ISSN 0032-9460, Problems of Information Transmission, 2016, Vol. 52, No. 2, pp. 137–150. © Pleiades Publishing, Inc., 2016.
Original Russian Text © N.A. Polyansky, 2016, published in Problemy Peredachi Informatsii, 2016, Vol. 52, No. 2, pp. 46–60.

Almost Cover-Free Codes[1]

N. A. Polyansky

Kharkevich Institute for Information Transmission Problems,
Russian Academy of Sciences, Moscow, Russia
Probability Theory Department, Faculty of Mathematics and Mechanics,
Lomonosov Moscow State University, Moscow, Russia
e-mail: nikitapolyansky@gmail.com

Received June 11, 2015; in final form, November 23, 2015

Abstract—We say that an s-subset of codewords of a code X is (s,ℓ)-*bad* if X contains ℓ other codewords such that the conjunction of these ℓ words is covered by the disjunction of the words of the s-subset. Otherwise, an s-subset of codewords of X is said to be (s,ℓ)-*bad*. A binary code X is called a *disjunctive* (s,ℓ) *cover-free* (CF) code if X does not contain (s,ℓ)-bad subsets. We consider a *probabilistic* generalization of (s,ℓ) CF codes: we say that a binary code is an (s,ℓ) almost cover-free (ACF) code if *almost all* s-subsets of its codewords are (s,ℓ)-good. The most interesting result is the proof of a lower and an upper bound for the capacity of (s,ℓ) ACF codes; the ratio of these bounds tends as $s \to \infty$ to the limit value $\log_2 e/(\ell e)$.

DOI: 10.1134/S0032946016020046

1. PROBLEM STATEMENT AND RESULTS

1.1. Background

Theory of disjunctive codes is one of important frontiers in combinatorial coding theory. Recall that a classical *disjunctive* s-code is an incidence matrix of a family of sets where no set is covered by a union of s other sets of the family. If sets of a family are subsets of $\{1, 2 \ldots, N\}$, then N is said to be the code *length*, and the cardinality of the set, denoted by t, is the *size* of the code. Disjunctive codes were introduces by Kautz and Singleton in the pioneering work [1], where a number of applied problems were described and several important constructions of such codes were given. Define the rate of s-codes to be

$$R(s,1) = \overline{\lim_{t\to\infty}} \frac{\log_2 t}{N(t,s,1)}, \tag{1}$$

where $N(t,s,1)$ is the minimum length of a disjunctive s-code of size t. The definition immediately implies [1] an information-theoretic upper bound on the rate: $R(s,1) \le 1/s$. A nontrivial upper bound on $R(s,1)$, which is the best presently known, was constructed by D'yachkov and Rykov in [2]. In the case of $s \to \infty$, the asymptotic of this bound is

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

The best presently known lower bound on $R(s,1)$ was established in [3], and its asymptotic behavior is given by

$$R(s,1) \ge \frac{1}{s^2 \log_2 e}(1+o(1)).$$

[1] The research was carried out at the Institute for Information Transmission Problems of the Russian Academy of Sciences at the expense of the Russian Science Foundation, project no. 14-50-00150.

Practically all classical problems in theory of disjunctive codes admit various generalizations. One of these is a *disjunctive* (s,ℓ) *cover-free* (CF) code. We say that an (s,ℓ) cover-free code 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 the family. This class of codes was introduced in [4] in connection with a cryptographic key distribution problem, a description of which can also be found in [5,6]. Basic constructions of (s,ℓ) CF codes from shortened Reed–Solomon codes were described in [7]. Later in [5] there was found the rate of some (s,ℓ) CF codes based on algebraic geometry codes.

Similarly to (1), we define the rate of (s,ℓ) CF codes, which will be denote by $R(s,\ell)$. In [6] there was proved a recurrence inequality for $R(s,\ell)$

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

which together with (2) leads to an asymptotic upper bound on the rate as $s \to \infty$:

$$R(s,\ell) \le \frac{(\ell+1)^{\ell+1}\log_2 s}{2e^{\ell-1}s^{\ell+1}}(1+o(1)). \tag{3}$$

Using the random coding method on the ensemble of constant-weight codes, the best presently known lower bound on $R(s,\ell)$ was established in [3]; also, its asymptotic was investigated, which in the case of $s \to \infty$ takes the form

$$R(s,\ell) \ge \frac{\ell^\ell \log_2 e}{e^\ell s^{\ell+1}}(1+o(1)). \tag{4}$$

One of further directions in theory of disjunctive codes appeared to be a probabilistic generalization of an s-code. In a recent work [8], such a generalization was described for a wider class of disjunctive codes. Let us give basic definitions. By a bad event, we mean the following: "the disjunctive sum of some s codewords covers some other codeword" (a subset of s codewords is chosen equiprobably). Then the *capacity* $C(s,1)$ is defined to be the supremum of rates of codes for which the probability of a bad event decreases exponentially with growing code length. In [8] the following bounds were proved:

$$C(s,1) \le \frac{1}{s} \quad \text{for any } s, \tag{5}$$

$$C(s,1) \ge \frac{\ln 2}{s}(1+o(1)), \quad s \to \infty. \tag{6}$$

Constructions of almost disjunctive codes based on shortened Reed–Solomon codes are given in [9]. In [10] an asymptotic bound for the rate of the corresponding codes was computed.

In the present paper we consider a probabilistic generalization for (s,ℓ) CF codes and prove an upper and a lower bound for the capacity of this generalization. Let us pass to a more formal description of the problem.

1.2. Definitions and Notation

We use terminology and notation previously used in [8]. Let N and t be natural numbers; symbol $\triangleq$ denotes equality by definition, and $|A|$ is the cardinality of a set A. For a positive integer n, define the set $[n] \triangleq \{1,2,\dots,n\}$. Introduce a binary matrix X with t columns $\boldsymbol{x}(1), \boldsymbol{x}(2), \dots, \boldsymbol{x}(t)$ (*codewords*):

$$\begin{gathered} X \triangleq \|x_i(j)\|, \quad x_i(j) = 0,1, \\ \boldsymbol{x}(j) \triangleq (x_1(j), x_2(j), \dots, x_N(j)), \quad i \in [N], \quad j \in [t]. \end{gathered} \tag{7}$$

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

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

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

Fix two natural numbers s and ℓ with $s + \ell \le t$. Define the set of all s-subsets of $[t]$

$$\mathcal{P}_s(t) \triangleq \{\mathcal{S} : \mathcal{S} \subset [t],\ |\mathcal{S}| = s\}.$$

Definition 1. Let $X = (\boldsymbol{x}(1), \boldsymbol{x}(2), \ldots, \boldsymbol{x}(t))$ be an arbitrary binary code of length N and size t. A set $\mathcal{S} \in \mathcal{P}_s(t)$ is said to be *(s,ℓ)-bad* for X if there exists a set $\mathcal{L} \subset [t] \setminus \mathcal{S}$ of cardinality $|\mathcal{L}| = \ell$ such that

$$\bigvee_{j \in \mathcal{S}} \boldsymbol{x}(j) \succeq \bigwedge_{j \in \mathcal{L}} \boldsymbol{x}(j). \tag{8}$$

Otherwise, we say that $\mathcal{S}$ is an *(s,ℓ)-good* set for X. By $\boldsymbol{B}(s,\ell,X)$ (respectively, $\boldsymbol{G}(s,\ell,X)$) we denote all (s,ℓ)-good (respectively, (s,ℓ)-bad) sets for a code X.

Definition 2. Fix a parameter ε, $0 \le \varepsilon \le 1$. A binary code X is called an *(s,ℓ) almost cover-free code with error probability ε* (an *(s,ℓ,ε) ACF code*) if

$$\frac{|\boldsymbol{B}(s,\ell,X)|}{\dbinom{t}{s}} \le \varepsilon \quad \iff \quad |\boldsymbol{G}(s,\ell,X)| \ge (1-\varepsilon)\binom{t}{s}. \tag{9}$$

Example. Consider a binary 5×5 code

$$X = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}. \tag{10}$$

Then one can easily check that the set of $(2,2)$-good sets is

$$\boldsymbol{G}(2,2,X) = \bigl\{\{1;2\}, \{1;3\}, \{1;4\}, \{1;5\}, \{2;3\}\bigr\},$$

which implies that X is a $(2, 2, \frac{1}{2})$ ACF code.

The following result immediately follows from the definitions.

Proposition 1. *Any $(s, \ell+1, \varepsilon)$ ACF code is an (s, ℓ, ε) ACF code.*

Moreover, a similar monotonicity property with respect to s is also valid, which can be stated as follows.

Proposition 2. *If X is an (s,ℓ,ε) ACF code of size t and length N, then there exists an $(s-1,\ell,\varepsilon)$ ACF code X' of size $t-1$ and length N.*

We omit the proof of this fact, since it is analogous to the proof of Proposition 3 in [8].

Using classical terminology [11, 12], we give the following definition.

Definition 3. Fix a parameter $R > 0$. In view of inequality (9), define the *error* for (s, ℓ, ε) ACF codes:

$$\varepsilon(s,\ell,R,N) \triangleq \min_{X:\, t=\lceil 2^{RN}\rceil} \left\{ \frac{|\boldsymbol{B}(s,\ell,X)|}{\binom{t}{s}} \right\}, \quad R > 0, \tag{11}$$

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

$$\boldsymbol{E}(s,\ell,R) \triangleq \varlimsup_{N\to\infty} \frac{-\log_2 \varepsilon(s,\ell,R,N)}{N}, \quad R > 0, \tag{12}$$

is called the *error exponent* for (s, ℓ) ACF codes, and the number

$$C(s,\ell) \triangleq \sup\{R:\ \boldsymbol{E}(s,\ell,R) > 0\} \tag{13}$$

is the *capacity* for (s, ℓ) ACF codes.

Definitions 1–3 and Propositions 1 and 2 imply the following.

Theorem 1 (monotonicity properties). *We have*

$$C(s+1,\ell) \le C(s,\ell) \le C(s,\ell-1). \tag{14}$$

1.3. Bounds for the Capacity $C(s,\ell)$

Let

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

and $h(a) \triangleq -a\log_2 a - (1-a)\log_2(1-a)$, $0 < a < 1$, denote, respectively, the positive part of x and the binary entropy function.

The core result of this paper is Theorems 2 and 3 (proofs are given in Section 2).

Theorem 2 (random coding bound $\underline{C}(s,\ell)$). *The following two claims hold true.*

1. *For $\ell \ge 2$, the capacity $C(s,\ell)$ for (s,ℓ) ACF codes satisfies*

$$C(s,\ell) \ge \underline{C}(s,\ell) \triangleq \frac{1}{\ell} \max_{0\le Q\le 1} \mathcal{D}(\ell,Q,\widehat{q}), \tag{15}$$

where

$$\begin{aligned}\mathcal{D}(\ell,Q,\widehat{q}) \triangleq{}& (1-Q)\ell\log_2 z - (1-\widehat{q})\log_2[1-(1-z)^\ell] \\ &+ \ell\left(\frac{1-Q}{z}(1-z) - \left(\frac{1-Q}{z} - \widehat{q}\right)(1-z)^\ell\right)\log_2[1-z] + \ell h(Q),\end{aligned} \tag{16}$$

and the parameters z and $\widehat{q}$ are defined as solutions to the following equations:

$$Q = \frac{(1-z)(1-(1-z)^\ell) - (1-\widehat{q})z(1-z)^\ell}{1-(1-z)^\ell}, \qquad \widehat{q} = 1-(1-Q)^s. \tag{17}$$

2. *For a fixed $\ell \ge 2$, there is a lower asymptotic bound for $C(s,\ell)$ as $s\to\infty$ of the form*

$$C(s,\ell) \ge \frac{\ell^{\ell-1}}{e^\ell}\frac{\log_2 e}{s^\ell}(1+o(1)). \tag{18}$$

Theorem 3 (upper bound $\overline{C}(s,\ell)$). *The following two claims hold true.*

1. *For any s and ℓ, the capacity $C(s,\ell)$ for (s,ℓ) ACF codes satisfies*

$$C(s,\ell) \le \overline{C}(s,\ell), \tag{19}$$

where $\overline{C}(s,\ell)$ is given by the initial condition

$$\overline{C}(s,1) \triangleq \frac{1}{s} \tag{20}$$

and the recurrence equation

$$\overline{C}(s,\ell) = \min_{\substack{i\in[s-1]\\ j\in[\ell-1]}} \left\{ \overline{C}(s-i,\ell-j)\frac{i^i j^j}{(i+j)^{i+j}} \right\}. \tag{21}$$

2. *For a fixed $\ell \ge 1$, there is an upper asymptotic bound for $C(s,\ell)$ as $s\to\infty$ of the form*

$$C(s,\ell) \le \frac{\ell^\ell}{e^{\ell-1}}\frac{1}{s^\ell}(1+o(1)). \tag{22}$$

Comparison of the lower bound (18) and upper bound (22) implies that the ratio of these bounds as $s\to\infty$ for any fixed $\ell \ge 2$ tends to the limit $\log_2 e/(\ell e)$. Note that for $\ell = 1$ the analogous ratio of (6) to (5) tends to the limit $\ln 2$. This is due to analytical complications when finding the maximum of the function in (15) and when choosing an optimal weight Q in the considered constant-weight ensemble. We think that the asymptotic in (18) can be improved, since the value of Q in our arguments is chosen in a nonoptimal way. For $\ell = 1$, the principal term in the asymptotic of the optimal parameter Q as $s\to\infty$ was found [8] to be equal to $\ln 2/s$.

Thus, the order of the principal term of the asymptotic of $C(s,\ell)$ is $1/s^\ell$. Recall that in the "classical" case for (s,ℓ) CF codes it was found that the order of the principal term of the asymptotic for the lower bound on $R(s,\ell)$ as $s\to\infty$ is $1/s^{\ell+1}$.

2. PROOFS OF THE THEOREMS

2.1. Proof of Theorem 2

First we prove claim 1. For an arbitrary code X, the number of (s,ℓ)-bad sets for X can be represented as

$$|\boldsymbol{B}(s,\ell,X)| \triangleq \sum_{\mathcal{S}\in\mathcal{P}_s(t)} \psi(X,\mathcal{S}), \quad \psi(X,\mathcal{S}) \triangleq \begin{cases} 1 & \text{if } \mathcal{S}\in\boldsymbol{B}(s,\ell,X),\\ 0 & \text{otherwise.}\end{cases} \tag{23}$$

Fix parameters Q, $0<Q<1$, and R, $0<R<1$. Define an ensemble $\{N,t,Q\}$ consisting of binary $N\times t$ matrices $X = (\boldsymbol{x}(1),\boldsymbol{x}(2),\ldots,\boldsymbol{x}(t))$ where columns $\boldsymbol{x}(i)$, $i\in[t]$, $t\triangleq\lfloor 2^{RN}\rfloor$, are chosen independently and equiprobably in the set of $\binom{N}{\lfloor QN\rfloor}$ columns of a fixed weight $\lfloor QN\rfloor$. Fix also two sets $\mathcal{S},\mathcal{L}\subset[t]$ with $|\mathcal{S}| = s$, $|\mathcal{L}| = \ell$, and $\mathcal{S}\cap\mathcal{L} = \varnothing$. It follows from (23) that in the ensemble $\{N,t,Q\}$ the expectation $\overline{|\boldsymbol{B}(s,\ell,X)|}$ of $|\boldsymbol{B}(s,\ell,X)|$ is

$$\overline{|\boldsymbol{B}(s,\ell,X)|} = |\mathcal{P}_s(t)| \Pr\{\mathcal{S}\in\boldsymbol{B}(s,\ell,X)\}.$$

Thus, the expectation of the error probability for (s,ℓ) ACF codes is

$$\mathcal{E}^{(N)}(s,\ell,R,Q) \triangleq |\mathcal{P}_s(t)|^{-1}\overline{|\boldsymbol{B}(s,\ell,X)|} = \Pr\{\mathcal{S}\in\boldsymbol{B}(s,\ell,X)\}, \tag{24}$$

where $t = \lfloor 2^{RN} \rfloor$. Then an obvious *random coding upper bound* on the error probability (11) for (s,ℓ) ACF codes can be given as follows:

$$\varepsilon(s,\ell,R,N) \triangleq \min_{X:t=\lfloor 2^{RN}\rfloor} \left\{ \frac{|\boldsymbol{B}(s,\ell,X)|}{|\mathcal{P}_s(t)|} \right\} \le \mathcal{E}^{(N)}(s,\ell,R,Q) \quad \text{for} \quad 0 < Q < 1. \tag{25}$$

The expectation $\mathcal{E}^{(N)}(s,\ell,R,Q)$ defined in (24) can be represented as

$$\begin{aligned}\mathcal{E}^{(N)}(s,\ell,R,Q) &= \sum_{k=\lfloor QN\rfloor}^{\min\{N,s\lfloor QN\rfloor\}} \Pr\left\{ \mathcal{S} \in \boldsymbol{B}(s,\ell,X) \Big/ \Big| \bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i) \Big| = k \right\} \mathcal{P}_2^{(N)}(s,Q,k) \\ &\le \sum_{k=\lfloor QN\rfloor}^{\min\{N,s\lfloor QN\rfloor\}} \mathcal{P}_2^{(N)}(s,Q,k) \min\left\{1, \binom{t-s}{\ell} \mathcal{P}_1^{(N)}(\ell,Q,k)\right\},\end{aligned} \tag{26}$$

where we have used the total probability formula, a standard estimate

$$\Pr\Big\{ \bigcup_i C_i \Big/ C \Big\} \le \min\Big\{1, \sum_i \Pr\{C_i/C\}\Big\},$$

and also adopted the following notation:

$$\mathcal{P}_1^{(N)}(\ell,Q,k) \triangleq \Pr\Big\{ \bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i) \succeq \bigwedge_{j\in\mathcal{L}} \boldsymbol{x}(j) \Big/ \Big| \bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i) \Big| = k \Big\}, \tag{27}$$

$$\mathcal{P}_2^{(N)}(s,Q,k) \triangleq \Pr\left\{ \Big| \bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i) \Big| = k \right\}, \quad \lfloor QN\rfloor \le k \le \min\{N, s\lfloor QN\rfloor\}. \tag{28}$$

Let $k \triangleq \lfloor qN \rfloor$. Define the functions

$$\mathcal{D}(\ell,Q,q) \triangleq \lim_{N\to\infty} \frac{-\log_2[\mathcal{P}_1^{(N)}(\ell,Q,k)]}{N}, \tag{29}$$

$$\mathcal{A}(s,Q,q) \triangleq \lim_{N\to\infty} \frac{-\log_2[\mathcal{P}_2^{(N)}(s,Q,k)]}{N} \tag{30}$$

as exponents of the logarithmic asymptotic of the probabilities of events (27) and (28) in the ensemble $\{N,t,Q\}$. Define $\widehat{q} \triangleq 1-(1-Q)^s$.

In [8], the following result was proved.

Lemma 1. *The function $\mathcal{A}(s,Q,q)$ of parameter q, $Q < q < \min\{1, sQ\}$, defined in* (30) *can be represented parametrically as*

$$\mathcal{A}(s,Q,q) \triangleq (1-q)\log_2(1-q) + q\log_2\left[\frac{Qy^s}{1-y}\right] + sQ\log_2\frac{1-y}{y} + sh(Q), \tag{31}$$

$$q = Q\frac{1-y^s}{1-y}, \quad 0 < y < 1. \tag{32}$$

Moreover, the function $\mathcal{A}(s,Q,q)$ is $\cup$-convex, monotone decreasing in the interval $(Q, 1-(1-Q)^s)$, monotone increasing in the interval $(1-(1-Q)^s, \min\{1,sQ\})$, and attains its unique minimum, equal to zero, at $q = \widehat{q} \triangleq 1-(1-Q)^s$, i.e.,

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

In the Appendix we prove the following fact.

Lemma 2. *For $\ell \geq 2$ the value at $q = \widehat{q}$ of the function $\mathcal{D}(\ell, Q, q)$ defined in* (29) *is*

$$\mathcal{D}(\ell, Q, \widehat{q}) = (1-Q)\ell \log_2 z - (1-\widehat{q})\log_2\bigl[1-(1-z)^\ell\bigr] \\ + \ell\left(\frac{1-Q}{z}(1-z) - \left(\frac{1-Q}{z} - \widehat{q}\right)(1-z)^\ell\right)\log_2[1-z] + \ell h(Q),$$

where z is uniquely determined from the following equation:

$$Q = \frac{(1-z)(1-(1-z)^\ell) - (1-\widehat{q})z(1-z)^\ell}{1-(1-z)^\ell}.$$

Inequality (26) and the random coding bound (25) yield an estimate for the error exponent (12):

$$\boldsymbol{E}(s,\ell,R) \geq \underline{\boldsymbol{E}}(s,\ell,R) \triangleq \max_{0\leq Q\leq 1} E(s,\ell,R,Q), \tag{33}$$

$$E(s,\ell,R,Q) \triangleq \min_{Q<q<\min\{1,sQ\}} \left\{\mathcal{A}(s,Q,q) + [\mathcal{D}(\ell,Q,q) - \ell R]^+\right\}. \tag{34}$$

Lemma 1 implies that $\mathcal{A}(s,Q,q) > 0$ for $q \neq \widehat{q}$. In particular, the condition $q \neq \widehat{q}$ implies $E(s,\ell,R,Q) > 0$. Hence we conclude that for $\ell R < \mathcal{D}(\ell,Q,\widehat{q})$ we have $E(s,\ell,R,Q) > 0$, which in turn means (see (13) (33)) that

$$C(s,\ell) \geq \underline{C}(s,\ell) \triangleq \frac{1}{\ell}\max_{0\leq Q\leq 1} \mathcal{D}(\ell,Q,\widehat{q}), \quad \text{where} \quad \widehat{q} = 1-(1-Q)^s.$$

Thus, we have proved the lower bound (15).

Now let us prove claim 2. Let $\ell \geq 2$ be fixed, and let $s \to \infty$. By substituting $z = s/(s+\ell)$ into (15)–(17), we obtain

$$Q = \frac{(1-z)(1-(1-z)^\ell) - (1-\widehat{q})z(1-z)^\ell}{1-(1-z)^\ell} = \frac{\ell}{s+\ell} - \frac{\ell^\ell e^{-\ell}}{s^\ell} + O\Bigl(\frac{1}{s^{\ell+1}}\Bigr),$$
$$\widehat{q} = 1-(1-Q)^s = 1 - e^{-\frac{s\ell}{s+\ell} + O(\frac{1}{s})} = 1 - e^{-\ell} + O\Bigl(\frac{1}{s}\Bigr)$$

and

$$C(s,\ell) \geq \frac{1}{\ell}\max_{0\leq Q\leq 1}\mathcal{D}(\ell,Q,\widehat{q}) = \frac{1}{\ell}\max_{0\leq z\leq 1}\mathcal{D}(\ell,Q(z),\widehat{q}(z)) \geq \frac{1}{\ell}\mathcal{D}(\ell,Q(s/(s+\ell)),\widehat{q}(s/(s+\ell))),$$

where

$$\mathcal{D}(\ell, Q, \widehat{q}) \triangleq (1-Q)\ell \log_2 z - (1-\widehat{q})\log_2\bigl[1-(1-z)^\ell\bigr] \\ + \ell\left(\frac{1-Q}{z}(1-z) - \left(\frac{1-Q}{z} - \widehat{q}\right)(1-z)^\ell\right)\log_2[1-z] + \ell h(Q).$$

Then

$$\begin{aligned} C(s,\ell) \geq{}& \left(\frac{s}{s+\ell} + \frac{\ell^\ell e^{-\ell}}{s^\ell} + O\Bigl(\frac{1}{s^{\ell+1}}\Bigr)\right)\log_2\left[\frac{s}{s+\ell}\right] - \left(\frac{e^{-\ell}}{\ell} + O\Bigl(\frac{1}{s}\Bigr)\right)\log_2\left[1-\left(\frac{\ell}{s+\ell}\right)^\ell\right] \\ &+ \left(1 + O\Bigl(\frac{1}{s^\ell}\Bigr)\right)\frac{\ell}{s+\ell}\log_2\left[\frac{\ell}{s+\ell}\right] - \left(e^{-\ell} + O\Bigl(\frac{1}{s}\Bigr)\right)\left(\frac{\ell}{s+\ell}\right)^\ell\log_2\left[\frac{\ell}{s+\ell}\right] \\ &- \left(\frac{\ell}{s+\ell} - \frac{\ell^\ell e^{-\ell}}{s^\ell} + O\Bigl(\frac{1}{s^{\ell+1}}\Bigr)\right)\log_2\left[\frac{\ell}{s+\ell} - \frac{\ell^\ell e^{-\ell}}{s^\ell} + O\Bigl(\frac{1}{s^{\ell+1}}\Bigr)\right] \\ &- \left(\frac{s}{s+\ell} + \frac{\ell^\ell e^{-\ell}}{s^\ell} + O\Bigl(\frac{1}{s^{\ell+1}}\Bigr)\right)\log_2\left[\frac{s}{s+\ell} + \frac{\ell^\ell e^{-\ell}}{s^\ell} + O\Bigl(\frac{1}{s^{\ell+1}}\Bigr)\right] \\ ={}& \frac{\ell^{\ell-1}\log_2 e}{e^\ell s^\ell} + O\Bigl(\frac{\log_2 s}{s^{\ell+1}}\Bigr), \end{aligned}$$

which completes the proof of claim 2. △

2.2. Proof of Theorem 3

We start with the proof of claim 1. Recall the notation

$$\mathcal{P}_s(t) \triangleq \{\mathcal{S} : \mathcal{S} \subset [t],\ |\mathcal{S}| = s\}.$$

Let X be an arbitrary binary code of size t and length N, and let $\mathcal{U}$ and $\mathcal{V}$ be two disjoint subsets of $[t]$ of cardinalities u and v, respectively. We denote by $D_{u,v}(\mathcal{U}, \mathcal{V}, X)$ the set of rows of X for which the condition

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

is fulfilled. Define the average cardinality of $D_{u,v}(\mathcal{U}, \mathcal{V}, X)$ over all choices of an ordered pair of sets $\mathcal{U}$ and $\mathcal{V}$

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

and the maximum average cardinality

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

over all codes X of a fixed size t and length N.

Lemma 3. *We have an asymptotic inequality*

$$\varlimsup_{t\to\infty} \frac{\overline{D}_{u,v}(t, N(t))}{N(t)} \le \max_{0\le z\le 1}\{z^u(1-z)^v\} = \frac{u^u v^v}{(u+v)^{u+v}}, \tag{35}$$

where $N(t)$ is an arbitrary integer-valued function.

We omit the proof of this lemma, since it is carried out similarly to that of Lemma 1 in [13]. Define the function

$$b(u, v, N) \triangleq \frac{u^u v^v}{(u+v)^{u+v}} N.$$

For each $\widehat{\varepsilon} > 0$ define $t(\widehat{\varepsilon})$ such that for any $t \ge t(\widehat{\varepsilon})$ we have

$$\overline{D}_{u,v}(t, N) \le b(u, v, N)(1 + \widehat{\varepsilon}). \tag{36}$$

A set $\mathcal{U} \subset [t]$, $|\mathcal{U}| = u$, will be called *δ-good* for a code X of size $t > t(\widehat{\varepsilon})$ if there exists a set $\mathcal{V}$ such that

$$|D_{u,v}(\mathcal{U}, \mathcal{V}, X)| \le (1 + \delta) b(u, v, N).$$

By $J_u(X, \delta) \subseteq \mathcal{P}_u(t)$ we denote the set of all δ-good sets in X. Then we obviously have the following inequality:

$$|J_u(X, \delta)| \ge \left(1 - \frac{1 + \widehat{\varepsilon}}{1 + \delta}\right)\binom{t}{u}. \tag{37}$$

For any fixed ε, $0 < \varepsilon < 1$, consider an arbitrary (s, ℓ, ε) ACF code X of size $t > t(\widehat{\varepsilon})$ and length N. Introduce the notation

$$B(\mathcal{U}, X) \triangleq \{\mathcal{S} : \mathcal{S} \in \mathcal{P}_s(t) \text{ with } \mathcal{S} \in \boldsymbol{B}(s, \ell, X) \text{ and } \mathcal{U} \subset \mathcal{S}\}.$$

Clearly, for the average cardinality of such sets we have

$$\overline{B}_u(X) \triangleq \sum_{\mathcal{U}\in\mathcal{P}_u(t)} \frac{|B(\mathcal{U},X)|}{\dbinom{t}{u}} \le \frac{\dbinom{\varepsilon}{s}u\dbinom{t}{s}}{\dbinom{t}{u}} \triangleq d(t,s,u,\varepsilon). \tag{38}$$

For an arbitrary fixed $c > 0$, define the following set:

$$G_u(X,c) \triangleq \{\mathcal{U} : \mathcal{U} \in \mathcal{P}_u(t) \text{ with } |B(\mathcal{U},X)| \le cd(t,s,u,\varepsilon)\} \subset \mathcal{P}_u(t).$$

It is easily seen that the cardinality of this set satisfies

$$|G_u(X,c)| \ge \left(1 - \frac{1}{c}\right)\binom{t}{u}. \tag{39}$$

Let a number T be such that for $t > T$ we have

$$\frac{\dbinom{s}{u}\dbinom{t}{s}}{\dbinom{t}{u}\dbinom{t-(u+v)}{s-u}} < 2.$$

Inequalities (37) and (39) imply that

$$|J_u(X,\delta) \cap G_u(X,c)| \ge \left(1 - \frac{1}{c} - \frac{1+\widehat{\varepsilon}}{1+\delta}\right)\binom{t}{u}.$$

Clearly, for any $\delta > 0$ there exist $c(\delta)$ and $\widehat{\varepsilon}(\delta)$ such that

$$1 - \frac{1}{c} - \frac{1+\widehat{\varepsilon}}{1+\delta} > 0 \quad \text{for any } c > c(\delta) \text{ and } \widehat{\varepsilon} \le \widehat{\varepsilon}(\delta). \tag{40}$$

Taking into account (36) and (40), define $t(\delta) \triangleq t(\widehat{\varepsilon}(\delta))$.

Define the minimum length of an (s,ℓ,ε) ACF code of size t and denote it by $N_\varepsilon(s,\ell,t)$.

Lemma 4. *For any fixed $\delta > 0$ and $t > \max\{t(\delta),T\}$, the length of an (s,ℓ,ε) ACF code satisfies the inequality*

$$N_{\varepsilon'}(s-u,\ell-v,t-u-v) \le (1+\delta)N_\varepsilon(s,\ell,t)\frac{u^u v^v}{(u+v)^{u+v}}, \tag{41}$$

where $\varepsilon' < C(\delta)\varepsilon$.

Define

$$C'(s,\ell) \triangleq \varlimsup_{\varepsilon\to 0}\varlimsup_{t\to\infty} \frac{\log_2 t}{N_\varepsilon(t,s,\ell)}. \tag{42}$$

Lemma 4 implies in particular that $\varepsilon' \to 0$ as $\varepsilon \to 0$ with a fixed $\delta > 0$. It is easily seen that

$$C'(s,\ell)(1+\delta) \le C'(s-u,\ell-v)\frac{u^u v^v}{(u+v)^{u+v}}.$$

Since this inequality holds for an arbitrary value of $\delta > 0$, equation (21) is proved. The condition $C'(s,1) \le 1/s$ can be proved similarly to Theorem 2 in [8]. The inequality $C'(s,\ell) \ge C(s,\ell)$ is obvious, since the condition of exponential decay of the error probability with growing length is stronger than the condition used in the definition (42) of $C'(s,\ell)$. Thus, claim 1 is proved.

Now we prove claim 2. Let $s \ge \ell \ge 2$. We will assume that the parameter p, $0 < p < 1$, is chosen so that sp is a natural number. Into the right-hand side of (21) we substitute $j \triangleq \ell - 1$ and $i \triangleq ps$. Then for inequality (19) we obtain

$$C(s,\ell) \le \overline{C}(s(1-p),1)\frac{(ps)^{ps}(\ell-1)^{\ell-1}}{(ps+\ell-1)^{ps+\ell-1}}.$$

Let $s \to \infty$ with a fixed $\ell \ge 2$. Using the initial condition (20) for $\overline{C}(s(1-p),1) = 1/(s(1-p))$, we obtain

$$\begin{aligned} C(s,\ell) &\le \inf_{0<p<1}\left\{\frac{(ps)^{ps}(\ell-1)^{\ell-1}}{(ps+\ell-1)^{ps+\ell-1}}\frac{1}{s(1-p)}\right\} \\ &= \frac{(\ell-1)^{\ell-1}}{e^{\ell-1}s^{\ell}} \min_{0<p<1}\left\{\frac{1}{p^{\ell-1}(1-p)}\right\}(1+o(1))\frac{\ell^{\ell}}{e^{\ell-1}s^{\ell}}(1+o(1)), \end{aligned}$$

where we have used the fact that

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

and that this maximum is attained at $p = \dfrac{\ell-1}{\ell}$. △

APPENDIX

Proof of Lemma 2. Let us compute the conditional probability

$$\mathcal{P}_1^{(N)}(\ell,Q,k) \triangleq \Pr\left\{\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i) \succeq \bigwedge_{j\in\mathcal{L}} \boldsymbol{x}(j) \Bigg/ \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k\right\}.$$

Fix q, $Q \le q \le \min\{1, sQ\}$, and define $k \triangleq \lfloor qN \rfloor$, $\lfloor QN \rfloor \le k \le s\lfloor QN \rfloor$. Using the method of *types* (see [3, 12])

$$\{n(\boldsymbol{a})\}, \quad \boldsymbol{a} \triangleq (a_1, a_2, \ldots, a_s) \in \{0,1\}^s, \quad 0 \le n(\boldsymbol{a}) \le N, \quad \sum_{\boldsymbol{a}} n(\boldsymbol{a}) = N, \tag{43}$$

we represent the probability $\mathcal{P}_1^{(N)}(\ell,Q,k)$ in the ensemble $\{N,t,Q\}$ as a sum

$$\mathcal{P}_1^{(N)}(\ell,Q,k) = \sum_{(45)} \frac{N!}{\prod\limits_{\boldsymbol{a}\in\{0,1\}^{\ell}} n(\boldsymbol{a})!} \frac{\dbinom{k}{n(\mathbf{1})}}{\dbinom{N}{n(\mathbf{1})}} \binom{N}{\lfloor QN \rfloor}^{-\ell}, \tag{44}$$

where the sum on the right-hand side of (44) is over all types $\{n(\boldsymbol{a})\}$ such that

$$\sum_{\boldsymbol{a}\colon a_i=1} n(\boldsymbol{a}) = \lfloor QN \rfloor, \quad \text{for all } i \in [\ell]. \tag{45}$$

Applying the Stirling formula, we obtain the following logarithmic asymptotic of the summand in (44):

$$\log_2\left[\frac{N!}{\prod\limits_{\boldsymbol{a}\in\{0,1\}^{\ell}} n(\boldsymbol{a})!} \frac{\dbinom{k}{n(\mathbf{1})}}{\dbinom{N}{n(\mathbf{1})}} \binom{N}{\lfloor QN \rfloor}^{-\ell}\right] = 2^{-NF(\tau,Q,q)(1+o(1))},$$

where

$$F(\tau,Q,q)\triangleq\sum_{\boldsymbol{a}\in\{0,1\}^{\ell}}\tau(\boldsymbol{a})\log_2\tau(\boldsymbol{a})-qh\Bigl(\frac{\tau(\mathbf{1})}{q}\Bigr)+h(\tau(\mathbf{1}))+\ell h(Q). \tag{46}$$

Here the *probability distribution* $\{\tau(\boldsymbol{a})\}$, $a\in\{0,1\}^{\ell}$, is defined as follows:

$$\tau(\boldsymbol{a})\triangleq\frac{n(\boldsymbol{a})}{N},\quad \text{for all } \boldsymbol{a}\in\{0,1\}^{\ell}.$$

Thus, to evaluate

$$\mathcal{D}(\ell,Q,q)\triangleq\lim_{N\to\infty}-\frac{\log_2 P_1^{(N)}(\ell,Q,k)}{N},$$

we have to solve the minimization problem

$$\mathcal{D}(\ell,Q,q)=\min_{\tau\in(48):\,(49)}F(\tau,Q,q)\triangleq F(\widehat{\tau},Q,q), \tag{47}$$

$$\Bigl\{\tau:\ 0<\tau(\boldsymbol{a})<1\ \ \forall\boldsymbol{a}=(a_1,\ldots,a_\ell)\in\{0,1\}^{\ell}\Bigr\}, \tag{48}$$

$$\sum_{\boldsymbol{a}}\tau(\boldsymbol{a})=1,\qquad \sum_{\boldsymbol{a}:\,a_i=1}\tau(\boldsymbol{a})=Q\quad\text{for all } i\in[\ell], \tag{49}$$

where the constraints (49) are obtained in a natural way from (43) and (45).

To find the minimum and the extremal probability distribution $\{\widehat{\tau}(\boldsymbol{a})\}$, we use the Lagrange multipliers method. Consider the Lagrangian

$$\begin{aligned}\Lambda\triangleq\sum_{\boldsymbol{a}\in\{0,1\}^{\ell}}\tau(\boldsymbol{a})\log_2\tau(\boldsymbol{a})-qh\Bigl(\frac{\tau(\mathbf{1})}{q}\Bigr)+h(\tau(\mathbf{1}))+\ell h(Q)&\\ +\mu_0\Bigl(\sum_{\boldsymbol{a}}\tau(\boldsymbol{a})-1\Bigr)+\sum_{i=1}^{\ell}\mu_i\Bigl(\sum_{\boldsymbol{a}:\,a_i=1}\tau(\boldsymbol{a})-Q\Bigr).&\end{aligned} \tag{50}$$

Now consider necessary conditions for the extremal distribution $\{\widehat{\tau}(\boldsymbol{a})\}$:

$$\begin{cases}\dfrac{\partial\Lambda}{\partial\tau(\boldsymbol{a})}=\log_2\widehat{\tau}(\boldsymbol{a})+\log_2 e+\mu_0+\displaystyle\sum_{i:\,a_i=1}\mu_i=0\quad\text{for }\boldsymbol{a}\neq\mathbf{1},\\ \dfrac{\partial\Lambda}{\partial\tau(\mathbf{1})}=\log_2\widehat{\tau}(\mathbf{1})+\log_2 e+\displaystyle\sum_{i=0}^{\ell}\mu_i+\log_2\Bigl[\frac{1-\widehat{\tau}(\mathbf{1})}{q-\widehat{\tau}(\mathbf{1})}\Bigr]=0.\end{cases} \tag{51}$$

One can easily check that the matrix of second derivatives of the Lagrangian is diagonal and positive definite in the region (48) and that the function $F(\tau,Q,q)$ defined in (46) is strictly $\cup$-convex in the region (46). The Karush–Kuhn–Tucker theorem states that any solution $\{\widehat{\tau}(\boldsymbol{a})\}$ satisfying system (51) and constraints (49) yields a local minimum for $F(\tau,Q,q)$. Thus, if there exists a solution to the system (51) and (49) belonging to the region (48), then it is unique and yields the minimum in the minimization problem (47)–(49).

Note also that symmetry of the problem implies the equalities $\mu\triangleq\mu_1=\mu_2=\ldots=\mu_\ell$. Let $\widehat{\mu}\triangleq\log_2 e+\mu_0$. Then we can rewrite (51) as follows:

$$\begin{cases}\widehat{\mu}+\mu\displaystyle\sum_{i=1}^{\ell}a_i+\log_2[\widehat{\tau}(\boldsymbol{a})]=0\quad\text{for }\boldsymbol{a}\neq\mathbf{1},\\ \widehat{\mu}+\mu\ell+\log_2[\widehat{\tau}(\mathbf{1})]+\log_2\Bigl[\dfrac{1-\widehat{\tau}(\mathbf{1})}{q-\widehat{\tau}(\mathbf{1})}\Bigr]=0.\end{cases} \tag{52}$$

The first equation in (52) implies

$$\widehat{\tau}(\boldsymbol{a}) = \frac{2^{-\widehat{\mu}}}{z^{\ell}} \prod P(a_i) \quad \text{for} \quad \boldsymbol{a} \neq \mathbf{1},$$

where we have used the following distribution:

$$P(a) \triangleq \begin{cases} z \triangleq \dfrac{1}{1+2^{-\mu}} & \text{for } a=0, \\ 1-z \triangleq \dfrac{2^{-\mu}}{1+2^{-\mu}} & \text{for } a=1. \end{cases}$$

In particular, this implies

$$\mu = \log_2\left[\frac{z}{1-z}\right]. \tag{53}$$

Since (see (49)) the total sum of probabilities is 1, we have

$$\widehat{\tau}(\mathbf{1}) = 1 - \sum_{k=0}^{\ell-1} \binom{\ell}{k} \frac{2^{-\widehat{\mu}}}{z^{\ell}} z^{\ell-k}(1-z)^k = 1 - \frac{2^{-\widehat{\mu}}}{z^{\ell}}\bigl(1-(1-z)^{\ell}\bigr). \tag{54}$$

From the second condition in (49) we obtain

$$Q = \frac{2^{-\widehat{\mu}}}{z^{\ell}} \sum_{k=0}^{\ell-2} \binom{\ell-1}{k} z^{\ell-k-1}(1-z)^{k+1} + 1 - \frac{2^{-\widehat{\mu}}}{z^{\ell}}\bigl(1-(1-z)^{\ell}\bigr) = 1 - \frac{2^{-\widehat{\mu}}}{z^{\ell-1}}.$$

Thus, there is a constraint equation for the parameters $\widehat{\mu}$, Q, and z:

$$\widehat{\mu} = -\log_2\bigl[(1-Q)z^{\ell-1}\bigr]. \tag{55}$$

Finally, by substituting (53)–(55) into the second equation in (52), we find

$$-\log_2\bigl[(1-Q)z^{\ell-1}\bigr] + \ell\log_2\left[\frac{z}{1-z}\right] + \log_2\left[1 - \frac{1-Q}{z}\bigl(1-(1-z)^{\ell}\bigr)\right] \\ + \log_2\left[\frac{1-Q}{z}\bigl(1-(1-z)^{\ell}\bigr)\right] - \log_2\left[q + \frac{1-Q}{z}\bigl(1-(1-z)^{\ell}\bigr) - 1\right] = 0.$$

Equivalently,

$$\log_2\left[\frac{\bigl(1-(1-z)^{\ell}\bigr)}{(1-z)^{\ell}}\right] + \log_2\left[\frac{z-(1-Q)\bigl(1-(1-z)^{\ell}\bigr)}{(q-1)z+(1-Q)\bigl(1-(1-z)^{\ell}\bigr)}\right] = 0.$$

From this we explicitly find an expression for Q through the parameters z, q, s, and ℓ:

$$Q = \frac{(1-z)\bigl(1-(1-z)^{\ell}\bigr) - (1-q)z(1-z)^{\ell}}{1-(1-z)^{\ell}}. \tag{56}$$

Note that for fixed values of q, s, and ℓ there is a bijection between $Q \in [0,1]$ and $z \in [0,1]$. It follows from (55) and (56) that

$$\frac{2^{-\widehat{\mu}}}{z^{\ell}} = \frac{1-Q}{z} = \frac{1-q(1-z)^{\ell}}{1-(1-z)^{\ell}}. \tag{57}$$

Substitute $q = \widehat{q} = 1 - (1 - Q)^s$ into (57). Then

$$\widehat{\tau}(\mathbf{1}) = \widehat{q}(1 - z)^{\ell}. \tag{58}$$

Recall (47) that

$$F(\widehat{\tau}, Q, \widehat{q}) = \sum_{\boldsymbol{a} \in \{0,1\}^{\ell}} \widehat{\tau}(\boldsymbol{a}) \log_2 \widehat{\tau}(\boldsymbol{a}) - \widehat{q} h\Bigl(\frac{\widehat{\tau}(\mathbf{1})}{\widehat{q}}\Bigr) + h(\widehat{\tau}(\mathbf{1})) + \ell h(Q). \tag{59}$$

Now, using (57), we rewrite the first sum in (59):

$$\begin{aligned}
\sum_{\boldsymbol{a} \in \{0,1\}^{\ell}} \widehat{\tau}(\boldsymbol{a}) \log_2 \widehat{\tau}(\boldsymbol{a}) &= \sum_{i=0}^{\ell-1} \binom{\ell}{i} \frac{2^{-\widehat{\mu}}}{z^{\ell}} (1-z)^i z^{\ell-i} \log_2 \Bigl[\frac{2^{-\widehat{\mu}}}{z^{\ell}} (1-z)^i z^{\ell-i}\Bigr] + \widehat{\tau}(\mathbf{1}) \log_2 \widehat{\tau}(\mathbf{1}) \\
&= \sum_{i=0}^{\ell-1} \binom{\ell}{i} \frac{2^{-\widehat{\mu}}}{z^{\ell}} (1-z)^i z^{\ell-i} \log_2 \Bigl[\frac{2^{-\widehat{\mu}}}{z^{\ell}}\Bigr] + \sum_{i=0}^{\ell-1} \binom{\ell}{i} \frac{2^{-\widehat{\mu}}}{z^{\ell}} (1-z)^i z^{\ell-i} \log_2 \bigl[z^{\ell-i}\bigr] \\
&\quad + \sum_{i=0}^{\ell-1} \binom{\ell}{i} \frac{2^{-\widehat{\mu}}}{z^{\ell}} (1-z)^i z^{\ell-i} \log_2 \bigl[(1-z)^i\bigr] + \widehat{\tau}(\mathbf{1}) \log_2 \widehat{\tau}(\mathbf{1}) \\
&= \Bigl(1 - \widehat{q}(1-z)^{\ell}\Bigr) \log_2 \Bigl[\frac{1 - \widehat{q}(1-z)^{\ell}}{1 - (1-z)^{\ell}}\Bigr] + (1-Q)\ell \log_2 z \\
&\quad + \frac{1-Q}{z} \ell \Bigl((1-z) - (1-z)^{\ell}\Bigr) \log_2 [1-z] + \widehat{\tau}(\mathbf{1}) \log_2 \widehat{\tau}(\mathbf{1}).
\end{aligned}$$

Taking into account (58), the second term in (59) can be represented as

$$\begin{aligned}
-\widehat{q} h\Bigl(\frac{\widehat{\tau}(\mathbf{1})}{\widehat{q}}\Bigr) &= \tau(\mathbf{1}) \log_2 \Bigl[\frac{\widehat{\tau}(\mathbf{1})}{q}\Bigr] + (q - \widehat{\tau}(\mathbf{1})) \log_2 \Bigl[\frac{q - \widehat{\tau}(\mathbf{1})}{q}\Bigr] \\
&= \ell \widehat{q}(1-z)^{\ell} \log_2 [1-z] + \widehat{q}\bigl(1 - (1-z)^{\ell}\bigr) \log_2 \bigl[1 - (1-z)^{\ell}\bigr].
\end{aligned}$$

The third term in (59) is

$$h(\widehat{\tau}(\mathbf{1})) = -\widehat{\tau}(\mathbf{1}) \log_2 \widehat{\tau}(\mathbf{1}) - (1 - \widehat{\tau}(\mathbf{1})) \log_2 [1 - \widehat{\tau}(\mathbf{1})].$$

Finally, the last term in (59) equals $\ell h(Q)$. Thus, the quantity $\mathcal{D}(\ell, Q, \widehat{q}) = F(\widehat{\tau}, Q, \widehat{q})$ can be represented as

$$\begin{aligned}
\mathcal{D}(\ell, Q, \widehat{q}) = (1-Q)\ell \log_2 z + \ell \left(\frac{1-Q}{z}(1-z) - \left(\frac{1-Q}{z} - \widehat{q}\right)(1-z)^{\ell}\right) \log_2 [1-z] \\
- (1 - \widehat{q}) \log_2 \bigl[1 - (1-z)^{\ell}\bigr] + \ell h(Q),
\end{aligned}$$

which completes the proof of Lemma 2. △

Proof of Lemma 4. Choose $c > c(\delta)$ and assume that an (s, ℓ, ε) ACF code X is of size $t > \max\{t(\delta), T\}$ and of length N. Choose and fix an arbitrary set $\mathcal{U} \in \{J_u(X, \delta) \cap G_u(X, c)\}$. Since $\mathcal{U}$ is δ-good, we can find a set $\mathcal{V}$ corresponding to it, i.e.,

$$|D_{u,v}(\mathcal{U}, \mathcal{V}, X)| \le (1 + \delta) b(u, v, N).$$

Define a code X' of size $t' = t - (u + v)$ and length $N' = |D_{u,v}(\mathcal{U}, \mathcal{V}, X)|$ as a subcode of X consisting of rows $D_{u,v}(\mathcal{U}, \mathcal{V}, X)$ and columns with indices $[t] \setminus \{\mathcal{U} \cup \mathcal{V}\}$. Let us show that X' is an $(s - u, \ell - v, \varepsilon')$ ACF code with ε' satisfying the inequality

$$\varepsilon' \le \frac{d(t, s, u, \varepsilon) c}{\dbinom{t - (u + v)}{s - u}} = 2c\varepsilon. \tag{60}$$

Indeed, since $\mathcal{U} \in G_u(X, c)$, we have $|B(\mathcal{U}, X)| \le cd(t, s, u, \varepsilon)$. This means that the number of $(s-u, \ell-v)$-bad sets for X' is not greater than $cd(t, s, u, \varepsilon)$. Then, since the total number of subsets of cardinality $s-u$ of the set $[t-(u+v)]$ is $\binom{t-(u+v)}{s-u}$, inequality (60) does hold. Note that the length of X' satisfies the relation

$$N' = |D_{u,v}(\mathcal{U}, \mathcal{V}, X)| \le (1+\delta)N \frac{u^u v^v}{(u+v)^{u+v}}.$$

This, in particular, implies (41). △

REFERENCES

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

2. 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].

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

4. Mitchell, C.J. and Piper, F.C., Key Storage in Secure Networks, *Discrete Appl. Math.*, 1988, vol. 21, no. 3, pp. 215–228.

5. 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].

6. 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].

7. 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.

8. D'yachkov, A.G., Vorobyev, I.V., Polyanskii, N.A., and Shchukin, V.Yu., Almost Disjunctive List-Decoding Codes, *Probl. Peredachi Inf.*, 2015, vol. 51, no. 2, pp. 27–49 [*Probl. Inf. Trans.* (Engl. Transl.), 2015, vol. 51, no. 2, pp. 110–131].

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

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

11. Gallager, R.G., *Information Theory and Reliable Communication*, New York: Wiley, 1968.

12. 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.

13. D'yachkov, A.G., Vorobyev, I.V., Polyanskii, N.A., and Shchukin, V.Yu., Cover-Free Codes and Separating System Codes, in *Proc. 2015 IEEE Int. Sympos. on Information Theory (ISIT'2015), Hong Kong, China, June 14–19, 2015*, pp. 2894–2898.