ISSN 0032-9460, Problems of Information Transmission, 2014, Vol. 50, No. 1, pp. 27–56. © Pleiades Publishing, Inc., 2014.
Original Russian Text © A.G. D'yachkov, I.V. Vorob'ev, N.A. Polyansky, V.Yu. Shchukin, 2014, published in Problemy Peredachi Informatsii, 2014, Vol. 50, No. 1, pp. 31–63.

CODING THEORY

Bounds on the Rate of Disjunctive 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
agd-msu@yandex.ru ilya.sparrow91@gmail.com nikitapolyansky@gmail.com
vpike@mail.ru

Received April 15, 2013; in final form, January 9, 2014

Abstract—A binary code is said to be a disjunctive (s, ℓ) cover-free code if it is an incidence matrix of a family of sets where the intersection of any ℓ sets is not covered by the union of any other s sets of this family. A binary code is said to be a list-decoding disjunctive of strength s with list size L if it is an incidence matrix of a family of sets where the union of any s sets can cover no more that $L-1$ other sets of this family. For $L=\ell=1$, both definitions coincide, and the corresponding binary code is called a disjunctive s-code. This paper is aimed at improving previously known and obtaining new bounds on the rate of these codes. The most interesting of the new results is a lower bound on the rate of disjunctive (s, ℓ) cover-free codes obtained by random coding over the ensemble of binary constant-weight codes; its ratio to the best known upper bound converges as $s \to \infty$, with an arbitrary fixed $\ell \geq 1$, to the limit $2e^{-2} = 0.271\ldots$. In the classical case of $\ell = 1$, this means that the upper bound on the rate of disjunctive s-codes constructed in 1982 by D'yachkov and Rykov is asymptotically attained up to a constant factor a, $2e^{-2} \leq a \leq 1$.

DOI: 10.1134/S0032946014010037

1. NOTATION, DEFINITIONS, AND RESULTS

Let N, t, s, L, and ℓ be integers, $1 \leq s < t$, $1 \leq L \leq t-s$, $1 \leq \ell \leq t-s$; $\triangleq$ denote equality by definition; $|A|$ be the cardinality of a set A; and $[N] \triangleq \{1, 2, \ldots, N\}$ be the set of positive integers from 1 to N. Introduce a binary $N \times t$ matrix with N rows $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N$ and t columns $\boldsymbol{x}(1), \ldots, \boldsymbol{x}(t)$ (codewords)

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

which hereafter will be referred to as a *code of length N and of size t*. The number of ones in a column $x(j)$, i.e., $|\boldsymbol{x}(j)| \triangleq \sum\limits_{i=1}^{N} x_i(j)$, will be called the *weight* of $\boldsymbol{x}(j)$, $j \in [t]$. We say that X is a *constant-weight* code if every codeword contains the same number w of ones, $1 \leq w < N$; i.e., $|\boldsymbol{x}(j)| = w$ for any $j \in [t]$. By $\vee$ we denote the operation of disjunctive (Boolean) sum of two binary numbers

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

as well as the componentwise disjunctive sum of two binary columns. We say that a column $\boldsymbol{u}$ covers column $\boldsymbol{v}$ ($\boldsymbol{u} \succeq \boldsymbol{v}$) if $\boldsymbol{u} \vee \boldsymbol{v} = \boldsymbol{u}$. By $\lfloor a \rfloor$ ($\lceil a \rceil$) we denote the largest (smallest) integer which is $\leq a$ ($\geq a$).

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

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

Taking into account the obvious symmetry in s and ℓ, we denote by $t_{\rm cf}(N,s,\ell)=t_{\rm cf}(N,\ell,s)$ the maximum size of an (s,ℓ) CF code of length N, and by $N_{\rm cf}(t,s,\ell)=N_{\rm cf}(t,\ell,s)$, the minimum number of rows of an (s,ℓ) CF code of size t. Define the *rate* of (s,ℓ) CF codes:

$$R(s,\ell)=R(\ell,s)\triangleq\varlimsup_{N\to\infty}\frac{\log_2 t_{\rm cf}(N,s,\ell)}{N}=\varlimsup_{t\to\infty}\frac{\log_2 t}{N_{\rm cf}(t,s,\ell)}. \tag{2}$$

Definition 2 [2,3]. A code X is said to be a *disjunctive list-decoding code of strength s with list size L (s_L-LD code)* if the disjunctive sum of any s columns of X covers no more than $L-1$ other columns of X that do not enter this sum. Denote by $t_{\rm ld}(N,s,L)$ the maximum size of an s_L-LD code of length N, and by $N_{\rm ld}(t,s,L)$, the minimum number of rows in an s_L-LD code of size t. Define the *rate* of s_L-LD codes:

$$R_L(s)\triangleq\varlimsup_{N\to\infty}\frac{\log_2 t_{\rm ld}(N,s,L)}{N}=\varlimsup_{t\to\infty}\frac{\log_2 t}{N_{\rm ld}(t,s,L)}. \tag{3}$$

For $L=\ell=1$, Definitions 1 and 2 coincide, $R_1(s)=R(s,1)$, $s=1,2,\dots$, and the corresponding codes is called a *disjunctive s-code*. Disjunctive s-codes were introduces in 1964 in the pioneering work by Kautz and Singleton [4], where first nontrivial properties of disjunctive s-codes were established, important applications and constructions of these codes were designed, which were further developed in [5,6], and the problem of finding bounds on the rate $R(s,1)$ was set up.

1.1. Lower and Upper Bounds on $R(s,1)$

The best presently known lower bound on the rate $R(s,1)$ was obtained in 1989 in [7], where random coding over the ensemble of binary constant-weight codes[1] was used to show that

$$R(s,1)\ge\underline{R}(s,1)\triangleq s^{-1}\max_{0<Q<1}A(s,Q),\quad s=1,2,\dots, \tag{4}$$

$$A(s,Q)\triangleq\log_2\frac{Q}{1-y}-sK(Q,1-y)-K\Big(Q,\frac{1-y}{1-y^s}\Big), \tag{5}$$

where we use the standard notation for the Kullback distance

$$K(a,b)\triangleq a\log_2\frac{a}{b}+(1-a)\log_2\frac{1-a}{1-b},\quad 0<a,b<1, \tag{6}$$

and $y=y(s,Q)$, $1-Q\le y<1$, is a unique root of the equation

$$y=1-Q+Qy^s\frac{1-y}{1-y^s},\quad 1-Q\le y<1. \tag{7}$$

Note that the random coding bound $\underline{R}(s,1)$ established in [7] is equivalent to (4)–(7) but differs in notation.

If $s\to\infty$, then the asymptotic form of (4)–(7) is

$$R(s,1)\ge\underline{R}(s,1)=\frac{1}{s^2\log_2 e}(1+o(1))=\frac{0.693\dots}{s^2}(1+o(1)), \tag{8}$$

where $e=2.718\dots$ is the base of the natural logarithm.

[1] The ensemble of constant-weight codes is a particular case of a code ensemble called a constant-composition ensemble (CCE), which was introduced in [8] when using the random coding method to construct the best upper bounds on the error probability for discrete memoryless channels. In [9], the CCE was used in a similar problem for memoryless multiple-access channels. In [10–12], logarithmic asymptotic of the error probability averaged over the CCE was studied.

It is obvious [4] that $R(s,1) \le 1/s$, $s = 1, 2, \ldots$; a nontrivial upper bound on $R(s,1)$, which is presently the best known, was constructed in 1982 in [13]. To describe this bound, denoted in the present paper by $\overline{R}(s,1)$, $s = 1, 2, \ldots$, and referred to as the *recurrent bound*, we introduce the standard notation for the binary entropy function

$$h(v) \triangleq -v \log_2 v - (1-v)\log_2(1-v), \quad 0 < v < 1, \tag{9}$$

and a function

$$f_s(v) \triangleq h(v/s) - vh(1/s), \quad 0 < v < 1, \quad s = 1, 2, \ldots, \tag{10}$$

of argument v, $0 < v < 1$. It is shown in [13] (see also [14]) that $f_s(v)$ is positive, $\cap$-convex, and

$$\max_{0<v<1} f_s(v) = f_s(v_s) \quad \text{for} \quad v_s \triangleq \frac{s}{1 + 2^{sh(1/s)}}, \quad s = 1, 2, \ldots. \tag{11}$$

Set

$$\overline{R}(1,1) \triangleq 1, \qquad \overline{R}(2,1) \triangleq \max_{0<v<1} f_2(v) = f_2(v_2) = 0.322\ldots, \tag{12}$$

and then the sequence $\overline{R}(s,1)$, $s = 3, 4, \ldots$, is defined [13] as a unique solution of the recurrence equation

$$\overline{R}(s,1) = f_s\biggl(1 - \frac{\overline{R}(s,1)}{\overline{R}(s-1,1)}\biggr), \quad s = 3, 4, \ldots. \tag{13}$$

For the rate $R(s,1)$ of disjunctive s-codes and for the recurrent sequence $\overline{R}(s,1)$, $s = 1, 2, \ldots$, described by (12) and (13), the inequalities

$$R(s,1) \le \overline{R}(s,1) \le \frac{2\log_2[e(s+1)/2]}{s^2}, \quad s = 2, 3, \ldots, \tag{14}$$

were proved in [13], which yield an asymptotic upper bound on the rate $R(s,1)$:

$$R(s,1) \le \frac{2\log_2 s}{s^2}(1 + o(1)), \quad s \to \infty. \tag{15}$$

For $s = 2, 3, \ldots, 6$, numerical values of the lower bound $\underline{R}(s,1)$ give by (4)–(7) and of the upper bound $\overline{R}(s,1)$ given by (12) and (13) are summarized in Table 1 (see below).

In Section 2.1 we prove the following statement.

Theorem 1. *If $s \ge 8$, then the recurrent sequence $\overline{R}(s,1)$ defined by* (12) *and* (13) *satisfies the inequality*

$$\overline{R}(s,1) \ge \frac{2\log_2[(s+1)/8]}{(s+1)^2}, \quad s \ge 8. \tag{16}$$

Bounds (14) and (16) imply the asymptotic equality

$$\overline{R}(s,1) = \frac{2\log_2 s}{s^2}(1 + o(1)), \quad s \to \infty. \tag{17}$$

A result of the present paper for classical disjunctive s-codes is as follows.

Theorem 2. *For the rate $R(s,1)$ we have the asymptotic inequality*

$$R(s,1) \ge \frac{4e^{-2}\log_2 s}{s^2}(1 + o(1)) = \frac{0.541\log_2 s}{s^2}(1 + o(1)), \quad s \to \infty. \tag{18}$$

Bound (18) considerably improves inequality (8). Bounds (15) and (18) specify the asymptotic of the rate $R(s,1)$ of disjunctive s-codes up to a factor a, $4e^{-2} \le a \le 2$. It is important to note that Theorem 2 will be obtained in Section 2.2 as a corollary of lower bounds on the rate $R(s,\ell)$ of (s,ℓ) CF codes with $\ell \ge 2$ formulated in Section 1.2 These lower bounds will be constructed in Section 2.2 using random coding over the ensemble of binary constant-weight codes.

1.2. Bounds on the Rate $R(s,\ell)$ of (s,ℓ) CF codes, $2 \le \ell \le s$

Disjunctive (s,ℓ) cover-free (CF) codes were introduced in 1988 in [1] in connection with a key distribution problem in cryptography; a description of this problem can also be found in [15, 16]. Biological applications and constructions of (s,ℓ) CF codes in nonadaptive group testing (finding supersets, or complexes) were proposed in [14, 17, 18]. An important application of $(s-\ell+1,\ell)$ CF codes, $2 \le \ell < s$, for the ℓ-threshold nonadaptive group testing model [19] (the problem of finding $\le s$ defects) was noted in [20]. Further constructions of (s,ℓ) CF codes were developed in [21, 22].

First results on upper bounds on the rate $R(s,\ell)$ for (s,ℓ) CF codes, $2 \le \ell \le s$, were obtained in [14, 23]. In [15, 16], the inequality

$$R(s,\ell) \le \frac{R(s-i,\ell-j)}{R(s-i,\ell-j)+\dfrac{(i+j)^{i+j}}{i^i j^j}}, \quad i \in [s-1], \quad j \in [\ell-1], \tag{19}$$

was proved, which is a refinement of the inequality

$$R(s,\ell) \le R(s-i,\ell-j)\frac{i^i j^j}{(i+j)^{i+j}}, \quad i \in [s-1], \quad j \in [\ell-1], \tag{20}$$

established previously in [24]. The recurrent inequality (19) and the recurrent upper bound $\overline{R}(s,1)$, $s \ge 1$, defined by equations (10)–(13) gives the best known recurrent upper bound for $R(s,\ell)$, $2 \le \ell \le s$:

$$R(s,\ell) \le \overline{R}(s,\ell) \triangleq \min_{i\in[s-1]} \min_{j\in[\ell-1]} \frac{\overline{R}(s-i,\ell-j)}{\overline{R}(s-i,\ell-j)+\dfrac{(i+j)^{i+j}}{i^i j^j}}. \tag{21}$$

Asymptotic of the bound (21) is described by the following theorem, which was previously presented in [25] and is proved in Section 2.2

Theorem 3 [25]. *If $s \to \infty$ and $\ell \ge 2$ is fixed, then*

$$R(s,\ell) \le \overline{R}(s,\ell) \le \frac{(\ell+1)^{\ell+1}}{2e^{\ell-1}} \frac{\log_2 s}{s^{\ell+1}}(1+o(1)), \quad \ell \ge 2, \quad s \to \infty. \tag{22}$$

The best presently known lower bound on the $R(s,\ell)$, $2 \le \ell \le s$, was obtained in 2002 in [14] using random coding over the ensemble with independent binary components of codewords and over a special ensemble with independent binary constant-weight codewords proposed in [26]. For fixed $\ell \ge 2$ and $s \to \infty$, the asymptotic of this bound is of the form

$$R(s,\ell) \ge \frac{e^{-\ell}\ell^{\ell+1}\log_2 e}{s^{\ell+1}}(1+o(1)), \quad \ell \ge 2, \quad s \to \infty. \tag{23}$$

The central result of the present paper is Theorem 4 proved in Section 2.2. In this theorem, using random coding over the ensemble of constant-weight binary codes, we find a lower bound $\underline{R}(s,\ell)$ on the rate $R(s,\ell)$, $2 \le \ell \le s$, and analyze the asymptotic of $\underline{R}(s,\ell)$ in the case where $s \to \infty$ and $\ell \ge 2$ is fixed.

Theorem 4 (random coding bound $\underline{R}(s,\ell)$). *The following two claims hold true.*

1. *Let $2 \le \ell \le s$. Then the rate of (s,ℓ) CF codes satisfies the inequality*

$$R(s,\ell) \ge \underline{R}(s,\ell) \triangleq \frac{1}{s+\ell-1} \max_{0<z<1} T(z,s,\ell), \tag{24}$$

where

$$T(z,s,\ell) \triangleq \frac{\ell z^s(1-z)^\ell}{1-z^s(1-z)^\ell}\log_2\Big[\frac{z}{1-z}\Big] + (s+\ell-1)\log_2[1-z^s(1-z)^\ell] - (s+\ell)\frac{z-z^s(1-z)^\ell}{1-z^s(1-z)^\ell}\log_2[1-z^{s-1}(1-z)^\ell]. \quad (25)$$

2. *If $s\to\infty$ and $\ell\geq 2$ is fixed, then for the lower bound $\underline{R}(s,\ell)$ we have the asymptotic equality*

$$\underline{R}(s,\ell) = \frac{e^{-\ell}\ell^{\ell+1}\log_2 s}{s^{\ell+1}}(1+o(1)), \quad s\to\infty, \quad \ell = 2,3,\dots \quad (26)$$

In Section 2.2 we also prove Theorem 5, in which, using Theorem 4, for the rate of (s,ℓ) CF codes, $1\leq\ell\leq s$, we establish a new asymptotic lower bound significantly improving the asymptotic of the right-hand side of (23).

Theorem 5. *For any fixed $\ell = 1,2,\dots$ and $s\to\infty$, the rate $R(s,\ell)$ satisfies the asymptotic inequality*

$$R(s,\ell) \geq \left(\frac{\ell+1}{e}\right)^{\ell+1}\frac{\log_2 s}{s^{\ell+1}}(1+o(1)), \quad \ell = 1,2,\dots, \quad s\to\infty. \quad (27)$$

Theorem 2 is implied by Theorem 5, since inequality (18) in Theorem 2 is a particular case of inequality (27) with $\ell = 1$. Comparing the upper bound (22) of Theorem 3 with the lower bound (27) implies that the ratio of the lower bound to the upper bound for $s\to\infty$ and any fixed value of $\ell\geq 1$ converges to the limit $2e^{-2} = 0.271\dots$.

For a fixed $s\geq 2$, any $i = 1,2,\dots$, and an integer j, $2\leq j\leq s$, inequality (19) can be written as

$$R(s+i,j) \leq \frac{R(s,1)}{R(s,1) + \dfrac{(i+j-1)^{i+j-1}}{i^i(j-1)^{j-1}}}, \quad 2\leq j\leq s, \quad i = 1,2,\dots,$$

or

$$R(s,1) \geq \frac{R(s+i,j)}{1-R(s+i,j)}\frac{(i+j-1)^{i+j-1}}{i^i(j-1)^{j-1}}, \quad 2\leq j\leq s, \quad i = 1,2,\dots$$

Hence it follows that the rate of disjunctive s-codes satisfies the inequality

$$R(s,1) \geq \underline{R}'(s,1) \triangleq \max_{\substack{i\geq 1\\ 2\leq j\leq s}}\left\{\frac{\underline{R}(s+i,j)}{1-\underline{R}(s+i,j)}\frac{(i+j-1)^{i+j-1}}{i^i(j-1)^{j-1}}\right\}, \quad (28)$$

where on the right-hand side of (28) we use the lower bound of Theorem 4. In Table 1, for $\ell = 1$ and $2\leq s\leq 6$, we give numerical values of the lower bound $\underline{R}'(s,1)$ together with optimal values of (i,j) in definition (28). For $3\leq s\leq 6$, these values improve the previously known bound $\underline{R}(s,1)$ obtained from (4)–(7) and presented in Table. For $2\leq\ell\leq s\leq 6$, in Table 1 we also present the upper bound $\overline{R}(s,\ell)$ given by the right-hand side of (21), the lower bound $\underline{R}(s,\ell)$, and the corresponding fraction $Q(s,\ell)$ of optimal-weight codewords for the ensemble of constant-weight binary codes in the random coding bound of Theorem 4. When proving claim 2 of Theorem 4, for $Q(s,\ell)$ we will establish the asymptotic equality

$$Q(s,\ell) = \frac{\ell}{s}(1+o(1)), \quad s\to\infty, \quad \ell = 2,3,\dots \quad (29)$$

Table 1

$(s,1)$	$(2,1)$	$(3,1)$	$(4,1)$	$(5,1)$	$(6,1)$
$\overline{R}(s,1)$	$3.22\cdot10^{-1}$	$1.99\cdot10^{-1}$	$1.40\cdot10^{-1}$	$1.06\cdot10^{-1}$	$8.30\cdot10^{-2}$
$\underline{R}(s,1)$	$1.82\cdot10^{-1}$	$7.9\cdot10^{-2}$	$4.4\cdot10^{-2}$	$2.8\cdot10^{-2}$	$1.9\cdot10^{-2}$
$\underline{R'}(s,1)$	$1.28\cdot10^{-1}$	$8.2\cdot10^{-2}$	$5.66\cdot10^{-2}$	$4.20\cdot10^{-2}$	$3.25\cdot10^{-2}$
(i,j)	$(1,2)$	$(2,2)$	$(3,2)$	$(3,2)$	$(4,2)$
(s,ℓ)	$(2,2)$	$(3,2)$	$(4,2)$	$(5,2)$	$(6,2)$
$\overline{R}(s,\ell)$	$1.61\cdot10^{-1}$	$7.44\cdot10^{-2}$	$4.55\cdot10^{-2}$	$2.86\cdot10^{-2}$	$2.03\cdot10^{-2}$
$\underline{R}(s,\ell)$	$5.84\cdot10^{-2}$	$3.1\cdot10^{-2}$	$1.85\cdot10^{-2}$	$1.2\cdot10^{-2}$	$8.25\cdot10^{-3}$
$Q(s,\ell)$	0.32	0.27	0.24	0.21	0.19
(s,ℓ)	$(3,3)$	$(4,3)$	$(5,3)$	$(6,3)$	$(4,4)$
$\overline{R}(s,\ell)$	$3.87\cdot10^{-2}$	$1.83\cdot10^{-2}$	$1.09\cdot10^{-2}$	$6.69\cdot10^{-3}$	$9.58\cdot10^{-3}$
$\underline{R}(s,\ell)$	$9.78\cdot10^{-3}$	$5.53\cdot10^{-3}$	$3.36\cdot10^{-3}$	$2.15\cdot10^{-3}$	$1.92\cdot10^{-3}$
$Q(s,\ell)$	0.34	0.31	0.28	0.26	0.35
(s,ℓ)	$(5,4)$	$(6,4)$	$(5,5)$	$(6,5)$	$(6,6)$
$\overline{R}(s,\ell)$	$4.55\cdot10^{-3}$	$2.56\cdot10^{-3}$	$2.39\cdot10^{-3}$	$1.14\cdot10^{-3}$	$5.97\cdot10^{-4}$
$\underline{R}(s,\ell)$	$1.1\cdot10^{-3}$	$6.71\cdot10^{-4}$	$4.04\cdot10^{-4}$	$2.34\cdot10^{-4}$	$8.83\cdot10^{-5}$
$Q(s,\ell)$	0.32	0.30	0.37	0.35	0.38

1.3. Bounds on $R_L(s)$ for s_L-LD Codes

Disjunctive list-decoding codes (s_L-LD codes) were introduced in 1981 in [2] in designing the ALOHA communication system with a base station in the case where coding is used for signal discrimination at the output of a synchronous random multiple access channel. After that some constructions of these codes were considered in [27] (see also [6,17]) in connection with the problem of constructing *two-stage group testing procedures* occurring in molecular biology and used for analyzing DNA clone libraries. In the first stage, a set of $\le s+L-1$ elements is selected, which are separately tested in the second stage. Note that for $s\ge 2$ the rate $R_L(s)$ of two-stage procedures is a monotonically nondecreasing function of $L\ge 1$, and its limit

$$R_\infty(s)\triangleq\lim_{L\to\infty}R_L(s) \tag{30}$$

can be interpreted as the *maximum rate* of two-stage group testing procedures in a disjunctive search model for $\le s$ defects.

Now, in Propositions 1–3, we formulate important properties of an s_L-LD code of length N and size t, which directly follow from Definition 2 using reasoning by contradiction.

Proposition 1 [3]. *For the minimum number $N_{\rm ld}(t,s,L)$ of rows (rate $R_L(s)$), we have a lower (upper) bound*

$$N_{\rm ld}(t,s,L)\ge\log_2\frac{\binom{t}{s}}{\binom{s+L-1}{s}}\quad\left(\Longrightarrow\ R_L(s)\le\frac{1}{s}\right),\quad s\ge1,\quad L\ge1. \tag{31}$$

Proof. Let X be an arbitrary s_L-LD code of length N and size t. By $M_s(\boldsymbol{y},X)$, $\boldsymbol{y}\in\{0,1\}^N$, we denote the set of all s-tuples of columns of X such that for each s-tuple in $M_s(\boldsymbol{y},X)$ the disjunctive sum of the corresponding s columns is $\boldsymbol{y}$. Reasoning by contradiction, we obtain that for any $\boldsymbol{y}\in\{0,1\}^N$ we have

$$|M_s(\boldsymbol{y},X)|\le\binom{s+L-1}{s}.$$

Since the number of all s-tuples of columns of X is $\binom{t}{s}$, we have

$$\binom{t}{s} = \sum_{\boldsymbol{y}} |M_s(\boldsymbol{y}, X)| \le \binom{s+L-1}{s} 2^N.$$

According to definition (3), these inequalities lead to (31). $\triangle$

Proposition 2. *For the maximum size $t_{\mathrm{ld}}(N, s, L)$ and rate $R_L(s)$, we have the upper bounds*

$$t_{\mathrm{ld}}(N, s, L) \le t_{\mathrm{ld}}\left(N, \lfloor s/L \rfloor, 1\right) + L - 1 \implies R_L(s) \le R\left(\lfloor s/L \rfloor, 1\right), \quad L \le s. \tag{32}$$

Proof. Let $s > L \ge 2$, and let X be an arbitrary s_L-LD code of length N and size t. We say that a column (codeword) of X is *bad* for X if in X there are $\lfloor s/L \rfloor$ other columns whose disjunctive sum covers it. Otherwise, we say that the column is *good* and note that the set of good columns of X is a disjunctive $\lfloor s/L \rfloor$ code. Note that an s_L LD code X cannot contain more than $L-1$ bad columns. Indeed, if there is an L-tuple of bad columns, then it is covered by a disjunctive sum of no more than $L\lfloor s/L \rfloor \le s$ columns of the code, which contradicts the definition of an s_L-LD code. In other words, any s_L-LD code of size t and length N contains at least $t - (L-1)$ codewords forming a disjunctive $\lfloor s/L \rfloor$-code of length N. Hence we obtain (32). $\triangle$

Properties (31) and (32) will be substantial in the proof of the upper bound of Theorem 6 for the rate $R_L(s)$, $s > L \ge 2$. This bounds will be constructed as a generalization of our recurrent upper bound (12) and (13) on the rate of disjunctive s-codes.

Proposition 3 [3]. *If disjunctive sums of all s-tuples of columns of a code X are distinct, X is an $(s-1)_2$-LD code.*

Proof. This sufficient condition for an $(s-1)_2$-LD code is proved by contradiction: if in X there exists a tuple of columns containing $s-1$ column whose disjunctive sum covers two extraneous columns, then, by taking the union of this tuple with each of these two columns, we obtain two tuples of s columns each, whose disjunctive sums coincide. $\triangle$

First results on upper and lower bounds on the rate $R_L(s)$ for $L \ge 2$ were published in 1983 in [3]. The upper bound was obtained as a consequence of the second inequality in (32), and then the upper bound (14) was applied to estimate its right-hand side. The lower bound on $R_L(s)$ was obtained by random coding over the ensemble of codes with independent identically distributed binary components of codewords.

In subsequent works [28–30], these bounds were improved; the best presently known upper and lower bounds on $R_L(s)$ are formulated in Theorems 6 and 7 below. These theorems were announced without proofs in [28, 30]; they are proved in Section 2.3 below.

Theorem 6 (recurrent upper bound $\overline{R}_L(s)$). *The following claims hold true.*

1. *For any fixed $L \ge 1$ the rate of an s_L-LD code satisfies the inequality $R_L(s) \le \overline{R}_L(s)$, $s = 1, 2, \ldots$, where the sequence $\overline{R}_L(s)$, $s = 1, 2, \ldots$, on the right-hand side is defined recursively*:
   - *If $1 \le s \le L$, then*
   $$\overline{R}_L(s) \triangleq 1/s, \quad s = 1, 2, \ldots, L; \tag{33}$$
   - *If $s \ge L+1$, then*
   $$\overline{R}_L(s) \triangleq \min\{1/s; r_L(s)\}, \quad s = L+1, L+2, \ldots, \tag{34}$$
   where $r_L(s)$ is a unique solution of the equation
   $$r_L(s) \triangleq \max_{(36)} f_{\lfloor s/L \rfloor}(v), \quad s = L+1, L+2, \ldots, \tag{35}$$

in which the function $f_n(v)$, $n = 1, 2, \dots$, *of parameter* v, $0 < v < 1$, *is defined in* (9) *and* (10), *and the maximum is over all* v *satisfying*

$$0 < v < 1 - \frac{r_L(s)}{\overline{R}_L(s-1)}; \tag{36}$$

- *If* $s > 2L$, *then equation* (35) *can be written in the form*

$$r_L(s) = f_{\lfloor s/L \rfloor}\left(1 - \frac{r_L(s)}{\overline{R}_L(s-1)}\right), \quad L \geq 1, \quad s > 2L. \tag{37}$$

2. *For any* $L \geq 1$ *there exists an integer* $s(L) \geq 2$ *such that*

$$\overline{R}_L(s) = 1/s \quad \text{if } s = s(L) - 1,$$
$$\overline{R}_L(s) < 1/s \quad \text{if } s \geq s(L),$$

and $s(L) = L \log_2 L(1 + o(1))$ *as* $L \to \infty$.

3. *If* $L \geq 1$ *is fixed and* $s \to \infty$, *then*

$$\overline{R}_L(s) = \frac{2L \log_2 s}{s^2}(1 + o(1)). \tag{38}$$

The definition of the recurrent bound (33)–(37) and asymptotic (38) are generalizations of the recurrent bound (12) and (13) and of asymptotic (17).

Theorem 7 (random coding bound $\underline{R}_L(s)$). *The following claims hold true.*

1. *For the rate of* s_L*-LD codes we have the inequality*

$$R_L(s) \geq \underline{R}_L(s) \triangleq \frac{1}{s + L - 1} \max_{0<Q<1} A_L(s, Q), \tag{39}$$

$$A_L(s, Q) \triangleq \log_2 \frac{Q}{1-y} - sK(Q, 1-y) - LK\Big(Q, \frac{1-y}{1-y^s}\Big), \quad s \geq 1, \quad L \geq 1, \tag{40}$$

where $K(\cdot\cdot)$ *is the Kullback dostance* (6), *and* y, $1 - Q \leq y < 1$, *is defined as a unique solution of the equation*

$$y = 1 - Q + Qy^s \left[1 - \Big(\frac{y - y^s}{1 - y^s}\Big)^L\right], \quad 1 - Q \leq y < 1. \tag{41}$$

2. *For a fixed* $L = 1, 2, \dots$ *and* $s \to \infty$ *the asymptotic of the random coding bound is of the form*

$$\underline{R}_L(s) = \frac{L}{s^2 \log_2 e}(1 + o(1)). \tag{42}$$

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

$$\underline{R}_\infty(s) \triangleq \lim_{L\to\infty} \underline{R}_L(s) = \log_2 \left[\frac{(s-1)^{s-1}}{s^s} + 1\right]. \tag{43}$$

If $s \to \infty$, *then* $\underline{R}_\infty(s) = \dfrac{\log_2 e}{es}(1 + o(1)) = \dfrac{0.5307\dots}{s}(1 + o(1))$.

Remark 1. In the particular case of disjunctive list-decoding codes with list size $L = 1$, the lower bound (39)–(41) and asymptotic (42) coincide with the lower bound (4)–(7) and asymptotic (8). In proofs of Theorems 4 and 7 we will analyze random coding for the ensemble of constant-weight codes and show the reason for the random coding bound asymptotic (26) ($s \to \infty$, $\ell \geq 2$ is fixed) for (s, ℓ) CF codes to be essentially different from the random coding bound asymptotic (8) for classical disjunctive s-codes.

Table 2

(s, L)	$(2,2)$	$(2,3)$	$(2,4)$	$(2,5)$	$(2,6)$
$\underline{R}_L(s)$	$2.35 \cdot 10^{-1}$	$2.59 \cdot 10^{-1}$	$2.72 \cdot 10^{-1}$	$2.81 \cdot 10^{-1}$	$2.87 \cdot 10^{-1}$
$Q_L(s)$	0.24	0.23	0.23	0.22	0.22
(s, L)	$(3,2)$	$(3,3)$	$(3,4)$	$(3,5)$	$(3,6)$
$\underline{R}_L(s)$	$1.14 \cdot 10^{-1}$	$1.34 \cdot 10^{-1}$	$1.46 \cdot 10^{-1}$	$1.55 \cdot 10^{-1}$	$1.61 \cdot 10^{-1}$
$Q_L(s)$	0.18	0.17	0.16	0.16	0.15
(s, L)	$(4,2)$	$(4,3)$	$(4,4)$	$(4,5)$	$(4,6)$
$\underline{R}_L(s)$	$6.84 \cdot 10^{-2}$	$8.37 \cdot 10^{-2}$	$9.40 \cdot 10^{-2}$	$1.01 \cdot 10^{-1}$	$1.06 \cdot 10^{-1}$
$Q_L(s)$	0.14	0.13	0.13	0.12	0.12
(s, L)	$(5,2)$	$(5,3)$	$(5,4)$	$(5,5)$	$(5,6)$
$\underline{R}_L(s)$	$4.55 \cdot 10^{-2}$	$5.74 \cdot 10^{-2}$	$6.59 \cdot 10^{-2}$	$7.22 \cdot 10^{-2}$	$7.71 \cdot 10^{-2}$
$Q_L(s)$	0.12	0.11	0.11	0.10	0.10
(s, L)	$(6,2)$	$(6,3)$	$(6,4)$	$(6,5)$	$(6,6)$
$\underline{R}_L(s)$	$3.25 \cdot 10^{-2}$	$4.20 \cdot 10^{-2}$	$4.90 \cdot 10^{-2}$	$5.44 \cdot 10^{-2}$	$5.86 \cdot 10^{-2}$
$Q_L(s)$	0.10	0.09	0.09	0.09	0.09
s	2	3	4	5	6
$\underline{R}_\infty(s)$	0.322	0.199	0.145	0.114	0.094

The right-hand side of (43) yields the best presently known lower bound on the maximum rate (30) of two-stage group testing. The problem of finding an upper bound on the rate (30) improving the obvious upper bound $R_\infty(s) \le 1/s$ implied by (31) remains open.

Remark 2. In [31] there is given a lower bound on the rate (30) better than the right-hand side of (43), which is, unfortunately, based on erroneous arguments.

Table 2 presents numerical values of the lower bound on the rate of s_L-LD codes for small values of s and L; also, the corresponding fraction $Q_L(s)$ of the optimum weight of codewords in the ensemble of constant-weight binary codes in the random coding bound $\underline{R}_L(s)$ from Theorem 7 is given. Some numerical values of the lower bound (43) are also presented. In the proof of claims 2 and 3 of Theorem 7, for $Q_L(s)$ we will establish asymptotic equalities

$$Q_L(s) = \frac{\ln 2}{s} + \frac{L \ln^2 2}{s^2} + o\Big(\frac{1}{s^2}\Big), \quad s \to \infty, \quad L = 1, 2, \dots, \tag{44}$$

$$Q_L(s) = \left[\frac{s^s}{(s-1)^{s-1}} + 1\right]^{-1} + o(1), \quad L \to \infty, \quad s = 2, 3, \dots \tag{45}$$

For the rate $R_L(s)$ of s_L-LD codes there is an obvious inequality

$$\underline{R'}(s, 1) \le R(s, 1) = R_1(s) \le R_L(s), \quad L = 1, 2, \dots, \quad s = 1, 2, \dots,$$

whose left-hand side $\underline{R'}(s, 1)$ is defined in (28). Therefore, the random coding bound $\underline{R}_L(s)$ given by (39)–(41) can be compared with the lower bound $\underline{R'}(s, 1)$ from (28). Comparing Tables 1 and 2 shows that values of $\underline{R}_2(s)$ for $L = 2$ and $2 \le s \le 6$ are better (greater) than those of $\underline{R'}(s, 1)$, and for $s \ge 7$, $\underline{R'}(s, 1)$ becomes better, which corresponds to the asymptotic ($s \to \infty$) of these bounds. The same conclusions hold for $L \ge 2$ too.

1.4. Disjunctive Search Designs

Definition 3 [3, 4]. A code X is said to be a *disjunctive s-design* ($\le s$-*design*) if the disjunctive (Boolean) sum of any tuple consisting of exactly s ($\le s$) columns of X differs from the disjunctive sum of any other tuple consisting of exactly s ($\le s$) columns of X. Denote by $N(t, = s)$ ($N(t, \le s)$)

Table 3

s	7	8	9	10	11	12	13	14
$1/s$	0.143	0.125	0.111	0.100	0.091	0.083	0.077	0.071
$\overline{R}_2(s-1)$	0.163	0.141	0.117	0.102	0.086	0.076	0.066	0.059

the minimum number of rows of disjunctive s-designs ($\le s$-designs) of size t, and define the *rate* of disjunctive s-designs ($\le s$-designs)

$$R(=s) \triangleq \varlimsup_{t\to\infty} \frac{\log_2 t}{N(t,=s)}, \qquad R(\le s) \triangleq \varlimsup_{t\to\infty} \frac{\log_2 t}{N(t,\le s)}. \tag{46}$$

Obviously [4], we have

$$R(\le s) \le R(=s) \le 1/s, \quad s = 1,2,\dots, \tag{47}$$

and Definition 3 gives a necessary and sufficient condition for unambiguous reconstruction in designing N nonadaptive group tests described by rows of X for the disjunctive search model with s ($\le s$) defectives in a set of t elements. A family of t subsets of $[N]$ for which a disjunctive s-design is an incidence matrix is called a *union-free* family [32]. For the rates (2), (3), and (46), the inequalities

$$R(s,1) \le R(\le s) \le R(s-1,1), \qquad R(=s) \le R_2(s-1), \quad s = 2,3,\dots, \tag{48}$$

hold; the first two of them were observed in [4], and the third was established in [3] as a corollary of Proposition 3.

Computations according to equations (33)–(36) yield $s(1) = 2$, $s(2) = 6$, $s(3) = 12$, $s(4) = 20$, $s(5) = 25$, $s(6) = 36,\dots$. For $L = 2$ and $s = 7,8,\dots,14$ we obtain the values of the upper bound $\overline{R}_2(s-1)$ presented in Table 3, whence we see that $\overline{R}_2(s-1) < 1/s$ if $s \ge 11$. Therefore, inequality (48) means that for the rate of disjunctive s-designs we have $R(=s) < 1/s$ for $s \ge 11$. For $s = 2$, a nontrivial inequality $R(=2) \le 0.4998\dots < 1/2$ was proved in [32]. For $3 \le s \le 10$, the inequality $R(=s) < 1/s$ can be considered as our conjecture.

2. PROOFS OF THE THEOREMS

2.1. Proof of Theorem 1

For a fixed $s = 2,3,\dots$, let the function $f_s(x)$ of a parameter x, $0 < x < 1$, be defined in (9) and (10), and let

$$K_s \triangleq \left[\max_{0\le x\le \frac{K_s-K_{s-1}}{K_s}} f_s(x)\right]^{-1}, \quad s = 2,3,\dots, \qquad K_1 \triangleq 1,$$

denotes the recurrent sequence introduced in [13]. Then the claim of Theorem 1, i.e., inequality (16), is equivalent to the inequality

$$K_s \le \frac{(s+1)^2}{2\log_2[(s+1)/8]}, \quad s \ge 8. \tag{49}$$

For $9 \le s \le 236$, validity of (49) can be verified by computer. For $s \ge 237$, the proof of (49) is based on the following properties of the sequence K_s:

$$K_s = \left[f_s\left(1 - \frac{K_{s-1}}{K_s}\right)\right]^{-1}, \qquad 1 - \frac{K_{s-1}}{K_s} < v_s, \quad s \ge 3, \tag{50}$$

$$v_s > \frac{s}{1+se} > \frac{2}{s}, \quad s \ge 8, \tag{51}$$

where we used the notation of (9)–(12). For a fixed $s \geq 3$, relation (50) and the first inequality in (51) were established in [13,14]. For $s \geq 8$, the second inequality in (51) is obvious. Furthermore, for $0 < x < 1$ and $s \geq 2$ we have the estimates

$$\begin{aligned} f_s(x) &\triangleq -\frac{x}{s}\Big(\log_2 x - \log_2 s\Big) - \Big(1 - \frac{x}{s}\Big)\log_2\Big[1 - \frac{x}{s}\Big] - \frac{x}{s}\log_2 s + x\Big(1 - \frac{1}{s}\Big)\log_2\Big[1 - \frac{1}{s}\Big] \\ &= -\frac{x}{s}\log_2 x + x\Big(1 - \frac{1}{s}\Big)\log_2\Big[1 - \frac{1}{s}\Big] - \Big(1 - \frac{x}{s}\Big)\log_2\Big[1 - \frac{x}{s}\Big] \\ &\geq -\frac{x}{s}\log_2 x + x\Big(1 - \frac{1}{s}\Big)\log_2\Big[1 - \frac{1}{s}\Big] + \Big(1 - \frac{x}{s}\Big)\frac{x}{s}\log_2 e, \quad 0 < x < 1, \quad s \geq 2, \end{aligned} \tag{52}$$

and

$$(s-1)\log_2\Big[1 - \frac{1}{s}\Big] > -\log_2 e, \quad s \geq 2, \tag{53}$$

which follow from definitions (9) and (10) of $f_s(x)$ and from a standard logarithmic inequality

$$\ln u \leq u - 1, \quad u > 0. \tag{54}$$

Below, in the proof of estimate (49) for $s \geq 237$, we analyze two cases separately. In the first case we consider values $s \geq 237$ for which $1 - \frac{K_{s-1}}{K_s} > \frac{2}{s}$, and in the second case, values of $s \geq 237$ for which $1 - \frac{K_{s-1}}{K_s} \leq \frac{2}{s}$.

Case 1. Let $s \geq 237$ and $1 - \frac{K_{s-1}}{K_s} > \frac{2}{s}$. Then, using the monotonic growth of $f_s(x)$, $0 < x \leq v_s$, and equations (50)–(53), one easily checks the chain

$$\begin{aligned} K_s &= \frac{1}{f_s\Big(1 - \frac{K_{s-1}}{K_s}\Big)} < \frac{1}{f_s\Big(\frac{2}{s}\Big)} \\ &\leq \frac{1}{\frac{2}{s^2}\log_2\Big[\frac{s}{2}\Big] + \frac{2\log_2 e}{s^2}\Big(1 - \frac{2}{s^2}\Big) + \frac{2(s-1)}{s^2}\log_2\Big[1 - \frac{1}{s}\Big]} \\ &= \frac{s^2}{2\log_2\Big[\frac{s}{2}\Big] + 2\log_2 e - \frac{4\log_2 e}{s^2} + 2(s-1)\log_2\Big[1 - \frac{1}{s}\Big]} < \frac{s^2}{2\log_2\Big[\frac{s}{4}\Big]}. \end{aligned}$$

Thus, inequality (49) is proved in this case.

Case 2. Let $s \geq 237$ and $1 - \frac{K_{s-1}}{K_s} \leq \frac{2}{s}$. Define $t_s \triangleq 1 - \frac{K_{s-1}}{K_s} \leq \frac{2}{s}$. From (52) and (53) we have

$$\begin{aligned} f_s(x) &\geq \frac{x}{s}\left(-\log_2 x + \log_2 e - \frac{x\log_2 e}{s} + (s-1)\log_2\Big[1 - \frac{1}{s}\Big]\right) \\ &\geq \frac{x}{s}\left(-\frac{x\log_2 e}{s} - \log_2 x\right), \quad 0 < x < 1, \quad s \geq 2. \end{aligned} \tag{55}$$

Note that the function $q_s(x) \triangleq \Big(-\frac{x\log_2 e}{s} - \log_2 x\Big)$ monotonically decreases for $x > 0$. Hence, $q_s(t_s) \geq q_s\Big(\frac{2}{s}\Big)$, since $t_s \leq \frac{2}{s}$. By virtue of (55), this means

$$f_s(t_s) \geq \frac{t_s}{s}q_s(t_s) \geq \frac{t_s}{s}q_s\left(\frac{2}{s}\right) = \frac{t_s}{s}\left(-\frac{2\log_2 e}{s^2} + \log_2\Big[\frac{s}{2}\Big]\right) > 0. \tag{56}$$

Therefore,

$$K_s - K_{s-1} = K_s t_s = \frac{t_s}{f_s(t_s)} \leq \frac{s}{\log_2\Big[\frac{s}{2}\Big] - \frac{2\log_2 e}{s^2}} \leq \frac{s}{\log_2\Big[\frac{s}{4}\Big]}, \quad s \geq 8, \tag{57}$$

where in the first two equalities we used the form of t_s and equation (50), then we applied (56), and finally we noted that $s \geq 8$. In other words, we have established the recurrent inequality

$$K_s \leq K_{s-1} + \frac{s}{\log_2\left[\frac{s}{4}\right]}, \quad s \geq 8,$$

which in our case gives (49) for $s \geq 237$ if we prove that

$$\frac{s^2}{2\log_2\left[\frac{s}{8}\right]} + \frac{s}{\log_2\left[\frac{s}{4}\right]} < \frac{(s+1)^2}{2\log_2\left[\frac{s+1}{8}\right]}, \quad s \geq 237. \tag{58}$$

By the logarithmic inequality (54), inequality (58) follows from

$$\frac{s^2}{2\log_2\left[\frac{s}{8}\right]} + \frac{s}{\log_2\left[\frac{s}{4}\right]} < \frac{(s+1)^2}{2\Big(\log_2 s + \frac{\log_2 e}{s} - 3\Big)}, \quad s \geq 237. \tag{59}$$

By elementary algebra we check that (59) is equivalent to the inequality

$$s\big((2-\log_2 e)\log_2 s + 2\log_2 e - 6\big) + \log_2^2 s - (5 + 2\log_2 e)\log_2 s + 6 + 6\log_2 e > 0,$$

whose validity for $s \geq 237$ is verified obviously. $\triangle$

2.2. Derivation of Bounds for (s,ℓ) CF Codes

2.2.1. Proof of Theorem 4. Let us prove the two claims of the theorem.

Proof of claim 1. In the proof of Theorem 4, as well as in the proof of Theorem 7, we use random coding over the ensemble of binary constant-weight codes, which is a generalization of the method developed in [7] for the classical case of disjunctive s-codes. Fix a parameter Q, $0 < Q < 1$. We use the notation (1) and (2) introduced for the definition of an (s,ℓ) CF code X of length N and size t. For an arbitrary code X and an arbitrary set $\mathcal{S} \subset [t]$, by $\boldsymbol{x}(\mathcal{S}) \triangleq \{\boldsymbol{x}(j) : j \in \mathcal{S}\}$ we denote the corresponding subset of codewords of X. For any disjoint sets $\mathcal{S}, \mathcal{L} \subset [t]$, $|\mathcal{S}| = s$, $|\mathcal{L}| = \ell$, $\mathcal{S} \cap \mathcal{L} = \varnothing$, we call the corresponding pair $(\boldsymbol{x}(\mathcal{S}), \boldsymbol{x}(\mathcal{L}))$ of subsets of X an (s,ℓ)-*good pair* if there is a row $\boldsymbol{x}_i$, $i \in [N]$, in which

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

Otherwise, a pair $(\boldsymbol{x}(\mathcal{S}), \boldsymbol{x}(\mathcal{L}))$ will be called an (s,ℓ)-*bad pair*. A column $\boldsymbol{x}(j)$ will be called an (s,ℓ)-*bad column in* X if in X there is an (s,ℓ)-bad pair $(\boldsymbol{x}(\mathcal{S}), \boldsymbol{x}(\mathcal{L}))$ and a column $\boldsymbol{x}(j) \in \boldsymbol{x}(\mathcal{L})$.

Define the ensemble $E(N,t,Q)$ of binary $N \times t$ matrices X with N rows and t columns, where columns are chosen independently and equiprobably from the set consisting of $\binom{N}{\lfloor QN \rfloor}$ columns of a fixed weight $\lfloor QN \rfloor$. Let sets $\mathcal{S}$ and $\mathcal{L}$ be fixed. For the ensemble $E(N,t,Q)$, by $P_0(N,Q,s,\ell)$ we denote the probability of the event "the pair $(\boldsymbol{x}(\mathcal{S}), \boldsymbol{x}(\mathcal{L}))$ is (s,ℓ)-bad." Clearly, $P_0(N,Q,s,\ell)$ does not depend of a choice of $\mathcal{S}$ and $\mathcal{L}$. For the ensemble $E(N,t,Q)$, by $P_1(N,t,Q,s,\ell)$ we denote the probability (independent of $j \in [t]$) of the event "column $\boldsymbol{x}(j)$ is (s,ℓ)-bad in X." It is easily seen that

$$P_1(N,t,Q,s,\ell) \leq \binom{t-1}{s+\ell-1}\binom{s+\ell-1}{s} P_0(N,Q,s,\ell) \leq \frac{t^{s+\ell-1}}{s!(\ell-1)!} P_0(N,Q,s,\ell).$$

Hence it follows that the expectation of the number of (s,ℓ)-bad columns in X is not greater than

$$tP_1(N,t,Q,s,\ell) < t\frac{t^{s+\ell-1}}{s!\,(\ell-1)!} P_0(N,Q,s,\ell).$$

Therefore, for

$$t < \left[\frac{s!\,(\ell-1)!}{2P_0(N,Q,s,\ell)}\right]^{1/(s+\ell-1)}$$

there exists an $N \times t/2$ matrix X which is an (s,ℓ) CF code. Hence, for any Q, $0 < Q < 1$, the maximum size of an (s,ℓ) CF code satisfies the inequality

$$t_{\mathrm{cf}}(N,s,\ell) \geq \left\lfloor \frac{1}{2}\left[\frac{s!\,(\ell-1)!}{2P_0(N,Q,s,\ell)}\right]^{1/(s+\ell-1)} \right\rfloor, \quad 0 < Q < 1.$$

Then, according to the definition (2) of the rate $R(s,\ell)$, we arrive at

$$\begin{gathered} R(s,\ell) \geq \underline{R}(s,\ell) \triangleq \frac{1}{s+\ell-1} \max_{0<Q<1} A(s,\ell,Q), \quad 2 \leq \ell \leq s, \\ A(s,\ell,Q) \triangleq \varlimsup_{N\to\infty} \frac{-\log_2 P_0(N,Q,s,\ell)}{N}, \quad 0 < Q < 1. \end{gathered} \tag{60}$$

To complete the proof of claim 1 it remains to compute the function $A(s,\ell,Q)$ explicitly and show that the right-hand side of (60) is given by (24).

We use the terminology of *types* [9] of sequences. Consider two fixed tuples consisting of binary constant-weight columns of length N:

$$\{\boldsymbol{x}(1),\boldsymbol{x}(2),\ldots,\boldsymbol{x}(s)\} \quad \text{and} \quad \{\boldsymbol{y}(1),\boldsymbol{y}(2),\ldots,\boldsymbol{y}(\ell)\}, \quad \text{where} \quad \boldsymbol{x}(i),\boldsymbol{y}(j) \in \{0,1\}^N,$$

such that $|\boldsymbol{x}(i)| = |\boldsymbol{y}(j)| = \lfloor QN \rfloor$ for any $i \in [s]4$, $j \in [\ell]$. The first tuple forms a binary $N \times s$ matrix X_s, and the second, an $N \times \ell$ matrix Y_ℓ. To these matrices, we assign their *types*, i.e., tuples of integers $\{n(\boldsymbol{a})\}$, $\boldsymbol{a} \triangleq (a_1,a_2,\ldots,a_s) \in \{0,1\}^s$, and $\{m(\boldsymbol{b})\}$, $\boldsymbol{b} \triangleq (b_1,b_2,\ldots,b_\ell) \in \{0,1\}^\ell$, where an element $n(\boldsymbol{a})$, $0 \leq n(\boldsymbol{a}) \leq N$ ($m(\boldsymbol{b})$, $0 \leq m(\boldsymbol{b}) \leq N$), is defined as the *number of rows in* X_s (Y_ℓ) *coinciding with* $\boldsymbol{a}$ ($\boldsymbol{b}$). Clearly, for any binary matrices X_s and Y_ℓ we have

$$\sum_{\boldsymbol{a}} n(\boldsymbol{a}) = \sum_{\boldsymbol{b}} m(\boldsymbol{b}) = N.$$

By $n(\mathbf{0})$ ($m(\mathbf{1})$) we denote the number of all-zero (all-one) rows in X_s (Y_ℓ). Note that if $N - n(\mathbf{0}) < m(\mathbf{1})$, then the corresponding pair (X_s,Y_ℓ) is (s,ℓ)-good. Otherwise, the number of different pairs of matrices (X_s,Y_ℓ) to which fixed types $(\{n(\boldsymbol{a})\},\{m(\boldsymbol{b})\})$ are assigned equals

$$\frac{N!}{\prod\limits_{\boldsymbol{a}} n(\boldsymbol{a})!}\frac{N!}{\prod\limits_{\boldsymbol{b}} m(\boldsymbol{b})!},$$

and the fraction of (s,ℓ)-bad pairs among the total number of pairs is

$$\binom{N-n(\mathbf{0})}{m(\mathbf{1})} \Big/ \binom{N}{m(\mathbf{1})}.$$

Thus,

$$P_0(N,Q,s,\ell) = \sum_{\{n(\boldsymbol{a})\}} \sum_{\{m(\boldsymbol{b})\}} \frac{N!}{\prod\limits_{\boldsymbol{a}} n(\boldsymbol{a})!}\frac{N!}{\prod\limits_{\boldsymbol{b}} m(\boldsymbol{b})!} \frac{\binom{N-n(\mathbf{0})}{m(\mathbf{1})}}{\binom{N}{m(\mathbf{1})}} \binom{N}{\lfloor QN \rfloor}^{-s-\ell}, \tag{61}$$

where the summation is over all possible types $\{n(\boldsymbol{a})\}$ and $\{m(\boldsymbol{b})\}$ for which

$$\begin{cases} n(\mathbf{0}) + m(\mathbf{1}) \le N, \\ 0 \le n(\boldsymbol{a}) \le N, \quad 0 \le m(\boldsymbol{b}) \le N, \\ \sum\limits_{\boldsymbol{a}} n(\boldsymbol{a}) = \sum\limits_{\boldsymbol{b}} m(\boldsymbol{b}) = N, \\ |\boldsymbol{x}(i)| = \sum\limits_{\boldsymbol{a}\colon a_i=1} n(\boldsymbol{a}) = |\boldsymbol{y}(j)| = \sum\limits_{\boldsymbol{b}\colon y_j=1} m(\boldsymbol{b}) = \lfloor QN \rfloor, \quad \text{for any } i \in [s],\ j \in [\ell]. \end{cases} \tag{62}$$

Let $N \to \infty$, and let $n(\boldsymbol{a}) \triangleq N[\tau(\boldsymbol{a}) + o(1)]$ and $m(\boldsymbol{b}) \triangleq N[\upsilon(\boldsymbol{b}) + o(1)]$, where fixed probability distributions $\tau \triangleq \{\tau(\boldsymbol{a})\}$, $\boldsymbol{a} \in \{0,1\}^s$, and $\upsilon \triangleq \{\upsilon(\boldsymbol{b})\}$, $\boldsymbol{y} \in \{0,1\}^\ell$, possess the properties induced by conditions (62), i.e.,

$$\begin{cases} \sum\limits_{\boldsymbol{a}\in\{0,1\}^s} \tau(\boldsymbol{a}) = 1, \quad \sum\limits_{\boldsymbol{b}\in\{0,1\}^\ell} \upsilon(\boldsymbol{b}) = 1, \quad \tau(\mathbf{0}) + \upsilon(\mathbf{1}) \le 1, \\ \sum\limits_{\boldsymbol{a}\colon a_i=1} \tau(\boldsymbol{a}) = Q, \quad \sum\limits_{\boldsymbol{b}\colon b_j=1} \upsilon(\boldsymbol{b}) = Q, \quad \text{for any } i \in [s],\ j \in [\ell]. \end{cases} \tag{63}$$

Using the Stirling formula for the types corresponding to these distributions, we find the logarithmic asymptotic of the summand in (61):

$$-\log_2 \left\{ \frac{N!}{\prod\limits_{\boldsymbol{a}} n(\boldsymbol{a})!} \frac{N!}{\prod\limits_{\boldsymbol{b}} m(\boldsymbol{b})!} \frac{\binom{N-n(\mathbf{0})}{m(\mathbf{1})}}{\binom{N}{m(\mathbf{1})}} \binom{N}{\lfloor QN \rfloor}^{-s-\ell} \right\} = N[F(\tau,\upsilon,Q) + o(1)],$$

where

$$F = F(\tau,\upsilon,Q) \triangleq \sum_{\boldsymbol{a}} \tau(\boldsymbol{a}) \log_2[\tau(\boldsymbol{a})] + \sum_{\boldsymbol{b}} \upsilon(\boldsymbol{b}) \log_2[\upsilon(\boldsymbol{b})] \\ - (1-\tau(\mathbf{0}))h\Big(\frac{\upsilon(\mathbf{1})}{1-\tau(\mathbf{0})}\Big) + (s+\ell)h(Q) + h(\upsilon(\mathbf{1})).$$

Let $\tau_Q \triangleq \{\tau_Q(\boldsymbol{a})\}$ and $\upsilon_Q \triangleq \{\upsilon_Q(\boldsymbol{b})\}$ be distributions with properties (63) that minimize $F(\tau,\upsilon,Q)$ for a given Q. Then the main term of the logarithmic asymptotic of the sum (61) is

$$A(s,\ell,Q) \triangleq \varlimsup_{N\to\infty} \frac{-\log_2 P_0(N,Q,s,\ell)}{N} = \min_{(\tau,\upsilon)\in(63)} F(\tau,\upsilon,Q) = F(\tau_Q,\upsilon_Q,Q). \tag{64}$$

Let us find the minimum of $F \triangleq F(\tau,\upsilon,Q)$ under constraints (63). Since F is continuous in the considered domain of admissible values of the argument (τ,υ) and on its boundary as well, it suffices to find the minimum of F under constrains (63) withe xcluded boundaries. Let us write the corresponding minimization problem: $F \to \min$.

$$\begin{aligned} &\text{Main function:} && F(\tau,\upsilon,Q)\colon \mathbb{X} \to \mathbb{R}; \\ &\text{Constraints:} && \begin{cases} \sum\limits_{\boldsymbol{a}\in\{0,1\}^s} \tau(\boldsymbol{a}) = 1, \\ \sum\limits_{\boldsymbol{b}\in\{0,1\}^\ell} \upsilon(\boldsymbol{b}) = 1, \\ \sum\limits_{\boldsymbol{a}\colon a_i=1} \tau(\boldsymbol{a}) = Q, \quad \text{for any } i \in [s], \\ \sum\limits_{\boldsymbol{b}\colon b_j=1} \upsilon(\boldsymbol{b}) = Q, \quad \text{for any } j \in [\ell]; \end{cases} \\ &\text{Search domain } \mathbb{X}: && \begin{cases} 0 < \tau(\boldsymbol{a}) < 1, \quad \text{for any } \boldsymbol{a} \in \{0,1\}^s, \\ 0 < \upsilon(\boldsymbol{b}) < 1, \quad \text{for any } \boldsymbol{b} \in \{0,1\}^\ell, \\ \tau(\mathbf{0}) + \upsilon(\mathbf{1}) < 1. \end{cases} \end{aligned} \tag{65}$$

To find the minimum point (τ_Q, υ_Q), we use the standard Lagrange multipliers method. Consider the Lagrangian

$$\Lambda \triangleq F(\tau,\upsilon,Q) + \lambda_0\Big(\sum_{\boldsymbol{a}}\tau(\boldsymbol{a})-1\Big) + \lambda_1\Big(\sum_{\boldsymbol{b}}\upsilon(\boldsymbol{b})-1\Big) + \sum_{i=1}^{s}\mu_i\Big(\sum_{\boldsymbol{a}\colon a_i=1}\tau(\boldsymbol{a})-Q\Big) + \sum_{i=1}^{\ell}\nu_i\Big(\sum_{\boldsymbol{b}\colon b_i=1}\upsilon(\boldsymbol{b})-Q\Big).$$

Necessary conditions for the extremal distribution (τ_Q, υ_Q) are

$$\begin{cases} \dfrac{\partial\Lambda}{\partial(\tau(\boldsymbol{a}))} = \log_2[\tau(\boldsymbol{a})] + \log_2 e + \lambda_0 + \sum\limits_{i\colon a_i=1}\mu_i = 0, \quad \text{for any } \boldsymbol{a}\neq\boldsymbol{0}, \\ \dfrac{\partial\Lambda}{\partial(\tau(\boldsymbol{0})} = \log_2[\tau(\boldsymbol{0})] + \log_2 e + \lambda_0 + \log_2\Big[\dfrac{1-\tau(\boldsymbol{0})}{1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1})}\Big] = 0, \\ \dfrac{\partial\Lambda}{\partial(\upsilon(\boldsymbol{b}))} = \log_2[\upsilon(\boldsymbol{b})] + \log_2 e + \lambda_1 + \sum\limits_{i\colon b_i=1}\nu_i = 0, \quad \text{for any } \boldsymbol{b}\neq\boldsymbol{1}, \\ \dfrac{\partial\Lambda}{\partial(\upsilon(\boldsymbol{1}))} = \log_2[\upsilon(\boldsymbol{1})] + \log_2 e + \lambda_1 + \sum\limits_{i=1}^{\ell}\nu_i + \log_2\Big[\dfrac{1-\upsilon(\boldsymbol{1})}{1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1})}\Big] = 0. \end{cases} \tag{66}$$

Remark 3. It should be noted that the inequality $\ell \geq 2$ is essential for (66), since for $\ell = L = 1$ the values $\upsilon(\boldsymbol{1}) \equiv Q$ and $\upsilon(\boldsymbol{0}) \equiv 1-Q$ are not variable. Therefore, in the proof of Theorem 7 for the case of $L = 1$ the analogous system (113) does not contain the last two equations of (66). As a result, this will lead to a principal (for the main result of this paper) distinction between the asymptotic ($s\to\infty$, $\ell\geq 2$ is fixed) of the random coding bound (26) for (s,ℓ) CF codes and the asymptotic of the random coding bound (8) for classical disjunctive s-codes. This property of random coding bounds was noted in Remark 1 (see Section 1.3).

Let us show that the matrix of second derivatives of the Lagrangian is positive definite. Indeed, for this matrix we have

$$\frac{\partial^2\Lambda}{\partial^2(\tau(\boldsymbol{a}))} = \frac{\log_2 e}{\tau(\boldsymbol{a})} > 0, \quad \text{for any } \boldsymbol{a}\neq\boldsymbol{0},$$

$$\frac{\partial^2\Lambda}{\partial^2(\upsilon(\boldsymbol{b}))} = \frac{\log_2 e}{\upsilon(\boldsymbol{b})} > 0, \quad \text{for any } \boldsymbol{b}\neq\boldsymbol{1},$$

$$a' \triangleq \frac{\partial^2\Lambda}{\partial(\tau(\boldsymbol{0}))^2} = \frac{\log_2 e}{\tau(\boldsymbol{0})} + \frac{\log_2 e\cdot\upsilon(\boldsymbol{1})}{(1-\tau(\boldsymbol{0}))(1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1}))} > 0,$$

$$b' \triangleq \frac{\partial^2\Lambda}{\partial(\tau(\boldsymbol{0}))\partial(\upsilon(\boldsymbol{1}))} = \frac{\log_2 e}{1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1})} > 0,$$

$$c' \triangleq \frac{\partial^2\Lambda}{\partial(\upsilon(\boldsymbol{1}))^2} = \frac{\log_2 e}{\upsilon(\boldsymbol{1})} + \frac{\log_2 e\cdot\tau(\boldsymbol{0})}{(1-\upsilon(\boldsymbol{1}))(1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1}))} > 0,$$

and all the other elements are zero. Therefore, it suffices to check that $a'c' - b'^2 > 0$. We have

$$\begin{aligned} \frac{a'c'-b'^2}{(\log_2 e)^2} &= \frac{1}{\tau(\boldsymbol{0})\upsilon(\boldsymbol{1})} + \frac{1}{(1-\tau(\boldsymbol{0}))(1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1}))} + \frac{1}{(1-\upsilon((\boldsymbol{1}))(1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1}))} \\ &\quad + \frac{\tau(\boldsymbol{0})\upsilon(\boldsymbol{1})}{(1-\tau(\boldsymbol{0}))(1-\upsilon(\boldsymbol{1}))(1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1}))^2} - \frac{1}{(1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1}))^2} \\ &= \frac{1}{\tau(\boldsymbol{0})\upsilon(\boldsymbol{1})} + \frac{1}{(1-\tau(\boldsymbol{0}))(1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1}))} + \frac{1}{(1-\upsilon(\boldsymbol{1}))(1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1}))} \\ &\quad - \frac{1}{(1-\tau(\boldsymbol{0}))(1-\upsilon(\boldsymbol{1}))(1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1}))} \geq \frac{1-\tau(\boldsymbol{0})\upsilon(\boldsymbol{1})}{1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1})} > 0. \end{aligned}$$

The matrix of second derivatives of F coincides with the above-described matrix, and therefore [33] F is strictly convex in the domain $\mathbb{X}$.

Note that the constraint equations (65) define an affine subspace $\mathbb{G}$ in $\mathbb{R}^{2^s+2^\ell}$ of dimension $(2^s+2^\ell-(s+\ell+2))$. This implies that F is strictly convex in $\mathbb{G}\cap\mathbb{X}$ too, which in turn means that a local minimum of F in $\mathbb{G}\cap\mathbb{X}$ is global and unique. Next, we apply the Karush–Kuhn–Tucker theorem [33], which states that each solution satisfying 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. Thus, if there is a solution to the system (66) and (65) in $\mathbb{X}$, then it is unique and this point is a minimum point of F in $\mathbb{X}$.

Let us prove that symmetry of the problem implies the equality $\mu \triangleq \mu_1 = \mu_2 = \ldots = \mu_s$. It suffices to show that $\mu_i = \mu_j$ for $i \neq j$. Let $\bar{\boldsymbol{a}}_i \triangleq (0,\ldots,1,\ldots,0)$ denote an s-row with 1 in the ith position. Upon interchanging the indices i and j, we obtain a minimization problem equivalent to theoriginal one. Hence, if (τ_Q^1, υ_Q) is a solution, then the distribution (τ_Q^2, υ_Q) for which $\tau_Q^2(\boldsymbol{a}) = \tau_Q^1(\widetilde{\boldsymbol{a}})$, where $\widetilde{\boldsymbol{a}}$ is a row obtained from $\boldsymbol{a}$ by interchanging the indices i and j, is also a solution. Uniqueness of a solution τ_Q implies that the distributions (τ_Q^1, υ_Q) and (τ_Q^2, υ_Q) coincide. In particular, $\tau_Q^1(\bar{\boldsymbol{a}}_i) = \tau_Q^1(\bar{\boldsymbol{a}}_j)$. Coincidence of Lagrange multipliers follows from the first equation in (66). Using the same arguments, we can prove that $\nu \triangleq \nu_1 = \nu_2 = \ldots = \nu_\ell$.

For brevity, introduce the parameters $\widehat{\mu} \triangleq \log_2 e + \lambda_0$ and $\widehat{\nu} \triangleq \log_2 e + \lambda_1$. Then equations (66) take the form

$$\begin{cases} \widehat{\mu} + \mu \sum\limits_{i=1}^{s} a_i + \log_2[\tau(\boldsymbol{a})] = 0, \quad \text{for } \boldsymbol{a} \neq \boldsymbol{0}, \\ \widehat{\mu} + \log_2[\tau(\boldsymbol{0})] + \log_2\Big[\dfrac{1-\tau(\boldsymbol{0})}{1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1})}\Big] = 0, \\ \widehat{\nu} + \nu \sum\limits_{i=1}^{\ell} b_i + \log_2[\upsilon(\boldsymbol{b})] = 0, \quad \text{for } \boldsymbol{b} \neq \boldsymbol{1}, \\ \widehat{\nu} + \nu\ell + \log_2[\upsilon(\boldsymbol{1})] + \log_2\Big[\dfrac{1-\upsilon(\boldsymbol{1})}{1-\tau(\boldsymbol{0})-\upsilon(\boldsymbol{1})}\Big] = 0. \end{cases} \tag{67}$$

The first equation in (67) implies

$$\tau(\boldsymbol{a}) = 2^{-\widehat{\mu}} 2^{-\mu\sum a_i} = \frac{2^{-\widehat{\mu}}}{z^s} \prod_{i=1}^{s} \widetilde{P}_1(a_i), \quad \text{for } \boldsymbol{a} \neq \boldsymbol{0},$$

where

$$\widetilde{P}_1(0) \triangleq \frac{1}{1+2^{-\mu}} \triangleq z, \qquad \widetilde{P}_1(1) \triangleq \frac{2^{-\mu}}{1+2^{-\mu}} \triangleq 1-z.$$

From conditions (65) we obtain

$$Q = \frac{2^{-\widehat{\mu}}}{z^s} \sum_{k=0}^{s-1} \binom{s-1}{k} z^{s-k-1}(1-z)^{k+1} = \frac{1-z}{2^{\widehat{\mu}} z^s} \quad \Longleftrightarrow \quad \widehat{\mu} = \log_2\Big[\frac{1-z}{Qz^s}\Big].$$

Next, since $\tau = \{\tau(\boldsymbol{a})\}$, $\boldsymbol{a} \in \{0,1\}^s$, is a probability distribution, we have

$$1-\tau(\boldsymbol{0}) = \sum_{\boldsymbol{a}>\boldsymbol{0}} \tau(\boldsymbol{a}) = \frac{2^{-\widehat{\mu}}}{z^s} \sum_{k=1}^{s} \binom{s}{k} z^{s-k}(1-z)^k = \frac{Q(1-z^s)}{1-z}.$$

Therefore, all probabilities of the extremal distribution $\tau_Q = \{\tau_Q(\boldsymbol{a})\}$ can be represented as functions of an independent variable z, $0 < z < 1$:

$$\tau_Q(\boldsymbol{a}) = \frac{Q}{1-z} z^{\,s-\sum\limits_{i=1}^{s} a_i} (1-z)^{\sum\limits_{i=1}^{s} a_i}, \quad \text{for } \boldsymbol{a} \neq \boldsymbol{0}, \qquad \tau_Q(\boldsymbol{0}) = 1 - \frac{Q(1-z^s)}{1-z}. \tag{68}$$

Similarly, using constraints (65), the parameters ν and $\widehat{\nu}$ in the third equation in (67), as well as probabilities of the extremal distribution $\upsilon_Q = \{\upsilon_Q(\boldsymbol{b})\}$, $\boldsymbol{b} \in \{0,1\}^\ell$, can be represented as functions of an independent variable u, $0 < u < 1$:

$$\begin{gathered}\frac{1}{1+2^{-\nu}} \triangleq u, \qquad \widehat{\nu} = \log_2\biggl[\frac{1-u}{Qu^\ell}\biggr],\\ \upsilon_Q(\boldsymbol{b}) = \frac{Q}{1-u}u^{\ell-\sum\limits_{j=1}^{\ell} b_j}(1-u)^{\sum\limits_{j=1}^{\ell} b_j}, \quad \text{for } \boldsymbol{b} \neq \mathbf{1},\\ \upsilon_Q(\mathbf{1}) = 1 - \frac{Q(1-(1-u)^\ell)}{1-u}.\end{gathered} \tag{69}$$

Upon substituting the obtained expressions for μ, $\widehat{\mu}$, ν, $\widehat{\nu}$, $\tau_Q(\mathbf{0})$, and $\upsilon_Q(\mathbf{1})$ into the second and fourth equations in (67), we obtain

$$\begin{cases}\log_2\biggl[\dfrac{1-z-Q(1-z^s)}{z^s}\biggr]\\ \quad + \log_2\biggl[\dfrac{(1-u)(1-z^s)}{Q(1-z)(1-(1-u)^\ell)+(1-u)(Q(1-z^s)-1+z)}\biggr] = 0,\\ \log_2\biggl[\dfrac{1-u-Q(1-(1-u)^\ell)}{(1-u)^\ell}\biggr]\\ \quad + \log_2\biggl[\dfrac{(1-z)(1-(1-u)^\ell)}{Q(1-z)(1-(1-u)^\ell)+(1-u)(Q(1-u^s)-1+z)}\biggr] = 0.\end{cases} \tag{70}$$

Note that any solution $0 < z, u < 1$ of system (70) defines the distributions τ_Q and υ_Q. Add to (70) an additional condition $z = u$. If in the extended system we find a solution $0 < z = u < 1$, it will also define τ_Q and υ_Q by uniqueness of a solution of a convex Lagrange problem. It is easily seen that equations (70) become equivalent under $z = u$:

$$\begin{cases}\dfrac{1-z-Q}{z^s} = -Q(1-z)^\ell,\\ \dfrac{1-z-Q}{(1-z)^\ell} = -Qz^s.\end{cases}$$

Hence we find

$$Q = Q(z) = \frac{1-z}{1-z^s(1-z)^\ell}. \tag{71}$$

The map $Q(z)\colon (0,1) \to (0,1)$ is bijective, since for any fixed $0 < Q < 1$ there exists a unique distribution $\tau_Q \triangleq \tau_{Q(z)} = \{\tau_{Q(z)}(\boldsymbol{x})\}$ defined by a unique parameter z, and $\tau_{Q(z_1)} \neq \tau_{Q(z_2)}$ for $z_1 \neq z_2$. Therefore, to find the maximum in (64) over Q, $0 < Q < 1$, we can use the equalities

$$\max_{0<Q<1} A(s,\ell,Q) = \max_{0<Q<1} F(\tau_Q, \upsilon_Q, Q) = \max_{0<z<1} F(\tau_{Q(z)}, \upsilon_{Q(z)}Q(z)), \tag{72}$$

where

$$\begin{aligned}F(\tau_{Q(z)}, \upsilon_{Q(z)}Q(z)) &= \sum_{\boldsymbol{a}} \tau_Q(\boldsymbol{a}) \log_2[\tau_Q(\boldsymbol{a})] + \sum_{\boldsymbol{b}} \upsilon_Q(\boldsymbol{b}) \log_2[\upsilon_Q(\boldsymbol{b})]\\ &\quad - (1-\tau_Q(\mathbf{0}))h\biggl(\frac{\upsilon_Q(\mathbf{1})}{1-\tau_Q(\mathbf{0})}\biggr) + (s+\ell)h(Q) + h(\upsilon_Q(\mathbf{1})).\end{aligned} \tag{73}$$

Set $u \triangleq z$ in (69). Then, using (68) and (69), represent all the five terms on the right-hand side of (73) as functions of one and the same independent variable z, $0 < z < 1$:

$$\sum_{\boldsymbol{a}} \tau_Q(\boldsymbol{a}) \log_2[\tau_Q(\boldsymbol{a})] = \Biggl\{ \sum_{k=1}^{s} \binom{s}{k} \frac{z^{s-k}(1-z)^k}{1-z^s(1-z)^\ell} \log_2 \Biggl[\frac{z^{s-k}(1-z)^k}{1-z^s(1-z)^\ell} \Biggr] \Biggr\}$$
$$+ \frac{z^s(1-(1-z)^\ell)}{1-z^s(1-z)^\ell} \log_2 \Biggl[\frac{z^s(1-(1-z)^\ell)}{1-z^s(1-z)^\ell} \Biggr] = \Biggl\{ \frac{s(1-z^s)-s(1-z)}{1-z^s(1-z)^\ell} \log_2 z$$
$$+ \frac{s(1-z)}{1-z^s(1-z)^\ell} \log_2[1-z] - \frac{1-z^s}{1-z^s(1-z)^\ell} \log_2[1-z^s(1-z)^\ell] \Biggr\}$$
$$+ \frac{sz^s(1-(1-z)^\ell)}{1-z^s(1-z)^\ell} \log_2 z + \frac{z^s(1-(1-z)^\ell)}{1-z^s(1-z)^\ell} \log_2[1-(1-z)^\ell]$$
$$- \frac{z^s(1-(1-z)^\ell)}{1-z^s(1-z)^\ell} \log_2[1-z^s(1-z)^\ell] = \frac{s(z-z^s(1-z)^\ell)}{1-z^s(1-z)^\ell} \log_2 z$$
$$+ \frac{s(1-z)}{1-z^s(1-z)^\ell} \log_2[1-z] + \frac{z^s(1-(1-z)^\ell)}{1-z^s(1-z)^\ell} \log_2[1-(1-z)^\ell]$$
$$- \log_2[1-z^s(1-z)^\ell], \tag{74}$$

$$\sum_{\boldsymbol{b}} \upsilon_Q(\boldsymbol{b}) \log_2[\upsilon_Q(\boldsymbol{b})] = \sum_{k=0}^{\ell} \binom{\ell}{k} \frac{z^{\ell-k}(1-z)^k}{1-z^s(1-z)^\ell} \log_2 \Biggl[\frac{z^{\ell-k}(1-z)^k}{1-z^s(1-z)^\ell} \Biggr]$$
$$+ \frac{(1-z)^\ell(1-z^s)}{1-z^s(1-z)^\ell} \log_2 \Biggl[\frac{(1-z)^\ell(1-z^s)}{1-z^s(1-z)^\ell} \Biggr] = \frac{\ell z}{1-z^s(1-z)^\ell} \log_2 z$$
$$+ \frac{\ell((1-z)-z^s(1-z)^\ell)}{1-z^s(1-z)^\ell} \log_2[1-z] + \frac{(1-z)^\ell(1-z^s)}{1-z^s(1-z)^\ell} \log_2[1-z^s]$$
$$- \log_2[1-z^s(1-z)^\ell], \tag{75}$$

$$-(1-\tau_Q(\boldsymbol{0}))h\Biggl(\frac{\upsilon_Q(\boldsymbol{1})}{1-\tau_Q(\boldsymbol{0})}\Biggr) = -(1-\tau_Q(\boldsymbol{0})) \log_2[1-\tau_Q(\boldsymbol{0})]$$
$$+ \upsilon_Q(\boldsymbol{1}) \log_2[\upsilon_Q(\boldsymbol{1})] + (1-\tau_Q(\boldsymbol{0})-\upsilon_Q(\boldsymbol{1})) \log_2[1-\tau_Q(\boldsymbol{0})-\upsilon_Q(\boldsymbol{1})]$$
$$= \frac{\ell(1-z^s)(1-z)^\ell}{1-z^s(1-z)^\ell} \log_2[1-z] + \frac{(1-z^s)(1-(1-z)^\ell)}{1-z^s(1-z)^\ell} \log_2[1-(1-z)^\ell], \tag{76}$$

$$(s+\ell)h(Q) = (s+\ell) \log_2[1-z^s(1-z)^\ell] - \frac{(s+\ell)(1-z)}{1-z^s(1-z)^\ell} \log_2[1-z]$$
$$- \frac{(s+\ell)(z-z^s(1-z)^\ell)}{1-z^s(1-z)^\ell} \log_2 z - \frac{(s+\ell)(z-z^s(1-z)^\ell)}{1-z^s(1-z)^\ell} \log_2[1-z^{s-1}(1-z)^\ell], \tag{77}$$

$$h(\upsilon_Q(\boldsymbol{1})) = -\frac{(1-z)^\ell(1-z^s)}{1-z^s(1-z)^\ell} \log_2 \Biggl[\frac{(1-z)^\ell(1-z^s)}{1-z^s(1-z)^\ell} \Biggr]$$
$$- \frac{1-(1-z)^\ell}{1-z^s(1-z)^\ell} \log_2 \Biggl[\frac{1-(1-z)^\ell}{1-z^s(1-z)^\ell} \Biggr] = \log_2[1-z^s(1-z)^\ell]$$
$$- \frac{1-(1-z)^\ell}{1-z^s(1-z)^\ell} \log_2[1-(1-z)^\ell] - \frac{\ell(1-z)^\ell(1-z^s)}{1-z^s(1-z)^\ell} \log_2[1-z]$$
$$- \frac{(1-z)^\ell(1-z^s)}{1-z^s(1-z)^\ell} \log_2[1-z^s]. \tag{78}$$

Substituting (74)–(78) into (73) and collecting like terms yields

$$F(\tau_{Q(z)}, \upsilon_{Q(z)}Q(z)) = T(z,s,\ell), \quad 0 < z < 1, \quad 2 \le \ell \le s, \tag{79}$$

where the function $T(z,s,\ell)$ of argument z, $0<z<1$, and parameters $2\le\ell\le s$ is introduced in (25). Therefore, it follows from (60), (72), and (79) that for the rate of (s,ℓ) CF codes we have

$$R(s,\ell)\ge\underline{R}(s,\ell)\triangleq\frac{1}{s+\ell-1}\max_{0<z<1}T(z,s,\ell). \tag{80}$$

Claim 1 is proved.

Proof of claim 2. Let $\ell\ge 2$ be fixed and $s\to\infty$. On the right-hand side of (80), replace the maximum over z, $0<z<1$, of the function (25) with its value at $z=\dfrac{s}{s+\ell}$. This gives a lower bound

$$\underline{R}(s,\ell)\ge\frac{1}{s+\ell-1}T\Big(\frac{s}{s+\ell},s,\ell\Big)=\frac{e^{-\ell}\ell^{\ell+1}\log_2 s}{s^{\ell+1}}(1+o(1)),\quad s\to\infty,\quad \ell\ge 2, \tag{81}$$

where the asymptotic equality is easily established by directly using the definition (25). To prove (26), we have to check that estimate (81) is tight. Also, directly using equation (25), we can show that for $s\to\infty$ and fixed $\ell\ge 2$ we have

$$\max_{0<z<1}T(z,s,\ell)\le\max_{0<z<1}\left\{z^s(1-z)^\ell\left(\ell\log_2\Big[\frac{z}{1-z}\Big]+1\right)\right\}(1+o(1)).$$

By finding a zero of the derivative in z, $0<z<1$, one can easily check that for any fixed $2\le\ell<s$ the maximum is attained at

$$z=\frac{s}{s+\ell}+\frac{\ell\log_2 e}{(s+\ell)\Big(\ell\log_2\Big[\frac{z}{1-z}\Big]+1\Big)}.$$

Therefore, we have the following asymptotic inequality:

$$\begin{aligned}\max_{0<z<1}T(z,s,\ell)&\le\left(\frac{s}{s+\ell}\right)^s\left(\frac{\ell}{s+\ell}\right)^\ell\ell\log_2\Big[\frac{s}{\ell}\Big](1+o(1))\\&=\frac{e^{-\ell}\ell^{\ell+1}\log_2 s}{s^\ell}(1+o(1)).\end{aligned} \tag{82}$$

The definition (80) and inequality (82) imply an asymptotic upper bound

$$\underline{R}(s,\ell)=\frac{1}{s+\ell-1}\max_{0<z<1}T(z,s,\ell)\le\frac{e^{-\ell}\ell^{\ell+1}\log_2 s}{s^{\ell+1}}(1+o(1)),\quad s\to\infty,\quad \ell\ge 2,$$

which completes the proof of equation (26). Claim 2 is proved. $\triangle$

To find the asymptotic (29) of the fraction $Q(s,\ell)$ of the optimal weight, we substitute $z=\dfrac{s}{s+\ell}$ into (71) to obtain

$$Q(s,\ell)=\frac{1-z}{1-z^s(1-z)^\ell}=\frac{\ell}{s}(1+o(1)),\quad s\to\infty.$$

2.2.2. Proof of Theorem 5. Let $s\ge k>\ell\ge 1$. If $p>0$ and ps is an integer, then inequality (20) can be represented as

$$R(s+sp,k)\le R(s,\ell)\frac{(sp)^{sp}(k-\ell)^{k-\ell}}{(sp+k-\ell)^{sp+k-\ell}}.$$

Hence it follows that

$$R(s,\ell)\ge\sup_{p>0,k>\ell}\left\{R((1+p)s,k)\frac{(sp+k-\ell)^{sp+k-\ell}}{(sp)^{sp}(k-\ell)^{k-\ell}}\right\}.$$

Using, as $s \to \infty$, the asymptotic lower bound (26) on the rate $R((1+p)s, k)$, we arrive at

$$\begin{aligned} R(s,\ell) &\geq \sup_{\substack{p>0\\k>\ell}} \left\{ \frac{e^{-k}k^{k+1}\log_2[s(1+p)]}{(s(1+p))^{k+1}} \frac{(sp+k-\ell)^{sp+k-\ell}}{(sp)^{sp}(k-\ell)^{k-\ell}} \right\} (1+o(1)) \\ &= \sup_{\substack{p>0\\k>\ell}} \left\{ \frac{e^{-k}k^{k+1}p^{k-\ell}\Big(1+\frac{k-\ell}{sp}\Big)^{sp+k-\ell}}{(1+p)^{k+1}(k-1)^{k-1}} \right\} \frac{\log_2 s}{s^{\ell+1}}(1+o(1)) \\ &= \sup_{k>\ell} \left\{ \frac{e^{-\ell}k^{k+1}\Big(\frac{k-\ell}{\ell+1}\Big)^{k-\ell}}{\Big(\frac{k+1}{\ell+1}\Big)^{k+1}(k-\ell)^{k-\ell}} \right\} \frac{\log_2 s}{s^{\ell+1}}(1+o(1)) = \left(\frac{\ell+1}{e}\right)^{\ell+1} \frac{\log_2 s}{s^{\ell+1}}(1+o(1)), \end{aligned}$$

where we took into account that

$$\max_{p>0} \frac{p^{k-\ell}}{(1+p)^{k+1}} = \left(\frac{k-\ell}{\ell+1}\right)^{k-\ell} \left(\frac{k+1}{\ell+1}\right)^{-k-1}$$

and the maximum is attained at $p = \dfrac{k-\ell}{\ell+1}$. $\triangle$

2.2.3. Proof of Theorem 3. Let $s \geq \ell \geq 2$. Of for a fixed p, $0 < p < 1$, the product sp is an integer, then by letting $j \triangleq \ell - 1$ on the right-hand side of (20), we obtain

$$R(s,\ell) \leq R(s(1-p),1) \frac{(ps)^{ps}(\ell-1)^{\ell-1}}{(ps+\ell-1)^{ps+\ell-1}}.$$

If $s \to \infty$ and $\ell \geq 2$ is fixed, then, applying the asymptotic equality (17) for the rate $R(s(1-p),1)$, we obtain

$$\begin{aligned} R(s,\ell) &\leq \min_{0<p<1} \left\{ \frac{2\log_2[s(1-p)]}{s^2(1-p)^2} \frac{(ps)^{ps}(\ell-1)^{\ell-1}}{(ps+\ell-1)^{ps+\ell-1}} \right\} (1+o(1)) \\ &= \frac{(\ell+1)^{\ell+1}}{2e^{\ell-1}} \frac{\log_2 s}{s^{\ell+1}}(1+o(1)), \end{aligned}$$

where we took into account that

$$\max_{0<p<1} \{(1-p)^2 p^{\ell-1}\} = (\ell-1)^{\ell-1} \frac{4}{(\ell+1)^{\ell+1}}$$

and the maximum is attained at $p = \dfrac{\ell-1}{\ell+1}$. $\triangle$

2.3. Derivation of Bounds for the Rate of s_L-LD Codes

2.3.1. Proof of Theorem 6. Let us prove the three claims of the theorem.

Proof of claim 1. Bound (31) means that for $s \leq L$ the claim of Theorem 6, i.e., the inequality $R_L(s) \leq 1/s$, is true. Now let $s > L \geq 1$, and let X be an arbitrary s_L-LD code of size t and length N containing at least one column (codeword) of an arbitrary fixed weight w, $1 \leq w \leq N$. By analogy with arguments in [13, 14] for the case of $L = 1$, we can deduce that

$$w \leq N - N_{\mathrm{ld}}(t-1, s-1, L), \tag{83}$$

where $N_{\mathrm{ld}}(t,s,L)$ denotes the minimum length of an s_L-LD code of size t from Definition 2.

Now from (83), the first inequality in (32), and upper bounds [13,14] on the number of codewords of a fixed weight in a disjunctive $\lfloor s/L \rfloor$-code it follows that for the size t of any s_L-LD code we have the upper bound

$$t \le N_{\mathrm{ld}}(t,s,L) + \sum_{w=\lfloor s/L\rfloor+1}^{N_{\mathrm{ld}}(t,s,L)-N_{\mathrm{ld}}(t-1,s-1,L)} \frac{s^2}{L^2} \frac{\binom{N_{\mathrm{ld}}(t,s,L)}{\lceil q\rceil}}{\binom{\lfloor q\rfloor \lfloor s/L\rfloor}{\lfloor q\rfloor}} + L - 1, \quad q = \frac{w}{\lfloor s/L\rfloor}. \tag{84}$$

Here and in what follows, we use notation (33)–(36) to describe the recurrent upper bound $\overline{R}_L(s)$. If $t \to \infty$, then using (84) and analytical arguments similar to [13, 14], we obtain

$$\frac{\log_2 t}{N_{\mathrm{ld}}(t,s,L)} \le \max_{0\le v\le 1-\frac{N_{\mathrm{ld}}(t-1,s-1,L)}{N_{\mathrm{ld}}(t,s,L)}} f_{\lfloor s/L\rfloor}(v)(1+o(1)), \quad s > L, \quad t \to \infty. \tag{85}$$

Now let us show that for s_L-LD codes we have $R_L(s) \le \overline{R}_L(s)$ for $s > L$. To this end, it suffices to prove by induction by contradiction that $R_L(s) \le r_L(s)$ for $s > L$. The induction base is the inequality

$$R_L(L+1) \le r_L(L+1). \tag{86}$$

To prove (86), it suffices to show that for $s = L+1$ the trivial bound is better than the recurrent bound, i.e.,

$$\frac{1}{L+1} \le r_L(L+1). \tag{87}$$

For each value of $s = 2, 3, \ldots$, we introduce an auxiliary function of x, $0 < x < 1$:

$$G_s(x) \triangleq x - \max_{0\le v\le 1-\frac{x}{\overline{R}_L(s-1)}} f_{\lfloor s/L\rfloor}(v), \quad 0 < x < 1. \tag{88}$$

The definition (88) immediately implies that $G_s(x)$, $0 < x < 1$, is monotonically increasing and that its unique zero is $r_L(s)$. Hence, to prove (87), it suffices to show that $G_{L+1}\Big(\frac{1}{L+1}\Big) \le 0$. Using inequality (55), we obtain the following bound:

$$\begin{aligned} G_{L+1}\Big(\frac{1}{L+1}\Big) &= \frac{1}{L+1} - \max_{0\le v\le 1-\frac{L}{L+1}} f_1(v) \le \frac{1}{L+1} - f_1\Big(\frac{1}{L+1}\Big) \\ &\le \frac{1}{L+1}\left(1 - \log_2(L+1) + \frac{\log_2 e}{L+1}\right) < 0. \end{aligned} \tag{89}$$

The last inequality for $L = 2$ is checked by direct substitution, and for larger L it is valid by monotonicity arguments. Therefore, (87) is proved, as well as the induction base (86).

Now we check by contradiction that the induction step holds. Taking into account the definition (3) of the rate $R_L(s)$ of s_L-LD codes, assume that

$$\begin{aligned} R_L(s-1) &\triangleq \varlimsup_{t\to\infty} \frac{\log_2 t}{N_{\mathrm{ld}}(t,s-1,L)} \le \overline{R}_L(s-1), \\ R_L(s) &\triangleq \varlimsup_{t\to\infty} \frac{\log_2 t}{N_{\mathrm{ld}}(t,s,L)} > r_L(s). \end{aligned} \tag{90}$$

Then by (90) we have the chain of inequalities

$$\begin{aligned} \varlimsup_{t\to\infty}\left(1 - \frac{N_{\mathrm{ld}}(t-1,s-1,L)}{N_{\mathrm{ld}}(t,s,L)}\right) &< \varlimsup_{t\to\infty}\left(1 - \frac{N_{\mathrm{ld}}(t-1,s-1,L) r_L(s)}{\log_2 t}\right) \\ &\le 1 - \frac{r_L(s)}{\overline{R}_L(s-1)}. \end{aligned}$$

It follows from (85) and the obtained inequality that for s_L-LD codes we have

$$R_L(s) = \overline{\lim_{t\to\infty}} \frac{\log_2 t}{N_{\rm ld}(t,s,L)} \le \overline{\lim_{t\to\infty}} \max_{0\le v\le 1-\frac{N_{\rm ld}(t-1,s-1,L)}{N_{\rm ld}(t,s,L)}} f_{\lfloor s/L\rfloor}(v)$$
$$\le \max_{0\le v\le 1-\frac{r_L(s)}{\overline{R}_L(s-1)}} f_{\lfloor s/L\rfloor}(v) = r_L(s),$$

where in the last inequality we used the definition (35) and (36) of $r_L(s)$. The obtained contradiction proves the induction step.

Now, to complete the proof of claim 1, we establish equality (37). We use reasoning by contradiction. Since the function $f_{\lfloor s/L\rfloor}(v)$ of the parameter v, $0 < v < 1$, defined by (9)–(11) is $\cap$-convex and attains its maximum at $v = v_{\lfloor s/L\rfloor}$, then the contradiction assumption can be written as

$$r_L(s) = f_{\lfloor s/L\rfloor}(v_{\lfloor s/L\rfloor}), \qquad v_{\lfloor s/L\rfloor} < 1 - \frac{r_L(s)}{\overline{R}_L(s-1)}, \qquad L \ge 1, \quad s > 2L. \tag{91}$$

Hence it follows that

$$v_{\lfloor s/L\rfloor} < 1 - \frac{f_{\lfloor s/L\rfloor}(v_{\lfloor s/L\rfloor})}{\overline{R}_L(s-1)} \quad\Longleftrightarrow\quad \overline{R}_L(s-1) > \frac{f_{\lfloor s/L\rfloor}(v_{\lfloor s/L\rfloor})}{1-v_{\lfloor s/L\rfloor}}. \tag{92}$$

Let us show that (92) is wrong, i.e., we have

$$\overline{R}_L(s-1) \le \frac{f_{\lfloor s/L\rfloor}(v_{\lfloor s/L\rfloor})}{1-v_{\lfloor s/L\rfloor}}, \quad L \ge 1, \quad s > 2L. \tag{93}$$

Since $v_{\lfloor \frac{s-1}{L}\rfloor}$ is a point where $f_{\lfloor \frac{s-1}{L}\rfloor}$ attains its global maximum, we have

$$\overline{R}_L(s-1) \le r_L(s-1) \le f_{\lfloor \frac{s-1}{L}\rfloor}(v_{\lfloor \frac{s-1}{L}\rfloor}), \quad L \ge 1, \quad s > 2L.$$

Therefore, to derive (93) it suffices to check that

$$f_{\lfloor \frac{s-1}{L}\rfloor}(v_{\lfloor \frac{s-1}{L}\rfloor}) \le \frac{f_{\lfloor s/L\rfloor}(v_{\lfloor s/L\rfloor})}{1-v_{\lfloor s/L\rfloor}}, \quad L \ge 1, \quad s > 2L. \tag{94}$$

If $s \ne kL$, then $\left\lfloor \frac{s-1}{L}\right\rfloor = \lfloor s/L\rfloor$, and therefore (94) is obviously valid. If $s = kL$, then $\left\lfloor \frac{s-1}{L}\right\rfloor = k-1$ and $\lfloor s/L\rfloor = k$. Then (94) follows from the inequality $f_{k-1}(v_{k-1}) \le \frac{f_k(v_k)}{1-v_k}$, $k > 2$, obtained in [13]. Claim 1 is proved completely.

Proof of claim 2. We will use the function $G_s(x)$ defined in (88). Taking into account an obvious inequality

$$\overline{R}_L(s-1) \le 1/(s-1), \quad s \ge 2, \quad L \ge 1,$$

monotonic growth of $f_{\lfloor s/L\rfloor}(v)$, $0 \le v \le 1/s$, implied by (51), and definitions (9) and (10), we obtain a chain of inequalities

$$G_s\Big(\frac{1}{s}\Big) \ge \frac{1}{s} - \max_{0\le v\le 1-\frac{s-1}{s}} f_{\lfloor s/L\rfloor}(v) = \frac{1}{s} - \max_{0\le v\le \frac{1}{s}} f_{\lfloor s/L\rfloor}(v) = \frac{1}{s} - f_{\lfloor s/L\rfloor}\Big(\frac{1}{s}\Big)$$
$$> \frac{1}{s} - h\Big(\frac{1}{s\lfloor s/L\rfloor}\Big) > \frac{1}{s} - \frac{1}{s\lfloor s/L\rfloor}\log_2[s\lfloor s/L\rfloor] - \frac{2\log_2 e}{s\lfloor s/L\rfloor}, \quad s > 3.$$

Hence it follows that for a fixed L, $L \geq 1$, there exists an integer $s(L) \geq 3$ such that $G_s\big(\frac{1}{s}\big) > 0$ for $s > s(L)$. Together with the property given immediately after definition (88), this means that $r_L(s) < \frac{1}{s}$ for $s > s(L)$. In particular, for L large enough and $s > L(\log_2 L + 3\log_2[\log_2 L])$, we have

$$\frac{1}{s} - \frac{1}{s\lfloor s/L\rfloor}\log_2(e^2 s\lfloor s/L\rfloor) = \frac{1}{s}\left(1 - \frac{\log_2\lfloor s/L\rfloor + \log_2[e^2 s]}{\lfloor s/L\rfloor}\right) > 0.$$

Thus, $s(L) \leq L\log_2 L(1+o(1))$.

To prove the inequality $s(L) \geq L\log_2 L(1+o(1))$, we check by induction that $G_s(1/s) < 0$ for $L < s < L\log_2 L - L$. The induction base for $s = L+1$, i.e., inequality (89), was proved when deriving claim 1. The induction hypothesis, i.e., the inequality $G_{s-1}(1/(s-1)) < 0$, implies that $1/(s-1) < r_L(s-1)$, and thus the upper bound for the rate $\overline{R}_L(s-1) = 1/(s-1)$ coincides with the trivial bound. Therefore, checking the induction step is the chain

$$\begin{aligned} G_s\Big(\frac{1}{s}\Big) &= \frac{1}{s} - \max_{0\leq v\leq 1-\frac{s-1}{s}} f_{\lfloor s/L\rfloor}(v) = \frac{1}{s} - f_{\lfloor s/L\rfloor}\Big(\frac{1}{s}\Big) \\ &\leq \frac{1}{s}\left(1 - \frac{\log_2 s - \dfrac{\log_2 e}{s\lfloor s/L\rfloor}}{\lfloor s/L\rfloor}\right) < 0, \end{aligned}$$

where in the first inequality for estimating the sequence $f_{\lfloor s/L\rfloor}(1/s)$ we used (55), and in the second inequality we took into account that $L < s < L\log_2 L - L$.

Thus, we obtain $s(L) = L\log_2 L(1+o(1))$. Claim 2 is proved.

Proof of claim 3. For a fixed $L \geq 1$, introduce a sequence $K_L(s)$, $s \geq L+1$, defined recursively:

$$K_L(L) \triangleq 1, \qquad K_L(s) \triangleq \left[f_{\lfloor s/L\rfloor}\left(1 - \frac{K_L(s-1)}{K_L(s)}\right)\right]^{-1}, \quad s = L+1, L+2, \ldots \tag{95}$$

It is easily seen from definitions (33)–(37) that for any fixed $L \geq 1$ we have

$$r_L(s) \leq \frac{1}{K_L(s)}, \quad s \geq 1, \qquad \text{and} \qquad r_L(s) = \frac{1}{K_L(s)}(1+o(1)), \quad \text{as} \quad s \to \infty.$$

Using arguments similar to the proof of Theorem 1, one can establish a nonasymptotic upper bound

$$K_L(s) \leq \frac{(s+1)^2}{2L\log_2\Big[\dfrac{s+1}{8}\Big]}, \quad L \geq 1, \quad s \geq 8. \tag{96}$$

Hence, to prove the asymptotic equality (38), it suffices to show that we have the asymptotic inequality

$$K_L(s) \geq \frac{s^2}{2L\log_2 s}(1+o(1)), \quad s \to \infty. \tag{97}$$

For any $s > L$, the function $f_{\lfloor s/L\rfloor}(v)$ of the argument v, $0 \leq v \leq 1$, is $\cap$-convex. Therefore, for any a, $0 < a < 1$, we have

$$f_{\lfloor s/L\rfloor}(v) \leq f_{\lfloor s/L\rfloor}(a) + (v-a)f'_{\lfloor s/L\rfloor}(a), \quad 0 \leq v \leq 1, \quad 0 < a < 1. \tag{98}$$

Set $v \triangleq 1 - \dfrac{K_L(s-1)}{K_L(s)}$ in (98). Then, substituting the right-hand side of (98) into definition (95), after simple transformations we arrive at the ineqiality

$$K_L(s) \geq K_L(s-1) + \frac{1 - g_{\lfloor s/L\rfloor}(a)K_L(s-1)}{f'_{\lfloor s/L\rfloor}(a) + g_{\lfloor s/L\rfloor}(a)}, \quad s > L, \quad 0 < a < 1, \tag{99}$$

where

$$g_{\lfloor s/L\rfloor}(a) \triangleq f_{\lfloor s/L\rfloor}(a) - af'_{\lfloor s/L\rfloor}(a), \quad s > L, \quad 0 < a < 1. \tag{100}$$

For the functions (10) and (100), the properties

$$g_{\lfloor s/L\rfloor}\Big(\frac{2}{\lfloor s/L\rfloor}\Big) \le \frac{2\log_2 e}{\lfloor s/L\rfloor^2 - 2}, \quad s > L, \tag{101}$$

$$f'_{\lfloor s/L\rfloor}\Big(\frac{2}{\lfloor s/L\rfloor}\Big) + g_{\lfloor s/L\rfloor}\Big(\frac{2}{\lfloor s/L\rfloor}\Big) \le \frac{\log_2\Big[\frac{\lfloor s/L\rfloor}{2}\Big]}{\lfloor s/L\rfloor}, \quad s > L, \tag{102}$$

were proved in [13, 14]. Note also that for $s > s_0$ large enough, (96) and (101) imply the inequality

$$1 - g_{\lfloor s/L\rfloor}\Big(\frac{2}{\lfloor s/L\rfloor}\Big)K_L(s-1) > 0. \tag{103}$$

If $s > s_0$, then, letting $a \triangleq \dfrac{2}{\lfloor s/L\rfloor}$ in (99) and taking into account (101)–(103), we obtain

$$K_L(s) \ge K_L(s-1) + \frac{\lfloor s/L\rfloor}{\log_2\Big[\frac{\lfloor s/L\rfloor}{2}\Big]} - K_L(s-1)\frac{2\lfloor s/L\rfloor\log_2 e}{(\lfloor s/L\rfloor^2 - 2)\log_2\Big[\frac{\lfloor s/L\rfloor}{2}\Big]}. \tag{104}$$

If $s \to \infty$, then by (96) for the last term on the right-hand side of (104) we have an asymptotic estimate

$$K_L(s-1)\frac{2\lfloor s/L\rfloor\log_2 e}{(\lfloor s/L\rfloor^2 - 2)\log_2\Big[\frac{\lfloor s/L\rfloor}{2}\Big]} = o\Big(\frac{s}{\log_2 s}\Big).$$

Therefore, as $s \to \infty$, the recurrent inequality (104) yields an asymptotic lower bound

$$\begin{aligned} K_L(s) &\ge \sum_{k=2L}^{s} \frac{\lfloor k/L\rfloor}{\log_2\Big[\frac{\lfloor k/L\rfloor}{2}\Big]}(1 + o(1)) \\ &\ge \sum_{k=2L}^{s} \frac{k}{L\log_2 s}(1 + o(1)) = \frac{s^2}{2L\log_2 s}(1 + o(1)). \end{aligned} \tag{105}$$

The asymptotic inequality (97) follows from (105). Claim 3 is proved. $\triangle$

2.3.2. Poof of Theorem 7. Let us prove the three claims of the theorem.

Proof of claim 1. Fix a parameter Q, $0 < Q < 1$, and integer parameters $s \ge 1$ and $L \ge 1$ with $s + L < t$. We use the notation introduced in the proof of Theorem 4. For any disjoint sets $\mathcal{S}, \mathcal{L} \subset [t]$, $|\mathcal{S}| = s$, $|\mathcal{L}| = L$, $\mathcal{S} \cap \mathcal{L} = \varnothing$ and any code $X = (\boldsymbol{x}(1), \boldsymbol{x}(2), \ldots, \boldsymbol{x}(t))$ of size t and length N, we call the corresponding pair $(\boldsymbol{x}(\mathcal{S}), \boldsymbol{x}(\mathcal{L}))$ an (s_L)-*bad pair* if

$$\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i) \succeq \bigvee_{j\in\mathcal{L}} \boldsymbol{x}(j).$$

For the ensemble $E(N, t, Q)$ of constant-weight codes X with weight $w \triangleq \lfloor QN\rfloor$, denote by $P_2(N, Q, s, L)$ the probability of the event "the pair $(\boldsymbol{x}(\mathcal{S}), \boldsymbol{x}(\mathcal{L}))$ is (s_L)-bad." Definition (3) of the rate $R_L(s)$ of s_L-LD codes and arguments similar to those in the beginning of the proof of Theorem 4 lead to the inequality

$$\begin{aligned} R_L(s) \ge \underline{R}_L(s) &\triangleq \frac{1}{s + L - 1}\max_{0<Q<1} A_L(s, Q), \\ A_L(s, Q) &\triangleq \varliminf_{N\to\infty} \frac{-\log_2 P_2(N, Q, s, L)}{N}. \end{aligned} \tag{106}$$

To complete the proof of claim 1 of Theorem 7, it suffices to compute the function $A_L(s,Q)$ explicitly and show that it is described by equations (40) and (41).

Using the terminology of types (see the proof of Theorem 4), the probability $P_2(N,Q,s,L)$ can be represented as

$$P_2(N,Q,s,L)=\sum_{\{n(\boldsymbol{a})\}}\frac{N!}{\prod\limits_{\boldsymbol{a}}n(\boldsymbol{a})!}\binom{N-n(\boldsymbol{0})}{\lfloor QN\rfloor}^{L}\binom{N}{\lfloor QN\rfloor}^{-s-L}, \tag{107}$$

where the summation is over all possible types $\{n(\boldsymbol{a})\}$, $\boldsymbol{a}\in\{0,1\}^s$, such that

$$\begin{gathered}0\le n(\boldsymbol{a})\le N,\qquad \sum_{\boldsymbol{a}}n(\boldsymbol{a})=N,\\ |\boldsymbol{x}(i)|=\sum_{\boldsymbol{a}\colon a_i=1}n(\boldsymbol{a})=\lfloor QN\rfloor,\quad \text{for any } i\in[s].\end{gathered} \tag{108}$$

Let $N\to\infty$ and $n(\boldsymbol{a})\triangleq N[\tau(\boldsymbol{a})+o(1)]$, where a fixed probability distribution $\tau\triangleq\{\tau(\boldsymbol{a})\}$, $\boldsymbol{a}\in\{0,1\}^s$, possesses the properties induced by conditions (108), i.e.,

$$\begin{gathered}0\le\tau(\boldsymbol{a})\le 1,\qquad \sum_{\boldsymbol{a}\in\{0,1\}^s}\tau(\boldsymbol{a})=1,\\ \sum_{\boldsymbol{a}\colon a_i=1}\tau(\boldsymbol{a})=Q,\quad \text{for any } i\in[s].\end{gathered} \tag{109}$$

Using the Stirling formula for the types corresponding to this distribution, we find the logarithmic asymptotic of the summand in (107):

$$-\log_2\left\{\frac{N!}{\prod\limits_{\boldsymbol{a}}n(\boldsymbol{a})!}\binom{N-n(\boldsymbol{0})}{\lfloor QN\rfloor}^{L}\binom{N}{\lfloor QN\rfloor}^{-s-L}\right\}=N[F(\tau,Q)+o(1)],$$

where

$$F(\tau,Q)\triangleq\sum_{\boldsymbol{a}}\tau(\boldsymbol{a})\log_2[\tau(\boldsymbol{a})]-(1-\tau(\boldsymbol{0}))Lh\biggl(\frac{Q}{1-\tau(\boldsymbol{0})}\biggr)+(s+L)h(Q). \tag{110}$$

Let the minimum of the function $F\triangleq F(\tau,Q)$ for a given Q be attained at $\tau_Q=\{\tau_Q(\boldsymbol{a})\}$. Then the main term of the logarithmic asymptotic of the sum (107) is

$$A_L(s,Q)\triangleq\varlimsup_{N\to\infty}\frac{-\log_2 P_2(N,Q,s,L)}{N}=\min_{\tau\in(109)}F(\tau,Q)=F(\tau_Q,Q). \tag{111}$$

Let us formulate the corresponding minimization problem: $F\to\min$.

$$\begin{aligned}&\text{Main function:}&&F(\tau,Q)\colon\mathbb{Y}\to\mathbb{R};\\ &\text{Constraints:}&&\begin{cases}\sum\limits_{\boldsymbol{a}\in\{0,1\}^s}\tau(\boldsymbol{a})=1,\\ \sum\limits_{\boldsymbol{a}:a_i=1}\tau(\boldsymbol{a})=Q,\quad \text{for any } i\in[s];\end{cases}\\ &\text{Search domain } \mathbb{Y}:&&0<\tau(\boldsymbol{a})<1,\quad \boldsymbol{a}\in\{0,1\}^s.\end{aligned} \tag{112}$$

We will find the minimum point τ_Q by the standard Lagrange multipliers method. Consider the Lagrangian

$$\Lambda\triangleq F(\tau,Q)+\lambda_0\biggl(\sum_{\boldsymbol{a}}\tau(\boldsymbol{a})-1\biggr)+\sum_{i=1}^{s}\lambda_i\biggl(\sum_{\boldsymbol{a}\colon a_i=1}\tau(\boldsymbol{a})-Q\biggr).$$

Then sufficient conditions for the extremal distribution are

$$\begin{cases} \dfrac{\partial\Lambda}{\partial(\tau(\boldsymbol{a}))} = \log_2[\tau(\boldsymbol{a})] + \log_2 e + \lambda_0 + \sum\limits_{i=1}^{s} a_i\lambda_i = 0, \quad \text{for } \boldsymbol{a} \neq \boldsymbol{0}, \\ \dfrac{\partial\Lambda}{\partial(\tau(\boldsymbol{0}))} = \log_2 [\tau(\boldsymbol{0})] + \log_2 e + \lambda_0 + L\log_2\Big[\dfrac{1-\tau(\boldsymbol{0})}{1-\tau(\boldsymbol{0})-Q}\Big] = 0. \end{cases} \tag{113}$$

Using the arguments given in the proof of claim 1 of Theorem 4 (see Remark 3 and below), we obtain that if a solution $\tau = \tau_Q = \{\tau_Q(\boldsymbol{a})\}$ of system (113) under constraints (112) exists in the domain $\mathbb{Y}$, then it is unique and minimizes F in $\mathbb{Y}$. Furthermore, the extremal distribution $\tau_Q = \{\tau_Q(\boldsymbol{x})\}$ satisfies the conditions

$$\begin{cases} \mu + \nu\sum\limits_{i=1}^{s} a_i + \log_2 \tau(\boldsymbol{a}) = 0, \quad \text{for } \boldsymbol{a} \neq \boldsymbol{0}, \\ \mu + \log_2 \tau(\boldsymbol{0}) + L\log_2\Big[\dfrac{1-\tau(\boldsymbol{0})}{1-\tau(\boldsymbol{0})-Q}\Big] = 0, \end{cases} \tag{114}$$

where

$$\nu \triangleq \lambda_1 = \lambda_2 = \ldots = \lambda_s, \qquad \mu \triangleq \log_2 e + \lambda_0.$$

By making the change of the parameter $y \triangleq \dfrac{1}{1+2^{-\nu}}$, $0 < y < 1$, from the first equation in (114) we obtain

$$\tau(\boldsymbol{a}) = \frac{2^{-\nu\sum a_i}}{2^{\mu}} = \frac{1}{2^{\mu}y^s}(1-y)^{\sum a_i}y^{s-\sum a_i}, \quad \text{for} \quad \boldsymbol{a} \neq \boldsymbol{0}. \tag{115}$$

The constraint on the probability distribution (115) in problem (112) leads to the equality

$$\begin{aligned} Q &= \sum_{\boldsymbol{a}:\, a_i=1} \tau_Q(\boldsymbol{a}) = \frac{1}{2^{\mu}y^s} \sum_{\boldsymbol{a}:\, a_i=1} (1-y)^{\sum a_j} y^{s-\sum a_j} \\ &= \frac{1}{2^{\mu}y^s} \sum_{k=0}^{s-1} \binom{s-1}{k} y^{s-k-1}(1-y)^{k+1} = \frac{1-y}{2^{\mu}y^s}, \quad \text{for any } i \in [s]. \end{aligned}$$

For a fixed Q, $0 < Q < 1$, this equality is a constraint equation between parameters μ and y that describe the extremal distribution $\tau_Q = \{\tau_Q(\boldsymbol{a})\}$:

$$\frac{1}{2^{\mu}y^s} = \frac{Q}{1-y} \quad \Longleftrightarrow \quad \mu = \log_2\Big[\frac{1-y}{Qy^s}\Big]. \tag{116}$$

Applying (116), to find the probability distribution (115) we compute

$$1 - \tau(\boldsymbol{0}) = \sum_{\boldsymbol{a}\neq\boldsymbol{0}} \tau(\boldsymbol{a}) = \frac{1}{2^{\mu}y^s} \sum_{k=1}^{s} \binom{s}{k} y^{s-k}(1-y)^k = \frac{Q(1-y^s)}{1-y}.$$

Thus, after eliminating the parameter μ, components of the extremal distribution (115) become functions of one and the same independent variable y, $0 < y < 1$:

$$\tau_Q(\boldsymbol{a}) = \frac{Q}{1-y} y^{[s-\sum a_i]}(1-y)^{\sum a_i}, \quad \text{for } \boldsymbol{a} \neq 0, \qquad \tau_Q(\boldsymbol{0}) = 1 - \frac{Q(1-y^s)}{1-y}. \tag{117}$$

Substituting (117) into the second equation in (114) and taking into account (116), we arrive at the equality

$$\log_2\Big[\frac{1-y-Q(1-y^s)}{Qy^s}\Big] + L\log_2\Big[\frac{1-y^s}{y-y^s}\Big] = 0, \tag{118}$$

which is equivalent to equation (41) for the parameter y, $1-Q<y<1$, from the statement of claim 1 of Theorem 7. Equation (118) has a unique solution $y=y(s,Q)$, since for the considered convex Lagrange problem there exists a unique extremal distribution (117) defined by a parameter y, $0<y<1$.

To evaluate $F(\tau_Q,Q)$ for the sought-for minimum in (111), substitute the probabilities (117) into the definition (110) of the function $F(\tau,Q)$. Then, collecting like terms in (110) with respect to s and L, we compute $F(\tau_Q,Q)$ as a function of the independent variable y, $0<y<1$. Using the notation for the Kullback distance (6), the result can be written as

$$F(\tau_Q,Q)=\log_2\biggl[\frac{Q}{1-y}\biggr]-sK(Q,1-y)-LK\biggl(Q,\frac{1-y}{1-y^s}\biggr). \tag{119}$$

Now (106), (111), (118), and (119) imply the lower bound (39)–(41) on the rate of s_L-LD codes given in claim 1 of Theorem 7. Claim 1 is proved.

Proof of claim 2. For fixed $s\ge 2$ and $L\ge 1$, let us interpret equation (41) as a function $Q=Q_L(y,s)$ of the argument y, $0<y<1$, i.e.,

$$Q=Q_L(y,s)\triangleq\frac{1-y}{1-r_L(y,s)},\qquad r_L(y,s)\triangleq y^s\biggl[1-\biggl(\frac{y-y^s}{1-y^s}\biggr)^L\biggr],\qquad 0<y<1. \tag{120}$$

Then, applying the explicit formula (6) for the Kullback distance, the definition of the random coding bound (39)–(41) can be rewritten as

$$\underline{R}_L(s)\triangleq\frac{1}{s+L-1}\max_{0<y<1}T_L(y,s), \tag{121}$$

where

$$\begin{aligned}T_L(y,s)\triangleq(1-sQ-LQ)\log_2\biggl[\frac{Q}{1-y}\biggr]-(s+L)(1-Q)\log_2\biggl[\frac{1-Q}{y}\biggr]\\ -L\log_2[1-y^s]+L(1-Q)\log_2[1-y^{s-1}]\end{aligned} \tag{122}$$

and the parameter Q on the right-hand side of (122) is given by (120).

Let $L\ge 1$ be fixed and $s\to\infty$. If in definitions (120) and (122) we put $y=1-c/s$, where the parameter $c=c_L>0$ is independent of s, then (121) means that

$$\underline{R}_L(s)\ge\frac{1}{s+L-1}T_L\Bigl(1-\frac{c}{s},s\Bigr),\quad c<s. \tag{123}$$

Computation of principal terms of the asymptotic expansions in equations (120) and (122) for $y=1-c/s$ and $s\to\infty$ leads to the asymptotic equalities

$$\begin{aligned}Q=Q_L\Bigl(1-\frac{c}{s},s\Bigr)=\frac{c}{s}(1+o(1)),\\ T_L\Bigl(1-\frac{c}{s},s\Bigr)=-\frac{L}{s}c\log_2(1-e^{-c})(1+o(1)).\end{aligned} \tag{124}$$

One can easily check that for $c=\ln 2=\dfrac{1}{\log_2 e}=0.619\ldots$,

$$\max_{c>0}\{-c\log_2(1-e^{-c})\}=\frac{1}{\log_2 e} \tag{125}$$

is attained. Therefore, equations (123)–(125) imply for the random coding bound (120)–(122) the asymptotic inequality

$$\underline{R}_L(s) \geq \frac{L}{s^2 \log_2 e}(1+o(1)), \quad s \to \infty, \quad L = 1, 2, \ldots. \tag{126}$$

Substituting $y = 1 - \ln 2/s$ into (120) and computing the corresponding value of Q leads to the asymptotic formula (44) for the fraction $Q_L(s)$ of the weight of codewords in the constant-weight code ensemble at which the asymptotic of the rate described by the right-hand side of (126) is attained.

To prove equality (42) and complete the proof of claim 2, one has to check the validity of the asymptotic equality in (126) using definitions (120)–(122). This asymptotic equality would imply that the lower bound $\underline{R}_L(s)$ on the rate of s_L-LD codes constructed in claim 1 cannot significantly be improved with the use of the constant-weight code ensemble. This checking is not presented here, since arguments to be used are cumbersome, and the result itself is not of great importance. Claim 2 is proved.

Proof of claim 3. For fixed $s \geq 2$, $L \geq 1$, and a parameter $c > 0$ independent of L, consider the equation

$$\left(\frac{y - y^s}{1 - y^s}\right)^L = c(1-y), \quad 0 < y < 1. \tag{127}$$

Since the left-hand side increases and the right-hand side decreases in y, equation (127) has precisely one root in the interval $y \in (0,1)$. Denote this root by $y_L(s,c)$. Upon substituting it into (120), introduce the values $Q = Q_L(s,c)$ and $r = r_L(s,c)$, which together with $y = y_L(s,c)$ will be interpreted as sequences of the argument $L = 1, 2, \ldots$.

Let $s \geq 2$ be fixed and $L \to \infty$. The following asymptotic properties of these sequences are obvious:

$$\begin{aligned} y = y_L(s,c) &= 1 + o(1), \\ r_L(s,c) &= 1 - (s+c)(1-y) + o(1-y), \\ Q_L(s,c) &= \frac{1}{s+c}(1+o(1)), \quad L \to \infty, \quad s = 2, 3, \ldots, \quad c > 0. \end{aligned} \tag{128}$$

Definition (120)–(122) means that for any $c > 0$ the random coding bound is of the form

$$\underline{R}_L(s) \geq \frac{1}{s+L-1} T_L(y_L(s,c), s), \quad c > 0, \tag{129}$$

where $T_L(y_L(s,c), s)$ is defined by equation (122) with $y = y_L(s,c)$ and $Q = Q_L(s,c)$. By applying definition (127) and property (128), we can compute the main term of the asymptotic on the right-hand side of (122) for $y = y_L(s,c)$ and $Q = Q_L(s,c)$ and then obtain the asymptotic equality

$$\begin{aligned} \frac{T_L(y_L(s,c), s)}{L} = \Bigg(&\log_2\Big[\frac{s+c}{s}\Big] - \frac{s+c-1}{s+c}\log_2\Big[\frac{s+c-1}{s-1}\Big] \\ &- \frac{c}{s+c}\log_2\Big[\frac{s-1}{s}\Big]\Bigg)(1+o(1)), \quad L \to \infty. \end{aligned} \tag{130}$$

Computing the derivative in c, one can easily check that the maximum of the right-hand side of (130) is attained at $c = c(s) \triangleq \frac{s^s - (s-1)^s}{(s-1)^{s-1}}$. If we now substitute this $c = c(s)$ into (130), then, using inequality (129), for the random coding bound (120)–(122) we establish the inequality

$$\underline{R}_\infty(s) \triangleq \lim_{L \to \infty} \underline{R}_L(s) \geq \log_2\left[\frac{(s-1)^{s-1}}{s^s} + 1\right], \quad s = 2, 3, \ldots. \tag{131}$$

If we substitute $c = c(s)$ into the formula for Q in (128), then we arrive at the asymptotic formula (45) for the fraction $Q_L(s)$ of the weight of codewords in the constant-weight ensemble at which the asymptotic of the rate described by the right-hand side of (131) is attained.

To prove equality (43) and complete the proof of claim 3, one has to check the validity of the equality in (131) using (120)–(122). This check is not given in the present paper for the same reason as is given in the proof of claim 2. $\triangle$

REFERENCES

1. Mitchell, C.J. and Piper, F.C., Key Storage in Secure Networks, *Discrete Appl. Math.*, 1988, vol. 21, no. 3, pp. 215–228.
2. 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.
3. 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.
4. Kautz, W.H. and Singleton, R.C., Nonrandom Binary Superimposed Codes, *IEEE Trans. Inform. Theory*, 1964, vol. 10, no. 4, pp. 363–377.
5. D'yachkov, A., Macula, A., and Rykov, V.V., New Constructions of Superimposed Codes, *IEEE Trans. Inform. Theory*, 2000, vol. 46, no. 1, pp. 284–290.
6. D'yachkov, A., Macula, A., and Rykov, V.V., New Applications and Results of Superimposed Code Theory Arising from Potentialities of Molecular Biology, *Numbers, Information, and Complexity*, 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.
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. Fano, R.M., *Transmission of Information; a Statistical Theory of Communications*, New York: M.I.T. Press, 1961. Translated under the title *Peredacha informatsii. Statisticheskaya teoriya svyazi*, Moscow: Mir, 1965.
9. 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.
10. D'yachkov, A.G., Bounds on the Average Error Probability for a Code Ensemble with Fixed Composition, *Probl. Peredachi Inf.*, 1980, vol. 16, no. 4, pp. 3–8 [*Probl. Inf. Trans.* (Engl. Transl.), 1980, vol. 16, no. 4, pp. 255–259].
11. D'yachkov, A.G., Random Constant-Composition Codes for Multiple Access Channels, *Probl. Control Inform. Theory*, 1984, vol. 13, no. 6, pp. 357–369.
12. 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.
13. 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].
14. 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.
15. Lebedev, V.S., Some Tables for (w, r) Superimposed Codes, in *Proc. 8th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-8), Tsarskoe Selo, Russia, 2002*, pp. 185–189.
16. Lebedev, V.S., Asymptotic Upper Bound for the Rate of (w, r) Cover-Free Codes, *Probl. Peredachi Inf.*, 2003, vol. 39, no. 4, pp. 3–9 [*Probl. Inf. Trans.* (Engl. Transl.), 2003, vol. 39, no. 4, pp. 317–323].

17. 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, 2000*, pp. 126–136.

18. D'yachkov, A.G., Vilenkin, P.A., Macula, A.J., and Torney, D.C., Two Models of Non-adaptive Group Testing for Designing Screening Experiments, in *Advances in Model Oriented Design and Analysis (Proc. 6th Int. Workshop on Model Oriented Design and Analysis, Puchberg/Schneeberg, Austria, 2001)*, Heidelberg: Physica, 2001, pp. 63–75.

19. D'yachkov, A.G., Rykov, V.V., Deppe, C., and Lebedev, V.S., Superimposed Codes and Threshold Group Testing, *Information Theory, Combinatorics, and Search Theory. In Memory of Rudolf Ahlswede*, Aydinian, H.K., Cicalese, F., and Deppe, C., Eds., Lect. Notes Comp. Sci., vol. 7777, Berlin: Springer, 2013, pp. 509–533.

20. Chen, H.B. and Fu, H.L., Nonadaptive Algorithms for Threshold Group Testing, *Discr. Appl. Math.*, 2009, vol. 157, no. 7, pp. 1581–1585.

21. Kim, H.K. and Lebedev, V.S., On Optimal Superimposed Codes, *J. Combin. Des.*, 2004, vol. 12, no. 2, pp. 79–91.

22. Sidelnikov, V.M. and Prikhodov, O.Yu., On the Construction of (w, r) Cover-Free Codes, *Probl. Peredachi Inf.*, 2009, vol. 45, no. 1, pp. 36–40 [*Probl. Inf. Trans.* (Engl. Transl.), 2009, vol. 45, no. 1, pp. 32–36].

23. Stinson, D.R., Wei, R., and Zhu, L., Some New Bounds for Cover-Free Families, *J. Combin. Theory, Ser. A*, 2000, vol. 90, pp. 224–234.

24. Engel, K., Interval Packing and Covering in the Boolean Lattice, *Combin. Probab. Comput.*, 1996, vol. 5, no. 4, pp. 373–384.

25. D'yachkov, A.G., Vilenkin, P.A., and Yekhanin, S.M., Upper Bounds on the Rate of Superimposed (s, ℓ)-Codes Based on Engel's Inequality, in *Proc. 8th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-8), Tsarskoe Selo, Russia, 2002*, pp. 95–99.

26. Nguyen Quang A, and Zeisel, T., Bounds on Constant Weight Binary Superimposed Codes, *Probl. Control Inform. Theory*, 1988, vol. 17, no. 4, pp. 223–230.

27. 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, 1998*, pp. 228–231.

28. D'yachkov, A.G., Rykov, V.V., and Antonov, M.A., Disjunctive Codes with List Decoding, in *Proc. 10th Sympos. on Reliability Problem in Information Systems*, Leningrad, Russia, 1989, Part 1, pp. 116–119.

29. Rashad, A.M., Random Coding Bounds on the Rate for List-Decoding Superimposed Codes, *Probl. Control Inform. Theory*, 1990, vol. 19, no. 2, pp. 141–149.

30. 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), 2003.

31. Cheng, Y.X. and Du, D.Z., New Constructions of One- and Two-Stage Pooling Designs, *J. Comput. Biol.*, 2008, vol. 15, no. 2, pp. 195–205.

32. 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.

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