ISSN 0032-9460, Problems of Information Transmission, 2015, Vol. 51, No. 2, pp. 110–131. © Pleiades Publishing, Inc., 2015.
Original Russian Text © A.G. D'yachkov, I.V. Vorob'ev, N.A. Polyansky, V.Yu. Shchukin, 2015, published in Problemy Peredachi Informatsii, 2015, Vol. 51, No. 2, pp. 27–49.

Almost Disjunctive List-Decoding Codes

A. G. D'yachkov, I. V. Vorob'ev, N. A. Polyansky, and V. Yu. Shchukin

Probability Theory Chair, Faculty of Mechanics and Mathematics,
Lomonosov Moscow State University, Moscow, Russia
e-mail: agd-msu@yandex.ru, vorobyev.i.v@yandex.ru,
nikitapolyansky@gmail.com, vpike@mail.ru

Received September 16, 2014; in final form, January 28, 2015

Abstract—We say that an s-subset of codewords of a binary code X is s_L-bad in X if there exists an L-subset of other codewords in X whose disjunctive sum is covered by the disjunctive sum of the given s codewords. Otherwise, this s-subset of codewords is said to be s_L-good in X. A binary code X is said to be a list-decoding disjunctive code of strength s and list size L (an s_L-LD code) if it does not contain s_L-bad subsets of codewords. We consider a *probabilistic* generalization of s_L-LD codes; namely, we say that a code X is an *almost disjunctive* s_L*-LD code* if the *fraction* of s_L-good subsets of codewords in X is close to 1. Using the random coding method on the ensemble of binary constant-weight codes, we establish lower bounds on the capacity and error exponent of almost disjunctive s_L-LD codes. For this ensemble, the obtained lower bounds are tight and show that the capacity of almost disjunctive s_L-LD codes is greater than the zero-error capacity of disjunctive s_L-LD codes.

DOI: 10.1134/S0032946015020039

1. PROBLEM SETTING AND RESULTS

1.1. Notation and Definitions

Let N, t, s, and L be integers, $1 \le s < t$, $1 \le L \le t - s$. By $\triangleq$ we denote equality by definition, $|A|$ is the cardinality of a set A, and $[N] \triangleq \{1, 2, \ldots, N\}$ is the set of integers from 1 to N. The standard notation $\lfloor a \rfloor$ ($\lceil a \rceil$) is used to denote the largest (smallest) integer $\le a$ ($\ge a$). Introduce a binary matrix X with t columns $\boldsymbol{x}(1), \boldsymbol{x}(2), \ldots, \boldsymbol{x}(t)$ (codewords)

$$\begin{gathered} X \triangleq \|x_i(j)\|, \quad x_i(j) = 0, 1, \\ \boldsymbol{x}(j) \triangleq (x_1(j), x_2(j), \ldots, x_N(j)), \quad i \in [N], \quad j \in [t]. \end{gathered} \tag{1}$$

In what follows we refer to X as a *code of length N and size $t = \lfloor 2^{RN} \rfloor$* (or an (N, R) *code*), where a fixed parameter $R > 0$ is the *rate* of X. The number of ones in a column $\boldsymbol{x}(j)$, i.e., $|\boldsymbol{x}(j)| \triangleq \sum\limits_{i=1}^{N} x_i(j)$, is the *weight* of $\boldsymbol{x}(j)$, $j \in [t]$. A code X is said to be a *constant-weight code* with weight w, $1 \le w \le N$, if every codeword of X contains exactly w ones, i.e., $|\boldsymbol{x}(j)| = w$ for any $j \in [t]$. The standard symbol $\vee$ denotes the disjunctive (Boolean) sum of two binary digits

$$0 \vee 0 = 0, \qquad 0 \vee 1 = 1 \vee 0 = 1 \vee 1 = 1,$$

as well as the componentwise disjunctive sum of two binary columns. We say that a binary column $\boldsymbol{u} \in \{0,1\}^N$ *covers* a binary column $\boldsymbol{v}$ ($\boldsymbol{u} \succeq \boldsymbol{v}$) if $\boldsymbol{u} \vee \boldsymbol{v} = \boldsymbol{u}$.

Definition 1 [1]. We say that a set $\mathcal{S}$, $\mathcal{S} \subset [t]$, of size $|\mathcal{S}| = s$ is s_L*-bad* for a code X if there exists a set $\mathcal{L}$ $\mathcal{L} \subset [t] \setminus \mathcal{S}$, of size $|\mathcal{L}| = L$ such that the disjunctive sum of codewords with indices from $\mathcal{S}$ covers the disjunctive sum of codewords with indices from $\mathcal{L}$, i.e.,

$$\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i) \succeq \bigvee_{j\in\mathcal{L}} \boldsymbol{x}(j), \quad \mathcal{L}\subset[t]\setminus\mathcal{S}, \quad |\mathcal{L}|=L. \tag{2}$$

Otherwise, $\mathcal{S}$ is said to be s_L-*good* for X. In other words, the disjunctive sum of any collection of columns of X whose indices form an s_L-good set $\mathcal{S}$ covers at most $L-1$ columns of X with indices outside $\mathcal{S}$.

Let $\boldsymbol{B}_L(s,X)$ (respectively, $\boldsymbol{G}_L(s,X)$) denote the set of all s_L-bad (respectively, s_L-good) subsets $\mathcal{S}$ for a code X, and let $|\boldsymbol{B}_L(s,X)|$ (respectively, $|\boldsymbol{G}_L(s,X)|$) be the cardinality of this set. Note that

$$0\le|\boldsymbol{B}_L(s,X)|\le\binom{t}{s}, \qquad 0\le|\boldsymbol{G}_L(s,X)|\le\binom{t}{s}, \qquad |\boldsymbol{B}_L(s,X)|+|\boldsymbol{G}_L(s,X)|=\binom{t}{s},$$

and observe the following obvious property.

Proposition 1. *For any code X, for all $s\ge1$ and $L\ge1$, every s_L-good (s_{L+1}-bad) set $\mathcal{S}$ for X is an s_{L+1}-good (s_L-bad) set for X; i.e., we have $\boldsymbol{B}_{L+1}(s,X)\subseteq\boldsymbol{B}_L(s,X)$ and $\boldsymbol{G}_L(s,X)\subseteq\boldsymbol{G}_{L+1}(s,X)$.*

Definition 2 [1]. Fix a parameter ε, $0\le\varepsilon<1$. A code X of length N and size t is called a *disjunctive list-decoding* (LD) code of *strength* s with *list size* L and *error probability* ε (or an *(s_L,ε)-LD code*) if

$$\frac{|\boldsymbol{B}_L(s,X)|}{\binom{t}{s}}\le\varepsilon \quad\Longleftrightarrow\quad |\boldsymbol{G}_L(s,X)|\ge(1-\varepsilon)\binom{t}{s}. \tag{3}$$

Example. Let a code X of length $N=5$ and size $t=6$ be given by the matrix

$$X=\begin{bmatrix}1&0&0&0&1&1\\0&1&1&1&0&0\\0&1&1&0&1&0\\0&1&0&1&1&0\\0&0&1&1&1&1\end{bmatrix}. \tag{4}$$

Then the number of 2-subsets in $\{1,2,\ldots,6\}$ is $\binom{6}{2}=15$, and the set $\boldsymbol{B}_2(2,X)$ consisting of 2_2-bad sets for X is

$$\boldsymbol{B}_2(2,X)=\{(2;5),(2;6),(3;5),(4;5)\}.$$

Thus, according to (3) we conclude that X is a $(2_2,\frac{4}{15})$-LD code.

Definition 2 and Proposition 1 imply the following result.

Proposition 2. *Any (s_L,ε)-LD code X of length N and size t is an (s_{L+1},ε)-LD code of length N and size t.*

A similar relation between (s_L,ε)-LD codes when reducing the parameter $s\ge2$ with fixed $L\ge1$ is formulated as follows.

Proposition 3. *Let $s\ge2$ and $L\ge1$. For any (s_L,ε)-LD code X of size t and length N there exists an $((s-1)_L,\varepsilon)$-LD code X' of size $t-1$ and length N.*

Proof. Consider an arbitrary (s_L,ε)-LD code X of size t and length N. Let $\boldsymbol{B}_L(s,X,i)\triangleq\{\mathcal{S}:\ i\in S\in\boldsymbol{B}_L(s,X)\}$ denote the set of all s_L-bad subsets $\mathcal{S}$ for X containing an element $i\in[t]$.

Note that the sizes $|\boldsymbol{B}_L(s,X,i)|$, $0 \le |\boldsymbol{B}_L(s,X,i)| \le \binom{t-1}{s-1}$, $i \in [t]$, satisfy the constraint equation

$$\sum_{i=1}^{t} |\boldsymbol{B}_L(s,X,i)| = s|\boldsymbol{B}_L(s,X)|. \tag{5}$$

It follows from definition (3) and equality (5) that there exists a number $j \in [t]$ for which

$$|\boldsymbol{B}_L(s,X,j)| \le \frac{s}{t}|\boldsymbol{B}_L(s,X)| \le \frac{s}{t}\binom{t}{s}\varepsilon = \binom{t-1}{s-1}\varepsilon.$$

This inequality means that the code X' obtained from X by deleting the column $\boldsymbol{x}(j)$ is an $((s-1)_L,\varepsilon)$-LD code of size $t-1$ and length N. $\triangle$

Note that the notion of (s_L,ε)-LD codes is a natural generalization of classical s-superimposed codes introduces in 1964 in the pioneering work [2]. In particular, an s-superimposed code is an $(s_1,0)$-LD code. For $L \ge 1$ and $\varepsilon = 0$ disjunctive list-decoding (s_L-LD) codes were studied in [3–14], where the terminology given in Definition 2 was proposed. The best presently known results for s_L-LD codes are described in [15] (see also [16]).

Denote by $t_{\rm ld}(N,s,L)$ the maximum size of s_L-LD codes of length N, and by $N_{\rm ld}(t,s,L)$, the minimum length of s_L-LD codes of size t. The quantity

$$R_L(s) \triangleq \varlimsup_{N\to\infty} \frac{\log_2 t_{\rm ld}(N,s,L)}{N} = \varlimsup_{t\to\infty} \frac{\log_2 t}{N_{\rm ld}(t,s,L)} \tag{6}$$

is called [6,15] the *rate* of s_L-LD codes.

Using the traditional information-theoretic terminology accepted in probabilistic coding theory [17,18], introduce the following notions.

Definition 3 [1]. Fix a parameter $R > 0$. Taking into account the first inequality in (3), define the *error probability for almost disjunctive s_L-LD codes*:

$$\varepsilon_L(s,R,N) \triangleq \min_{X:\,t=\lfloor 2^{RN}\rfloor} \left\{ \frac{|\boldsymbol{B}_L(s,X)|}{\binom{t}{s}} \right\}, \quad R > 0, \tag{7}$$

where the minimum is over all (N,R) codes X. The function

$$\mathbf{E}_L(s,R) \triangleq \varlimsup_{N\to\infty} \frac{-\log_2 \varepsilon_L(s,R,N)}{N}, \quad R > 0, \tag{8}$$

will be referred to as the *error exponent for almost disjunctive s_L-LD codes*, the quantity

$$C_L(s) \triangleq \sup\{R:\ \mathbf{E}_L(s,R) > 0\}, \tag{9}$$

the *capacity of almost disjunctive s_L-codes*, and the rate $R_L(s)$ of s_L-LD code given by (6) will also be referred to as the *zero-rate capacity of almost disjunctive s_L-LD codes.*

Definitions (7)–(9) and Propositions 2 and 3 immediately imply the following result.

Theorem 1 (monotonicity properties). *For the capacities and error exponent of almost disjunctive s_L-LD codes we have the inequalities*

$$\begin{gathered} R_L(s+1) \le R_L(s) \le R_{L+1}(s), \qquad C_L(s+1) \le C_L(s) \le C_{L+1}(s), \\ \mathbf{E}_L(s+1,R) \le \mathbf{E}_L(s,R) \le \mathbf{E}_{L+1}(s,R), \quad s \ge 1, \quad L \ge 1, \quad R > 0. \end{gathered} \tag{10}$$

It was proved in [15] that, for any values of the parameters $s \geq 1$ and $L \geq 1$, the zero-rate capacity satisfies $R_L(s) \leq 1/s$. Using arguments similar to [15] (see Theorem 2), the same upper bound is established for the capacity $C_L(s)$ too. In [15], the *random coding method on the ensemble of constant-weight binary codes* was also developed and, based on it, a lower bound for $R_L(s)$ was constructed (see the statement of Theorem 3). The main goal of the present paper is to further develop this method to obtain (see the statement of Theorem 4 in Section 1.3) lower bounds on the capacity $C_L(s)$ and error exponent $\mathbf{E}_L(s, R)$. Furthermore, we will show that these bounds cannot be improved for the considered ensemble. Comparison of the upper bound on $R_L(s)$ obtained in [15] with the lower bound of Theorem 4 for a fixed $L \geq 1$ and large values of s leads to the strict inequality $R_L(s) < C_L(s)$, which, perhaps, is the most interesting result of this paper. Constructions and applications of s_L-LD and (s_L, ε)-LD codes are recalled and discussed in Sections 1.4 and 1.5.

1.2. Upper Bound for the Capacity $C_L(s)$

We prove the following result.

Theorem 2 ($C_L(s)$). *We have*

$$C_L(s) \leq 1/s, \quad s \geq 1, \quad L \geq 1.$$

Proof. Fix parameters R, $R > 0$, and ε, $0 \leq \varepsilon < 1$. Let X be an arbitrary (s_L, ε)-LD code of length N and size $t \triangleq \left\lfloor 2^{RN} \right\rfloor$. For any binary sequence $\boldsymbol{u} \in \{0,1\}^N$ consider the set

$$\boldsymbol{G}_L(s, \boldsymbol{u}, X) \triangleq \left\{ \mathcal{S} : \; \mathcal{S} \in \boldsymbol{G}_L(s, X), \; \bigvee_{i \in \mathcal{S}} \boldsymbol{x}(i) = \boldsymbol{u} \right\} \subset \boldsymbol{G}_L(s, X) \tag{11}$$

consisting of all s_L-good sets $\mathcal{S}$ for which the corresponding disjunctive sum of columns of X equals $\boldsymbol{u}$. It immediately follows from (11) and the interpretation of an s_L-good set in Definition 1 that

$$\boldsymbol{G}_L(s, \boldsymbol{u}, X) \cap \boldsymbol{G}_L(s, \boldsymbol{v}, X) = \varnothing, \quad \boldsymbol{u} \neq \boldsymbol{v}, \qquad \sum_{\boldsymbol{u} \in \{0,1\}^N} \boldsymbol{G}_L(s, \boldsymbol{u}, X) = \boldsymbol{G}_L(s, X), \tag{12}$$

and furthermore, for any $\boldsymbol{u} \in \{0,1\}^N$ we have

$$|\boldsymbol{G}_L(s, \boldsymbol{u}, X)| \leq \binom{s + L - 1}{s}, \quad \boldsymbol{u} \in \{0,1\}^N, \quad s \geq 1, \quad L \geq 1. \tag{13}$$

The second inequality in (3) and properties (12) and (13) mean that

$$(1 - \varepsilon)\binom{t}{s} \leq \sum_{\boldsymbol{u} \in \{0,1\}^N} |\boldsymbol{G}_L(s, \boldsymbol{u}, X)| \leq \binom{s + L - 1}{s} 2^N, \quad t = \left\lfloor 2^{RN} \right\rfloor. \tag{14}$$

Comparing the left- and right-hand sides of (14), we arrive at an asymptotic (as $N \to \infty$) lower bound on the error probability (7) of almost disjunctive s_L-LD codes:

$$\varepsilon_L(s, R, N) \geq 1 - \binom{s + L - 1}{s} 2^N \binom{t}{s}^{-1} = 1 - 2^{-N[(sR-1)+o(1)]}, \quad N \to \infty. \tag{15}$$

It follows from inequality (15) and definition (8) that the inequality $R < 1/s$ is a necessary condition for the error exponent $\mathbf{E}_L(s, R)$ as a function of R to be positive. Therefore, definition (9) implies that $C_L(s) \leq 1/s$. $\triangle$

Remark 1. The problem of improving the bound of Theorem 2 remains open. Note that the upper bound on $R_L(s)$ proved in [15] shows that an improvement of the upper bound $R_L(s) \leq 1/s$ for the zero-rate capacity is possible.

1.3. Lower Bounds for $R_L(s)$, $C_L(s)$, and $\mathbf{E}_L(s,R)$

The best presently known upper and lower bounds on the zero-rate capacity $R_L(s)$ are presented in [15] (see also [16]). In the classical case $L=1$, these bounds are

$$R_1(s) \le \overline{R}_1(s) = \frac{2\log_2 s}{s^2}(1+o(1)), \quad s\to\infty, \tag{16}$$

$$R_1(s) \ge \underline{R}_1(s) = \frac{4e^{-2}\log_2 s}{s^2}(1+o(1)) = \frac{0.542\log_2 s}{s^2}(1+o(1)), \quad s\to\infty. \tag{17}$$

For $L\ge 2$ and $s\ge 1$, random coding bounds on $R_L(s)$ are described in the following theorem.

Theorem 3 [15] (lower bounds on $R_L(s)$). *The following statements hold true*:

1. *For the zero-rate capacity, we have*

$$R_L(s) \ge \underline{R}_L^{(1)}(s) \triangleq \frac{1}{s+L-1}\max_{0<Q<1} A_L(s,Q) = \frac{1}{s+L-1}A_L(s,Q_L^{(1)}(s)), \tag{18}$$

$$A_L(s,Q) \triangleq \log_2\frac{Q}{1-y} - sK(Q,1-y) - LK\Bigl(Q,\frac{1-y}{1-y^s}\Bigr), \tag{19}$$

$$K(a,b) \triangleq a\log_2\frac{a}{b} + (1-a)\log_2\frac{1-a}{1-b}, \quad 0<a,b<1, \tag{20}$$

where y, $1-Q\le y<1$, on the right-hand side of (19) *is defined as a unique root of the equation*

$$y = 1-Q+Qy^s\left[1-\left(\frac{y-y^s}{1-y^s}\right)^L\right], \quad 1-Q\le y<1; \tag{21}$$

2. *For a fixed $L=2,3,\dots$ and $s\to\infty$, the asymptotic of the random coding bound $\underline{R}_L^{(1)}(s)$ given by* (18)–(21) *is of the form*

$$\underline{R}_L^{(1)}(s) = \frac{L}{s^2\log_2 e}(1+o(1)) = \frac{L\ln 2}{s^2}(1+o(1));$$

3. *For a fixed $s=1,2,3,\dots$ and $L\to\infty$, there exists the limit*

$$\begin{aligned} R_\infty(s) &\ge \underline{R}_\infty^{(1)}(s) \triangleq \lim_{L\to\infty}\underline{R}_L^{(1)}(s) \\ &= \log_2\left[\frac{(s-1)^{s-1}}{s^s}+1\right] = \frac{\log_2 e}{es}(1+o(1)) = \frac{0.5307}{s}(1+o(1)), \quad s\to\infty. \end{aligned} \tag{22}$$

By

$$[x]^+ \triangleq \begin{cases} x, & x\ge 0,\\ 0, & x<0,\end{cases}$$

and

$$h(a) \triangleq -a\log_2 a - (1-a)\log_2(1-a), \quad 0<a<1,$$

we denote the positive part of a function and the binary entropy function, respsectively.

Theorem 4 (lower bounds on $C_L(s)$ and $\mathbf{E}_L(s,R)$). *The following claims hold true*:

1. *The quantities $C_L(s)$ and $\mathbf{E}_L(s,R)$ satisfy the inequalities*

$$C_L(s) \ge \underline{C}(s) \triangleq \max_{0<Q<1} C(s,Q) = C(s,Q(s)), \quad s\ge 1, \quad L\ge 1, \tag{23}$$

$$C(s,Q) \triangleq h(Q) - [1-(1-Q)^s]\,h\Bigl(\frac{Q}{1-(1-Q)^s}\Bigr), \quad s\ge 1, \quad 0<Q<1, \tag{24}$$

and

$$\mathbf{E}_L(s,R) \ge \underline{\mathbf{E}}_L(s,R) \triangleq \max_{0<Q<1} E_L(s,R,Q), \quad s \ge 1, \quad L \ge 1, \quad R > 0, \tag{25}$$

$$E_L(s,R,Q) \triangleq \min_{Q \le q \le \min\{1,sQ\}} \left\{\mathcal{A}(s,Q,q) + L[h(Q) - qh(Q/q) - R]^+\right\}, \tag{26}$$

where the function $\mathcal{A}(s,Q,q)$, $Q < q < \min\{1,sQ\}$, *is defined as follows*:

$$\mathcal{A}(s,Q,q) \triangleq (1-q)\log_2(1-q) + q\log_2\left[\frac{Qy^s}{1-y}\right] + sQ\log_2\frac{1-y}{y} + sh(Q), \tag{27}$$

and y *on the right-hand side of* (27) *is a unique root of the equation*

$$q = Q\frac{1-y^s}{1-y}, \quad 0 < y < 1; \tag{28}$$

2. *As* $s \to \infty$, *the asymptotic of the random coding bound* $\underline{C}(s)$ *given by* (23) *and* (24) *and the asymptotic of the optimal value* $Q(s)$ *in* (23) *are of the forms*

$$\underline{C}(s) = \frac{\ln 2}{s}(1+o(1)), \qquad Q(s) = \frac{\ln 2}{s}(1+o(1)); \tag{29}$$

3. *For any* $s \ge 1$ *and* $L \ge 1$, *the lower bound* $\underline{E}_L(s,R)$ *defined in* (25)–(28) *is a cup-convex function of the parameter* $R > 0$. *For* $0 < R < \underline{C}(s)$ *we have* $\underline{E}_L(s,R) > 0$. *If* $R \ge \underline{C}(s)$, *then* $\underline{E}_L(s,R) = 0$. *Furthermore, there exists a number* $\underline{R}_L^{(\mathrm{cr})}(s)$, $0 \le \underline{R}_L^{(\mathrm{cr})}(s) < \underline{C}(s)$, *such that*

$$\underline{E}_L(s,R) = (s+L-1)\underline{R}_L^{(1)}(s) - LR \quad \text{if} \quad 0 \le R \le \underline{R}_L^{(\mathrm{cr})}(s) \tag{30}$$

and

$$\underline{E}_L(s,R) > (s+L-1)\underline{R}_L^{(1)}(s) - LR \quad \text{if} \quad R > \underline{R}_L^{(\mathrm{cr})}(s), \tag{31}$$

where the random coding bound $\underline{R}_L^{(1)}(s)$ *in Theorem* 3 *is defined by* (18)–(21).

Remark 2. In the proof of Theorem 4 we will show that the lower bound $\underline{E}_L(s,R)$ of the error exponent, $L \ge 2$, $s \ge 2$, given by (25)–(28) and obtained by the random coding method on the ensemble of constant-weight binary codes is *tight* for this ensemble, i.e., determines the logarithmic asymptotic of the ensemble average error probability of almost disjunctive s_L-LD codes.

In the table we give some numerical values of the function

$$\underline{R}_L(s) \triangleq \max\left\{\underline{R}_1(s), \underline{R}_L^{(1)}(s)\right\}, \quad 2 \le s \le 10, \quad 2 \le L \le 10,$$

and also optimal values $Q_L(s)$ which for $\underline{R}_L(s) = \underline{R}_L^{(1)}(s)$ equal to the weight $Q_L^{(1)}(s)$ on the right-hand side of (18), and for $\underline{R}_L(s) = \underline{R}_1(s)$ are denoted by $Q_L(s) \triangleq *$ (values of $\underline{R}_1(s)$ were computed in [15]). Thus, we have

$$Q_L(s) \triangleq \begin{cases} Q_L^{(1)}(s) & \text{if } \underline{R}_L(s) = \underline{R}_L^{(1)}(s) \text{ for } (2 \le s \le 6,\ L = 2) \cup (2 \le s \le 10,\ 3 \le L \le 10), \\ * & \text{if } \underline{R}_L(s) = \underline{R}_1(s) \text{ for } (7 \le s \le 10,\ L = 2). \end{cases}$$

Furthermore, the table presents numerical values of the lower bound on the capacity $\underline{C}(s)$ defined by (23) and (24) together with the optimal weight $Q(s)$ for $2 \le s \le 10$, and also numerical values of the upper bound on the zero-rate capacity $\overline{R}_1(s) < \underline{C}(s)$. This means that for $2 \le s \le 10$ the inequality $R_1(s) < C(s)$ holds. Moreover, asymptotic formulas (16) and (29) yield the strict inequality $R_1(s) < C(s)$ for large values of s.

In Fig. 1, for some values of s and L, we plot graphs of the error exponent $\underline{\mathbf{E}}_L(s,R)$ defined by (25)–(28) for the ensemble of constant-weight codes.

Table

s	2	3	4	5	6	7	8	9	10
$\underline{C}(s)$	0.3832	0.2455	0.1810	0.1434	0.1188	0.1014	0.0884	0.0784	0.0704
$Q(s)$	0.2864	0.2028	0.1569	0.1280	0.1080	0.0935	0.0824	0.0736	0.0666
$R_1^{(\mathrm{cr})}(s)$	0.3510	0.2284	0.1705	0.1364	0.1137	0.0976	0.0855	0.0761	0.0685
$\overline{R}_1(s)$	0.3219	0.1993	0.1405	0.1056	0.0830	0.0673	0.0559	0.0473	0.0407
s_L	2_2	2_3	2_4	2_5	2_6	2_7	2_8	2_9	2_{10}
$Q_L(s)$	0.244	0.233	0.226	0.221	0.218	0.215	0.212	0.211	0.209
$\underline{R}_L(s)$	0.2358	0.2597	0.2729	0.2813	0.2871	0.2915	0.2948	0.2975	0.2997
$\underline{R}_L^{(\mathrm{cr})}(s)$	0.3355	0.3279	0.3242	0.3226	0.3218	0.3216	0.3215	0.3215	0.3216
s_L	3_2	3_3	3_4	3_5	3_6	3_7	3_8	3_9	3_{10}
$Q_L(s)$	0.176	0.167	0.161	0.156	0.152	0.149	0.147	0.145	0.143
$\underline{R}_L(s)$	0.1147	0.1346	0.1469	0.1552	0.1611	0.1656	0.1690	0.1718	0.1741
$\underline{R}_L^{(\mathrm{cr})}(s)$	0.2177	0.2109	0.2065	0.2036	0.2017	0.2006	0.1998	0.1994	0.1992
s_L	4_2	4_3	4_4	4_5	4_6	4_7	4_8	4_9	4_{10}
$Q_L(s)$	0.139	0.133	0.128	0.123	0.120	0.117	0.115	0.113	0.111
$\underline{R}_L(s)$	0.0684	0.0838	0.0941	0.1014	0.1068	0.1110	0.1143	0.1170	0.1192
$\underline{R}_L^{(\mathrm{cr})}(s)$	0.1632	0.1580	0.1542	0.1514	0.1494	0.1479	0.1468	0.1460	0.1455
s_L	5_2	5_3	5_4	5_5	5_6	5_7	5_8	5_9	5_{10}
$Q_L(s)$	0.115	0.110	0.106	0.103	0.100	0.098	0.096	0.094	0.092
$\underline{R}_L(s)$	0.0456	0.0575	0.0660	0.0723	0.0771	0.0809	0.0840	0.0865	0.0886
$\underline{R}_L^{(\mathrm{cr})}(s)$	0.1311	0.1271	0.1240	0.1216	0.1197	0.1183	0.1171	0.1162	0.1155
s_L	6_2	6_3	6_4	6_5	6_6	6_7	6_8	6_9	6_{10}
$Q_L(s)$	0.098	0.095	0.092	0.089	0.086	0.084	0.083	0.081	0.080
$\underline{R}_L(s)$	0.0325	0.0420	0.0490	0.0544	0.0587	0.0621	0.0649	0.0672	0.0692
$\underline{R}_L^{(\mathrm{cr})}(s)$	0.1098	0.1067	0.1041	0.1021	0.1004	0.0991	0.0980	0.0971	0.0963
s_L	7_2	7_3	7_4	7_5	7_6	7_7	7_8	7_9	7_{10}
$Q_L(s)$	$*$	0.083	0.080	0.078	0.076	0.074	0.073	0.072	0.070
$\underline{R}_L(s)$	0.0260	0.0321	0.0380	0.0426	0.0463	0.0494	0.0519	0.0541	0.0559
$\underline{R}_L^{(\mathrm{cr})}(s)$	0.0945	0.0920	0.0899	0.0882	0.0868	0.0855	0.0845	0.0837	0.0829
s_L	8_2	8_3	8_4	8_5	8_6	8_7	8_8	8_9	8_{10}
$Q_L(s)$	$*$	0.074	0.072	0.070	0.068	0.067	0.065	0.064	0.063
$\underline{R}_L(s)$	0.0213	0.0253	0.0303	0.0343	0.0376	0.0403	0.0426	0.0446	0.0463
$\underline{R}_L^{(\mathrm{cr})}(s)$	0.0830	0.0810	0.0793	0.0778	0.0765	0.0754	0.0745	0.0737	0.0730
s_L	9_2	9_3	9_4	9_5	9_6	9_7	9_8	9_9	9_{10}
$Q_L(s)$	$*$	0.067	0.065	0.063	0.062	0.061	0.059	0.058	0.057
$\underline{R}_L(s)$	0.0178	0.0205	0.0248	0.0283	0.0312	0.0336	0.0357	0.0375	0.0391
$\underline{R}_L^{(\mathrm{cr})}(s)$	0.0741	0.0724	0.0709	0.0696	0.0685	0.0676	0.0667	0.0660	0.0654
s_L	10_2	10_3	10_4	10_5	10_6	10_7	10_8	10_9	10_{10}
$Q_L(s)$	$*$	0.061	0.059	0.058	0.057	0.056	0.054	0.054	0.053
$\underline{R}_L(s)$	0.0151	0.0169	0.0206	0.0237	0.0263	0.0285	0.0304	0.0320	0.0335
$\underline{R}_L^{(\mathrm{cr})}(s)$	0.0668	0.0654	0.0642	0.0631	0.0621	0.0612	0.0605	0.0598	0.0592

1.4. Constructions of s_1-LD and (s_1, ε)-LD Codes

Constructions of s_1-LD codes base on shortened Reed–Solomon codes were given in [10,11]. The authors of those papers considerably extended a number of optimal and close-to-optimal constructions of s-superimposed codes proposed in the classical paper [2] and developed *systematic tables* for the description of parameters of these constructions. Furthermore, Table 3 in [11], as well

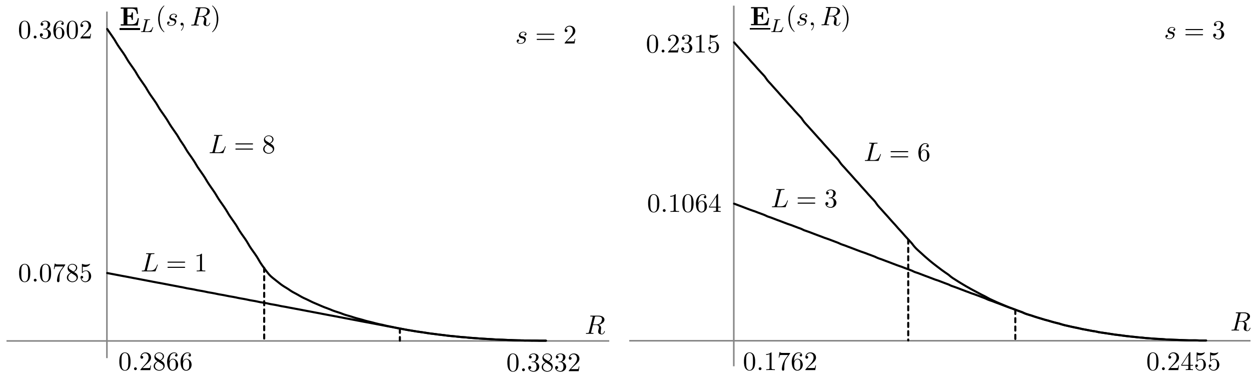

Fig. 1. Error exponent $\underline{\mathbf{E}}_L(s,R)$.

as a similar table in [12], presented series of numerical values of (t,N,s,ε) for the best presently known constructions of (s_1,ε)-LD codes based on MDS codes. In a recent paper [19], for the values (t,N,s,ε) there were established the following parametric constraint relations:

$$t = q^{\left\lfloor \frac{q}{\log_2 q} \right\rfloor}, \quad N = q(q+1), \quad \varepsilon = \varepsilon(q) \to 0 \quad \text{for} \quad s = q\sigma, \quad \sigma < \ln 2, \tag{32}$$

where q is a prime power, $q \to \infty$. Formulas (32) mean that, as $s \to \infty$ and $q \to \infty$, the asymptotic of the rate of the corresponding (s_1,ε)-LD codes is

$$\frac{\log_2 t}{N} = \frac{1}{q}(1+o(1)) = \frac{\ln 2}{s}(1+o(1)),$$

which coincides with the asymptotic of the random coding bound $\underline{C}(s)$ given in (29).

1.5. Applications of s_L-LD and (s_L,ε)-LD Codes

1. Consider a *feedback communication system* [8] (see also [3]) containing M *terminal stations* $S_1,\dots,S_M$ and a *multiple access channel* (MAC) which links them to a *central station* (CS). At each of the M stations there is a *source* of packets, which are sequences sequences of binary symbols (0 and 1) of the same length K. The generated packets, referred to as *information* packets, or *requests*, are transmitted to the CS, which is interested in *only content* of a request but not in which station it has come from. This situation may occur in an enquiry system[1] when answers to all requests are simultaneously transmitted through a broadcasting channel (BC) from the CS to all the M stations (Fig. 2).

Put $t \triangleq 2^K$ and enumerate all the 2^K packets (requests) that can arrive at a station by integers from 1 to t. Let $N \ge K$ be an integer, and let X (see (1)) be a binary code of length N and size t; its codeword $\boldsymbol{x}(j) \triangleq (x_1(j), x_2(j), \dots, x_N(j))$, $j \in [t]$, will be referred to as a *code* packet for the request with number $j \in [t]$. Assume that operation time of the MAC is split into slots of the same length. Within each slot, which is split into N time units synchronously for all the M stations, each station is either silent or uses *one and the same code* X known to the CS to transmit a code packet corresponding to the generated request, and in each time unit one binary symbol of the code packet is transmitted. We assume that *pulse modulation* is used to transmit binary symbols $(0,1)$ *through a real time channel*; for instance, 1 (0) is encoded by a signal in which a given pulse is present (absent) during this time unit. We also assume that during a slot of length N requests to be transmitted to the CS appear at no more than $s \ge 1$ stations, where $s \ll t = 2^K$. Let $\mathcal{S}$, $\mathcal{S} \subset [t]$, $0 \le |\mathcal{S}| \le s$, denotes a set of numbers of requests (unknown to the CS) generated at the stations

[1] For example, when all stations enquire about weather forecast.

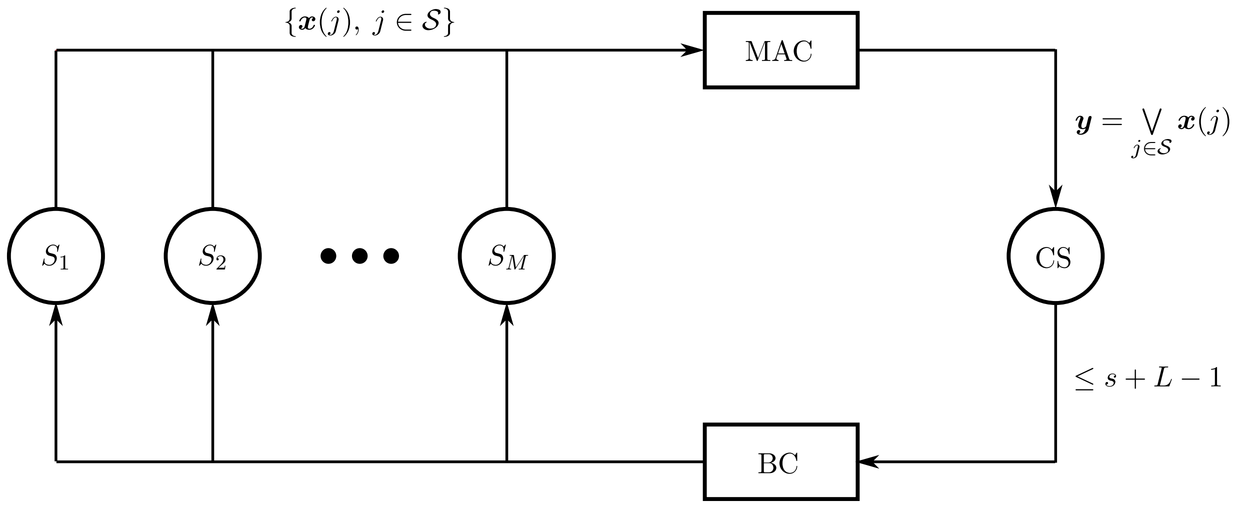

Fig. 2. Feedback communication system.

during this slot. Clearly, for this pulse modulation, as a model of the MAC we may consider a *disjunctive* model, which by definition means that a sequence $\boldsymbol{y}$ of length N at the output of the MAC is the disjunctive sum composed of the code packets $\boldsymbol{x}(j)$, $j \in \mathcal{S}$.

For a fixed $s \ge 1$, let an integer $L \ge 1$ be chosen so that $s+L-1$ defines the *capacity* of the BC, i.e., the maximum possible number of packets that can be (correctly) transmitted through the BC over time N. Operation of a CS using either an s_L-LD or (s_L,ε)-LD code X is described as follows. After receiving a packet $\boldsymbol{y}$, the CS *selects* (finds) in the code X, known to it, all code packets $\boldsymbol{x}(j_1), \boldsymbol{x}(j_2), \ldots, \boldsymbol{x}(j_k)$ that are *covered by* $\boldsymbol{y}$. Necessarily, among them there are the packets $\boldsymbol{x}(j)$, $j \in \mathcal{S} \subseteq \mathcal{S}_k \triangleq \{j_1, j_2, \ldots, j_k\} \subset [t]$. The number $k = k(\boldsymbol{y}, X) \ge |\mathcal{S}|$ of code packets covered by $\boldsymbol{y}$ is interpreted by the CS as the *number of requests* arrived within this slot. Then two situations are considered.

(a) If $k \le s+L-1$, then the CS *answers* through the BC to all requests corresponding to the numbers $\mathcal{S}_k = \{j_1, j_2, \ldots, j_k\}$ of the selected packets, in particular, to *real* requests with numbers in $\mathcal{S}$ (successful transmission of requests). In this case the CS transmits $k - |\mathcal{S}| \le s+L-1-|\mathcal{S}|$ superfluous answers through the BC.

(b) If $k \ge s+L$, which is possible when an (s_L,ε)-LD code X is used, then the CS *is silent*, answering to none of the requests arrived within this slot (refusal). By the definition of an (s_L,ε)-LD code, the refusal probability in this system is at most ε.

2. Consider the classical disjunctive (or superimposed) model [2] of *nonadaptive* (or static) *search* for $\le s$, $s < t$, *defectives* among elements of $[t]$. Assume that it is required to find an unknown set $\mathcal{S} \subset [t]$, $|\mathcal{S}| \le s$, of defectives (*defective set*) using N *group tests* $G_i \subset [t]$, $i \in [N]$, which are in a one-to-one correspondence with rows $\boldsymbol{x}_i \triangleq (x_i(1), x_i(2), \ldots, x_i(t))$, $i \in [N]$, of a binary code $X = \|x_i(j)\|$, $i \in [N]$, $j \in [t]$, namely:

$$x_i(j) \triangleq \begin{cases} 1 & \text{if } j \in G_i, \\ 0 & \text{if } j \notin G_i,\ i \in [N],\ j \in [t]. \end{cases}$$

The code X is said to be a nonadaptive (static) search *design*, and a binary *outcome* y_i of a test $G_i \subset [t]$, $i \in [N]$, for a defective set $\mathcal{S}$ in the disjunctive search model is

$$y_i \triangleq \begin{cases} 1 & \text{if } \mathcal{S} \cap G_i \ne \varnothing, \\ 0 & \text{if } \mathcal{S} \cap G_i = \varnothing,\ i \in [N],\ j \in [t]. \end{cases}$$

In other words, $y_i = 1$ is the outcome of a test if and only if the tested group G_i, $i \in [N]$, contains at least one element of the defective set $\mathcal{S}$. After carrying out all N tests, defective set $\mathcal{S}$ is identified based on the binary sequence $\boldsymbol{y} \triangleq (y_1, y_2, \ldots, y_N)$, which, as is easily seen, is the disjunctive sum of the codewords $\boldsymbol{x}(j)$, $j \in \mathcal{S}$.

Constructions and application of s_L-LD codes for this search model (for $s \ll t$) were studied in [11, 12] (see also [9]) in connection with the problem of constructing *two-stage* group tests for the analysis of a DNA clone library arising in molecular biology. At the *first* nonadaptive stage, as well as in the above-described application for the MAC and CS, an s_L-LD or (s_L, ε)-LD code X is applied to *select* some subset

$$\mathcal{S}_k = \{j_1, j_2, \ldots, j_k\} \subset [t], \quad 1 \le j_1 < j_2 < \cdots < j_k \le t, \quad \mathcal{S} \subseteq \mathcal{S}_k,$$

consisting of $k = k(\boldsymbol{y}, X) \ge |\mathcal{S}|$, $k \le s + L - 1$ ($k \le s + L - 1$ *with reliability* $\ge 1 - \varepsilon$), elements of $[t]$ and containing a defective set $\mathcal{S}$, $|\mathcal{S}| \le s$. After that, at the *second* nonadaptive stage, both in the cases of an s_L-LD and (s_L, ε)-LD code, the selected elements $\mathcal{S}_k$ are tested *one by one*; i.e., for $i = N+1, N+2, \ldots, N+k$ the group test is

$$G_i \triangleq \{j_i\}, \quad |G_i| = 1.$$

Analysis of the outcomes y_i, $i = N+1, N+2, \ldots, N+k$, of these last $k \le s + L - 1$ static tests, where $y_i = 1$ if and only if $j_i \in \mathcal{S}$, yields an obvious *identification* of the defective set $\mathcal{S} \subseteq \mathcal{S}_k$.

By virtue of Theorem 3 and monotonicity property (10), the zero-rate capacity $R_L(s)$ for large values of L can be interpreted as the *maximum rate* $\log_2 t/N$ of operation of a communication system (in application 1) or as the maximum rate of two-stage group testing (in application 2) with the use of s_L-LD codes. Therefore, it follows from (22) that *when using s_L-LD codes*, for large values of s we have the lower bound for the rate

$$\log_2 t/N \ge \lim_{L\to\infty} \underline{R}^1_L(s) = \frac{\log_2 e}{es}(1 + o(1)) = \frac{0.5307}{s}(1 + o(1)), \quad s \to \infty.$$

According to Theorem 4, for large values of L the capacity of (s_L, ε)-LD codes $C_L(s)$ can be interpreted as the maximum rate $\log_2 t/N$ of operation of a communication system (in application 1) with refusal probability $\varepsilon \to 0$ or as the maximum rate of two-stage group testing (in application 2) with reliability $(1 - \varepsilon) \to 1$. Therefore, if follows from (23), (24), and (29) that *when using (s_L, ε)-LD codes*, for large values of s we have the lower bound for the rate

$$\log_2 t/N \ge \lim_{L\to\infty} \underline{C}_L(s) = \underline{C}(s) = \frac{\ln 2}{s}(1 + o(1)) = \frac{0.6931}{s}(1 + o(1)), \quad s \to \infty.$$

1.6. Disjunctive Weakly Separating Search Designs

Notions similar to Definitions 1–3 were previously introduced in [20–26] to describe an information-theoretic and coding-theoretic model referred to as *designing screening experiments*; in our particular case of a disjunctive model, the following terminology was used.

A set $\mathcal{S}$, $\mathcal{S} \subset [t]$, $|\mathcal{S}| = s$, is said to be *s-bad* for a code X if there exists a set $\widetilde{\mathcal{S}} \subset [t]$, $\widetilde{\mathcal{S}} \ne \mathcal{S}$, of size $|\widetilde{\mathcal{S}}| = |\mathcal{S}| = s$ such that $\bigvee\limits_{i\in\widetilde{\mathcal{S}}} \boldsymbol{x}(i) = \bigvee\limits_{j\in\mathcal{S}} \boldsymbol{x}(j)$. Otherwise, $\mathcal{S}$ is said to be *s-good* for X.

Let $\widetilde{\boldsymbol{B}}(s, X)$ (respectively, $\widetilde{\boldsymbol{G}}(s, X)$) denote the set of *all* s-bad (s-good) sets $\mathcal{S}$ for a code X, and let $|\widetilde{\boldsymbol{B}}(s, X)|$ (respectively, $|\widetilde{\boldsymbol{G}}(s, X)|$) be the cardinality of this set. Clearly, we have

$$0 \le |\widetilde{\boldsymbol{B}}(s, X)| \le \binom{t}{s}, \qquad 0 \le |\widetilde{\boldsymbol{G}}(s, X)| \le \binom{t}{s}, \qquad |\widetilde{\boldsymbol{B}}(s, X)| + |\widetilde{\boldsymbol{G}}(s, X)| = \binom{t}{s},$$

and arguing by contradiction (cf. [6, 15]) one can check that for any value of $s \ge 1$ there are the following relations with notions introduced in Definition 1:

$$\widetilde{\boldsymbol{B}}(s,X) \subseteq \boldsymbol{B}_1(s,X), \quad \boldsymbol{G}_1(s,X) \subseteq \widetilde{\boldsymbol{G}}(s,X),$$
$$|\widetilde{\boldsymbol{B}}(s,X)| \le |\boldsymbol{B}_1(s,X)|, \quad |\boldsymbol{G}_1(s,X)| \le |\widetilde{\boldsymbol{G}}(s,X)|.$$

By analogy with Definition 2, a code X (1) is called [21, 22] a disjunctive *weakly separating design of strength* s with *error probability* ε, $0 < \varepsilon < 1$ (or an (s,ε)-*design*) if

$$\frac{|\widetilde{\boldsymbol{B}}(s,X)|}{\binom{t}{s}} \le \varepsilon \quad \Longleftrightarrow \quad |\widetilde{\boldsymbol{G}}(s,X)| \ge (1-\varepsilon)\binom{t}{s}.$$

For $\varepsilon = 0$, following [15], we will refer to disjunctive $(s,0)$-designs as disjunctive s-designs. The best presently known results for disjunctive s-designs are described in [15]. Denote by $\widetilde{t}(N,s)$ the maximum size of disjunctive s-designs of length N, and by $\widetilde{N}(t,s)$, the maximum length of disjunctive s-designs of size t. The function

$$\widetilde{R}(s) \triangleq \varlimsup_{N\to\infty} \frac{\log_2 \widetilde{t}(N,s)}{N} = \varlimsup_{t\to\infty} \frac{\log_2 t}{\widetilde{N}(t,s)} \tag{33}$$

is called [6, 15] the *rate* of disjunctive s-designs.

Fix a parameter $R \ge 0$ and define the *error probability of disjunctive weakly separating* s-*designs*

$$\widetilde{\varepsilon}(s,R,N) \triangleq \min_{X:\, t=\lfloor 2^{RN}\rfloor} \left\{ \frac{|\widetilde{\boldsymbol{B}}(s,X)|}{\binom{t}{s}} \right\}, \quad R > 0, \tag{34}$$

where the minimum is over all (N,R) codes X. We call the function

$$\widetilde{E}(s,R) \triangleq \varlimsup_{N\to\infty} \frac{-\log_2 \widetilde{\varepsilon}(s,R,N)}{N}, \quad R > 0, \tag{35}$$

the *error exponent of disjunctive weakly separating* s-*designs*, the number

$$\widetilde{C}(s) \triangleq \sup\{R:\ \widetilde{E}(s,R) > 0\} \tag{36}$$

is the *capacity of disjunctive weakly separating* s-*designs*, and the rate $\widetilde{R}(s)$ of disjunctive s-designs defined in (33) will also be referred to as the *zero-rate capacity of disjunctive weakly separating* s-*designs*.

It was shown in [20,21] that $\widetilde{C}(s) = 1/s$ for $s \ge 1$. We conjecture that for any $s \ge 2$ the zero-rate capacity satisfies the inequality $\widetilde{R}(s) < 1/s$, i.e., is *strictly less* than $\widetilde{C}(s)$. At present, validity of this conjecture is proved for the cases $s = 2$ and $s \ge 11$: for $s = 2$ the inequality $\widetilde{R}(2) < 1/2$ is established in [27], and for $s \ge 11$ the inequality $\widetilde{R}(s) < 1/s$ is obtained in [15].

The numerical values presented in the table show that for the lower bound on the capacity of almost disjunctive s_L-LD for $2 \le s \le 10$ we have $\underline{C}(s) < 1/s = \widetilde{C}(s)$, and the asymptotic relation (29) means that, as $s \to \infty$, this lower bound behaves as $\underline{C}(s) \sim \dfrac{\ln 2}{s}$.

However, despite their high rate, *using* (s,ε)-designs in the identification problem for defective sets $\mathcal{S}$, $|\mathcal{S}| = s$, with the use of nonadaptive group tests is *practically impossible* due to the very high complexity of analysis of results, which obviously coincides with the exhaustive search complexity $\binom{t}{s} \sim t^s/s!$. For comparison, as is shown in Section 1.5, for $s \ge 2$ the identification complexity for a defective set $\mathcal{S}$, $|\mathcal{S}| \le s$, with the use of (s_L, ε)-codes is considerably smaller and is of the order of t.

Disjunctive weakly separating s-designs are [14, 26] an important example of an information-theoretic model for a *multiple access channel* (MAC) [18]. The capacity of weakly separating designs for the general MAC model was found in [22]. In the case of a symmetric MAC, the ensemble average error exponent for weakly separating designs was studied and has been computed in a series of works [23–26].

2. PROOF OF THEOREM 4

Proof of Claim 1. The number $|\boldsymbol{B}_L(s, X)|$ of all s_L-bad sets $\mathcal{S} \subset [t]$, $|\mathcal{S}| = s$, for a code X can be represented as follows:

$$|\boldsymbol{B}_L(s, X)| \triangleq \sum_{\mathcal{S} \in [t],\, |\mathcal{S}|=s} \psi_L(X, \mathcal{S}), \tag{37}$$

where

$$\psi_L(X, \mathcal{S}) \triangleq \begin{cases} 1 & \text{if } \mathcal{S} \in \boldsymbol{B}_L(s, X), \\ 0 & \text{otherwise.} \end{cases}$$

Fix parameters Q, $0 < Q < 1$, and $R > 0$. Define an ensemble $\{N, t, Q\}$ of binary matrices X with N rows and $t \triangleq \lfloor 2^{RN} \rfloor$ columns, where columns are independently and uniformly chosen from the set consisting of $\binom{N}{w}$ columns of a fixed weight $w \triangleq \lfloor QN \rfloor$. It directly follows from (37) that for the ensemble $\{N, t, Q\}$ the expectation of $|\boldsymbol{B}_L(s, X)|$ is

$$\overline{|\boldsymbol{B}_L(s, X)|} = \binom{t}{s} \Pr\{\mathcal{S} \in \boldsymbol{B}_L(s, X)\},$$

where for any s-set $\mathcal{S}$ the probability on the right-hand side depends only on the parameters s, L, R, Q, and N and does not depend on the choice of a particular set $\mathcal{S}$. Hence, the expectation of the fraction of all s_L-bad sets $\mathcal{S} \subset [t]$, $|\mathcal{S}| = s$, is

$$\mathcal{E}_L^{(N)}(s, R, Q) \triangleq \binom{t}{s}^{-1} \overline{|\boldsymbol{B}_L(s, X)|} = \Pr\{\mathcal{S} \in \boldsymbol{B}_L(s, X)\}. \tag{38}$$

Therefore, an obvious *random coding* upper bound for the error probability (7) of almost disjunctive s_L-codes can be represented as follows:

$$\varepsilon_L(s, R, N) \triangleq \min_{X:\, t=\lfloor 2^{RN} \rfloor} \left\{ \frac{|\boldsymbol{B}_L(s, X)|}{n\binom{t}{s}} \right\} \le \mathcal{E}_L^{(N)}(s, R, Q), \quad 0 < Q < 1. \tag{39}$$

We rewrite the function $\mathcal{E}_L^{(N)}(s, R, Q)$ defined in (38) as

$$\mathcal{E}_L^{(N)}(s, R, Q) = \sum_{k=\lfloor QN \rfloor}^{\min\{N, s\lfloor QN \rfloor\}} \Pr\left\{ \mathcal{S} \in \boldsymbol{B}_L(s, X) \Big/ \left| \bigvee_{i \in \mathcal{S}} \boldsymbol{x}(i) \right| = k \right\} \mathcal{P}^{(N)}(s, Q, k). \tag{40}$$

Here we have applied the total probability formula and used the notation

$$\mathcal{P}^{(N)}(s, Q, k) \triangleq \Pr\left\{ \left| \bigvee_{i \in \mathcal{S}} \boldsymbol{x}(i) \right| = k \right\}, \quad \lfloor QN \rfloor \le k \le \min\{N, s\lfloor QN \rfloor\}. \tag{41}$$

For the ensemble $\{N,t,Q\}$ and an arbitrary k, $\lfloor QN\rfloor \le k \le \min\{N, s\lfloor QN\rfloor\}$, the conditional probability of the event (2) is

$$\Pr\left\{\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i) \succeq \bigvee_{j\in\mathcal{L}}\boldsymbol{x}(j) \Bigm/ \left|\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\right| = k\right\} = \left[\frac{\binom{k}{\lfloor QN\rfloor}}{\binom{N}{\lfloor QN\rfloor}}\right]^L. \tag{42}$$

Furthermore, using the terminology of *types* (see [18])

$$\{n(\boldsymbol{u})\}, \quad \boldsymbol{u} \triangleq (u_1,u_2,\ldots,u_s)\in\{0,1\}^s, \quad 0\le n(\boldsymbol{u})\le N, \quad \sum_{\boldsymbol{u}} n(\boldsymbol{u}) = N,$$

we may write the probability of the event (41) in the ensemble $\{N,t,Q\}$ as

$$\mathcal{P}^{(N)}(s,Q,k) = \binom{N}{\lfloor QN\rfloor}^{-s}\sum_{(44)}\frac{N!}{\prod\limits_{\boldsymbol{u}} n(\boldsymbol{u})!}, \quad \lfloor QN\rfloor \le k\le \min\{N, s\lfloor QN\rfloor\}, \tag{43}$$

where the sum on the right-hand side of (43) is over all types $\{n(\boldsymbol{u})\}$ satisfying the condition

$$n(\boldsymbol{0}) = N-k, \qquad \sum_{\boldsymbol{u}\colon u_i=1} n(\boldsymbol{u}) = \lfloor QN\rfloor, \quad \text{for any } i\in[s]. \tag{44}$$

Let

$$\mathcal{A}(s,Q,q) \triangleq \lim_{N\to\infty}\frac{-\log_2\mathcal{P}^{(N)}(s,Q,\lfloor qN\rfloor)}{N}, \quad Q\le q\le\min\{1,sQ\}, \tag{45}$$

denote the main term of the asymptotic of the probability (41) computed according to (43) and (44).

Then, using representation (40), conditional probability (42), and the standard estimate

$$\Pr\left\{\bigcup_i C_i \,/C\right\} \le \min\left\{1; \sum_i \Pr\{C_i/C\}\right\},$$

we obtain an upper bound

$$\mathcal{E}_L^{(N)}(s,R,Q) \le \sum_{k=\lfloor QN\rfloor}^{\min\{N,s\lfloor QN\rfloor\}}\mathcal{P}^{(N)}(s,Q,k)\min\left\{1; \binom{t-s}{L}\left[\frac{\binom{k}{\lfloor QN\rfloor}}{\binom{N}{\lfloor QN\rfloor}}\right]^L\right\}, \tag{46}$$

where the code size is $t\triangleq\lfloor 2^{RN}\rfloor$. Inequality (46) and the random coding bound (39) imply the *lower bound* on the error exponent (8) given by (25) and (26).

In Section 3 we will prove the following result.

Lemma 1. *Let* $\lfloor QN\rfloor \le k\le\min\{N, s\lfloor QN\rfloor\}$. *For the conditional probability on the right-hand side of* (40) *we have the estimate*

$$\Pr\left\{\mathcal{S}\in\boldsymbol{B}_L(s,X) \Bigm/ \left|\bigvee_{i\in\mathcal{S}}\boldsymbol{x}(i)\right| = k\right\} \ge D(s,L)\min\left\{1; \binom{t-s}{L}\left[\frac{\binom{k}{\lfloor QN\rfloor}}{\binom{N}{\lfloor QN\rfloor}}\right]^L\right\}, \tag{47}$$

where the quantity $D(s,L)$ *is independent of the length* N *and size* t *of the code* X.

It is readily seen that Lemma 1 establishes asymptotic tightness of estimate (46); i.e., there exists the limit

$$\lim_{N\to\infty}\frac{-\log_2\mathcal{E}_L^{(N)}(s,R,Q)}{N} = E_L(s,R,Q), \quad R>0.$$

Analytical properties of the function (45) are formulated as Lemmas 2–4, which will also be proved in Section 3.

Lemma 2. *The function $\mathcal{A}(s,Q,q)$ of the parameter q, $Q < q < \min\{1, sQ\}$, defined in* (45) *can be represented in the parametric form* (27) *and* (28). *Furthermore, this function is $\cup$-convex, monotonically decreases on the interval $(Q, 1-(1-Q)^s)$, and monotonically decreases on the interval $(1-(1-Q)^s, \min\{1,sQ\})$; the minimum of $\mathcal{A}(s,Q,q)$, equal to zero, is attained at the point $q = 1-(1-Q)^s$, i.e.*,

$$\min_{Q<q<\min\{1,sQ\}} \mathcal{A}(s,Q,q) = \mathcal{A}(s,Q,1-(1-Q)^s) = 0, \quad 0 < Q < 1.$$

Lemma 3. *For any fixed Q, $0 < Q < 1$, the function*

$$f(Q,q) \triangleq qh(Q/q), \quad Q < q < \min\{1, sQ\},$$

is cap-convex and monotonically increasing.

Lemma 4. *For any fixed Q, $0 < Q < 1$, the function*

$$\mathcal{A}(s,Q,q) + L[h(Q) - qh(Q/q)], \quad Q < q < \min\{1, sQ\}, \tag{48}$$

is cup-convex. Its minimum is attained at $q = q_L^{(2)}(s,Q) > 1-(1-Q)^s$ and is equal to the quantity $A_L(s,Q)$ given by (19)–(21), *i.e.*,

$$\min_{Q<q<\min\{1,sQ\}} \{\mathcal{A}(s,Q,q) + L[h(Q) - qh(Q/q)]\} = A_L(s,Q),$$
$$q_L^{(2)}(s,Q) \triangleq \operatorname*{arg\,min}_{Q<q<\min\{1,sQ\}} \{\mathcal{A}(s,Q,q) + L[h(Q) - qh(Q/q)]\}.$$

Following the assertion of Lemma 2 and equations (24) and (26), one can easily check that $E_L(s,Q) > 0$ for $0 < R < C(s,Q)$.

Claim 1 is proved. $\triangle$

Proof of Claim 2. Rewrite (24) in a more convenient form:

$$C(s,Q) = (1 - Q - (1-Q)^s)\log_2\left[1 - \frac{Q(1-Q)^{s-1}}{1-(1-Q)^s}\right] \\ - Q\log_2[1-(1-Q)^s] - (1-Q)^s\log_2[1-Q]. \tag{49}$$

Fix a parameter $a > 0$. Then, with the substitution $Q = \dfrac{a}{s}$ in (49), the asymptotic of $C(s,Q)$ takes the following form:

$$C\left(s, \frac{a}{s}\right) = \frac{-a\log_2\left[1-e^{-a}\right]}{s}(1+o(1)), \quad s \to \infty. \tag{50}$$

Taking the derivative with respect to a, one easily checks that the maximum

$$\max_{a>0}\left\{-a\log_2\left[1-e^{-a}\right]\right\} = \ln 2$$

is attained at $a = \ln 2$. Hence,

$$\underline{C}(s) = \max_{0<Q<1} C(s,Q) \ge \frac{\ln 2}{s}(1+o(1)), \quad s \to \infty. \tag{51}$$

To complete the proof of claim 2, we show that the reverse asymptotic inequality also holds.

Let $0 < Q(s) < 1$, $s = 2, 3, \ldots$, be a sequence such that

$$\max_{0<Q<1} C(s,Q) \triangleq C(s, Q(s)) = \underline{C}(s).$$

Assume that $Q(s) > b$ for some $b > 0$. Then from (49) one can obtain the inequality

$$C(s, Q(s)) \le (1-b)^s O(1), \quad s \to \infty,$$

which contradicts (51). Thus, without loss of generality, we may assume that $Q(s) \to 0$ as $s \to \infty$.

Similarly, assume that

$$0 < Q(s) = f(s)/s < 1, \qquad \lim_{s\to\infty} f(s) = \infty, \qquad f(s) = o(s).$$

Then

$$\lim_{s\to\infty} (1 - Q(s))^s \le \lim_{s\to\infty} e^{-f(s)} = 0.$$

Using this property and the expansion of the logarithm at zero

$$\log_2(1+x) = \log_2 e \cdot x(1+o(1)),$$

we transform (49) to

$$C(s, Q(s)) = Q(s)[1-Q(s)]^s O(1), \quad s \to \infty.$$

Then we arrive at the equality

$$\lim_{s\to\infty} sC(s, Q(s)) = \lim_{s\to\infty} sQ(s)(1-Q(s))^s O(1) = 0,$$

which contradicts (51). Hence, we may assume without loss of generality that $sQ(s) \to a$ as $s \to \infty$, and moreover, $0 \le a < \infty$.

Similarly it can be shown that if $a = 0$, we arrive at the asymptotic inequality $C(s, Q(s)) = Q \ln[sQ]O(1)$, which contradicts (51). Thus, we have the asymptotic (29). $\triangle$

Proof of Claim 3. It is easily seen that if $E_L(s, R, Q)$ is a $\cup$-convex function of R for $0 < Q < 1$, then $\underline{E}_L(s, R)$ is also a $\cup$-convex function of R. Let us prove the $\cup$-convexity of $E_L(s, R, Q)$.

Fix parameters Q and R, $0 < Q < 1$, $0 < R < 1$. Let $q^{(0)}(s, Q) \triangleq 1 - (1-Q)^s$. Lemmas 2–4 imply that the minimum in (26) is attained at some point in the interval $[q^{(0)}(s, Q), q_L^{(2)}(s, Q)]$. Consider the function

$$\mathcal{B}(R, Q, q) = h(Q) - qh(Q/q) - R.$$

Let a solution of $q = q^{(1)}(R, Q)$ of the equation $\mathcal{B}(R, Q, q) = 0$, $0 < q < 1$, exist. Then note that the minimum in (26) is attained at $q = q_L^{(\min)}(s, R, Q)$, where

$$q_L^{(\min)}(s, R, Q) = \begin{cases} q_L^{(2)}(s, Q) & \text{if } \mathcal{B}(R, Q, q^{(2)}) \ge 0, \\ q^{(1)}(R, Q) & \text{if } \mathcal{B}(R, Q, q^{(0)}) > 0 \text{ and } \mathcal{B}(R, Q, q^{(2)}) < 0, \\ q^{(0)}(s, Q) & \text{if } \mathcal{B}(R, Q, q^{(0)}) \le 0. \end{cases}$$

Substituting $q = q_L^{(\min)}(s, R, Q)$ into (26) yields

$$E_L(s, R, Q) = \begin{cases} A_L(s, Q) - LR & \text{if } 0 \le R \le \underline{R}_L^{(\mathrm{cr})}(s, Q), \\ \mathcal{A}(s, Q, q^{(1)}) & \text{if } \underline{R}_L^{(\mathrm{cr})}(s, Q) \le R \le C(s, Q), \\ 0 & \text{if } C(s, Q) \le R, \end{cases} \tag{52}$$

where $A_L(s, Q)$ is defined in (19)–(21), $\mathcal{A}(s, Q, q)$ in (27) and (28), $C(s, Q)$ in (24), and

$$\underline{R}_L^{(\mathrm{cr})}(s, Q) \triangleq h(Q) - q^{(2)} h(Q/q^{(2)}). \tag{53}$$

Since $q^{(1)}(R, Q)$ is an implicit function of the parameter R defined by $\mathcal{B}(R, Q, q) = 0$, its derivative is easily computed:

$$\left(q^{(1)}(R, Q)\right)'_R = \left(\log_2 \frac{q - Q}{q}\right)^{-1}. \tag{54}$$

Now we use (52) and (54) to write the derivative of $E_L(s, R, Q)$ with respect to R:

$$\left(E_L(s, R, Q)\right)'_R = \begin{cases} -L & \text{if } 0 \le R \le \underline{R}_L^{(\mathrm{cr})}(s, Q), \\ \log_2 \dfrac{Qy^s}{1 - Q - y + Qy^s} \left(\log_2 \dfrac{q - Q}{q}\right)^{-1} & \text{if } \underline{R}_L^{(\mathrm{cr})}(s, Q) \le R \le C(s, Q), \\ 0 & \text{if } C(s, Q) \le R, \end{cases}$$

where in the second line we for brevity denote $q = q^{(1)}(R, Q)$, and y is defined by (28). Clearly, the function in the second line is a nondecreasing function of R. Furthermore, at $R = \underline{R}_L^{(\mathrm{cr})}(s, Q)$ this functions equals $-L$, and at $R = C(s, Q)$ it is zero. Thus, the derivative of $E_L(s, R, Q)$ with respect to R exists and is a continuous nondecreasing function; i.e., $E_L(s, R, Q)$ is $\cup$-convex.

If $R = 0$, then for any $0 < Q < 1$ we have $h(Q) - qh(Q/q) \ge 0$. Hence, in the case of $R = 0$ we have (30).

If $R = \underline{C}(s)$, then $\underline{E}_L(s, R) = 0$. Hence, for $R = \underline{C}(s)$ we have (31).

Thus, since $\underline{E}_L(s, R)$ is $\cup$-convex, there exists $\underline{R}_L^{(\mathrm{cr})}(s)$ such that (30) holds for $0 \le R \le \underline{R}_L^{(\mathrm{cr})}(s)$, and for $R > \underline{R}_L^{(\mathrm{cr})}(s)$ we have (31). △

3. PROOFS OF LEMMAS 1–4

Proof of Lemma 1. For a fixed set $\mathcal{S} \subset [t]$, $|\mathcal{S}| = s$, and each set $\mathcal{L} \subset [t] \backslash \mathcal{S}$, $|\mathcal{L}| = L$, introduce the event

$$A(\mathcal{L}) = A_{\mathcal{S}}(\mathcal{L}) \triangleq \left\{X : \bigvee_{i \in \mathcal{S}} \boldsymbol{x}(i) \succeq \bigvee_{j \in \mathcal{L}} \boldsymbol{x}(j)\right\}, \quad \mathcal{L} \subset [t] \setminus \mathcal{S}. \tag{55}$$

Then for any $\mathcal{S} \subset [t]$, $|\mathcal{S}| = s$, the conditional probability on the left-hand side of the desired inequality (47) is

$$\Pr\left\{\mathcal{S} \in \boldsymbol{B}_L(s, X) \Big/ \left|\bigvee_{i \in \mathcal{S}} \boldsymbol{x}(i)\right| = k\right\} = \Pr\left\{\bigcup_{\mathcal{L} \subset [t] \backslash \mathcal{S}} A(\mathcal{L}) \Big/ \left|\bigvee_{i \in \mathcal{S}} \boldsymbol{x}(i)\right| = k\right\}. \tag{56}$$

By (42), in the ensemble $\{N, t, Q\}$ for any $\mathcal{S} \subset [t]$, $|\mathcal{S}| = s$, and any $\mathcal{L} \subset [t] \setminus \mathcal{S}$, $|\mathcal{L}| = L$, we have

$$\Pr\left\{A(\mathcal{L}) \Big/ \left|\bigvee_{i \in \mathcal{S}} \boldsymbol{x}(i)\right| = k\right\} = p^L, \quad p \triangleq \frac{\dbinom{k}{\lfloor QN \rfloor}}{\dbinom{N}{\lfloor QN \rfloor}}. \tag{57}$$

Applying the standard lower bound

$$\Pr\left\{\bigcup_i C_i \Big/ C\right\} \ge \sum_i \Pr\{C_i/C\} - \sum_{i<j} \Pr\{C_i C_j/C\}$$

to the conditional probability of the union (56) and taking into account (57), we obtain

$$\begin{aligned} \Pr\left\{\mathcal{S} \in \boldsymbol{B}_L(s, X) \Big/ \left|\bigvee_{i \in \mathcal{S}} \boldsymbol{x}(i)\right| = k\right\} &= \Pr\left\{\bigcup_{\mathcal{L} \subset [t] \backslash \mathcal{S}} A(\mathcal{L}) \Big/ \left|\bigvee_{i \in \mathcal{S}} \boldsymbol{x}(i)\right| = k\right\} \\ &\ge \binom{t-s}{L} p^L - \sum_{\mathcal{L} \ne \mathcal{L}' \subset [t] \backslash \mathcal{S}} \Pr\left\{A(\mathcal{L}) \cap A(\mathcal{L}') \Big/ \left|\bigvee_{i \in \mathcal{S}} \boldsymbol{x}(i)\right| = k\right\}. \end{aligned} \tag{58}$$

By symmetry of the events (55), we have

$$\sum_{\mathcal{L}\neq\mathcal{L}'\subset[t]\setminus\mathcal{S}} \Pr\left\{A(\mathcal{L})\cap A(\mathcal{L}') \Big/ \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k\right\}$$
$$= \frac{\binom{t-s}{L}}{2} \sum_{\substack{\mathcal{L}'\subset[t]\setminus\mathcal{S}\\ \mathcal{L}'\neq\mathcal{L}}} \Pr\left\{A(\mathcal{L})\cap A(\mathcal{L}') \Big/ \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k\right\}, \quad \text{for any } \mathcal{L}\subset[t]\setminus\mathcal{S}. \tag{59}$$

Let us group the terms in the last sum according to the cardinality of the intersection of $\mathcal{L}'$ and $\mathcal{L}$ and then estimate from above the obtained terms using properties of binomial coefficients:

$$\sum_{\substack{\mathcal{L}'\subset[t]\setminus\mathcal{S}\\ \mathcal{L}'\neq\mathcal{L}}} \Pr\left\{A(\mathcal{L})\cap A(\mathcal{L}') \Big/ \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k\right\}$$
$$= \sum_{l=0}^{L-1} \sum_{\substack{\mathcal{L}'\subset[t]\setminus\mathcal{S}\\ |\mathcal{L}\cap\mathcal{L}'|=l}} \Pr\left\{A(\mathcal{L})\cap A(\mathcal{L}') \Big/ \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k\right\}$$
$$= \sum_{l=0}^{L-1} \binom{L}{l}\binom{t-s-L}{L-l} p^{2L-l} < p^L \sum_{l=0}^{L-1} \binom{L}{L-l}(tp)^{L-l} < p^L((1+tp)^L-1). \tag{60}$$

Equations (58)–(60) yield the lower bound

$$\Pr\left\{\mathcal{S}\in\boldsymbol{B}_L(s,X) \Big/ \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k\right\} \ge \binom{t-s}{L} p^L\left(2-(1+tp)^L\right). \tag{61}$$

Denote by t_0 the root of the equation $(1+tp)^L - 1 = 0.5$, i.e.,

$$t_0 = \frac{1.5^{\frac{1}{L}}-1}{p}.$$

If $t\le t_0$, then $(1+pt)^L\le 1.5$ and

$$\Pr\left\{\mathcal{S}\in\boldsymbol{B}_L(s,X) \Big/ \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k\right\} \ge \frac{1}{2}\binom{t-s}{L} p^L.$$

Consider the case $t > t_0 > s+L$. Since the conditional probability in question monotonically grows with t, we have

$$\Pr\left\{\mathcal{S}\in\boldsymbol{B}_L(s,X) \Big/ \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k\right\} \ge \frac{1}{2}\binom{t_0-s}{L} p^L \ge \frac{1}{2}\left(\frac{t_0 p}{s+L+1}\right)^L = D_1(s,L).$$

Consider the last case $t_0\le s+L$. Note the inequality

$$p \ge \frac{1.5^{\frac{1}{L}}-1}{s+L}.$$

Since $t\ge s+L$, we have

$$\Pr\left\{\mathcal{S}\in\boldsymbol{B}_L(s,X) \Big/ \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k\right\} \ge \frac{1}{2}\binom{s+L-s}{L} p^L = D_2(s,L).$$

Letting $D(s,L) = \min\left(D_1(s,L), D_2(s,L), 0.5\right)$, we obtain (47). $\triangle$

Proof of Lemma 2. Fix $s \ge 2$ and also parameters Q and q, $0 < Q < 1$, $Q < q < \min\{1, sQ\}$. Set $k = \lfloor qN \rfloor$ and tend N to infinity. For each type $\{n(\boldsymbol{u})\}$, consider the corresponding distribution τ: $\tau(\boldsymbol{u}) = \dfrac{n(\boldsymbol{u})}{N}$, $\forall\, \boldsymbol{u} \in \{0,1\}^s$.

Using Stirling's formula for the types corresponding to these distributions, we find the logarithmic asymptotic of the summand in (43):

$$-\log_2 \frac{N!}{\prod\limits_{\boldsymbol{u}} n(\boldsymbol{u})!} \binom{N}{\lfloor QN \rfloor}^{-s} = NF(\tau, Q, q)(1 + o(1)),$$

where

$$F(\tau, Q, q) = \sum_{\boldsymbol{u}} \tau(\boldsymbol{u}) \log_2 \tau(\boldsymbol{u}) + sh(Q). \tag{62}$$

Thus, to compute $\mathcal{A}(s, Q, q)$ we have to find the following minimum:

$$\mathcal{A}(s, Q, q) = \min_{\tau \in (64):\,(65)} F(\tau, Q, q), \tag{63}$$

$$\{\tau :\ \forall\, \boldsymbol{u} = (u_1, \ldots, u_s) \in \{0,1\}^s \quad 0 < \tau(\boldsymbol{u}) < 1\}, \tag{64}$$

$$\sum_{\boldsymbol{u}} \tau(\boldsymbol{u}) = 1, \quad \tau(\boldsymbol{0}) = 1 - q, \quad \sum_{\boldsymbol{u}:\, u_i = 1} \tau(\boldsymbol{u}) = Q, \quad \forall\, i \in [s], \tag{65}$$

where constraints (65) are induced by properties (44) and conditions imposed on the types.

To compute the minimum point, we apply the standard Lagrange multipliers method. Consider the Lagrangian

$$\Lambda \triangleq \sum_{\tau(\boldsymbol{u})} \tau(\boldsymbol{u}) \log_2 \tau(\boldsymbol{u}) + sh(Q) + \lambda_0(\tau(\boldsymbol{0}) + q - 1) + \sum_{i=1}^{s} \lambda_i \left(\sum_{\boldsymbol{u}:\, u_i = 1} \tau(\boldsymbol{u}) - Q \right) + \lambda_{s+1} \left(\sum_{\boldsymbol{u}} \tau(\boldsymbol{u}) - 1 \right).$$

Necessary conditions for the extremal distribution are

$$\begin{cases} \dfrac{\partial \Lambda}{\partial \tau(\boldsymbol{0})} = \log_2 \tau(\boldsymbol{0}) + \log_2 e + \lambda_0 + \lambda_{s+1} = 0, \\ \dfrac{\partial \Lambda}{\partial \tau(\boldsymbol{u})} = \log_2 \tau(\boldsymbol{u}) + \log_2 e + \lambda_{s+1} + \sum\limits_{i=1}^{s} u_i \lambda_i = 0, \quad \text{for any } \boldsymbol{u} \ne \boldsymbol{0}. \end{cases} \tag{66}$$

It is easily seen that the matrix of second derivatives of the Lagrangian is a diagonal matrix. Also, we conclude that this matrix is positive definite in the domain (64). Hence, $F(\tau, Q)$ is a strictly $\cup$-convex function in the domain (64).

Then we use the Karush–Kuhn–Tucker theorem [28], which states that every solution τ in the domain (64) satisfying the system (66) and constraints (65) and having a positive definite matrix of second derivatives of the Lagrangian at this point is a local minimum of $F(\tau, Q)$. Thus, if there is a solution of the system (66) and (65) in the domain (64), then it is unique, and this point is also a solution in the minimization problem (63)–(65).

Note that symmetry of the problem implies the equalities $\eta \triangleq \lambda_1 = \lambda_2 = \ldots = \lambda_s$. For brevity, introduce the parameters $\mu \triangleq \log_2 e + \lambda_{s+1}$ and $\nu \triangleq \lambda_0$. Then equations (65) and (66) take the form

$$\begin{cases} \log_2 \tau(\boldsymbol{u}) + \mu + \eta \sum\limits_{i=1}^{s} u_i = 0, \quad \text{for } \boldsymbol{u} \neq \boldsymbol{0}, \\ \log_2 \tau(\boldsymbol{0}) + \mu + \nu = 0, \\ \tau(\boldsymbol{0}) = 1 - q, \\ \sum\limits_{\boldsymbol{u}} \tau(\boldsymbol{u}) = 1, \\ \sum\limits_{\boldsymbol{u}:\, u_i = 1} \tau(\boldsymbol{u}) = Q, \quad \text{for } i \in [s]. \end{cases} \tag{67}$$

Using the notation $y \triangleq \dfrac{1}{1 + 2^{-\eta}}$, rewrite the first equation:

$$\tau(\boldsymbol{u}) = \frac{1}{2^{\mu} y^s} (1 - y)^{\sum u_j} y^{s - \sum u_j}, \quad \text{for } \boldsymbol{u} \neq \boldsymbol{0}. \tag{68}$$

Substituting (68) into the fifth equation in (67), we obtain

$$\sum_{\boldsymbol{u}:\, u_i = 1} \frac{1}{2^{\mu} y^s} (1 - y)^{\sum u_j} y^{s - \sum u_j} = \frac{1 - y}{2^{\mu} y^s}.$$

Hence we find

$$\mu = \log_2 \frac{1 - y}{Q y^s}. \tag{69}$$

Substitution of (68), (69), and the third equation in (67) into the fourth equation in (67) yields

$$q(y) = \sum_{\boldsymbol{u} \neq 0} \tau(\boldsymbol{u}) = \frac{Q(1 - y^s)}{1 - y},$$

which is precisely equation (28). Thus, constraints (65) and conditions (66) give a unique solution τ in the domain (64):

$$\tau(\boldsymbol{0}) = 1 - q, \qquad \tau(\boldsymbol{u}) = \frac{Q}{1 - y} (1 - y)^{\sum u_j} y^{s - \sum u_j}, \quad \text{for } \boldsymbol{u} \neq \boldsymbol{0}, \tag{70}$$

where the parameters q and y are related by (28). To obtain the exact formula (27), it suffices to substitute (70) into (62).

Now let us prove the properties of $A(s, Q, q)$. First, note that $q(y)$ monotonically decreases with y in the interval $y \in (0, 1)$ and takes the values Q and sQ at the endpoints of this interval. Therefore, instead of (27) we may consider the function $\mathcal{T}(s, Q, y) = \mathcal{A}(s, Q, q(y))$ of the parameter y in the interval $y \in (0, y_1)$, and $q(y_1) = \min\{1, sQ\}$. Compute the derivative of $\mathcal{T}(s, Q, y)$ with respect to y:

$$\frac{\partial \mathcal{T}(s, Q, y)}{\partial y} = q'(y) \log_2 \left[\frac{Q y^s}{1 - Q - y + Q y^s} \right]. \tag{71}$$

Thus, $\mathcal{T}(s, Q, y)$ decreases with y for $y \in (0, 1 - Q)$, increases for $y \in (1 - Q, y_1)$, and is $\cup$-convex. It attains its minimum, equal to zero, at the point $y_0 = 1 - Q$. $\triangle$

Proof of Lemma 3. Fix a parameter $0 < Q < 1$. Find the derivative of $f(Q, q) \triangleq q h(Q/q)$ with respect to q:

$$\frac{\partial f(Q, q)}{\partial q} = -\log_2 \left[\frac{q - Q}{q} \right], \quad Q < q < 1. \tag{72}$$

Hence, the function $f(Q, q)$ increases in the interval $q \in (Q, 1)$ and is $\cap$-convex, and on any semi-interval $q \in (Q, a]$, $Q < a < 1$, it attains its unique maximum at the point $q = a$. $\triangle$

Proof of Lemma 4. Fix a parameter $0 < Q < 1$. By properties (28), instead of (48) we may consider the function

$$\mathcal{F}(s, L, Q, y) \triangleq \mathcal{A}(s, Q, q(y)) + L[h(Q) - q(y)h(Q/q(y))]$$

of the parameter $0 < y < y_1$, and $q(y_1) = \min\{1, sQ\}$. Using (71) and (72), compute the derivative of $\mathcal{F}(s, L, Q, y)$ with respect to y:

$$\begin{aligned}\frac{\partial \mathcal{F}(s, L, Q, y)}{\partial y} &= \mathcal{T}'(s, Q, y) - Lq'(y) f_q'(Q, y) \\ &= q'(y) \log_2 \left[\frac{Qy^s}{1 - Q - y + Qy^s} \left(\frac{y - y^s}{1 - y^s}\right)^L\right].\end{aligned}$$

Thus, the equation $\mathcal{F}'(s, L, Q, y) = 0$ is valid if ad only if we have

$$y = 1 - Q + Qy^s \left[1 - \left(\frac{y - y^s}{1 - y^s}\right)^L\right];$$

i.e., (21) holds. Obviously, the function (48) is $\cap$-convex and attains its minimum at $q = q(y_2)$, where by y_2 we denote the solution of equation (21).

Note that

$$1 - q(y_2) = 1 - \frac{Q(1 - y_2^s)}{1 - y_2} = \frac{Qy_2^s}{1 - y_2} \left(\frac{y_2 - y_2^s}{1 - y_2^s}\right)^L.$$

Hence,

$$\begin{aligned}\mathcal{F}(s, L, Q, y_2) = &\left(1 - Q\frac{1 - y_2^s}{1 - y_2}\right) \log_2 \left[\frac{Qy_2^s}{1 - y_2} \left(\frac{y_2 - y_2^s}{1 - y_2^s}\right)^L\right] + Q\frac{1 - y_2^s}{1 - y_2} \log_2 \frac{Qy_2^s}{1 - y_2} \\ &+ sQ \log_2 \frac{1 - y_2}{y_2} + sh(Q) + Lh(Q) + LQ \log_2 \frac{1 - y_2}{1 - y_2^s} + LQ\frac{y_2 - y_2^s}{1 - y_2} \log_2 \frac{y_2 - y_2^s}{1 - y_2^s}.\end{aligned}$$

Simplifying the above equality, we obtain

$$\min_{0<y<y_1} \mathcal{F}(s, L, Q, y) = A_L(s, Q),$$

where the function $A_L(s, Q)$ is defined in (19)–(21). △

REFERENCES

1. D'yachkov, A.G., Vorobyev, I.V., Polyanskii, N.A., and Shchukin, V.Yu., Almost Disjunctive List-Decoding Codes (Two Talks), in *Proc. 14th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-14), Svetlogorsk, Russia, Sept. 7–13, 2014*, pp. 115–126.

2. Kautz, W.H. and Singleton, R.C., Nonrandom Binary Superimposed Codes, *IEEE Trans. Inform. Theory*, 1964, vol. 10, no. 4, pp. 363–377.

3. D'yachkov, A.G. and Rykov, V.V., On One Application of Codes for a Multiple Access Channel in the ALOHA System, in *Proc. VI All-Union School-Seminar on Computer Networks, Moscow–Vinnitsa, 1981*, Part 4, pp. 18–24.

4. D'yachkov, A.G. and Rykov, V.V., Bounds on the Length of Disjunctive Codes, *Probl. Peredachi Inf.*, 1982, vol. 18, no. 3, pp. 7–13 [*Probl. Inf. Trans.* (Engl. Transl.), 1982, vol. 18, no. 3, pp. 166–171].

5. Erdős, P., Frankl, F., and Füredi, F., Families of Finite Sets in Which No Set Is Covered by the Union of Two Others, *J. Combin. Theory, Ser. A*, 1982, vol. 33, no. 2, pp. 158–166.

6. D'yachkov, A.G. and Rykov, V.V., A Survey of Superimposed Code Theory, *Probl. Control Inform. Theory*, 1983, vol. 12, no. 4, pp. 229–242.

7. D'yachkov, A.G., Rykov, V.V., and Rashad, A.M., Superimposed Distance Codes, *Probl. Control Inform. Theory*, 1989, vol. 18, no. 4, pp. 237–250.

8. D'yachkov, A.G. and Rykov, V.V., Superimposed Codes for Multiple Accessing of the OR-Channel, in *Proc. 1998 IEEE Int. Sympos. on Information Theory (ISIT'98), Cambridge, MA, USA, Aug. 16–21, 1998*, pp. 404.

9. Vilenkin, P.A., On Constructions of List-Decoding Superimposed Codes, in *Proc. 6th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-6), Pskov, Russia, Sept. 6–12, 1998*, pp. 228–231.

10. D'yachkov, A.G., Macula, A.J., Jr., and Rykov, V.V., New Constructions of Superimposed Codes, *IEEE Trans. Inform. Theory*, 2000, vol. 46, no. 1, pp. 284–290.

11. D'yachkov, A.G., Macula, A.J., and Rykov, V.V., New Applications and Results of Superimposed Code Theory Arising from Potentialities of Molecular Biology, *Numbers, Information, and Complexity (Bielefeld, 1998)*, Althöfer, I., Cai, N., Dueck, G., Khachatrian, L., Pinsker, M.S., Sárközy, A., Wegener, I., and Zhang, Z., Eds., Boston: Kluwer, 2000, pp. 265–282.

12. D'yachkov, A.G., Vilenkin, P.A., Macula, A.J., Torney, D.C., and Yekhanin, S.M., New Results in the Theory of Superimposed Codes, in *Proc. 7th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-7), Bansko, Bulgaria, June 18–24, 2000*, pp. 126–136.

13. D'yachkov, A., Vilenkin, P., Macula, A., and Torney, V., Families of Finite Sets in Which No Intersection of ℓ Sets Is Covered by the Union of s Others, *J. Combin. Theory, Ser. A*, 2002, vol. 99, no. 2, pp. 195–218.

14. D'yachkov, A.G., Lectures on Designing Screening Experiments, *Com*^{2}*MaC Lect. Note Ser.*, vol. 10, Pohang, Korea: Pohang Univ. of Science and Technology (POSTECH), 2004.

15. D'yachkov, A.G., Vorob'ev, I.V., Polyansky, N.A., and Shchukin, V.Yu., Bounds on the Rate of Disjunctive Codes, *Probl. Peredachi Inf.*, 2014, vol. 50, no. 1, pp. 31–63 [*Probl. Inf. Trans.* (Engl. Transl.), 2014, vol. 50, no. 1, pp. 27–56].

16. D'yachkov, A.G., Vorobyev, I.V., Polyanskii, N.A., Shchukin, V.Yu., Bounds on the Rate of Superimposed Codes, in *Proc. 2014 IEEE Int. Sympos. on Information Theory (ISIT'2014), Honolulu, HI, USA, June 29 – July 4, 2014*, pp. 2341–2345.

17. Gallager, R.G., *Information Theory and Reliable Communication*, New York: Wiley, 1968. Translated under the title *Teoriya informatsii i nadezhnaya svyaz'*, Moscow: Sov. Radio, 1974.

18. Csiszár, I. and Körner, J., *Information Theory: Coding Theorems for Discrete Memoryless Systems*, New York: Academic; Budapest: Akad. Kiadó, 1981. Translated under the title *Teoriya informatsii: teoremy kodirovaniya dlya diskretnykh sistem bez pamyati*, Moscow: Mir, 1985.

19. Bassalygo, L.A. and Rykov, V.V., Multiple-Access Hyperchannel, *Probl. Peredachi Inf.*, 2013, vol. 49, no. 4, pp. 3–12 [*Probl. Inf. Trans.* (Engl. Transl.), 2013, vol. 49, no. 4, pp. 299–307].

20. Malyutov, M.B., On Planning of Screening Experiments, in *Proc. 1975 IEEE–USSR Joint Workshop on Information Theory, Moscow, USSR, Dec. 15–19, 1975*, New York: IEEE, 1976, pp. 144–147.

21. Freidlina, V.L., On a Design Problem for Screening Experiments, *Teor. Veroyatn. Primen.*, 1975, vol. 20, no. 1, pp. 100–114 [*Theory Probab. Appl.* (Engl. Transl.), 1975, vol. 20, no. 1, pp. 102–115].

22. Malyutov, M.B., The Separating Property of Random Matrices, *Mat. Zametki*, 1978, vol. 23, no. 1, pp. 155–167 [*Math. Notes* (Engl. Transl.), 1978, vol. 23, no. 1, pp. 84–91].

23. D'yachkov, A.G., Bounds on the Error Probability for Certain Ensembles of Random Codes, *Probl. Peredachi Inf.*, 1979, vol. 15, no. 2, pp. 23–35 [*Probl. Inf. Trans.* (Engl. Transl.), 1979, vol. 15, no. 2, pp. 99–108].

24. D'yachkov, A.G., Error Probability Bounds for Two Models of Randomized Design of Screening Experiments, *Probl. Peredachi Inf.*, 1979, vol. 15, no. 4, pp. 17–31 [*Probl. Inf. Trans.* (Engl. Transl.), 1979, vol. 15, no. 4, pp. 258–269].

25. D'yachkov, A.G., Bounds for Error Probability for a Symmetrical Model in Designing Screening Experiments, *Probl. Peredachi Inf.*, 1981, vol. 17, no. 4, pp. 41–52 [*Probl. Inf. Trans.* (Engl. Transl.), 1981, vol. 17, no. 4, pp. 245–253].

26. D'yachkov, A.G. and Rashad, A.M., Universal Decoding for Random Design of Screening Experiments, *Microelectron. Reliab.*, 1989, vol. 29, no. 6, pp. 965–971.

27. Coppersmith, D. and Shearer, J., New Bounds for Union-free Families of Sets, *Electron. J. Combin.*, 1998, vol. 5, no. 1, Res. Paper R39, 16 pp.

28. Galeev, E.M. and Tikhomirov, V.M., *Optimizatsiya: teoriya, primery, zadachi* (Optimization: Theory, Examples, Problems), Moscow: Editorial URSS, 2000.