Boolean Compressed Sensing and Noisy Group Testing

George Atia[†], *Member, IEEE*, and Venkatesh Saligrama[‡], *Senior Member, IEEE*

Abstract

The fundamental task of group testing is to recover a small distinguished subset of items from a large population while efficiently reducing the total number of tests (measurements). The key contribution of this paper is in adopting a new information-theoretic perspective on group testing problems. We formulate the group testing problem as a channel coding/decoding problem and derive a single-letter characterization for the total number of tests used to identify the defective set. Although the focus of this paper is primarily on group testing, our main result is generally applicable to other compressive sensing models.

The single letter characterization is shown to be tight for many interesting noisy group testing scenarios. Specifically, we consider an additive Bernoulli(q) noise model where we show that, for N items and K defectives, the number of tests T is $O\left(\frac{K \log N}{1-q}\right)$ for arbitrarily small average error probability and $O\left(\frac{K^2 \log N}{1-q}\right)$ for a worst case error criterion. We also consider dilution effects whereby a defective item in a positive pool might get diluted with probability u and potentially missed. In this case, it is shown that T is $O\left(\frac{K \log N}{(1-u)^2}\right)$ and $O\left(\frac{K^2 \log N}{(1-u)^2}\right)$ for the average and the worst case error criteria, respectively. Furthermore, our bounds allow us to verify existing known bounds for noiseless group testing including the deterministic noise-free case and approximate reconstruction with bounded distortion. Our proof of achievability is based on random coding and the analysis of a Maximum Likelihood Detector, and our information theoretic lower bound is based on Fano's inequality.

I. INTRODUCTION

Group testing has been effectively used in numerous applications. It was originally proposed during World War II to reduce the total number of blood tests required to detect soldiers with Syphilis [3], [4]. Instead of conducting a separate blood test for each and every soldier, the idea was to pool blood samples from many soldiers and test them simultaneously. Group testing has been used in general in biology for screening libraries of DNA clones (strings of DNA sequence) of the human genome and for screening blood for diseases. Other applications include quality control for detecting defective parts in production lines, data forensics to test collections of documents by applying one-way hash functions, computer fault diagnosis, and contention algorithms in multiple access communications. Recently, group testing methods have also been applied to spectrum enforcement in cognitive radios [5], [6].

In the basic group testing problem [3], we are given a population of N items. Among them, at most K items, also called defectives, are of interest. The set of defectives is denoted by $\mathcal{G}$. Associated with the group testing problem is a binary matrix $\mathcal{C}$ known as the measurement matrix. This matrix defines the assignment of each of the items to different pools or collections. The (i, j) entry is 1 if the i-th item is contained in the j-th pool and 0 otherwise. A test conducted on the pool is positive if there is at least one item belonging to the pool which is also an element of $\mathcal{G}$, and is negative otherwise. A measurement matrix for a non-adaptive group testing algorithm is a $N \times T$ matrix where the T columns correspond to pools of items and N is the number of items. Each item is associated with a row codeword of length T. If K items are defective, then the T tests are a boolean sum of K rows of the measurement matrix. The goal is to construct a pooling design to recover the defective set while reducing the required number of tests. Group testing is related in spirit to compressed sensing (CS). In CS we are given an N-dimensional sparse signal with support size K. Random projections of the sparse signal are obtained. The goal is to identify the support set while minimizing the number of projections. In this sense, group testing can be viewed as a boolean version of CS where we apply a measurement matrix to a sparse vector corresponding to the defective set with the goal of reconstructing the support, i.e. identify the defective items. The main distinction is that in group testing the test matrix used to collect the measurements is binary, so is the sparse vector, and the arithmetic is boolean. Multiplication of 0s and 1s is the logical AND (coincides with usual multiplication) but addition is replaced by the logical OR.

While the degradation of CS with noise has been characterized (see [7]–[13] and references therein), the noisy group testing problem, the main focus of this paper, has not been systematically studied. Our attention in this paper is on the so called non-adaptive testing problem [3], where the measurement matrix

is formed prior to performing the tests.

A significant part of the existing research on group testing is focused on combinatorial pool design (i.e. construction of measurement matrices) to guarantee the detection of the items of interest using a small number of tests. Two types of matrix constructions have been considered. Disjunct matrices [3] satisfy the so called covering property[1]. In the context of group testing this property implies that a test pattern obtained by taking any K rows of the measurement matrix does not cover any other boolean sum of K or smaller number of rows[2]. Equivalently, for any $K+1$ rows, there always exists a column with 1 in a row and 0s in the other K rows. Matrices that satisfy this property are often referred to as superimposed codes and combinatorial constructions were extensively developed by [14]–[16]. Superimposed codes are not only desirable because they ensure identifiability but they also lead to efficient decoding. Separability [3] is a weaker notion that is also often employed. A separable matrix ensures that the boolean sum of K rows are all distinct, which ensures identifiability. Uniquely decipherable codes [14], [15] are codes that guarantee that every boolean sum of K or smaller number of rows are distinct. Recently, it has been shown [17] that all of these notions are equivalent up to a scaling factor on the number of tests T.

A different approach to group testing based on probabilistic method has also been advocated by several researchers [18]–[22]. Dyachkov and Rykov [18], Du and Hwang [23], and Ruszinko [19] developed upper and lower bounds on the number of rows T for a matrix to be K-disjunct (bound on length of superimposed codes). Random designs were used to compute upper bounds on the lengths of superimposed codes by investigating when randomly generated matrices have the desired covering/separability properties. They showed that for $N \to \infty$ and $K \to \infty$, the number of tests T must scale as $T = O\left(\frac{K^2 \log N}{\log K}\right)$ for exact reconstruction with worst-case input. Sebo [20] investigated average error probabilities and showed that for an arbitrarily small error probability, a randomly generated matrix will be K-disjunct if $T = O(K \log N)$ as $N \to \infty$. Recently Berger et al. [21] proved upper and lower bounds on the number of tests for two-stage disjunctive testing. Approximate reconstruction [22], whereby a fraction α of the defective items are allowed to be in error, has been described. Again the number of tests here has been shown to scale as $T = O(K \log N)$ as $N \to \infty$.

While these approaches have generally characterized fundamental tradeoffs for noiseless group testing, the noisy counterpart of group testing has not been systematically addressed. In this paper we present

---

[1]We say that a row x is covered by a row y iff $x \vee y = y$.

[2]In the combinatorial pool design literature, the roles of rows and columns are interchanged. In other words, the measurement matrix is $\mathcal{C}^T$, i.e., the transpose of our matrix $\mathcal{C}$. What motivates our choice is consistency with the standard information theoretic convention for codewords being rows of a codebook.

a novel information theoretic approach to group testing problems. The common approach to previous related work was to prove bounds on the size of randomly generated matrices to exhibit the aforementioned separability and covering properties. In contrast, we formulate the problem as a detection problem and establish its connection to Shannon coding theory [24] which, to the best of our knowledge, is explored in this paper for the first time. While there exists a one-to-one mapping between both formulations, the new perspective allows us to easily obtain results for a wide range of models including noisy versions of group testing. Our approach, which is fairly general, is to map the group testing problem to a corresponding channel model which allows the computation of simple mutual information expressions to derive achievable bounds on the required number of tests. To summarize, our approach offers several advantages, including:

- **Mutual information characterization:** Our main result is a simple single letter characterization providing order-wise tight necessary and sufficient conditions on the total number of tests.
- **Characterization for new group testing problems:** This result allows us to verify existing bounds for some of the known scenarios and extend the analysis to many new interesting setups including noisy versions of group testing.
- **Extensions to sparse models:** Although the focus of this paper is on the Boolean case, the main result and the methods that we develop in this paper are more generally applicable to Compressed Sensing models and not just to group testing. Consequently, some of the information theoretic Compressed Sensing results [25] can also be recovered using the mutual information expressions derived herein.

One major contribution of this paper is to develop tools to analyze long standing noisy versions of the group testing problem. In particular we consider two models: The dilution model and the additive model.

- **Additive model:** False alarms could arise from errors in some of the screening tests. This arises when some tests are erroneously positive.
- **Dilution model:** Even though a positive item is contained in a given pool, the test's outcome could be negative if the defective item gets diluted for that specific test. For example, in blood testing the positive sample might get diluted in one or more tests leading to potential misses of infected blood samples. To account for such a case we analyze the group testing problem where some of the positive entries get flipped into zeros with a given probability u.

We also consider the case of partial reconstruction where we only aim for approximate recovery of the defective set. An error occurs only if the number of missed defectives is greater than a fraction α of

Model	T (average P_e criterion)	T (max P_e criterion)
Noise-free	$O(K \log N)$	$O(K^2 \log N)$
Partial reconstruction	$O(K \log N)$	$O(K \log N)$
Noisy with additive noise	$O\left(\frac{K \log N}{1-q}\right)$	$O\left(\frac{K^2 \log N}{1-q}\right)$
Noisy with dilution	$O\left(\frac{K \log N}{(1-u)^2}\right)$	$O\left(\frac{K^2 \log N}{(1-u)^2}\right)$

TABLE I

THIS TABLE SUMMARIZES THE SCALING RESULTS FOR THE VARIOUS MODELS CONSIDERED IN THE PAPER WHICH HOLD ASYMPTOTICALLY FOR $N \to \infty$. IN PARTICULAR, IT SHOWS THE REQUIRED NUMBER OF TESTS T AS A FUNCTION OF THE SIZE OF THE DEFECTIVE SET K, THE TOTAL NUMBER OF ITEMS N, AND THE MODEL PARAMETERS FOR THE NOISELESS, ADDITIVE NOISE, AND DILUTION MODELS FOR BOTH THE AVERAGE ERROR AND WORST-CASE ERROR CRITERIA. THE PROBABILITY q IS THE PARAMETER OF THE BERNOULLI(q) ADDITIVE NOISE, AND u IS THE DILUTION PROBABILITY FOR THE DILUTION MODEL.

the total K defectives.

Table I summarizes the scaling results we obtained for the various models considered in the paper for the average error and worst case error criteria.

The rest of the paper is organized as follows. Section II describes the problem setup. The main achievable result mapping the problem to mutual information expression is provided in Section III. In Section IV we prove a converse bound using Fano's inequality [24]. Section V considers the noise free (deterministic) version of the problem with average and worst case errors. Approximate (partial) reconstruction is investigated in Section VI. In Section VII we consider different noisy models with additive and dilution effects. Finally, we present our conclusions in Section VIII.

II. PROBLEM SETUP

Among a population of N items, K unknown items are of interest. The collection of these K items represents the defective set. The goal is to construct a pooling design, i.e., a collection of tests, to recover the defective set while reducing the number of required tests. The idea is illustrated in Fig. 1. In this example, the defective set $\mathcal{G} = \{2\}$, i.e., $K = 1$, since only the second item is defective. The binary valued matrix shown in Fig. 1 represents the measurement matrix (transposed) defining the assignment of items to tests. The entry is 1 if the item is a member of the designated test and 0 otherwise. At the bottom of the figure we highlight the positive tests. The outcome of a test is positive if and only if the second item is a member of that test. Observing the output for a number of tests T, the goal is to recover the defective set $\mathcal{G}$. While in combinatorial group testing the goal is to find the defective set for the

codeword of item 1 (row in this figure)

X_1 | 1 0 1 1 0 1 0 0 0 1 1 0 0 0 1 0 0 0 |....

Defective → (X_2) 0 0 1 0 1 1 0 1 1 1 0 0 0 1 1 0 0 0 ....

X_3 1 1 0 0 1 0 1 0 0 0 1 1 0 0 1 0 1 0 ....

$\vdots$

X_N 1 0 0 1 1 0 1 1 0 0 0 1 0 1 0 0 0 1 ....

Positive tests   - - t_3 - t_5 t_6 - t_8 t_9 t_{10} - - - t_{14} t_{15} - - -
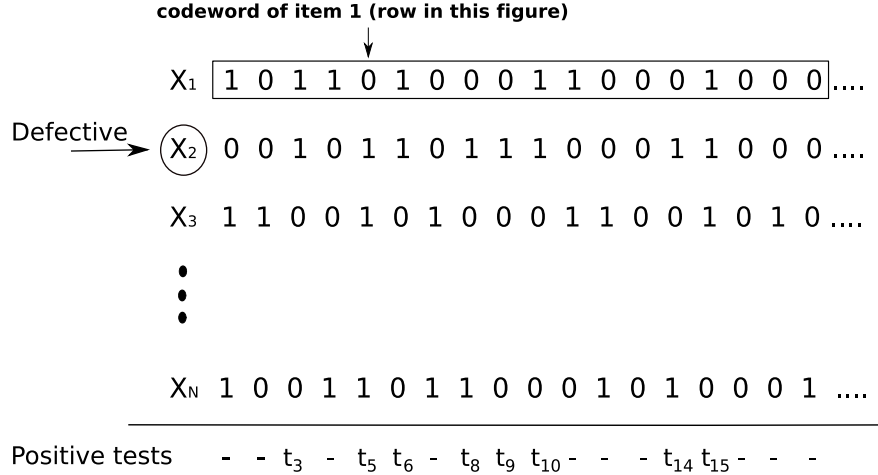
Fig. 1. A binary matrix defines the assignment of items to tests. Rows are codewords for corresponding items, and columns correspond to pools of items (tests). The entry is 1 if the item is a member of the designated test and 0 otherwise. In the shown example, the defective set $\mathcal{G} = \{2\}$, i.e. only the second item is defective. At the bottom of the figure we show the positive tests. The outcome of a test is positive if and only if the second item is a member of that test. The goal is to recover the defective set $\mathcal{G}$ from T test outcomes.

worst-case input, probabilistic group testing requires the average error to be small. Both formulations are considered in this paper in subsequent sections. We assume that the item-test assignment is generated randomly. Before we provide our main result we introduce the notation that will be used throughout the paper.

A. Notation

We use bold-face to denote matrices, while regular font is used to denote vectors, scalars and components of matrices. For clarity, figure 2 illustrates our notation by means of a simple example.

- N is the total number of items, K is the known number of defectives (or positive items), p denotes the probability that an item is part of a given test, and T is the total number of tests.
- Codewords: For the j-th item, X_j^T is a binary row vector $\in \{0,1\}^T$, with the t-th entry $X_j(t) = 1$ if the j-th item is pooled in test t, and 0 otherwise. Following an information theoretic convention, we call it the j-th codeword. The observation vector Y^T is a binary vector of length T, with entries equal to 1 for the tests with positive outcome. Similarly, $Y(t)$ denotes the t-th component of the vector Y^T.

- Given a subset $S \subset \{1, 2 \ldots N\}$ with cardinality $|S|$, the matrix $\boldsymbol{X}_S$ is an $|S| \times T$ matrix formed from the rows indexed by S. In other words, $\boldsymbol{X}_S$ denotes the collection of codewords (each of length T) corresponding to the items in S. Similarly, X_S denotes a vector, whose components are restricted to the set of components indexed by S. Thus, X_S is a column of the matrix $\boldsymbol{X}_S$. When time indexing is needed, $X_S(t)$ is used to specifically denote the t-th column of the matrix $\boldsymbol{X}_S$, and $X_j(t)$ is the t-th component of the vector X_j^T.

- $\mathcal{C}$: The $N \times T$ measurement matrix, or the codebook, is a collection of N codewords defining the pool design, i.e., the assignment of items to tests.

- Index the different sets of items of size K as S_ω with index ω. Since there are N items in total, there are $\binom{N}{K}$ such sets, hence

$$\omega \in \mathcal{I} = \left\{ 1, 2, \ldots \binom{N}{K} \right\} \tag{1}$$

Note that S_ω is a set of K indices corresponding to the ω-th set of items. Also, without loss of generality, we assume that $\omega = 1$ corresponds to the ground truth, i.e., the true defective set is S_1. The empty set is denoted $\emptyset$ and "$\bigvee$" is used to denote the Boolean OR operation.

- Hence $\boldsymbol{X}_{S_\omega}$ is the matrix of codewords corresponding to the items in the index set S_ω.

B. Noise-free case

For the noise-free case, the outcome of the tests Y^T is deterministic. It is the Boolean sum of the codewords corresponding to the defective set $\mathcal{G}$. In other words

$$Y^T = \bigvee_{i \in \mathcal{G}} X_i^T. \tag{2}$$

Alternatively, if $R_i \in \{0, 1\}$ is an indicator function for the i-th item determining whether it belongs to the defective set, i.e., $R_i = 1$ if $i \in \mathcal{G}$ and $R_i = 0$ otherwise. Then, the outcome $Y(t)$ of the t-th test in the noise-free case can be written as

$$Y(t) = \bigvee_{i=1}^{N} X_i(t) R_i \tag{3}$$

where $X_i(t)$ is the t-th entry of the vector X_i^T, or equivalently, the binary entry at cell (i, t) of the measurement matrix $\boldsymbol{X}$.

C. Noisy cases

In this paper we also consider two noisy models, the additive model and the dilution model. However, we point out that our main achievability result is fairly general and is not restricted to these specific noise models or to Boolean channels.
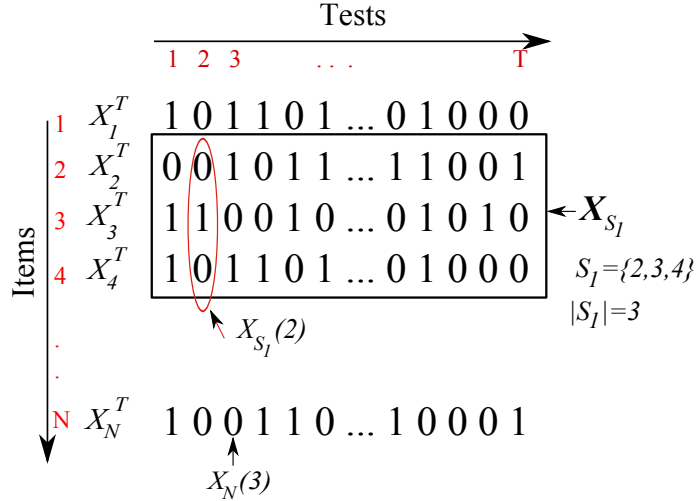
Fig. 2. The shown figure illustrates the notation through a simple example. Rows are codewords of length T for corresponding items (denoted X_j^T). A defective set $S_1 = \{2, 3, 4\}$ consists of items $2, 3$ and 4. The corresponding matrix $\boldsymbol{X}_{S_1}$ is formed from rows indexed by S_1, i.e., consists of rows $2, 3, 4$. The figure also illustrates the notation $X_{S_1}(2)$ which refers to the vector indexed by the set S_1 at time $t = 2$. $X_N(3)$ refers to the 3-rd test for item N. Since the matrix is generated i.i.d., the vector X_{S_1} (without time index) refers to a vector whose components are restricted to the set of components indexed by S_1.

- Additive Model: In this model we account for false alarms in the outcome of pooling tests. The outcome of a test can still be 1 even if no positive items are pooled in that test. This effect is captured by adding independent Bernoulli(q) random variables $W(t)$ to the outcome of the t-th test of the noise-free model in Eq.(3), i.e.,

$$Y(t) = \left(\bigvee_{i=1}^{N} X_i(t) R_i \right) \vee W(t) \tag{4}$$

where $W(t) \sim B(q), t = 1 \dots T$.

- Dilution Model: The dilution model refers to the case when a defective item in a pool gets diluted. If all positive items in a given test appear as absent, that could potentially lead to erroneously zero outcomes. This model is motivated by blood dilution due to pooling with other negative tests or imperfectly diluted blood samples. This effect is captured by the Z-channel model of Fig.3. A Z-channel with crossover probability u is a binary-input-binary-output channel that flips the input bit 1 with probability u, but maps input bit 0 to 0 with probability 1 (for different Z-channel models the roles of 0 and 1 may be interchanged) [26]. In the dilution context, the input 1 corresponds to the inclusion of a positive item in a test while input 0 corresponds to the item being absent in that test.

The asymmetric crossover captures the dilution effect, that is, in this model we might have misses but no false alarms. The outcome of the t-th test can be written as:

$$Y(t) = \bigvee_{i=1}^{N} \mathcal{Z}(X_i(t)R_i) \tag{5}$$

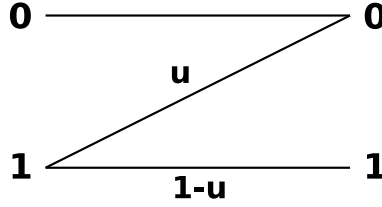where $\mathcal{Z}$ represents the Z-channel model of Fig. 3.

Fig. 3. Dilution channel (Z-channel): positive items taking part in a given test might probabilistically behave as absent (diluted). In other words, even though a positive item is contained in a given pool, the test's outcome could be negative if the item's presence gets diluted for that specific test. For example, in blood testing the positive sample might get diluted in one or more tests leading to potential misses of infected blood samples.

Note that in the additive model, the outcome of testing a pool with no defective items might be erroneously positive, i.e., false positives would occur. On the other hand, the membership of a defective item in a given test might go unnoticed in the dilution model. If all defectives appearing in a given pool are diluted, a false negative occurs. The effect of dilution on the increase in number of tests is expected to be more severe than the effect of additive noise. This is explained by the fact that tests with negative outcomes are generally more informative; while a truly positive test merely indicates that at least one defective is present in the pool, a truly negative test exonerates all the members pooled in that test. With additive noise, a test with a negative outcome is never erroneous. In contrast, dilution diminishes our confidence in pools with negative outcomes, since a seemingly negative outcome would not necessarily mean all pooled members are perfect. Intuitively speaking, additive noise can be potentially mitigated by repetition of tests whereas the dilution effect is more intricate to resolve. This intuition is verified by the results we obtained through theoretical analysis as will be shown in the next sections.

D. Performance criteria

The different sets of items of size K are indexed S_ω, where $\omega \in \mathcal{I} = \{1, 2, \ldots \binom{N}{K}\}$. Define a decoding function $g(.) : Y^T \to \mathcal{I}$. The function $g(.)$ maps the outcome of the T tests, Y^T, to an index $\omega \in \mathcal{I}$

corresponding to a specific set of defectives S_ω. Now define the conditional error probability λ_ω as

$$\lambda_\omega = \sum_{Y^T} p(Y^T | \boldsymbol{X}_{S_\omega}) \mathbb{1}\{g(Y^T) \neq \omega | \omega\} \tag{6}$$

where $\mathbb{1}\{.\}$ is an indicator function which takes the value 1 when its argument is realized and 0 otherwise, i.e., it takes the value 1 when the defective set is misclassified. The conditional probability $p(Y^T | \boldsymbol{X}_{S_\omega})$ is the probability of getting Y^T as the tests' outcomes given that S_ω is the defective set with corresponding codewords matrix $\boldsymbol{X}_{S_\omega}$. Essentially, the conditional probability defines a group testing channel which is analogous to a communication channel where the output sequence depends on the transmitted input sequence, the message being the defective set and the encoded sequence being the matrix of codewords corresponding to that set. The probability λ_ω is the probability of error conditioned on a given ω, i.e., the probability that the decoded set is not the true defective set given that S_ω is the true defective set. Note that for the deterministic noise-free case this simplifies to $\lambda_\omega = \mathbb{1}\{g(Y^T) \neq \omega | \omega\}$. Averaging over all possible inputs ω, we define the average error probability λ as:

$$\lambda = \frac{1}{\binom{N}{K}} \sum_\omega \lambda_\omega \tag{7}$$

For the aforementioned models (noiseless and noisy), we prove achievable and converse bounds on the total number of tests T as $N, K \to \infty$. Namely, we consider the following criteria:

- Arbitrarily small average error probability:

$$\lambda = \frac{1}{\binom{N}{K}} \sum_\omega \lambda_\omega$$

- Worst-case error probability:

$$\lambda_{\max} = \max_\omega \lambda_\omega$$

- Partial reconstruction: In this case, we are satisfied with approximate reconstruction of the defective set. Let d be a distance function between the decoded set $g(Y^T)$ and the index ω of the true defective set such that $d(g(Y^T), \omega)$ is equal to the number of misses. In other words, d is the Hamming distance on ordered K-element subsets of $\{1,\ldots,N\}$. Given K declared candidates, an error occurs only if the number of missed items is greater than αK, i.e.,

$$\lambda_\omega = \sum_{Y^T} p(Y^T | \boldsymbol{X}_{S_\omega}) \mathbb{1}\{d(g(Y^T), \omega) > \alpha K | \omega\}$$

In the following section we will derive our main result. We will prove a sufficient condition on the number of tests T. The result is fairly general as it applies to the noise-free and the noisy versions of the problem as we elaborate in the following sections.

III. MAIN RESULT: ACHIEVABLE BOUND

To derive an achievable bound on the number of tests T, we show how the group testing problem can be mapped to an equivalent channel model. Using random coding and maximum likelihood decoding we upper bound the error probability, i.e., the probability of misclassifying the defective set.

A. Random matrix generation and the encoding process

The binary measurement matrix is randomly generated. Associated with each item is a codeword that represents its assignment to tests. Assume that the codewords are generated randomly and independently according to some distribution Q. A defective set S_ω corresponds to a collection of K codewords, which is a $K \times T$ matrix $\boldsymbol{X}_{S_\omega}$, and can be thought of as an encoded message transmitted through the group testing channel. In other words, the encoder $f : \mathcal{I} \to \{0,1\}^{KT}$, maps an index $\omega \in \mathcal{I}$ (defective set S_ω) to a matrix of codewords $\boldsymbol{X}_{S_\omega} \in \{0,1\}^{KT}$, where $\{0,1\}^{KT}$ is the space of binary $K \times T$ matrices. The encoded message $f(\omega) = \boldsymbol{X}_{S_\omega}$ is then transmitted through a channel with transition probability $p(Y(t)|\boldsymbol{X}_{S_\omega})$.

Since the channel is memoryless, i.e., each test outcome $Y(t)$ depends only on the corresponding input $X_{S_\omega}(t)$, the probability of the output sequence $Y^T = (Y(1), Y(2), \ldots, Y(T))$ given the input $\boldsymbol{X}_{S_\omega} = (X_{S_\omega}(1), X_{S_\omega}(2), \ldots, X_{S_\omega}(T))$ is given by

$$p(Y^T|\boldsymbol{X}_{S_\omega}) = \prod_{t=1}^{T} p(Y(t)|X_{S_\omega}(t))$$

And the K codewords and the observed Y^T have a joint distribution

$$p(\boldsymbol{X}_{S_\omega}, Y^T) = \prod_{t=1}^{T} p(X_{S_\omega}(t))p(Y(t)|X_{S_\omega}(t))$$

B. Decoder

Decoding is achieved using ML decoding [26]. The decoder goes through all $\binom{N}{K}$ possible sets of size K, where K is the size of the defective set, and chooses the set that is most likely. The decoding rule is thus defined by: given the tests'outcomes Y^T, choose ω^* for which

$$p(Y^T|\boldsymbol{X}_{S_{\omega^*}}) > p(Y^T|\boldsymbol{X}_{S_\omega}); \quad \forall \omega \neq \omega^* \tag{8}$$

i.e., choose the set for which the given Y^T is most likely given ω. An error occurs if any set other than the true defective set is more likely. This ML decoder is a minimum probability of error decoder assuming uniform prior on the input messages (defective sets). Next, we derive an upper bound on the

average error probability of the ML decoder, where the average is taken over defective sets and ensembles of codewords.

C. Probability of error analysis

Given the random codebook generation, let P_e denote the average probability of error, averaged over all codebooks $\mathcal{C}$, and over all sets of size K, i.e.,

$$
\begin{aligned}
P_e &= \sum_{\mathcal{C}} P(\mathcal{C})\lambda(\mathcal{C}) \\
&= \sum_{\mathcal{C}} P(\mathcal{C})\frac{1}{\binom{N}{K}}\sum_{\omega}\lambda_{\omega}(\mathcal{C}) \\
&= \frac{1}{\binom{N}{K}}\sum_{\omega}\sum_{\mathcal{C}} P(\mathcal{C})\lambda_{\omega}(\mathcal{C})
\end{aligned}
\tag{9}
$$

By symmetry of the codebook construction, $\sum_{\mathcal{C}} P(\mathcal{C})\lambda_{\omega}(\mathcal{C})$ does not depend on ω (and consequently not on the set S_{ω}). Thus,

$$
P_e = \sum_{\mathcal{C}} P(\mathcal{C})\lambda_{\omega}(\mathcal{C}) = P_{e|\omega}
\tag{10}
$$

In other words, the average error probability does not depend on the input ω due to averaging over randomly generated codebooks and we can assume, without loss of generality, that $\omega = 1$, i.e., S_1 is the defective set.

To simplify the exposition we introduce some further notation. As pointed out earlier, the matrix $\boldsymbol{X}_S$ is formed from rows indexed by the set S. For any 2 sets S_i and S_j, we define $S_{i,j}$, $S_{i^c,j}$, and S_{i,j^c} as the overlap set, the set of indices in S_j but not in S_i, and the set of indices in S_i but not in S_j, respectively. Namely,

$$
S_{i,j} = S_i \cap S_j \quad \text{overlap}
$$

$$
S_{i^c,j} = S_i^c \cap S_j \quad \text{in } j \text{ but not in } i
$$

$$
S_{i,j^c} = S_i \cap S_j^c \quad \text{in } i \text{ but not in } j
$$

Now define the error event E_i as the event that a set which differs from the defective set S_1 in exactly i items is more likely to the decoder. The probability of such an event is denoted $P(E_i)$. The event E_i implies that there exists some set which differs from the defective set in i items and is more likely. Hence,

$$
P(E_i) \leq \Pr\Big[\exists j \neq 1 : p(Y^T|\boldsymbol{X}_{S_j}) \geq P(Y^T|\boldsymbol{X}_{S_1})
$$

$$
\text{where} \quad |S_{1^c,j}| = |S_{1,j^c}| = i, \text{ and } |S_1| = |S_j| = K\Big]
\tag{11}
$$

The probability $P(E_i)$ can be written as a summation over all inputs X_{S_1} and all test outcomes Y^T

$$P(E_i) = \sum_{\boldsymbol{X}_{S_1}} \sum_{Y^T} Q(\boldsymbol{X}_{S_1}) p(Y^T | \boldsymbol{X}_{S_1}) \Pr[\text{error}_i | \omega = 1, \boldsymbol{X}_{S_1}, Y^T] \tag{12}$$

where $\Pr[\text{error}_i | \omega = 1, \boldsymbol{X}_{S_1}, Y^T]$ is the probability of decoding error in exactly i items, conditioned on message $\omega = 1$ entering the decoder, the selection of a particular $\boldsymbol{X}_{S_1}$ as the codewords for the set S_1, and on the reception of a sequence Y^T.

Using the union bound, the conditional error probability averaged over ensembles of codewords is upper bounded by,

$$P_{e|1} \leq \sum_{i=1}^{K} P(E_i)$$

$$= \sum_{i=1}^{K} \sum_{\boldsymbol{X}_{S_1}} \sum_{Y^T} Q(\boldsymbol{X}_{S_1}) p(Y^T | \boldsymbol{X}_{S_1}) \Pr[\text{error}_i | \omega = 1, \boldsymbol{X}_{S_1}, Y^T] \tag{13}$$

Next we state our main result. The following theorem provides a sufficient condition on the number of tests T for an arbitrarily small average error probability.

Theorem III.1 *(Sufficiency). Define $\Xi_S^{\{i\}}$ as the set of tuples $(\mathcal{S}^1, \mathcal{S}^2)$ partitioning the defective set S into disjoint sets $\mathcal{S}^1$ and $\mathcal{S}^2$ with cardinalities i and $K - i$, respectively, i.e.,*

$$\Xi_S^{\{i\}} = \left\{ (\mathcal{S}^1, \mathcal{S}^2) : \mathcal{S}^1 \bigcap \mathcal{S}^2 = \emptyset, \mathcal{S}^1 \bigcup \mathcal{S}^2 = S, |\mathcal{S}^1| = i, |\mathcal{S}^2| = K - i \right\} \tag{14}$$

Let N be the size of a population of items with the defective set S of cardinality K. If the number tests T is such that

$$T > \max_{i:(\mathcal{S}^1, \mathcal{S}^2) \in \Xi_S^{\{i\}}} \frac{\log \binom{N-K}{i} \binom{K}{i}}{I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y)}, \quad i = 1, 2, \ldots K$$

then asymptotically the average error probability approaches zero, namely,

$$\lim_{K \to \infty} \lim_{N \to \infty} P_e \to 0 \tag{15}$$

$I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y)$ is the mutual information [24] between $X_{\mathcal{S}^1}$ and $(X_{\mathcal{S}^2}, Y)$.

Before we prove our main result we need to prove the following lemma and the following theorem. In the next lemma, we upper bound the conditional error probability $\Pr[\text{error}_i | \omega = 1, \boldsymbol{X}_{S_1}, Y^T]$ in (13).

Lemma III.1 *Conditioned on the message index $\omega = 1$, the selection of particular codewords $\boldsymbol{X}_{S_1}$ for the set S_1 and the sequence Y^T of tests outcomes, the probability of decoding error in any i items is*

upper bounded by

$$\Pr[error_i | \omega = 1, \boldsymbol{X}_{S_1}, Y^T] \leq \sum_{S_{1,\omega}} \phi(\boldsymbol{X}_{S_{1,\omega}}, \boldsymbol{X}_{S_{1,\omega^c}}, Y) \tag{16}$$

where,

$$\phi(\boldsymbol{X}_{S_{1,\omega}}, \boldsymbol{X}_{S_{1,\omega^c}}, Y) = \sum_{S_{1^c,\omega}} \sum_{\boldsymbol{X}_{S_{1^c,\omega}}} Q(\boldsymbol{X}_{S_{1^c,\omega}}) \frac{p(Y^T, \boldsymbol{X}_{S_{1,\omega}} | \boldsymbol{X}_{S_{1^c,\omega}})^s}{p(Y^T, \boldsymbol{X}_{S_{1,\omega}} | \boldsymbol{X}_{S_{1,\omega^c}})^s}$$

$$= \binom{N-K}{i} \sum_{\boldsymbol{X}_{S_{1^c,\omega}}} Q(\boldsymbol{X}_{S_{1^c,\omega}}) \frac{p(Y^T, \boldsymbol{X}_{S_{1,\omega}} | \boldsymbol{X}_{S_{1^c,\omega}})^s}{p(Y^T, \boldsymbol{X}_{S_{1,\omega}} | \boldsymbol{X}_{S_{1,\omega^c}})^s} \quad \forall s > 0 \tag{17}$$

where the outer summation in the first equality corresponds to a sum over all sets S_ω of size K differing from S_1 in the set of items S_{1,ω^c}.

Proof: See Appendix A ∎

The next Theorem establishes an upper bound on the probability $P(E_i)$ in (12) of erroneously picking a set which differs from the true defective set in i items.

Theorem III.2 *The probability of the error event E_i defined in (12) that a set which differs from the defective set S_1 in exactly i items is selected by the ML decoder (averaged over all codebooks and test outcomes) is bounded from above by*

$$P(E_i) \leq \binom{N-K}{i}^\rho \binom{K}{i}^\rho \left\{ \sum_Y \sum_{X_{\mathcal{S}^2}} \left[\sum_{X_{\mathcal{S}^1}} Q(X_{\mathcal{S}^1}) p(Y, X_{\mathcal{S}^2} | X_{\mathcal{S}^1})^{\frac{1}{1+\rho}} \right]^{1+\rho} \right\}^T \quad 0 \leq \rho \leq 1$$

where $X_{\mathcal{S}^1}$ and $X_{\mathcal{S}^2}$ are any disjoint partitions of the $K \times 1$ input X_{S_1} of lengths $i \times 1$ and $(K-i) \times 1$, respectively.

Proof: First note that

$$p(\boldsymbol{X}_{S_1}, Y) = p(\boldsymbol{X}_{S_{1,\omega}}, \boldsymbol{X}_{S_{1,\omega^c}}, Y) = p(\boldsymbol{X}_{\sigma(S_{1,\omega})}, \boldsymbol{X}_{\sigma(S_{1,\omega^c})}, Y)$$

for any permutation σ permuting the codewords across items. Also define $[\boldsymbol{X}_{S_1}]$ as the set of codebooks formed from a particular codebook X_{S_1} and all its permutations, i.e.,

$$[\boldsymbol{X}_{S_1}] = \{\boldsymbol{X}_{S_1} : \boldsymbol{X}_{\sigma(S_1)} = \boldsymbol{X}_{S_1} \text{ for some } \sigma\} \tag{18}$$

The partitions $\boldsymbol{X}_{S_{1,\omega^c}}$ and $\boldsymbol{X}_{S_1^c,\omega}$ are dummy variables, hence, we can bound $P(E_i)$ as

$$P(E_i) \leq \left[\binom{N-K}{i} \binom{K}{i} \right]^{\rho} \sum_{Y^T} \sum_{\boldsymbol{X}_{S_{1,\omega}}} \left[\sum_{\boldsymbol{X}} Q(\boldsymbol{X}) p(Y^T, \boldsymbol{X}_{S_{1,\omega}} | \boldsymbol{X})^{\frac{1}{1+\rho}} \right]^{1+\rho} \tag{22}$$

By time independence

$$Q(\boldsymbol{X}) = \prod_{t=1}^{T} Q(X(t))$$

where $X(t)$ is an $i \times 1$ vector corresponding to the t-th time instant. Assume $X(t)$ takes values X. Similar argument holds for Y and $X_{S_{1,\omega}}$. By time independence and the memoryless property of the channel, the bound simplifies to

$$P(E_i) \leq \left[\binom{N-K}{i} \binom{K}{i} \right]^{\rho} \left\{ \sum_{Y \in \{0,1\}} \sum_{X_{S_{1,\omega}}} \left[\sum_{X} Q(X) p(Y, X_{S_{1,\omega}} | X)^{\frac{1}{1+\rho}} \right]^{1+\rho} \right\}^{T} \tag{23}$$

Note that, since all codewords are generated independently and identically, as far as it matters to the bounding of the error probability $P(E_i)$, X and $X_{S_{1,\omega}}$ are now dummy vectors denoting any disjoint partitions of the encoded message X_{S_1} of lengths i and $K-i$, respectively. Hence,

$$P(E_i) \leq 2^{-T\left(E_o - \frac{\rho \log \binom{N-K}{i}\binom{K}{i}}{T}\right)} \tag{24}$$

where,

$$E_o = -\log \sum_{Y \in \{0,1\}} \sum_{X_{\mathcal{S}^2}} \left[\sum_{X_{\mathcal{S}^1}} Q(X_{\mathcal{S}^1}) p(Y, X_{\mathcal{S}^2} | X_{\mathcal{S}^1})^{\frac{1}{1+\rho}} \right]^{1+\rho} \tag{25}$$

for $(\mathcal{S}^1, \mathcal{S}^2) \in \Xi_S^{\{i\}}$ defined in (14), proving Theorem III.2. ∎

Proof of Theorem III.1: Now we can readily prove our main result. First, we need to derive a sufficient condition for the error exponent of the error probability $P(E_i)$ in (24) to be positive, i.e.,

$$f(\rho) = E_o(\rho) - \frac{\rho \log \binom{N-K}{i}\binom{K}{i}}{T} > 0 \tag{26}$$

where $E_o(\rho)$ is defined in (25). We state the result in the following lemma.

Lemma III.3 *A sufficient condition for the error exponent in (24) to be positive is*

$$T > \frac{\log \binom{N-K}{i}\binom{K}{i}}{I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y)}$$

where $I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y)$ is the mutual information between $X_{\mathcal{S}^1}$ and $(X_{\mathcal{S}^2}, Y)$.

Proof: Note that $f(0) = 0$. We follow the argument in [26] here. Since the function $f(\rho)$ is infinitely differentiable and has a power series expansion, for a sufficiently small δ, we get by Taylor series expansion in the neighborhood of $\rho \in [0, \delta]$ that,

$$f(\rho) = f(0) + \rho \frac{df}{d\rho}\Big|_{\rho=0} + O(\rho^2)$$

But we can show that

$$\frac{\partial E_o}{\partial \rho}\Big|_{\rho=0} = \sum_Y \sum_{X_{\mathcal{S}^2}} \left[\sum_{X_{\mathcal{S}^1}} Q(X_{\mathcal{S}^1}) p(Y, X_{\mathcal{S}^2}|X_{\mathcal{S}^1}) \log p(Y, X_{\mathcal{S}^2}|X_{\mathcal{S}^1}) \right.$$
$$\left. - \sum_{X_{\mathcal{S}^1}} Q(X_{\mathcal{S}^1}) p(Y, X_{\mathcal{S}^2}|X_{\mathcal{S}^1}) \log \sum_{X_{\mathcal{S}^1}} Q(X_{\mathcal{S}^1}) p(Y, X_{\mathcal{S}^2}|X_{\mathcal{S}^1}) \right] \tag{27}$$

which simplifies to

$$\frac{\partial E_o}{\partial \rho}\Big|_{\rho=0} = \sum_Y \sum_{X_{\mathcal{S}^2}} \sum_{X_{\mathcal{S}^1}} Q(X_{\mathcal{S}^1}) p(Y, X_{\mathcal{S}^2}|X_{\mathcal{S}^1}) \log \frac{p(Y, X_{\mathcal{S}^2}|X_{\mathcal{S}^1})}{\sum_{X_{\mathcal{S}^1}} Q(X_{\mathcal{S}^1}) p(Y, X_{\mathcal{S}^2}|X_{\mathcal{S}^1})}$$
$$= I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y) \tag{28}$$

We have just shown that $\frac{df}{d\rho} > 0$ at $\rho = 0$ if $\frac{\log \binom{N-K}{i}\binom{K}{i}}{T} < I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y)$. Since $\frac{df}{d\rho}$ is a continuous function of ρ, there exists a δ neighborhood around zero such that $\frac{df}{d\rho} > 0$ for $\rho \in [0, \delta]$. Thus, $f(\rho) > 0$ for sufficiently small ρ. ■

We have just shown that $T > \frac{\log \binom{N-K}{i}\binom{K}{i}}{I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y)}$ is sufficient to ensure an arbitrarily small $P(E_i)$. Since the average error probability $P_e \leq \sum_{i=1}^{K} P(E_i)$, it follows that for any fixed K, $\lim_{N \to \infty} \sum_{i=1}^{K} P(E_i) = 0$. Consequently, since this is true for any K, $\lim_{K \to \infty} \lim_{N \to \infty} \sum_{i=1}^{K} P(E_i) = 0$. Hence, Theorem III.1 now follows.

General case where $K = o(N)$:

To this end, we would like to explicitly differentiate between 2 different scaling regimes considered in the paper. The result of Theorem III.1 we just presented provides a sufficient condition for the case where *N scales to infinity for every fixed K* ensuring that

$$\lim_{K \to \infty} \lim_{N \to \infty} P_e \to 0$$

However, we point out that the result in Theorem III.1 can be extended to the more general case where *both N and K are allowed to scale simultaneously such that $K = o(N)$*. We first note that from the Lagrange form of the Taylor Series expansion (essentially an application of the mean value theorem) we can write $E_o(\rho)$ in terms of its first derivative evaluated at zero and a remainder term, i.e.,

$$E_o(\rho) = E_o(0) + \rho E_o'(0) + \frac{\rho^2}{2} (E_o)''(\psi)$$

for some $\psi \in [0, \rho]$. We have already shown that $E_o(0) = 0$ and $E_o'(0) = I(X_{\mathcal{S}^1}; Y \mid X_{\mathcal{S}^2}) > 0$. Consequently, we need to lower bound $E_o(\rho)$ by taking the worst-case second derivative. Establishing this result requires a more careful analysis and hence we present it in Appendix C. It is shown that the same sufficient condition on the number of tests T in Theorem III.1 holds up to an extra polylog(K) factor for an arbitrarily small average error probability, namely,

$$\lim_{\substack{N \to \infty \\ K = o(N)}} P_e \to 0$$

Relation to channel coding:

The mutual information $I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y)$ between $X_{\mathcal{S}^1}$ and $(X_{\mathcal{S}^2}, Y)$ is the relative entropy between the joint distribution $p(X_{\mathcal{S}^1}, X_{\mathcal{S}^2}, Y)$ and the product distribution $p(X_{\mathcal{S}^1})p(X_{\mathcal{S}^2}, Y)$. It is a measure of the amount of information that the variables $X_{\mathcal{S}^2}$ and Y contain about $X_{\mathcal{S}^1}$ [24]. Intuitively this means that the upper bound on the error probability $P(E_i)$, where the event E_i represents the event that the decoded set is misclassified in exactly i items (replacing i codewords of the true set with i independent codewords), scales exponentially with the negative of the per-test mutual information between i codewords of the set, and the remaining $K - i$ codewords and the output.

It is worthwhile mentioning that in the classical channel coding problem [24], [26], the error probability analysis for Maximum Likelihood or Typical Set Decoding separates well due to the independence of the channel output and every codeword other than the truly transmitted one. However, in the group testing problem, a main difficulty arises from the fact that an arbitrary set of K items and the true defective set could be overlapping. Hence, independence of the output and the collection of codewords indexed by that set does not hold anymore. That required introducing the previous machinery to analyze the error probability. Two ingredients that were key to our analysis are

1) Separating the error events E_i of misclassifying the defective set in i items
2) For every i, we averaged over realizations of ensemble of codewords of every candidate set while holding fixed the partition common to these sets and the true set of defectives.

Further Intuition: Intuitively, the numerator in Theorem III.1 represents the number of bits required to describe how many sets we can form with i misclassified items (i out K), and the denominator represents the amount of information per test if $K - i$ of the defective items are known. One key idea behind the described approach is illustrated in Fig. 4. The group testing problem has been mapped to an equivalent multiple channel model. Each channel accounts for the case where $K - i$ of the defective items are recovered and i items are still to be recognized, where $K - i$ represents the overlap between the true defective set and a false candidate set. The capacity of each channel contributes partially to the total
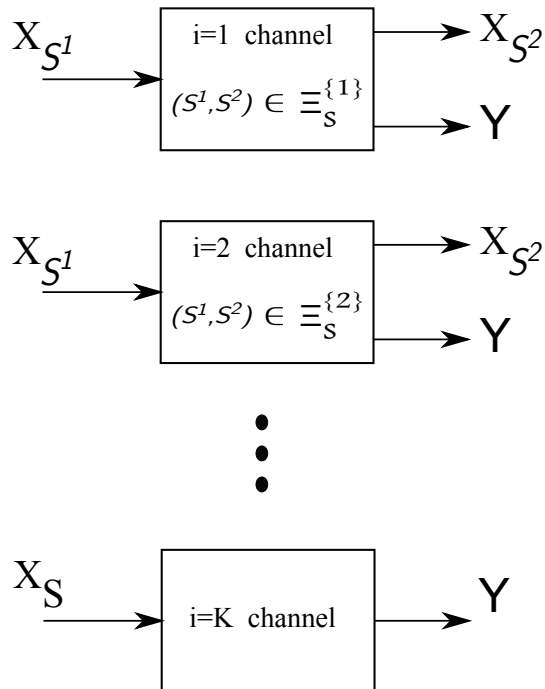
Fig. 4. Equivalent channel model. Each channel accounts for the case, where $K - i$ of the defective items are recovered and i items are still to be recognized. The capacity of each channel contributes partially to the total error probability in decoding the true defective set. $K - i$ represents the overlap between the true defective set and a false candidate set.

error probability in decoding the true defective set. By studying each error channel separately, we upper bound the overall error probability.

The previous result is a simple mutual information expression that can be used to determine the tradeoffs between K, N, T, and noise for various models as we show in the following sections. We are interested in determining the required number of tests T to achieve an arbitrarily small error probability for the 2 aforementioned scaling regimes for different models and different performance criteria. The probability p is a test design parameter, so we choose $p = \frac{1}{K}$. Table I summarizes the scaling results for the considered models for the average error and worst case error criteria. Note that the number of tests increases by $1/(1-u)^2$ factor for the dilution model and only by $1/(1-q)$ for the additive noise model which matches the aforementioned intuition.

IV. LOWER BOUND: FANO'S INEQUALITY

In this section we also derive lower bounds on the required number of tests using Fano's inequality [24]. We state the following theorem

Theorem IV.1 *For N items and a set S_ω of K defectives, a lower bound on the total number of tests required to recover the defective set is given by*

$$T \geq \max_{i:(\mathcal{S}^1, \mathcal{S}^2) \in \Xi_{S_\omega}^{\{i\}}} \frac{\log \binom{N-K+i}{i}}{I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y)}, \quad i = 1, 2, \ldots K \tag{29}$$

where Y is a binary random variable denoting a test outcome, X_{S_ω} is the per-test input indexed by S_ω, and the set $\Xi_S^{\{i\}}$ is the set of tuples $(\mathcal{S}^1, \mathcal{S}^2)$ partitioning the set S into disjoint sets $\mathcal{S}^1$ and $\mathcal{S}^2$ with cardinalities i and $K - i$, respectively as defined in (14).

Proof: The tests outcomes Y^T is probabilistically related to the index $\omega \in \mathcal{I} = \{1, 2, \ldots, \binom{N}{K}\}$. Suppose $K - i$ codewords $\boldsymbol{X}_{\mathcal{S}^2}$, corresponding to $K - i$ items, are revealed to us. From Y^T we estimate the defective set ω. Let the estimate be $\hat{\omega} = g(Y^T)$. Define the probability of error

$$P_e = \Pr[\hat{\omega} \neq \omega]$$

If E is a binary random variable that takes the value 1 in case of an error i.e., if $\hat{\omega} \neq \omega$, and 0 otherwise. Then using the chain rule of entropies [24] [26] we have

$$H(E, \omega | Y^T, \boldsymbol{X}_{\mathcal{S}^2}) = H(\omega | Y^T, \boldsymbol{X}_{\mathcal{S}^2}) + H(E | \omega, Y^T, \boldsymbol{X}_{\mathcal{S}^2})$$
$$= H(E | Y^T, \boldsymbol{X}_{\mathcal{S}^2}) + H(\omega | E, Y^T, \boldsymbol{X}_{\mathcal{S}^2}) \tag{30}$$

The random variable E is fully determined given Y^T and ω. It follows that $H(E | \omega, Y^T, \boldsymbol{X}_{\mathcal{S}^2}) = 0$. Since E is a binary random variable $H(E | Y^T, \boldsymbol{X}_{\mathcal{S}^2}) \leq 1$. Consequently we can bound $H(\omega | E, Y^T, \boldsymbol{X}_{\mathcal{S}^2})$ as follows

$$H(\omega | E, Y^T, \boldsymbol{X}_{\mathcal{S}^2}) = P(E=0) H(\omega | E=0, Y^T, \boldsymbol{X}_{\mathcal{S}^2}) + P(E=1) H(\omega | E=1, Y^T, \boldsymbol{X}_{\mathcal{S}^2})$$
$$\leq (1 - P_e) 0 + P_e \log \left(\binom{N-K+i}{i} - 1 \right)$$
$$\leq P_e \log \binom{N-K+i}{i} \tag{31}$$

The second inequality follows from the fact that revealing $K - i$ items, and given that $E = 1$, the conditional entropy can be upper bounded by the logarithm of the number of outcomes. From (30), we obtain the genie aided Fano's inequality

$$H(\omega | Y^T, \boldsymbol{X}_{\mathcal{S}^2}) \leq 1 + P_e \log \binom{N-K+i}{i} \tag{32}$$

Since for a fixed code $\boldsymbol{X}_{S_\omega}$ is a function of ω, then

$$H(\boldsymbol{X}_{S_\omega} | Y^T, \boldsymbol{X}_{\mathcal{S}^2}) \leq H(\omega | Y^T, \boldsymbol{X}_{\mathcal{S}^2})$$

and hence

$$H(\boldsymbol{X}_{S_\omega}|Y^T, \boldsymbol{X}_{\mathcal{S}^2}) \leq 1 + P_e \log \binom{N-K+i}{i} \tag{33}$$

Since the set $\mathcal{S}^2$ of $K - i$ defectives is revealed, ω is uniformly distributed over the set of indices that correspond to subsets of size K containing $\mathcal{S}^2$. It follows that

$$\log \binom{N-K+i}{i} = H(\omega|\boldsymbol{X}_{\mathcal{S}^2}) = H(\omega|Y^T, \boldsymbol{X}_{\mathcal{S}^2}) + I(\omega; Y^T|\boldsymbol{X}_{\mathcal{S}^2})$$

$$\leq 1 + P_e \log \binom{N-K+i}{i} + I(\boldsymbol{X}_{S_\omega}; Y^T|\boldsymbol{X}_{\mathcal{S}^2}) \tag{34}$$

Since $S_\omega = \mathcal{S}^1 \cup \mathcal{S}^2$, where $(\mathcal{S}^1, \mathcal{S}^2) \in \Xi_{S_\omega}^{\{i\}}$, we have

$$P_e \geq 1 - \frac{I(\boldsymbol{X}_{\mathcal{S}^1}; Y^T|\boldsymbol{X}_{\mathcal{S}^2}) + 1}{\log \binom{N-K+i}{i}} \tag{35}$$

Thus, for the probability of error to be asymptotically bounded away from zero, it is necessary that

$$\log \binom{N-K+i}{i} \leq I(\boldsymbol{X}_{\mathcal{S}^1}; Y^T|\boldsymbol{X}_{\mathcal{S}^2}) \tag{36}$$

Following a standard set of inequalities we have

$$\log \binom{N-K+i}{i} \leq I(\boldsymbol{X}_{\mathcal{S}^1}; Y^T|\boldsymbol{X}_{\mathcal{S}^2})$$

$$= H(Y^T|\boldsymbol{X}_{\mathcal{S}^2}) - H(Y^T|\boldsymbol{X}_{S_\omega})$$

$$\overset{(a)}{=} \sum_{t=1}^{T} H(Y(t)|Y^{t-1}, \boldsymbol{X}_{\mathcal{S}^2}) - H(Y(t)|X_{S_\omega}(t))$$

$$\overset{(b)}{\leq} \sum_{t=1}^{T} H(Y(t)|X_{\mathcal{S}^2}(t)) - H(Y(t)|X_{S_\omega}(t))$$

$$= \sum_{t=1}^{T} I(X_{S_\omega}(t); Y(t)|X_{\mathcal{S}^2}(t))$$

$$= \sum_{t=1}^{T} I(X_{\mathcal{S}^1}(t); Y(t)|X_{\mathcal{S}^2}(t))$$

$$\overset{(c)}{=} T I(X_{\mathcal{S}^1}; Y|X_{\mathcal{S}^2})$$

$$\overset{(d)}{=} T I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y) \tag{37}$$

In (a) we made use of the chain rule for entropy and the memoryless property of the channel and (b) is true since conditioning reduces entropy. (c) is due to the i.i.d. assumption. Finally, (d) follows from the

chain rule for mutual information and the independence of the codewords, i.e.,

$$I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y) = I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}) + I(X_{\mathcal{S}^1}; Y | X_{\mathcal{S}^2}) \tag{38}$$

and $I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}) = 0$.

Since (37) has to be true for all i, a necessary condition on the total number of tests is given by

$$T \geq \max_{i:(\mathcal{S}^1, \mathcal{S}^2) \in \Xi_{S_\omega}^{\{i\}}} \frac{\log \binom{N-K+i}{i}}{I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y)} \tag{39}$$

proving theorem IV.1. ∎

Remark IV.1 *Note that the bound in Theorem III.1 is achievable when $N \to \infty$ for every fixed K. As pointed out earlier, for the case where both N and K scale simultaneously with $K = o(N)$, which parallels the lower bound in Theorem IV.1, the achievable bound has an extra polylog factor in K. Unlike the lower bound in Theorem IV.1, our achievability result is an order result. However, the mutual information expression in the denominator in Theorem IV.1 matches the mutual information expression in the achievable bound in Theorem III.1. Furthermore, since the combinatorial terms in the numerators have a similar asymptotic scaling, the achievable bound and the lower bound are order-wise tight in the asymptotic regime considered in this paper up to a small polylog factor.*

Remark IV.2 *According to this lower bound, it is not hard to see that for the noise free case $T \geq c \cdot K \log \left(\frac{N}{K}\right)$, for some positive constant c, is a necessary condition on the total number of tests.*

V. NOISE FREE CASE-DETERMINISTIC OUTPUT

In this section, we consider the noise-free (deterministic) case: the test outcome Y is 1 if and only if a defective item is pooled in that test. Hence Y is give by (2). We consider two scenarios: average and worst-case error. As mentioned earlier, the former requires the average error to be small and the latter considers the worst-case input since bounding the average error probability does not guarantee error-free performance for all possible defective sets.

A. Average Error Probability

Theorem V.1 *For N items and K defectives, the number of tests $T = O(K \log N)$ is sufficient to satisfy an average error criterion, i.e., achieve an arbitrarily small average error probability. In other words, there is a constant c independent of N and K such that if $T = cK \log N$ then the probability of errors goes to zero.*

Proof: In the noise free case, if S is the defective set, then $H(Y|X_S) = 0$, where $H(Y|X_S)$ is the conditional entropy of Y given X_S [24]. The conditional entropy $H(Y|X)$ of a random variable Y given another random variable X is formally defined as the negative of the expected value of the logarithm of the conditional probability $p(Y|X)$, i.e.,

$$H(Y|X) = -E\log(p(Y|X)$$

and hence $H(Y|X_S)$ is a measure of uncertainty of the test outcome Y given the input X_S corresponding to the defective set S. In other words, since we are dealing with a noise-free channel, Y is determined with certainty if we know that X_S was "transmitted". For a given i and any $(\mathcal{S}^1, \mathcal{S}^2) \in \Xi_S^{\{i\}}$, the mutual information expression $I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y)$ can be written as

$$
\begin{aligned}
I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y) &= H(Y|X_{\mathcal{S}^2}) - H(Y|X_S) \\
&= (1-p)^{K-i} H((1-p)^i) \\
&\geq \left(1 - \frac{1}{K}\right)^{K-i} \left(1 - \frac{1}{K}\right)^i \log \frac{1}{(1-\frac{1}{K})^i}
\end{aligned}
\tag{40}
$$

Thus, for large K,

$$I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y) \geq e^{-1} \frac{i}{K \ln 2} = \Theta\left(\frac{i}{K}\right)$$

Now we upper bound the numerator in Theorem III.1.

$$
\begin{aligned}
\log \binom{N-K}{i}\binom{K}{i} &\leq (N-K) \left[\frac{i}{N-K} \log \frac{N-K}{i} + \left(1 - \frac{i}{N-K}\right) \log \frac{1}{1 - \frac{i}{N-K}} \right] \\
&\quad + K \left[\frac{i}{K} \log \frac{K}{i} + \left(1 - \frac{i}{K}\right) \log \frac{1}{1 - \frac{i}{K}} \right] \\
&\leq i \log N + \frac{1}{\ln 2}(N-K)\left(1 - \frac{i}{N-K}\right) \sum_{j=1}^{\infty} \frac{1}{j}\left(\frac{i}{N-K}\right)^j \\
&\quad + i \log K + \frac{1}{\ln 2} K \left(1 - \frac{i}{K}\right) \sum_{j=1}^{\infty} \frac{1}{j}\left(\frac{i}{K}\right)^j \\
&\leq i \log N + \frac{i}{\ln 2} - \frac{1}{\ln 2} \sum_{j=2}^{\infty} \frac{1}{j(j-1)} \frac{i^j}{(N-K)^{j-1}} \\
&\quad + i \log K + \frac{i}{\ln 2} - \frac{1}{\ln 2} \sum_{j=2}^{\infty} \frac{1}{j(j-1)} \frac{i^j}{(K)^{j-1}} \\
&= \Theta(i \log N)
\end{aligned}
\tag{41}
$$

Hence, from Theorem III.1, $T = O(K \log N)$ is sufficient.

Theorem VIII.1 in Appendix C provides a sufficient condition on the total number of tests T for the noiseless case when both N and K scale simultaneously with $K = o(N)$. This amounts to an extra $\log^2 K$ factor in the final scaling. This polylog factor introduces some conservatism but appears difficult to avoid based on the bounding techniques that we employ for bounding the error exponents.

B. Maximum Probability of error

The previous analysis considered the average error case. Maintaining the average error probability below ϵ is not enough if we are interested in the worst-case input, i.e. maximum error case. For exact reconstruction, the worst-case error is required to be zero.

Theorem V.2 *For N items and K defectives, $T = O(K^2 \log N)$ is achievable for exact reconstruction (worst-case error criteria).*

Proof: Since the average error probability is below ϵ, then:

$$P_e = \sum_{\mathcal{C}} \Pr[\mathcal{C}]\lambda(\mathcal{C}) < \epsilon \to \exists \mathcal{C} : \lambda(\mathcal{C}) < \epsilon \tag{42}$$

to say that, since the average probability of error (over codebooks and inputs) is below ϵ, then there exist a codebook $\mathcal{C}$ such that $\lambda(\mathcal{C}) = \frac{1}{\binom{N}{K}} \sum_v \lambda_v(\mathcal{C}) < \epsilon$. Choosing $\epsilon = \frac{1}{\binom{N}{K}}$ guarantees that the worst case error is also 0 since for the noiseless case $\lambda_v \in \{0, 1\}$.

If $f(\rho)$ denotes the exponent of the error probability $P(E_i)$ in (24), and noting that $f(0) = 0$, we get by the Lagrange form of the Taylor series expansion in the neighborhood of zero that

$$f(\rho) = \rho \frac{df}{d\rho} + O(\rho^2)$$

where

$$\frac{df}{d\rho} = I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y) - \frac{\log \binom{N-K}{i}\binom{K}{i}}{T}$$

Hence, the existence of a good codebook combined with the conditions $P(E_i) < \frac{1}{\binom{N}{K}}, \forall i$, ensure perfect reconstruction, i.e.,

$$2^{-T(\rho(I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y) - \frac{\log \binom{N-K}{i}\binom{K}{i}}{T}) + O(\rho^2))} < \frac{1}{\binom{N}{K}} \tag{43}$$

which asymptotically translates to the sufficient condition

$$\Omega\left(\frac{i}{K}\right) - \frac{\Theta(i \log N)}{T} - \frac{\Theta(K \log N)}{T} > 0$$

and $T = O(K^2 \log N)$ is achievable. Note that we have ignored the $O(\rho^2)$ term in deriving this result. Nevertheless, it follows from Lemma VIII.1 in Appendix C that this term is not dominant and consequently the result follows.

∎

VI. ACHIEVABILITY WITH DISTORTION

In this section we relax our goal. We are satisfied with recovering a large fraction of the defective items. In other words, we allow an approximate reconstruction [22] in the sense that if K candidates are declared, up to αK misses are allowed (α small).

Theorem VI.1 *If N is the total number of items and K the size of the defective set, approximate reconstruction of the defective set, i.e., with up to αK misses, is achievable with $T = O(K \log N)$.*

Proof: In this case, $P_e \leq \sum_{i=\alpha K}^{K} P(E_i)$. Using an argument analogous to (43), we verify the error exponent of $P(E_i)$. Since the smallest i is $\Theta(K)$, the sufficient condition on T becomes

$$\frac{\Theta(K \log N)}{T} > \text{constant}$$

Hence, $T = O(K \log N)$. ∎

VII. NOISY GROUP TESTING

The derived upper bound in Thm. III.1 is fairly general as it maps the group testing problem to an equivalent channel model. This does not restrict the model to the noise-free scenario and hence could also be used to account for different noisy versions of the problem. The question reduces to how easy it is to compute the mutual information expression. In this section, we derive sufficient conditions on the number of tests for two types of noisy channels. It is to be noted that the result could also be applied to other noise models.

A. Additive Observation Noise

First, we consider the additive output model of Eq.4, i.e.,

$$Y(t) = \left(\bigvee_{i=1}^{N} X_i(t) R_i \right) \vee W(t)$$

where W is Bernoulli(q). This model captures the possibility of probabilistic false alarms. This accounts for errors in blood tests or background wireless losses [6] etc.

Now we state the following theorem:

Theorem VII.1 *For the additive noise model in (4), N items, K defectives, $T = O\left(\frac{K \log N}{1-q}\right)$ is achievable, where q is the parameter of the bernoulli distribution of the binary noise.*

Note: As q increases, the number of tests required to identify the defective set increases since the outcome of a pooling test becomes less reliable due to false alarms.

Proof: Consider any partition $(\mathcal{S}^1, \mathcal{S}^2) \in \Xi_S^{\{i\}}$. Unlike the noise-free model, the conditional entropy $H(Y|X_S)$ is no longer zero. Although, the test outcome is certainly positive if X_S is anything but the all-zero vector, the test outcome is uncertain if X_S is all zero due to the additive noise. Then

$$
\begin{aligned}
I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y) &= H(Y|X_{\mathcal{S}^2}) - H(Y|X_S) \\
&= (1-p)^{K-i} H\left((1-p)^i(1-q)\right) - (1-p)^K H(q) \\
&= (1-p)^{K-i} \left[H\left((1-p)^i(1-q)\right) - (1-p)^i H(q)\right]
\end{aligned}
\tag{44}
$$

The first entropy term in (44) can be written as

$$
H\left((1-p)^i(1-q)\right) = (1-p)^i(1-q)\log\frac{1}{(1-p)^i(1-q)} + (1 - (1-p)^i(1-q))\log\frac{1}{1-(1-p)^i(1-q)}
$$

$$
= i\left(1-\frac{1}{K}\right)^i(1-q)\log\left(\frac{1}{1-\frac{1}{K}}\right) + \left(1-\frac{1}{K}\right)^i(1-q)\log\left(\frac{1}{1-q}\right) + \sum_{j=1}^{\infty}\frac{1}{j\ln 2}\left(1-\frac{1}{K}\right)^{ji}(1-q)^j
$$

$$
- \frac{1}{\ln 2}\left(1-\frac{1}{K}\right)^i(1-q)\left[\sum_{j=1}^{\infty}\frac{1}{j}\left(1-\frac{1}{K}\right)^{ji}(1-q)^j\right]
\tag{45}
$$

where the last equality is obtained through simple Taylor series expansion. Expanding the second entropy term in (44) we get

$$
(1-p)^i H(q) = \left(1-\frac{1}{K}\right)^i q\log\frac{1}{q} + \left(1-\frac{1}{K}\right)^i(1-q)\log\frac{1}{1-q}
\tag{46}
$$

Subtracting (45) and (46), and multiplying by $(1-p)^{K-i}$, the mutual information expression simplifies

to

$$I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y) = \left(1 - \frac{1}{K}\right)^{K-i} \left[\frac{i}{\ln 2} \left(1 - \frac{1}{K}\right)^i (1-q) \left(\sum_{j=1}^{\infty} \frac{1}{jK^j}\right) + \frac{1}{\ln 2} \left(1 - \frac{1}{K}\right)^i (1-q) \right.$$

$$\left. - \frac{1}{\ln 2} \left(\sum_{j=2}^{\infty} \frac{1}{j(j-1)} \left(1 - \frac{1}{K}\right)^{ji} (1-q)^j\right) - \left(1 - \frac{1}{K}\right)^i q \log \frac{1}{q} \right]$$

$$\geq \frac{i}{\ln 2} \left(1 - \frac{1}{K}\right)^K (1-q) \left(\sum_{j=1}^{\infty} \frac{1}{jK^j}\right) + \frac{1}{\ln 2} \left(1 - \frac{1}{K}\right)^K (1-q)$$

$$- \frac{1}{\ln 2} \left(1 - \frac{1}{K}\right)^K \left[\sum_{j=2}^{\infty} \frac{(1-q)^j}{j(j-1)}\right] - \left(1 - \frac{1}{K}\right)^K q \log \frac{1}{q} \tag{47}$$

Now note that

$$\sum_{j=2}^{\infty} \frac{(1-q)^j}{j(j-1)} = 1 - q - q \ln 2 \log \frac{1}{q} \tag{48}$$

This is not hard to verify since

$$\begin{aligned}
\frac{(1-q)^2}{2} + \frac{(1-q)^3}{6} + \ldots &= (1-q)^2 \left(1 - \frac{1}{2}\right) + (1-q)^3 \left(\frac{1}{2} - \frac{1}{3}\right) + \ldots \\
&= (1-q) \left(1 - q + \frac{(1-q)^2}{2} + \ldots\right) - \left(\frac{(1-q)^2}{2} + \frac{(1-q)^3}{3} + \ldots\right) \\
&= (1-q) \ln 2 \log \frac{1}{q} - \left(\ln 2 \log \frac{1}{q} - (1-q)\right) \\
&= 1 - q - q \ln 2 \log \frac{1}{q} \tag{49}
\end{aligned}$$

Replacing in (47) we get

$$I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y) \geq \frac{i}{K \ln 2} \left(1 - \frac{1}{K}\right)^K (1-q) \tag{50}$$

Following the same argument in the proof of theorem V.1, replacing (50) and (41) in Theorem III.1, we have that $T \leq \frac{K \ln 2 \log N}{1-q}$, i.e., $T = O\left(\frac{K \log N}{1-q}\right)$ is achievable. ∎

The same scaling holds for the regime where N and K simultaneously approach infinity with $K = o(N)$. This follows immediately from Lemma VIII.4 and the Lagrange form of the Taylor series expansion of the error exponent in Lemma VIII.1 in Appendix C.

Remark VII.1 *Following the same argument in Section V-B, it is not hard to see that the same scaling holds for the worst case error criteria but replacing K with K^2 as shown in table I. Recall that the worst-case error criterion implied exact recovery in the noise-free model. Exact recovery emerged from*

the fact that if the average probability of error using a randomly generated codebook is bounded from above by some ϵ, then there exist a good *codebook as argued in Section V-B. Hence choosing such a "good" codebook by design, and by proper choice of ϵ, we could guarantee exact recovery for the worst case input in the noise-free model. However, in this noisy setup, the worst case error criteria only means that the worst-case error probability goes to zero in contrast to the noise-free case where this scaling ensured exact reconstruction of the defective set.*

The next theorem establishes a necessary condition on the number of tests for the additive noise model.

Theorem VII.2 *Considering the additive noise model in (4), a total number of items N and K defectives, a necessary condition for the number of tests is that*

$$T = \Omega \left(\frac{K \log \frac{N}{K}}{2(1-q) + \ln(\frac{1}{q})} \right)$$

where q is the parameter of the bernoulli distribution of the binary noise. Namely, if $T = o \left(\frac{K \log \frac{N}{K}}{2(1-q)+\ln(\frac{1}{q})} \right)$ then the error probability approaches 1.

Proof: See Appendix B ∎

B. Dilution

The second noisy model we consider is the "dilution" model. Positive items taking part in a given test might probabilistically behave as absent (diluted). If all positive items in a given test appear as absent that could potentially lead to erroneously zero outcomes. This model is motivated by blood dilution due to pooling with other negative tests, or imperfectly diluted blood samples, or adversarial camouflage-in the form of probabilistic transmission-in communication systems [6]. This is captured by the Z-channel model of Fig. 3. For this case, we show that $T = O(\frac{K \log N}{(1-u)^2})$ is achievable. Intuitively, a larger flip probability u implies that more items will get diluted. As the tests become less reliable, a larger number of tests is needed to identify the defective set.

Theorem VII.3 *Considering N items, K defectives and the dilution model represented by the Z-channel in Fig.(3) and (5), a number of tests $T = \frac{K \log N}{(1-u)^2}$ is achievable, where u is the transition probability of the Z-channel (i.e. the probability that 1 is flipped into 0).*

Proof: For notational convenience we let $u = 1 - s$. Again, consider a partition $(\mathcal{S}^1, \mathcal{S}^2) \in \Xi_S^{\{i\}}$

$$
I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y) = H(Y|X_{\mathcal{S}^2}) - H(Y|X_S)
$$

$$
= \sum_{j=0}^{K-i} \binom{K-i}{j} \left(\frac{1}{K}\right)^j \left(1 - \frac{1}{K}\right)^{K-i-j} H\left(\sum_{\ell=0}^{i} \binom{i}{\ell}(1-s)^{j+\ell} \left(\frac{1}{K}\right)^{\ell} \left(1 - \frac{1}{K}\right)^{i-\ell}\right)
$$

$$
- \sum_{j=1}^{K} \binom{K}{j} \left(\frac{1}{K}\right)^j \left(1 - \frac{1}{K}\right)^{K-j} H\left((1-s)^j\right) \tag{51}
$$

The first sum i.e., $H(Y|X_{\mathcal{S}^2})$, can be written as

$$
H(Y|X_{\mathcal{S}^2}) = \sum_{j=0}^{K-i} \binom{K-i}{j} \left(\frac{1}{K}\right)^j \left(1 - \frac{1}{K}\right)^{K-i-j} H\left((1-s)^j(1-\frac{s}{K})^i\right)
$$

$$
= \sum_{j=0}^{K-i} \binom{K-i}{j} \left(\frac{1}{K}\right)^j \left(1 - \frac{1}{K}\right)^{K-i-j} \left[(1-s)^j(1-\frac{s}{K})^i \log \frac{1}{(1-s)^j(1-\frac{s}{K})^i}\right]
$$

$$
+ \sum_{j=0}^{K-i} \binom{K-i}{j} \left(\frac{1}{K}\right)^j \left(1 - \frac{1}{K}\right)^{K-i-j} \left[\left(1 - (1-s)^j(1-\frac{s}{K})^i\right) \log \frac{1}{1 - (1-s)^j(1-\frac{s}{K})^i}\right]
$$

$$
= \eta_1 + \eta_2 \tag{52}
$$

Notice that

$$
\sum_{j=0}^{K-i} \binom{K-i}{j} \left(\frac{1}{K}\right)^j \left(1 - \frac{1}{K}\right)^{K-i-j} (1-s)^j = \left(1 - \frac{s}{K}\right)^{K-i} \tag{53}
$$

$$
\sum_{j=0}^{K-i} j \cdot \binom{K-i}{j} \left(\frac{1}{K}\right)^j \left(1 - \frac{1}{K}\right)^{K-i-j} (1-s)^j = \frac{1}{K}(K-i)(1-s)\left(1 - \frac{s}{K}\right)^{K-i-1} \tag{54}
$$

Using (53) and (54), the first term η_1 in (52) simplifies to

$$
\eta_1 = i(1 - \frac{s}{K})^K \log(\frac{1}{1 - \frac{s}{K}}) + \frac{1}{K}(K-i)(1 - \frac{s}{K})^{K-1}(1-s) \log \frac{1}{1-s} \tag{55}
$$

The second sum in (51) i.e., $H(Y|X_S)$, simplifies to

$$
H(Y|X_S) = \sum_{j=0}^{K} \binom{K}{j} \left(\frac{1}{K}\right)^j \left(1 - \frac{1}{K}\right)^{K-j} (1-s)^j \log \frac{1}{(1-s)^j}
$$

$$
+ \sum_{j=0}^{K} \binom{K}{j} \left(\frac{1}{K}\right)^j \left(1 - \frac{1}{K}\right)^{K-j} (1 - (1-s)^j) \log \frac{1}{1 - (1-s)^j}
$$

$$
= \theta_1 + \theta_2 \tag{56}
$$

From (54), the term θ_1 simplifies to

$$
\theta_1 = \frac{1}{K}K(1-s)\left(1 - \frac{s}{K}\right)^{K-1} \log \frac{1}{1-s} \tag{57}
$$

Combining η_1 and θ_1 we get

$$
\begin{aligned}
\eta_1 - \theta_1 &= i\left(1 - \frac{s}{K}\right)^{K-1}\left[\left(1 - \frac{s}{K}\right)\log\frac{1}{1 - \frac{s}{K}} - \frac{1}{K}(1 - s)\log\frac{1}{1 - s}\right] \\
&= \frac{i}{\ln 2}\left(1 - \frac{s}{K}\right)^{K-1}\left[\frac{s}{K} + O\left(\frac{1}{K^2}\right) - \frac{1}{K}(1 - s)\left(s + \frac{s^2}{2} + \ldots\right)\right] \\
&= \frac{i}{\ln 2}\left(1 - \frac{s}{K}\right)^{K-1}\left[\frac{s^2}{K}\left(1 - \frac{1}{2}\right) + \frac{s^3}{K}\left(\frac{1}{2} - \frac{1}{3}\right) + \ldots\right] \\
&\geq \frac{is^2}{2K\ln 2}\left(1 - \frac{s}{K}\right)^{K-1}
\end{aligned}
\tag{58}
$$

Now we consider the remaining terms i.e., η_2 and θ_2. It is sufficient to show that the difference $\eta_2 - \theta_2$ is ≥ 0. First consider the term η_2 in (52)

$$
\begin{aligned}
\eta_2 &= \sum_{j=0}^{K-i}\binom{K-i}{j}\left(\frac{1}{K}\right)^j\left(1 - \frac{1}{K}\right)^{K-i-j}\left[\left(1 - (1-s)^j\left(1 - \frac{s}{K}\right)^i\right)\log\frac{1}{1 - (1-s)^j(1 - \frac{s}{K})^i}\right] \\
&= \frac{1}{\ln 2}\sum_{j=0}^{K-i}\binom{K-i}{j}\left(\frac{1}{K}\right)^j\left(1 - \frac{1}{K}\right)^{K-i-j}\left[1 - (1-s)^j\left(1 - \frac{s}{K}\right)^i\right]\left[\sum_{\ell=1}^{\infty}\frac{1}{\ell}(1-s)^{\ell j}\left(1 - \frac{s}{K}\right)^{\ell i}\right]
\end{aligned}
\tag{59}
$$

From (53), η_2 simplifies to:

$$
\begin{aligned}
\eta_2 &= \frac{1}{\ln 2}\left[\left(1 - \frac{s}{K}\right)^K - \sum_{j=0}^{K-i}\binom{K-i}{j}\left(\frac{1}{K}\right)^j\left(1 - \frac{1}{K}\right)^{K-i-j}\left(\sum_{\ell=2}^{\infty}\frac{1}{\ell(\ell-1)}(1-s)^{\ell j}\left(1 - \frac{s}{K}\right)^{\ell i}\right)\right] \\
&= \frac{1}{\ln 2}\left[\left(1 - \frac{s}{K}\right)^K - \sum_{\ell=2}^{\infty}\frac{1}{\ell(\ell-1)}\left(1 - \frac{s}{K}\right)^{\ell i}\left(1 - \frac{1}{K} + \frac{1}{K}(1-s)^{\ell}\right)^{K-i}\right]
\end{aligned}
\tag{60}
$$

Now consider the term θ_2 in (56),

$$
\begin{aligned}
\theta_2 &= \frac{1}{\ln 2}\left[\left(1 - \frac{s}{K}\right)^K - \sum_{j=0}^{K}\binom{K}{j}\left(\frac{1}{K}\right)^j\left(1 - \frac{1}{K}\right)^{K-j}\left(\sum_{\ell=2}^{\infty}\frac{1}{\ell(\ell-1)}(1-s)^{\ell j}\right)\right] \\
&= \frac{1}{\ln 2}\left[\left(1 - \frac{s}{K}\right)^K - \sum_{\ell=2}^{\infty}\frac{1}{\ell(\ell-1)}\left(1 - \frac{1}{K} + \frac{1}{K}(1-s)^{\ell}\right)^K\right]
\end{aligned}
\tag{61}
$$

Comparing (60) and (61) it is now clear that for large K, the difference $\eta_2 - \theta_2 \geq 0$. This is easy to verify since

$$
\left(1 - \frac{1}{K} + \frac{1}{K}(1-s)^{\ell}\right)^K = \left(1 - \frac{1}{K} + \frac{1}{K}(1-s)^{\ell}\right)^{K-i}\left(1 - \frac{1}{K} + \frac{1}{K}(1-s)^{\ell}\right)^i
$$

and we only need to verify that

$$
\left(1 - \frac{s}{K}\right)^{\ell} < 1 - \frac{1}{K} + (1-s)^{\ell}
\tag{62}
$$

which is obviously true for large K, since the LHS goes to 1 and the RHS goes to $1 + (1 - s)^\ell$ in the limit. Thus, $T = O(\frac{K \log N}{s^2})$ is achievable. Replacing for $s = 1 - u$, Theorem VII.3 follows. ∎

The same result with an extra $\log^2 K$ factor holds for the asymptotic regime where N and K simultaneously approach infinity with $K = o(N)$. This follows immediately from Lemma VIII.5 and the Lagrange form of the Taylor series expansion of the error exponent in Lemma VIII.1 in Appendix C. Again, we point out that this polylog factor introduces some conservatism but appears difficult to avoid based on the bounding techniques that we employ for bounding the error exponents.

Remark VII.2 *Following the same argument in Section V-B using (58) and Lemma VIII.5 it is not hard to see that the same scaling holds for the worst-case error criteria but replacing K with K^2 as shown in table I.*

VIII. CONCLUSIONS

In this paper, we adopted a new information theoretic framework to address group testing problems. This approach shifts the philosophy of random disjunct/separable matrix generation to an equivalent channel model and capacity computation. The result is a fairly general achievable bound that enables us to obtain the required tradeoffs between the number of tests, number of items and number of defective items for a wide range of group testing problems. Obtaining these tradeoffs reduces to a simple computation of mutual information expressions. We obtain the asymptotic scaling for i) noise-free setups with average and worst-case errors; ii) Approximate reconstruction and iii) Noisy versions of group testing, namely additive and dilution models.

Appendix A: Proof of Lemmas III.1 and III.2

Proof of Lemma III.1

We look at errors in which we confuse the defective set with another set that differs in exactly i items. Let $\mathcal{A}$ be the set of indices corresponding to sets of K items that differ from the true defective set S_1 in exactly i items, i.e.,

$$\mathcal{A} = \{\omega \in \mathcal{I} : |S_{1^c, \omega}| = i, |S_\omega| = K\} \tag{A.1}$$

If ζ_ω denotes the event where $\omega \in \mathcal{A}$ is more likely than 1, then the 2 encoded messages differ in i codewords. Hence

$$\Pr[\text{error}_i | \omega = 1, \boldsymbol{X}_{S_1}, Y^T] \leq P(\bigcup_{\omega \in \mathcal{A}} \zeta_\omega)$$

$$\leq \sum_{\omega \in \mathcal{A}} P(\zeta_\omega) \quad (\text{A.2})$$

Now note that $\boldsymbol{X}_{S_1}$ shares $(K-i)$ codewords with $\boldsymbol{X}_{S_\omega}$. Following the introduced notation, the common codewords are denoted $\boldsymbol{X}_{S_{1,\omega}}$, which is a $(K-i) \times T$ submatrix. The remaining i codewords which are in $\boldsymbol{X}_{S_1}$ but not in $\boldsymbol{X}_{S_\omega}$ are $\boldsymbol{X}_{S_{1,\omega^c}}$. Similarly, $\boldsymbol{X}_{S_{1^c,\omega}}$ denotes the codewords in $\boldsymbol{X}_{S_\omega}$ but not in $\boldsymbol{X}_{S_1}$. In other words $\boldsymbol{X}_{S_1} = (\boldsymbol{X}_{S_{1,\omega}}; \boldsymbol{X}_{S_{1,\omega^c}})$ and $\boldsymbol{X}_{S_\omega} = (\boldsymbol{X}_{S_{1,\omega}}; \boldsymbol{X}_{S_{1^c,\omega}})$. Thus,

$$P(\zeta_\omega) = \sum_{\boldsymbol{X}_{S_\omega}:p(Y^T|\boldsymbol{X}_{S_\omega}) \geq p(Y^T|\boldsymbol{X}_{S_1})} Q(\boldsymbol{X}_{S_\omega}|\boldsymbol{X}_{S_1})$$

$$\leq \sum_{\boldsymbol{X}_{S_{1^c,\omega}}} Q(\boldsymbol{X}_{S_{1^c,\omega}}) \frac{p(Y^T|\boldsymbol{X}_{S_\omega})^s}{p(Y^T|\boldsymbol{X}_{S_1})^s} \quad \forall s > 0, \ \forall \omega \in \mathcal{A} \quad (\text{A.3})$$

By independence $Q(\boldsymbol{X}_{S_1}) = Q(\boldsymbol{X}_{S_{1,\omega}})Q(\boldsymbol{X}_{S_{1,\omega^c}})$. Similarly, $Q(\boldsymbol{X}_{S_\omega}) = Q(\boldsymbol{X}_{S_{1,\omega}})Q(\boldsymbol{X}_{S_{1^c,\omega}})$. Since we are conditioning on a particular $\boldsymbol{X}_{S_1}$, the partition $\boldsymbol{X}_{S_{1,\omega}}$ is fixed in the summation in (A.3) and

$$P(\zeta_\omega) \leq \sum_{\boldsymbol{X}_{S_{1^c,\omega}}} Q(\boldsymbol{X}_{S_{1^c,\omega}}) \frac{p(Y^T, \boldsymbol{X}_{S_{1,\omega}}|\boldsymbol{X}_{S_{1^c,\omega}})^s}{Q(\boldsymbol{X}_{S_{1,\omega}}|\boldsymbol{X}_{S_{1^c,\omega}})^s} \frac{Q(\boldsymbol{X}_{S_{1,\omega}}|\boldsymbol{X}_{S_{1,\omega^c}})^s}{p(Y^T, \boldsymbol{X}_{S_{1,\omega}}|\boldsymbol{X}_{S_{1,\omega^c}})^s}$$

$$\leq \sum_{\boldsymbol{X}_{S_{1^c,\omega}}} Q(\boldsymbol{X}_{S_{1^c,\omega}}) \frac{p(Y^T, \boldsymbol{X}_{S_{1,\omega}}|\boldsymbol{X}_{S_{1^c,\omega}})^s}{p(Y^T, \boldsymbol{X}_{S_{1,\omega}}|\boldsymbol{X}_{S_{1,\omega^c}})^s} \quad \forall s > 0 \quad (\text{A.4})$$

where the second inequality follows from the independence of the codewords, i.e. $Q(\boldsymbol{X}_{S_{1,\omega}}|\boldsymbol{X}_{S_{1,\omega^c}}) = Q(\boldsymbol{X}_{S_{1,\omega}}|\boldsymbol{X}_{S_{1^c,\omega}}) = Q(\boldsymbol{X}_{S_{1,\omega}})$. Replacing in (A.2)

$$\Pr[\text{error}_i | \omega = 1, \boldsymbol{X}_{S_1}, Y^T] \leq \sum_{\omega \in \mathcal{A}} \sum_{\boldsymbol{X}_{S_{1^c,\omega}}} Q(\boldsymbol{X}_{S_{1^c,\omega}}) \frac{p(Y^T, \boldsymbol{X}_{S_{1,\omega}}|\boldsymbol{X}_{S_{1^c,\omega}})^s}{p(Y^T, \boldsymbol{X}_{S_{1,\omega}}|\boldsymbol{X}_{S_{1,\omega^c}})^s}$$

$$= \sum_{S_{1^c,\omega}} \sum_{\boldsymbol{X}_{S_{1^c,\omega}}} Q(\boldsymbol{X}_{S_{1^c,\omega}}) \frac{p(Y^T, \boldsymbol{X}_{S_{1,\omega}}|\boldsymbol{X}_{S_{1^c,\omega}})^s}{p(Y^T, \boldsymbol{X}_{S_{1,\omega}}|\boldsymbol{X}_{S_{1,\omega^c}})^s}$$

$$(\text{A.5})$$

Note that there are exactly $\binom{N-K}{i}$ such sets differing from S_1 in i items.

Proof of Lemma III.2

First note that

$$P(E_i) \leq \sum_{[\boldsymbol{X}_{S_1}]} \sum_Y p([\boldsymbol{X}_{S_1}], Y) p(\text{error}_i | 1, [\boldsymbol{X}_{S_1}], Y) \quad (\text{A.6})$$

However, using the union bound we have that

$$p(\text{error}_i|1, [\boldsymbol{X}_{S_1}], Y) \leq \binom{K}{i} \sum_{\sigma} \phi(\boldsymbol{X}_{S_{1,\omega}}, \boldsymbol{X}_{S_{1,\omega^c}}, Y) \tag{A.7}$$

In addition to the bound in A.7, the error probability $p(\text{error}_i|1, [\boldsymbol{X}_{S_1}], Y)$ is also bounded from above by 1. Now if

$$\binom{K}{i} \sum_{\sigma} \phi(\boldsymbol{X}_{S_{1,\omega}}, \boldsymbol{X}_{S_{1,\omega^c}}, Y) < 1$$

then it is increased by raising it to the power of ρ which implies that

$$p(\text{error}_i|1, [\boldsymbol{X}_{S_1}], Y) \leq \binom{K}{i}^{\rho} \left[\sum_{\sigma} \phi(\boldsymbol{X}_{S_{1,\omega}}, \boldsymbol{X}_{S_{1,\omega^c}}, Y) \right]^{\rho} \tag{A.8}$$

Conversely, if it is greater than 1 then

$$\binom{K}{i}^{\rho} \left[\sum_{\sigma} \phi(\boldsymbol{X}_{S_{1,\omega}}, \boldsymbol{X}_{S_{1,\omega^c}}, Y) \right]^{\rho} \geq 1 \tag{A.9}$$

and still serves as an upper bound on the error probability. Hence, the bound in (A.8) is also true establishing that

$$p(\text{error}_i|1, [\boldsymbol{X}_{S_1}], Y) \leq \binom{K}{i}^{\rho} \left[\sum_{\sigma} \phi(\boldsymbol{X}_{S_{1,\omega}}, \boldsymbol{X}_{S_{1,\omega^c}}, Y) \right]^{\rho}$$

$$\leq \sum_{\sigma} \binom{K}{i}^{\rho} \phi^{\rho}(\boldsymbol{X}_{S_{1,\omega}}, \boldsymbol{X}_{S_{1,\omega^c}}, Y) \tag{A.10}$$

Using the bound in (A.10) and substituting for ϕ in (A.6) we get

$$P(E_i) \leq \sum_{[\boldsymbol{X}_{S_1}]} \sum_{Y} p([\boldsymbol{X}_{S_1}], Y) \sum_{\sigma} \left[\binom{N-K}{i} \binom{K}{i} \sum_{\boldsymbol{X}_{S_{1c,\omega}}} Q(\boldsymbol{X}_{S_{1c,\omega}}) \frac{p(Y^T, \boldsymbol{X}_{S_{1,\omega}}|\boldsymbol{X}_{S_{1c,\omega}})^s}{p(Y^T, \boldsymbol{X}_{S_{1,\omega}}|\boldsymbol{X}_{S_{1,\omega^c}})^s} \right]^{\rho}$$

$$= \sum_{\sigma} \sum_{[\boldsymbol{X}_{S_1}]} \sum_{Y} p([\boldsymbol{X}_{S_1}], Y) \left[\binom{N-K}{i} \binom{K}{i} \sum_{\boldsymbol{X}_{S_{1c,\omega}}} Q(\boldsymbol{X}_{S_{1c,\omega}}) \frac{p(Y^T, \boldsymbol{X}_{S_{1,\omega}}|\boldsymbol{X}_{S_{1c,\omega}})^s}{p(Y^T, \boldsymbol{X}_{S_{1,\omega}}|\boldsymbol{X}_{S_{1,\omega^c}})^s} \right]^{\rho}$$

$$\tag{A.11}$$

establishing the result in Lemma III.2.

Appendix B: Proof of Theorem VII.2

We derive a necessary condition on the number of tests T for the additive noise model in (4) based on the Fano bound in Theorem IV.1. All we need is to upper bound the mutual information expression $I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y)$ when the test outcome Y is given by (4). From (45) and (46) we see that

$$I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y) = \frac{i}{K \ln 2} \left(1 - \frac{1}{K} \right)^K (1-q) + O\left(\frac{1}{K^2} \right) + \frac{1}{\ln 2} \left(1 - \frac{1}{K} \right)^K (1-q)$$

$$- \frac{1}{\ln 2} \sum_{j=2}^{\infty} \frac{1}{j(j-1)} \left(1 - \frac{1}{K} \right)^{K+i(j-1)} (1-q)^j - \left(1 - \frac{1}{K} \right)^K q \log \frac{1}{q} \tag{B.1}$$

Combining terms using (48) and simplifying we get

$$
\begin{aligned}
I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y) &= \frac{i}{K \ln 2}\left(1 - \frac{1}{K}\right)^K (1 - q) + O\left(\frac{1}{K^2}\right) \\
&\quad + \frac{1}{\ln 2}\left(1 - \frac{1}{K}\right)^K \sum_{j=2}^{\infty} \frac{1}{j(j-1)}(1 - q)^j \left(1 - \left(1 - \frac{1}{K}\right)^{i(j-1)}\right) \\
&\leq \frac{i}{K \ln 2}\left(1 - \frac{1}{K}\right)^K (1 - q) + O\left(\frac{1}{K^2}\right) \\
&\quad + \frac{1}{\ln 2}\left(1 - \frac{1}{K}\right)^K \left(1 - q + q \ln \frac{1}{q}\right)
\end{aligned}
\tag{B.2}
$$

where in the last inequality we made use of the fact that

$$
\sum_{n=1}^{\infty} \frac{x^n}{n(n+1)} = x + (x - 1)\log\left(\frac{1}{1-x}\right)
$$

Since the lower bound in IV.1 has to be satisfied for every i, then letting $i = K$ we have that

$$
I(X_{\mathcal{S}^1}; X_{\mathcal{S}^2}, Y) = I(X_S, Y) \leq \frac{1}{\ln 2}\left(1 - \frac{1}{K}\right)^K \left(2(1 - q) + q \ln \frac{1}{q}\right) + O\left(\frac{1}{K^2}\right)
\tag{B.3}
$$

Replacing in (29) we get the result in Theorem VII.2.

Appendix C

In this appendix we extend the result of Theorem III.1 to the case where both N and K are allowed to scale simultaneously such that $K = o(N)$.

We will now establish a lower bound for the error exponent. First, we begin with a simple lemma.

Lemma VIII.1

$$
E_o(\rho) \geq \rho I(X_{\mathcal{S}^1}; Y \mid X_{\mathcal{S}^2}) - \frac{\rho^2}{2} \max_{0 \leq \psi < 1} \left|(E_o(\psi))''\right|
$$

Proof: We first note that from the Lagrange form of the Taylor Series expansion (essentially an application of the mean value theorem) we can write $E_o(\rho)$ in terms of its first derivative evaluated at zero and a remainder term, i.e.,

$$
E_o(\rho) = E_o(0) + \rho E_o'(0) + \frac{\rho^2}{2}(E_o)''(\psi)
$$

for some $\psi \in [0, \rho]$. We have already shown that $E_o(0) = 0$ and $E_o'(0) = I(X_{\mathcal{S}^1}; Y \mid X_{\mathcal{S}^2}) > 0$. Consequently, we now lower bound $E_o(\rho)$ by taking the worst-case second derivative, i.e.,

$$
E_o(\rho) \geq \rho I(X_{\mathcal{S}_1}; Y \mid X_{\mathcal{S}_2}) - \frac{\rho^2}{2} \max_{\psi \in [0, \rho]} \left|(E_o)''(\psi)\right|
$$

■

We are left to bound the second derivative. Recall that, $E_o(\rho)$ is defined as

$$E_o(\rho) = -\log \sum_{Y \in \{0,1\}} \sum_{X_{\mathcal{S}^2}} \left[\sum_{X_{\mathcal{S}^1}} Q(X_{\mathcal{S}^1}) p(Y, X_{\mathcal{S}^2} | X_{\mathcal{S}^1})^{\frac{1}{1+\rho}} \right]^{1+\rho} \tag{C.1}$$

For notational convenience we define:

$$b_\rho \models b_\rho(Y, X_{\mathcal{S}^2}, X_{\mathcal{S}^1}) = p(Y, X_{\mathcal{S}^2} | X_{\mathcal{S}^1})^{\frac{1}{1+\rho}}$$

Note, that b_ρ is a function of Y, $X_{\mathcal{S}^2}$, $X_{\mathcal{S}^1}$ but we suppress these dependencies since we do not make use of this in our calculations other than to note that $0 \leq b_\rho \leq 1$. Let,

$$f_\rho \models E(b_\rho) = \sum_{X_{\mathcal{S}^1}} Q(X_{\mathcal{S}^1}) p(Y, X_{\mathcal{S}^2} | X_{\mathcal{S}^1})^{\frac{1}{1+\rho}}$$

Similarly, f_ρ is still a random variable since it is dependent on $Y, X_{\mathcal{S}^2}$ but again this dependency is not used in much of our computation other than the fact that $f_\rho \in [0, 1]$. Let,

$$g_\rho \models g_\rho(Y, X_{\mathcal{S}^2}) = f_\rho^{1+\rho}$$

Again $g_\rho \in [0, 1]$. Finally note that with these substitutions, we can rewrite, $E_o(\rho)$ as:

$$E_o(\rho) = -\log \sum_{Y \in \{0,1\}} \sum_{X_{\mathcal{S}^2}} g_\rho(Y, X_{\mathcal{S}^2})$$

Finally, let

$$u_\rho = \frac{b_\rho}{E(b_\rho)} = \frac{p(Y | X_{\mathcal{S}^1} X_{\mathcal{S}^2})^{\frac{1}{1+\rho}}}{\sum_{X_{\mathcal{S}^1}} Q(X_{\mathcal{S}^1}) p(Y | X_{\mathcal{S}^1} X_{\mathcal{S}^2})^{\frac{1}{1+\rho}}} = \frac{p(Y | X_{\mathcal{S}_1} X_{\mathcal{S}_2})^{\frac{1}{1+\rho}}}{\sum_{X_{\mathcal{S}_1}} Q(X_{\mathcal{S}_1}) p(Y | X_{\mathcal{S}_1} X_{\mathcal{S}_2})^{\frac{1}{1+\rho}}}$$

where the expectation is taken with respect to $X_{\mathcal{S}^1}$. Note that the second equality follows by canceling out the common term $Q(X_{\mathcal{S}^2})$ from both the numerator and denominator. Next, we have the following bound for the second derivative:

Lemma VIII.2

$$|(E_o(\rho))''| \leq \left| \sum_{X_{\mathcal{S}^2}} \sum_{Y} g_\rho E(u_\rho \log^2(u_\rho)) \right|$$

where the expectation is taken with respect to $X_{\mathcal{S}^1}$.

To prove this lemma we first establish the following propositions.

Proposition VIII.1

$$|E_o''(\rho)| \leq \left| \frac{\sum_{Y, X_{\mathcal{S}^2}} g_\rho''}{\sum_{Y, X_{\mathcal{S}^2}} g_\rho} \right| \tag{C.2}$$

Proof: We rewrite the first and second derivatives of $E_0(\rho)$ in terms of b_ρ, f_ρ, g_ρ and their first and second derivatives. Specifically, note that

$$(E_o(\rho))'' = -\frac{\sum_{Y,X_{\mathcal{S}^2}}(g_\rho(Y,X_{\mathcal{S}^2}))''}{\sum_{Y,X_{\mathcal{S}^2}}(g_\rho(Y,X_{\mathcal{S}^2}))} + \left(\frac{\sum_{Y,X_{\mathcal{S}^2}}(g_\rho(Y,X_{\mathcal{S}}))'}{\sum_{Y,X_{\mathcal{S}^2}}(g_\rho(Y,X_{\mathcal{S}^2}))}\right)^2$$

Note that the second derivative of $E(\rho)$ is negative for $\rho > 0$. This follows from the fact that $E_0(\rho)$ is a concave function (see [26]). Furthermore, $g_\rho(\cdot)$ is a positive increasing function with $\sum_{Y,X_{\mathcal{S}^2}} g_\rho = 1$. The proof now follows. ■

Also note that the denominator in proposition C.2 is bounded from below by 1 since

$$\sum_{Y,X_{\mathcal{S}^2}} g_\rho = 2^{-E_0(\rho)} \geq 2^{-I(X_{\mathcal{S}^1};X_{\mathcal{S}^2},Y)} \geq 1 \tag{C.3}$$

We are now left to compute the second derivative for g_ρ. We have the following proposition:

Proposition VIII.2 *The following property holds:* $g'_\rho = -g_\rho E(u_\rho \log(u_\rho))$

Proof: Note that,

$$f'_\rho = -\frac{1}{1+\rho}E(b_\rho \log b_\rho), \ \ g'_\rho = g_\rho \log(f_\rho) + (1+\rho)f_\rho^\rho f'_\rho$$

Note that $0 \leq b_\rho \leq 1$ it follows that $f'_\rho > 0$ for positive ρ. Simplifying the expression for g'_ρ through substitution we obtain

$$g'_\rho = f_\rho^\rho(f_\rho \log(f_\rho) - E(b_\rho \log(b_\rho))) = -f_\rho^\rho E\left(b_\rho \log\frac{b_\rho}{E(b_\rho)}\right) = -g_\rho E\left(\frac{b_\rho}{E(b_\rho)}\log\frac{b_\rho}{E(b_\rho)}\right)$$

The proof now follows.

■

We have the following result for the second derivative:

Proposition VIII.3
$$g''_\rho = \frac{g_\rho}{1+\rho}E(u_\rho \log^2(u_\rho)) + \frac{\rho g_\rho}{1+\rho}(E(u_\rho \log(u_\rho)))^2$$

It follows that if $E(u_\rho \log(u_\rho))$ *is a decreasing function of* ρ *then*

$$0 \leq g''_\rho \leq g_\rho E(u_\rho \log^2(u_\rho))$$

A situation where this arises is when $u_\rho \notin (1/2, 1), \ \forall \rho \in [0,1]$.

Proof: Note that,

$$g''_\rho = -g'_\rho E(u_\rho \log(u_\rho)) - g_\rho \frac{d}{d\rho} E(u_\rho \log(u_\rho))$$

$$= g_\rho E(u_\rho \log(u_\rho))^2 - g_\rho \frac{d}{d\rho} E(u_\rho \log(u_\rho))$$

$$= g_\rho E(u_\rho \log(u_\rho))^2 - g_\rho E(u'_\rho \log(u_\rho) + u'_\rho)$$

$$= g_\rho E(u_\rho \log(u_\rho))^2 - g_\rho E(u'_\rho \log(u_\rho))$$

where the last equality follows from the fact that $E(u_\rho) = 1$ and so $E(u'_\rho) = 0$. We now compute u'_ρ:

$$u'_\rho = -\frac{1}{1+\rho}(u_\rho \log b_\rho - u_\rho E(u_\rho \log(b_\rho))) = -\frac{1}{1+\rho}(u_\rho \log u_\rho - u_\rho E(u_\rho \log(u_\rho))) \qquad \text{(C.4)}$$

The first result now follows by direct substitution. To establish the second result we first note that the positivity of the expression is obvious since $u_\rho \geq 0$. For the upper bound we note from Equation C.4 that,

$$\phi_\rho = \frac{d}{d\rho} E(u_\rho \log(u_\rho)) = E(u'_\rho \log(u_\rho) + u'_\rho) = E(u'_\rho \log(u_\rho))$$

$$= -\frac{1}{1+\rho} \left(E(u_\rho \log^2 u_\rho) - (E(u_\rho \log(u_\rho)))^2 \right)$$

Now if $\phi_\rho \leq 0$ then it follows that $E(u_\rho \log^2(u_\rho)) \geq (E(u_\rho \log(u_\rho)))^2$ and the upper bound in the second part of the proposition would follow by direct substitution. Therefore, we are left to establish that $\phi_\rho < 0$ or equivalently $E(u_\rho \log(u_\rho))$ when $u_\rho \notin (1/2, 1)$ is a monotonically decreasing function of ρ. To see this note that u_ρ monotonically increases if $u_\rho < 1$ and monotonically decreases if $u_\rho > 1$. The function $|u_\rho \log(u_\rho)|$ has a maxima at $u_\rho = 1/2$ and so is monotonically increasing for $u_\rho < 1/2$ and monotonically decreasing for $u_\rho \geq 1$. Since $u_\rho \notin (1/2, 1)$ we can decompose the expected value of the function as follows:

$$E(u_\rho \log(u_\rho)) = E\left(\mathbf{1}_{\{u_\rho < 1/2\}} u_\rho \log(u_\rho) + \mathbf{1}_{\{u_\rho \geq 1\}} u_\rho \log(u_\rho)\right) = E\left(\mathbf{1}_{\{u_\rho < 1/2\}} u_\rho \log(u_\rho) + \mathbf{1}_{\{u_\rho \geq 1\}} u_\rho \log(u_\rho)\right)$$

So,

$$E(u_\rho \log(u_\rho)) = E(\mathbf{1}_{\{u_\rho \geq 1\}} u_\rho \log(u_\rho)) - |E\left(\mathbf{1}_{\{u_\rho < 1/2\}} u_\rho \log(u_\rho)\right)|$$

Now the first term above is positive and decreasing and the second term is positive but increasing. Finally, $E(u_\rho \log(u_\rho))$ is positive from Property (2) of Proposition VIII.2. So, $E(u_\rho \log(u_\rho))$ is positive and decreasing function of ρ. ∎

We have the following Lemmas for each of the different channels considered in the paper.

Lemma VIII.3 *Consider the noiseless channel. Then the worst-case second derivative* $(E_o(\psi))''$ *satisfies:*

$$|(E_o(\psi))''| \leq 2\frac{i}{K}\log^2 K$$

Proof: We first compute u_ρ for the different cases. Note that for $X_{\mathcal{S}^2} = 0$ (i.e. all the components are zero) and $Y = 0$ we have,

$$P(Y = 0 \mid X_{\mathcal{S}^2} = 0, X_{\mathcal{S}^1}) = \begin{cases} 0 & \text{if } X_{\mathcal{S}^1} \neq 0 \\ 1 & X_{\mathcal{S}^1} = 0 \end{cases}$$

$$P(Y = 0 \mid X_{\mathcal{S}^2} = 0) = (1 - 1/K)^i$$

Therefore, $u_\rho = \frac{1}{(1-1/K)^i}$ or $u_\rho = 0$ for this case. Consequently, we immediately note that $E(u_\rho \log u_\rho)$ is independent of ρ. This implies that from Proposition VIII.2

$$g''_\rho = g_\rho \log^2 \frac{1}{(1 - 1/K)^i}$$

which is a decreasing function of ρ. Hence the worst-case second derivative is realized at $\rho = 0$. Furthermore, note that in this case,

$$(g_\rho)_{\rho=0} = P(Y = 0, X_{\mathcal{S}^2} = 0) = (1 - 1/K)^K$$

Suppose on the other hand $X_{\mathcal{S}^2} = 0$ but $Y = 1$, then we get

$$P(Y = 1 \mid X_{\mathcal{S}^1}, X_{\mathcal{S}^2} = 0) = \begin{cases} 1 & \text{if } X_{\mathcal{S}^1} \neq 0 \\ 0 & X_{\mathcal{S}^1} = 0 \end{cases}$$

$$P(Y = 0 \mid X_{\mathcal{S}_1} = 0) = 1 - (1 - 1/K)^i$$

Therefore, $u_\rho = \frac{1}{1-(1-1/K)^i}$ or $u_\rho = 0$ for this case. Consequently, we immediately note that $E(u_\rho \log(u_\rho))$ is independent of ρ. This implies that from Proposition VIII.2

$$g''_\rho = g_\rho \log^2 \frac{1}{(1 - (1 - 1/K)^i)}$$

which is a decreasing function of ρ. Hence the worst-case second derivative is realized at $\rho = 0$. Furthermore, note that in this case,

$$(g_\rho)_{\rho=0} = P(Y = 1, X_{\mathcal{S}^2} = 0) = (1 - 1/K)^{K-i}(1 - (1 - 1/K)^i)$$

Note that $X_{\mathcal{S}^2} \neq 0$ always results in $Y = 1$ regardless of $X_{\mathcal{S}^1}$ and hence u_ρ for this case is always zero.

We are now ready to compute the second derivative based on the expression in Proposition VIII.3. It follows by direct computation that,

$$|(E_o(\psi))''| \leq |\sum_{X_{\mathcal{S}^2}, Y} (g_\rho)_{\rho=0} E(u_\rho \log^2 u_\rho)| \leq \frac{i}{K} \log^2 \frac{K}{i} + O\left(\left(\frac{i}{K}\right)^2\right)$$

∎

We are now ready to state our main result:

Theorem VIII.1 *Consider now the noiseless channel. If*

$$T \geq \Omega(K \log N \log^2 K)$$

then it follows that the probability of misidentifying the K defectives goes to zero.

Proof: Note that from the expression of $P(E_i)$ we have that,

$$\sum_i P(E_i) \leq K \max_i P(E_i) \leq \max_i K \exp\left(-T\left(E_o(\rho) - \frac{\rho}{T} \log \binom{N-K}{i}\binom{K}{i}\right)\right)$$

Consequently, we need to ensure that,

$$T E_o(\rho) \geq \rho \log \binom{N-K}{i}\binom{K}{i} + \log K$$

Now using the lower bound for $E_o(\rho)$ we have

$$
\begin{aligned}
E_o(\rho) &\geq \rho I(X_{\mathcal{S}_2}; Y \mid X_{\mathcal{S}_1}) - \frac{\rho^2}{2}|(E_o(0))''| \geq \rho I(X_{\mathcal{S}_2}; Y \mid X_{\mathcal{S}_1}) - \frac{\rho^2}{2}\frac{i}{K} \log^2 \frac{K}{i} \\
&\geq \rho \frac{i}{K} - \frac{\rho^2}{2}\frac{i}{K} \log^2 \frac{K}{i}
\end{aligned}
$$

where the last inequality follows from the lower bound for the mutual information in the noiseless case (see Theorem V.1). Substituting this lower bound we obtain

$$T \rho \frac{i}{K}\left(1 - \frac{\rho}{2}\log^2 \frac{K}{i}\right) \geq \rho \log \binom{N-K}{i}\binom{K}{i} + \log K$$

By choosing $\rho = \frac{1}{\log^2(K/i)}$ and $T = 2K \log N \log^2(K)$ the inequality is satisfied. ∎

Lemma VIII.4 *Consider the additive noise channel. Then the worst-case second derivative $(E_o(\psi))''$ satisfies*

$$|(E_o(\psi))''| \leq 2\frac{i}{K} \log^2 \left(\frac{2}{q}\right) + O\left(\left(\frac{i}{K}\right)^2\right)$$

Proof: We consider all the possible combinations for Y and $X_{\mathcal{S}^2}$.

- Case $Y = 1$, $X_{\mathcal{S}^2} = 0$

  1) $E[u_\rho \log u_\rho]$ is monotone decreasing

Proof:

$$u_\rho = \begin{cases} \dfrac{q^{\frac{1}{1+\rho}}}{(1-\frac{1}{K})^i q^{\frac{1}{1+\rho}}+1-(1-\frac{1}{K})^i} & \text{if } X_{\mathcal{S}^1}=0 \\[3mm] \dfrac{1}{(1-\frac{1}{K})^i q^{\frac{1}{1+\rho}}+1-(1-\frac{1}{K})^i} & X_{\mathcal{S}^1}\neq 0 \end{cases}$$

To simplify notation define:

$$a_1 \triangleq \left(1-\frac{1}{K}\right)^i$$

$$q_\rho \triangleq q^{\frac{1}{1+\rho}}$$

$$p \triangleq \frac{a_1 q_\rho}{a_1 q_\rho + 1 - a_1}$$

Hence,

$$E[u_\rho \log u_\rho] = p \log \frac{q_\rho}{a_1 q_\rho + 1 - a_1} + (1-p)\log \frac{1}{a_1 q_\rho + 1 - a_1}$$

$$= -p \log \frac{1}{p} + p \log \frac{1}{a_1} + (1-p)\log(1-p) + (1-p)\log \frac{1}{1-a_1}$$

$$= -H(p) - p \log \left(\frac{a_1}{1-a_1}\right) + \log \frac{1}{1-a_1} \tag{C.5}$$

p is a monotonically increasing function of ρ. Hence, taking the derivative w.r.t. p

$$\frac{d}{d\rho}E[u_\rho \log u_\rho] = \log \frac{p(1-a_1)}{a_1(1-p)} = \log q_\rho < 0 \tag{C.6}$$

∎

2) $E[u_\rho \log u_\rho]$ is positive

Proof: $E[u_\rho \log u_\rho]$ is monotone decreasing. At $p=1$, $H(p)=0$, hence

$$E[u_\rho \log u_\rho] = p \log \frac{a_1}{1-a_1} + \log \frac{1}{1-a_1} > 0 \tag{C.7}$$

establishing its positivity for all p. ∎

Hence, $g_\rho'' \leq g_\rho E(u_\rho \log^2(u_\rho))$. Now we are left to compute $E(u_\rho \log^2(u_\rho))$. Note that the maximum is further achieved at $\rho = 0$ since $E(u_\rho \log^2(u_\rho))$ is monotone decreasing. This is not hard to see since u_ρ takes 2 values which approach 1 as ρ increases. Hence, $E(u_\rho \log^2(u_\rho))$ can be expanded as the sum of two monotone decreasing terms. Replacing with the values of u_ρ at $Y=1$, $X_{\mathcal{S}^2}=0$ we see that

$$E[u_\rho \log^2 u_\rho] \leq 2\frac{i}{K}\log^2\left(\frac{2}{q}\right) \tag{C.8}$$

and

$$(g_\rho)_{\rho=0} = P(Y=1, X_{\mathcal{S}^2}=0) = \left(1-\frac{1}{K}\right)^{K-i}\left(q+1-\left(1-\frac{1}{K}\right)^i\right) \tag{C.9}$$

- Case $Y = 0$, $X_{\mathcal{S}^2} = 0$

  In this case,

  $$u_\rho = \begin{cases} 0 & \text{if } X_{\mathcal{S}^1} \neq 0 \\ \frac{1}{(1-\frac{1}{K})^i} & X_{\mathcal{S}^1} = 0 \end{cases}$$

  so u_ρ is independent of ρ. Hence,

  $$g''_\rho = -g'_\rho E[u_\rho \log u_\rho] = g_\rho E^2[u_\rho \log u_\rho] \tag{C.10}$$

  Noting that the first derivative $g'_\rho = -g_\rho E[u_\rho \log u_\rho] = -g_\rho \log \frac{1}{(1-\frac{1}{K})^i} \leq 0$, it follows that the third derivative $g'''_\rho = g'_\rho \log^2 \frac{1}{(1-\frac{1}{K})^i} \leq 0$. Hence, the maximum of g''_ρ is achieved at $\rho = 0$ and

  $$g''_\rho = (1-q)(1-\frac{1}{K})^K \log^2 \frac{1}{(1-\frac{1}{K})^i} \tag{C.11}$$

Combining C.8, C.9, and C.11 Lemma VIII.4 follows. This result implies the same sufficient condition obtained in Theorem VII.1 for the additive noise channel. $\blacksquare$

Lemma VIII.5 *Consider a dilution channel with dilution probability p. Then the worst-case second derivative $(E_o(\psi))''$ satisfies:*

$$|(E_o(\psi))''| \leq \frac{i(1-p)}{K} \log^2 K$$

Proof:

- Case $Y = 0, X_{\mathcal{S}^2} = 0, ||X_{\mathcal{S}^1}||_1 = \ell$ i.e., $X_{\mathcal{S}^1}$ has ℓ ones.

  $$u_\rho(\ell) = \frac{p_\rho^\ell}{\sum_{\ell=0}^i \binom{i}{\ell}(\frac{1}{K})^\ell(1-\frac{1}{K})^{i-\ell}p_\rho^\ell} \tag{C.12}$$

  where $p_\rho = p^{\frac{1}{1+\rho}}$. Thus for $p \leq \frac{1}{2}$, $u_\rho(\ell = 0) > 1$ and $u_\rho(\ell \neq 0) < \frac{1}{2}$ implying that $E[u_\rho \log u_\rho]$ is monotone decreasing. In this case

  $$(g_\rho)_{\rho=0} = P(Y = 0, X_{\mathcal{S}^2} = 0) = \left(1 - \frac{1}{K}\right)^{K-i}\left(1 - \frac{1-p}{K}\right)^i$$

- Case $Y = 0, X_{\mathcal{S}^2} \neq 0, ||X_{\mathcal{S}^1}||_1 = j$

  This case parallels the previous case but replacing p_ρ^ℓ with $p_\rho^{\ell+j}$

- Case $Y = 1, X_{\mathcal{S}^2} = 0, ||X_{\mathcal{S}^1}||_1 = \ell$

  $$u_\rho = \frac{(1-p^\ell)^{\frac{1}{1+\rho}}}{\sum_{\ell=0}^i \binom{i}{\ell}(\frac{1}{K})^\ell(1-\frac{1}{K})^{i-\ell}(1-p^\ell)^{\frac{1}{1+\rho}}} \tag{C.13}$$

  In this case, $u_\rho \geq 1$, $\forall i, \ell \neq 0$ and

  $$(g_\rho)_{\rho=0} = P(Y = 1, X_{\mathcal{S}^2} = 0) = \left(1 - \frac{1}{K}\right)^{K-i}\left[1 - \left(1 - \frac{1-p}{K}\right)^i\right] = \frac{i(1-p)}{K} + O\left(\left(\frac{i}{K}\right)^2\right)$$

- Case $Y = 1, X_{\mathcal{S}^2} = j \neq 0, ||X_{\mathcal{S}^1}||_1 = \ell$

  This case parallels the previous case replacing $1 - p^\ell$ with $1 - p^{\ell+j}$. Also

  $$(g_\rho)_{\rho=0} = P(Y = 1, ||X_{\mathcal{S}^2}||_1 = j)$$

  $$= \left(\frac{1}{K}\right)^j \left(1 - \frac{1}{K}\right)^{K-i-j} \left[1 - p^j \left(1 - \frac{1-p}{K}\right)^i\right]$$

  $$\leq \left(\frac{1}{K}\right)^j (1 - p^{j+1}) \tag{C.14}$$

Now following similar arguments to the previous additive and noiseless cases.

1) $E[u_\rho \log u_\rho]$ is monotone decreasing since $u_\rho \notin (\frac{1}{2}, 1)$

2) To establish the positivity of $E[u_\rho \log u_\rho]$ consider the first case and other cases could be handled similarly. We note that

$$E[u_\rho \log u_\rho] = \sum_{\ell=0}^{i} \binom{i}{\ell} \left(\frac{1}{K}\right)^\ell \left(1 - \frac{1}{K}\right)^{i-\ell} \frac{p_\rho^\ell}{(1 - \frac{1-p_\rho}{K})^i} \log \frac{p_\rho^\ell}{(1 - \frac{1-p}{K})^i}$$

$$= \sum_{\ell=0}^{i} \ell \binom{i}{\ell} (\frac{p_\rho}{K})^\ell (1 - \frac{1}{K})^{i-\ell} \frac{1}{(1 - \frac{1-p_\rho}{K})^i} \log p_\rho + \log \frac{1}{(1 - \frac{1-p_\rho}{K})^i}$$

$$= \frac{i p_\rho \log p_\rho}{K(1 - \frac{1-p_\rho}{K})} + \log \frac{1}{(1 - \frac{1-p_\rho}{K})^i} \tag{C.15}$$

Using first order log Taylor expansion the right hand side goes to $\frac{1}{K} - \frac{p_\rho}{K} \log \frac{e}{p_\rho}$ which is greater than 0 for p less than some constant.

3) Following a similar argument we can also show that $E[u_\rho \log^2 u_\rho]$ is monotonically decreasing. Now for the $Y = 0$, $X_{\mathcal{S}^2} = 0$ case

$$E[u_\rho \log^2 u_\rho] = \sum_{\ell} \binom{i}{\ell} \left(\frac{1}{K}\right)^\ell \left(1 - \frac{1}{K}\right)^{i-\ell} \frac{p_\rho^\ell}{(1 - \frac{1-p_\rho}{K})^i} \log^2 \frac{p_\rho^\ell}{(1 - \frac{1-p_\rho}{K})^i}$$

$$= \frac{(\frac{i p_\rho}{K})^2 \log^2 p_\rho}{(1 - \frac{1-p_\rho}{K})^2} + i^2 \log^2 \frac{1}{(1 - \frac{1-p_\rho}{K})} \tag{C.16}$$

Similarly, for $Y = 1$, $X_{\mathcal{S}^2} = 0$, at $\rho = 0$

$$E[u_\rho \log^2 u_\rho] = \sum_{\ell=0}^{i} \binom{i}{\ell} \left(\frac{1}{K}\right)^\ell \left(1 - \frac{1}{K}\right)^{i-\ell} \frac{1 - p^\ell}{1 - (1 - \frac{1-p_\rho}{K})^i} \log^2 \frac{1 - p^\ell}{1 - (1 - \frac{1-p}{K})^i}$$

$$\leq \log^2 \frac{K(1-p)}{i} \tag{C.17}$$

Combining the results for the various cases establishes the result in Lemma VIII.5.

∎

IX. Acknowledgments

References

[1] George Atia and Venkatesh Saligrama, "Noisy group testing: An information theoretic perspective," in *Proceedings of the 47th Annual Allerton Conf. on Communication, Control, and Computing*, Monticello, IL, Sept 2006.

[2] George Atia and Venkatesh Saligrama, "Boolean compressed sensing and noisy group testing," *Available: http://arxiv.org/abs/0907.1061*, July 2009.

[3] Ding-Zhu Du and Frank K. Hwang, *Combinatorial Group Testing and Its Applications*, World Scientific Publishing Company, second edition, 2000.

[4] R. Dorfman, "The detection of defective members of large populations," *Ann. Math. Stat.*, 1943.

[5] George Atia, Anant Sahai, and Venkatesh Saligrama, "Spectrum enforcement and liability assignment in cognitive radio systems," in *Proceedings of the IEEE DySpAN*, Chicago, IL, Oct. 2008.

[6] George Atia, Venkatesh Saligrama, and Anant Sahai, "Codes to unmask spectrum violators," in *Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, Oct. 2008.

[7] D.L. Donoho, "Compressed sensing," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289 –1306, apr. 2006.

[8] E. J. Candes, J. Romberg, and T. Tao, "Stable signal recovery from incomplete and inaccurate measurements," *Comm. Pure Appl. Math.*, vol. 59, pp. 1207–1223, 2005.

[9] M. Wainwright, "Information-theoretic bounds on sparsity recovery in the high-dimensional and noisy setting," in *International Symposium on Information Theory*, Nice, France, June 2007.

[10] M. J. Wainwright, "Sharp thresholds for high-dimensional and noisy sparsity recovery using ℓ_1-constrained quadratic programs," in *Allerton Conference on Communication, Control and Computing*, Monticello, IL, 2006.

[11] G. Reeves and M. C. Gastpar, "A note on optimal support recovery in compressed sensing," in *43rd Annual IEEE Asilomar Conference on Signals, Systems, and Computers*, Monterey, CA, Nov. 2009.

[12] A. K. Fletcher, S. Rangan, and V. K. Goyal, "Necessary and sufficient conditions for sparsity pattern recovery," *IEEE Trans. Inf. Theor.*, vol. 55, no. 12, pp. 5758–5772, 2009.

[13] A. K. Fletcher, S. Rangan, V. K. Goyal, and K. Ramchandran, "Denoising by sparse approximation: Error bounds based on rate-distortion theory," *EURASIP Journal on Applied Signal Processing*, pp. 1–19, 2006.

[14] W. H. Kautz and R.C. Singleton, "Nonrandom binary superimposed codes," *IEEE Trans. Inf. Theory*, vol. 10, no. 4, pp. 363–377, Oct. 1964.

[15] A. G. Dyachkov and V. V. Rykov, "A survey of superimposed code theory," *Problems of Control and Information Theory*, vol. 12, no. 4, pp. 1–13, 1983.

[16] P. Erdös, P. Frankl, and Z. Füredi, "Family of finite sets in which no set is covered by the union of n others," *Isr. J. Math.*, vol. 51, pp. 79–89, 1985.

[17] Hong-Bin Chen and Frank K. Hwang, "Exploring the missing link among d-separable, -separable and d-disjunct matrices," *Discrete Applied Mathematics*, vol. 155, no. 5, pp. 662 – 664, 2007.

[18] A. G. Dyachkov, V. V. Rykov, and A. M. Rashad, "Bounds of the length of disjunct codes," *Problems Control Information Theory*, vol. 11, pp. 7–13, 1982.

[19] M. Ruszinkó, "Family of finite sets in which no set is covered by the union of n others," *Isr. J. Math.*, vol. 51, pp. 79–89, 1985.

[20] Andras Sebo, "On two random search problems," *Journal of Statistical Planning and Inference*, vol. 11, pp. 23–31, 1985.

[21] T. Berger and V.I. Levenshtein, "Asymptotic efficiency of two-stage disjunctive testing," *Information Theory, IEEE Transactions on*, vol. 48, no. 7, pp. 1741–1749, Jul 2002.

[22] A. C. Gilbert, M. A. Iwen, and M. J. Strauss, "Group testing and sparse signal recovery," in *42nd Asilomar Conference on Signals, Systems and Computers*, 2008.

[23] Ding-Zhu Du and Frank K. Hwang, *Pooling designs and non-adaptive group testing: Important tools for DNA sequencing*, World Scientific Publishing Company, 2006.

[24] Thomas M. Cover and Joy A. Thomas, *Elements of Information Theory*, New York: John Wiley and Sons, Inc., 1991.

[25] S. Aeron, M. Zhao, and V. Saligrama, "Information theoretic bounds for compressed sensing," *submitted to IEEE Transactions on Information Theory*, 2010.

[26] Robert G. Gallager, *Information Theory and Reliable Communication*, John Wiley & Sons, Inc., New York, NY, USA, 1968.