Received: 28 May 2021 | Revised: 16 May 2022 | Accepted: 6 June 2022

DOI: 10.1002/rsa.21114

RESEARCH ARTICLE

WILEY

Haystack hunting hints and locker room communication

Artur Czumaj[1] | **George Kontogeorgiou**[2] | **Mike Paterson**[3]

[1]Department of Computer Science and Centre for Discrete Mathematics and its Applications (DIMAP), University of Warwick, Coventry, UK
[2]Mathematics Institute, University of Warwick, Coventry, UK
[3]Department of Computer Science and Centre for Discrete Mathematics and its Applications (DIMAP), University of Warwick, UK

Correspondence
George Kontogeorgiou, Mathematics Institute, University of Warwick, Coventry, UK.
Email: George.Kontogeorgiou@warwick.ac.uk

Funding information
Centre for Discrete Mathematics and its Applications (DIMAP); IBM Faculty Award; EPSRC, Grant/Award Number: EP/V01305X/1; EPSRC Doctoral Training Partnership.

Abstract

We want to efficiently find a specific object in a large unstructured set, which we model by a *randomn-permutation*, and we have to do it by revealing just a single element. Clearly, without any help this task is hopeless and the best one can do is to select the element at random, and achieve the success probability $\frac{1}{n}$. Can we do better with some small amount of advice about the permutation, even without knowing the target object? We show that by providing advice of just one integer in $\{0, 1, \ldots, n-1\}$, one can improve the success probability considerably, by a $\Theta\left(\frac{\log n}{\log \log n}\right)$ factor. We study this and related problems, and show asymptotically matching upper and lower bounds for their optimal probability of success. Our analysis relies on a close relationship of such problems to some intrinsic properties of random permutations related to the rencontres number.

KEYWORDS

communication complexity, random permutations, search

1 | INTRODUCTION

Understanding basic properties of random permutations is an important concern in modern data science. For example, a preliminary step in the analysis of a very large data set presented in an unstructured way is often to model it assuming the data is presented in a random order. Understanding properties of random permutations would guide the processing of this data and its analysis. In this paper, we consider a very natural problem in this setting. You are given a set S of n objects stored in locations

FIGURE 1 Consider the above randomly shuffled deck, one card per locker. What advice should Alice give to Bob—just by swapping the locations of at most one pair of cards—to increase the probability that Bob will find his randomly chosen card by opening at most two lockers?

$x_0, \ldots, x_{n-1}$ according to a random permutation σ of S. This is the *haystack*, and you want to find one specific object, not surprisingly called the *needle*, by drawing from just one location. We will take the set S to be $[n] = \{0, 1, \ldots, n-1\}$.

Clearly, the probability of finding this object $\mathfrak{s}$ in a single draw is always $\frac{1}{n}$, whichever location you choose. Since the permutation σ is random, the probability that your object is there is exactly $\frac{1}{n}$. But can I give you any advice or *hint* about σ—*without knowing which object you are seeking*—to improve your chance of finding $\mathfrak{s}$? If I could tell you the entire σ, which can be encoded with $\log(n!) = \Theta(n \log n)$ bits, then this task is trivial and you would know the location of $\mathfrak{s}$. But what if I give you just a small hint (on the basis of σ), one number $\mathfrak{h}$ from $[n]$ (or equivalently, one $\log n$-bit sequence)—even when I know nothing about the target object?

Formally, the goal is to design a strategy to choose a *hint* $\mathfrak{h} = \mathfrak{h}(\sigma)$ and an *index* $\mathfrak{i} = \mathfrak{i}(\mathfrak{h}, \mathfrak{s})$, with both $\mathfrak{h}, \mathfrak{i} \in [n]$, such that for a given $\mathfrak{s} \in [n]$, $\mathbf{Pr}\left[\sigma(\mathfrak{i}) = \mathfrak{s}\right]$ is maximized, where the probability is over the random choice of σ.

1.1 | Related puzzle: *Communication in the locker room*

The *needle in a haystack* problem is closely related to the following *locker room* problem(see Figure 1): The locker room has n lockers, numbered $0, \ldots, n-1$. A set of n cards, numbered $0, \ldots, n-1$, is inserted in the lockers according to a uniformly random permutation σ. Alice and Bob are a team with a task. Before the game begins, Alice and Bob may communicate to decide on a strategy. Alice enters the locker room, opens all the lockers and can swap the cards between just two lockers, or may choose to leave them unchanged. She closes all the lockers and leaves the room. Bob is given a number $\mathfrak{s} \in [n]$ and his task is to find card $\mathfrak{s}$. He can open at most two lockers. What is their optimal strategy, and how efficient is it?

As in the *needle in a haystack* problem, without help from Alice, Bob can do no better than open lockers at random. If he opens one locker his probability of success is $\frac{1}{n}$ and if he opens two lockers this probability is $\frac{2}{n}$. With the help of Alice, he can do better when opening one locker. For example, their strategy could be that Bob will open locker $\mathfrak{s}$, where $\mathfrak{s}$ is his given number. Alice would then try to increase the number of fixed points in the permutation above the expected number of 1. If there is a transposition she can reverse it, increasing the number of fixed points by two, and if not she can produce one more fixed point (unless the permutation is the identity). This strategy succeeds with probability just under $\frac{12}{5n}$. When Bob can open two lockers, the challenge is to increase the success probability to $\omega\left(\frac{1}{n}\right)$.

The answer involves viewing Bob's first locker opening in a different way: not as looking for his card but as receiving a communication from Alice. The interest is in finding what kind of information Alice can send about the permutation which could help Bob in his search.

Now, we invite the reader to stop for a moment: to think about this puzzle, to find any strategy that could ensure the success probability would be $\omega\left(\frac{1}{n}\right)$.

It is easy to see that a solution to the *needle in a haystack* problem immediately yields a solution to the *locker room* problem: Alice just takes the card corresponding to the advice and swaps it into the

first locker. For example, the shuffled deck from Figure 1 corresponds to the following permutation σ:

$$\sigma(0, 1, \ldots, 19) = (13, 10, 14, 15, 4, 17, 2, 9, 7, 19, 5, 1, 6, 11, 16, 18, 8, 0, 3, 12).$$

If in the *needle in a haystack* problem the advice is a number $\mathfrak{h} \in [n]$, then Alice swaps the contents of locker 0 and the locker containing the card corresponding to number $\mathfrak{h}$. This way, Bob gets the advice $\mathfrak{h}$ by opening locker 0.

For the strategy we propose in Theorem 7, Alice would swap cards **13** and **8**. But can we do better?

1.2 | Results for the *needle in a haystack* and *locker room* problems

We present a tight analysis of the *needle in a haystack* problem. While some basic examples suggest that it is difficult to ensure success probability $\omega\left(\frac{1}{n}\right)$, we will show that one can improve this probability considerably. Our main results are tight (up to lower order terms) lower and upper bounds for the maximum probability that with a single number hint one can find the target object. First, we will show that for any strategy, this probability is at most $\frac{(1+o(1))\log n}{n\log\log n}$ (Theorem 5). As the main result of this paper, we will complement this by designing a simple strategy that with a hint ensures that the target is found with probability at least $\frac{(1+o(1))\log n}{n\log\log n}$ (Theorem 7).

Further, we demonstrate essentially the same results for the *locker room* problem. Theorem 7 for the *needle in a haystack* problem immediately implies that there is a simple strategy for Alice and Bob which ensures that Bob finds his card with probability at least $\frac{(1+o(1))\log n}{n\log\log n}$. We will complement this claim, and extend in Theorem 21 the result from Theorem 5 for the *needle in a haystack* problem, to prove that for any strategy for Alice and Bob, the probability that Bob finds the required card is at most $O\left(\frac{\log n}{n\log\log n}\right)$.

Techniques. Our analysis exploits properties of random permutations to ensure that some short advice can reveal information about the input permutation, which can be used to increase the success probability substantially. Our approach depends on intrinsic properties of random permutations related to the *rencontres number*, the number of n-permutations with a given number of fixed points.

To show the upper bound for the success probability (Theorem 5), we observe that every deterministic strategy corresponds to a unique partition of $\mathbb{S}_n$ (set of all permutations of $[n]$) into n parts, with part $\mathfrak{h}$ containing those permutations that cause the choice of hint $\mathfrak{h}$. By a careful analysis of the properties of this partition, we devise a metric for the best possible accuracy of the prediction, counting instances in each part of the partition in which a permutation maps a given choice $\mathfrak{i}$ to $\mathfrak{s}$. By combining these estimates with the bounds for the rencontres number, we prove the upper bound for the success probability in the *needle in a haystack* problem.

To show the lower bound for the success probability (Theorem 7), we present a simple *shift strategy*, and then provide a non-trivial analysis of random permutations that demonstrates desirable properties of this strategy. The analysis here is related to the maximum load problem for balls and bins, where one allocates n balls into n bins, chosen independently and uniformly at random (*i.u.r.*). However, the dependencies between locations of distinct elements in the random permutations make this analysis more complex (see Remark 11 for more detailed discussion).

Finally, while a solution to the *needle in a haystack* problem immediately yields a solution to the *locker room* problemwith the same success probability, we complement our analysis by showing (Theorem 21) that no strategy of Alice and Bob can do much better. We show that Alice can do little more than just to send a few numbers to Bob, which is essentially the setup of the *needle in a haystack* problem.

1.3 | Background: Permutations, puzzles, and locker rooms

Our *locker room* problemfollows a long line of combinatorial puzzles involving the analysis of properties of permutations. One such example is the following locker problem involving prisoners and lockers: There are n lockers into which a random permutation of n cards are inserted. Then n prisoners enter the locker room one at a time and are allowed to open half the lockers in an attempt to find their own card. The team of prisoners wins if every one of them is successful. The surprising result is that there is a strategy which wins with probability about $1 - \ln 2$. This problem was initially considered by Peter Bro Miltersen and appeared in his paper with Anna Gál [8], which won a best paper award at ICALP 2003. In that paper they refer to a powerful strategy approach suggested by Sven Skyum but it was left to the readers to find it for themselves. This is the idea of using the number contained in each locker as a pointer to another locker. Thus using a sequence of such steps corresponds to following a cycle in the permutation. Solutions to these problems are of a *combinatorial and probabilistic flavor* and involve an *analysis of the cycle structure of random permutations*. The original paper [8] stimulated many subsequent papers considering different variants (see, for example, [4, 5, 9]), including a matching upper bound provided in [6]. An early version giving the problem where each prisoner can open half the lockers was published by [15] (see also [16, p. 18]). If each prisoner begins with the locker corresponding to the number they seek then they will all succeed provided that there is no cycle in the permutation which is longer than $\frac{n}{2}$. It is easy to show that a helpful prison warder, Alice, can always find an appropriate transposition of the contents of two lockers so that the resulting permutation has no cycle longer than $\frac{n}{2}$. We were told of this observation recently by Kazuo Iwama and this stimulated the current paper, in which we subvert the locker problem tradition with a problem which has little to do with the cycle structure of permutations and is more concerned with some basic communication complexity and rather different properties of permutations.

Various results about permutations have found diverse applications in computer science, especially for sorting algorithms (e.g., see [11, chapter 5]). In this article, we are particularly interested in rencontres numbers. Firstly, to apply known results concerning their asymptotic growth, in order to approximate the optimal success probabilities in both the *needle in a haystack* problem and the *locker room* problem. Secondly, to use them to examine the way in which the sizes of "shift sets" (sets of elements which a permutation displaces by the same number of positions "to the right") are distributed in permutations of $\mathbb{S}_n$ for a fixed natural number n. In particular, to determine the mean size of the largest shift set of a permutation chosen uniformly at random from $\mathbb{S}_n$, as well as to show that it is typical, that is, that the variance of the size of the largest shift set is small. These results are useful for providing a concrete optimal strategy for both of the titular search problems.

2 | PRELIMINARIES

2.1 | Formal framework and justification about worst-case versus random $\mathfrak{s}$

We consider the problem with two inputs: a number $\mathfrak{s} \in [n]$ and a permutation $\sigma \in \mathbb{S}_n$. We are assuming that σ is a random permutation in $\mathbb{S}_n$; no assumption is made about $\mathfrak{s}$.

For the *needle in a haystack* problem (a similar framework can be easily set up for the *locker room* problem), a *strategy* (or an *algorithm*) is defined by a pair of functions, $\mathfrak{h} = \mathfrak{h}(\sigma)$ and $\mathfrak{i} = \mathfrak{i}(\mathfrak{h}, \mathfrak{s})$, with both $\mathfrak{h}, \mathfrak{i} \in [n]$.

For a fixed strategy, let $\mathfrak{p}(\mathfrak{s})$ be the success probability for a given $\mathfrak{s}$ and for a randomly chosen $\sigma \in \mathbb{S}_n$. That is,

$$\mathfrak{p}(\mathfrak{s}) = \mathbf{Pr}\big[\sigma(\mathfrak{i}) = \mathfrak{s}\big],$$

where the probability is over σ taken i.u.r. from $\mathbb{S}_n$.

The goal is to design an algorithm (find a strategy) that will achieve some given success probability for every $\mathfrak{s} \in [n]$. That is, we want to have a strategy which maximizes

$$\mathbf{Pr}[\mathcal{V}] = \min_{\mathfrak{s}\in[n]}\{\mathfrak{p}(\mathfrak{s})\}.$$

In our analysis for the upper bounds in Sections 2 and 3 (Theorem 5) and Section 6 (Theorem 21), for simplicity, we will be making the assumption that $\mathfrak{s}$ (the input to the *needle in a haystack* problem and to the *locker room* problem) is random, that is, $\mathfrak{s}$ is chosen i.u.r. from [n]. (We do not make such assumption in the lower bound in Section 4 (Theorem 7), where the analysis is done explicitly for arbitrary $\mathfrak{s}$.) Then the main claim (Theorem 5) is that if we choose $\mathfrak{s}$ i.u.r. then $\mathfrak{p}(\mathfrak{s}) \leq \frac{(1+o(1))\log n}{n\log\log n}$. Observe that one can read this claim equivalently as that $\sum_{\mathfrak{s}\in[n]} \frac{\mathfrak{p}(\mathfrak{s})}{n} \leq \frac{(1+o(1))\log n}{n\log\log n}$. However, notice that this trivially yields

$$\mathbf{Pr}[\mathcal{V}] = \min_{\mathfrak{s}\in[n]}\{\mathfrak{p}(\mathfrak{s})\} \leq \sum_{\mathfrak{s}\in[n]} \frac{\mathfrak{p}(\mathfrak{s})}{n},$$

and therefore Theorem 5 yields $\mathbf{Pr}[\mathcal{V}] \leq \frac{(1+o(1))\log n}{n\log\log n}$, as required.

Note that such arguments hold only for the upper bound. Indeed, since $\min_{\mathfrak{s}\in[n]}\{\mathfrak{p}(\mathfrak{s})\}$ may be much smaller than $\sum_{\mathfrak{s}\in[n]} \frac{\mathfrak{p}(\mathfrak{s})}{n}$, in order to give a lower bound for the success probability, Theorem 7 proves that there is a strategy that ensures that $\mathfrak{p}(\mathfrak{s}) \geq \frac{(1+o(1))\log n}{n\log\log n}$ for every $\mathfrak{s} \in [n]$; this clearly yields $\mathbf{Pr}[\mathcal{V}] \geq \frac{(1+o(1))\log n}{n\log\log n}$, as required.

2.2 | Describing possible strategies for *needle in a haystack*

In this section, we prepare a framework for the study of strategies to prove an upper bound for the success probability for the *needle in a haystack* problem (see Section 3). First, we rephrase the original problem as an equivalent communication game between Alice and Bob. Bob, the *seeker*, has as his input a (random) number $\mathfrak{s} \in [n]$. Alice, the *adviser*, sees a permutation σ chosen i.u.r. from $\mathbb{S}_n$, and uses σ to send advice to Bob in the form of a number $\mathfrak{h} \in [n]$. Bob does not know σ, but on the basis of $\mathfrak{s}$ and $\mathfrak{h}$, he picks some $\mathfrak{i} \in [n]$ trying to maximize the probability that $\sigma(\mathfrak{i}) = \mathfrak{s}$.

First we will consider *deterministic strategies*, and will later argue separately that randomized strategies cannot help much. For deterministic strategies, the advice sent is a function $\mathbb{S}_n \to [n]$, which can be defined by a partition of $\mathbb{S}_n$ into n sets.

Definition 1. A **strategy** $\mathbb{C}$ for $\mathbb{S}_n$ is a partition of $\mathbb{S}_n$ into n sets $C_0, C_1, \ldots, C_{n-1}$. Such a strategy $\mathbb{C}$ is denoted by $\mathbb{C} = \langle C_0, C_1, \ldots, C_{n-1}\rangle$.

Given a specific strategy $\mathbb{C}$, we examine the success probability. Let $\mathcal{V}$ be the event that the target is found, $\mathcal{A}_\mathfrak{h}$ the event that $\mathfrak{h}$ is the received advice, and $\mathcal{B}_\mathfrak{s}$ the event that $\mathfrak{s}$ is the target. Notice that for every $\mathfrak{h} \in [n]$ we have $\mathbf{Pr}\big[\mathcal{A}_\mathfrak{h}\big] = \frac{|C_\mathfrak{h}|}{n!}$ and for every $\mathfrak{s} \in [n]$ we have $\mathbf{Pr}[\mathcal{B}_\mathfrak{s}] = \frac{1}{n}$. Therefore, since the events $\mathcal{A}_\mathfrak{h}$ and $\mathcal{B}_\mathfrak{s}$ are independent,

$$\mathbf{Pr}[\mathcal{V}] = \sum_{\mathfrak{s}=0}^{n-1}\sum_{\mathfrak{h}=0}^{n-1}\mathbf{Pr}\big[\mathcal{V}|\mathcal{A}_\mathfrak{h}\cap\mathcal{B}_\mathfrak{s}\big]\cdot\mathbf{Pr}\big[\mathcal{A}_\mathfrak{h}\cap\mathcal{B}_\mathfrak{s}\big] = \sum_{\mathfrak{s}=0}^{n-1}\sum_{\mathfrak{h}=0}^{n-1}\mathbf{Pr}\big[\mathcal{V}|\mathcal{A}_\mathfrak{h}\cap\mathcal{B}_\mathfrak{s}\big]\cdot\mathbf{Pr}\big[\mathcal{A}_\mathfrak{h}\big]\cdot\mathbf{Pr}[\mathcal{B}_\mathfrak{s}]$$

$$= \frac{1}{n}\sum_{\mathfrak{h}=0}^{n-1}\frac{|C_{\mathfrak{h}}|}{n!}\cdot\sum_{\mathfrak{s}=0}^{n-1}\mathbf{Pr}\left[\mathcal{V}|\mathcal{A}_{\mathfrak{h}}\cap\mathcal{B}_{\mathfrak{s}}\right]. \tag{1}$$

Definition 2. Let $\mathbb{C} = \langle C_0, C_1, \ldots, C_{n-1}\rangle$ be a strategy. The **magneticity** of an element i for an element k in the class C_j is defined as $\mathsf{mag}(C_j, i, k) = |\{\sigma \in C_j : \sigma(i) = k\}|$.

The element with the greatest magneticity for k in the class C_j is called the **magnet in** C_j **of** k and is denoted $\mathsf{max\text{-}mag}(C_j, k)$; ties are broken arbitrarily. The magneticity of $\mathsf{max\text{-}mag}(C_j, k)$ is called the **intensity of** k **in** C_j, denoted by $\mathsf{int}(C_j, k)$; that is, $\mathsf{int}(C_j, k) = \max_{i\in[n]}\{\mathsf{mag}(C_j, i, k)\}$.

Let us discuss the intuitions. Firstly, the *magneticity* in the class C_j of an element i for an element k, $\mathsf{mag}(C_j, i, k)$, denotes the number of permutations in C_j with k in position i. Therefore, the *magnet* in C_j of k is an index $i \in [n]$ such that, among all permutations in C_j, k is most likely to be in position i. The *intensity* in C_j of k denotes just the number of times (among all permutations in C_j) that k appears in the position of the magnet i.

In the *needle in a haystack* problem, Alice sends to Bob a message $\mathfrak{h}$ which points to a class $C_{\mathfrak{h}}$ of their agreed strategy $\mathbb{C}$, and Bob has to choose a number $\mathfrak{i}$ in order to find whether $\sigma(\mathfrak{i})$ is the number $\mathfrak{s} \in [n]$ which he seeks. The maximum probability that they succeed is $\frac{\mathsf{int}(C_{\mathfrak{h}},\mathfrak{s})}{|C_{\mathfrak{h}}|}$, realized if Bob opts for the magnet of $\mathfrak{s}$ in $C_{\mathfrak{h}}$. Thus, by (1), we obtain

$$\mathbf{Pr}[\mathcal{V}] \le \frac{1}{n}\cdot\frac{1}{n!}\sum_{\mathfrak{s},\mathfrak{h}\in[n]}\mathsf{int}(C_{\mathfrak{h}},\mathfrak{s}).$$

Definition 3. Let the **field** of $\mathbb{S}_n$ be $F(n) = \max_{\mathbb{C}=\langle C_0,C_1,\ldots,C_{n-1}\rangle}\sum_{\mathfrak{s},\mathfrak{h}\in[n]}\mathsf{int}(C_{\mathfrak{h}},\mathfrak{s})$.

With this definition, a strategy which yields the field of $\mathbb{S}_n$ is called *optimal*, and

$$\mathbf{Pr}[\mathcal{V}] \le \frac{1}{n}\cdot\frac{1}{n!}\sum_{\mathfrak{s},\mathfrak{h}\in[n]}\mathsf{int}(C_{\mathfrak{h}},\mathfrak{s}) \le \frac{1}{n}\cdot\frac{F(n)}{n!}. \tag{2}$$

We will use this bound to prove Theorem 5 in Section 3, that whatever the strategy, we always have $\mathbf{Pr}[\mathcal{V}] \le \frac{(1+o(1))\cdot\log n}{n\log\log n}$.

2.3 | Derangements

We use properties of random permutations related to derangements and rencontres numbers.

Definition 4. A permutation $\sigma \in \mathbb{S}_n$ with no fixed points is called a **derangement**. The number of derangements in $\mathbb{S}_n$ is denoted D_n. A permutation $\sigma \in \mathbb{S}_n$ with exactly r fixed points is called an r**-partial derangement**. The number of r-partial derangements in $\mathbb{S}_n$ (also known as the rencontres number) is denoted $D_{n,r}$.

Definition 4 yields $D_{n,0} = D_n$ and it is easy to see that $D_{n,r} = \binom{n}{r} D_{n-r}$. It is also known (see, e.g., [10, p. 195]) that $D_n = \lfloor\frac{n!}{e} + \frac{1}{2}\rfloor$, and hence one can easily show $D_{n,r} \le \frac{n!}{r!}$.

3 | UPPER BOUND FOR THE SUCCESS PROBABILITY FOR NEEDLE IN A HAYSTACK

We will use the framework set up in the previous section, in particular the tools in Definition 2 and inequality (2) and that $\mathfrak{s}$ is chosen i.u.r. from $[n]$, to bound from above the best possible success probability for the *needle in a haystack* problem.

Theorem 5. *For any strategy in the needle in a haystack problem, the success probability satisfies*

$$\mathbf{Pr}[\mathcal{V}] \leq \frac{(1+o(1))\log n}{n\log\log n}.$$

Proof. Consider a strategy $\mathbb{C} = \langle C_0, \ldots, C_{n-1}\rangle$. For a permutation $\sigma \in C_j$ to contribute at least r to $\sum_{i\in[n]} \mathsf{int}(C_j, i)$, σ^{-1} must map at least r elements to their magnets in C_j. Hence, there are at most $\binom{n}{r}(n-r)! = \frac{n!}{r!}$ permutations in C_j that contribute at least r to $\sum_{i\in[n]} \mathsf{int}(C_j, i)$, so all in all there are at most $n \cdot \frac{n!}{r!}$ permutations that contribute at least r to $F(n)$.

Let X be the random variable measuring the contribution to $F(n)$ of a permutation σ chosen uniformly at random from $\mathbb{S}_n$. Then for any natural ℓ,

$$\frac{F(n)}{n!} = E[X] = \sum_{i=1}^{n} P(X \geq k) \leq \ell + \sum_{r=\ell+1}^{n} \frac{n}{r!}.$$

We choose some $\ell = \frac{(1+o(1))\log n}{\log\log n}$ to ensure that $n = o(\ell!)$, yielding $(\ell+s)! \geq (\ell+1)^s \ell! \geq (\ell+1)^s n$ for every $s \in \mathbb{N}$, whence we obtain

$$\frac{F(n)}{n!} \leq \ell + \sum_{s=1}^{\infty} (\ell+1)^{-s} = \ell + \frac{1}{\ell} = \frac{(1+o(1))\log n}{\log\log n}. \tag{3}$$

We can combine (2) and (13) to obtain the following,

$$\mathbf{Pr}[\mathcal{V}] \leq \frac{1}{n} \cdot \frac{F(n)}{n!} \leq \frac{(1+o(1))\log n}{n\log\log n}.$$

■

Remark 6. The upper bound of $\frac{(1+o(1))\log n}{n\log\log n}$ is valid not only for deterministic strategies, but also for randomized strategies. Let $c(\mathbb{C}, (\sigma, i))$ be the indicator function of the event that the strategy $\mathbb{C}$ fails to guess the image of i under the permutation σ. Let us consider a probability measure P over the set D of all deterministic strategies, and the distribution $U = \left(U_{\mathbb{S}_n}, U_{[n]}\right)$ over $\mathbb{S}_n \times [n]$, where U_S denotes the uniform probability measure over the set S. Let S be a random strategy chosen according to P, and let X be a random set-up chosen according to U. Then, by Yao's principle, $\max_{(\sigma,i)\in\mathbb{S}_n\times[n]} \mathbf{E}\left[c(S,(\sigma,i))\right] \geq \min_{\mathbb{C}\in D} \mathbf{E}\left[c(\mathbb{C}, X)\right]$. That is, the probability that a randomized strategy fails for the worst-case input exceeds the probability that an optimal deterministic strategy fails. Hence, the worst-case probability that a randomized strategy succeeds is also bounded above by $\frac{(1+o(1))\log n}{n\log\log n}$.

4 | LOWER BOUND: SOLUTION FOR THE NEEDLE IN A HAYSTACK SEARCH

In Theorem 5, we showed that whatever strategy we use in the *needle in a haystack* problem, the best success probability we can hope for is $\frac{(1+o(1))\log n}{n\log\log n}$. In this section we will show that such success probability is achievable by a simple strategy, which we call the *shift strategy*.

- Let $\mathfrak{h} \in [n]$ maximize $|\{\ell \in [n] : \ell = \sigma(\ell + \mathfrak{h} \pmod n)\}|$.
- In order to find number $\mathfrak{s} \in [n]$ in σ, check $\sigma(\mathfrak{s} + \mathfrak{h} \pmod n)$.

(Observe that our choice of $\mathfrak{h}$ is equivalent to maximizing $|\{\ell \in [n] : (\ell - \mathfrak{h} \pmod n) = \sigma(\ell)\}|$.)

We will prove that the shift strategy ensures a success probability of at least $\frac{(1+o(1))\log n}{n\log\log n}$. Notice that this is equivalent to saying that $\mathbf{Pr}\big[\sigma(\mathfrak{s} + \mathfrak{h} \pmod n) = \mathfrak{s}\big] \geq \frac{(1+o(1))\log n}{n\log\log n}$, and hence, by the definition of $\mathfrak{h}$, that with probability $1 - o(1)$,

$$\max_{s\in[n]} \left\{ \Big| \{\ell \in [n] : \ell - \sigma(\ell) = s \pmod n\} \Big| \right\} \geq \frac{(1+o(1))\log n}{\log\log n}.$$

This also implies, by Theorem 5 (Section 3), that the shift strategy is asymptotically optimal.

Theorem 7. *For any $\mathfrak{s} \in [n]$, the shift strategy satisfies* $\mathbf{Pr}[\mathcal{V}] \geq \frac{(1+o(1))\log n}{n\log\log n}$.

In order to prove Theorem 7, we introduce some notation. For every $i \in [n]$, let $v(i) = i - \sigma(i) \pmod n$. Since σ is random, $v(i)$ has uniform distribution over $[n]$.

Let $S_\ell = |\{i \in [n] : v(i) = \ell\}|$. Notice that in the shift strategy $\mathbb{C} = \langle C_0, C_1, \ldots, C_{n-1}\rangle$, if $\sigma \in C_\mathfrak{h}$ then $S_\mathfrak{h} = \max_{\ell\in[n]}\{S_\ell\}$. Therefore, our goal is to study basic properties of the distribution of $S_\mathfrak{h}$, and in particular, to estimate the largest value of S_j over all $j \in [n]$.

Example 1. Using the example presented in Figure 1 with

$$\sigma(0, 1, \ldots, 19) = (13, 10, 14, 15, 4, 17, 2, 9, 7, 19, 5, 1, 6, 11, 16, 18, 8, 0, 3, 12),$$

we have

$$v(0, 1, \ldots, 19) = (7, 11, 8, 8, 0, 8, 4, 18, 1, 10, 5, 10, 6, 2, 18, 17, 8, 17, 15, 7).$$

Then

$$(S_0, S_1, \ldots, S_{19}) = (1, 1, 1, 0, 1, 1, 1, 2, 4, 0, 2, 1, 0, 0, 0, 1, 0, 2, 2, 0),$$

so $\mathfrak{h} = 8$ and $S_\mathfrak{h} = 4$. Alice delivers this hint to Bob by exchanging cards **13** and **8**. Then, over all $\mathfrak{s} \in [n]$, $\mathbf{Pr}[\sigma(\mathfrak{s} + 8 \pmod{20}) = \mathfrak{s}] = \frac{4}{20}$. ⊠

Let us first notice the following simple auxiliary lemma which should give the *intuition* behind our approach (see Appendix A.1 for a standard and elementary proof).

Lemma 8. *The expected number of values $j \in [n]$ with $S_j \geq \frac{(1+o(1))\log n}{\log\log n}$ is at least one.*

Lemma 8 tells us that in expectation, there is at least one value j such that $S_j \geq \frac{(1+o(1))\log n}{\log\log n}$. Notice however that in principle, we could have that this expectation is high but only because with small probability the random variable takes a very high value. Therefore the bound in Lemma 8 is fairly weak. We will now prove, using the second moment method, that with high probability there is some j such that $S_j \geq \frac{(1+o(1))\log n}{\log\log n}$. This yields Theorem 7.

Lemma 9. *With probability $1-o(1)$, there is some $j \in [n]$ such that $S_j \geq \frac{(1+o(1))\log n}{\log\log n}$.*

Proof. Let Z_j^t be the indicator random variable that $S_j = t$. Let $R_t = \sum_{j=0}^{n-1} Z_j^t$. With this notation, our goal is to show that $R_t = 0$ is unlikely for our choice of some $t = \frac{(1+o(1))\log n}{\log\log n}$ (since if $R_t > 0$ then $\max_{j\in[n]} S_j \geq t$, and hence $\mathbf{Pr}\left[\max_{j\in[n]} S_j \geq t\right] \geq \mathbf{Pr}[R_t > 0]$). We use the second moment method relying on a standard implication of Chebyshev's inequality,

$$\mathbf{Pr}\left[\max_{j\in[n]} S_j < t\right] \leq \mathbf{Pr}[R_t = 0] \leq \frac{\mathbf{Var}[R_t]}{\mathbf{E}[R_t]^2}. \tag{4}$$

Let us recall that

$$\mathbf{Var}[R_t] = \mathbf{Var}\left[\sum_{j=0}^{n-1} Z_j^t\right] = \sum_{j=0}^{n-1} \mathbf{Var}\left[Z_j^t\right] + \sum_{i,j\in[n],i\neq j} \mathbf{Cov}\left[Z_i^t, Z_j^t\right]. \tag{5}$$

Next, since every Z_j^t is a 0-1 random variable, we obtain the following,

$$\mathbf{Var}\left[Z_j^t\right] = \mathbf{Pr}\left[Z_j^t = 1\right] \cdot \mathbf{Pr}\left[Z_j^t = 0\right] \leq \mathbf{Pr}\left[Z_j^t = 1\right] = \mathbf{E}\left[Z_j^t\right]. \tag{6}$$

Our main technical claim is that the covariance of random variables Z_j^t, Z_i^t is small. Although the proof of Lemma 10 is the *main technical contribution* of this section, for clarity of presentation, we defer its proof to Section 5.

Lemma 10. *Let $t \leq O(\log n)$. Then, the following holds for any $i \neq j$, $i,j \in [n]$:*

$$\mathbf{Cov}\left[Z_i^t, Z_j^t\right] = \mathbf{E}\left[Z_i^t \cdot Z_j^t\right] - \mathbf{E}\left[Z_i^t\right] \cdot \mathbf{E}\left[Z_j^t\right] \leq o(1) \cdot \mathbf{E}\left[Z_i^t\right] \cdot \mathbf{E}\left[Z_j^t\right]. \tag{7}$$

Therefore, if we combine (6) and Lemma 10 in identity (5), then (assuming $t \leq O(\log n)$)

$$\begin{aligned}\mathbf{Var}[R_t] &= \sum_{j=0}^{n-1} \mathbf{Var}\left[Z_j^t\right] + \sum_{i,j\in[n],i\neq j} \mathbf{Cov}\left[Z_i^t, Z_j^t\right] \leq \sum_{j=0}^{n-1} \mathbf{E}\left[Z_j^t\right] + o(1) \sum_{i,j\in[n],i\neq j} \mathbf{E}\left[Z_i^t\right] \mathbf{E}\left[Z_j^t\right] \\ &= \mathbf{E}[R_t] + o(1) \cdot \mathbf{E}[R_t]^2.\end{aligned}$$

If we plug this into (4), we will get the following (assuming $t \leq O(\log n)$),

$$\mathbf{Pr}[R_t = 0] \leq \frac{\mathbf{Var}\,[R_t]}{\mathbf{E}[R_t]^2} \leq \frac{1}{\mathbf{E}\,[R_t]} + o(1). \tag{8}$$

Therefore, if for some $\varsigma > 0$ we have $\mathbf{E}[R_t] \geq \varsigma$ (with $t \leq O(\log n)$) then the bound above yields $\mathbf{Pr}\left[\max_{i\in[n]} S_i < t\right] \leq \frac{1}{\varsigma} + o(1)$. Hence we can combine this with (A1) to obtain $\mathbf{E}[R_t] = \sum_{j=0}^{n-1}\mathbf{E}\left[Z_j^t\right] = \sum_{j=0}^{n-1}\mathbf{Pr}\left[S_j = t\right] > \frac{n}{2et!}$, which is $\omega(1)$ for any t such that $t! = o(n)$. This in particular holds for some $t = \frac{(1+o(1))\log n}{\log\log n}$, and thus concludes Lemma 9. ∎

Remark 11. A reader may notice a close similarity of the problem of estimating $\max_{i\in[n]} S_i$ to the maximum load problem for balls and bins, where one allocates n balls into n bins i.u.r. Indeed, random variables $S_0, \ldots, S_{n-1}$ have similar distribution to the random variables $B_0, \ldots, B_{n-1}$, where B_i represents the number of balls allocated to bin i. However, the standard approaches used in the analysis of balls-and-bins processes seem to be more complicated in our setting. The main reason is that while every single random variable S_i has approximately Poisson distribution with mean 1, as has B_i, the analysis of $\max_{i\in[n]} S_i$ is more complicated than the analysis of $\max_{i\in[n]} B_i$ because of the intricate *correlation* of random variables $S_0, \ldots, S_{n-1}$. For example, one standard approach to show that $\max_{i\in[n]} B_i \geq \frac{(1+o(1))\log n}{\log\log n}$ with high probability relies on the fact that the load of a set of bins B_i with $i \in I$ decreases if we increase the load of bins B_j with $j \in J$, $I \cap I = \emptyset$. However, the same property holds only *approximately* for $S_0, \ldots, S_{n-1}$ (and in fact, the $o(1)$ error term in Lemma 10 corresponds to this notion of "approximately"; for balls and bins the covariance is known to be always non-positive). To see the difficulty (see also the classic reference for permutations [14, chapters 7–8]), notice that, for example, if $\sigma(i) = i + \ell$ then we cannot have $\sigma(i+1) = i + \ell$, meaning that there is a special correlation between S_ℓ (which counts i with $\sigma(i) = i + \ell$) and $S_{\ell-1}$ (which counts i with $\sigma(i+1) = i + \ell$). In particular, from what we can see, random variables $S_0, \ldots, S_{n-1}$ are not negatively associated [7]. In a similar way, we do not expect the Poisson approximation framework from [1] (see also [12, chapter 5.4]) to work here. Our approach is therefore closer to the standard second moment method, see, for example, [2, chapter 3] and [13].

5 | PROOF OF LEMMA 10: BOUNDING THE COVARIANCE OF Z_i^t AND Z_j^t

The main technical part of the analysis of the lower bound for the *needle in a haystack* problem in Section 4 (see Theorem 7) relies on the proof of Lemma 9. This proof, in turn, is quite simple except for one central claim, Lemma 10, bounding the covariance of Z_i^t and Z_j^t. The proof of Lemma 10 is rather lengthy, and therefore for the convenience of the reader the proofs of some lemmas are deferred to Section A.

Let Z_j^t be the indicator random variable that $S_j = t$. Since Z_i^t and Z_j^t are 0-1 random variables, we have $\mathbf{E}\left[Z_i^t \cdot Z_j^t\right] = \mathbf{Pr}\left[S_i = t, S_j = t\right]$, $\mathbf{E}\left[Z_i^t\right] = \mathbf{Pr}[S_i = t]$ and $\mathbf{E}\left[Z_j^t\right] = \mathbf{Pr}\left[S_j = t\right]$. Since $\mathbf{Pr}[S_i = t] = \mathbf{Pr}\left[S_j = t\right] = \frac{u(n-t)}{et!} = \frac{1+o(1)}{et!}$ by (A1), to complete the proof of Lemma 10, we only have to show that, for $i \neq j$,

$$\mathbf{Pr}\left[S_i = t, S_j = t\right] \leq (1 + o(1))\frac{1}{(et!)^2}. \tag{9}$$

We will prove this claim with Lemma 19 in Section 5.2.4 below.

5.1 | Notation and key intuitions

For any set $I \subseteq [n]$ and any integer $\ell \in [n]$, let $\mathcal{F}_{I,\ell} = \{\sigma \in \mathbb{S}_n : \sigma(i) = i + \ell \pmod n \text{ iff } i \in I\}$ and $\mathcal{F}^*_{I,\ell} = \{\sigma \in \mathbb{S}_n : \forall_{i\in I}\ \sigma(i) = i + \ell \pmod n\}$. Notice that $\mathcal{F}_{I,\ell} \subseteq \mathcal{F}^*_{I,\ell}$. Further, $|\mathcal{F}_{I,\ell}| = D_{n-t,0}$ where

$t = |I|$, and

$$\mathbf{Pr}[S_i = t] = \frac{|\bigcup_{I\subseteq[n],|I|=t} \mathcal{F}_{I,i}|}{n!} = \frac{\sum_{I\subseteq[n],|I|=t} |\mathcal{F}_{I,i}|}{n!} = \frac{\binom{n}{t} D_{n-t,0}}{n!}.$$

Next, with this notation and for $i \neq j$, we also have

$$\mathbf{Pr}[S_i = t, S_j = t] = \frac{1}{n!}\Big|\bigcup_{I,J\subseteq[n],|I|=|J|=t} \mathcal{F}_{I,i} \cap \mathcal{F}_{J,j}\Big| = \frac{1}{n!}\sum_{I,J\subseteq[n],|I|=|J|=t} |\mathcal{F}_{I,i} \cap \mathcal{F}_{J,j}|.$$

Notice that in the sum above one can restrict attention just to $I \cap J = \emptyset$, since $\mathcal{F}_{I,i} \cap \mathcal{F}_{J,j} = \emptyset$ otherwise. In view of this, our goal is to estimate $|\mathcal{F}_{I,i} \cap \mathcal{F}_{J,j}|$ for disjoint sets $I, J \subseteq [n]$.

In what follows, we will consider sets S_i and S_j with $i = 0$ and $j = s$ for some $s \in [n] \setminus \{0\}$. By symmetry, we can consider the first shift to be 0 without loss of generality; s is an arbitrary non-zero value. As required in our analysis (see Lemma 10), we will consider $t \leq O(\log n)$.

Our approach now is to focus on a typical pair I and J, and consider some atypical pairs separately. We will show in Lemma 13 that almost all pairs of disjoint sets I and J are so-called *compatible for shift s*. As a result, the contribution of pairs I and J that are not compatible for s is negligible, and so we will focus on pairs compatible for s. Then, for the pair of indices I and J we will estimate $|\mathcal{F}_{I,i} \cap \mathcal{F}_{J,j}|$ using the Principle of Inclusion-Exclusion. For that, we must consider the contributions of all possible sets $K \subseteq [n] \setminus (I \cup J)$ to the set of permutations in $\mathcal{F}^*_{I,i} \cap \mathcal{F}^*_{J,j}$. As before, contributions of some sets are difficult to be captured and so we will show in Lemma 15 that almost all sets $K \subseteq [n] \setminus (I \cup J)$ are so-called *feasible for I, J, and s*. As a result, the contribution of sets K that are not feasible for I, J, and s is negligible, and so we will focus on sets that are feasible for I, J, and s. The final simplification follows from the fact that we do not have to consider all such sets K, but only small sets K, of size $O(\log n)$. Once we have prepared our framework, we can use the Principle of Inclusion-Exclusion to estimate $|\bigcup_{I,J\subseteq[n],|I|=|J|=t} \mathcal{F}_{I,i} \cap \mathcal{F}_{J,j}|$ in Lemmas 18 and 19.

5.2 | The analysis

For an integer ℓ and subset $L \subseteq [n]$, we use $L + \ell$ to denote the set of elements in L shifted by ℓ, in arithmetic modulo n, that is, $L + \ell = \{i + \ell \pmod n : i \in L\}$. Similarly, $L - \ell = \{i - \ell \pmod n : i \in L\}$.

Let $\Phi_{0,s}(I,J) = \mathcal{F}_{I,0} \cap \mathcal{F}_{J,s} = \{\sigma \in \mathbb{S}_n : \sigma(i) = i \text{ iff } i \in I \text{ and } \sigma(j) = j + s \pmod n \text{ iff } j \in J\}$. Let $\Phi^*_{0,s}(I,J) = \mathcal{F}^*_{I,0} \cap \mathcal{F}^*_{J,s} = \{\sigma \in \mathbb{S}_n : \forall_{i\in I}\ \sigma(i) = i \text{ and } \forall_{j\in J}\ \sigma(j) = j + s \pmod n\}$.

It is easy to compute the size of $\Phi^*_{0,s}(I,J)$. Notice first that if $I \cap J \neq \emptyset$ or $I \cap (J + s) \neq \emptyset$, then $\Phi^*_{0,s}(I,J) = \Phi_{0,s}(I,J) = \emptyset$. Otherwise, if $I \cap J = \emptyset$ and $I \cap (J + s) = \emptyset$, then $|\Phi^*_{0,s}(I,J)| = (n - |I \cup J|)!$ (see also 12).

However, our main goal, to compute the size of $\Phi_{0,s}(I,J)$, is significantly more complicated, as this quantity cannot be reduced to an intersection test and a simple formula over n, $|I|$, $|J|$, and s.

5.2.1 | Disjoint sets $I \subseteq [n]$ and $J \subseteq [n] \setminus I$ compatible for shift s

Let I and J be two arbitrary subsets of $[n]$ of size t. We say *I and J are compatible for shift s* if the four sets I, J, $I - s$, and $J + s$ are all pairwise disjoint.

Lemma 12. *If I and J are compatible for shift s, then $\Phi_{0,s}(I,J) \neq \emptyset$ and $|\Phi^*_{0,s}(I,J)| = (n - |I \cup J|)!$.*

Proof. If I and J are compatible for shift s then any permutation $\sigma \in \mathbb{S}_n$ with $\sigma(i) = i$ for all $i \in I$, $\sigma(j) = j + s \pmod n$ for all $j \in J$ and complemented by an arbitrary permutation $[n] \setminus (I \cup J)$ is in $\Phi^*_{0,s}(I, J)$. Hence the claim follows from the fact that since I, J, and $J + s$ are pairwise disjoint, such permutations always exist. ∎

The following lemma shows that almost all pairs of disjoint sets of size $t \le O(\log n)$ are compatible (see A.2 for a proof).

Lemma 13. *Let s be an arbitrary nonzero integer in $[n]$. If we choose two disjoint sets $I, J \subseteq [n]$ of size t i.u.r., then the probability that I and J are compatible for shift s is at least $\left(1 - \frac{4t}{(n-2t)}\right)^{2t}$. In particular, if $t \le O(\log n)$, then this probability is at least $1 - O\left(\frac{\log^2 n}{n}\right)$.*

Because of Lemma 13, our goal will be to compute the sizes of sets $\Phi_{0,s}(I, J)$ only for compatible sets I and J. For given disjoint sets I and J compatible for shift s, we will consider all sets $K \subseteq [n] \setminus (I \cup J)$, and their contributions to $|\Phi^*_{0,s}(I, J)|$ using the Principle of Inclusion-Exclusion.

5.2.2 | Properties of sets $K \subseteq [n]$ feasible for I, J, and s

Define $\mathcal{P}_{I,J,0,s}(K) = \{\sigma \in \Phi^*_{0,s}(I, J) : \text{ for every } \ell \in K, \sigma(\ell) \in \{\ell, \ell + s \pmod n\}\}$. While it is difficult to study $\mathcal{P}_{I,J,0,s}(K)$ for all sets $K \subseteq [n] \setminus (I \cup J)$, we will focus our attention only on subsets with some good properties. We call a *set $K \subseteq [n]$ feasible for I, J, and s*, if I and J are compatible for shift s, $K \cap (K + s) = \emptyset$, and $K \cap (I \cup J \cup (I - s) \cup (J + s)) = \emptyset$.

To justify this definition, we begin with the following simple lemma (see A.3 for a proof).

Lemma 14. *If $K \subseteq [n]$ is feasible for I, J, and s, then $|\mathcal{P}_{I,J,0,s}(K)| = 2^{|K|}(n - |I \cup J \cup K|)!$.*

Next, similarly to Lemma 13, we argue that almost all suitably small sets are feasible for pairs of disjoint small sets (see A.4 for a simple proof).

Lemma 15. *Let s be an arbitrary non-zero integer in $[n]$. Let I and J be a pair of compatible sets for s with $|I| = |J| = t$. Let k be a positive integer with $2k \le n - 4t$. If we choose set $K \subseteq [n] \setminus (I \cup J)$ of size k i.u.r., then the probability that K is feasible for I, J, and s is at least $\left(1 - \frac{2t+k}{n-2t-k}\right)^k$.*

In particular, if $t, k \le O(\log n)$, then this probability is at least $1 - O\left(\frac{\log^2 n}{n}\right)$.

5.2.3 | Approximating $|\Phi_{0,s}(I, J)|$ for compatible sets I, J for s

In this section we will complete our analysis to provide a tight bound for the size of $\Phi_{0,s}(I, J)$ for any pair I and J of sets compatible for shift s with $|I| = |J| \le O(\log n)$. Our analysis relies on properties of sets feasible for I, J, and s, as proven in Lemmas 14 and 15.

We begin with two auxiliary claims (for simple proofs, see Appendices A.5 and A.6). For both, let r be the smallest integer such that $2r \ge \log_2 n$ and let $t = |I| = |J| \le O(\log n)$.

Claim 16.

$$\sum_{k=1}^{2r} (-1)^{k+1} \sum_{\substack{K \subseteq [n] \setminus (I \cup J), |K| = k \\ K \text{ feasible for } I, J, \text{ and } s}} |\mathcal{P}_{I,J,0,s}(K)| \ge \left(1 - O\left(\frac{\log^2 n}{n}\right)\right)(n - 2t)!\,(1 - e^{-2}). \tag{10}$$

Claim 17.

$$\sum_{k=1}^{2r}(-1)^{k+1}\sum_{\substack{K\subseteq[n]\setminus(I\cup J),|K|=k\\ K \text{ not feasible for } I,\ J,\text{ and } s}}|\mathcal{P}_{I,J,0,s}(K)|\geq -O\left(\frac{\log^2 n}{n}\right)(n-2t)!.$$

To approximate the size of $\Phi_{0,s}(I,J)$ for sets I and J compatible for shift s, we first notice that

$$\Phi_{0,s}(I,J)=\Phi^*_{0,s}(I,J)\setminus\bigcup_{\ell\in[n]\setminus(I\cup J)}\mathcal{P}_{I,J,0,s}(\{\ell\}). \tag{11}$$

Therefore, since we know that $|\Phi^*_{0,s}(I,J)|=(n-(|I|+|J|))!$ by (12), we only have to approximate $|\bigcup_{\ell\in[n]\setminus(I\cup J)}\mathcal{P}_{I,J,0,s}(\{\ell\})|$. We need a good lower bound.

We compute $|\bigcup_{\ell\in[n]\setminus(I\cup J)}\mathcal{P}_{I,J,0,s}(\{\ell\})|$ using the Principle of Inclusion-Exclusion:

$$\begin{aligned}\left|\bigcup_{\ell\in[n]\setminus(I\cup J)}\mathcal{P}_{I,J,0,s}(\{\ell\})\right| &= \sum_{K\subseteq[n]\setminus(I\cup J),K\neq\emptyset}(-1)^{|K|+1}\left|\bigcap_{\ell\in K}\mathcal{P}_{I,J,0,s}(\{\ell\})\right|\\ &= \sum_{K\subseteq[n]\setminus(I\cup J),K\neq\emptyset}(-1)^{|K|+1}\left|\mathcal{P}_{I,J,0,s}(K)\right|\\ &= \sum_{k=1}^{n-(|I|+|J|)}(-1)^{k+1}\sum_{K\subseteq[n]\setminus(I\cup J),|K|=k}\left|\mathcal{P}_{I,J,0,s}(K)\right|.\end{aligned}$$

Since computing $|\mathcal{P}_{I,J,0,s}(K)|$ for arbitrary nonempty sets $K\subseteq[n]\setminus(I\cup J)$ is difficult, we make further simplifications by restricting our attention to *small* sets K which are *feasible for I, J, and s*. For that, we need to show that by restricting only to small sets K easible for I, J, and s, we will not make too big errors in the calculations.

Let r be the smallest integer such that $2r\geq\log_2 n$. We can use the Bonferroni inequality [3] to obtain the following,

$$\begin{aligned}\left|\bigcup_{\ell\in[n]\setminus(I\cup J)}\mathcal{P}_{I,J,0,s}(\{\ell\})\right| &\geq \sum_{k=1}^{2r}(-1)^{k+1}\sum_{K\subseteq[n]\setminus(I\cup J),|K|=k}\left|\mathcal{P}_{I,J,0,s}(K)\right|\\ &= \sum_{k=1}^{2r}(-1)^{k+1}\left(\sum_{\substack{K\subseteq[n]\setminus(I\cup J),|K|=k\\ K \text{ feasible for } I,\ J,\text{ and } s}}\left|\mathcal{P}_{I,J,0,s}(K)\right|+\sum_{\substack{K\subseteq[n]\setminus(I\cup J),|K|=k\\ K \text{ not feasible for } I,\ J,\text{ and } s}}\left|\mathcal{P}_{I,J,0,s}(K)\right|\right)\\ &\geq -O\left(\frac{\log^2 n}{n}\right)(n-2t)!+\left(1-O\left(\frac{\log^2 n}{n}\right)\right)(n-2t)!\,(1-e^{-2})\\ &= \left(1-O\left(\frac{\log^2 n}{n}\right)\right)(n-2t)!\,(1-e^{-2}),\end{aligned} \tag{12}$$

where the last inequality follows from the auxiliary Claims 16 and 17.

If we combine (11) and (12), then we get the following lemma.

Lemma 18. *If I and J are compatible for shift s and $|I|=|J|=t=O(\log n)$, then*

$$|\Phi_{0,s}(I,J)|=|\Phi^*_{0,s}(I,J)|-\left|\bigcup_{\ell\in[n]\setminus(I\cup J)}\mathcal{P}_{I,J,0,s}(\{\ell\})\right|\leq\frac{(n-2t)!}{e^2}\left(1+O\left(\frac{\log^2 n}{n}\right)\right).$$

Proof. Indeed, by (11), we have

$$|\Phi_{0,s}(I,J)| = |\Phi^*_{0,s}(I,J)| - \Big|\bigcup_{\ell\in[n]\setminus(I\cup J)} \mathcal{P}_{I,J,0,s}(\{\ell\})\Big|,$$

by Lemma 12 we get

$$|\Phi^*_{0,s}(I,J)| = (n-(|I|+|J|))!,$$

and by (12) we have

$$\Big|\bigcup_{\ell\in[n]\setminus(I\cup J)} \mathcal{P}_{I,J,0,s}(\{\ell\})\Big| \geq \left(1-O\left(\frac{\log^2 n}{n}\right)\right)(n-2t)!\,(1-e^{-2}).$$

Putting these three bounds together yields the promised bound. ∎

5.2.4 | Completing the proof of inequality (9)

Now, with (18) at hand, we are ready to complete our analysis in the following lemma.

Lemma 19. *For any $i,j\in[n]$, $i\neq j$, and for $t\leq O(\log n)$, we have,*

$$\mathbf{Pr}\big[S_i=t, S_j=t\big] \leq \left(1+O\left(\frac{\log^2 n}{n}\right)\right)\frac{1}{(et!)^2}.$$

Proof. Without loss of generality we assume that $i=0$ and $j\in[n]\setminus\{0\}$.

First, let us recall the following

$$\sum_{I,J\subseteq[n],|I|=|J|=t,I\cap J=\emptyset}\Big|\mathcal{F}_{I,0}\cap\mathcal{F}_{J,j}\Big| = \sum_{I,J\subseteq[n],|I|=|J|=t,I\cap J=\emptyset}\Big|\Phi_{0,j}(I,J)\Big|$$
$$= \sum_{\substack{I,J\subseteq[n],|I|=|J|=t,I\cap J=\emptyset\\ I \text{ and } J \text{ not compatible for } j}}\Big|\Phi_{0,j}(I,J)\Big| + \sum_{\substack{I,J\subseteq[n],|I|=|J|=t\\ I \text{ and } J \text{ compatible for } j}}\Big|\Phi_{0,j}(I,J)\Big|.$$

We see that if I and J are *not* compatible for shift j and $I\cap J=\emptyset$, then $|\Phi_{0,s}(I,J)|\leq(n-2t)!$ (since once we have fixed $2t$ positions, we can generate at most $(n-2t)!$ distinct n-permutations). Further, by (18), we know that if I and J are compatible for shift j, then $|\Phi_{0,s}(I,J)|\leq\frac{(n-2t)!}{e^2}\left(1+O\left(\frac{\log^2 n}{n}\right)\right)$. Next, we notice that by (13), we have,

$$\Big|\{I,J\subseteq[n]:|I|=|J|=t, I\cap J=\emptyset \text{ and } I,J \text{ not compatible for } j\}\Big|$$
$$= O\left(\frac{\log^2 n}{n}\right)\Big|\{I,J\subseteq[n]:|I|=|J|=t, I\cap J=\emptyset\}\Big| = O\left(\frac{\log^2 n}{n}\right)\binom{n}{t}\binom{n-t}{t}.$$

This immediately gives,

$$\sum_{\substack{I,J\subseteq[n],|I|=|J|=t,I\cap J=\emptyset\\ I \text{ and } J \text{ not compatible for } j}}\Big|\Phi_{0,j}(I,J)\Big| \leq O\left(\frac{\log^2 n}{n}\right)\binom{n}{t}\binom{n-t}{t}(n-2t)! = O\left(\frac{\log^2 n}{n}\right)\frac{n!}{(t!)^2}$$

and

$$\sum_{\substack{I,J\subseteq[n],|I|=|J|=t\\ I \text{ and } J \text{ compatible for } j}} \left|\Phi_{0,j}(I,J)\right| \le \binom{n}{t}\binom{n-t}{t}\frac{(n-2t)!}{e^2}\left(1+O\left(\frac{\log^2 n}{n}\right)\right)$$
$$= \left(1+O\left(\frac{\log^2 n}{n}\right)\right)\frac{n!}{(et!)^2}.$$

Therefore,

$$\sum_{\substack{I,J\subseteq[n],I\cap J=\emptyset\\ |I|=|J|=t}} \left|\mathcal{F}_{I,0}\cap\mathcal{F}_{J,j}\right| = \sum_{\substack{I,J\subseteq[n],|I|=|J|=t,I\cap J=\emptyset\\ I \text{ and } J \text{ not compatible for } j}} \left|\Phi_{0,j}(I,J)\right| + \sum_{\substack{I,J\subseteq[n],|I|=|J|=t\\ I \text{ and } J \text{ compatible for } j}} \left|\Phi_{0,j}(I,J)\right|$$
$$\le \left(1+O\left(\frac{\log^2 n}{n}\right)\right)\frac{n!}{(et!)^2}.$$

Hence, we can conclude that for $i \neq j$ we have,

$$\mathbf{Pr}\left[S_i = t, S_j = t\right] = \frac{1}{n!}\sum_{\substack{I,J\subseteq[n],I\cap J=\emptyset\\ |I|=|J|=t}} |\mathcal{F}_{I,i}\cap\mathcal{F}_{J,j}| \le \left(1+O\left(\frac{\log^2 n}{n}\right)\right)\frac{1}{(et!)^2}.$$

■

6 | ANALYSIS OF THE *COMMUNICATION IN THE LOCKER ROOM* SETTING

A lower bound for the success probability in the *locker room* problemis provided by a straightforward adaptation of the *shift strategy*: Alice enters her message relaying the most common shift $\mathfrak{h}$ to locker 0, then Bob opens locker 0 and uses Alice's message to check location $(\mathfrak{s}+\mathfrak{h}) \bmod n$ for his card. This strategy ensures a success probability of $\frac{(1+o(1))\log n)}{n\log\log n}$.

As in Sections 2 and 3, we will consider the case when $\mathfrak{s}$ is chosen i.u.r. from [n] (see Section 2.1). In order to obtain an upper bound for the success chance in the *locker room* problem, we shall introduce some intermediate settings, or "protocols". In the *CLR* protocol, the rules which govern the *locker room* problem, Alice views the contents of all the lockers, interchanges the contents of two lockers, then Bob is given a number and can open two lockers in search of it. In the *NH* protocol, the rules which govern the *needle in a haystack* game, Alice views the contents of all the lockers, communicates a message of length $\log n$ to Bob, then Bob is given a number and can open one locker in search of it. Moreover, we could append the modifier "-with-r-bits" to NH, which substitutes r for $\log n$ in the above description.

We write $\mathbf{Pr}[\mathcal{V}(\mathcal{P})]$ for the optimal probability of success in protocol $\mathcal{P}$ and $\mathbf{Pr}\left[\mathcal{V}(\mathbb{C},\mathcal{P})\right]$ for the probability of success for strategy $\mathbb{C}$ in protocol $\mathcal{P}$. For example, we have already shown that $\mathbf{Pr}[\mathcal{V}(NH)] = \frac{(1+o(1))\log n}{n\log\log n}$.

Lemma 20. $\mathbf{Pr}[\mathcal{V}(\text{CLR})] \le \mathbf{Pr}\left[\mathcal{V}(\text{NH-with-}(4\log n)\text{-bits})\right]$.

Proof. We will interpolate between CLR and NH-with-$(4\log n)$-bits with two other protocols.

In the protocol *CLR0*, Alice views the contents of all the lockers and interchanges the contents of two lockers, then Bob is given a number and can open two lockers in search of it, and he can recognize upon seeing the content of the first locker whether it has been altered by Alice.

In the protocol *CLR1*, Alice views the contents of all the lockers, interchanges the contents of two lockers, and leaves these two lockers open with their contents visible to Bob, then Bob is given a number and can open one locker in search of it.

Also, let *Sim* be the strategy in *NH-with-*$(4\log n)$*-bits* in which Alice uses her message to communicate to Bob the cards whose positions she would exchange, and the positions of these cards, if she encountered the permutation σ while working in the *CLR1* protocol, simulating an optimal strategy $\mathbb{C}$ in *CLR1*. Since this is an ordered quadruple in $[n]^4$, it can indeed be communicated in at most $4\log n$ bits.

The proof is in four parts:

(i) $\mathbf{Pr}[\mathcal{V}(CLR)] \le \mathbf{Pr}[\mathcal{V}(CLR0)]$,
(ii) $\mathbf{Pr}[\mathcal{V}(CLR0)] \le \mathbf{Pr}[\mathcal{V}(CLR1)] + O\left(\frac{1}{n}\right)$,
(iii) $\mathbf{Pr}[\mathcal{V}(CLR1)] \le \mathbf{Pr}\left[\mathcal{V}(Sim,\ NH\text{-}with\text{-}(4\log n)\text{-}bits)\right]$,
(iv) $\mathbf{Pr}\left[\mathcal{V}(Sim,\ NH\text{-}with\text{-}(4\log n)\text{-}bits)\right] \le \mathbf{Pr}\left[\mathcal{V}(NH\text{-}with\text{-}(4\log n)\text{-}bits)\right]$.

(i), (iii), (iv) are straightforward and so we only have to show (ii). Let p_t be the maximum probability that Bob finds his target in the t^{th} locker that he opens, $t \in \{1, 2\}$.

Firstly, we bound p_1. Suppose that Alice and Bob have settled on a specific strategy. Let $e_{x,w}$ be the probability that σ is such that Alice's transposition sends the card x to locker w. Evidently, $0 \le e_{x,w} \le \frac{n-1}{n}$ for all $x, w \in [n]$ and $\sum_{x,w\in[n]} e_{x,w} \le 2$.

Having received his number $\mathfrak{s}$, Bob has to open a specific locker, let us say $b = b(\mathfrak{s})$. The probability that Bob happens upon the card $\mathfrak{s}$ in the locker b is at most $e_{\mathfrak{s},b(\mathfrak{s})} + \frac{1}{n}$ (either Alice substitutes the content of $b(\mathfrak{s})$ for $\mathfrak{s}$, or the content of $b(\mathfrak{s})$ is initially $\mathfrak{s}$ and Alice does not interfere). Thus, choosing $\mathfrak{s}$ i.u.r. from $[n]$, the probability that Bob finds $\mathfrak{s}$ at his first try is at most $\frac{1}{n}\sum_{\mathfrak{s}\in[n]}\left(e_{\mathfrak{s},b(\mathfrak{s})} + \frac{1}{n}\right) < \frac{3}{n} = O\left(\frac{1}{n}\right)$.

Then, we bound p_2. If Bob opens first one of the lockers whose contents have been altered by Alice, then there is one remaining locker for him to open, and he has at most as much information as in the *CLR0* protocol. Hence, in this case, $p_2 \le \mathbf{Pr}[\mathcal{V}(CLR0)]$.

Alternatively, Bob first opens one of the lockers whose contents have not been altered by Alice. This requires a more detailed analysis of the *CLR0* protocol.

Alice's choice of a transposition is informed solely by the initial permutation σ of the cards inside the lockers. Hence, there should be a function $a : \mathbb{S}_n \to \binom{[n]}{2}$ which directs Alice to a pair of lockers. Then, Bob's choice of a first locker to open is informed only by his target, and is given by the function $b : [n] \to [n]$. Finally, Bob chooses his second locker by considering his target and the content of the first locker, so there should be a function $b' : \{0, 1\} \times [n]^2 \to [n]$ which directs Bob to his second locker, where the binary factor distinguishes whether Bob's first locker has had its content altered by Alice or not. The strategy which Alice and Bob employ in the *CLR0* protocol can therefore be identified with a triple $[a, b, b']$.

Let $F_w = b^{-1}(w)$ be the event that Bob opens the w^{th} locker first, so $\mathbf{Pr}[F_w] = \frac{|b^{-1}(w)|}{n}$. Let G_y be the event that the initial content of Bob's first locker is y, so $\mathbf{Pr}\left[G_y\right] = \frac{1}{n}$. If $s(y, w) \subseteq \mathbb{S}_n$ is the set of permutations which map w to y, and $E_{u,v} = a^{-1}(\{u, v\})$ is the event that Alice transposes the contents of the u^{th} and v^{th} lockers, then $\mathbf{Pr}\left[E_{u,v}|F_w \cap G_y\right] = \frac{|a^{-1}(\{u,v\})\cap s(y,w)|}{(n-1)!}$.

The probability that Bob finds his target in his second attempt given that his first locker was not altered by Alice is

$$p_2 \le \sum_{\substack{u,v,w,y\in[n]\\ u,v,w \text{ distinct}}} \mathbf{Pr}\left[E_{u,v}|F_w \cap G_y\right] \cdot \mathbf{Pr}[F_w] \cdot \mathbf{Pr}\left[G_y\right] \cdot \mathbf{Pr}\left[\mathcal{V}(CLR0)|E_{u,v} \cap F_w \cap G_y\right] \ .$$

Observe that

$$\mathbf{Pr}\left[\mathcal{V}(CLR0)|E_{u,v}\cap F_w\cap G_y\right]\le\frac{(n-2)!}{\left|\left(\mathbb{S}_n\setminus\bigcup_{\ell\in[n]}a^{-1}(\{w,\ell\})\right)\cap s(y,w)\right|}+\frac{2}{n}\,.$$

This holds because, barring the $\frac{2}{n}$ probability for Bob's target to be in a locker whose content was changed by Alice, Bob is only going to find his target in his second locker if the permutation σ maps both w to y and Bob's second locker to his target. There are exactly $(n-2)!$ such permutations, which yields the numerator. For the denominator, when Bob opens the locker w and views the card inside, he sees that its content is y and that it has not been touched by Alice, so he knows that σ is a permutation which maps w to y and which does not prompt Alice to transpose y with some other card, and there are exactly $\left|\left(\mathbb{S}_n\setminus\bigcup_{\ell\in[n]}a^{-1}(\{w,\ell\})\right)\cap s(y,w)\right|$ such permutations.

Also, note that

$$\bigcup_{\substack{u,v\in[n]\\u,v,w\text{ distinct}}}(a^{-1}(\{u,v\})\cap s(y,w))=\left(\mathbb{S}_n\setminus\bigcup_{\ell\in[n]}a^{-1}(\{w,\ell\})\right)\cap s(y,w)\Rightarrow$$

$$\sum_{\substack{u,v\in[n]\\u,v,w\text{ distinct}}}|a^{-1}(\{u,v\})\cap s(y,w)|=\left|\left(\mathbb{S}_n\setminus\bigcup_{\ell\in[n]}a^{-1}(\{w,\ell\})\right)\cap s(y,w)\right|.$$

Combining the above, we obtain that

$$\begin{aligned}p_2&\le\sum_{\substack{u,v,w,y\in[n]\\u,v,w\text{ distinct}}}\frac{1}{n}\cdot\frac{|a^{-1}(\{u,v\})\cap s(y,w)|}{(n-1)!}\cdot\frac{|b^{-1}(w)|}{n}\left(\mathbf{Pr}\left[\mathcal{V}(CLR0)|E_{u,v}\cap F_w\cap G_y\right]+\frac{2}{n}\right)\\&\le\sum_{w,y\in[n]}\frac{1}{n}\cdot\frac{1}{n-1}\cdot\frac{|b^{-1}(w)|}{n}+\frac{2}{n}=\frac{1}{n-1}+\frac{2}{n}.\end{aligned}$$

Thus, in this case, $p_2\le\frac{4}{n}$.

Ultimately, $p_2\le\mathbf{Pr}[\mathcal{V}(CLR1)]+\frac{4}{n}$, and hence $\mathbf{Pr}[\mathcal{V}(CLR0)]\le p_1+p_2\le\mathbf{Pr}[\mathcal{V}(CLR1)]+O\left(\frac{1}{n}\right)$, concluding the proof. ∎

Theorem 21. $\mathbf{Pr}[\mathcal{V}(CLR)]\le\frac{(4+o(1))\log n}{n\log\log n}$.

Proof. We use Lemma 20 along with the fact that $\mathbf{Pr}\left[\mathcal{V}(NH\text{-}with\text{-}(4logn)\text{-}bits)\right]\le\frac{(4+o(1))\log n}{n\log\log n}$, which can be immediately derived from Theorem 22 in Section 7.1 by setting $m=n^4$. ∎

7 | GENERALIZATIONS

There are several natural generalizations of the problem studied in this paper and related questions about properties of random permutations, which we will discuss here.

7.1 | Simple generalization: Longer message

In the *needle in a haystack* problem, when Alice sends the message $\mathfrak{h}$ to Bob, there is no reason why she must choose a number in $[n]$; instead, she could transmit a number $\mathfrak{h} \in [m]$ for an arbitrary integer m. One can easily generalize the analysis from Theorems 5 and 7 in this setting for a large range of m.

Let us denote the maximum attainable sum of intensities received from partitioning $\mathbb{S}_n$ to m parts the *m-field* of $\mathbb{S}_n$, and denote it by $F(n,m)$. Fields are simply diagonal m-fields (fields of the form $F(n,n)$).

We have $F(n,1) = n!$ (yielding a success probability of $\frac{1}{n}$, corresponding to not receiving advice) and $F(n,m) = n \cdot n!$ for every $m \geq n!$ (yielding a success probability of 1, corresponding to obtaining full information). For other values of m we can follow the approach used in Theorem 5. First, notice that there is $\ell = \frac{(1+o(1))\log m}{\log\log m}$, such that $m = o(\ell!)$. Then, using the techniques from the proof of Theorem 5, we obtain for a random variable X recording the contribution of a random permutation to $F(n,m)$ that

$$E[X] = \frac{F(n,m)}{n!} \leq \ell + \sum_{s=1}^{\infty}(\ell+1)^{-s} = \ell + \frac{1}{\ell} = \frac{(1+o(1))\log m}{\log\log m}. \tag{13}$$

By (2), this yields the success probability of $\frac{(1+o(1))\log m}{n\log\log m}$, giving the following theorem.

Theorem 22. *If Alice can choose a number $\mathfrak{h} \in [m]$, then the maximum attainable success probability is at most $\frac{(1+o(1))\log m}{n\log\log m}$. In particular, if $m = \mathrm{poly}(n)$, then the maximum attainable success probability is at most $O\left(\frac{\log n}{n\log\log n}\right)$.*

Since the algorithm given in Theorem 7, using the shift strategy with hint $\mathfrak{h} \in [n]$, has success probability $\Omega\left(\frac{\log n}{n\log\log n}\right)$, Theorem 22 implies that this shift strategy is asymptotically optimal to within a constant factor for any hint $\mathfrak{h}$ which is polynomial in n. A similar conclusion holds also for the communication in the locker room setting: even if Alice leaves Bob a message by altering the contents of a constant number c of lockers rather than just one, this message is $c\log n$ bits long, and hence the success probability is still at most $O\left(\frac{\log n}{n\log\log n}\right)$.

Asymptotic results for several other interesting domains of m could be found in a similar way. However, for super-polynomial domains, the upper bound derived above is far from the lower bound in Theorem 7. Determining some properties of the rate of growth of $F(n,m)$ for fixed n would be a good step towards determining its values. With this in mind, we have the following natural conjecture.

Conjecture 1. *For any fixed n, the function $f(m) = F(n,m)$ is concave.*

7.2 | Optimal strategies

Although we have successfully calculated the maximum field and the maximum success probability for the *needle in a haystack* problem, the problem of determining a characterization of, or even some major properties for, optimal strategies remains. Indeed, the only optimal strategy that we have explicitly described so far is the shift strategy (which is in fact a set of different strategies, since, for permutations which have several $S_{\mathfrak{h}}$'s of maximum size, there are multiple legitimate options for their class). A natural generalization of shift strategies are *latin strategies*; in these, Alice and Bob decide on a $n \times n$ latin square S, and Alice's message indicates the row of S which coincides with σ at the maximum number of places.

We present a couple of interesting questions concerning the optimal strategies for $\mathbb{S}_n$ in *needle in a haystack*.

Conjecture 2. *For every natural number n, there is an optimal strategy for* $\mathbb{S}_n$ *whose parts all contain exactly* $(n-1)!$ *permutations.*

Conjecture 3. *Optimal strategies are exactly the latin strategies.*

7.3 | Alice-In-Chains

Let us explore another specific strategy. The *naive strategy* is to group permutations according to the content of location 0. That is, σ, σ' belong to the same class if and only if $\sigma(0) = \sigma'(0)$. This is a natural strategy to conceive, and it agrees with the common (but erroneous) notion that efficiency in the lockers game cannot be improved beyond $O\left(\frac{1}{n}\right)$. Indeed, straightforward calculations yield a success probability of $\frac{2}{n}$ for the naive strategy in the *needle in a haystack* problem.

Intuitive though it is, in the preceding sections we have proven the naive strategy to be suboptimal. In fact, the naive strategy fails to fully utilize the possibilities provided by the problem's framework. In this subsection, we show that, with only a minor restriction for our problem, the naive strategy becomes optimal. This demonstrates that strategic efficiency is very sensitive to changes in our assumptions about the *needle in a haystack*.

Suppose that Alice and Bob face a challenge similar to the *needle in a haystack*, but with this restriction: the chosen strategy $\mathbb{C} = \langle C_0, \ldots, C_{n-1} \rangle$ must satisfy

$$\exists_{s\in[n]}\ \forall_{i\in[n]}\ \exists_{h\in[n]}\ \forall_{\sigma\in C_h}\ \sigma(i) \neq s,$$

that is, "there exists a needle s such that for each location i there is a corresponding message h from Alice which tells Bob that s is not in i". We call this the *Alice-In-Chains* (AIC) variant.

Theorem 23. *The naive strategy is optimal in Alice-In-Chains.*

Proof. It is easy to see that the naive strategy satisfies the AIC rules. For instance, we can take $s = 0$, in which case the message $h = 1$ informs Bob that s is not in locker 0, and the message $h = 0$ informs Bob that s is not in locker i for any $i > 0$.

We proceed by induction. For $n \leq 3$, it is easy to see that the naive strategy is optimal, even without the restriction.

Suppose that it is optimal for $n \leq N$. Let $\mathbb{C} = \langle C_0, \ldots, C_N \rangle$ be an optimal strategy for $\mathbb{S}_{N+1}$ in the AIC variant. Without loss of generality, let $s = N$.

Let A_m be the subset of $\mathbb{S}_{N+1}$ which contains every permutation that maps N to m. To bound the field $F_{AIC}(N+1)$, we will try to maximize the sum of the intensities produced by distributing the members of A_m across the $N+1$ classes. That is, we partition each A_m into a collection $C^{(m)} = [A_{m,0}, \ldots, A_{m,N}]$ which maximizes the sum $\sum_{0\leq s,h\leq N} \mathsf{int}(A_{m,h}, s)$. We claim that

$$F_{AIC}(N+1) \leq \sum_{m=0}^{N} \sum_{0\leq s,h\leq N} \mathsf{int}(A_{m,h}, s). \tag{14}$$

To see that, observe that partitioning one set of permutations to several does not decrease the sum of the intensities. Indeed,

$$\mathsf{int}(C_h, s) = \mathsf{mag}(C_h, s, \text{max-mag}(C_h, s)) = \sum_{m=0}^{N} \mathsf{mag}(A_{m,h}, s, \text{max-mag}(C_h, s))$$
$$\leq \sum_{m=0}^{N} \mathsf{mag}(A_{m,h}, s, \text{max-mag}(A_{m,h}, s)) = \sum_{m=0}^{N} \mathsf{int}(A_{m,h}, s).$$

Hence,

$$F_{AIC}(N+1) = \sum_{0 \leq s,h \leq N} \mathsf{int}(C_h, s) \leq \sum_{m=0}^{N} \sum_{0 \leq s,h \leq N} \mathsf{int}(A_{m,h}, s).$$

However, each A_m is a copy of $\mathbb{S}_n$, and one of its parts must be empty (because of the restriction of AIC, and the fact that all of the members of A_m agree on the image of N). Therefore, $\sum_{0 \leq s,h \leq N} \mathsf{int}(A_{m,h}, s) = F_{AIC}(N)$ for all $m \in [N]$, and so (14) yields

$$F_{AIC}(N+1) \leq (N+1) F_{AIC}(N). \tag{15}$$

From our inductive hypothesis, the naive strategy is an optimal strategy for $\mathbb{S}_n$ in the AIC variant, so $F_{AIC}(N) = 2N!$, which from (15) implies $F_{AIC}(N+1) \leq 2(N+1)!$. Since the yield of the naive strategy for $\mathbb{S}_{N+1}$ is exactly $2(N+1)!$, we have that the naive strategy is optimal for $\mathbb{S}_{N+1}$ in the AIC variant.

Remark 24. The above implies that the Alice-In-Chains variant has a maximum attainable probability of $\frac{2}{n}$. It also proves an interesting result about the form of optimal strategies: every optimal strategy in the needle in a haystack setting is such that every element $c \in [n]$ has an image which is present in all of the strategy's classes.

■

ACKNOWLEDGEMENTS

The authors thank Joe Buhler for his many detailed and constructive comments. The authors also thank Richard Stong for providing an alternative proof of Theorem 5 (communicated to us by Buhler), which is the one used in this final version of the article.

FUNDING INFORMATION

Research partially supported by the Centre for Discrete Mathematics and its Applications (DIMAP), by an IBM Faculty Award, by EPSRC award EP/V01305X/1, and by an EPSRC Doctoral Training Partnership.

REFERENCES

1. M. Adler, S. Chakrabarti, M. Mitzenmacher, and L. E. Rasmussen. *Parallel randomized load balancing*. Proc. 27th Annu. ACM Symp. Theory of Computing (STOC), 1995, pp. 238–247.
2. B. Bollobás, Random graphs, 2nd ed., Cambridge University Press, Cambridge, UK, 2001.
3. Carlo Emilio Bonferroni, *Teoria statistica delle classi e calcolo delle probabilità*, Pubbl. R Ist. Sup. Sci. Econ. Commer. Fir. **8** (1936), 3–62.
4. P. Joe Buhler, *Hat tricks*, Math. Intell. **24** (2002), no. 4, 44–49.
5. L. Carter and S. Wagon, *The Mensa correctional institute*, Am. Math. Mon. **125** (2018), no. 4, 306–319.
6. E. Curtin and M. Warshauer, *The locker puzzle*, Math. Intell. **28** (2006), no. 1, 28–31.
7. D. P. Dubhashi and D. Ranjan, *Balls and bins: A study in negative dependence*, Random Struct. Algor. **13** (1998), no. 2, 99–124.

8. Anna Gál and Peter Bro Miltersen. *The cell probe complexity of succinct data structures*. Proc. 30th Annu. Int. Colloquium on Automata, Languages and Programming (ICALP), 2003, 332–344.
9. N. Goyal and M. E. Saks, *A parallel search game*, Random Struct. Algor. **27** (2005), no. 2, 227–234.
10. R. L. Graham, D. E. Knuth, and O. Patashnik, Concrete mathematics: A Foundation for Computer Science, 2nd ed., Addison-Wesley, Reading, MA, 1994.
11. D. E. Knuth, The art of computer programming: Sorting and searching, 2nd ed., Vol **III**, Addison-Wesley, Reading, MA, 1998.
12. M. Mitzenmacher and E. Upfal, Probability and computing: Randomized and probabilistic techniques in algorithms and data analysis, 2nd ed., Cambridge University Press, Cambridge, UK, 2017.
13. M. Raab and A. Steger. *"Balls into bins"—A simple and tight analysis*. Proc. 2nd Int. Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM), 1998, 159–170.
14. J. Riordan, An introduction to combinatorial analysis, John Wiley & Sons, Inc., New York, NY, 1958.
15. P. Winkler, *Names in boxes puzzle*, College Math. J. **37** (2006), no. 4, 260, 285, 289.
16. P. Winkler, Mathematical mind-benders, A K Peters, Ltd., Wellesley, MA, 2007.

How to cite this article: A. Czumaj, G. Kontogeorgiou, and M. Paterson, *Haystack hunting hints and locker room communication*, Random Struct. Algorithms. (2022), 1–25. https://doi.org/10.1002/rsa.21114

APPENDIX A: PROOFS OF AUXILIARY CLAIMS

A.1 | Proof of Lemma 8 (from Section 4)

We present an elementary proof of Lemma 8 (following standard arguments) showing that the expected number of $j \in [n]$ with $S_j \geq \frac{(1+o(1))\log n}{\log\log n}$ is at least one.

Proof of Lemma 8. Let us recall Definition 4 for derangements and r-partial derangements. The probability that a random permutation in $\mathbb{S}_n$ is a derangement is $D_n/n! = \left\lfloor \frac{n!}{e} + \frac{1}{2} \right\rfloor / n! \sim \frac{1}{e}$. Let $u(n) = \left\lfloor \frac{n!}{e} + \frac{1}{2} \right\rfloor / \frac{n!}{e}$ and note that $D_n = u(n)\, n!/e$, that $u(n) = 1 + o(1)$, and $u(n) > 0.9$ for all $n > 1$. Since the permutation $\sigma \in \mathbb{S}_n$ is chosen i.u.r., we have

$$\mathbf{Pr}[S_0 = k] = \frac{D_{n,k}}{n!} = \frac{\binom{n}{k} D_{n-k}}{n!} = \frac{\binom{n}{k} \frac{(n-k)!}{e} u(n-k)}{n!} = \frac{u(n-k)}{ek!} .$$

The same bound can be obtained for S_j for every $j \geq 0$. For any permutation $\sigma \in \mathbb{S}_n$ and any integer $\ell \in [n]$, define the permutation $\sigma_\ell \in \mathbb{S}_n$ given by

$$\sigma_\ell(i) = \sigma(i) + \ell \pmod{n} .$$

For any permutation $\sigma \in \mathbb{S}_n$ and any ℓ, the operator $\sigma \mapsto \sigma_\ell$ is a bijection from $\mathbb{S}_n$ to $\mathbb{S}_n$, and a permutation $\sigma \in \mathbb{S}_n$ with $\ell \in [n]$ has exactly k fixed points if and only if permutation σ_ℓ has exactly k points with $\sigma_\ell(i) = i + \ell \pmod{n}$. Hence for every $j, j' \in [n]$ and $k \in [n]$, we have $\mathbf{Pr}\big[S_j = k\big] = \mathbf{Pr}\big[S_{j'} = k\big]$.

Therefore, for any integers $j \in [n]$ and $k \in [n-2]$,

$$\mathbf{Pr}\big[S_j = k\big] = \frac{u(n-k)}{ek!} > \frac{1}{2ek!}. \tag{A1}$$

Let $k(n)$ be the largest k such that $2ek! \le n$. Then $\mathbf{Pr}\big[S_j = k(n)\big] > 1/n$. Hence, if we let Q_j be the indicator random variable that $S_j = k(n)$, then $\mathbf{Pr}\big[Q_j = 1\big] > 1/n$, and hence $\mathbf{E}\Big[\sum_{j=0}^{n-1} Q_j\Big] = \sum_{j=0}^{n-1} \mathbf{E}\big[Q_j\big] = \sum_{j=0}^{n-1} \mathbf{Pr}\big[Q_j = 1\big] > 1$. Therefore, in expectation, there is at least one value j such that $S_j = k(n)$. It is easy to show that $k(n) = \frac{\log n}{\log\log n}(1 + o(1))$. ∎

A.2 | Proof of Lemma 13 (from Section 5.2.1)

Proof of Lemma 13. I and J are compatible for shift s if sets $I, J, I-s$, and $J+s$ are pairwise disjoint. We will give a construction of sets I and J, each of size t, such that I and J are compatible for shift s.

We begin by selecting t elements from I one by one. We will ensure that sets $I, I-s$, and $I-2s$ are pairwise disjoint. The first element i_1 is arbitrary, and we can select it in n ways. We choose the second element i_2 from $[n] \setminus \{i_1, i_1 - s \pmod n, i_1 - 2s \pmod n\}$ in at least $n-3$ ways, the third element i_3 in at least $n-6$ ways, and so on; since the elements in I can be ordered arbitrarily, the number of choices is at least $\frac{n(n-3)\ldots(n-3(t-1))}{t!}$.

Next, we choose t elements from J. We will ensure that J is pairwise disjoint from sets I and $I-s$, and $J+s$ is pairwise disjoint from sets I and $I-s$; notice that the latter means that J is pairwise disjoint from sets $I-s$ and $I-2s$. The first element j_1 is selected in at least $(n-3t)$ ways, since $j_1 \in [n] \setminus (I \cup I-s \cup I-2s)$ implies that $\{j_1\} \cap (I \cup I-s) = \emptyset$ and $\{j_1 + s \pmod n\} \cap (I \cup I-s) = \emptyset$. Next, we select $j_2 \in [n] \setminus (I \cup I-s \cup I-2s \cup \{j_1, j_1+s \pmod n, j_1 - s \pmod n\})$ to ensure that the constructed I and $J = \{j_1, j_2\}$ are compatible for shift s. Then we select $j_3 \in [n] \setminus (I \cup I-s \cup I-2s \cup \{j_1,j_2\} \cup \{j_1,j_2\}+s \cup \{j_1,j_2\}-s)$ in at least $(n-3(t+2))$ ways, and so on. Since the elements in J can be ordered arbitrarily, the number of choices is $\frac{(n-3t)(n-3(t+1))\ldots(n-3(2t-1))}{t!}$.

Therefore, we have presented a way of selecting at least

$$\frac{n(n-3)\ \ldots\ (n-3(t-1))}{t!} \cdot \frac{(n-3t)(n-3(t+1))\ \ldots\ (n-3(2t-1))}{t!}$$

distinct pairs of sets I and J of size t that are compatible for shift s. This implies that if we choose two disjoint sets $I, J \subseteq [n]$ of size t i.u.r., then the probability that I and J are compatible for shift s is at least

$$\frac{1}{\binom{n}{t}\binom{n-t}{t}} \cdot \frac{n(n-3)\ \ldots\ (n-3(t-1))}{t!} \cdot \frac{(n-3t)(n-3(t+1))\ \ldots\ (n-3(2t-1))}{t!}$$

$$= \prod_{\ell=0}^{2t-1} \frac{(n-3\ell)}{(n-\ell)} = \prod_{\ell=0}^{2t-1} \left(1 - \frac{2\ell}{n-\ell}\right) \ge \left(1 - \frac{4t}{n-2t}\right)^{2t}.$$

Next, we use $\left(1 - \frac{1}{a+1}\right)^a > e^{-1}$ to get $\left(1 - \frac{4t}{n-2t}\right)^{2t} > e^{\frac{-8t^2}{n-6t}}$ and then we use the assumption $t \le O(\log n)$ to get $e^{\frac{-8t^2}{n-6t}} \ge e^{-O(\log^2 n)/n} \ge 1 - O\left(\frac{\log^2 n}{n}\right)$. ∎

A.3 | Proof of Lemma 14 (from Section 5.2.2)

Proof of Lemma 14. Let $\zeta : K \to \{0,1\}$. We call a permutation $\sigma \in \mathbb{S}_n$ consistent with I, J, s, K, and ζ, when

- if $i \in I$ then $\sigma(i)$,

- if $j \in J$ then $\sigma(j) = j + s \pmod n$, and
- if $k \in K$ then $\sigma(k) = k + \zeta(k) \cdot s \pmod n$.

Let $\mathsf{PC}^{\zeta}_{I,J,0,s}(K)$ be the set of all permutations consistent with I, J, s, K, and ζ. We notice that $\mathcal{P}_{I,J,0,s}(K)$ is the union over all $2^{|K|}$ functions $\zeta : K \to \{0,1\}$ of the sets of all permutations consistent with I, J, s, K, and ζ, that is, $\mathcal{P}_{I,J,0,s}(K) = \bigcup_{\zeta : K \to \{0,1\}} \mathsf{PC}^{\zeta}_{I,J,0,s}(K)$.

First, let us note that if K is feasible for I, J, and s, then for any two distinct functions $\zeta, \zeta' : K \to \{0,1\}$ the set of all permutations consistent with I, J, s, K, and ζ and the set of all permutations consistent with I, J, s, K, and ζ' are disjoint, that is, $\mathsf{PC}^{\zeta}_{I,J,0,s}(K) \cap \mathsf{PC}^{\zeta'}_{I,J,0,s}(K) = \emptyset$. Indeed, let us take two distinct $\zeta, \zeta' : K \to \{0,1\}$ and let σ be an arbitrary permutation in $\mathsf{PC}^{\zeta}_{I,J,0,s}(K)$. We will show that $\sigma \notin \mathsf{PC}^{\zeta'}_{I,J,0,s}(K)$. Since ζ and ζ' are distinct, there is some ℓ such that $\zeta(\ell) \neq \zeta'(\ell)$; without loss of generality let $\zeta(\ell) = 0$. But then, for any permutation $\sigma' \in \mathsf{PC}^{\zeta'}_{I,J,0,s}(K)$, we have $\sigma'(\ell) = \ell + \zeta'(\ell) \cdot s \pmod n \neq \ell + \zeta(\ell) \cdot s \pmod n$, and thus $\sigma \notin \mathsf{PC}^{\zeta'}_{I,J,0,s}(K)$, and hence $\mathsf{PC}^{\zeta}_{I,J,0,s}(K) \cap \mathsf{PC}^{\zeta'}_{I,J,0,s}(K) = \emptyset$.

Next, we argue that for any $\zeta : K \to \{0,1\}$, if K is feasible for I, J, and s, then $|\mathsf{PC}^{\zeta}_{I,J,0,s}(K)| = (n - |I \cup J \cup K|)!$. Indeed, for a given $\zeta : K \to \{0,1\}$, let $K + \zeta = \{k + \zeta(k) \cdot s \pmod n : k \in K\}$ and let $\mathbb{S}_{I,J,K,s}(\zeta)$ be the set of all permutations $\pi^* : [n] \setminus (I \cup J \cup K) \to [n] \setminus (I \cup J + s \cup K + \zeta)$. Notice that since K is feasible for I, J, and s, both

(1) I, J, and K are pairwise disjoint, and
(2) I, $J + s$, and $K + \zeta$ are pairwise disjoint.

Therefore $\mathbb{S}_{I,J,K,s}(\zeta)$ is non-empty, and hence $|\mathbb{S}_{I,J,K,s}(\zeta)| = (n - |I \cup J \cup K|)!$. Now, the claim that $|\mathsf{PC}^{\zeta}_{I,J,0,s}(K)| = (n - |I \cup J \cup K|)!$ follows directly from the fact that any permutation consistent with I, J, s, K, and ζ corresponds in a unique way to a permutation in $\mathbb{S}_{I,J,K,s}(\zeta)$.[1]

We now summarize our discussion under the assumption that K is feasible for I, J, and s. We have

- $\mathcal{P}_{I,J,0,s}(K) = \bigcup_{\zeta : K \to \{0,1\}} \mathsf{PC}^{\zeta}_{I,J,0,s}(K)$,
- for any $\zeta : K \to \{0,1\}$, $|\mathsf{PC}^{\zeta}_{I,J,0,s}(K)| = (n - |I \cup J \cup K|)!$, and
- for any two distinct functions $\zeta, \zeta' : K \to \{0,1\}$, sets $\mathsf{PC}^{\zeta}_{I,J,0,s}(K)$ and $\mathsf{PC}^{\zeta'}_{I,J,0,s}(K)$ are disjoint.

This clearly implies that $|\mathcal{P}_{I,J,0,s}(K)| = 2^{|K|}(n - |I \cup J \cup K|)!$. ∎

A.4 | Proof of Lemma 15 (from Section 5.2.2)

Proof of Lemma 15. Following the approach from Lemma 13, for given disjoint sets I and J that are compatible for s, we will construct sets $K \subseteq [n] \setminus (I \cup J)$ that are feasible for I, J, and s.

We select set $K \subseteq [n] \setminus (I \cup J)$ by choosing k elements one by one. We will want to ensure that K is pairwise disjoint with the sets I, J, $I - s$, $J + s$, and $K + s$. The first element k_1 is selected arbitrarily from $[n] \setminus (I \cup J \cup I - s \cup J + s)$ in at least $n - 4t$ ways. The second element cannot be in $I \cup J \cup I - s \cup J + s$ and also must be distinct from k_1 and $k_1 + s \pmod n$; hence, it can be chosen in at least $n - 4t - 2$ ways. In the same way, inductively, k_ℓ is selected from $[n] \setminus (I \cup J \cup I - s \cup J + s \cup \{k_r : 1 \leq r < \ell\} \cup \{k_r + s : 1 \leq r < \ell\})$ in at least $n - 4t - 2(\ell - 1)$ ways. Since the elements in K can be ordered arbitrarily, we constructed a set of at least $\frac{(n-4t) \ldots (n-4t-2(k-1))}{k!}$ distinct sets $K \subseteq [n] \setminus (I \cup J)$ of size k that are feasible for I,

[1] That is, for any $\sigma \in \mathbb{S}_n$ consistent with I, J, s, K, and ζ, and any $\sigma^* \in \mathbb{S}_{I,J,K,s}(\zeta)$, we define $\sigma' \in \mathbb{S}_n$ such that

$$\sigma'(\ell) = \begin{cases} \ell & \text{if } \ell \in I \cup J \cup K, \\ \sigma^*(\ell) & \text{if } \ell \in [n] \setminus (I \cup J \cup K). \end{cases}$$

J, and s. Thus the probability that a set $K \subseteq [n]\setminus(I \cup J)$ of size k chosen i.u.r. is feasible for I, J, and s is at least

$$\frac{1}{\binom{n-2t}{k}} \cdot \frac{(n-4t)\ \ldots\ (n-4t-2(k-1))}{k!} = \prod_{\ell=0}^{k-1} \frac{n-4t-2\ell}{n-2t-\ell} = \prod_{\ell=0}^{k-1} \left(1 - \frac{2t+\ell}{n-2t-\ell}\right)$$
$$\geq \prod_{\ell=0}^{k-1} \left(1 - \frac{2t+k}{n-2t-k}\right) = \left(1 - \frac{2t+k}{n-2t-k}\right)^k.$$

Next, assuming that $t, k \leq O(\log n)$, we have $\left(1 - \frac{2t+k}{n-2t-k}\right)^k \geq e^{\frac{-(2t+k)k}{n-4t-2k}} \geq 1 - O\left(\frac{\log^2 n}{n}\right)$. ∎

A.5 | Proof of Claim 16 (from Section 5.2.3)

Proof of Claim 16. Let ε be such that the $1 - O\left(\frac{\log^2 n}{n}\right)$ probability in Lemma 15 is at least $1-\varepsilon$. For simplicity of notation, let

$$A_k = \{K \subseteq [n] \setminus (I \cup J) : |K| = k \text{ and } K \text{ is feasible for } I, J, \text{ and } s\}.$$

By combining Lemma 15 with the trivial upper bound for $|A_k|$, we have

$$(1-\varepsilon)\binom{n-2t}{k} \leq |A_k| \leq \binom{n-2t}{k}. \tag{A2}$$

Then,

$$\sum_{k=1}^{2r}(-1)^{k+1}\sum_{K\in A_k}|\mathcal{P}_{I,J,0,s}(K)| \tag{A3}$$
$$=^{(\text{by Lemma 14})} \sum_{k=1}^{2r}(-1)^{k+1}\sum_{K\in A_k}2^k(n-2t-k)! \tag{A4}$$
$$\geq^{(\text{by (17)})} \sum_{k=1}^{2r}2^k(n-2t-k)!\ \binom{n-2t}{k}\cdot\begin{cases}(1-\varepsilon) & \text{if } k \text{ odd}\\ -1 & \text{if } k \text{ even}\end{cases}$$
$$= (n-2t)!\left(-\sum_{k=1}^{2r}\frac{(-2)^k}{k!} - \varepsilon\sum_{k=1,\ k\ \text{odd}}^{2r}\frac{2^k}{k!}\right)$$
$$\geq (n-2t)!\left(1-\sum_{k=0}^{\infty}\frac{(-2)^k}{k!} - \frac{2^{2r}}{(2r)!} - \varepsilon\sum_{k=0}^{\infty}\frac{2^k}{k!}\right) \tag{A5}$$
$$= (n-2t)!\ (1-e^{-2} - \frac{2^{2r}}{(2r)!} - \varepsilon\ e^2). \tag{A6}$$

Inequality (A4) holds since $\frac{2^{2r}}{(2r)!} \geq \frac{2^{2r+1}}{(2r+1)!}$ for all $r > 0$. Equality (A5) holds since $\sum_{k=0}^{\infty}\frac{(-2)^k}{k!} = e^{-2}$ and $\sum_{k=0}^{\infty}\frac{2^k}{k!} = e^2$. Inequality (10) then follows because $2r \geq \log_2 n$ and $(\log n)! = n^{\Omega(\log\log n)}$. ∎

A.6 | Proof of Claim 17 (from Section 5.2.3)

Proof of Claim 17. For simplicity of notation, let

$$NA_k = \{K \subseteq [n] \setminus (I \cup J) : |K| = k \text{ and } K \text{ is not feasible for } I, J, \text{ and } s\} .$$

In our analysis we use two basic facts for sets $K \in N\,A_k$: that $|\mathcal{P}_{I,J,0,s}(K)| \leq 2^k(n-2t-k)!$ and that the set of such $K \subseteq [n] \setminus (I \cup I)$ is, by Lemma 15, of size at most $O\left(\frac{\log^2 n}{n}\right)\binom{n-2t}{k}$:

$$\begin{aligned}
\sum_{k=1}^{2r}(-1)^{k+1}\sum_{K\in NA_k}|\mathcal{P}_{I,J,0,s}(K)| &\geq -\sum_{k=1}^{2r}\sum_{K\in NA_k}|\mathcal{P}_{I,J,0,s}(K)| \geq -\sum_{k=1}^{n-2t}\sum_{K\in NA_k}|\mathcal{P}_{I,J,0,s}(K)| \\
&\geq -\sum_{k=1}^{n-2t}\sum_{K\in NA_k}2^k(n-2t-k)! \\
&\geq -\sum_{k=1}^{n-2t}O\left(\frac{\log^2 n}{n}\right)\binom{n-2t}{k}2^k(n-2t-k)! \\
&= -O\left(\frac{\log^2 n}{n}\right)(n-2t)!\sum_{k=1}^{n-2t}\frac{2^k}{k!} \geq -O\left(\frac{\log^2 n}{n}\right)(n-2t)!\sum_{k=1}^{\infty}\frac{2^k}{k!} \\
&= -O\left(\frac{\log^2 n}{n}\right)(n-2t)!e^2 = -O\left(\frac{\log^2 n}{n}\right)(n-2t)! .
\end{aligned}$$

■