

# A near-optimal algorithm for adaptive searching of two counterfeit coins

Zilin Jiang<sup>1</sup>, Nikita Polyanskii<sup>2</sup>, and Ilya Vorobyev<sup>2,3</sup>

<sup>1</sup> Massachusetts Institute of Technology

<sup>2</sup> Skolkovo Institute of Science and Technology

<sup>3</sup> Moscow Institute of Physics and Technology

zilinj@mit.edu, {n.polyanskii,i.vorobyev}@skoltech.ru

**Abstract.** We consider the coin weighing problem, which is one of the most well-known in group testing. The goal is to minimize the number of weighings with a spring scale to determine two counterfeit (heavier) coins in a set of  $n$  coins. We focus only on adaptive strategies, that is the latter weighings may depend on the results of the previous ones. In fact, the problem is equivalent to the following game on graph  $G = K_n$ . Given graph  $G = (V, E)$ , Alice selects an edge  $e \in E$ , and Bob wants to guess it by asking the minimal number  $N(G)$  of specific questions. One question is a subset  $S \subset V$ . The answer is the cardinality of  $e \cap S$ . It is known that  $N(K_{n,n}) \leq N(K_{2n}) \leq N(K_{n,n}) + 1$ . In most previous papers, base search strategies were obtained for complete bipartite graphs  $K_{n,n}$  with some small values  $n$ , whereas the recursion was performed for an arbitrarily large number of coins. We generalize this approach and propose to “mix” base strategies. Given the union of  $\ell$  copies of  $K_{n,n}$ , we design  $\ell$  strategies for  $K_{n,n}$ , and apply to each copy the corresponding strategy. As an outcome, we want to get at most  $\ell$  disjoint edges-candidates. Based on such a collection of strategies, we recursively construct an algorithm for an arbitrarily large number of coins. Our asymptotic analysis shows that the proposed scheme outperforms previously known explicit algorithms and requires  $1.2938 \log_2 n(1 + o(1))$  weighings in the worst case, and  $1.2710 \log_2 n(1 + o(1))$  weighings on average. The information theory bound established by Belokopytov says that at least  $1.2640 \log_2 n(1 + o(1))$  weighings are necessary on average.

**Keywords:** Sequential algorithm · coin weighing problem · search on graphs.

## 1 Introduction

We investigate one famous coin weighing problem. Suppose there is a collection of  $n$  coins so that  $s$  of them are false. In other words, we know that the weight of  $n - s$  coins is  $a$ , and the weight of the remaining coins is  $b$ , where integers  $a$  and  $b$  are given. The goal is to identify the weight of each coin by weighing subsets of coins on a spring scale. The problem is to design an adaptive weighing strategy, where the latter weighings may depend on the results of the previous ones, that minimizes the number of required weighings in the worst-case (WC) and in the average-case (AC). In this paper we mainly concentrate on the settings with a very large number of coins.

If the number of false coins is  $s = 1$ , then the answer to the problem is trivial, and coincide with results for non-adaptive strategy, namely  $\log_2 n(1 + o(1))$  weighings are necessary and sufficient in WC and in AC. However, the simplest non-trivial case of the problem, i.e.,  $s = 2$ , is open, and hence we focus on it in this work.

The problem considered in this paper can be rephrased using the language [Aig86] of graphs and group testing. Let a graph  $G = (V, E)$  be given. Alice conceals an edge  $e \in E$ . Bob tries to identify it by asking the

number of questions, which are answered by Alice. Each question is a subset  $S \subset V$ ; each answer is  $|e \cap S|$ . The problem is how to minimize the numbers  $N_{wc}(G)$  and  $N_{ac}(G)$  of tests in WC and in AC, respectively. If a statement holds for both AC and WC, then we omit a subscript and write  $N(G)$ . One can easily see that the minimal number of weighting to identify two false coins among  $n$  coins is exactly  $N(K_n)$ . It is also known that  $N(K_{n,n}) \leq N(K_{2n}) \leq N(K_{n,n}) + 1$ , and the main term of  $N(K_n)$  has order  $\log_2 n$  as  $n \rightarrow \infty$ . The constant factor for  $N_{wc}(K_n)$  is still not determined.

### 1.1 Related Work

It is worth noticing that the value  $N(K_{n,n})$  has been studied in coding theory and combinatorics independently. Indeed, the coin weighting problem corresponds to the two-user binary adder (erasure) channel with complete feedback [CT06]. We highlight that the strongest results were established in coding theory.

Cover and Leung [CL81] derived a random coding bound for the symmetric point in the capacity region for the binary two-user adder channel with complete feedback, and, thus, gave an upper bound for  $N_{av}(K_{n,n}) \leq 1.2640 \log_2 n(1 + o(1))$ . Based on the results in [Wil82, Wil84], the exact value of constant factor for  $N_{av}(K_{n,n})$  was finally determined by Belokopytov [Bel86], namely the upper bound by Cover and Leung is tight. However, so far there is no explicit construction achieving this constant factor. Very recently, Karimy et al. [KKHS18] suggested a simple explicit scheme which requires about  $1.365 \log_2 n$  weighings on average.

As for the worst case scenario, Dueck [Due85, Section 2] established a characterization for a class of discrete memoryless multiple-access channels including the two-user adder channel with complete feedback. But, pinning down the precise value of constant factor for  $N_{wc}(K_n)$  is an open problem. The best upper bound  $N_{wc}(K_n) \leq 1.2662 \log_2 n(1 + o(1))$  was proved by Belokopytov [Bel89] based on Dueck's characterization. Although Dueck's characterization shows that there exist good strategies, it does not provide a way of constructing the best algorithm explicitly. If we use the scheme suggested by the proof of Dueck's theorem and generate an algorithm at random with the appropriate distribution, the algorithm constructed is likely to be good. However, without some structure in the algorithm, it is computationally very difficult to decode. Hence the theorem does not provide a practical scheme.

In the context of group testing or a search problem on graphs, the ‘‘Fibonacci algorithm’’ by Christen [Chr80] and Aigner [Aig86] gives an explicit algorithm for searching an edge in  $K_{F_{n+1}, F_n}$ , where  $F_n$  is the  $n$ th Fibonacci number, which implies that  $N_{wc}(K_n) \leq \log_\phi 2 \log_2 n(1 + o(1)) = 1.4404 \log_2 n(1 + o(1))$ , where  $\phi = 1.61834$  is the golden ratio. Later, the Fibonacci algorithm was rediscovered by Zhang *et al.* [ZBM87, Theorem 1], and was refined [ZBM87, Theorem 2] to achieve  $N_{wc}(K_n) \leq \log_{\phi'} 2 \log_2 n(1 + o(1)) = 1.3954 \log_2 n(1 + o(1))$ , where  $\phi' = 1.64333$  is the real root of  $x^{11} = x^{10} + x^9 + 5$ . Using the language of decision trees, Gargano *et al.* [GMSV92] constructs an algorithm for  $K_{32,32}$  with at most 7 steps in an attempt to improve the Fibonacci code, i.e.,  $\leq 1.4 \log_2 n(1 + o(1))$  tests are sufficient for their scheme. Before our work, the best construction is an algorithm for  $K_{2^{235n+61}, 2^{235n+61}}$  with at most  $312n + 123$  weighings due to Belokopytov [BL87], achieving  $N_{wc}(K_n) \leq 312/235 \log_2 n(1 + o(1)) = 1.3277 \log_2 n(1 + o(1))$ .

If all the weighings are predetermined, then we emphasize that the situation is completely different. In particular, searching two coins among  $n$  coins is equivalent to the problem of the binary  $B_2$ -sequences for which the best known construction and upper bound were presented in [Lin69] and in [CLZ01], respectively. In particular, the number of weighings in WC is between  $1.7382 \log_2 n(1 + o(1))$  and  $2 \log_2 n(1 + o(1))$ . As for AC, we mention [Ahl73, Lia72], where it was proved for a related problem that  $4/3 \log_2 n(1 + o(1)) = 1.3333 \log_2 n(1 + o(1))$  weighings are sufficient and necessary. For larger number of false coins  $s$ , we refer the reader to [Dja75, DR81, Pol87].

## 1.2 Outline

We propose to “mix” base strategies for  $K_{n,n}$ . Given the union of  $\ell$  copies of  $K_{n,n}$ , we devise  $\ell$  strategies for  $K_{n,n}$ , and apply to each copy of  $K_{n,n}$  the corresponding strategy. As an outcome, we want to get at most  $m$  disjoint edges-candidates. Based on such collection of strategies, we recursively construct an algorithm for arbitrary large number of coins. Using a language of decision trees, we present in Section 2 a near-optimal algorithm for adaptive searching of two counterfeit coins. Our asymptotic analysis in the worst case shows that the proposed algorithm outperforms the previously known explicit schemes, and  $x' \log_2 n(1 + o(1)) = 1.2938 \log_2 n(1 + o(1))$  are sufficient in WS, where  $x'$  is a root of the equation  $1 = x'h(1/x')$  and  $h(x)$  is the binary entropy function. The analysis of the proposed strategy in AC is carried out in Section 3. We describe the same algorithm in the language of coding theory, and derive that, for our scheme,  $1.2710 \log_2 n(1 + o(1))$  weighings are sufficient in AC.

## 2 An Algorithm in the Worst-Case Setting

Let a graph  $G = (V, E)$  be given. Suppose there is only one *defective* edge  $e_d$  in the set of edges  $E$ . After each test  $S \subset V$ , which depends on the previous weightings, we receive a result  $y$  which is the cardinality of  $e_d \cap S$ . After  $m$  weightings  $S_1, \dots, S_m$  and  $m$  results  $y_1, \dots, y_m$ , we present our knowledge in the form of a subgraph  $G' = G'(y_1, \dots, y_m) = (V, E')$  of graph  $G$  which contains edge-candidates of the defective edge, i.e., each edge in  $E'$  is consistent with all previous weightings and results. In other words, any adaptive strategy which finds a defective edge forms a ternary decision tree such that any vertex at height  $m$  denoted by  $(y_1, \dots, y_m)$  is assigned with graph  $G'(y_1, \dots, y_m)$  and all the leafs are assigned with either one edge or the empty graph. Define the value  $N_{wc}(G)$  as the minimal number of consecutive tests to search a defective edge in  $G$ , i.e., the minimal height in a decision tree which finds a defective edge. A basic observation says that to find asymptotically good constructions it is sufficient to focus on finite  $n$ .

**Lemma 1 (Theorem 6 of [Hao90]).** *Given an upper bound  $N_{wc}(K_{n',n'}) \leq N_0$ , the minimal number of weighings  $N_{wc}(K_{n,n})$  satisfies*

$$N_{wc}(K_{n,n}) \leq \frac{N_0}{\log_2 n'} \log_2 n(1 + o(1)).$$

One illustrative example based on this concept was provided in [GMSV92]. In particular, it was proved  $N_{wc}(K_{32,32}) = 7$  what leads to  $N_{wc}(K_{n,n}) \leq 7/5 \log_2 n(1 + o(1))$ .

We now generalize this approach. Let  $G$  be a disjoint union of  $m$  copies of a complete bipartite graph  $K_{n,n}$ . Define the value  $N_{wc}(K_{n,n}, m)$  as the minimal number of consecutive tests to find at most  $m$  disjoint edge-candidates in  $G$ , i.e., the defective edge is one of the candidates.

**Lemma 2.** *Given an upper bound  $N_{wc}(K_{n',n'}, m) \leq N_0$ , the minimal number of weighings  $N_{wc}(K_{n,n})$  satisfies*

$$N_{wc}(K_{n,n}) \leq \frac{N_0}{\log_2 n'} \log_2 n(1 + o(1)).$$

*Proof.* Let us fix an integer  $k$  and  $N = n^k$ . First we prove

$$N_{wc}(K_{N,N}) \stackrel{(a)}{\leq} N_{wc}(K_{N,N}, m) + \lceil \log_2 m \rceil \stackrel{(b)}{\leq} k N_{wc}(K_{n,n}, m) + \lceil \log_2 m \rceil.$$

The inequality (a) holds since after applying strategy designed for the disjoint union of  $m$  copies of  $K_{N,N}$  directly to the graph  $K_{N,N}$  we find at most  $m$  disjoint edge-candidates. In addition, we need at most  $\lceil \log(m) \rceil$

tests to find a defective edge among  $m$  edge candidates. Now let us explain the inequality (b). We can think about  $N$  vertices in each part of  $K_{N,N}$  as a disjoint union of  $n$  classes of vertices consisting of  $N/n$  vertices. In other words,  $m$  copies of  $K_{N,N}$  can be represented as  $m$  copies of  $K_{n,n}$  in which each vertex is a class of vertices. At first step we may apply the strategy designed for the disjoint union of  $m$  copies of  $K_{n,n}$  to the  $m$  copies of  $K_{N,N}$  and find at most  $m$  disjoint edges connecting classes of vertices which can be seen as  $m$  copies of  $K_{N/n,N/n}$ . Then we recursively use the same arguments and after  $kN_{wc}(K_{n,n}, m)$  tests we find at most  $m$  disjoint edges.

The statement of this lemma holds, since  $m$  is fixed and  $k$  can be taken arbitrary large.

Now we are ready to state the main result.

**Theorem 1.** *Let integers  $n$  and  $m$ ,  $n/2 \leq m \leq n$  satisfy*

$$\binom{2n-2m}{n-m} 2^{3m-2n} \leq \binom{n}{m}.$$

*Then we have*

$$N_{wc}\left(K_{2^m, 2^m}, \binom{n}{m} 2^{n-m}\right) \leq n.$$

*Moreover,*

$$N_{wc}(K_{n,n}) \leq \log_2 n(1 + o(1))/x,$$

*where  $x$  is a nonzero root of the equation  $x = h(x)$  and  $h(x)$  is the binary entropy function.*

*Remark 1.* Notice that the upper bound provided by Theorem 1 is  $\leq 1.2938 \log_2 n(1 + o(1))$  which is a bit worse than the bound  $\leq 1.2662 \log_2 n(1 + o(1))$  due to Belokopytov [Bel89]. However, the strategy given in the proof of Theorem 1 is explicit unlike Belokopytov's proof of existence.

*Proof.* Fix two integers  $n \geq 2$  and  $m$ ,  $n/2 \leq m \leq n$ . Let  $N = 2^m$ . Let  $S(m, n)$  be a collection sequences of length  $n$  over  $\{*, 0, 1\}$  so that the number of stars is  $m$ . For any sequence  $(t_1, \dots, t_n) \in S(m, n)$  define a decision tree of height  $n$  recursively. In the root of the decision tree we always set  $G = K_{N,N}$ . Assume by induction that all the graphs assigned to the vertices at height  $i$  have the form either  $G' = \underbrace{K_{2^v, 2^v} + \dots + K_{2^v, 2^v}}_{2^s \text{ times}}$ ,  $s + v \leq m$ , or  $G' = \emptyset$ . If  $t_i = 1$  ( $t_i = 0$ ), then we take  $S_i = V(G')$  ( $S_i = \emptyset$ ). One can see that a child corresponding to the result 2 (0) is assigned with the same graph  $G'$ , while other two children are assigned with the empty graph. If  $t_i = *$ , then we take each disjoint component of  $G'$ , namely,  $K_{2^v, 2^v}$  and divide each (left and right) part into 2 equal portions. Then the first portion of vertices is included to  $S_i$ . A child corresponding to the result 0 or 2 is assigned with a copy of  $\underbrace{K_{2^{v-1}, 2^{v-1}} + \dots + K_{2^{v-1}, 2^{v-1}}}_{2^s \text{ times}}$ , while a child corresponding to the branch 1 is assigned with  $\underbrace{K_{2^{v-1}, 2^{v-1}} + \dots + K_{2^{v-1}, 2^{v-1}}}_{2^{s+1} \text{ times}}$ .

Now let us check what goes to the leaf denoted by  $(y_1, \dots, y_n)$ . First, if for some  $i \in \{1, \dots, n\}$  we have  $t_i = 0$  or  $t_i = 1$  and  $y_i \neq 2t_i$ , then the leaf is assigned with the empty graph. If the leaf is not assigned with the empty graph, then a disjoint union of at most  $2^m$  edges comes to this leaf. Moreover, the number of edges is a power of 2. To define this value, we calculate the number  $p$  of  $i$ 's,  $i \in \{1, \dots, n\}$ , such that  $t_i = *$  and  $y_i = 1$ . In this case  $2^p$  disjoint edges come to the leaf.

Consider  $|S(m, n)| = \binom{n}{m} 2^{n-m}$  copies of graph  $K_{N,N}$  and apply to the  $i$ -th copy the decision tree corresponding to the  $i$ -th sequence in  $S(m, n)$ . Let us find the restrictions on  $n$  and  $m$  so that, for any leaf in the

union of decision trees, the total number of disjoint edges, coming there, is at most  $|S(m, n)|$ . For any leaf, denoted by  $(y_1, \dots, y_n)$ , compute the number  $u$  of  $i$ 's,  $i \in \{1, \dots, n\}$ , such that  $y_i = 1$ . The total number of edges, denoted by  $L(y_1, \dots, y_n)$ , is

$$L(y_1, \dots, y_n) = \binom{n-u}{n-m} 2^u,$$

because any decision tree has either the empty graph, or  $2^u$  disjoint edges in the leaf  $(y_1, \dots, y_n)$  and the number of decision trees with non-empty graph in the leaf  $(y_1, \dots, y_n)$  is exactly  $\binom{n-u}{n-m}$ . In other words, we could apply Lemma 2 to the union of decision trees if we have

$$\max_{u \in \{0, \dots, m\}} \binom{n-u}{n-m} 2^u \leq |S(m, n)| = \binom{n}{m} 2^{n-m}.$$

One can easily check that the maximum in the left hand side of the inequality is attained at  $u_{max} = \max(0, 2m - n)$ . If  $m \geq n/2$ , then  $u_{max} = 2m - n$ . For any  $n \geq 2$  and  $m$ ,  $n/2 \leq m \leq n$  provided that

$$\binom{2n-2m}{n-m} 2^{2m-n} \leq \binom{n}{m} 2^{n-m},$$

we have  $N_{wc}(K_{2^m, 2^m}, \binom{n}{m} 2^{n-m}) \leq n$ . Let  $x = m/n$ ,  $x \in (1/2, 1)$ . Since we can take  $n$  arbitrary large, Lemma 2 completes the statement of the given theorem.

### 3 An Algorithm in the Average-Case Setting

In this section we analyze the problem in language of the coding theory. The two-user adder (erasure) channel takes symbols  $x_1, x_2$  from the input alphabet  $\mathcal{X} := \{0, 1\}$  given by two senders, and outputs the sum  $y = x_1 + x_2$  from the output alphabet  $\mathcal{Y} := \{0, 1, 2\}$ .

Since a received  $y \in \mathcal{Y}$  cannot be unambiguously decoded, the central problem in two-user communication theory is to coordinate the two senders to send simultaneously as much information as possible to a single receiver through  $n$  uses of the union channel.

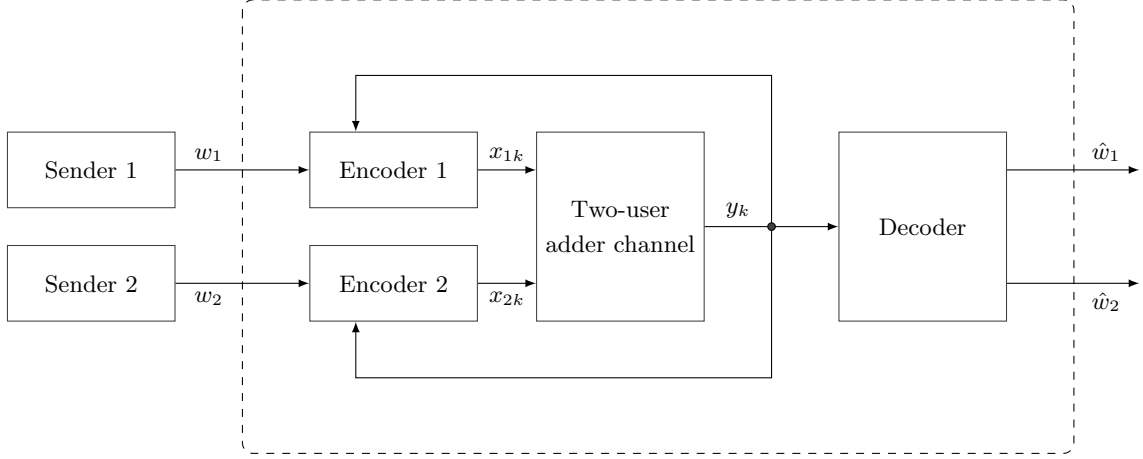
Let the message sets  $U_1$  and  $U_2$  specified for the senders be of size  $M_1$  and  $M_2$ , and let  $w_1 \in S_1, w_2 \in S_2$  be two messages chosen by the two senders beforehand. During the  $k$ th use of the channel, two functions  $e_{1k}$  and  $e_{2k}$  respectively encode  $w_1$  and  $w_2$  to two codewords  $x_{1k} \in \{0, 1\}$  and  $x_{2k} \in \{0, 1\}$ . The binary adder channel then takes  $x_{1k}, x_{2k}$  and outputs  $y_k := x_{1k} + x_{2k} \in \mathcal{Y}$ . The sequence of outputs  $(y_k)_{k=1}^n$  is decoded by the receiver to the estimate  $(\hat{w}_1, \hat{w}_2)$  of  $(w_1, w_2)$ .

Now we describe a zero-error communication scheme for the two-user union channel with complete feedback. This scheme uses a large number  $B+1$  of blocks with carefully chosen length of each block. Suppose the message sets of the senders are both  $\{0, 1\}^N$ ,  $N = Bm$ , and let  $w_1, w_2 \in \{0, 1\}^{Bm}$  be the messages of the two senders. Here we analyze the average-case, i.e., we suppose that both users choose their messages independently and uniformly and we want to estimate the average number of channel uses.

To state the communication scheme in each block, we represent the current uncertainty left over from block  $b$  by  $U(b) \subseteq (\{0, 1\} \times \{0, 1\})^{bm}$ . In other words, the receiver, at the end of block  $b$ , has learned that the first  $bm$  digits of  $w_1$  and  $w_2$  are in  $U(b)$ , that is, the receiver knows that

$$((w_{1i}, w_{2i}))_{i=1}^{bm} \in U(b).$$

In addition, we assume for a moment that at the end of block  $b$  each sender also knows the first  $bm$  digits of the other message.



**Fig. 1.** Two-user adder channel with complete feedback.

At the start of block  $b + 1$ , the senders and the receiver index the elements in  $U(b)$  by

$$S = \{(s_1, \dots, s_{n_{b+1}}) : s_k \in \{*, 0, 1\} \text{ such that } |\{k : s_k = *\}| = m\}.$$

We shall choose as a length of block the minimal number  $n_{b+1}$  such that  $|U_b| \leq |S| = \binom{n_{b+1}}{m} 2^{n_{b+1}-m}$ . The method of indexing can be agreed beforehand between the senders and the receiver. For example, they can order both  $U(b)$  and  $S$  lexicographically, and index the elements in the ordered set  $U(b)$  by the first elements in  $S$ . According to the assumption of our scheme, both senders know  $((w_{1i}, w_{2i}))_{i=1}^{bm}$ , and so they share its index  $(s_1, \dots, s_{n_{b+1}})$ .

During the  $k$ th use of the channel in block  $b$ , both senders simply send  $s_k$  if  $s_k \in \{0, 1\}$ ; or send  $w_{1,bm+i}$  and  $w_{2,bm+i}$  respectively if  $s_k$  is the  $i$ th star in  $(s_1, \dots, s_{n_b})$ . In the latter case, based on the feedback, each sender learns the  $(bm + i)$ th digit of the other message. Because there are a total of  $m$  stars in  $(s_1, \dots, s_{n_b})$ , at the end of block  $b + 1$ , both senders know  $m$  more digits of the other message, maintaining the assumption of the scheme.

In the last block  $B + 1$ , the senders simply resolve the rest of the uncertainty  $U(B)$  through  $\lceil \log_3 |U(B)| \rceil$  uses of the channel.

**Theorem 2.** *The average length of the code in the communication scheme described above less than  $x' \log_2 N(1 + o(1))$ , where  $x' = 1.2710$  is the unique root of the equation*

$$(x - 0.5)h\left(\frac{1}{2x - 1}\right) + 1.5 - x \leq xh(1/x).$$

*Proof.* Note that  $U(0)$  consists of the empty sequence, hence,  $n_1 = m$ . During the  $(b + 1)$ st block, the receiver has received  $(y_1, \dots, y_{n_{b+1}}) \in \{0, 1, 2\}^n$ . We shall estimate the size of the uncertainty set  $U(b + 1)$  at the end of the  $(b + 1)$ st block. Suppose that  $((\hat{w}_{1i}, \hat{w}_{2i}))_{i=1}^{bm}$  in  $U(b)$  is indexed by  $(s_1, \dots, s_{n_{b+1}})$ . Recall that if  $s_k \in \{0, 1\}$ , then  $y_k = 2s_k$ ; otherwise  $s_k$  is the  $i$ th star and  $y_k = \hat{w}_{1,bm+i} + \hat{w}_{2,bm+i}$ . Suppose  $L := \{k : y_k = 1\}$  and  $\ell := |L|$ . A potential  $(s_1, \dots, s_{n_{b+1}}) \in S$  must have stars on coordinates indexed by  $L$  and additional  $m - \ell$  stars on the rest  $n_{b+1} - \ell$  positions. This  $(s_1, \dots, s_{n_{b+1}})$ , if it indexes an element in  $U(b)$ , will contribute  $2^\ell$  elements to  $U(b + 1)$ . Therefore, we can estimate  $|U(b + 1)| \leq \binom{n_{b+1} - \ell}{m - \ell} 2^\ell$ .

We can obtain  $y_k = 1$  only if  $s_k = *$  and  $y_k = \hat{w}_{1,bm+i} + \hat{w}_{2,bm+i}$ . Recall that both users choose their messages uniformly and independently from  $\{0, 1\}^{Bm}$ , hence  $\ell$  has binomial distribution  $\text{Bin}(m, 0.5)$ .

Let  $\varepsilon = 1/\ln m$ . If we obtain that  $\ell$  satisfies  $|\ell - 0.5m| > \varepsilon m$  in some block, then users may apply trivial strategy with code length  $2Bm$  to transmit their messages. In this case the total number of channel uses could be roughly upper-bounded by  $4Bm$ . We estimate the probability that at any block  $|\ell - 0.5m| > \varepsilon m$  by the union bound and the Chernoff bound as follows

$$\leq B \cdot \Pr(|\text{Bin}(m, 0.5) - 0.5m| > m\varepsilon) \leq 2Be^{-2m\varepsilon^2}$$

Now consider the case when  $|\ell - 0.5m| \leq \varepsilon m$  for every block. We must find the minimal  $n_{b+1}$  such that

$$\binom{n_b - \ell}{m - \ell} 2^\ell \leq \binom{n_{b+1}}{m} 2^{n_{b+1} - m}.$$

Let  $x_b = n_b/m$  and  $x = \max_{b \in \{1, \dots, B\}} x_b$ . Taking logarithm, dividing by  $m$ , and letting  $m$  tend to infinity, we obtain sufficient condition

$$(x - 0.5)h\left(\frac{1}{2x - 1}\right) + 1.5 - x \leq xh(1/x).$$

Solving the equation with respect to  $x$  numerically, we find an unique root  $x' = 1.2710$ . Therefore, the mathematical expectation of code length is upper bounded by

$$4m \cdot 2Be^{-2m/(\ln m)^2} + (B + 1)mx'(1 + o(1)) = \frac{B + 1}{B}x' \log_2 N(1 + o(1)).$$

Letting  $B$  tend to infinity, we obtain the statement of the theorem.

## 4 Open Problems

One can see that the asymptotic bounds on the number of weighings in the worst-case are still not sharp. It would be quite interesting and challenging to close the gap. We suspect that the upper bound on  $N_{wc}(K_n)$  proved by Belokopytov [Bel89] is tight, but are not able to prove that.

*Conjecture A.* The minimal number of weighings to find 2 false coins among  $n$  coins in the worst-case setting is

$$N_{wc}(K_n) = 1.2662 \log_2 n(1 + o(1)).$$

There is much less known for the case  $s > 2$  coins. Deriving new upper and lower bounds on the minimal number of weighings to search  $s$  false coins is one of possible future research directions.

## 5 Acknowledgment

N. Polyanskii was supported in part the Russian Foundation for Basic Research (RFBR) through grant nos. 18-07-01427 A, 18-31-00310 MOL\_A. I. Vorobyev was supported in part by RFBR through grant nos. 18-07-01427 A, 18-31-00361 MOL\_A.

## References

- [Ahl73] Rudolf Ahlswede. Multi-way communication channels. In *Second International Symposium on Information Theory: Tsahkadsor, Armenia, USSR, Sept. 2-8, 1971*, 1973.
- [Aig86] M. Aigner. Search problems on graphs. *Discrete Appl. Math.*, 14(3):215–230, 1986.

- [Bel86] A. Y. Belokopytov. On a lower bound in one problem for sequential design of screening experiments. In *Proceedings. 1986 Combinatorial analysis. In Russian*, volume 7, pages 38–41, 1986.
- [Bel89] A. Ya. Belokopytov. On the zero error feedback capacity region of the binary adder channel. *Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform.*, 18(2):125–133, 1989.
- [BL87] A.Ya. Belokopytov and V.N. Luzgin. Block transmission of information in a summing multiple access channel with feedback. *Probl. Inf. Transm.*, 23(4):347–351, 1987.
- [Chr80] C Christen. *A Fibonacci algorithm for the detection of two elements*. PhD thesis, Département d’IRO, Université de Montréal, Montréal Qué, 1980.
- [CL81] Thomas M. Cover and Cyril S. K. Leung. An achievable rate region for the multiple-access channel with feedback. *IEEE Trans. Inform. Theory*, 27(3):292–298, 1981.
- [CLZ01] Gérard Cohen, Simon Litsyn, and Gilles Zémor. Binary B2-sequences: A new upper bound. *Journal of Combinatorial Theory, Series A*, 94(1):152 – 155, 2001.
- [CT06] Thomas M. Cover and Joy A. Thomas. *Elements of information theory*. Wiley-Interscience [John Wiley & Sons], Hoboken, NJ, second edition, 2006.
- [Dja75] AG Djakov. On a search model of false coins. In *Topics in Information Theory (Colloquia Mathematica Societatis Janos Bolyai 16). Budapest, Hungary: Hungarian Acad. Sci*, pages 163–170, 1975.
- [DR81] Arkadii Georgievich D’yachkov and Vladimir Vasil’evich Rykov. On a coding model for a multiple-access adder channel. *Problemy Peredachi Informatsii*, 17(2):26–38, 1981.
- [Due85] G. Dueck. The zero error feedback capacity region of a certain class of multiple-access channels. *Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform.*, 14(2):89–103, 1985.
- [GMSV92] L. Gargano, V. Montouri, G. Setaro, and U. Vaccaro. An improved algorithm for quantitative group testing. *Discrete Applied Mathematics*, 36(3):299 – 306, 1992.
- [Hao90] Fred H. Hao. The optimal procedures for quantitative group testing. *Discrete Appl. Math.*, 26(1):79–86, 1990.
- [KKHS18] Esmaeil Karimi, Fatemeh Kazemi, Anoosheh Heidarzadeh, and Alex Sprintson. A simple and efficient strategy for the coin weighing problem with a spring scale. *Proc. IEEE Int’l Symp. on Inf. Theory*, pages 1730–1734, 2018.
- [Lia72] Henry Herng-Jiunn Liao. Multiple access channels. Technical report, Hawaii University, Honolulu, September 1972.
- [Lin69] Bernt Lindström. Determination of two vectors from the sum. *J. Combinatorial Theory*, 6:402–407, 1969.
- [Pol87] G Sh Poltyrev. Improved upper bound on the probability of decoding error for codes of complex structure. *Problemy Peredachi Informatsii*, 23(4):5–18, 1987.
- [Wil82] Frans M. J. Willems. The feedback capacity region of a class of discrete memoryless multiple access channels. *IEEE Trans. Inform. Theory*, 28(1):93–95, 1982.
- [Wil84] F Willems. On multiple access channels with feedback (corresp.). *IEEE Transactions on Information Theory*, 30(6):842–845, 1984.
- [ZBM87] Zhen Zhang, T. Berger, and J. Massey. Some families of zero-error block codes for the two-user binary adder channel with feedback. *IEEE Transactions on Information Theory*, 33(5):613–619, September 1987.