
This is the author accepted manuscript (AAM). The final published version (version of record) is available online via IEEE at http://ieeexplore.ieee.org/document/7907220/. Please refer to any applicable terms of use of the publisher.

University of Bristol - Explore Bristol Research
General rights

This document is made available in accordance with publisher policies. Please cite only the published version using the reference above. Full terms of use are available: http://www.bristol.ac.uk/pure/about/ebr-terms.html
Strong converses for group testing from finite blocklength results

Oliver Johnson

Abstract—We prove new strong converse results in a variety of group testing settings, generalizing a result of Baldassini, Johnson and Aldridge. First, in the non-adaptive case, we mimic the hypothesis testing argument introduced in the finite blocklength channel coding regime by Polyanskiy, Poor and Verdú, and using joint source–channel coding arguments of Kostina and Verdú. In the adaptive case, we combine this approach with a novel model formulation based on causal probability and directed information theory. In both cases, we prove results which are valid for finite sized problems, and imply capacity results in the asymptotic regime. These results are illustrated graphically for a range of models.

Index Terms—Group testing, converse bounds, finite blocklength, sparse models.

I. INTRODUCTION AND GROUP TESTING MODEL

The group testing problem was introduced by Dorfman [1] in the 1940s, and captures the idea of efficiently isolating a small subset $K$ of defective items in a larger set containing $N$ items. The models used vary slightly, but fundamentally we perform a sequence of tests, each defined by a testing pool of items, with the outcome of each depending on the number of defective items in the pool. The most basic model, which we refer to as ‘standard noiseless group testing’ is that the test outcome equals 1 if and only if the testing pool contains at least one defective item. Given $T$ tests, the group testing problem requires us to design test pools and estimation algorithms to maximise $P(suc)$, the success probability (probability of recovering the defective set exactly), where the randomness enters through the defectivity status of the items (see Definition I.2 below) and any noise in the measurements.

This paper focuses on converse results, giving upper bounds on the $P(suc)$ that can be achieved by any algorithm given $T$ tests. We generalize the following strong result proved by Baldassini, Johnson and Aldridge [2] Theorem 3.1:

Theorem I.1. Suppose the defective set $K$ is chosen uniformly from the $N\choose K$ possible sets of given size $K$. For adaptive or non-adaptive standard noiseless group testing:

$$P(suc) \leq 2^T \frac{2^T}{N}.$$ (1)

As Figure 1 illustrates, Theorem I.1 is a strong result in this context, giving a converse which closely matches the achievability results provided by Hwang’s algorithm [3]. This paper extends Theorem I.1 to a variety of settings. We first discuss four dichotomies in the modelling of the group testing problem. There are a number of further variations beyond these, as described in an ever-increasing body of literature.

1) [Combinatorial vs Probabilistic] First, consider how the defective items are chosen. Combinatorial group testing (see for example [4], [5], [6]) is the model from Theorem I.1 we suppose the defective set $K$ is chosen uniformly from the $N\choose K$ possible sets of fixed size $K$. In probabilistic group testing (see for example [7], [8]) the $i$th item is defective independently with probability $p_i$ (with $p_i$ not necessarily identical). In fact, we put both these models in a common setting:

Definition I.2. Write $U \in \{0,1\}^N$ for the (random) defectivity vector, where component $U_i$ is the indicator of the event that the $i$th item is defective. For any vector $u \in \{0,1\}^N$ write $P_U(u) = P(U = u)$, and define entropy

$$H(U) = -\sum_{u \in \{0,1\}^N} P_U(u) \log_2 P_U(u).$$ (2)

Example I.3. For the two models as described above:

a) For combinatorial group testing, $U$ is uniform over $N\choose K$ outcomes and $H(U) = \log_2 N\choose K$.

b) For probabilistic group testing, entropy $H(U) = \sum_{i=1}^N h(p_i)$, where $h(t)$ is the binary entropy function. If $p_i \equiv p$ then $H(U) = Nh(p)$.

We prove in Corollary IV.4 that results resembling Theorem I.1 hold for general sources satisfying the Shannon-McMillan-Breiman theorem. This includes settings where $U$ is generated by a stationary ergodic Markov chain, which is a natural model of a setting where nearest neighbours are susceptible to infection.

2) [Binary vs Non-binary] Second, consider the set of possible outcomes $Y$ of each test. We refer to $Y$ as the alphabet, since in this paper (as in [4], [5] and other papers) we consider an analogy between group testing and channel coding problems. It is most standard to consider the binary case, though our techniques will work in a more general setting, and write $Y \in \{0,1\}^T = \{0,1\}^T$ for the outcome of the group testing process.

3) [Noisy vs Noiseless] Third, consider how the outcome of each test is formed. To fix notation, we perform a sequence of $T$ tests defined by test pools $X_1, \ldots, X_T$, where each $X_t \subseteq \{1,2,\ldots,N\}$. We represent this by a binary test matrix $X = (x_{it} : i = 1, \ldots, N$ and $t = \ldots, T$. 

The author is with the School of Mathematics, University of Bristol, University Walk, Bristol, BS8 1TW, UK Email: maotj@bristol.ac.uk Copyright (c) 2017 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.
of previous test pools can improve performance. However, Definition I.4 allows a wider range of noise models, including the dilution channel. For a fixed test matrix $X$, we take $P = P_0$, and previous outputs $Y_1, Y_2, \ldots, Y_t$ and test outcomes $y_1, y_2, \ldots, y_t$. We can think (see [9]) of the directed information of Marko [11]. Using this probability distribution implies the form of the directed information of Marko [11].

In Lemma IV.1 below, assuming the Only Defects Matter property Definition I.4 we decompose the joint probability of $(U, X, Y)$ in the general adaptive setting, using the term $P_{X|Y} \cdot (X'|Y')$, which is defined in (16). Here we adapt the causal conditional probability notation (5) above, with superscript $y^-$ referring to the fact that there is a lag in the index of $y$ (we choose the set $X_t$ based on a knowledge of the previous sets $X_{1,t-1}$ and test outcomes $y_{1,t-1}$).

Lemma IV.1 shows the $t$-th output symbol $Y_t$ is conditionally independent of $U$, given values $K_{1,t}$ and previous outputs $Y_{1,t-1}$. This is precisely the definition of a causal system between $K$ and $Y$ given by Massey in [12] Equation (8)), under which condition feedback does not increase the capacity of a discrete memoryless channel.

Regardless of these variations, we always make an estimate $Z = \hat{U}$, based only on a knowledge of outputs $Y = y$ and test matrix $X = \mathcal{X}$, using a probabilistic estimator (decoder) that gives $Z = z$ with probability $P_{Z|Y,X}(z|y, \mathcal{X})$.

The main results of the paper are Theorem III.2 which gives an upper bound on $P_{\text{stic}}$ in the non-adaptive case, and Theorem IV.2 which gives the corresponding result in the adaptive case. The strength of these results is illustrated in results such as Example V.4 where we calculate bounds on the success probability in the case where $X$ forms the input and $Y$ the output of a binary symmetric channel with error probability $p$, with the resulting bounds being plotted in Figure 3.

The structure of the paper is as follows. In Section II we review existing results concerning group testing converses. In Section III we use an argument based on the papers [15] and [16] to prove Theorem III.2 which implies a strong converse for non-adaptive group testing. In Section IV we discuss the adaptive case, by extending these arguments using the causal probability formulation described above. We prove a bound (Theorem IV.2 which specializes in the noiseless case to give
a result (Theorem IV.3) which generalizes Theorem I.1. We consider examples of this noiseless result in the probabilistic case in Section V-A. Finally in Section V-B we apply Theorem IV.3 in the noisy adaptive case. The proofs of the main theorems are given in Appendices.

While this paper only considers group testing, we remark that group testing lies in the area of sparse inference, which includes problems such as compressed sensing and matrix completion, as reviewed by [17]. It is likely that results proved here will extend to more general settings. Group testing itself has a number of applications, including cognitive radios [10], [13], [17], network tomography [19] and efficient gene sequencing [20], [21]. The bounds proved here should provide fundamental performance limits in these contexts.

II. EXISTING CONVERSE RESULTS

Information-theoretic considerations mean that to find all the defectives in the noiseless case will require at least \( T^* = H(U) \) (the “magic number”) tests. In the language of channel coding, the focus of this paper is on converse results; that is given \( T^* \) tests, we give strong upper bounds on the success probability \( P(suc) \) of any possible algorithm.

There has been considerable work on the achievability part of the problem, in developing group testing algorithms and proving performance guarantees. Early work on group testing considered algorithms which could be proved to be order optimal (see for example the analysis of [22], [23], [24]), often using combinatorial properties such as separability or disjunctness. More recently there has been interest (see for example [4], [5], [6], [8], [25], [26], [27], [28], [29], [30]) in finding the best possible constant, that is to find algorithms which succeed with high probability using \( T = cT^* = cH(U) \) tests, for \( c \) as small as possible. In this context, the paper [2] defined the capacity of combinatorial group testing problems, a definition extended to both combinatorial and probabilistic group testing in [7]. We state this definition for both weak and strong capacity in the sense of Wolfowitz:

**Definition II.1.** Consider a sequence of group testing problems where the \( i \)th problem has defectivity vector \( U^{(i)} \), and consider algorithms which are given \( T(i) \) tests. We think of \( H(U^{(i)})/T(i) \) (the number of bits of information learned per test) as the rate of the algorithm and refer to a constant \( C \) as the weak group testing capacity if for any \( \epsilon > 0 \):

1) any sequence of algorithms with

\[
\liminf_{i \to \infty} \frac{H(U^{(i)})}{T(i)} \geq C + \epsilon,
\]

has success probability satisfying \( \limsup_{i \to \infty} P(suc) < 1 \).

2) and there exists a sequence of algorithms with

\[
\liminf_{i \to \infty} \frac{H(U^{(i)})}{T(i)} \geq C - \epsilon
\]

with success probability satisfying \( \lim_{i \to \infty} P(suc) = 1 \). \( C \) is the strong capacity if \( \lim_{i \to \infty} P(suc) = 0 \) for any sequence of algorithms satisfying (7).

For example, in [2] we proved that noiseless adaptive combinatorial group testing has strong capacity 1. This result is proved by combining Hwang’s Generalized Binary Splitting Algorithm [3] (which is essentially optimal – see also [2], [23] for a discussion of this) with the converse result Theorem I.1. However, even in the noiseless non-adaptive case the capacity remains unknown in general, although some results are known in some regimes, under assumptions about the distribution of \( X \) (see for example [25], [4], [28], [29]).

Capacity results are asymptotic in character, whereas we will consider the finite blocklength regime (in the spirit of [31], [15]) and prove bounds on \( P(suc) \) for any size of problem. We briefly review existing converse results. First, we mention that results (often referred to as folklore) can be proved using arguments based on Fano’s inequality.

**Lemma II.2.** Using \( T \) tests in the noiseless case:

1) For combinatorial group testing Chan et al. [6] Theorem I] give

\[
P(suc) \leq \frac{T}{\log_2 \left( \frac{N}{K} \right)},
\]

(9)

2) For probabilistic group testing Li et al. [8] Theorem I give

\[
P(suc) \leq \frac{T}{Nh(p)}.
\]

(10)

In order to understand the relationship between (9) and Theorem I.1 fix \( \delta > 0 \) and use \( T = T^*(1 - \delta) \) tests, in a regime where \( \log_2 \left( \frac{N}{K} \right) \to \infty \) and hence \( T^* \to \infty \). Chan et al.’s result (9) gives that \( P(suc) \leq (1 - \delta) \), whereas (1) implies \( P(suc) \leq 2^{-\delta T^*} \). In the language of Definition II.1 Chan et al. [6] give a weak converse whereas Baldassini, Johnson and Aldridge [2] give a strong converse. In fact, [1] shows that the success probability converges to zero exponentially fast.

To understand why Chan et al’s result (9) is not as strong as Theorem I.1 we examine the proof, which uses Fano’s inequality, bounding the entropy \( H(U|Y) \) in a standard way using

\[
H(U|Y) \leq 1 + P(E = 1)H(U|Y, E = 1)
\]

(11)

where \( E \) is the indicator of the error event \( U \neq Z \). In (11) this last term is bounded by \( \log_2 \left( \frac{N}{K} \right) \), since a priori \( U \) could be any defective set. However, in practice, this is a significant overestimate. For example, in the noiseless case there is a relatively small collection of defective sets that a particular defective set \( U \) can mistakenly be estimated as (referred to as \( A(\cdot) \) later in this paper). For example, any item appearing in a test pool \( X_t \) giving result \( Y_t = 0 \) cannot be defective. Essentially, Theorem I.1 exploits such facts.

Tan and Atia [32] Theorem 2] prove a strong converse for combinatorial group testing, however, they do not achieve exponential decay. Since the result of the test only depends on whether the items in the defective set \( K \) are present, we can restrict our attention to the submatrix \( X_L \) indexed by subsets \( L \subseteq K \).

**Theorem II.3** ([32], Theorem 2). Define parameters \( \zeta_T := T^{-1/4}P(suc)^{-1/2} \) and \( \eta_T := T^{-1} + h(T^{-1/4}) \). If the components of \( X \) are independent and identically distributed then for
each \( L \), then \( T \) (the number of tests required to achieve the given probability of success) satisfies:

\[
T(I(X_K;L:X_L,Y) + \eta T) \geq (1 - \zeta T) \log_2 \left( \frac{N - |L|}{K - |L|} \right).
\]

Rearranging, and writing \( I = I(X_K;L:X_L,Y) \) we obtain

\[
\mathbb{P}(\text{suc}) \leq \frac{1}{T^{1/2} \left( 1 - T(I + \eta T) / \log_2 \left( \frac{N - |L|}{K - |L|} \right) \right)^2} \sim \frac{1}{\delta^2 T^{1/2}},
\]

taking \( T^* = \log_2 \left( \frac{N - |L|}{K - |L|} \right) / I \) for \( T = (1 - \delta)T^* \). This gives a strong converse, though not the exponential decay achieved in [11] above. However Tan and Atia’s results [32] are valid in a variety of settings and noise models.

Pedagogically, we note a parallel between these various approaches and treatments of the channel coding problem in the literature. That is [9], due to Chan et al. [6], is proved using Fano’s inequality, parallelling the proof of Shannon’s noisy coding theorem exemplified for example in [33] Section 8.9. The argument of Tan and Atia [32] is based on Marton’s blowing up lemma, mirroring the treatment of Shannon’s theorem in the book of Csiszár and Körner [34] Section 6.

Our work in the non-adaptive case is based on the more recent work of Polyanskiy, Poor and Verdú [15], which has been adapted to the problem of data compression in [35]. We remark that Scarlett and Cevher use an approach parallel to ours, based on the Verdú–Han information spectrum method of Definition III.1.

Write \( \text{coding error probabilities} \). Noting that as in [16], we do not assume that \( Q \) is a probability measure, and simply think of \( \beta_{1-\epsilon} \) as the maximum value of \( Q \) (do not reject null \( \in \) alternative is true).

We use the same analogy as [15] for the group testing problem, given a process generating random chosen defective sets \( U \) (a source). To some extent this is simply a question of adapting the notation of [15]. However, unlike [15] we do not require that \( U \) is uniform (allowing us to consider probabilistic as well as combinatorial group testing). In a pure channel coding scenario it seems less natural to consider non-uniform \( U \), however such \( U \) were considered in [16], where a list-decoding argument was used to analyse the joint source–channel coding problem. In fact, we combine the approaches of [16] and [15].

Since we consider non-adaptive group testing, we fix \( X = X' \) in advance. We identify the Only Defects Matter property, Definition [4], as playing a key role. We write \( P_{K|Y} (k|y) \) for the joint probability distribution of \( K \) and \( Y \) and consider an algorithm which estimates (decodes) the defective set \( Z = U \), using only outputs \( Y \) and test matrix \( X = X' \). Since \( X = X' \) is fixed, we can simplify (6) above and write \( P_{Z|Y}(z|y) \) for the probability that the estimator gives \( Z = z \) when \( Y = y \). We prove the following result in Appendix A.

**Theorem III.2.** Suppose that the group testing model satisfies the Only Defects Matter property, Definition [4] For any non-adaptive choice of test design, any estimation rule \( P_{Z|Y} \) with \( \mathbb{P}(\text{suc}) \geq 1 - \epsilon \) and probability mass function \( Q_{Y} \) satisfies:

\[
\beta_{1-\epsilon}(P_{K|Y}, P_{K} \times Q_{Y}) \leq \sum_{z \in \{0,1\}^N} P_{U}(z) Q^*(z),
\]

where \( Q^*(z) = \sum_{y} Q_{Y}(y) P_{Z|Y}(z|y) \) is the probability that \( Y \sim Q_{Y} \) is decoded to \( z \).

**Corollary III.3.** In the noiseless non-adaptive case consider any defective set distribution \( P_{U} \) and write \( \Pi_{U}(m) \) for the sum of the largest \( m \) values of \( P_{U}(z) \). Then

\[
\mathbb{P}(\text{suc}) \leq \Pi_{U}(2^T).
\]

**Proof.** See Appendix A.

In particular, Corollary III.3 extends Theorem I.1 under the additional assumption of non-adaptivity; we discuss how to remove this assumption in Theorem IV.3 below. That is, if for some set \( M \) of size \( |M| \), the \( P_{U}(z) = \mathbb{I}(z \in M) / |M| \) then

\[
\mathbb{P}(\text{suc}) \leq 2^T / |M|.
\]

In retrospect, perhaps this result is not surprising; we think of an optimal list decoding by simply choosing the defective set of highest probability compatible with each output \( y \).

**Theorem III.2** also implies a converse for the non-adaptive binary symmetric channel case, which will hold more generally in the adaptive case. We discuss this in Section V-B below (since an upper bound on success probabilities for adaptive group testing implies an upper bound for non-adaptive group testing).
IV. ADAPTIVE GROUP TESTING

As discussed in Section I, a precise formulation of adaptive group testing (corresponding to channels with feedback) requires the use of directed probability distributions and information theory. For any $t$, we write $Y_{1,t} = \{Y_1, \ldots, Y_t\}$ and $X_{1,t} = \{X_1, \ldots, X_t\}$. We first prove the following representation of the joint probability distribution of $(U, X, Y)$ for adaptive group testing:

**Lemma IV.1.** Assuming the Only Defects Matter property (Definition I.4) with transition matrix $P(Y_t = y|K_t = k) = P(y|k)$ for all $k, y, t$, we can write

$$P_{U,X,Y}(u, x, y) = P_U(u) P_{X|Y}(x|y) \prod_{t=1}^{T} P(y_t|k_t),$$

where $k_t = u, x_t$ (matrix product) is the number of defectives in the $t$-th test and

$$P_{X|Y}(x|y) = \prod_{t=1}^{T} P(x_t|y_{1:t-1}, x_{1:t-1})$$

is the causal conditional probability, with the key property that for any fixed $y$:

$$\sum_x P_{X|Y}(x|y) = 1.$$

**Proof.** We write (omitting the subscripts on $P$ for brevity) $P(u, x, y)/P(u)$ as a collapsing product of the form:

$$\prod_{t=1}^{T} P(u, x_{1:t-1}, y_{1:t-1}) \prod_{t=1}^{T} P(x_t|y_{1:t-1}, x_{1:t-1}) = \prod_{t=1}^{T} \sum_{x_t} P(x_t|y_{1:t-1}, x_{1:t-1}) \prod_{t=1}^{T} P(y_t|x_t, x_{1:t-1}, y_{1:t-1})$$

where we remove the conditioning in the final line since $y_t$ is the result of sending $k_t = U^T x_t$ through a memoryless channel (the output of which is independent of previous test designs and their output) and since the choice of the $t$-th test pool $x_t$ is conditionally independent of $U$, given the previous tests and their output.

Recall from (6) that we write $P_{Z|Y,X}(z|y, x)$ for the probability that some algorithm estimates the defective set as $U = Z = z \in \{0, 1\}^N$ when the group testing process with test matrix $X = x$ returns $Y = y$. We write $S_x^T(y)$ for the set of values that $y$ may be decoded to; that is $u \in S_x^T(y)$ if and only if $P_{Z|Y,X}(u|y, x) > 0$.

**Theorem IV.2.** Take any probability mass function $Q_Y$ on $\{0, 1\}^T$. For any model of group testing (adaptive or non-adaptive), satisfying the Only Defects Matter property Definition I.4, if there is a decoding rule $P_{Z|Y,X}$ with success probability $P(suc) \geq 1 - \epsilon$ and a probability measure $Q_U$ such that $Q_U(S_x^T(y)) \leq L$ for all $y$, then

$$\beta_{1-\epsilon}(P_{U|P_X|Y} - P_{Y|K, U} Q_U P_{X|Y} Q_Y) \leq L.$$

**Proof.** See Appendix [B].

Note that this result resembles the list decoding version of the meta-converse [16] Lemma 4. We use arguments based on Theorem IV.2 to prove a result which extends Theorem I.1 for general defective set distributions $P_U$ in the noiseless binary case. This result applies to both adaptive and non-adaptive group testing.

**Theorem IV.3.** For noiseless adaptive binary group testing, if we write $\Pi_U(m)$ for the sum of the largest $m$ values of $P_U(z)$

$$P(suc) \leq \Pi_U(2^T).$$

**Proof.** See Appendix [C].

For combinatorial group testing, since $P_U$ is uniform on a set of size $2^N$, Theorem IV.3 implies that $\Pi_U(m) = m/2^N$ and we recover Theorem I.1. We show how sharp this result is in Figure 1 which is reproduced from [2, Figure 1].

**Corollary IV.4.** Consider a sequence $U(i)$ of defectivity vectors of length $i$, generated as independent realisations of a stationary ergodic stochastic process of entropy rate $H$. Given $T(i) = (H - \epsilon)i$ tests to solve the $i$th noiseless adaptive group testing problem, the success probability tends to zero. (Hence the strong capacity cannot be more than 1).

**Proof.** We define the typical set

$$T(i) = \left\{ \left[ -\log P_{U(i)}(u) \right] / i \leq \frac{\epsilon}{2} \right\}$$

By the Shannon-McMillan-Breiman theorem (AEP) (see for example [33] Theorem 15.7.1), the probability $P(T(i)) \rightarrow 1$. Then, in Theorem IV.3, the $2^T(i)$ strings of largest probability will certainly be contained in a list containing the elements of $(T(i))^c$ and the $2^T(i)$ strings of largest probability in $T(i)$. Since, by definition, any string in $T(i)$ has probability less than $2^{-iH+i\epsilon/2}$, we deduce that

$$P(suc) \leq \Pi_U(m) \left( 2^{T(i)} \right) \leq P \left( (T(i))^c \right) + 2^{T(i)} 2^{-iH+i\epsilon/2} = P \left( (T(i))^c \right) + 2^{-i\epsilon/2}.$$

Given a quantitative form of the Shannon-McMillan-Breiman theorem (proved for example using the concentration inequalities described in [32]), we can deduce an explicit (exponential) rate of convergence to zero of $P(suc)$.

Note that (since it is proved using concentration inequalities only), although this result gives a strong converse, it may do so with a sub-optimal exponent (rate of convergence). It remains of interest to categorise the optimal strong converse exponent in these problems.

We give more explicit bounds which show how Theorem IV.3 can be applied in the noiseless probabilistic case in Section V-A below. Section V-B contains an illustrative example of results that can be proved using Theorem IV.2 in the noisy
A. Noiseless adaptive probabilistic group testing

In this section, we give an example of bounds which can be proved using Theorem IV.3 for noiseless adaptive probabilistic group testing. Note that the control of the source strings with highest probabilities is an operation that lies at the analysis of the finite blocklength data compression problem in [33].

Example V.1. We consider the identical Probabilistic case, where \( p_i \equiv p < 1/2 \), so \( P_U(z) = p^w(1-p)^{N-w} \), where \( w = w(z) \) is the Hamming weight of \( z \). Write

\[
L_{N,T}^* := \min \left\{ L : \sum_{i=0}^{L} \binom{N}{i} \geq 2^T \right\}
\]

and define \( s \geq 0 \) via

\[
2^T = \sum_{i=0}^{L_{N,T}^*-1} \binom{N}{i} + s,
\]

meaning the \( 2^T \) highest probability defective sets are all of those of weight \( \leq L_{N,T}^* - 1 \), plus \( s \) of weight \( L_{N,T}^* \). We evaluate \( \Pi_U(2^T) \) to obtain a bound on which we plot in Figure 2

\[
\Pi_U(2^T) = \sum_{i=0}^{L_{N,T}^*-1} \binom{N}{i} p^i (1-p)^{N-i} + sp^{L_{N,T}^*}(1-p)^{N-L_{N,T}^*}.
\]  

(22)

Remark V.2. We give a Gaussian approximation to the bound (22), in the spirit of [15]. Since we need to control tail probabilities we use the approximation given by Chernoff bounds (see Theorem D.1). If \( L = L(y) := Np + y\sqrt{Np(1-p)} \) and \( T(y) = Nh(L(y))/N \) then (22) gives

\[
\mathbb{P}(\text{Bin}(N,1/2) \leq L(y)) \simeq 2^{-N+T(y)},
\]  

(23)

giving an approximate solution to (20) (as discussed in Appendix D here \( \simeq \) denotes equality on an exponential scale). Substituting in (22) and using a second normal approximation, we obtain an approximation in parametric form, that with \( T(y) \) tests the

\[
\mathbb{P}(\text{suc}) \leq \Pi_U(2T(y)) \simeq \mathbb{P}(\text{Bin}(N,p) \leq L(y)) = \Phi(y) + o(1).
\]  

(24)

For example, if \( y = 0 \) then \( T = T(0) = Nh(p) \) (the magic number) and \( L = Np \), and \( \Pi_U(2T) - 1/2 = o(1) \).

Indeed using the Chernoff bound, we use (24) to deduce a strong capacity result:

Corollary V.3. Noiseless binary probabilistic group testing has strong capacity \( C = 1 \) in any regime where \( p \to 0 \) and \( Np \to \infty \).
Sketch proof. For any \( p \leq 1/2 \) and \( \epsilon > 0 \), we consider the asymptotic regime where \( T = Nh(p - \epsilon) \) as \( N \to \infty \). Choosing \( L = N(p - \epsilon/2) \), we know that using standard bounds (see for example [33] Equation (12.40))

\[
\sum_{i=0}^{L} \left( N \right)_i \geq \left( N \right)_{N/2} \geq 2^{Nh(L/N)} N + 1 \geq 2^{Nh(p - \epsilon/2)} N + 1 \geq 1,
\]

which is larger than \( 2^T \) in the asymptotic regime. Hence, summing over the strings of weight \( \leq L \) will give at least the \( 2^T \) strings of highest probability, and we deduce by Theorem D.1 that

\[
P(\text{suc}) \leq P(\text{Bin}(N,p) \leq N(p - \epsilon/2)) \leq 2^{-ND(p - \epsilon/2)|p|},
\]

which tends to zero exponentially fast. This complements the performance guarantee proved in [7], strengthening the result of [7] Corollary 1.5 where the corresponding weak capacity result was stated using (10).

B. Noisy adaptive group testing example

We now use Theorem IV.2 to prove a bound on \( P(\text{suc}) \) in a noisy example. For simplicity we state the following example in the case of uniform \( U \). Further generalizations (in the spirit of Theorem IV.3) are possible by adapting the proofs along the lines of Section C.

**Example V.4.** Suppose \( U \) is uniformly distributed on a set \( M \) of size \( M \) and suppose the output of standard combinatorial noiseless non-adaptive group testing \( X \) is fed through a memoryless binary symmetric channel with error probability \( p < 1/2 \) to produce \( Y \). We write \( x_i = 1(k_i \geq 1) \), and observe that \( P(y_i|k_i) = (1-p)^{T-d(x_i,y_i)}p^{d(x_i,y_i)} \), where \( d \) represents the Hamming distance.

Consider the optimal rule for deciding between null hypothesis \( P_U P_X|Y - P_U|K \) and alternative \( Q_U P_X|Y - Q_Y \). If \( Q_U = P_U \) and \( Q_Y = 1/2T \), the likelihood ratio is

\[
P_U(u) P_X|Y = (X|Y) P_Y|K (y|k) \quad Q_U(u) P_X|Y = (X|Y) Q_Y (y) \equiv 1/2T.
\]

By the Neyman–Pearson lemma, the optimal rule is to accept the null if \( d(x,y) > d^* \), to accept the null with probability \( \lambda \) if \( d(x,y) = d^* \) and to reject the null otherwise, where we calculate \( d^* \) and \( \lambda \) as follows:

\[
\frac{1}{M} \geq \beta_{1-\epsilon}(P_U P_X|Y = P_Y|K, Q_U P_X|Y = Q_Y)
\]

where the first inequality follows from Theorem IV.2. Then, for this value of \( d^* \) we write that

\[
P(\text{suc}) = 1 - P(\text{type I error}) = \sum_{x,y} P_{KY}(k,y) P(\text{accept } P_{KY})
\]

\[
= P(\text{Bin}(T,p) \leq d^* - 1) + \lambda P(\text{Bin}(T,p) = d^*).
\]

In Figure 3(a), we plot this in the case \( N = 500, K = 10, p = 0.11 \), and for comparison plot the Fano bound taken from [6] Theorem 2:

\[
P(\text{suc}) \leq \frac{T(1 - h(p))}{\log_2 \left( \frac{N}{K} \right)}.
\]

In Figure 3(b) we give the group testing analogue of [15] Figure 1. We use the regime of [13]; that is, we vary \( N \) and take \( K = \lceil N^{1-\beta} \rceil \), where \( \beta = 0.37 \) (this gives the value \( K = 10 \) for \( N = 500 \)). Again taking \( p = 0.11 \), we fix \( P(\text{suc}) = 0.999 \), and use the lower bound on \( T \) corresponding to the analysis above. This gives an upper bound on the rate \( \log_2 \left( \frac{N}{K} \right) / T \), which we plot in Figure 3(b).

Note that in this finite size regime, exactly as in [15] Figure 1, the resulting bound rate is significantly smaller than the capacity \( C = 1 - h(p) = 0.500 \), which we only approach asymptotically.

**Remark V.5.** As in Remark IV.2 we can give a Gaussian approximation in the setting of Example IV.4 and deduce a capacity result. Using (38) we deduce from (25) that \( d^* \) satisfies

\[
\frac{1}{M} \simeq P(\text{Bin}(T,1/2) \leq d^*) \simeq 2^{-T + T h(d^* / T)},
\]

or \( h(d^* / T) = 1 - \log_2 M / T + o(1) \). Hence for a sequence of problems where the \( i \)th problem has \( U^{(i)} \) uniformly distributed on a set of size \( M(i) \) we know that

\[
\liminf_{i \to \infty} \frac{\log_2 M(i)}{T(i)} \geq C + \epsilon := 1 - h(p) + \epsilon,
\]

so \( d^* / T < p - \delta \) and we can deduce by Theorem D.1 that

\[
P(\text{suc}) \simeq P(\text{Bin}(T,p) \leq d^*) \leq 2^{-TD(p - \epsilon)}.
\]
so tends to zero exponentially fast, meaning that the strong capacity must be less than $1 - h(p)$.

Note the similarity between the calculations in Examples V.1 and V.4 in the former case we control source probabilities (see also [15] Theorem 35) in the latter case we control concentration of channel probabilities. This fits with the idea that we analyse group testing as a joint source-channel coding problem.

**Appendix A**

**Proof of Non-Adaptive Results**

We use an argument based on [13], adapted to the scenario where $U$ need not be uniform. Note that while this case is considered in [16], that paper uses a different (list-decoding) rule; in effect we combine the hypothesis testing rule of [15] and the model of [16]. We use the list-decoding rule of [35] in Appendix [9].

Consider a hypothesis testing problem where we are given a pair $(k, y)$ and asked to test the null hypothesis that it comes from joint distribution $P_{KY}$ against an alternative of some other specific $Q_{KY}$. This is a counterfactual exercise; in group testing we do not know $K$, however, it is helpful to imagine a separate user who is asked to make inference using this information, and uses the following hypothesis testing rule:

Given pair $(k, y)$ send $y$ to the decoder to produce $z$, and then accept $P_{KY}$ with probability

$$P_{U|K}(z|k) = \frac{P_U(z) P_{K|U}(k|z)}{P_K(k)}.$$  \hspace{1cm} (28)

**Proof of Theorem III.2** The key is to notice that $U \rightarrow K \rightarrow Y \rightarrow Z$ form a Markov chain, so for estimation algorithm $P_{Z|Y}$ we obtain

$$P_{Z|U}(w|z) = \sum_{k, y} P_{Z|Y}(w|y) P_{Y|K}(y|k) P_{K|U}(k|z).$$

Using this, there is an equivalence between group testing error probability and $P$(Type I error) since

$$P(\text{suc}) = \sum_{z, w} P_U(z) \mathbb{1}(w = z) P_{Z|U}(w|z)$$

$$= \sum_{z, w} P_U(z) \mathbb{1}(w = z)$$

$$\times \left[ \sum_{k, y} P_{Z|Y}(w|y) P_{Y|K}(y|k) P_{K|U}(k|z) \right]$$

$$= \sum_{k, y, z} P_{KY}(k, y) P_{Z|Y}(z|y) \frac{P_U(z) P_{K|U}(k|z)}{P_K(k)}$$  \hspace{1cm} (29)

$$= \sum_{k, y} P_{KY}(k, y) \sum_z P_{Z|Y}(z|y) P_{K|U}(k|z)$$

$$= \sum_{k, y} P_{KY}(k, y) \mathbb{1}(\text{accept } P_{KY} \text{ given pair } (k, y))$$

$$= 1 - \mathbb{P}(\text{Type I error})$$

where we use the expression (28) to deal with (29). We find the probability of a Type II error in the same way. We focus on the case where $Q_{KY} = P_K \times Q_Y$ (so $K$ and $Y$ are independent under $Q_{KY}$), where

$$P(\text{Type II error})$$

$$= \sum_{k, y} Q_{KY}(k, y) \mathbb{1}(\text{accept } P_{KY} \text{ given pair } (k, y))$$

$$= \sum_{k, y} P_K(k) Q_Y(y) \sum_z P_{Z|Y}(z|y) \frac{P_U(z) P_{K|U}(k|z)}{P_K(k)}$$
follows since there are at most $2^Z$ distinct values $u^*(x)$, which are distinct, since they each map to a different value under $\theta$. These various definitions are illustrated in Figure 4. Using (31) we deduce:

$$\mathbb{P}(\text{succ}) = (1 - \epsilon) \leq 2^T \sum_{x \in \{0,1\}^N} P_U(z) Q^*(z)$$

$$\leq 2^T \sum_{y \in \{0,1\}^T} P_U(z) P_{Z|Y}(z|y)$$

$$\leq \sum_{y \in \{0,1\}^T} \sum_{z \in \{0,1\}^N} P_{max}(y) P_{Z|Y}(u|y)$$

$$\leq \sum_{y \in \{0,1\}^T} P_{max}(y)$$

$$= \sum_{y \in \{0,1\}^T} P_{U}(u^*(y))$$

$$\leq \Pi_U(2^T).$$

Here (32) follows since for given $y$ the success probability is maximised by restricting to $P_{Z|Y}(z|y)$ supported on the set $z \in A(y)$, so we know that $P_U(z) \leq P_{max}(y)$. The result follows since there are at most $2^T$ distinct values $u^*(x)$, so at most $2^T$ strings $u^*(x)$. This result generalizes (14).

Note that (as expected) the success probability is maximised by the maximum likelihood decoder $P_{Z|Y}$ which places all its support on members of $U^*(y)$.

**APPENDIX B**

** proof of adaptive result, Theorem IV.2**

**Proof of Theorem IV.2** We use the machinery of Kostina and Verdú [16]. That is, given $(U, X, Y)$ we perform a hypothesis test between

$$H_0 : P_U(u) P_{X|Y = \bar{x}}(x|y^-) P_{Y|K}(y|k)$$

$$H_1 : Q_U(u) P_{X|Y = \bar{x}}(x|y^+) Q_{Y}(y),$$

for some probability mass functions $Q_U, Q_Y$. For estimation algorithm $P_{Z|Y,X}$, recall that we write $S^*_K(y)$ for the set of values that $Z$ may be decoded to; that is $u \in S^*_K(y)$ if and only if $P_{Z|Y,X}(u|y, X) > 0$, and use the (sub-optimal) decision rule that we choose $H_0$ if $U \not\in S^*_K(y)$.

We write $u, X, Y$ as indices of summation for brevity, to refer to sums over $u \in \{0,1\}^N, X \in \{0,1\}^{N_T}$ and $Y \in \{0,1\}^T$. Using the fact that for the estimation algorithm $P_{Z|Y,X}$

$$\mathbb{P}(\text{succ}) = u, X = \bar{x}, Y = y$$

$$= \sum_{z} P_{Z|Y,X}(z|y, X) \mathbb{I}(z = u) = P_{Z|Y,X}(u|y, X),$$

as in the proof of Theorem IV.2 there is a relationship between between group testing error probability and $\mathbb{P}(\text{Type I error})$ since:

$$1 - \mathbb{P}(\text{Type I error})$$

$$= \sum_{u, X, Y} P_U(u) P_{X|Y = \bar{x}}(x|y^-) P_{Y|K}(y|k) \mathbb{I}(u \in S^*_K(y))$$

$$= \sum_{u, X, Y} P_U(u) P_{X|Y = \bar{x}}(x|y^-) P_{Y|K}(y|k)$$

$$\times \sum_{z} \mathbb{I}(u \in S^*_K(y)) P_{Z|Y,X}(z|y, X)$$

$$\geq \sum_{u, X, Y} P_U(u) P_{X|Y = \bar{x}}(x|y^-) P_{Y|K}(y|k)$$

$$\times P_{Z|Y,X}(u|y, X)$$

$$= \sum_{u, X, Y} P_U(u) P_{X|Y = \bar{x}}(x|y^-) P_{Y|K}(y|k)$$

$$\times \mathbb{P}(\text{succ}|U = u, X = \bar{x}, Y = y),$$

which we recognise as $\mathbb{P}(\text{succ})$, where the result follows since the inner sum in (33) includes the term $P_{Z|Y,X}(u|y, X)$. Hence, if $\mathbb{P}(\text{succ}) \geq 1 - \epsilon$ then $\mathbb{P}(\text{Type I error}) \leq \epsilon$, so the type II error probability of this decision rule satisfies

$$\beta_1(\epsilon) \leq \mathbb{P}(\text{Type II error}) \leq \mathbb{P}(\text{Type II error})$$

We can write this type II error probability using a similar argument (based on [16], Eq. (60-63)) as

$$\mathbb{P}(\text{Type II error})$$

$$= \sum_{u, X, Y} Q_U(u) P_{X|Y = \bar{x}}(x|y^-) Q_Y(y) \mathbb{I}(u \in S^*_K(y))$$

$$= \sum_{x, y} P_{X|Y = \bar{x}}(x|y^-) Q_Y(y) \sum_{u} Q_U(u) \mathbb{I}(u \in S^*_K(y))$$

$$\leq \sum_{x, y} P_{X|Y = \bar{x}}(x|y^-) Q_Y(y) L$$

$$= L.$$
where the final line follows from (17).

**APPENDIX C**

**PROOF OF THEOREM IV.3**

**Proof of Theorem IV.3**

In general, in the noiseless case, for each defective set $A$, we write $X = Y = \theta(U, X)$. For a particular $Y = y$ and $X = X$, we write $A(y, X) = \theta^{-1}(y, X) = \{z : \theta(z, X) = y\}$ for the defective sets that get mapped to $y$ by the testing procedure defined by $X$. We write $p_{\text{max}}(y, X) = \max_{z \in A(y, X)} P_U(z)$ for the maximum probability in $A(y, X)$ and $U^*(y, X) = \{u : P_U(u) = p_{\text{max}}(y, X)\}$ for the collection of defective sets achieving this probability. For each $y$, pick a string $u^*(y, X) \in U^*(y, X)$ in any arbitrary fashion; and note that there are up to $2^T$ strings $u^*(y, X)$, which are distinct, since they each map to a different value under $\theta(\cdot, X)$. These definitions are illustrated in Figure 4.

![Figure 4. Schematic illustration of the sets used to prove Theorem IV.3.](image)

Since the channel is noiseless, $u \in A(y, X)$, so using the fact that for any $u$ the $1 = \sum_w I(u \in A(w, X))$, we deduce from (34) that $P(\text{suc})$ is

$$
\sum_{u, X, Y} P_U(u) P_{X|Y}(X|y^{-}) P_{Y|K}(y|k) P_{Z|Y, X}(u|y, X)
= \sum_{u, X, Y} P_U(u) P_{X|Y}(X|y^{-}) P_{Y|K}(y|k)
\times P_{Z|Y, X}(u|y, X) \sum_w I(u \in A(w, X))
= \sum_{w, X} P_{X|Y}(X|w^{-}) \sum_u P_U(u)
\times P_{Z|Y, X}(u|w, X) \sum_w I(u \in A(w, X))
\leq \sum_{w, X} P_{X|Y}(X|w^{-}) p_{\text{max}}(w)
\leq \sum_w p_{\text{max}}(w) \sum_X P_{X|Y}(X|w^{-})
= \sum_w p_{\text{max}}(w)
\leq \Pi_U(2^T),
$$

(35)

where (35) follows since $P_U(u) \leq p_{\text{max}}(w)$ on this set and since $\sum_u P_{Z|Y, X}(u|w, X) = 1$. (36) follows by (17). Finally

(37)

where (37) follows since there are at most $2^T$ separate messages $w$, so at most $2^T$ distinct values $u^*(w)$.

**APPENDIX D**

**CONCENTRATION INEQUALITY**

We require an exponential bound in terms of relative entropy. There is a wide literature on this subject, and we take a one-sided form of the Chernoff bound stated as [42 Theorem 5] (for $p \leq 1/2$, we take $d = (1 - p)$ and $\sigma^2 = p(1 - p)$ in the result stated there):

**Theorem D.1.** For $q < p \leq 1/2$, we bound the probability

$$
P(\text{Bin}(n, p) \leq nq) \leq 2^{-nD(q||p)},
$$

where we write $D(q||p)$ for the relative entropy from a Bernoulli($q$) random variable to a Bernoulli($p$), calculated using logarithms to base 2.

Since this is generally a tight bound, we use it to motivate the following approximation, which comes from writing $D(q||1/2) = \log 2 - h(q)$. For any $L$ we deduce that

$$
P(\text{Bin}(N, 1/2) \leq L) \simeq 2^{-N D(L/N||1/2)} = 2^{-Nq Nh(L/N)}.
$$

(38)

Here and throughout the paper, $\simeq$ refers to equality on an exponential scale (the logarithms of both sides are approximately equal). If we take $L = L(y) := Np + y\sqrt{Np(1 - p)}$ and $T(y) = Nh(L(y)/N)$ we deduce that

$$
P(\text{Bin}(N, 1/2) \leq L(y)) \simeq 2^{-N + T(y)}.
$$

(39)

**ACKNOWLEDGMENT**

The author thanks Matthew Aldridge, Leonardo Baldassini and Thomas Kealy for useful discussions regarding the group testing problem, and Vanessa Didelez for help in understanding causal conditional probability. The author would like to thank two anonymous referees and the Associate Editor for their thorough and careful reading of the paper and very helpful suggestions.

**REFERENCES**


