



Generalized framework for Group Testing: Queries, feedbacks and adversaries

Marek Klonowski^a, Dariusz R. Kowalski^{b,*}, Dominik Pająk^a

^a Wrocław University of Science and Technology, Wrocław, Poland

^b Augusta University, Augusta, GA, USA

ARTICLE INFO

Article history:

Received 27 November 2021

Accepted 20 March 2022

Available online 25 March 2022

Communicated by P. Lu

Keywords:

Group testing

Queries

Feedback functions

Adversaries

Non-adaptive algorithms

Deterministic algorithms

Randomized algorithms

Lower bound

ABSTRACT

In the Group Testing problem, the objective is to learn a subset K of some much larger domain N , using the shortest-possible sequence of queries Q . A feedback to a query provides some information about the intersection between the query and subset K . Several specific feedbacks have been studied in the literature, often proving different formulas for the estimate of the query complexity of the problem, defined as the shortest length of queries' sequence solving Group Testing problem with specific feedback. In this paper we study what are the properties of the feedback that influence the query complexity of Group Testing and what is their measurable impact. We propose a generic framework that covers a vast majority of relevant settings considered in the literature, which depends on two fundamental parameters of the feedback: input capacity α and output expressiveness β . They upper bound the logarithm of the size of the feedback function domain and image, respectively. To justify the value of the framework, we prove upper bounds on query complexity of non-adaptive, deterministic Group Testing under some "efficient" feedbacks, for minimum, maximum and general expressiveness, and complement them with a lower bound on all feedbacks with given parameters α, β . Our upper bounds also hold if the feedback function could get an input twisted by a malicious adversary, in case the intersection of a query and the hidden set is bigger than the feedback capacity α . We also show that slight change in the feedback function may result in substantial worsening of the query complexity. Additionally, we analyze explicitly constructed randomized counterparts of the deterministic results. Our results provide some insights to what are the most useful bits of information an output-restricted feedback could provide, and open a number of challenging research directions.

© 2022 Elsevier B.V. All rights reserved.

1. Introduction

Group Testing, introduced by [25], is an inference problem, where the goal is to identify, by asking queries, all elements of an unknown set K . All we initially know about set K is that $|K| \leq k$ and that it is a subset of some much larger set N with $|N| = n$, for given parameters k, n . To learn set K , we must have answers to the queries that provide some information about set K . In our model, the answer to a query Q depends on the intersection between K and Q and equals to $\text{Feed}(K \cap Q)$, where Feed is some known pre-defined feedback function. The sequence of queries is a correct solution to Group Testing if and only if for any two different sets K_1, K_2 such that $|K_1|, |K_2| \leq k$, the sequence of feedback answers computed for

* Corresponding author.

E-mail address: dkowalski@augusta.edu (D.R. Kowalski).

sets K_1 and K_2 are different; we say then that the sequence of queries distinguishes any pair of sets, or identifies any set of size at most k .¹ The objective is, for a given deterministic feedback function $\text{Feed}(\cdot)$, to find a sequence of queries that identifies any set K of size at most k and the length of this sequence, called query complexity, will be shortest possible. In particular, we are interested in algorithms that have query complexity logarithmic in $n = |N|$ and polynomial in $k = |K|$. In the classic variant, studied in most of the existing relevant literature, the function Feed simply answers whether the intersection between K and Q is empty or not, while another popular feedback returns the size of the intersection [26,29]. These variants were applied in many domains, including pattern matching [14,35], compressed sensing [16], streaming algorithms [17] and graph reconstruction [12,30] or even accelerating computations in neural networks [39]. Though one of the most prominent examples of applications of Group Testing is in conflict resolution in communication networks [8,9,11,29,31,32,38,41,45].

There is a large body of literature introducing new variants of the Group Testing [10,30,7,22,21], which could be simply viewed as different feedback functions applied to some generic Group Testing framework. Therefore, in this paper we aim at designing such a universal framework allowing a holistic view at many previous modifications of Group Testing setting, and study the dependence of the query complexity on two identified fundamental parameters of the feedback function:

Capacity: this parameter denotes the maximum set size that can be processed by the feedback function. In other words, the domain of the feedback function with capacity α is the family of all subsets of N of size at most α . The capacity is denoted by α throughout this paper and varies between 1 and k .

Expressiveness: this parameter denotes the number of output bits of the feedback function.

It is denoted by β throughout this paper, and varies between 1 and $\bar{\alpha}$, where the latter denotes a binary logarithm of the number of all subsets of N of size at most α , i.e., $\bar{\alpha} = \log_2 \sum_{i=0}^{\alpha} \binom{n}{i}$.

A feedback function with capacity α and expressiveness β is called an (α, β) -feedback.

If for some query Q , $|Q \cap K| > \alpha$, then the intersection set $Q \cap K$ cannot be passed directly to the feedback function, because (α, β) -feedback functions are not defined for such sets. Therefore, in our framework we resolve this issue by presence of an adversary – a non-deterministic feature which, for such queries with large intersection, selects a set with at most α elements and the answer to query Q is the feedback on this set. We consider different models of an adversary, including a powerful Malicious Adversary, who could “fool” the feedback with *arbitrary* sets of at most α elements of N ,² and more benign Honest Adversary, who always returns *some subset* of the intersection.

Clearly, increasing the capacity parameter α or expressiveness β increases the number of (α, β) -feedback functions, and thus should decrease the query complexity of the best feedbacks in this family. But what is the asymptotic pace of this query complexity decrease? Is there a substantial difference in query complexity of Group Testing under Honest and Malicious adversaries? Are there better and worse feedback functions for given α, β , i.e., resulting in smaller (resp., larger) query complexity? This paper provides partial answers to these questions.

Document structure. In Section 2 we formally define the general framework of (n, k) -Group-Testing, including (α, β) -feedback functions and adversaries, and outline the contribution of the paper. Then we discuss a related work on specific feedbacks in Section 3. In Section 4 we prove upper bounds on the query complexity for efficient feedbacks with minimal, maximal and general expressiveness β and any capacity α , under powerful Malicious Adversary. Section 5 presents a lower bound for feedbacks with maximum expressiveness, i.e., $(\alpha, \bar{\alpha})$ -feedbacks, which holds even for more benign Honest adversaries. A case study of two $(\alpha, 2 \log n)$ -feedback functions with (provably) substantially different query performance is given in Section 6. Discussion of results from perspective of future directions is given in Section 7.

2. Generalized framework and our contribution

As we will discuss in Sections 2.1 and 3, many previously considered variants of (n, k) -Group-Testing problem could be expressed by, and their query complexities depend on, specific parameters of the feedback to the queries. Here, we formally introduce generalized framework, including families of (α, β) -feedbacks, where α is the feedback capacity while β is its expressiveness, and adversaries that provide input to the feedback function in case the intersection has more than α elements. We consider *non-adaptive deterministic* solutions, in which subsequent queries do not depend on the feedback from the previous ones nor on random bits. This class is very popular in the literature, due to its applicability and relevance to coding [37] and information theory [28,3].

In subsequent technical sections, we will be studying query complexity of the whole classes of (α, β) -feedbacks, depending on parameters n, k, α, β and specific adversary, as well as several interesting sub-classes. We will also discuss

¹ In this work we abstract from computational efficiency of decoding of sets, which is a large research area by itself, cf., [2].

² One could also assume that the Malicious Adversary could give *any* input to the feedback function in case of exceeded capacity – this could however require re-definition of the feedback function to handle non-valid input sets.

Example of an adversary, widely but implicitly considered in the literature, is the mechanism of feedback in radio networks or multiple access channels, when the feedback provides answers “collision” or “silence” or an arbitrary element if two or more neighbors of a communication device transmit simultaneously, cf., [4,11].

randomized counterparts of our deterministic solutions, cf., Definition 4, as in some cases they could be computed more efficiently.

We assume that the universe of all elements N , with $|N| = n$, is enumerated with integers $1, 2, \dots, n$. Throughout the paper we will associate an element with its identifier.

Specification of generalized group testing framework.

Definition 1. The generalized (n, k) -Group-Testing framework is defined as follows:

1. An (n, k) -Group-Testing Algorithm is defined as a sequence of queries $\mathcal{Q} = \mathcal{Q}^{n,k} = \langle Q_1, Q_2, \dots, Q_t \rangle$ depending on n, k , where each query is an arbitrary subset of N . The sequence length t is called a query complexity of the sequence/algorithm.³
2. An adversary is defined as an entity that performs two actions. Firstly, it chooses set K as an arbitrary subset of N with $|K| \leq k$. Secondly, it defines a function $\text{Adv}(X, i \mid \mathcal{Q}, K)$, for every $X \subseteq N$, and every $i \in \{1, \dots, |\mathcal{Q}|\}$, where i denotes the index⁴ in sequence \mathcal{Q} . This function must satisfy:
 - $\text{Adv}(X, i \mid \mathcal{Q}, K) \subseteq N$,
 - $|\text{Adv}(X, i \mid \mathcal{Q}, K)| \leq \alpha$,
 - $\text{Adv}(X, i \mid \mathcal{Q}, K) = X$, if $|X| \leq \alpha$.
3. An adversary strategy, under a given query sequence \mathcal{Q} and a set K fixed by an adversary is defined as a function $\text{Adv}(X, i \mid \mathcal{Q}, K)$ of two arguments: set $X \subseteq N$ and index $i \in \{1, 2, \dots, |\mathcal{Q}|\}$. $\mathcal{S}_{adv}(\mathcal{Q}, K)$ denotes the set of all adversarial strategies under a given query sequence \mathcal{Q} and a set K fixed by an adversary, and $\mathcal{S}_{adv}(\mathcal{Q}, \cdot) = \{\mathcal{S}_{adv}(\mathcal{Q}, K)\}_{K \subseteq N, |K| \leq k}$ is the set of all possible strategies of the adversary over sets K of at most k elements.
4. An (α, β) -feedback function Feed is a function that takes as an input any subset of N with at most α elements and outputs a binary vector of β bits.
5. A feedback vector is defined as a sequence of outputs of the feedback function on the intersections between K and the subsequent queries Q_1, Q_2, \dots, Q_t :

$$\mathcal{F}(K, \text{Adv}) = (\text{Feed}(\text{Adv}(Q_1 \cap K, 1 \mid \mathcal{Q}, K)), \text{Feed}(\text{Adv}(Q_2 \cap K, 2 \mid \mathcal{Q}, K)), \dots, \text{Feed}(\text{Adv}(Q_t \cap K, t \mid \mathcal{Q}, K))) .$$

6. For any fixed n, k , we say that a sequence of queries \mathcal{Q} solves (n, k) -Group-Testing problem under some adversary with the set of possible strategies $\mathcal{S}_{adv}(\mathcal{Q}, \cdot)$ if we have:

$$\bigvee_{\substack{K_1, K_2 \subseteq N \\ |K_1|, |K_2| \leq \alpha \\ K_1 \neq K_2}} \{ \mathcal{F}(K_1, \text{Adv}) : \text{Adv} \in \mathcal{S}_{adv}(\mathcal{Q}, K_1) \} \cap \{ \mathcal{F}(K_2, \text{Adv}) : \text{Adv} \in \mathcal{S}_{adv}(\mathcal{Q}, K_2) \} = \emptyset$$

In other words, the sets of possible (under the given adversary) feedback vectors for two different sets K_1, K_2 are disjoint.

In the above framework, the adversary could be deterministic (if the set of strategies $\mathcal{S}_{adv}(\mathcal{Q}, K)$ for any given \mathcal{Q}, K is a single function, e.g., always passing an empty set to the feedback function for intersections larger than α) or non-deterministic (otherwise). The feedback function is always deterministic. Observe also that in case of non-adaptive algorithms considered in this work the order of queries does not matter from perspective of query complexity, but helps in the analysis to relate queries with their corresponding feedbacks in the feedback vector.

Decoding of elements. It follows from our Definition 1, point 6, of solving (n, k) -Group-Testing problem that elements of the hidden set K could be enlisted. A straightforward, though not computationally efficient way, would be to consider all possible sets K of size at most k ; then, for each of them – consider a family of all possible adversarial strategies and compute feedback vectors for them; finally, one could find among them a matching copy of the actual feedback vector. This copy is in some computed family corresponding to a set K , which is the actual hidden set to be enlisted. The correctness of this solution follows directly from Definition 1, point 6: all possible feedback vectors obtained for all possible adversarial strategies are disjoint for different sets K of size at most k . In this work we do not study more efficient decoding algorithms than the above mentioned method – this topic could be an interesting and challenging future direction.

³ Due to the scope of this paper, our definition considers non-adaptive algorithms, i.e., in which the sequence of queries is fixed in advance. However, an analogous framework can be defined for adaptive algorithm, in which consecutive queries are defined based on the partial feedback vector, i.e., feedbacks on the preceding queries.

⁴ This means that the adversary receives not only the whole sequence \mathcal{Q} but also the step number; hence, may output different values for two identical intersection sets but obtained for different queues.

Maximum capacity. The intersection between a query and set K has always at most k elements, hence having α larger than k does not increase the power of the model compared to the case of $k = \alpha$. Therefore, in all our results we assume that $k \geq \alpha$ (for a setting $\alpha > k$ one could use a sequence of queries for $k = \alpha$).

Maximum expressiveness. Similarly, we may restrict our considerations to $\beta \leq \bar{\alpha}$ because of the following fact.

Proposition 1. *For any feedback function f_1 , there exists a feedback function f_2 with expressiveness $\beta \leq \bar{\alpha}$ such that for any two sets $K_1, K_2 \subseteq N$, with $|K_1|, |K_2| \leq \alpha$,*

$$f_1(K_1) = f_1(K_2) \Leftrightarrow f_2(K_1) = f_2(K_2).$$

Adversaries and feedback functions. In this paper we consider the following adversaries and feedback functions. Note that one could consider also other types of adversaries and feedback functions.

Definition 2. We define the following two adversary types:

1. α -Malicious Adversary. This adversary, whenever for some query Q we have $|Q \cap K| > \alpha$, chooses an arbitrary subset of at most α elements from set N and passes this set to the feedback function. Effectively, such adversary has the power to choose an arbitrary value of feedback for queries that intersect with the hidden set K on more than α elements.
2. α -Honest Adversary. This adversary, whenever for some query Q we have $|Q \cap K| > \alpha$, chooses a subset of exactly α elements from set $Q \cap K$ and passes this set to the feedback function.
 - α -Honest x -Avoiding Adversary, is a special case of α -Honest Adversary that for some element $x \in N$, if $x \in K \cup Q$ and $|K \cup Q| > \alpha$ then the set chosen by the adversary does **not** contain element x . In other words it hides element x , whenever possible.

Definition 3. We define the following three feedback functions:

1. $\text{Parity}^{(\alpha)}(X) = (|X| \bmod 2)$. It is an $(\alpha, 1)$ -feedback, function because the returned value can be encoded on one bit.
2. $\text{Full}^{(\alpha)}(X) = X$. It is an $(\alpha, \bar{\alpha})$ -feedback, as any subset of N of at most α elements can be encoded by $\bar{\alpha}$ bits.
3. $\text{General}^{(\alpha, \beta)}(X) = (|X| \bmod 2) \parallel (\bigoplus_{x \in X} \text{BCC}(x))$, where $\text{BCC}(x)$ is an $\left[n, \beta - 1, \left\lfloor \frac{\beta - 1}{c \log \frac{n}{k}} \right\rfloor \right]$ -BCC code of element x , cf., Definition 5, and c is a constant from [10, Lemma 2] \bigoplus denotes bitwise XOR operation and \parallel denotes concatenation of vectors. It is an (α, β) -feedback, because BCC code uses $\beta - 1$ bits and the remaining bit denotes the parity of $|X|$.

The above Definition 2 of adversaries and the third defined feedback function in Definition 3 have not been considered in the Group Testing literature, to the best of our knowledge. We will derive upper bounds under the strongest of the defined adversaries, α -Malicious Adversary, while we also prove nearly matching lower bound(s) that holds also under the weaker α -Honest x -Avoiding Adversary; thus, the power of the adversary does not have a substantial impact on the query complexity of Group Testing.

The next observation specifies useful criteria for the analysis of algorithms against α -Malicious Adversary, which we will apply in all our proofs of upper bounds.

Proposition 2. *Fix any n, k . If for query sequence $\mathcal{Q}^{n,k} = \langle Q_i \rangle_{i=1}^t$ we have that for any $K_1, K_2 \subset N$, with $|K_1|, |K_2| \leq \alpha$ and $K_1 \neq K_2$:*

$$\exists_{\tau} |Q_{\tau} \cap K_1| \leq \alpha \wedge |Q_{\tau} \cap K_2| \leq \alpha \wedge \text{Feed}(Q_{\tau} \cap K_1) \neq \text{Feed}(Q_{\tau} \cap K_2),$$

then $\mathcal{Q}^{n,k}$ solves (n, k) -Group-Testing under α -Malicious Adversary.

In the following we will say that a query Q_{τ} distinguishes sets K_1 and K_2 under some feedback function Feed if $|Q_{\tau} \cap K_1| \leq \alpha$, $|Q_{\tau} \cap K_2| \leq \alpha$ and $\text{Feed}(Q_{\tau} \cap K_1) \neq \text{Feed}(Q_{\tau} \cap K_2)$.

2.1. Technical results

Binary feedback. First, we consider feedbacks with minimum possible expressiveness, namely, returning only one bit of information. In this setting we have to answer the question of *What is the most useful bit of information about a set of elements?* It turns out that a parity bit allows us to obtain an efficient solution in the family of $(\alpha, 1)$ -feedbacks. Interestingly, this result, and all our other upper bounds, hold for the strongest adversary.

Theorem 1. *Under $\text{Parity}^{(\alpha)}$ feedback and under α -Malicious Adversary, there exists a deterministic solution to (n, k) -Group-Testing with query complexity $O\left(\left(k + \frac{k^2}{\alpha}\right) \cdot \log \frac{n}{k}\right)$.*

The proof is based on derandomization of random queries drawn from different random distribution, after proving that these queries satisfy a certain Separation Property (formulated and proved in Lemma 1).

Full feedback. Our second result is in the setting with the maximum possible expressiveness $\beta = \bar{\alpha} = \Theta(\alpha \log(n/\alpha))$, i.e., sufficient to return all identifiers of any set of size at most α . We show that maximum expressiveness allows to design algorithms with small query complexity $O\left(\min\left\{\frac{n}{\alpha}, \frac{k^2}{\alpha^2} \cdot \log^c n\right\}\right)$ for some $c \in [1, 2]$, more precisely:

Theorem 2. *Under Full^(α) feedback and under α -Malicious Adversary, there exists a deterministic solution to (n, k) -Group-Testing with query complexity:*

$$O\left(\min\left\{\frac{n}{\alpha}, \frac{k^2}{\alpha^2} \cdot \log n\right\}\right) \quad \text{if } \alpha > 18 \log k,$$

$$O\left(\min\left\{\frac{n}{\alpha}, \frac{k^2}{\alpha} \cdot \log \frac{n}{k}\right\}\right) \quad \text{otherwise.}$$

The proof is via derandomization of a random sequence of queries \mathcal{Q} , from which we require to simultaneously satisfy two conditions: on the number of queries containing a specific element, and on the sizes of the intersections of queries from any subset of \mathcal{Q} of certain size and any possible instantiation of set K .

Interestingly, for $\alpha = \omega(\sqrt{k \log n})$, the obtained query complexity is sublinear in k . This can be contrasted with an $\Omega(k \log(n/k))$ lower bound for classical Group Testing (i.e., for $\alpha = O(1)$) that holds also for any randomized algorithm working with non-vanishing probability [15]. This proves the impact of feedback capacity on query complexity.

General feedback. After considering both extreme values of β we study the general case, where a feedback needs to work for an arbitrary $1 \leq \beta \leq \bar{\alpha}$. In this case our first contribution is a design of a more sophisticated general feedback function General^(α, β), cf., Definition 3, which works for almost any α, β . Our proposed feedback is a concatenation of a specific code (called BCC code) with an additional parity bit. Under this feedback we obtain the main result of the paper:

Theorem 3. *Under General^(α, β) feedback and under α -Malicious Adversary, there exists a deterministic solution to (n, k) -Group-Testing with query complexity $O\left(\frac{k^2}{\alpha\beta} \log^{c+1} n\right)$ for some $c \in [1, 2]$, more precisely:*

$$O\left(\frac{k^2}{\alpha\beta} \log n \left(\frac{\beta}{\alpha} + \log n\right)\right) \quad \text{if } \alpha > 18 \log k,$$

$$O\left(\frac{k^2}{\alpha} \cdot \log \frac{n}{k}\right) \quad \text{otherwise.}$$

Our main result shows that the query complexity decreases linearly with α and with β . Intuitively factor $\frac{k}{\alpha}$ in our complexity comes from *congestion*, since the feedback function has capacity to serve at most α elements out of k in a single query. The second factor $\frac{k \log \frac{n}{k}}{\beta} \approx \frac{\log \binom{n}{k}}{\beta}$ comes from the information-theoretic bound that we need $\log_2 \binom{n}{k}$ bits to uniquely encode any subset of k elements and the fact that the feedback function provides only β bits per round. What is surprising and challenging to prove is that the query complexity of efficient (but not all!) (α, β) -feedbacks is (close to) a multiplication of these two characteristics.

The proof combines ideas from the analysis of the binary feedback and full feedback. In the binary feedback case we observe that sets that differ on many elements can be distinguished quickly using the parity feedback. On the other hand, sets that differ only on few elements are handled using a combination of full feedback algorithm with a specific coding to encapsulate the feedback into β bits.

Lower bound. We show a lower bound that proves that our upper bound shown in Theorem 2 is optimal up to polylogarithmic factor, for any α . It holds even for a weaker adversary, α -Honest Adversary, or more specifically, for its sub-type of α -Honest x -Avoiding Adversary. Thus, it also holds for the stronger α -Malicious Adversary, for which all our algorithms are analyzed.

Theorem 4. *If $n > k^2 \log n / \log k$, then any deterministic solution to (n, k) -Group-Testing under any (α, β) -feedback has query complexity $\Omega\left(\frac{k^2}{\alpha^2} \log^{-1} k\right)$ for some α -Honest Adversary.*

The proof of Theorem 4 is by transformation of our generalized Group Testing framework to selectors – structures studied in related literature, formally defined in Section 5. We show that if there were shorter query sequences, there would exist selectors violating some of their lower bound. This transformation is however possible only in one way, as we will show in the next result.

Table 1

Results on non-adaptive (n, k) -Group-Testing with (α, β) -feedback. The upper bound column states query complexity of the best found (α, β) -feedback found for parameters α, β fixed in the first two columns; as we will show, not all (α, β) -feedbacks could reach that complexity. Symbol $*$ stands for any valid value of the parameter, and $\bar{\alpha}$ stands for a ceiling of the binary logarithm of the number of all subsets of N of size at most α . We display results from Theorem 2 and 3 in regime $\alpha > 18 \log k$, however our theorems cover the whole range of α .

α	β	Upper bound	Lower bound
1	1	$O(k^2 \log \frac{n}{k})$ [19]	$\Omega(k^2 \frac{\log n}{\log k})$ [13]
k	1	$O(k \log \frac{n}{k})$ [10]	$\Omega(k \log \frac{n}{k})$ [10]
k	$\log k$	$O(k \frac{\log \frac{n}{k}}{\log k})$ [30]	$\Omega(k \frac{\log \frac{n}{k}}{\log k})$ [23,40]
*	1	$O((k + \frac{k^2}{\alpha}) \log \frac{n}{k})$ Theorem 1	$\Omega(\frac{k^2}{\alpha^2} \log^{-1} k)$ Theorem 4
*	$\bar{\alpha}$	$O(\min\{\frac{n}{\alpha}, \frac{k^2}{\alpha^2} \log n\})$ Theorem 2	$\Omega(\frac{k^2}{\alpha^2} \log^{-1} k)$ Theorem 4
*	*	$O(\frac{k^2}{\alpha \beta} \log^2 n)$ Theorem 3	$\Omega(\frac{k^2}{\alpha^2} \log^{-1} k)$ Theorem 4

Minimum elements feedbacks. Our two final results show that designing an efficient feedback function is very subtle. We show that a reasonable $(\alpha, 2 \log n)$ -feedback function that returns two minimal elements from the set leads to very large query complexity of $\Omega(\min\{n, k^2\})$ if we restrict the function to return the elements *in fixed order*, cf., Theorem 5. Without this restriction it is possible to obtain feedback function for which there exists a deterministic algorithm with query complexity $O(\frac{k^2}{\alpha} \cdot \log \frac{n}{k})$, cf., Corollary 5.

Theorem 5 with Corollary 5 provide an argument that there is no universal reduction between selectors and our general Group Testing framework, as both the considered feedback functions have the same parameters α and β and differ only (slightly) in the definition of the feedback function, yet having query complexities different nearly by factor α . Thus, our general framework is provably more complex than the theory of selectors.

Table 1 presents our main deterministic results in comparison to the most related previous work on specific feedback functions. In this work we also analyze explicitly constructed randomized counterparts of the deterministic results.

Definition 4. A randomized algorithm solves (n, k) -Group-Testing against Adaptive Adversary with probability $1 - c$, for some $0 \leq c < 1$, if with probability $1 - c$ it generates a sequence of queries \mathcal{Q} that solves (n, k) -Group-Testing according to Definition 1.

Note that in Definition 4 the adversary is assumed to know sequence \mathcal{Q} (see Definition 1(3)). Hence, our analysis' of randomized counterparts of deterministic solutions also hold against *Adaptive Adversary*. This is to distinguish from the case, where the adversary does not know all the queries when choosing set K [20,5].

3. Motivation, previous and related work

The problem of Group Testing (and related equivalent problems such as coin weighting) has been considered in various feedback models. In this section we present details of implementation of some classical feedback models in our framework. Our framework, with two parameters of feedback α and β , allows, among others, a comparison of results in different models, for a discussion about what is the best utilization of feedback output bits, and for comparison and generalization of existing results obtained for specific feedbacks, cf., Table 1.

Beeping model and shared channel communication. Beeping feedback model is a standard model considered in most of the Group Testing literature [26], where the feedback tells whether the intersection between query Q and set K is empty or not. Solutions to Group Testing in this feedback model have direct applications to conflict resolution on a multiple access channel and broadcast in unknown radio networks, cf., [13].

Observe that in Beeping feedback model, the feedback returns 0 if the intersection is empty and 1 otherwise. Thus beeping feedback is a $(1, 1)$ -feedback.

In this feedback model, the Group Testing problem is known to be solvable using $O(k^2 \log(n/k))$ [19] queries and an explicit construction of length $O(k^2 \log^2 n)$ [37] exists. Best known lower bound (for $k < \sqrt{n}$) is $\Omega(k^2 \log n / \log k)$ [13].

A related model, where the feedback equals NULL if the intersection is of size 0, the identifier of the element, if the intersection is of size 1 and a value COLLISION otherwise, can be seen as $(2, \log n)$ -feedback. This model is applicable to communication on shared channel and has been an area of extensive research. The solutions in literature include adaptive algorithms [8,9], semi-oblivious algorithms where an element can deactivate after successful transmission [38,32] (see surveys [29,11] for more details on results in this model). As mentioned earlier, some of the previous works also consider non-adaptive adversarial component of the feedback, cf., [4].

Finite-field additive radio network. In this model, the feedback to a query is a parity of the size of the intersection between set K and a query. One can observe that using BCC-codes of length $O(k \log \frac{n}{k})$ [10] it is possible to design a sequence of queries of the same length, that solves (n, k) -Group-Testing in this model. This construction solves (n, k) -Group-Testing with $O(k \log \frac{n}{k})$ in a Parity^(k) feedback model (which is an example of $(k, 1)$ -feedback), because by the definition of BCC-codes any bit-wise XOR of up to k codewords is unique. The construction of BCC codes has also been applied to solutions of standard communication problems (such as broadcast) in specific models of communication networks [10].

We note that Parity^(α) feedback for borderline value of $\alpha = k$ corresponds to the setting considered in [10]. In this case our algorithm matches the best known upper bound, hence our proposed feedback function and our algorithm are a valid generalization, showing the smooth transition of query complexity between settings of $\alpha = \log k$ and $\alpha = k$ in a pace inversely proportional to the feedback capacity α .

Coin weighting. The problem of coin weighting is exactly the Group Testing problem with a different feedback. In the coin weighting problem, we have a set of n coins of two distinct weights w_0 (true coin) and w_1 (counterfeit coin), out of which up to k are counterfeit ones. We are allowed to weight any subset of coins in a spring scale, hence we can deduce the number of counterfeit coins in each weighting. The task is to identify all the counterfeit coins.

The coin weighting can be implemented in our framework as a $(k, \log k)$ -feedback, where the feedback returns the size of the intersection between the query and the set K . The problem is solvable with $O(k \log(n/k) / \log k)$ [30] queries.

Bounds for both BCC codes and non-adaptive coin weighting are tight, thus increasing the number of output bits from 1 to $\log k$ results in decrease in query complexity by a factor of $\log k$.

Threshold group testing. In this variant of Group Testing introduced in [18], a number of thresholds $0 < t_1 \leq t_2 \leq \dots \leq t_s$ are defined. Thresholds divide the set $[k]$ into set of discrete intervals $[0, t_1), [t_1, t_2), \dots, [t_{s-1}, t_s), [t_s, k]$. The feedback to query Q is the index of the interval to which $|K \cap Q|$ belongs. This feedback can be implemented as a $(t_s + 1, \log s)$ -feedback. An upper bound for a single threshold t of approximately $O(\frac{k^2}{\sqrt{t}} \log \frac{n}{k})$ [22] suggests that single threshold feedback is probably not the optimal feedback (according to our parameters) since we know that $(t, 1)$ -feedbacks can lead to query complexity $O(\frac{k^2}{t} \log \frac{n}{k})$. On the other hand, in [21] the authors analyze a feedback with $\sqrt{k \log k}$ thresholds out of which maximum threshold is $\Omega(k)$, which in our framework translates to a $(k, \log k)$ -feedback. Result in [21] is an algorithm with query complexity $O(\frac{k}{\log k} \cdot \log \frac{n}{k})$, which is logarithmically far from $O(\frac{k}{\log k} \log^2 n)$ obtained from our generic upper bound $O(\frac{k^2}{\alpha \beta} \log^2 n)$ in Theorem 3 instantiated for $\alpha = k, \beta = \log k$.

Other related results. The problem of Group Testing has been recently discussed from different perspectives. Some papers consider different models of generating (or constraining) the subset K . This may lead to critically different optimal strategies, even for non-adaptive settings. In [1] the author considers the model, wherein each element is included in K with a fixed probability p – we need $\Omega(n)$ tests to have error probability tending to zero. Somehow related randomized model has been discussed in [20], wherein the algorithm may fail on a small fraction of inputs. In [34] the authors consider “sparse” Group Testing, where the size of each query is limited. They also consider settings wherein each element can be included in a limited number of queries.

4. Upper bounds

4.1. Minimal expressiveness – binary feedback

We first show (Lemma 1) an upper bound on length of a sequence that distinguishes any pair of sets satisfying a certain size restriction. This length is inversely proportional to the product of capacity α and the lower bound on the size of the symmetric difference between the sets, denoted by δ . This proof is based on analyzing a certain Separation Property of a sequence of random queries drawn from specific probabilistic distribution, and showing that it yields distinguishing between two sets K_1, K_2 with a large probability, sufficient to derandomize it. In the second step (Lemma 3), we show how to remove the size restrictions from the result. Finally, Theorem 1 will follow directly from Lemma 3 applied for $\delta = 1$.

In Lemma 3 we will need the following notation and basic facts.

Basic notation and tools. We will use the following notation for the symmetric difference of two sets $A \triangle B = (A \setminus B) \cup (B \setminus A)$. In our proofs, we also use the following two elementary facts:

Fact 1. Let $X \sim \text{Binomial}(n, p)$, then $\mathbb{P}[X \text{ is odd}] = \frac{1}{2} - \frac{1}{2}(1 - 2p)^n$.

The proof of Fact 1 can be found in the appendix. The following fact can be found e.g., in [42, (p. 34, eq. 6)].

Fact 2. For any $0 \leq x \leq 1$ and $n \in \mathbf{N}_+$: $(1 - x)^n \leq 1 - nx + \frac{1}{2}n(n - 1)x^2$.

Main technical tools. We first show how to construct sequences distinguishing pairs of sets K_1, K_2 satisfying specific conditions.

Lemma 1. For any $1 \leq \delta \leq k/\alpha$ and if $k \geq \alpha$, there exists a sequence of $O\left(\frac{k^2}{\alpha\delta} \cdot \log(n/k)\right)$ sets \mathcal{Q} such that for any two sets $K_1, K_2 \subseteq N$ satisfying $k \geq |K_1| \geq k/2$ and $|K_1| \geq |K_2|$ and $|K_1 \triangle K_2| \geq \delta$ there exists $Q \in \mathcal{Q}$ that satisfies $|Q \cap K_1| \leq \alpha$, $|Q \cap K_2| \leq \alpha$ and $\text{Parity}^{(\alpha)}(Q \cap K_1) \neq \text{Parity}^{(\alpha)}(Q \cap K_2)$.

Proof. We will show this result using the probabilistic method. More precisely, we first define a sequence of random queries \mathcal{Q} of length $O\left(\frac{k^2}{\alpha\delta} \cdot \log(n/k)\right)$. Next, we fix any two different sets $K_1, K_2 \subseteq N$ whose cardinalities satisfy the conditions of the lemma. Recall that, by Proposition 2, a query $Q \in \mathcal{Q}$ distinguishes K_1 from K_2 if it satisfies the three conditions from the statement of the Lemma: $|Q \cap K_1| \leq \alpha$, $|Q \cap K_2| \leq \alpha$ and $\text{Parity}^{(\alpha)}(Q \cap K_1) \neq \text{Parity}^{(\alpha)}(Q \cap K_2)$. We will compute the probability that no query from sequence \mathcal{Q} distinguishes the considered sets K_1 and K_2 . Then, we apply the union bound over all pairs of K_1, K_2 and take the complementary event, which, as we show, holds with a positive probability. This implies existence of the sought query sequence. The details follow.

Definition of random sequence \mathcal{Q} . We define a sequence of probabilities \mathcal{P} of length $O\left(\frac{k^2}{\alpha\delta} \cdot \log(n/k)\right)$ as probability $\frac{\alpha}{16k}$ repeated $\left\lceil \frac{150k^2}{\alpha\delta} \cdot \log \frac{4n}{k} \right\rceil$ times. We define Q_i , an i -th element of the sequence \mathcal{Q} , as a set generated by including each element of N independently with the i -th probability from sequence \mathcal{P} .

Proving Separation Property. Consider two different sets $K_1, K_2 \subseteq N$ whose cardinalities satisfy the conditions of the lemma. Let $S = K_1 \triangle K_2$ be the symmetric difference of K_1 and K_2 . Note that $2k \geq |K_1 \cup K_2| \geq |S| \geq \delta$. We also know, by the assumed restriction on the size of K_1 , that $|K_1 \cup K_2| \geq k/2$. We want to show the following:

Separation Property: for any positive integer $i \leq |\mathcal{Q}|/2$ and for some constant $c > 0$, the probability that query $Q_i \in \mathcal{Q}$, distinguishes K_1 and K_2 is at least $c\alpha\delta/k$.

Before proving the Separation Property we need the following technical claim.

Claim. For any $Q_j \in \mathcal{Q}$, where $j \leq |\mathcal{Q}|$:

$$\mathbb{P}[Q_j \text{ distinguishes } K_1 \text{ from } K_2] \geq \mathbb{P}[|(K_1 \cup K_2) \cap Q_j| \leq \alpha \text{ and } |S \cap Q_j| \text{ is odd}].$$

Proof of the Claim. Consider a query Q_j , for some $j \leq |\mathcal{Q}|$, from the random sequence \mathcal{Q} , and assume that the event “ $|(K_1 \cup K_2) \cap Q_j| \leq \alpha$ and $|S \cap Q_j|$ is odd” holds. It follows from $|(K_1 \cup K_2) \cap Q_j| \leq \alpha$ that $|K_1 \cap Q_j| \leq \alpha$ and $|K_2 \cap Q_j| \leq \alpha$. Moreover, since the event also implies that $|S \cap Q_j|$ is odd, then $|K_1 \cap Q_j| \neq |K_2 \cap Q_j| \pmod{2}$. Hence, $\text{Parity}^{(\alpha)}(K_1 \cap Q_j) \neq \text{Parity}^{(\alpha)}(K_2 \cap Q_j)$. This completes the proof of the Claim. ■

We continue the proof of the Separation Property. In the case, where $\alpha \geq \log \frac{256k}{7\alpha\delta}$ we have, that:

$$\mathbb{P}[|(K_1 \cup K_2) \cap Q| \leq \alpha \text{ and } |S \cap Q| \text{ is odd}] \geq \mathbb{P}[|S \cap Q| \text{ is odd}] - \mathbb{P}[|(K_1 \cup K_2) \cap Q| > \alpha].$$

Random variable $H_2 = |(K_1 \cup K_2) \cap Q|$ is distributed according to the Binomial distribution with parameters $|K_1 \cup K_2|$ and p , and $\mathbb{E}[H_2] = p|K_1 \cup K_2| \leq 2pk = \alpha/8$. Then, by Chernoff bound (cf., [24]):

$$\mathbb{P}[H_2 \geq \alpha] \leq 2^{-\alpha}.$$

Random variable $|S \cap Q|$ is also distributed according to the Binomial distribution with parameters $|S|$ and p . By Fact 1 we have

$$\mathbb{P}[|S \cap Q| \text{ is odd}] = \frac{1}{2} - \frac{1}{2}(1-2p)^{|S|}.$$

Term $\frac{1}{2}(1-2p)^{|S|}$ is maximized, when $|S|$ is minimized, which gives us:

$$\mathbb{P}[|S \cap Q| \text{ is odd}] \geq \frac{1}{2} - \frac{1}{2}(1-2p)^\delta.$$

Using Fact 2, we get:

$$\frac{1}{2} - \frac{1}{2}(1-2p)^\delta \geq \frac{1}{2} - \frac{1}{2}\left(1 - 2p\delta + 4\delta(\delta-1)p^2\right) = \frac{\alpha\delta}{16k} - \frac{\delta(\delta-1)\alpha^2}{128k} = \frac{\alpha\delta}{16k} \left(1 - \frac{(\delta-1)\alpha}{8k}\right),$$

and knowing that $\delta < k/\alpha$ we get $\left(1 - \frac{(\delta-1)\alpha}{8k}\right) \geq 7/8$. Finally, combining the above and knowing that $\alpha \geq \log \frac{256k}{7\alpha\delta}$, we get:

$$\mathbb{P}[|S \cap Q| \text{ is odd}] - \mathbb{P}[|(K_1 \cup K_2) \cap Q| > \alpha] \geq \frac{7\alpha\delta}{128k} - 2^{-\alpha} \geq \frac{7\alpha\delta}{256k} \geq \frac{\alpha\delta}{50k}.$$

In the second case assume, that $\alpha \leq \log \frac{256k}{7\alpha\delta}$. In this case we have:

$$\begin{aligned} \mathbb{P}[Q_j \text{ distinguishes } K_1 \text{ from } K_2] &\geq \mathbb{P}[|(K_1 \cup K_2) \cap Q_j| \leq \alpha \text{ and } |S \cap Q_j| \text{ is odd}] \\ &\geq \mathbb{P}[|(K_1 \cap K_2) \cap Q_j| \leq \alpha - 1 \text{ and } |S \cap Q_j| = 1] \\ &\geq \mathbb{P}[|(K_1 \cap K_2) \cap Q_j| \leq \alpha - 1] \cdot \mathbb{P}[|S \cap Q_j| = 1], \end{aligned}$$

where the last equality is true, because sets S and $K_1 \cap K_2$ are disjoint.

Random variable $H_1 = |(K_1 \cap K_2) \cap Q|$ is distributed according to the Binomial distribution with parameters $|K_1 \cap K_2|$ and p , and $\mathbb{E}[H_1] = p|K_1 \cap K_2| \leq pk = \alpha/16$. Then, by Markov inequality $\mathbb{P}[H_2 \geq \alpha] \leq 1/16$. We want to lowerbound term

$$\mathbb{P}[|S \cap Q_j| = 1] = p|S|(1-p)^{|S|-1} = \frac{\alpha|S|}{16k} \cdot \left(1 - \frac{\alpha}{16k}\right)^{|S|-1}$$

If $|S| \leq 16k/\alpha$, then $(1 - \alpha/(16k))^{|S|-1} \geq e^{-1}$ and:

$$\mathbb{P}[|S \cap Q_j| = 1] \geq \frac{\alpha\delta}{16ek}.$$

Hence $\mathbb{P}[Q_j \text{ distinguishes } K_1 \text{ from } K_2] \geq \frac{15}{16} \cdot \frac{\alpha\delta}{16ek} \geq \frac{\alpha\delta}{50k}$.

If $|S| > 16k/\alpha$, then $p|S| \geq 1$ and (knowing that $|S| \leq 2k$), we get:

$$\left(1 - \frac{\alpha}{16k}\right)^{|S|-1} \geq \left(1 - \frac{\alpha}{16k}\right)^{\left(\frac{16k}{\alpha}-1\right)\frac{\alpha}{8}+\frac{\alpha}{8}} \geq e^{-\alpha/8} \cdot e^{-\alpha/8} \geq e^{-\alpha} \geq \frac{7\alpha\delta}{256k}.$$

Hence, also in this case, we get $\mathbb{P}[Q_j \text{ distinguishes } K_1 \text{ from } K_2] \geq \frac{15}{16} \cdot \frac{7\alpha\delta}{256k} \geq \frac{\alpha\delta}{50k}$.

This completes the proof of the Separation Property for $c = 1/50$.

Computing the probability of Q distinguishing K_1 from K_2 . By the proven Separation Property for $c = 1/50$ and by independence of selection of each query in the sequence Q of length $150k^2/(\alpha\delta) \cdot \log(4n/k)$, the probability that Q fails to distinguish K_1 from K_2 is at most:

$$\left(1 - \frac{\alpha\delta}{50k}\right)^{150k^2/(\alpha\delta) \cdot \log(4n/k)} = \left(1 - \frac{\alpha\delta}{50k}\right)^{50k/(\alpha\delta) \cdot 3k \log(4n/k)} \leq e^{-3k \log(4n/k)} = \left(\frac{4n}{k}\right)^{-3k}.$$

Applying the union bound and probabilistic argument. The number of possible pairs of sets K_1, K_2 for the case $k \leq n/2$ can be upper bounded as follows:

$$\left(\sum_{i=1}^k \binom{n}{i}\right)^2 \leq k^2 \binom{n}{k}^2 \leq k^2 \left(\frac{en}{k}\right)^{2k}.$$

If $n \geq k \geq n/2$ the number of possible pairs K_1, K_2 can be simply upper bounded by:

$$2^n \cdot 2^n \leq \left(\frac{4n}{k}\right)^{2k}.$$

In both cases the number of possible pairs of K_1, K_2 is upper bounded by

$$k^2 \cdot \left(\frac{4n}{k}\right)^{2k}.$$

Thus, using the Union Bound, the probability that some pair of sets is not distinguished by Q is at most:

$$\left(\frac{4n}{k}\right)^{-3k} \cdot k^2 \cdot \left(\frac{4n}{k}\right)^{2k} \leq 4^{-k} \cdot k^2 < 1.$$

Hence, there is a positive probability of the complementary event that there exists a sequence of length $O(\frac{k^2}{\alpha\delta} \cdot \log(n/k))$ that distinguishes any pair K_1 and K_2 (satisfying the conditions of the lemma) under the Parity^(α) feedback function, and by the probabilistic argument – such a sequence exists. \square

In the next lemma we show that it is possible to also distinguish sets of size at most α .

Lemma 2. *If $k \leq \alpha$, there exists a sequence of $O(k \cdot \log(n/k))$ sets \mathcal{Q} such that for any two sets $K_1, K_2 \subseteq N$ satisfying $k \geq |K_1|$, $k \geq |K_2|$ and $K_1 \neq K_2$ there exists $Q \in \mathcal{Q}$ that satisfies $\text{Parity}^{(\alpha)}(Q \cap K_1) \neq \text{Parity}^{(\alpha)}(Q \cap K_2)$.*

Proof. The proof follows in a similar vein as proof of Lemma 1. We construct a sequence of $\lceil 3k \log(4n/k) \rceil$ queries \mathcal{Q} as follows: i -th element of the sequence is generated by including each element of N independently with probability $\frac{1}{2}$. Since $|K_1| \leq \alpha$ and $|K_2| \leq \alpha$, then $\mathbb{P}[Q_j \text{ distinguishes } K_1 \text{ from } K_2] \geq \mathbb{P}[|(K_1 \Delta K_2) \cap Q_j| \text{ is odd}]$. By Fact 1 we have $\mathbb{P}[|(K_1 \Delta K_2) \cap Q_j| \text{ is odd}] = \frac{1}{2}$.

Similarly as in Lemma 1, the number of possible pairs of K_1, K_2 can be upper bounded by $k^2 \cdot \left(\frac{4n}{k}\right)^{2k}$. Thus, using the Union Bound, the probability that some pair of sets is not distinguished by \mathcal{Q} is at most:

$$\left(\frac{4n}{k}\right)^{-3k} \cdot k^2 \cdot \left(\frac{4n}{k}\right)^{2k} \leq 4^{-k} \cdot k^2 < 1.$$

Hence, there is a positive probability of the complementary event that there exists a sequence of length $O(k \cdot \log(n/k))$ that distinguishes any pair K_1 and K_2 (satisfying the conditions of the lemma) under the $\text{Parity}^{(\alpha)}$ feedback function, and by the probabilistic argument – such a sequence exists. \square

In the next lemma we show that the sequences constructed in Lemma 1 and Lemma 2 could be concatenated in order to obtain a sequence that distinguishes sets without the lower restriction on their sizes.

Lemma 3. *There exists a sequence \mathcal{Q} of length $O\left(\left(k + \frac{k^2}{\alpha\delta}\right) \cdot \log(n/k)\right)$ for any $1 \leq \delta \leq \max\{k/\alpha, 1\}$, such that for any sets $K_1, K_2 \subseteq N$ satisfying $|K_1|, |K_2| \leq k$ and $|K_1 \Delta K_2| \geq \delta$ there exists $Q \in \mathcal{Q}$ that satisfies $|Q \cap K_1| \leq \alpha$, $|Q \cap K_2| \leq \alpha$ and $\text{Parity}^{(\alpha)}(Q \cap K_1) \neq \text{Parity}^{(\alpha)}(Q \cap K_2)$.*

Proof. Assume that k is a power of 2 (if it is not, we can increase k to the closest power of 2 without increasing the asymptotic complexity of our sequence). From Lemma 1, we have that there exists a sequence of length $ck^2 \log(n/k)/(\alpha\delta)$, for some constant c , distinguishing any two sets K_1, K_2 satisfying $|K_1| \geq |K_2|$ and $k \geq |K_1| \geq k/2$ and $|K_1 \Delta K_2| \geq \delta$. We want to show that such a sequence exists for any pair of sets of size at most k . We call the sequences from Lemma 1 applied to parameter $k/2^i$ instead of k as \mathcal{Q}_i . By concatenating such sequences for $i = 0, 1, \dots, \lfloor \log_2(k/\alpha) \rfloor$ and with sequence $\hat{\mathcal{Q}}$ from Lemma 2, we obtain sequence \mathcal{Q} of length: $\lceil 3k \log(4n/k) \rceil + \sum_{i=0}^{\lfloor \log_2(k/\alpha) \rfloor} c \frac{k^2 \log(2^i n/k)}{4^i \alpha \delta} \in O\left(\left(k + \frac{k^2}{\alpha\delta}\right) \cdot \log(n/k)\right)$. Take any two sets K_1 and K_2 such that $|K_1|, |K_2| \leq k$ and $|K_1 \Delta K_2| \geq \delta$. Without loss of generality assume that $|K_1| \geq |K_2|$. If $|K_1| \leq \alpha$, then the pair is distinguished by $\hat{\mathcal{Q}}$ due to Lemma 2. Otherwise, we find such i , that $k2^{-i} \geq |K_1| \geq k2^{-i-1}$. By Lemma 1, sequence \mathcal{Q}_i distinguishes K_1 from K_2 . Since \mathcal{Q} contains \mathcal{Q}_i as subsequence, then \mathcal{Q} also distinguishes K_1 from K_2 . \square

As mentioned earlier, Theorem 1 follows directly from Lemma 3 applied for $\delta = 1$. It is worth mentioning that Lemma 3, based on technical development in Lemma 1, could be seen as more universal tool that could be applied to the analysis of other feedbacks related to or using parity as its part, cf., Section 4.3.

Randomized counterpart construction. First note that the explicit randomized construction used in the proof of Lemma 1 leads directly to the following corollary:

Corollary 1. *There exists an explicit randomized algorithm that generates a sequence \mathcal{Q} of $O\left(\frac{k^2}{\alpha\delta} \cdot \log(n/k)\right)$ sets such that with probability at least $1 - k^2/4^{-k}$ the following holds: for any sets $K_1, K_2 \subseteq N$ such that $k \geq |K_1| \geq k/2$ and $|K_1| \geq |K_2|$ and $|K_1 \Delta K_2| \geq \delta$, there exists $Q \in \mathcal{Q}$ that satisfies $|Q \cap K_1| \leq \alpha$, $|Q \cap K_2| \leq \alpha$ and $\text{Parity}^{(\alpha)}(Q \cap K_1) \neq \text{Parity}^{(\alpha)}(Q \cap K_2)$.*

A randomized algorithm generating a concatenation of sequences \mathcal{Q}_i , taken from Corollary 1 for parameters $k/2^i$, in the same manner as in Lemma 3 for $\delta = 1$, results in an explicit randomized algorithm for (n, k) -Group-Testing under α -Malicious Adversary. It is easy to see that if each of $\lfloor \log_2 k \rfloor$ concatenated sequences \mathcal{Q}_i does not fail (i.e., it does distinguish all pairs of sets of certain sizes), then the resulting sequence distinguishes all pairs of sets of sizes at most k .

Corollary 2. *Under $\text{Parity}^{(\alpha)}$ feedback and under adaptive α -Malicious Adversary, there exists an explicit randomized solution to (n, k) -Group-Testing with query complexity $O\left(\left(k + \frac{k^2}{\alpha}\right) \cdot \log \frac{n}{k} \log 1/c\right)$ working with probability at least $1 - c$, for any $c \in (0, 1)$.*

Proof. The probability that a single of the sequences concatenated in Lemma 3 fails to distinguish all sets of certain sizes is at most:

$$k^2 \cdot 4^{-k} + \sum_{i=0}^{\lfloor \log_2(k/\alpha) \rfloor} (k/2^i)^2 4^{-(k/2^i)} \leq \frac{1}{4} + \sum_{j=1}^{\infty} j^2 4^{-j} = \frac{107}{108},$$

because $\sum_{j=1}^{\infty} j^2 4^{-j} = 20/27$. If we concatenate $\lceil \log_{108/107} 1/c \rceil$ independently generated such sequences, we get a sequence that distinguishes all sets with probability at least $1 - c$. \square

4.2. Maximum expressiveness – full feedback

In this section we consider $\text{Full}^{(\alpha)}$ feedback. Using it, we show that larger expressiveness of feedback allows for smaller query complexity. The following lemma is independent of any feedback function and shows that there exists a query sequence that α -isolates each element of K , in the following sense: for any set K of size at most k and each element in K , there exists a query such that this element and at most $\alpha - 1$ other elements from K belong to this query.

Lemma 4. *If $\alpha \geq 9 \log k$ and $k \geq \alpha$, then there exists a sequence \mathcal{Q} of $t = O((k^2/\alpha^2) \cdot \log n)$ subsets of N with the property that for any set $K \subseteq N$ such that $|K| \leq k$ and any element $x \in K$, there exists $Q \in \mathcal{Q}$ with the property that $x \in Q$ and $|K \cap Q| \leq \alpha$.*

Proof. We prove existence of such family \mathcal{Q} by a probabilistic argument. Let $h = \lceil 16 \log(3n) \rceil$. The family \mathcal{Q} consists of $t = 6h \cdot x \cdot k^2/\alpha^2$ subsets denoted as Q_1, \dots, Q_t . For each $i = 1, \dots, t$ the set Q_i is generated in the following manner: each element $x \in N$ belongs to Q_i with probability $\frac{\alpha}{6k}$. All the random choices are independent over all elements and subsets.

Claim 1. *With probability at least $2/3$ each element of N belongs to at least $\frac{k}{2\alpha}$ queries in the sequence \mathcal{Q} .*

Proof of Claim 1. For a fixed $x \in N$, let $L_x = \{i \in [t] : x \in Q_i\}$. Clearly, L_x is a sum of Bernoulli trials and $\mathbb{E}[L_x] = \frac{h\alpha k}{\alpha}$. Due to the independence of random inclusion of consecutive elements we can use a standard Chernoff bound [24] to get $\mathbb{P}\left[L_x < h \cdot \frac{k}{2\alpha}\right] \leq e^{-\frac{hk}{16\alpha}} < \frac{1}{3n}$, where the last inequality follows from the fact that, $\frac{hk}{16\alpha} \geq \log(3n)$. Using the union bound over all n possible elements $v \in N$ we get Claim 1. \blacksquare

Consider a sub-sequence of queries from \mathcal{Q} , and from all these queries we remove all elements that do not belong to K , namely: $\mathcal{Q}_{K,T} = \{Q_i \cap K : Q_i \in \mathcal{Q} \text{ \& \& } i \in T\}$.

Claim 2. *With probability at least $2/3$, for any choice of K with k elements and any T of $\frac{hk}{2\alpha}$ indices, the resulting sequence $\mathcal{Q}_{K,T}$ contains a set with at most α elements.*

Proof of Claim 2. Let us fix any subset $K \subseteq N$ and a set T with proper cardinalities. In any fixed set $Q' \in \mathcal{Q}_{K,T}$ we define its number of elements as $X_{Q'}$. Clearly, $X_{Q'}$ is a sum of Bernoulli random variables.

We have $\mathbb{E}[X_{Q'}] = \frac{\alpha}{6}$ and by the Chernoff bound we get $\mathbb{P}[X_{Q'} > \alpha] < \mathbb{P}[X > 6\mathbb{E}[X]] < e^{-\alpha}$. Due to independence of choices elements in different queries, the probability that the number of elements is greater than α in all $\frac{h\alpha k}{2\alpha}$ sets in $\mathcal{Q}_{K,T}$ is at most $e^{-\alpha \cdot \frac{hk}{2\alpha}} = e^{-\frac{hk}{2}}$. Recall that the above reasoning was performed for a fixed choice of sets K and T . To apply a union bound argument one needs to multiply the above value by the number of all possible choices of sets K and T . The logarithm of the number of possible combinations of K and T equals to:

$$\log \left(\binom{n}{k} \cdot \left(\frac{6hk^2}{\alpha^2} \right) \right) \leq k \log \left(\frac{en}{k} \right) + \frac{h\alpha k}{2\alpha} \log \left(\frac{6ek}{\alpha} \right),$$

and since $\alpha > 9 \log k$ we obtain the logarithm of the union-bounded probability multiplied by the number of choices we get:

$$\begin{aligned} \log \left(e^{-\frac{hk}{2}} \cdot \binom{n}{k} \cdot \left(\frac{6h \cdot \frac{k^2}{\alpha^2}}{h \cdot \frac{k}{2\alpha}} \right) \right) &\leq -\frac{hk}{2} + k \log \left(\frac{en}{k} \right) + \frac{hk}{2\alpha} \log \left(\frac{6ek}{\alpha} \right) \\ &\leq -\frac{hk}{2} + k \log \left(\frac{en}{k} \right) + \frac{hk \log k}{18 \log k} \leq -\frac{4hk}{9} + k \log \left(\frac{en}{k} \right) \\ &\leq -14k \log \frac{3n}{k} + k \log \frac{en}{k} \leq -13k \log \frac{3n}{k} < \log \frac{1}{3}. \end{aligned}$$

Hence, $e^{-k \cdot 32 \log(3n/k)} \cdot \binom{n}{k} \cdot \left(\frac{6hk^2}{\alpha^2} \right) < \frac{1}{3}$. This concludes the proof of Claim 2. \blacksquare

Observe that with probability at least $1/3$, a randomly chosen family \mathcal{Q} simultaneously meets conditions described in Claim 1 and Claim 2, by the union bound. Consequently, with probability at least $1/3$, in the randomly generated family \mathcal{Q} for any set K of size k and every sub-sequence T of $\frac{hk}{\alpha}$ queries from \mathcal{Q} there is at least one query Q_i such that $|Q_i \cap K| \leq \alpha$, for some $i \in T$. Hence, such a family \mathcal{Q} exists, by straightforward probabilistic argument. Finally, observe that since \mathcal{Q} works for any set K of exactly k elements, then it also does for any K such that $|K| \leq k$. \square

Interestingly, sequence \mathcal{Q} from Lemma 4 with parameters n, k does **not** distinguish all pairs of sets K_1, K_2 of size at most k . We only know, that each element $x \in K_1$ belongs to some query $Q_\tau \in \mathcal{Q}$, with $|K_1 \cap Q_\tau| \leq \alpha$. But we may have $|K_2 \cap Q_\tau| > \alpha$ and the α -Malicious Adversary may force the feedbacks to be equal on this position for sets K_1 and K_2 . To solve this problem, in the proof of Theorem 2, we take the sequence from Lemma 4 with parameters $n, 2k$, and use it for set $K = K_1 \cup K_2$.

Proof of Theorem 2. The component $\frac{n}{\alpha}$ follows from the fact, that a simple selector, where each element belongs to one query and each query contains α elements (except the last query that contains at most α) has query complexity $O(\frac{n}{\alpha})$ and solves (n, k) -Group-Testing under the $\text{Full}^{(\alpha)}$ feedback and works under α -Malicious Adversary. The first part of theorem is a consequence of Lemma 4. Specifically, we take the family \mathcal{Q} from Lemma 4 with parameters $n, 2k$. We observe that for any two sets K_1, K_2 , with $|K_1|, |K_2| \leq \alpha$ and $K_1 \neq K_2$, we have $|K_1 \cup K_2| \leq 2k$ and $K_1 \triangle K_2 \neq \emptyset$. Take any $x \in K_1 \triangle K_2$ and observe that due to Lemma 4 there is a query $Q \in \mathcal{Q}$ such that $x \in Q$ and $|Q \cap (K_1 \cup K_2)| \leq \alpha$. Hence, $|Q \cap K_1| \leq \alpha$, $|Q \cap K_2| \leq \alpha$ and $\text{Full}^{(\alpha)}(Q \cap K_1) \neq \text{Full}^{(\alpha)}(Q \cap K_2)$. Consequently, \mathcal{Q} solves (n, k) -Group-Testing under α -Malicious Adversary, by Proposition 2.

The second part of the theorem follows from the fact that we can use the result from Theorem 1 and obtain a sequence of length $O(\frac{k^2}{\alpha} \log(n/k))$ (this results does not require the assumption on α and also works under α -Malicious Adversary). Note that we do not need the $O(k \log(n/k))$ component here because under $\text{Full}^{(\alpha)}$ in the case where $k \leq \alpha$, the problem is solvable using a single query. \square

Randomized counterpart construction. In the proof of Lemma 4 we construct a sequence at random and show that it satisfies a certain condition with probability at least $1/3$. Clearly, from this we can obtain an explicit randomized construction that succeeds with probability $1/3$, and by iterating it a certain number of times we get the following:

Corollary 3. Under $\text{Full}^{(\alpha)}$ feedback and under adaptive α -Malicious Adversary, there exists an explicit randomized solution to (n, k) -Group-Testing with query complexity

$$\begin{aligned} O\left(\frac{k^2}{\alpha\beta} \left(\frac{\beta}{\alpha} + \log n\right) \cdot \log n \cdot \log 1/c\right) & \quad \text{if } \alpha > 18 \log k, \\ O\left(\frac{k^2}{\alpha} \cdot \log \frac{n}{k} \cdot \log 1/c\right) & \quad \text{otherwise,} \end{aligned}$$

working with probability at least $1 - c$, for any $c \in (0, 1)$.

Proof. We first observe that if $k \leq \alpha$ then, because of the $\text{Full}^{(\alpha)}$ feedback, a single query containing all elements from set N solves (n, k) -Group-Testing. Hence, we focus on case $k \geq \alpha$. If $\alpha \leq 18 \log k$, then we can use the result from Corollary 2 and obtain a desired sequence of length $O((k + \frac{k^2}{\alpha}) \log(n/k) \log 1/c)$ with probability of success at least $1 - c$, which becomes $O(\frac{k^2}{\alpha} \log(n/k) \log 1/c)$, because $k \geq \alpha$. Finally if $18 \log k < \alpha \leq k$, we can use the construction from the proof of Lemma 4 that fails with probability at most $1/3$. By repeating it $\lceil \log_3 1/c \rceil$ times, independently, and concatenating the resulting sequences we obtain a desired probability of success. \square

4.3. General feedback

In our construction of $\text{General}^{(\alpha, \beta)}(X)$ (introduced in Definition 3) we use the following code, where notation $\oplus S$ denotes bit-wise XOR of all the elements of set S . Such a code was defined in [10] and its explicit construction can be found in [43].

Definition 5. An $[n, \beta, \gamma]$ -BCC-code is a set $C \subseteq \{0, 1\}^\beta$ of size $|C| = n$ such that for any two subsets $S_1, S_2 \subseteq C$ (with $S_1 \neq S_2$) of sizes $|S_1|, |S_2| \leq \gamma$ it holds that $\oplus S_1 \neq \oplus S_2$.

Lemma 5. [10, Lemma 2] There exist $[n, \beta, \gamma]$ -BCC codes with $\beta = O(\gamma \log n)$.

Proof of Theorem 3. First we prove the part of the theorem that works under the assumption $\alpha > 18 \log k$. We denote $\beta' = \min \left\{ \left\lfloor \frac{\beta-1}{c \log n} \right\rfloor, \alpha \right\}$. We note that if $\beta < \log n$, then we get $\beta' = 0$ but the result follows simply by choosing \mathcal{Q} as the sequence from Theorem 1. Note that we must have $\beta' \leq \alpha$ because input set X cannot contain more than α elements.

Assume that $\beta > \log n$ and let us take the family from Lemma 3 with parameter $\delta = \beta'$ and concatenate it with the family from Lemma 4 with parameters $2k$ and n . Observe, that this resulting family \mathcal{Q} (composed of two parts \mathcal{Q}_1 and \mathcal{Q}_2) has length $O\left(\frac{k^2}{\alpha\beta'} \cdot \log n\right) = O\left(\max \left\{ \frac{k^2}{\alpha^2} \log n, \frac{k^2}{\alpha\beta} \log^2 n \right\}\right)$. We will show that this family distinguishes under $\text{General}^{(\alpha, \beta)}$ feedback model, any two sets K_1, K_2 satisfying $|K_1|, |K_2| \leq k$. We will consider two cases.

In the case, where $|K_1 \Delta K_2| < \beta'$, we pick an arbitrary element $s \in K_1 \Delta K_2$. Without loss of generality assume that $s \in K_1$. By Lemma 4 in some $Q \in \mathcal{Q}_2$ we have $|Q \cap (K_1 \cup K_2)| \leq \alpha$ and $s \in Q$.

We want to show that:

$$\bigoplus_{s \in Q \cap K_1} \text{BCC}(s) \neq \bigoplus_{s \in Q \cap K_2} \text{BCC}(s).$$

We denote $K'_1 = (K_1 \setminus K_2) \cap Q$ and $K'_2 = (K_2 \setminus K_1) \cap Q$ and $T = K_1 \cap K_2 \cap Q$. We know that $K'_1 \neq \emptyset$, because $s \in K'_1$ and also $K'_1 \neq K'_2$ because $s \notin K'_2$. Since $|K_1 \Delta K_2| < \beta'$, and $K'_1, K'_2 \subset K_1 \Delta K_2$ then also $|K'_1|, |K'_2| < \beta'$. By the definition of BCC codes [10, Lemma 2] we have that: $\bigoplus_{s \in K'_1} \text{BCC}(s) \neq \bigoplus_{s \in K'_2} \text{BCC}(s)$. Using the properties of operation XOR:

$$\bigoplus_{s \in Q \cap K_1} \text{BCC}(s) = \bigoplus_{s \in K'_1} \text{BCC}(s) \oplus \bigoplus_{s \in T} \text{BCC}(s) \neq \bigoplus_{s \in K'_2} \text{BCC}(s) \oplus \bigoplus_{s \in T} \text{BCC}(s) = \bigoplus_{s \in Q \cap K_2} \text{BCC}(s).$$

Hence, if $|K_1 \Delta K_2| \leq \beta'$ then there exists Q such that $|Q \cap (K_1 \cup K_2)| \leq \alpha$. Consequently, $|Q \cap K_1| \leq \alpha$ and $|Q \cap K_2| \leq \alpha$. We have obtained that $\text{General}^{(\alpha, \beta)}(Q \cap K_1) \neq \text{General}^{(\alpha, \beta)}(Q \cap K_2)$, thus Q distinguishes K_1 and K_2 .

If $|K_1 \Delta K_2| \geq \beta'$, then by Lemma 3 the first part of our sequence \mathcal{Q}_1 distinguishes K_1 and K_2 under the binary feedback. Since $\text{General}^{(\alpha, \beta)}$ includes the binary feedback, our sequence \mathcal{Q} distinguishes K_1 from K_2 .

After considering both cases, we have that sequence \mathcal{Q} distinguishes any two sets K_1, K_2 of size at most α and thus we can use Proposition 2 and obtain that \mathcal{Q} solves the (n, k) -Group-Testing problem under α -Malicious Adversary.

The second part of the theorem follows from the fact that we can use the result from Theorem 1 and obtain a sequence of length $O(\frac{k^2}{\alpha} \log(n/k))$ (this results does not require the assumption on α). \square

Randomized counterpart construction. Unlike in previous sections, for $\text{General}^{(\alpha, \beta)}(X)$ feedback it is not simple to provide an explicit algorithm, even randomized. This is because an explicit (even randomized) construction of BCC-codes is not known. Therefore, we suggest this problem as one of interesting open directions.

5. Lower bound

Proof of Theorem 4. An (n, k, k) -selector is a sequence of queries Q_1, Q_2, \dots, Q_t such that for any $|K| \leq k$ and any element $x \in K$, for some query Q we have $Q \cap K = \{x\}$. An (n, k, k) -selector is known to have query complexity $\Omega(\min\{n, (k^2/\log k) \cdot \log n\})$ [13] and is known to exist with query complexity $O(k^2 \log n)$ [27]. Assume that n is sufficiently large and let c_1 be such a constant that (n, k, k) -selector of query complexity $t_1 \leq c_1(k^2/\log k) \cdot \log n$ does not exist; c_1 is well-defined by [13]. Let c_2 be a constant such that $(n, \alpha + 1, \alpha + 1)$ -selector of size $t_2 \leq c_2 \alpha^2 \log n$ exists; c_2 is well-defined by [27]. Let $\mathcal{R} = \langle R_1, R_2, \dots, R_{t_2} \rangle$ be such a selector.

The proof of the theorem is by contradiction. Assume that there exists a sequence $\mathcal{Q} = \langle Q_1, Q_2, \dots, Q_t \rangle$ solving (n, k) -Group-Testing with some (α, β) -feedback function, such that the length of the sequence is $t \leq \frac{c_1}{c_2} \cdot \frac{k^2}{\alpha^2} \log^{-1} k$.

First we show the following fact: for any set $K \subset N$ of size $|K| \leq k$ and any element $x \in K$ there exists a set Q in sequence \mathcal{Q} such that $|K \cap Q| \leq \alpha + 1$. Assume the contrary and fix K and x that violate the fact. Observe that sets K and $K \setminus \{x\}$ may produce the same feedback for any (α, β) -feedback function (regardless of the value of β). This is because for any Q_i such that $x \in Q_i$ we have $|Q_i \cap K| \geq \alpha + 2$ and $|Q_i \cap (K \setminus \{x\})| \geq \alpha + 1$. Hence, in the case of $Q_i \cap K$ the α -Honest Adversary may provide to the feedback function the same α elements as in $Q_i \cap (K \setminus \{x\})$. Since the feedback function is deterministic, the results will be the same, which is a contradiction with the fact that \mathcal{Q} solves the (n, k) -Group-Testing problem.

Next we transform \mathcal{Q} into an (n, k, k) -selector: we take the $(n, \alpha + 1, \alpha + 1)$ -selector $\mathcal{R} = \langle R_1, R_2, \dots, R_{t_2} \rangle$ and construct a sequence $\mathcal{S} = \langle Q \cap R, \text{ for each } R = R_1, R_2, \dots, R_{t_2}, \text{ for each } Q = Q_1, Q_2, \dots, Q_t \rangle$. The obtained family \mathcal{C} has $t \cdot t_2 \leq t_1$ queries. We prove that it is also an (n, k, k) -selector. For any set K with $|K| \leq k$ and any $s \in S$ there exists, by the property of the sequence \mathcal{Q} proved above, a set Q in sequence \mathcal{Q} such that $|Q \cap K| \leq \alpha + 1$. Now, since \mathcal{R} is an $(n, \alpha + 1, \alpha + 1)$ -selector, there exists a set R in \mathcal{R} such that $R \cap (Q \cap K) = \{s\}$. By the construction of \mathcal{S} , set $Q \cap R$ belongs to sequence \mathcal{S} , hence element s is selected by family \mathcal{S} . Hence \mathcal{S} is an (n, k, k) -selector. We know however that (n, k, k) -selector of length at most t_1 does not exist, and thus obtain a contraction showing that such a family \mathcal{Q} cannot exist. \square

Randomized counterpart result. In Theorem 4 we show that any sequence that solves (n, k) -Group-Testing must have length of at least $\Omega\left(\frac{k^2}{\alpha^2} \log^{-1} k\right)$. Thus, a randomized algorithm generating sequences that solve (n, k) -Group-Testing with at least a constant probability must have expected query complexity of $\Omega\left(\frac{k^2}{\alpha^2} \log^{-1} k\right)$, since each correct sequence must have such length (by Theorem 4).

Corollary 4. If $n > k^2 \log n / \log k$, then any randomized solution to (n, k) -Group-Testing under any (α, β) -feedback has expected query complexity $\Omega\left(\frac{k^2}{\alpha^2} \log^{-1} k\right)$ for some adaptive α -Honest Adversary.

6. Some (α, β) -feedbacks are better than others

One could be tempted to develop a similar universal reduction, as in the proof of the lower bound in Section 5, also for upper bounds – between a setting with any (α, β) -feedback and some strong selectors. However, in this section we show that such a reduction does not exist: we define two seemingly very similar feedback functions with the same values of α, β and show that the resulting query complexities for these two feedbacks are asymptotically very different.

Consider the following two feedback functions, both being (α, β) -feedbacks for any $\alpha \leq k$ and $\beta = 2\lceil \log_2 n \rceil$. In the following we associate each element with its identifier. We assume that each identifier has exactly $\lceil \log_2 n \rceil$ bits and is different from the string of all zeros.

$$F_1(S) = \begin{cases} (\min S) \parallel (\min(S \setminus \{\min S\})), & \text{if } 2 \leq |S| \leq \alpha \\ (\min S) \parallel 00 \dots 0, & \text{if } |S| = 1. \end{cases}$$

$$F_2(S) = \begin{cases} (\min S) \parallel \min(S \setminus \{\min S\}), & \text{if } 2 \leq |S| \leq \alpha \text{ and } |S| \text{ is odd} \\ (\min(S \setminus \{\min S\})) \parallel \min S, & \text{if } 2 \leq |S| \leq \alpha \text{ and } |S| \text{ is even} \\ (\min S) \parallel 00 \dots 0, & \text{if } |S| = 1. \end{cases}$$

We show that the query complexity of (n, k) -Group-Testing with feedback F_2 is substantially lower than with feedback F_1 .

Corollary 5. For any $\alpha \leq k$, query complexity of (n, k) -Group-Testing under feedback F_2 under α -Malicious Adversary is $O\left(\frac{k^2}{\alpha} \log(n/k)\right)$.

Proof. We can see that under feedback F_2 we can deduce the parity bit from the feedback from every request with intersection at most α , by checking the order of the two outputted elements (note that if there is only one or no outputted elements, the parity is obvious). Hence, the corollary is a direct consequence of Theorem 1. \square

Remark. An unexpected inspiration for the feedback F_2 is a type of move, called *count signal*, used in contract bridge. Contract bridge is a card game, where players play in pairs (but without seeing non-revealed cards of other players) and sometimes it is crucial to exchange some information between the partners about their cards. The only way to disclose is by revealing (playing) the cards, but the *order* in which the cards are played can have some meaning. A count signal is exactly the F_2 feedback, where the parity of one player's cards (in some particular suit) is disclosed by the order in which he/she plays the cards. For example a player holding $\diamond Q 9 6 3$ (meaning Queen, 9, 6, 3 in diamonds) plays 6 and then 3 to show even number of cards in diamonds.

On the other hand, returning the same two minimal values as in F_2 but always in order, results in a dramatic increase in the query complexity, even under Honest Adversary.

Theorem 5. For any k, α , query complexity of (n, k) -Group-Testing under feedback F_1 is $\Omega(\min\{n, k^2\})$ under α -Honest Adversary.

Proof. Assume, that we have a sequence of queries solving (n, k) -Group-Testing. Let us denote the queries by Q_1, Q_2, \dots, Q_t , where t is the number of queries. Recall that N denotes the set of all the elements.

If $k \geq n/2$, then assuming that we had $t < k/2$, take an arbitrary set of k elements $K \subset N$. And observe that feedback to each query reveals at most two identifiers. The total number of identifiers revealed is $t \cdot 2 < k$. Hence there is an element $x \in K$ that is never returned by the feedback. It is easy to see that by the properties of the feedback function F_1 , the feedbacks for set $K \setminus \{x\}$ would be identical as for set K for each query. Hence if $k \geq n/2$ we must have $t \geq k/2 \geq n/4$.

Let us now consider the more interesting range of $k < n/2$. We define sets of indices $T_{>1} = \{\tau : |Q_\tau| > 1\}$, $T_{=1} = \{\tau : |Q_\tau| = 1\}$. Denote the following set of elements:

$$M = \bigcup_{\tau \in T_{=1}} Q_\tau \cup \bigcup_{\tau \in T_{>1}} ((\min Q_\tau) \cup \{\min(Q_\tau \setminus \min Q_\tau)\}).$$

We know that $|M| \leq 2t$, because we take at most 2 elements from each query. Denote set $R = N \setminus M$. Set R are the elements from N that are not smallest (or second smallest) in any of the queries.

If we have $|R| < k$, then $n - 2t < k$ and since $k \leq n/2$ we have $t \geq n/4$.

Assume that $|R| \geq k$, consider R ordered in the decreasing order of identifiers. Denote this ordering as r_1, r_2, \dots and let $R_{i,j} = \{r_i, r_2, \dots, r_j\}$. Denote the indices of queries that include element r_i as $T_{>1}^{(r_i)} = \{\tau \in T_{>1} | r_i \in Q_\tau\}$.

For any $j \in N$ and $i = 1, 2, \dots, j$, define two sets of query indices:

$$A_j(i) = \{\tau \in T_{>1}^{r_i} : |Q_\tau \cap R_{i+1,j}| = 0\},$$

$$B_j(i) = \{\tau \in T_{>1}^{r_i} : |Q_\tau \cap R_{i+1,j}| = 1\}.$$

We will prove the following:

Claim 1: For any j, i we have $2 \cdot |A_j(i)| + |B_j(i)| > k - j$.

Assume on the contrary that this does not hold for some particular j, i and observe that then we can find for every query Q_τ for $\tau \in A_j(i)$ two elements that belong to Q_τ and are smaller than r_i . Take such two elements for each $\tau \in A_j(i)$. We have $2|A_j(i)|$ elements, call this set A . For every $\tau \in B_j(i)$ find one element that belongs to Q_τ and is smaller than r_i . We take $|B_j(i)|$ such elements (one for each of $B_j(i)$) and call this set B . Consider two sets

$$S = R_{1,j} \cup A \cup B, \\ S' = R_{1,j} \cup A \cup B \setminus \{r_i\}.$$

Observe that $|S| \leq |S'| \leq j + k - j = k$. We will compare the feedbacks for S and S' and show that the feedbacks are identical for each query. Note that for every $\tau \in T_{>1}^{(r_i)}$, $S' \cap Q_\tau$ has at least two elements that are smaller than r_i . Hence if $|S \cap Q_\tau| \leq \alpha$ then surely $F_1(S' \cap Q_\tau) = F_1(S \cap Q_\tau)$. If $|S \cap Q_\tau| > \alpha$, there is a simple strategy of an adversary to ensure equal feedbacks. The adversary selects an arbitrary set X with $|X| = \alpha$ satisfying, $X \subset S' \cap Q_\tau$ and $X \subset S \cap Q_\tau$ and passes X to the feedback function. Hence the feedback in step τ is identical for both S and S' . Note that, since $r_i \notin M$, then r_i does not belong to any other query than the queries with indices in $T_{>1}^{(r_i)}$, hence we cannot distinguish S from S' . This means that the query sequence does not solve the set learning problem. We obtained a contradiction, which proves the claim.

In the next claim we prove that sets $A_j(i)$ and $B_j(i)$ are disjoint.

Claim 2: For any j , we have $A_j(i) \cap A_j(i') = \emptyset$ and $B_j(i) \cap B_j(i') = \emptyset$, for $i, i' \leq j$ and $i \neq i'$.

Assume on the contrary that for some j and $i, i' \leq j$ we have $A_j(i) \cap A_j(i') \neq \emptyset$ and take arbitrary $\tau^* \in A_j(i) \cap A_j(i')$. Assume without loss of generality that $i < i'$. By the definition of sets A we have $r_i \in Q_{\tau^*}$ and $r_{i'} \in Q_{\tau^*}$. Since $i < i' \leq j$ we also have $r_{i'} \in R_{i+1,j}$, hence $|Q_{\tau^*} \cap R_{i+1,j}| \geq 1$ and $\tau^* \notin A_j(i)$ a contradiction. Now if $B_j(i) \cap B_j(i') \neq \emptyset$ then similarly take $\tau^* \in B_j(i) \cap B_j(i')$ and assume $i < i'$. We have $r_i, r_{i'} \in Q_{\tau^*}$. We know that $|Q_{\tau^*} \cap R_{i'+1,j}| = 1$ thus $|Q_{\tau^*} \cap R_{i',j}| = 2$. Which implies that $|Q_{\tau^*} \cap R_{i+1,j}| \geq 2$ and $\tau^* \notin B_j(i)$. We obtained a contradiction proving the claim.

We fix $j^* = \lfloor k/2 \rfloor$. From Claim 1 we have $2 \cdot |A_{j^*}(i)| + |B_{j^*}(i)| > k/2$ for each $i = 1, 2, \dots, j^*$. Sets $A_j(i)$ contain indices of queries hence using Claim 2 we get:

$$t \geq \left| \bigcup_{i=1}^{j^*} A_{j^*}(i) \right| = \sum_{i=1}^{j^*} |A_{j^*}(i)|, \\ t \geq \left| \bigcup_{i=1}^{j^*} B_{j^*}(i) \right| = \sum_{i=1}^{j^*} |B_{j^*}(i)|.$$

Adding up the above inequalities gives us:

$$3t \geq 2 \cdot \sum_{i=1}^{j^*} |A_{j^*}(i)| + \sum_{i=1}^{j^*} |B_{j^*}(i)| = \sum_{i=1}^{j^*} (2|A_{j^*}(i)| + |B_{j^*}(i)|) \geq j^* \cdot k/2 \geq k^2/4 - k/2.$$

Thus, finally we get $t \geq k^2/12 - k/6$. \square

Randomized counterpart result. In Theorem 5 we show that any sequence that solves (n, k) -Group-Testing under feedback F_1 under α -Honest Adversary must have length of at least $\Omega(\min\{n, k^2\})$. Thus, a randomized algorithm generating sequences that solve (n, k) -Group-Testing under this feedback with at least a constant probability must have expected query complexity of $\Omega(\min\{n, k^2\})$, since each correct sequence must have such length (by Theorem 5).

Corollary 6. For any k, α , query complexity of any randomized solution to (n, k) -Group-Testing under feedback F_1 is $\Omega(\min\{n, k^2\})$ under adaptive α -Honest Adversary.

7. Discussion of results and open directions

We conclude the paper with four promising future directions.

Sparsity. In addition to the query complexity, there are two additional metrics of Group Testing solutions that are studied in literature. These parameters are: the maximum number of queries to which an element belongs to (typically denoted by w) and the maximum size of a query (typically denoted by ρ). The interplay between all these three parameters, i.e., query complexity, w and ρ , was carefully studied in [34] in case of the Beeping feedback, and in some other recent works [33,36] the sparsity of some particular selectors was established and discussed. It is possible to derive bounds on parameters w

and ρ also for the query sequences considered in this paper. In particular, the sequence in Theorem 1 under the Parity^(α) feedback has $w = O(k \log(n/k))$ and $\rho = O(n\alpha/k)$, where both bounds can be obtained by a small modification of the analysis in Section 4.1. An interesting future direction would be to study tradeoffs between query complexity and the values of w, ρ for different feedback models, in particular, for different capacity α and expressiveness β .

Randomness. A popular line of research in Group Testing is to consider randomized solutions [15,6,36]. While in this work we focus on deterministic solutions, some of our algorithms have their simply constructed randomized counterparts, also presented in this work. Randomized algorithms defined in this way correctly distinguish *all* sets K . This can be contrasted with existing solutions that, typically, have weaker guarantees: with some probability, to correctly distinguish a *randomly chosen* set K from other sets of size at most k , or to correctly identify each element only with some probability (resulting in some false-positives and/or false-negatives with non-zero probability). Moreover, they typically work against a weaker non-adaptive version of an adversary, who has to choose the unknown set K before the random choices of the algorithm. An interesting future direction would be to investigate how different probabilistic guarantees and types of adversaries influence the query complexity of generalized Group Testing. Another intriguing question is how random perturbations of the feedback function (see e.g., [44]) affect the query complexity. Finally, designing efficient coding (i.e., constructing queries) and decoding (i.e., reconstructing set K from the feedback) algorithms, working in polynomial time, is a challenging open direction, sometimes even for randomized algorithms (cf., Section 4.3 with General^(α, β)(X) feedback).

Other feedbacks. The third direction, motivated by subtle examples of the considered $(\alpha, 2\lceil \log_2 n \rceil)$ -feedbacks of different query complexity in Section 6, is to study other specific well-motivated classes of (α, β) -feedbacks and their complexities. Although all (α, β) -feedbacks have to observe the universal lower bounds, such as the one in Theorem 4, their actual query complexity might be asymptotically larger.

Other adversaries. Observe that in our proofs of the lower bounds, Theorems 4 and 5, we use a weak α -Honest Adversary. This makes our lower bounds stronger and suggests that in case of deterministic non-adaptive algorithms, the adversary that uses *some* fixed function Adv may have similar power to the one being allowed to return arbitrary subsets. What actually follows from our results is that this adversarial impact may be similar for the best feedbacks in the class of (α, β) -feedbacks, but does not necessarily tell us about the impact for a specific feedback function. This opens an interesting direction of studying the impact of adversarial power, and more generally non-adaptiveness and “maliciousness”, to the Group Testing problem, not only for general classes of (α, β) -feedbacks (universal lower bounds, matching by upper bounds obtained for some (α, β) -feedbacks), but also for specific well-motivated feedback functions.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

Partially supported by Polish National Science Center (NCN) grants 2019/33/B/ST6/02988 and 2017/25/B/ST6/02553, and by NSF Secure and Trustworthy Cyberspace Award 2131538.

Appendix A. Auxiliary tools

A.1. Proof of Proposition 1

Proof. There are at most $2^{\bar{\alpha}}$ possible inputs to function f_1 . Hence, since it is deterministic, there are at most $2^{\bar{\alpha}}$ possible outputs. Take the family of all subsets of N of size at most N and define the partition of this family into subfamilies – each consisting of sets with the same value of f_1 . This partition has at most $2^{\bar{\alpha}}$ elements, because this is the size of the domain of f_1 . Fix an arbitrary ordering of this partition and enumerate its elements. Each subfamily receives a unique label with at most $\bar{\alpha}$ bits. Let feedback function f_2 for each set K return the label of the subfamily to which K belongs. Such feedback function has expressiveness at most $\bar{\alpha}$ and clearly it satisfies the property required from f_2 in the statement of the fact. \square

A.2. Proof of Proposition 2

Proof. Let S_{adv} denotes the set of all strategies of α -Malicious Adversary. From the definition of the adversary, we have $\text{Adv}(Q_\tau \cap K_1, \tau) = Q_\tau \cap K_1$ and $\text{Adv}(Q_\tau \cap K_2, \tau) = Q_\tau \cap K_2$. Hence position τ of feedback vector $\mathcal{F}(K_1, \text{Adv})$ equals to $\text{Feed}(Q_\tau \cap K_1)$ for any strategy of the adversary. Similarly position τ of feedback vector $\mathcal{F}(K_2, \text{Adv})$ equals to $\text{Feed}(Q_\tau \cap K_2)$ for any strategy of the adversary. Since $\text{Feed}(Q_\tau \cap K_1) \neq \text{Feed}(Q_\tau \cap K_2)$, then $\{\mathcal{F}(K_1, \text{Adv}) : \text{Adv} \in S_{adv}(Q, K_1)\} \cap \{\mathcal{F}(K_2, \text{Adv}) : \text{Adv} \in S_{adv}(Q, K_2)\} = \emptyset$. \square

A.3. Proof of Fact 1

Proof. We have:

$$\begin{aligned}
 (1 - 2p)^n &= ((1 - p) - p)^n = \sum_{k=0}^n \binom{n}{k} (-p)^k (1 - p)^{n-k} \\
 &= \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} p^{2k} (1 - p)^{n-2k} - \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k+1} p^{2k+1} (1 - p)^{n-2k-1} \\
 &= \mathbb{P}[X \text{ is even}] - \mathbb{P}[X \text{ is odd}].
 \end{aligned}$$

An since $1 = \mathbb{P}[X \text{ is even}] + \mathbb{P}[X \text{ is odd}]$, we get $\mathbb{P}[X \text{ is odd}] = (1 - (1 - 2p)^n)/2$. \square

References

- [1] Matthew Aldridge, Individual testing is optimal for nonadaptive group testing in the linear regime, *IEEE Trans. Inf. Theory* 65 (4) (2019) 2058–2061.
- [2] Matthew Aldridge, Leonardo Baldassini, Oliver Johnson, Group testing algorithms: bounds and simulations, *IEEE Trans. Inf. Theory* 60 (6) (2014) 3671–3687.
- [3] Matthew Aldridge, Oliver Johnson, Jonathan Scarlett, Group testing: an information theory perspective, *Found. Trends Commun. Inf. Theory* 15 (3–4) (2019) 196–392.
- [4] Reuven Bar-Yehuda, Oded Goldreich, Alon Itai, On the time-complexity of broadcast in multi-hop radio networks: an exponential gap between determinism and randomization, *J. Comput. Syst. Sci.* 45 (1) (1992) 104–126.
- [5] Wei Heng Bay, Eric Price, Jonathan Scarlett, Optimal non-adaptive probabilistic group testing in general sparsity regimes, *arXiv preprint, arXiv:2006.01325*, 2020.
- [6] Steffen Bendor, Binbin Chen, Jonathan Scarlett, Haifeng Yu, Yuda Zhao, Sublinear-time non-adaptive group testing with $\mathcal{O}(k \log n)$ tests via bit-mixing coding, *IEEE Trans. Inf. Theory* 67 (3) (2021) 1559–1570.
- [7] Nader H. Bshouty, Optimal algorithms for the coin weighing problem with a spring scale, in: *COLT 2009 - the 22nd Conference on Learning Theory*, Montreal, Quebec, Canada, June 18–21, 2009, 2009.
- [8] John Capetanakis, Generalized tdma: the multi-accessing tree protocol, *IEEE Trans. Commun.* 27 (10) (1979) 1476–1484.
- [9] John Capetanakis, Tree algorithms for packet broadcast channels, *IEEE Trans. Inf. Theory* 25 (5) (1979) 505–515.
- [10] Keren Censor-Hillel, Bernhard Haeupler, Nancy A. Lynch, Muriel Médard, Bounded-contention coding for the additive network model, *Distrib. Comput.* 28 (5) (2015) 297–308.
- [11] Bogdan S. Chlebus, Randomized communication in radio networks, *CoRR*, arXiv:1801.00074 [abs], 2018.
- [12] Sung-Soon Choi, Jeong Han Kim, Optimal query complexity bounds for finding graphs, *Artif. Intell.* 174 (9–10) (2010) 551–569.
- [13] Andrea E.F. Clementi, Angelo Monti, Riccardo Silvestri, Selective families, superimposed codes, and broadcasting on unknown radio networks, in: *Proceedings of the Twelfth Annual Symposium on Discrete Algorithms*, January 7–9, 2001, ACM/SIAM, Washington, DC, USA, 2001, pp. 709–718.
- [14] Raphaël Clifford, Klim Efremenko, Ely Porat, Amir Rothschild, Pattern matching with don't cares and few errors, *J. Comput. Syst. Sci.* 76 (2) (2010) 115–124.
- [15] Amin Coja-Oghlan, Oliver Gebhard, Max Hahn-Klimroth, Philipp Loick, Information-theoretic and algorithmic thresholds for group testing, *IEEE Trans. Inf. Theory* 66 (12) (2020) 7911–7928.
- [16] Graham Cormode, S. Muthukrishnan, Combinatorial algorithms for compressed sensing, in: *International Colloquium on Structural Information and Communication Complexity*, Springer, 2006, pp. 280–294.
- [17] Graham Cormode, Shan Muthukrishnan, What's hot and what's not: tracking most frequent items dynamically, *ACM Trans. Database Syst.* 30 (1) (2005) 249–278.
- [18] Peter Damaschke, Threshold group testing, in: *General Theory of Information Transfer and Combinatorics*, in: *Electronic Notes in Discrete Mathematics*, vol. 21, 2005, pp. 265–271.
- [19] Annalisa De Bonis, Leszek Gasieniec, Ugo Vaccaro, Generalized framework for selectors with applications in optimal group testing, in: *Automata, Languages and Programming*, 30th International Colloquium, ICALP 2003, Eindhoven, the Netherlands, June 30 – July 4, 2003. *Proceedings*, in: *Lecture Notes in Computer Science*, vol. 2719, Springer, 2003, pp. 81–96.
- [20] Annalisa De Bonis, Ugo Vaccaro, ϵ -Almost selectors and their applications to multiple-access communication, *IEEE Trans. Inf. Theory* 63 (11) (2017) 7304–7319.
- [21] Gianluca De Marco, Tomasz Jurdzinski, Dariusz R. Kowalski, Optimal channel utilization with limited feedback, in: *Fundamentals of Computation Theory - 22nd International Symposium, FCT 2019, Copenhagen, Denmark, August 12–14, 2019*, *Proceedings*, in: *Lecture Notes in Computer Science*, vol. 11651, Springer, 2019, pp. 140–152.
- [22] Gianluca De Marco, Tomasz Jurdzinski, Dariusz R. Kowalski, Michał Różanski, Grzegorz Stachowiak, Subquadratic non-adaptive threshold group testing, *J. Comput. Syst. Sci.* 111 (2020) 42–56.
- [23] A.G. Djakov, On a search model of false coins, in: *Topics in Information Theory*, *Colloquia Mathematica Societatis Janos Bolyai* 16, Hungarian Acad. Sci., Budapest, Hungary, 1975, pp. 163–170.
- [24] Benjamin Doerr, Probabilistic tools for the analysis of randomized optimization heuristics, *CoRR*, arXiv:1801.06733 [abs], 2018.
- [25] Robert Dorfman, The detection of defective members of large populations, *Ann. Math. Stat.* 14 (4) (1943) 436–440.
- [26] Dingzhu Du, Frank K. Hwang, Frank Hwang, *Combinatorial Group Testing and Its Applications*, vol. 12, World Scientific, 2000.
- [27] Paul Erdős, Peter Frankl, Zoltán Füredi, Families of finite sets in which no set is covered by the union of r others, *Isr. J. Math.* 51 (1–2) (1985) 79–89.
- [28] Paul Erdős, Alfréd Rényi, On two problems of information theory, *Magy. Tud. Akad. Mat. Kut. Intéz. Közl.* 8 (1963) 229–243.
- [29] Robert Gallager, A perspective on multiaccess channels, *IEEE Trans. Inf. Theory* 31 (2) (1985) 124–142.
- [30] Vladimir Grebinski, Gregory Kucherov, Optimal reconstruction of graphs under the additive model, *Algorithmica* 28 (1) (2000) 104–124.
- [31] Albert G. Greenberg, Philippe Flajolet, Richard E. Ladner, Estimating the multiplicities of conflicts to speed their resolution in multiple access channels, *J. ACM* 34 (2) (1987) 289–325.
- [32] Albert G. Greenberg, Schmel Winograd, A lower bound on the time needed in the worst case to resolve conflicts deterministically in multiple access channels, *J. ACM* 32 (3) (1985) 589–596.

- [33] Elijah Hradovich, Marek Klonowski, Dariusz R. Kowalski, Contention resolution on a restrained channel, in: 26th IEEE International Conference on Parallel and Distributed Systems, ICPADS 2020, Hong Kong, December 2–4, 2020, IEEE, 2020, pp. 89–98.
- [34] Huseyin A. Inan, Peter Kairouz, Ayfer Özgür, Sparse combinatorial group testing, *IEEE Trans. Inf. Theory* 66 (5) (2020) 2729–2742.
- [35] Piotr Indyk, Deterministic superimposed coding with applications to pattern matching, in: 38th Annual Symposium on Foundations of Computer Science, FOCS '97, October 19–22, 1997, IEEE Computer Society, Miami Beach, Florida, USA, 1997, pp. 127–136.
- [36] Oliver Johnson, Matthew Aldridge, Jonathan Scarlett, Performance of group testing algorithms with near-constant tests per item, *IEEE Trans. Inf. Theory* 65 (2) (2019) 707–723.
- [37] William Kautz, Roy Singleton, Nonrandom binary superimposed codes, *IEEE Trans. Inf. Theory* 10 (4) (1964) 363–377.
- [38] János Komlós, Albert G. Greenberg, An asymptotically fast nonadaptive algorithm for conflict resolution in multiple-access channels, *IEEE Trans. Inf. Theory* 31 (2) (1985) 302–306.
- [39] Weixin Liang, James Zou, Neural group testing to accelerate deep learning, in: IEEE International Symposium on Information Theory, ISIT 2021, IEEE, 2021.
- [40] Bernt Lindstrom, Determining subsets by unramified experiments, in: A Survey of Statistical Design and Linear Models, 1975, pp. 407–418.
- [41] James L. Massey, Collision-resolution algorithms and random-access communications, in: Multi-User Communication Systems, Springer, 1981, pp. 73–137.
- [42] Dragoslav S. Mitrinovic, Petar M. Vasic, *Analytic inequalities*, vol. 1, Springer, 1970.
- [43] Ron M. Roth, Introduction to coding theory, *IET Commun.* 47 (2006).
- [44] Jonathan Scarlett, Oliver Johnson, Noisy non-adaptive group testing: a (near-)definite defectives approach, *IEEE Trans. Inf. Theory* 66 (6) (2020) 3775–3797.
- [45] Jack Wolf, Born again group testing: multiaccess communications, *IEEE Trans. Inf. Theory* 31 (2) (1985) 185–191.