Generalized Group Testing

Xiwei Cheng
The Chinese University of Hong Kong

Sidharth Jaggi
University of Bristol

Qiaoqiao Zhou
National University of Singapore

Abstract

In the problem of classical group testing one aims to identify a small subset (of size d) diseased individuals/defective items in a large population (of size n) via a minimal number of suitably-designed group tests on subsets of items, where the test outcome is positive iff the given test contains at least one defective item. Motivated by physical considerations, we consider a generalized setting that includes as special cases multiple other group-testing-like models in the literature. In our setting, which subsumes as special cases a variety of noiseless and noisy group-testing models in the literature, the test outcome is positive with probability $f(x)$, where x is the number of defectives tested in a pool, and $f(\cdot)$ is an arbitrary *monotonically increasing* (stochastic) test function. Our main contributions are as follows.

1. We present a non-adaptive scheme that with probability $1-\varepsilon$ identifies all defective items. Our scheme requires at most $\mathcal{O}\left(H(f)d\log\left(\frac{n}{\varepsilon}\right)\right)$ tests, where $H(f)$ is a suitably defined "sensitivity parameter" of $f(\cdot)$, and is never larger than $\mathcal{O}\left(d^{1+o(1)}\right)$, but may be substantially smaller for many $f(\cdot)$.

2. We argue that any non-adaptive group testing scheme needs at least $\Omega\left((1-\varepsilon)h(f)d\log\left(\frac{n}{d}\right)\right)$ tests to ensure reliable recovery. Here $h(f)\geq 1$ is a suitably defined "concentration parameter" of $f(\cdot)$.

3. We prove that our sample-complexity bounds for generalized group testing are information-theoretically near-optimal for a variety of sparse-recovery group-testing models in the literature. That is, for *any* "noisy" test function $f(\cdot)$ (i.e., $0<f(0)<f(d)<1$), and for a variety of "(one-sided) noiseless" test functions $f(\cdot)$ (i.e., either $f(0)=0$, or $f(d)=1$, or both) studied in the literature we show that $\frac{H(f)}{h(f)}\in\Theta(1)$. As a by-product we tightly characterize the heretofore open information-theoretic order-wise sample-complexity for the well-studied model of threshold group-testing. For general (near)-noiseless test functions $f(\cdot)$ we show that $\frac{H(f)}{h(f)}\in\mathcal{O}\left(d^{1+o(1)}\right)$. We also demonstrate a "natural" test-function $f(\cdot)$ whose sample complexity scales "extremally" as $\Theta(d^2\log n)$, rather than $\Theta(d\log n)$ as in the case of classical group-testing.

Some of our techniques may be of independent interest – in particular our achievability requires a delicate saddle-point approximation, our impossibility proof relies on a novel bound relating the mutual information of pair of random variables with the mean and variance of a specific function, and we derive novel structural results about monotone functions.

1 INTRODUCTION

Group testing [Dorfman, 1943] is the non-linear sparse recovery process of identifying a small subset of defective items from a larger set of items based on a series of judiciously designed tests. Each test is carried out on a subset of items, and each binary outcome indicates whether or not the test includes at least one defective item. In other words, the test outcome is specified by the "OR" function. In designing the testing scheme, it is desirable to minimize the number of tests while still enabling high probability of correct identification of the subset of defective items. The group testing paradigm has found applications in a wide variety of contexts, including biology [Ngo and Du, 2000], pattern finding [Macula and Popyack, 2004], wireless communications [Berger et al., 1984, Wolf, 1985], and testing for diseases recently COVID-19 testing [Gollier and Gossner, 2020].

Proceedings of the 25th International Conference on Artificial Intelligence and Statistics (AISTATS) 2022, Valencia, Spain. PMLR: Volume 151.

Many variants of the classical group testing paradigm have already been considered in the literature. For example, Damaschke [Damaschke, 2006] considered *threshold test functions*: the test outcome is negative if the number of defectives in a test is no larger than the lower threshold ℓ; positive if no smaller than the upper threshold u; and arbitrary (negative or positive) otherwise. Let n and d be the number of all items and the number of defective items, respectively. For $u = \ell + 1$, Damaschke proposed an adaptive algorithm with the number of tests scaling as $\mathcal{O}\left((d + u^2)\log n\right)$ to exactly identify the defectives. However, for $u > \ell + 1$, he proved that the defectives cannot be exactly identified, but $\mathcal{O}\left((dn^b + d^u)\log n\right)$ adaptive tests suffice to identify the defectives if up to $(u-1)(1+\frac{1}{b})-\ell$ misidentifications are allowed (here $b > 0$ is an arbitrary constant). Chen and Fu [Chen and Fu, 2009] proposed a non-adaptive algorithm for which the number of tests scales as $\mathcal{O}\left(\sigma d^{u+1}\log(\frac{n}{d})\right)$ if up to $u - \ell - 1$ misidentifications and σ erroneous tests are allowed. Subsequently, Cheraghchi [Cheraghchi, 2010] showed that it can be reduced to $\mathcal{O}\left(d^{u-\ell+1}\log d\log(\frac{n}{d})\right)$. More recently, for the special case $u = \ell + 1$, it was further reduced to $\mathcal{O}\left(d^{\frac{3}{2}}\log(\frac{n}{d})\right)$ when u is asymptotically close to $\frac{d}{2}$ [De Marco et al., 2020]. The works of [Bui et al., 2019, Bui et al., 2020] sought to find schemes that admit low decoding complexity. Chan *et al.* [Chan et al., 2013] studied stochastic threshold group testing. They introduced two stochastic variants of the threshold test function: Bernoulli gap stochasticity and linear gap stochasticity. For Bernoulli gap stochasticity, the test outcome is equally likely to be negative or positive whenever the number of defectives in a test is in the interval (ℓ, u). For linear gap stochasticity, the probability of having positive outcome increases linearly as the number of defectives ranges from ℓ to u. By allowing a small error probability ε, they proposed a two-stage adaptive algorithm with $11.09e^2 d\log n + \mathcal{O}\left(d\log(\frac{1}{\varepsilon})\right)$ number of tests and a non-adaptive algorithm with $\mathcal{O}\left(\log(\frac{1}{\varepsilon})d\sqrt{\ell}\log n\right)$ number of tests for Bernoulli gap stochasticity, and a non-adaptive algorithm with $\mathcal{O}\left((u-\ell-1)^2 d\log n\right)+\mathcal{O}\left(d\log(\frac{1}{\varepsilon})\right)$ number of tests for linear gap stochasticity. Recently, for Bernoulli gap stochasticity, Reisizadeh *et al.* [Reisizadeh et al., 2018] improved the number of tests required to $\mathcal{O}\left(\sqrt{u}d\log^3 n\right)$.

In this paper, motivated by physical considerations such as scenarios with imperfect test apparatus, we formulate and analyze group testing with a general monotonically increasing stochastic test function $f(\cdot)$ (i.e., $x \geq y \Rightarrow f(x) \geq f(y)$) that takes as input the number of defective items in a test and outputs the probability of the given test having a positive outcome. This formulation subsumes as special cases a variety of noiseless and noisy group-testing models in the literature. In this work, as detailed in Section 4, we provide (i) a non-adaptive scheme that with high probability reliably recovers the set of defectives for *any* monotone test function, (ii) an information-theoretic lower bound on the sample complexity for reliable recovery for any non-adaptive testing scheme, and (iii) arguments comparing (i) to (ii) showing that for a wide variety of monotone test functions the sample complexity of our non-adaptive scheme is order-optimal (and for any other test function it is no more than a factor $\mathcal{O}(d^{1+o(1)})$ from optimal).

2 PROBLEM FORMULATION

A set $\mathcal{N} := \{1, \ldots, n\}$ of n items contains a subset $\mathcal{D} \subsetneq \mathcal{N}$ of *defective* items – elements in $\mathcal{N} \setminus \mathcal{D}$ are called *non-defective*. We follow the "combinatorial group testing model", which assumes that the size of defective set $\mathcal{D}$ is fixed as d, and each such subset has the same probability. The identity of $\mathcal{D}$ is unknown *a priori* – the goal of group testing is to correctly identify $\mathcal{D}$ through a minimal series of *group* tests on subsets of items. In "classical" group testing a test outcome is negative if every item in the pool is non-defective, and is positive if at least one item is defective. As such this may be viewed as a *disjunctive* measurement, i.e., viewing each item as a 0 or a 1 depending on whether it is non-defective or defective, each test performs an OR of the items in its pool. A canonical setting in which this measurement model is pertinent is when a small number of individuals in a large population are diseased but only a small number of testing kits are available; in this case samples from different individuals may be "pooled" together in different combinations and the set of test outcomes analyzed jointly to infer $\mathcal{D}$. In this work we assume that the *number* $d = |\mathcal{D}|$ of defectives is known *a priori*.[1]

Instantiating disjunctive tests which are sensitive to even a single defective in a testing pool may be tricky, for instance due to the impact of dilution on the chem-

[1] Some works (e.g. [Damaschke and Muhammad, 2010, Falahatgar et al., 2016, Bshouty et al., 2018]) consider the problem of reliably estimating the number d (rather than the set $\mathcal{D}$) with a minimal number of adaptive or non-adaptive tests. In classical group-testing, most algorithms are reasonably robust to small perturbations in the value of d, and the task of roughly estimating the number d is an "easier" task, requiring asymptotically fewer tests than the task of estimating the set $\mathcal{D}$. In this generalized group-testing setting, our algorithms and bounds are sensitive to small perturbations in the value of d, and require the exact value of d. In Appendix Q, we present an algorithm for exactly estimating the number d. It turns out to be a "harder" task, requiring asymptotically more tests than the task of estimating the set $\mathcal{D}$.

istry used in pooled tests [Zenios and Wein, 1998]. Our primary contribution in this work is to consider a very general class of (probabilistic) measurement functions $f(\cdot) : \mathbb{Z}_{\geq 0} \to [0, 1]$. The input, say x, to the measurement function $f(x)$ is the number of defective items x in a given pool, and the value of $f(x)$ is the probability that the given test results in a positive test outcome.

A slight notational subtlety here – since we will be interested in asymptotic results (when d and n are "large"), in the interest of generality we allow the function $f(\cdot)$ to also depend on the value of d. Hence our notation $f(\cdot)$ actually indexes a set $\{f_d(\cdot)\}_d$ of measurement functions. Since we assume the number d to be known in advance,[1] so the function $f_d(\cdot)$ in the set $f(\cdot)$ is well-specified. Thus for notational convenience we suppress the dependence of $f(\cdot)$ on d in the rest of this paper. Hence a statement like $f(0) \xrightarrow{d\to\infty} 0$ should be interpreted as meaning that $\lim_{d\to\infty} f_d(0) = 0$.

In this work we restrict ourselves to the natural class of measurement, *monotone* measurement functions, i.e., $x \geq y \Rightarrow f(x) \geq f(y)$. Monotone measurement functions subsume many existing models of group-testing as special cases. For instance, when

$$f(x) = \begin{cases} 0 & x = 0, \\ 1 & x \geq 1, \end{cases} \tag{1}$$

this reduces to the problem of classical group testing. Observe that when

$$f(x) = \begin{cases} 0 & x \leq \ell, \\ \frac{x-\ell}{u-\ell} & \ell < x < u, \\ 1 & x \geq u, \end{cases} \tag{2}$$

for some integers $0 < \ell < u < d$, this reduces to the "linear gap" stochastic group testing examined by [Chan et al., 2013]. To avoid triviality, we further assume that $f(0) < f(d)$. (If $f(0) = f(d)$, no sequence of tests can ever reliably recover the defective set $\mathcal{D}$.)

We distinguish between two types of test functions:

• If $0 < f(0) < f(d) < 1$, we say that $f(\cdot)$ is *noisy*. For such $f(\cdot)$, even pools with no defective items have a probability $f(0)$ (some positive constant independent of d) of resulting in a positive test outcome, and pools with one or more defective items have a probability of at least $1 - f(d)$ (again, a constant bounded away from 0, independent of d) of resulting in a negative test outcome. The corresponding notion of noisy test outcomes in the classical group-testing literature (see for instance [Scarlett and Cevher, 2018]) often focuses on test functions of the form

$$f(x) = \begin{cases} a & x = 0, \\ b & x \geq 1, \end{cases} \tag{3}$$

for some $0 < a < b < 1$ (with the *symmetric noise setting*, i.e. $b = 1 - a$, receiving the most attention).

• In contrast, if either $f(0) \xrightarrow{d\to\infty} 0$ or $f(d) \xrightarrow{d\to\infty} 1$ we say that $f(\cdot)$ is *one-sided near-noiseless*, and if both limits hold we say that $f(\cdot)$ is *near-noiseless*. Analogously, if either $f(0) = 0$ or $f(d) = 1$ we say that $f(\cdot)$ is *one-sided noiseless*, and if both equalities hold we say that $f(\cdot)$ is *noiseless*.

Note that (one-sided) near-noiselessness is a significantly weaker requirement on $f(\cdot)$ than in much of the noiseless group-testing literature, where it is often assumed that $f(0) = 0$ and $f(1) = 1$ (the corresponding one-sided noiseless version was studied in [Scarlett and Johnson, 2020]).

Group testing schemes can be adaptive (where each test may be designed based on the outcomes of all preceding tests) or non-adaptive (where all tests must be chosen prior to observing any test outcomes). Here, we focus on non-adaptive group testing.[2]

Non-adaptive generalized group-testing test designs are specified by a (possibly randomly chosen) binary matrix $\boldsymbol{M} \in \{0, 1\}^{T\times n}$, where $M_{ji} = 1$ if test j includes item i and $M_{ji} = 0$ otherwise. The rows of $\boldsymbol{M}$ correspond to tests, and the columns correspond to items. The probability of error of any non-adaptive algorithm (with a specified test matrix $\boldsymbol{M}$) is defined as the probability that the estimated defective set $\hat{\mathcal{D}}$ differs from the true $\mathcal{D}$. This probability is over $\mathcal{D}$ (distributed uniformly over all d-sized subsets of $\{1, \dots, n\}$) and the randomness in test outcomes (governed by $f(\cdot)$). We require that the probability of error, $\Pr(\hat{\mathcal{D}} \neq \mathcal{D}) \leq \varepsilon$ – such test designs will be called $(1 - \varepsilon)$-reliable.

3 TEST DESIGN AND DECODING

We now present our non-adaptive test designs, and the corresponding decoding rules. We emphasis here that the algorithm below depends critically on a priori knowledge of the size d of the defective set.

Test design: We consider Bernoulli designs – see, for example, [Atia and Saligrama, 2012]. That is, the test matrix $\boldsymbol{M}$ is a $T \times n$ binary matrix in which each entry is independently chosen to equal 1 with probability q and 0 otherwise, for design parameters T and $q \in (0, 1)$ specified below.

[2]The adaptive version of group-testing has also been extensively studied – see for instance the survey in [Du et al., 2000]. However, since non-adaptive tests allow for test-parallelization, and also make it easier to design hardware to perform the tests (unlike adaptive test designs, where the composition of (at least some) tests may depend on prior test outcomes), we restrict our attention in this work to designing non-adaptive schemes.

Parameters for the decoding rule: First some definitions and notation:

1. *Item-included test-positivity probability:* For any item i in a test, the quantity $P(-,q)$ denotes the probability that the test has a positive outcome conditioned on the event that item i is non-defective.[3] Analogously $P(+,q)$ denotes[3] the probability that the test has a positive outcome conditioned on the event that item i is defective. Mathematically,

$$\begin{aligned} P(-,q) &:= \sum_{j=0}^{d} \binom{d}{j} q^j (1-q)^{d-j} f(j), \text{ and} \\ P(+,q) &:= \sum_{j=0}^{d-1} \binom{d-1}{j} q^j (1-q)^{d-1-j} f(j+1). \end{aligned} \tag{4}$$

2. *Item-not-included test-positivity probability:* For any non-defective item i not in a given test, $Q(-,q)$ denotes[3] the probability of a positive test outcome. Analogously, for any defective item i not in a given test, $Q(+,q)$, denotes[3] the probability of a positive test outcome. Mathematically,

$$\begin{aligned} Q(-,q) &:= \sum_{j=0}^{d} \binom{d}{j} q^j (1-q)^{d-j} f(j), \text{ and} \\ Q(+,q) &:= \sum_{j=0}^{d-1} \binom{d-1}{j} q^j (1-q)^{d-1-j} f(j). \end{aligned} \tag{5}$$

3. *Item test sensitivity:* For any item i in (respectively not in) a test, its test sensitivity $\Delta(q)$ (respectively $\nabla(q)$) is defined as the difference between the probabilities of positive test outcomes conditioned on item i being defective or not.[3] Mathematically,

$$\begin{aligned} \Delta(q) &:= P(+,q) - P(-,q), \text{ and} \\ \nabla(q) &:= Q(-,q) - Q(+,q). \end{aligned} \tag{6}$$

4. *Minimal test sensitivity:* A parameter that will be useful in our code design and analysis is the minimal test sensitivity $P_{\min}(q)$, defined as

$$P_{\min}(q) := \min\left\{P(+,q), 1 - Q(+,q)\right\}. \tag{7}$$

Lemma 1, (proof is given in Appendix C) provides (in)equalities relating the quantities defined above.

Lemma 1. *For all $q \in (0,1)$, we have*

$$f(d) \geq P(+,q) > P(-,q) = Q(-,q) > Q(+,q) \geq f(0), \tag{8}$$

$$\nabla(q) = \frac{q}{1-q}\Delta(q), \tag{9}$$

$$1 \geq P_{\min}(q) \geq \max\left\{\Delta(q), \nabla(q)\right\}. \tag{10}$$

5. *Test participation parameters:* It also helps to define the test participation parameter m as in (11) below. As shown in Lemma 3 in Appendix A.1, with high probability each item in $\mathcal{N}$ participates in at least m tests.

$$m := \frac{8.32 P_{\min}(q)}{\left(\Delta(q)\right)^2} \log\left(\frac{2n}{\varepsilon}\right). \tag{11}$$

Correspondingly, we define s as below so that, as shown in Lemma 5 in Appendix A.1, with high probability each item in $\mathcal{N}$ participates in at most $T - s$ tests.

$$s := \frac{8.32 P_{\min}(q)}{\left(\nabla(q)\right)^2} \log\left(\frac{2n}{\varepsilon}\right). \tag{12}$$

6. *Number of tests:* We set the number of tests T as

$$T \geq \Gamma(q) := \frac{13(1-q)}{3q} m \tag{13}$$

7. *Choice of q:* One wishes to choose q such that the defective set $\mathcal{D}$ can be reliably recovered while minimizing the required number of tests. As shown in Appendix A.1, for all $q \in (0,1)$, $\Gamma(q)$ tests of the above design can reliably recover the defective set $\mathcal{D}$. Therefore we should choose q as the value in $(0,1)$ that minimizes $\Gamma(q)$. However, such a minimizing q is hard to analyze and analytically characterize. Instead, we consider the quantity $\hat{\Gamma}(q)$ defined as

$$\hat{\Gamma}(q) := \frac{\Gamma(q)}{P_{\min}(q)} = \frac{36.06(1-q)}{q(\Delta(q))^2} \log\left(\frac{2n}{\varepsilon}\right). \tag{14}$$

The equality in (14) follows by using (11) and (13). Note that $\hat{\Gamma}(q) \geq \Gamma(q)$ for all $q \in (0,1)$ since $P_{\min}(q) \leq 1$ by (10), and hence an upper bound on $\hat{\Gamma}(q)$ is also an upper bound for $\Gamma(q)$. We will choose q as

$$q^* := \operatorname*{argmin}_{q \in (0,1)} \hat{\Gamma}(q). \tag{15}$$

It turns out such a q^* can be efficiently characterized – see Theorem 1-c) for details.

Decoding rules: We are now ready to describe our two decoding rules, each of which proceeds by separately estimating whether or not each item $i \in \mathcal{N}$ is defective or not (instead of jointly estimating the (non)-defective status of all i simultaneously). Note that both decoding rules work for all $q \in (0,1)$. However, as we will elaborate in Section A.1 that, the first rule requires fewer tests for $(1-\varepsilon)$-reliable recovery when $q \in (0, 1/2]$, whereas the second rule requires fewer

[3] Due to the symmetry of randomness in the defective set $\mathcal{D}$ this value is independent of the index value i, hence in our notation we do not index the notation for these probabilities with i.

tests for $(1-\varepsilon)$-reliable recovery when $q \in (1/2, 1)$. Hence we use decoding rule 1 if $q \leq \frac{1}{2}$, and decoding rule 2 otherwise.

Decoding Rule 1: This rule uses the tests that each item participates in. Denote by m_i the number of tests that item i participates in, and denote by m_i^+ (respectively m_i^-) the number of tests with positive (respectively negative) outcomes within these m_i tests. We then classify i as follows:

$$i = \begin{cases} \text{non-defective} & \text{if } \frac{m_i^+}{m_i} \leq \frac{P(-,q)+P(+,q)}{2}, \\ \text{defective} & \text{if } \frac{m_i^+}{m_i} > \frac{P(-,q)+P(+,q)}{2}. \end{cases} \quad (16)$$

Decoding Rule 2: This rule uses the tests that *exclude* the item. Let s_i denote the number of tests that item i is excluded from, and let s_i^+ (respectively s_i^-) denote the number of tests with positive (respectively negative) outcomes within these s_i tests. We then classify i as follows:

$$i = \begin{cases} \text{non-defective} & \text{if } \frac{s_i^+}{s_i} > \frac{Q(-,q)+Q(+,q)}{2}, \\ \text{defective} & \text{if } \frac{s_i^+}{s_i} \leq \frac{Q(-,q)+Q(+,q)}{2}. \end{cases} \quad (17)$$

4 MAIN RESULTS

4.1 Achievability/Upper bound

Before stating our achievability, it is useful to define the "sensitivity parameter" $H(f)$ of a given monotone test function $f(\cdot)$. This sensitivity parameter, in a certain manner, measures the "fastest rate of change" of $f(\cdot)$, maximized over all intervals $[L, U] \subseteq [0, d]$.

Definition 8. *Sensitivity parameter: Given a monotone test function $f(\cdot)$, its sensitivity parameter $H(f)$ is defined as*

$$H(f) := \min_{0 \leq L < U \leq d} \left(\frac{1}{\beta} \times \frac{U-L}{f(U)-f(L)} \right)^2, \text{ where} \quad (18)$$
$$\beta := \min \left\{ U-L, \sqrt{L+1}, \sqrt{d-U+1} \right\}.$$

Here the $\frac{U-L}{f(U)-f(L)}$ term bounds the inverse slope of the test function $f(\cdot)$ in the region $[L, U]$, and β is an amortization factor that, at a high level, relates to the standard deviation of $f(\cdot)$ w.r.t. a certain binomial distribution in that interval.

Further, for any monotone test function $f(\cdot)$, Lemma 2 below (whose proof may be found in Appendix B) bounds the sensitivity parameter $H(f)$ of $f(\cdot)$, and asserts $H(f) \in \mathcal{O}\left(d^{1+o(1)}\right)$.

Lemma 2. *For any monotone test function $f(\cdot)$ and $d \geq 2$, we have*[4]

$$\frac{1}{(f(d)-f(0))^2} \leq H(f) \leq \frac{16d}{(f(d)-f(0))^2} (\log\log d + 2)^2. \quad (19)$$

While the bounds in Lemma 2 hold universally for any monotone $f(\cdot)$, the upper bound in (19) may be unduly pessimistic. For instance, for any $w \in [0, 1]$, consider the natural class of test functions for which the slope is $\frac{1}{d^w}$. Namely:

Example 1. *Let the test function $f(\cdot)$ be defined as*

$$f(x) = \begin{cases} \frac{x}{d^w} & x \in [0, d^w] \cap \mathbb{Z}^+, \\ 1 & \text{otherwise}, \end{cases} \quad (20)$$

For such $f(\cdot)$, one can see that $H(f) \in \mathcal{O}(d^w)$, for instance by choosing $L = \left\lfloor \frac{d^w}{3} \right\rfloor$ and $U = \left\lceil \frac{2d^w}{3} \right\rceil$.

With the definition of $H(f)$ and the corresponding bounds at hand, we can now state our main achievability result, including the computation of the test design parameter q^* in (15).

Theorem 1. *The non-adaptive test design and decoding outlined in Section 3 has the following performance:*

a) The probability of error is at most ε;

b) The number of tests T satisfies

$$T \leq 376017 P_{min}(q^*) H(f) d \log\left(\frac{2n}{\varepsilon}\right) + 1 \quad (21)$$
$$\leq 376017 H(f) d \log\left(\frac{2n}{\varepsilon}\right) + 1; \quad (22)$$

c) The test design parameter q^* in (15) can be efficiently characterized in $\mathcal{O}(d^7 \log^2(d))$ time;

d) The computation complexity of decoding is $\mathcal{O}\left(nH(f)d\log\left(\frac{n}{\varepsilon}\right)\right)$.

Proofs of each part of Theorem 1 may be found in consecutive sub-sections in Appendix A. The q^* is found to some extend in a brute-force manner, and the computation can potentially be improved.

Remark 1. *Due to Lemma 2, Theorem 1 guarantees that our scheme requires at most $\mathcal{O}\left(d^{2+o(1)} \log\left(\frac{n}{\varepsilon}\right)\right)$ tests for $(1-\varepsilon)$-reliable recovery. However, as noted in Example 1, the universal bound on $H(f)$ presented in Lemma 2 may be loose – for the class of test functions in Example 1, the number of tests required by our scheme actually scales as $\mathcal{O}\left(d^{1+w} \log\left(\frac{n}{\varepsilon}\right)\right)$.*

[4]For $d = 1$, we directly have $H(f) = \frac{1}{(f(d)-f(0))^2}$ by definition.

4.2 Converse/Lower bound

To complement our achievability result in Theorem 1, we also present an information-theoretic lower bound on the number of tests required by any non-adaptive group testing algorithm that has a probability of error of at most ε. To this end, it is useful to define the "concentration parameter" $h(f)$ of a given monotone function $f(\cdot)$. This definition parallels (but is distinct from) the definition of $H(f)$ in the previous Section 4.1) – it may be thought of as a measure of concentration of $f(\cdot)$ under hypergeometric sampling. Note that for a pool size of χ, the quantities $\mu(\chi)$ and $\sigma^2(\chi)$, defined respectively as

$$\begin{aligned}\mu(\chi) &\coloneqq \sum_{a=0}^{d} \frac{\binom{d}{a}\binom{n-d}{\chi-a}}{\binom{n}{\chi}} f(a),\\ \sigma^2(\chi) &\coloneqq \sum_{a=0}^{d} \frac{\binom{d}{a}\binom{n-d}{\chi-a}}{\binom{n}{\chi}} (f(a)-\mu(\chi))^2,\end{aligned} \tag{23}$$

correspond respectively to (the hypergeometrically weighted) mean and variance of the test function $f(\cdot)$, given that the pool-size is χ. That is, conditioned on choosing a random pool of size χ, these are the mean and variance of the test positivity probability.

Remark 2. *We have $f(0) \le \mu(\chi) \le f(d)$ by the monotonicity of $f(\cdot)$.*

Definition 9. *For test function $f(\cdot)$ and $\chi \in \{1,\dots,n-1\}$, we define the concentration parameter $h(f)$ of $f(\cdot)$ as*

$$h(f) \coloneqq \min_{\chi\in\{1,\dots,n-1\}} \frac{\mu(\chi)\left(1-\mu(\chi)\right)}{\sigma^2(\chi)}. \tag{24}$$

We are now in a position to state our main converse/impossibility result (whose proof can be found in Appendix J) as follows:

Theorem 2. *For any non-adaptive group testing algorithm that ensures a reconstruction error of at most ε, the number of tests T must satisfy*

$$T \ge \frac{1}{\log e} h(f) \left((1-\varepsilon)\log\binom{n}{d} - 1 \right). \tag{25}$$

Remark 3. *Note also that for any test function $h(f) \ge 1$. This is because $f^2(a) \le f(a) \le 1$ for all a, so using the identity $(f(a)-\mu(\chi))^2 = f^2(a)+\mu^2(\chi)-2f(a)\mu(\chi)$, we have that for all χ,*

$$\sigma^2(\chi) \le \sum_{a=0}^{d} \frac{\binom{d}{a}\binom{n-d}{\chi-a}}{\binom{n}{\chi}} f(a) - \mu^2(\chi) = \mu(\chi)\left(1-\mu(\chi)\right).$$

Hence the lower bound in (25) scales as $\Omega\left(\log\binom{n}{d}\right)$, which in turns scales as $\Omega\left(d\log\left(\frac{n}{d}\right)\right)$. However, as noted in Section 4.3 (see Corollary 1.c) below), the bound $h(f) \ge 1$ is in general loose – there exist test functions for which $h(f)$ can be as large as $\Omega(d)$. Hence, due to the $h(f)$ term in (25), this impossibility result may scale as $\Omega\left(d^2\log\left(\frac{n}{d}\right)\right)$, which is a strict tightening of the information-theoretic lower bounds $\Omega\left(d\log\left(\frac{n}{d}\right)\right)$ existing in the literature (see for instance [Chan et al., 2014]).

4.3 Comparison between upper and lower bounds

The ratio between the upper bound in (21) and the lower bound in (25) scales order-wise as $\frac{H(f)}{h(f)}$. Corollary 1 below (whose proof may be found in Appendix N) shows that for a variety of test functions in the literature $\frac{H(f)}{h(f)} \in \Theta(1)$. Thus our bounds are order-wise tight for those test functions.

Corollary 1. *In the sparse regime $d = n^\theta, 0 \le \theta < 1$:*

a) For the classical group testing measurement function $f(\cdot)$ given in (1), both the $H(f)$ and $h(f)$ functionals equal 1, enabling us to recover the well-known fact (see for instance [Chan et al., 2014]) that the sample-complexity of classical group-testing is $\Theta(d\log n)$

b) For the threshold test function, i.e., for some $\ell \in \{0,\dots,d-1\}$,

$$f(x) = \begin{cases} 0 & \text{if } x \le \ell, \\ 1 & \text{if } x > \ell, \end{cases} \tag{26}$$

both the upper bound on the number of tests required for $(1-\varepsilon)$-reliable recovery in Theorem 1 and the corresponding lower bound in Theorem 2 scale as $\Theta(d\log n)$. To the best of our knowledge this is the first order-wise tight characterization of the optimal sample-complexity of threshold group testing.

c) For the "linear" test function, i.e.,

$$f(x) = \frac{x}{d}, \quad x \in \{0,\dots,d\}, \tag{27}$$

the upper bound on the number of tests required for $(1-\varepsilon)$-reliable recovery in Theorem 1 matches (order-wise) the lower bound in Theorem 2, both scaling as $\Theta\left(d^2\log n\right)$. Hence, by Lemma 2, this test function is essentially extremal in its sample complexity.

For general (near-noiseless) monotone test functions $f(\cdot)$, while we are not able to show that the sample-complexities in Theorems 1 and 2 match up to constant factors, we nonetheless show in Theorem 3 below

(for which a proof may be found in Appendix L) that they match up to a $\mathcal{O}\left(\frac{P_{min}(q^*)}{\mu(\chi^*)(1-\mu(\chi^*))}\right)$ factor. Here χ^* denotes an optimal solution to (24), i.e.,

$$\chi^* \coloneqq \operatorname*{argmin}_{\chi\in\{1,\ldots,n-1\}} \frac{\mu(\chi)(1-\mu(\chi))}{\sigma^2(\chi)}. \tag{28}$$

Theorem 3. *In the sparse regime $d = n^\theta, 0 \leq \theta < 1$, the number of tests required in Theorem 1 is no more than a $\mathcal{O}\left(\frac{P_{min}(q^*)}{\mu(\chi^*)(1-\mu(\chi^*))}\right)$ factor larger than the lower bound presented in Theorem 2. In particular, the number of tests required in Theorem 1 is never more than an $\mathcal{O}\left(d^{1+o(1)}\right)$ factor larger than the information-theoretic lower bound in Theorem 2.*

Using Theorem 3, we show in Corollary 2 below (whose proof is in Appendix O) that for *any* noisy test function our non-adaptive scheme is indeed order-wise optimal.

Corollary 2. *In the sparse regime $d = n^\theta, 0 \leq \theta < 1$, the upper and lower bounds are order-wise tight for all noisy test functions.*

Indeed, we present the following conjecture, whose positive resolution would resolve the order-wise sample-complexity for *any* monotone test function.

Conjecture 1. *We conjecture that for any monotone test function $f(\cdot)$, $\frac{\min_{q\in(0,1)}\Gamma(q)}{h(f)d\log n} \in \Theta(1)$.*

5 INTUITION AND PROOF SKETCHES

We give here some high-level intuition behind our main results and provide corresponding proof sketches. The detailed proofs and simulations may be found in the Appendices in the Supplementary Materials. For readers' convenience, we also provide a road-map of the intermediate results leading to our main results in Figs. 1 and 3 in the Supplementary Materials.

A. Achievability/Theorem 1: As noted in Section 3 we use a Bernoulli test design, where each item participates in a test in an i.i.d. manner with probability q. Both of our two decoding rules, specified in (16) and (17), proceed by classifying each item $i \in \{1,\ldots,n\}$ as defective or non-defective independently of any other item.

In particular, Decoding Rule 1, specified in (16), proceeds as follows. For any test including item i, we denote by $P(-,q)$ the probability of having a positive outcome is if item i is non-defective and by $P(+,q)$ if item i is defective. Due to the monotonicity of our test function $f(\cdot)$, $P(+,q) > P(-,q)$. By the law of large numbers, when item i participates in a large enough number of tests, the fraction of positive-outcome tests converges to either $P(-,q)$ or $P(+,q)$ depending on whether the item is non-defective or defective respectively. So decoding rule (16) proceeds by classifying i as defective or not by checking that the fraction of positive test outcomes is closer to $P(+,q)$ or $P(-,q)$. Analogously, Decoding Rule 2 specified in (17) is similar, but now makes use of the tests *not* including item i, with $Q(-,q)$ denoting the probability of having a positive outcome if item i is non-defective, and $Q(+,q)$ denoting the corresponding probability if item i is defective. As above, due to the monotoncity of $f(\cdot)$, $Q(-,q) > Q(+,q)$. The fraction of positive-outcome tests converges to $Q(-,q)$ and $Q(+,q)$, respectively, and i is classified according to which fraction is closer.

We have two different decoding rules since, as shown in Fig. 2 when $q \in (0,1/2]$, the first rule requires fewer tests than the second does for $(1-\varepsilon)$-reliable recovery, with the situation reversed in $q \in (1/2,1)$.

• *Lemma 2 – $H(f)$:* Lemma 2, whose proof can be found in Appendix B, provides a universal bound on the sensitivity parameter for any monotone $f(\cdot)$.

In order to simplify the $\min\left\{U-L, \sqrt{L+1}, \sqrt{d-U+1}\right\}$ term, we first split our analysis into two cases, corresponding to the scenarios $f(\lceil d/2\rceil) \geq (f(0)+f(d))/2$ and $f(\lceil d/2\rceil) < (f(0)+f(d))/2$ – we choose L and U from $[0,d/2]$ or $(d/2,d]$ accordingly. This enables us to argue that only one of $\sqrt{L+1}$ and $\sqrt{d-U+1}$ is active in the $\min\left\{U-L, \sqrt{L+1}, \sqrt{d-U+1}\right\}$ term, simplifying our argumentation. We focus on the first case – the proof of the second case is analogous. Considering any $\upsilon \in (0,1]$ and $k = \lceil \log(1/\upsilon)+1\rceil$, we construct a sequence $\{S_i\}$ with $k+1$ elements such that $\frac{S_{i+1}^2}{S_i+1} \leq 2d^{1+\upsilon}$ for all i. We then argue that there exists two adjacent elements S_ℓ and $S_{\ell+1}$ such that $f(S_{\ell+1}) - f(S_\ell) \geq (f(d)-f(0))/2k$. Finally, using the definition of $H(f)$ in (18) with $L = S_\ell$ and $U = S_{\ell+1}$ and letting $\upsilon = 1/\log d$, one can prove Lemma 2.

• *Theorem 1.a) – Probability of error:* We first collect various inequalities relating quantities such as $P(+,q)$, $P(-,q)$, $Q(+,q)$, $Q(-,q)$, etc., in Lemma 1, whose proof may be found in Appendix C. With these relations at hand, the probability of error of these two decoding rules can be analyzed via standard concentration inequalities, collected in Appendix D.

In particular Propositions 1 and 2 respectively posit that Decoding Rules 1 and 2 allow for $(1-\varepsilon)$-reliable recovery of $\mathcal{D}$ via $\frac{13}{6q}m$ and $\frac{13}{6(1-q)}s$ tests respectively. Each of Propositions 1 and 2 proceeds in two steps. First, Lemmas 3 and 5 use the Chernoff bound to show that the probability that an arbitrary item participates in less than m tests or in more than $T-s$ tests is

each no larger than $\frac{\varepsilon}{2n}$. Second, conditioning on the event that each item participates in $[m, T-s]$ tests, Lemmas 4 and 6 again use the Chernoff bound to show that the probability of misidentification (either false alarm or missed detection) is no larger than $\frac{\varepsilon}{2n}$. These error events are then combined via a union bound.

• *Theorem 1.b) – Bound on T:* The number of tests chosen in (13) as $\lceil \Gamma(q) \rceil$ suffices to ensure $(1-\varepsilon)$-reliable recovery, but it is not immediately apparent how this quantity relates to the bound claimed in (21). As a simplifying first step, as noted in the text surrounding (14), instead of bounding $\Gamma(q)$ directly, we bound instead $\hat{\Gamma}(q) = \frac{\Gamma(q)}{P_{\min}(q)}$ – since $P_{\min}(q) \leq 1$ (see Lemma 1) this suffices to give an upper bound on T allowing $(1-\varepsilon)$-reliable recovery.

Perhaps the most technically involved part of our work focuses on providing a reasonably tight upper bound – as accomplished in Proposition 3 – on $\hat{\Gamma}(q^*)$ in terms of the sensitivity parameter $H(f)$ defined in Definition 8.

Before discussing Proposition 3 in the context of general monotone functions, consider first the example of the threshold group-testing function described in (26) (corresponding to negative test outcomes if there are at most ℓ defectives in a pool). Intuitively speaking, for accurately classifying each item, we should choose some q such that the gap $\Delta(q) = P(+,q) - P(-,q)$ is "large" (bounded away from 0). This can also be seen from (14), wherein to minimize $\hat{\Gamma}(q)$, we would like $\Delta(q)$ to be as large as possible. For the threshold group testing scenario, if we choose $q = \ell/d$, then on the one hand if an item i is non-defective the expected number defectives in a pool is ℓ; and on the other hand if item i is defective the expected number of defectives is $\frac{\ell}{d}(d-1)+1 \approx \ell+1$, and hence the gap $\Delta(q)$ in test positivity is about as large as can be hoped for – one can see that choices of q signficantly larger or smaller than this would result in a smaller gap $\Delta(q)$.

For a general test function $f(\cdot)$, the gap $\Delta(q)$ can be regarded as the "binomially-weighted mean of the increment" of $f(\cdot)$ (see (53) for the precise expression). To make $\Delta(q)$ larger, we should attempt to assign a larger weight to a carefully chosen region "large-increment-interval" $[L, U]$ where $f(\cdot)$ exhibits a large increment.

More precisely, for general test functions $f(\cdot)$ our pathway to proving Proposition 3 relies on bounding the integral of $\Delta(q)$ from L/d to U/d, which, by the mean value theorem, gives a bound on $\Delta(q_0)$ for some $q_0 \in [L/d, U/d]$. To this end in Lemmas 14 and 15 we provide a delicate saddle-point-approximation style bound for $\int_{L/d}^{U/d} q^j (1-q)^{d-j}\, \mathrm{d}q$. This together with Stirling's approximation summarized in Lemma 13 results in Lemma 9, which almost gets us to Proposition 3, except for two issues. Firstly, there is a $\frac{(d-L')U'}{(d-U')L'}$ multiplicative term that appears in Lemma 9 but not in Proposition 3. Towards this end, we divide $[L', U')$ into suitably small intervals $[\lambda_i, \lambda_{i+1})$, $i \in \{0, \ldots, \tau-1\}$. The criteria are that i) Lemma 10 – each $\lambda_{i+1} - \lambda_i$ should larger than $\min\{U'-L', \sqrt{L'}, \sqrt{U'-L'}\}$ appeared in the denominator of Lemma 9; ii) Lemma 11 – each $\lambda_{i+1} - \lambda_i$ should also small enough so that $\frac{(d-\lambda_i)\lambda_{i+1}}{(d-\lambda_{i+1})\lambda_i}$ can be bounded from above by a constant. By substituting $L' = \lambda_\ell$ and $U' = \lambda_{\ell+1}$ for some specific ℓ identified by the mean value theorem in Lemma 12, allow us to get Proposition 4. Secondly, the "boundary points", i.e., $L = 0$ or $U = d$, are handled separately in Proposition 5. Proposition 3 is then proved by unifying Propositions 4 and 5.

• *Theorem 1.c) – Complexity of approximating q^*:* A critical part of our test-design and decoding algorithms is an appropriate choice of $q \in (0,1)$. We proceed as follows: we uniformly quantize the interval $(0,1)$ into $\Theta(d^4)$ intervals and calculate the corresponding $\Gamma(q)$ for each q, and then set q to equal the value $\hat{q}$ that minimizes $\Gamma(q)$. We then prove that choosing $q = \hat{q}$ results in our scheme having similar performance to using the value $q = q^*$, i.e., $\Gamma(\hat{q}) = \Theta(\Gamma(q^*))$.

To this end, in Lemma 7 we first show that q^* can never be either "too small" or "too large" – i.e., $q^* \in \left(\frac{1}{376017d^3}, 1 - \frac{1}{376017d^3}\right)$. Next, we prove in Lemma 8 that for all $\hat{q}^*$ that is close enough to q^*, i.e., $|\hat{q}^* - q^*| \leq \frac{1}{376017d^4}$, we have $\Gamma(\hat{q}^*) \leq 64e^2\Gamma(q^*)$.

• *Theorem 1.d) – Complexity of decoding:* Since our decoder only needs to count the number of tests and tests with positive outcomes that one item is included in (respectively not included in) and check the ratio via Decoding Rule 1 in (16) (respectively Decoding Rule 2 in (17)), the computational complexity of decoding is $\mathcal{O}(nT) = \mathcal{O}\left(nH(f)d\log\left(\frac{n}{\varepsilon}\right)\right)$.

B. Converse/Theorem 2: The proof of our converse argument, which may be found in Appendix J, proceeds as follows. Let $\boldsymbol{X}$ be the input vector and $\boldsymbol{Y}$ be the outcome vector. We decompose the entropy $H(\boldsymbol{X})$ into the conditional entropy term $H(\boldsymbol{X}|\boldsymbol{Y})$ and the mutual information $I(\boldsymbol{X};\boldsymbol{Y})$. By the assumption that $\mathcal{D}$ is uniformly distributed over all $\binom{n}{d}$ size-d subsets of $\{1,\ldots,n\}$, we have $H(\boldsymbol{X}) = \log\binom{n}{d}$. Using Fano's inequality, $H(\boldsymbol{X}|\boldsymbol{Y})$ can be bounded in terms of the error probability ε. Following techniques similar to the channel coding literature (see for instance [Yeung, 2008, Sec. 7.3]), one can upper bound $I(\boldsymbol{X};\boldsymbol{Y}) \leq \sum_{i=1}^{T}[H(Y_i) - H(Y_i|Z_i)]$, where Z_i denotes the number of defectives in the i-th pool. One salient feature of generalized group testing is that the test outcome is no longer deterministic when given the number of de-

fectives in the test pool. That is, $H(Y_i|Z_i) > 0$ and is not negligible. Next (by resorting to an inequality on the $\ln(\cdot)$ function presented in Lemma 17) in Lemma 16 we bound each $H(Y_i) - H(Y_i|Z_i) \leq \frac{\sigma^2(\chi_i)}{\mu(\chi_i)(1-\mu(\chi_i))}$, where χ_i is the size of the i-th pool, $\mu(\chi_i)$ and $\sigma^2(\chi_i)$ are, respectively, the mean and variance of being positive. Finally, optimizing the pool-size parameter χ, give the lower bound.

C. Tightness/Theorem 3: To prove the tightness of our achievability and converse in Theorem 3 (whose proof is given in Appendix L), we show there exists a pair of $(\hat{L}, \hat{U})$ such that $\frac{1}{\min\left\{\hat{U}-\hat{L}, \sqrt{\hat{L}+1}, \sqrt{d-\hat{U}+1}\right\}} \times \frac{\hat{U}-\hat{L}}{f(\hat{U})-f(\hat{L})} = \mathcal{O}\left(\frac{1}{\sigma(\chi^*)}\right)$. From the definition of χ^* in (28), we know that $\sigma^2(\chi^*)$ is "relatively large". This implies that $f(\cdot)$ increases rapidly in the region adjacent to $\chi^* \frac{d}{n}$ (which quantity equals the expected number of defectives in the test pool). Thus it is reasonable to choose $\chi^* \frac{d}{n}$ as one of the pair $(\hat{L}, \hat{U})$. The existence of the other one is shown in a proof by contradiction in Lemma 18, making use of the mean and variance formulae for hypergeometric distributions. Based on Lemma 18, in Proposition 6 we deal with integrality issues and specify $(\hat{L}, \hat{U})$. Finally, invoking Proposition 3 with this pair of $(\hat{L}, \hat{U})$, one can prove Theorem 3.

Acknowledgements

The authors wish to acknowledge useful discussions with Profs. Oliver Johnson and Jonathan Scarlett. We would also like to thank the anonymous reviewers for many helpful suggestions which greatly improved the quality of this work.

References

[Atia and Saligrama, 2012] Atia, G. K. and Saligrama, V. (2012). Boolean compressed sensing and noisy group testing. *IEEE Trans. Inf. Theory*, 58(3):1880–1901.

[Berger et al., 1984] Berger, T., Mehravari, N., Towsley, D., and Wolf, J. (1984). Random multiple-access communication and group testing. *IEEE Transactions on Communications*, 32(7):769–779.

[Bruijn, 1981] Bruijn, N. G. D. (1981). *Asymptotic Methods Analysis*. Courier Corporation, Chelmsford, MA, USA.

[Bshouty et al., 2018] Bshouty, N. H., Bshouty-Hurani, V. E., Haddad, G., Hashem, T., Khoury, F., and Sharafy, O. (2018). Adaptive group testing algorithms to estimate the number of defectives. In *Algorithmic Learning Theory*, pages 93–110. PMLR.

[Bui et al., 2020] Bui, T. V., Cheraghchi, M., and Echizen, I. (2020). Improved non-adaptive algorithms for threshold group testing with a gap. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, pages 1414–1419, LA, CA, USA.

[Bui et al., 2019] Bui, T. V., Kuribayashi, M., Cheraghchi, M., and Echizen, I. (2019). Efficiently decodable non-adaptive threshold group testing. *IEEE Trans. Inf. Theory*, 65(9):5519–5528.

[Chan et al., 2013] Chan, C. L., Cai, S., Bakshi, M., Jaggi, S., and Saligrama, V. (2013). Stochastic threshold group testing. In *Proc. IEEE Inf. Theory Workshop (ITW)*, pages 1–5, Sevilla, Spain.

[Chan et al., 2014] Chan, C. L., Jaggi, S., Saligrama, V., and Agnihotri, S. (2014). Non-adaptive group testing: Explicit bounds and novel algorithms. *IEEE Trans. Inf. Theory*, 60(5):3019–3035.

[Chen and Fu, 2009] Chen, H.-B. and Fu, H.-L. (2009). Nonadaptive algorithms for threshold group testing. *Discrete Applied Mathematics*, 157(7):1581–1585.

[Cheraghchi, 2010] Cheraghchi, M. (2010). Improved constructions for non-adaptive threshold group testing. In *International Colloquium on Automata, Languages, and Programming*, pages 552–564. Springer.

[Chernoff et al., 1952] Chernoff, H. et al. (1952). A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *The Annals of Mathematical Statistics*, 23(4):493–507.

[Damaschke, 2006] Damaschke, P. (2006). Threshold group testing. In *General theory of information transfer and combinatorics*, pages 707–718. Springer.

[Damaschke and Muhammad, 2010] Damaschke, P. and Muhammad, A. S. (2010). Competitive group testing and learning hidden vertex covers with minimum adaptivity. *Discrete Mathematics, Algorithms and Applications*, 2(03):291–311.

[De Marco et al., 2020] De Marco, G., Jurdziński, T., Kowalski, D. R., Różański, M., and Stachowiak, G. (2020). Subquadratic non-adaptive threshold group testing. *Journal of Computer and System Sciences*, 111:42–56.

[Dorfman, 1943] Dorfman, R. (1943). The detection of defective members of large populations. *The Annals of Mathematical Statistics*, 14(4):436–440.

[Du et al., 2000] Du, D., Hwang, F. K., and Hwang, F. (2000). *Combinatorial group testing and its applications*, volume 12. World Scientific.

[Falahatgar et al., 2016] Falahatgar, M., Jafarpour, A., Orlitsky, A., Pichapati, V., and Suresh, A. T. (2016). Estimating the number of defectives with group testing. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 1376–1380. IEEE.

[Gollier and Gossner, 2020] Gollier, C. and Gossner, O. (2020). Group testing against Covid-19. *Covid Economics*, 2.

[Macula and Popyack, 2004] Macula, A. J. and Popyack, L. J. (2004). A group testing method for finding patterns in data. *Discrete applied mathematics*, 144(1-2):149–157.

[Ngo and Du, 2000] Ngo, H. Q. and Du, D.-Z. (2000). A survey on combinatorial group testing algorithms with applications to DNA library screening. *Discrete mathematical problems with medical applications*, 55:171–182.

[Reisizadeh et al., 2018] Reisizadeh, A., Abdalla, P., and Pedarsani, R. (2018). Sub-linear time stochastic threshold group testing via sparse-graph codes. In *Proc. IEEE Inf. Theory Workshop (ITW)*, pages 1–5, Guangzhou, China.

[Scarlett and Cevher, 2018] Scarlett, J. and Cevher, V. (2018). Near-optimal noisy group testing via separate decoding of items. *IEEE Journal of Selected Topics in Signal Processing*, 12(5):902–915.

[Scarlett and Johnson, 2020] Scarlett, J. and Johnson, O. (2020). Noisy non-adaptive group testing: A (near-) definite defectives approach. *IEEE Transactions on Information Theory*, 66(6):3775–3797.

[Wolf, 1985] Wolf, J. K. (1985). Born again group testing: Multiaccess communications. *IEEE Trans. Inf. Theory*, 31(2):185–191.

[Yeung, 2008] Yeung, R. W. (2008). *Information Theory and Network Coding*. Springer, New York, NY, USA.

[Zenios and Wein, 1998] Zenios, S. A. and Wein, L. M. (1998). Pooled testing for hiv prevalence estimation: exploiting the dilution effect. *Statistics in Medicine*, 17(13):1447–1467.

Supplementary Material: Generalized Group Testing

All citations below are to the reference list in the main document.

A Proof of Theorem 1

A.1 Proof of Theorem 1-a)

First, we separately discuss the performance of the decoding rules proposed in (16) and (17).

A.1.1 Performance of Decoding Rule 1 in (16)

Proposition 1. *Suppose that the decoding rule used is* (16)*. Then we show that the probability of error is at most ε if*

$$T \geq \Gamma_1(q) := \frac{13}{6q} m. \tag{29}$$

This is proved in two steps. First, we compute the probability that an arbitrary item participates in less than m tests, which can be made sufficiently small. Second, assuming that each item participates in at least m tests, we compute the probability of misidentification, which again can be made sufficiently small. Formally, we have the following two lemmas, whose proofs are relegated to Appendices D.1 and D.2, respectively.

Lemma 3. *With probability at least $1 - \frac{\varepsilon}{2}$ over the test design, each item $i \in \mathcal{N}$ participates in at least m tests.*

Lemma 4. *Conditioning on the event that each item participates in at least m tests, with probability at least $1 - \frac{\varepsilon}{2}$ over the test design, all items are correctly identified using* (16)*.*

Upon combining Lemmas 3 and 4, via the union bound, the probability that all items are correctly identified is bounded from below by $1 - \varepsilon$, which proves Proposition 1.

A.1.2 Performance of Decoding Rule 2 in (17)

Proposition 2. *Suppose that the decoding rule used is* (17)*. Then we show that the probability of error is at most ε if*

$$T \geq \Gamma_2(q) := \frac{13}{6(1-q)} s. \tag{30}$$

Similarly to Proposition 1, this is established by proving the following two lemmas whose proofs can be found in Appendices D.3 and D.4.

Lemma 5. *With probability at least $1 - \frac{\varepsilon}{2}$ over the test design, each item $i \in \mathcal{N}$ participates in at most $T - s$ tests.*

Lemma 6. *Conditioning on the event that each item participates in at most $T - s$ tests, with probability at least $1 - \frac{\varepsilon}{2}$ over the test design, all items are correctly identified using* (17)*.*

Next, since both decoding rules are applicable to all $q \in (0, 1)$, we shall compare the bound given in (29) and (30) and choose the more efficient one, i.e., the one that has a smaller lower bound on T. Using (9) along with

Parameters in the Problem Formulation	
$\mathcal{N}$	The set of all items.
n	The total number of items, and $n = \lvert\mathcal{N}\rvert$.
$\mathcal{D}$	The unknown subset of defective items, distributed uniformly at random over all $\binom{n}{d}$ sets of size d.
d	The number of defective items, with $d = \lvert\mathcal{D}\rvert$.
$f(\cdot)$	The *test function*, a monotone function indicating the probability $f(x)$ that a test pool with x defectives has a positive test outcome.
ε	The pre-specified upper bound on the probability of incorrect reconstruction of $\mathcal{D}$.
T	The number of tests.

Test Design and Decoding Parameters	
$\boldsymbol{M}$	The $T \times n$ binary test matrix: $M_{ji} = 1$ if item i is in test j; $M_{ji} = 0$ otherwise.
q	Probability with which each element in $\boldsymbol{M}$ is chosen as 1 in an i.i.d. manner.
$P(-, q)$	The probability that a test containing i has a positive outcome when i is non-defective, as defined in (4).
$P(+, q)$	The probability that a test containing i has a positive outcome when i is defective, as defined in (4).
$Q(-, q)$	The probability that a test excluding i has a positive outcome when i is non-defective, as defined in (5).
$Q(+, q)$	The probability that a test excluding i has a positive outcome when i is defective, as defined in (5).
$\Delta(q)$,$\nabla(q)$	The difference of test-positivity probability conditioned on item i being defective or not, as defined in (6).
$P_{\min}(q)$	Minimal test sensitivity, as defined in (7).
m, s	Test participation parameter such that one item is included in $[m, T-s]$ tests with high probability, as defined in (11) and (12).
$\Gamma(q)$	The number of tests required in our algorithm, as defined in (13).
$\hat{\Gamma}(q)$	As defined in (14), an upper bound on $\Gamma(q)$ that is easier to analyze and optimize than $\Gamma(q)$.
q^*	The parameter that minimizes $\hat{\Gamma}(q)$, as defined in (15) – it can be efficiently approximated by Theorem 1-c).

Parameters in the Achievability/Theorem 1	
$H(f)$	The sensitivity parameter (as defined in (18)) which helps bound T from above in Theorem 1-b) and is bounded in Lemma 2.
$\Gamma_1(q)$	The number of tests required by Decoding Rule 1 in (16), as defined in (29).
$\Gamma_2(q)$	The number of tests required by Decoding Rule 2 in (17), as defined in (30).
$\hat{q}^*$	Any q that is "close enough" to q^* – the corresponding $\Gamma(q)$ can be bounded by $\Theta(\Gamma(q^*))$ in Lemma 8.
$\hat{q}$	An approximation to q^*.
α	A useful parameter w.r.t. L' and U' in the saddle-point approximation in Lemma 15, defined as $\frac{1}{2}\min\left\{U'-L', \sqrt{L'}, \sqrt{d-U'}\right\}$.
β	The minimum term in $H(f)$ w.r.t. L and U, as defined in (89).

Parameters in the Converse/Theorem 2	
χ	The pool size.
$\mu(\chi)$,$\sigma^2(\chi)$	The mean and variance of the test positivity probability, given that the pool size is χ.
$h(f)$	The concentration parameter (as defined in (24)) which helps bound T from below in Theorem 2.
χ^*	The pool size that minimizes $(\mu(1-\mu))/\sigma^2$, as defined in (28).
$\boldsymbol{X}$	The length-n binary vector that is a weight d vector representing the locations of the defective set $\mathcal{D}$.
$\boldsymbol{Y}$	The length-T binary vector representing the outcome of each test.
$\boldsymbol{Z}$	The length-T vector representing the number of defectives in each test.
$\hat{\boldsymbol{X}}$	The length-n binary vector representing the estimated locations of the defective set $\mathcal{D}$.

Tightness Parameters/Theorem 3	
ϑ	The expected number of defectives in a test of pool size χ^*, as defined in (167).
$(\hat{L}, \hat{U})$	A pair of parameters for $H(f)$ such that $H(f)$ is upper bounded by $\Theta(1/\sigma^2(\chi^*))$.
η	The closest integer to ϑ, as defined in (168), which is one of the pair $(\hat{L}, \hat{U})$.
κ	The other one of the pair $(\hat{L}, \hat{U})$, whose existence is proved in Lemma 18.
$\gamma(\cdot)$	A parameter similar to β defined as $\gamma(\kappa) := \min\left\{\lvert\kappa-\vartheta\rvert, \sqrt{\kappa+1}, \sqrt{d-\kappa+1}, \sqrt{\vartheta+1}, \sqrt{d-\vartheta+1}\right\}$.

Table 1: Table of frequently used notation.

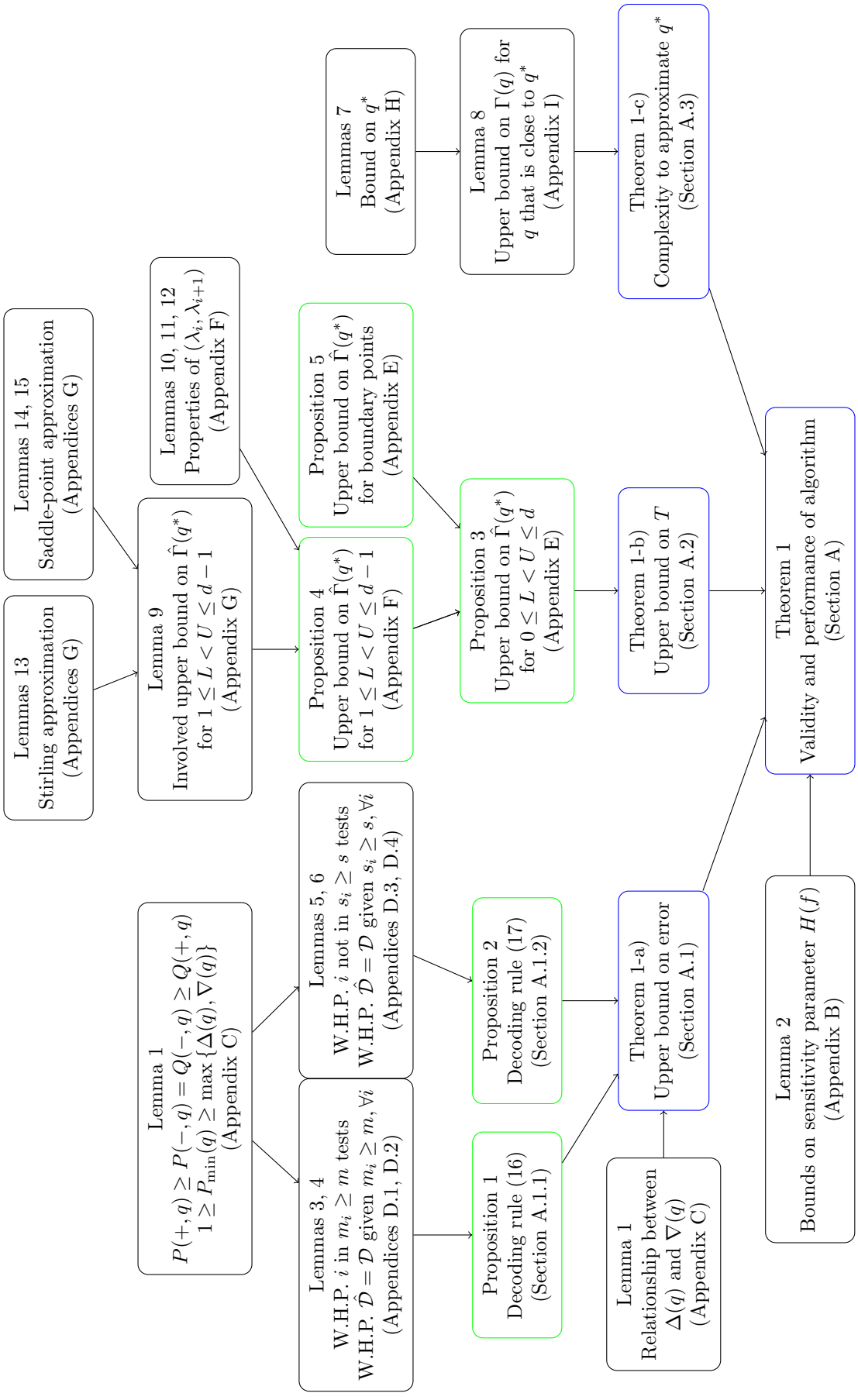


Figure 1: Organization of Propositions, Lemmas, and Theorems for our proof of achievability.

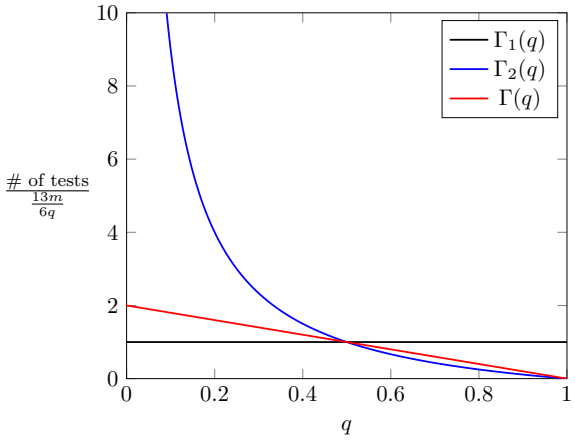


Figure 2: Comparisons of the number of tests defined in (13), (29) and (30). The black line corresponds to the performance of decoding rule (16), the blue line corresponds to that of decoding rule (17), and the red line corresponds to that of our algorithm, which is a combination of the two decoding rules.

(11) and (12), we have

$$\begin{aligned}\frac{13}{6(1-q)}s &= \frac{13}{6(1-q)} \times \frac{8.32P_{\min}(q)}{(\nabla(q))^2}\log\left(\frac{2n}{\varepsilon}\right)\\ &= \frac{1-q}{q}\times\frac{13}{6q}\times\frac{8.32P_{\min}(q)}{(\Delta(q))^2}\log\left(\frac{2n}{\varepsilon}\right)\\ &= \frac{1-q}{q}\times\frac{13}{6q}m,\end{aligned}$$

which suggests that the decoding rule (16) is more efficient when $q \le 1/2$, whereas the decoding rule (17) is more efficient when $q > 1/2$. By leveraging this observation, we argue that the value given in (13) is always an upper bound on the minimum of (29) and (30) for all $q \in (0,1)$, i.e.,

$$\min\{\Gamma_1(q), \Gamma_2(q)\} \le \Gamma(q), \forall q \in (0,1).$$

To see this, when $q \le 1/2$, we have

$$\Gamma_1(q) = \frac{13}{6q}m \le \frac{13(1-q)}{3q}m = \Gamma(q);$$

on the other hand, when $q > 1/2$, we have

$$\Gamma_2(q) = \frac{13}{6(1-q)}s = \frac{13(1-q)}{6q^2}m < \frac{13(1-q)}{3q}m = \Gamma(q).$$

This is also illustrated in Fig. 2, where we plot the values of (13), (29) and (30) as a function of q.

Thus, for $q \le 1/2$ (respectively $q > 1/2$), the number of tests T given in (13) can output the defective set $\mathcal{D}$ with probability of error at most ε using the decoding rule (16) (respectively (17)). This proves Theorem 1-a).

A.2 Proof of Theorem 1-b)

We provide an explicit bound on the value of $\hat{\Gamma}(q)$ defined in (14) for some q, namely Proposition 3 below, whose proof is presented in Appendix E.

Proposition 3. *There exists some $q_0 \in (0,1)$ such that*

$$\hat{\Gamma}(q_0) \le 376017H(f)d\log\left(\frac{2n}{\varepsilon}\right), \tag{31}$$

where $H(f)$ is the "sensitivity parameter" defined in (18).

Combined with (10), (14) and (15), this result yields

$$\begin{aligned} T = \lceil \Gamma(q^*) \rceil &= \left\lceil P_{min}(q^*)\hat{\Gamma}(q^*) \right\rceil \\ &\leq \left\lceil P_{min}(q^*)\hat{\Gamma}(q_0) \right\rceil \\ &\leq 376017 P_{min}(q^*) H(f) d \log\left(\frac{2n}{\varepsilon}\right) + 1 \\ &\leq 376017 H(f) d \log\left(\frac{2n}{\varepsilon}\right) + 1, \end{aligned}$$

which proves Theorem 1-b).

A.3 Proof of Theorem 1-c)

We first show in Lemma 7 below, whose proof is presented in Appendix H, that q^* can never be too small nor too large.

Lemma 7. *We have*

$$q^* \in \left(\frac{1}{376017d^3}, 1 - \frac{1}{376017d^3}\right). \tag{32}$$

Next, we show in Lemma 8 below, whose proof is presented in Appendix I, that for any q that is within $\frac{1}{376017d^4}$ distance of q^*, $\Gamma(q)$ is bounded from above by $64e^2\Gamma(q^*)$. This means that our algorithm still performs well for an estimator of q^* with small error.

Lemma 8. *For any* $\hat{q}^* \in \left[q^* - \frac{1}{376017d^4}, q^* + \frac{1}{376017d^4}\right]$,

$$\Gamma(\hat{q}^*) \leq 64e^2\Gamma(q^*). \tag{33}$$

Armed with Lemma 8, we are now ready to describe our algorithm to selecting q: First, calculate $\Gamma(q)$ for all $q = \frac{j}{376017d^4}$, $j = 1, 2, \cdots, 376017d^4 - 1$. Then choose the one having the smallest $\Gamma(q)$ value, denoted by $\hat{q}$. It follows that $\Gamma(\hat{q}) \leq \Gamma(\hat{q}^*) \leq 64e^2\Gamma(q^*)$. The computational complexity of computing binomial coefficients is $\mathcal{O}(d^2 \log^2 d)$, and the computational complexity of multiplying the binomial coefficient (which comprises of $\mathcal{O}(d \log d)$ bits) with $q^j(1-q)^{d-j}$ (which comprises $\mathcal{O}(d)$ bits), is $\mathcal{O}(d^2 \log d)$. According to (53), the computational complexity of computing $\Delta(q)$ is $\mathcal{O}(d^3 \log^2 d)$. Hence the overall computational complexity of this algorithm is $\mathcal{O}(d^7 \log^2 d)$.

A.4 Proof of Theorem 1-d)

Given the tests and their outcomes, the computational complexity of counting all m_i (respectively s_i) and m_i^+ (respectively s_i^+) is $\mathcal{O}(nT)$. Thus, the complexity of decoding is $\mathcal{O}(nT)$. According to Theorem 1-b), the complexity is at most $\mathcal{O}\left(nH(f)d \log\left(\frac{n}{\varepsilon}\right)\right)$.

B Proof of Lemma 2

Since $\min\left\{U - L, \sqrt{L+1}, \sqrt{d-U+1}\right\} \leq U - L$, it follows from the definition of $H(f)$ in (18) that

$$\begin{aligned} H(f) &\geq \min_{0 \leq L < U \leq d} \left(\frac{1}{U-L} \times \frac{U-L}{f(U) - f(L)}\right)^2 \\ &\geq \frac{1}{(f(d) - f(0))^2} \end{aligned}$$

where the second line follows from the assumption that $f(\cdot)$ is monotonically increasing.

The upper bound is proved by taking into account the "shape" of the monotone test function $f(\cdot)$. For any $\upsilon \in (0, 1]$, define

$$k := \left\lceil \log \frac{1}{\upsilon} + 1 \right\rceil. \tag{34}$$

For notational convenience, let

$$\delta := f(d) - f(0) > 0.$$

There are two possible cases for $f(\cdot)$:

i) $f\left(\left\lceil \frac{d}{2} \right\rceil\right) \geq f(0) + \frac{\delta}{2}$;

ii) $f\left(\left\lceil \frac{d}{2} \right\rceil\right) < f(0) + \frac{\delta}{2}$.

Case i): For $f\left(\left\lceil \frac{d}{2} \right\rceil\right) \geq f(0) + \frac{\delta}{2}$, define a sequence $\{S_i\}$ such that

$$S_i := \begin{cases} \left\lfloor \frac{1}{2} d^{1-2^{-i+1}} \right\rfloor & i = 1, 2, \cdots, k, \\ \left\lceil \frac{1}{2} d \right\rceil & i = k+1. \end{cases} \tag{35}$$

From (35) we have that for $i \in \{1, \cdots, k-1\}$,

$$\frac{S_{i+1}^2}{S_i + 1} \leq \left(\frac{d^{1-2^{-i}}}{2} \right)^2 \frac{2}{d^{1-2^{-i+1}}} = \frac{d}{2}; \tag{36}$$

for $i = k$,

$$\frac{S_{i+1}^2}{S_i + 1} \leq \left(\frac{d+1}{2} \right)^2 \frac{2}{d^{1-2^{-k+1}}} \leq d^2 \frac{2}{d^{1-2^{-k+1}}} \leq 2d^{1+\upsilon}, \tag{37}$$

where the last inequality follows from the definition of k in (34). Combining (36) and (37), we see that

$$\frac{S_{i+1}^2}{S_i + 1} \leq 2d^{1+\upsilon}, \quad \forall i \in \{1, \ldots, k\}. \tag{38}$$

Note that the sequence $\{S_i\}$ is increasing in terms of i. It follows that $S_i + S_{i+1} \leq \left\lfloor \frac{1}{2} d \right\rfloor + \left\lceil \frac{1}{2} d \right\rceil = d$. This implies

$$S_i + 1 \leq d - S_{i+1} + 1, \quad \forall i \in \{1, \ldots, k\}. \tag{39}$$

Then we argue that $\exists \ell \in \{1, \cdots, k\}$ such that

$$f(S_{\ell+1}) - f(S_\ell) \geq \frac{\delta}{2k}, \tag{40}$$

because, if to the contrary that such a ℓ does not exist, then

$$f\left(\left\lceil \frac{d}{2} \right\rceil \right) - f(0) = f(S_{k+1}) - f(S_1) = \sum_{i=1}^{k} \left(f(S_{i+1}) - f(S_i) \right) < k \frac{\delta}{2k} = \frac{\delta}{2}$$

contradicts our assumption that $f\left(\left\lceil \frac{d}{2} \right\rceil\right) \geq f(0) + \frac{\delta}{2}$.

Next, letting $L = S_\ell$ and $U = S_{\ell+1}$, we obtain from (39) that

$$\min\left\{ U - L, \sqrt{L+1}, \sqrt{d - U + 1} \right\} = \min\left\{ S_{\ell+1} - S_\ell, \sqrt{S_\ell + 1} \right\}$$

It then follows from (18) that

$$\begin{aligned} H(f) &\leq \left(\frac{1}{\min\left\{ (S_{\ell+1} - S_\ell), \sqrt{S_\ell + 1} \right\}} \times \frac{S_{\ell+1} - S_\ell}{f(S_{\ell+1}) - f(S_\ell)} \right)^2 \\ &\leq \frac{4k^2}{\delta^2} \times \max\left\{ 1, \frac{(S_{\ell+1} - S_\ell)^2}{S_\ell + 1} \right\} \\ &\leq \frac{4k^2}{\delta^2} \times \max\left\{ 1, \frac{S_{\ell+1}^2}{S_\ell + 1} \right\} \\ &\leq \frac{8k^2}{\delta^2} \times d^{1+\upsilon} \\ &\leq \frac{8}{\delta^2} \left(\log \frac{1}{\upsilon} + 2 \right)^2 d^{1+\upsilon} \end{aligned} \tag{41}$$

where the second line follows from (40); the fourth line follows from (38); the last line follows from the definition of k in (34).

Case ii): For $f\left(\left\lceil \frac{d}{2} \right\rceil\right) < f(0) + \frac{\delta}{2}$, we define

$$\tilde{f}(x) := 1 - f(d-x), \quad x \in \{0, \ldots, d\}. \tag{42}$$

It follows that

$$\tilde{f}\left(\left\lceil \frac{d}{2} \right\rceil\right) - \tilde{f}(0) \geq \tilde{f}\left(\left\lfloor \frac{d}{2} \right\rfloor\right) - \tilde{f}(0) = 1 - f\left(d - \left\lfloor \frac{d}{2} \right\rfloor\right) - (1 - f(d)) = f(d) - f\left(\left\lceil \frac{d}{2} \right\rceil\right) > \frac{\delta}{2}. \tag{43}$$

Consider the sequence $\{S_i\}$ defined in (35). Following the same argument as above, we have that $\exists \ell \in \{1, \cdots, k\}$ such that

$$\tilde{f}(S_{\ell+1}) - \tilde{f}(S_\ell) \geq \frac{\delta}{2k}. \tag{44}$$

Using (44) along with the definition of $\tilde{f}$ in (42) implies

$$f(d - S_\ell) - f(d - S_{\ell+1}) = 1 - \tilde{f}(S_\ell) - (1 - \tilde{f}(S_{\ell+1})) = \tilde{f}(S_{\ell+1}) - \tilde{f}(S_\ell) \geq \frac{\delta}{2k}. \tag{45}$$

Setting $L = d - S_{\ell+1}$ and $U = d - S_\ell$, we have from (39) that

$$\min\left\{U - L, \sqrt{L+1}, \sqrt{d - U + 1}\right\} = \min\left\{S_{\ell+1} - S_\ell, \sqrt{S_\ell + 1}\right\}$$

Similar to the derivation of (41), we have from (18) that

$$\begin{aligned} H(f) &\leq \left(\frac{1}{\min\left\{(S_{\ell+1} - S_\ell), \sqrt{S_\ell + 1}\right\}} \times \frac{d - S_\ell - (d - S_{\ell+1})}{f(d - S_\ell) - f(d - S_{\ell+1})} \right)^2 \\ &\leq \frac{8}{\delta^2} \left(\log \frac{1}{\upsilon} + 2 \right)^2 d^{1+\upsilon} \end{aligned} \tag{46}$$

Summarizing the two cases, we see that for any monotone test function $f(\cdot)$,

$$H(f) \leq \frac{8}{\left(f(d) - f(0)\right)^2} \left(\log \frac{1}{\upsilon} + 2 \right)^2 d^{1+\upsilon}. \tag{47}$$

For $d \geq 2$, upon setting $\upsilon = \frac{1}{\log d}$, we obtain from (47) that

$$H(f) \leq \frac{16}{\left(f(d) - f(0)\right)^2} \left(\log \log d + 2\right)^2 d, \tag{48}$$

which completes the proof.

C Proof of Lemma 1

We expand $P(-, q), P(+, q), Q(-, q)$ and $P(+, q)$ using elementary combinatorial and algebraic identities. Regarding $P(-, q)$, we have that

$$\begin{aligned} P(-, q) &= \sum_{j=0}^{d} \binom{d}{j} q^j (1-q)^{d-j} f(j) \\ &= (1-q)^d f(0) + \sum_{j=1}^{d-1} \binom{d}{j} q^j (1-q)^{d-j} f(j) + q^d f(d) \\ &= (1-q)^d f(0) + \sum_{j=1}^{d-1} \left(\binom{d-1}{j} + \binom{d-1}{j-1} \right) q^j (1-q)^{d-j} f(j) + q^d f(d) \\ &= \sum_{j=0}^{d-1} \binom{d-1}{j} q^j (1-q)^{d-j} f(j) + \sum_{j=1}^{d} \binom{d-1}{j-1} q^j (1-q)^{d-j} f(j). \end{aligned} \tag{49}$$

Regarding $P(+,q)$, by relabelling, we have that

$$P(+,q) = \sum_{j=0}^{d-1} \binom{d-1}{j} q^j (1-q)^{d-1-j} f(j+1) \tag{50}$$

$$= \sum_{j=1}^{d} \binom{d-1}{j-1} q^{j-1} (1-q)^{d-j} f(j). \tag{51}$$

From (50) and (51), we can rewrite $P(+,q)$ as

$$\begin{aligned} P(+,q) &= (1-q) \sum_{j=0}^{d-1} \binom{d-1}{j} q^j (1-q)^{d-1-j} f(j+1) + q \sum_{j=1}^{d} \binom{d-1}{j-1} q^{j-1} (1-q)^{d-j} f(j) \\ &= \sum_{j=0}^{d-1} \binom{d-1}{j} q^j (1-q)^{d-j} f(j+1) + \sum_{j=1}^{d} \binom{d-1}{j-1} q^j (1-q)^{d-j} f(j). \end{aligned} \tag{52}$$

Combining (49) and (52), we can write $\Delta(q)$ as

$$\begin{aligned} \Delta(q) &= P(+,q) - P(-,q) \\ &= \sum_{j=0}^{d-1} \binom{d-1}{j} q^j (1-q)^{d-j} (f(j+1) - f(j)). \end{aligned} \tag{53}$$

Under the assumption that $f(\cdot)$ is monotonically increasing and $f(0) < f(d)$, we conclude that

$$\Delta(q) > 0 \;\text{ or equivalently }\; P(+,q) > P(-,q). \tag{54}$$

Similarly, regarding $Q(-,q)$, we have

$$\begin{aligned} Q(-,q) &= \sum_{j=0}^{d} \binom{d}{j} q^j (1-q)^{d-j} f(j) \\ &= \sum_{j=0}^{d-1} \binom{d-1}{j} q^j (1-q)^{d-j} f(j) + \sum_{j=1}^{d} \binom{d-1}{j-1} q^j (1-q)^{d-j} f(j). \end{aligned}$$

And regarding $Q(+,q)$, we have

$$\begin{aligned} Q(+,q) &= \sum_{j=0}^{d-1} \binom{d-1}{j} q^j (1-q)^{d-1-j} f(j) \\ &= \sum_{j=1}^{d} \binom{d-1}{j-1} q^{j-1} (1-q)^{d-j} f(j-1) \\ &= (1-q) \sum_{j=0}^{d-1} \binom{d-1}{j} q^j (1-q)^{d-1-j} f(j) + q \sum_{j=1}^{d} \binom{d-1}{j-1} q^{j-1} (1-q)^{d-j} f(j-1) \\ &= \sum_{j=0}^{d-1} \binom{d-1}{j} q^j (1-q)^{d-j} f(j) + \sum_{j=1}^{d} \binom{d-1}{j-1} q^j (1-q)^{d-j} f(j-1). \end{aligned}$$

It then follows that

$$\begin{aligned}\nabla(q) &= Q(-,q) - Q(+,q) \qquad (55)\\ &= \sum_{j=1}^{d}\binom{d-1}{j-1}q^j(1-q)^{d-j}(f(j)-f(j-1))\\ &= \sum_{j=0}^{d-1}\binom{d-1}{j}q^{j+1}(1-q)^{d-j-1}(f(j+1)-f(j))\\ &= \frac{q}{1-q}\Delta(q), \qquad (56)\end{aligned}$$

where the last equality follows from (53). This together with (54) implies that

$$\nabla(q) > 0 \text{ or equivalently } Q(-,q) > Q(+,q). \qquad (57)$$

Using the monotonicity of $f(\cdot)$, we see that

$$P(+,q) \le \sum_{j=0}^{d-1}\binom{d-1}{j}q^j(1-q)^{d-1-j}f(d) = f(d) \qquad (58)$$

$$Q(+,q) \ge \sum_{j=0}^{d-1}\binom{d-1}{j}q^j(1-q)^{d-1-j}f(0) = f(0) \qquad (59)$$

Combining (54), (57), (58) and (59), along with the definitions of $P(-,q)$ in (4) and $Q(-,q)$ in (5), we obtain

$$f(d) \ge P(+,q) > P(-,q) = Q(-,q) > Q(+,q) \ge f(0). \qquad (60)$$

Recalling the definition

$$P_{\min}(q) = \min\left\{P(+,q), 1-Q(+,q)\right\}, \qquad (61)$$

we have from (60) that

$$\begin{aligned}1 \ge P_{\min}(q) &\ge \min\{P(+,q), 1-P(-,q)\}\\ &\ge \min\{P(+,q)-P(-,q), P(+,q)-P(-,q)\}\\ &= \Delta(q), \qquad (62)\end{aligned}$$

and

$$\begin{aligned}P_{\min}(q) &\ge \min\{Q(-,q), 1-Q(+,q)\}\\ &\ge \min\{Q(-,q)-Q(+,q), Q(-,q)-Q(+,q)\}\\ &= \nabla(q), \qquad (63)\end{aligned}$$

Combining (62) and (63), we have that

$$1 \ge P_{\min}(q) \ge \max\left\{\Delta(q), \nabla(q)\right\}.$$

This concludes the proof.

D Proofs of tail-bound lemmas

The proofs of the tail-bound lemmas that bound the probability of error of our decoding rules in Theorem 1 are collected in this Appendix.

D.1 Proof of Lemma 3

We shall use the following well-known Chernoff bound [Chernoff et al., 1952].

Fact 1 (Chernoff bound [Chernoff et al., 1952]). *Suppose that $X \sim$ Binomial(n,p). Then, for any $\delta' \in (0,1)$, we have*

$$\begin{aligned}\Pr\left(X \le (1-\delta')np\right) &\le \exp\left(-\frac{\delta'^2}{2}np\right) \le \exp\left(-\frac{\delta'^2}{3}np\right),\\ \Pr\left(X \ge (1+\delta')np\right) &\le \exp\left(-\frac{\delta'^2}{2+\delta'}np\right) \le \exp\left(-\frac{\delta'^2}{3}np\right).\end{aligned} \tag{64}$$

We now proceed with the proof of Lemma 3. Recall that in (29), T was selected to satisfy $T \ge \frac{13}{6q}m$. Consider an arbitrary item $i \in \mathcal{N}$. Since each item participates in a test i.i.d. with probability q, the expected number of tests item i involving is

$$\begin{aligned}\mathbb{E}(m_i) &= qT\\ &\ge \frac{13}{6}m\\ &= 2m + \frac{1}{6}\times\frac{12P_{\min}(q)}{(\Delta(q))^2}\ln\left(\frac{2n}{\varepsilon}\right)\\ &\ge 2m + 2\ln\left(\frac{2n}{\varepsilon}\right),\end{aligned} \tag{65}$$

where the third line follows from the definition of m in (11); the last line follows from (10).

Let $\mathcal{E}_i$ be the event that item i participates in less than m tests. By Fact 1, we have

$$\begin{aligned}\Pr(\mathcal{E}_i) &= \Pr\left(m_i < m = \left(1-\frac{\mathbb{E}(m_i)-m}{\mathbb{E}(m_i)}\right)\mathbb{E}(m_i)\right)\\ &\le \exp\left(-\left(\frac{\mathbb{E}(m_i)-m}{\mathbb{E}(m_i)}\right)^2\frac{\mathbb{E}(m_i)}{2}\right)\\ &= \exp\left(-\frac{\mathbb{E}(m_i)}{2}+m-\frac{m^2}{2\mathbb{E}(m_i)}\right)\\ &\le \exp\left(-\frac{\mathbb{E}(m_i)}{2}+m\right)\\ &\le \exp\left(-\ln\left(\frac{2n}{\varepsilon}\right)\right) = \frac{\varepsilon}{2n},\end{aligned}$$

where the last inequality follows from (65). By the union bound, the probability that all items participate in at least m tests can be bounded from below by

$$1-\Pr\left(\bigcup_{i\in\mathcal{N}}\mathcal{E}_i\right) \ge 1-\sum_{i\in\mathcal{N}}\Pr(\mathcal{E}_i) > 1-\frac{\varepsilon}{2n}\times n = 1-\frac{\varepsilon}{2}.$$

D.2 Proof of Lemma 4

To begin with, assume that each item participates in at least m tests, i.e., $m_i \ge m$ for all items i. As discussed in Decoding Rule 1, we identify item i via (16). Two types of error can happen:

1. Item i is non-defective, but is identified as defective, i.e., false alarm;
2. Item i is defective, but is identified as non-defective, i.e., missed detection.

We will bound the probabilities of 1) and 2) occuring separately as follows. For notational simplicity, let $\rho = P(-,q)$, $\nu = P(+,q)$, $\Delta = \Delta(q)$, $P_{\min} = P_{\min}(q)$. Recall that by Definition 3, $\Delta = \nu - \rho$.

D.2.1 False alarm for item i

In this scenario, each test outcome is positive with probability ρ, and

$$\frac{m_i^+}{m_i} > \frac{\rho+\nu}{2}. \tag{66}$$

Let P_{FA} denote the probability of this false alarm. Since the test outcomes are independent due to the tests being constructed in an i.i.d. manner, $m_i^+ \sim \text{Binomial}(m_i, \rho)$. From Fact 1, P_{FA} can be bounded as

$$\begin{aligned}
P_{\text{FA}} &= \Pr\left(\frac{m_i^+}{m_i} > \frac{\rho+\nu}{2}\right) \\
&= \Pr\left(m_i^+ > \left(1+\frac{\Delta}{2\rho}\right)\rho m_i\right) \\
&\le \exp\left(-\frac{1}{3}\times\frac{\Delta^2}{4\rho^2}\times\rho m_i\right) \\
&= \exp\left(-\frac{\Delta^2}{12\rho}m_i\right) \\
&\le \exp\left(-\frac{\Delta^2}{12\rho}m\right).
\end{aligned} \tag{67}$$

On the other hand, we also have $m_i^- \sim \text{Binomial}(m_i, 1-\rho)$. From Fact 1, P_{FA} can also be bounded as

$$\begin{aligned}
P_{\text{FA}} &= \Pr\left(\frac{m_i^+}{m_i} > \frac{\rho+\nu}{2}\right) \\
&= \Pr\left(\frac{m_i^-}{m_i} < 1-\frac{\rho+\nu}{2}\right) \\
&= \Pr\left(m_i^- < \left(1-\frac{\Delta}{2(1-\rho)}\right)(1-\rho)m_i\right) \\
&\le \exp\left(-\frac{1}{3}\times\frac{\Delta^2}{4(1-\rho)^2}(1-\rho)m_i\right) \\
&= \exp\left(-\frac{\Delta^2}{12(1-\rho)}m_i\right) \\
&\le \exp\left(-\frac{\Delta^2}{12(1-\rho)}m\right).
\end{aligned} \tag{68}$$

Combining (67) and (68), we obtain

$$\begin{aligned}
P_{\text{FA}} &\le \exp\left(-\frac{\Delta^2}{12\min\{\rho,1-\rho\}}m\right) \\
&\le \exp\left(-\frac{\Delta^2}{12P_{\min}}m\right) \\
&\le \frac{\varepsilon}{2n},
\end{aligned} \tag{69}$$

where the second inequality follows from (7) and (8); the last inequality follows by substituting the definition of m in (11).

D.2.2 Missed detection for item i

The calculations are similar to those above analyzing the probability of a false alarm for item i. In this case, each test outcome is positive with probability ν, and

$$\frac{m_i^+}{m_i} \le \frac{\rho+\nu}{2}. \tag{70}$$

Let P_{MD} denote the probability of this false non-defective. Again since the test outcomes are independent, we have $m_i^+ \sim \mathrm{Binomial}(m_i, \nu)$. From Fact 1, we can bound P_{MD} as

$$\begin{aligned} P_{\mathrm{MD}} &= \Pr\left(\frac{m_i^+}{m_i} \le \frac{\rho+\nu}{2}\right) \\ &= \Pr\left(m_i^+ \le \left(1-\frac{\Delta}{2\nu}\right)\nu m_i\right) \\ &\le \exp\left(-\frac{1}{3}\times\frac{\Delta^2}{4\nu^2}\times\nu m_i\right) \\ &= \exp\left(-\frac{\Delta^2}{12\nu}m_i\right) \\ &\le \exp\left(-\frac{\Delta^2}{12\nu}m\right). \end{aligned} \tag{71}$$

From another perspective, $m_i^- \sim \mathrm{Binomial}(m_i, 1-\nu)$. From Fact 1, we can also bound P_{MD} as

$$\begin{aligned} P_{\mathrm{MD}} &= \Pr\left(\frac{m_i^+}{m_i} \le \frac{\rho+\nu}{2}\right) \\ &= \Pr\left(\frac{m_i^-}{m_i} \ge 1-\frac{\rho+\nu}{2}\right) \\ &= \Pr\left(m_i^- \ge \left(1+\frac{\Delta}{2(1-\nu)}\right)(1-\nu)m_i\right) \\ &\le \exp\left(-\frac{1}{3}\times\frac{\Delta^2}{4(1-\nu)^2}(1-\nu)m_i\right) \\ &= \exp\left(-\frac{\Delta^2}{12(1-\nu)}m_i\right) \\ &\le \exp\left(-\frac{\Delta^2}{12(1-\nu)}m\right). \end{aligned} \tag{72}$$

Combining (71) and (72), we see that

$$\begin{aligned} P_{\mathrm{MD}} &\le \exp\left(-\frac{\Delta^2}{12\min\{\nu,1-\nu\}}m\right) \\ &\le \exp\left(-\frac{\Delta^2}{12P_{\min}}m\right) \\ &\le \frac{\varepsilon}{2n}, \end{aligned} \tag{73}$$

where the second inequality follows from (7) and (8); the last inequality follows from the definition of m in (11).

From (69) and (73) we conclude that for any item $i \in \mathcal{N}$, the probability of misidentification (either false alarm or missed detection) is smaller than $\frac{\varepsilon}{2n}$. Therefore, when all items participate in at least m tests, by the union bound the probability that all items are correctly identified is bounded from below by

$$1-\frac{\varepsilon}{2n}\times n = 1-\frac{\varepsilon}{2}, \tag{74}$$

which concludes the proof of Lemma 4.

D.3 Proof of Lemma 5

Recall that in (30), T was chosen to satisfy $T \geq \frac{13}{6(1-q)}s$. Consider an arbitrary item $i \in \mathcal{N}$. Since each item does not participate in a test i.i.d. with probability $1-q$, the expected number of tests without item i is

$$\begin{aligned}\mathbb{E}(s_i) &= (1-q)T \\ &\geq \frac{13}{6}s \\ &= 2s + \frac{1}{6} \times \frac{12P_{\min}(q)}{(\nabla(q))^2} \ln\left(\frac{2n}{\varepsilon}\right) \\ &\geq 2s + 2\ln\left(\frac{2n}{\varepsilon}\right), \end{aligned} \tag{75}$$

where the third line follows from the definition of s in (12); the last line follows from (10).

Let $\hat{\mathcal{E}}_i$ be the event that item i participates in more than $T-s$. In other words, the number of tests without item i is less than s. By Fact 1, we have

$$\begin{aligned}\Pr(\hat{\mathcal{E}}_i) &= \Pr\left(s_i < s = \left(1 - \frac{\mathbb{E}(s_i) - s}{\mathbb{E}(s_i)}\right)\mathbb{E}(s_i)\right) \\ &\leq \exp\left(-\left(\frac{\mathbb{E}(s_i) - s}{\mathbb{E}(s_i)}\right)^2 \frac{\mathbb{E}(s_i)}{2}\right) \\ &= \exp\left(-\frac{\mathbb{E}(s_i)}{2} + s - \frac{s^2}{2\mathbb{E}(s_i)}\right) \\ &\leq \exp\left(-\frac{\mathbb{E}(s_i)}{2} + s\right) \\ &\leq \exp\left(-\ln\left(\frac{2n}{\varepsilon}\right)\right) = \frac{\varepsilon}{2n}, \end{aligned}$$

where the last inequality follows from (75). By the union bound, the probability that each item participates in at most $T-s$ tests can be bounded from below by

$$1 - \Pr\left(\bigcup_i \hat{\mathcal{E}}_i\right) \geq 1 - \sum_i \Pr(\hat{\mathcal{E}}_i) > 1 - \frac{\varepsilon}{2n} \times n = 1 - \frac{\varepsilon}{2}. \tag{76}$$

D.4 Proof of Lemma 6

To begin with, assume that each item participates in at most $T-s$ tests, i.e., $s_i \geq s$ for all items i. As discussed in Decoding Rule 2, we identify item i via (17). Two types of error can happen:

1. Item i is non-defective, but is identified as defective, i.e., false alarm;
2. Item i is defective, but is identified as non-defective, i.e., missed detection.

We will bound the probabilities of 1) and 2) occuring separately as follows. For notational simplicity, let $\hat{\rho} = Q(-,q)$, $\hat{\nu} = Q(+,q)$, $\nabla = \nabla(q)$, $P_{\min} = P_{\min}(q)$. Recall that by Definition 3, $\nabla = \hat{\rho} - \hat{\nu}$.

D.4.1 <u>False alarm for item i</u>

In this scenario, each test outcome is positive with probability $\hat{\rho}$, and

$$\frac{s_i^+}{s_i} \leq \frac{\hat{\rho} + \hat{\nu}}{2}. \tag{77}$$

Let $\hat{P}_{\text{FA}}$ denote the probability of this false alarm. Since the test outcomes are independent due to the tests being constructed in an i.i.d. manner, $s_i^+ \sim \text{Binomial}(s_i, \hat{\rho})$. From Fact 1, $\hat{P}_{\text{FA}}$ can be bounded as

$$\begin{aligned}
\hat{P}_{\text{FA}} &= \Pr\left(\frac{s_i^+}{s_i} \leq \frac{\hat{\rho}+\hat{\nu}}{2}\right) \\
&= \Pr\left(s_i^+ \leq \left(1 - \frac{\nabla}{2\hat{\rho}}\right)\hat{\rho} s_i\right) \\
&\leq \exp\left(-\frac{1}{3} \times \frac{\nabla^2}{4\hat{\rho}^2} \times \hat{\rho} s_i\right) \\
&= \exp\left(-\frac{\nabla^2}{12\hat{\rho}} s_i\right) \\
&\leq \exp\left(-\frac{\nabla^2}{12\hat{\rho}} s\right).
\end{aligned} \tag{78}$$

On the other hand, we also have $s_i^- \sim \text{Binomial}(s_i, 1-\hat{\rho})$. From Fact 1, $\hat{P}_{\text{FA}}$ can also be bounded as

$$\begin{aligned}
\hat{P}_{\text{FA}} &= \Pr\left(\frac{s_i^+}{s_i} \leq \frac{\hat{\rho}+\hat{\nu}}{2}\right) \\
&= \Pr\left(\frac{s_i^-}{s_i} \geq 1 - \frac{\hat{\rho}+\hat{\nu}}{2}\right) \\
&= \Pr\left(s_i^- \geq \left(1 + \frac{\nabla}{2(1-\hat{\rho})}\right)(1-\hat{\rho}) s_i\right) \\
&\leq \exp\left(-\frac{1}{3} \times \frac{\nabla^2}{4(1-\hat{\rho})^2}(1-\hat{\rho}) s_i\right) \\
&= \exp\left(-\frac{\nabla^2}{12(1-\hat{\rho})} s_i\right) \\
&\leq \exp\left(-\frac{\nabla^2}{12(1-\hat{\rho})} s\right).
\end{aligned} \tag{79}$$

Combining (78) and (79), we obtain

$$\hat{P}_{\text{FA}} \leq \exp\left(-\frac{\nabla^2}{12\min\{\hat{\rho}, 1-\hat{\rho}\}} s\right) \leq \exp\left(-\frac{\nabla^2}{12P_{\min}} s\right) \leq \frac{\varepsilon}{2n}, \tag{80}$$

where the second inequality follows from (7) and (8); the last inequality follows by substituting the definition of s in (12).

D.4.2 Missed detection for item i

The calculations are similar to those above analyzing the probability of a false alarm for item i. In this case, each test outcome is positive with probability $\hat{\nu}$, and

$$\frac{s_i^+}{s_i} > \frac{\hat{\rho}+\hat{\nu}}{2}. \tag{81}$$

Let $\hat{P}_{\mathrm{MD}}$ denote the probability of this false non-defective. Again since the outcomes are independent, we have $s_i^+ \sim \text{Binomial}(s_i, \hat{\nu})$. From Fact 1, we can bound $\hat{P}_{\mathrm{MD}}$ as

$$\begin{aligned}
\hat{P}_{\mathrm{MD}} &= \Pr\left(\frac{s_i^+}{s_i} > \frac{\hat{\rho}+\hat{\nu}}{2}\right) \\
&= \Pr\left(s_i^+ > \left(1+\frac{\nabla}{2\hat{\nu}}\right)\hat{\nu}s_i\right) \\
&\le \exp\left(-\frac{1}{3}\times\frac{\nabla^2}{4\hat{\nu}^2}\times\hat{\nu}s_i\right) \\
&= \exp\left(-\frac{\nabla^2}{12\hat{\nu}}s_i\right) \\
&\le \exp\left(-\frac{\nabla^2}{12\hat{\nu}}s\right). \qquad (82)
\end{aligned}$$

From another perspective, $s_i^- \sim \text{Binomial}(s_i, 1-\hat{\nu})$. From Fact 1, we can also bound $\hat{P}_{\mathrm{MD}}$ as

$$\begin{aligned}
\hat{P}_{\mathrm{MD}} &= \Pr\left(\frac{s_i^+}{s_i} > \frac{\hat{\rho}+\hat{\nu}}{2}\right) \\
&= \Pr\left(\frac{s_i^-}{s_i} < 1-\frac{\hat{\rho}+\hat{\nu}}{2}\right) \\
&= \Pr\left(s_i^- < \left(1-\frac{\nabla}{2(1-\hat{\nu})}\right)(1-\hat{\nu})s_i\right) \\
&\le \exp\left(-\frac{1}{3}\times\frac{\nabla^2}{4(1-\hat{\nu})^2}(1-\hat{\nu})s_i\right) \\
&= \exp\left(-\frac{\nabla^2}{12(1-\hat{\nu})}s_i\right) \\
&\le \exp\left(-\frac{\nabla^2}{12(1-\hat{\nu})}s\right). \qquad (83)
\end{aligned}$$

Combining (82) and (83), we see that

$$\hat{P}_{\mathrm{MD}} \le \exp\left(-\frac{\nabla^2}{12\min\{\hat{\nu},1-\hat{\nu}\}}s\right) \le \exp\left(-\frac{\nabla^2}{12P_{\min}}s\right) \le \frac{\varepsilon}{2n}, \qquad (84)$$

where the second inequality follows from (7) and (8); the last inequality follows from the definition of s in (12).

From (80) and (84) we conclude that for any item $i \in \mathcal{N}$, the probability of misidentification (either false alarm or missed detection) is smaller than $\frac{\varepsilon}{2n}$. Therefore, when each item participates in at most $T-s$ tests, by the union bound the probability that all items are correctly identified is bounded from below by

$$1-\frac{\varepsilon}{2n}\times n = 1-\frac{\varepsilon}{2}, \qquad (85)$$

which concludes the proof of Lemma 6.

E Proof of Proposition 3

From (14), we know that the value of $\hat{\Gamma}(q)$ depends on the choice of q. For $q \in \left(\frac{1}{d}, \frac{d-1}{d}\right)$ with $d \ge 3$, the following result asserts that by choosing q properly, we can give an explicit bound on the value of $\hat{\Gamma}(q)$.

Proposition 4. *Let $d \ge 3$. For any $L', U' \in \{1, \dots, d-1\}$ with $L' < U'$ and $f(L') < f(U')$, there exists $q_0 \in \left(\frac{L'}{d}, \frac{U'}{d}\right)$ such that $\hat{\Gamma}(q_0)$ in (14) satisfies*

$$\hat{\Gamma}(q_0) \le 31334.75 \times \frac{1}{\alpha^2}\left(\frac{U'-L'}{f(U')-f(L')}\right)^2 d\log\left(\frac{2n}{\varepsilon}\right) \qquad (86)$$

where $\alpha := \frac{1}{2}\min\left\{U'-L', \sqrt{L'}, \sqrt{d-U'}\right\}$.

Proof. The proof of Proposition 4 is rather involved and is deferred to Appendix F. □

Below, the boundary points are handled separately.

Proposition 5. *1. By choosing $q_0 = \frac{1}{d+1}$, which implicitly requires $f(1) - f(0) > 0$,[5] $\hat{\Gamma}(q_0)$ in (14) satisfies*

$$\hat{\Gamma}(q_0) \leq \frac{266.45}{(f(1)-f(0))^2} d \log\left(\frac{2n}{\varepsilon}\right). \tag{87}$$

2. By choosing $q_0 = \frac{d}{d+1}$, which implicitly requires $f(d) - f(d-1) > 0$,[5] $\hat{\Gamma}(q_0)$ in (14) satisfies

$$\hat{\Gamma}(q_0) \leq \frac{266.45}{(f(d)-f(d-1))^2} d \log\left(\frac{2n}{\varepsilon}\right). \tag{88}$$

Proof. We prove the first part of the lemma directly. Upon choosing $q_0 = \frac{1}{d+1}$, we have from (53) that

$$\begin{aligned}
\Delta(q_0) &= \sum_{j=0}^{d-1} \binom{d-1}{j} q_0^j (1-q_0)^{d-j} (f(j+1) - f(j)) \\
&\geq q_0^0 (1-q_0)^d (f(1) - f(0)) \\
&\geq \frac{f(1)-f(0)}{e},
\end{aligned}$$

where the last inequality follows from the fact that $\left(1 - \frac{1}{d+1}\right)^d$ is decreasing in d and $\lim_{d\to\infty} \left(1 - \frac{1}{d+1}\right)^d = \frac{1}{e}$. Then, plugging this into (14), we obtain

$$\hat{\Gamma}(q_0) = \frac{36.06(1-q_0)}{q_0(\Delta(q_0))^2} \log\left(\frac{2n}{\varepsilon}\right) \leq \frac{266.45}{(f(1)-f(0))^2} d \log\left(\frac{2n}{\varepsilon}\right),$$

which yields (87) as desired.

We now turn to prove the second part of the lemma. Under the choice $q_0 = \frac{d}{d+1}$, we have from (53) that

$$\begin{aligned}
\Delta(q_0) &= \sum_{j=0}^{d-1} \binom{d-1}{j} q_0^j (1-q_0)^{d-j} (f(j+1) - f(j)) \\
&\geq q_0^{d-1} (1-q_0)^1 (f(d) - f(d-1)) \\
&= \left(1 - \frac{1}{d+1}\right)^d \frac{f(d)-f(d-1)}{d} \\
&\geq \frac{f(d)-f(d-1)}{ed}.
\end{aligned}$$

Then, plugging this into (14), we obtain

$$\hat{\Gamma}(q_0) = \frac{36.06(1-q_0)}{q_0(\Delta(q_0))^2} \log\left(\frac{2n}{\varepsilon}\right) \leq \frac{266.45}{(f(d)-f(d-1))^2} d \log\left(\frac{2n}{\varepsilon}\right).$$

This completes the proof of Proposition 5. □

Proposition 3 is proved by unifying Propositions 4 and 5. To begin with, consider any $L, U \in \{0, \ldots, d\}$ such that $L < U$ and $f(L) < f(U)$.[6] Define

$$\beta := \min\left\{U - L, \sqrt{L+1}, \sqrt{d-U+1}\right\}. \tag{89}$$

Consider the following four cases:

[5] If $f(1) - f(0) = 0$ or $f(d) - f(d-1) = 0$, we can choose q_0 as in Proposition 4.

[6] If there is no such pair of (L, U), we have $f(x)$=constant for all x. In this case, the defective set $\mathcal{D}$ can never be recovered.

i) $1 \le L < U \le d-1$;

ii) $0 = L < U \le d-1$;

iii) $1 \le L < U = d$;

iv) $0 = L < U = d$.

Case i): For $1 \le L < U \le d-1$, we have

$$\beta = \min\left\{U-L, \sqrt{L+1}, \sqrt{d-U+1}\right\} \le \min\left\{\sqrt{2}(U-L), \sqrt{2L}, \sqrt{2(d-U)}\right\}. \tag{90}$$

Then, applying Proposition 4 with $L' = L$ and $U' = U$, we have that $\beta \le 2\sqrt{2}\alpha$ and

$$\begin{aligned}\hat{\Gamma}(q_0) &\le 250678 \times \frac{1}{\beta^2}\left(\frac{U-L}{f(U)-f(L)}\right)^2 d\log\left(\frac{2n}{\varepsilon}\right)\\ &\le 376017 \times \frac{1}{\beta^2}\left(\frac{U-L}{f(U)-f(L)}\right)^2 d\log\left(\frac{2n}{\varepsilon}\right)\end{aligned} \tag{91}$$

for some $q_0 \in \left(\frac{L}{d}, \frac{U}{d}\right)$.

Case ii): For $0 = L < U \le d-1$, we have $\beta = 1$ by definition (89). We proceed with two further sub-cases.

- $\underline{U = 1}$: From Proposition 5 we see that

$$\begin{aligned}\hat{\Gamma}(q_0) &\le \frac{266.45}{(f(1)-f(0))^2} d\log\left(\frac{2n}{\varepsilon}\right)\\ &\le 376017 \times \frac{1}{\beta^2}\left(\frac{U-L}{f(U)-f(L)}\right)^2 d\log\left(\frac{2n}{\varepsilon}\right)\end{aligned} \tag{92}$$

  for $q_0 = \frac{1}{d+1} \in \left(\frac{L}{d}, \frac{U}{d}\right)$.

- $\underline{U \ge 2}$: Both Propositions 4 and 5 are applicable, we prefer to choose the one with smaller upper bound. Applying Proposition 4 with $L' = 1$ and $U' = U$, we have that $\alpha = \frac{1}{2}$ and

$$\hat{\Gamma}(q_0') \le 125339 \times \left(\frac{U-1}{f(U)-f(1)}\right)^2 d\log\left(\frac{2n}{\varepsilon}\right) \tag{93}$$

  for some $q_0' \in \left(\frac{1}{d}, \frac{U}{d}\right)$. On the other hand, Proposition 5 gives

$$\hat{\Gamma}(q_0'') \le \frac{266.45}{(f(1)-f(0))^2} d\log\left(\frac{2n}{\varepsilon}\right) \tag{94}$$

  for $q_0'' = \frac{1}{d+1} \in \left(\frac{L}{d}, \frac{1}{d}\right)$. Since

$$\begin{aligned}\min\left\{\frac{1}{(f(1)-f(0))^2}, \frac{(U-1)^2}{(f(U)-f(1))^2}\right\} &\le \frac{1+(U-1)^2}{(f(1)-f(0))^2+(f(U)-f(1))^2}\\ &\le \frac{2U^2}{(f(U)-f(0))^2},\end{aligned} \tag{95}$$

it follows that

$$\begin{aligned}\hat{\Gamma}(q_0) &\leq \min\left\{125339 \times \left(\frac{U-1}{f(U)-f(1)}\right)^2 d\log\left(\frac{2n}{\varepsilon}\right), \frac{576.96}{(f(1)-f(0))^2} d\log\left(\frac{2n}{\varepsilon}\right)\right\} \\ &\leq 125339 \times \min\left\{\frac{1}{(f(1)-f(0))^2}, \frac{(U-1)^2}{(f(U)-f(1))^2}\right\} \times d\log\left(\frac{2n}{\varepsilon}\right) \\ &\leq 250678 \times \frac{U^2}{(f(U)-f(0))^2} d\log\left(\frac{2n}{\varepsilon}\right) \\ &= 250678 \times \frac{1}{\beta^2}\left(\frac{U-L}{f(U)-f(L)}\right)^2 d\log\left(\frac{2n}{\varepsilon}\right) \\ &\leq 376017 \times \frac{1}{\beta^2}\left(\frac{U-L}{f(U)-f(L)}\right)^2 d\log\left(\frac{2n}{\varepsilon}\right) \end{aligned} \tag{96}$$

for some $q_0 \in \left(\frac{L}{d}, \frac{U}{d}\right)$.

Case iii): For $1 \leq L < U = d$, we have $\beta = 1$ by definition (89). The proof is similar to Case ii). Consider the following two sub-cases.

- $\underline{L = d-1}$: From Proposition 5 we see that

$$\begin{aligned}\hat{\Gamma}(q_0) &\leq \frac{266.45}{(f(d)-f(d-1))^2} d\log\left(\frac{2n}{\varepsilon}\right) \\ &\leq 376017 \times \frac{1}{\beta^2}\left(\frac{U-L}{f(U)-f(L)}\right)^2 d\log\left(\frac{2n}{\varepsilon}\right) \end{aligned} \tag{97}$$

  for $q_0 = \frac{d}{d+1} \in \left(\frac{L}{d}, \frac{U}{d}\right)$.

- $\underline{L \leq d-2}$: Applying Proposition 4 with $L' = L$ and $U' = d-1$, we have that $\alpha = \frac{1}{2}$ and

$$\hat{\Gamma}(q_0') \leq 125339 \times \left(\frac{d-1-L}{f(d-1)-f(L)}\right)^2 d\log\left(\frac{2n}{\varepsilon}\right) \tag{98}$$

  for some $q_0' \in \left(\frac{L}{d}, \frac{d-1}{d}\right)$. On the other hand, Proposition 5 gives

$$\hat{\Gamma}(q_0'') \leq \frac{266.45}{(f(d)-f(d-1))^2} d\log\left(\frac{2n}{\varepsilon}\right) \tag{99}$$

  for $q_0'' = \frac{1}{d+1} \in \left(\frac{d-1}{d}, \frac{U}{d}\right)$. Since

$$\begin{aligned}\min\left\{\frac{1}{(f(d)-f(d-1))^2}, \frac{(d-1-L)^2}{(f(d-1)-f(L))^2}\right\} &\leq \frac{1+(d-1-L)^2}{(f(d)-f(d-1))^2+(f(d-1)-f(L))^2} \\ &\leq \frac{2(d-L)^2}{(f(d)-f(L))^2}, \end{aligned} \tag{100}$$

  it follows that

$$\begin{aligned}\hat{\Gamma}(q_0) &\leq \min\left\{125339 \times \left(\frac{d-1-L}{f(d-1)-f(L)}\right)^2 d\log\left(\frac{2n}{\varepsilon}\right), \frac{266.45}{(f(d)-f(d-1))^2} d\log\left(\frac{2n}{\varepsilon}\right)\right\} \\ &\leq 125339 \times \min\left\{\frac{1}{(f(d)-f(d-1))^2}, \frac{(d-1-L)^2}{(f(d-1)-f(L))^2}\right\} \times d\log\left(\frac{2n}{\varepsilon}\right) \\ &\leq 250678 \times \frac{(d-L)^2}{(f(d)-f(L))^2} d\log\left(\frac{2n}{\varepsilon}\right) \\ &= 250678 \times \frac{1}{\beta^2}\left(\frac{U-L}{f(U)-f(L)}\right)^2 d\log\left(\frac{2n}{\varepsilon}\right) \\ &\leq 376017 \times \frac{1}{\beta^2}\left(\frac{U-L}{f(U)-f(L)}\right)^2 d\log\left(\frac{2n}{\varepsilon}\right) \end{aligned} \tag{101}$$

for some $q_0 \in \left(\frac{L}{d}, \frac{U}{d}\right)$.

Case iv): For $0 = L < U = d$, we have $\beta = 1$ by definition (89). The proof is similar to Case ii). Consider three sub-cases:

- $\underline{d = 1}$: In this sub-case, the two bounds in Proposition 5 are identical and give

$$\begin{aligned}\hat{\Gamma}(q_0) &\leq \frac{266.45}{(f(1)-f(0))^2} d \log\left(\frac{2n}{\varepsilon}\right) \\ &\leq 376017 \times \frac{1}{\beta^2}\left(\frac{U-L}{f(U)-f(L)}\right)^2 d \log\left(\frac{2n}{\varepsilon}\right) \end{aligned} \tag{102}$$

for $q_0 = \frac{1}{d+1} \in \left(\frac{L}{d}, \frac{U}{d}\right)$.

- $\underline{d = 2}$: From Proposition 5 we see that

$$\hat{\Gamma}(q_0') \leq \frac{266.45}{(f(1)-f(0))^2} d \log\left(\frac{2n}{\varepsilon}\right) \tag{103}$$

for $q_0' = \frac{1}{d+1} \in \left(\frac{L}{d}, \frac{1}{d}\right)$, and

$$\hat{\Gamma}(q_0'') \leq \frac{266.45}{(f(2)-f(1))^2} d \log\left(\frac{2n}{\varepsilon}\right) \tag{104}$$

for $q_0'' = \frac{d}{d+1} \in \left(\frac{1}{d}, \frac{U}{d}\right)$. Since

$$\begin{aligned}\min\left\{\frac{1}{(f(1)-f(0))^2}, \frac{1}{(f(2)-f(1))^2}\right\} &\leq \frac{2}{(f(1)-f(0))^2 + (f(2)-f(1))^2} \\ &\leq \frac{4}{(f(2)-f(0))^2}, \end{aligned} \tag{105}$$

it follows that

$$\begin{aligned}\hat{\Gamma}(q_0) &\leq \min\left\{\frac{266.45}{(f(1)-f(0))^2} d \log\left(\frac{2n}{\varepsilon}\right), \frac{266.45}{(f(2)-f(1))^2} d \log\left(\frac{2n}{\varepsilon}\right)\right\} \\ &\leq 266.45 \times \min\left\{\frac{1}{(f(1)-f(0))^2}, \frac{1}{(f(2)-f(1))^2}\right\} \times d \log\left(\frac{2n}{\varepsilon}\right) \\ &\leq 266.45 \times \frac{4}{(f(2)-f(0))^2} d \log\left(\frac{2n}{\varepsilon}\right) \\ &= 266.45 \times \frac{1}{\beta^2}\left(\frac{U-L}{f(U)-f(L)}\right)^2 d \log\left(\frac{2n}{\varepsilon}\right) \\ &\leq 376017 \times \frac{1}{\beta^2}\left(\frac{U-L}{f(U)-f(L)}\right)^2 d \log\left(\frac{2n}{\varepsilon}\right) \end{aligned} \tag{106}$$

for some $q_0 \in \left(\frac{L}{d}, \frac{U}{d}\right)$.

- $\underline{d \geq 3}$: Applying Proposition 4 with $L' = 1$ and $U' = d-1$, we have that $\alpha = \frac{1}{2}$

$$\hat{\Gamma}(q_0') \leq 125339 \times \left(\frac{d-2}{f(d-1)-f(1)}\right)^2 d \log\left(\frac{2n}{\varepsilon}\right) \tag{107}$$

for some $q_0' \in \left(\frac{1}{d}, \frac{d-1}{d}\right)$. On the other hand, Proposition 5 gives

$$\hat{\Gamma}(q_0'') \leq \frac{266.45}{(f(1)-f(0))^2} d \log\left(\frac{2n}{\varepsilon}\right) \tag{108}$$

for $q_0'' = \frac{1}{d+1} \in \left(\frac{L}{d}, \frac{1}{d}\right)$, and

$$\hat{\Gamma}(q_0''') \leq \frac{266.45}{(f(d)-f(d-1))^2} d \log\left(\frac{2n}{\varepsilon}\right) \tag{109}$$

for $q_0''' = \frac{d}{d+1} \in \left(\frac{d-1}{d}, \frac{U}{d}\right)$. Since

$$\begin{aligned} &\min\left\{\frac{1}{(f(1)-f(0))^2}, \frac{1}{(f(d)-f(d-1))^2}, \frac{(d-2)^2}{(f(d-1)-f(1))^2}\right\} \\ &\leq \frac{1+1+(d-2)^2}{(f(1)-f(0))^2+(f(d)-f(d-1))^2+(f(d-1)-f(1))^2} \\ &\leq \frac{3d^2}{(f(d)-f(0))^2}, \end{aligned} \tag{110}$$

it follows that

$$\begin{aligned} \hat{\Gamma}(q_0) &\leq \min\left\{125339 \times \left(\frac{d-2}{f(d-1)-f(1)}\right)^2 d \log\left(\frac{2n}{\varepsilon}\right), \frac{266.45}{(f(1)-f(0))^2} d \log\left(\frac{2n}{\varepsilon}\right), \right. \\ &\qquad \left. \frac{266.45}{(f(d)-f(d-1))^2} d \log\left(\frac{2n}{\varepsilon}\right)\right\} \\ &\leq 125339 \times \min\left\{\frac{(d-2)^2}{(f(d-1)-f(1))^2}, \frac{1}{(f(1)-f(0))^2}, \frac{1}{(f(d)-f(d-1))^2}\right\} \times d \log\left(\frac{2n}{\varepsilon}\right) \\ &\leq 376017 \times \frac{d^2}{(f(d)-f(0))^2} d \log\left(\frac{2n}{\varepsilon}\right) \\ &= 376017 \times \frac{1}{\beta^2}\left(\frac{U-L}{f(U)-f(L)}\right)^2 d \log\left(\frac{2n}{\varepsilon}\right) \end{aligned} \tag{111}$$

for some $q_0 \in \left(\frac{L}{d}, \frac{U}{d}\right)$.

Summarizing the above, we see that for any $0 \leq L < U \leq d$, there exists $q_0 \in \left(\frac{L}{d}, \frac{U}{d}\right)$ such that

$$\hat{\Gamma}(q_0) \leq 376017 \times \frac{1}{\beta^2}\left(\frac{U-L}{f(U)-f(L)}\right)^2 d \log\left(\frac{2n}{\varepsilon}\right).$$

This along with the definitions of $H(f)$ and β in (18) and (89), respectively, yields

$$\hat{\Gamma}(q_0) \leq 376017 H(f) d \log\left(\frac{2n}{\varepsilon}\right) \tag{112}$$

for some $q_0 \in (0,1)$. Proposition 3 is proved.

F Proof of Proposition 4

The following technical result will serve as a stepping stone to establishing Proposition 4.

Lemma 9. *Let $d \geq 3$. For any $L', U' \in \{1, \ldots, d-1\}$ with $L' < U'$ and $f(L') < f(U')$, there exists $q_0 \in \left(\frac{L'}{d}, \frac{U'}{d}\right)$ such that $\hat{\Gamma}(q_0)$ defined in (14) satisfies*

$$\hat{\Gamma}(q_0) \leq 1253.39 \times \frac{(d-L')U'}{\alpha^2(d-U')L'}\left(\frac{U'-L'}{f(U')-f(L')}\right)^2 d \log\left(\frac{2n}{\varepsilon}\right), \tag{113}$$

where $\alpha := \frac{1}{2}\min\left\{U'-L', \sqrt{L'}, \sqrt{d-U'}\right\}$.

Proof. See Appendix G. □

Comparing Proposition 4 and Lemma 9, we see that the main difference is the $\frac{(d-L')U'}{(d-U')L'}$ term. In the remainder of the proof, we manage to eliminate the $\frac{(d-L')U'}{(d-U')L'}$ term from (113). Since $\alpha = \frac{1}{2}\min\left\{U'-L', \sqrt{L'}, \sqrt{d-U'}\right\}$, we consider the following two cases.

Case i): $\alpha = \frac{U'-L'}{2}$, i.e.,

$$U' - L' \leq \min\left\{\sqrt{L'}, \sqrt{d-U'}\right\}. \tag{114}$$

Then we immediately obtain

$$\frac{(d-L')U'}{(d-U')L'} \leq \frac{(d-U'+\sqrt{d-U'})(L'+\sqrt{L'})}{(d-U')L'} = \frac{\sqrt{d-U'}+1}{\sqrt{d-U'}} \cdot \frac{\sqrt{L'}+1}{\sqrt{L'}} \leq 2 \times 2 < 25, \tag{115}$$

where the second inequality follows from the assumption that $1 \leq L' < U' \leq d-1$. Substituting into (113), we have the desired result (86).

Case ii): $\alpha \neq \frac{U'-L'}{2}$, i.e.,

$$\alpha = \frac{1}{2}\min\left\{\sqrt{L'}, \sqrt{d-U'}\right\} < \frac{U'-L'}{2}. \tag{116}$$

Define

$$\tau := \left\lfloor \frac{U'-L'}{\lceil 2\alpha \rceil} \right\rfloor, \tag{117}$$

$$\lambda_i := L' + i \cdot \lceil 2\alpha \rceil \text{ for } i = 0, \cdots, \tau-1, \tag{118}$$

$$\lambda_\tau := U'. \tag{119}$$

For the ease of notation, let

$$\alpha_i := \frac{1}{2}\min\left\{\lambda_{i+1}-\lambda_i, \sqrt{\lambda_i}, \sqrt{d-\lambda_{i+1}}\right\} \text{ for } i = 0, \cdots, \tau-1. \tag{120}$$

The following lemma shows that for all $i = 0, \ldots, \tau-1$, α_i is bounded from below by α.

Lemma 10. *$\alpha_i \geq \alpha$ for all $i \in \{0, \cdots, \tau-1\}$.*

Proof. For $i = 0, \cdots, \tau-1$, we have from (118) that

$$L' \leq \lambda_i < \lambda_{i+1} \leq U'. \tag{121}$$

It follows that

$$\frac{1}{2}\min\left\{\sqrt{\lambda_i}, \sqrt{d-\lambda_{i+1}}\right\} \geq \frac{1}{2}\min\left\{\sqrt{L'}, \sqrt{d-U'}\right\} = \alpha. \tag{122}$$

Next, for $i = 0, \cdots, \tau-2$,

$$\frac{\lambda_{i+1}-\lambda_i}{2} = \frac{\lceil 2\alpha \rceil}{2} \geq \alpha; \tag{123}$$

for $i = \tau-1$,

$$\frac{\lambda_\tau - \lambda_{\tau-1}}{2} = \frac{U'-L'-(\tau-1)\lceil 2\alpha \rceil}{2} \geq \frac{U'-L'-\left(\frac{U'-L'}{\lceil 2\alpha \rceil}-1\right)\lceil 2\alpha \rceil}{2} = \frac{\lceil 2\alpha \rceil}{2} = \alpha. \tag{124}$$

Combining the above three inequalities, along with the definition of α_i in (120), yields the desired result. □

To complete the proof of Case ii), the following two lemmas will also be used.

Lemma 11. *$\frac{(d-\lambda_i)\lambda_{i+1}}{(d-\lambda_{i+1})\lambda_i} \leq 25$ for any $i = 0, \cdots, \tau-1$.*

Proof. Observe that for any $i = 0, \cdots, \tau - 2$,

$$\lambda_{i+1} - \lambda_i = \lceil 2\alpha \rceil \leq 4\alpha + 2; \tag{125}$$

and for $i = \tau - 1$,

$$\begin{aligned}
\lambda_\tau - \lambda_{\tau-1} &= U' - (L' + (\tau - 1)\lceil 2\alpha \rceil) \\
&= U' - L' - \left(\left\lfloor \frac{U' - L'}{\lceil 2\alpha \rceil} \right\rfloor - 1 \right) \lceil 2\alpha \rceil \\
&< U' - L' - \left(\frac{U' - L'}{\lceil 2\alpha \rceil} - 2 \right) \lceil 2\alpha \rceil \\
&= 2\lceil 2\alpha \rceil \\
&\leq 4\alpha + 2.
\end{aligned} \tag{126}$$

It then follows that for all $i = 0, \cdots, \tau - 1$,

$$\begin{aligned}
\lambda_{i+1} - \lambda_i &\leq 4\alpha + 2 \\
&= 2\min\{\sqrt{L'}, \sqrt{d - U'}\} + 2 \\
&\leq 4\min\{\sqrt{L'}, \sqrt{d - U'}\} \\
&\leq 4\min\{\sqrt{\lambda_i}, \sqrt{d - \lambda_{i+1}}\},
\end{aligned} \tag{127}$$

where the equality follows from (116); the second inequality follows from the assumption that $1 \leq L' < U' \leq d-1$; the last inequality follows from (121). Using this observation along with $1 \leq \lambda_i \leq \lambda_{i+1} \leq d - 1$, we obtain

$$\frac{(d - \lambda_i)\lambda_{i+1}}{(d - \lambda_{i+1})\lambda_i} \leq \frac{(d - \lambda_{i+1} + 4\sqrt{d - \lambda_{i+1}})(\lambda_i + 4\sqrt{\lambda_i})}{(d - \lambda_{i+1})\lambda_i} = \frac{(\sqrt{d - \lambda_{i+1}} + 4)}{\sqrt{d - \lambda_{i+1}}} \cdot \frac{(\sqrt{\lambda_i} + 4)}{\sqrt{\lambda_i}} \leq 5 \times 5 = 25, \tag{128}$$

which finishes the proof. □

Lemma 12. *$\exists \ell \in \{0, \cdots, \tau - 1\}$ such that $\frac{f(\lambda_{\ell+1}) - f(\lambda_\ell)}{\lambda_{\ell+1} - \lambda_\ell} \geq \frac{f(U') - f(L')}{U' - L'}$.*

Proof. Suppose to the contrary that $\frac{f(\lambda_{i+1}) - f(\lambda_i)}{(\lambda_{i+1} - \lambda_i)} < \frac{f(U') - f(L')}{U' - L'}$ for all $i = 0, \cdots, \tau - 1$. In other words,

$$f(\lambda_{i+1}) - f(\lambda_i) < \frac{f(U') - f(L')}{U' - L'}(\lambda_{i+1} - \lambda_i), \forall i = 0, \cdots, \tau - 1. \tag{129}$$

Summing (129) over all $i \in \{0, \cdots, \tau - 1\}$, we obtain that

$$f(U') - f(L') = \sum_{i=0}^{\tau-1} (f(\lambda_{i+1}) - f(\lambda_i)) < \sum_{i=0}^{\tau-1} \frac{f(U') - f(L')}{U' - L'}(\lambda_{i+1} - \lambda_i) = f(U') - f(L') \tag{130}$$

yielding a contradiction. Lemma 12 is proved. □

We are now ready to finish the proof of Case ii) using the above results. Upon applying Lemma 9 with $L' = \lambda_\ell$ and $U' = \lambda_{\ell+1}$ as defined in Lemma 12, we have that $\exists q_0 \in \left(\frac{\lambda_\ell}{d}, \frac{\lambda_{\ell+1}}{d} \right)$ such that

$$\begin{aligned}
\hat{\Gamma}(q_0) &\leq 1253.39 \times \frac{(d - \lambda_\ell)\lambda_{\ell+1}}{{\alpha_\ell}^2 (d - \lambda_{\ell+1})\lambda_\ell} \left(\frac{\lambda_{\ell+1} - \lambda_\ell}{f(\lambda_{\ell+1}) - f(\lambda_\ell)} \right)^2 d \log \left(\frac{2n}{\varepsilon} \right) \\
&\leq 31334.75 \times \frac{1}{{\alpha_\ell}^2} \left(\frac{\lambda_{\ell+1} - \lambda_\ell}{f(\lambda_{\ell+1}) - f(\lambda_\ell)} \right)^2 d \log \left(\frac{2n}{\varepsilon} \right) \\
&\leq 31334.75 \times \frac{1}{{\alpha_\ell}^2} \left(\frac{U' - L'}{f(U') - f(L')} \right)^2 d \log \left(\frac{2n}{\varepsilon} \right) \\
&\leq 31334.75 \times \frac{1}{\alpha^2} \left(\frac{U' - L'}{f(U') - f(L')} \right)^2 d \log \left(\frac{2n}{\varepsilon} \right)
\end{aligned} \tag{131}$$

where the second inequality follows from Lemma 11; the third inequality follows from Lemma 12; the last inequality follows from Lemma 10. This completes the proof of Proposition 4.

G Proof of Lemma 9

We now prove Lemma 9, first giving some preliminary lemmas.

Lemma 13. *For any $j = 1, \dots, d-1$, we have*

$$\frac{\sqrt{2\pi}}{e^2}\sqrt{\frac{d}{j(d-j)}} \le \binom{d}{j}\left(\frac{j}{d}\right)^j\left(\frac{d-j}{d}\right)^{d-j} \le \frac{e}{\pi}\sqrt{\frac{d}{j(d-j)}}.$$

Proof. We shall use the following well-known Stirling's approximation [Bruijn, 1981] for the factorial function.

Fact 2 (Stirling's approximation [Bruijn, 1981])**.**

$$\sqrt{2\pi}\, n^{n+\frac{1}{2}}\, e^{-n} \le n! \le e\, n^{n+\frac{1}{2}}\, e^{-n}. \tag{132}$$

Using the upper and lower bounds on $n!$ in (132), we have

$$\begin{aligned}
\binom{d}{j}\left(\frac{j}{d}\right)^j\left(\frac{d-j}{d}\right)^{d-j} &= \frac{d!}{j!(d-j)!}\left(\frac{j}{d}\right)^j\left(\frac{d-j}{d}\right)^{d-j} \\
&\ge \frac{\sqrt{2\pi}d^{d+1/2}e^{-d}}{ej^{j+1/2}e^{-j}e(d-j)^{d-j+1/2}e^{-d+j}}\left(\frac{j}{d}\right)^j\left(\frac{d-j}{d}\right)^{d-j} \\
&= \frac{\sqrt{2\pi}}{e^2}\sqrt{\frac{d}{j(d-j)}}.
\end{aligned}$$

Similarly, we also have

$$\begin{aligned}
\binom{d}{j}\left(\frac{j}{d}\right)^j\left(\frac{d-j}{d}\right)^{d-j} &= \frac{d!}{j!(d-j)!}\left(\frac{j}{d}\right)^j\left(\frac{d-j}{d}\right)^{d-j} \\
&\le \frac{ed^{d+1/2}e^{-d}}{\sqrt{2\pi}j^{j+1/2}e^{-j}\sqrt{2\pi}(d-j)^{d-j+1/2}e^{-d+j}}\left(\frac{j}{d}\right)^j\left(\frac{d-j}{d}\right)^{d-j} \\
&= \frac{e}{2\pi}\sqrt{\frac{d}{j(d-j)}}.
\end{aligned}$$

Combining the two bounds gives the desired result. □

Lemma 14. *For any $j > i > 0$ and $d > j + i$, we have*

$$\int_{\frac{j}{d}}^{\frac{j+i}{d}} q^j(1-q)^{d-j}\,\mathrm{d}q \ge \left(\frac{j}{d}\right)^j\left(\frac{d-j}{d}\right)^{d-j}\frac{j(d-j-i)}{id^2}\left(1-\exp\left(\frac{-i^2d}{j(d-j-i)}\right)\right), \tag{133}$$

$$\int_{\frac{j-i}{d}}^{\frac{j}{d}} q^j(1-q)^{d-j}\,\mathrm{d}q \ge \left(\frac{j}{d}\right)^j\left(\frac{d-j}{d}\right)^{d-j}\frac{(j-i)(d-j)}{id^2}\left(1-\exp\left(\frac{-i^2d}{(j-i)(d-j)}\right)\right). \tag{134}$$

Proof. We first prove (133). Define

$$\varphi(x) := j\ln(j+xd) + (d-j)\ln(d-j-xd), \quad x \in \left[-\frac{i}{d}, \frac{i}{d}\right]. \tag{135}$$

Taking the derivative of $\varphi(x)$, we obtain that

$$\varphi'(x) = \frac{-xd^3}{(j+xd)(d-j-xd)} \ge \frac{-xd^3}{j(d-j-i)} \ge \frac{-id^2}{j(d-j-i)},\ \forall x \in \left[0, \frac{i}{d}\right].$$

This implies that

$$\varphi(t) - \varphi(0) = \int_0^t \varphi'(x)\,\mathrm{d}x \ge \int_0^t \frac{-id^2}{j(d-j-i)}\,\mathrm{d}x = \frac{-id^2}{j(d-j-i)}t,\ \forall t \in \left[0, \frac{i}{d}\right]. \tag{136}$$

By the definition of φ in (135), we have

$$\varphi(t) - \varphi(0) = \ln\left(\left(\frac{j+td}{j}\right)^j \left(\frac{d-j-td}{d-j}\right)^{d-j}\right),\ \forall t \in \left[-\frac{i}{d}, \frac{i}{d}\right]. \tag{137}$$

It follows that

$$\begin{aligned}
\int_{\frac{j}{d}}^{\frac{j+i}{d}} q^j(1-q)^{d-j}\,\mathrm{d}q &= \int_0^{\frac{i}{d}} \left(\frac{j+td}{d}\right)^j \left(\frac{d-j-td}{d}\right)^{d-j} \mathrm{d}t \\
&= \int_0^{\frac{i}{d}} \left(\frac{j}{d}\right)^j \left(\frac{d-j}{d}\right)^{d-j} \left(\frac{j+td}{j}\right)^j \left(\frac{d-j-td}{d-j}\right)^{d-j} \mathrm{d}t \\
&= \left(\frac{j}{d}\right)^j \left(\frac{d-j}{d}\right)^{d-j} \int_0^{\frac{i}{d}} \exp(\varphi(t)-\varphi(0))\,\mathrm{d}t \\
&\geq \left(\frac{j}{d}\right)^j \left(\frac{d-j}{d}\right)^{d-j} \int_0^{\frac{i}{d}} \exp\left(\frac{-id^2}{j(d-j-i)}t\right) \mathrm{d}t \\
&= \left(\frac{j}{d}\right)^j \left(\frac{d-j}{d}\right)^{d-j} \frac{j(d-j-i)}{id^2}\left(1-\exp\left(\frac{-i^2d}{j(d-j-i)}\right)\right),
\end{aligned}$$

where the first line follows by setting q to equal $t + \frac{j}{d}$ for some t; the third line follows from (137); the fourth line follows from (136). This proves the desired inequality (133).

Next, we prove (134) by a similar argument. We see that

$$\varphi'(x) = \frac{-xd^3}{(j+xd)(d-j-xd)} \leq \frac{id^2}{(j-i)(d-j)},\ \forall x \in \left[-\frac{i}{d}, 0\right].$$

This implies that

$$\varphi(0) - \varphi(t) = \int_t^0 \varphi'(x)\,\mathrm{d}x \leq \int_t^0 \frac{id^2}{(j-i)(d-j)}\,\mathrm{d}x = -\frac{id^2}{(j-i)(d-j)}t,\ \forall t \in \left[-\frac{i}{d}, 0\right].$$

Then we can deduce that

$$\begin{aligned}
\int_{\frac{j-i}{d}}^{\frac{j}{d}} q^j(1-q)^{d-j}\,\mathrm{d}q &= \int_{-\frac{i}{d}}^0 \left(\frac{j+td}{d}\right)^j \left(\frac{d-j-td}{d}\right)^{d-j} \mathrm{d}t \\
&= \int_{-\frac{i}{d}}^0 \left(\frac{j}{d}\right)^j \left(\frac{d-j}{d}\right)^{d-j} \left(\frac{j+td}{j}\right)^j \left(\frac{d-j-td}{d-j}\right)^{d-j} \mathrm{d}t \\
&= \left(\frac{j}{d}\right)^j \left(\frac{d-j}{d}\right)^{d-j} \int_{-\frac{i}{d}}^0 \exp(\varphi(t)-\varphi(0))\,\mathrm{d}t \\
&\geq \left(\frac{j}{d}\right)^j \left(\frac{d-j}{d}\right)^{d-j} \int_{-\frac{i}{d}}^0 \exp\left(\frac{id^2}{(j-i)(d-j)}t\right) \mathrm{d}t \\
&= \left(\frac{j}{d}\right)^j \left(\frac{d-j}{d}\right)^{d-j} \frac{(j-i)(d-j)}{id^2}\left(1-\exp\left(\frac{-i^2d}{(j-i)(d-j)}\right)\right),
\end{aligned}$$

which establishes the inequality (134). □

Lemma 15. *Let $L', U' \in \{1, \ldots, d-1\}$ with $d \geq 3$ and $L' < U'$, we have that for all $j \in [L', U']$,*

$$\int_{\frac{L'}{d}}^{\frac{U'}{d}} q^j(1-q)^{d-j}\,\mathrm{d}q \geq \left(\frac{j}{d}\right)^j \left(\frac{d-j}{d}\right)^{d-j} \frac{\alpha}{2d},$$

where $\alpha := \frac{1}{2}\min\left\{U'-L', \sqrt{L'}, \sqrt{d-U'}\right\}$.

Proof. We split the proof into the following two cases, depending on whether j is in the range $j \in \left[L', \frac{L'+U'}{2}\right]$, or in the range $j \in \left(\frac{L'+U'}{2}, U'\right]$.

Case i): $L' \le j \le \frac{U'+L'}{2}$. It follows that $j+\alpha \le U' < d$ since $\alpha \le \frac{U'-L'}{2}$ by definition. We also have $j > \alpha > 0$ since $L' > \alpha$ by definition. Thus $j, d, i = \alpha$ satisfy the premise of Lemma 14. Using the inequality (133) with $i = \alpha$, we obtain

$$\begin{aligned}\int_{\frac{L'}{d}}^{\frac{U'}{d}} q^j(1-q)^{d-j}\,\mathrm{d}q &\ge \int_{\frac{j}{d}}^{\frac{j+\alpha}{d}} q^j(1-q)^{d-j}\,\mathrm{d}q \\ &\ge \left(\frac{j}{d}\right)^j \left(\frac{d-j}{d}\right)^{d-j} \frac{j(d-j-\alpha)}{\alpha d^2}\left(1-\exp\left(\frac{-\alpha^2 d}{j(d-j-\alpha)}\right)\right). \end{aligned} \tag{138}$$

Using the fact that

$$1-e^{-x} \ge \frac{1}{2}x(2-x),\ \forall x \ge 0, \tag{139}$$

we have

$$\begin{aligned}\frac{j(d-j-\alpha)}{\alpha d^2}\left(1-\exp\left(\frac{-\alpha^2 d}{j(d-j-\alpha)}\right)\right) &\ge \frac{j(d-j-\alpha)}{\alpha d^2} \times \frac{1}{2}\frac{\alpha^2 d}{j(d-j-\alpha)}\left(2-\frac{\alpha^2 d}{j(d-j-\alpha)}\right) \\ &= \frac{\alpha}{2d}\left(2-\frac{\alpha^2 d}{j(d-j-\alpha)}\right). \end{aligned} \tag{140}$$

Next, we argue that $\frac{\alpha^2 d}{j(d-j-\alpha)} \le 1$. This is done by dividing into the following two sub-cases:

- $\underline{j < \frac{d}{2}}$:

$$\frac{\alpha^2 d}{j(d-j-\alpha)} \le \frac{\left(\frac{\sqrt{L'}}{2}\right)^2 d}{j\left(d-j-\frac{\sqrt{d-2}}{2}\right)} \le \frac{\left(\frac{\sqrt{L'}}{2}\right)^2 d}{L'\left(\frac{d}{2}-\frac{\sqrt{d-2}}{2}\right)} = \frac{d}{2\left(d-\sqrt{d-2}\right)} \le 1,$$

  where the first inequality follows from the definition that $\alpha \le \frac{\sqrt{L'}}{2} \le \frac{\sqrt{d-2}}{2}$; the second inequality follows from the fact that $L' \le j < \frac{d}{2}$; the last inequality follows from the assumption that $d \ge 3$.

- $\underline{j \ge \frac{d}{2}}$:

$$\frac{\alpha^2 d}{j(d-j-\alpha)} \le \frac{\alpha^2 d}{\frac{d}{2}(d-U')} \le \frac{\left(\frac{\sqrt{d-U'}}{2}\right)^2 d}{\frac{d}{2}(d-U')} = \frac{1}{2} \le 1,$$

  where the first inequality is because $j \ge \frac{d}{2}$ and $j+\alpha \le U'$ as argued above; the second inequality is because $\alpha \le \frac{\sqrt{d-U'}}{2}$ by definition.

Using this observation along with (138) and (140), we conclude that

$$\int_{\frac{L'}{d}}^{\frac{U'}{d}} q^j(1-q)^{d-j}\,\mathrm{d}q \ge \left(\frac{j}{d}\right)^j \left(\frac{d-j}{d}\right)^{d-j} \frac{\alpha}{2d}.$$

Case ii): $\frac{U'+L'}{2} < j \le U'$. This case can be proved in a similar manner as the above one. Note that $j-\alpha \ge L' > 0$ since $\alpha \le \frac{U'-L'}{2}$ by definition. We also have $j+\alpha < d$ since $\alpha < d-U'$. Hence $j, d, i = \alpha$ satisfy the premise of Lemma 14. Using the inequality (134) with $i = \alpha$, we have

$$\begin{aligned}\int_{\frac{L'}{d}}^{\frac{U'}{d}} q^j(1-q)^{d-j}\,\mathrm{d}q &\ge \int_{\frac{j-\alpha}{d}}^{\frac{j}{d}} q^j(1-q)^{d-j}\,\mathrm{d}q \\ &\ge \left(\frac{j}{d}\right)^j \left(\frac{d-j}{d}\right)^{d-j} \frac{(j-\alpha)(d-j)}{\alpha d^2}\left(1-\exp\left(\frac{-\alpha^2 d}{(j-\alpha)(d-j)}\right)\right). \end{aligned}$$

Applying the standard identity (139) again, we see that

$$\frac{(j-\alpha)(d-j)}{\alpha d^2}\left(1-\exp\left(\frac{-\alpha^2 d}{(j-\alpha)(d-j)}\right)\right) \geq \frac{(j-\alpha)(d-j)}{\alpha d^2} \times \frac{1}{2}\frac{\alpha^2 d}{(j-\alpha)(d-j)}\left(2-\frac{\alpha^2 d}{(j-\alpha)(d-j)}\right)$$
$$= \frac{\alpha}{2d}\left(2-\frac{\alpha^2 d}{(j-\alpha)(d-j)}\right).$$

Similar to the above case, we prove $\frac{\alpha^2 d}{(j-\alpha)(d-j)} \leq 1$ by considering the following two sub-cases:

- $\underline{j < \frac{d}{2}}$:

$$\frac{\alpha^2 d}{(j-\alpha)(d-j)} \leq \frac{\alpha^2 d}{L'\frac{d}{2}} \leq \frac{\left(\frac{\sqrt{L'}}{2}\right)^2 d}{L'\frac{d}{2}} = \frac{1}{2} \leq 1,$$

  where the first inequality follows by noting that $j < \frac{d}{2}$ and $j-\alpha \geq L'$ as argued above; the second inequality follows from the fact that $\alpha \leq \frac{\sqrt{L'}}{2}$.

- $\underline{j \geq \frac{d}{2}}$:

$$\frac{\alpha^2 d}{(j-\alpha)(d-j)} \leq \frac{\alpha^2 d}{\left(\frac{d}{2}-\alpha\right)(d-U')} \leq \frac{\left(\frac{\sqrt{d-U'}}{2}\right)^2 d}{\left(\frac{d}{2}-\frac{\sqrt{d-2}}{2}\right)(d-U')} = \frac{d}{2\left(d-\sqrt{d-2}\right)} \leq 1,$$

  where the first inequality is because $\frac{d}{2} \leq j \leq U'$; the second inequality follows since $\alpha \leq \frac{\sqrt{d-U'}}{2} \leq \frac{\sqrt{d-2}}{2}$ by its definition; and the last inequality follows from $d \geq 3$.

It follows that

$$\int_{\frac{L'}{d}}^{\frac{U'}{d}} q^j(1-q)^{d-j}\,\mathrm{d}q \geq \left(\frac{j}{d}\right)^j\left(\frac{d-j}{d}\right)^{d-j}\frac{\alpha}{2d}.$$

Summarizing the two cases, Lemma 15 is proved. □

Using the above results, we are now in a position to prove Lemma 9. Recalling from (53) that

$$\Delta(q) = \sum_{j=0}^{d-1}\binom{d-1}{j}q^j(1-q)^{d-j}(f(j+1)-f(j)).$$

Note that $\Delta(q)$ is continuous w.r.t. q. Assuming $L', U' \in \{1,\ldots,d-1\}$ with $L' < U'$ and $f(L') < f(U')$, we can

calculate the integral of $\Delta(q)$ for $q \in \left[\frac{L'}{d}, \frac{U'}{d}\right]$ as follows:

$$\begin{aligned}
\int_{\frac{L'}{d}}^{\frac{U'}{d}} \Delta(q)\,\mathrm{d}q &= \int_{\frac{L'}{d}}^{\frac{U'}{d}} \sum_{j=0}^{d-1} \binom{d-1}{j} q^j (1-q)^{d-j} (f(j+1)-f(j))\,\mathrm{d}q \\
&\geq \int_{\frac{L'}{d}}^{\frac{U'}{d}} \sum_{j=L'}^{U'-1} \binom{d-1}{j} q^j (1-q)^{d-j} (f(j+1)-f(j))\,\mathrm{d}q \\
&= \sum_{j=L'}^{U'-1} \frac{d-j}{d} \binom{d}{j} (f(j+1)-f(j)) \int_{\frac{L'}{d}}^{\frac{U'}{d}} q^j (1-q)^{d-j}\,\mathrm{d}q \\
&\geq \sum_{j=L'}^{U'-1} \frac{d-j}{d} \binom{d}{j} (f(j+1)-f(j)) \left(\frac{j}{d}\right)^j \left(\frac{d-j}{d}\right)^{d-j} \frac{\alpha}{2d} \qquad (141) \\
&\geq \sum_{j=L'}^{U'-1} \frac{\sqrt{2\pi}}{e^2} \sqrt{\frac{d}{j(d-j)}} \frac{d-j}{d} (f(j+1)-f(j)) \frac{\alpha}{2d} \qquad (142) \\
&= \sum_{j=L'}^{U'-1} \sqrt{\frac{\pi\alpha^2(d-j)}{2e^4 j d^3}} (f(j+1)-f(j)) \\
&\geq \sum_{j=L'}^{U'-1} \sqrt{\frac{\pi\alpha^2(d-U')}{2e^4 U' d^3}} (f(j+1)-f(j)) \\
&= \sqrt{\frac{\pi\alpha^2(d-U')}{2e^4 U' d^3}} (f(U')-f(L')), \qquad (143)
\end{aligned}$$

where (141) follows from Lemma 15 and $\alpha = \frac{1}{2}\min\left\{U'-L', \sqrt{L'}, \sqrt{d-U'}\right\}$; (142) follows from Lemma 13. By the mean value theorem, from (143), we know there exists some $q_0 \in \left(\frac{L'}{d}, \frac{U'}{d}\right)$ such that

$$\Delta(q_0) \geq \frac{\sqrt{\frac{\pi\alpha^2(d-U')}{2e^4 U' d^3}} (f(U')-f(L'))}{\frac{U'}{d}-\frac{L'}{d}} = \sqrt{\frac{\pi\alpha^2(d-U')}{2e^4 U' d}} \frac{f(U')-f(L')}{U'-L'}.$$

Using this observation, we can bound $\hat{\Gamma}(q_0)$ in (14) as

$$\begin{aligned}
\hat{\Gamma}(q_0) = \frac{36.06(1-q_0)}{q_0(\Delta(q_0))^2} \log\left(\frac{2n}{\varepsilon}\right) &\leq \frac{36.06(1-q_0)}{q_0} \times \frac{2e^4 U' d}{\pi\alpha^2(d-U')} \left(\frac{U'-L'}{f(U')-f(L')}\right)^2 \log\left(\frac{2n}{\varepsilon}\right) \\
&\leq 1253.39 \times \frac{(d-L')U'}{\alpha^2(d-U')L'} \left(\frac{U'-L'}{f(U')-f(L')}\right)^2 d \log\left(\frac{2n}{\varepsilon}\right),
\end{aligned}$$

which proves Lemma 9.

H Proof of Lemma 7

Suppose to the contrary that $q^* \in \left(0, \frac{1}{376017d^3}\right] \cup \left[1 - \frac{1}{376017d^3}, 1\right)$. From (53) we can bound

$$\begin{aligned}
\frac{q^*}{1-q^*}\left(\Delta(q^*)\right)^2 &= \left(\sum_{j=0}^{d-1}\binom{d-1}{j}q^{*j}(1-q^*)^{d-j-1}(f(j+1)-f(j))\right)^2 \cdot q^*(1-q^*) \\
&\leq \left(\sum_{j=0}^{d-1}\binom{d-1}{j}q^{*j}(1-q^*)^{d-j-1}\left(f(d)-f(0)\right)\right)^2 \cdot q^*(1-q^*) \\
&= \left(f(d)-f(0)\right)^2 \cdot q^*(1-q^*) \\
&\leq \left(f(d)-f(0)\right)^2 \times \frac{1}{376017d^3}\left(1-\frac{1}{376017d^3}\right) \\
&\leq \left(f(d)-f(0)\right)^2 \times \frac{1}{376017d^3}.
\end{aligned}$$

This along with the definition of $\hat{\Gamma}(q)$ in (14) yields that

$$\hat{\Gamma}(q^*) \geq 36.06 \times \frac{376017d^3}{\left(f(d)-f(0)\right)^2}\log\left(\frac{2n}{\varepsilon}\right). \tag{144}$$

On the other hand, applying Proposition 3 with $L = 0$ and $U = d$, we have that $\exists q_0 \in (0,1)$ such that

$$\hat{\Gamma}(q_0) \leq \frac{376017d^3}{\left(f(d)-f(0)\right)^2}\log\left(\frac{2n}{\varepsilon}\right). \tag{145}$$

From (144) and (145) we have that

$$\hat{\Gamma}(q^*) > \hat{\Gamma}(q_0),$$

which is a contradiction to the definition that $q^* = \operatorname{argmin}_{q^* \in (0,1)} \hat{\Gamma}(q)$ in (15). Hence we prove Lemma 7.

I Proof of Lemma 8

For notational simplicity, let $\varsigma = \frac{1}{376017d^4}$. It follows from Lemma 7 that

$$0 < \frac{\varsigma}{q^*} < \frac{1}{d} \text{ and } 0 < \frac{\varsigma}{1-q^*} < \frac{1}{d}. \tag{146}$$

For any $\hat{q}^* \in [q^* - \varsigma, q^* + \varsigma]$, we have from (53) that

$$\begin{aligned}
&\frac{\hat{q}^*}{1-\hat{q}^*}(\Delta(\hat{q}^*))^2 \\
&= \left(\sum_{j=0}^{d-1}\binom{d-1}{j}\hat{q}^{*j}(1-\hat{q}^*)^{d-j-1}(f(j+1)-f(j))\right)^2 \cdot \hat{q}^*(1-\hat{q}^*) \\
&\geq \left(\sum_{j=0}^{d-1}\binom{d-1}{j}(q^*-\varsigma)^j(1-q^*-\varsigma)^{d-j-1}(f(j+1)-f(j))\right)^2 \cdot (q^*-\varsigma)(1-q^*-\varsigma) \\
&= \left(\sum_{j=0}^{d-1}\binom{d-1}{j}q^{*j}\left(\frac{q^*-\varsigma}{q^*}\right)^j(1-q^*)^{d-j-1}\left(\frac{1-q^*-\varsigma}{1-q^*}\right)^{d-j-1}(f(j+1)-f(j))\right)^2 \cdot (q^*-\varsigma)(1-\hat{q}^*-\varsigma) \\
&\geq \left(\sum_{j=0}^{d-1}\binom{d-1}{j}q^{*j}\left(\frac{q^*-\varsigma}{q^*}\right)^{d-1}(1-q^*)^{d-j-1}\left(\frac{1-q^*-\varsigma}{1-q^*}\right)^{d-1}(f(j+1)-f(j))\right)^2 \cdot (q^*-\varsigma)(1-\hat{q}^*-\varsigma) \\
&= \left(\sum_{j=0}^{d-1}\binom{d-1}{j}q^{*j}(1-q^*)^{d-j-1}(f(j+1)-f(j))\right)^2 \cdot q^*(1-q^*)\cdot\left(\frac{q^*-\varsigma}{q^*}\right)^{2d-1}\left(\frac{1-q^*-\varsigma}{1-q^*}\right)^{2d-1} \\
&\geq \left(\sum_{j=0}^{d-1}\binom{d-1}{j}q^{*j}(1-q^*)^{d-j-1}(f(j+1)-f(j))\right)^2 \cdot q^*(1-q^*)\cdot\left(1-\frac{1}{d}\right)^{2d-1}\left(1-\frac{1}{d}\right)^{2d-1} \\
&\geq \left(\sum_{j=0}^{d-1}\binom{d-1}{j}q^{*j}(1-q^*)^{d-j-1}(f(j+1)-f(j))\right)^2 \times q^*(1-q^*)\times\frac{1}{8}\times\frac{1}{8} \\
&= \frac{1}{64}\times\frac{q^*(\Delta(q^*))^2}{1-q^*}.
\end{aligned} \tag{147}$$

Using (147) along with the definition of $\hat{\Gamma}(q)$ in (14), we have

$$\hat{\Gamma}(\hat{q}^*) \leq 64\hat{\Gamma}(q^*). \tag{148}$$

For any $\hat{q}^* \in [q^* - \varsigma, q^* + \varsigma]$, we also have

$$\begin{aligned}
P(+,\hat{q}^*) &= \sum_{j=0}^{d-1}\binom{d-1}{j}\hat{q}^{*j}(1-\hat{q}^*)^{d-1-j}f(j+1) \\
&\leq \sum_{j=0}^{d-1}\binom{d-1}{j}(q^*+\varsigma)^j(1-q^*+\varsigma)^{d-1-j}f(j+1) \\
&\leq \sum_{j=0}^{d-1}\binom{d-1}{j}q^{*j}(1-q^*)^{d-1-j}f(j+1)\cdot\left(\frac{q^*+\varsigma}{q^*}\right)^{d-1}\left(\frac{1-q^*+\varsigma}{1-q^*}\right)^{d-1} \\
&\leq \sum_{j=0}^{d-1}\binom{d-1}{j}q^{*j}(1-q^*)^{d-1-j}f(j+1)\cdot\left(1+\frac{1}{d}\right)^{d-1}\left(1+\frac{1}{d}\right)^{d-1} \\
&\leq \sum_{j=0}^{d-1}\binom{d-1}{j}q^{*j}(1-q^*)^{d-1-j}f(j+1)\cdot e^2 \\
&= e^2 P(+,q^*).
\end{aligned} \tag{149}$$

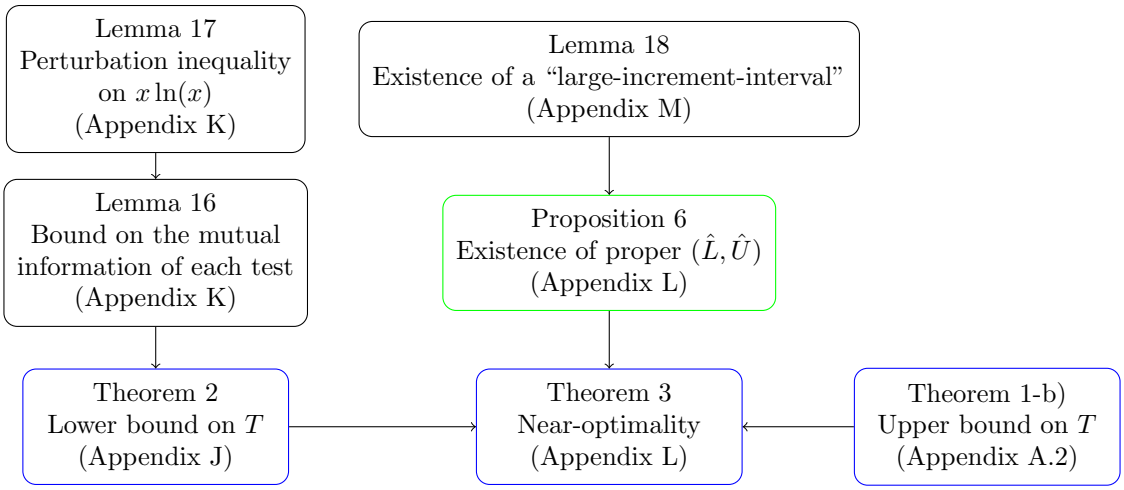


Figure 3: Organization of Propositions, Lemmas, and Theorems for our proof of converse and its tightness.

And similarly,

$$\begin{aligned}
1-Q(+,\hat{q}^*) &= \sum_{j=0}^{d-1}\binom{d-1}{j}\hat{q}^{*j}(1-\hat{q}^*)^{d-1-j}(1-f(j)) \\
&\le \sum_{j=0}^{d-1}\binom{d-1}{j}q^{*j}(1-q^*)^{d-1-j}(1-f(j))\cdot\left(\frac{q^*+\varsigma}{q^*}\right)^{d-1}\left(\frac{1-q^*+\varsigma}{1-q^*}\right)^{d-1} \\
&\le \sum_{j=0}^{d-1}\binom{d-1}{j}q^{*j}(1-q^*)^{d-1-j}(1-f(j))\cdot\left(1+\frac{1}{d}\right)^{d-1}\left(1+\frac{1}{d}\right)^{d-1} \\
&\le \sum_{j=0}^{d-1}\binom{d-1}{j}q^{*j}(1-q^*)^{d-1-j}(1-f(j))\cdot e^2 \\
&= e^2(1-Q(+,q^*)). \qquad (150)
\end{aligned}$$

Combining (149) and (150), along with the definition of $P_{\min}(q)$ in (7), we have that

$$P_{min}(\hat{q}^*) \le e^2 P_{min}(q^*). \qquad (151)$$

Finally, using (148) and (151) along with (14) implies that

$$\Gamma(\hat{q}^*) = \hat{\Gamma}(\hat{q}^*)P_{min}(\hat{q}^*) \le 64\hat{\Gamma}(q^*)e^2 P_{min}(q^*) = 64e^2\Gamma(q^*),$$

which completes the proof.

J Proof of Theorem 2

In this section, for any given monotone test function $f(\cdot)$, we provide an information-theoretic lower bound on the number of tests required by *any* non-adaptive group testing algorithm that can be adaptive and is allowed to make an error with probability at most ε.

Let us first introduce some notation which will be used in the proof. We use a binary vector $\boldsymbol{X} \in \{0,1\}^n$ to represent the set $\mathcal{N}$, where 1s indicate which items are defective. To estimate $\boldsymbol{X}$, we perform T suitable-designed tests, in which each test must be designed prior to observing any outcomes. Let $\boldsymbol{Z} = (Z_1,\ldots,Z_T)$ be a length T vector, where Z_i denotes the number of defectives in the i-th test. The test outcomes are represented by a binary vector $\boldsymbol{Y} = (Y_1,\ldots,Y_T) \in \{0,1\}^T$, where $Y_i = 1$ indicates the outcome of the i-th test is positive. We emphasize that Z_i is independent of $(Y_1,\ldots,Y_{i-1},Y_{i+1},\ldots,Y_T)$. Given the tests and their outcomes, let $\hat{\boldsymbol{X}}$ be an estimate of $\boldsymbol{X}$.

By standard information-theoretic definitions, we have

$$\begin{aligned} H(\boldsymbol{X}) &= H(\boldsymbol{X}|\boldsymbol{Y}) + I(\boldsymbol{X};\boldsymbol{Y}) \\ &= H(\boldsymbol{X}|\boldsymbol{Y},\hat{\boldsymbol{X}}) + I(\boldsymbol{X};\boldsymbol{Y}) \\ &\leq H(\boldsymbol{X}|\hat{\boldsymbol{X}}) + I(\boldsymbol{X};\boldsymbol{Y}) \end{aligned} \tag{152}$$

where the second line follows since $\hat{\boldsymbol{X}}$ is a function of $\boldsymbol{Y}$; the thrid line follows from the fact that conditioning reduces entropy. Since the defective set $\mathcal{D}$ is uniformly distributed over all length n vector of Hamming weight d, we have

$$H(\boldsymbol{X}) = \log \binom{n}{d}. \tag{153}$$

By Fano's inequality,

$$H(\boldsymbol{X}|\hat{\boldsymbol{X}}) \leq 1 + \varepsilon \log \binom{n}{d}. \tag{154}$$

Let $Y^{i-1} := (Y_1, \ldots, Y_{i-1})$ and $Z^{i-1} := (Z_1, \ldots, Z_{i-1})$.[7] Similar to channel coding (see for example [Yeung, 2008, Sec. 7.3]), it can be easily verified that

$$(\boldsymbol{X}, Z^{i-1}, Y^{i-1}) - Z_i - Y_i$$

which implies

$$(\boldsymbol{X}, Y^{i-1}) - Z_i - Y_i. \tag{155}$$

Following a standard set of inequalities we have

$$\begin{aligned} I(\boldsymbol{X};\boldsymbol{Y}) &= \sum_{i=1}^{T} \left[H(Y_i|Y^{i-1}) - H(Y_i|\boldsymbol{X}, Y^{i-1})\right] \\ &\leq \sum_{i=1}^{T} \left[H(Y_i) - H(Y_i|\boldsymbol{X}, Y^{i-1})\right] \\ &\leq \sum_{i=1}^{T} \left[H(Y_i) - H(Y_i|\boldsymbol{X}, Y^{i-1}, Z_i)\right] \\ &= \sum_{i=1}^{T} \left[H(Y_i) - H(Y_i|Z_i)\right] \end{aligned} \tag{156}$$

where the first line follows from chain rule; the second and third lines follow from the fact that conditioning reduces entropy; the last line follows from (155).

Let χ_i denote the pool-size of the i-th test and $\Pr(Z_i = a)$ denote the probability that $Z_i = a$. We have

$$\Pr(Z_i = a) = \frac{\binom{d}{a}\binom{n-d}{\chi_i - a}}{\binom{n}{\chi_i}}. \tag{157}$$

For simplicity, we define

$$\begin{aligned} \mu(\chi_i) &\coloneqq \sum_{a=0}^{d} \Pr(Z_i = a) f(a), \\ \sigma^2(\chi_i) &\coloneqq \sum_{a=0}^{d} \Pr(Z_i = a)(f(a) - \mu(\chi_i))^2, \end{aligned} \tag{158}$$

where $\mu(\chi_i)$ and $\sigma^2(\chi_i)$ denote the mean and variance of $\Pr(Y_i = 1|Z_i)$. It turns out we are able to bound the bracketed term $[\cdot]$ in (156) as follows:

[7] For $i = 1$, we follow the convention that $Y^{i-1} = Z^{i-1} = \emptyset$.

Lemma 16.

$$H(Y_i) - H(Y_i|Z_i) \leq \frac{\sigma^2(\chi_i)\log e}{\mu(\chi_i)(1-\mu(\chi_i))} \tag{159}$$

Proof. See Appendix K. □

Now substituting (159) into (156), we see that

$$\begin{aligned} I(\boldsymbol{X};\boldsymbol{Y}) &\leq \sum_{i=1}^{T} \frac{\sigma^2(\chi_i)\log e}{\mu(\chi_i)(1-\mu(\chi_i))} \\ &\leq T \times \frac{\sigma^2(\chi^*)\log e}{\mu(\chi^*)(1-\mu(\chi^*))}, \end{aligned} \tag{160}$$

where the second line follows by defining

$$\chi^* := \underset{\chi\in\{1,\ldots,n-1\}}{\operatorname{argmax}} \frac{\sigma^2(\chi)}{\mu(\chi)(1-\mu(\chi))}. \tag{161}$$

The reason for restricting $\chi \in \{1,\ldots,n-1\}$ is that $\sigma^2(0) = \sigma^2(n) = 0$.

Finally, combining (152), (153), (154) and (160) gives us the desired result

$$T \geq \frac{\mu(\chi^*)\,(1-\mu(\chi^*))}{\sigma^2(\chi^*)\log e}\left((1-\varepsilon)\log\binom{n}{d} - 1\right). \tag{162}$$

This along with the definition of $h(f)$ in (24) completes the proof of Theorem 2.

K Proof of Lemma 16

The proof of Lemma 16 will resort to the following technical lemma:

Lemma 17. *For any $b \in (0,1)$ and $c \in (-b, 1-b)$, it follows that*

$$-b\ln b + (b+c)\ln(b+c) \leq c(1+\ln b) + \frac{c^2}{b}.$$

Proof. Since $b + c > 0$, $\frac{c}{b} > -1$, we have

$$\begin{aligned} 0 &\leq (b+c)\left(\frac{c}{b} - \ln\left(1+\frac{c}{b}\right)\right) \\ &= c + \frac{c^2}{b} - (b+c)\ln(b+c) + (b+c)\ln b, \end{aligned}$$

which, via simple rearrangement, gives the promised inequality. □

We now set out to prove Lemma 16. First, we have

$$\begin{aligned} H(Y_i) - H(Y_i|Z_i) &= H(Y_i) - \sum_{a=0}^{d} \Pr(Z_i = a) H(Y_i|Z_i = a) \\ &= \sum_{a=0}^{d} \Pr(Z_i = a)\left[H(Y_i) - H(Y_i|Z_i = a)\right] \end{aligned} \tag{163}$$

For the sake of notational brevity, let $\mu = \mu(\chi_i)$ and $\sigma^2 = \sigma^2(\chi_i)$. Since

$$\Pr(Y_i = 1|Z_i = a) = f(a),$$

$$\Pr(Y_i = 1) = \sum_{a=0}^{d} \Pr(Z_i = a) \Pr(Y_i = 1 | Z_i = a) = \sum_{a=0}^{d} \Pr(Z_i = a) f(a) = \mu,$$

we have

$$\begin{aligned} H(Y_i) &= -\mu \log \mu - (1-\mu) \log(1-\mu) \\ &= [-\mu \ln \mu - (1-\mu) \ln(1-\mu)] \log e, \\ H(Y_i | Z_i = a) &= -f(a) \log f(a) - (1-f(a)) \log(1-f(a)) \\ &= [-f(a) \ln f(a) - (1-f(a)) \ln(1-f(a))] \log e. \end{aligned} \tag{164}$$

Next, we argue that

$$-\mu \ln \mu - (1-\mu) \ln(1-\mu) + f(a) \ln f(a) + (1-f(a)) \ln(1-f(a)) \leq (f(a)-\mu)(\ln \mu - \ln(1-\mu)) + \frac{(f(a)-\mu)^2}{\mu(1-\mu)}. \tag{165}$$

This is done for each of the following possible cases.

- When $f(a) = 0$,
$$\text{L.H.S.} - \text{R.H.S.} = 1 - \frac{1}{1-\mu} - \ln(1-\mu) \leq 0, \quad \forall\, 0 < \mu < 1.$$
- When $f(a) = 1$,
$$\text{L.H.S.} - \text{R.H.S.} = 1 - \frac{1}{\mu} - \ln \mu \leq 0, \quad \forall\, 0 < \mu < 1.$$
- When $f(a) \in (0,1)$, applying Lemma 17 with $b = \mu$ and $c = f(a) - \mu$ we obtain
$$-\mu \ln \mu + f(a) \ln f(a) \leq (f(a)-\mu)(1 + \ln \mu) + \frac{(f(a)-\mu)^2}{\mu}.$$
Applying Lemma 17 again with $b = 1-\mu$ and $c = \mu - f(a)$, we obtain
$$-(1-\mu) \ln(1-\mu) + (1-f(a)) \ln(1-f(a)) \leq (\mu - f(a))(1 + \ln(1-\mu)) + \frac{(f(a)-\mu)^2}{1-\mu}.$$
Upon combining the above two inequalities, we have L.H.S. $\leq$ R.H.S. as desired.

Substituting (164) and (165) into (163), we arrive at

$$\begin{aligned} H(Y_i) - H(Y_i|Z_i) &\leq \sum_{a=0}^{d} \Pr(Z_i = a) \left[(f(a)-\mu)(\ln \mu - \ln(1-\mu)) + \frac{(f(a)-\mu)^2}{\mu(1-\mu)} \right] \log e \\ &= \frac{\sigma^2 \log e}{\mu(1-\mu)} \end{aligned}$$

where the equality follows from (158). This proves Lemma 16.

L Proof of Theorem 3

In this section, we argue that the upper bound in (21) given by the proposed testing algorithm is at most a $\mathcal{O}\left(\frac{P_{min}(q^*)}{\mu(\chi^*)(1-\mu(\chi^*))}\right)$ factor larger than the lower bound in (25).

Before presenting the proof, let us give some technical results that constitute the basic ingredients of the proof. To proceed, recall the definitions of $\mu(\chi), \sigma^2(\chi)$ in (23) and χ^* in (28), which we repeat here for convenience:

$$\begin{aligned}\chi^* &\coloneqq \underset{\chi\in\{1,\ldots,n-1\}}{\operatorname{argmin}} \frac{\mu(\chi)(1-\mu(\chi))}{\sigma^2(\chi)},\\ \mu(\chi) &\coloneqq \sum_{i=0}^{d} \frac{\binom{d}{i}\binom{n-d}{\chi-i}}{\binom{n}{\chi}} f(i),\\ \sigma^2(\chi) &\coloneqq \sum_{i=0}^{d} \frac{\binom{d}{i}\binom{n-d}{\chi-i}}{\binom{n}{\chi}} \left(f(i)-\mu(\chi)\right)^2.\end{aligned} \tag{166}$$

Define

$$\vartheta := \chi^* \frac{d}{n}, \tag{167}$$

$$\eta := \begin{cases} \lfloor \vartheta \rfloor & \text{if } \vartheta - \lfloor \vartheta \rfloor < 0.5,\\ \lceil \vartheta \rceil & \text{if } \vartheta - \lfloor \vartheta \rfloor \geq 0.5. \end{cases} \tag{168}$$

Since $0 < \chi^* < n$, we have $\vartheta \in (0, d)$.

Lemma 18. *$\exists\, \kappa \in \{0, 1, \cdots, d-1, d\} \backslash \{\eta\}$ such that*

$$\left(\gamma(\kappa)\frac{f(\kappa)-f(\eta)}{\kappa-\vartheta}\right)^2 > \frac{\sigma^2(\chi^*)}{11}, \tag{169}$$

where $\gamma(\kappa) := \min\left\{|\kappa-\vartheta|, \sqrt{\kappa+1}, \sqrt{d-\kappa+1}, \sqrt{\vartheta+1}, \sqrt{d-\vartheta+1}\right\}$.

Proof. See Appendix M. □

The following proposition plays a key role in the proof of Theorem 3.

Proposition 6. *$\exists\, \hat{L}, \hat{U} \in \{0, \ldots, d\}$ with $\hat{L} < \hat{U}$ such that*

$$\left(\beta\frac{f(\hat{U})-f(\hat{L})}{\hat{U}-\hat{L}}\right)^2 \geq \frac{\sigma^2(\chi^*)}{176}, \tag{170}$$

where $\beta := \min\left\{\hat{U}-\hat{L}, \sqrt{\hat{L}+1}, \sqrt{d-\hat{U}+1}\right\}$ and $\sigma^2(\chi^*)$ is defined in (166).

Proof. Using κ in Lemma 18, we construct a pair of $(\hat{L}, \hat{U})$ that satisfies (170). Set

$$\hat{L} := \min\{\kappa, \eta\}, \quad \hat{U} := \max\{\kappa, \eta\}. \tag{171}$$

It follows that

$$|\hat{U}-\hat{L}| = |\kappa-\eta|, \tag{172}$$

$$\sqrt{\hat{L}+1} = \min\left\{\sqrt{\kappa+1}, \sqrt{\eta+1}\right\}, \tag{173}$$

$$\sqrt{d-\hat{U}+1} = \min\left\{\sqrt{d-\kappa+1}, \sqrt{d-\eta+1}\right\}, \tag{174}$$

$$\left(f(\hat{U})-f(\hat{L})\right)^2 = \left(f(\kappa)-f(\eta)\right)^2. \tag{175}$$

From the definition of η in (168), we have $|\eta-\vartheta| \leq 0.5$. From the assumption that $\kappa \in \{0, 1, \cdots, d-1, d\} \setminus \{\eta\}$, we have $|\kappa-\eta| \geq 1$. Using the triangle inequality, we have

$$|\kappa-\vartheta| = |\kappa-\eta+\eta-\vartheta| \geq |\kappa-\eta| - |\eta-\vartheta| \geq 0.5 \geq |\eta-\vartheta|.$$

Using this observation together with (172), it follows that

$$4(\kappa-\vartheta)^2 \geq 2(\kappa-\vartheta)^2 + 2(\vartheta-\eta)^2 \geq (\kappa-\vartheta+\vartheta-\eta)^2 = (\hat{U}-\hat{L})^2. \tag{176}$$

Recalling the definition of $\gamma(\kappa)$ in Lemma 18, we have

$$\begin{aligned}
\gamma(\kappa) &= \min\left\{|\kappa-\vartheta|, \sqrt{\kappa+1}, \sqrt{d-\kappa+1}, \sqrt{\vartheta+1}, \sqrt{d-\vartheta+1}\right\} \\
&\leq \min\left\{|\kappa-\eta|+|\eta-\vartheta|, \sqrt{\kappa+1}, \sqrt{d-\kappa+1}, \sqrt{\vartheta+1}, \sqrt{d-\vartheta+1}\right\} \\
&\leq \min\left\{|\kappa-\eta|+1, \sqrt{\kappa+1}, \sqrt{d-\kappa+1}, \sqrt{\eta+2}, \sqrt{d-\eta+2}\right\} \\
&\leq \min\left\{2|\kappa-\eta|, 2\sqrt{\kappa+1}, 2\sqrt{d-\kappa+1}, 2\sqrt{\eta+1}, 2\sqrt{d-\eta+1}\right\} \\
&= \min\left\{2|\hat{U}-\hat{L}|, 2\sqrt{\hat{L}+1}, 2\sqrt{d-\hat{U}+1}\right\} \\
&= 2\beta,
\end{aligned} \tag{177}$$

where the second line follows from the triangle inequality $|\kappa-\vartheta| \leq |\kappa-\eta|+|\eta-\vartheta|$; the third line is because $|\eta-\vartheta| \leq 1$; the fourth line follows from $|\kappa-\eta| \geq 1$; the fifth line follows from (172), (173) and (174). Combining (175), (176) (177), along with (169) in Lemma 18, we obtain

$$\left(\beta\frac{f(\hat{U})-f(\hat{L})}{\hat{U}-\hat{L}}\right)^2 \geq \frac{\gamma(\kappa)^2}{4} \times \frac{(f(\kappa)-f(\eta))^2}{4(\kappa-\vartheta)^2} > \frac{\sigma^2(\chi^*)}{176}. \tag{178}$$

This completes the proof of Proposition 6. □

Now we set out to prove Theorem 3. Recalling the upper bound on T in (21), we have

$$\begin{aligned}
T &\leq 376017 P_{min}(q^*) H(f) d \log\left(\frac{2n}{\varepsilon}\right) + 1 \\
&\leq 376017 P_{min}(q^*) \left(\frac{1}{\min\left\{\hat{U}-\hat{L}, \sqrt{\hat{L}+1}, \sqrt{d-\hat{U}+1}\right\}} \times \frac{\hat{U}-\hat{L}}{f(\hat{U})-f(\hat{L})}\right)^2 d \log\left(\frac{2n}{\varepsilon}\right) + 1 \\
&\leq 376017 P_{min}(q^*) \frac{176}{\sigma^2(\chi^*)} d \log\left(\frac{2n}{\varepsilon}\right) + 1
\end{aligned}$$

where the second inequality follows from the definition of $H(f)$ in (18) by letting (L,U) therein to be the pair $(\hat{L},\hat{U})$ in Proposition 6; the last inequality follows from Proposition 6. This implies that the upper bound in (21) scales as $\mathcal{O}\left(\frac{P_{min}(q^*)}{\sigma^2(\chi^*)} d \log\left(\frac{2n}{\varepsilon}\right)\right)$. On the other hand, by the definition of $h(f)$ in (24), the lower bound in (25) scales as $\Omega\left(\frac{\mu(\chi^*)(1-\mu(\chi^*))}{\sigma^2(\chi^*)} \log\binom{n}{d}\right)$. By standard arguments via Stirling's approximation, $\log\binom{n}{d}$ is at least $d \log \frac{n}{d}$. Thus, under the assumptions that $d = n^\theta, 0 \leq \theta < 1$, the number of tests T required for $(1-\varepsilon)$-reliable recovery in Theorem 1 is up to a $\mathcal{O}\left(\frac{P_{min}(q^*)}{\mu(\chi^*)(1-\mu(\chi^*))}\right)$ factor larger than the lower bound presented in Theorem 2.

From Remarks 1 and 3, we know that our upper and lower bounds scale as $\mathcal{O}\left(d^2 \log n\right)$ and $\Omega\left(d \log n\right)$, respectively. Therefore, the number of tests required in Theorem 1 is never more than an $\mathcal{O}(d)$ factor larger than the information-theoretic lower bound in Theorem 2.

M Proof of Lemma 18

We prove the claim by contradiction. To begin with, assume the contrary is true, i.e.,

$$(\gamma(i)(f(i)-f(\eta)))^2 \leq \frac{\sigma^2(\chi^*)}{11}(i-\vartheta)^2, \ \forall i \in \{0,1,\ldots,d-1,d\} \setminus \{\eta\}. \tag{179}$$

Noting that (179) always holds for $i = \eta$. It then follows that

$$(\gamma(i)(f(i) - f(\eta)))^2 \leq \frac{\sigma^2(\chi^*)}{11}(i - \vartheta)^2, \quad \forall i \in \{0, 1, \ldots, d-1, d\}. \tag{180}$$

In the sequel, we adopt the convention that $\frac{i-\vartheta}{\gamma(i)} = \frac{0}{0} = 1$ for $i = \vartheta$. Then equation (180) can be equivalently written as

$$(f(i) - f(\eta))^2 \leq \frac{\sigma^2(\chi^*)}{11} \cdot \left(\frac{i - \vartheta}{\gamma(i)}\right)^2, \ \forall i \in \{0, 1, \ldots, d-1, d\}. \tag{181}$$

For notational convenience, let

$$p(i) := \frac{\binom{d}{i}\binom{n-d}{\chi^*-i}}{\binom{n}{\chi^*}}, \ \forall i \in \{0, 1, \ldots, d-1, d\}. \tag{182}$$

By definition, $(p(0), \ldots, p(d))$ is the hypergeometric distribution with parameters n, d and χ^*. The mean and variance formulae for hypergeometric distributions (n, d, χ^*) are, respectively,

$$\chi^* \frac{d}{n} \ \text{ and } \ \chi^* \frac{d}{n} \cdot \frac{n-d}{n} \cdot \frac{n-\chi^*}{n-1}. \tag{183}$$

Taking expectations on both sides of (181) w.r.t. the distribution (182), we get

$$\mathbb{E}\left((f(i) - f(\eta))^2\right) \leq \frac{\sigma^2(\chi^*)}{11}\mathbb{E}\left(\left(\frac{i - \vartheta}{\gamma(i)}\right)^2\right). \tag{184}$$

On the other hand,

$$\begin{aligned}
\mathbb{E}\left((f(i) - f(\eta))^2\right) &= \mathbb{E}\left((f(i) - \mu(\chi^*))^2\right) + \mathbb{E}\left((\mu(\chi^*) - f(\eta))^2\right) + \mathbb{E}\left(2\left(f(i) - \mu(\chi^*)\right)\left(\mu(\chi^*) - f(\eta)\right)\right) \\
&= \sigma^2(\chi^*) + (\mu(\chi^*) - f(\eta))^2 + 0 \\
&\geq \sigma^2(\chi^*),
\end{aligned} \tag{185}$$

where the second line follows from (166) and (182). Combining (184) and (185), we deduce that

$$\mathbb{E}\left(\left(\frac{i - \vartheta}{\gamma(i)}\right)^2\right) \geq 11. \tag{186}$$

However, we will argue that $\mathbb{E}\left(\left(\frac{i-\vartheta}{\gamma(i)}\right)^2\right) < 11$, which is a contradiction to (186). This is proved for each of the two possible cases:

i) $\vartheta \in (0, 1) \cup (d-1, d)$;

ii) $\vartheta \in [1, d-1]$.

Case i): For $\vartheta \in (0, 1) \cup (d-1, d)$, we have for any $i \in \{0, \ldots, d\}$ that

$$\min\{i + 1, d - i + 1\} \geq 1 > \min\{\vartheta, d - \vartheta\}. \tag{187}$$

It then follows that

$$\begin{aligned}\left(\frac{i-\vartheta}{\gamma(i)}\right)^2 &= \frac{(i-\vartheta)^2}{\min\{(i-\vartheta)^2, i+1, d-i+1, \vartheta+1, d-\vartheta+1\}} \\ &\le \frac{(i-\vartheta)^2}{\min\{(i-\vartheta)^2, i+1, d-i+1, \vartheta, d-\vartheta\}} \\ &= \frac{(i-\vartheta)^2}{\min\{(i-\vartheta)^2, \vartheta, d-\vartheta\}} \\ &\le \frac{(i-\vartheta)^2}{(i-\vartheta)^2} + \frac{(i-\vartheta)^2}{\min\{\vartheta, d-\vartheta\}} \\ &= 1 + \frac{(i-\vartheta)^2 \max\{\vartheta, d-\vartheta\}}{\vartheta(d-\vartheta)} \\ &\le 1 + \frac{(i-\vartheta)^2 d}{\vartheta(d-\vartheta)}. \end{aligned} \tag{188}$$

Taking expectations on both sides of (188) w.r.t. the hypergeometric distribution (182), we get

$$\mathbb{E}\left(\left(\frac{i-\vartheta}{\gamma(i)}\right)^2\right) \le 1 + \frac{d}{\vartheta(d-\vartheta)}\mathbb{E}\left((i-\vartheta)^2\right). \tag{189}$$

From the mean formula in (183), we have that $\mathbb{E}(i) = \chi^* \frac{d}{n} = \vartheta$. Then using the variance formula in (183), we have

$$\mathbb{E}\left((i-\vartheta)^2\right) = \chi^* \frac{d}{n} \cdot \frac{n-d}{n} \cdot \frac{n-\chi^*}{n-1},$$

which implies

$$\frac{d}{\vartheta(d-\vartheta)}\mathbb{E}\left((i-\vartheta)^2\right) = \frac{n-d}{n-1} \le 1. \tag{190}$$

Note that (190) holds for all $\vartheta \in (0, d)$. Substituting (190) into (189), we have $\mathbb{E}\left(\left(\frac{i-\vartheta}{\gamma(i)}\right)^2\right) \le 2$.

Case ii): For $\vartheta \in [1, d-1]$, we must have $d \ge 2$. It follows that for any $i \in \{0, \ldots, d\}$,

$$\begin{aligned}\left(\frac{i-\vartheta}{\gamma(i)}\right)^2 &= \frac{(i-\vartheta)^2}{\min\{(i-\vartheta)^2, i+1, d-i+1, \vartheta+1, d-\vartheta+1\}} \\ &\le \frac{(i-\vartheta)^2}{\min\{(i-\vartheta)^2, i+1, d-i+1, \vartheta, d-\vartheta\}} \\ &\le \frac{(i-\vartheta)^2}{(i-\vartheta)^2} + \frac{(i-\vartheta)^2}{\min\{i+1, d-i+1\}} + \frac{(i-\vartheta)^2}{\min\{\vartheta, d-\vartheta\}} \\ &= 1 + \frac{(i-\vartheta)^2 \max\{i+1, d-i+1\}}{(i+1)(d-i+1)} + \frac{(i-\vartheta)^2 \max\{\vartheta, d-\vartheta\}}{\vartheta(d-\vartheta)} \\ &\le 1 + \frac{(i-\vartheta)^2 (d+1)}{(i+1)(d-i+1)} + \frac{(i-\vartheta)^2 d}{\vartheta(d-\vartheta)}. \end{aligned} \tag{191}$$

Taking the expectation of (191) w.r.t. the hypergeometric distribution (182), we have

$$\begin{aligned}\mathbb{E}\left(\left(\frac{i-\vartheta}{\gamma(i)}\right)^2\right) &\le 1 + (d+1)\,\mathbb{E}\left(\frac{(i-\vartheta)^2}{(i+1)(d-i+1)}\right) + \frac{d}{\vartheta(d-\vartheta)}\mathbb{E}\left((i-\vartheta)^2\right) \\ &\le 2 + (d+1)\,\mathbb{E}\left(\frac{(i-\vartheta)^2}{(i+1)(d-i+1)}\right), \end{aligned} \tag{192}$$

where the second line follows from (190) since it continues to hold for this case.

Next, we proceed to bound the term on the right hand side of (192). We can expand

$$\begin{aligned}
\mathbb{E}\left(\frac{(i-\vartheta)^2}{(i+1)(d-i+1)}\right) &= \sum_{i=0}^{d}\left(\frac{\binom{d}{i}\binom{n-d}{\chi^*-i}}{\binom{n}{\chi^*}}\cdot\frac{(i-\vartheta)^2}{(i+1)(d-i+1)}\right)\\
&= \sum_{i=0}^{d}\left(\frac{\binom{d+2}{i+1}\binom{n-d}{\chi^*-i}}{\binom{n+2}{\chi^*+1}}\cdot\frac{(n+1)(n+2)}{(\chi^*+1)(n-\chi^*+1)(d+1)(d+2)}\cdot(i-\vartheta)^2\right)\\
&= \frac{(n+1)(n+2)}{(\chi^*+1)(n-\chi^*+1)(d+1)(d+2)}\cdot\sum_{i=0}^{d}\left(\frac{\binom{d+2}{i+1}\binom{n-d}{\chi^*-i}}{\binom{n+2}{\chi^*+1}}\cdot(i-\vartheta)^2\right)\\
&\le \frac{(n+1)(n+2)}{(\chi^*+1)(n-\chi^*+1)(d+1)(d+2)}\cdot\sum_{i=-1}^{d+1}\left(\frac{\binom{d+2}{i+1}\binom{n-d}{\chi^*-i}}{\binom{n+2}{\chi^*+1}}\cdot(i-\vartheta)^2\right)\\
&= \frac{(n+1)(n+2)}{(\chi^*+1)(n-\chi^*+1)(d+1)(d+2)}\cdot\sum_{i=0}^{d+2}\left(\frac{\binom{d+2}{i}\binom{n-d}{\chi^*+1-i}}{\binom{n+2}{\chi^*+1}}\cdot(i-\vartheta-1)^2\right). \qquad (193)
\end{aligned}$$

Using the formula for the mean of hypergeometric distributions $(n+2, d+2, \chi^*+1)$, we have

$$\sum_{i=0}^{d+2}\left(\frac{\binom{d+2}{i}\binom{n-d}{\chi^*+1-i}}{\binom{n+2}{\chi^*+1}}\cdot i\right) = (\chi^*+1)\frac{d+2}{n+2}.$$

Then, using the formula for the variance of hypergeometric distributions $(n+2, d+2, \chi^*+1)$, we have

$$\begin{aligned}
&\sum_{i=0}^{d+2}\left(\frac{\binom{d+2}{i}\binom{n-d}{\chi^*+1-i}}{\binom{n+2}{\chi^*+1}}\cdot(i-\vartheta-1)^2\right)\\
&= \sum_{i=0}^{d+1}\left(\frac{\binom{d+2}{i}\binom{n-d}{\chi^*+1-i}}{\binom{n+2}{\chi^*+1}}\cdot\left(i-(\chi^*+1)\frac{d+2}{n+2}+(\chi^*+1)\frac{d+2}{n+2}-\vartheta-1\right)^2\right)\\
&= \sum_{i=0}^{d+1}\left(\frac{\binom{d+2}{i}\binom{n-d}{\chi^*+1-i}}{\binom{n+2}{\chi^*+1}}\cdot\left(i-(\chi^*+1)\frac{d+2}{n+2}\right)^2\right)+\left((\chi^*+1)\frac{d+2}{n+2}-\vartheta-1\right)^2\\
&= (\chi^*+1)\frac{d+2}{n+2}\cdot\frac{n-d}{n+2}\cdot\frac{n-\chi^*+1}{n+1}+\left((\chi^*+1)\frac{d+2}{n+2}-\vartheta-1\right)^2\\
&\le (\chi^*+1)\frac{d+2}{n+2}\cdot\frac{n-d}{n+2}\cdot\frac{n-\chi^*+1}{n+1}+4, \qquad (194)
\end{aligned}$$

where the last line follows from

$$0 = \chi^*\frac{d}{n}-\vartheta \le (\chi^*+1)\frac{d+2}{n+2}-\vartheta \le (\chi^*+1)\frac{d+2}{n}-\vartheta = \frac{d+2(\chi^*+1)}{n} \le 3.$$

Substituting (194) into (193), we conclude that

$$\begin{aligned}
\mathbb{E}\left(\frac{(i-\vartheta)^2}{(i+1)(d-i+1)}\right) &= \frac{1}{d+1}\cdot\frac{n-d}{n+2}+\frac{4(n+1)(n+2)}{(\chi^*+1)(n-\chi^*+1)(d+1)(d+2)}\\
&\le \frac{1}{d+1}+\frac{4(n+1)(n+2)}{(\chi^*+1)(n-\chi^*+1)(d+1)(d+2)}\\
&\le \frac{1}{d+1}+\frac{4}{d+1}\cdot\frac{n+2}{n+d}\cdot\frac{n+1}{n-\frac{n}{d}+1}\cdot\frac{d}{d+2}\\
&\le \frac{1}{d+1}+\frac{4}{d+1}\cdot\frac{n+1}{n-\frac{n}{2}+1}\cdot\frac{nd+2d}{nd+2d+2n+d^2}\\
&< \frac{1}{d+1}+\frac{4}{d+1}\times 2\times 1\\
&= \frac{9}{d+1}, \qquad (195)
\end{aligned}$$

where the third line follows from

$$\begin{aligned}(\chi^*+1)(n-\chi^*+1) &= -\left(\chi^*-\frac{n}{2}\right)^2+\frac{n^2}{4}+n+1\\ &\geq -\left(\frac{n}{d}-\frac{n}{2}\right)^2+\frac{n^2}{4}+n+1\\ &= \left(\frac{n}{d}+1\right)\left(n-\frac{n}{d}+1\right)\end{aligned}$$

since we have from (167) that $\frac{n}{d}\leq\chi^*\leq n-\frac{n}{d}$ for $1\leq\vartheta\leq d-1$. Upon combining (192) and (195), we arrive at

$$\mathbb{E}\left(\frac{(i-\vartheta)^2}{\gamma(i)^2}\right)<2+(d+1)\cdot\frac{9}{d+1}=11.$$

Summarizing the above two cases, we see that $\mathbb{E}\left(\left(\frac{i-\vartheta}{\gamma(i)}\right)^2\right)<11$, which contradicts (186). Therefore, the assumption in (179) is false and Lemma 18 is proved.

N Proof of Corollary 1

N.1 Proof of Corollary 1-a)

Proof. For test function (1), letting $L=0$ and $U=1$, we have from definition (18) that $H(f)\leq 1$.[8] It then follows that the upper bound in (21) scales as $\mathcal{O}\left(d\log n\right)$.

On the other hand, recall from Remark 3 that the lower bound in (25) scales as $\Omega\left(\log\binom{n}{d}\right)$. Indeed, we can show that the lower bound is precisely $\log\binom{n}{d}$, i.e., $h(f)=1$ for this test function. To see this, noting that $f(0)=0$ and $f(a)=1,\forall a\geq 1$, we can compute that

$$\mu(\chi)=\sum_{a=0}^{d}\frac{\binom{d}{a}\binom{n-d}{\chi-a}}{\binom{n}{\chi}}f(a)=1-\frac{\binom{n-d}{\chi}}{\binom{n}{\chi}}, \tag{196}$$

$$\sum_{a=0}^{d}\frac{\binom{d}{a}\binom{n-d}{\chi-a}}{\binom{n}{\chi}}f^2(a)=1-\frac{\binom{n-d}{\chi}}{\binom{n}{\chi}}. \tag{197}$$

Since $(f(a)-\mu(\chi))^2=f^2(a)+\mu^2(\chi)-2f(a)\mu(\chi)$, we have from (196) and (197) that

$$\begin{aligned}\sigma^2(\chi) &= \sum_{a=0}^{d}\frac{\binom{d}{a}\binom{n-d}{\chi-a}}{\binom{n}{\chi}}(f(a)-\mu(\chi))^2\\ &= \sum_{a=0}^{d}\frac{\binom{d}{a}\binom{n-d}{\chi-a}}{\binom{n}{\chi}}f^2(a)-\mu^2(\chi)\\ &= 1-\frac{\binom{n-d}{\chi}}{\binom{n}{\chi}}-\left(1-\frac{\binom{n-d}{\chi}}{\binom{n}{\chi}}\right)^2\\ &= \frac{\binom{n-d}{\chi}}{\binom{n}{\chi}}\left(1-\frac{\binom{n-d}{\chi}}{\binom{n}{\chi}}\right).\end{aligned}$$

It follows that

$$\frac{\mu(\chi)(1-\mu(\chi))}{\sigma^2(\chi)}=1,\ \forall\chi\in\{1,\ldots,n-1\}.$$

[8] Indeed, we have $H(f)=1$ for this test function. The reverse inequality follows from (19).

Thus we have $h(f) = 1$ for this test function. Now the expression (25) reduces to the classical Fano's inequality based information theoretic lower bound [Chan et al., 2014] on the number of tests required for $(1-\varepsilon)$-reliable recovery

$$T \geq (1-\varepsilon)\log\binom{n}{d} - 1.$$

By standard arguments via Stirling's approximation, this quantity scales as $\Omega\left(d\log\frac{n}{d}\right)$.

Finally, the assumption that $d = n^\theta, \theta \in (0,1)$ implies that our upper and lower bounds are order-wise tight, both scaling as $\Theta(d\log n)$. □

N.2 Proof of Corollary 1-b)

Proof. The proof is very similar to the proof of Corollary 1-b) and appears for completeness. For test function (26), letting $L = \ell$ and $U = \ell + 1$, we have from (18) that $H(f) \leq 1$.[8] Substituting into (21), the upper bound scales as $\mathcal{O}(d\log n)$.

On the other hand, recall from Remark 3 that the lower bound in (25) scales as $\Omega\left(\log\binom{n}{d}\right)$.[9] By standard arguments via Stirling's approximation, $\log\binom{n}{d}$ is at least $d\log\frac{n}{d}$. Using the assumption that $d = n^\theta, \theta \in (0,1)$, we see that our upper and lower bounds are order-wise tight, both scaling as $\Theta(d\log n)$. □

N.3 Proof of Corollary 1-c)

Proof. For linear test function (27), letting $L = \left\lfloor\frac{d}{3}\right\rfloor$ and $U = \left\lceil\frac{2d}{3}\right\rceil$, we have that

$$\begin{aligned}
\min\left\{U-L, \sqrt{L+1}, \sqrt{d-U+1}\right\} &= \min\left\{\left\lceil\frac{2d}{3}\right\rceil - \left\lfloor\frac{d}{3}\right\rfloor, \sqrt{\left\lfloor\frac{d}{3}\right\rfloor+1}, \sqrt{d-\left\lceil\frac{2d}{3}\right\rceil+1}\right\} \\
&\geq \min\left\{\frac{2d}{3}-\frac{d}{3}, \sqrt{\frac{d}{3}-1+1}, \sqrt{d-\left(\frac{2d}{3}+1\right)+1}\right\} \\
&= \sqrt{\frac{d}{3}}.
\end{aligned}$$

It follows from (18) that

$$\begin{aligned}
H(f) &\leq \left(\frac{1}{\sqrt{\frac{d}{3}}} \times \frac{\left\lceil\frac{2d}{3}\right\rceil - \left\lfloor\frac{d}{3}\right\rfloor}{f\left(\left\lceil\frac{2d}{3}\right\rceil\right) - f\left(\left\lfloor\frac{d}{3}\right\rfloor\right)}\right)^2 \\
&= 3d
\end{aligned}$$

Plugging this into (21), the upper bound scales as $\mathcal{O}\left(d^2\log n\right)$.

The mean and variance formulae for hypergeometric distributions with parameters n, d and χ are, respectively, $\chi\frac{d}{n}$ and $\chi\frac{d}{n}\frac{n-d}{n}\frac{n-\chi}{n-1}$. For this test function we can therefore compute that

$$\mu(\chi) = \sum_{a=0}^{d}\frac{\binom{d}{a}\binom{n-d}{\chi-a}}{\binom{n}{\chi}}f(a) = \frac{1}{d}\sum_{a=0}^{d}\frac{\binom{d}{a}\binom{n-d}{\chi-a}}{\binom{n}{\chi}}a = \frac{\chi}{n},$$

[9] By a similar argument to the one above, one can show the lower bound is precisely $\log\binom{n}{d}$, i.e., we also have $h(f) = 1$ for this test function.

and

$$\begin{aligned}\sigma^2(\chi) &= \sum_{a=0}^{d} \frac{\binom{d}{a}\binom{n-d}{\chi-a}}{\binom{n}{\chi}}(f(a)-\mu(\chi))^2 \\ &= \frac{1}{d^2}\sum_{a=0}^{d} \frac{\binom{d}{a}\binom{n-d}{\chi-a}}{\binom{n}{\chi}}(a-d\mu(\chi))^2 \\ &= \frac{1}{d^2}\sum_{a=0}^{d} \frac{\binom{d}{a}\binom{n-d}{\chi-a}}{\binom{n}{\chi}}\left(a-\chi\frac{d}{n}\right)^2 \\ &= \frac{1}{d^2}\cdot\chi\frac{d}{n}\frac{n-d}{n}\frac{n-\chi}{n-1} \\ &= \frac{\chi(n-\chi)}{n^2}\cdot\frac{n-d}{d(n-1)}.\end{aligned}$$

It follows that

$$\frac{\mu(\chi)(1-\mu(\chi))}{\sigma^2(\chi)} = \frac{d(n-1)}{n-d} \geq d, \quad \forall \chi \in \{1,\ldots,n-1\}.$$

This together with the definition of $h(f)$ in (24) implies $h(f) \geq d$. Plugging into (25), we have

$$T \geq d\left((1-\varepsilon)\log\binom{n}{d} - 1\right)$$

which, by standard arguments via Stirling's approximation, scales as $\Omega\left(d^2\log\frac{n}{d}\right)$.

Finally, under the assumption that $d = n^\theta, \theta \in (0,1)$, we see that both the upper and lower bounds scale as $\Theta\left(d^2\log n\right)$.

□

O Proof of Corollary 2

Proof. Applying the inequalities in (8) to the definition of $P_{\min}(q)$ in (7), we have

$$\min\{f(0), 1-f(d)\} \leq P_{\min}(q) \leq \min\{f(d), 1-f(0)\}, \quad \forall q \in (0,1). \tag{198}$$

From Remark 2 we have

$$f(0)(1-f(d)) \leq \mu(\chi)(1-\mu(\chi)) \leq f(d)(1-f(0)), \quad \forall \chi \in \{1,\ldots,n-1\}. \tag{199}$$

Combining (198) and (199), we see that

$$\frac{\min\{f(0),1-f(d)\}}{f(d)(1-f(0))} \leq \frac{P_{min}(q^*)}{\mu(\chi^*)\left(1-\mu(\chi^*)\right)} \leq \frac{\min\{f(d),1-f(0)\}}{f(0)(1-f(d))}. \tag{200}$$

Recalling the definition of noisy test functions, we have $f(0), 1-f(d) \in \Theta(1)$. It then follows from (200) that

$$\frac{P_{min}(q^*)}{\mu(\chi^*)\left(1-\mu(\chi^*)\right)} \in \Theta(1).$$

This along with Theorem 3 yields that our bounds are order-wise tight. □

P Simulation

In this section we report the results of our computer simulations to evaluate the performance of our proposed schemes.[10] Our algorithm takes as input

[10]The computing resource we use is an Intel(R) Xeon(R) CPU E5-2699 v4 @ 2.20GHz CPU.

- number of items n;
- number of defectives d;
- test function f;
- number of tests T.

We then run the proposed test design and decoding rule multiple times to evaluate the probability of successful reconstruction.

Testing: For given (n, d, f, T), we randomly generate an array $\boldsymbol{X}$ of length n with $(n-d)$ 0s and d 1s, where 0 represents non-defective and 1 represents defective. Then we choose the parameter q accordingly, and randomly generate a $T \times n$ matrix $\boldsymbol{M}$ where each entry is i.i.d. Bernoulli(q). Each row of $\boldsymbol{M}$ corresponds to a distinct test, and each column corresponds to a distinct item. Finally, we compute $\boldsymbol{Z} = (Z_1, \ldots, Z_T) = \boldsymbol{M}\boldsymbol{X}$ and generate the test outcomes according to $f(Z_i), i = 1, \ldots, T$.

Decoding: Depending on the value of q, we then use the decoding rules (16) or (17). Let $\hat{\boldsymbol{X}}$ be the estimation of the decoder. The test succeeds if $\hat{\boldsymbol{X}} = \boldsymbol{X}$, and fails otherwise.

P.1 Simulation result for threshold test function in Corollary 1-b)

Consider the function $f(\cdot)$ defined in (26) for $\ell = 5$ i.e.,

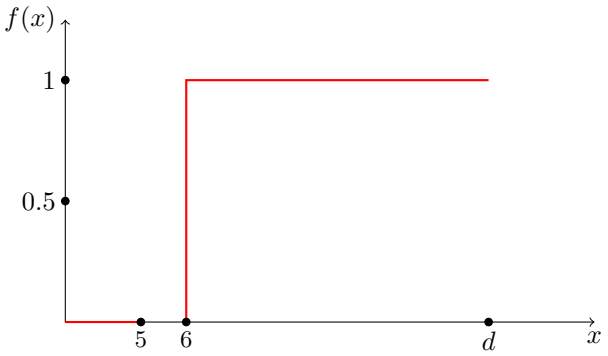
$$f(x) = \begin{cases} 0 & \text{if } x \leq 5, \\ 1 & \text{if } x > 5, \end{cases} \tag{201}$$

which is also illustrated in Figure 4a. In Corollary 1-b), we have shown that our algorithm is order-wise optimal and the number of tests T scales as $\Theta(d \log n)$. For ease of implementation, we assign $q = \frac{5}{d}$. In the waterfall plot in Figure 4b, $n = 2000$, $d = 20$, the x-axis plots the number of tests T ranging from $T_{min} = 0$ to $T_{max} = \lfloor 40 d \log n \rfloor$ with step size $\Delta_T = \left\lfloor \frac{T_{max} - T_{min}}{100} \right\rfloor$, and the y-axis plots the probability of successful reconstruction calculated by 1000 trials for each test $T = T_{min} + j \times \Delta_T, j \in \{0, 1, \ldots, 100\}$. When $T \gtrapprox 19.2 d \log n$, the probability of successful reconstruction generally exceeds 0.99.[11] In the heat-map in Figure 4c, $n = 2000$, the x-axis denotes the number of defectives d ranging from 20 to 120, and the y-axis denotes the number of tests T as a multiple of $d \log n$. In the heat-map in Figure 4d, $d = 20$, the x-axis corresponds to the number of items n ranging from 2000 to 6000, and the y-axis corresponds to the number of tests T as a multiple of $d \log n$. In both Figures 4c and 4d, each pixel is coloured according to the probability of successful reconstruction calculated by 1000 trials for each test T– the lighter the colour, the higher the probability of reconstruction success. For each value of d (respectively n) in Figure 4c (respectively Figure 4d), the corresponding red dot in that column represents the number of tests for which this probability first equals 0.99. The horizontal blue dashed line indicates that when $T \gtrapprox 17.2 d \log n$ (respectively $20.4 d \log n$), the probability of successful reconstruction generally exceeds 0.99.

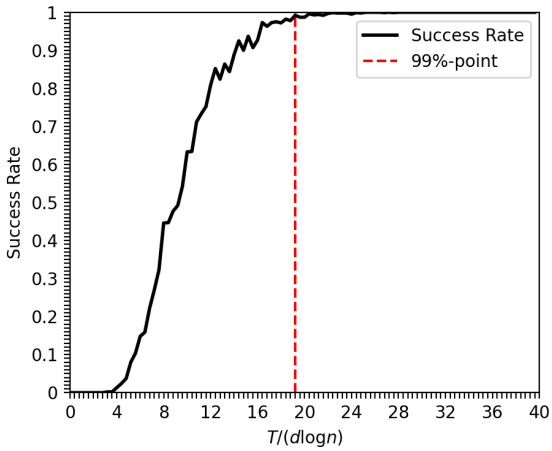
P.2 Simulation result for linear test function in Corollary 1-c)

We now consider the function $f(\cdot)$ defined in (27) and illustrated in Figure 5a. In Corollary 1-c), we have shown that our algorithm is order-wise optimal and the number of tests T scales as $\Theta(d^2 \log n)$. For ease of implementation, we assign $q = \frac{1}{2}$. In the waterfall plot in Figure 5b, $n = 2000$, $d = 20$, the x-axis plots the number of tests T ranging from $T'_{min} = 0$ to $T'_{max} = \lfloor 40 d^2 \log n \rfloor$ with step size $\Delta'_T = \left\lfloor \frac{T_{max} - T_{min}}{100} \right\rfloor$, and the y-axis plots the probability of successful reconstruction calculated by 100 trials for each test $T = T'_{min} + j \times \Delta'_T, j \in \{0, 1, \ldots, 100\}$. When $T \gtrapprox 21.6 d^2 \log n$, the probability of successful reconstruction exceeds 0.99. In the heat-map figure 5c, $n = 2000$, the x-axis denotes the number of defectives d ranging from 20 to 70, and the y-axis denotes the number of tests T as a multiple of $d^2 \log n$. In the heat-map figure 5d, $d = 20$, the x-axis corresponds to the number of items n ranging from 2000 to 4000, and the y-axis corresponds to the number of tests T as a multiple of $d^2 \log n$. In both figures 5c and 5d, each pixel is coloured according to the probability of successful reconstruction calculated by 100 trials for each test T– the lighter the colour, the higher

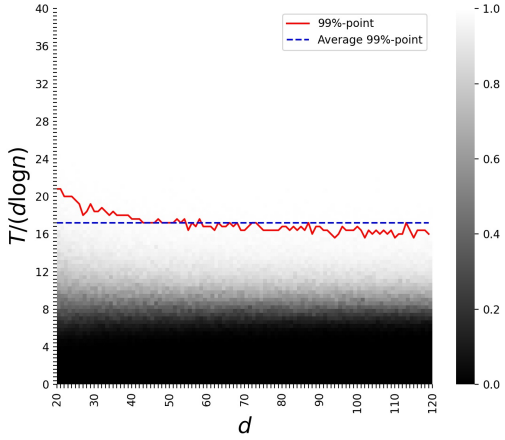
[11] Here and below, "generally exceeds" means that the average of itself and two tests prior to it is larger than 0.99.



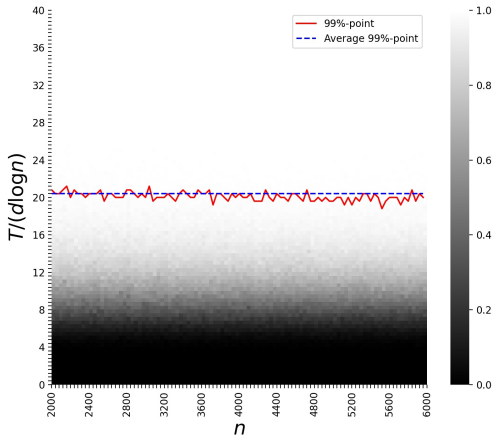
(a) *Example test function defined in* (201)*: The test outcome is positive if and only if at least* 6 *items in a pool are defective.*



(b) *The* x*-axis plots the number of tests* T *as a multiple of* $d \log n$*, and the* y*-axis plots the probability of successful reconstruction, for fixed* $n = 2000, d = 20$*. When* $T \gtrapprox 19.2 d \log n$*, the probability of successful reconstruction exceeds* 0.99*.*

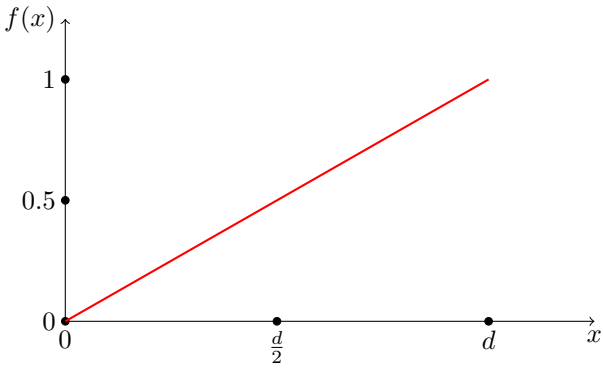


(c) *The* x*-axis corresponds to the number of defectives* d *ranging from* 20 *to* 120*, and the* y*-axis corresponds to the number of tests* T *as a multiple of* $d \log n$*–the number of items* n *is fixed to be* 2000*. Each pixel is coloured according to the probability of successful reconstruction– the lighter the colour, the higher the probability of reconstruction success. For each value of* d*, the corresponding red dot in that column represents the number of tests for which this probability first equals* 0.99*. The horizontal blue dashed line indicates that when* $T \gtrapprox 17.2 d \log n$*, the probability of successful reconstruction generally exceeds* 0.99*.*

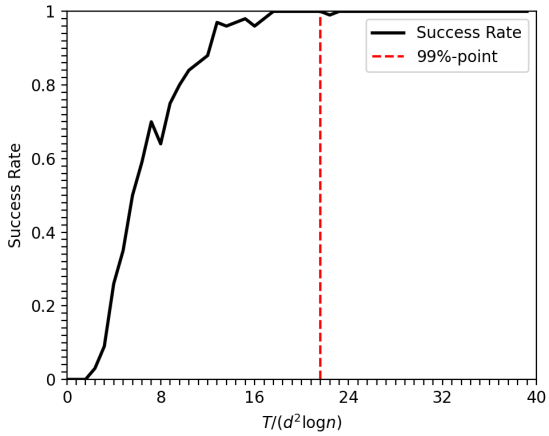


(d) *The* x*-axis denotes the number of items* n *ranging from* 2000 *to* 6000*, and the* y*-axis denotes the number of tests* T *as a multiple of* $d \log n$*–the number of defectives* d *equals* 20*. Each pixel is coloured according to the probability of successful reconstruction – the lighter the colour, the higher the probability of reconstruction success. For each value of* n*, the corresponding red dot in that column represents the number of tests for which this probability first equals* 0.99*. The horizontal blue dashed line indicates that when* $T \gtrapprox 20.4 d \log n$*, the probability of successful reconstruction generally exceeds* 0.99*.*

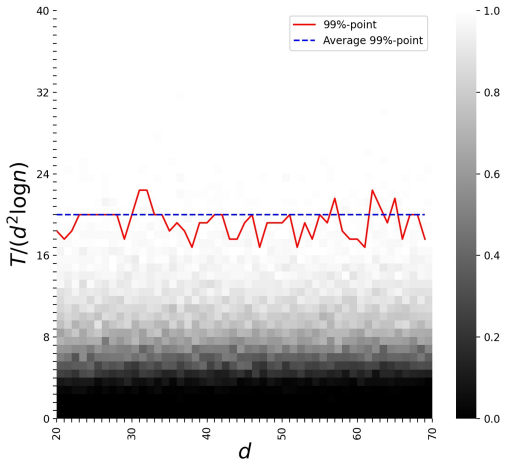
Figure 4: *Simulation result for threshold test function in Corollary 1-b).*



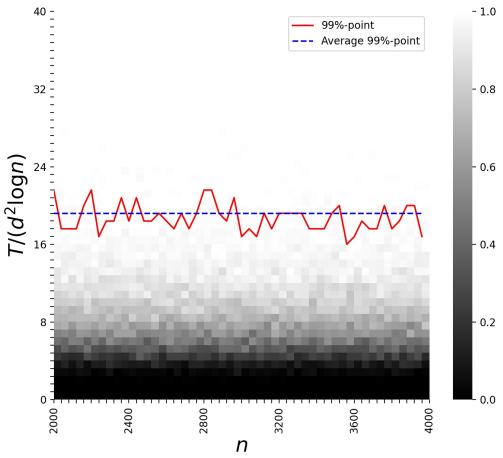
(a) *Example test function f defined in* (27)*: The probability that test outcome is positive increases linearly.*



(b) *The x-axis plots the number of tests T as a multiple of $d^2 \log n$, and the y-axis plots the probability of successful reconstruction, for fixed $n = 2000$ and $d = 20$. When $T \gtrapprox 21.6d^2 \log n$, the probability of successful reconstruction exceeds* 0.99.

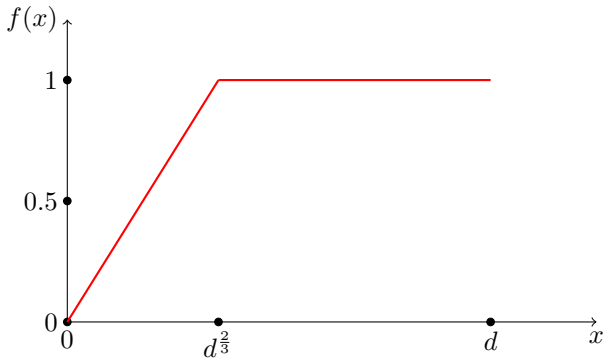


(c) *The x-axis corresponds to the number of defectives d ranging from* 20 *to* 70*, and the y-axis corresponds to the number of tests T as a multiple of $d^2 \log n$, for fixed number of items $n = 2000$. Each pixel is coloured according to the probability of successful reconstruction– the lighter the colour, the higher the probability of reconstruction success. For each value of d, the corresponding red dot in that column represents the number of tests for which this probability first equals* 0.99*. The horizontal blue dashed line indicates that when $T \gtrapprox 20.0d^2 \log n$, the probability of successful reconstruction generally exceeds* 0.99.

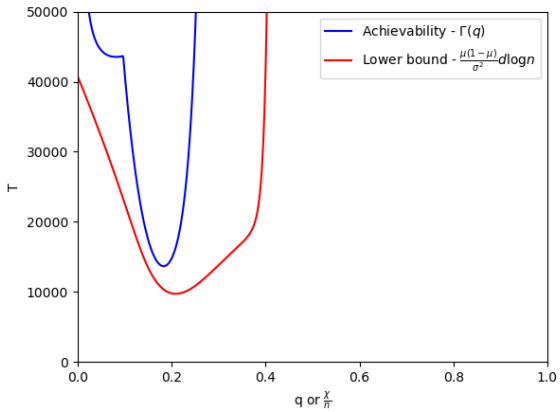


(d) *The x-axis denotes the number of items n ranging from* 2000 *to* 4000*, and the y-axis denotes the number of tests T as a multiple of $d^2 \log n$, for fixed number of defectives $d = 20$. Each pixel is coloured according to the probability of successful reconstruction – the lighter the colour, the higher the probability of reconstruction success. For each value of n, the corresponding red dot in that column represents the number of tests for which this probability first equals* 0.99*. The horizontal blue dashed line indicates that when $T \gtrapprox 19.6d^2 \log n$, the probability of successful reconstruction generally exceeds* 0.99.

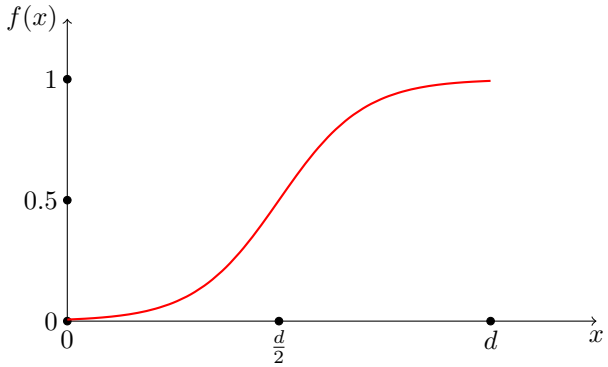
Figure 5: *Simulation result for linear test function in Corollary 1-c).*



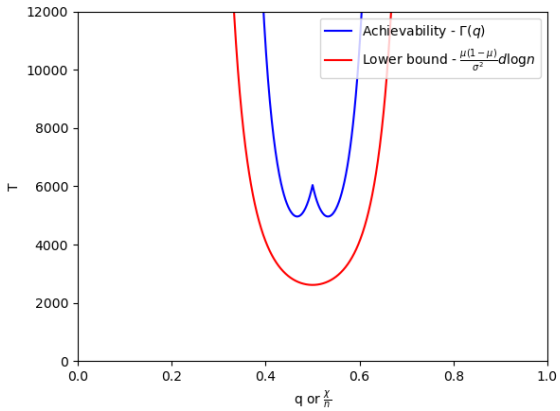
(a) *Example test function f defined in* (202).



(b) *Performance of our algorithm for the "partial linear" function.*



(c) *Example test function f defined in* (203).



(d) *Performance of our algorithm for the sigmoid function.*

Figure 6: *Simulation result for Conjecture 1.*

the probability of reconstruction success. For each value of d (respectively n) in figure 5c (respectively figure 5d), the corresponding red dot in that column represents the number of tests for which this probability first equals 0.99. The horizontal blue dashed line indicates that when $T \gtrapprox 20.0d^2 \log n$ (respectively $19.6d^2 \log n$), the probability of successful reconstruction generally exceeds 0.99.

P.3 Simulation result for Conjecture 1

We first provide some functions and the corresponding performance of our algorithm. Consider one specific "partial linear" function defined in (20) in Example 1:

$$f(x) = \begin{cases} \frac{x}{d^{2/3}} & x \in \left[0, d^{2/3}\right] \cap \mathbb{Z}^+, \\ 1 & \text{otherwise}, \end{cases} \tag{202}$$

Letting $n = 1250$ and $d = 125$, its performance is presented in Fig. 6b. Then consider the well-known sigmoid function:

$$f(x) = \frac{e^{\frac{x}{2} - \frac{d}{4}}}{e^{\frac{x}{2} - \frac{d}{4}} + 1}. \tag{203}$$

Letting $n = 2000$ and $d = 100$, its performance is presented in Fig. 6d. One can see from the figures that $\frac{\min_{q \in (0,1)} \Gamma(q)}{h(f) d \log n} \leq 2$ in the two cases, which supports our conjecture.

Q Estimating the exact number of defectives

Our algorithms and bounds depend critically on the assumption that the number of defectives d is known a priori. Moreover, different from the classical group-testing in which most algorithms are robust to small perturbations in the value of d, our algorithms require the exact value of d. If the value of d is not available, it will be useful to have an algorithm for exactly estimating this. In this section, we develop such an algorithm. Let us first analyze a useful subroutine, and then present the full algorithm.

Q.1 A useful subroutine

Let $\hat{d} \geq 2$ be a putative number of defective items, and consider the goal of deciding whether $d \leq \hat{d}-1$ or $d \geq \hat{d}$. Towards this end, we use a Bernoulli test design in which each item is independently placed into each test with probability ζ. Let $P(\hat{d}, \zeta)$ denote the probability of having a positive test outcome conditioned on $d = \hat{d}$. It follows that

$$P(\hat{d}, \zeta) = \sum_{j=0}^{\hat{d}} \binom{\hat{d}}{j} \zeta^j (1-\zeta)^{\hat{d}-j} f(j). \tag{204}$$

Similar to (53), define

$$\Delta(\hat{d}, \zeta) := \sum_{j=0}^{\hat{d}-1} \binom{\hat{d}-1}{j} \zeta^j (1-\zeta)^{\hat{d}-j} \left(f(j+1) - f(j)\right). \tag{205}$$

The subroutine $\texttt{LoM}(\hat{d}, \zeta, \epsilon)$ for deciding whether $d \leq \hat{d}-1$ or $d \geq \hat{d}$ is described in Algorithm 1.

Algorithm 1 $\texttt{LoM}(\hat{d}, \zeta, \epsilon)$

1: Take $t(\hat{d}, \zeta, \epsilon)$ tests of the Bernoulli test design with parameter ζ, where

$$t(\hat{d}, \zeta, \epsilon) := \left\lceil 8.32 \left(\frac{1-\zeta}{\zeta \Delta(\hat{d}, \zeta)} \right)^2 \log \frac{1}{\epsilon} \right\rceil. \tag{206}$$

2: Let $t^+(\hat{d}, \zeta, \epsilon)$ denote the number of tests with positive outcome within these $t(\hat{d}, \zeta, \epsilon)$ tests. If

$$\frac{t^+(\hat{d}, \zeta, \epsilon)}{t(\hat{d}, \zeta, \epsilon)} \leq P(\hat{d}, \zeta) - \frac{\zeta}{2(1-\zeta)} \Delta(\hat{d}, \zeta), \tag{207}$$

return $d \leq \hat{d}-1$; otherwise, return $d \geq \hat{d}$.

Lemma 19. *The error probability of* $\texttt{LoM}(\hat{d}, \zeta, \epsilon)$ *is at most* ϵ.

Proof. Let $P(\hat{d}-1, \zeta)$ denote the probability of having a positive test outcome conditioned on $d = \hat{d}-1$. It follows that

$$P(\hat{d}-1, \zeta) = \sum_{j=0}^{\hat{d}-1} \binom{\hat{d}-1}{j} \zeta^j (1-\zeta)^{\hat{d}-1-j} f(j).$$

Then we have

$$\begin{aligned}
P(\hat{d},\zeta)-P(\hat{d}-1,\zeta) &= \sum_{j=0}^{\hat{d}}\binom{\hat{d}}{j}\zeta^j(1-\zeta)^{\hat{d}-j}f(j)-\sum_{j=0}^{\hat{d}-1}\binom{\hat{d}-1}{j}\zeta^j(1-\zeta)^{\hat{d}-1-j}f(j)\\
&= (1-\zeta)\sum_{j=0}^{\hat{d}}\left(\binom{\hat{d}-1}{j}+\binom{\hat{d}-1}{j-1}\right)\zeta^j(1-\zeta)^{\hat{d}-1-j}f(j)-\sum_{j=0}^{\hat{d}-1}\binom{\hat{d}-1}{j}\zeta^j(1-\zeta)^{\hat{d}-1-j}f(j)\\
&= (1-\zeta)\sum_{j=1}^{\hat{d}}\binom{\hat{d}-1}{j-1}\zeta^j(1-\zeta)^{\hat{d}-1-j}f(j)-\zeta\sum_{j=0}^{\hat{d}-1}\binom{\hat{d}-1}{j}\zeta^j(1-\zeta)^{\hat{d}-1-j}f(j)\\
&= \zeta\sum_{j=1}^{\hat{d}}\binom{\hat{d}-1}{j-1}\zeta^{j-1}(1-\zeta)^{\hat{d}-j}f(j)-\zeta\sum_{j=0}^{\hat{d}-1}\binom{\hat{d}-1}{j}\zeta^j(1-\zeta)^{\hat{d}-1-j}f(j)\\
&= \zeta\sum_{j=0}^{\hat{d}-1}\binom{\hat{d}-1}{j}\zeta^j(1-\zeta)^{\hat{d}-1-j}(f(j+1)-f(j))\\
&= \frac{\zeta}{1-\zeta}\Delta(\hat{d},\zeta). \qquad (208)
\end{aligned}$$

Using this observation, the threshold equation (207) is equivalent to

$$\frac{t^+(\hat{d},\zeta,\epsilon)}{t(\hat{d},\zeta,\epsilon)} \le \frac{P(\hat{d},\zeta)+P(\hat{d}-1,\zeta)}{2}. \qquad (209)$$

For $\texttt{LoM}(\hat{d},\zeta,\epsilon)$ two types of error can happen:

i) We have $d \le \hat{d}-1$, but is claimed to be $d \ge \hat{d}$;

ii) We have $d \ge \hat{d}$, but is claimed to be $d \le \hat{d}-1$.

Case i): It is worth noting that $t^+(\hat{d},\zeta,\epsilon) \sim \text{Binomial}\Big(t(\hat{d},\zeta,\epsilon), P(d,\zeta)\Big)$. From (209) we know the probability of error is

$$\begin{aligned}
\Pr\left(\frac{t^+(\hat{d},\zeta,\epsilon)}{t(\hat{d},\zeta,\epsilon)} > \frac{P(\hat{d},\zeta)+P(\hat{d}-1,\zeta)}{2}\right) &= \Pr\left(t^+(\hat{d},\zeta,\epsilon) > \frac{P(\hat{d},\zeta)+P(\hat{d}-1,\zeta)}{2}\cdot t(\hat{d},\zeta,\epsilon)\right)\\
&\le \Pr\left(\text{Binomial}\Big(t(\hat{d},\zeta,\epsilon), P(\hat{d}-1,\zeta)\Big) > \frac{P(\hat{d},\zeta)+P(\hat{d}-1,\zeta)}{2}\cdot t(\hat{d},\zeta,\epsilon)\right)\\
&\le \exp\left(-\frac{1}{3}\left(\frac{P(\hat{d},\zeta)-P(\hat{d}-1,\zeta)}{2P(\hat{d}-1,\zeta)}\right)^2\cdot t(\hat{d},\zeta,\epsilon)P(\hat{d}-1,\zeta)\right)\\
&\le \exp\left(-\frac{\Big(P(\hat{d},\zeta)-P(\hat{d}-1,\zeta)\Big)^2}{12}t(\hat{d},\zeta,\epsilon)\right)\\
&\le \epsilon.
\end{aligned}$$

where the first inequality follows from the fact that $P(d,\zeta)$ is monotonically increasing with respect to d and $d \le \hat{d}-1$; the second inequality follows from Chernoff bound in Fact 1; the third inequality follows from the fact that $P(\hat{d}-1,\zeta) \le 1$; the last inequality follows by substituting (206) and (208).

Case ii): The calculations are similar to Case i). Again $t^+(\hat{d},\zeta,\epsilon) \sim \text{Binomial}\Big(t(\hat{d},\zeta,\epsilon), P(d,\zeta)\Big)$. We know from

(209) that the probability of error is

$$\begin{aligned}
\Pr\left(\frac{t^+(\hat{d},\zeta,\epsilon)}{t(\hat{d},\zeta,\epsilon)} \le \frac{P(\hat{d},\zeta)+P(\hat{d}-1,\zeta)}{2}\right) &= \Pr\left(t^+(\hat{d},\zeta,\epsilon) \le \frac{P(\hat{d},\zeta)+P(\hat{d}-1,\zeta)}{2}\cdot t(\hat{d},\zeta,\epsilon)\right) \\
&\le \Pr\left(\text{Binomial}\left(t(\hat{d},\zeta,\epsilon),P(\hat{d},\zeta)\right) \le \frac{P(\hat{d},\zeta)+P(\hat{d}-1,\zeta)}{2}\cdot t(\hat{d},\zeta,\epsilon)\right) \\
&\le \exp\left(-\frac{1}{3}\left(\frac{P(\hat{d},\zeta)-P(\hat{d}-1,\zeta)}{2P(\hat{d},\zeta)}\right)^2 \cdot t(\hat{d},\zeta,\epsilon)P(\hat{d},\zeta)\right) \\
&\le \exp\left(-\frac{\left(P(\hat{d},\zeta)-P(\hat{d}-1,\zeta)\right)^2}{12}t(\hat{d},\zeta,\epsilon)\right) \\
&\le \epsilon.
\end{aligned}$$

where the first inequality follows from the fact that $P(d,\zeta)$ is monotonically increasing with respect to d and $d \ge \hat{d}$; the second inequality follows from Chernoff bound in Fact 1; the third inequality follow from the fact that $P(\hat{d},\zeta) \le 1$; the last inequality follows by substituting (206) and (208).

Combining the two cases we conclude that the error probability of $\texttt{LoM}(\hat{d},\zeta,\epsilon)$ is at most ϵ. □

Q.2 Algorithm for exactly estimating d

Armed with the above subroutine $\texttt{LoM}(\hat{d},\zeta,\epsilon)$, the algorithm for exactly estimating d is now described in Algorithm 2.

Algorithm 2 Exact estimation of d

Initialize $\epsilon \leftarrow \frac{\varepsilon}{2\log n+2}$, $d_u \leftarrow 2$
while true **do**
  set $\zeta^* = \text{argmin}_{\zeta\in(0,1)} \frac{1-\zeta}{\zeta(\Delta(d_u,\zeta))^2}$
  run $\texttt{LoM}(d_u,\zeta^*,\epsilon)$
  if $d \le d_u - 1$ **then halt**
  else set $d_u \leftarrow 2d_u$
end while
set $d_l \leftarrow \frac{d_u}{2}$
while $d_u - d_l \ge 2$ **do**
  set $d_m = \left\lfloor \frac{d_l+d_u}{2} \right\rfloor$, $\zeta^* = \text{argmin}_{\zeta\in(0,1)} \frac{1-\zeta}{\zeta(\Delta(d_m,\zeta))^2}$
  run $\texttt{LoM}(d_m,\zeta^*,\epsilon)$
  if $d \le d_m - 1$ **then set** $d_u \leftarrow d_m$
  else set $d_l \leftarrow d_m$
end while
output d_l

Lemma 20. *Algorithm 2 outputs d_l satisfying $d_l = d$ with probability at least $1-\varepsilon$, using $\mathcal{O}\left(d^4(\log\log d)^4 \log d \log((\log n)/\varepsilon)\right)$ tests. Moreover, it uses at most $2\log(2d)$ stages of adaptivity.*

Proof. We start by noting that both while loops in Algorithm 2 invoke at most $\log(2d)$ calls to the subroutine $\texttt{LoM}(\hat{d},\zeta,\epsilon)$. By Lemma 19 and the union bound, we know that the error probability of Algorithm 2 is bounded from above by

$$2\log(2d)\cdot\epsilon = 2\log(2d)\frac{\varepsilon}{2\log n+2} \le \varepsilon.$$

From (206) we have

$$\begin{aligned} t(\hat{d},\zeta^*,\epsilon) &= \left\lceil 8.32\left(\frac{1-\zeta^*}{\zeta^*\Delta(\hat{d},\zeta^*)}\right)^2 \log\frac{1}{\epsilon}\right\rceil \\ &\le \left\lceil 8.32\left(\frac{1-\zeta^*}{\zeta^*(\Delta(\hat{d},\zeta^*))^2}\right)^2 \log\frac{1}{\epsilon}\right\rceil \\ &\le 8.32\left(376017H(f,\hat{d})\,\hat{d}\right)^2 \log\frac{1}{\epsilon}+1 \\ &= 8.32\left(376017H(f,\hat{d})\,\hat{d}\right)^2 \log\left(\frac{2\log n+2}{\varepsilon}\right)+1. \end{aligned}$$

The first inequality follows by noting that $\Delta(\hat{d},\zeta^*)\le 1$ since $\Delta(\hat{d},\zeta)$ in (205) is the same as $\Delta(q)$ in (53) (with $(\hat{d},\zeta^*)$ in place of (d,q)), and $\Delta(q)\le 1$ for all q by Lemma 1. The second inequality can be justified as follows: The expression in $(\cdot)^2$ is similar to $\bar{\Gamma}(q)$ in (14). By the same argument as in Proposition 3 and the discussions that follow, we can bound the expression in $(\cdot)^2$ by $376017H(f,\hat{d})\,\hat{d}$, where $H(f,\hat{d})$ is the same as $H(f)$ in (18) but with $\hat{d}$ in place of d.

Lastly, since $\texttt{LoM}(\hat{d},\zeta,\epsilon)$ is called $\mathcal{O}(\log d)$ times and $\hat{d}\in\mathcal{O}(d)$, by Lemma 2, the above inequality implies that the total number of tests in Algorithm 2 scales as $\mathcal{O}\left(d^4(\log\log d)^4\log d\log\left(\frac{\log n}{\varepsilon}\right)\right)$. □