

# An Improved Lower Bound for Matroid Intersection Prophet Inequalities

Raghuvansh R. Saxena

Microsoft Research, Cambridge, MA, USA

Santhoshini Velusamy

Harvard University, Cambridge, MA, USA

S. Matthew Weinberg

Princeton University, NJ, USA

---

## Abstract

We consider prophet inequalities subject to feasibility constraints that are the intersection of  $q$  matroids. The best-known algorithms achieve a  $\Theta(q)$ -approximation, even when restricted to instances that are the intersection of  $q$  partition matroids, and with i.i.d. Bernoulli random variables [13, 22, 2]. The previous best-known lower bound is  $\Theta(\sqrt{q})$  due to a simple construction of [28] (which uses i.i.d. Bernoulli random variables, and writes the construction as the intersection of partition matroids).

We establish an improved lower bound of  $q^{1/2+\Omega(1/\log \log q)}$  by writing the construction of [28] as the intersection of asymptotically fewer partition matroids. We accomplish this via an improved upper bound on the product dimension of a graph with  $p^p$  disjoint cliques of size  $p$ , using recent techniques developed in [5].

**2012 ACM Subject Classification** Mathematics of computing → Discrete mathematics

**Keywords and phrases** Prophet Inequalities, Intersection of Matroids

**Digital Object Identifier** 10.4230/LIPIcs.ITCS.2023.95

**Related Version** *Full Version:* <https://arxiv.org/abs/2209.05614>

## 1 Introduction

Consider a gambler who faces the following challenge: There is a sequence of  $n$  independent random variables  $X_1, \dots, X_n$ , and a set system  $\mathcal{I}$  of feasibility constraints over  $[n]$ . The gambler knows  $\mathcal{I}$ , and the distribution  $D_i$  of each  $X_i$ , but not its realization. One at a time,  $X_i$  will be drawn from  $D_i$  and revealed to the gambler, at which point she must immediately and irrevocably accept or reject the element. At all times, the set  $A$  of accepted elements must be in  $\mathcal{I}$  (meaning that if  $A \cup \{i\} \notin \mathcal{I}$ , the gambler must reject  $i$ ). The gambler's payoff at the end of the game is  $\sum_{i \in A} X_i$ .

The gambler's goal is to design an algorithm that maximizes her expected reward, and competes against a prophet. The prophet knows all realizations when making decisions, and therefore achieves expected reward  $\mathbb{E}_{\bar{X} \leftarrow \bar{D}}[\max_{S \in \mathcal{I}} \{\sum_{i \in S} X_i\}]$ . The ratio of the prophet's expected reward to the optimal gambler's expected reward is referred to as a prophet inequality.

Prophet inequalities have received significant attention within optimization under uncertainty, and within TCS broadly, due to their similarity to online algorithms and additionally, due to a deep connection to multi-dimensional mechanism design discovered by [11]. The canonical question asked is the following: for a given class  $\mathcal{C}$  of potential feasibility constraints, what is  $\alpha(\mathcal{C})$ , the best prophet inequality that can be guaranteed on any instance with  $\mathcal{I} \in \mathcal{C}$ ? [11, 3, 28, 8, 24, 18, 22, 33, 30, 25, 6, 21, 10, 13].



© Raghuvansh R. Saxena, Santhoshini Velusamy, and S. Matthew Weinberg;  
licensed under Creative Commons License CC-BY 4.0

14th Innovations in Theoretical Computer Science Conference (ITCS 2023).

Editor: Yael Tauman Kalai; Article No. 95; pp. 95:1–95:20

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

In this direction, asymptotically tight (and sometimes, exactly tight) bounds are known on  $\alpha(\mathcal{C})$  for many classes of interest. For example, when  $\mathcal{C}$  is the class of 1-uniform matroids<sup>1</sup>,  $\alpha(\mathcal{C}) = 2$  [29, 35]. When  $\mathcal{C}$  is the class of  $k$ -uniform matroids,  $\alpha(\mathcal{C}) = 1 + \Theta(1/\sqrt{k})$  [3]. When  $\mathcal{C}$  is the class of all matroids,  $\alpha(\mathcal{C}) = 2$  [28]. See Section 1.2 for further discussion.

Perhaps the most canonical class of constraints where asymptotically-tight guarantees remain unknown is the intersection of  $q$  matroids. Here, state-of-the-art algorithms achieve an  $e(q+1)$ -approximation [22], and an improved  $(q+1)$ -approximation for the intersection of  $q$  partition matroids [13].<sup>2</sup> Note also that even if we restrict attention to cases where each  $D_i$  is i.i.d. Bernoulli, asymptotically better algorithms are not known. On the other hand, the best-known lower bound of  $\Omega(\sqrt{q})$  comes from a simple construction of [28], where feasibility constraints can be written as the intersection of partition matroids and are fully-symmetric (see Section 2 for a formal definition), and the distributions are i.i.d. Bernoulli. Our main result provides the first improvement on their lower bound.

► **Theorem 1.** *For any  $q$ , let  $\mathcal{C}_{\text{PARTINT}}(q)$  be the class of feasibility constraints that are the intersection of  $q$  partition matroids. Then  $\alpha(\mathcal{C}_{\text{PARTINT}}(q)) \geq q^{1/2 + \Omega(1/\log \log q)}$ .*

While the quantitative improvement in Theorem 1 over  $\Omega(\sqrt{q})$  is relatively minor, we highlight several aspects of the significance of our approach below.

## 1.1 Context and Technical Highlights

First, we note that the construction and analysis of [28] is exceptionally simple, and has not previously been improved. Specifically, for any  $p$ , their construction provides a prophet inequality instance with i.i.d. Bernoulli distributions where:

- (a) it is straightforward to argue that the gambler achieves at most an  $\Omega(p)$  fraction of the prophet's expected reward, and
- (b) it is reasonably simple (although non-trivial) to argue that the feasibility constraints can be written as the intersection of  $p^2$  partition matroids.

We overview both aspects of their construction in Section 3. Their simple construction is a canonical hard instance, and plausibly witnesses (asymptotically) the strongest inapproximability among matroid intersection prophet inequalities. Prior to our work, it was plausible that  $p^2$  is the minimum number of matroids needed to write their construction. Beyond Theorem 1, one contribution of our results is an improved analysis of this canonical construction.

Beyond matroid intersection prophet inequalities as an application, analysis of their construction has connections to a purely graph-theoretic problem in Combinatorics. Specifically, the *product dimension* of a graph  $G$  is the minimum number of proper vertex colorings of  $G$  so that every pair of non-adjacent edges in  $G$  have the same color in at least one coloring. If  $Q(s, r)$  denotes the disjoint union of  $r$  cliques each of size  $s$ , then the number of partition matroids needed to write the [28] construction is exactly the product dimension of  $Q(p, p^p)$  (we will formally state this when we overview their construction). Prior to our work, the best-known upper bound on the product dimension of  $Q(p, p^p)$  was  $p^2$ . Our work improves this to  $p^{2 - \Omega(1/\log \log p)}$ , leveraging recent work on the product dimension of  $Q(s, r)$  for  $r \gg s^s$  [5]. We overview further related work on the product dimension of  $Q(s, r)$  in Section 1.2.

<sup>1</sup> A 1-uniform matroid is just the collection of  $n$  singleton sets and the empty set.

<sup>2</sup> Note that the intersection of  $q$  partition matroids is equivalent to the case where each element is a hyperedge in a  $q$ -dimensional  $q$ -partite hypergraph, and  $\mathcal{I}$  contains all matchings.

Finally, we additionally note a broader agenda in our work that, to the best of our knowledge, has not been previously studied within the TCS community: given a set system  $\mathcal{I}$ , what is the minimum number  $q$  of matroids  $\mathcal{I}_1, \dots, \mathcal{I}_q$  so that  $\mathcal{I} = \cap_{i=1}^q \mathcal{I}_i$ ? Our work brings advanced tools from Combinatorics to address questions of this form when we additionally ask that all  $\mathcal{I}_j$  are partition matroids. A stronger toolkit for this agenda will be useful to analyze broad algorithmic questions on matroid intersections, especially in cases where it is straightforward to construct a canonical hard instance (such as the [28] construction), but it is not straightforward to write it as a matroid intersection.

## 1.2 Related Work

Krengel, Sucheston, and Garling [29] pose the first single-choice prophet inequality, and Samuel-Cahn shows how to achieve the same optimal guarantee with an exceptionally simple thresholding algorithm [35]. Chawla et al. identify a fundamental connection between prophet inequalities and multidimensional mechanism design, and design novel prophet inequalities for the case when  $\mathcal{I}$  is the intersection of two partition matroids [11]. Following this, numerous works identify asymptotically optimal (and sometimes, exactly optimal) prophet inequalities for uniform matroids [3, 8, 27], arbitrary matroids [28, 22, 30], polymatroids [18], the intersection of two partition matroids [25, 21], independent sets in graphs [24], and arbitrary downwards-closed set systems [33]. Recent works also consider efficient approximation schemes for the optimal gambler strategy [6], and algorithms with limited samples [8, 34, 10].

One canonical class of feasibility constraints for which an asymptotically-tight prophet inequality remains unknown is the intersection of  $q$  matroids. On the positive side, state-of-the-art algorithms achieve an approximation guarantee of  $O(q)$  [28, 22, 13]. For the intersection of  $q$  arbitrary matroids, the best-known guarantee is  $e(q + 1)$  [22]. For the intersection of  $q$  partition matroids, the best-known guarantee is  $q + 1$  [13]. The best known lower bound is  $\Omega(\sqrt{q})$ , due to a simple construction of [28].<sup>3</sup>

Also related to our work is the distinction between adversarial-order prophet inequalities vs. random-order prophet inequalities, and arbitrary product distributions vs. i.i.d. distributions. There is a very rich literature on single-choice prophet inequalities from i.i.d. distributions [1, 16, 14, 34, 12, 15, 26], and an equally rich literature on random-order prophet inequalities [20, 19, 9, 2, 23, 17, 32, 7]. However, all of these works identify constant-factor improvements under i.i.d. or random-order restrictions. Most consider settings (such as matroids, matchings, or single-choice) where constant-factor prophet inequalities exist with adversarial order and non-i.i.d. distributions (and therefore beyond constant-factor improvements are not possible). The most relevant of these works to our results is [2], which provides an improved prophet inequality of  $q + 1$  (from  $e(q + 1)$ ) for the intersection of  $q$  matroids subject to random arrival order (instead of adversarial). The relevant aspect of this body of works to our paper is that the best-known algorithms, even when restricted to instances with i.i.d. Bernoulli random variables and intersections of  $q$  partition matroids, achieve at best a  $O(q)$  approximation guarantee. At the same time, the hardest-known construction, witnessing an inapproximability of  $\Omega(\sqrt{q})$ , also uses i.i.d. Bernoulli random variables and is the intersection of  $q$  partition matroids. We emphasize this aspect when stating our main results.

<sup>3</sup> Incidentally, [28] mistakenly claim a lower bound of  $\Omega(q)$  in their paper. This mistake, which was later realized by the authors, does not affect any of the other results in the paper, which include an  $O(q)$  prophet inequality for intersection of  $q$  matroids. However, it does quantitatively affect the obtained lower bound, which was used to claim that the algorithm is tight. We elaborate on this when we overview their construction.

Our results provide improved upper bounds on the product dimension of  $Q(p, p^p)$ , the disjoint union of  $p^p$  cliques of size  $p$ . Our result leverages recent progress of [5] on the product dimension of  $Q(s, r)$  when  $r \gg s^s$ . Prior to their work, [31, 4] nail down  $Q(2, r)$ .

### 1.3 Summary and Roadmap

We improve the best-known lower bound on matroid intersection prophet inequalities to  $q^{1/2+\Omega(1/\log \log q)}$ , via an improved upper bound of  $p^{2-\Omega(1/\log \log p)}$  on the product dimension of  $Q(p, p^p)$ .

This paper is structured as follows: After providing the required definitions in Section 2, we provide the known connection between the product dimension and matroid intersection prophet inequalities in Section 3. We then overview the framework of [5] in Section 5 and present our improvement in Section 4. We finish with some concluding remarks in Section 6.

## 2 Preliminaries

### Basic Notation

We use  $[a, b]$  to denote the set of integers between  $a$  and  $b$  including  $a$  and  $b$ . We also use  $[n]$  in place of  $[1, n]$  to denote the set of integers  $\{1, \dots, n\}$ . For prime  $p$ , we interchangeably view  $\mathbb{Z}_p$  as the field  $\mathbb{Z}/p\mathbb{Z}$  and the set  $[0, p - 1]$ . The notion considered will be clear from context.

### Refresher on Matroids

A set system  $\mathcal{I}$  over  $[n]$  is a matroid if  $\mathcal{I}$  is downwards-closed (for all  $S \subseteq T$ ,  $T \in \mathcal{I} \Rightarrow S \in \mathcal{I}$ ), non-trivial ( $\emptyset \in \mathcal{I}$ ), and satisfies the augmentation property (for all  $S, T \in \mathcal{I}$ , if  $|T| > |S|$ , there exists an  $i \in T \setminus S$  such that  $S \cup \{i\} \in \mathcal{I}$ ). A partition matroid  $\mathcal{I}$  partitions  $[n]$  into disjoint sets  $S_1, \dots, S_k$ , and deems a set  $T \in \mathcal{I}$  if and only if  $|T \cap S_i| \leq 1$  for all  $i$ . The intersection of  $q$  matroids is a set system  $\mathcal{I}$  that can be written as  $\mathcal{I} = \bigcap_{j=1}^q \mathcal{I}_j$ , where each  $\mathcal{I}_j$  is a matroid. If each  $\mathcal{I}_j$  is a partition matroid, we will call this the intersection of  $q$  partition matroids. Observe that  $\mathcal{I}$  is an intersection of  $q$  partition matroids if and only if there exists a  $q$ -partite  $q$ -dimensional hypergraph with edges as elements of  $[n]$  so that a set  $S$  of edges is feasible if and only if they form a matching.<sup>4</sup>

## 2.1 Approach to Bound Product Dimension

### Product Dimension

Recall that the product dimension of a graph  $G$  is the minimum number of proper colorings of the vertices of  $G$  such that for every non-adjacent pair  $(u, v) \in V(G)$ , they share the same color in at least one coloring. We'll use the notation  $\text{PD}(s, r)$  to refer to the product dimension of the graph consisting of  $r$  disjoint cliques of size  $s$ . Our approach to upper bound  $\text{PD}(s, r)$ , also used in [5], is based on the following definitions:

<sup>4</sup> To see one direction, let  $G = (V_1 \sqcup \dots \sqcup V_q, E)$  be a  $q$ -partite  $q$ -dimensional hypergraph. For each  $j$ , define a partition matroid  $\mathcal{I}_j$  that partitions edges by which node in  $V_j$  they are adjacent to. To see the other direction, let  $\mathcal{I}_1, \dots, \mathcal{I}_q$  be partition matroids. Make a  $q$ -partite  $q$ -dimensional hypergraph with nodes  $V_1, \dots, V_q$ , where  $|V_j|$  is equal to the number of parts in  $\mathcal{I}_j$ . For each element  $i \in [n]$ , make an edge in the graph containing exactly one node in  $V_j$ , corresponding to the part containing  $i$ .

► **Definition 2** ( $(\ell, p)$ -Family). Let  $\ell$  be a non-negative integer and  $p$  be a prime. We use the term  $(\ell, p)$ -Family to refer to subsets of  $\mathbb{Z}_p^\ell$ .

► **Definition 3** ( $S$ -covering). For two vectors  $\vec{v}, \vec{w} \in \mathbb{Z}_p^\ell$ , and a set  $S \subseteq \mathbb{Z}_p$ , we say that the pair  $\vec{v}, \vec{w}$  is  $S$ -covering if for all  $s \in S$ , there exists an index  $i \in [\ell]$  such that  $v_i - w_i = s \pmod{p}$ . We say that an  $(\ell, p)$ -Family  $\mathcal{F}$  is  $S$ -covering if every pair of distinct elements in  $\mathcal{F}$  is  $S$ -covering.

In particular, we will be interested in the following quantity:

► **Definition 4.** Define  $AAM(p, N)$  (the “Alon-Alweiss Measure”) to be the minimum  $\ell$  such that a  $\mathbb{Z}_p$ -covering  $(\ell, p)$ -Family of size  $N$  exists.

Intuitively, we think of being given a fixed (large) prime  $p$ , and a target  $N$ . Our goal is to find a family of  $N$  vectors over  $\mathbb{Z}_p$ , such that for any pair of vectors  $\vec{v}, \vec{w}$  in the family, and any  $s \in \mathbb{Z}_p$ , there exists an index  $i$  such that  $v_i - w_i = s \pmod{p}$ . As the dimension  $\ell$  of the vectors grows, this becomes easier. Our goal is to find constructions of this form with the smallest possible  $\ell$ , and  $AAM(p, N)$  denotes the minimum  $\ell$  for which this is possible. We now confirm the relation between  $AAM(p, N)$  and the product dimension of disjoint cliques.

► **Observation 5** ([5]).  $PD(p, N) \leq AAM(p, N)$ .

**Proof.** Consider a graph  $G$  with  $N$  disjoint cliques of size  $p$ . We show that if there exists a  $\mathbb{Z}_p$ -covering  $(\ell, p)$ -Family of size  $N$ , then there exist  $\ell$  proper colorings of  $G$  such that any two non-adjacent vertices in  $G$  have the same color in at least one coloring. For  $k \in [\ell]$ , define coloring  $k$  to be such that vertex  $i$  in clique  $j$  is given color  $v_k^j + i \pmod{p}$ , where  $v^j$  is the  $j$ -th vector in the family. These colorings are indeed proper as the  $p$  nodes in each clique receive distinct colors. Now, consider any two non-adjacent vertices, say vertex  $i$  in clique  $j$  and vertex  $i'$  in clique  $j' \neq j$ . We have to show that there exists  $k \in [\ell]$  such that  $v_k^j + i = v_k^{j'} + i' \pmod{p} \iff v_k^j - v_k^{j'} = i' - i \pmod{p}$ . However, this is true by definition of a  $\mathbb{Z}_p$ -covering Family and the fact that  $j \neq j'$ . ◀

Essentially,  $AAM(p, N)$  captures the minimum product dimension that can be achieved by using exactly  $p$  colors, and by having every coloring be “cyclic” within each clique. Our main technical results will upper bound  $AAM(p, N)$ .

## 2.2 Matroid Intersection Prophet Inequalities

We briefly formally define terminology that we will use when discussing approximation guarantees of prophet inequalities.

► **Definition 6** (Approximability of a Prophet Inequality Instance). For a given prophet inequality instance  $\mathcal{I}, D_1, \dots, D_n$ , let  $OptG(\vec{X})$  denote the set of elements selected by the optimal gambler strategy on the realizations  $\vec{X}$ .<sup>5</sup> Then the approximability  $\alpha(\mathcal{I}, D_1, \dots, D_n)$  of the instance is:

$$\alpha(\mathcal{I}, D_1, \dots, D_n) := \frac{\mathbb{E}_{\vec{X} \leftarrow \vec{D}} \left[ \max_{S \in \mathcal{I}} \left\{ \sum_{i \in S} X_i \right\} \right]}{\mathbb{E}_{\vec{X} \leftarrow \vec{D}} \left[ \sum_{i \in OptG(\vec{X})} X_i \right]}.$$

<sup>5</sup> Note that the optimal gambler strategy is well-defined in all cases, and can be computed (not necessarily in polynomial time) via dynamic programming.

We will also use the following two quantities to refer to the approximability of a class of prophet inequality instances. Below,  $\mathcal{C}_n$  refers to a class of feasibility constraints on  $n$  elements, and  $\mathcal{C} := \{\mathcal{C}_n\}_{n \in \mathbb{N}}$  refers to an ensemble of such classes,  $\mathcal{P}_n$  refers to a class of product distributions on  $n$  elements,  $\mathcal{P} := \{\mathcal{P}_n\}_{n \in \mathbb{N}}$  refers to an ensemble of such classes, and  $\mathcal{D}_n$  refers to the set of all product distributions on  $n$  elements.

$$\alpha(\mathcal{C}) := \sup_{n \in \mathbb{N}, \mathcal{I} \in \mathcal{C}_n, \vec{D} \in \mathcal{D}_n} \{\alpha(\mathcal{I}, \vec{D})\}.$$

$$\alpha(\mathcal{C}, \mathcal{P}) := \sup_{n \in \mathbb{N}, \mathcal{I} \in \mathcal{C}_n, \vec{D} \in \mathcal{P}_n} \{\alpha(\mathcal{I}, \vec{D})\}.$$

For example, when  $\mathcal{C}$  represents the class of all one-uniform matroids and  $\mathcal{P}$  represents the class of i.i.d. distributions, we have  $\alpha(\mathcal{C}) = 2$  [29, 35] and  $\alpha(\mathcal{C}, \mathcal{P}) \approx 1/0.745$  [16]. Similarly, when  $\mathcal{C}$  represents the class of all matroids, we have  $\alpha(\mathcal{C}) = 2$  [28].

### 3 Connecting Prophet Inequalities to AAM( $p, N$ )

The following classes of feasibility constraints, and of distributions, are relevant for implications of our results:

- $\mathcal{C}_{\text{MATINT}}(q)$ : feasibility constraints that can be written as the intersection of  $q$  matroids.
- $\mathcal{C}_{\text{PARTINT}}(q)$ : feasibility constraints that can be written as the intersection of  $q$  partition matroids. Note that this is equivalent to the class of all feasibility constraints that can be written with elements as hyperedges in a  $q$ -partite  $q$ -dimensional hypergraph, and feasible sets as matchings in that hypergraph.
- $\mathcal{C}_{\text{SYMPARTINT}}(q)$ : feasibility constraints that are *fully symmetric* and can be written as the intersection of  $q$  partition matroids. For a permutation  $\sigma$  over the elements and a set of feasibility constraints  $\mathcal{I}$ , we say that  $\mathcal{I}$  is invariant under  $\sigma$  if for all sets  $S$ ,  $S \in \mathcal{I} \Leftrightarrow \sigma(S) \in \mathcal{I}$ . We say that  $\mathcal{I}$  is fully symmetric if for all elements  $x, y$ , there exists a permutation  $\sigma$  such that  $\sigma(x) = y$  and  $\mathcal{I}$  is invariant under  $\sigma$ .
- $\mathcal{P}_{\text{IID}}$ : The class of all i.i.d distributions
- $\mathcal{P}_{\text{IIDBERNOULLI}}$ : The class of all i.i.d. Bernoulli distributions.

We first summarize the positive results known for prophet inequalities in these settings.

► **Theorem 7** ([22, 2, 13]). *The following bounds are known on the approximability of prophet inequalities for the intersection of  $q$  matroids:*

- $\alpha(\mathcal{C}_{\text{MATINT}}(q)) \leq e(q + 1)$  [22], and  $\alpha(\mathcal{C}_{\text{MATINT}}(q)) \leq 4(q - 2)$  [28].
- $\alpha(\mathcal{C}_{\text{PARTINT}}(q)) \leq q + 1$  [13].
- $\alpha(\mathcal{C}_{\text{MATINT}}(q), \mathcal{P}_{\text{IID}}) \leq q + 1$  [2].
- *No improvements are known for further special cases, even  $\alpha(\mathcal{C}_{\text{SYMPARTINT}}(q), \mathcal{P}_{\text{IIDBERNOULLI}})$ .*

In terms of lower bounds on  $\alpha(\mathcal{C}_{\text{MATINT}}(q))$ , a construction of [28] establishes the following. We repeat the construction below for completeness.

► **Proposition 8** ([28]). *Let  $q > 0$  be given and let  $p > 0$  be the largest such that  $q \geq \text{AAM}(p, p^p)$ . It holds that:*

$$\alpha(\mathcal{C}_{\text{SYMPARTINT}}(q), \mathcal{P}_{\text{IIDBERNOULLI}}) \geq (1 - 1/e)p/2.$$

**Proof.** Consider a graph  $G$  with  $p^p$  disjoint cliques of size  $p$ . As  $q \geq \text{AAM}(p, p^p)$ , we conclude from Observation 5 that  $q \geq \text{PD}(p, p^p)$ . Thus, there exist  $q$  proper colorings of  $G$  such that two vertices are adjacent if and only if they have different colors in all  $q$  colorings. The colorings define  $q$  partitions of the vertices in  $G$  and for all  $k \in [q]$ , we let  $\mathcal{I}_k$  be the partition matroid over the partition defined by the  $k$ -th coloring. Let  $\mathcal{I} = \bigcap_{i=1}^q \mathcal{I}_i$ .



We first claim that  $\mathcal{I}$  is just the set of all cliques in  $G$ . Indeed, a subset of vertices  $S \in \mathcal{I}$  if and only if  $S \in \mathcal{I}_k$  for all  $k \in [q]$ . The latter happens if and only if the vertices in  $S$  have different colors in all  $q$  colorings which by definition, happens if and only if they form a clique.

It follows from the definition of  $G$  and the above claim that  $\mathcal{I}$  is fully symmetric.<sup>6</sup> Now, consider the prophet inequality instance whose elements are vertices in  $G$ , the feasibility constraints are given by  $\mathcal{I}$  and distribution for all elements is i.i.d. Bernoulli, and equal to 1 with probability  $1/p$ . The prophet for this instance simply selects the clique with the most number of 1s. As with probability  $1 - (1 - 1/p^p)^p \geq 1 - 1/e$ , there exists some clique with all  $p$  vertices set to 1, the prophet's expected reward is at least  $(1 - 1/e)p$ .

However, as soon as the gambler accepts some element, they are locked into a clique, without knowing the value of the other elements of the clique. The reward from the accepted element is at most 1, and the expected reward from the rest of the clique is at most  $1 - 1/p$ . Therefore, the optimal gambler strategy gets expected reward at most 2. Thus the multiplicative gap between the prophet and the optimal gambler is at least  $(1 - 1/e)p/2$  and the proposition holds.  $\blacktriangleleft$

Proposition 8 provides a path towards showing that<sup>7</sup> the algorithms referenced in Theorem 7 are asymptotically tight, by showing strong upper bounds on  $\text{AAM}(p, p^p)$ . Here is what is known about  $\text{AAM}(p, N)$  prior to our work:

► **Theorem 9.** *The following are upper and lower bounds on  $\text{AAM}(p, N)$ , for prime  $p$ :*

1.  $\text{AAM}(p, N) \leq p \cdot \lceil \log_p(N) \rceil$ . This implies that  $\text{AAM}(p, p^p) \leq p^2$ .
2. For sufficiently large  $p$ ,  $\text{AAM}(p, N) \leq \max\{p^{1+5 \log_2 \log_2 p}, \log_{\left(2 - \frac{1}{\log_2 p}\right)} N\}$  [5].
3.  $\text{AAM}(p, N) \geq \max\{p, \log_{\left(2 + \frac{12}{p-6}\right)}(N)\}$ .

**Proof.** We prove each item in turn:

1. As  $\text{AAM}(p, N)$  is monotone in  $N$ , we can assume that  $N$  is a power of  $p$  without losing generality. Define  $\ell = p \cdot \log_p(N)$  for convenience. For  $i \in [N]$ , define the  $\ell$  length vector whose first  $\ell/p$  coordinates are the representation of  $i$  in base  $p$ , the second  $\ell/p$  coordinates are the representation of  $i$  in base  $p$  multiplied by 2 modulo  $p$  and so on. It suffices to show that  $(\ell, p)$ -Family consisting of all these vectors in  $\mathbb{Z}_p$ -covering. Indeed, for any two vectors  $i \neq i'$  differ in at least one coordinate of their base  $p$ -representation and let  $\Delta \neq 0$  be the difference between the two values of this coordinate modulo  $p$ . By our construction, the vectors  $i, i'$  cover all multiples of  $\Delta$  modulo  $p$  which is all of  $\mathbb{Z}_p$  (as  $p$  is a prime).
2. Note that if  $N \leq p^{5 \log_2 \log_2 p}$ , the result follows from Item 1. If not, we define  $\ell = \log_{\left(2 - \frac{1}{\log_2 p}\right)} N$  and observe that  $\ell > p^{5 \log_2 \log_2 p}$ . By the definition of  $\text{AAM}(\cdot)$  (Definition 4, it suffices to show that there exists a  $\mathbb{Z}_p$ -covering  $(\ell, p)$ -Family of size  $N$ . This essentially is the result of [5], and is recapped as Theorem 16 below.

<sup>6</sup> To see this, let  $\tau : [p^p] \rightarrow [p^p]$  permute cliques, and  $\rho : [p] \rightarrow [p]$  permute within a clique. Then for any  $\tau, \rho$ , the feasibility constraints are invariant under the permutation  $\sigma_{\tau, \rho}$  that defines  $\sigma_{\tau, \rho}((i, j)) := (\rho(i), \tau(j))$ . Now, for any  $(i, j), (i', j')$ , there is a  $\rho$  with  $\rho(i) = i'$  and  $\tau$  with  $\tau(j) = j'$ . For this  $(\tau, \rho)$ ,  $\sigma_{\tau, \rho}(i, j) = (i', j')$ , and the constraints are invariant under  $\sigma_{\tau, \rho}$ . Therefore, the constraints are fully symmetric.

<sup>7</sup> [28] also mistakenly claim that  $\text{AAM}(p, p^p) = \Theta(p)$ . If true, this would imply that all the quantities  $\{\alpha(\mathcal{C}_{\text{MATINT}}(q)), \alpha(\mathcal{C}_{\text{PARTINT}}(q)), \alpha(\mathcal{C}_{\text{SYMPARTINT}}(q)), \alpha(\mathcal{C}_{\text{MATINT}}(q), \mathcal{P}_{\text{HIDBERNOULLI}}), \alpha(\mathcal{C}_{\text{PARTINT}}(q), \mathcal{P}_{\text{HIDBERNOULLI}}), \alpha(\mathcal{C}_{\text{SYMPARTINT}}(q), \mathcal{P}_{\text{HIDBERNOULLI}})\}$  are  $\Theta(q)$ . However, this part of their proof has a subtle error.

3.  $\text{AAM}(p, N) \geq p$  simply because in order for two distinct vectors to possibly be  $\mathbb{Z}_p$ -covering, they must have at least  $p$  coordinates. We now show that  $\text{AAM}(p, N) \geq \log_{(2+\frac{12}{p-6})}(N)$ . To this end, let  $x$  be the largest integer at most  $p/4 - 1$  and let  $\ell > 0$  be arbitrary such that there exists a  $\mathbb{Z}_p$  covering  $(\ell, p)$ -Family  $\mathcal{F}$  of size  $N$ . By our choice of  $x$ , we have that  $x > p/4 - 2$  and there exists  $y \in \mathbb{Z}_p$  that is not in the set  $\{-2x, \dots, 2x\} \pmod{p}$ . We first claim that for all  $\vec{z} \in \mathbb{Z}_p^\ell$ , there is at most one element  $\vec{v}$  of  $\mathcal{F}$  such that  $z_i - v_i \in \{-x, \dots, x\} \pmod{p}$  for all  $i \in [\ell]$ . Indeed, if there were two distinct vectors  $\vec{v} \neq \vec{w}$ , then this pair only covers the set  $\{-2x, \dots, 2x\}$ , and does not cover  $y \in \mathbb{Z}_p$ , a contradiction. With this claim and the fact that  $x > p/4 - 2$ , we can upper bound  $N$  as:

$$N \leq \left(\frac{p}{2x+1}\right)^\ell \leq \left(\frac{2p}{p-6}\right)^\ell \implies \ell \geq \log_{(2+\frac{12}{p-6})} N. \quad \blacktriangleleft$$

## 4 Proof of Main Result

### 4.1 Overview of The Proof

We now give a brief overview covering all of our main ideas. Our goal is to show Theorem 1 that is a lower bound for prophet inequalities for the intersection of  $q$  partition matroids. As mentioned in the introduction, we shall follow the approach of [28, 5] that says that such a lower bound follows if we prove strong enough upper bounds on the measure  $\text{AAM}(p, N)$  from Definition 4. Specifically, we shall employ Proposition 8 that shows that if we have a better than quadratic bound on  $\text{AAM}(p, p^p)$ , say we show that  $\text{AAM}(p, p^p) \leq p^{2-\delta}$ , then we also get  $\alpha(\mathcal{C}_{\text{SYM PART INT}}(p^{2-\delta}), \mathcal{P}_{\text{IDBERNOULLI}}) \geq \Omega(p)$ , or equivalently, that

$$\alpha(\mathcal{C}_{\text{SYM PART INT}}(q), \mathcal{P}_{\text{IDBERNOULLI}}) \geq q^{1/2+O(\delta)},$$

and Theorem 1 follows.

#### 4.1.1 Getting a Quadratic Bound

In order to understand how we get a better than quadratic bound on  $\text{AAM}(p, p^p)$ , it will be instructive to first understand how to get a quadratic bound and show that  $\text{AAM}(p, p^p) \leq \tilde{O}(p^2)$  (such a bound, using a different argument, was also observed by the authors of [28]). Recall from Definition 4 that in order to show such a bound, we have to show that there exists a  $\mathbb{Z}_p$ -covering  $(\tilde{O}(p^2), p)$ -Family of size  $p^p$ . We construct such a family by starting with a  $\{0, 1\}$ -covering  $(2, p)$ -Family of size 2, namely the family  $\mathcal{F}_0$  consisting of the vectors  $(0, 0)$  and  $(0, 1)$ , and using it to get families with better parameters. We define two different boosting operations:

1. **Size for length boosting:** This operation increases the size of the family by a power of 2, *i.e.*, takes it from  $N$  to  $N^2$ , at the cost of also increasing the length  $\ell$  be a factor 2. That is, we want to start with an  $S$ -covering  $(\ell, p)$ -Family  $\mathcal{F}$  of size  $N$  and get an  $S$ -covering  $(2\ell, p)$ -Family  $\mathcal{F}'$  of size  $N^2$ . To do this, define the family  $\mathcal{F}'$  to have all possible  $N^2$  concatenations obtained by concatenating 2 vectors from the family  $\mathcal{F}$  and observe that  $\mathcal{F}'$  satisfies all the required properties.
2. **Cover for length boosting:** This operation increases the number of elements covered by a factor of 2 at the cost of also increasing the length  $\ell$  be a factor 2. That is, we want to start with an  $S$ -covering  $(\ell, p)$ -Family  $\mathcal{F}$  of size  $N$  and get an  $S'$ -covering  $(2\ell, p)$ -Family  $\mathcal{F}'$



of size  $N$ , where  $|S'| = 2 \cdot |S|$ . To do this, sample a uniformly random element  $s \in \mathbb{Z}_p \setminus \{0\}$  and define the family  $\mathcal{F}'$  to have the vector  $(\vec{v}, s \cdot \vec{v})$  for every vector  $\vec{v} \in \mathcal{F}$ . Observe that the new family  $\mathcal{F}'$  shatters all the elements in  $S' = S \cup sS$ .<sup>8</sup> and has length  $2\ell$ .

In general, it may happen that  $|S'| < 2 \cdot |S|$  if we are unlucky in our sample of  $s$  or if the set  $S$  that we started with was very large. Thus, this boosting operation is not without “flaws”. Nonetheless, there are ways one can overcome these flaws when we use it in the actual construction by, say, ensuring all sets  $S$  have a certain form and/or being clever in the choice of the element  $s$ . We elide these details for now and assume that this operation indeed satisfies  $|S'| = 2 \cdot |S|$ .

Starting from our family  $\mathcal{F}_0$  and using these two operations  $\log_2 p$  times (for a total of  $2 \log_2 p$  operations in total) each indeed gives us a  $\mathbb{Z}_p$ -covering  $(\tilde{O}(p^2), p)$ -Family of size  $p^p$ , as claimed.

### 4.1.2 Getting a Better Bound

Our main idea towards getting a better bound is to “combine” the two operations in Items 1 and 2 in order to save on some of the  $2 \log_2 p$  operations. To this end, we recall the construction of [5] (recapped in Theorem 16) that shows that if  $\ell$  is huge as compared to  $p$ , say  $\ell \geq p^{5 \log_2 \log_2 p}$ , then there exists a  $\mathbb{Z}_p$ -covering  $(\ell, p)$ -Family of size (almost)  $2^\ell$ . Observe that the above construction actually does better than simply using the operations in Items 1 and 2. Indeed, if we were to use the operations in Items 1 and 2 to get the same parameters, we would end up with an  $(\ell \cdot p, p)$ -Family instead of the  $(\ell, p)$ -Family that they get. If  $\ell = p^{5 \log_2 \log_2 p}$ , the saving is a  $\left(1 - O\left(\frac{1}{\log_2 \log_2 p}\right)\right)$  factor in the exponent, which is exactly what we want.

The problem is that their requirement that  $\ell \geq p^{5 \log_2 \log_2 p}$  is already much larger than the quadratic bound we are hoping to beat, and therefore unaffordable. However, they also use this larger value of  $\ell$  to get a family of size  $2^\ell$  which is also much larger than the  $p^p$  size family that we want to construct. Is it possible to get around their requirement at the cost of reducing the size of the obtained family?

The answer is yes, and our approach to do this starts by applying their construction for a value  $k$  that satisfies  $2^{k^{O(\log_2 \log_2 k)}} = p^p$ . As  $\log_2 \log_2 k$  and  $\log_2 \log_2 p$  are the same order of magnitude, this does not affect our improvement in the bound. At the same time, this reduces their requirement to  $\ell \geq k^{5 \log_2 \log_2 k} = p \log_2 p$  which is something we can afford and also keeps the size of the obtained family above  $p^p$ , as needed. However, the problem is that the obtained family does arithmetic over  $\mathbb{Z}_k$  (instead of  $\mathbb{Z}_p$ ) and is only  $\mathbb{Z}_k$ -covering (instead of  $\mathbb{Z}_p$ -covering). We fix these two problems next.

1. **Fixing the arithmetic:** Even though  $\mathbb{Z}_k \subseteq \mathbb{Z}_p$  and thus, every element of  $\mathbb{Z}_k$  can be “naturally” seen as an element of  $\mathbb{Z}_p$ , observe that we do not have the guarantee that a  $\mathbb{Z}_k$ -covering  $(\ell, k)$ -Family “naturally” implies a  $\mathbb{Z}_k$ -covering  $(\ell, p)$ -Family. This is because of the fact that the difference of two numbers  $a$  and  $b$  modulo  $k$  may not be the same as their difference modulo  $p$ .

However, observe that if  $a \geq b$  (as an integer), then it is indeed the case  $a - b \pmod{k}$  is the same as  $a - b \pmod{p}$ , and thus the transformation follows naturally. However, if  $a < b$  (as an integer), then  $a - b \pmod{k}$  is the same as  $a + k - b \pmod{p}$  and we do

<sup>8</sup> We define  $sS$  to be the set  $sS = \{s \cdot s' \pmod{p} \mid s' \in S\}$ .

not get the required guarantee. The way we fix this is to replace  $a$  by a vector of length  $\log_2 k$  whose  $j$ -th entry, for  $j \in [\log_2 k]$  is  $a$ , if the  $j$ -th bit in the binary representation of  $a$  is 1 and  $a + k$  otherwise (and likewise for  $b$ ).

Now, if  $a < b$  (as an integer), there exists a  $j \in [\log_2 k]$  such that the  $j$ -th bit in the binary representation of  $a$  is 0 and the  $j$ -th bit in the binary representation of  $b$  is 1. Then, the difference in the  $j$ -th entry of the vectors is exactly  $a + k - b \pmod p$ , as desired. This does blow up the length of the vector by a factor of  $\log_2 k \leq \log_2 p$  but as we save a factor of  $p^{\Omega\left(\frac{1}{\log_2 \log_2 p}\right)} \gg \log_2 p$  using the [5] construction, this is affordable.

2. **Fixing the set covered:** It remains to boost the covered set from  $\mathbb{Z}_k$  to  $\mathbb{Z}_p$ , and we do this using ideas similar to those described in the boosting operation in Item 2 above. Specifically, we take  $M = \frac{p \cdot \log_2 p}{k}$  random elements  $s_1, \dots, s_M$  and replace each vector  $\vec{v}$  in the original family with the vector  $(s_1 \cdot \vec{v}, \dots, s_M \cdot \vec{v})$ .<sup>9</sup> This ensures that new family covers the set  $s_1 \mathbb{Z}_k \cup \dots \cup s_M \mathbb{Z}_k$ , which can be shown to be equal to  $\mathbb{Z}_p$  with non-zero probability. Thus, there exists a choice of  $s_1, \dots, s_M$  such that the resulting family will be  $\mathbb{Z}_p$ -covering, as desired.

### 4.1.3 Limitations

We finish this section with some remarks on the limitations of our two boosting operations. Observe that our two operations are extremely simple, only requiring concatenation and scaling of vectors in the original family. On the other hand, the [5] construction we use as a starting point is significantly more involved. One may wonder whether it is possible to get a better than quadratic bound using simple concatenation procedures alone and not work with the [5] construction at all.

In Section 4.4, we show that this is not possible, by studying a broad class of concatenation procedures, that we call agnostic, and showing that they do not give any significant improvement over applying the two boosting operations in Items 1 and 2 separately. This shows not only that we must use something more involved like [5] but also that our procedure to fix the set covered in Item 2 in Section 4.1.2 is almost tight amongst a large class of procedures. We conclude that the possible avenues towards better bounds on  $\text{AAM}(p, p^p)$  using a similar approach are:

- (a) a better starting point than Theorem 16, or
- (b) a vastly different boosting procedure.

## 4.2 A Key Theorem

In this section, we prove Theorem 1. The core of the proof is the following improved bound on  $\text{AAM}(p, p^p)$ :

- **Theorem 10.** *For all primes  $p > p_0$  large enough, we have:*

$$\text{AAM}(p, p^p) \leq p^{2 - \Omega\left(\frac{1}{\log_2 \log_2 p}\right)}.$$

Before proving Theorem 10, we show why it implies Theorem 1.

---

<sup>9</sup> Recall that we only want to increase the size of the set covered by a factor of  $\frac{p}{k}$  and we increase the length by a factor of  $M = \frac{p \cdot \log_2 p}{k}$ . The extra  $\log_2 p$  factor is again affordable as it is much smaller than  $p^{\Omega\left(\frac{1}{\log_2 \log_2 p}\right)}$ .

**Proof of Theorem 1.** The inequality  $\alpha(\mathcal{C}_{\text{PARTINT}}(q)) \geq \alpha(\mathcal{C}_{\text{SYMPARTINT}}(q), \mathcal{P}_{\text{IDBERNOULLI}})$  is straightforward from our definitions. Thus, it suffices to show that  $\alpha(\mathcal{C}_{\text{SYMPARTINT}}(q), \mathcal{P}_{\text{IDBERNOULLI}}) \geq q^{1/2+\Omega(1/\log_2 \log_2 q)}$ . Owing to Proposition 8, this follows if we show that for all large enough  $q$ , there exists  $p \geq q^{1/2+\Omega(1/\log_2 \log_2 q)}$  such that  $\text{AAM}(p, p^p) \leq q$ . This is because, by Theorem 10 and with an appropriate choice of constants, we have:

$$\text{AAM}(p, p^p) \leq p^{2-\Omega\left(\frac{1}{\log_2 \log_2 p}\right)} \leq q^{\left(\frac{1}{2}+\Omega\left(\frac{1}{\log_2 \log_2 q}\right)\right)} \cdot \left(2^{-\Omega\left(\frac{1}{\log_2 \log_2 p}\right)}\right) \leq q. \quad \blacktriangleleft$$

### 4.3 Proof of Theorem 10

We now prove Theorem 10 by showing the following stronger theorem, that proves a bound on  $\text{AAM}(p, N)$ , for general  $N$ .

► **Theorem 11.** *For all  $p, N$  large enough that satisfy  $N \leq 2^{p^{\log_2 \log_2 p}}$ , we have:*

$$\text{AAM}(p, N) \leq p \log_2 p \cdot (\log_2 N)^{\left(1-\Omega\left(\frac{1}{\log_2 \log_2 \log_2 N}\right)\right)}.$$

Indeed, Theorem 11 implies Theorem 10, as plugging  $N = p^p$  gives:

$$\text{AAM}(p, p^p) \leq (p \log_2 p)^{2-\Omega\left(\frac{1}{\log_2 \log_2 p}\right)} \leq p^{2-\Omega\left(\frac{1}{\log_2 \log_2 p}\right)}.$$

Thus, it suffices to show Theorem 11, which we do in the rest of this section. Fix  $p, N$  as in the statement of Theorem 11 and define  $\ell_1 = 2 \log_2 N$  and  $k$  to be the largest prime that satisfies  $k^{5 \log_2 \log_2 k} \leq \log_2 N$ . As it is well known that there is a prime between  $m$  and  $2m$  for every integer  $m$  and we have  $N \leq 2^{p^{\log_2 \log_2 p}}$ , our choice of  $k$  implies that  $(\log_2 N)^{\frac{1}{15 \log_2 \log_2 \log_2 N}} \leq k \leq p$  and thus, Theorem 11 follows if we show that:

$$\text{AAM}(p, N) \leq \frac{p \log_2 p \log_2 N}{\sqrt{k}}. \quad (1)$$

Henceforth, we denote the right hand side in Equation (1) by  $\ell^*$ . We start by applying Theorem 16 (which can be applied as  $N$ , and therefore  $k$ , is large enough) with  $k$  and  $\ell = \ell_1$  to get that there exists  $\mathbb{Z}_k$ -covering  $(\ell_1, k)$ -Family  $\mathcal{F}_1$  of size at least  $N$ .

The existence of  $\mathcal{F}_1$  makes some progress towards Equation (1), which by Definition 4 requires us to show  $\mathbb{Z}_p$ -covering  $(\ell^*, p)$ -Family of size  $N$ . However, a key difference is that the arithmetic in the family  $\mathcal{F}_1$  is done modulo  $k$  while we desire a family with arithmetic modulo  $p$ . We show how to do this in the next lemma, that also blows up  $\ell_1$  by a small factor. Define  $\ell_2 = 2\ell_1 \cdot \log_2 k$ .

► **Lemma 12.** *There exists a  $[0, k-1]$ -covering  $(\ell_2, p)$ -family  $\mathcal{F}_2$  of size  $N$ .*

**Proof.** For every  $\vec{u} \in \mathcal{F}_1$  (which we interpret as an element of  $\mathbb{Z}_p^{\ell_1}$ ), we construct a vector  $\vec{v} \in \mathbb{Z}_p^{\ell_2}$  and define  $\mathcal{F}_2$  to be the set containing all the constructed  $\vec{v}$ . To construct  $\vec{v}$  from  $\vec{u}$ , we use the following procedure: To start, define  $\vec{v}$  to be  $2 \log_2 k$  copies of  $\vec{u}$ , concatenated to each other. We keep the last  $\log_2 k$  copies unchanged<sup>10</sup> but update the first  $\log_2 k$  copies. In this update, for copy  $j \in [\log_2 k]$ , we add  $k$  to every coordinate whose  $j$ -th bit in its binary representation is 0. More formally, for  $i \in [\ell_1]$ , if the  $j$ -th bit in the binary representation of  $u_i$  is 0, we set coordinate  $i$  in copy  $j$  to be  $u_i + k \pmod{p}$ , and keep it unchanged as  $u_i$  otherwise.

<sup>10</sup> Actually, only 1 out of these  $\log_2 k$  are needed to make the argument work. The remaining are used only to ensure that the length of  $\vec{v}$  is as needed.

## 95:12 An Improved Lower Bound for Matroid Intersection Prophet Inequalities

Due to the unchanged copies, the constructed  $\vec{v}$  are all distinct, and thus the size of  $\mathcal{F}_2$  is  $N$ , as needed. It remains to show that  $\mathcal{F}_2$  is  $[0, k-1]$ -covering. Consider any two distinct vectors  $\vec{v}, \vec{v}' \in \mathcal{F}_2$  and let  $u, u'$  be the elements of  $\mathcal{F}_1$  they are constructed from. We need to show that for all  $k' \in [0, k-1]$ , there is a coordinate where  $\vec{v}$  and  $\vec{v}'$  differ by  $k'$  modulo  $p$ . For this, note first that as  $\mathcal{F}_1$  is a  $\mathbb{Z}_k$ -covering  $(\ell_1, k)$ -Family, there exists a coordinate  $i \in [\ell_1]$  such that  $u_i - u'_i = k' \pmod{k}$ . Viewing  $u_i$  and  $u'_i$  as integers, this implies that either  $u_i - u'_i = k'$  or  $u_i - u'_i = k' - k$ . As the former case implies that  $u_i - u'_i = k' \pmod{p}$ , we are done by taking coordinate  $i$  in the last copy of  $\vec{v}$  and  $\vec{v}'$ .

For the latter case, note that this only happens if  $u_i < u'_i$  (as an integer). Thus, there exists  $j \in [\log_2 k]$  such that the  $j$ -th bit in the binary representation  $u_i$  is 0 and the  $j$ -th bit in the binary representation  $u'_i$  is 1. This means that coordinate  $i$  in the copy  $j$  of  $\vec{v}$  is  $u_i + k \pmod{p}$  and coordinate  $i$  in the copy  $j$  of  $\vec{v}'$  is  $u'_i$ . It follows that the difference is  $k' \pmod{p}$  as desired.  $\blacktriangleleft$

Finally, we use  $\mathcal{F}_2$  to construct an  $\mathbb{Z}_p$ -covering  $(\ell^*, p)$ -Family of size  $N$ , finishing the proof. We will do this by creating many copies of all vectors in  $\mathcal{F}_2$  and “scaling” each copy appropriately. To show that such a scaling is possible, we need the following lemma:

► **Lemma 13.** *There exists a set  $S \subseteq \mathbb{Z}_p$  with  $|S| \leq \frac{p \ln p}{k-1}$  such that for all  $g \in \mathbb{Z}_p$ , there exist  $i \in [0, k-1]$  and  $j \in S$  such that  $i \cdot j = g \pmod{p}$ .*

**Proof.** We prove this via the probabilistic method. Draw  $\frac{p \ln p}{k-1}$  elements (as  $k \leq p$ ,  $\frac{p \ln p}{k-1}$  can be made an integer by multiplying by a small constant) from  $\mathbb{Z}_p$  uniformly at random with replacement and let  $S$  be the set of these elements. Clearly, we have  $|S| \leq \frac{p \ln p}{k-1}$  and it suffices to show that the probability that there exists  $g \in \mathbb{Z}_p$  such that for all  $i \in [0, k-1]$ ,  $j \in S$  we have  $i \cdot j \neq g \pmod{p}$  is strictly smaller than 1. For this we union bound over all the  $p$  values of  $g$  and show that for a fixed  $g$ , the probability that for all  $i \in [0, k-1]$ ,  $j \in S$  we have  $i \cdot j \neq g \pmod{p}$  is strictly smaller than  $1/p$ .

This is clearly true for  $g = 0$  as the fact that  $i$  can be 0 implies the stated event will never happen. If  $g \neq 0$ , the probability the stated event happens is exactly the probability that none of the elements  $g \cdot 1^{-1}, \dots, g \cdot (k-1)^{-1}$  (inverses modulo  $p$ ) are ever sampled, which is  $\left(1 - \frac{k-1}{p}\right)^{\frac{p \ln p}{k-1}} < e^{-\ln p} = 1/p$ .  $\blacktriangleleft$

We are now ready to finish the proof of Theorem 11.

**Proof of Theorem 11.** As hinted above, we create many copies of all vectors in  $\mathcal{F}_2$  and scale each copy appropriately. Specifically, let  $S$  be the set promised by Lemma 13 and let  $s_1, \dots, s_{|S|}$  be the elements of  $S$ . Define  $\ell_3 = |S| \cdot \ell_2$ . Construct an  $(\ell_3, p)$ -family  $\mathcal{F}_3$  of size  $N$  by constructing, for every  $\vec{v} \in \mathcal{F}_2$ , a vector  $\vec{w} = (s_1 \cdot \vec{v}, \dots, s_{|S|} \cdot \vec{v})$  and adding it to  $S$ . As Lemma 13 implies that there are non-zero elements in  $S$ , the constructed  $\vec{w}$  are different for every  $\vec{v}$ , and thus the size of  $\mathcal{F}_3$  equals that of  $\mathcal{F}_2$ , which is  $N$ .

We claim that  $\mathcal{F}_3$  is  $\mathbb{Z}_p$ -covering. Consider any two distinct vectors  $\vec{w}, \vec{w}' \in \mathcal{F}_3$  and let  $\vec{v}, \vec{v}'$  be the elements of  $\mathcal{F}_2$  they are constructed from. We need to show that for all  $g \in \mathbb{Z}_p$ , there is a coordinate where  $\vec{w}$  and  $\vec{w}'$  differ by  $g$  modulo  $p$ . Let  $i \in [0, k-1]$  and  $j \in |S|$  be such that  $i \cdot s_j = g \pmod{p}$  and note that these exist by Lemma 13. Note first that as  $\mathcal{F}_2$  is a  $[0, k-1]$ -covering  $(\ell_2, p)$ -Family, there exists a coordinate  $a \in [\ell_2]$  such that  $\vec{v}_a - \vec{v}'_a = i \pmod{p}$ . This means that in copy  $j$  of  $\vec{w}$  and  $\vec{w}'$ , the  $i$ -th coordinates differ by  $s_j \cdot (\vec{v}_a - \vec{v}'_a) = i \cdot s_j = g \pmod{p}$ , as desired. As  $k$  is large enough, we also have:

$$\ell_3 = |S| \cdot \ell_2 \leq \frac{p \ln p}{k-1} \cdot \ell_2 = \frac{p \ln p}{k-1} \cdot 4 \cdot \log_2 k \cdot \log_2 N < \ell^*,$$

and Equation (1) follows and we are done.  $\blacktriangleleft$

## 4.4 Limitations of Our Approach

This section fleshes out the limitations of our approach that we discussed at a high level in Section 4.1.3. We start by defining an agnostic concatenation procedure.

► **Definition 14** (Concatenation Procedure). *Let  $z, k, k', p$  be integers such that  $k \leq k' \leq p$ . A  $(z, k, k', p)$ -agnostic concatenation procedure takes as input a sequence  $(\alpha_1, \dots, \alpha_z)$ , where each  $\alpha_j \in \mathbb{Z}_p \setminus \{0\}$  and an  $S$ -covering  $(\ell, p)$ -Family  $\mathcal{V}$ , for some  $\ell > 0$  and some set  $S \subseteq \mathbb{Z}_p \setminus \{0\}$  of size  $k^{11}$  and outputs a set  $S' \subseteq \mathbb{Z}_p \setminus \{0\}$  of size  $k'$  and the largest  $S'$ -covering  $(z\ell, p)$ -Family  $\mathcal{V}'$  that is a subset of the set  $\mathcal{W} := \{(\alpha_1 \vec{v}_1, \dots, \alpha_z \vec{v}_z) \mid \forall j \in [z] : \vec{v}_j \in \mathcal{V}\}$ .*

*For  $\eta > 0$ , we say that the concatenation procedure boosts the size by  $\eta$  if  $|\mathcal{V}'| \geq |\mathcal{V}|^\eta$  regardless of the choice of  $\mathcal{V}$  (and therefore, also regardless of  $\ell$  and  $S$ ).*

Observe that the two boosting procedures mentioned in Section 4.1.1 are indeed agnostic concatenation procedures. The first one is a  $(2, k, k, p)$ -agnostic concatenation procedure (for all integers  $k$ ) that boosts the size by 2 as it increases the length by a factor of 2 and squares the size. The second one is a  $(2, k, 2k, p)$ -agnostic concatenation procedure (for all integers  $k < \sqrt{p}$ ) that boosts the size by 1 as it increases length by a factor of 2 and keeps the size unchanged. Note that we assume  $k < \sqrt{p}$  in the second one as that ensures that for all sets  $S \subseteq \mathbb{Z}_p \setminus \{0\}$  of size  $k$ , there exists  $s \in \mathbb{Z}_p$  such that  $S$  and  $sS$  are disjoint, as needed for Item 2 in Section 4.1.1. To avoid such issues, we assume that  $k$  is small enough in this section.

By combining these two procedures in sequence, it is possible to get for any integers  $a$  and  $b$ , a  $(2^{a+b}, k, 2^b k, p)$ -agnostic concatenation procedure that boosts the size by  $2^a$ . We show that, up to constants, this is the best possible bound for all agnostic concatenation procedures.

► **Proposition 15.** *Let  $z, k, k', p$  be integers and  $k \leq k' \leq p$ . Every  $(z, k, k', p)$ -agnostic concatenation procedure boosts the size by at most  $\frac{4kz}{k'}$  (even for small  $k$ ).*

**Proof.** Fix an  $(z, k, k', p)$ -agnostic concatenation procedure and a sequence  $(\alpha_1, \dots, \alpha_z)$ . Let  $\mathcal{V}$  be the  $[0, k-1]$ -covering  $(\ell_2, p)$ -family  $\mathcal{F}_2$  constructed in Lemma 12. We run the procedure on  $(\alpha_1, \dots, \alpha_z)$  and  $\mathcal{V}$  and let  $S'$  and  $\mathcal{V}'$  be its output.

Observe that every coordinate of every vector in  $\mathcal{V}$  lies in  $[0, 2k-1] \pmod{p}$ . This immediately implies that for any  $\vec{v}, \vec{w} \in \mathcal{V}$  and every coordinate  $i$ , we have  $v_i - w_i \in [1-2k, 2k-1] \pmod{p}$ , and in particular there are at most  $4k-1$  possibilities. Use this to conclude that for all  $j \in [z]$ , the set  $S_j = \{\alpha_j \cdot (v_i - w_i) \mid i \in [\ell_2], \vec{v}, \vec{w} \in \mathcal{V}\}$  satisfies  $|S_j| < 4k$ .

Next, define  $S'$  to be the set output by the  $(z, k, k', p)$ -agnostic concatenation procedure and recall that  $|S'| = k'$  and  $0 \notin S'$ . As  $|S_j| < 4k$  for all  $j \in [z]$ , there exists a  $g' \in S'$  such that  $g' \in S_j$  for at most  $\frac{4kz}{k'}$  many values of  $j \in [z]$ . Define  $T = \{j \in [z] \mid g' \in S_j\}$  to be the set of these values and note that  $|T| \leq \frac{4kz}{k'}$ .

Now, consider any two elements  $\vec{v} := (\alpha_1 \vec{v}_1, \dots, \alpha_z \vec{v}_z), \vec{w} := (\alpha_1 \vec{w}_1, \dots, \alpha_z \vec{w}_z)$  of the set  $\mathcal{V}'$  output by the  $(z, k, k', p)$ -agnostic concatenation procedure. By definition, the pair  $(\vec{v}, \vec{w})$  is  $S'$  covering and therefore, there exists  $j \in [z]$  and  $i \in [\ell_2]$  such that  $\alpha_j \cdot (\vec{v}_{j,i} - \vec{w}_{j,i}) = g' \pmod{p}$ . As  $g' \in S'$  implies  $g' \neq 0$ , this is only possible if  $\vec{v}_j \neq \vec{w}_j$  and  $g' \in S_j \implies j \in T$ . Overall, we get that for any two vectors  $\vec{v}, \vec{w} \in \mathcal{V}'$ , there exists  $j \in T$  such that  $\vec{v}_j \neq \vec{w}_j$ .

However, this means that  $|\mathcal{V}'| \leq |\mathcal{V}|^{|T|} \leq |\mathcal{V}|^{\frac{4kz}{k'}}$  and the lemma follows. ◀

<sup>11</sup>That  $0 \notin S$  is without loss of generality as getting a 0-covering family is easy.

## 5 Summary of [5]

The goal of this section is to prove the following theorem, which is a quantitative statement of the main result of [5].

► **Theorem 16.** *There exists a sufficiently large  $p_1$  such that for all primes  $p > p_1$  and all  $\ell \geq p^{5 \log \log p}$ , there is a  $\mathbb{Z}_p$ -covering  $(\ell, p)$ -Family of size at least  $\left(2 - \frac{1}{\log p}\right)^\ell$ .*

To prove Theorem 16, we actually show the following result which implies it.

► **Theorem 17.** *There exists a sufficiently large  $p_1$  such that for all primes  $p > p_1$ , there exists an  $\ell(p) \leq p^{4 \log \log p}$  for which there is a  $(\mathbb{Z}_p \setminus \{0\})$ -covering  $(\ell, p)$ -Family  $\mathcal{A}(p)$  of size at least  $\left(2 - \frac{0.75}{\log p}\right)^{\ell(p)}$ .*

We argue why Theorem 16 follows from Theorem 17.

**Proof of Theorem 16 assuming Theorem 17.** Fix  $p, \ell$  as in Theorem 16. Let  $\ell'$  be the largest integer multiple of  $\ell(p)$  that is strictly smaller than  $\ell$ . We claim that there exists a  $(\mathbb{Z}_p \setminus \{0\})$ -covering  $(\ell', p)$ -Family  $\mathcal{A}'$  of size at least  $\left(2 - \frac{0.75}{\log p}\right)^{\ell'}$ . Indeed, consider the set of all vectors formed by concatenating  $\ell/\ell'$  elements of  $\mathcal{A}(p)$  together. This set clearly has size  $\left(2 - \frac{0.75}{\log p}\right)^\ell$ , and is clearly still  $(\mathbb{Z}_p \setminus \{0\})$ -covering.

Next, define an  $(\ell, p)$ -Family  $\mathcal{A}$  to be the same as the family  $\mathcal{A}'$  except that each element in  $\mathcal{A}'$  is appended by  $\ell - \ell'$  zeros. Note that  $\mathcal{A}$  is  $\mathbb{Z}_p$ -covering because  $\mathcal{A}'$  is  $(\mathbb{Z}_p \setminus \{0\})$ -covering. Thus, the only remaining step in the proof is to show that  $|\mathcal{A}| \geq \left(2 - \frac{1}{\log p}\right)^\ell$ . This is because our choice of  $\ell'$  implies:

$$|\mathcal{A}| = |\mathcal{A}'| \geq \left(2 - \frac{0.75}{\log p}\right)^{\ell'} \geq \left(2 - \frac{0.75}{\log p}\right)^{\ell - p^{4 \log \log p}} \geq \left(2 - \frac{1}{\log p}\right)^\ell.$$

The final inequality holds for sufficiently large  $p$ , which defines  $p_1$ . ◀

The rest of this section is dedicated to proving Theorem 17. Fix  $p$  as in the statement of Theorem 17. We first capture the main steps of [5] in Sections 5.1 and 5.2, and finally establish Theorem 17 in Section 5.3.

### 5.1 Families Closed Under Multiplication

For a set  $S \subseteq \mathbb{Z}_p$  and a value  $a \in \mathbb{Z}_p$ , we use  $aS$  to denote the set  $aS = \{as \mid s \in S\}$ . The main result of this section is Lemma 19, which provides a technique to turn a (structured)  $S$ -covering family into an  $(aS \cup S)$ -covering family for any  $a \in \mathbb{Z}_p$ . This procedure is a key step that will be applied repeatedly to grow from a family that covers a small set to a  $\mathbb{Z}_p$ -covering family.

► **Definition 18.** *Let  $\ell > 0$  be an integer and  $\mathcal{V}$  be an  $(\ell, p)$ -Family. We say that  $\mathcal{V}$  is closed under scalar multiplication if for all  $a \neq 0 \in \mathbb{Z}_p$  and all  $\vec{v} \in \mathcal{V}$ , we have  $a\vec{v} \in \mathcal{V}$ .*

► **Lemma 19.** *Let  $\ell > 0$  be an integer and  $\mathcal{V}$  be an  $(\ell, p)$ -Family closed under scalar multiplication. Let  $S \subseteq \mathbb{Z}_p$ . If there exist integers  $N, K > 0$  such that  $\mathcal{V}$  can be partitioned into  $K$  (disjoint)  $S$ -covering families  $\mathcal{V} = \mathcal{V}_1 \cup \dots \cup \mathcal{V}_K$ , each of size at least  $N$ , then, for all  $m \geq 0$  and all  $a \neq 0 \in \mathbb{Z}_p$ , there exists an  $((m+1)\ell, p)$ -Family  $\mathcal{V}' \subseteq \mathcal{V}^{m+1}$  of size at least  $\frac{N^m}{|\mathcal{V}|}$  that is  $(aS \cup S)$ -covering.*



**Proof.** In this proof, for  $z > 0$ , it shall sometimes be convenient to view vectors in  $\mathbb{Z}_p^{z\ell}$  and elements of  $(\mathbb{Z}_p^\ell)^z$ . For a vector  $\vec{v} \in \mathcal{V}$ , we define the value  $k(\vec{v})$  to be the unique value  $k \in [K]$  such that  $\vec{v} \in \mathcal{V}_k$ . Observe that  $k(\vec{v})$  is well defined as  $\mathcal{V}_1 \cup \dots \cup \mathcal{V}_K$  form a partition of  $\mathcal{V}$ . Let  $\vec{w}_0 \in \mathcal{V}$  be arbitrary. For all  $z > 0$ , define the  $(z\ell, p)$  family  $\mathcal{W}_z$  as the set of all  $z$ -tuples  $(\vec{w}_1, \dots, \vec{w}_z)$  of elements of  $\mathcal{V}$  such that for all  $i$ ,  $\vec{w}_i$  is in the same part as  $a^{-1}\vec{w}_{i-1}$  (observe that because  $\mathcal{V}$  is closed under scalar multiplication,  $a^{-1}\vec{w}_{i-1} \in \mathcal{V}$ ). That is:

$$\mathcal{W}_z = \{ \vec{w} \in \mathcal{V}^z \mid \forall i \in [z] : \vec{w}_i \in \mathcal{V}_{k(a^{-1}\vec{w}_{i-1})} \}.$$

We claim that for all  $z > 0$ , we have  $|\mathcal{W}_z| \geq N^z$ . Indeed, observe that when  $z = 1$ ,  $\mathcal{W}_1$  consists of all  $\vec{w}_1$  such that  $\vec{w}_1$  is in the same part as  $a^{-1}\vec{w}_0$ . Whatever part this is, it contains at least  $N$  elements (by hypothesis in the lemma statement), so therefore the claim holds for  $z = 1$ . We now prove the claim for all  $z$  by induction. Indeed, observe that every element of  $\mathcal{W}_z$  is an element  $(\vec{w}_1, \dots, \vec{w}_{z-1})$  of  $\mathcal{W}_{z-1}$  concatenated by some  $\vec{w}_z$  in the same part as  $a^{-1}\vec{w}_{z-1}$ . Whatever part this is, it has size at least  $N$  by hypothesis. Therefore, for every element in  $\mathcal{W}_{z-1}$ , there are at least  $N$  ways to extend it to an element in  $\mathcal{W}_z$ , and each of these extensions are unique. This implies that  $|\mathcal{W}_z| \geq N^z$  for all  $z > 0$ , and in particular that  $|\mathcal{W}_m| \geq N^m$ .

We now partition the elements  $\vec{w}$  of the set  $\mathcal{W}_m$  based on the value of  $\vec{w}_m$  (the last coordinate), and define  $\vec{v}^* \in \mathcal{V}$  to be such that the part corresponding to  $\vec{w}_m = \vec{v}^*$  is the largest, breaking ties arbitrarily. We define our set  $\mathcal{V}'$  using this part, specifically:

$$\mathcal{V}' = \{ \vec{w}' \in (\mathbb{Z}_p^\ell)^{m-1} \mid (\vec{w}', \vec{v}^*) \in \mathcal{W}_m \}.$$

Observe that  $\mathcal{V}' \subseteq \mathcal{V}^{m-1}$ . Also, by our choice of  $\vec{v}^*$ , we have  $|\mathcal{V}'| \geq \frac{N^m}{|\mathcal{V}|}$ , as claimed. It remains to show that  $\mathcal{V}$  is  $(aS \cup S)$ -covering. For this we recall Definition 3 and fix two arbitrary vectors  $\vec{v} \neq \vec{v}' \in \mathcal{V}'$ . As  $\vec{v} \neq \vec{v}'$ , there exists an  $i \in [m-1]$  such that  $\vec{v}_i \neq \vec{v}'_i$ . Define  $i_s$  and  $i_b$  to be the smallest and the largest such  $i$ , respectively. As both  $(\vec{v}, \vec{v}^*), (\vec{v}', \vec{v}^*) \in \mathcal{W}_m$  by definition of  $\mathcal{V}'$ , we get (defining  $\vec{v}_m = \vec{v}'_m = \vec{v}^*$  for convenience):

$$\vec{v}_{i_s}, \vec{v}'_{i_s} \in \mathcal{V}_{k(a^{-1}\vec{w}_{i_s-1})} \quad \text{and} \quad \vec{v}_{i_b+1} \in \mathcal{V}_{k(a^{-1}\vec{v}_{i_b})} \cap \mathcal{V}_{k(a^{-1}\vec{v}'_{i_b})}.$$

As  $\vec{v}_{i_s} \neq \vec{v}'_{i_s}$  by our choice of  $i_s$  and we have that  $\mathcal{V}_{k(a^{-1}\vec{w}_{i_s-1})}$  is  $S$ -covering, we get from the former that for all  $s' \in S$ , there exists  $j \in [\ell]$  such that  $\vec{v}_{i_s,j} - \vec{v}'_{i_s,j} = s' \pmod{p}$ . Similarly, as the sets  $\mathcal{V}_1 \cup \dots \cup \mathcal{V}_K$  form a partition of  $\mathcal{V}$ , the latter is only possible if  $k(a^{-1}\vec{v}_{i_b}) = k(a^{-1}\vec{v}'_{i_b})$ . However, this means that there exists  $k \in [K]$  such that  $a^{-1}\vec{v}_{i_b} \neq a^{-1}\vec{v}'_{i_b}$  are two elements of  $\mathcal{V}_k$ . As  $\mathcal{V}_k$  is  $S$ -covering, this means that for all  $s' \in aS$ , there exists  $j \in [\ell]$  such that  $\vec{v}_{i_b,j} - \vec{v}'_{i_b,j} = s' \pmod{p}$ . Combining the two results and using Definition 3, we get that  $\mathcal{V}$  is  $(aS \cup S)$ -covering, as desired.  $\blacktriangleleft$

## 5.2 Balanced Codewords

This section introduced Balanced Codewords, the main object used to build a base case family that covers a small set, and that is structured enough to repeatedly apply until it covers all of  $\mathbb{Z}_p$  Lemma 19.

For a non-negative integer  $\ell$  that is a multiple of  $p-1$ , we define  $\mathcal{B}_\ell$  to be the  $(\ell, p)$ -Family such that all  $\vec{b} \in \mathcal{B}$  contain all elements  $a \neq 0 \in \mathbb{Z}_p$  the same number of times and do not contain 0. In particular, we have that the family  $\mathcal{B}_\ell$  is closed under scalar multiplication

► **Lemma 20.** *Consider an integer  $\ell > 0$  that is a multiple of  $p-1$ . Let  $S \subseteq \mathbb{Z}_p$  and  $\mathcal{A} \subseteq \mathcal{B}_\ell$  be an  $S$ -covering  $(\ell, p)$ -Family of size at least  $10\ell \cdot \log p$ . There exists  $K > 0$  and a partition  $\mathcal{B}_\ell = \mathcal{C}_1 \cup \dots \cup \mathcal{C}_K$  such that for all  $k \in [K]$ , we have that  $\mathcal{C}_k$  is an  $S$ -covering family of size at least  $\frac{|\mathcal{A}|}{10\ell \cdot \log p}$ .*

## 95:16 An Improved Lower Bound for Matroid Intersection Prophet Inequalities

**Proof.** The proof will use the following lemma (from [5]) that is based on the well-known Hall's theorem.

► **Lemma 21** ([5], Lemma 2.1). *Let  $G = (L \cup R, E)$  be a bipartite graph such that all vertices in  $L$  have the same degree, say  $d_L$ , and all vertices in  $R$  have the same degree, say  $d_R$ . Assume that  $d_R \geq \log(2|R|)$ . There exists a subset of  $E$  that is a union of vertex-disjoint stars with centers in  $L$ , each star having at least  $\frac{d_L}{4 \cdot \log(2|R|)}$  leaves, such that all vertices of  $R$  are leaves.*

To see why Lemma 21 holds, note that if we only had to show a bound of  $\frac{d_L}{d_R}$  on the number of leaves, it would follow from Hall's theorem. In fact, this would hold even under the weaker assumption that all vertices in  $R$  have degree at most  $d_R$ . Lemma 21 now follows as one can use  $d_R \geq \log(2|R|)$  to subsample vertices in  $L$  so that the degree of each vertex in  $R$  is reduced to be between 1 and  $4 \cdot \log(2|R|)$ .

We now prove Lemma 20. Define a bipartite graph  $G = (L \cup R, E)$  where  $L$  is the set of all permutations  $\pi$  on  $\ell$  elements and  $R$  is the set  $\mathcal{B}_\ell$ . A vertex  $\pi \in L$  is adjacent to a vertex  $\vec{b} \in R$  if and only if  $\pi(\vec{b}) \in \mathcal{A}$ , where  $\pi(\vec{b})$  denotes the string obtained by permuting the coordinates of  $\vec{b}$  according to  $\pi$ . Using the notation of Lemma 21, we have for this graph that:

$$\begin{aligned} |L| &= \ell! & |R| &= \frac{\ell!}{((\ell/(p-1))!)^{p-1}} \leq p^\ell \\ d_L &= |\mathcal{A}| & d_R &= \frac{|L| \cdot |\mathcal{A}|}{|R|} \geq |\mathcal{A}| \geq \log(2|R|). \end{aligned}$$

Thus, we can apply Lemma 21 and get a union of vertex-disjoint stars as claimed in the lemma. We get that the leaves of these stars form a partition of  $R = \mathcal{B}_\ell$ , and we define  $K$  to be the number of stars and  $\mathcal{B}_\ell = \mathcal{C}_1 \cup \dots \cup \mathcal{C}_K$  to be the partition. By Lemma 21, we have for all  $k \in [K]$  that  $|\mathcal{C}_k| \geq \frac{|\mathcal{A}|}{10\ell \cdot \log p}$  and to finish the proof it suffices to show that  $\mathcal{C}_k$  is  $S$ -covering for all  $k \in [K]$ . We do this next using Definition 3.

Fix  $k \in [K]$ . Let  $\vec{b} \neq \vec{b}'$  be a pair of elements in  $\mathcal{C}_k$ . By definition of our bipartite graph  $G$ , there exists  $\pi \in L$  such that  $\pi(\vec{b}), \pi(\vec{b}') \in \mathcal{A}$ . As  $\mathcal{A}$  is  $S$ -covering, we get that the pair  $\pi(\vec{b}), \pi(\vec{b})'$  is  $S$ -covering. It follows that the pair  $\vec{b}, \vec{b}'$  is also  $S$ -covering, finishing the proof. ◀

### 5.3 Proof of Theorem 17

We now prove Theorem 17

**Proof of Theorem 17.** Let  $\ell = p(p-1) \cdot p^{3.5 \log \log p}$ . We shall actually show a stronger statement, as explained next. Let  $\alpha$  be a primitive root of  $p$ . For  $z \geq 0$ , define  $\ell_z = p(p-1) \cdot 2^{3.5z \cdot \log \log p}$  and the set  $S_z = \{\alpha^0, \alpha^1, \alpha^2, \alpha^3, \dots, \alpha^{2^z-1}\}$ . We will show that for all  $0 \leq z \leq \log p$ , there exists an  $S_z$ -covering  $(\ell_z, p)$ -Family  $\mathcal{A}_z$  of size at least  $\left(2 - \frac{0.5(z+1)}{(\log p)^2}\right)^{\ell_z}$  that satisfies  $\mathcal{A}_z \subseteq \mathcal{B}_{\ell_z}$ . The theorem then follows by taking  $z = \log p$  and using the fact that  $(\mathbb{Z}_p \setminus \{0\}) \subseteq S_{\log p}$  (which is because  $\alpha$  is a generator). We define  $\mathcal{A}_z$  inductively.

**Base case.** For the base case, we define  $\mathcal{A}_0$  to be the set of all  $\vec{b} \in \mathcal{B}_{\ell_0}$  for which the first  $\frac{2\ell_0}{p-1}$  locations only contain the elements 1 and 2 and contain them the same number of times, the next  $\frac{2\ell_0}{p-1}$  locations only contain the elements 3 and 4 and contain them the same number of times, and so on. Note that  $\mathcal{A}_0 \subseteq \mathcal{B}_{\ell_0}$  is  $S_0$  covering and satisfies  $\binom{2n}{n} \geq \frac{2^{2n}}{2^n}$  for all  $n > 0$ ):

$$|\mathcal{A}_0| = \left( \frac{2\ell_0}{p-1} \right)^{\frac{p-1}{2}} \geq \frac{2^{\ell_0}}{\left( \frac{2\ell_0}{p-1} \right)^{\frac{p-1}{2}}} \geq \left( 2 - \frac{0.5}{(\log p)^2} \right)^{\ell_0}.$$

**Inductive case.** For the inductive case, we consider  $z > 0$  and define  $\mathcal{A}_z$  assuming  $\mathcal{A}_{z-1}$  is already defined. First, apply Lemma 20 to get an integer  $K_{z-1} > 0$  and a partition  $\mathcal{B}_{\ell_{z-1}} = \mathcal{C}_{z-1,1} \cup \dots \cup \mathcal{C}_{z-1,K_{z-1}}$  of  $\mathcal{B}_{\ell_{z-1}}$  such that for all  $k \in [K_{z-1}]$ , we have that  $\mathcal{C}_{z-1,k}$  is an  $S_{z-1}$ -covering family of size at least  $\frac{|\mathcal{A}_{z-1}|}{10\ell_{z-1} \cdot \log p} \geq \frac{1}{\ell_{z-1}^2} \cdot \left( 2 - \frac{0.5z}{(\log p)^2} \right)^{\ell_{z-1}}$ .

We can now apply Lemma 19 (as  $\mathcal{B}_{\ell_{z-1}}$  is closed under scalar multiplication) with  $m = (\log p)^{3.5} + 1$  and  $a = \alpha^{2^{z-1}}$  to get an  $S_z$ -covering  $(\ell_z, p)$ -family  $\mathcal{A}_z \subseteq \mathcal{B}_{\ell_z}$  of size at least:

$$\begin{aligned} |\mathcal{A}_z| &\geq \left( \frac{1}{\ell_{z-1}^2} \cdot \left( 2 - \frac{0.5z}{(\log p)^2} \right)^{\ell_{z-1}} \right)^m \cdot \frac{1}{|\mathcal{B}_{\ell_{z-1}}|} \\ &\geq \left( \frac{1}{\ell_{z-1}^2} \cdot \left( 2 - \frac{0.5z}{(\log p)^2} \right)^{\ell_{z-1}} \right)^m \cdot \frac{1}{p^{\ell_{z-1}}} \\ &\geq \left( \frac{1}{\ell_{z-1}^2} \cdot \left( 2 - \frac{0.5z}{(\log p)^2} \right)^{\ell_{z-1}} \right)^m \cdot \left( 1 - \frac{0.1}{(\log p)^2} \right)^{\ell_{z-1} \cdot m} \quad (\text{As } m = (\log p)^{3.5} + 1) \\ &\geq \left( \left( 1 - \frac{1}{\sqrt{\ell_{z-1}}} \right) \cdot \left( 2 - \frac{0.5z}{(\log p)^2} \right) \cdot \left( 1 - \frac{0.1}{(\log p)^2} \right) \right)^{\ell_{z-1} \cdot m} \\ &\geq \left( 2 - \frac{0.5(z+1)}{(\log p)^2} \right)^{\ell_{z-1} \cdot m} \\ &\geq \left( 2 - \frac{0.5(z+1)}{(\log p)^2} \right)^{\ell_z}. \end{aligned}$$

## 6 Conclusion

We improve the best-known lower bound for matroid intersection prophet inequalities to  $q^{1/2+\Omega(1/\log \log q)}$ , via an improved upper bound on the product dimension of  $Q(p, p^p)$  to  $p^{1/2-\Omega(1/\log \log p)}$ . There are numerous open directions posed by our work. For example:

- What is the product dimension of  $Q(p, p^p)$ ? By Proposition 8, improved upper bounds on  $Q(p, p^p)$  imply improved lower bounds on  $\alpha(\mathcal{C}_{\text{SYMPARTINT}}(q), \mathcal{P}_{\text{IIDBERNOULLI}})$ .
- Can the [28] construction be written using  $p^{2-\Omega(1)}$  (perhaps not partition) matroids?
- Are there asymptotically better algorithms for the matroid intersection prophet inequality? What about the special case of partition matroids, symmetric feasibility constraints, and i.i.d. Bernoulli random variables?

More generally, our work also proposes consideration of the following class of problems: given a set system  $\mathcal{I}$ , what is the minimum number  $q$  of (partition) matroids  $\mathcal{I}_1, \dots, \mathcal{I}_q$  such that  $\mathcal{I} = \cap_{i=1}^q \mathcal{I}_i$ ?<sup>12</sup>

<sup>12</sup>The authors thank Bobby Kleinberg for suggesting this broader agenda.

---

References

---

- 1 Melika Abolhassani, Soheil Ehsani, Hossein Esfandiari, MohammadTaghi Hajiaghayi, Robert D. Kleinberg, and Brendan Lucier. Beating  $1-1/e$  for ordered prophets. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 61–71, 2017.
- 2 Marek Adamczyk and Michal Wlodarczyk. Random order contention resolution schemes. In *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*, pages 790–801, 2018.
- 3 Saeed Alaei. Bayesian Combinatorial Auctions: Expanding Single Buyer Mechanisms to Many Buyers. In *the 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2011.
- 4 Noga Alon. Covering graphs by the minimum number of equivalence relations. *Comb.*, 6(3):201–206, 1986.
- 5 Noga Alon and Ryan Alweiss. On the product dimension of clique factors. *European Journal of Combinatorics*, 86:103097, 2020.
- 6 Nima Anari, Rad Niazadeh, Amin Saberi, and Ali Sharneli. Nearly optimal pricing algorithms for production constrained and laminar bayesian selection. In *Proceedings of the 2019 ACM Conference on Economics and Computation, EC 2019, Phoenix, AZ, USA, June 24-28, 2019.*, pages 91–92, 2019.
- 7 Nick Arnosti and Will Ma. Tight guarantees for static threshold policies in the prophet secretary problem. In David M. Pennock, Ilya Segal, and Sven Seuken, editors, *EC '22: The 23rd ACM Conference on Economics and Computation, Boulder, CO, USA, July 11 - 15, 2022*, page 242. ACM, 2022.
- 8 Pablo Daniel Azar, Robert Kleinberg, and S. Matthew Weinberg. Prophet inequalities with limited information. In *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2014, Portland, Oregon, USA, January 5-7, 2014*, pages 1358–1377, 2014.
- 9 Yossi Azar, Ashish Chiplunkar, and Haim Kaplan. Prophet secretary: Surpassing the  $1-1/e$  barrier. In *Proceedings of the 2018 ACM Conference on Economics and Computation, Ithaca, NY, USA, June 18-22, 2018*, pages 303–318, 2018.
- 10 Constantine Caramanis, Paul Dütting, Matthew Faw, Federico Fusco, Philip Lazos, Stefano Leonardi, Orestis Papadigenopoulos, Emmanouil Pountourakis, and Rebecca Reiffenhäuser. Single-sample prophet inequalities via greedy-ordered selection. In *Proceedings of the 2022 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1298–1325, 2022.
- 11 Shuchi Chawla, Jason D. Hartline, David L. Malec, and Balasubramanian Sivan. Multi-Parameter Mechanism Design and Sequential Posted Pricing. In *the 42nd ACM Symposium on Theory of Computing (STOC)*, 2010.
- 12 José R. Correa, Andrés Cristi, Boris Epstein, and José A. Soto. The two-sided game of googol and sample-based prophet inequalities. In Shuchi Chawla, editor, *Proceedings of the 2020 ACM-SIAM Symposium on Discrete Algorithms, SODA 2020, Salt Lake City, UT, USA, January 5-8, 2020*, pages 2066–2081. SIAM, 2020.
- 13 José R. Correa, Andrés Cristi, Andrés Fielbaum, Tristan Pollner, and S. Matthew Weinberg. Optimal item pricing in online combinatorial auctions. In *Integer Programming and Combinatorial Optimization - 23rd International Conference, IPCO 2022, Eindhoven, The Netherlands, June 27-29, 2022, Proceedings*, 2022.
- 14 José R. Correa, Paul Dütting, Felix A. Fischer, and Kevin Schewior. Prophet inequalities for I.I.D. random variables from an unknown distribution. In *Proceedings of the 2019 ACM Conference on Economics and Computation, EC 2019, Phoenix, AZ, USA, June 24-28, 2019.*, pages 3–17, 2019. doi:10.1145/3328526.3329627.
- 15 José R. Correa, Paul Dütting, Felix A. Fischer, Kevin Schewior, and Bruno Ziliotto. Unknown I.I.D. prophets: Better bounds, streaming algorithms, and a new impossibility (extended abstract). In *12th Innovations in Theoretical Computer Science Conference, ITCS 2021, January 6-8, 2021, Virtual Conference*, volume 185, pages 86:1–86:1, 2021.

- 16 José R. Correa, Patricio Foncea, Ruben Hoeksma, Tim Oosterwijk, and Tjark Vredeveld. Posted price mechanisms for a random stream of customers. In *Proceedings of the 2017 ACM Conference on Economics and Computation, EC '17, Cambridge, MA, USA, June 26-30, 2017*, pages 169–186, 2017. doi:10.1145/3033274.3085137.
- 17 José R. Correa, Raimundo Saona, and Bruno Ziliotto. Prophet secretary through blind strategies. *Math. Program.*, 190(1):483–521, 2021. doi:10.1007/s10107-020-01544-8.
- 18 Paul Dütting and Robert Kleinberg. Polymatroid prophet inequalities. In Nikhil Bansal and Irene Finocchi, editors, *Algorithms - ESA 2015 - 23rd Annual European Symposium, Patras, Greece, September 14-16, 2015, Proceedings*, volume 9294 of *Lecture Notes in Computer Science*, pages 437–449. Springer, 2015. doi:10.1007/978-3-662-48350-3\_37.
- 19 Soheil Ehsani, MohammadTaghi Hajiaghayi, Thomas Kesselheim, and Sahil Singla. Prophet secretary for combinatorial auctions and matroids. In *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2018, New Orleans, LA, USA, January 7-10, 2018*, pages 700–714, 2018.
- 20 Hossein Esfandiari, MohammadTaghi Hajiaghayi, Vahid Liaghat, and Morteza Monemizadeh. Prophet secretary. In *Algorithms - ESA 2015 - 23rd Annual European Symposium, Patras, Greece, September 14-16, 2015, Proceedings*, pages 496–508, 2015.
- 21 Tomer Ezra, Michal Feldman, Nick Gravin, and Zhihao Gavin Tang. Online stochastic max-weight matching: Prophet inequality for vertex and edge arrival models. In *EC '20: The 21st ACM Conference on Economics and Computation, Virtual Event, Hungary, July 13-17, 2020*, pages 769–787. ACM, 2020.
- 22 Moran Feldman, Ola Svensson, and Rico Zenklusen. Online contention resolution schemes. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016, Arlington, VA, USA, January 10-12, 2016*, pages 1014–1033, 2016.
- 23 Hu Fu, Zhihao Gavin Tang, Hongxun Wu, Jinzhao Wu, and Qianfan Zhang. Random order vertex arrival contention resolution schemes for matching, with applications. In *48th International Colloquium on Automata, Languages, and Programming, ICALP 2021, July 12-16, 2021, Glasgow, Scotland (Virtual Conference)*, 2021.
- 24 Oliver Göbel, Martin Hoefer, Thomas Kesselheim, Thomas Schleiden, and Berthold Vöcking. Online independent set beyond the worst-case: Secretaries, prophets, and periods. In *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part II*, pages 508–519, 2014.
- 25 Nikolai Gravin and Hongao Wang. Prophet inequality for bipartite matching: Merits of being simple and non adaptive. In *Proceedings of the 2019 ACM Conference on Economics and Computation, EC 2019, Phoenix, AZ, USA, June 24-28, 2019.*, pages 93–109, 2019.
- 26 Chenghao Guo, Zhiyi Huang, Zhihao Gavin Tang, and Xinzhi Zhang. Generalizing complex hypotheses on product distributions: Auctions, prophet inequalities, and pandora’s problem. In *Conference on Learning Theory, COLT 2021, 15-19 August 2021, Boulder, Colorado, USA, 2021*.
- 27 Jiashuo Jiang, Will Ma, and Jiawei Zhang. Tight guarantees for multi-unit prophet inequalities and online stochastic knapsack. In *Proceedings of the 2022 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1221–1246, 2022.
- 28 Robert Kleinberg and S. Matthew Weinberg. Matroid prophet inequalities. In *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 123–136, 2012.
- 29 Ulrich Krenzel and Louis Sucheston. On semiamarts, amarts, and processes with finite value. *Advances in Probability and Related Topics*, 4:197–266, 1978.
- 30 Euiwoong Lee and Sahil Singla. Optimal online contention resolution schemes via ex-ante prophet inequalities. In *26th Annual European Symposium on Algorithms, ESA 2018, August 20-22, 2018, Helsinki, Finland, 2018*.
- 31 László Lovász, Jaroslav Nešetřil, and Ales Pultr. On a product dimension of graphs. *J. Comb. Theory, Ser. B*, 29(1):47–67, 1980.

## 95:20 An Improved Lower Bound for Matroid Intersection Prophet Inequalities

- 32 Tristan Pollner, Mohammad Roghani, Amin Saberi, and David Wajc. Improved online contention resolution for matchings and applications to the gig economy. In *EC '22: The 23rd ACM Conference on Economics and Computation, Boulder, CO, USA, July 11 - 15, 2022*, 2022.
- 33 Aviad Rubinfeld. Beyond matroids: secretary problem and prophet inequality with general constraints. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, pages 324–332, 2016.
- 34 Aviad Rubinfeld, Jack Z. Wang, and S. Matthew Weinberg. Optimal single-choice prophet inequalities from samples. In *11th Innovations in Theoretical Computer Science Conference, ITCS 2020, January 12-14, 2020, Seattle, Washington, USA, 2020*.
- 35 Ester Samuel-Cahn. Comparison of threshold stop rules and maximum for independent nonnegative random variables. *Annals of Probability*, 12(4):1213–1216, 1984.