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

Huseyin A. Inan, *Member, IEEE*, Peter Kairouz, *Member, IEEE*, Mary Wootters, *Member, IEEE*, and Ayfer Özgür, *Member, IEEE*

***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 the $\Theta(d \log N)$ tests are necessary and sufficient to recover the defective set with vanishing probability of error when $d = O(N^{\alpha})$ for some $\alpha \in (0, 1)$. However, to the best of our knowledge, there is no explicit (deterministic) construction achieving $\Theta(d \log N)$ tests in general. In this paper, 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 when $d = \Omega(\log^2 N)$. This provides a strongly explicit construction achieving the order optimal result in the probabilistic group testing setting for a wide range of values of d. 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.**

***Index Terms*— Algorithm design and analysis, group testing, explicit constructions, efficient decoding.**

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.

Manuscript received August 4, 2018; revised February 23, 2019; accepted February 23, 2019. Date of publication March 1, 2019; date of current version August 16, 2019. This work was supported in part by NSF under Award NeTS: 1817205. This paper was presented at the 2018 Allerton.

H. A. Inan is with the Department of Electrical Engineering, Stanford, CA 94305 USA (e-mail: hinan1@stanford.edu).

P. Kairouz is with Google AI, Mountain View, CA 94043 USA (e-mail: kairouz@google.com).

M. Wootters is with the Department of Computer Science and the Department of Electrical Engineering, Stanford, CA 94305 USA (e-mail: marykw@stanford.edu).

A. Özgür is with the Department of Electrical Engineering, Stanford, CA 94305 USA (e-mail: aozgur@stanford.edu).

Communicated by A. Rudra, Associate Editor for Complexity.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2019.2902397

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]–[20].

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 $t = \min\{N, \Omega(d^2 \log_d N)\}$ tests [21], [22]. A strongly explicit construction[1] that achieves $t = O(d^2 \log_d^2 N)$ was introduced by Kautz and Singleton in [23]. A more recent explicit construction achieving $t = O(d^2 \log N)$ was introduced by Porat and Rothschild [24]. We note that the Kautz-Singleton construction matches the best known lower bound $\Omega(d^2 \log_d N)$ in the regime where $d = \Theta(N^{\alpha})$ for some $\alpha \in (0, 1)$. However, for moderate values of d (e.g., $d = O(\text{poly}(\log N))$), the construction introduced by Porat and Rothschild achieving $t = O(d^2 \log N)$ is more efficient and the Kautz-Singleton construction is suboptimal in this regime.

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 only $t = \Theta(d \log N)$ tests when $d = O(N^{1-\alpha})$ for some $\alpha \in (0, 1)$ [15]–[17]. 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

[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).

randomized (i.e., M is randomly constructed) [13]–[20]. Recently, Mazumdar [25] presented explicit schemes (deterministic constructions of M) for probabilistic group testing framework. 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 [25] 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 a strongly explicit scheme that achieves $t = O(d \log N)$ in the regime where $d = \Omega(\log^2 N)$. We show that Kautz and Singleton's well-known scheme is order-optimal for probabilistic group testing. This is perhaps surprising because for moderate values of d (e.g., $d = O(\text{poly}(\log N))$), this scheme is known to be sub-optimal for combinatorial 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 [23]–[25].

We say a group testing scheme, which consists of a group testing strategy (i.e., M) and a decoding rule, achieves probability of error ϵ and is *efficiently decodable* if the decoding rule can identify the defective set in poly(t)-time complexity with ϵ probability of error. While we can achieve the decoding complexity of $O(tN)$ with the "cover decoder" (c.f. Section II),[2] our goal is to bring the decoding complexity to poly(t). To this end, we use a recursive technique inspired by [26] 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 proofs of the results to their corresponding sections in the appendix. We provide, in Section V, a brief survey of related results on group testing and a detailed comparison with Mazumdar's recent work in [25]. Finally, we conclude our paper in Section VI with a few interesting open problems.

[2]Common constructions in group testing literature have density $\Theta(1/d)$, therefore, the decoding complexity can be brought to $O(tN/d)$.

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 $\mathcal{S}$.[3] The goal is to determine S from the binary measurement vector Y of size t taking the form

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

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, $\upsilon \in \{0, 1\}^t$ 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 the noiseless and noisy variants of the model in (1). In the noiseless case, we simply consider $\upsilon = 0$, 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 $\upsilon \sim \text{Bernoulli}(p)$ 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 υ (in the noisy case). The goal is to minimize the total number of tests t while achieving a vanishing probability of error, i.e., satisfying $P_e \to 0$.

A. Disjunctiveness

We say that a column M_i is *covered* by a set of columns $M_{j_1}, \ldots, M_{j_l}$ with $j_1, \ldots, j_l \in [N]$ if the support of M_i is contained in the union of the supports of columns $M_{j_1}, \ldots, M_{j_l}$. 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* (also referred as the COMP decoder [15], [17]) which runs in $O(tN)$-time. The cover decoder simply scans through the columns of M, and returns

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

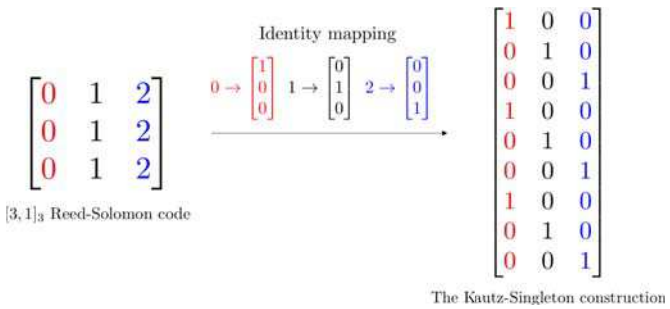

Fig. 1. An example of the Kautz-Singleton construction with $[3, 1]_3$ Reed-Solomon code.

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 the 0-error condition is relaxed into a vanishing probability of error. Therefore we can relax the d-disjunctiveness property. Note that to achieve an arbitrary but fixed ϵ average probability of error 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 [25], [27]–[29] 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, Kautz and Singleton [23] provide a construction of disjunct matrices by converting a Reed-Solomon (RS) code [30] 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:*

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

The Kautz-Singleton construction starts with a $[n, k]_q$ RS code with $n = q$ and $N = q^k$. Each q-ary symbol is then replaced by a unit weight binary vector of length q, via "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 $t = nq = q^2$ tests. An example illustrating the Kautz-Singleton construction is depicted in Figure 1. 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 the choice $n = q$ is appropriate for the combinatorial group testing problem, we will shortly see that we need to set $n = \Theta(\log N)$ in order to achieve the order-optimal result in the probabilistic group testing problem.

While this is a strongly explicit construction, it is suboptimal for combinatorial group testing in the regime $d = O(\mathrm{poly}(\log N))$: an explicit construction with smaller t (achieving $t = O(d^2 \log N)$) is introduced by Porat and Rothschild [24]. Interestingly, we will show in the next section that this same strongly explicit construction that is suboptimal for combinatorial 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 ($\upsilon = 0$ in (1)). The next theorem shows the optimality of the Kautz-Singleton construction with properly chosen parameters n and q.

Theorem 1. *Let $\delta > 0$. Under the noiseless model introduced in Section II, the Kautz-Singleton construction with parameters $q = c_1\, d$ for any $c_1 \geq 4$ and $n = (1 + \delta) \log N$ has average probability of error $P_e \leq N^{-\Omega(\log q)} + N^{-\delta}$ under the cover decoder in the regime $d = \Omega(\log^2 N)$.*

The proof of the above theorem can be found in Appendix A. We note that the Kautz-Singleton construction in Theorem 1 has $t = nq = \Theta(d \log N)$ tests, therefore, achieving the order-optimal result in the probabilistic group testing problem in the noiseless case. It is further possible to extend this result to the noisy setting where we consider $\upsilon \sim$ 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. *Let $\delta > 0$. Under the noisy model introduced in Section II with some fixed noise parameter $p \in (0, 0.5)$, the Kautz-Singleton construction with parameters $q = c_1\, d$ for any $c_1 \geq 24$ and $n = c_2(1 + \delta) \log N$ for any $c_2 \geq \max\{\frac{8}{9(0.5-p)^2}, 40.57\}$ has average probability of error $P_e \leq N^{-\Omega(\log q)} + 3N^{-\delta}$ under the modified version of cover decoder 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.

Given that the Kautz-Singleton construction achieves a vanishing probability of error with $t = \Theta(d \log N)$ order-optimal number of tests, a natural question of interest is how large the constant is and how the performance of this construction compares to random designs for given finite values of d and N. To illustrate the empirical performance of the Kautz-Singleton construction in the noiseless case, we provide simulation results in Figure 2 and 3 for different choices of N and d and compare the results to random designs considered in the literature. We used the code in [31] (see [32] for the associated article) for the Kautz-Singleton construction. For comparison, we take two randomized constructions from the literature, namely the Bernoulli design (see [17]) and the near-constant column weight design studied in [18]. We use the cover decoder for decoding. The simulation results illustrate

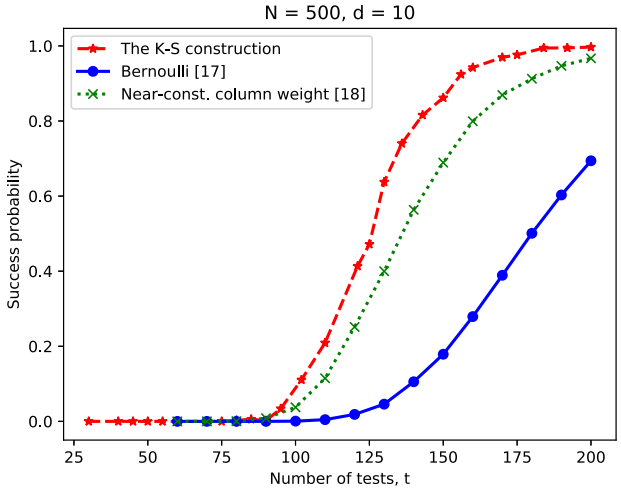

Fig. 2. Empirical performances of the Kautz-Singleton construction along with the random near-constant column weight [18] and Bernoulli designs [17] under the cover decoder for $N = 500$ items and $d = 10$ defectives. For the Kautz-Singleton construction, empirical performance was judged using 5000 random trials and the number of tests correspond to a range of (q, n) pair selections. For the random matrices, empirical performance was judged from 100 trials each on 100 random matrices.

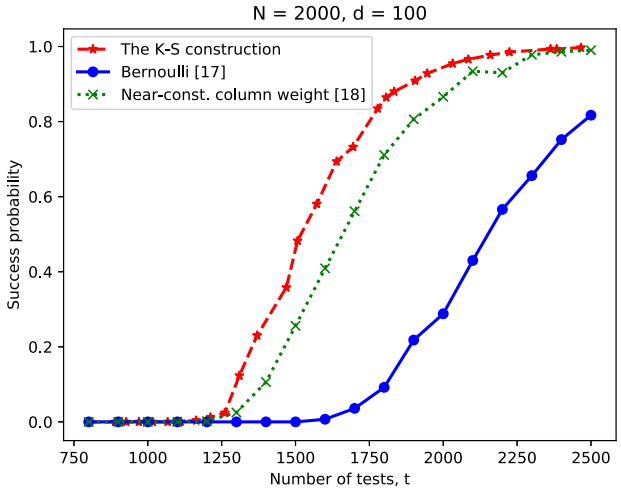

Fig. 3. Empirical performances of the Kautz-Singleton construction along with the random near-constant column weight [18] and Bernoulli designs [17] under the cover decoder for $N = 2000$ items and $d = 100$ defectives. For the Kautz-Singleton construction, empirical performance was judged using 5000 random trials and the number of tests correspond to a range of (q, n) pair selections. For the random matrices, empirical performance was judged from 100 trials each on 100 random matrices.

that the Kautz-Singleton construction achieves better success probability for the same number of tests, which suggests that the implied constant for the Kautz-Singleton construction may be better than those for these random designs; we note that similar empirical findings were observed in [32]. Since the Kautz-Singleton construction additionally has an explicit and simple structure, this construction may be a good choice for designing measurement matrices for probabilistic group testing in practice.

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], [33]–[36]. The target is a decoding complexity of 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 vanishing probability of error), there is no known efficiently decodable scheme with optimal $t = \Theta(d \log N)$ tests to the best of our knowledge. The work [35] 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, [36], 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 [35] and [36], 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 [26] 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.

The cover decoder goes through the columns of M and decides whether the corresponding item is defective or not. This results in decoding complexity $O(tN)$. Assume we were given a superset S' such that S' is guaranteed to include the defective set S, i.e. $S \subseteq S'$, then the cover decoder could run in time $O(t \cdot |S'|)$ over the columns corresponding to S', which depending on the size of S' could result in significantly lower complexity. 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 $M^{(1)}$ which can be used to detect at most d defectives among $\sqrt{N}$ items with probability of error $P_e \leq \epsilon/4$ when the noise parameter is p by using $t_1(d, \sqrt{N}, \epsilon/4, p)$ tests. We construct two $t_1(d, \sqrt{N}, \epsilon/4, p) \times N$ matrices $M^{(F)}$ and $M^{(L)}$ using $M^{(1)}$ as follows. For $i \in [N]$, the i'th column of $M^{(F)}$ is equal to j'th column of $M^{(1)}$ if the *first* $\frac{1}{2} \log N$ bits in the binary representation of i are given by the binary representation of j for $j \in [\sqrt{N}]$. Similarly, for $i \in [N]$, the i'th columns of $M^{(L)}$ is equal to the j'th column of $M^{(1)}$ if the *last* $\frac{1}{2} \log N$ bits in the binary representation of i are given by the binary representation of j for $j \in [\sqrt{N}]$.

The final matrix M is constructed by vertically stacking $M^{(F)}$, $M^{(L)}$ and a $t_2(d, N, \epsilon/2, p) \times N$ matrix $M^{(2)}$ which is not necessarily efficiently decodable (e.g., the Kautz-Singleton construction). As before, $t_2(d, N, \epsilon/2, p)$ is the number of tests for $M^{(2)}$, which we assume can be used to detect d defectives among N items with probability of error $P_e \leq \epsilon/2$ when the noise parameter is p. The decoding works as follows. We obtain the measurement vectors $Y^{(F)}$, $Y^{(L)}$, and $Y^{(2)}$ given by $Y^{(F)} = \bigvee_{i \in S} M_i^{(F)} \oplus v^{(F)}$, $Y^{(L)} = \bigvee_{i \in S} M_i^{(L)} \oplus v^{(L)}$, and $Y^{(2)} = \bigvee_{i \in S} M_i^{(2)} \oplus v^{(2)}$ respectively where $v^{(F)}$, $v^{(L)}$, and $v^{(2)}$ are the noise terms corrupting

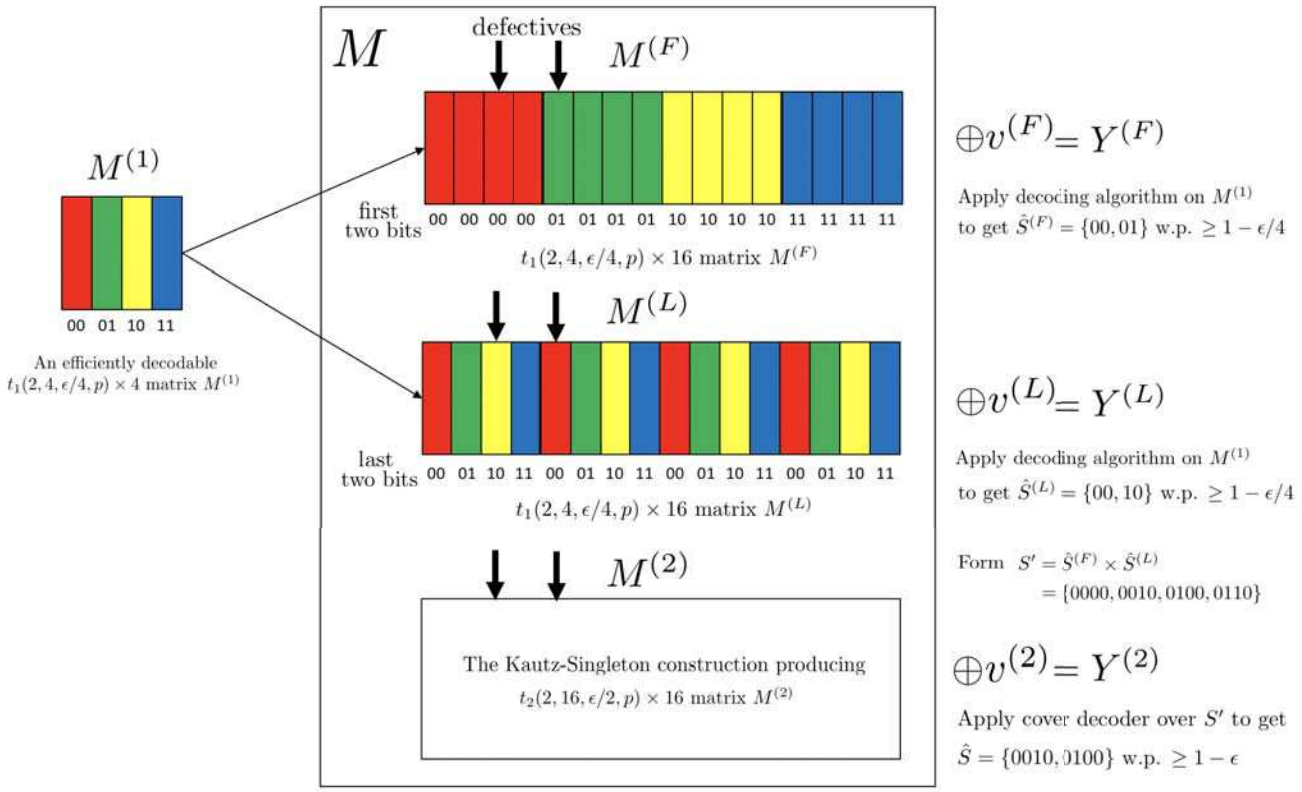

Fig. 4. An illustration of the construction presented in Section IV for the case $d = 2$ and $N = 16$. The illustration depicts the main idea, and the full construction is achieved by applying this idea recursively.

the corresponding measurements. We next 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 $\hat{S}^{(L)}$ can decode the first and last $\frac{1}{2}\log N$-bits of the defective items respectively with probability at least $1-\epsilon/2$ by the union bound. Therefore, we can construct the set $S' = \hat{S}^{(F)} \times \hat{S}^{(L)}$ where $\times$ denotes the Cartesian product and obtain a super set that contains the defective set S with error probability at most $\epsilon/2$. We further note that since $|\hat{S}^{(F)}| \leq d$ and $|\hat{S}^{(L)}| \leq d$, we have $|S'| \leq d^2$. We finally apply the naive cover decoder to $M^{(2)}$ by running it over the set S' to compute the final estimate $\hat{S}$ which can be done in additional $O(t_2 \cdot d^2)$ time. Note that by the union bound the probability of error is bounded by ϵ. Figure 4 illustrates the main idea with the example of $d = 2$ and $N = 16$. We provide this decoding scheme in Algorithm 1 for the special case $N = d^{2^i}$ for some non-negative integer i although the results hold in the general case and no extra assumption beyond $d = \Omega(\log^2 N)$ is needed. The next theorem is the result of applying this idea recursively.

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);
    Ŝ^(F) = decode(Y^(F), M^(1), d, √N);
    Ŝ^(L) = decode(Y^(L), M^(1), d, √N);
    if |Ŝ^(F)| > d or |Ŝ^(L)| > d then
        return {};
    Construct S' = Ŝ^(F) × Ŝ^(L);
    Apply the cover decoder to M^(2) over the set S' and compute Ŝ;
    Return Ŝ;
```

Theorem 3. *Under the noiseless/noisy model introduced in Section II, there exists a strongly explicit construction and a decoding rule 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 $d = \Omega(\log^2 N)$.*

The proof of the above theorem can be found in Appendix C. 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.

TABLE I

COMPARISON OF NON-ADAPTIVE PROBABILISTIC GROUP TESTING RESULTS. WE NOTE THAT THE MAIN FOCUS IN [17], [37] IS THE IMPLIED CONSTANT IN $t = \Theta(d \log N)$

Reference	Number of tests	Decoding complexity	Construction
[17], [37]	$t = \Theta(d \log N)$	$O(tN)$	Randomized
[25]	$t = O(d \log^2 N / \log d)$	$O(tN)$	Strongly explicit
[35]	$t = O(d \log d \log N)$	$O(d \log d \log N)$	Randomized
[36]	$t = O(d \log d \log N)$	$O(d(\log^2 d + \log N))$	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

We refer the reader to [12] for a survey. In combinatorial group testing, the famous construction introduced by Kautz and Singleton [23] achieves $t = O(d^2 \log_d^2 N)$ tests matching the best known lower bound $\min\{N, \Omega(d^2 \log_d N)\}$ [21], [22] 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 [24]. 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 *et al.* [34] introduced a randomized construction with $t = O(d^2 \log(N))$ tests that could be decoded in time poly(t). Furthermore, the construction in [34] can be derandomized in the regime $d = O(\log N / \log \log N)$. Later, Ngo *et al.* [26] removed the constraint on d and provided an explicit construction that can be decoded in time poly(t). The main idea of [34] was to consider *list-disjunct* matrices; a similar idea was considered by Cheraghchi [33], which obtained explicit constructions of non-adaptive group testing schemes that handle noisy tests and return a list of defectives that may include false positives.

There are various schemes relaxing the zero-error criteria in the group testing problem. For instance, the model mentioned above, where the decoder always outputs a small superset of the defective items, was studied in [33], [38]–[40]. These constructions have efficient (poly(t)-time) decoding algorithms, and so can be used alongside constructions without sublinear time decoding algorithms to speed up decoding. 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 [35] 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 [41], [42] or can be threshold based [43]–[45]. More recently, sparse group testing frameworks for both combinatorial and probabilistic settings were studied in [46]–[48].

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 vanishing probability of error (which is the model considered in this work) in the broad regime $d = O(N^\alpha)$ for some $\alpha \in (0, 1)$ using random designs and information-theoretical tools [16], [37]. These results also include the noisy variants of the group testing problem. Efficient recovery algorithms with nearly optimal number of tests were introduced recently in [35] and [36]. Regarding deterministic constructions of almost disjunct matrices, recently Mazumdar [25] 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 moderate values of d (e.g., $d = O(\text{poly}(\log N))$). The performance of the Kautz-Singleton construction in the random model has been studied empirically [32], 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 for poly-logarithmic (in N) values of d. 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.

APPENDIX

A. 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 which takes a $[n,k]_q$ RS code and replaces each q-ary symbol by a unit weight binary vector of length q using identity mapping. This corresponds to mapping a symbol $i \in [q]$ to the vector in $\{0,1\}^q$ that has a 1 in the i'th position and zero everywhere else (see Section II-B for the full description). Note that the resulting $t \times N$ binary matrix M has $t = nq$ tests. We shall later see that the choice $q = 4d$ and $n = \Theta(\log N)$ is appropriate, therefore, leading to $t = \Theta(d \log N)$ tests.

We note that for any defective set the cover decoder provides an exact recovery given that none of the non-defective items are covered by the defective set. Recall that a column M_i is covered by a set of columns $M_{j_1}, \ldots, M_{j_l}$ with $j_1, \ldots, j_l \in [N]$ if the support of M_i is contained in the union of the supports of columns $M_{j_1}, \ldots, M_{j_l}$. Note that in the noiseless case the measurement vector Y is given by the Boolean OR of the columns corresponding to the defective items. Therefore, the measurement vector Y covers all defective items, and the cover decoder can achieve exact recovery if none of the non-defective items are covered by the measurement vector Y (or equivalently the defective set).

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 $(i \notin s)$ is covered by the defective set s. We can bound the probability of error as follows:

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

where in the last equation $S_{[N]/\{i\}}$ 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 are contained in the union of symbols of S in the RS code for all rows in $[n]$. Recall that there is a $k-1$ degree polynomial $f_m(X) = \sum_{i=0}^{k-1} m_i X^i$ corresponding to each column in the RS code and the corresponding symbols in the column are the evaluation of $f_m(X)$ at $\alpha_1, \alpha_2, \ldots, \alpha_n$. Denoting $f_{m_i}(X)$ as the polynomial corresponding to the column M_i, we have

$$\begin{aligned} &\Pr\left(\mathcal{A}_i^{S_{[N]/\{i\}}}\right) \\ &\quad= \Pr\left(f_{m_i}(\alpha) \in \left\{f_{m_j}(\alpha) : j \in S_{[N]/\{i\}}\right\} \ \forall\ \alpha \in \Psi\right) \\ &\quad= \Pr\left(0 \in \left\{f_{m_j}(\alpha) - f_{m_i}(\alpha) : j \in S_{[N]/\{i\}}\right\} \ \forall\ \alpha \in \Psi\right). \end{aligned}$$

We note that the columns of the RS code contain all possible (at most) $k-1$ degree polynomials, therefore, the set $\left\{f_{m_j}(\alpha) - f_{m_i}(\alpha) : j \in [N]/\{i\}\right\}$ is sweeping through all possible (at most) $k-1$ degree polynomials except the zero polynomial. Therefore, the randomness of $S_{[N]/\{i\}}$ that generates the random set $\left\{f_{m_j}(\alpha) - f_{m_i}(\alpha) : j \in S_{[N]/\{i\}}\right\}$ can be translated to the random set of polynomials $\{f_{m_j}(X) : j \in S'\}$ that is generated by picking d nonzero polynomials of degree (at most) $k-1$ without replacement. This gives

$$\begin{aligned} &\Pr\left(0 \in \left\{f_{m_j}(\alpha) - f_{m_i}(\alpha) : j \in S_{[N]/\{i\}}\right\} \ \forall\ \alpha \in \Psi\right) \\ &\qquad= \Pr\left(0 \in \left\{f_{m_j}(\alpha) : j \in S'\right\} \ \forall\ \alpha \in \Psi\right). \end{aligned}$$

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 [49].

Lemma 1 ([49, 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,*

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

Let r denote the number of roots of a random nonzero polynomial of degree at most $k-1$. One can observe that $\mathbb{E}[r] \le 1$ by noting that there is exactly one value of m_0 that makes $f_m(X) = 0$ for any fixed X and $m_1, \ldots, m_{k-1}$ and the inequality is due to excluding the zero polynomial. Furthermore, using Lemma 1, we get

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

where the first inequality is due to $\Pr(r = i) = |R_q(i, k-1)|/q^k \le 1/i!$ from Lemma 1. 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 $r_h \le \sum_{j\in S'} r_j$. We will use the following Bernstein concentration bound for sampling without replacement [50]:

Proposition 1 ([50, Proposition 1.4]). *Let $\mathcal{X} = \{x_1, \ldots, x_N\}$ be a finite population of N points and $X_1, \ldots, X_n$ be a random*

sample drawn without replacement from $\mathcal{X}$. Let $a = \min_{1\le i\le N} x_i$ and $b = \max_{1\le i\le N} x_i$. Then for all $\epsilon > 0$,

$$\Pr\left(\frac{1}{n}\sum_{i=1}^{n} X_i - \mu > \epsilon\right) \le \exp\left(-\frac{n\epsilon^2}{2\sigma^2 + (2/3)(b-a)\epsilon}\right)$$

where $\mu = \frac{1}{N}\sum_{i=1}^{N} x_i$ is the mean of $\mathcal{X}$ and $\sigma^2 = \frac{1}{N}\sum_{i=1}^{N}(x_i-\mu)^2$ is the variance of $\mathcal{X}$.

We apply the inequality above to $\sum_{j\in S'} r_j$ and obtain

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

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 $2d$ with high probability.

Given the condition that the number of roots of the polynomial $h(X)$ is bounded by $2d$ 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 in the position of the roots of the randomly selected polynomials, 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 $2d$ elements randomly without replacement. We next prove this claim. We define the set $R(h) := \{\alpha \in \mathbb{F}_q : h(\alpha) = 0\}$ 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

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

Let $\Lambda' \subseteq \mathbb{F}_q$ such that $|\Lambda'| = l$ and $\Lambda' \ne \Lambda$. 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 $\Phi(\{f_1,\ldots,f_d\}) := \{\Phi(f_1),\ldots,\Phi(f_d)\}$ is a bijection.

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

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

where (i) is due to $|H_\Lambda| = |H_{\Lambda'}|$ and we pick $f_1,\ldots,f_d$ uniformly without replacement. □

Based on this, if we ensure $n \le 2d$, then it follows that

$$\begin{aligned}&\Pr\{R(h) \supseteq \Psi \mid |R(h)| \le 2d\}\\ &= \sum_{l\le 2d}\Big(\Pr\{R(h)\supseteq\Psi \mid |R(h)| = l\}\\ &\qquad\cdot\Pr\{|R(h)| = l \mid |R(h)| \le 2d\}\Big)\\ &\le \max_{n\le l\le 2d}\Pr\{R(h)\supseteq\Psi \mid |R(h)| = l\}\\ &= \max_{n\le l\le 2d}\frac{\binom{q-n}{l-n}}{\binom{q}{l}}.\end{aligned}$$

Let us fix $q = 4d$. We then have

$$\begin{aligned}\Pr\{R(h)\supseteq\Psi \mid |R(h)| \le 2d\} &\le \frac{\binom{4d-n}{2d-n}}{\binom{4d}{2d}}\\ &= \frac{(4d-n)!}{(2d-n)!(2d)!}\frac{(2d)!(2d)!}{(4d)!}\\ &= \frac{2d\ldots(2d-n+1)}{4d\ldots(4d-n+1)}\\ &\le \left(\frac{1}{2}\right)^n.\end{aligned}$$

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

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

Applying the summation overall $i \in [N]$ in (2), we obtain $P_e \le N^{1-c\log q} + N2^{-n}$. Therefore, under the regime $d = \Omega(\log^2 N)$, the average probability of error can be bounded as $P_e \le N^{-\Omega(\log q)} + N^{-\delta}$ by choosing $n = (1+\delta)\log N$. The condition $n \le 2d$ required in the proof is also satisfied under this regime. Note that the resulting $t \times N$ binary matrix M has $t = nq = \Theta(d\log N)$ tests.

B. 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 [37] 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:

$$\begin{aligned}
P_e &\leq \frac{1}{\binom{N}{d}} \sum_{s\subseteq[N],|s|=d} \Bigg[\sum_{i\in[N]\setminus s} \Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))\} \\
&\qquad + \sum_{i\in s} \Pr\{\hat{w}_i < w_i(1-p(1+\tau))\}\Bigg] \\
&= \frac{1}{\binom{N}{d}} \sum_{i\in[N]} \sum_{s\subseteq[N]/\{i\},|s|=d} \Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))\} \\
&\qquad + \frac{1}{\binom{N}{d}} \sum_{s\subseteq[N],|s|=d} \sum_{i\in s} \Pr\{\hat{w}_i < w_i(1-p(1+\tau))\} \\
&= \frac{\binom{N-1}{d}}{\binom{N}{d}} \Bigg(\sum_{i\in[N]} \frac{1}{\binom{N-1}{d}} \\
&\qquad \cdot \sum_{s\subseteq[N]/\{i\},|s|=d} \Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))\}\Bigg) \\
&\qquad + \frac{1}{\binom{N}{d}} \sum_{s\subseteq[N],|s|=d} \sum_{i\in s} \Pr\{\hat{w}_i < w_i(1-p(1+\tau))\} \\
&= \frac{N-d}{N} \sum_{i\in[N]} \Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))\} \\
&\qquad + \frac{1}{\binom{N}{d}} \sum_{s\subseteq[N],|s|=d} \sum_{i\in s} \Pr\{\hat{w}_i < w_i(1-p(1+\tau))\} \qquad (3) \\
&=: P_1 + P_2,
\end{aligned}$$

where we denote the first term of (3) as P_1 and the second one as P_2 in the last equation. We point out that in the first term of (3) the randomness is both due to the noise and the defective set that is uniformly distributed among the items in $[N]/\{i\}$ whereas in the second term the randomness is due to the noise.

We will employ the Kautz-Singleton construction which takes a $[n,k]_q$ RS code and replaces each q-ary symbol by unit weight binary vectors of length q using identity mapping. This corresponds to mapping a symbol $i \in [q]$ to the vector in $\{0,1\}^q$ that has a 1 in the i'th position and zero everywhere else (see Section II-B for the full description). Note that the resulting $t \times N$ binary matrix M has $t = nq$ tests. We shall later see that the choice $q = 24d$ and $n = \Theta(\log N)$ is appropriate, therefore, leading to $t = \Theta(d \log N)$ tests. 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 structure of 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

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

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

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 $2d$ number of roots. We then have

$$\begin{aligned}
&\Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))\} \\
&\quad = \Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))|\mathcal{A}\}\Pr\{\mathcal{A}\} \\
&\qquad\qquad + \Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))|\mathcal{A}^c\}\Pr\{\mathcal{A}^c\} \\
&\quad \leq \Pr\{\hat{w}_i \geq w_i(1-p(1+\tau))|\mathcal{A}\} + \Pr\{\mathcal{A}^c\}. \qquad (4)
\end{aligned}$$

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 (4). We choose $q = 24d$ and define the random set $\Upsilon = \{\alpha \in \Psi : f_{m_i}(\alpha) \in \{f_{m_j}(\alpha) : j \in S\}\}$. We then have

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

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. This holds since $i \notin S$ and the columns of the RS code contain all possible (at most) $k-1$ degree polynomials, therefore, the randomness of $\{f_{m_j}(\alpha) - f_{m_i}(\alpha) : j \in S\}$ can be translated to the random set of polynomials $\{f_{m_j}(X) : j \in S'\}$ that 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 $2d$ symbols from $[q]$ uniformly at random without replacement. Hence, if we ensure $n \leq 8d$,

then we have

$$\begin{aligned}\Pr\{|\Upsilon| > n/4|\mathcal{A}\} &\leq \frac{\binom{n}{n/4}\binom{q-n/4}{2d-n/4}}{\binom{q}{2d}} \\ &= \frac{\binom{n}{n/4}\binom{24d-n/4}{2d-n/4}}{\binom{24d}{2d}} \\ &\leq (4e)^{n/4}\frac{(24d-n/4)!}{(2d-n/4)!(22d)!}\frac{(2d)!(22d)!}{(24d)!} \\ &= (4e)^{n/4}\frac{2d\ldots(2d-n/4+1)}{24d\ldots(24d-n/4+1)} \\ &\leq \left(\frac{4e}{12}\right)^{n/4}\end{aligned}$$

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

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

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

$$\begin{aligned}P_e &\leq N^{1-c\log q} + N(e/3)^{n/4} + Ne^{-2n(3/4-3p/2-p\tau)^2} \\ &\qquad + de^{-2\ np^2\tau^2} \\ &\leq N^{1-c\log q} + N(e/3)^{n/4} + Ne^{-2n(3/4-3p/2-p\tau)^2} \\ &\qquad + Ne^{-2\ np^2\tau^2} \\ &= N^{-\Omega(\log q)} + e^{\log N - \frac{n}{4}\log(\frac{3}{e})} + 2\ e^{\log N - \frac{9}{8}(0.5-p)^2\ n}\end{aligned}$$

where in the last step we pick $\tau = \frac{3(0.5-p)}{4p}$. Therefore, under the regime $d = \Omega(\log^2\ N)$, the average probability of error can be bounded as $P_e \leq N^{-\Omega(\log q)} + 3N^{-\delta}$ by choosing $n = \max\{\frac{4}{\log(3/e)}, \frac{8}{9(0.5-p)^2}\}(1+\delta)\log N$. The condition $n \leq 8d$ required in the proof is also satisfied under this regime. Note that the resulting $t \times N$ binary matrix M has $t = nq = \Theta(d \log N)$ tests.

C. Proof of Theorem 3

We begin with the noiseless case. We will use a recursive approach to obtain an efficiently decodable group testing matrix. Let M_n^{ED} denote such a matrix with n columns in the recursion and M_n^{KS} denote the matrix with n columns obtained by the Kautz-Singleton construction. Note that the final matrix is M_N^{ED}. Let $t^{\mathrm{ED}}(d,n,\epsilon)$ and $t^{\mathrm{KS}}(d,n,\epsilon)$ denote the number of tests for M_n^{ED} and M_n^{KS} respectively to detect at most d defectives among n columns with average probability of error ϵ. We further define $D^{\mathrm{ED}}(d,n,\epsilon)$ to be the decoding time for M_n^{ED} with $t^{\mathrm{ED}}(d,n,\epsilon)$ rows.

We first consider the case $N = d^{2^i}$ for some non-negative integer i. The base case is $i = 0$, i.e., $N = d$ for which we can use individual testing and have $t^{\mathrm{ED}}(d,d,\epsilon) = d$ and $D^{\mathrm{ED}}(d,d,\epsilon) = O(d)$. For $i > 0$, we use $t^{\mathrm{ED}}(d,\sqrt{N},\epsilon/4) \times \sqrt{N}$ matrix $M_{\sqrt{N}}^{\mathrm{ED}}$ to construct two $t^{\mathrm{ED}}(d,\sqrt{N},\epsilon/4) \times N$ matrices $M^{(F)}$ and $M^{(L)}$ as follows. The jth column of $M_{\sqrt{N}}^{\mathrm{ED}}$ 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 $M_{\sqrt{N}}^{\mathrm{ED}}$ 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. We finally construct M_N^{KS} that achieves $\epsilon/2$ average probability of error and stack $M^{(F)}$, $M^{(L)}$, and M_N^{KS} to obtain the final matrix M_N^{ED}. Note that, this construction gives us the following recursion in terms of the number of tests

$$t^{\mathrm{ED}}(d,N,\epsilon) = 2\ t^{\mathrm{ED}}(d,\sqrt{N},\epsilon/4) + t^{\mathrm{KS}}(d,N,\epsilon/2).$$

When $N = d^{2^i}$, note that $2^i = \log_d N$ and $i = \log\log_d N$. To solve for $t^{\mathrm{ED}}(d,d^{2^i},\epsilon)$, we iterate the recursion as follows.

$$\begin{aligned}&t^{\mathrm{ED}}\left(d,d^{2^i},\epsilon\right) \\ &= 2t^{\mathrm{ED}}\left(d,d^{2^{i-1}},\frac{\epsilon}{4}\right) + t^{\mathrm{KS}}\left(d,d^{2^i},\frac{\epsilon}{2}\right) \\ &= 4t^{\mathrm{ED}}\left(d,d^{2^{i-2}},\frac{\epsilon}{16}\right) + 2t^{\mathrm{KS}}\left(d,d^{2^{i-1}},\frac{\epsilon}{8}\right) + t^{\mathrm{KS}}\left(d,d^{2^i},\frac{\epsilon}{2}\right) \\ &\ \ \vdots \\ &= 2^i t^{\mathrm{ED}}\left(d,d,\frac{\epsilon}{2^{2i}}\right) + \sum_{j=0}^{i-1} 2^j t^{\mathrm{KS}}\left(d,d^{2^{i-j}},\frac{\epsilon}{2^{j+1}}\right) \\ &= 2^i\cdot d + \sum_{j=0}^{i-1} 2^j\cdot 4d\log\left(d^{2^{i-j}}/\left(\epsilon/2^{j+1}\right)\right) \qquad (5) \\ &= 2^i\cdot d + \sum_{j=0}^{i-1} 2^j\cdot 4d\left(2^{i-j}\log d + (j+1)\log 2 + \log(1/\epsilon)\right) \\ &\leq 2^i\cdot d + i\cdot 2^i\cdot 4d\log d + 4d\left(\sum_{j=0}^{i-1} 2^j(j+1) + 2^i\log(1/\epsilon)\right) \\ &\leq 2^i\cdot d + i\cdot 2^i\cdot 4d\log d + i\cdot 2^i\cdot 4d + 2^i\cdot 4d\log(1/\epsilon) \qquad (6)\end{aligned}$$

where in (5) for simplicity we ignore the term $N^{-\Omega(\log q)}$ in the probability of error for Theorem 1 and take $t^{\mathrm{KS}}(d,N,\epsilon) = 4\ d\log N/\epsilon$. Replacing $2^i = \log_d N$ and $i = \log\log_d N$ in (6), it follows that

$$\begin{aligned}&t^{\mathrm{ED}}(d,N,\epsilon) \\ &\qquad = O\left(d\log N\log\log_d N + d\log_d N\log\left((\log_d N)/\epsilon\right)\right).\end{aligned}$$

Note that this gives $t^{\mathrm{ED}}(d,N) = O(d\log N\log\log_d N)$ in the case where $\epsilon = \Theta(1)$.

In the more general case, let $i \geq 1$ be the smallest integer such that $d^{2^{i-1}} < N \leq d^{2^i}$. It follows that $i < \log\log_d N + 1$. We can construct M_N^{ED} from $M_{d^{2^i}}^{\mathrm{ED}}$ by removing its last $d^{2^i} - N$ columns. We can operate on M_N^{ED} as if the removed columns were all defective. Therefore the number of tests satisfies $t^{\mathrm{ED}}(d,N) = O(d\log N\log\log_d N)$.

We next describe the decoding process. We run the decoding algorithm for $M^{\mathrm{ED}}_{\sqrt{N}}$ with the components of the outcome vector Y corresponding to $M^{(F)}$ and $M^{(L)}$ to compute the estimate sets $\hat{S}^{(F)}$ and $\hat{S}^{(L)}$. By induction and the 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 finally apply the naive cover decoder to the component of M^{ED}_N corresponding to M^{KS}_N over the set S' to compute the final estimate $\hat{S}$ which can be done with an additional $O(d^2 \cdot t^{\mathrm{KS}}(d, N, \epsilon/2))$ time. By the union bound overall probability of error is bounded by ϵ. This decoding procedure gives us the following recursion in terms of the decoding complexity

$$D^{\mathrm{ED}}(d, N, \epsilon) = 2\ D^{\mathrm{ED}}(d, \sqrt{N}, \epsilon/4) + O(d^2 \cdot t^{\mathrm{KS}}(d, N, \epsilon/2)).$$

When $N = d^{2^i}$, to solve for $D^{\mathrm{ED}}(d, d^{2^i}, \epsilon)$, we iterate the recursion as follows.

$$\begin{aligned}
&D^{\mathrm{ED}}\left(d, d^{2^i}, \epsilon\right) \\
&= 2D^{\mathrm{ED}}\left(d, d^{2^{i-1}}, \frac{\epsilon}{4}\right) + c \cdot d^2 \cdot t^{\mathrm{KS}}\left(d, d^{2^i}, \frac{\epsilon}{2}\right) \\
&= 4D^{\mathrm{ED}}\left(d, d^{2^{i-2}}, \frac{\epsilon}{16}\right) + 2c \cdot d^2 \cdot t^{\mathrm{KS}}\left(d, d^{2^{i-1}}, \frac{\epsilon}{8}\right) \\
&\qquad + c \cdot d^2 \cdot t^{\mathrm{KS}}\left(d, d^{2^i}, \frac{\epsilon}{2}\right) \\
&\ \ \vdots \\
&= 2^i D^{\mathrm{ED}}\left(d, d, \frac{\epsilon}{2^{2i}}\right) + \sum_{j=0}^{i-1} 2^j c \cdot d^2 \cdot t^{\mathrm{KS}}\left(d, d^{2^{i-j}}, \frac{\epsilon}{2^{j+1}}\right) \\
&= 2^i \cdot O(d) + \sum_{j=0}^{i-1} 2^j c \cdot 4d^3 \log\left(d^{2^{i-j}} / \left(\epsilon/2^{j+1}\right)\right) \\
&\leq 2^i \cdot O(d) + i \cdot 2^i \cdot 4cd^3 \log d + i \cdot 2^i \cdot 4cd^3 \\
&\qquad + 2^i \cdot 4cd^3 \log(1/\epsilon) \quad (7)
\end{aligned}$$

where (7) is obtained in the same way as (6). Replacing $2^i = \log_d N$ and $i = \log\log_d N$ in (7), it follows that

$$\begin{aligned}
&D^{\mathrm{ED}}(d, N, \epsilon) \\
&\quad = O\left(d^3 \log N \log\log_d N + d^3 \log_d N \log\left((\log_d N)/\epsilon\right)\right).
\end{aligned}$$

Note that this gives $D^{\mathrm{ED}}(d, N) = O(d^3 \log N \log\log_d N)$ in the case where $\epsilon = \Theta(1)$.

The noisy case follows similar lines except the difference is that in the base case where $N = d$, we cannot use individual testing due to the noise. In this case we can do individual testing with repetitions which requires $t^{\mathrm{ED}}(d, d, \epsilon) = O(d \log(d/\epsilon))$ and $D^{\mathrm{ED}}(d, d, \epsilon) = O(d \log(d/\epsilon))$. We can proceed similarly as in the noiseless case and show that $t^{\mathrm{ED}}(d, N) = O(d \log N \log\log_d N)$ and $D^{\mathrm{ED}}(d, N) = O(d^3 \log N \log\log_d N)$.

ACKNOWLEDGEMENTS

The third author would like to thank Atri Rudra and Hung Ngo for helpful conversations. The authors would also like to thank the anonymous reviewers for helpful comments and suggestions.

REFERENCES

[1] R. Dorfman, "The detection of defective members of large populations," *Ann. Math. Statist.*, vol. 14, no. 4, pp. 436–440, Dec. 1943.
[2] H.-B. Chen and F. K. Hwang, "A survey on nonadaptive group testing algorithms through the angle of decoding," *J. Combinat. Optim.*, vol. 15, no. 1, pp. 49–59, 2008.
[3] A. Ganesan, S. Jaggi, and V. Saligrama, "Learning immune-defectives graph through group tests," *IEEE Trans. Inf. Theory*, vol. 63, no. 5, pp. 3010–3028, May 2017.
[4] D. Malioutov and K. Varshney, "Exact rule learning via Boolean compressed sensing," in *Proc. Int. Conf. Mach. Learn.*, 2013, pp. 765–773.
[5] A. C. Gilbert, M. A. Iwen, and M. J. Strauss, "Group testing and sparse signal recovery," in *Proc. 42nd Asilomar Conf. Signals, Syst. Comput.*, Oct. 2008, pp. 1059–1063.
[6] A. Emad and O. Milenkovic, "Poisson group testing: A probabilistic model for nonadaptive streaming Boolean compressed sensing," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2014, pp. 3335–3339.
[7] T. Berger, N. Mehravari, D. Towsley, and J. Wolf, "Random multiple-access communication and group testing," *IEEE Trans. Commun.*, vol. COM-32, no. 7, pp. 769–779, Jul. 1984.
[8] J. Wolf, "Born again group testing: Multiaccess communications," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 2, pp. 185–191, Mar. 1985.
[9] J. Luo and D. Guo, "Neighbor discovery in wireless ad hoc networks based on group testing," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2008, pp. 791–797.
[10] A. K. Fletcher, S. Rangan, and V. K. Goyal, "A sparsity detection framework for on-off random access channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun./Jul. 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," *DIMACS Ser. Discrete Math. Problems Theor. Comput. Sci.*, vol. 55, pp. 171–182, Feb. 2000.
[12] D.-Z. Du and F. Hwang, *Combinatorial Group Testing and Its Applications*, vol. 12. Singapore: World Scientific, 2000.
[13] G. K. Atia and V. Saligrama, "Boolean compressed sensing and noisy group testing," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1880–1901, Mar. 2012.
[14] D. Sejdinovic and O. Johnson, "Note on noisy group testing: Asymptotic bounds and belief propagation reconstruction," in *Proc. 48th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Allerton, IL, USA, 2010, pp. 998–1003.
[15] 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 *Proc. 49th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2011, pp. 1832–1839.
[16] J. Scarlett and V. Cevher, "Phase transitions in group testing," in *Proc. 27th Annu. ACM-SIAM Symp. Discrete Algorithms (SODA)*, 2016, pp. 40–53.
[17] M. Aldridge, L. Baldassini, and O. Johnson, "Group testing algorithms: Bounds and simulations," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3671–3687, Jun. 2014.
[18] O. Johnson, M. Aldridge, and J. Scarlett, "Performance of group testing algorithms with near-constant tests per item," *IEEE Trans. Inf. Theory*, vol. 65, no. 2, pp. 707–723, Feb. 2019.
[19] J. Scarlett and V. Cevher, "Near-optimal noisy group testing via separate decoding of items," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 5, pp. 902–915, Oct. 2018.
[20] J. Scarlett and O. Johnson. (Aug. 2018). "Noisy non-adaptive group testing: A (near-)definite defectives approach." [Online]. Available: https://arxiv.org/abs/1808.09143
[21] 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.
[22] Z. Furedi, "Onr-cover-free families," *J. Combinat. Theory Series A*, vol. 73, no. 1, pp. 172–173, 1996.
[23] W. Kautz and R. Singleton, "Nonrandom binary superimposed codes," *IEEE Trans. Inf. Theory*, vol. 10, no. 4, pp. 363–377, Oct. 1964.
[24] E. Porat and A. Rothschild, "Explicit non-adaptive combinatorial group testing schemes," in *Proc. 35th Int. Colloq. Automata, Lang. Program. (ICALP)*. Berlin, Germany: Springer, 2008, pp. 748–759.
[25] A. Mazumdar, "Nonadaptive group testing with random set of defectives," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 7522–7531, Dec. 2016.
[26] H. Q. Ngo, E. Porat, and A. Rudra, "Efficiently decodable error-correcting list disjunct matrices and applications," in *Automata, Languages and Programming*, Berlin, Germany: Springer, 2011, pp. 557–568.

[27] A. J. Macula, V. V. Rykov, and S. Yekhanin, "Trivial two-stage group testing for complexes using almost disjunct matrices," *Discrete Appl. Math.*, vol. 137, no. 1, pp. 97–107, 2004.
[28] M. B. Malyutov, "The separating property of random matrices," *Math. Notes*, vol. 23, no. 1, pp. 84–91, 1978.
[29] A. Zhigljavsky, "Probabilistic existence theorems in group testing," *J. Stat. Planning Inference*, vol. 115, no. 1, pp. 1–43, 2003.
[30] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *J. Soc. Ind. Appl. Math.*, vol. 8, no. 2, pp. 300–304, Jun. 1960.
[31] Y. Erlich. (2017). *Combinatorial Pooling Using RS Codes*. [Online]. Available: https://github.com/TeamErlich/pooling
[32] Y. Erlich *et al.*, "Biological screens from linear codes: Theory and tools," *BioRxiv*, p. 035352, Jan. 2015.
[33] M. Cheraghchi, "Noise-resilient group testing: Limitations and constructions," in *Fundamentals of Computation Theory* Berlin, Germany: Springer, 2009, pp. 62–73.
[34] P. Indyk, H. Q. Ngo, and A. Rudra, "Efficiently decodable non-adaptive group testing," in *Proc. 21st Annu. ACM-SIAM Symp. Discrete Algorithms*. Philadelphia, PA, USA: Soc. Ind. Appl. Math., 2010, pp. 1126–1142.
[35] K. Lee, R. Pedarsani, and K. Ramchandran, "Saffron: A fast, efficient, and robust framework for group testing based on sparse-graph codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 2873–2877.
[36] S. Cai, M. Jahangoshahi, M. Bakshi, and S. Jaggi, "Efficient algorithms for noisy group testing," *IEEE Trans. Inf. Theory*, vol. 63, no. 4, pp. 2113–2136, Apr. 2017.
[37] C. L. Chan, S. Jaggi, V. Saligrama, and S. Agnihotri, "Non-adaptive group testing: Explicit bounds and novel algorithms," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 3019–3035, May 2014.
[38] A. G. D'yachkov and V. V. Rykov, "A survey of superimposed code theory," *Problems Control Inf. Theory*, vol. 12, no. 4, pp. 229–242, 1983.
[39] A. de Bonis, A. Gąsieniec, and U. Vaccaro, "Optimal two-stage algorithms for group testing problems," *SIAM J. Comput.*, vol. 34, no. 5, pp. 1253–1270, 2005.
[40] A. M. Rashad, "Random coding bounds on the rate for list-decoding superimposed codes," *Problems Control Inf. Theory-Problemy Upravleniya I Teorii Informatsii*, vol. 19, no. 2, pp. 141–149, 1990.
[41] M. Sobel, S. Kumar, and S. Blumenthal, "Symmetric binomial group-testing with three outcomes," in *Proc. Purdue Symp. Decis. Procedure*, 1971, pp. 119–160.
[42] F. K. Hwang, "Three versions of a group testing game," *SIAM J. Algebr. Discrete Methods*, vol. 5, no. 2, pp. 145–153, 1984.
[43] H.-B. Chen and H.-L. Fu, "Nonadaptive algorithms for threshold group testing," *Discrete Appl. Math.*, vol. 157, no. 7, pp. 1581–1585, 2009.
[44] M. Cheraghchi, "Improved constructions for non-adaptive threshold group testing," *Algorithmica*, vol. 67, no. 3, pp. 384–417, 2013.
[45] T. V. Bui, M. Kuribayashi, M. Cheraghchi, and I. Echizen, "Efficiently decodable non-adaptive threshold group testing," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Vail, CO, USA, Dec. 2017, pp. 2584–2588.
[46] H. A. Inan, P. Kairouz, and A. Ozgur, "Sparse group testing codes for low-energy massive random access," in *Proc. 55th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2017, pp. 658–665.
[47] V. Gandikota, E. Grigorescu, S. Jaggi, and S. Zhou, "Nearly optimal sparse group testing," in *Proc. 54th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2016, pp. 401–408.
[48] H. A. Inan, P. Kairouz, and A. Ozgur, "Energy-limited massive random access via noisy group testing," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2018, pp. 1101–1105.
[49] T. Hartman and R. Raz, "On the distribution of the number of roots of polynomials and explicit weak designs," *Random Struct. Algorithms*, vol. 23, no. 3, pp. 235–263, 2003.
[50] R. Bardenet and O.-A. Maillard, "Concentration inequalities for sampling without replacement," *Bernoulli*, vol. 21, no. 3, pp. 1361–1385, 2015.

Huseyin A. Inan is a Ph.D. candidate in the department of Electrical Engineering at Stanford University. He received the B.Sc. degrees in electrical engineering and mathematics from Bogazici University, Istanbul, Turkey, in 2012 and the M.Sc. degree in electrical engineering from Koc University, Istanbul, Turkey in 2014. His research interests include coding theory, wireless communication, and machine learning.

Peter Kairouz is a research scientist at Google. Before joining Google, he was a postdoctoral research fellow at Stanford University. He received his Ph.D. in ECE, M.S. in Maths, and M.S. in ECE from the University of Illinois at Urbana-Champaign (UIUC). During his Ph.D., he interned twice at Qualcomm and once at Google, where he designed privacy-aware utility-optimal unsupervised learning algorithms. He taught classes on big data and probabilities at UIUC, and was the General Chair for the 10th Annual Coordinated Science Laboratory Student Conference. His work on data privacy was recently featured on Forbes. He is the recipient of the 2012 Roberto Padovani Scholarship from Qualcomm's Research Center, the 2015 ACM SIGMETRICS Best Paper Award, the 2015 Qualcomm Innovation Fellowship Finalist Award, and the 2016 Harold L. Olesen Award for Excellence in Undergraduate Teaching from UIUC. His research interests span the areas of privacy-preserving data analysis, machine learning, and information theory.

Mary Wootters is an assistant professor of Computer Science and Electrical Engineering at Stanford University. She received a Ph.D. in mathematics from the University of Michigan in 2014, and a BA in math and computer science from Swarthmore College in 2008; she was an NSF postdoctoral fellow at Carnegie Mellon University from 2014 to 2016. Her research interests include randomized algorithms, coding theory, dimension reduction, matrix completion, and sparse signal processing.

Ayfer Özgür (M'06) received her B.Sc. degrees in electrical engineering and physics from Middle East Technical University, Turkey, in 2001 and the M.Sc. degree in communications from the same university in 2004. From 2001 to 2004, she worked as hardware engineer for the Defense Industries Development Institute in Turkey. She received her Ph.D. degree in 2009 from the Information Processing Group at EPFL, Switzerland. In 2010 and 2011, she was a post-doctoral scholar at the same institution. She is currently an Assistant Professor in the Electrical Engineering Department at Stanford University where she is a Hoover and Gabilan Fellow. Her current research interests include distributed communication and learning, wireless systems, and information theory. Dr. Özgür received the EPFL Best Ph.D. Thesis Award in 2010, the NSF CAREER award in 2013, the Okawa Foundation Research Grant and the IEEE Communication Theory Technical Committee (CTTC) Early Achievement Award in 2018.