2018 56th Annual Allerton Conference on Communication, Control, and Computing (Allerton)
Allerton Park and Retreat Center
Monticello, IL, USA, October 2-5, 2018

On the Optimality of the Kautz-Singleton Construction in Probabilistic Group Testing

Huseyin A. Inan[1], Peter Kairouz[1], Mary Wootters[2], and Ayfer Ozgur[1]

***Abstract*— We consider the probabilistic group testing problem where d random defective items in a large population of N items are identified with high probability by applying binary tests. It is known that $\Theta(d \log N)$ tests are necessary and sufficient to recover the defective set with vanishing probability of error. However, to the best of our knowledge, there is no explicit (deterministic) construction achieving $\Theta(d \log N)$ tests in general. In this work, we show that a famous construction introduced by Kautz and Singleton for the combinatorial group testing problem (which is known to be suboptimal for combinatorial group testing for moderate values of d) achieves the order optimal $\Theta(d \log N)$ tests in the probabilistic group testing problem. This provides the first strongly explicit construction achieving the order optimal result in the probabilistic group testing setting. To prove the order-optimality of Kautz and Singleton's construction in the probabilistic setting, we provide a novel analysis of the probability of a non-defective item being covered by a random defective set directly, rather than arguing from combinatorial properties of the underlying code, which has been the main approach in the literature. Furthermore, we use a recursive technique to convert this construction into one that can also be efficiently decoded with only a log-log factor increase in the number of tests.**

I. Introduction

The objective of group testing is to efficiently identify a small set of d defective items in a large population of size N by performing binary tests on groups of items, as opposed to testing the items individually. A positive test outcome indicates that the group contains at least one defective item. A negative test outcome indicates that all the items in the group are non-defective. When d is much smaller than N, the defectives can be identified with far fewer than N tests.

The original group testing framework was developed in 1943 by Robert Dorfman [1]. Back then, group testing was devised to identify which WWII draftees were infected with syphilis, without having to test them individually. In Dorfman's application, items represented draftees and tests represented actual blood tests. Over the years, group testing has found numerous applications in fields spanning biology [2], medicine [3], machine learning [4], data analysis [5], signal processing [6], and wireless multiple-access communications [7]–[10].

A. Non-adaptive probabilistic group testing

Group testing strategies can be *adaptive*, where the i^{th} test is a function of the outcomes of the $i-1$ previous tests, or *non-adaptive*, where all tests are designed in one shot. A non-adaptive group testing strategy can be represented by a $t \times N$ binary matrix M, where $M_{ij} = 1$ indicates that item j participates in test i. Group testing schemes can also be *combinatorial* [11], [12] or *probabilistic* [13]–[16]. The goal of combinatorial group testing schemes is to recover any set of up to d defective items with zero-error and require at least $t = \Omega(d^2 \log N / \log d)$ tests [17], [18]. Existing constructions in this setting achieve $t = O(d^2 \log_d^2 N)$ [19] and $t = O(d^2 \log N)$ [20] tests. In contrast, probabilistic group testing schemes assume a random defective set of size d, allow for an arbitrarily small probability of reconstruction error, and require $t = \Theta(d \log N)$ tests only [13]. In this paper, we are interested in non-adaptive probabilistic group testing schemes.

B. Our contributions

To best of our knowledge, all known probabilistic group testing strategies that achieve $t = O(d \log N)$ tests are randomized (i.e., M is randomly constructed) [13]–[16]. Recently, Mazumdar [21] presented explicit schemes (deterministic constructions of M) for probabilistic group testing. This was done by studying the average and minimum Hamming distances of constant-weight codes (such as Algebraic-Geometric codes) and relating them to the properties of group testing strategies. However, the explicit schemes in [21] achieve $t = \Theta(d \log^2 N / \log d)$, which is not order-optimal when d is poly-logarithmic in N. It is therefore of interest to find explicit, deterministic schemes that achieve $t = O(d \log N)$ tests.

This paper presents the first strongly explicit[1] scheme that achieves $t = O(d \log N)$. We show, perhaps surprisingly, that Kautz and Singleton's construction [19], a well known sub-optimal (for moderate values of d) explicit scheme for combinatorial group testing, is actually optimal for probabilistic group testing. We prove this result for both the noiseless and noisy (where test outcomes can be flipped at random) settings of probabilistic group testing framework. We prove the order-optimality of Kautz and Singleton's construction by analyzing the probability of a non-defective item being "covered" (c.f. Section II) by a random defective set directly, rather than arguing from combinatorial properties of the underlying code, which has been the main approach in the literature [19]–[21].

[1]Department of Electrical Engineering, Stanford University. hinan1, kairouzp, aozgur@stanford.edu

[2]Departments of Computer Science and Electrical Engineering, Stanford University. marykw@stanford.edu

This work was supported in part by NSF awards CCF-1514538 and NeTS-1817205.

[1]We will call a $t \times N$ matrix *strongly explicit* if any column of the matrix can be constructed in time poly(t). A matrix will be called *explicit* if it can be constructed in time poly(t, N).

We say a group testing scheme is *efficiently decodable* if there is a decoding strategy that runs in poly(t)-time. While we can achieve the decoding complexity of $O(tN)$ with the "cover decoder" (c.f. Section II), our goal is to bring the decoding complexity to poly(t). To this end, we use a recursive technique to convert the Kautz-Singleton construction into a strongly explicit construction with $t = O(d \log N \log\log_d N)$ tests and decoding complexity $O(d^3 \log N \log\log_d N)$. This provides an efficiently decodable scheme with only a log-log factor increase in the number of tests. Searching for order-optimal explicit or randomized constructions that are efficiently decodable remains an open problem.

C. Outline

The remainder of this paper is organized as follows. In Section II, we present the system model and necessary prerequisites. The optimality of the Kautz-Singleton construction in the probabilistic group testing setting is formally presented in Section III. We propose an efficiently decodable group testing strategy in Section IV. We defer the proof of the results to their corresponding sections in the appendix. We provide, in Section V, a brief survey of important results on group testing and a detailed comparison with Mazumdar's recent work in [21]. Finally, we conclude our paper in Section VI with a few interesting open problems.

II. System Model and Basic Definitions

For any $t \times N$ matrix M, we use M_i to refer to its i'th column and M_{ij} to refer to its (i,j)'th entry. The *support* of a column M_i is the set of coordinates where M_i has nonzero entries. For an integer $m \geq 1$, we denote the set $\{1, \ldots, m\}$ by $[m]$. The Hamming weight of a column of M will be simply referred to as the *weight* of the column.

We consider a model where there is a random defective set S of size d among the items $[N]$. We define $\mathcal{S}$ as the set of all possible defective sets, i.e., the set of $\binom{N}{d}$ subsets of $[N]$ of cardinality d and we let S be uniformly distributed over $\mathcal{S}$.[2] The goal is to determine S from the binary measurement vector Y of size t taking the form

$$Y = \left(\bigvee_{i \in S} M_i \right) \oplus v, \tag{1}$$

where $t \times N$ measurement matrix M indicates which items are included in the test, i.e., $M_{ij} = 1$ if the item j is participated in test i, $v \in \{0,1\}^t$ is a noise term, and $\oplus$ denotes modulo-2 addition. In words, the measurement vector Y is the Boolean OR combination of the columns of the measurement matrix M corresponding to the defective items in a possible noisy fashion. We are interested in both noiseless and noisy variant of the model in (1). In the noiseless case, we simply consider $v = 0$, i.e., $Y = \bigvee_{i \in S} M_i$. Note that the randomness in the measurement vector Y is only due to the random defective set in this case. On the other hand, in the noisy case we consider $v \sim \text{Bernoulli}(p)$ for some fixed constant $p \in (0, 0.5)$, i.e., each measurement is independently flipped with probability p.

Given M and Y, a decoding procedure forms an estimate $\hat{S}$ of S. The performance measure we consider in this paper is the *exact recovery* where the average probability of error is given by

$$P_e \triangleq \Pr(\hat{S} \neq S),$$

and is taken over the realizations of S and v (in the noisy case). The goal is to minimize the total number of tests t while achieving an arbitrary but fixed ϵ average probability of error, i.e., satisfying $P_e \leq \epsilon$.

A. Disjunctiveness

We say that a column M_i is *covered* by a set of columns $M_1, \ldots, M_l$ if the support of M_i is contained in the union of the supports of columns $M_1, \ldots, M_l$. A binary matrix M is called *d-disjunct* if any column of M is not covered by any other d columns. The d-disjunctiveness property ensures that we can recover any defective set of size d with zero error from the measurement vector Y in the noiseless case. This can be naively done using the *cover decoder* which runs in $O(tN)$-time. The cover decoder simply scans through the columns of M, and returns the ones that are covered by the measurement vector Y. When M is d-disjunct, the cover decoder succeeds at identifying all the defective items without any error.

In this work, we are interested in the probabilistic group testing problem where we allow an arbitrary but fixed ϵ average probability of error. Therefore we can relax the d-disjunctiveness property. In the noiseless case, it is sufficient to ensure that at least $(1-\epsilon)$ fraction of all possible defective sets do not cover any other column. A binary matrix satisfying this relaxed form is called an *almost disjunct* matrix [21]–[24] and with this condition one can achieve the desired ϵ average probability of error by applying the cover decoder.

B. Kautz-Singleton Construction

In their work [19], Kautz and Singleton provide a construction of disjunct matrices by converting a Reed-Solomon (RS) code [25] to a binary matrix. We begin with the definition of Reed-Solomon codes.

Definition 1: Let $\mathbb{F}_q$ be a finite field and $\alpha_1, \ldots, \alpha_n$ be distinct elements from $\mathbb{F}_q$. Let $k \leq n \leq q$. The Reed-Solomon code of dimension k over $\mathbb{F}_q$, with evaluation points $\alpha_1, \ldots, \alpha_n$ is defined with the following encoding function. The encoding of a message $m = (m_0, \ldots, m_{k-1})$ is the evaluation of the corresponding $k-1$ degree polynomial $f_m(X) = \sum_{i=0}^{k-1} m_i X^i$ at all the α_i's:

$$\text{RS}(m) = (f_m(\alpha_1), \ldots, f_m(\alpha_n)).$$

The Kautz-Singleton construction starts with a $[n,k]_q$ RS code with $n = q-1$ and $N = q^k$. Each q-ary symbol is then replaced by unit weight binary vectors of length q, via

[2] This assumption is not critical. Our results carry over to the setting where the defective items are sampled with replacement.

"identity mapping" which takes a symbol $i \in [q]$ and maps it to the vector in $\{0,1\}^q$ that has a 1 in the i'th position and zero everywhere else. Note that the resulting binary matrix will have $t = q(q-1)$ tests. This construction achieves a d-disjunct $t \times N$ binary matrix with $t = O(d^2 \log_d^2 N)$ by choosing the parameter q appropriately.

While this is a strongly explicit construction, it is sub-optimal for combinatorial group testing in the regime $d = O(\text{poly}(\log N))$: an explicit construction with smaller t (achieving $t = O(d^2 \log N)$) is introduced by Porat and Rothschild in [20]. Interestingly, we will show in the next section that this same strongly explicit construction that is suboptimal for combintorial group testing in fact achieves the order-optimal $t = \Theta(d \log N)$ result in both the noiseless and noisy versions of probabilistic group testing.

III. Optimality of the Kautz-Singleton construction

We begin with the noiseless case ($v = 0$ in (1)). The next theorem shows the optimality of the Kautz-Singleton construction with properly chosen parameters n and q.

Theorem 1: Under the noiseless model introduced in Section II, the Kautz-Singleton construction with parameters $q = \Theta(d)$ and $n = \Theta(\log N)$ achieves an arbitrary but fixed ϵ average probability of error with $t = \Theta(d \log N)$ tests in the regime $d = \Omega(\log^2 N)$.

The proof of the above theorem can be found in Appendix A. It is further possible to extend this result to the noisy setting where we consider $v \sim \text{Bernoulli}(p)$ for some fixed constant $p \in (0, 0.5)$, i.e., each measurement is independently flipped with probability p. Our next theorem shows the optimality of the Kautz-Singleton construction in this case.

Theorem 2: Under the noisy model introduced in Section II with some fixed constant $p \in (0, 0.5)$, the Kautz-Singleton construction with parameters $q = \Theta(d)$ and $n = \Theta(\log N)$ achieves an arbitrary but fixed ϵ average probability of error with $t = \Theta(d \log N)$ tests in the regime $d = \Omega(\log^2 N)$.

The proof of the above theorem can be found in Appendix B. Similar to the noiseless setting, the Kautz-Singleton construction provides a strongly explicit construction achieving optimal number of tests $t = \Theta(d \log N)$ in the noisy case.

IV. Decoding

While the cover decoder, which has a decoding complexity of $O(tN)$, might be reasonable for certain applications, there is a recent research effort towards low-complexity decoding schemes due to the emerging applications involving massive datasets [26]–[29]. The target is a decoding complexity of $\text{poly}(t)$. This is an exponential improvement in the running time over the cover decoder for moderate values of d. For the model we consider in this work (i.e., exact recovery of the defective set with $P_e \leq \epsilon$), there is no known efficiently decodable scheme with optimal $t = \Theta(d \log N)$ tests to the best of our knowledge. However, there is a recent line of work towards practical decoding schemes while preserving the order of t as much as possible. The work [28] presented a randomized scheme which identifies all the defective items with high probability with $O(d \log d \log N)$ tests and time complexity $O(d \log d \log N)$. Another recent result, [29], introduced an algorithm which requires $O(d \log d \log N)$ tests with $O(d(\log^2 d + \log N))$ decoding complexity. Note that the decoding complexity reduces to $O(d \log N)$ when $d = O(\text{poly}(\log N))$ which is order-optimal (and sub-linear in the number of tests), although the number of tests is not. In both [28] and [29], the number of tests is away from the optimal number of tests by a factor of $\log d$.

We can convert the strongly explicit constructions in Theorem 1 and 2 into strongly explicit constructions that are also efficiently decodable by using a recursive technique introduced in [27] where the authors construct efficiently decodable error-tolerant list disjunct matrices. For the sake of completeness, we next discuss the main idea applied to our case.

For a defective set S, the cover decoder goes through the columns of M and makes a decision whether an item is inside the defective set or not. This gives us the decoding complexity $O(tN)$. However, if we were to somehow obtain a superset S' where it is guaranteed that $S \subseteq S'$, then the naive decoder would run in time $O(t \cdot |S'|)$ which could potentially be more efficient depending on the size of S'. It turns out that we can construct this small set S' recursively.

Suppose that we have access to an efficiently decodable $t_1(d, \sqrt{N}, \epsilon/4, p) \times \sqrt{N}$ matrix $M^{(1)}$ that achieves exact recovery of the defective set with $P_e \leq \epsilon/4$. We will construct two $t_1(d, \sqrt{N}, \epsilon/4, p) \times N$ matrices $M^{(F)}$ and $M^{(L)}$ using $M^{(1)}$ as follows. The jth column of $M^{(1)}$ for $j \in [\sqrt{N}]$ is identical to all ith columns of $M^{(F)}$ for $i \in [N]$ if the *first* $\frac{1}{2}\log N$ bits of i is j where i and j are considered as their respective binary representations. Similarly, the jth column of $M^{(1)}$ for $j \in [\sqrt{N}]$ is identical to all ith columns of $M^{(L)}$ for $i \in [N]$ if the *last* $\frac{1}{2}\log N$ bits of i is j.

After getting the measurement vectors $Y^{(F)}$ and $Y^{(L)}$ from $Y^{(F)} = \bigvee_{i \in S} M_i^{(F)} \oplus v$ and $Y^{(L)} = \bigvee_{i \in S} M_i^{(L)} \oplus v$ we can apply the decoding algorithm for $M^{(1)}$ to $Y^{(F)}$ and $Y^{(L)}$ to obtain the estimate sets $\hat{S}^{(F)}$ and $\hat{S}^{(L)}$ respectively. Note that the sets $\hat{S}^{(F)}$ and $\hat{S}^{(L)}$ consist of $\frac{1}{2}\log N$-bit vectors and by union bound the set $S' = \hat{S}^{(F)} \times \hat{S}^{(L)}$ contains all the indices $i \in S$ with error probability at most $\epsilon/2$. We further note that $|S'| \leq d^2$.

We can now vertically stack $M^{(F)}$ and $M^{(L)}$ with a $t_2(d, N, \epsilon/2, p) \times N$ matrix $M^{(2)}$ which is not necessarily efficiently decodable to obtain our final matrix M. The decoding is as follows. We first decode the components of M corresponding to $M^{(F)}$ and $M^{(L)}$ to obtain $\hat{S}^{(F)}$ and $\hat{S}^{(L)}$ respectively. We next construct the set $S' = \hat{S}^{(F)} \times \hat{S}^{(L)}$. We finally apply the naive cover decoder to the component of M corresponding to $M^{(2)}$ over the set S' to compute the final estimate $\hat{S}$ which can be done with an additional $O(t_2 \cdot d^2)$ time. We provide this decoding scheme in Algorithm 1 for the special case $N = d^{2^i}$ for some non-negative integer i. Note that by union bound the probability of error is bounded by ϵ. The next theorem is the result of applying this idea recursively.

Theorem 3: Under the noiseless/noisy model introduced

Reference	Number of tests	Decoding complexity	Construction
[30]	$t = \Theta(d \log N)$	$O(tN)$	Randomized
[21]	$t = O(d \log^2 N / \log d)$	$O(tN)$	Strongly explicit
[28]	$t = O(d \log d \log N)$	$O(d \log d \log N)$	Randomized
[29]	$t = O(d \log d \log N)$	$O(d(\log^2 d + \log N))$	Randomized
This work	$t = \Theta(d \log N)$	$O(tN)$	Strongly explicit
This work	$t = O(d \log N \log \log_d N)$	$O(d^3 \log N \log \log_d N)$	Strongly explicit

TABLE I

COMPARISON OF NON-ADAPTIVE PROBABILISTIC GROUP TESTING RESULTS.

Algorithm 1: The decoding alg. *decode*(Y, M, d, N)

Input: The measurement vector Y, the group testing matrix M, the defective set size d, the number of items N

Output: The defective set estimate $\hat{S}$

if $N = d$ **then**
  Return the defective set using Y (individual testing);
else
  Compute $M^{(1)}$ and $M^{(2)}$ (as described in the text);
  Compute $Y^{(F)}$ and $Y^{(L)}$ (as described in the text);
  $\hat{S}^{(F)} = decode(Y^{(F)}, M^{(1)}, d, \sqrt{N})$;
  $\hat{S}^{(L)} = decode(Y^{(L)}, M^{(1)}, d, \sqrt{N})$;
  if $|\hat{S}^{(F)}| > d$ *or* $|\hat{S}^{(L)}| > d$ **then**
    return $\{\}$;
  Construct $S' = \hat{S}^{(F)} \times \hat{S}^{(L)}$;
  Apply the cover decoder to $M^{(2)}$ over the set S' and compute $\hat{S}$;
  Return $\hat{S}$;

in Section II, there exists a strongly explicit construction achieving an arbitrary but fixed ϵ average probability of error with $t = O(d \log N \log \log_d N)$ number of tests that can be decoded in time $O(d^3 \log N \log \log_d N)$ in the regime $d = \Omega(\log^2 N)$.

We defer a formal proof of this result to the full version of the paper. We note that with only $\log \log_d N$ extra factor in the number of tests, the decoding complexity can be brought to the desired $O(\text{poly}(t))$ complexity. We further note that the number of tests becomes order-optimal in the regime $d = \Theta(N^\alpha)$ for some $\alpha \in (0, 1)$. In Table I we provide the results presented in this work along with the related results in the literature.

V. RELATED WORK

The literature on the non-adaptive group testing framework includes both explicit and random test designs [12]. In combinatorial group testing, a famous construction introduced by Kautz and Singleton [19] achieves $t = O(d^2 \log_d^2 N)$ tests matching the best known lower bound $\Omega(d^2 \log_d N)$ [17], [18] in the regime where $d = \theta(N^\alpha)$ for some $\alpha \in (0, 1)$. However, this strongly explicit construction is suboptimal in the regime where $d = O(\text{poly}(\log N))$. An explicit construction achieving $t = O(d^2 \log N)$ was introduced by Porat and Rothschild in [20]. While $t = O(d^2 \log N)$ is the best known achievability result in combinatorial group testing framework, there is no strongly explicit construction matching it to the best of our knowledge. Regarding efficient decoding, recently Indyk, Ngo and Rudra [26] introduced a randomized construction with $t = O(d^2 \log(N))$ tests that could be decoded in time poly(t). Furthermore, their construction can be derandomized in the regime $d = O(\log N / \log \log N)$. Later Ngo, Porat and Rudra [27] removed the constraint on d and provided an explicit construction that can be decoded in time poly(t).

On the other hand, there are various schemes relaxing the 0-error criteria in the group testing problem. For instance, a model where the decoder always outputs a super-set of the defectives containing less than l other non-defective items was studied in [31]–[33]. Another framework where the goal is to recover at least a $(1 - \epsilon)$-fraction (for any arbitrarily small $\epsilon > 0$) of the defective set with high probability was studied in [28] where the authors provided a scheme with order-optimal $O(d \log N)$ tests and the computational complexity. There are also different versions of the group testing problem in which a test can have more than two outcomes [34], [35] or can be threshold based [36]–[38]. More recently, sparse group testing frameworks for both combinatorial and probabilistic settings were studied in [39]–[41].

When the defective set is assumed to be uniformly random, it is known that $t = \Theta(d \log N)$ is order-optimal for achieving the exact recovery of the defective set with ϵ error probability guarantee (which is the model considered in this work) using random designs and information-theoretical tools [13], [16], [30]. These results also include noisy variants of the group testing problem. Efficient recovery algorithms with nearly optimal number of tests were introduced recently in [28] and [29]. Regarding deterministic constructions in this model, recently Mazumdar [21] introduced an analysis connecting the group testing properties with the *average* Hamming distance between the columns of the measurement matrix and obtained (strongly) explicit constructions with $t = O(d \log^2 N / \log d)$ tests. While this result is order-optimal in the regime where $d = \Theta(N^\alpha)$ for some $\alpha \in (0, 1)$, it is

suboptimal for the moderate values of d. The performance of the Kautz-Singleton construction in the random model has been studied empirically [42], but we are not aware of any theoretical analysis of it beyond what follows immediately from the distance of Reed-Solomon codes. To the best of our knowledge there is no known explicit/strongly explicit construction achieving $t = \Theta(d \log N)$ tests in general for the noiseless/noisy version of the probabilistic group testing problem.

VI. Conclusion

In this work, we showed that the Kautz-Singleton construction is order-optimal in the noiseless and noisy variants of the probabilistic group testing problem. To the best of our knowledge, this is the first (strongly) explicit construction achieving order-optimal number of tests in the probabilistic group testing setting. We provided a novel analysis departing from the classical approaches in the literature that use combinatorial properties of the underlying code. We instead directly explored the probability of a non-defective item being covered by a random defective set using the properties of Reed-Solomon codes in our analysis. Furthermore, by using a recursive technique, we converted the Kautz-Singleton construction into a construction that is also efficiently decodable with only a log-log factor increase in number of tests which provides interesting tradeoffs compared to the existing results in the literature.

There are a number of nontrivial extensions to our work. Firstly, it would be interesting to extend these results to the regime $d = o(\log^2 N)$. Another interesting line of work would be to find a deterministic/randomized construction achieving order-optimal $t = \Theta(d \log N)$ tests and is also efficiently decodable.

Acknowledgements

The third author would like to thank Atri Rudra and Hung Ngo for helpful conversations.

Appendix

A. The proof of Theorem 1

Let N be the number of items and d be the size of the random defective set. We will employ the Kautz-Singleton construction. We use a $[n, k]_q$ RS code such that $N = q^k$ and we pick n and q appropriately in the following. Note that the resulting $t \times N$ binary matrix M has $t = nq$ tests.

We note that for any defective set the cover decoder provides the exact recovery given that none of the non-defective items are covered. For $s \subseteq [N]$, we define $\mathcal{A}^s$ as the event that there exists a non-defective column of M that is covered by the defective set s. Define $\mathcal{A}_i^s$ as the event that the non-defective column M_i is covered by the defective set s. We can bound the probability of error as follows:

$$\begin{aligned}
P_e &\leq \sum_{s\subseteq[N],|s|=d} 1(\mathcal{A}^s)\Pr(S=s) \\
&\leq \frac{1}{\binom{N}{d}} \sum_{s\subseteq[N],|s|=d} \sum_{i\in[N]\setminus s} 1(\mathcal{A}_i^s) \\
&= \frac{1}{\binom{N}{d}} \sum_{i\in[N]} \sum_{s\subseteq[N]/\{i\},|s|=d} 1(\mathcal{A}_i^s) \\
&= \frac{\binom{N-1}{d}}{\binom{N}{d}} \sum_{i\in[N]} \frac{1}{\binom{N-1}{d}} \sum_{s\subseteq[N]/\{i\},|s|=d} 1(\mathcal{A}_i^s) \\
&= \frac{N-d}{N} \sum_{i\in[N]} \Pr(\mathcal{A}_i^S) \qquad (2)
\end{aligned}$$

where in the last equation S is uniformly distributed on the sets of size d among the items in $[N]/\{i\}$ and $1(\cdot)$ denotes the indicator function of an event.

Fix any n distinct elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ from $\mathbb{F}_q$. We denote $\Psi \triangleq \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. We note that due to the structure of mapping to the binary vectors in the Kautz-Singleton construction, a column M_i is covered by the random defective set S if and only if the corresponding symbols of M_i is contained in the union of symbols of S in RS code for all rows in $[n]$. Denoting $f_{m_i}(X)$ as the polynomial corresponding to the column M_i, we have

$$\begin{aligned}
\Pr(\mathcal{A}_i^S) &= \Pr(f_{m_i}(\alpha) \in \{f_{m_j}(\alpha) : j \in S\} \ \forall\ \alpha \in \Psi) \\
&= \Pr(0 \in \{f_{m_j}(\alpha) - f_{m_i}(\alpha) : j \in S\} \ \forall\ \alpha \in \Psi) \\
&= \Pr(0 \in \{f_{m_j}(\alpha) : j \in S\} \ \forall\ \alpha \in \Psi)
\end{aligned}$$

where in the last step the random set of polynomials $\{f_{m_j}(X) : j \in S\}$ is generated by picking d nonzero polynomials of degree at most $k-1$ without replacement. We define the random polynomial $h(X) \triangleq \prod_{j\in S} f_{m_j}(X)$. Note that

$$0 \in \{f_{m_j}(\alpha) : j \in S\} \ \forall\ \alpha \in \Psi \ \Leftrightarrow\ h(\alpha) = 0 \ \forall\ \alpha \in \Psi.$$

We next bound the number of roots of the polynomial $h(X)$. We will use the following result from [43].

Lemma 1 ([43], Lemma 3.9): Let $R_q(l, k)$ denote the set of nonzero polynomials over $\mathbb{F}_q$ of degree at most k that have exactly l distinct roots in $\mathbb{F}_q$. For all powers q and integers l, k,

$$|R_q(l, k)| \leq q^{k+1} \cdot \frac{1}{l!}.$$

Let r denote the number of roots of a random nonzero polynomial of degree at most $k-1$. It is easy to observe that $\mathbb{E}[r] \leq 1$ and using Lemma 1, we get

$$\begin{aligned}
\mathbb{E}[r^2] &\leq \sum_{i=1}^{k-1} \frac{i^2}{i!} \\
&= \sum_{i=1}^{k-1} \frac{i-1}{(i-1)!} + \sum_{i=1}^{k-1} \frac{1}{(i-1)!} \\
&< 2e.
\end{aligned}$$

Hence we can bound $\mathbb{E}[r^2] < 6$. We denote r_i as the number of roots of the polynomial $f_{m_i}(X)$ and r_h as the number of roots of the polynomial $h(X)$. Note that $r_h \leq \sum_{j\in S} r_j$. We next use the Bernstein concentration bound for sampling without replacement [44]:

$$\begin{aligned}\Pr\left(\sum_{j\in S} r_j > 7d\right) &= \Pr\left(\frac{1}{d}\sum_{j\in S} r_j > 7\right)\\ &\leq \Pr\left(\frac{1}{d}\sum_{j\in S}(r_j - \mathbb{E}[r_j]) > 6\right)\\ &\leq \exp\left(-\frac{36d}{12+6k(2/3)}\right)\\ &\leq \exp\left(-\frac{36d}{16k}\right).\end{aligned}$$

We have $k = \log N/\log q$, hence, under the regime $d = \Omega(\log^2 N)$, the last quantity is bounded by $N^{-c\log q}$ for some constant $c > 0$. Hence the number of roots of the polynomial $h(X)$ is bounded by $7d$ with high probability.

Given the condition that the number of roots of the polynomial $h(X)$ is bounded by $7d$ and the random set of polynomials $\{f_{m_j}(X) : j \in S\}$ is picked from the nonzero polynomials of degree at most $k-1$ without replacement, due to the symmetry, we claim that the probability of satisfying $h(\alpha) = 0$ for all $\alpha \in \Psi$ is bounded by the probability of covering n elements from a field of size q by picking $7d$ elements randomly without replacement. We next prove this claim. We define the set $R(h) \coloneqq \{\alpha \in \mathbb{F}_q : h(\alpha) = 0\}$ and we emphasize that this is not a multiset, i.e., the repeated roots appear as a single element. We begin with the following observation.

Claim 1: Let $l > 0$, and condition on the event that $|R(h)| = l$. Then $R(h)$ is uniformly distributed among all sets $\Lambda \subseteq \mathbb{F}_q$ of size l.

Proof: For $f \in \mathbb{F}_q[X]$, we can write

$$f(X) = g_f(X)\cdot\prod_{\gamma_i\in R(f)}(X-\gamma_i)^{c_i},$$

where c_i is the corresponding multiplicity of the root γ_i and $g_f \in \mathbb{F}_q[X]$ does not have any linear factor. We note that this decomposition is unique. For $\Lambda \subseteq \mathbb{F}_q$ of size l, let

$$H_\Lambda \coloneqq \left\{\{f_1(X),\dots,f_d(X)\} : R\left(\prod_i f_i(X)\right) = \Lambda\right\}.$$

Let $\Lambda' \subseteq \mathbb{F}_q$ such that $|\Lambda'| = l$ and $\Lambda' \neq \Lambda$. Then $|H_\Lambda| = |H_{\Lambda'}|$. Indeed, let $\varphi : \mathbb{F}_q \to \mathbb{F}_q$ be a bijection such that $\varphi(\Lambda) = \Lambda'$. Then $\Phi : H_\Lambda \to H_{\Lambda'}$ given by

$$\Phi(f) = g_f(X)\cdot\prod_{\gamma_i\in R(f)}(X-\varphi(\gamma_i))^{c_i},$$

and $\Phi(\{f_1,\dots,f_d\}) \coloneqq \{\Phi(f_1),\dots,\Phi(f_d)\}$ is a bijection.

We further note that $R(h) = \Lambda \Rightarrow |R(h)| = l$, so

$$\begin{aligned}\Pr\{R(h) = \Lambda \,\big|\, |R(h)| = l\} &= \frac{\Pr\{R(h)=\Lambda\}}{\Pr\{|R(h)|=l\}}\\ &= \frac{\Pr\{\{f_1,\dots,f_d\}\in H_\Lambda\}}{\Pr\{|R(h)|=l\}}\\ &\overset{(i)}{=} \frac{\Pr\{\{f_1,\dots,f_d\}\in H_{\Lambda'}\}}{\Pr\{|R(h)|=l\}}\\ &= \Pr\{R(h)=\Lambda' \,\big|\, |R(h)|=l\},\end{aligned}$$

where (i) is due to $|H_\Lambda| = |H_{\Lambda'}|$ and we pick $f_1,\dots,f_d$ uniformly with replacement. ∎

Based on this, we have

$$\begin{aligned}&\Pr\{R(h)\supseteq\Psi \,\big|\, |R(h)|\leq 7d\}\\ &= \sum_{l\leq 7d}\Pr\{R(h)\supseteq\Psi \,\big|\, |R(h)|=l\}\\ &\qquad\cdot\Pr\{|R(h)|=l \,\big|\, |R(h)|\leq 7d\}\\ &\leq \max_{l\leq 7d}\Pr\{R(h)\supseteq\Psi \,\big|\, |R(h)|=l\}\\ &= \max_{l\leq 7d}\frac{\binom{q-n}{l-n}}{\binom{q}{l}}.\end{aligned}$$

Let us fix $q = 14d$. We then have

$$\begin{aligned}\Pr\{R(h)\supseteq\Psi \,\big|\, |R(h)|\leq 7d\} &\leq \frac{\binom{14d-n}{7d-n}}{\binom{14d}{7d}}\\ &= \frac{(14d-n)!}{(7d-n)!(7d)!}\frac{(7d)!(7d)!}{(14d)!}\\ &= \frac{7d\dots(7d-n+1)}{14d\dots(14d-n+1)}\\ &\leq \left(\frac{1}{2}\right)^n.\end{aligned}$$

Therefore, $\Pr(\mathcal{A}_i^S)$ is bounded by

$$\begin{aligned}\Pr(\mathcal{A}_i^S) &\leq \Pr\{R(h)\supseteq\Psi \,\big|\, |R(h)|\leq 7d\} + \Pr\{|R(h)|>7d\}\\ &\leq \left(\frac{1}{2}\right)^n + N^{-c\log q}.\end{aligned}$$

Applying the summation over all $i \in [N]$ in (2), we obtain $P_e \leq N^{1-c\log q} + N2^{-n}$. Therefore, under the regime $d = \Omega(\log^2 N)$, an arbitrary but fixed ϵ average probability of error can be achieved with $n = \Theta(\log N)$. The resulting $t \times N$ binary matrix M has $t = nq = \Theta(d\log N)$ tests.

B. The proof of Theorem 2

We begin with describing the decoding rule. Since we are considering the noisy model, we will slightly modify the cover decoder employed in the noiseless case. For any defective item with codeword weight w, in the noiseless outcome the tests in which this item participated will be all positive. On the other hand, when the noise is added, wp of these tests will flip in expectation. Based on this observation (see **No-CoMa** in [30] for a more detailed discussion), we consider the following decoding rule. For any item $i \in [N]$, we first denote w_i as the weight of the corresponding column M_i and $\hat{w}_i$ as the number of rows $k \in [t]$ where both

$M_{k,i} = 1$ and $Y_k = 1$. If $\hat{w}_i \geq w_i(1-p(1+\tau))$, then the ith item is declared as defective, else it is declared to be non-defective.

Under the aforementioned decoding rule, an error event happens either when $\hat{w}_i < w_i(1-p(1+\tau))$ for a defective item i or $\hat{w}_i \geq w_i(1-p(1+\tau))$ for a non-defective item i. Using the union bound, we can bound the probability of error as follows:

$$\begin{aligned}
P_e &\leq \frac{1}{\binom{N}{d}} \sum_{s\subseteq[N],|s|=d} \Bigg[\sum_{i\in[N]\setminus s} \Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))\} \\
&\qquad + \sum_{i\in s} \Pr\{\hat{w}_i < w_i(1-p(1+\tau))\}\Bigg] \\
&= \frac{1}{\binom{N}{d}} \sum_{i\in[N]} \sum_{s\subseteq[N]/\{i\},|s|=d} \Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))\} \\
&\qquad + \frac{1}{\binom{N}{d}} \sum_{s\subseteq[N],|s|=d} \sum_{i\in s} \Pr\{\hat{w}_i < w_i(1-p(1+\tau))\} \\
&= \frac{\binom{N-1}{d}}{\binom{N}{d}} \Bigg(\sum_{i\in[N]} \frac{1}{\binom{N-1}{d}} \\
&\qquad \cdot \sum_{s\subseteq[N]/\{i\},|s|=d} \Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))\}\Bigg) \\
&\quad + \frac{1}{\binom{N}{d}} \sum_{s\subseteq[N],|s|=d} \sum_{i\in s} \Pr\{\hat{w}_i < w_i(1-p(1+\tau))\} \\
&= \frac{N-d}{N} \sum_{i\in[N]} \Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))\} \\
&\qquad + \frac{1}{\binom{N}{d}} \sum_{s\subseteq[N],|s|=d} \sum_{i\in s} \Pr\{\hat{w}_i < w_i(1-p(1+\tau))\} \\
&=: P_1 + P_2,
\end{aligned}$$

where in the first quantity of the last equation S is randomly distributed on the sets of size d among the items in $[N]/\{i\}$. We denote the first quantity as P_1 and the second one as P_2 in the last equation.

We will employ the Kautz-Singleton construction. We use a $[n,k]_q$ RS code such that $N = q^k$ and we pick n and q appropriately in the following. Fix any n distinct elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ from $\mathbb{F}_q$. We denote $\Psi \triangleq \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$.

We begin with P_2. Fix any defective set s in $[N]$ with size d and fix an arbitrary element i of this set. We first note that $w_i = n$ due to the Kautz-Singleton construction. We further note that before the addition of noise the noiseless outcome will have positive entries corresponding to the ones where $M_{k,i} = 1$. Therefore $\Pr\{\hat{w}_i < w_i(1-p(1+\tau))\}$ only depends on the number of bit flips due to the noise. Using Hoeffding's inequality, we have

$$\Pr\{\hat{w}_i < w_i(1-p(1+\tau))\} \leq e^{-2np^2\tau^2}.$$

Summing over the d defective items $i \in s$, we get $P_2 \leq de^{-2np^2\tau^2}$.

We continue with P_1. We fix an item $i \in [N]$ and note that $w_i = n$. We similarly define the random polynomial $h(X) \triangleq \prod_{j\in S} f_{m_j}(X)$. Let $\mathcal{A}$ be the event of $h(X)$ having at most $7d$ number of roots. We then have

$$\begin{aligned}
&\Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))\} \\
&\qquad \leq \Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))|\mathcal{A}\} + \Pr\{\mathcal{A}^c\}.
\end{aligned} \tag{3}$$

Following similar steps as in the proof of Theorem 1 we obtain $\Pr\{\mathcal{A}^c\} \leq N^{-c\log q}$ for some constant $c > 0$ in the regime $d = \Omega(\log^2 N)$.

We next bound the first term in (3). We choose $q = 84d$ and define the random set $\Upsilon = \{\alpha \in \Psi : f_{m_i}(\alpha) \in \{f_{m_j}(\alpha) : j \in S\}\}$. We then have

$$\begin{aligned}
&\Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))|\mathcal{A}\} \leq \\
&\Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))|\mathcal{A}, |\Upsilon| \leq n/4\} \Pr\{|\Upsilon| \leq n/4|\mathcal{A}\} \\
&\qquad + \Pr\{|\Upsilon| > n/4|\mathcal{A}\} \\
&\leq \Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))|\mathcal{A}, |\Upsilon| \leq n/4\} \\
&\qquad + \Pr\{|\Upsilon| > n/4|\mathcal{A}\}.
\end{aligned}$$

Let us first bound the second term $\Pr\{|\Upsilon| > n/4|\mathcal{A}\}$. We note that

$$\begin{aligned}
|\Upsilon| &= |\{\alpha \in \Psi : f_{m_i}(\alpha) \in \{f_{m_j}(\alpha) : j \in S\}\}| \\
&= |\{\alpha \in \Psi : 0 \in \{f_{m_j}(\alpha) - f_{m_i}(\alpha) : j \in S\}\}| \\
&= |\{\alpha \in \Psi : 0 \in \{f_{m_j}(\alpha) : j \in S\}\}|
\end{aligned}$$

where in the last equality the random set of polynomials $\{f_{m_j}(X) : j \in S\}$ is generated by picking d nonzero polynomials of degree at most $k-1$ without replacement. Following similar steps of the proof of Theorem 1 we can bound $\Pr\{|\Upsilon| > n/4|\mathcal{A}\}$ by considering the probability of having at least $n/4$ symbols from Ψ when we pick $7d$ symbols from $[q]$ uniformly at random without replacement. Hence we have

$$\begin{aligned}
\Pr\{|\Upsilon| > n/4|\mathcal{A}\} &\leq \frac{\binom{n}{n/4}\binom{q-n/4}{7d-n/4}}{\binom{q}{7d}} \\
&= \frac{\binom{n}{n/4}\binom{84d-n/4}{7d-n/4}}{\binom{84d}{7d}} \\
&\leq (4e)^{n/4} \frac{(84d-n/4)!}{(7d-n/4)!(77d)!} \frac{(7d)!(77d)!}{(84d)!} \\
&\leq \left(\frac{4e}{12}\right)^{n/4}
\end{aligned}$$

where we use $\binom{n}{k} \leq (en/k)^k$ in the second inequality.

We continue with $\Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))|\mathcal{A}, |\Upsilon| \leq n/4\}$. Note that $w_i = n$. We further note that

$$\mathbb{E}[\hat{w}_i] = \mathbb{E}[\mathbb{E}[\hat{w}_i|\Upsilon]] = \mathbb{E}[|\Upsilon|](1-p) + (n - \mathbb{E}[|\Upsilon|])p.$$

Since $p \in (0, 0.5)$ we have $\mathbb{E}[\hat{w}_i \mid |\Upsilon| \leq n/4] \leq (n/4)(1-p) + (3n/4)p = n/4 + (n/2)p$. Using Hoeffding's inequality, we have

$$\begin{aligned}
&\Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))|\mathcal{A}, |\Upsilon| \leq n/4\} \\
&\leq \Pr\{\hat{w}_i - \mathbb{E}[\hat{w}_i] \geq n(3/4 - 3p/2 - p\tau)|\mathcal{A}, |\Upsilon| \leq n/4\} \\
&\leq e^{-2n(3/4-3p/2-p\tau)^2}
\end{aligned}$$

where the condition $3/4 - 3p/2 - p\tau > 0$ or $\tau < (3/4 - 3p/2)/p$ can be satisfied with our choice of free parameter τ since $p < 1/2$. Combining everything, we obtain

$$P_e \leq N^{1-c\log q} + N(e/3)^{n/4} + Ne^{-2n(3/4-3p/2-p\tau)^2} + de^{-2np^2\tau^2}.$$

Therefore, under the regime $d = \Omega(\log^2 N)$, an arbitrary but fixed ϵ average probability of error can be achieved with $n = \Theta(\log N)$. The resulting $t \times N$ binary matrix M has $t = nq = \Theta(d \log N)$ tests.

REFERENCES

[1] R. Dorfman, "The detection of defective members of large populations," *The Annals of Mathematical Statistics*, vol. 14, no. 4, pp. 436–440, 1943.

[2] H-B. Chen and F. K. Hwang, "A survey on nonadaptive group testing algorithms through the angle of decoding," *Journal of Combinatorial Optimization*, vol. 15, no. 1, pp. 49–59, 2008.

[3] A. Ganesan, S. Jaggi, and V. Saligrama, "Learning immune-defectives graph through group tests," *IEEE Transactions on Information Theory*, 2017.

[4] D. Malioutov and K. Varshney, "Exact rule learning via boolean compressed sensing," in *International Conference on Machine Learning*, 2013, pp. 765–773.

[5] A. C. Gilbert, M. A. Iwen, and M. J. Strauss, "Group testing and sparse signal recovery," in *Signals, Systems and Computers, 2008 42nd Asilomar Conference on*. IEEE, 2008, pp. 1059–1063.

[6] A. Emad and O. Milenkovic, "Poisson group testing: A probabilistic model for nonadaptive streaming boolean compressed sensing," in *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*. IEEE, 2014, pp. 3335–3339.

[7] T. Berger, N. Mehravari, D. Towsley, and J. Wolf, "Random multiple-access communication and group testing," *Communications, IEEE Transactions on*, vol. 32, no. 7, pp. 769 – 779, jul 1984.

[8] J. K. Wolf, "Born again group testing: Multiaccess communications," *Information Theory, IEEE Transactions on*, vol. 31, no. 2, pp. 185–191, 1985.

[9] J. Luo and D. Guo, "Neighbor discovery in wireless ad hoc networks based on group testing," in *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on*. IEEE, 2008, pp. 791–797.

[10] A. K. Fletcher, V.K. Goyal, and S. Rangan, "A sparsity detection framework for on-off random access channels," in *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*. IEEE, 2009, pp. 169–173.

[11] H. Q. Ngo and D-Z. Du, "A survey on combinatorial group testing algorithms with applications to dna library screening," *Discrete mathematical problems with medical applications*, vol. 55, pp. 171–182, 2000.

[12] D. Du and F. K. Hwang, *Combinatorial group testing and its applications*, vol. 12, World Scientific, 2000.

[13] G. K. Atia and V. Saligrama, "Boolean compressed sensing and noisy group testing," *Information Theory, IEEE Transactions on*, vol. 58, no. 3, pp. 1880–1901, 2012.

[14] C. L. Chan, P. H. Che, S. Jaggi, and V. Saligrama, "Non-adaptive probabilistic group testing with noisy measurements: Near-optimal bounds with efficient algorithms," in *2011 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sept 2011, pp. 1832–1839.

[15] D. Sejdinovic and O. Johnson, "Note on noisy group testing: Asymptotic bounds and belief propagation reconstruction," *CoRR*, vol. abs/1010.2441, 2010.

[16] J. Scarlett and V. Cevher, "Phase Transitions in Group Testing," in *ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2016.

[17] A. G. D'yachkov and V. V. Rykov, "Bounds on the length of disjunctive codes," *Problemy Peredachi Informatsii*, vol. 18, no. 3, pp. 7–13, 1982.

[18] F. Zoltán, "On r-cover-free families," *Journal of Combinatorial Theory, Series A*, vol. 73, no. 1, pp. 172–173, 1996.

[19] W. Kautz and R. Singleton, "Nonrandom binary superimposed codes," *IEEE Transactions on Information Theory*, vol. 10, no. 4, pp. 363–377, October 1964.

[20] E. Porat and A. Rothschild, "Explicit non-adaptive combinatorial group testing schemes," *Automata, Languages and Programming*, pp. 748–759, 2008.

[21] A. Mazumdar, "Nonadaptive group testing with random set of defectives," *IEEE Transactions on Information Theory*, vol. 62, no. 12, pp. 7522–7531, Dec 2016.

[22] A. J. Macula, V. V. Rykov, and S. Yekhanin, "Trivial two-stage group testing for complexes using almost disjunct matrices," *Discrete Applied Mathematics*, vol. 137, no. 1, pp. 97 – 107, 2004.

[23] M. B. Malyutov, "The separating property of random matrices," *Math. Notes*, vol. 23, no. 1, pp. 84–91, 1978.

[24] A. Zhigljavsky, "Probabilistic existence theorems in group testing," *J. Statist. Planning Inference*, vol. 115, no. 1, pp. 1–43, 2003.

[25] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300–304, 1960.

[26] P. Indyk, H. Q. Ngo, and A. Rudra, "Efficiently decodable non-adaptive group testing," in *Proceedings of the Twenty-First Annual ACM-SIAM Symposium on Discrete Algorithms*. Society for Industrial and Applied Mathematics, 2010, pp. 1126–1142.

[27] H. Q. Ngo, E. Porat, and A. Rudra, "Efficiently decodable error-correcting list disjunct matrices and applications," in *Automata, Languages and Programming*, Berlin, Heidelberg, 2011, pp. 557–568, Springer Berlin Heidelberg.

[28] K. Lee, R. Pedarsani, and K. Ramchandran, "Saffron: A fast, efficient, and robust framework for group testing based on sparse-graph codes," in *ISIT 2016*, pp. 2873–2877.

[29] S. Cai, M. Jahangoshahi, M. Bakshi, and S. Jaggi, "Efficient algorithms for noisy group testing," *IEEE Transactions on Information Theory*, vol. 63, no. 4, pp. 2113–2136, April 2017.

[30] C. L. Chan, S. Jaggi, V. Saligrama, and S. Agnihotri, "Non-adaptive group testing: Explicit bounds and novel algorithms," *IEEE Trans. on Information Theory*, vol. 60, no. 5, pp. 3019–3035, May 2014.

[31] A. G. D'yachkov and V. V. Rykov, "A survey of superimposed code theory," *Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform.*, vol. 12, pp. 229–242, 1983.

[32] A. De Bonis., L. Gasieniec, and U. Vaccaro, "Optimal two-stage algorithms for group testing problems," *SIAM J. Comput.*, vol. 34, no. 5, pp. 1253–1270, 2005.

[33] A. M. Rashad, "Random coding bounds on the rate for list-decoding superimposed codes," *Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform.*, vol. 19(2), pp. 141–149, 1990.

[34] M. Sobel, S. Kumar, and S. Blumenthal, "Symmetric binomial group-testing with three outcomes," in *Proc. Purdue Symp. Decision Procedure*, 1971, pp. 119–160.

[35] F. Hwang, "Three versions of a group testing game," *SIAM Journal on Algebraic Discrete Methods*, vol. 5, no. 2, pp. 145–153, 1984.

[36] H-B. Chen and H-L. Fu, "Nonadaptive algorithms for threshold group testing," *Discrete Applied Mathematics*, vol. 157, no. 7, pp. 1581 – 1585, 2009.

[37] M. Cheraghchi, "Improved constructions for non-adaptive threshold group testing," *CoRR*, vol. abs/1002.2244, 2010.

[38] T. V. Bui, M. Kuribayashi, M. Cheraghchi, and I. Echizen, "Efficiently decodable non-adaptive threshold group testing," *CoRR*, vol. abs/1712.07509, 2017.

[39] H. A. Inan, P. Kairouz, and A. Ozgur, "Sparse group testing codes for low-energy massive random access," in *2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Oct 2017, pp. 658–665.

[40] V. Gandikota, E. Grigorescu, S. Jaggi, and S. Zhou, "Nearly optimal sparse group testing," in *2016 54th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sept 2016, pp. 401–408.

[41] H. A. Inan, P. Kairouz, and A. Ozgur, "Energy-limited massive random access via noisy group testing," in *Information Theory (ISIT), 2018 IEEE International Symposium on*. IEEE, 2018, pp. 1101–1105.

[42] Y. Erlich, A. Gilbert, H. Ngo, A. Rudra, N. Thierry-Mieg, M. Wootters, D. Zielinski, and O. Zuk, "Biological screens from linear codes: theory and tools," *bioRxiv*, 2015.

[43] T. Hartman and R. Raz, "On the distribution of the number of roots of polynomials and explicit weak designs," *Random Structures & Algorithms*, vol. 23, no. 3, pp. 235–263, 2003.

[44] S. Boucheron, G. Lugosi, and P. Massart, *Concentration inequalities. A nonasymptotic theory of independence*, Oxford University Press, 2013.