Hypothesis Test for Upper Bound on the Size of Random Defective Set

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

***Abstract*—The conventional model of disjunctive group testing assumes that there are several defective elements (or defectives) among the total number t items, and a group test yields the positive response if and only if the testing group contains at least one defective element. The basic problem is to find all defectives using a minimal possible number of group tests. However, when the number of defectives is unknown there arises an additional problem, namely: how to estimate the random number of defective elements. In this paper, we concentrate on testing of hypothesis H_0: the number of defectives $\le s$, for a fixed constant s. For the nonadaptive group testing, we introduce a new decoding algorithm based on the simple comparison of the number of tests having positive responses with a fixed threshold. For the given threshold decoding algorithm which does not depend on t, we apply the random coding arguments to the ensemble of constant-weight binary codes and prove that $4s^2\ln\frac{1}{\varepsilon}$ nonadaptive group tests are sufficient to accept or reject H_0 with error probability $\le \varepsilon$ provided that $s\to\infty$ and $\varepsilon\to 0$. Our simulation results verify the advantages of the proposed algorithm over known algorithms. If the total number t of items is sufficiently large, then with the help of nontrivial combinatorial arguments we establish the necessity of $\frac{s}{\ln 2}\ln\frac{1}{\varepsilon}$ nonadaptive group tests for any decoding algorithm with error probability $\le \varepsilon$.**

I. Introduction

The idea of *group testing* was introduced by R. Dorfman [2]. It was proposed to save on blood tests for infection by grouping individuals and testing the mixture. The group testing scheme suggested by R. Dorfman is constructed in such way that the successive groups depend on the results of the previous tests. Such schemes are called *adaptive*. There are *nonadaptive* schemes also. A nonadaptive scheme is a series of N a priori group tests that can be carried out simultaneously. This is the essential advantage for the most important applications [3], [4]. In this paper we focus on nonadaptive group testing schemes.

Let t be the total number of elements and $\mathscr{S}$ $\left(\mathscr{S}\subseteq[t],\,[t]\triangleq\{1,2,\ldots,t\}\right)$ is an unknown subset of defectives. We will use these notations throughout the paper. The conventional group testing problem assumes that the number of defectives $|\mathscr{S}|$ is upper bounded by a known fixed constant s, i.e., $|\mathscr{S}|\le s$, where s does not depend on t. In this regime the main attention is given to disjunctive s-codes [5], [6] which will be defined in the next section. However, a more common assumption is that the defectives are rare, with $|\mathscr{S}|=o(t)$ as $t\to\infty$. So, the regime $|\mathscr{S}|=\Theta(t^{\alpha})$, $0<\alpha<1$, is studied in the recent works [7], [8], [9].

The other authors consider the settings for which the number of defectives is unknown. Originally it was proposed in Dorfman's paper [2] that each element is defective with probability p, $0<p<1$. Exactly the same model is discussed in the recent papers [10], [11], [12], where the authors focus on nonadaptive schemes and study algorithms for which the error probability of finding defectives is $o(1)$ as $t\to\infty$. A more general model in which $p=p(t)$ depends on t is considered in paper [13]. T. Berger and V. Levenshtein [13] study the use of so called 2-stage testing schemes to find all defectives with zero-error probability. They propose to run a fixed number of nonadaptive tests at the first stage and to test individually potential candidates after the first stage at the second stage. For some dependencies $p(t)$, the lower and upper bounds on asymptotics of the expected number of tests in the described 2-stage scheme are obtained in [13], [14]. Another problem of nonadaptive group testing schemes is considered by A. Sharma and C. Murthy in [15], where the authors derive upper bounds on the number of nonadaptive group tests required to identify a given number L of *non-defective* items from a large population of size t, containing a small number s of defective items.

An interesting approach to finding the defective set of an unknown size is proposed by P. Damaschke and A.S. Muhammad in [16]. In the beginning one should estimate the number of defectives $|\mathscr{S}|$ with the help of group tests, and then it remains to use one of the well-known algorithms for finding the defective set $\mathscr{S}$ of the estimated size.

The aim of our work is to discuss testing of hypothesis H_0: the random number of defectives is upper bounded by a fixed parameter s which does not depend on t. In fact, the considered disjunctive group testing model is a special case of noiseless symmetric multiple-access channel (MAC) such that the output of MAC equals the disjunctive sum of the inputs. The given model represents one described in the recent paper [17], where the model of MAC has the following key differences from the usual information-theoretic models of MAC: a) all the users employ the same code of size t; b) the code size t is independent from the code length N and t can be arbitrary large; c) at any time unit i, $i=1,2,\ldots,N$, there is the same random collection of active users.

The remainder of this paper is organized as follows. In

The material of this work was presented in part at the 2017 IEEE International Symposium on Information Theory [1]. This paper provides a refined upper bound and a novel lower bound on the optimal number of tests.

A. D'yachkov is with the Lomonosov Moscow State University, Moscow 119991, Russia (e-mail: agd-msu@yandex.ru).

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

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

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

N. Polyanskii and I. Vorobyev are supported by the Russian Foundation for Basic Research under grant No. 18-07-01427 A.

Section II we introduce notations and give basic definitions. Section III starts with the exhaustive proposition in the case of zero-error probability and discusses the known results related to the testing of hypothesis H_0. The exact formulations of the results of our paper leading to the asymptotical bounds announced in the abstract will be presented in Section IV. Section V is devoted to simulations of hypothesis testing problem. The detailed proofs will be given in Section VI.

II. Notation and Definitions

Let the symbol $\triangleq$ denote the equality by definition and the symbol $\boldsymbol{u}\bigvee\boldsymbol{v}$ will be used to denote the disjunctive (Boolean) sum of binary columns $\boldsymbol{u},\boldsymbol{v}\in\{0,1\}^N$. We say that a column $\boldsymbol{u}$ *covers* a column $\boldsymbol{v}$ if $\boldsymbol{u}\bigvee\boldsymbol{v}=\boldsymbol{u}$. An $(N\times t)$-matrix $X=\|x_i(j)\|$, $x_i(j)\in\{0,1\}$, with t columns (codewords) $\boldsymbol{x}(j)\triangleq(x_1(j),\ldots,x_N(j))$, $j\in[t]$, and N rows $\boldsymbol{x}_i\triangleq(x_i(1)\ldots,x_i(t))$, $i\in[N]$, is called a binary code of size t and length N.

Definition 1. [5], [6]. A binary code X is called a *disjunctive s-code*, $s\in[t-1]$, if the disjunctive sum of any s-subset of columns of X covers those and only those columns of X which are the terms of the given disjunctive sum.

In the classical problem of non-adaptive group testing, we describe N tests as a binary code $X=\|x_i(j)\|$, where the j-th column $\boldsymbol{x}(j)$ corresponds to the j-th element, and the i-row $\boldsymbol{x}_i$ corresponds to the i-th test and $x_i(j)\triangleq 1$ if and only if the j-th element is included into the i-th testing group. Let $\mathscr{S}$, $\mathscr{S}\subseteq[t]$, be an arbitrary fixed set of defective elements of size $|\mathscr{S}|$. For a code X and a set $\mathscr{S}$, define the binary *response vector* $\boldsymbol{x}(\mathscr{S})$ of length N, namely:

$$\boldsymbol{x}(\mathscr{S})\triangleq\begin{cases}\bigvee\limits_{j\in\mathscr{S}}\boldsymbol{x}(j) & \text{if}\quad \mathscr{S}\neq\emptyset,\\ (0,0,\ldots,0)^T & \text{if}\quad \mathscr{S}=\emptyset.\end{cases}$$

The result of each test equals 1 if at least one defective element is included into the testing group and 0 otherwise. So, the column of results is exactly equal to the response vector $\boldsymbol{x}(\mathscr{S})$. Definition 1 of disjunctive s-code gives the important sufficient condition for identification of any unknown defective set $\mathscr{S}$, namely, one can recover $\mathscr{S}$ based on the response vector if the number of defective elements $|\mathscr{S}|\le s$. In the case of disjunctive s-codes, the identification of the unknown $\mathscr{S}$ is equivalent to searching all columns of matrix X covered by $\boldsymbol{x}(\mathscr{S})$, and its complexity is equal to $\Theta(N\cdot t)$. This conventional algorithm of finding defectives is called *COMP* (*Combinatorial Optimal Matching Pursuit*) [7]. The best detection algorithm is based on enumerating all possible defective sets $\mathscr{S}$, and one of candidates is called *SSS* (*Smallest Satisfying Set*) [7]. But this algorithm is impractical because of the high time complexity which equals $\Theta\left(N\cdot\binom{t}{s}\right)$ if $|\mathscr{S}|=s$. Among other detection algorithms we highlight *DD* (*Definite Defectives*) [7], [9] because it has the same complexity as COMP but the best known non-adaptive random scheme requires up to 50% fewer tests in the regime $|\mathscr{S}|=\Theta(t^\alpha)$, $0<\alpha<1$. The DD algorithm finds all columns $\mathscr{S}'$ of matrix X covered by $\boldsymbol{x}(\mathscr{S})$ at first. But element j is considered to be defective if $\boldsymbol{x}(\mathscr{S}'\setminus\{j\})\neq\boldsymbol{x}(\mathscr{S})$.

Let us introduce two hypothesis: the null hypothesis $\{H_0:|\mathscr{S}|\le s\}$ and the alternative $\{H_1:|\mathscr{S}|\ge s+1\}$. In this work we consider testing hypothesis H_0 versus H_1 using group tests in the reasonable probabilitic model in which the random defective sets of the same size are equiprobable. More accurately, the probability distribution of the random defective set $\mathscr{S}$ is defined by vector

$$\boldsymbol{p}\triangleq(p_0,p_1,\ldots,p_t),\quad p_k\ge 0,\ k=0,1,\ldots,t,\quad \sum_{k=0}^{t}p_k=1,$$

as follows:

$$\Pr\{\mathscr{S}=\mathscr{S}_0\}\triangleq\frac{p_{|\mathscr{S}_0|}}{\binom{t}{|\mathscr{S}_0|}}\quad\text{for any}\quad \mathscr{S}_0\subseteq[t].\tag{1}$$

Let $\mathscr{D}:\{0,1\}^N\to\{H_0,H_1\}$ be an arbitrary *decision rule* which associates a response vector with the hypothesis. So, we will call the adapted for hypothesis testing problem the COMP algorithm by the COMP decision rule which accepts H_0 if the number of columns covered by the response vector is at most s. Introduce the (*maximal*) *error probability* for the decision rule $\mathscr{D}$ and testing matrix X:

$$\varepsilon_s(\boldsymbol{p},\mathscr{D},X)\triangleq\max\left\{\Pr\{\text{accept } H_1\big|H_0\},\Pr\{\text{accept } H_0\big|H_1\}\right\},\tag{2}$$

where the probability measure in the conditional probabilities is defined by (1). If the $\Pr\{H_0\}=0$ or $\Pr\{H_1\}=0$ let the error probability be zero. We use also the notation of *universal error probability* which does not depend on $\boldsymbol{p}$ and equals the worst error probability:

$$\varepsilon_s(\mathscr{D},X)\triangleq\max_{\boldsymbol{p}}\varepsilon_s(\boldsymbol{p},\mathscr{D},X).\tag{3}$$

III. Related Results

The problem of optimal zero-error nonadaptive hypothesis testing is reduced to the problem of optimal disjunctive codes in the following way:

Proposition 1. *A code X is a disjunctive s-code if and only if for any probability distribution $\boldsymbol{p}$ with positive components $p_s>0$ and $p_{s+1}>0$, there exists a decision rule $\mathscr{D}$ such that the error probability $\varepsilon_s(\boldsymbol{p},\mathscr{D},X)=0$.*

Proof. If X is a disjunctive s-code, then obviously the COMP decision rule allows to check the hypothesis H_0 without error. Converse can be proved by contradiction. Indeed, if matrix X is not a disjunctive s-code, then there exists a set $\mathscr{S}\subseteq[t]$ of size $|\mathscr{S}|=s$, and a number $j\in[t]\setminus\mathscr{S}$ such that $\boldsymbol{x}(\mathscr{S})=\boldsymbol{x}(\mathscr{S}\cup\{j\})$. So, for any decision rule we cannot distinguish the set $\mathscr{S}$ of size s from the set $\mathscr{S}\cup\{j\}$ of size $s+1$. $\square$

The best known practical constructions of disjunctive s-codes are based on shortened RS-codes. These constructions presented in [18] essentialy extend optimal and suboptimal ones suggested in [5].

Recall some results for optimal disjunctive s-codes. Denote by $t(s,N)$ the maximal number of columns for disjunctive s-codes with N rows. Introduce the *rate* of disjunctive s-codes:

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

The best known upper and lower bounds on the rate $R(s)$ are presented in [6] and [19], respectively. These bounds are written in the complex form, but the asymptotics are as follows

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

Further we will consider the case of positive error probability. First let us mention some results for the problem of estimating the number of defectives which are related to ours. In [16] the authors present a randomized algorithm that uses $G(\varepsilon,c)\log_2 t$ nonadaptive tests and produces the statistic $\hat{s}$ which satisfies the following properties: probability $\Pr\{\hat{s}<|\mathscr{S}|\}$ is upper bounded by a small parameter $\varepsilon \ll 1$ and the expected value of $\hat{s}/|\mathscr{S}|$ is upper bounded by a number $c>1$. Note that this result is *universal*, i.e., it does not depend on the distribution of the defective set. In [20] the authors construct adaptive randomized algorithm which uses at most $2\log_2\log_2|\mathscr{S}|+O(\frac{1}{\delta^2}\log_2\frac{1}{\varepsilon})$ adaptive tests and estimates $|\mathscr{S}|$ up to a multiplicative factor of $1\pm\delta$ with error probability $\le\varepsilon$. Also there is a converse result in [20] which states the necessity of $(1-\varepsilon)\log_2\log_2|\mathscr{S}|-1$ tests on average.

The first thought which comes to mind from Proposition 1 is that in order to solve the hypothesis testing problem one may use the COMP decision rule. Note that this rule always accepts H_1 if it holds, i.e., $\Pr(H_0|H_1)=0$. Moreover, it is not difficult to obtain that the maximum of the error probability $\varepsilon_s(\boldsymbol{p},\mathrm{COMP},X)$ in (3) is attained at any vector $\boldsymbol{p}$ such that $0<p_s<1$ and $p_k=0$ for $\forall k<s$, e.g., one can take $p_s=p_{s+1}=1/2$. The reader may refer to Lemma 1 about a similar statement which is given in Section IV and proved in Section VI-A. That is why the universal error probability $\varepsilon_s(\mathrm{COMP},X)$ equals the probability that an s-subset of columns of X covers an external column. But this probability is exactly the error probability for almost disjunctive s-codes [21]. The properties of the universal error probability $\varepsilon_s(\mathrm{COMP},X)$ obtained in [21] are presented below as Propositions 2 and 3.

Proposition 2. [21]. *If X is an arbitrary code of length N and size $t=\Omega(2^{N/s})$, then $\varepsilon_s(COMP,X)=\Omega(1)$ as $N\to\infty$.*

In other words, Proposition 2 means that the *rate* of matrix X defined by

$$R \triangleq \frac{\ln t}{N}$$

is at most $\ln 2/s$ for attaining an arbitrary small error probability.

Introduce the standard notations

$$h(Q)\triangleq -Q\ln Q-(1-Q)\ln[1-Q], \quad [x]^+\triangleq\max\{x,0\}.$$

In [21], using the ensemble of constant-weight binary codes we established the following random coding bound.

Proposition 3. [21]. *Let R, $0<R<1$, be fixed. If $N\to\infty$, then there exists $(N\times t)$ testing matrix X with $t=\lfloor\exp RN\rfloor$ such that*

$$\varepsilon_s(COMP,X)\le\exp\left\{-N\underline{E}^{COMP}(s,R)(1+o(1))\right\},$$

where

$$\begin{aligned}\underline{E}^{COMP}(s,R) &\triangleq \max_{0<Q<1}\ \min_{Q\le q<\min\{1,sQ\}}\left\{\mathscr{A}(s,Q,q)+\right.\\ &\qquad \left.[h(Q)-qh(Q/q)-R]^+\right\},\\ \mathscr{A}(s,Q,q) &\triangleq (1-q)\ln(1-q)+q\ln\left[\frac{Qy^s}{1-y}\right]\\ &\qquad +sQ\ln\frac{1-y}{y}+sh(Q),\end{aligned} \tag{4}$$

and y is the unique root of the equation

$$q=Q\frac{1-y^s}{1-y}, \quad 0<y<1. \tag{5}$$

In addition, for $s\to\infty$ and $R\le\frac{(\ln 2)^2}{s}(1+o(1))$, the exponent $\underline{E}^{COMP}(s,R)>0$.

IV. Main Results

Note that our hypothesis testing problem is very different from the detection of defectives because there are only two answers: H_0 or H_1. However, in the zero-error case hypothesis testing requires nearly the same number of group tests as a detection of defectives does. Our main result is devoted to hypothesis group testing in the small-error case. We introduce a decision rule which is essentially better than COMP and provide an upper bound on the error probability which does not depend on the number of elements t, whereas the result in Proposition 3 does.

Fix an arbitrary parameter τ, $0<\tau<1$, and introduce a *τ-weight decision rule (τ-WDR)*

$$\begin{cases}\text{accept } \{H_0: |\mathscr{S}|\le s\} & \text{if } |\boldsymbol{x}(\mathscr{S})|\le\tau N,\\ \text{accept } \{H_1: |\mathscr{S}|> s\} & \text{if } |\boldsymbol{x}(\mathscr{S})|>\tau N.\end{cases} \tag{6}$$

Remark 1. In the zero-error case τ-WDR requires a special condition on a disjunctive s-code X: for any subset $\mathscr{S}$ of size $|\mathscr{S}|=s$, the weight $|\boldsymbol{x}(\mathscr{S})|$ of the response vector is at most $\lfloor\tau N\rfloor$, and, for any subset $\mathscr{S}'$ of size $|\mathscr{S}'|=s+1$, the weight $|\boldsymbol{x}(\mathscr{S}')|$ of the response vector is at least $\lfloor\tau N\rfloor+1$. A similar model of specific disjunctive s-codes was considered in [22], where a disjunctive s-code is supplied with a weaker additional condition: the weight $|\boldsymbol{x}(\mathscr{S})|$ of the response vector for any subset $\mathscr{S}$, $\mathscr{S}\subseteq[t]$, $|\mathscr{S}|\le s$, is at most T. In [22] the authors motivate their group testing model by a risk for the safety of the persons who perform tests, in some contexts, when the number of positive test results is too large.

We study only the universal error probability for τ-WDR, and the following lemma proved in Section VI-A determines the worst probability distribution.

Lemma 1. *For any integer $s\ge1$ and testing matrix X, the maximum of the error probability $\varepsilon_s(\boldsymbol{p},\tau\text{-}WDR,X)$ in (3) is attained at any $\boldsymbol{p}$ such that $p_s>0$, $p_{s+1}>0$ and $p_s+p_{s+1}=1$.*

The following upper bound on the error probability for τ-WDR is proved in Section VI-C by the probabilistic method based on the ensemble of constant-weight binary codes. A parameter Q in the statement of Theorem 1 corresponds to the relative weight of columns in the random matrix.

Theorem 1. **1.** *For any N and t, there exists an $(N\times t)$ testing matrix X such that the error probability*

$\varepsilon_s(\tau\text{-}WDR, X) \le \overline{\varepsilon}_s(\tau, N)$, where the bound $\overline{\varepsilon}_s(\tau, N)$ does not depend on the number of elements t and has the form:

$$\overline{\varepsilon}_s(\tau, N) = \exp\{-N\underline{E}(s,\tau)(1+o(1))\}, \text{ as } N \to \infty, \quad (7)$$

$$\underline{E}(s,\tau) \triangleq \mathscr{A}(s, Q^*(s,\tau), \tau), \quad (8)$$

where $\mathscr{A}(s,Q,\tau)$ is defined by $(4)-(5)$ and $Q^*(s,\tau)$ is the unique solution of the equation

$$\mathscr{A}(s,Q,\tau) = \mathscr{A}(s+1,Q,\tau),$$
$$\max\left\{1-(1-\tau)^{1/(s+1)}, \frac{\tau}{s}\right\} < Q < 1-(1-\tau)^{1/s}. \quad (9)$$

2. *The optimal value of $\underline{E}(s,\tau)$ satisfies the asymptotic inequality:*

$$\underline{E}^{WDR}(s) \triangleq \max_{0<\tau<1} \underline{E}(s,\tau) \ge \frac{1}{4s^2}(1+o(1)), \quad s \to \infty, \quad (10)$$

where the right-hand side is attained at the parameters that satisfy $\tau \sim s \cdot Q = o(1)$, and $Q \cdot s^2 \to \infty$.

Independence from the number of elements t is crucial in this bound. In other words, one can construct a sequence of $(N \times t(N))$ matrices with exponentially decreasing error probability for any function $t(N)$. Recall that by Proposition 2 the rate $R = \ln t(N)/N$ has to be $\le \ln 2/s$ if the error probability for the COMP decision rule vanishes as $N \to \infty$. That is why the τ-WDR decision rule has a significant advantage over the COMP decision rule for the large number of elements t.

The next converse theorem derives the lower bound on the error probability for the worst distribution and any decision rule.

Theorem 2. *Let $\boldsymbol{p}$ be such that $p_s > 0$, $p_{s+1} > 0$ and $p_s + p_{s+1} = 1$. For any decision rule $\mathscr{D}$ and any testing matrix X, the error probability is lower bounded by:*

$$\varepsilon_s(\boldsymbol{p}, \mathscr{D}, X) \ge \frac{1}{2}\left(2^{-N/s}\frac{t}{t-s} - \frac{s}{t-s}\right). \quad (11)$$

Theorems 1 and 2 proved in Section VI obviously lead to

Proposition 4. *If $s \to \infty$ and $\varepsilon \to 0$, then the following two statements take place.* 1) *There exist an $(N \times t)$-code X and a decoding algorithm $\mathscr{D}$, using*

$$N = 4s^2 \ln\frac{1}{\varepsilon}(1+o(1)), \quad s \to \infty, \quad \varepsilon \to 0, \quad (12)$$

nonadaptive group tests, which accept or reject H_0 provided that the universal error probability $\varepsilon_s(\mathscr{D}, X) \le \varepsilon$. 2) *Any $(N \times t)$-code X of sufficiently large size t and any decoding algorithm $\mathscr{D}$, which accept or reject H_0 provided that the universal error probability $\varepsilon_s(\mathscr{D}, X) \le \varepsilon$, need to use*

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

nonadaptive group tests as $s \to \infty$ and $\varepsilon \to 0$.

Remark 2. We would like to emphasize that the analysis over the ensemble of random matrices, where each entry is an independent Bernoulli random variable with probability p, is much simpler as compared to one we carry out in the proof of Theorem 1 in Section VI. However, for $s \to \infty$ and $\varepsilon \to 0$, such analysis would lead to the bound

$$N = \frac{2}{(\ln 2)^2} s^2 \ln\frac{1}{\varepsilon}(1+o(1)) = 4.163\, s^2 \ln\frac{1}{\varepsilon}(1+o(1)),$$

which is worse than the bound (12).

The numerical values of the optimal lower bound $\underline{E}^{\text{WDR}}(s)$ on the error exponent along with the corresponding optimal weight parameter $\tau = \tau(s)$ and the ensemble parameter $Q = Q(s)$ are presented in Table I. The table also depicts the values of

$$\underline{E}^{\text{COMP}}(s,0) \triangleq \lim_{R\to 0} \underline{E}^{\text{COMP}}(s,R)$$

(the maximal known lower bound on the error exponent for COMP and positive rate),

$$\underline{R}^{\text{COMP}}(s) \triangleq \sup\{R : \underline{E}_s^{\text{COMP}}(R) > 0\}$$

(the maximal rate for which the known lower bound on the error exponent for COMP is positive) and

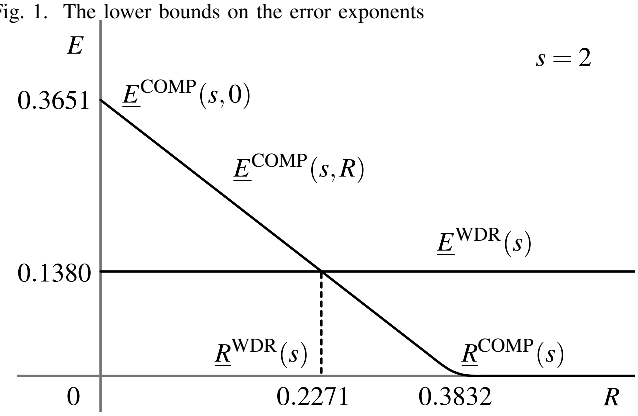
$$\underline{R}^{\text{WDR}}(s) \triangleq \sup\{R : \underline{E}_s^{\text{COMP}}(R) > \underline{E}^{\text{WDR}}(s)\}$$

(the maximal rate for which the known lower bound on the error exponent for COMP is better than for τ-WDR). Also these relations are presented on Figure 1.

TABLE I
THE NUMERICAL VALUES OF THE LOWER BOUNDS ON THE ERROR EXPONENTS

s	2	3	4	5	6
$\underline{E}^{\text{WDR}}(s)$	0.1380	0.0570	0.0311	0.0196	0.0135
$\tau(s)$	0.2065	0.1365	0.1021	0.0816	0.0679
$Q(s)$	0.1033	0.0455	0.0255	0.0163	0.0113
$\underline{E}_s^{\text{COMP}}(0)$	0.3651	0.2362	0.1754	0.1397	0.1161
$\underline{R}^{\text{COMP}}(s)$	0.3832	0.2455	0.1810	0.1434	0.1188
$\underline{R}^{\text{WDR}}(s)$	0.2271	0.1792	0.1443	0.1201	0.1027

Fig. 1. The lower bounds on the error exponents



V. Simulation

For finite N and t, we carried out a simulation as follows. The probability distribution vector $\boldsymbol{p}$ is defined by

$$p_s = p_{s+1} = 1/2, \qquad p_k = 0 \quad \forall k \in [t] \setminus \{s, s+1\},$$

i.e., $\boldsymbol{p}$ is a distribution at which the maximum in the right-hand side of (3) is attained for the COMP and the τ-WDR decision rules. A matrix X is generated randomly from the ensemble of constant column weight matrices, i.e., for some weight parameter w, $1 \le w \le N$, each column of X is chosen independently and equiprobably from the set of all $\binom{N}{w}$ columns of weight w. For every weight w and every decision rule, we repeat the procedure 1000 times and choose the matrix with the minimal error probability. Some results of simulation are presented in Table II. The best values of the error probability for fixed parameters s, t and N are given in boldface.

TABLE II
RESULTS OF SIMULATION

	τ-WDR decision rule				COMP decision rule	
N	$\Pr\{H_1\|H_0\}$	$\Pr\{H_0\|H_1\}$	w	$\lfloor \tau N \rfloor$	$\Pr\{H_1\|H_0\}$	w
			$s=2,\quad t=15$			
5	0.2571	**0.2571**	2	3	0.9333	2
8	**0.1619**	0.1604	3	5	0.7048	2
10	0	**0.1429**	1	2	0.4571	3
12	0	**0.0857**	1	2	0.1810	3
14	0	**0.0571**	1	2	0.0952	3
15	0	0.0462	2	4	**0.0286**	3
			$s=2,\quad t=20$			
5	**0.2632**	0.2588	2	3	0.9579	2
8	0.1632	**0.1649**	3	5	0.8316	2
11	0.1053	**0.1509**	4	7	0.5158	3
12	**0.1158**	0.1123	4	7	0.4158	3
14	0	**0.0842**	2	4	0.2316	3
15	0	**0.0693**	2	4	0.1526	4
			$s=2,\quad t=100$ (Estimated error probabilities)			
5	**0.2420**	0.2300	2	3	0.9980	2
8	0.1830	**0.1950**	3	5	0.9940	5
11	0.1570	**0.1630**	5	8	0.9830	4
12	0.1280	**0.1350**	4	7	0.9810	4
14	0	**0.1080**	2	4	0.9600	5
15	0	**0.0970**	2	4	0.9610	5

For $s=2$, any number of tests N from Table II and an arbitrary number of columns t, $t>N$, it is recommended to choose the corresponding column weight w, $1<w<N$, specified in Table II and generate an "optimal" random $(N\times t)$ constant column weight matrix with weight w. So then, for the corresponding threshold τ depicted in Table II, an "optimal" error probability for the τ-WDR decision rule should be similar to the corresponding one indicated in Table II in boldface. As an example of such comparison, we put in Table II the error probabilities for $s=2$ and $t=100$ which were estimated by the Monte Carlo method, namely, subsets $\mathscr{S}$, $\mathscr{S}\subseteq[100]$, of size $|\mathscr{S}|=2$ and $|\mathscr{S}|=3$ were chosen randomly 1000 times.

The results of simulation verify the advantage of the τ-WDR decision rule over the COMP decision rule and the independence of the error probability for τ-WDR decision rule from the number of elements t.

VI. PROOFS OF MAIN RESULTS

A. Proof of Lemma 1

Proof. For a fixed $(N\times t)$-matrix X and parameters s and $T\triangleq\lfloor\tau N\rfloor$, introduce the sets $B_k^i(T,X)$, $i=1,2$, $k=0,1,\ldots,t$, of k-subsets of set $[t]$ as follows:

$$\begin{aligned} B_k^1(T,X) &\triangleq \{\mathscr{S}:\mathscr{S}\subseteq[t],\ |\mathscr{S}|=k,\ |\boldsymbol{x}(\mathscr{S})|\ge T+1\},\\ B_k^2(T,X) &\triangleq \{\mathscr{S}:\mathscr{S}\subseteq[t],\ |\mathscr{S}|=k,\ |\boldsymbol{x}(\mathscr{S})|\le T\}. \end{aligned} \tag{13}$$

Then the error probability for the τ-WDR decision rule is represented by

$$\varepsilon_s(\boldsymbol{p},\tau\text{-WDR},X)$$

$$\triangleq \max\left\{\sum_{k=0}^{s}\frac{p_k}{\sum\limits_{l=0}^{s}p_l}\frac{\left|B_k^1(T,X)\right|}{\binom{t}{k}},\ \sum_{k=s+1}^{t}\frac{p_k}{\sum\limits_{l=s+1}^{t}p_l}\frac{\left|B_k^2(T,X)\right|}{\binom{t}{k}}\right\}. \tag{14}$$

For any $k<t$, $\mathscr{S}\in B_k^1(T,X)$, and $j\in[t]\setminus\mathscr{S}$, one can construct a set $\mathscr{S}'=\mathscr{S}\cup\{j\}$ belonging to $B_{k+1}^1(T,X)$. Moreover, there exist at most $k+1$ ways leading to the same set $\mathscr{S}'\in B_{k+1}^1(T,X)$. This implies the following inequality:

$$|B_{k+1}^1(T,X)|\ge\frac{t-k}{k+1}|B_k^1(T,X)|.$$

Similarly, one can construct set $\mathscr{S}\in B_k^2(T,X)$ by removing from any set $\mathscr{S}'\in B_{k+1}^2(T,X)$ any index $j\in\mathscr{S}'$, and at most $(t-k)$ such different pairs $(\mathscr{S}',j)$ may construct the same $\mathscr{S}\triangleq\mathscr{S}'\setminus\{j\}$. Therefore

$$|B_k^2(T,X)|\ge\frac{k+1}{t-k}|B_{k+1}^2(T,X)|.$$

Definition (14) and these inequalities yield

$$\varepsilon_s(\boldsymbol{p},\tau\text{-WDR},X)\le\max\left\{\frac{\left|B_s^1(T,X)\right|}{\binom{t}{s}},\frac{\left|B_{s+1}^2(T,X)\right|}{\binom{t}{s+1}}\right\}, \tag{15}$$

and the equality (15) holds for any distribution with the properties: $p_s>0$, $p_{s+1}>0$, and $p_j=0$ for $j\in[t]\setminus\{s,s+1\}$. In particular, it means that for τ-WDR the definition of the universal error probability (3) is equivalent to the right-hand side of (15). □

B. Proof of Theorem 2

Proof. Let an $(N\times t)$-matrix X be a testing matrix, $\mathscr{D}:\{0,1\}^N\to\{H_0,H_1\}$ is a decision rule and $\boldsymbol{p}$ is a distribution so that $p_s>0$, $p_{s+1}>0$ and $p_j=0$ for any $j\in[t]\setminus\{s,s+1\}$. Obviously, the maximal error probability (2) is bounded below by the half of the sum:

$$\varepsilon_s(\boldsymbol{p},\mathscr{D},X)\ge\frac{1}{2}\left(\Pr\{\text{accept } H_1|H_0\}+\Pr\{\text{accept } H_0|H_1\}\right). \tag{16}$$

Denote the number of k-subsets with the response vector $\boldsymbol{y}$ by $n_k(\boldsymbol{y},X)$, i.e.,

$$n_k(\boldsymbol{y},X)\triangleq|\{\mathscr{S}:|\mathscr{S}|=k,\ \boldsymbol{x}(\mathscr{S})=\boldsymbol{y}\}|.$$

The considered special type of distribution $\boldsymbol{p}$ allows to rewrite the error probabilities in a simple form. The right-hand side of (16) can be represented as follows

$$\varepsilon_s(\boldsymbol{p},\mathscr{D},X)\ge\frac{1}{2}\sum_{\boldsymbol{y}\in\{0,1\}^N}\left(\frac{n_s(\boldsymbol{y},X)}{\binom{t}{s}}\mathbb{1}\{\mathscr{D}(\boldsymbol{y})\ne H_0\}+\frac{n_{s+1}(\boldsymbol{y},X)}{\binom{t}{s+1}}\mathbb{1}\{\mathscr{D}(\boldsymbol{y})\ne H_1\}\right). \tag{17}$$

One of the two indicators $\mathbb{1}\{\mathscr{D}(\boldsymbol{y})\ne H_0\}$, $\mathbb{1}\{\mathscr{D}(\boldsymbol{y})\ne H_1\}$ equals 0 and the other one equals 1. It is easy to understand which decision rule $\mathscr{D}$ minimizes the right-hand side of (17), therefore

$$\varepsilon_s(\boldsymbol{p},\mathscr{D},X)\ge\frac{1}{2}\sum_{\boldsymbol{y}\in\{0,1\}^N}\min\left\{\frac{n_s(\boldsymbol{y},X)}{\binom{t}{s}},\frac{n_{s+1}(\boldsymbol{y},X)}{\binom{t}{s+1}}\right\}. \tag{18}$$

Further we consider only those $\boldsymbol{y}$ for which $n_s(\boldsymbol{y},X)>0$. It is obvious that for other $\boldsymbol{y}$ the minimum in the sum (18) equals 0. Denote the relative number of s-subsets with the response vector $\boldsymbol{y}$ by $\beta_{\boldsymbol{y}}$, i.e., $\beta_{\boldsymbol{y}}\triangleq n_s(\boldsymbol{y},X)/\binom{t}{s}$, and note that

$$n_s(\boldsymbol{y},X)=\beta_{\boldsymbol{y}}\binom{t}{s}=\beta_{\boldsymbol{y}}\frac{(t-s+1)\dots t}{s!}$$
$$\geq\frac{(\beta_{\boldsymbol{y}}^{\frac{1}{s}}t-s+1)\dots(\beta_{\boldsymbol{y}}^{\frac{1}{s}}t)}{s!}=\binom{\beta_{\boldsymbol{y}}^{\frac{1}{s}}t}{s}$$

because $0<\beta_{\boldsymbol{y}}\leq 1$. By $\mathscr{S}_{\boldsymbol{y}}$ denote a set of all column's indexes which are included into some s-subset $\mathscr{S}$ for which the response vector $\boldsymbol{x}(\mathscr{S})=\boldsymbol{y}$, i.e.,

$$\mathscr{S}_{\boldsymbol{y}}=\bigcup_{\mathscr{S}:\boldsymbol{x}(\mathscr{S})=\boldsymbol{y}}\mathscr{S},$$

and suppose that $|\mathscr{S}_{\boldsymbol{y}}|=s+L$. The previous inequality and this assumption lead to

$$\binom{\beta_{\boldsymbol{y}}^{\frac{1}{s}}t}{s}\leq n_s(\boldsymbol{y},X)\leq\binom{s+L}{s}.$$

It gives $L\geq\beta_{\boldsymbol{y}}^{\frac{1}{s}}t-s$ (the right-hand side can be replaced by the ceiling). Given $\mathscr{S}$, $|\mathscr{S}|=s$, with the response vector $\boldsymbol{x}(\mathscr{S})=y$, and index $j\in\mathscr{S}_{\boldsymbol{y}}\setminus\mathscr{S}$, one one can construct an $(s+1)$-subset $\mathscr{S}'=\mathscr{S}\cup\{j\}$ with the same response vector $\boldsymbol{x}(\mathscr{S}')=\boldsymbol{y}$. Moreover, any $\mathscr{S}'$ can be constructed in at most $(s+1)$ such ways. Hence

$$n_{s+1}(\boldsymbol{y},X)\geq n_s(\boldsymbol{y},X)\frac{L}{s+1}\geq\beta_{\boldsymbol{y}}\binom{t}{s}(\beta_{\boldsymbol{y}}^{\frac{1}{s}}t-s)\frac{1}{s+1}$$
$$=\left(\beta_{\boldsymbol{y}}^{\frac{s+1}{s}}\frac{t}{t-s}-\beta_{\boldsymbol{y}}\frac{s}{t-s}\right)\binom{t}{s+1}.\quad(19)$$

Recall that $0<\beta_{\boldsymbol{y}}\leq 1$. Therefore, the following inequality holds:

$$\beta_{\boldsymbol{y}}^{\frac{s+1}{s}}\frac{t}{t-s}-\beta_{\boldsymbol{y}}\frac{s}{t-s}\leq\beta_{\boldsymbol{y}}.$$

That is why the lower bound (19) also gives a lower bound on the minimum in the sum (18) and one can derive

$$\varepsilon_s(\boldsymbol{p},\mathscr{D},X)\geq\frac{1}{2}\sum_{\boldsymbol{y}\in\{0,1\}^N:\beta_{\boldsymbol{y}}>0}\left(\beta_{\boldsymbol{y}}^{\frac{s+1}{s}}\frac{t}{t-s}-\beta_{\boldsymbol{y}}\frac{s}{t-s}\right)$$
$$\geq\frac{1}{2}\left(2^{-\frac{N}{s}}\frac{t}{t-s}-\frac{s}{t-s}\right),$$

where we use the property of values $\beta_{\boldsymbol{y}}$ that their sum equals 1, i.e., $\sum_{\boldsymbol{y}\in\{0,1\}^N}\beta_{\boldsymbol{y}}=1$, and Jensen's inequality for a $\cup$-convex function $f(x)=x^{-\frac{1}{s}}$:

$$\sum_{\boldsymbol{y}\in\{0,1\}^N:\beta_{\boldsymbol{y}}>0}\beta_{\boldsymbol{y}}f(\beta_{\boldsymbol{y}}^{-1})\geq f\left(\sum_{\boldsymbol{y}\in\{0,1\}^N:\beta_{\boldsymbol{y}}>0}\beta_{\boldsymbol{y}}\cdot\beta_{\boldsymbol{y}}^{-1}\right).$$

□

C. Proof of Theorem 1

Proof of Statement 1. Fix $s\geq 2$, $t\geq s+1$, $N\geq 2$, $0<\tau<1$ and a parameter Q, $\frac{\tau}{s}<Q<\tau$. The bound (7) is obtained by the probabilistic method. Define an ensemble of constant column weight matrices [19] as ensemble $E(N,t,Q)$ of binary matrices X with N rows and t columns, where the columns are chosen independently and equiprobably from the set of all $\binom{N}{\lfloor QN\rfloor}$ columns of a fixed weight $\lfloor QN\rfloor$.

By Lemma 1 the error probability can be rewritten as

$$\varepsilon_s(\tau\text{-WDR},X)\triangleq\max\left\{\frac{\left|B_s^1(\lfloor\tau N\rfloor,X)\right|}{\binom{t}{s}},\frac{\left|B_{s+1}^2(\lfloor\tau N\rfloor,X)\right|}{\binom{t}{s+1}}\right\},\quad(20)$$

where the sets $B_s^1(\lfloor\tau N\rfloor,X)$ and $B_{s+1}^2(\lfloor\tau N\rfloor,X)$ are defined by (13). For the ensemble $E(N,t,Q)$, denote the expectation of the error probability (20) by

$$\mathscr{E}_s(\tau,Q,N,t)\triangleq\mathbb{E}\Big[\varepsilon_s(\tau\text{-WDR},X)\Big].\quad(21)$$

It is obvious that there exists a matrix X with N rows and t columns such that its error probability (20) is upper bounded by $\mathscr{E}_s(\tau,Q,N,t)$ minimized over all admissible Q. Further we show that the logarithmic asymptotics of this value equals (8). Define

$$\underline{E}(s,\tau)\triangleq\max_{\tau/s<Q<\tau}\lim_{N\to\infty}\frac{-\ln\mathscr{E}_s(\tau,Q,N,t)}{N}.\quad(22)$$

The cardinality of set $B_s^1(\lfloor\tau N\rfloor,X)$ can be expressed through indicator functions:

$$\left|B_s^1(\lfloor\tau N\rfloor,X)\right|=\sum_{\mathscr{S}\subseteq[t],|S|=s}\mathbb{1}\big\{\mathscr{S}\in B_s^1(\lfloor\tau N\rfloor,X)\big\}.$$

Therefore, the expectation of the cardinality $\left|B_s^1(\lfloor\tau N\rfloor,X)\right|$equals

$$\mathbb{E}\Big[\left|B_s^1\right|\Big]=\binom{t}{s}\Pr\big\{\mathscr{S}\in B_s^1\,\big|\,|\mathscr{S}|=s\big\}.\quad(23)$$

Similarly, the expectation of $\left|B_{s+1}^2(\lfloor\tau N\rfloor,X)\right|$

$$\mathbb{E}\Big[\left|B_{s+1}^2\right|\Big]=\binom{t}{s+1}\Pr\big\{\mathscr{S}\in B_{s+1}^2\,\big|\,|\mathscr{S}|=s+1\big\}.$$

For the ensemble $E(N,t,Q)$, denote the probabilities $\Pr\big\{\mathscr{S}\in B_s^1(\lfloor\tau N\rfloor,X)\,\big|\,|\mathscr{S}|=s\big\}$ and $\Pr\big\{\mathscr{S}\in B_{s+1}^2(\lfloor\tau N\rfloor,X)\,\big|\,|\mathscr{S}|=s+1\big\}$ by $P_s^1(\tau,Q,N)$ and $P_{s+1}^2(\tau,Q,N)$, respectively. It is obvious, that these probabilities depend only on s, τ, Q, N and do not depend on t. The formulas (23) yield that the expectation (21) satisfies the inequalities:

$$\max\big\{P_s^1(\tau,Q,N),P_{s+1}^2(\tau,Q,N)\big\}$$
$$\leq\mathscr{E}_s(\tau,Q,N,t)\leq P_s^1(\tau,Q,N)+P_{s+1}^2(\tau,Q,N).\quad(24)$$

Given matrix X, for a fixed subset $\mathscr{S}\subseteq[t]$, $|\mathscr{S}|=k$, of size k and a fixed integer w, consider a probability

$$P_k^N(Q,w)\triangleq\Pr\left\{\left|\bigvee_{j\in\mathscr{S}}\boldsymbol{x}(j)\right|=w\right\}.\quad(25)$$

Note that the probability $P_k^N(Q,w)$ does not depend on the choice of the set $\mathscr{S}$ and depends only on k, w, N and Q.

Probabilities $P_s^1(\tau,Q,N)$ and $P_{s+1}^2(\tau,Q,N)$ can be rewritten as follows:

$$\begin{aligned} P_s^1(\tau,Q,N) &= \sum_{w=\lfloor \tau N\rfloor+1}^{\min\{N,s\lfloor QN\rfloor\}} P_s^N(Q,w), \\ P_{s+1}^2(\tau,Q,N) &= \sum_{w=\lfloor QN\rfloor}^{\lfloor \tau N\rfloor} P_{s+1}^N(Q,w). \end{aligned} \tag{26}$$

The logarithmic asymptotics of the probability $P_k^N(Q,w)$ was calculated in [21]. To make the present paper self-contained, we repeat the proof in Section VI-D.

Lemma 2. *If q satisfies $Q<q<\min\{kQ,1\}$, then*

$$\lim_{N\to\infty}\frac{-\log_2 P_k^N(Q,\lfloor qN\rfloor)}{N} = \mathscr{A}(k,Q,q), \tag{27}$$

where the function $\mathscr{A}(k,Q,q)$ is defined by (4)-(5).

In Section VI-D we prove the following analytical properties:

Lemma 3. **1.** *Function $\mathscr{A}(k,Q,q)$ as a function of the parameter q decreases in the interval $q\in(Q,1-(1-Q)^k]$, increases in the interval $q\in[1-(1-Q)^k,\min\{1,kQ\})$ and equals 0 at the point $q=1-(1-Q)^k$.*
2. *Function $\mathscr{A}(k,Q,q)$ as a function of the parameter Q decreases in the interval $Q\in(\frac{q}{k},1-(1-q)^{1/k}]$, increases in the interval $Q\in[1-(1-q)^{1/k},q)$ and equals 0 at the point $Q=1-(1-q)^{1/k}$.*

One can obtain the logarithmic asymptotics of the probabilities $P_s^1(\tau,Q,N)$ and $P_{s+1}^2(\tau,Q,N)$ from formulas (26) and (27):

$$\begin{aligned} &\lim_{N\to\infty}\frac{-\log_2 P_s^1(\tau,Q,N)}{N} = \min_{q\in(\mathrm{i}1)}\mathscr{A}(s,Q,q), \\ &\lim_{N\to\infty}\frac{-\log_2 P_{s+1}^2(\tau,Q,N)}{N} = \min_{q\in(\mathrm{i}2)}\mathscr{A}(s+1,Q,q), \\ &(\mathrm{i}1)\triangleq[\tau,\min\{1,sQ\}],\quad (\mathrm{i}2)\triangleq[Q,\tau]. \end{aligned} \tag{28}$$

Therefore, (24) and (28) yield the existence of the limit

$$\begin{aligned} &\lim_{N\to\infty}\frac{-\log_2 \mathscr{E}_s^N(\tau,Q,N,t)}{N} \\ &\quad = \min\left\{\min_{q\in(\mathrm{i}1)}\mathscr{A}(s,Q,q),\min_{q\in(\mathrm{i}2)}\mathscr{A}(s+1,Q,q)\right\}. \end{aligned} \tag{29}$$

By Lemma 3 the function $\mathscr{A}(k,Q,q)$ equals 0 at $q=1-(1-Q)^k$. This property yields

$$\begin{aligned} &\min_{q\in(\mathrm{i}1)}\mathscr{A}(s,Q,q)=0 && \text{if } \tau\le 1-(1-Q)^s, \\ &\min_{q\in(\mathrm{i}2)}\mathscr{A}(s+1,Q,q)=0 && \text{if } \tau\ge 1-(1-Q)^{s+1}. \end{aligned}$$

Finally, we exclude from (22) values of Q for which the minimum (29) equals 0, and from the monotonicity properties given in Lemma 3 we derive

$$\begin{aligned} &\underline{E}(s,\tau) = \max_{Q\in(\mathrm{i}Q)}\min\{\mathscr{A}(s,Q,\tau),\mathscr{A}(s+1,Q,\tau)\}, \\ &(\mathrm{i}Q)\triangleq\left(\max\left\{1-(1-\tau)^{1/(s+1)},\frac{\tau}{s}\right\},1-(1-\tau)^{1/s}\right). \end{aligned}$$

By applying the monotonicity properties given in the second statement of Lemma 3 we finish the proof of Statement 1 of Theorem 1. $\square$

Proof of Statement 2. We shall establish a lower bound on the asymptotic behaviour (as *to*∞) of the expression

$$\underline{E}^{\mathrm{WDR}}(s)\triangleq\max_{0<\tau<1}\max_{Q\in(\mathrm{i}Q)}\min\{\mathscr{A}(s,Q,\tau),\mathscr{A}(s+1,Q,\tau)\}. \tag{30}$$

For any fixed τ, $0<\tau<1$, and any fixed Q, $Q\in(\mathrm{i}Q)$, let us denote the solutions of the equation (5) for $\mathscr{A}(s,Q,\tau)$ and $\mathscr{A}(s+1,Q,\tau)$ by $y_1(Q,\tau)$ and $y_2(Q,\tau)$, respectively. Note that y_1 can be greater than 1. It follows from (5) that the parameter τ can be expressed in two forms:

$$\tau = Q\frac{1-y_1^s}{1-y_1} = Q\frac{1-y_2^{s+1}}{1-y_2}.$$

This means that the inequality $1-(1-\tau)^{1/(s+1)}<Q \Leftrightarrow \tau<1-(1-Q)^{s+1}$ is equivalent to

$$\frac{1-y_2^{s+1}}{1-y_2}<\frac{1-(1-Q)^{s+1}}{1-(1-Q)}.$$

Note that, for any integer $n\ge 2$, the function $f(x)=\frac{1-x^n}{1-x}$ is increasing in the interval $x\in(0,+\infty)$. Hence, we have

$$1-(1-\tau)^{1/(s+1)}<Q \quad\Leftrightarrow\quad Q<1-y_2,$$

and similarly,

$$Q<1-(1-\tau)^{1/s} \quad\Leftrightarrow\quad Q>1-y_1.$$

In conclusion, a pair of parameters (y_1,Q), $y_1>0$, $0<Q<1$, uniquely defines the parameters τ and y_2. Moreover, if the inequalities

$$0<\tau<1,\quad Q<1-y_2,\quad Q>1-y_1. \tag{31}$$

hold, then the parameters τ and Q are in the region, in which the maximum (30) is searched.

Let some constant $c>0$ be fixed, $s\to\infty$ and $y_1\triangleq 1-c/s^2+o(1/s^3)$. Then, the asymptotic behavior of τ/Q equals

$$\frac{1-y_2^{s+1}}{1-y_2}=\frac{\tau}{Q}=\frac{1-y_1^s}{1-y_1}=s-\frac{c}{2}+o(1),$$

and, therefore,

$$y_2 = 1-\frac{c+2}{(s+1)^2}+o\left(\frac{1}{s^3}\right)=1-\frac{c+2}{s^2}+\frac{2(c+2)}{s^3}+o\left(\frac{1}{s^3}\right).$$

To satisfy the inequalities (31) the parameter Q should be in the interval $(1-y_1,1-y_2)$. Let us define the parameter Q as $Q\triangleq d/s^2$, where d, $c<d<c+2$, is some constant. Hence, Q is in that interval.

The full list of the asymptotic behaviors of the parameters is presented below:

$$\begin{aligned} \tau &= \frac{d}{s}-\frac{cd}{2s^2}+o\left(\frac{1}{s^2}\right), \\ Q &= \frac{d}{s^2}, \\ y_1 &= 1-\frac{c}{s^2}+o\left(\frac{1}{s^2}\right), \\ y_2 &= 1-\frac{c+2}{s^2}+o\left(\frac{1}{s^2}\right),\quad s\to\infty, \end{aligned} \tag{32}$$

where c and d are arbitrary constants such that $c>0$, $c<d<c+2$. The parameters defined by (32) satisfy the inequalities (31), and, therefore, the substitution of asymptotic behaviors (32) into (30) leads to some lower bound on $\underline{E}^{\text{WDR}}(s)$.

Let us calculate the asymptotics of

$$\frac{\mathscr{A}(s,Q,\tau)}{\log_2 e} = (1-\tau)\ln(1-\tau) + (sQ-\tau)\ln\left[\frac{1-y_1}{Q}\right] + s(\tau-Q)\ln y_1 - s(1-Q)\ln(1-Q).$$

The first two terms of the asymptotic expansion of the summands are

$$(1-\tau)\ln(1-\tau) = -\frac{d}{s} + \frac{cd}{2s^2} + \frac{d^2}{2s^2} + o\left(\frac{1}{s^2}\right),$$
$$(sQ-\tau)\ln\left[\frac{1-y_1}{Q}\right] = \frac{cd}{2s^2}\ln\left[\frac{c}{d}\right] + o\left(\frac{1}{s^2}\right),$$
$$s(\tau-Q)\ln y_1 = -\frac{cd}{s^2} + o\left(\frac{1}{s^2}\right),$$
$$-s(1-Q)\ln(1-Q) = \frac{d}{s} + o\left(\frac{1}{s^2}\right).$$

Therefore,

$$\frac{\mathscr{A}(s,Q,\tau)}{\log_2 e} = \frac{d(d-c+c\ln[c/d])}{2s^2} + o\left(\frac{1}{s^2}\right).$$

Further, let us calculate the asymptotics of

$$\frac{\mathscr{A}(s+1,Q,\tau)}{\log_2 e} = (1-\tau)\ln(1-\tau) + (sQ-\tau)\ln\left[\frac{1-y_2}{Q}\right] + s(\tau-Q)\ln y_2 - s(1-Q)\ln(1-Q) + Q\ln\left[\frac{1-y_2}{Q}\right] + (\tau-Q)\ln y_2 - (1-Q)\ln(1-Q).$$

The first two terms of the asymptotic expansion of the new summands equals

$$(sQ-\tau)\ln\left[\frac{1-y_2}{Q}\right] = \frac{cd}{2s^2}\ln\left[\frac{c+2}{d}\right] + o\left(\frac{1}{s^2}\right),$$
$$s(\tau-Q)\ln y_2 = -\frac{(c+2)d}{s^2} + o\left(\frac{1}{s^2}\right),$$
$$Q\ln\left[\frac{1-y_2}{Q}\right] = \frac{d}{s^2}\ln\left[\frac{c+2}{d}\right] + o\left(\frac{1}{s^2}\right),$$
$$(\tau-Q)\ln y_2 = o\left(\frac{1}{s^2}\right).$$

Therefore,

$$\frac{\mathscr{A}(s+1,Q,\tau)}{\log_2 e} = \frac{d(d-c-2+(c+2)\ln[(c+2)/d])}{2s^2} + o\left(\frac{1}{s^2}\right).$$

Finally, the maximum value

$$\max_{c>0}\ \max_{c<d<c+2}\ \min\left\{d\left(d-c+c\ln\left[\frac{c}{d}\right]\right),\ d\left(d-c-2+(c+2)\ln\left[\frac{c+2}{d}\right]\right)\right\}$$

is at least $\frac{1}{2}$, that is attained at $c\to\infty$ and $d=c+1$. $\square$

D. Proofs of Analytical Lemmas

Proof of Lemma 2. Let $w \triangleq \lfloor qN \rfloor$. We will use the terminology of *types* [23]. Consider an arbitrary set of size k consisting of binary columns of height N and weight $\lfloor QN \rfloor$: $(\boldsymbol{x}(1),\ldots,\boldsymbol{x}(k))$, where $\boldsymbol{x}(i)\in\{0,1\}^N$, $\forall i\in[k]$. The set forms $(N\times k)$-matrix X_k. Let $\boldsymbol{u}\triangleq(u_1,\ldots,u_k)\in\{0,1\}^k$ is a row. Denote a *type* of the matrix X_k by $\{n(\boldsymbol{u})\}$, where $n(\boldsymbol{u})$, $0\le n(\boldsymbol{u})\le N$, is the number of rows $\boldsymbol{u}$ in the matrix X_k. Obviously, for any matrix X_k we have $\sum_{\boldsymbol{u}} n(\boldsymbol{u}) = N$. By $n(\boldsymbol{0})$ ($n(\boldsymbol{1})$) denote the number of the rows in X_k consisting of all zeros (ones). It allows to represent the probability (25) as follows:

$$P_k^N(Q,w) = \binom{N}{\lfloor QN \rfloor}^{-k} \cdot \sum_{(34)} \frac{N!}{\prod_{\boldsymbol{u}} n(\boldsymbol{u})!}, \tag{33}$$

where the sum is taken over all types $\{n(\boldsymbol{u})\}$ such that

$$\sum_{\boldsymbol{u}} n(\boldsymbol{u}) = N, \qquad n(\boldsymbol{0}) = N-w, \tag{34}$$
$$\sum_{\boldsymbol{u}:u_i=1} n(\boldsymbol{u}) = \lfloor QN \rfloor \quad \text{for any } i\in[k]. \tag{35}$$

Denote the logarithmic asymptotics of the probability (33) by

$$\mathscr{A}(k,Q,q) \triangleq \lim_{N\to\infty} \frac{-\log_2 P_k^N(Q,\lfloor qN \rfloor)}{N}, \quad Q<q<\min\{1,kQ\}. \tag{36}$$

Let $N\to\infty$. For every type $\{n(\boldsymbol{u})\}$, consider the corresponding distribution $\rho:\rho(\boldsymbol{u}) = \frac{n(\boldsymbol{u})}{N}$, $\forall \boldsymbol{u}\in\{0,1\}^k$. Applying the Stirling's approximation, we obtain the following logarithmic asymptotic behavior of the summand in the sum (33):

$$-\log_2 \frac{N!}{\prod_{\boldsymbol{u}} n(\boldsymbol{u})!}\binom{N}{\lfloor QN \rfloor}^{-k} = NF(\rho,Q,q)(1+o(1)), \quad \text{where}$$

$$F(\rho,Q,q) = \sum_{\boldsymbol{u}} \rho(\boldsymbol{u})\log_2\rho(\boldsymbol{u}) + k\cdot h(Q). \tag{37}$$

Thus, to calculate $\mathscr{A}(k,Q,q)$ one needs to find the following minimum:

$$\mathscr{A}(k,Q,q) = \min_{\rho\in(39):(40)} F(\rho,Q,q), \tag{38}$$

$$\left\{\rho:\ \forall\ \boldsymbol{u}=(u_1,\ldots,u_k)\in\{0,1\}^k \quad 0<\rho(\boldsymbol{u})<1\right\}, \tag{39}$$

$$\sum_{\boldsymbol{u}} \rho(\boldsymbol{u}) = 1, \qquad \rho(\boldsymbol{0}) = 1-q, \qquad \sum_{\boldsymbol{u}:u_i=1} \rho(\boldsymbol{u}) = Q \quad \forall\ i\in[k], \tag{40}$$

where restrictions (40) are induced by (34).

To find the extremal distribution ρ we apply the standard Lagrange multipliers method. Consider the Lagrangian:

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

The necessary conditions for the extremal distribution are

$$\begin{cases} \frac{\partial \Lambda}{\partial \rho(\boldsymbol{0})} = \log_2 \rho(\boldsymbol{0}) + \log_2 e + \lambda_0 + \lambda_{k+1} = 0, \\ \frac{\partial \Lambda}{\partial \rho(\boldsymbol{u})} = \log_2 \rho(\boldsymbol{u}) + \log_2 e + \lambda_{k+1} + \sum_{i=1}^{k} u_i \lambda_i = 0 \quad \forall \boldsymbol{u} \neq \boldsymbol{0}. \end{cases} \tag{41}$$

It is obvious that the matrix of second derivatives of the Lagrangian is diagonal, so this matrix is positive definite in the domain (39). Therefore [24], $F(\rho, Q)$ is strictly $\cup$-convex in the domain (39) and any local minimum is also a global minimum.

Recall that the Karush-Kuhn-Tacker theorem [24] states that every solution $\rho \in (39)$ is a local minimum of $F(\rho, Q)$ if it satisfies the restrictions (40) and the system (41) and has the positive definite matrix of second derivatives of the Lagrangian in this point ρ. Hence, if there exists a solution of (40) and (41) in the domain (39), then this solution is a unique and is a solution of the minimization problem (38)-(40).

Note that the symmetry of the problem yields equality: $\eta \triangleq \lambda_1 = \lambda_2 = \cdots = \lambda_k$. To prove this, we need to check that $\lambda_i = \lambda_j$ for $i \neq j$. Let $\bar{\boldsymbol{u}}_i \triangleq (0, \ldots, 1, \ldots, 0)$ be a row of length k, which has 1 at the i-th position and 0's at the other positions. A permutation of indices i and j leads to an equivalent problem. Hence, if ρ_1 is a solution, then ρ_2 is also a solution, where $\rho_2(\boldsymbol{u}) \triangleq \rho_1(\tilde{\boldsymbol{u}})$ and $\tilde{\boldsymbol{u}}$ is a row, obtained by permutation of indices i and j from the row $\boldsymbol{u}$. The uniqueness of the solution ρ implies that the distribution ρ_1 coincides with the distribution ρ_2. In particular, $\rho_1(\bar{\boldsymbol{u}}_i) = \rho_2(\bar{\boldsymbol{u}}_i) = \rho_1(\bar{\boldsymbol{u}}_j)$. From the second equation of (41), it follows that $\lambda_i = \lambda_j$.

Introduce parameters $\mu \triangleq \log_2 e + \lambda_{k+1}$ and $\nu \triangleq \lambda_0$. The equations (40) and (41) can be represented as follows:

$$\begin{cases} 1)\ \log_2 \rho(\boldsymbol{u}) + \mu + \eta \sum_{i=1}^{k} u_i = 0 \quad \forall \boldsymbol{u} \neq \boldsymbol{0}, \\ 2)\ \log_2 \rho(\boldsymbol{0}) + \mu + \nu = 0, \\ 3)\ \rho(\boldsymbol{0}) = 1 - q, \\ 4)\ \sum_{\boldsymbol{u}} \rho(\boldsymbol{u}) = 1, \\ 5)\ \sum_{\boldsymbol{u}: u_i = 1} \rho(\boldsymbol{u}) = Q \quad \forall i \in [k]. \end{cases} \tag{42}$$

After replacement of η by $y \triangleq \frac{1}{1+2^{-\eta}}$ the 1st equation of (42) becomes

$$\rho(\boldsymbol{u}) = \frac{1}{2^\mu y^k} (1-y)^{\sum u_j} y^{k - \sum u_j} \quad \forall \boldsymbol{u} \neq \boldsymbol{0}. \tag{43}$$

Substitution of (43) into 5th equation of (42) gives

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

Therefore, one can derive

$$\mu = \log_2 \frac{1-y}{Q y^k}. \tag{44}$$

Substitution of (43), (44) and 3rd equation of (42) into 4th equation of (42) leads to

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

i.e., the equation (5). Thus, restrictions (40) and conditions (41) give a unique solution ρ in the domain (39):

$$\rho(\boldsymbol{0}) = 1 - q, \qquad \rho(\boldsymbol{u}) = \frac{Q}{1-y} (1-y)^{\sum u_j} y^{k - \sum u_j} \quad \forall \boldsymbol{u} \neq \boldsymbol{0}, \tag{45}$$

where parameters q and y are related by (5). To obtain formula (4) it is sufficient to substitute (45) into (37). $\square$

Proof of Lemma 3. First, note that the function $q(y)$ defined by (5) is increasing in the interval $y \in (0,1)$, and $q(0) = Q$ and $\lim q(y) = sQ$ as $y \to 1^-$. Therefore, it suffices to prove that there is only one local minimum of the function $\mathscr{T}(k, Q, y) = \mathscr{A}(k, Q, q(y))$ of parameter y on the interval $y \in (0, y_1)$, where $q(y_1) = \min\{1, sQ\}$. The derivative of $\mathscr{T}(k, Q, y)$ with respect to y equals

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

Therefore, the function $\mathscr{T}(k, Q, y)$ decreases in $y \in (0, 1-Q)$, increases in $y \in (1-Q, y_1)$ and attains its minimum 0 at the point $y_0 = 1 - Q$. Note that $y < 1 - Q$ is equivalent to $q < 1 - (1-Q)^k$ because $q(y)$ is an increasing function. The first statement is proved. To prove the second statement it is sufficient to calculate the derivative of $\mathscr{A}(k, Q, y)$ with respect to Q:

$$\frac{\partial \mathscr{A}(k, Q, y)}{\partial Q} = k \log_2 \left[\frac{(1-y)(1-Q)}{yQ} \right].$$

This derivative is positive if and only if $Q < 1 - y$ which is equivalent to $Q > 1 - (1-q)^{1/k}$. So, the second statement holds. $\square$

References

[1] A. D'yachkov, I. Vorobyev, N. Polyanskii, and V. Shchukin, "Hypothesis test for upper bound on the size of random defective set," in *Proc. of the IEEE Int. Symposium on Inform. Theory (ISIT)*, 2017, pp. 978–982.

[2] R. Dorfman, "The detection of defective members of large populations," *Ann. Math. Stat.*, vol. 14, no. 4, pp. 436–440, 1943.

[3] D.-Z. Du and F. K. Hwang, *Combinatorial Group Testing and Its Applications*, 2nd ed., ser. Series on Applied Mathematics. World Scientific Publishing Co., 2000, vol. 12.

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

[5] W. Kautz and R. Singleton, "Nonrandom binary superimposed codes," *IEEE Trans. Inform. Theory*, vol. 10, no. 4, pp. 363–377, 1964.

[6] A. G. D'yachkov and V. V. Rykov, "Bounds on the length of disjunctive codes," *Probl. Inf. Transm.*, vol. 18, no. 3, pp. 166–171, 1982.

[7] M. Aldridge, L. Baldassini, and O. Johnson, "Group testing algorithms: bounds and simulations," *IEEE Trans. Inform. Theory*, vol. 60, no. 6, pp. 3671–3687, 2014. [Online]. Available: https://doi.org/10.1109/TIT.2014.2314472

[8] M. Aldridge, O. Johnson, and J. Scarlett, "Performance of group testing algorithms with near-constant tests-per-item," *arXiv preprint*, 2017. [Online]. Available: http://arxiv.org/pdf/1612.07122v2

[9] J. Scarlett and V. Cevher, "Limits on support recovery with probabilistic models: an information-theoretic framework," *IEEE Trans. Inform. Theory*, vol. 63, no. 1, pp. 593–620, 2017. [Online]. Available: https://doi.org/10.1109/TIT.2016.2606605

[10] T. Wadayama, "Nonadaptive group testing based on sparse pooling graphs," *IEEE Trans. Inform. Theory*, vol. 63, no. 3, pp. 1525–1534, 2017. [Online]. Available: https://doi.org/10.1109/TIT.2016.2621112

[11] A. Agarwal, S. Jaggi, and A. Mazumdar, "Novel impossibility results for group-testing," *arXiv preprint*, 2018. [Online]. Available: http://arxiv.org/pdf/1801.02701v2

[12] M. Aldridge, "Individual testing is optimal for nonadaptive group testing in the linear regime," *arXiv preprint arXiv:1801.08590*, 2018. [Online]. Available: http://arxiv.org/pdf/1801.08590v1

[13] T. Berger and V. I. Levenshtein, "Asymptotic efficiency of two-stage disjunctive testing," *IEEE Trans. Inform. Theory*, vol. 48, no. 7, pp. 1741–1749, 2002. [Online]. Available: https://doi.org/10.1109/TIT.2002.1013122

[14] M. M'ezard and C. Toninelli, "Group testing with random pools: optimal two-stage algorithms," *IEEE Trans. Inform. Theory*, vol. 57, no. 3, pp. 1736–1745, 2011. [Online]. Available: https://doi.org/10.1109/TIT.2010.2103752

[15] A. Sharma and C. R. Murthy, "On finding a subset of non-defective items from a large population," *IEEE Transactions on Signal Processing*, vol. 66, no. 21, pp. 5762–5775, 2018.

[16] P. Damaschke and A. Sheikh Muhammad, "Competitive group testing and learning hidden vertex covers with minimum adaptivity," *Discrete Math. Algorithms Appl.*, vol. 2, no. 3, pp. 291–311, 2010. [Online]. Available: https://doi.org/10.1142/S179383091000067X

[17] Y. Polyanskiy, "A perspective on massive random-access," in *Proc. of the IEEE Int. Symposium on Inform. Theory (ISIT)*, 2017, pp. 2523–2527.

[18] A. G. D'yachkov, A. J. Macula, and V. V. Rykov, "New constructions of superimposed codes," *IEEE Trans. Inform. Theory*, vol. 46, no. 1, pp. 284–290, 2000. [Online]. Available: https://doi.org/10.1109/18.817530

[19] A. G. D'yachkov, V. V. Rykov, and A. M. Rashad, "Superimposed distance codes," *Problems Control Inform. Theory*, vol. 18, no. 4, pp. 237–250, 1989.

[20] M. Falahatgar, A. Jafarpour, A. Orlitsky, V. Pichapati, and A. T. Suresh, "Estimating the number of defectives with group testing," in *Proc. of the IEEE Int. Symposium on Inform. Theory (ISIT)*, 2016, pp. 1376–1380.

[21] A. G. D'yachkov, I. V. Vorob'ev, N. A. Polyansky, and V. Y. Shchukin, "Almost disjunctive list-decoding codes," *Probl. Inf. Transm.*, vol. 51, no. 2, pp. 110–131, 2015. [Online]. Available: https://doi.org/10.1134/S0032946015020039

[22] A. De Bonis, "Constraining the number of positive responses in adaptive, non-adaptive, and two-stage group testing," *J. Comb. Optim.*, vol. 32, no. 4, pp. 1254–1287, 2016. [Online]. Available: https://doi.org/10.1007/s10878-015-9949-8

[23] I. Csiszar and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, 2011.

[24] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.