

Hypothesis Test for Bounds on the Size of Random Defective Set

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

Abstract—The conventional model of disjunctive group testing assumes that there are several defective elements (or defectives) among a large population, 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 the hypothesis H_0 : the number of defectives $\leq s_1$ against the alternative hypothesis H_1 : the number of defectives $\geq s_2$. We introduce a new decoding algorithm based on the comparison of the number of tests having positive responses with an appropriate fixed threshold. For some asymptotic regimes on s_1 and s_2 , the proposed algorithm is shown to be order-optimal. Additionally, our simulation results verify the advantages of the proposed algorithm such as low complexity and a small error probability compared with known algorithms.

Index Terms—Compressed sensing, parameter estimation, error probability, sparse matrices.

I. INTRODUCTION

GROUP testing, also known as Boolean compressed sensing [1], is a method for identifying a group of elements with some distinguishable characteristic, frequently referred to as defectives, from a large population. The main point of the group testing approach is that for a relatively small number of defectives, one can reduce the required number of experiments by testing subgroups of elements rather than all individuals separately. The idea of group testing was introduced by R. Dorfman [2]. He 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 a way that

Manuscript received February 12, 2019; revised June 20, 2019 and August 1, 2019; accepted August 24, 2019. Date of publication September 9, 2019; date of current version October 22, 2019. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Byonghyo Shim. The work of N. Polyanskii was supported by the Russian Foundation for Basic Research (RFBR) under Grants 18-07-01427 and 18-31-00310. The work of I. Vorobyev was supported by the RFBR under Grant 18-07-01427 and 18-31-00361. This paper was presented in part at the IEEE International Symposium on Information Theory, Aachen, Germany, June 2017. (Corresponding author: Nikita Polyanskii.)

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).

Digital Object Identifier 10.1109/TSP.2019.2940120

the successive groups depend on the results of the previous tests. Such a setting is called adaptive. However, nonadaptive procedures turn out to be useful for practice purposes. A nonadaptive scheme is a series of N group tests that are carried out simultaneously. This is the essential advantage for the most important applications [3] such as DNA library screening [4], compressive sensing [5], medical testing [2]. So, the design and analysis of group testing algorithms remain an active ongoing area of research.

A. Related Work

The group testing literature may be divided into two categories based on how the number of defectives is modeled. First, let us discuss combinatorial group testing, i.e., the number of defectives, or an upper bound on the number of defectives, is fixed and assumed to be known in advance. Let t be the total number of elements and $\mathcal{S}, \mathcal{S} \subset [t]$, be an unknown subset of defectives. The classic group testing problem assumes that the number of defectives $|\mathcal{S}|$ is upper bounded by some known fixed constant s , where the parameter s does not depend on t . In this regime, the main attention is devoted to disjunctive s -codes [6], which allow finding all the defective elements (a formal definition of disjunctive codes will be given in the next section). A specific group testing problem was discussed in [7], where the authors used group tests to identify a given number of non-defective items from a large population containing s defective items. A more general assumption in combinatorial group testing is that the number of defectives is relatively small, i.e., $\lim_{t \rightarrow \infty} \frac{|\mathcal{S}|}{t} = 0$. For example, the regime $|\mathcal{S}| = t^\alpha$, $0 < \alpha < 1$, was studied in the recent works [8]–[10]. Some studies [5], [11] use random test designs, and develop computationally efficient algorithms for identifying defective items from the test outcomes by exploiting the bit-mixing coding and the connection with compressed sensing.

Many other authors consider the settings when the number of defectives is unknown. For instance, in the original paper [2], each element in the population is assumed to be defective with some fixed probability p . The same model was discussed in the recent papers [12], [13], where the authors focused on nonadaptive schemes and studied algorithms allowing vanishing error probability as $t \rightarrow \infty$. A more general model in which $p = p(t)$ depends on t was considered in paper [14] of T. Berger and V. Levenshtein. They studied so-called 2-stage testing schemes which find all defectives without error. They proposed to run a fixed number of nonadaptive tests at the first stage and to test potential candidates individually at the second stage.

For some dependencies $p(t)$, the lower and upper bounds on the asymptotics of the expected number of tests in the described 2-stage scheme were obtained in [14], [15].

Now let us refer to the most relevant papers to our work. We first highlight the work of Y. Cheng [16], where the number of defective items can be found with a small error probability using adaptive testing. In [17], the authors developed a four-stage adaptive algorithm, which finds the approximate size of the defective set with high probability. One interesting approach to finding the defective set of unknown size was proposed by P. Damaschke and A.S. Muhammad in [18]. In the beginning, one should estimate the number of defectives $|\mathcal{S}|$ with the help of group tests, and then it remains to use one of the well-known algorithms for finding the defective set \mathcal{S} of the estimated size. We also mention a concept of strict group testing [19], where the searcher must find the defective set when its size is at most s or indicate that the size of the defective set is larger than s . Further details (in particular, the number of tests) for the existing works will be given in Section III.

B. Our Contribution

We consider a model without making any assumptions on the distribution of the number of the subject population, but instead, we focus on modeling the number of defectives using an arbitrary distribution. Our work aims to discuss testing the hypothesis H_0 : the random number of defectives is upper bounded by s_1 against the alternative hypothesis H_1 : the random number of defectives is at least s_2 . The main contributions of this work are two-fold. First, we introduce a new simple testing strategy that uses random tests and compares the number of positive outcomes with an appropriate fixed threshold in order to choose the most likely hypothesis. This low-complexity algorithm can be used for different testing scenarios in practice. Second, we derive closely matching lower and upper bounds on the number of tests required for testing the hypothesis with a small error probability. For instance, our proposed algorithm is shown to be order-optimal when s_1 and s_2 are asymptotically the same up to a multiplicative constant.

C. Application

We describe a possible application of our research in terms of sparse signal models. A signal model is said to be sparse if the number of input variables contributing to the observed outcome (the set of defectives) is relatively small. The study of such models is a new area primarily stimulated by the study of social, computer networks, transportation, power-line. Since most real systems are large and sparse, there are special models developed to understand and analyze them. For consistency of estimation and model prediction, almost all existing methods of variable/feature selection critically depend on the sparsity of models. When this parameter is unknown, we need (at least) to bound the sparsity in the model. Therefore, testing the hypothesis on the size of the defective set can be seen as a preprocessing step for analysis of real-life systems.

Numerous procedures in biology, medicine and functional genomics require that some bacteria and cells be counted.

More frequently, one needs to know only the cell concentration or the concentration of various macromolecules within one or multiple cells in an organism (for example, between 10^3 and 10^4 cells per milliliter, or large than 10^{10} molecules per cell). Therefore, testing the hypothesis can give crucial information regarding the progress of an infectious disease, or a person's immune system, or the genomic features of different organisms.

D. Outline

The remainder of this paper is organized as follows. In Section II, we introduce notation and a hypothesis testing model and give some basic definitions and a conventional algorithm used in group testing. Section III discusses the most relevant results in more detail. We summarize our results in Section IV. Section V is devoted to simulations of the hypothesis testing problem and comparing different algorithms. The detailed proofs of the main results will be given in Section VI. Finally, we conclude the paper with Section VII.

II. PROBLEM SETUP

We introduce several useful notation in Section II-A, describe a general non-adaptive group testing model in Section II-B, give the definition of the most conventional codes for group testing in Section II-C and discuss a hypothesis testing model we wish to investigate in Section II-D.

A. Notation

Throughout the paper we adopt the following notation. Let the symbol \triangleq denote the equality by definition and the symbol $\mathbf{u} \vee \mathbf{v}$ denote the disjunctive (Boolean) sum of binary columns $\mathbf{u}, \mathbf{v} \in \{0, 1\}^N$. We say that a column \mathbf{u} covers a column \mathbf{v} if $\mathbf{u} \vee \mathbf{v} = \mathbf{u}$.

For some function $f(x)$ and $g(x)$, we write $f(x) = O(g(x))$ and $f(x) = \Omega(g(x))$ as $x \rightarrow \infty$ if there exists some real x_0 and C such that $|f(x)| \leq C|g(x)|$ and $|f(x)| \geq C|g(x)|$ for $x \geq x_0$, respectively. If both equalities $f(x) = O(g(x))$ and $f(x) = \Omega(g(x))$ hold, then we use notation $f(x) = \Theta(g(x))$. Finally, we write $f(x) = o(g(x))$ as $x \rightarrow \infty$ if $|f(x)| \leq \varepsilon(x)|g(x)|$ for some function $\varepsilon(x)$ such that $\varepsilon(x) \rightarrow 0$ as $x \rightarrow \infty$.

B. Non-Adaptive Group Testing Model

In the classical problem of non-adaptive group testing, we describe N tests as a binary matrix (code) $X \in \{0, 1\}^{N \times t}$, where the j th column, denoted by $\mathbf{x}(j)$, corresponds to the j th element, and the i th row, abbreviated by \mathbf{x}_i , corresponds to the i th test. X is often referred to as a testing matrix. Let $x_i(j)$ be the (i, j) th element in X and $x_i(j) \triangleq 1$ if and only if the j th element is included into the i th testing group. Let $\mathcal{S}, \mathcal{S} \subseteq [t]$, be an arbitrary set of defective elements of size $|\mathcal{S}|$. For a code X and a set \mathcal{S} , define the binary response vector $\mathbf{x}(\mathcal{S})$ of length N , namely:

$$\mathbf{x}(\mathcal{S}) \triangleq \begin{cases} \bigvee_{j \in \mathcal{S}} \mathbf{x}(j) & \text{if } \mathcal{S} \neq \emptyset, \\ (0, 0, \dots, 0)^T & \text{if } \mathcal{S} = \emptyset. \end{cases}$$

The result of a test equals 1 if at least one defective element is included into the corresponding test and 0 otherwise. So the column of test results is equal to the response vector $\mathbf{x}(\mathcal{S})$.

C. Disjunctive Codes and the Conventional Decoding Algorithm

Now let us give the definition of disjunctive (binary superimposed) codes introduced in [6].

Definition 1: A binary code X is called a *disjunctive s-code* 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.

Definition 1 of disjunctive codes gives the important sufficient condition for identification of any unknown defective set, namely, one can recover all the defectives based on the response vector if the number of defective elements is at most s . In the case of disjunctive s -codes, the identification of the unknown set \mathcal{S} is equivalent to searching all columns of matrix X covered by $\mathbf{x}(\mathcal{S})$, and its complexity is equal to $\Theta(Nt)$ (we run over all t columns in X and compare the covering property of the columns with the response vector of length N). This conventional algorithm of finding defectives is called *COMP (Combinatorial Optimal Matching Pursuit)* [8]. We refer the reader to [20] for a survey on decoding algorithms used in group testing.

D. Hypothesis Testing Model

Given integers s_1 and s_2 so that $s_1 < s_2$, we introduce two hypothesis:

- 0) the null hypothesis $\{H_0 : |\mathcal{S}| \leq s_1\}$,
- 1) the alternative hypothesis $\{H_1 : |\mathcal{S}| \geq s_2\}$.

In other words, we want to distinguish reliably two events: the number of defective elements is at most s_1 or at least s_2 . We consider testing the hypothesis using group tests in the probabilistic model in which the random defective sets of the same size are equiprobable. This assumption is reasonable when there is no prior knowledge on the location of defective elements among the population. In fact, most of the papers in literature discuss such a scenario; e.g., see [2], [17], [21], [22].

More accurately, let us define the probability distribution of the random defective set \mathcal{S} using the vector

$$\mathbf{p} \triangleq (p_0, p_1, \dots, p_t), \quad p_k \geq 0, \quad k = 0, 1, \dots, t, \quad \sum_{k=0}^t p_k = 1,$$

in the following manner

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

Here, p_i corresponds to the probability that there are i defective elements among the population of size t . Since there are $\binom{t}{i}$ choices to locate i items in the population of size t , the equation (1) does set the probability distribution. Let us provide a few examples of possible probability distributions.

Example 1: In [21], the authors consider a truncated Poisson distribution $\text{Pois}(t, \lambda)$ and motivate that by the experience in clinical testing. In other words, the probability distribution \mathbf{p} is

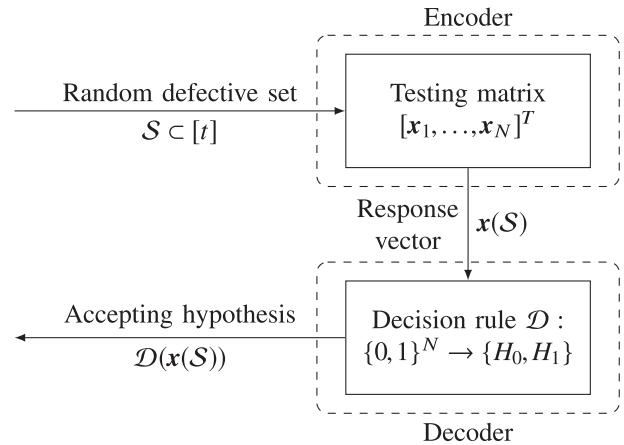


Fig. 1. Hypothesis testing model.

defined as follows

$$\mathbf{p} = (p_0, p_1, \dots, p_t), \quad p_i = \frac{e^{-\lambda} \lambda^i}{i! m}, \quad m = \sum_{i=0}^t \frac{e^{-\lambda} \lambda^i}{i!}.$$

However, the most popular assumption in group testing is that the vector \mathbf{p} has a Binomial distribution $B(t, p)$, that is

$$\mathbf{p} = (p_0, p_1, \dots, p_t), \quad p_i = p^i (1-p)^{t-i} \binom{t}{i}.$$

We note that the probability of the null hypothesis and the alternative hypothesis can be expressed with the help of the vector \mathbf{p} as follows

$$\Pr\{H_0\} = \sum_{i=0}^{s_1} p_i, \quad \Pr\{H_1\} = \sum_{i=s_2}^t p_i.$$

However, the vector \mathbf{p} can be unknown to the searcher. Therefore, we must use some tolerant approach. Let us give some key definitions for hypothesis testing and depict the corresponding model in Fig. 1.

Definition 2: An arbitrary map $\mathcal{D} : \{0, 1\}^N \rightarrow \{H_0, H_1\}$ is said to be a *decision rule*, which associates a response vector with some hypothesis. Introduce the error probability for the decision rule \mathcal{D} and the testing matrix X :

$$\begin{aligned} \varepsilon_{s_1}^{s_2}(\mathbf{p}, \mathcal{D}, X) &\triangleq \max \left\{ \Pr\{\text{accept } H_1 | H_0\}, \right. \\ &\quad \left. \Pr\{\text{accept } H_0 | H_1\} \right\}, \end{aligned} \quad (2)$$

where the probability measure in the conditional probabilities is defined by (1). The *universal error probability* is defined by

$$\varepsilon_{s_1}^{s_2}(\mathcal{D}, X) \triangleq \max_{\mathbf{p}} \varepsilon_{s_1}^{s_2}(\mathbf{p}, \mathcal{D}, X). \quad (3)$$

Later we shall omit indices s_1 and s_2 in notation $\varepsilon_{s_1}^{s_2}(\mathbf{p}, \mathcal{D}, X)$ and $\varepsilon_{s_1}^{s_2}(\mathcal{D}, X)$, whenever it is clear from the context.

Remark 1: Given the testing matrix X and the decision rule \mathcal{D} , we search for the worst probability distribution \mathbf{p} and the corresponding maximal error probability in (3). In other words, we would like to handle the worst-case scenario which may appear in practice.

Let us discuss one important example of hypothesis and a decision rule adopted from the COMP algorithm. Later we will concentrate on this hypothesis and compare this algorithm with one we suggest.

Example 2: Consider the case $s_1 = s$ and $s_2 = s + 1$, that is, we wish to decide whether the number of defective elements is smaller than $s + 1$. The COMP algorithm can be used for the hypothesis testing problem in the following way. We say that the COMP decision rule maps the vector $\mathbf{y} \in \{0, 1\}^N$ to H_0 if the number of columns in X covered by \mathbf{y} is at most s and to H_1 otherwise.

For instance, let the testing matrix X and two possible response vectors \mathbf{y}_1 and \mathbf{y}_2 be as follows

$$X = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad \mathbf{y}_1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad \mathbf{y}_2 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}.$$

For $s = 2$, the null hypothesis H_0 says that the number of defectives is at most 2, whereas H_1 — the number of defectives is at least 3. If \mathbf{y}_1 is the response vector, then the COMP decision rule accepts H_0 (there are two columns, $\mathbf{x}(2)$ and $\mathbf{x}(3)$, covered by \mathbf{y}_1). If \mathbf{y}_2 is the response vector, then the COMP decision rule accepts H_1 (there are three columns, $\mathbf{x}(2)$, $\mathbf{x}(4)$ and $\mathbf{x}(5)$, covered by \mathbf{y}_2).

One natural question for testing the hypothesis appears to be as follows. Given the size of population t , the error probability level ε and two thresholds s_1 and s_2 , how to minimize the number of tests in a $(N \times t)$ testing matrix X to achieve the universal error probability $\varepsilon(\mathcal{D}, X)$ of level at most ε . We derive lower and upper bounds on the optimal number of tests required for this problem in Section IV. We carry out Monte-Carlo simulations to estimate the minimal number of tests required for certain hypothesis testing model in Section V.

III. RELATED RESULTS

First, we consider testing the hypothesis without error. After that, we outline some state-of-the-art papers on the estimation of the number of defectives with a small error probability. Then we recall some known results for the COMP decision rule used for hypothesis testing. Finally, we shortly discuss an opportunity to apply the likelihood ratio test for this problem.

A. Zero-Error Hypothesis Testing

Let us consider the case $s_1 = s$ and $s_2 = s + 1$. Suppose one wishes to decide whether the number of defectives is smaller than $s + 1$ without error, i.e., $\varepsilon(\mathcal{D}, X) = 0$ for some decision rule \mathcal{D} and testing matrix X . The problem of optimal zero-error nonadaptive hypothesis testing is reduced to the problem of optimal disjunctive codes with the help of the following statement. This proposition turns out to be a group testing folklore result.

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

Proof: If X is a disjunctive s -code, then obviously the COMP decision rule allows us to check the hypothesis H_0 without error (see Example 2). The converse result can be proved by contradiction. Indeed, if the matrix X is not a disjunctive s -code, then there exists a set $\mathcal{S} \subseteq [t]$ of size $|\mathcal{S}| = s$, and a number $j \in [t] \setminus \mathcal{S}$ such that $\mathbf{x}(\mathcal{S}) = \mathbf{x}(\mathcal{S} \cup \{j\})$. So, for any decision rule we cannot distinguish the set \mathcal{S} of size s from the set $\mathcal{S} \cup \{j\}$ of size $s + 1$. ■

The best known practical constructions of disjunctive s -codes are based on shortened Reed Solomon codes. These constructions presented in [4] essentially extend optimal and suboptimal ones suggested in [6].

Recall some results for optimal disjunctive s -codes. Denote by $N(t, s)$ the minimal number of rows for disjunctive s -codes with t columns. The best known lower and upper bounds on $N(t, s)$ are presented in [23] and [24], respectively. These bounds are written in the complex form, but for fixed integer s , the asymptotics are as follows

$$\begin{aligned} N(t, s) &= O(s^2 \ln t) \quad \text{as } t \rightarrow \infty, \\ N(t, s) &= \Omega\left(\frac{s^2}{\ln s} \ln t\right) \quad \text{as } t \rightarrow \infty. \end{aligned}$$

B. Estimating the Number of Defectives With a Small Error Probability

Further we will consider the case of positive error probability. In [18] the authors present a randomized algorithm that uses $g(\varepsilon, c) \log_2 t$ nonadaptive tests (here, $g(\varepsilon, c)$ is a some function which depends only on c and ε) and produces some statistic \hat{s} which satisfies the following properties: probability $\Pr\{\hat{s} < |\mathcal{S}|\}$ is upper bounded by a small parameter $\varepsilon \ll 1$ and the expected value of $\hat{s}/|\mathcal{S}|$ 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 [25] the authors construct an adaptive randomized algorithm which uses at most $2 \log_2 \log_2 |\mathcal{S}| + O(\frac{1}{\delta^2} \log_2 \frac{1}{\varepsilon})$ adaptive tests and estimates $|\mathcal{S}|$ up to a multiplicative factor of $1 \pm \delta$ with error probability $\leq \varepsilon$. Also there is a converse result in [25] which states the necessity of $(1 - \varepsilon) \log_2 \log_2 |\mathcal{S}| - 1$ tests on average.

C. COMP Decision Rule for Hypothesis Testing

Let us consider the case $s_1 = s$ and $s_2 = s + 1$ again. 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 $\varepsilon(\mathbf{p}, \text{COMP}, X)$ in (3) is attained at any vector \mathbf{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 Proposition 4 about a similar statement which is given in Section IV and proved in Section VI-A. That is why the universal error probability $\varepsilon(\text{COMP}, X)$ 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 [22]. The properties of the universal error

probability $\varepsilon(\text{COMP}, X)$ obtained in [22] are presented below as Propositions 2 and 3.

Proposition 2. (*Follows from Theorem 2 in [22]*): Let $\varepsilon > 0$ be a fixed real scalar, and s, t be integers such that $s \leq t$. If X is an arbitrary code of size t such that the universal error probability for the COMP decision rule and the testing matrix X is less than ε , then length of the code X must be $N = \Omega(s \ln(t/s))$ as $t \rightarrow \infty$.

Remark 2: In other words, Proposition 2 says that to guarantee a vanishing error probability, the number of tests, accompanied with the COMP decision rule, should be linear with $\ln(t/s)$, the logarithm of the ratio between the size of the population and the number of defectives. It will be shown in Theorem 2 that for the hypothesis testing problem, the optimal number of tests does not depend asymptotically on the size t .

In [22], using the probabilistic method we established the existence result on the almost disjunctive codes. We interpret that results in terms of hypothesis testing.

Proposition 3. (*Follows from Theorem 4 in [22]*): Given real scalar $\varepsilon > 0$ and fixed integer $s > 0$, there exists a $(t \times N)$ testing matrix X with $N = O(s \ln t)$ tests such that the COMP decision rule provides the universal error probability less than ε .

Remark 3: Given fixed integer $s > 0$, by Propositions 2 and 3, the COMP decision rule needs $\Theta(s \ln t)$ tests to distinguish the null hypothesis H_0 : the number of defective elements is at most s from the alternative hypothesis H_1 : the number of defective elements is at least $s + 1$.

D. Alternative Decision Rule

For the case $s_2 = s_1 + 1$, one may try to use the generalized likelihood ratio test. Such a test has critical region $R := \{\mathbf{y} : \lambda(\mathbf{y}) \leq a\}$, where

$$\lambda(\mathbf{y}) := \frac{\max_{s \leq s_1} \Pr\{\mathbf{x}(\mathcal{S}) = \mathbf{y} | |\mathcal{S}| = s\}}{\max_{s \in [t]} \Pr\{\mathbf{x}(\mathcal{S}) = \mathbf{y} | |\mathcal{S}| = s\}}$$

is the generalized likelihood ratio and parameter a is chosen to satisfy requirements on $\Pr\{H_1 | H_0\}$. In other words, we accept H_1 when $\lambda(\mathbf{y}) \in R$. However, the decoding complexity of this rule is exponential with the number of items.

IV. MAIN RESULTS

Note that our hypothesis testing problem is very different from the finding the defectives because there are only two answers: H_0 or H_1 . However, in the zero-error case, due to Proposition 1 testing the hypothesis requires nearly the same number of group tests as the searching the defectives does. Our main results are devoted to hypothesis group testing in the case of a small error probability. First, we introduce a low-complexity weight decision rule which turns out to be better than the COMP decision rule in terms of the optimal number of tests. Then Proposition 4 shows that the worst probability distribution \mathbf{p} in (3) for the weight decision rule should be concentrated in only two points p_{s_1} and p_{s_2} . Finally we obtain lower and upper bounds on the optimal number of tests for the hypothesis testing problem in Section IV-C and Section IV-D, respectively. All the proofs will be given in Section VI.

A. Weight Decision Rule

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

$$\begin{cases} \text{accept } \{H_0 : |\mathcal{S}| \leq s_1\} & \text{if } |\mathbf{x}(\mathcal{S})| \leq \tau N, \\ \text{accept } \{H_1 : |\mathcal{S}| > s_2\} & \text{if } |\mathbf{x}(\mathcal{S})| > \tau N. \end{cases} \quad (4)$$

Remark 4: We note that the τ -weight decision rule is related to some model of specific disjunctive s -codes considered in [26]. The authors of that paper supply a disjunctive s -code with a weaker additional condition: the weight $|\mathbf{x}(\mathcal{S})|$ of the response vector for any subset \mathcal{S} , $\mathcal{S} \subseteq [t]$, $|\mathcal{S}| \leq s$, is at most T . Such a group testing model is motivated 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.

B. Worst-Case Probability Distribution for the Weight Decision Rule

We study only the universal error probability for the weight decision rule, and the following statement proved in Section VI-A determines the worst probability distribution in (3).

Proposition 4: For any integers $s_1, s_2 < t/2$, real scalar τ , $0 < \tau < 1$, and the testing $(N \times t)$ matrix X , the maximum of the error probability $\varepsilon(\mathbf{p}, \tau\text{-WDR}, X)$ in (3) is attained at any \mathbf{p} such that $p_{s_1} > 0$, $p_{s_2} > 0$ and $p_{s_1} + p_{s_2} = 1$.

C. Lower Bound on the Number of Tests

The next converse theorem derives the lower bound on the error probability for the worst distribution from Proposition 4 and any decision rule.

Theorem 1: Let the distribution \mathbf{p} be such that $p_{s_1} > 0$, $p_{s_2} > 0$ and $p_{s_1} + p_{s_2} = 1$. For any decision rule \mathcal{D} and any testing $(N \times t)$ matrix X with $N \leq s_1 \log_2(t/s_2)$, the error probability is lower bounded by

$$\varepsilon(\mathbf{p}, \mathcal{D}, X) \geq \frac{\left(2^{-\frac{N}{s_1}} t - s_1\right) \dots \left(2^{-\frac{N}{s_1}} t - s_2 + 1\right)}{2(t - s_1) \dots (t - s_2 + 1)}.$$

This lower bound consequently leads to the bound on the minimal number of tests for optimal testing strategy. We focus on two special cases: when two thresholds s_1 and s_2 are the same up to a multiplicative factor or an additive factor.

Corollary 1: Let $s_1 < s_2$ and $s_2 = o(t)$. For any $(N \times t)$ -code X and any decision rule \mathcal{D} with the universal error probability $\varepsilon(\mathcal{D}, X) \leq \varepsilon$, the number of non-adaptive group tests is lower bounded as follows

$$N \geq \min \left\{ s_1 \log_2(t/s_2), \frac{s_1}{s_2 - s_1} \log_2 \frac{1}{\varepsilon} (1 + o(1)) \right\}$$

as $\varepsilon \rightarrow 0$.

(a) Given the real number $\alpha > 1$, let $s_1 = s$ and $s_2 = \alpha s$. Then

$$N \geq \min \left\{ s_1 \log_2(t/s_2), \frac{1}{\alpha - 1} \log_2 \frac{1}{\varepsilon} (1 + o(1)) \right\}$$

as $\varepsilon \rightarrow 0$.

(b) Given the integer $c = o(s)$, let $s_1 = s$ and $s_2 = s + c$. Then

$$N \geq \min \left\{ s_1 \log_2(t/s_2), \frac{s}{c} \log_2 \frac{1}{\varepsilon} (1 + o(1)) \right\} \quad \text{as } \varepsilon \rightarrow 0.$$

D. Upper Bound on the Number of Tests

The next statement establishes an upper bound on the optimal number of tests. The testing matrix is constructed probabilistically, with the entries of the matrix being independent and Bernoulli distributed. We make use of the fact that a Binomial distribution is concentrated around its mean, with exponentially small tail.

Theorem 2: Given two thresholds s_1 and s_2 , real scalar $\varepsilon > 0$ and integer $t > 0$, for any integer $N \geq N_0$, there exists a testing $(N \times t)$ -matrix X such that the τ -weight decision rule provides the universal error probability $\varepsilon(X, \tau\text{-WDR})$ for testing the hypothesis H_0 against H_1 less than ε , where

$$\begin{aligned} N_0 &\triangleq \frac{1}{2\delta^2} \ln \frac{1}{\varepsilon}, \quad \tau \triangleq 1 - (1-p)^{s_1}/2 - (1-p)^{s_2}/2, \\ \delta &\triangleq (1-p)^{s_1}/2 - (1-p)^{s_2}/2, \quad p \triangleq \frac{\ln s_2 - \ln s_1}{s_2 - s_1}. \end{aligned}$$

(a) Given the real number $\alpha > 1$, let $s_1 = s$ and $s_2 = \alpha s$. Then

$$N_0 = \frac{2\alpha^{\frac{2\alpha}{\alpha-1}}}{(\alpha-1)^2} \ln \frac{1}{\varepsilon} (1 + o(1)) \quad \text{as } s \rightarrow \infty.$$

(b) Given the integer $c = o(s)$, let $s_1 = s$ and $s_2 = s + c$. Then

$$N_0 = \frac{2e^2 s^2}{c^2} \ln \frac{1}{\varepsilon} (1 + o(1)) \quad \text{as } s \rightarrow \infty.$$

Remark 5: Independence from the number of elements t is crucial in Theorem 2. In other words, we can construct a sequence of $(N \times t(N))$ matrices with exponentially decreasing error probability for any function $t(N)$. Due to Proposition 2 the number of tests should be linear with $\ln t$ whenever the error probability for the COMP decision rule is vanishing. Therefore, the weight decision rule has a significant advantage over the COMP decision rule when the size of the population is large.

Let us also mention a stronger bound from the conference paper [27] than one given in Theorem 2. This result has more narrow applications and is related to distinguishing the null hypothesis H_0 : the number of defective elements is at most s from the alternative hypothesis H_1 : the number of defective elements is at least $s + 1$. The proof of the following statement is quite technical and is based on the probabilistic method. We generate random codes with a fixed Hamming weight and derive an upper bound on the number of tests for hypothesis testing.

Theorem 3. (Theorem 3 in [27]): Given the real scalar $\varepsilon > 0$ and the integer t , for any integer $N \geq N_0$, there exists a testing $(N \times t)$ -matrix X with fixed weight wN such that the τ -weight decision rule provides the universal error probability $\varepsilon(X, \tau\text{-WDR})$ for testing the hypothesis H_0 against H_1 less than ε , where

$$\begin{aligned} N_0 &\triangleq 4s^2 \ln \frac{1}{\varepsilon} (1 + o(1)) \quad \tau \triangleq \frac{c}{s}, \\ w &\triangleq \frac{c}{s^2}, \quad c = o(s) \quad \text{as } s \rightarrow \infty. \end{aligned}$$

Remark 6: By Theorem 2 Claim (b), we need $2e^2 s^2 \ln \frac{1}{\varepsilon} \approx 14.8s^2 \ln \frac{1}{\varepsilon}$ tests to provide the error probability less than ε when testing whether the number of defectives is less than $s + 1$, whereas Theorem 3 guarantees that $4s^2 \ln \frac{1}{\varepsilon}$ tests are enough. Another advantage of Theorem 3 is that the testing matrix has a low density. Indeed, the relative weight of columns turns out to be of order $1/s^2$ (versus $1/s$ in Theorem 2). Therefore, for practical applications, we recommend to generate a constant-weight testing matrix with the relative Hamming weight of order $1/s^2$ to test the hypothesis that the number of defectives is at most s against the hypothesis that the number of defectives is at least $s + 1$.

V. SIMULATION

In this section, we first compare the weight decision rule and the COMP decision rule in a specific setting. Second, we estimate more carefully the minimum number of tests required for the weight decision rule to guarantee small error probability in the setting when the number of items can be arbitrary large and (i) $s_2 - s_1 = \Theta(1)$, (ii) $s_2 - s_1 = \Theta(\sqrt{s_1})$, (iii) $s_2 - s_1 = \Theta(s_1)$.

A. Comparison Between the COMP Decision Rule and the Weight Decision Rule

Now we carry out Monte Carlo simulations to find the minimal number of tests required for the COMP decision rule and the weight decision rule to guarantee the universal error probability less than the level $\varepsilon = 0.01$.

We test the hypothesis H_0 : the number of defectives is at most 2, against the hypothesis H_1 : the number of defectives is at least 3. To this end, for all $t \in \{8, 16, 32, \dots, 8192\}$, following Remark 6, we generate $(N \times t)$ binary matrices of some constant weight w with minimal possible N so that the universal error probability is less than ε . We generate matrices with different $w \in \{1, \dots, N/2\}$ and repeat the procedure 100 times for any given w and N to find a matrix with the universal error probability less than ε . To estimate the universal error probability of some testing matrix and some decision rule, we employ the Monte Carlo method, namely, subsets $S \subset [t]$, of size 2 and 3 are chosen randomly 10000 times and the corresponding error probability is estimated using (5)–(6). We depict our results in Fig. 2, where the x -axis corresponds to different t , number of items, and the y -axis corresponds to “optimal” N , number of tests. Additionally, a base-2 logarithmic scale is used for the x -axis. One can easily see the series of numbers of tests for the weight decision rule converges to some level as t is growing, whereas the number of tests for the COMP decision rule is linear with $\ln t$, the logarithm of the number of items.

The simulation results verify the advantage of the WDR over the COMP decision rule in pursuing the minimal possible number of tests. Also, we recall that the decoding complexity of the WDR decision rule is $\Theta(N)$, whereas the complexity of the COMP decision rule is significantly higher, namely, $\Theta(Nt)$.

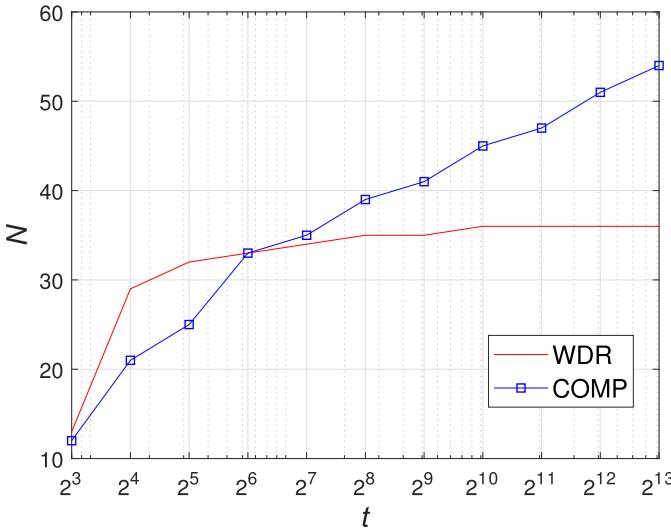


Fig. 2. “Optimal” number of tests for the COMP decision rule and the weight decision rule estimated by the Monte-Carlo simulation method.

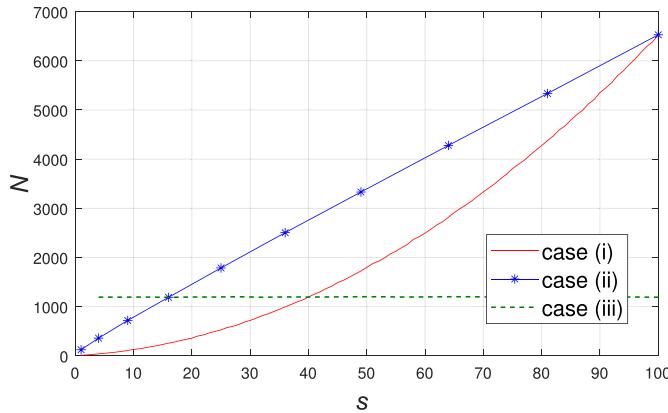


Fig. 3. Sufficient number of tests in a random testing matrix.

B. Weight Decision Rule When the Number of Items is Large

Now we consider the case when the number of items, denoted by t , can be arbitrary large. We apply the weight decision rule to test the hypothesis H_0 : the number of defectives is at most s , against the hypothesis H_1 : the number of defectives is at least (i) $s + 10$, (ii) $s + \sqrt{s}$, (iii) $1.25s$. Let the universal error probability be at most $\varepsilon = 0.001$. By Corollary 1 and Theorem 2 we know that the optimal number of tests in these regimes as $s \rightarrow \infty$ can be bounded as follows

- i) $9.9s = \frac{\varepsilon}{c} \log_2 \frac{1}{\varepsilon} \lesssim N \lesssim \frac{2e^2 s^2}{c^2} \ln \frac{1}{\varepsilon} = 1.02s^2$;
- ii) $9.9\sqrt{s} = \frac{\varepsilon}{c} \log_2 \frac{1}{\varepsilon} \lesssim N \lesssim \frac{2e^2 s^2}{c^2} \ln \frac{1}{\varepsilon} = 102s$;
- iii) $39.9 = \frac{1}{\alpha-1} \log_2 \frac{1}{\varepsilon} \leq N \lesssim \frac{2\alpha \frac{2\alpha}{\alpha-1}}{(\alpha-1)^2} \ln \frac{1}{\varepsilon} = 2058.7$.

For i) $s \in \{1, 2, 3, 4, \dots, 100\}$, ii) $s \in \{1, 4, 9, 16, \dots, 100\}$, iii) $s \in \{4, 8, 12, 16, \dots, 100\}$, we estimate the minimal number of tests in a random testing matrix with Bernoulli entries more carefully than in the proof of Theorem 2. More precisely, we compute probabilities (15)–(16) directly instead of applying Hoeffding's inequalities. The results are depicted in Fig. 3,

where the x -axis corresponds to different s , thresholds in the testing model, and the y -axis corresponds to the number of tests.

VI. PROOFS OF MAIN RESULTS

A. Proof of Proposition 4

Proof: For an arbitrary binary $(N \times t)$ -matrix X and parameters s_1, s_2 and $T \triangleq \lfloor \tau N \rfloor$, introduce the sets $B_k^i(T, X)$, $i = 1, 2$, $k = 0, 1, \dots, t$, of k -subsets of set $[t]$ as follows:

$$\begin{aligned} B_k^1(T, X) &\triangleq \left\{ \mathcal{S} : \mathcal{S} \subseteq [t], |\mathcal{S}| = k, |\mathbf{x}(\mathcal{S})| \geq T + 1 \right\}, \\ B_k^2(T, X) &\triangleq \left\{ \mathcal{S} : \mathcal{S} \subseteq [t], |\mathcal{S}| = k, |\mathbf{x}(\mathcal{S})| \leq T \right\}. \end{aligned} \quad (5)$$

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

$$\varepsilon(\mathbf{p}, \tau\text{-WDR}, X) \triangleq \max$$

$$\left\{ \sum_{k=0}^{s_1} \frac{p_k}{\sum_{l=0}^{s_1} p_l} \frac{|B_k^1(T, X)|}{\binom{t}{k}}, \sum_{k=s_2}^t \frac{p_k}{\sum_{l=s_2}^t p_l} \frac{|B_k^2(T, X)|}{\binom{t}{k}} \right\}. \quad (6)$$

For any $k < t$, $\mathcal{S} \in B_k^1(T, X)$, and $j \in [t] \setminus \mathcal{S}$, one can construct a set $\mathcal{S}' \triangleq \mathcal{S} \cup \{j\}$ belonging to $B_{k+1}^1(T, X)$. Since the number of choices for j is $(t - k)$ and there exist at most $(k + 1)$ ways leading to the same set $\mathcal{S}' \in B_{k+1}^1(T, X)$, we obtain the following inequality:

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

Applying such inequality $(s_1 - k)$ times, we obtain for any $k < s_1$

$$|B_{s_1}^1(T, X)| \geq \frac{s_1 \dots (k + 1)}{(t - s_1 + 1) \dots (t - k)} |B_k^1(T, X)|.$$

Equivalently, we have

$$\frac{|B_k^1(T, X)|}{\binom{t}{k}} \leq \frac{|B_{s_1}^1(T, X)|}{\binom{t}{s_1}}. \quad (7)$$

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

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

Thus, for any $k > s_2$, we have

$$\frac{|B_k^2(T, X)|}{\binom{t}{k}} \leq \frac{|B_{s_2}^2(T, X)|}{\binom{t}{s_2}}. \quad (8)$$

Definition (6) and inequalities (7)–(8) yield

$$\varepsilon(\mathbf{p}, \tau\text{-WDR}, X) \leq \max \left\{ \frac{|B_{s_1}^1(T, X)|}{\binom{t}{s_1}}, \frac{|B_{s_2}^2(T, X)|}{\binom{t}{s_2}} \right\}, \quad (9)$$

and equality holds in (9) for any distribution with the properties: $p_{s_1} > 0$, $p_{s_2} > 0$, and $p_j = 0$ for $j \in [t] \setminus \{s_1, s_2\}$. In particular, it means that for τ -WDR the definition of the universal error probability (3) is equivalent to the right-hand side of (9). ■

B. Proof of Theorem 1

Proof: Let an $(N \times t)$ -matrix X be a testing matrix, $\mathcal{D} : \{0, 1\}^N \rightarrow \{H_0, H_1\}$ be a decision rule and \mathbf{p} be a distribution so that $p_{s_1} > 0$, $p_{s_2} > 0$ and $p_j = 0$ for any $j \in [t] \setminus \{s_1, s_2\}$. Obviously, the maximal error probability (2) is bounded below by the half of the sum:

$$\varepsilon(\mathbf{p}, \mathcal{D}, X) \geq \frac{1}{2} (\Pr\{\text{accept } H_1 | H_0\} + \Pr\{\text{accept } H_0 | H_1\}). \quad (10)$$

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

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

Since the distribution of \mathbf{p} is concentrated in only two coordinates p_{s_1} and p_{s_2} , we can rewrite the right-hand side of (10) as follows

$$\begin{aligned} \varepsilon(\mathbf{p}, \mathcal{D}, X) &\geq \frac{1}{2} \sum_{\mathbf{y} \in \{0, 1\}^N} \left(\frac{n_{s_1}(\mathbf{y}, X)}{\binom{t}{s_1}} \mathbb{1}\{\mathcal{D}(\mathbf{y}) \neq H_0\} \right. \\ &\quad \left. + \frac{n_{s_2}(\mathbf{y}, X)}{\binom{t}{s_2}} \mathbb{1}\{\mathcal{D}(\mathbf{y}) \neq H_1\} \right). \end{aligned} \quad (11)$$

One of the two indicators $\mathbb{1}\{\mathcal{D}(\mathbf{y}) \neq H_0\}$, $\mathbb{1}\{\mathcal{D}(\mathbf{y}) \neq H_1\}$ equals 0 and the other one equals 1. Therefore

$$\varepsilon(\mathbf{p}, \mathcal{D}, X) \geq \frac{1}{2} \sum_{\mathbf{y} \in \{0, 1\}^N} \min \left\{ \frac{n_{s_1}(\mathbf{y}, X)}{\binom{t}{s_1}}, \frac{n_{s_2}(\mathbf{y}, X)}{\binom{t}{s_2}} \right\}. \quad (12)$$

Further we consider only such \mathbf{y} 's that $n_{s_1}(\mathbf{y}, X) > 0$. It is obvious that for other \mathbf{y} 's the minimum in the sum (12) equals 0. Denote the relative number of s_1 -subsets with the response vector \mathbf{y} by β_y , i.e., $\beta_y \triangleq n_{s_1}(\mathbf{y}, X)/\binom{t}{s_1}$, and note that

$$\begin{aligned} n_{s_1}(\mathbf{y}, X) &= \beta_y \binom{t}{s_1} = \beta_y \frac{(t - s_1 + 1) \dots t}{s_1!} \\ &\geq \frac{(\beta_y^{\frac{1}{s_1}} t - s_1 + 1) \dots (\beta_y^{\frac{1}{s_1}} t)}{s_1!} = \binom{\beta_y^{\frac{1}{s_1}} t}{s_1} \end{aligned}$$

because $0 < \beta_y \leq 1$. By \mathcal{S}_y denote a set of all column's indices which are included into some s_1 -subset \mathcal{S} so that the response vector $\mathbf{x}(\mathcal{S}) = \mathbf{y}$, i.e.,

$$\mathcal{S}_y = \bigcup_{\mathcal{S}: \mathbf{x}(\mathcal{S})=\mathbf{y}} \mathcal{S},$$

and suppose that $|\mathcal{S}_y| = s_1 + L$ for some integer L . The previous inequality and this assumption lead to

$$\binom{\beta_y^{\frac{1}{s_1}} t}{s_1} \leq n_{s_1}(\mathbf{y}, X) \leq \binom{s_1 + L}{s_1}.$$

It follows that $L \geq \beta_y^{\frac{1}{s_1}} t - s_1$ (the right-hand side can be replaced by the ceiling). Given \mathcal{S} , $|\mathcal{S}| = s_1$, with the response vector $\mathbf{x}(\mathcal{S}) = \mathbf{y}$, and $(s_2 - s_1)$ distinct indices $j_1, \dots, j_{s_2-s_1} \in \mathcal{S}_y \setminus \mathcal{S}$, one can construct the s_2 -subset $\mathcal{S}' = \mathcal{S} \cup \{j_1, \dots, j_{s_2-s_1}\}$ with the same response vector $\mathbf{x}(\mathcal{S}') = \mathbf{y}$. Moreover, any \mathcal{S}' can

be constructed in at most $\binom{s_2}{s_1}$ such ways. Hence

$$\begin{aligned} n_{s_2}(\mathbf{y}, X) &\geq n_{s_1}(\mathbf{y}, X) \frac{\binom{L}{s_2-s_1}}{\binom{s_2}{s_1}} \\ &\geq \beta_y \binom{t}{s_1} \frac{\left(\beta_y^{\frac{1}{s_1}} t - s_1 \right) \dots \left(\beta_y^{\frac{1}{s_1}} t - s_2 + 1 \right)}{s_2(s_2 - 1) \dots (s_1 + 1)} \\ &= \beta_y \binom{t}{s_2} \frac{\left(\beta_y^{\frac{1}{s_1}} t - s_1 \right) \dots \left(\beta_y^{\frac{1}{s_1}} t - s_2 + 1 \right)}{(t - s_1) \dots (t - s_2 + 1)}. \end{aligned} \quad (13)$$

Therefore, the minimum in the sum (12), that is,

$$\min \left\{ \frac{n_{s_1}(\mathbf{y}, X)}{\binom{t}{s_1}}, \frac{n_{s_2}(\mathbf{y}, X)}{\binom{t}{s_2}} \right\}$$

is bounded below by

$$\min \left\{ \beta_y, \beta_y \frac{\left(\beta_y^{\frac{1}{s_1}} t - s_1 \right) \dots \left(\beta_y^{\frac{1}{s_1}} t - s_2 + 1 \right)}{(t - s_1) \dots (t - s_2 + 1)} \right\}.$$

Recall that $0 < \beta_y \leq 1$. Thus, we have $\frac{\beta_y^{\frac{1}{s_1}} t - c}{t - c} \leq 1$ for any real c , $c < t$, and the above minimum is attained at the second argument. It follows

$$\begin{aligned} \min \left\{ \frac{n_{s_1}(\mathbf{y}, X)}{\binom{t}{s_1}}, \frac{n_{s_2}(\mathbf{y}, X)}{\binom{t}{s_2}} \right\} \\ \geq \beta_y \frac{\left(\beta_y^{\frac{1}{s_1}} t - s_1 \right) \dots \left(\beta_y^{\frac{1}{s_1}} t - s_2 + 1 \right)}{(t - s_1) \dots (t - s_2 + 1)}. \end{aligned}$$

Finally, we conclude

$$\begin{aligned} \varepsilon(\mathbf{p}, \mathcal{D}, X) &\geq \frac{1}{2} \sum_{\mathbf{y} \in \{0, 1\}^N: \beta_y > 0} \beta_y \frac{\left(\beta_y^{\frac{1}{s_1}} t - s_1 \right) \dots \left(\beta_y^{\frac{1}{s_1}} t - s_2 + 1 \right)}{(t - s_1) \dots (t - s_2 + 1)} \\ &= \frac{1}{2} \sum_{\mathbf{y} \in \{0, 1\}^N: \beta_y > 0} \beta_y f(\beta_y^{-1}) \\ &\stackrel{(a)}{\geq} \frac{1}{2} f \left(\sum_{\mathbf{y} \in \{0, 1\}^N: \beta_y > 0} \beta_y \cdot \beta_y^{-1} \right) \\ &\stackrel{(b)}{\geq} \frac{\left(2^{-\frac{N}{s_1}} t - s_1 \right) \dots \left(2^{-\frac{N}{s_1}} t - s_2 + 1 \right)}{2(t - s_1) \dots (t - s_2 + 1)}, \end{aligned}$$

where the function $f(x)$ is defined by

$$f(x) \triangleq \frac{\left(x^{-\frac{1}{s_1}} t - s_1 \right) \dots \left(x^{-\frac{1}{s_1}} t - s_2 + 1 \right)}{(t - s_1) \dots (t - s_2 + 1)}.$$

We use *i*) the property $\sum_{\mathbf{y} \in \{0, 1\}^N} \beta_y = 1$, *ii*) the inequality $f(x) > 0$ for all $x \in [1, 2^N]$ and *iii*) Jensen's inequality for

the \cup -convex function $f(x)$ in the interval $x \in [1, 2^N]$ to prove the inequality (a). To obtain the inequality (b), we observe *i*) the number of distinct y 's in the sum is at most 2^N or

$$\sum_{y \in \{0,1\}^N : \beta_y > 0} \beta_y \cdot \beta_y^{-1} \leq 2^N,$$

and *ii*) the function $f(x)$ is decreasing in the interval $[1, 2^N]$. This completes the proof. ■

C. Proof of Corollary 1

Proof: By Theorem 1, we know that the universal error probability of any testing matrix X and any decision rule \mathcal{D} is bounded below by

$$\varepsilon(\mathcal{D}, X) \geq \frac{\left(2^{-\frac{N}{s_1}}t - s_1\right) \dots \left(2^{-\frac{N}{s_1}}t - s_2 + 1\right)}{2(t - s_1) \dots (t - s_2 + 1)}.$$

Since the universal error probability should be at most ε we obtain

$$\varepsilon \geq \frac{\left(2^{-\frac{N}{s_1}}t - s_1\right) \dots \left(2^{-\frac{N}{s_1}}t - s_2 + 1\right)}{2(t - s_1) \dots (t - s_2 + 1)}.$$

Recall $s_2 = o(t)$. Suppose that all the factors in the right-hand side are positive. By taking the binary logarithm, we get

$$\log_2 \varepsilon \geq -\frac{(s_2 - s_1)N}{s_1}(1 + o(1)).$$

Therefore,

$$N \geq \frac{s_1}{s_2 - s_1} \log_2 \frac{1}{\varepsilon}(1 + o(1)) \quad \text{as } \varepsilon \rightarrow 0.$$

Claims (a) and (b) immediately follow. ■

D. Proof of Theorem 2

Proof: The existence result shall be proved by the probabilistic method. We consider a binary $(N \times t)$ -matrix X whose entries are independent Bernoulli random variables and equal to 1 with probability $p = \frac{\ln s_2 - \ln s_1}{s_2 - s_1}$. Take the threshold parameter τ to be $1 - (1 - p)^{s_1}/2 - (1 - p)^{s_2}/2$. By Proposition 4 the error probability can be rewritten as

$$\varepsilon(\tau\text{-WDR}, X) = \max \left\{ \frac{|B_{s_1}^1(\lfloor \tau N \rfloor, X)|}{\binom{t}{s_1}}, \frac{|B_{s_2}^2(\lfloor \tau N \rfloor, X)|}{\binom{t}{s_2}} \right\}, \quad (14)$$

where the sets $B_{s_1}^1(\lfloor \tau N \rfloor, X)$ and $B_{s_2}^2(\lfloor \tau N \rfloor, X)$ are defined by (5). Denote

$$P_1 \triangleq \frac{|B_{s_1}^1(\lfloor \tau N \rfloor, X)|}{\binom{t}{s_1}}, \quad P_2 \triangleq \frac{|B_{s_2}^2(\lfloor \tau N \rfloor, X)|}{\binom{t}{s_2}}.$$

We estimate the probability P_1 that the union of s_1 columns have the weight greater than τN and the probability P_2 that the union of s_2 columns has weight at most τN .

The weight of s_i random columns from matrix X is a binomial random variable $Y_i \sim B(N, q_i)$ with parameters N and $q_i \triangleq 1 - (1 - p)_i^s$. Then $P_1 = \Pr\{Y_1 > \tau N\}$ and $P_2 = \Pr\{Y_2 \leq$

$\tau N\}$. Define $\delta \triangleq \tau - q_1 = q_2 - \tau = (1 - p)^{s_1}/2 - (1 - p)^{s_2}/2$. Using Hoeffding's inequalities [28, Theorem 2] of the forms

$$\Pr\{B(n, p) \geq (p + \varepsilon)n\} \leq e^{-2\varepsilon^2 n},$$

and

$$\Pr\{B(n, p) \leq (p - \varepsilon)n\} \leq e^{-2\varepsilon^2 n},$$

we conclude that

$$P_1 = \Pr\{Y_1 > \tau N\} = \Pr\{Y_1 > (q_1 + \delta)N\} \leq e^{-2\delta^2 N}, \quad (15)$$

and

$$P_2 = \Pr\{Y_2 \leq \tau N\} = \Pr\{Y_2 \leq (q_2 - \delta)N\} \leq e^{-2\delta^2 N}. \quad (16)$$

Therefore, there exists a testing $(N \times t)$ -matrix X such that the τ -WDR has the error probability less than ε whenever $e^{-2\delta^2 N} \leq \varepsilon$. The last inequality is equivalent to the following one

$$N \geq \frac{1}{2\delta^2} \ln \frac{1}{\varepsilon}$$

To prove claim (a), we use the property $s_1 = s$ and $s_2 = \alpha s$. First, the probability p can be written as

$$p = \frac{\ln s_2 - \ln s_1}{s_2 - s_1} = \frac{\ln \alpha}{s(\alpha - 1)}.$$

Then we find the asymptotics of δ as $s \rightarrow \infty$

$$\begin{aligned} \delta &= \frac{(1 - p)^{s_1}}{2} - \frac{(1 - p)^{s_2}}{2} \\ &= \frac{\exp(s_1 \ln(1 - p)) - \exp(s_2 \ln(1 - p))}{2} \\ &= \frac{\exp(-\frac{\ln \alpha}{\alpha - 1}) - \exp(-\frac{\alpha \ln \alpha}{\alpha - 1})}{2} + o(1) = \frac{\alpha - 1}{2\alpha^{\frac{\alpha}{\alpha - 1}}} + o(1). \end{aligned}$$

Therefore, there exists a testing $(N \times t)$ -matrix X such that the τ -WDR has the error probability less than ε if

$$N \geq \frac{1}{2\delta^2} \ln \frac{1}{\varepsilon} = \frac{2\alpha^{\frac{2\alpha}{\alpha-1}}}{(\alpha - 1)^2} \ln \frac{1}{\varepsilon}(1 + o(1)) \quad \text{as } s \rightarrow \infty.$$

To prove claim (b), we use the property $s_1 = s$ and $s_2 = s + c$, where $c = o(s)$. For $s \rightarrow \infty$, the parameter p is then

$$p = \frac{\ln s_2 - \ln s_1}{s_2 - s_1} = \frac{\ln(1 + c/s)}{c} = \frac{1}{s} - \frac{c}{2s^2} + o\left(\frac{c}{s^2}\right).$$

Now we find the asymptotics of $(1 - p)^{s_1} = (1 - p)^s$ as $s \rightarrow \infty$

$$\begin{aligned} (1 - p)^s &= \exp\left(s \ln\left(1 - \left(\frac{1}{s} - \frac{c}{2s^2} + o\left(\frac{c}{s^2}\right)\right)\right)\right) \\ &= \exp\left(s\left(-\frac{1}{s} + \frac{c}{2s^2} + o\left(\frac{c}{s^2}\right)\right) - \frac{s}{2s^2} + o\left(\frac{c}{s}\right)\right) \\ &= \exp\left(-1 + \frac{c - 1}{2s} + o\left(\frac{c}{s}\right)\right) \\ &= e^{-1} \left(1 + \frac{c - 1}{2s} + o\left(\frac{c}{s}\right)\right). \end{aligned}$$

Similarly we obtain the asymptotic behaviour of $(1-p)^{s_2} = (1-p)^{s+c}$ as $s \rightarrow \infty$

$$\begin{aligned} (1-p)^{s+c} &= \exp \left((s+c) \ln \left(1 - \left(\frac{1}{s} - \frac{c}{2s^2} + o\left(\frac{c}{s^2}\right) \right) \right) \right) \\ &= \exp \left((s+c) \left(-\frac{1}{s} + \frac{c}{2s^2} + o\left(\frac{c}{s^2}\right) \right) \right. \\ &\quad \left. - \frac{s+c}{2s^2} + o\left(\frac{c}{s}\right) \right) \\ &= \exp \left(-1 + \frac{c-1}{2s} - \frac{c}{s} + o\left(\frac{c}{s}\right) \right) \\ &= e^{-1} \left(1 - \frac{c+1}{2s} + o\left(\frac{c}{s}\right) \right). \end{aligned}$$

Therefore, we obtain the asymptotics for δ

$$\delta = \frac{(1-p)^{s_1}}{2} - \frac{(1-p)^{s_2}}{2} = \frac{c}{2es} + o\left(\frac{c}{s}\right).$$

Finally, there exists a testing $(N \times t)$ -matrix X such that the τ -WDR has the error probability less than ε whenever

$$N \geq \frac{1}{2\delta^2} \ln \frac{1}{\varepsilon} = \frac{2e^2 s^2}{c^2} \ln \frac{1}{\varepsilon} (1 + o(1)) \quad \text{as } s \rightarrow \infty.$$

■

VII. CONCLUSION

In this paper, we discuss a hypothesis in the boolean group testing model, namely, how to distinguish reliably the null hypothesis H_0 : the number of defective elements is at most s_1 , and the alternative one H_1 : the number of defective elements is at least s_2 . For the case $s_1 = s$ and $s_2 = \alpha s$, where the real number $\alpha \geq 1$ is fixed, we show that the optimal number of non-adaptive tests required to accept or reject H_0 with error probability ε is $\Theta(\log \frac{1}{\varepsilon})$. When $s_1 = s$ and $s_2 = s + c$ for $c = o(s)$, we prove the necessity of $O(s/c \log \frac{1}{\varepsilon})$ tests and provide a simple weight algorithm with $O(s^2/c^2 \log \frac{1}{\varepsilon})$ tests. Our simulation results confirm the advantage of this algorithm over the COMP algorithm adapted for this problem.

There are several directions for future research on testing the hypothesis. First, the gap between our upper and lower bounds on the minimal number of tests is still quite large in some regimes. Therefore, it would be great to find some order-optimal results for other settings. Second, it is of high interest to consider the problem under other multiple-access channel models, e.g. testing the hypothesis under the A channel would give an estimate on the number of sources of pirate copies of a copyrighted multimedia content [29].

REFERENCES

- [1] G. K. Atia and V. Saligrama, "Boolean compressed sensing and noisy group testing," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1880–1901, Mar. 2012.
- [2] R. Dorfman, "The detection of defective members of large populations," *Ann. Math. Statist.*, vol. 14, no. 4, pp. 436–440, 1943.
- [3] D.-Z. Du and F. K. Hwang, *Combinatorial Group Testing and Its Applications*, (Series on Applied Mathematics), 2nd ed, vol. 12. Singapore: World Scientific, 2000.
- [4] A. G. D'yachkov, A. J. Macula, and V. V. Rykov, "New constructions of superimposed codes," *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 284–290, Jan. 2000.
- [5] C. L. Chan, S. Jaggi, V. Saligrama, and S. Agnihotri, "Non-adaptive group testing: Explicit bounds and novel algorithms," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 3019–3035, May 2014.
- [6] W. Kautz and R. Singleton, "Nonrandom binary superimposed codes," *IEEE Trans. Inf. Theory*, vol. 10, no. 4, pp. 363–377, Oct. 1964.
- [7] A. Sharma and C. R. Murthy, "On finding a subset of non-defective items from a large population," *IEEE Trans. Signal Process.*, vol. 66, no. 21, pp. 5762–5775, Nov. 2018.
- [8] M. Aldridge, L. Baldassini, and O. Johnson, "Group testing algorithms: Bounds and simulations," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3671–3687, Jun. 2014.
- [9] O. Johnson, M. Aldridge, and J. Scarlett, "Performance of group testing algorithms with near-constant tests per item," *IEEE Trans. Inf. Theory*, vol. 65, no. 2, pp. 707–723, Feb. 2019.
- [10] J. Scarlett and V. Cevher, "Limits on support recovery with probabilistic models: An information-theoretic framework," *IEEE Trans. Inf. Theory*, vol. 63, no. 1, pp. 593–620, Jan. 2017.
- [11] S. Bondorf, B. Chen, J. Scarlett, H. Yu, and Y. Zhao, "Sublinear-time non-adaptive group testing with $o(k \log n)$ tests via bit-mixing coding," 2019, *arXiv:1904.10102*.
- [12] A. Agarwal, S. Jaggi, and A. Mazumdar, "Novel impossibility results for group-testing," in *Proc. IEEE Int. Symp. Inf. Theory*, 2018, pp. 2579–2583.
- [13] M. Aldridge, "Individual testing is optimal for nonadaptive group testing in the linear regime," *IEEE Trans. Inf. Theory*, vol. 65, no. 4, pp. 2058–2061, 2018.
- [14] T. Berger and V. I. Levenshtein, "Asymptotic efficiency of two-stage disjunctive testing," *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 1741–1749, Jul. 2002.
- [15] M. M'ezard and C. Toninelli, "Group testing with random pools: optimal two-stage algorithms," *IEEE Trans. Inf. Theory*, vol. 57, no. 3, pp. 1736–1745, Mar. 2011.
- [16] Y. Cheng, "An efficient randomized group testing procedure to determine the number of defectives," *Operations Res. Lett.*, vol. 39, no. 5, pp. 352–354, 2011.
- [17] M. Falahatgar, A. Jafarpour, A. Orlitsky, V. Pichapati, and A. T. Suresh, "Estimating the number of defectives with group testing," in *Proc. IEEE Int. Symp. Inf. Theory*, 2016, pp. 1376–1380.
- [18] 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.
- [19] P. Damaschke, A. S. Muhammad, and G. Wiener, "Strict group testing and the set basis problem," *J. Combinatorial Theory, Series A*, vol. 126, pp. 70–91, 2014.
- [20] M. Aldridge, O. Johnson, and J. Scarlett, "Group testing: An information theory perspective," 2019, *arXiv:1902.06002*.
- [21] A. Emad and O. Milenkovic, "Poisson group testing: A probabilistic model for boolean compressed sensing," *IEEE Trans. Signal Process.*, vol. 63, no. 16, pp. 4396–4410, Aug. 2015.
- [22] A. G. D'yachkov, I. V. Vorob'ev, N. A. Polyansky, and V. Y. Shchukin, "Almost disjunctive list-decoding codes," *Problems Inf. Transmiss.*, vol. 51, no. 2, pp. 110–131, 2015.
- [23] A. G. D'yachkov and V. V. Rykov, "Bounds on the length of disjunctive codes," *Problem Inf. Transmiss.*, vol. 18, no. 3, pp. 166–171, 1982.
- [24] A. G. D'yachkov, V. V. Rykov, and A. M. Rashad, "Superimposed distance codes," *Problems Control Inf. Theory*, vol. 18, no. 4, pp. 237–250, 1989.
- [25] M. Falahatgar, A. Jafarpour, A. Orlitsky, V. Pichapati, and A. T. Suresh, "Estimating the number of defectives with group testing," in *Proc. IEEE Int. Symp. Inf. Theory*, 2016, pp. 1376–1380.
- [26] A. De Bonis, "Constraining the number of positive responses in adaptive, non-adaptive, and two-stage group testing," *J. Combinatorial Optim.*, vol. 32, no. 4, pp. 1254–1287, 2016.
- [27] A. D'yachkov, I. Vorob'ev, N. Polyanskii, and V. Shchukin, "Hypothesis test for upper bound on the size of random defective set," in *Proc. IEEE Int. Symp. Inf. Theory*, 2017, pp. 978–982.
- [28] W. Hoeffding, "Probability inequalities for sums of bounded random variables," in *The Collected Works of Wassily Hoeffding*. Berlin, Germany: Springer, 1994, pp. 409–426.
- [29] M. Cheng and Y. Miao, "On anti-collusion codes and detection algorithms for multimedia fingerprinting," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4843–4851, Jul. 2011.