Lower Bound Constructions for Matroid Intersection Prophet Inequalities

Arya Maheshwari
Adviser: Matthew Weinberg

Abstract

We study new constructions aimed at strengthening the lower bound for the intersection of m matroids prophet inequality. Current algorithms obtain at best $O(m)$-approximations while the strongest lower bound is $m^{\frac{1}{2}+\Omega(1/\log\log m)}$, leaving the tight bound unknown. In this project, we explore three main avenues to improve the lower bound that vary between extending the current construction due to [KW12] and trying out entirely new starting points. Specifically, we consider (1) close variants of the existing construction, (2) intersections of arbitrary matroids for recovering the existing construction's constraints, and (3) intersections of randomly constructed vector matroids. Our main results rule out certain approaches or classes of constructions across these avenues, thus narrowing down which approaches will be promising to consider in the future.

1. Introduction

Prophet inequalities are an intriguing class of optimal stopping problems that have yielded important implications within computer science and economics, particularly in the context of online algorithms and mechanism design. The basic setup of the problem is as follows. A gambler is faced with a sequence of items $[n]$ with values $\vec{X} = X_1, ..., X_n$ revealed one at a time in some order, where each X_i is a non-negative random variable drawn independently from a distribution D_i. Given a set system $\mathcal{I} \subseteq 2^{[n]}$ of *feasibility constraints*, the gambler's goal is to select a feasible set $S \in \mathcal{I}$ of items and maximize the total value $\sum_{i\in S} X_i$ of this selected set. The key is that the gambler knows the constraints $\mathcal{I}$ and distributions $\vec{D} = \{D_i\}_i$ ahead of time but only learns the specific realizations of each value X_i as they are revealed one by one, at which point the gambler must *immediately* and *irrevocably* decide whether to select or discard that item.

Given this setup, we want to understand how well such a gambler could do in relation to a *prophet* who can see all values X_i ahead of time. Such a prophet can simply select the maximum-value feasible set (the offline optimum) to achieve a final expected value of $V_P := \mathbb{E}_{\vec{X}\leftarrow\vec{D}}[\max_{S\in\mathcal{I}}\{\sum_{i\in S} X_i\}]$. The gambler, meanwhile, will have to use some online strategy to select some set $T \in \mathcal{I}$ that will not necessarily be the offline optimum. Let $V_G := \mathbb{E}_{\vec{X}\leftarrow\vec{D}}[\sum_{i\in T} X_i]$ denote the gambler's expected final value. The key question is how small the approximation ratio $\frac{V_P}{V_G}$ can be (for T obtained via some optimal online strategy), termed the *prophet inequality* (PI) for a given instance of $\mathcal{I}$ and $\vec{D}$.

Observe that it will always be at least 1, since clearly $V_G \leq V_P$. Often of interest are PIs for a given *class* $\mathcal{C}$ of constraints, where we want to determine the best (smallest) $\frac{V_P}{V_G}$ ratio achievable on *all* instances where $\mathcal{I} \in \mathcal{C}$. We refer to this optimal approximation ratio as α.

The first PI was introduced in 1978 [KS78] for the class of "single-choice" constraints, where the gambler can only choose one item. Here [KS78] present an algorithm achieving a 2-approximation PI (i.e. *upper bounding* $\alpha \leq 2$) and furthermore show that this is optimal (i.e. a *tight bound* of $\alpha = 2$). Subsequent investigations into PIs have motivated their study by demonstrating significant applications, perhaps most notably to Bayesian optimal mechanism design [HKS07, CHMS10]. Meanwhile, recent work [SVW22, AA20] has revealed connections to purely mathematical questions in combinatorics, where improved PI bounds are directly related to stronger bounds on a graph's product dimension.

Our work focuses on *matroid prophet inequalities*, in which the constraints $\mathcal{I}$ are based on matroids. Matroids have become a cornerstone of combinatorial optimization since their introduction in 1935 [Whi35], and they present an interesting constraint structure under which to understand online optimization problems like PIs. [KW12]'s pioneering study in this area demonstrated a tight 2-approximation PI when the class $\mathcal{C}$ is all matroids, and other work has led to asymptotically tight bounds for various related constraint classes (e.g. k-uniform matroids [Ala11], polymatroids [DK15]). However, an important unsolved question is the tight bound when $\mathcal{C}$ is the class of constraints $\mathcal{I}$ defined by an *intersection* of m matroids. That is, $\mathcal{I} = \bigcap_{j=1}^{m} \mathcal{I}_j$, such that a set is feasible under $\mathcal{I}$ iff it is independent in all matroid constraints $\mathcal{I}_j$. We will refer to this as the "INT(m)" problem for convenience. The best known algorithms achieve $(4m-2)$- and $e(m+1)$-approximations (upper bounds on α) for INT(m) ([KW12, FSZ16]) and a $(m+1)$-approximation for the intersection of m *partition* matroids [CCF+22]. Meanwhile, [KW12] present a construction witnessing a $\Omega(\sqrt{m})$ lower bound on α for INT(m), which was then improved slightly via stronger analysis to the current best lower bound of $m^{\frac{1}{2}+\Omega(1/\log\log m)}$ [SVW22]. The gap between the $O(m)$ upper bounds and roughly-$\Omega(\sqrt{m})$ lower bounds has thus resisted significant improvement for over a decade, and the task of bridging it remains a difficult open problem.

In this study we target this problem from the lower bounds direction. Concretely, demonstrating some lower bound $\Omega(f(m))$ for INT(m) requires showing that there is a particular instance whose constraints can be written as an intersection of m matroids and in which the optimal prophet-gambler ratio α must be *at least* $f(m)$ asymptotically. While we do not know whether the true tight bound is a stronger lower or upper bound (or both), the lower bound direction specifically remains fairly unexplored: it has not received significant attention beyond [KW12] and [SVW22], and the existing construction (§2.2) satisfies many stronger assumptions (e.g. uses partition matroids, i.i.d Bernoulli distributions) that need not hold in the general INT(m) problem. Thus the goal of this project is to more deeply explore the space of potential lower bound constructions, both by extending the current

construction and by trying out new starting points, in order to demonstrate an improved lower bound or otherwise narrow down which approaches are promising for future studies.

1.1. Approach and Summary

We investigate three avenues of potential constructions for improving the $\textsc{Int}(m)$ lower bound. In §3 we explore close variants of the existing [KW12] construction; in §4 we consider using arbitrary matroids to write the [KW12] construction's constraints; and in §5 we begin exploring vector matroid constructions from a probabilistic starting point. In each avenue, our main results are to rule out certain types of constructions or approaches: that is, we show that they cannot yield anything stronger than a $\Omega(\sqrt{m})$ lower bound on α for $\textsc{Int}(m)$ constraints. We then discuss important takeaways and propose possibilities for future work in each avenue (§3.4, §4.2, §5.2).

Our three avenues can be viewed as becoming iteratively more general, in terms of the matroid classes used (see §2.1 for more) and similarity to the specific [KW12] construction. There are trade-offs between these levels of generality. On one hand, the [KW12] construction exhibits clear "hardness properties" (as we will discuss in §2.2.1) that induce the desired gap between V_P and V_G, so maintaining or leveraging this structure through similar constructions seems useful. On the other hand, a more general space of constructions (e.g using more general matroid classes) has more possibilities for a successful hard instance; indeed, expanding beyond the restricted conditions of the [KW12] construction is one of our motivations for this lower bounds study. We thus distribute our search across both close extensions of the existing construction in §3 and more general approaches in §4 and §5.

Summary. We briefly summarize our specific results in informal terms. In §3.4 we consider and rule out three variants of the base [KW12] construction, based on optimizing the specific parameters (§3.1) and changing the structure by dropping subsets of matroids from the intersection (§3.2 and §3.3). In §4 we rule out the utility of arbitrary matroids in the context of the [KW12] construction by proving that partition matroids are optimal for writing these constraints. In §5 we analyze intersections of randomly constructed vector matroids over infinite and finite fields to understand why a probabilistic method-style argument on such constructions does not seem viable.

1.2. Related Work

As mentioned, Krengel, Sucheston, and Garling initiated the study of PIs in 1978 with a tight 2-approximation for the single-choice PI setup. Samuel-Cahn subsequently presented an algorithm for achieving this bound based on setting thresholds [SC84] that, albeit simple, has also been a central idea in more recent work on matroid PIs [KW12]. Important applications to mechanism design have been essential in motivating the study of PIs. [HKS07] first explored the correspondence between strategyproof online mechanisms and PI algorithms, and seminal work by [CHMS10] deepened

the link by connecting PIs with multiparameter mechanism design in the context of approximation guarantees of sequential posted-price mechanisms.

Numerous papers have since determined bounds on matroid PIs (and their extensions) in particular, from a tight 2-approximation algorithm for arbitrary matroids [KW12] to the same tight bound for polymatroids [DK15], asymptotically tight bounds for uniform matroids [Ala11], and more. In terms of the INT(m) problem, [KW12] present a $(4m-2)$-approximation algorithm and a construction witnessing a $\Omega(\sqrt{m})$ lower bound. [FSZ16] achieve a state-of-the-art $e(m+1)$-approximation, and while no $o(m)$ algorithm is known even under much stronger assumptions, better constant factors have been obtained for some special cases like random order [AW18] or partition matroid intersections [CCF+22]. On the lower bounds side, [SVW22] apply recent progress on graph product dimensions [AA20] to better analyze the [KW12] construction and improve the lower bound to $m^{\frac{1}{2}+\Omega(1/\log\log m)}$. We discuss [KW12] and [SVW22] in more detail in §2.2 and §2.3. Matroid constraints have also been considered for similar online optimization questions like the secretary problem [BIK07]. Within the matroid secretary domain, some studies have suggested the utility of drawing on deeper matroid theory [Din13], which we believe may be worthwhile to consider for our PI lower bounds as well.

2. Background

2.1. Matroids

We start by defining matroids and overviewing some specific classes of matroids relevant to this study, and we in particular highlight how these classes relate to one another. For more background on matroids and omitted proofs, see e.g. [Von17] or [Oxl11] for a comprehensive treatment.

Definition 1 A *matroid* $\mathcal{M}$ is a pair $\mathcal{M} = (E, \mathcal{I})$ of a base set E and a non-empty set family $I \subseteq 2^E$ satisfying the following properties:
(M1) *Downward-closed*: if $B \in \mathcal{I}$ and $A \subseteq B$, then $A \in \mathcal{I}$.
(M2) *Independence augmentation*: if $A, B \in \mathcal{I}$ and $|B| > |A|$, then $\exists\, j \in B \setminus A$ s.t. $A \cup \{j\} \in \mathcal{I}$.

Any set $S \in \mathcal{I}$ is called an *independent* set of matroid $\mathcal{M} = (E, \mathcal{I})$; S is a *dependent* set if $S \notin \mathcal{I}$. The downward-closed property (M1) says that any subset of an independent set will also be independent, and similarly any superset of a dependent set will also be dependent. A maximal independent set of a matroid $\mathcal{M}$ is called a *basis* of $\mathcal{M}$, while a minimal dependent set is called a *circuit* of $\mathcal{M}$. A simple but important fact that follows from the independence augmentation property (M2) is that all bases of a matroid $\mathcal{M}$ must have the same size. This size gives the *rank* $r(\mathcal{M})$ of the matroid, which is defined by $r(\mathcal{M}) = \max_{S \in \mathcal{I}} |S|$.

We often consider matroids that arise from a particular setting or construction, which we refer to as a class of matroids. The five classes defined below are among the most commonly considered, but there are many other classes (e.g. transversal matroids, gammoids, regular matroids, binary/ternary matroids) that may be of interest in future matroid PI investigations.

Definition 2 The following are five classes of matroids. For the first three, let E be an arbitrary base set.

1. **Uniform Matroids**: Given E and a positive integer k, define $\mathcal{I} = \{S \subseteq E : |S| \leq k\}$. Then $\mathcal{M} = (E, \mathcal{I})$ defines a matroid and is called a *k-uniform matroid*.
2. **Partition Matroids**: Let $S_1 \sqcup ... \sqcup S_p = E$ be a partition of E. Define $\mathcal{I} = \{S \subseteq E : |S \cap S_k| \leq 1,\ \forall k \in [p]\}$. Then $\mathcal{M} = (E, \mathcal{I})$ defines a matroid and is called a *partition matroid*. [1]
3. **Laminar Matroids**: A *laminar family* $\mathcal{A} \subseteq 2^E$ is a set family s.t. for all $A_1, A_2 \in \mathcal{A}$, either $A_1 \subseteq A_2$, $A_2 \subseteq A_1$, or $A_1 \cap A_2 = \emptyset$. Given a laminar family $\mathcal{A}$ and a capacity function $c : \mathcal{A} \mapsto \mathbb{Z}_{\geq 0}$, let $\mathcal{I} = \{S \subseteq E : |S \cap A| \leq c(A),\ \forall A \in \mathcal{A}\}$. Then $\mathcal{M} = (E, \mathcal{I})$ defines a matroid and is called a *laminar matroid*.
4. **Graphic Matroids**: For a graph $G = (V, E)$, define $\mathcal{I} = \{S \subseteq E :\ S$ does not contain any cycles$\}$. Then $\mathcal{M} = (E, \mathcal{I})$ defines a matroid and is called the *cycle matroid* of G. A matroid is called *graphic* if it is the cycle matroid of some graph G.
5. **Vector Matroids**: Given a vector space V and a set of vectors $E \subseteq V$, define $\mathcal{I} = \{S \subseteq E :$ S is linearly independent in $V\}$. Then $\mathcal{M} = (E, \mathcal{I})$ defines a matroid and is called a *vector matroid*.

A natural question that arises is whether these classes of matroids are related in any way. Indeed, we show in Fact 1 that some of the above classes are special cases of others, that is, when any matroid from some class A can be equivalently expressed and represented as a matroid from another class B. In this case we say that class B *generalizes* class A.

Fact 1 *The classes of graphic matroids and laminar matroids both generalize partition matroids. Vector matroids generalize both graphic and laminar matroids. [Oxl11]*

The proof of Fact 1 below is constructive in the sense that we show that a class B generalizes a class A by explicitly showing how an arbitrary matroid $\mathcal{M}$ from class A can be represented with a construction from class B. These constructions are useful for translating between different viewpoints of a particular matroid, for instance in §5.2 where we express a partition matroid as a vector matroid as a basis for future work. Furthermore, as we have mentioned, the order of generality between matroid classes also informs our search for an improved Int(m) lower bound construction. The

[1] A more general view of partition matroids associates capacities $c_1, ..., c_p$ with each partite set $S_1, \ldots, S_p$ and instead defines $\mathcal{I} = \{S \subseteq E : |S \cap S_k| \leq c_k,\ \forall k \in [p]\}$.

existing construction (discussed in §2.2) uses partition matroids; Fact 1 tells us this is a relatively restricted class of matroids, while in general a hard instance for INT(m) could involve arbitrary matroids. Given the trade-offs discussed in §1.1, our avenues of investigation cover matroids of varying generality, from continuing with partition matroids in §3 to considering vector and arbitrary matroid intersections in §5 and §4 respectively.

Proof of Fact 1: Consider an arbitrary partition matroid $\mathcal{M} = (E, \mathcal{I})$ defined by partition $S_1 \sqcup ... \sqcup S_k = E$. To prove the first statement, we will show how the same $\mathcal{M}$ can be recovered as (1) the laminar matroid obtained from some laminar family $\mathcal{A}$ and capacity function $c(\cdot)$, and (2) a graphic matroid, i.e. the cycle matroid of some graph G.

(1) Simply notice that the partition $\mathcal{A} = \{S_i : i \in [k]\}$ itself is in fact a laminar family, since $S_i \cap S_j = \emptyset$ for $i \neq j$. Then defining our capacity function $c(\cdot)$ to be given by $c(A) = 1, \forall A \in \mathcal{A}$, it is easy to see that the laminar matroid on E defined by A and $c(\cdot)$ exactly recovers the independent sets $\mathcal{I}$ of our partition matroid.

(2) Consider a simple path graph with k edges, and then turn each edge i of the k total edges into a multi-edge of size $|S_i|$, i.e. $|S_i|$ parallel edges. Observe that this yields a graph G with $|E|$ edges, and we can map each element $e \in E$ into a distinct edge of G s.t. each partite set $S_i \subseteq E$ of elements corresponds to one multi-edge. Now, observe that a set S of edges of G is acyclic iff it does not contain any two parallel edges, i.e. if $|S \cap S_i| \leq 1$ for all $i \in [k]$. It follows that the cycle matroid of G exactly recovers our partition matroid $\mathcal{M}$.

For the second statement, we omit the proof that vector matroids generalize laminar matroids; details can be found in [Fin11, Oxl11]. A graphic matroid $\mathcal{M}$, defined by some graph $G = (V, E)$, can be expressed as the vector matroid of the column set of the *vertex-edge incidence matrix* of (a directed version of) G. The proof of this is deferred to Appendix A. ■

2.2. The [KW12] Construction

We now review the original [KW12] lower bound construction, which given a parameter p yields an instance with $\frac{V_P}{V_G} = \Omega(p)$ as an intersection of p^2 matroids. Viewing $m := p^2$, overall this yields an $\Omega(\sqrt{m})$ lower bound on α for the INT(m) problem. We will assume without loss of generality that p is a prime below and henceforth where applicable (in the case that it is not, we can equivalently work with a prime chosen between $\frac{p}{2}$ and p and obtain the same asymptotic results).

Setup. Consider a set E of p^{p+1} items viewed as the elements of a grid with $r = p^p$ rows and $c = p$ columns. The value X_e of each element $e \in E$ is $X_e \overset{iid}{\sim} \text{BERN}(\frac{1}{p})$. In general each element is specified by its row x and column y, and hence we will identify elements as (x, y) for $0 \leq x \leq p^p - 1$, $0 \leq y \leq p - 1$. However, we will consider the row value x base-p and hence view the row as a sequence of digits $\vec{x} = (x_0, ..., x_{p-1})$ where $0 \leq x_i \leq p-1$ for each $0 \leq i \leq p-1$, since $x \leq p^p - 1$.

Constraints. Define p^2 matroids as follows: for each $0 \le i, j \le p-1$, let $\mathcal{M}^{i,j}$ be the partition matroid defined by the partition $E = \bigsqcup_k S_k^{i,j}$ for $0 \le k \le p-1$, with partite sets $S_k^{i,j} := \{(\vec{x}, y) : x_i \cdot j + y \equiv k \pmod p\}$. This defines p^2 matroids since there are p choices for both i and j. We now have the following intersection of matroids constraints: $\mathcal{I} = \{S \subseteq E : |S \cap S_k^{i,j}| \le 1, \text{ for all } 0 \le i, j, k \le p-1\}$. We claim that the resulting feasible sets are exactly any set of elements that all belong to the same row, stated precisely below.

Proposition 2 *Consider the matroid intersection constraints* $\mathcal{I} := \{S \subseteq E : |S \cap S_k^{i,j}| \le 1, \text{ for all } 0 \le i, j, k \le p-1\}$ *as defined above with partite sets* $S_k^{i,j} := \{(\vec{x}, y) : x_i \cdot j + y \equiv k \pmod p\}$. *Then* $\mathcal{I} = \{S \subseteq E : \forall (\vec{x_1}, y_1), (\vec{x_2}, y_2) \in S, \vec{x_1} = \vec{x_2}\}$. *That is, the definition of* $\mathcal{I}$ *is equivalent to defining the feasible sets to be any row or subset of a row.*

Proof: Define $\mathcal{I} := \{S \subseteq E : |S \cap S_k^{i,j}| \le 1, \text{ for all } 0 \le i, j, k \le p-1\}$ as in the statement. First we show that a subset of a row is always feasible, that is, for $S \subseteq E$ s.t. $\forall (\vec{x_1}, y_1), (\vec{x_2}, y_2) \in S$, $\vec{x_1} = \vec{x_2}$, $S \in \mathcal{I}$. In particular we show that for any two distinct elements $(\vec{x}, y_1), (\vec{x}, y_2)$ in the same row , $\nexists$ a partite set $S_k^{i,j}$ s.t. $(\vec{x}, y_1)$ and $(\vec{x}, y_2)$ are both in $S_k^{i,j}$. This is because for any $0 \le i, j \le p-1$, we have $x_i \cdot j + y_1 \neq x_i \cdot j + y_2 \pmod p$, since $0 \le y_1, y_2 \le p-1$ and $y_1 \neq y_2$ given that the elements to be distinct.

Now observe that it suffices to show that any two elements $(\vec{x_1}, y_1), (\vec{x_2}, y_2)$ in *different* rows (i.e. $\vec{x_1} \neq \vec{x_2}$) are dependent in some matroid. We have $\vec{x_1} \neq \vec{x_2} \Rightarrow \exists\ 0 \le i \le p-1$ s.t. $x_{1i} \neq x_{2i}$. Then the key is that there exists $0 \le j \le p-1$ s.t. $x_{1i} \cdot j + y_1 = x_{2i} \cdot j + y_2 \pmod p$. This follows since $x_{1i} - x_{2i} \neq 0$ and so there is a solution $0 \le j \le p-1$ to $(x_{1i} - x_{2i})j = (y_2 - y_1) \mod p$ by inverting $(x_{1i} - x_{2i})$ in the field $\mathbb{F}_p$ (prime p). Thus letting $k := x_{1i} \cdot j + y_1 \mod p$, it follows that both $(\vec{x_1}, y_1), (\vec{x_1}, y_1) \in S_k^{i,j}$. Thus both elements are dependent in matroid $\mathcal{M}^{i,j}$. ■

Value analysis. The analysis for V_P and V_G from [KW12] is repeated here, using the row-characterization of feasible sets from Proposition 2. The upshot is that $V_P = \Theta(p)$ while $V(G) = \Theta(1)$, so $\frac{V_P}{V_G} = \Theta(p)$. Thus viewing $m = p^2$, this yields a $\Omega(\sqrt{m})$ lower bound for $\textsc{Int}(m)$.

Terminology: We will often work with Bernoulli (0-1) random variable distributions for item values in the constructions we consider. We refer to value-1 items as *active*, following terminology from prior work for items with value above a threshold [FSZ16].

Prophet: For the prophet, since any particular row is all active with probability $(\frac{1}{p})^c$, there will be some active row (i.e. total value c) with probability $1 - (1 - \frac{1}{p^c})^r = 1 - (1 - \frac{1}{p^p})^{p^p} \ge (1 - \frac{1}{e})$. Thus $V_P \ge c \cdot (1 - \frac{1}{e}) = (1 - \frac{1}{e})p$. We also know $V_P \le p$ since the maximum feasible set size is $c = p$, so $V_P = \Theta(p)$.

Gambler: As soon as the gambler accepts any element, they can only select elements from the same row. There are up to $c - 1 = p - 1$ remaining elements, which are i.i.d $\textsc{Bern}(\frac{1}{p})$, in the row, so

the expected value from remaining elements is $\frac{p-1}{p}$. Hence $V_G \leq 1 + \frac{p-1}{p} \leq 2$, where the 1 comes from the selection of the first element (that locks the gambler in to a particular row). Meanwhile certainly $V_G = \Omega(1)$, since with at least constant probability there will be an active element in the whole grid. Thus $V_G = \Theta(1)$ as desired.

2.2.1. Hardness Principles. Here we highlight some of the broader principles and properties that make this construction a successful hard instance. A key consequence of the grid constraint structure is that the gambler is "locked in" to a particular maximal feasible set (a row) as soon as she selects an item. Indeed, the disjointness between these maximal feasible sets is essential to limiting V_G, as we wish to do when demonstrating a lower bound. Intuitively, it strongly restricts the gambler's optionality: she must immediately decide which single row to pursue, while the prophet can see the outcome of each row before picking one. In general, to limit V_G in a construction we might aim to ensure that a large fraction of remaining feasible items gets blocked each time the gambler selects a new item. The existing construction excels in this regard, with only a $\frac{1}{p^p}$-fraction of items *not* blocked after the gambler's first selection itself. We also note that the structure of blocking any different-row pair of items in this construction is one instance of what we can more generally view as *sufficient conditions* for asymptotically separating V_P and V_G, which we will delve further into in §4.2. The downside of such strong restrictions is that we do need many feasible sets and expected active elements to ensure that V_P is high, and then the challenge becomes writing the constraints as a minimal intersection of matroids. Overall, however, the construction's structure induces a separation between V_P and V_G as desired, so these properties are useful to keep in mind as guiding principles while searching for new lower bound constructions.

2.3. Graph Formulation and Lower Bound Improvements in [SVW22]

Recent work of [SVW22] improves the $\textsc{Int}(m)$ lower bound to $m^{\frac{1}{2}+\Omega(1/\log\log m)}$ through a stronger combinatorial analysis of the same construction introduced by [KW12]. Specifically, they show that the same constraints $\mathcal{I}$ can be written as an intersection of asymptotically fewer partition matroids through a connection to the *product dimension* (PD) of a graph and then leveraging recent progress on PD bounds [AA20]. We briefly overview [SVW22]'s graph formulation of the [KW12] construction and the basics idea for the analysis via PD bounds.

Let $Q(c, r)$ denote the graph of r disjoint cliques of size c. We can view the [KW12] construction setup, again parameterized by p, in terms of $Q(p, p^p)$ as follows. The p^{p+1} elements are the vertices, where each row corresponds to one of the p^p disjoint p-cliques, and then the desired constraints $\mathcal{I}$ are exactly defined by any clique in the graph being feasible. Using this graph formulation, the key observation of [AA20, SVW22] is that the minimum number of partition matroids that need to be intersected to write $\mathcal{I}$ is exactly the product dimension of $Q(p, p^p)$, denoted $\text{PD}(Q(p, p^p))$, where the product dimension is defined as the minimum number of proper vertex colorings such that

every pair of non-adjacent vertices are colored the same in some coloring.[2] The simple canonical procedure from [KW12] for constructing these partition matroids (described above) thus witnesses an upper bound of p^2 for PD$(Q(p, p^p)$. Using an advanced combinatorial argument based on the idea of finding large covering families of vectors, the authors of [AA20] prove an improved upper bound on PD$(Q(c, r))$ in the regime where $r > c^{c^{5 \lg \lg c}} \gg c^c$. Unfortunately the parameters of $Q(p, p^p)$ do not fall in this regime, but what [SVW22] show is precisely how to adapt the [AA20] argument to obtain a weaker but still overall improved result for this case where $r = c^c$. Specifically, they obtain a $p^{2-\Omega(1/\log\log p)}$ upper bound for PD$(Q(p, p^p))$. Then, since the [KW12] construction achieves $\frac{V_P}{V_G} = \Omega(p)$ with this many partition matroids, by inversion this implies the claimed $m^{\frac{1}{2}+\Omega(1/\log\log m)}$ lower bound for the Int(m) problem.

3. [KW12] Construction Variants

While the [KW12] construction features many desirable properties (§2.2.1) for inducing a separation between the prophet and gambler values, it is not clear a priori that the specific parameters and details of the construction are necessarily optimal. That is, it may be possible to obtain a better lower bound through small variations on the base structure of the existing construction. In this first avenue of investigation, we consider three such natural variants (§3.1, §3.2, §3.3) and show why they do *not* improve on the existing $\Omega(\sqrt{m})$ lower bound for the Int(m) problem.

3.1. General Grid(r, c, q) Construction and Analysis

Our first variant generalizes the specific parameters of the existing lower bound construction. In particular, the grid-based structure of the [KW12] construction can be defined more generally as a function of three parameters: (1) the number of rows r, (2) the number of columns c, and (3) the success probability q such that each element e (of the $r \cdot c$ total elements) has value $X_e \overset{iid}{\sim}$ Bern(q). The feasible sets are still to be exactly any row of elements (or subset of a row), though we will need to show how to write these constraints as an intersection of matroids for arbitrary (r, c) values (note that q is not relevant to the feasibility constraints). We refer to this parameterized setup as the Grid(r, c, q) construction and to the corresponding constraints as $\mathcal{I}(r, c)$, abbreviated to $\mathcal{I}$ when context is clear. The [KW12] construction is thus Grid$(p^p, p, \frac{1}{p})$.

In this section we ask the following question: are there values of (r, c, q) for which the corresponding Grid(r, c, q) construction yields an improved lower bound? Our main result, stated formally via

[2] The idea is to define a partition matroid $\mathcal{M}_k$ for each coloring k with each color defining a partite set; the PD definition then guarantees that any non-adjacent vertices will be colored the same (i.e. be dependent) in some coloring (i.e. some partition matroid), thus recovering the clique-based constraints $\mathcal{I}$ in the intersection overall.

Principle 3 and Theorem 4 below, is that the answer is no, *assuming* we write the $\mathcal{I}(r, c)$ constraints analogously to the canonical procedure from [KW12].

Principle 3 *To write the feasibility constraints $\mathcal{I}(r, c)$ of a GRID(r, c, q) construction as an intersection of matroids, we only consider the canonical procedure using partition matroids and modular arithmetic from [KW12] (discussed in §2.2 and §3.1.1).*

Theorem 4 *Assuming that constraints are written according to Principle 3, there do not exist parameter values (r, c, q) for which the GRID(r, c, q) construction yields an improvement over the $\Omega(\sqrt{m})$ lower bound on α for the INT(m) problem.*

Why it is reasonable to make an assumption like Principle 3 in our analysis? First, relaxing the assumption of using partition matroids is the subject of §4.1, where we show that indeed one cannot do better with arbitrary matroids, i.e. partition matroids are optimal for writing $\mathcal{I}(r, c)$ constraints. Then, generalizing the ideas in §2.3 to the case of arbitrary (r, c) tells us that the minimum number of partition matroids needed to write $\mathcal{I}(r, c)$ is exactly the *product dimension* of r disjoint c-cliques, denoted PD$(Q(c, r))$. While recent work in [AA20] improves PD$(Q(c, r))$ beyond what is obtained from our canonical procedure in some cases, the improvement only applies to regimes that have far too many rows relative to columns and in turn already require too many matroids for our purposes, for any (r, c, q).[3] [SVW22] do adapt the techniques of [AA20] to obtain (weaker) improvements in applicable regimes, in particular showing how $\mathcal{I}(p^p, p)$ can be written in $p^{2-\Omega(1/\log\log p)}$ instead of the p^2 partition matroids obtained by the canonical procedure. However, quantitatively this is only a minor (sub-polynomial) improvement, and hence the canonical procedure remains the best we can do up to such lower order terms. Thus the only other option would be to directly improve the product dimension of $Q(c, r)$ further. Given the involved nature of the current results due to leading combinatorists [AA20], this would be a very challenging combinatorial problem, which is not the focus of this project, so we proceed with the tools available to us.

3.1.1. Writing $\mathcal{I}(r, c)$ as a partition matroid intersection. Here we show that the canonical procedure for writing GRID constraints, generalized to the case of arbitrary (r, c), yields $\mathcal{I}(r, c)$ as an intersection of $m := c \cdot \log_c(r)$ partition matroids. We re-parameterize an arbitrary GRID(r, c, q) construction in terms of a base parameter p for the remainder of this section. Specifically, write $q = \frac{1}{p}$, $c = p^{a(p)}$, and $r = p^{b(p)}$, which we can do WLOG by defining p based on q, and then setting $a(p) = \log_p c$ and $b(p) = \log_p r$. Hence we want an intersection of $m := c \cdot \log_c(r) = p^{a(p)} \cdot \frac{b(p)}{a(p)}$ partition matroids.[4] Interpreting this parametrization under the desired constraints on probability

[3] Specifically, the limited regime in which [AA20] bounds apply translates to always requiring a minimum of $m := c^{1+5\lg\log c}$ matroids. But we can show that $\frac{V_P}{V_G} = O(c)$ since the maximum feasible set size in GRID(r, c, q) is c, while $m \gg c^2$, so this does not help us.

[4] We disregard integrality issues: one can take ceilings of terms like $\log_r(c)$ to be fully rigorous.

and the number of rows/columns (i.e. $q \leq 1$; r and c should be larger-than-constant integers) gives us bounds of $p \geq 1$ and $a(p), b(p) = \omega(1/\log p)$. Note that to prove an asymptotic lower bound, we want to consider our construction asymptotically in the number of matroids m, but one can check with the above bounds that it is equivalent to consider asymptotics with respect to p (as we sometimes do in derivations).

The argument is analogous to the proof of Proposition 2. As before, we identify each element $e \in E$ by its row and column (x, y) s.t. $0 \leq x \leq r-1$, $0 \leq y \leq c-1$. We want constraints $\mathcal{I} = \mathcal{I}(r, c)$ such that a set S belongs to $\mathcal{I}$ iff it is a row or subset of a row, i.e. $\forall (x_a, y_a), (x_b, y_b) \in S, x_a = x_b$. The canonical procedure that we follow is to now define a partition matroid $\mathcal{M}^{i,j}$ for each i, j in a range that is to be determined, where the partition to which an element (x, y) belongs is determined by $x_i \cdot j + y$, working modulo some value P to be determined. For elements in the same row x to independent in any matroid, we can observe that we should work mod $P := c = p^{a(p)}$, so that $y_a \neq y_b \Rightarrow y_a \not\equiv y_b \pmod{P}$. Note that we again assume that P is a prime here, as in §2.2.

As such, define $P := p^{a(p)}$, $i_{max} := \log_P p^{b(p)} = \frac{b(p)}{a(p)}$, and now write each element's row x with base P digits, as $\vec{x} = (x_0, ..., x_{i_{max}-1})$. Then define $\mathcal{M}^{i,j}$ for $0 \leq j \leq P-1$, $0 \leq i \leq i_{max}-1$ as the partition matroid for partite sets $S_k^{i,j} := \{(\vec{x}, y) : x_i \cdot j + y \equiv k \pmod{P}\}$, for all $0 \leq k \leq P-1$. In words, j ranges across the number of columns, and i across the number of digits needed base-c to write r. The same analysis from §2.2 shows that the intersection of these matroids recovers the desired constraints $\mathcal{I}(p^{b(p)}, p^{a(p)})$. Specifically, any set of elements in the same row will be independent under all matroids; while whenever there are two elements $(\vec{x_a}, y_a)$ and $(\vec{x_b}, y_b)$ such that $\vec{x_a} \neq \vec{x_b}$, there must be some index $0 \leq i \leq i_{max} - 1$ s.t. $x_{a,i} \neq x_{b,i} \pmod{P}$, and so $\exists\, 0 \leq j \leq P-1$ s.t. $x_{a,i} \cdot j + y_a = x_{b,i} \cdot j + y_b \pmod{P}$. Therefore any set of elements with elements from more than one row will be dependent in some matroid, as desired. Thus we conclude that the constraints $\mathcal{I}(p^{b(p)}, p^{a(p)})$ can be written as an intersection of $P \cdot i_{max} = p^{a(p)} \cdot \frac{b(p)}{a(p)}$ matroids.

3.1.2. Grid(r, c, q) Value Analysis. We now continue on to analyzing the prophet and gambler values in order to *upper bound* $\frac{V_P}{V_G}$ and, when combined with the derived number of matroids, thereby prove Theorem 4. We begin with the following useful fact that provides a tight characterization of the prophet value V_P assuming we know that $V_P = \Omega(1)$.

Fact 5 *Consider a Grid(r, c, q) construction, and suppose $V_P = \Omega(1)$ is known. Let T be the largest value up to c such that a particular row has total value at least T with probability $\Omega(\frac{1}{r})$. Then $V_P = \Theta(T)$.*

The proof of Fact 5 is deferred to Appendix B. Note that the total value of any particular row in Grid(r, c, q) is given by a Bin(c, q) random variable. Thus notice that the [KW12] prophet value analysis is an instance of this fact for their Grid$(p^p, p, \frac{1}{p})$ construction, where $V_P = \Theta(T)$ for $T = c = p$ since a given row is all 1's with probability $(\frac{1}{p})^c = \frac{1}{p^p} = \frac{1}{r}$.

Proof of Theorem 4:
Consider an arbitrary $\textsc{Grid}(p^{b(p)}, p^{a(p)}, \frac{1}{p})$ construction, whose constraints $\mathcal{I}$ we have shown can be written as an intersection of $p^{a(p)} \cdot \frac{b(p)}{a(p)}$ matroids.

Case 1: We separately handle the edge case where $V_G = o(1)$. Let A denote the event that there exists an active element in an instance of this $\textsc{Grid}$, and let N_A be a random variable denoting the number of active elements. We claim that $V_G = o(1)$ implies $\mathbb{E}[N_A] \leq \frac{1}{2}$, and then we can bound $V_G \geq \Pr[A] \geq \mathbb{E}[N_A] \cdot (1 - \mathbb{E}[N_A]) \geq \mathbb{E}[N_A]/2 \geq V_P/2$. The brief proof of these claims is deferred to Appendix C. The upshot is that $V_G \geq \frac{V_P}{2}$, in particular $\frac{V_P}{V_G} = \Theta(1)$. Since the gambler achieves a constant-factor approximation of the prophet, this case clearly cannot yield an improved lower bound.

Case 2: Otherwise, we analyze V_G and V_P as follows.

(I) **Gambler value** V_G. In this case we know $V_G = \Omega(1)$. We claim that furthermore $V_G = \Omega(1 + p^{a(p)-1})$. To see why, observe that the gambler could with probability $\frac{1}{2}$ either (a) use the strategy that yields $\Omega(1)$ or (b) select a row $\vec{x}$ and pick all elements from $\vec{x}$, which in expectation yields $c \cdot q = p^{a(p)-1}$. Thus indeed $V_G = \Omega(\frac{1}{2}(1 + p^{a(p)-1})) = \Omega(1 + p^{a(p)-1})$. In fact, we can conclude $V_G = \Theta(1 + p^{a(p)-1})$ by analogous reasoning to [KW12]'s analysis of V_G in $\textsc{Grid}(p^p, p, \frac{1}{p})$. Specifically, as soon as the gambler selects an element, she is locked in to a single row of $c = p^{a(p)}$ elements that are i.i.d $\textsc{Bern}(\frac{1}{p})$, and thus $V_G \leq 1 + \frac{p^{a(p)}-1}{p} \leq 1 + p^{a(p)-1}$.

(II) **Prophet value** V_P: Since $V_G = \Omega(1) \Rightarrow V_P = \Omega(1)$, we are in the regime where Fact 5 applies. So, since each row is a $\textsc{Bin}(p^{a(p)}, \frac{1}{p})$ random variable, we have that $V_P = \Theta(T)$, where T is the largest value up to $c = p^{a(p)}$ such that $\Pr\left[\textsc{Bin}(p^{a(p)}, \frac{1}{p}) \geq T\right] = \Omega(r) = \Omega(p^{b(p)})$. To upper bound the resulting prophet-gambler ratio, we want to determine or upper bound the value of T.

Case 2A: $b(p) \geq p^{a(p)}$. Intuitively, this case corresponds to there being sufficiently many rows that T will be set to c according to Fact 5. Formally, $\Pr[\textsc{Bin}(c, q) \geq c] = \Pr[\textsc{Bin}(c, q) = c] = (\frac{1}{p})^{p^{a(p)}} \geq (\frac{1}{p})^{b(p)} = \frac{1}{r}$, so $T = c = p^{a(p)}$. Hence $V_P = \Theta(p^{a(p)})$. Then the ratio $\frac{V_P}{V_G} = \Theta(\frac{p^{a(p)}}{1+p^{a(p)-1}}) = \Theta(p^{\min\{1,a(p)\}})$. Notice that this does not involve $b(p)$, so to determine the best bound that we can obtain, we should minimize the $p^{a(p)} \cdot \frac{b(p)}{a(p)}$ number of matroids by minimizing $b(p)$ in this case. Hence we pick $b(p) = p^{a(p)}$ and obtain a $\Theta(p^{\min\{1,a(p)\}})$ ratio with $\frac{p^{2 \cdot a(p)}}{a(p)}$ matroids.

There are two brief sub-cases. First, for $a(p) \geq 1$, the number of matroids $\frac{p^{2 \cdot a(p)}}{a(p)}$ is increasing in $a(p)$, while the ratio $\Theta(p^{\min\{1,a(p)\}}) = \Theta(p)$ is fixed over $a(p)$. Hence in the regime of $a(p) \geq 1$, it is optimal to pick the smallest $a(p)$ to minimize the number of matroids. Choosing $a(p) = 1$ yields p^2 matroids with ratio $\Theta(p)$, implying that the best lower bound for the $\textsc{Int}(m)$ problem we can claim from this case is $\Omega(\sqrt{m})$. Otherwise, in the $a(p) < 1$ regime, the ratio is $\Theta(p^{\min\{1,a(p)\}}) = \Theta(p^{a(p)})$. Then notice that letting $m := \frac{p^{2 \cdot a(p)}}{a(p)}$ denote the number of matroids, we have $\sqrt{m} = \frac{p^{a(p)}}{\sqrt{a(p)}} > p^{a(p)}$,

so the $\frac{V_P}{V_G}$ ratio must be $O(\sqrt{m})$, ruling this case out too.

Case 2B: $b(p) < p^{a(p)}$. This case corresponds to there being relatively fewer rows. Specifically, T as defined per Fact 5 may no longer set to c as before. We instead handle this case by considering what *minimum* value of T' (up to constants) the prophet would need to achieve to obtain a square-root bound overall. Since there are $m := p^{a(p)} \cdot \frac{b(p)}{a(p)}$ matroids and $V_G = \Theta(1 + p^{a(p)-1})$, we let $T' = (1 + p^{a(p)-1})\sqrt{m} = (1 + p^{a(p)-1})\sqrt{p^{a(p)} \cdot \frac{b(p)}{a(p)}}$.

According to the definition of T, there exists a constant k such that $\Pr\left[\textsc{Bin}(p^{a(p)}, \frac{1}{p}) \geq T\right] \geq \frac{k}{r}$ asymptotically. To show that this case does not yield improved bounds and thus complete the proof, we observe that it suffices to show that $\Pr\left[\textsc{Bin}(p^{a(p)}, \frac{1}{p}) \geq T'\right] \leq \frac{k}{r} = \frac{k}{p^{b(p)}}$ $(\star)$. This is because then $\Pr\left[\textsc{Bin}(p^{a(p)}, \frac{1}{p}) \geq T'\right] \leq \frac{k}{r} \leq \Pr\left[\textsc{Bin}(c, q) \geq T\right]$, which implies $T \leq T'$ since $\Pr\left[\textsc{Bin}(p^{a(p)}, \frac{1}{p}) \geq x\right]$ is decreasing in x. Hence we conclude $V_P = \Theta(T) = O(T') \Rightarrow \frac{V_P}{V_G} = O(\frac{T'}{1+p^{a(p)-1}}) = O(\sqrt{m})$ as desired. The proof of $(\star)$ is based on a Chernoff bound from Fact 16 and is deferred to Appendix C. ■

3.2. Ruled Out: Shaving Matroids in i Dimension

With parameter optimization of $\textsc{Grid}(r, c, q)$ ruled out, we now consider variants aimed at modifying the Grid structure in a way that preserves the hardness properties of the construction while decreasing the number of matroids used. For instance, a modified construction that uses only e.g. $p^{2-\varepsilon}$ while preserving the $\frac{V_P}{V_G} = \Omega(p)$ gap would by inversion improve the lower bound for $\textsc{Int}(m)$ to $m^{\frac{1}{2}+\Omega(\varepsilon)}$.

A natural first idea to this end is to understand what happens to the Grid structure (in particular, the $\frac{V_P}{V_G}$ ratio) if we simply drop some matroids from the intersection constraints. In particular, how does the construction change if we start with the $\textsc{Grid}(p^p, p, \frac{1}{p})$ structure and then remove some of the matroids $\{\mathcal{M}^{i,j}\}_{0 \leq i,j < p}$ by "shaving off" some set of the indices? In this section we consider such a "matroid shaving" along the i index dimension: given the same set of elements, we now define constraints by the intersection of matroids $\mathcal{M}^{i,j}$ only over all $i \in T \subsetneq \{0, ..., p-1\}$ and all $j \in \{0, ..., p-1\}$, i.e. shaving off the i indices $\{0, ..., p-1\} \setminus T$. We will show that for any (non-empty) $T \subsetneq \{0, ..., p-1\}$, such a shaving implies that $\frac{V_P}{V_G} = \Theta(1)$ (Theorem 6); with such a constant-factor approximation, we conclude that this variant cannot yield an improved $\textsc{Int}(m)$ lower bound.

Theorem 6 *Consider the $\textsc{Grid}(p^p, p, \frac{1}{p})$ construction modified such that constraints are defined by the intersection of matroids $\mathcal{M}^{i,j}$ only for $i \in T$ for some non-empty $T \subsetneq \{0, ..., p-1\}$ and $0 \leq j \leq p-1$. Then $V_P = \Theta(p), V(G) = \Theta(p)$, and hence $\frac{V_P}{V_G} = \Theta(1)$.*

Writing $T = \{i_1, i_2, \ldots, i_t\}$ s.t. $t = |T| < p$, the key idea is that such a shaving induces a *row grouping* where the p^{p+1} elements, normally divided in p^p rows with p elements each,

are now divided into p^t row groups of p^{p-t+1} elements each.[5] Specifically, for an element $e = (\vec{x}, y) = (x_0, ..., x_{p-1}, y)$ specified with base-p digits, the row group of e is determined by $\overline{x_T} = (x_{i_1}, x_{i_2}, \ldots, x_{i_t})$. In particular, the new feasible sets will now be the subsets of row groups, rather than just rows, but with the additional constraint that the columns of the elements are distinct, as the next lemma states.

Lemma 7 *Define $\mathcal{I}$ based on the intersection of matroids $\mathcal{M}^{i,j}$, each as defined for $\textsc{Grid}(p^p, p, \frac{1}{p})$, but only over all $i \in T$, $0 \leq j \leq p-1$. Then $\mathcal{I} = \{S \subseteq E : \forall(\vec{x_a}, y_a), (\vec{x_b}, y_b) \in S, \overline{x_{a,T}} = \overline{x_{b,T}}$ and $y_a \neq y_b\}$.*

The proof of this lemma is largely analogous to that of Proposition 2 and hence is deferred to Appendix C. We now analyze the prophet and gambler values to complete the proof of the theorem.

Proof of Theorem 6:

(I) **Prophet value** V_P. We claim that V_P is still $\Theta(p)$. Since we have only removed matroids (i.e. made strictly more subsets feasible), certainly the prophet value is at least as good as in the original $\textsc{Grid}(p^p, p, \frac{1}{p})$ construction. The key is that by Lemma 7, the elements of any $S \in \mathcal{I}$ must all be in distinct columns, so since there are $c = p$ columns, it follows that $|S| \leq p \Rightarrow V_P \leq p$.

(II) **Gambler value** V_G. The gambler now does much better: after accepting the first element, the gambler is only locked into a given row *group*, rather than a row. Each row group has p^{p-t+1} elements, with p^{p-t} elements in each of the p columns. Fix an arbitrary row group, and for each column j define an indicator variable Z_j that is 1 iff any of the p^{p-t} elements in column j in that row group is active (value-1). Then $\Pr[Z_j = 1] = 1 - \Pr[Z_j = 0] = 1 - (1 - \frac{1}{p})^{p^{p-t}} \geq 1 - (\frac{1}{e})^{p^{p-t-1}}$. Now observe that Z_j is exactly the value that the gambler can get from column j if the gambler is selecting from this particular row group, and so it follows that $V_G \geq \sum_{j=0}^{p-1} \mathbb{E}[Z_j] \geq (1 - (\frac{1}{e})^{p^{p-t-1}}) \cdot p = \Omega(p)$ since $(1 - (\frac{1}{e})^{p^{p-t-1}}) \geq (1 - \frac{1}{e})$ when $t < p$. Then since the maximum feasible set size is p, $V_G = \Theta(p)$. Hence we conclude that $\frac{V_P}{V_G} = \Theta(1)$. ■

Equivalence. From this analysis we can observe the following equivalence of the new structure. We can view a row group as having p "types" (i.e. columns) of elements, now with p^{p-t} copies per type (instead of each row having 1 copy per type), where for each row group what we now care about is precisely the random variable Z_j defined in the gambler analysis. But the Z_j variables (for $0 \leq j \leq p-1$) for each row group are just i.i.d Bernoulli variables—like the original element values $X_e \overset{iid}{\sim} \textsc{Bern}(q)$, but with a different success probability. In particular, this means the new structure is equivalent to the standard grid construction with p^t rows, p columns, and element success probability equal to $\Pr[Z_j = 1]$. This is stated precisely in Proposition 8.

[5] As a sanity check, note that the case of $T = \{0, ..., p-1\}$, i.e. $t = p$, means not removing any matroids, and then we recover the original $\textsc{Grid}(p^p, p, \frac{1}{p})$ construction as expected: the row groups are just the rows.

Proposition 8 *Consider the* GRID$(p^p, p, \frac{1}{p})$ *construction modified so that constraints are defined by the intersection of matroids* $\mathcal{M}^{i,j}$ *only for* $i \in T \subsetneq \{0, ..., p-1\}$, $0 \leq j \leq p-1$. *Then the modified structure is equivalent to* GRID$(\hat{r}, \hat{c}, \hat{q})$ *with* $\mathcal{I} = \mathcal{I}(\hat{r}, \hat{c})$, *where* $\hat{c} = p$, $\hat{r} = p^t$, *and* $\hat{q} = 1 - (1 - \frac{1}{p})^{p^{p-t}}$.

With this equivalent formulation, we can appeal to Theorem 4 as a more general reason for why shaving matroids in the i dimension won't improve the lower bound beyond $\Omega(\sqrt{m})$ — though for these particular parameters, the specific constant-factor approximation can be deduced directly as shown in this section.

3.3. Ruled Out: Shaving Matroids in j Dimension

We now turn to our final variant, in which we consider the natural follow-up question of whether shaving off matroids along the j dimension can yield improvements, if shaving along the i dimension does not. Specifically, how does the GRID$(p^p, p, \frac{1}{p})$ construction structure (in particular, the $\frac{V_P}{V_G}$ ratio) change if we consider the intersection of matroids $\mathcal{M}^{i,j}$ for all $i \in \{0, ..., p-1\}$ but only $j \in T \subsetneq \{0, ..., p-1\}$, i.e. shaving off the j indices $\{0, ..., p-1\} \setminus T$?

The changes to the constraint structure are harder to characterize than in the i shaving case, where Lemma 7 pins down the feasibility constraints and Proposition 8 provides an equivalent characterization of the overall modification. Indeed, the two indices i and j are far from symmetric in the definition of our matroid intersection structure. Now, for instance, two elements $e_a = (\vec{x_a}, y_a), e_b = (\vec{x_a}, y_a)$ in different rows become feasible so long as for all i, the j_i that satisfies $(x_{a,i} - x_{b,i}) \cdot j_i = y_b - y_a \pmod{p}$ is not in the set T. For arbitrary T and larger sets S of elements, this structure becomes increasingly complex. Instead of trying to directly characterize this structure, we will use a union bound argument to show that shaving matroids in this way again cannot improve the existing INT(m) lower bound, stated precisely below.

Theorem 9 *Consider the* GRID$(p^p, p, \frac{1}{p})$ *construction modified such that constraints are defined by the intersection of matroids* $\mathcal{M}^{i,j}$ *only for* $0 \leq i \leq p-1$ *and* $j \in T$ *for some non-empty* $T \subseteq \{0, ..., p-1\}$. *Then* $V_G = \Omega(\frac{p}{|T|})$, *which implies at best a* $\Omega(\sqrt{m})$ *bound for* INT(m).

Before stating the proof of Theorem 9, we first observe a simple but useful fact on the maximum feasible set size in any setup with a partition matroid $\mathcal{M}^{i,j}$ of the form we have been considering.

Fact 10 *Consider a construction with constraints* $\mathcal{I}$ *defined by the intersection of a positive number of* $\mathcal{M}^{i,j}$ *matroids, where* $\mathcal{M}^{i,j}$ *is defined as before by a partition* $E = \bigsqcup_k S_k^{i,j}$ *for* $0 \leq k \leq p-1$. *Then for any* $S \in \mathcal{I}$, $|S| \leq p$: *that is, the maximum feasible set size is* p.

The proof of Fact 10 simply follows from the fact that any $\mathcal{M}^{i,j}$ is a partition matroid defined by p partite sets $S_0, ..., S_{p-1}$, so by the Pigeonhole Principle, a set of size greater than p must have intersection larger than 1 with some partite set and thus cannot be independent in $\mathcal{M}^{i,j}$.

We are now ready to prove the main theorem.

Proof of Theorem 9:

Consider arbitrary non-empty $T \subseteq \{0, ..., p-1\}$ as the set of indices still present in the j dimension; the number of matroids is thus $p \cdot |T|$. Since we are just removing matroids, V_P will be at least as large as in the standard $\textsc{Grid}(p^p, p, \frac{1}{p})$ construction; combined with Fact 10, we have $V_P = \Theta(p)$.

For the gambler, we consider a strategy of only trying to select feasible elements from distinct columns. That is, for a currently selected gambler set $S = \{(\vec{x_1}, y_1), ..., (\vec{x_s}, y_s)\}$ where we inductively assume the columns $S_y := \{y_1, \ldots, y_s\}$ are all distinct, we will only try to add elements $(\vec{x}, y)$ from a column $y \notin S_y$. We will use a union bound argument to show the sufficient claim $(\star)$ that for any currently selected set $S = \{(\vec{x}_1, y_1), ..., (\vec{x}_s, y_s)\}$ such that $|S| = s < \frac{p-2}{|T|}$, then for any new column $y \notin S_y$, there are at least 2^p elements, i.e. rows $\vec{x}$, s.t. it is feasible to add $(\vec{x}, y)$ to S.

Let us first understand why claim $(\star)$ will be sufficient. First, given that $\textsc{Grid}$ element values are i.i.d $\textsc{Bern}(\frac{1}{p})$ random variables, note that we will always assume the gambler only tries to select active elements: it is clearly always worthless to select a value-0 element. Claim $(\star)$ implies that when the gambler has so far selected set S of some size $s < \frac{p-2}{|T|}$, then focusing on a specific new column $y \notin S_y$, the probability that there are no *active* elements $(\vec{x}, y)$ to feasibly extend S with is at most $(1 - \frac{1}{p})^{2^p} \leq (\frac{1}{e})^{\frac{2^p}{p}}$. Let us denote such a "failure event" at the stage where the gambler set S has size s as the event F_s, so $\Pr[F_s] \leq (\frac{1}{e})^{\frac{2^p}{p}}$. Observe that if F_s does *not* happen, the gambler can extend the set S to a set (of active elements) of size $s+1$ (for any $s < \frac{p-2}{|T|}$). In particular, putting these extensions together, this means that overall the gambler can obtain a final set S of size $\frac{p-2}{|T|}$ in the event $\neg(\bigcup_{i=1}^{\frac{p-2}{|T|}-1} F_i)$ that no failures occur. Applying a union bound, this occurs with probability at least $1 - \sum_{i=1}^{\frac{p-2}{|T|}-1} \Pr[F_i] \geq 1 - (\frac{p-2}{|T|}) \cdot (\frac{1}{e})^{\frac{2^p}{p}} \geq 1 - (\frac{1}{e})^{\frac{2^p}{p} - \ln(p)} \geq 1 - \frac{1}{e}$. This result is sufficient because it implies $V_G \geq (1 - \frac{1}{e}) \cdot \frac{p-2}{|T|} = \Omega(\frac{p}{|T|})$, and thus $\frac{V_P}{V_G} = O(\frac{p}{p/|T|}) = O(|T|)$. We have $m := p \cdot |T|$ matroids; since $|T| \leq \sqrt{p \cdot |T|}$, it follows that $\frac{V_P}{V_G} = O(\sqrt{m})$, and the overall claim follows.

Thus it just remains to prove claim $(\star)$. Suppose the gambler has accepted $S = \{(\vec{x}_1, y_1), ..., (\vec{x}_s, y_s)\}$ such that $|S| = s < \frac{p-2}{|T|}$ as above, and we want to determine how many elements $(\vec{x}, y)$ are feasible to add to S from a particular column $y \notin S_y$. For any $a \in [s]$, $(\vec{x}, y)$ is dependent with $(\vec{x_a}, y_a)$ if for any i, $(x_{a,i} - x_i) \cdot j \equiv (y - y_a) \pmod{p} \Leftrightarrow x_i \equiv x_{a,i} - j^{-1}(y - y_a) \pmod{p}$ for some $j \in T \setminus \{0\}$, recalling that $y - y_a \neq 0$. Defining the set $T_{a,i} := \{x_{a,i} - j^{-1}(y - y_a) \pmod{p} : j \in T \setminus \{0\}\}$, we

can write that $(\vec{x}, y)$ is dependent with $(\vec{x_a}, y_a)$ if for any i, $x_i \in T_{a,i}$. Then considering all possible $a \in [s]$, we have that $(\vec{x}, y)$ is not feasible to add to S iff for any i, $x_i \in \bigcup_{a\in[s]} T_{a,i}$.

Now we apply the union bound: $|\cup_{a\in[s]} T_{a,i}| \leq \sum_{a\in[s]} |T_{a,i}| = s(|T|-1) \leq p-2$, since $s < \frac{p-2}{|T|}$. Hence for each coordinate i, there are at least 2 values in the set $\{0, ..., p-1\} \setminus \bigcup_{a\in[s]} T_{a,i}$, so there are at least 2 choices for each coordinate x_i s.t. overall $(\vec{x}, y)$ is feasible to add to S. Since there are p coordinates $0 \leq i \leq p-1$, this means there are at least 2^p choices for $\vec{x}$ given the column y, as desired. ■

Remark: The above proof remains valid if the set T of kept indices is allowed to vary across i, i.e. for each $0 \leq i \leq p-1$ we have matroids $\mathcal{M}^{i,j}$ for all (i, j) s.t. $j \in T_i \subseteq \{0, ..., p-1\}$, where $|T_0| = |T_1| = ... = |T_{p-1}|$ but otherwise each T_i can be arbitrary.

3.4. Discussion and Future Work with GRID$(p^p, p, \frac{1}{p})$ Variants

We briefly discuss some extensions of the three variants presented above. First, in §3.2 and §3.3 we only rule out matroid shavings from $\{\mathcal{M}^{i,j} : 0 \leq i, j, \leq p-1\}$ along the i or j dimension separately, which itself does not rule out the utility of a *mixed* shaving that removes some i and some j indices. However, notice that the specific result in Theorem 6 for i-dimension shaving says that as soon as we lose any i index we have $V_P = \Theta(p)$. We claim this also rules out any mixed shaving that *completely* removes some i index. Formally, if we only keep matroids $\mathcal{M}^{i,j}$ for (i, j) in some non-empty set $S \subsetneq \{(i, j) : 0 \leq i, j \leq p-1\}$ such that $\exists\, i_0$ s.t. $(i_0, j) \notin S$ for all j, then $V_P = V_G = \Theta(p) \Rightarrow \frac{V_P}{V_G} = \Theta(1)$. We can see this by first considering the i-dimension shaving with $T = \{0, ..., p-1\} \setminus \{i_0\}$ and applying Theorem 6, and then noticing that the mixed shaving defined by S only possibly removes more matroids. Then V_P and V_G can only increase, but they must still be $O(p)$ since the maximum feasible set size remains p by Fact 10.

Then the question that remains open is whether there is any *arbitrary* set $S \subsetneq \{(i, j) : 0 \leq i, j \leq p-1\}$—that for each i contains some pair (i, j)—such that only keeping $\mathcal{M}^{i,j}$ for $(i, j) \in S$ might yield an improvement. An additional extension would be to mesh the general parameterization with matroid shavings by considering an arbitrary GRID(r, c, q) construction and keeping an arbitrary set of indices $S \subsetneq \{(i, j) : 0 \leq i < \log_c r, 0 \leq j \leq c-1\}$. We have focused on GRID$(p^p, p, \frac{1}{p})$ when considering matroid shavings for concreteness and ease of analysis, and it is at least not immediate that the same conclusions must hold for any GRID(r, c, q).

Our i- and j-dimension shaving and parameter optimization results are thus not exhaustive, and the generalizations discussed above could be considered in future work. That said, we do believe that the results so far suggest that similar micro-optimizations focused directly on the [KW12] construction are unlikely to yield improvements. Hence alternate avenues of future work like those discussed in §4.2 and §5.2 may be more fruitful.

4. Writing GRID(r, c, q) with More General Matroids

Having ruled out some variants of the partition-matroid-based [KW12] construction in §3, we turn to a second avenue of investigation. Here, we generalize our question one step further: instead of partition matroids, can we obtain the GRID(r, c, q) construction via an intersection of matroids from other classes in a way that achieves an improved INT(m) lower bound? In particular, is it possible to construct arbitrary matroids $\{\mathcal{M}_i = (E, \mathcal{I}_i)\}_{i\in[m]}$ such that $\mathcal{I} := \bigcap_{i\in[m]} \mathcal{I}_i$ recovers the GRID constraints with r rows and c columns, i.e. $\mathcal{I} = \mathcal{I}(r, c)$, with an asymptotically fewer number of matroids m than if we were to only use partition matroids?

The answer is no: in §4.1, we show that partition matroids are optimal for minimizing the number of matroids needed to write $\mathcal{I}(r, c)$ as a matroid intersection (Theorem 11). While this result rules out the utility of e.g. laminar or graphic matroids in the context of GRID constructions, in §4.2 we discuss future work on relaxing our insistence on recovering exactly GRID constraints to consider more general hardness constructions, for which more general matroid classes may still be useful. We also note that our question falls within the broader, relatively unstudied agenda proposed in [SVW22] of, when given a set system $\mathcal{I}$, trying to pin down the minimum number of matroids needed to write $\mathcal{I}$ as a matroid intersection. As such, this result provides some partial progress on the [SVW22] agenda for the special case of the the GRID constraint set system.

4.1. Partition Matroids Are Optimal for GRID

In this section we show that partition matroids are optimal for writing the constraints $\mathcal{I}(r, c)$ of a GRID(r, c, q) construction as an intersection of the minimum number of matroids possible. Specifically, we will constructively prove in Theorem 11 that for any (r, c), if the constraints $\mathcal{I}(r, c)$ can be written as an intersection of m *arbitrary* matroids, then $\mathcal{I}(r, c)$ can in fact be written as an intersection of m *partition* matroids.

Theorem 11 *Consider a base set E as in the* GRID(r, c, q) *construction, and suppose we have m matroids $\mathcal{M}_1, \ldots, \mathcal{M}_m$ with corresponding constraints $\mathcal{I}_1, \ldots, \mathcal{I}_m$ such that $\mathcal{I} := \bigcap_{i=1}^m \mathcal{I}_i = \mathcal{I}(r, c)$. Then there exist partition matroids $\mathcal{M}'_1, \ldots, \mathcal{M}'_m$ with corresponding constraints $\mathcal{I}'_1, \ldots, \mathcal{I}'_m$ such that $\bigcap_{i=1}^m \mathcal{I}'_i = \mathcal{I}(r, c)$.*

The direct consequence is that we can rule out trying to improve the INT(m) lower bound by using a more general set of matroids to obtain the $\mathcal{I}(r, c)$ constraints, in the hopes of using fewer matroids than the number of partition matroids required. In particular, based on the connection between partition matroid intersections for $\mathcal{I}(r, c)$ and the product dimension of $Q(c, r)$ discussed previously, the following is an immediate corollary of the theorem:

Corollary 12 *The minimum number of (possibly arbitrary) matroids that need to be intersected to yield* GRID(r, c, q) *constraints* $\mathcal{I}(r, c)$ *is the product dimension* $PD(Q(c, r))$.

A central concept for the proof of the theorem will be the set $\mathcal{C}$ of minimal infeasible sets corresponding to some intersection constraints $\mathcal{I}$. Specifically, any set $S \in \mathcal{C}$ is a set of elements not in $\mathcal{I}$ whose proper subsets are all in $\mathcal{I}$. We refer to $\mathcal{C}$ as the *inter-circuits* of $\mathcal{I}$, extending the analogous notion of circuits of a matroid to matroid intersections. Importantly, the inter-circuits $\mathcal{C}$ characterize their corresponding intersection constraints $\mathcal{I}$, in the sense that to preserve $\mathcal{I}$ it suffices to preserve $\mathcal{C}$. This is because for any set $S \subseteq E$, $S \in \mathcal{I} \Leftrightarrow \nexists\, C \in \mathcal{C}$ s.t. $S \supseteq C$.

The crux of Theorem 11's proof below is the fact that the inter-circuits $\mathcal{C}$ corresponding to $\mathcal{I}(r, c)$ are very structured: they are exactly any pair of elements not in the same row, and thus in particular any $C \in \mathcal{C}$ has size 2. Concretely, for instance, the inter-circuits for an intersection of graphic matroids that yields $\mathcal{I}(r, c)$ must appear as parallel edges in some matroid; for laminar matroids that intersect to $\mathcal{I}(r, c)$, inter-circuits will appear as subsets of sets A with capacity $c(A) = 1$ in some laminar family $\mathcal{A}$. The proof will show how these dependent size-2 sets satisfy a transitivity relation that naturally induces a partition structure, which will be sufficient for preserving the inter-circuits, and hence the $\mathcal{I}(r, c)$ constraints, overall.

Proof of Theorem 11:

Suppose we have a set of arbitrary matroids $\mathcal{M}_1, \ldots, \mathcal{M}_m$ defined by $\mathcal{I}_1, \ldots, \mathcal{I}_m$ such that $\bigcap_{i=1}^m \mathcal{I}_i = \mathcal{I}(r, c) =: \mathcal{I}$ (where items E are elements of a GRID with r rows, c columns). Let $\mathcal{C}$ denote the inter-circuits of $\mathcal{I}$. For $\mathcal{I} = \mathcal{I}(r, c)$, observe that the corresponding inter-circuits are exactly given by $\mathcal{C} = \{\{e_1, e_2\} : e_1, e_2 \text{ are in different rows}\}$. Since it is sufficient to preserve $\mathcal{C}$ in order to preserve $\mathcal{I}$, we will show how to construct from the original matroids a set of partition matroids $\mathcal{M}'_1, \ldots, \mathcal{M}'_m$ with intersection constraints $\mathcal{I}' := \bigcap_{i=1}^m \mathcal{I}'_i$, such that the corresponding inter-circuits $\mathcal{C}'$ are equal to $\mathcal{C}$. This will allow us to conclude that $\mathcal{I}' = \mathcal{I} = \mathcal{I}(r, c)$ as desired.

For a given matroid $\mathcal{M}_i = (E, \mathcal{I}_i)$, the key idea is to consider the relation $\sim$ defined on E such that for any $e_1 \neq e_2 \in E$, $e_1 \sim e_2 \Leftrightarrow \{e_1, e_2\} \notin \mathcal{I}_i$. This relation is clearly symmetric, and the crucial observation is that it is also transitive: if $e_1 \sim e_2$ and $e_2 \sim e_3$, then $e_1 \sim e_3$. To see why, suppose that instead $e_1 \nsim e_3$, i.e. $B := \{e_1, e_3\} \in \mathcal{I}_i$. Then since $A := \{e_2\} \in \mathcal{I}_i$ (any single element is certainly feasible in $\mathcal{I} = \mathcal{I}(r, c)$) and $|B| > |A|$, by the independence augmentation property of matroids (M2) we must have that $\exists\, f \in B \setminus A$ s.t. $A \cup \{f\} \in \mathcal{I}$. But the only options for f are e_1 and e_3, and we know $e_1 \sim e_2$ and $e_2 \sim e_3$, yielding a contradiction.

As a consequence, we can partition the elements E into partite sets $E = S_1^i \sqcup \ldots \sqcup S_k^i$ with the following properties: (P1) for all j, either $|S_j^i| = 1$ or $\forall e_1 \neq e_2 \in S_j$, $\{e_1, e_2\} \notin \mathcal{I}_i$, and (P2) for any $e_1, e_2 \in E$ in different partite sets, $\{e_1, e_2\} \in \mathcal{I}_i$. We do this by starting with a partition into all singleton sets and iteratively merging two partite sets if one contains some e_a and the other contains

some e_b such that $e_a \sim e_b$. The transitivity of $\sim$ preserves the invariant that $\forall e_1 \neq e_2$ in some partite set, $e_1 \sim e_2$. When this procedure terminates, we will thus be left with sets satisfying (P1), and (P2) will be satisfied due to the termination condition itself. (For concrete examples in terms of laminar and graphic matroids, see (†) below.)

Now, we let $\mathcal{M}'_i$ be the partition matroid defined by the partition $\{S^i_1, \ldots, S^i_k\}$, with constraints $\mathcal{I}'_i = \{S \subseteq E : |S \cap S^i_j| \leq 1, \forall j \in [k]\}$. From properties (P1) and (P2) above, it follows that for all $e_1 \neq e_2 \in E$, $\{e_1, e_2\} \in \mathcal{I}'_i \Leftrightarrow \{e_1, e_2\} \in \mathcal{I}_i$ ($\star$). Furthermore, observe that $\mathcal{I}'_i \supseteq \mathcal{I}_i$: a set $S \notin \mathcal{I}'_i$ iff $|S \cap S^i_j| \geq 2$ for some j, which means that S contains some $\{e_1, e_2\} \subseteq S^i_j$ s.t. $e_1 \sim e_2$, i.e $\{e_1, e_2\} \notin \mathcal{I}_i$, and so $S \notin \mathcal{I}_i$. In words, we have only possibly added independent sets, not made any sets newly dependent. In particular, while we have possibly changed some sets of size more than 2 from dependent in $\mathcal{M}_i$ to independent in $\mathcal{M}'_i$, the key is that keeping such sets dependent is in fact useless given that any inter-circuit is size 2, and we have exactly preserved the dependence status of all size-2 sets by ($\star$).

Formally, consider the new intersection $\mathcal{I}'$ and corresponding inter-circuits $\mathcal{C}'$. First, $\mathcal{C} \subseteq \mathcal{C}'$, because using ($\star$) we have $\{e_1, e_2\} \in \mathcal{C} \Rightarrow \{e_1, e_2\} \notin \mathcal{I}_i$ for some $i \Rightarrow \{e_1, e_2\} \notin \mathcal{I}'_i \Rightarrow \{e_1, e_2\} \in \mathcal{C}'$, where the last implication follows since any singleton is always feasible in partition matroids, and so $\{e_1, e_2\}$ is indeed minimally infeasible. Finally, we claim $\mathcal{C}' \subseteq \mathcal{C}$ as well. If there were some set $C_1 \in \mathcal{C}' \setminus \mathcal{C}$, then $C_1 \notin \mathcal{I}'_i$ for some $i \Rightarrow C_1 \notin \mathcal{I}_i$, since $\mathcal{I}_i \subseteq \mathcal{I}'_i$. Then $C_1 \notin \mathcal{I}$ and so $\exists C_0 \subsetneq C$ s.t. $C_0 \in \mathcal{C}$ by definition of inter-circuits. But then $C_0 \in \mathcal{C}'$, and so C_1 is not minimally infeasible under $\mathcal{I}'$, yielding a contradiction. Thus we conclude $\mathcal{C}' = \mathcal{C}$ as desired. ■

(†) **Example cases of graphic and laminar matroids**. For concreteness, consider the following examples of the procedure in the proof above. If the original matroids $\{\mathcal{M}_i\}$ are graphic matroids, then the partition $S^i_1 \sqcup \cdots \sqcup S^i_k$ we construct for a given $\mathcal{M}_i$ is equivalent to breaking apart all cycles of length at least 3 (i.e. true cycles in the underlying simple graph) while keeping the parallel edges (which are the size-2 dependent sets), such that the partite sets are exactly given by the multi-edges. If $\{\mathcal{M}_i\}$ are laminar matroids, the partition is equivalent to dropping all sets A with capacity 2 or more, i.e. only keeping the capacity-1 sets, and possibly adding some singleton partite sets with capacity-1 as needed. The remainder of the proof shows that though we have changed the individual graphic and laminar matroid structures (into partition matroids), they intersect to the same $\mathcal{I}(r, c)$ intersection constraints.

4.2. Future Work with Other Sufficiency Conditions

We can more generally view the GRID(r, c, q) construction as an instance of the following framework: first identify a *sufficient condition* for witnessing a separation between V_P and V_G, and then determine how to write it as an intersection of matroids. For GRID constructions, the sufficient condition is

that any pair of elements in different rows is blocked from being feasible; these are precisely the inter-circuits $\mathcal{C}$ for $\mathcal{I} = \mathcal{I}(r, c)$.

Indeed, this condition is essential for our proof of the optimality of partition matroids for GRID: since only the size-2 dependent sets in each matroid matter for the overall constraints, the additional dependence structure that is possible in more general matroids becomes superfluous. But the GRID condition is not the only sufficient condition that could plausibly induce a useful gap between V_P and V_G. For instance, one easy extension that would still be sufficient (but perhaps not a useful change overall) would be to block any set of elements all in distinct rows at least whenever the set has size 3, instead of 2, or more generally at least size k for some constant k. For constructions based on such conditions, the argument used for the above theorem would no longer work to rule out even e.g. graphic or laminar matroids from improving upon partition matroids, as these classes can have circuits of size greater than 2 that might now become useful. Hence it may be fruitful to consider other sufficient conditions that can leverage the more expressive structure of matroid classes that generalize partition matroids.

An alternative extension of our result would be to reduce other mild generalizations of the GRID construction back to product dimension difficulty (as in Corollary 12). As a simplistic concrete example, suppose we thought a sufficient condition of blocking all different-row pairs *except* one (or a constant number) could be useful, i.e. could be written as an intersection of asymptotically fewer matroids. But then we could simply add in a constant number of partition matroids to block all the missing pairs and recover the GRID sufficiency condition itself, and so asymptotically we can only do as well as we can do with the GRID condition. Applying similar reasoning more generally could help rule out the utility of other potential constructions relative to a product dimension-based improvement with GRID$(p^p, p, \frac{1}{p})$ itself.

5. Vector Matroid Constructions

The third avenue we consider is to start afresh and search for a new lower bound construction based on *vector matroids*. As discussed in Fact 1, vector matroids generalize each of the matroid classes discussed so far: any construction with partition, laminar, or graphic matroids can be expressed as a vector matroid construction. In that sense, vector matroids are the most expressive of the classes discussed, but this also means that the space of possible constructions to consider is much wider, and indeed largely unexplored.

As a first step into this space, we consider intersections of vector matroids each constructed independently and uniformly at random, motivated by a probabilistic method-based approach to demonstrating a lower bound. The goal would be to prove that with positive probability there must exist a hard instance, with some desired property that induces a separation between V_P and V_G, under

an intersection of few enough matroids to yield an improved $\textsc{Int}(m)$ lower bound. To understand the viability of such an approach, we investigate the properties of these random intersections, in particular the probabilities with which sets will be feasible or infeasible. In Fact 13 and Proposition 15 we provide characterizations that suggest why we cannot use probabilistic arguments to demonstrate a hard instance by intersecting such uniformly random vector matroids, *under the assumption* of Bernoulli item values. Overall, these preliminary results inform which avenues with vector matroids may be more promising to consider in the future, as discussed in §5.2.

5.1. Ruling Out Uniformly Random Mappings

We consider the following general setup for an intersection of vector matroids constructed independently and uniformly at random, parameterized over the number of items n; the vector space dimension d; and the number of matroids m. For convenience, we will refer to this as the "$\textsc{RandVec}(n, d, m)$" setup. View the item set as $E = [n]$. Independently for each $i \in [m]$, draw n vectors $v_1^i, ..., v_n^i$ independently and uniformly at random (with replacement) from the vector space $V = \mathbb{F}^d$ for some field $\mathbb{F}$. If $\mathbb{F}$ is an infinite field e.g. $\mathbb{F} = \mathbb{R}$, we define such a uniformly random draw as selecting a point uniformly at random from the unit sphere S^d in $\mathbb{F}^d$. Then define $\mathcal{M}_i = (E, \mathcal{I}_i)$ where $\mathcal{I}_i = \{S \subseteq E : \{v_j^i : j \in S\}$ is linearly independent in $V\}$, and finally the overall intersection constraints are $\mathcal{I} = \bigcap_{i=1}^m \mathcal{I}_i$. For the rest of the section, a set of vectors being "drawn randomly" from a vector space will mean that they are drawn as specified above: independently and uniformly at random, with replacement (so repetition is possible).

We begin by observing that this construction will not be useful when $\mathbb{F} = \mathbb{R}$, because in this case, the vector matroids actually recover d-uniform matroids.

Fact 13 *When $V = \mathbb{R}^d$, then each $\mathcal{M}_i = (E, \mathcal{I}_i)$ in the $\textsc{RandVec}(n, d, m)$ construction will be equivalent to a d-uniform matroid with probability 1. In particular, the intersection constraints $\mathcal{I} = \bigcap_{i=1}^m \mathcal{I}_i$ then yield an d-uniform matroid $\mathcal{M} = (E, \mathcal{I})$.*

> *Proof:* Consider each $\mathcal{M}_i = (E, \mathcal{I}_i)$ defined in the $\textsc{RandVec}(n, d, m)$ setup, with vectors $v_{[n]}^i$ randomly drawn from $V = \mathbb{R}^d$ and setting $\mathcal{I}_i = \{S \subseteq E : \{v_j^i : j \in S\}$ is linearly independent in $V\}$. We show that $\mathcal{M}_i$ is an d-uniform matroid. Clearly any set of $n' > d$ items must be dependent, since a set of more than d vectors cannot be independent in $\mathbb{R}^d$. Hence it suffices to show that for $r = \min(n, d)$, an arbitrary r-subset U of $v_{[n]}^i$ is linearly independent with probability 1, as this will imply that any $S \subseteq E$ is in $\mathcal{I}_i$ iff $|S| \leq d$ as desired.
>
> Consider arbitrary $U \subseteq v_{[n]}^i$ s.t. $|U| = r$. $U = \{u_1, \ldots, u_r\}$ is linearly dependent iff $\exists\ j \in [r]$ s.t. $u_j \in \text{span}(U \setminus \{u_j\})$. For any $j \in [r]$, $\text{span}(U \setminus \{u_j\})$ is at most a $(d-1)$-dimensional subspace of $\mathbb{R}^d$, so since u_j is drawn uniformly at random from the unit

hypersphere in $\mathbb{R}^d$, it follows that $\Pr[u_j \in \text{span}(U \setminus \{u_j\})] = 0$.[6] Union bounding over j, we have $\Pr[U \text{ is dependent}] \leq \sum_{j=1}^{r} \Pr[u_j \in \text{span}(U \setminus \{u_j\})] = 0$, as desired. The overall claim that $\mathcal{M} = (E, \bigcap_{i=1}^{m} \mathcal{I}_i)$ is an d-uniform matroid simply follows from noting that any set S of size at most d will be independent under each $\mathcal{I}_i$, since each $\mathcal{M}_i$ is an d-uniform matroid. ■

It immediately follows from Fact 13 that for any instance obtained in this way, $\frac{V_P}{V_G} = \Theta(1)$, since the intersection constraints just recover a single matroid and then we can apply the 2-approximation algorithm of [KW12]. Hence we cannot use such constructions to demonstrate an improved $\textsc{Int}(m)$ lower bound. Notice that there is nothing special about $\mathbb{R}$ used in the proof, so Fact 13 remains true if we replace $\mathbb{R}$ with any infinite field $\mathbb{F}$.

The failure of the infinite field case motivates the question of whether the dependence situation improves significantly for finite fields. We will see that the answer is negative: informally, large sets of items are still feasible with too high a probability to hope to induce any useful separation between V_P and V_G. We examine the case of $V = \mathbb{F}_2^d$, but the proofs can be generalized to other $\mathbb{F}_r^d$ for constant r. To start, we pin down the probability that a k-set of vectors randomly drawn from $V = \mathbb{F}_2^d$ is dependent.

Lemma 14 *Consider $V = \mathbb{F}_2^d$, and let U be a k-subset of vectors randomly drawn from V for some $k \leq d$. Then $\Pr[U \text{ is linearly dependent}] = \frac{2^k - 1}{2^d}$.*

Proof: Write $U = \{u_1, \ldots, u_k\}$, and let $U_0 = \emptyset$, $U_i = \{u_1, ..., u_i\} \subseteq U$ for all $1 \leq i < k$. Denote event $A_i = \{u_i \in \text{span}(U_{i-1}) \mid U_{i-1} \text{ is linearly independent in } V\}$. Then notice the events A_i are pairwise disjoint for all $1 \leq i \leq k$, and the event $\{U \text{ is linearly dependent}\}$ is exactly equal to $A_1 \sqcup \cdots \sqcup A_k$ (i.e. it occurs iff one of the A_i's occurs).

Thus $\Pr[U \text{ is linearly dependent}] = \sum_{i=1}^{k} \Pr[A_i]$. Now observe that $\Pr[A_i] = \frac{2^{i-1}}{2^d}$. This is because U_{i-1} being linearly independent in $V = \mathbb{F}_2^d \Rightarrow |\text{span}(U_{i-1})| = 2^{i-1}$, since U_{i-1} can be viewed as isomorphic to $\mathbb{F}_2^{i-1}$, and so for a vector u_i randomly drawn from $\mathbb{F}_2^d$ (independently of U_{i-1}), $\Pr[A_i] = \frac{|U_{i-1}|}{|V|} = \frac{2^{i-1}}{2^d}$. Hence $\Pr[U \text{ is linearly dependent}] = \frac{2^0}{2^d} + \frac{2^1}{2^d} + \cdots + \frac{2^{k-1}}{2^d} = \frac{2^k - 1}{2^d}$. ■

We will now use this lemma to now analyze feasibility in intersections of vector matroids under the general $\textsc{RandVec}(n, d, m)$ setup for $V = \mathbb{F}_2^d$. The crucial idea of large sets being feasible with high probability (for $m = \text{poly}(d)$ matroids) is presented formally in Proposition 15.

[6] Formally, extend a basis of $U \setminus \{u_j\}$ into a basis B of $\mathbb{R}^d$. Observe that u_j being in the span would mean having at least 1 exactly 0 coordinate w.r.t. B, which occurs with probability 0 for a random draw from the unit hypersphere.

Proposition 15 *Consider the* RandVec(n, d, m) *setup with* $V = \mathbb{F}_2^d$*, for any* $m = \text{poly}(d)$ *number of matroids and any* n*. Consider any* $k \leq n$ *such that* $d - k = \Theta(d)$*. Then for any* k*-subset* $S \subseteq E$*,* $\Pr[S \in \mathcal{I}] = 2^{-2^{-\Omega(d)}}$.

Before we prove Proposition 15, let us first understand why it suggests that a probabilistic method approach to lower bounds will not be viable under this RandVec(n, d, m) setup. We assume Bernoulli (0-1) item values (like in Grid setups) and hence view set sizes as equivalent with set value, since only active items will be picked. First, fixing d and $V = \mathbb{F}_2^d$, note that the maximum feasible set size will be d under any resulting vector matroid intersection, and so $\frac{V_P}{V_G} = O(d)$.[7] Then if m is super-$\text{poly}(d)$, this can yield at best a sub-polynomial lower bound for Int(m) and thus is not helpful.

Otherwise if m is $\text{poly}(d)$, Proposition 15 applies. We leave a rigorous proof of this case for future work and instead sketch our general intuition and reasoning. Intuitively, the issue is that we expect the gambler to do too well in the resulting RandVec(n, d, m) construction if any particular large (e.g. $\frac{d}{2}$-size) sets will be feasible with high probability. More specifically, a probabilistic lower bound argument would need to show that the probability of some desired hardness condition *not* occurring is *less than* 1. For instance, the Grid$(p^p, p, \frac{1}{p})$ construction is characterized by different-row pairs being blocked. One can show that intersecting $\Theta(p^2 \log(p))$ properly-defined random partition matroids ensures that the probability of such a feasible "bad" pair existing is less than 1, while preserving the feasibility of rows. Thus there must be some choice of $\Theta(p^2 \log(p))$ partition matroids that blocks all bad pairs and recovers Grid$(p^p, p, \frac{1}{p})$ constraints. Returning to our RandVec(n, d, m) setup, consider the consequences of the high feasibility probabilities. For example, we cannot even prove using the standard union bound of the probabilistic method that, fixing two arbitrary $\frac{d}{2}$-size subsets of items S_1 and S_2, there is some instance where both S_1 and S_2 are guaranteed to be blocked, since $2 \cdot \Pr[S_i \in \mathcal{I}] = 2 \cdot 2^{-2^{-\Omega(d)}} \not< 1$. Given the maximum feasible set size of d, it seems that any sufficient condition for hardness (or even just preventing the gambler from getting a constant-factor approximation) would certainly require blocking at least some two specific $\frac{d}{2}$-size sets, which we cannot guarantee through these constructions.

Proof of Proposition 15: Let $\mathcal{M}_1, \ldots, \mathcal{M}_m$ denote our m vector matroids, where in each $\mathcal{M}_i$ the corresponding vectors randomly drawn from $V = \mathbb{F}_2^d$ (independently across i) are denoted $v_1^i, \ldots, v_n^i$. Fix an arbitrary k-subset $S \subseteq E$, and then let $U_i = \{v_j^i : j \in S\}$ denote the corresponding vectors in the ith matroid. Then $\Pr[S \in \mathcal{I}] = \Pr[U_i \text{ is linearly independent in } V,\ \forall i \in [m]] = (1 - \frac{2^k - 1}{2^d})^m$ by Lemma 14, since $\{v_1^i, \ldots, v_n^i\}$ being drawn randomly means U_i itself can be viewed as a uniformly

[7] To see this rigorously, let B be the event that there is not even a single feasible active item. Then we can write $V_P \leq \Pr[B] \cdot 0 + (1 - \Pr[B]) \cdot d$ and $V_G = \Pr[B] \cdot 0 + (1 - \Pr[B]) \cdot 1 \Rightarrow \frac{V_P}{V_G} = O(d)$.

randomly-drawn k-subset from V, and by assumption certainly $k \leq d$. Thus we have

$$\begin{aligned}
\Pr[S \in \mathcal{I}] &\geq (1 - \frac{2^k}{2^d})^m \\
&= (1 - \frac{1}{2^{d-k}})^{2^{d-k} \cdot \frac{m}{2^{d-k}}} \\
&\geq \left(\frac{1}{4}\right)^{m \cdot 2^{k-d}} && \text{since } f(x) = (1 - \frac{1}{2^x})^{2^x} \text{ is increasing, and } f(1) = \frac{1}{4} \\
&\geq \left(\frac{1}{4}\right)^{2^{-d+k+c \lg d}} && \text{since } m = \text{poly}(d) \leq d^c \text{ for some } c > 0 \\
&= 2^{-2^{-\Theta(d)}} && \text{since } d - k = \Theta(d).
\end{aligned}$$

Thus, accounting for the lower bounding in the derivation, overall $\Pr[S \in \mathcal{I}] = 2^{-2^{-\Omega(d)}}$. ■

5.2. Discussion and Future Work with Vector Matroids

Our results in Fact 13 and Proposition 15 broadly suggest that we will need more structured mappings of items to vectors in $\mathbb{F}^d$, perhaps cleverly correlated across the set of matroids, in order to get mileage out of vector matroids for lower bound constructions. As we have discussed, what makes the RandVec(n, d, m) constructions inadequate for deriving useful lower bounds is that the setup is "too easy" for the gambler, due to arbitrary large sets being feasible with high probability. Thus the overarching question is how to derive a more complex dependence structure from vector matroid intersections in order to obtain a more meaningful hard instance.

We can gain some inspiration for future constructions by expressing the current Grid$(p^p, p, \frac{1}{p})$ construction in terms of vector matroids, recalling that partition matroids are special cases of vector matroids. Using the chain of constructions from the proof of Fact 1 and making some simplifications, we find that a partition matroid defined by a partition $E = S_1 \sqcup \cdots \sqcup S_k$ can be viewed as the vector matroid of the set of $|E|$ vectors in $\mathbb{F}_2^k$ given by $|S_i|$ copies of the i-th basis vector of $\mathbb{F}_2^k$, $\forall i \in [k]$. Applying this representation, we can write the Grid$(p^p, p, \frac{1}{p})$ constraints as an intersection of p^2 vector matroids, each defined by mapping the p^{p+1} elements to the p basis vectors of $\mathbb{F}_2^p$ in a particular way (as in §2.2) such that there are ultimately p^p copies of each basis vector.

Notice that, unlike our uniformly random setting, this is indeed a very structured mapping of elements to vectors: p^p copies of each of the p basis vectors are fixed, and then in the (i, j)-th matroid, element $(\vec{x}, y)$ is mapped to a copy of the k-th basis vector according to the expression $k := x_i \cdot j + y \mod p$. It may be fruitful to try to leverage parts of this structure when searching for vector matroid-based constructions in the future, particularly given the hardness properties (§2.2.1) we consider as guiding principles for lower bound constructions. For instance, one such variation

that could be considered is the following: instead of having p 1-dimensional sets of p^p vectors each as in the vector version of $\textsc{Grid}(p^p, p, \frac{1}{p})$, is there a useful generalization to having some q r-dimensional sets of $\frac{|E|}{q}$ vectors each, for some q and some (likely small) r?

6. Conclusion

In this study, we investigate new constructions aimed at demonstrating an improved lower bound for the $\textsc{Int}(m)$ PI problem. The gap between an $O(m)$ upper bounds and roughly-$\Omega(\sqrt{m})$ lower bounds has remained open for over a decade, so any asymptotic improvements would represent major progress, while even ruling out certain constructions would point future work in the right direction. To this end, we consider three main avenues that involve (1) extending the [KW12] construction to some close variants, (2) writing the [KW12] construction's constraints with arbitrary matroids, and (3) constructing vector matroid intersections uniformly at random. Our main results rule out certain constructions or approaches in each avenue.

We have discussed takeaways and future work specific to each of our three avenues in §3.4, §4.2, and §5.2, so we conclude with two overarching implications that we draw from our results. First, our first two avenues of investigation (§3 and §4) suggest that the only viable way forward with the existing construction is likely to attack the combinatorial problem of improving the product dimension: alternatives based on modifying or optimizing the existing structure simply does not seem to help. Second, our work with vector matroids in §5 is just one starting point out of many potential constructions with more general matroid classes. In particular, we have only scratched the surface of an extensive body of matroid theory that could certainly inform an $\textsc{Int}(m)$ lower bound construction or reveal connections to useful linear algebraic and graph theoretic tools, just like the connection between partition matroid intersections and the product dimension of graphs. We believe that combining this matroid theory with the hardness principles drawn from the [KW12] construction will be central to the search for an improved lower bound going forward.

7. Acknowledgements

I thank Professor Matthew Weinberg for his unwavering support and mentorship in this project over the past year, and for guiding me through all things college and career over the past three years. I also thank my parents for supporting me through the ups and downs of the research process.

This paper represents my own work according to University regulations. X - Arya Maheshwari

Appendix

A. Proof: Vector Matroids Generalize Graphic Matroids

We show that vector matroids generalize graphic matroids by proving that any graphic matroid $\mathcal{M}$, i.e. the cycle matroid of some graph $G = (V, E)$, can be recovered as the vector matroid of the column set of the *vertex-edge incidence matrix* of (a directed version of) G.

Proof [Oxl11]: Let $\mathcal{M}$ be the cycle matroid of $G = (V, E)$. First, arbitrarily orient the edges of G to obtain directed $\vec{G}$. We refer to an edge with the same head and tail as a "loop" edge; all other edges are "non-loop" edges. Define the incidence matrix $A(\vec{G})$, with entries viewed over *any* field $\mathbb{F}$, as the $|V| \times |E|$ matrix where each column represents an edge, and

$$a_{ij} = \begin{cases} 1 & \text{edge } j \text{ is non-loop, vertex } i \text{ is its head} \\ -1 & \text{edge } j \text{ is non-loop, vertex } i \text{ is its tail} \\ 0 & \text{otherwise} \end{cases}$$

.

We first show why a dependent set in $\mathcal{M}$, i.e. a set S of edges that contains a cycle, corresponds to a linearly dependent set of columns of $A(\vec{G})$. If S contains a loop edge e_0, then observe that the corresponding column in $A(\vec{G})$ is the zero vector $\vec{0}$ and hence S is already linearly dependent. Otherwise, S contains some cycle $C \subseteq E$ given by edges $C = e_1 \to \cdots \to e_t$ of (undirected) G, with some corresponding vertices $v_1 \to \cdots \to v_t \to v_1$. Let $\vec{e_1}, \ldots, \vec{e_t}$ denote the column vectors corresponding to the edges of C. For each $k \in [t]$, let $c_k = \pm 1$: 1 if the orientation of e_k in $\vec{G}$ matches the orientation we traverse e_k when traversing the cycle C as $e_1 \to \cdots \to e_t$, and -1 otherwise. Then one can observe that the linear combination given by $c_1\vec{e_1} + \cdots + c_t\vec{e_t}$ is equal to $\vec{0}$: each row/vertex in the cycle gets exactly one $+1$ and -1 in the sum, which cancel out and leave an overall sum of $\vec{0}$.

To complete the proof, we need to show why any linearly dependent set T of $A(\vec{G})$'s columns correspond to a set of edges T_e of G containing a cycle; then it will follow that independence constraints of the vector matroid of $A(\vec{G})$ must be exactly equal to those of $\mathcal{M}$. First, if T contains some column $\vec{e} = \vec{0}$, then the corresponding edge $e \in T_e$ must be a self-loop, and hence we are done. Otherwise, suppose $T = \{\vec{e_1}, ..., \vec{e_t}\}$ is our set of columns, corresponding to edges $T_e = \{e_1, \ldots, e_t\}$, such that some not-all-zero linear combination $c_1\vec{e_1} + \cdots + c_t\vec{e_t}$ yields $\vec{0}$. Consider any vertex v incident to any edge in T_e, i.e. the corresponding row v is non-zero in some vector $\vec{e_j} \in T$. For the overall sum in row v to be zero, notice that there must be a non-zero entry at row v in some other vector $\vec{e_k}$ as well. Translated to graph language, each vertex v incident to an edge in T_e has degree at least 2 in the subgraph defined by T_e. This immediately implies that T_e must contain a

cycle: one can consider an extremal argument by taking a longest path in the subgraph, and then noticing that there must be another edge from the final vertex that creates a cycle. Hence for any linearly dependent set T of columns, the corresponding set of edges T_e contains a cycle and hence is dependent in the original graphic matroid $\mathcal{M}$. ■

B. Binomial Analysis for Prophet Value

To rigorously prove Fact 5 on the prophet's value we must analyze the underlying binomial distributions in $\textsc{Grid}(r, c, q)$ constructions. Recall that in the $\textsc{Grid}(r, c, q)$ construction, the total value of elements in a given row i is given by a random variable $R_i \sim \textsc{Bin}(c, q)$. Thus the prophet's value is given by $V_P = \mathbb{E}[\max_{1\le i\le r} R_i]$. Then to pin down V_P in the case that $V_P = \Omega(1)$ is known, the key question is what the largest ("threshold") value T is that the $\textsc{Bin}(c, q)$ distribution will exceed with probability $\Omega(\frac{1}{r})$, as formalized in Fact 5 rewritten below.

Fact 5 (rewritten). Consider a $\textsc{Grid}(r, c, q)$ construction with row values $R_i \sim \textsc{Bin}(c, q)$, and suppose $V_P = \Omega(1)$ is known. Let T be the *largest* value of x up to c such that $\Pr[R_i \ge x] = \Omega(\frac{1}{r})$ Then $V_P = \Theta(T)$.

Proof: We first show that for T as defined above, $V_P = \Omega(T)$. We have $V_P = \mathbb{E}[\max_{1\le i\le r} R_i] \ge \Pr[\max_{1\le i\le r}(R_i) \ge T] \cdot T$. Then we have that $\Pr[\max_{1\le i\le r}(R_i) \ge T] = 1-(1-\Pr[R \ge T])^r \ge 1 - (1 - \frac{k}{r})^r \ge 1 - (\frac{1}{e})^k$, for some constant k (asymptotically). Here R represents the random value of any particular row (noting that the row values R_i are all i.i.d). Hence we conclude $V_P \ge (1 - (\frac{1}{e})^k)T = \Omega(T)$, since k is a constant.

The upper bound is the main content of this statement. We can express the prophet value precisely as follows:

$$
\begin{aligned}
V_P &= \mathbb{E}[\max_{1\le i\le r}(R_i)] \\
&= \int_{x=0}^{\infty} \Pr\left[\max_{1\le i\le r}(R_i) \ge x\right] dx && \mathbb{E} \text{ of non-neg. r.v.} \\
&\le \int_{x=0}^{\infty} \min\{r \cdot \Pr[R \ge x], 1\} dx && \text{by union bound, where } R \sim \textsc{Bin}(c, q) \\
&= \int_{x=0}^{T} 1 dx + \int_{x=T}^{\infty} r \cdot \Pr[R \ge x] && \text{by def'n of } T \\
&= T + r \int_{x=T}^{\infty} \cdot \Pr[R \ge x]
\end{aligned}
$$

The key assertion that we use but do not prove here is the following: given our definition of T, under the assumption that $V_P = \Omega(1)$, the integral $r \int_{x=T}^{\infty} \cdot \Pr[R \ge x]$ is in fact $O(T)$.

This technical fact can be derived using binomial tail bounds; the rough idea is that binomial distributions are not tail-heavy. Then we have $V_P \leq T + O(T) = O(T)$, and hence overall we conclude $V_P = \Theta(T)$. ■

We also use the following concentration inequality that results from applying a Chernoff bound to a binomial random variable, which can be found in e.g. [HB23].

Fact 16 *For $X \sim \textsc{Bin}(n, p)$ with mean $\mu = np$ and any $\delta \geq 0$,*

$$\Pr[X \geq (1+\delta)\mu] \leq \exp(-\mu[(1+\delta)\ln(1+\delta) - \delta])$$

.

C. Proofs from §4: [KW12] Construction Variants

We complete the omitted sections of Theorem 4's proof in the following two claims. We assume a general $\textsc{Grid}(r, c, q)$ setup as in the theorem (but we do not re-parameterize for the following claim, for simplicity).

Claim 17 *Let A denote the event that there exists an active element in an instance of $\textsc{Grid}(r, c, q)$, and let N_A be a random variable denoting the number of active elements. Then $V_G = o(1)$ implies $\mathbb{E}[N_A] \leq \frac{1}{2}$ and furthermore that $V_G \geq V_P/2$.*

Proof: We show the first implication by contrapositive, so assume $\mathbb{E}[N_A] \geq \frac{1}{2}$. Given $r \cdot c$ elements each with $\textsc{Bern}(q)$ values, by linearity $\mathbb{E}[N_A] = rcq$. Then $q \geq \frac{1}{2rc}$, and in particular $\Pr[A] = 1 - (1-q)^{rc} \geq 1 - (1 - \frac{1}{2rc})^{rc} \geq 1 - (1/e)^{1/2} = \Theta(1)$. Now observe that gambler value V_G is at least $\Pr[A]$, by considering the strategy of simply picking the first active element seen, and so $V_G = \Theta(1)$.

We now show that $V_G = o(1) \Rightarrow V_G \geq V_P/2$. The key claim is that $\Pr[A] \geq \mathbb{E}[N_A](1 - \mathrm{E}[N_A])$: this is clearly only useful when $\mathbb{E}[N_A] < 1$, but this is exactly the case we are in. To see why this is sufficient, observe that $V_G \geq \Pr[A]$ while $V_P \leq \mathbb{E}[N_A]$, since for Bernoulli values we have $V_P = \mathbb{E}[\max_{S \in \mathcal{I}}\{\text{number of active elements in } S\}] \leq \mathbb{E}[N_A]$. Then, since we have shown that $V_G = o(1) \Rightarrow \mathbb{E}[N_A] \leq \frac{1}{2}$, we can conclude $V_G \geq \Pr[A] \geq \mathbb{E}[N_A](1 - \mathbb{E}[N_A]) \geq \mathbb{E}[N_A]/2 \geq V_P/2$.

The short proof of the key claim follows. Let E denote the set of elements, and let E_A denote the

(random) set of active elements below.

$$\begin{aligned}
\Pr[A] &\geq \Pr[N_A = 1] \\
&= \sum_{e \in E} \Pr[e \in E_A] \Pr[f \notin E_A, \forall f \neq e \in E] \\
&\geq \sum_{e \in E} \Pr[e \in E_A] (1 - \mathbb{E}[N_A]) && (\star) \\
&= (1 - \mathbb{E}[N_A]) \sum_{e \in E} \Pr[e \in E_A] \\
&= (1 - \mathbb{E}[N_A])\mathbb{E}[N_A] && \text{by linearity}
\end{aligned}$$

where $(\star)$ is true because at least one element is active in the event $\neg\{f \notin E_A, \forall f \neq e \in E\}$, and so $\mathbb{E}[N_A] \geq 1 \cdot (1 - \Pr[f \notin E_A, \forall f \neq e \in E])$. ■

We complete the final derivation in Theorem 4 in the following claim.

Claim 18 *Let $p, a(p), b(p), m, k$ be as defined in §3.1 and the proof of Theorem 4. For $T' = (1+p^{a(p)-1})\sqrt{m} = (1+p^{a(p)-1})\sqrt{p^{a(p)} \cdot \frac{b(p)}{a(p)}}$, it holds asymptotically that $\Pr\left[\textsc{Bin}(p^{a(p)}, \frac{1}{p}) \geq T'\right] \leq \frac{k}{r} = \frac{k}{p^{b(p)}}$.*

Proof: We henceforth write $a := a(p)$, $b := b(p)$ for brevity throughout the derivation but we emphasize these are still functions of p. Let $X \sim \textsc{Bin}(p^a, \frac{1}{p})$, with $\mu = \mathbb{E}[X] = p^{a-1}$. Observe that $T' = (1 + p^{a-1})\sqrt{p^a \cdot \frac{b}{a}} > \mu$, so let $\delta > 0$ be such that $T' = (1 + \delta)\mu$.

By the Chernoff bound from Fact 16, we have $\Pr[X \geq T'] \leq \exp(-\mu[(1 + \delta)\ln(1 + \delta) - \delta])$. By rewriting the claimed bound, observe that it suffices to show that $\mu[(1 + \delta)\ln(1 + \delta) - \delta] \geq (b \ln p - \ln k)$, as derived below.

$$\begin{aligned}
\mu(1 + \delta)\ln(1 + \delta) - \mu\delta &= T' \ln(1 + \delta) - (T' - \mu) && \text{def'n of } \delta \\
&= T' [\ln(T'/\mu) - 1] + \mu && (1 + \delta) = \frac{T'}{\mu} \\
&= (1 + p^{a-1})\sqrt{p^a \cdot \frac{b}{a}} \cdot \left[\ln\left(\frac{1 + p^{a-1}}{p^{a-1}}\sqrt{p^a \cdot \frac{b}{a}}\right) - 1\right] + \mu && \text{def'n of } T', \mu \\
&\geq (1 + p^{a-1})\sqrt{p^a \cdot \frac{b}{a}} \cdot \left[\ln\left((1 + p^{1-a})\sqrt{p^a \cdot \frac{b}{a}}\right) - 1\right]
\end{aligned}$$

Since $\ln\left((1 + p^{1-a})\sqrt{p^a \cdot \frac{b}{a}}\right) \gg 1$ asymptotically in the parameter $m = p^a \cdot \frac{b}{a}$, we can drop the final -1 in the above expression. We want to show that this expression is at least $(b \ln p - \ln k)$ but

observe that $\ln k$ is just a constant, while the above expression again is $\gg 1$ asymptotically in our parameters. Hence we can neglect the $\ln k$ term as well. Now, when $a > 1$, we have

$$\begin{aligned}
(1+p^{a-1})\sqrt{p^a \cdot \frac{b}{a}} \cdot \left[\ln\left((1+p^{1-a})\sqrt{p^a \cdot \frac{b}{a}}\right)\right] &\geq \frac{p^{a-1}}{\sqrt{a}}\sqrt{p^a \cdot b} && \text{drop the } \ln \text{ term} \\
&\geq \frac{p^{a-1}}{\sqrt{a}} b && b < p^a \text{ by assumption} \\
&> b \ln p
\end{aligned}$$

where the last inequality follows because it can be shown that $\frac{p^{a-1}}{\sqrt{a}} > \ln(p)$ holds asymptotically in p for $a = a(p) > 1$.

In the other case when $a \leq 1$,

$$\begin{aligned}
(1+p^{a-1})\sqrt{p^a \cdot \frac{b}{a}} \cdot \ln\left((1+p^{1-a})\sqrt{p^a \cdot \frac{b}{a}}\right) &\geq (\sqrt{p^a \cdot b}) \cdot \ln\left(p^{1-a}\sqrt{p^a \cdot b}\right) \\
&= (\sqrt{p^a \cdot b}) \cdot \ln\left(\sqrt{p \cdot p^{1-a} \cdot b}\right) \\
&= b \cdot \sqrt{\frac{p^a}{b}} \cdot \ln\left(p/\sqrt{\frac{p^a}{b}}\right) \\
&\geq b \ln p
\end{aligned}$$

where the last inequality follows because $k(p) \cdot \ln(\frac{p}{k(p)}) > \ln(p)$ is true asymptotically in p, for any $1 < k(p) < p$ (and we set $k = \sqrt{\frac{p^a}{b}}$, which satisfies this as $b < p^a$ and $a \leq 1$).

Thus we can conclude overall that $\mu[(1+\delta)\ln(1+\delta) - \delta] \geq b \ln p$ for all a, which completes the proof of the claim and in turn the proof of Theorem 4. ■

The proof for Lemma 7 (repeated from above) is also presented below.

Lemma 7. Define $\mathcal{I}$ based on the intersection of matroids $\mathcal{M}^{i,j}$, each as defined for $\textsc{Grid}(p^p, p, \frac{1}{p})$, but only over all $i \in T$, $0 \leq j \leq p-1$. Then $\mathcal{I} = \{S \subseteq E : \forall (\vec{x_a}, y_a), (\vec{x_b}, y_b) \in S, \overline{x_{a,T}} = \overline{x_{b,T}}$ and $y_a \neq y_b\}$.

Proof of Lemma 7: We first show that any set S satisfying the conditions in the statement is independent in all matroids $\mathcal{M}^{i,j}$ for $i \in T$, $0 \leq j \leq p-1$. Specifically, for any two elements $e_a = (\vec{x_a}, y_a)$ and $e_b = (\vec{x_b}, y_b)$ s.t. $\overline{x_{a,T}} = \overline{x_{b,T}}$ and $y_a \neq y_b$, $\nexists S_k^{i,j}$ s.t. both e_a and e_b are in $S_k^{i,j}$. This is because for any $i \in T$, $x_{a,i} = x_{b,i}$, so $x_{a,i} \cdot j + y_a \neq x_{b,i} \cdot j + y_b \pmod p$ for all $0 \leq j \leq p-1$ since $y_a \neq y_b \pmod p$.

Any set S not satisfying the conditions in the statement must have two elements $e_a = (\vec{x_a}, y_a)$, $e_b = (\vec{x_b}, y_b)$ s.t. either $y_a = y_b$ or $\overline{x_{a,T}} \neq \overline{x_{b,T}}$. Thus to complete the proof, it suffices to show that $\exists S_k^{i,j}$ s.t. e_a and e_b are both in $S_k^{i,j}$, and hence the set S containing them is not independent in $M^{i,j}$.

First, if $\overline{x_{a,T}} \neq \overline{x_{b,T}}$, then $\exists\, i \in T$ s.t. $x_{a,i} \neq x_{b,i}$. Then the same argument from Proposition 2 shows that there exists $0 \leq j \leq p-1$ s.t. $x_{a,i} \cdot j + y_a = x_{b,i} \cdot j + y_b \pmod p =: k$, and then $e_a, e_b \in S_k^{i,j}$. The new case to handle is $y_a = y_b$: here, observe that $x_{a,i} \cdot 0 + y_a = x_{b,i} \cdot 0 + y_b \pmod p$ holds for any i, and in particular both e_a, e_b are in $S_{y_a}^{i,0}$. ■

References

[AA20] Noga Alon and Ryan Alweiss, *On the product dimension of clique factors*, European Journal of Combinatorics **86** (2020), 103097.

[Ala11] Saeed Alaei, *Bayesian combinatorial auctions: Expanding single buyer mechanisms to many buyers*, Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science (USA), FOCS '11, IEEE Computer Society, 2011, p. 512–521.

[AW18] Marek Adamczyk and Michal Wlodarczyk, *Random order contention resolution schemes*, 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS) (Paris), IEEE, October 2018, p. 790–801.

[BIK07] Moshe Babaioff, Nicole Immorlica, and Robert Kleinberg, *Matroids, secretary problems, and online mechanisms*, Symposium on Discrete Algorithms (SODA'07), 2007, pp. 434–443.

[CCF+22] José Correa, Andrés Cristi, Andrés Fielbaum, Tristan Pollner, and S Matthew Weinberg, *Optimal item pricing in online combinatorial auctions*, International Conference on Integer Programming and Combinatorial Optimization, Springer, 2022, pp. 126–139.

[CHMS10] Shuchi Chawla, Jason D Hartline, David L Malec, and Balasubramanian Sivan, *Multi-parameter mechanism design and sequential posted pricing*, Proceedings of the forty-second ACM symposium on Theory of computing, 2010, pp. 311–320.

[Din13] Michael Dinitz, *Recent advances on the matroid secretary problem*, ACM SIGACT News **44** (2013), no. 2, 126–142.

[DK15] Paul Dütting and Robert Kleinberg, *Polymatroid prophet inequalities*, Algorithms - ESA 2015 (Berlin, Heidelberg) (Nikhil Bansal and Irene Finocchi, eds.), Lecture Notes in Computer Science, Springer, 2015, p. 437–449 (en).

[Fin11] Liri Finkelstein, *Two algorithms for the matroid secretary problem*, Citeseer, 2011.

[FSZ16] Moran Feldman, Ola Svensson, and Rico Zenklusen, *Online contention resolution schemes*, Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, Society for Industrial and Applied Mathematics, January 2016, p. 1014–1033 (en).

[HB23] Mor Harchol-Balter, *Introduction to probability for computing*, Cambridge University Press, 2023.

[HKS07] Mohammad Taghi Hajiaghayi, Robert D. Kleinberg, and Tuomas Sandholm, *Automated online mechanism design and prophet inequalities*, Proceedings of the Twenty-Second AAAI Conference on Artificial Intelligence, July 22-26, 2007, Vancouver, British Columbia, Canada, AAAI Press, 2007, pp. 58–65.

[KS78] Ulrich Krengel and Louis Sucheston, *On semiamarts, amarts, and processes with finite value*, Probability on Banach spaces **4** (1978), 197–266.

[KW12] Robert Kleinberg and Seth Matthew Weinberg, *Matroid prophet inequalities*, Proceedings of the forty-fourth annual ACM symposium on Theory of computing, 2012, pp. 123–136.

[Oxl11] James Oxley, *Matroid Theory*, Oxford University Press, 02 2011.

[SC84] Ester Samuel-Cahn, *Comparison of Threshold Stop Rules and Maximum for Independent Nonnegative Random Variables*, The Annals of Probability **12** (1984), no. 4, 1213 – 1216.

[SVW22] Raghuvansh R. Saxena, Santhoshini Velusamy, and S. Matthew Weinberg, *An improved lower bound for matroid intersection prophet inequalities*, arXiv:2209.05614 [cs].

[Von17] Jan Vondrák, *Math 233b: Polyhedral techniques in combinatorial optimization, lecture 7: Spanning trees and matroids*, February 2017.

[Whi35] Hassler Whitney, *On the abstract properties of linear dependence*, American Journal of Mathematics **57** (1935), no. 3, 509–533.