, q, R, \boldsymbol{p})$ and $E_{CR}^{(f)}(s, q, R, \boldsymbol{p})$ are $\cup$-convex functions of the parameter $R > 0$ of the following form:

$$E_{FC}^{(f)}(s, q, R, \boldsymbol{p}) \triangleq \min_{m \in [s]} E_{FC}^{(f)}(s, q, R, \boldsymbol{p}, m),$$

$$E_{FC}^{(f)}(s, q, R, \boldsymbol{p}, m) \triangleq \min_{\{\tau\}^{(f)}(\boldsymbol{p})} \left\{ \mathcal{H}^{(f)}(\boldsymbol{p}, \tau) + [I_m(\boldsymbol{p}, \tau) - mR]^+ \right\}, \tag{40}$$

and

$$E_{CR}^{(f)}(s,q,R,\boldsymbol{p}) \triangleq \min_{m\in[s]} E_{CR}^{(f)}(s,q,R,\boldsymbol{p},m),$$
$$E_{CR}^{(f)}(s,q,R,\boldsymbol{p},m) \triangleq \min_{\{\tau\}^{(f)}} \left\{\mathcal{H}^{(f)}(\boldsymbol{p},\tau)+[I_m(\boldsymbol{p},\tau)-mR]^{+}\right\}. \tag{41}$$

The minimum in (40) *is taken over the subset* $\{\tau\}^{(f)}(\boldsymbol{p})$ *of distributions* $\{\tau\}^{(f)}$ (36) *for which the marginal probabilities* $\tau(x_k)$ *are fixed and coincide with* $p(x_k)$, $k \in [s]$, *i.e.,* $\{\tau\}^{(f)}(\boldsymbol{p})$ *is defined as*

$$\left\{\tau \in \{\tau\}^{(f)} : \sum_{x_1^{k-1}} \sum_{x_{k+1}^{s}} \sum_{z} \tau(x_1^s, z) = p(x_k), k \in [s]\right\}. \tag{42}$$

The minimum in (41) *is taken over the set of all distributions* (36).

Remark 5: Proposition 4 and the properties of the *random error exponents* (38) and (39) were formulated and proved in the papers [31] and [34] for the particular binary case $q = 2$ only. In the general case $q \ge 2$, we omit the proofs because one can check that the given results are based on the same methods developed in [31] and [34]. Here we only note that for the symmetric f-MAC, definitions (40)-(42) lead to the inequality

$$E_{CR}^{(f)}(s,q,R,\boldsymbol{p}) \le E_{FC}^{(f)}(s,q,R,\boldsymbol{p}), \quad 0 < R < \frac{H_{\boldsymbol{p}}^{(f)}(s,q)}{s}.$$

Random coding bounds (33)-(34) and Proposition 4 imply that the error exponent $E^{(f)}(s,q,R)$ defined by (28)-(29) is

$$E^{(f)}(s,q,R) \ge \max_{\boldsymbol{p}} E_{FC}^{(f)}(s,q,R,\boldsymbol{p}) > 0$$
$$0 < R < \overline{C}^{(f)}(s,q) = \frac{\max_{\boldsymbol{p}} H_{\boldsymbol{p}}^{(f)}(s,q)}{s} \tag{43}$$

and, obviously, the inequality (43) means that for the capacity $C^{(f)}(s,q)$ of the f-MAC, defined by (28)-(30), the lower bound

$$C^{(f)}(s,q) \ge \overline{C}^{(f)}(s,q) = \frac{\max_{\boldsymbol{p}} H_{\boldsymbol{p}}^{(f)}(s,q)}{s}, \tag{44}$$

holds. The inequalities (31) and (44) lead to

Corollary 2: The capacity $C^{(f)}(s,q)$ of the f-MAC for the exponentially decreasing error probability coincides with the entropy bound $\overline{C}^{(f)}(s,q)$, i.e.,

$$C^{(f)}(s,q) = \overline{C}^{(f)}(s,q) = \frac{\max_{\boldsymbol{p}} H_{\boldsymbol{p}}^{(f)}(s,q)}{s}, \tag{45}$$

and the number defined by the right-hand side (45) can be considered as the Shannon capacity of the symmetric f-MAC [44].

The following statement called the random coding lower bound on the rate $R^{(f)}(s,q)$ of s-separable q-ary codes for the symmetric f-MAC can be obtained as a consequence of Proposition 4.

Proposition 5 [31]: The rate $R^{(f)}(s,q)$ *of* s*-separable* q*-ary codes for the symmetric* f*-MAC satisfies the inequality*

$$R^{(f)}(s,q) \ge \underline{R}^{(f)}(s,q), \quad s \ge 2, \; q \ge 2,$$

where for any fixed distribution $\boldsymbol{p}$ *the lower bound* $\underline{R}^{(f)}(s,q)$ *can be represented in the form*

$$\underline{R}^{(f)}(s,q) \triangleq \min_{m\in[s]} \frac{E_{FC}^{(f)}(s,q,0,\boldsymbol{p},m)}{s+m-1} = \min_{m\in[s]} \frac{\min_{\{\tau\}^{(f)}(\boldsymbol{p})} \left\{\mathcal{H}^{(f)}(\boldsymbol{p},\tau)+I_m(\boldsymbol{p},\tau)\right\}}{s+m-1}$$

or in the form

$$\underline{R}^{(f)}(s,q) \triangleq \min_{m\in[s]} \frac{E_{CR}^{(f)}(s,q,0,\boldsymbol{p},m)}{s+m-1} = \min_{m\in[s]} \frac{\min_{\{\tau\}^{(f)}} \left\{\mathcal{H}^{(f)}(\boldsymbol{p},\tau)+I_m(\boldsymbol{p},\tau)\right\}}{s+m-1}.$$

In paper [31], Proposition 5 was proved for the particular case of the B-MAC with binary ($q = 2$) alphabet only. For an arbitrary symmetric f-MAC, one can use the same arguments. The asymptotic lower bound on the rate $R^{(disj)}(s)$ for the disjunctive MAC formulated in Sect. III-B was actually obtained in [31] as a nontrivial consequence of Proposition 5.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewers for their many comments and suggestions which improved both the exposition of the paper and the clarity of the proofs.

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. Inf. Theory*, vol. IT-27, no. 1, pp. 41–48, Jan. 1981, doi: 10.1109/TIT.1981.1056304.
[2] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[3] M. Cheng and Y. Miao, "On anti-collusion codes and detection algorithms for multimedia fingerprinting," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4843–4851, Jul. 2011.
[4] E. Egorova and V. Potapova, "Signature codes for a special class of multiple access channel," in *Proc. XV Int. Symp. Problems Redundancy Inf. Control Syst. (REDUNDANCY)*, Sep. 2016, pp. 38–42.
[5] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inf. Theory*, vol. 44, no. 5, pp. 1897–1905, Sep. 1998.
[6] M. L. Fredman and J. Komlós, "On the size of separating systems and families of perfect hash functions," *SIAM J. Algebr. Discrete Methods*, vol. 5, no. 1, pp. 61–68, 1984, doi: 10.1137/0605009.
[7] K. Mehlhorn, *Sorting and Searching* (Data Structures and Algorithms), vol. 1. Berlin, Germany: Springer, 1984.
[8] M. Cheng, L. Ji, and Y. Miao, "Separable codes," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1791–1803, Mar. 2012.
[9] F. Gao and G. Ge, "New bounds on separable codes for multimedia fingerprinting," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5257–5262, Sep. 2014, doi: 10.1109/TIT.2014.2331989.
[10] S. R. Blackburn, "Probabilistic existence results for separable codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 5822–5827, Nov. 2015, doi: 10.1109/TIT.2015.2473848.
[11] E. Egorova, M. Fernandez, G. Kabatiansky, and M. H. Lee, "Signature codes for the A-channel and collusion-secure multimedia fingerprinting codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 3043–3047.

[12] C. Shangguan, X. Wang, G. Ge, and Y. Miao, "New bounds for frameproof codes," *IEEE Trans. Inf. Theory*, vol. 63, no. 11, pp. 7247–7252, Nov. 2017, doi: 10.1109/TIT.2017.2745619.

[13] J. N. Staddon, D. R. Stinson, and R. Wei, "Combinatorial properties of frameproof and traceability codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 1042–1049, Mar. 2001.

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

[15] M. S. Pinsker and Y. L. Sagalovich, "Lower bound on the cardinality of code of automata's states," *Problems Inf. Transmiss.*, vol. 8, no. 3, pp. 59–66, 1972.

[16] Y. Sagalovich, "Fully separated systems," *Problems Inf. Transmiss.*, vol. 18, no. 2, pp. 74–82, 1982.

[17] A. G. D'yachkov, I. V. Vorobyev, N. A. Polyanskii, and V. Y. Shchukin, "Cover-free codes and separating system codes," *Des., Codes Cryptogr.*, vol. 82, nos. 1–2, pp. 197–209, 2017.

[18] Y. L. Sagalovich, "A method for increasing the reliability of finite automata," *Problemy Peredachi Informatsii*, vol. 1, no. 2, pp. 27–35, 1965.

[19] Y. L. Sagalovich, "Separating systems," *Problems Inf. Transmiss.*, vol. 30, no. 2, pp. 105–123, 1994.

[20] C. J. Mitchell and F. C. Piper, "Key storage in secure networks," *Discrete Appl. Math.*, vol. 21, no. 3, pp. 215–228, 1988.

[21] A. G. D'yachkov, A. J. Macula, and V. V. Rykov, "New applications and results of superimposed code theory arising from the potentialities of molecular biology," in *Numbers, Information and Complexity*. Dordrecht, The Netherlands: Kluwer Academic, 2000, pp. 265–282.

[22] D. R. Stinson, R. Wei, and K. Chen, "On generalized separating hash families," *J. Combinat. Theory A*, vol. 115, no. 1, pp. 105–120, 2008, doi: 10.1016/j.jcta.2007.04.005.

[23] L. A. Bassalygo, M. Burmester, A. Dyachkov, and G. Kabatianski, "Hash codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Aug. 1997, p. 174.

[24] W. Kautz and R. Singleton, "Nonrandom binary superimposed codes," *IEEE Trans. Inf. Theory*, vol. IT-10, no. 4, pp. 363–377, Oct. 1964.

[25] A. G. D'yachkov and V. V. Rykov, "A survey of superimposed code theory," *Problems Control Inf. Theory*, vol. 12, no. 4, pp. 229–242, 1983.

[26] S. R. Blackburn, "Frameproof codes," *SIAM J. Discrete Math.*, vol. 16, no. 3, pp. 499–510, 2003.

[27] A. G. D'yachkov, "An upper bound for hash codes," in *Proc. Conf. Comput. Sci. Inf. Technol.*, 1997, pp. 219–221.

[28] J. Körner and K. Marton, "New bounds for perfect hashing via information theory," *Eur. J. Combinatorics*, vol. 9, no. 6, pp. 523–530, 1988, doi: 10.1016/S0195-6698(88)80048-9.

[29] Y. Erlich, A. Gordon, M. Brand, G. J. Hannon, and P. P. Mitra, "Compressed genotyping," *IEEE Trans. Inf. Theory*, vol. 56, no. 2, pp. 706–723, Feb. 2010, doi: 10.1109/TIT.2009.2037043.

[30] D.-Z. Du and F. K. Hwang, *Combinatorial Group Testing and Its Applications* (Series on Applied Mathematics), vol. 12, 2nd ed. River Edge, NJ, USA: World Scientific Publishing, 2000.

[31] A. G. D'yachkov. (2003). "Lectures on designing screening experiments." [Online]. Available: https://arxiv.org/abs/1401.7505

[32] A. G. D'yachkov, "On a search model of false coins," in *Topics in Information Theory (Colloquia Mathematica Societatis Janos Bolyai)*, vol. 16. Amsterdam, The Netherlands: North Holland, 1977, pp. 163–170.

[33] M. B. Malyutov, "The separating property of random matrices," *Math. Notes Acad. Sci. USSR*, vol. 23, no. 1, pp. 84–91, 1978.

[34] A. G. D'yachkov and A. Rashad, "Universal decoding for random design of screening experiments," *Microelectron. Rel.*, vol. 29, no. 6, pp. 965–971, 1989.

[35] D. Coppersmith and J. B. Shearer, "New bounds for union-free families of sets," *Electron. J. Combinatorics*, vol. 5, no. 1, p. 39, 1998. [Online]. Available: http://www.combinatorics.org/Volume 5/Abstracts/v5i1r39.html

[36] A. G. D'yachkov, I. V. Vorob'ev, N. A. Polyansky, and V. Y. Shchukin, "Bounds on the rate of disjunctive codes," *Problems Inf. Transmiss.*, vol. 50, no. 1, pp. 27–56, 2014, doi: 10.1134/S0032946014010037.

[37] A. M. Rashad, "On symmetrical superimposed codes," *J. Inf. Process. Cybern.*, vol. 25, no. 7, pp. 337–341, 1989.

[38] V. Y. Shchukin, "List decoding for a multiple access hyperchannel," *Problems Inf. Transmiss.*, vol. 52, no. 4, pp. 329–343, 2016.

[39] A. D'yachkov, V. Rykov, C. Deppe, and V. Lebedev, "Superimposed codes and threshold group testing," in *Information Theory, Combinatorics, and Search Theory* (Lecture Notes in Computer Science), vol. 7777. Berlin, Germany: Springer, 2013, pp. 509–533, doi: 10.1007/978-3-642-36899-8_25.

[40] A. D. Bonis and U. Vaccaro, "Optimal algorithms for two group testing problems, and new bounds on generalized superimposed codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4673–4680, Oct. 2006, doi: 10.1109/TIT.2006.881740.

[41] A. G. D'yachkov and V. V. Rykov, "On a coding model for a multiple-access adder channel," *Problemy Peredachi Informatsii*, vol. 17, no. 2, pp. 26–38, 1981.

[42] P. Mateev, "On the entropy of the multinomial distribution," *Theory Probab. Appl.*, vol. 23, no. 1, pp. 188–190, 1978.

[43] A. Naor and J. Verstraëte, "A note on bipartite graphs without $2k$-cycles," *Combinatorics, Probab. Comput.*, vol. 14, nos. 5–6, pp. 845–849, 2005, doi: 10.1017/S0963548305007029.

[44] M. B. Malyutov and P. S. Mateev, "Planning of screening experiments for a nonsymmetric response function," *Math. Notes Acad. Sci. USSR*, vol. 27, no. 1, pp. 57–68, 1980.

Arkadii D'yachkov was born in Russia in 1944. He received the Ph.D degree in Mathematics from the Institute for Information Transmission Problems, Moscow, Russia, in 1971 and the Doctor of Sciences degree in Mathematics from the Lomonosov Moscow State University, Moscow, Russia, in 1985. In 1972 he joined the Faculty of Mechanics and Mathematics, the Lomonosov Moscow State University, where he is currently a Full Professor at the Department of Probability Theory. His research interests include information theory, combinatorial coding theory, probability theory and statistics.

Nikita Polyanskii was born in Russia in 1991. He received the M.Sc. degree in Mathematics and the Ph.D. degree in Mathematics from the Lomonosov Moscow State University, Moscow, Russia, in 2013 and 2016, respectively. During 2015–2017 he was a researcher at the Institute for Information Transmission Problems, Moscow, Russia, and a senior engineer at Huawei Technologies, Moscow, Russia. Since 2017 Nikita has been a postdoctoral researcher in the Department of Mathematics, Technion–Israel Institute of Technology, Haifa, Israel. Since 2018 he has been a research scientist in the Center for Computational and Data-Intensive Science and Engineering, Skolkovo Institute of Science and Technology, Moscow, Russia. His research interests include coding theory and its applications to communications, group testing, storage systems, and combinatorics.

Vladislav Shchukin received the M.Sc. degree in Mathematics and the Ph.D. degree in Mathematics from the Lomonosov Moscow State University in 2013 and 2017, respectively. Since 2015 he has been a researcher at the Institute for Information Transmission Problems, Moscow. Since 2018 Vladislav has been a senior engineer at Huawei Technologies R&D department in Moscow. His research interests include coding theory, information theory, combinatorics and algorithms.

Ilya Vorobyev received the M.Sc. degree in Mathematics and the Ph.D. degree in Mathematics from the Lomonosov Moscow State University in 2013 and 2017, respectively. In 2015–2017 he worked as a research engineer at Huawei R&D department in Moscow. He also was a researcher at the Institute for Information Transmission Problems, Moscow, in 2015–2017. Since 2017 Ilya has been a senior researcher in the Advanced Combinatorics and Complex Networks Lab, Moscow Institute of Physics and Technology. Since 2018 he has been a research scientist in the Center for Computational and Data-Intensive Science and Engineering, Skolkovo Institute of Science and Technology. His research interests include extremal combinatorics and coding theory.