Limitations of Stochastic Selection with Pairwise Independent Priors

Shaddin Dughmi *
Department of Computer Science
University of Southern California
shaddin@usc.edu

Yusuf Hakan Kalayci *
Department of Computer Science
University of Southern California
kalayci@usc.edu

Neel Patel *
Department of Computer Science
University of Southern California
neelbpat@usc.edu

Abstract

Motivated by the growing interest in correlation-robust stochastic optimization, we investigate stochastic selection problems beyond independence. Specifically, we consider the instructive case of pairwise-independent priors and matroid constraints. We obtain essentially-optimal bounds for contention resolution and prophet inequalities. The impetus for our work comes from the recent work of Caragiannis et al. [19], who derived a constant-approximation for the single-choice prophet inequality with pairwise-independent priors.

For general matroids, our results are tight and largely negative. For both contention resolution and prophet inequalities, our impossibility results hold for the full linear matroid over a finite field. We explicitly construct pairwise-independent distributions which rule out an $\omega\left(\frac{1}{\mathrm{Rank}}\right)$ -balanced offline CRS and an $\omega\left(\frac{1}{\log\mathrm{Rank}}\right)$ -competitive prophet inequality against the (usual) oblivious adversary. For both results, we employ a generic approach for constructing pairwise-independent random vectors — one which unifies and generalizes existing pairwise-independence constructions from the literature on universal hash functions and pseudorandomness. Specifically, our approach is based on our observation that random linear maps turn linear independence into stochastic independence.

We then examine the class of matroids which satisfy the so-called partition property — these include most common matroids encountered in optimization. We obtain positive results for both online contention resolution and prophet inequalities with pairwise-independent priors on such matroids, approximately matching the corresponding guarantees for fully independent priors. These algorithmic results hold against the almighty adversary for both problems.

^{*}Supported by NSF Grant CCF-2009060.

Contents

1	Introduction	3				
2	Preliminaries2.1 Basic Notation and Terminology2.2 Matroid Theory2.3 Contention Resolution2.4 Prophet Inequalities2.5 A Useful Lemma for Pairwise Independent Events	6 6 6 7 8 8				
3	Overview of Technical Results 3.1 A Recipe for Pairwise-Independent Vector Families	9 10 11 13				
4	A Recipe for Pairwise-independent Vector Families 4.1 Ordered Pairwise Independent Vector Families	14 14 16				
5	Pairwise-independent Contention Resolution on Matroids 5.1 Limits of Pairwise Independent Contention Resolution	18 18 20				
6	$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	21 22 23 25 26 27 28 32				
7	The Partition Property and its Implications 7.1 Prophet Inequalities	34 35 37 38				
8	8 Open Questions					
\mathbf{A}	Missing Proofs from Section 4					

1 Introduction

Combinatorial optimization subject to uncertainty has gained substantial interest in recent years, initially motivated by its applications in computational economics ([34, 21]). In many of these tasks, the underlying uncertainty or stochasticity arises from either the random availability of elements of a set system or from a stochastic weight assignment to these elements. Two fundamental stochastic selection problems, contention resolution (e.g., [23, 2, 30, 48, 45]) and generalized prophet inequalities (e.g., [41, 32, 28]), fit into this paradigm. These problems appear either directly, or indirectly as subroutines, throughout the fields of algorithms and combinatorial optimization with a wide range of applications including approximation algorithms [23, 50, 32], mechanism design [48, 30, 29, 28, 4], online algorithms [38, 26, 50], stochastic probing [30, 3, 14], sparsification [27], and algorithmic delegation [40, 15, 16].

A rich literature examines the design of algorithms for these problems when the input is a product distribution or negatively correlated. However, our understanding is relatively limited when the input distribution exhibits correlations, particularly positive correlations, which are often present in many intended applications. For instance, consider the scenario of sequential posted pricing where a seller with a single item encounters n prospective buyers in sequence, each possessing a valuation for the product. The seller, with the goal of maximizing profit, offers a fixed, nonnegotiable price to each buyer, who then decides to buy the item if the price is less than or equal to their valuation. Yet, in today's hyper-connected world, it is unrealistic to presume buyers remain unaffected by or ignorant of each other's valuations. In fact, notable studies [47, 8] demonstrate this phenomenon by showing that the aggregate online reviews from a large group of buyers play a critical role in shaping customer behavior.

A deeper understanding of the interplay between correlation and optimal selection, and an expansion of the algorithmic and complexity-theoretic toolkit thereof, promises to impact the myriad aforementioned applications of decision-making subject to uncertainty. Of particular note is the matroid secretary conjecture of Babaioff et al. [9], which has recently been shown equivalent to stochastic selection in the presence of a particular kind of positive correlation by Dughmi [25, 26]. Algorithmic approaches for near-optimal decision making in the presence of correlation, as well as proof techniques for ruling out such algorithms, could therefore shed light on the conjecture.

A number of recent works explore a variety of models in which decisions must be made in the presence of correlated inputs [11, 17, 18, 31, 13, 36]. It is either known (e.g. [35, 49]), or easy to show, that not much can be achieved in the presence of arbitrary positive correlation. Even under assumptions like the *linear correlation model* of Bateni et al. [13], in the worst case there are no positive algorithmic results for prophet inequalities with non-sparse dependencies even for the rank one matroid as shown by Immorlica et al. [36].

Particularly inspiring our investigation is the recent work by Caragiannis et al. [19], which initiates the study of stochastic selection problems with inputs that are pairwise independent: any two random variables are independent, though positive or negative correlations can manifest when considering larger groups of variables. Pairwise independence significantly relaxes the usual assumption of full independence, and pairwise independent distributions have found application in hashing, derandomization, and constructions of pseudo-random generators (for more details, see surveys [43, 52]). In the context of the sequential posted pricing mechanism, empirical studies [47, 8] emphasize the significant impact of a large number of aggregated online reviews on shaping customer behavior. These studies suggest that a buyer's valuation is influenced by reviews from a large number of consumers, whereas a small selection of customer reviews (which reflect their

valuations) have little effect. As such, pairwise (or more generally k-wise) independence serves as a reasonable idealization of such settings where correlations live largely in the higher-order moments of a distribution.

Caragiannis et al. [19] show that pairwise independence suffices for a constant approximation in the single-choice prophet inequality problem and sequential posted price mechanisms. This finding encourages further exploration of stochastic selection problems under the same pairwise independent assumption. Our focus is particularly on prophet inequalities and contention resolution schemes. This naturally leads us to the following question:

Question 1.1. Do constant approximation prophet inequalities or contention resolution schemes exist for a broader class of set-systems when the input distribution is pairwise independent?

We resolve the above question for matroids. We prove strong impossibility results for matroid prophet inequalities and contention resolution schemes when the stochastic inputs are only pairwise independent. These impossibility results hold even for the most permissive computational models considered for these problems, and stand in contrast to the strong algorithmic results for inputs that are mutually independent [41, 22, 42, 30]. The following summarizes our main contribution.

- There is no $\omega\left(\frac{1}{\log \mathbf{Rank}}\right)$ -competitive matroid prophet inequality for pairwise independent distributions. This holds even for the *oblivious adversary* who selects the order of elements in advance, and even for binary matroids.
- There is no $\omega\left(\frac{1}{\mathbf{Rank}}\right)$ -balanced contention resolution scheme for pairwise independent distributions. This holds even in the *offline* setting of contention resolution, and even for linear matroids.

We complement these negative results with simple algorithms that match these bounds when inputs are pairwise independent, even in the most restrictive of computational models considered for these problems: a $\Theta\left(\frac{1}{\log \mathbf{Rank}}\right)$ -competitive matroid prophet inequality and a $\Theta\left(\frac{1}{\mathbf{Rank}}\right)$ -balanced online contention resolution scheme. In contrast to our impossibility results, both our algorithmic results hold even for the almighty adversary who selects the order of elements with knowledge of all the realized inputs and any internal randomness of the algorithm

For both of our impossibility results, we carefully construct a pairwise independent distribution for the linear matroid \mathbb{F}_q^d for some large $d \in \mathbb{Z}_+$ and a suitable prime q. Our approach to constructing pairwise independent distributions is founded on the observation that uniformly random linear maps between vector spaces convert linear independence in the domain space to stochastic independence in the range space. To put it formally, when a family of k-wise linearly independent vectors is embedded in another vector space via a uniformly random linear map, the embedded vectors exhibit k-wise stochastic independence and each assumes a uniform marginal distribution over the second vector space. Special instances of this observation have previously been employed to define k-wise independent hash functions [20, 53] and k-wise independent random bits [5, 39, 6, 44]. For a comprehensive overview of prior work on the construction of pairwise independent distributions, we refer interested readers to the survey by [43] and to [52, Chapter 3]. Our method for constructing k-wise stochastically independent vectors can be viewed as a simple unification and vector-generalization of existing constructions of scalar-valued random variables.¹

¹Despite the simplicity of our construction, we have been unable to identify another construction with this level of generality. The concepts presented here permeate existing work on constructing k-wise independent random variables.

Later, we examine the class of matroids that satisfy the partition property — these include the most common matroids encountered in optimization. Informally, this property holds if a matroid can be approximated by a (random) partition matroid. We demonstrate that, when a matroid fulfills the partition property, we can reduce the problem to one defined over rank one matroids. Leveraging the results and machinery of [19], we obtain constant factor prophet inequalities and contention resolution schemes for pairwise independent distributions on matroids satisfying the partition property. As in our previous algorithmic results, our bounds hold even for the almighty adversary for both problems. We note the concurrent independent work of Gupta et al. [33], which also studies pairwise-independent stochastic selection. They obtain similar contention resolution schemes and prophet inequalities for a number of natural matroid classes such as the uniform, laminar, graphic, co-graphic, and regular matroids.

Finally, we mention that our results deepen the existing schism between matroids that admit the partition property and those that do not, and in doing so might shed light on the matroid secretary conjecture. Much of the interest in the partition property is due to the fact — pointed out in a survey by Dinitz [24] — that matroids satisfying the α partition property also admit an $O(\alpha)$ -competitive secretary algorithm. In fact, most classes of matroids for which constant-competitive secretary algorithms are known — such as graphic [10], co-graphic [51], and laminar [37] — satisfy a constant partition property. Moreover, many such algorithms either explicitly or implicitly exploit the partition property. Dinitz [24] therefore asked whether every matroid satisfies a constant partition property, as a possible route to resolving the matroid secretary conjecture. This question was answered negatively by the recent work of Abdolazimi et al. [1], who show that the full binary matroid of rank d does not satisfy the α -partition property for any $\alpha \leq O(d^{1/4})$. The parallel work of Bahrani et al. [12] also provides evidence of the limitations of partition-based algorithms for the secretary problem.

Our results add to this literature in two distinct ways. First, as corollaries of our results we show that full linear matroid \mathbb{F}_q^d with $q \geq d$ does not satisfy the α partition property for any $\alpha \leq O(d)$, and that the full binary matroid of rank d does not satisfy the partition property for any $\alpha \leq O(d/\log d)$, strengthening the bound of [1]. Second, by constructing provably "hard instances" for selection problems that are easy in the presence of the partition property, our techniques might shed light on the analogous question for the matroid secretary problem. In fact, showing that our construction for prophet inequalities remains hard in the random order model would disprove the matroid secretary conjecture. On the flip side, providing an algorithm for our construction in the random order model appears highly nontrivial, and therefore might stimulate the development of algorithmic techniques pertinent to the conjecture.

How to Read this Paper

We present pertinent preliminaries in Section 2, of which a light perusal is sufficient for the reader comfortable the basics of matroid theory, contention resolution, and prophet inequalities. We then present an abridged technical overview of our results and techniques in Section 3, followed by a more detailed treatment in Sections 4 through 7. The reader looking to get a high-level sense of our results and techniques is invited to focus primarily on Section 3, referring to the later technical sections for more detail as needed. We close with open questions in Section 8.

2 Preliminaries

2.1 Basic Notation and Terminology

We use bold lowercase letters to denote vectors, with the ℓ^{th} component of a vector \mathbf{v} denoted by $\mathbf{v}(\ell)$. Sets and matrices are denoted by uppercase letters, while collections of sets or matrices are denoted by bold uppercase letters. For a set S of indices into a vector \mathbf{v} , we denote $\mathbf{v}(S) = \sum_{\ell \in S} \mathbf{v}(\ell)$. We denote the set of positive integers up to n by [n]. For a set X, we denote its power set by 2^X , and use $\Delta(X)$ to denote the family of all distributions supported on X.

A set system is a pair $\mathcal{M}=(E,\mathcal{I})$ where E is a set of elements and $\mathcal{I}\subseteq 2^E$ is a family of feasible (a.k.a. independent) sets. We concern ourselves primarily with set systems where E is finite, and \mathcal{I} is downwards-closed: If $B\in\mathcal{I}$ and $A\subseteq B$ then $A\in\mathcal{I}$. For a vector $\mu\in[0,1]^E$ of marginals indexed by the elements, we use $\Delta_{pw}(2^E)(\mu)\subseteq\Delta(2^E)$ to denote the family of pairwise independent distributions over sets of elements with marginal probabilities μ , i.e. for every $\mathcal{D}(\mu)\in\Delta_{pw}(2^E)(\mu)$, $\mathbf{Pr}_{Q\sim\mathcal{D}(\mu)}[e\in Q]=\mu(e)$ and the events $\{e\in Q\}_{e\in E}$ are pairwise independent. We also consider distributions in $\Delta(\mathbb{R}^E_{\geq 0})$ that assign a nonnegative weight (a.k.a. value) to each element. We let $\Delta_{pw}(\mathbb{R}^E_{\geq 0})\subseteq\Delta(\mathbb{R}^E_{\geq 0})$ be the class of pairwise independent weight distribution over elements E—i.e., if $\mathbf{w}\sim\mathcal{D}\in\Delta_{pw}(\mathbb{R}^E_{\geq 0})$ then for any distinct pair of elements $e,f\in E$ their weights $\mathbf{w}(e)$ and $\mathbf{w}(f)$ are pairwise independent random variables. Throughout the paper, we interchangeably use the terms "weight" and "value".

For a prime number q, \mathbb{F}_q denotes the finite field with q elements and \mathbb{F}_q^d denotes the vector space of dimension d over \mathbb{F}_q . For a given set of integer labels $L \subseteq \mathbb{Z}$, we denote the collection of labeled vectors by $\mathbb{F}_q^d \times L := \{\mathbf{v}^i : \text{for all } i \in L \text{ and } \mathbf{v} \in \mathbb{F}_q^d\}$. We use capital letters to symbolize matrices over these finite fields, and their rank is denoted by $\mathbf{Rank}(\cdot)$. A matrix $R \in \mathbb{F}_q^{r \times c}$ is a full column-rank matrix if $\mathbf{Rank}(R) = c$, i.e. its columns constitute a set of linearly independent vectors. Additionally, we often refer to the columns of a matrix $R \in \mathbb{F}_q^{d \times n}$ using lowercase letters and subscripts, such as $\mathbf{r}_1, \dots \mathbf{r}_n \in \mathbb{F}_q^d$, and we occasionally allow ourselves some flexibility in notation (clarifying with re-declarations in context) to use the matrix R interchangeably with the set of its columns. For any matrix A, we denote its column space as $\mathbf{cl}(A)$.

2.2 Matroid Theory

We use standard definitions from matroid theory; for details see [46, 54]. A matroid $\mathcal{M} = (E, \mathcal{I})$ is a set-system with elements E and a family of independent sets $\mathcal{I} \subseteq 2^E$ satisfying the three matroid axioms. A weighted matroid incorporates a matroid $\mathcal{M} = (E, \mathcal{I})$ with weights $w \in \mathbb{R}^E$ for its elements.

By duplicating or making parallel labeled copies of each element of a matroid $\mathcal{M} = (E, \mathcal{I})$ "m" times, we construct a larger matroid $\mathcal{M}^{\times m} = (E^{\times m}, \mathcal{I}^{\times m})$. Here $E^{\times m}$ contains m parallel copies e^1, \ldots, e^m of each $e \in E$, and $T \subseteq E^{\times m}$ is in $\mathcal{I}^{\times m}$ if $\{e : e^i \in T \text{ for some i}\} \in \mathcal{I}$ and $|T \cap \{e^i : i \in [m]\}| \leq 1$ for all $e \in E$.

The rank function of matroid $\mathcal{M} = (E, \mathcal{I})$ is denoted by $\mathbf{Rank}^{\mathcal{M}}$, where $\mathbf{Rank}^{\mathcal{M}}(S) = \max\{|T| : T \subseteq S, T \in \mathcal{I}\}$. The weighted rank function $\mathbf{Rank}^{\mathcal{M}}_{\mathbf{w}}$ is defined for weighted matroids $(\mathcal{M}, \mathbf{w})$ as $\mathbf{Rank}^{\mathcal{M}}_{\mathbf{w}}(S) = \max\{\mathbf{w}(T) : T \subseteq S, T \in \mathcal{I}\}$. The span function of matroid \mathcal{M} is denoted by $\mathbf{Span}^{\mathcal{M}}(S)$ where $\mathbf{Span}^{\mathcal{M}}(S) = \{e \in E : \mathbf{Rank}^{\mathcal{M}}(S \cup \{e\}) = \mathbf{Rank}^{\mathcal{M}}(S)\}$. We

²Unless otherwise specified, we think of vectors as column vectors.

slightly abuse notation and use $\mathbf{Rank}(\mathcal{M}) = \mathbf{Rank}^{\mathcal{M}}(E)$ for the rank of the matroid. We may omit the superscript \mathcal{M} when it is clear from context.

The matroid polytope $\mathcal{P}(\mathcal{M}) \subseteq [0,1]^E$ associated with \mathcal{M} is the convex hull of all indicator vectors of its independent sets. Equivalently, a nonnegative vector μ is in $\mathcal{P}(\mathcal{M})$ if and only if $\sum_{e \in S} \mu_e \leq \mathbf{Rank}^{\mathcal{M}}(S)$ for all $S \subseteq E$.

A linear matroid $\mathcal{M}=(E,\mathcal{I})$ is a matroid where E is a family of vectors in some vector space, and \mathcal{I} consists of the linearly-independent subsets of E. We consider linear matroids where the underlying vector space is \mathbb{F}_q^d , for q a prime and $d \in \mathbb{N}$. When q=2, this is also referred to as a binary matroid. When $E=\mathbb{F}_q^d$ we call this the full linear matroid over \mathbb{F}_q^d , and when $E=\mathbb{F}_2^d$ we call it the full binary matroid with rank d.

The rank one matroid on elements E is the matroid whose independent sets are the singletons in E as well as the empty set. A simple partition matroid on E is the disjoint union of rank one matroids; i.e., there is a partition E_1, \ldots, E_k of E such that S is independent if and only if $|S \cap E_i| \leq 1$ for all i.

2.3 Contention Resolution

Contention Resolution is the algorithmic task of converting a random set which is feasible "on average" to on to one which is always feasible. Contention resolution in the offline setting was originally formalized by Chekuri et al. [23] for application to approximation algorithms. It has since been generalized, studied, and applied in various online models (see [30, 2, 42]). An algorithm for contention resolution is referred to as a Contention Resolution Scheme (CRS).

Fix a downward-closed set-system $\mathcal{M} = (E, \mathcal{I})$ over a ground set E of elements, as well as a convex relaxation $\mathcal{P}(\mathcal{M}) \subseteq [0, 1]^E$ of the indicator vectors of sets in \mathcal{I} . Let $\mu \in \mathcal{P}(\mathcal{M})$ be a vector of marginal probabilities, and let $A \subseteq E$ be a set of active elements drawn from a known distribution $\mathcal{D} \in \Delta(2^E)$ satisfying $\mathbf{Pr}_{A \sim \mathcal{D}}[e \in A] = \mu(e)$ for all $e \in E$. Given these inputs, the goal of a CRS is to select (a.k.a. accept) a feasible subset of the active elements — i.e., a set $I \in \mathcal{I}$ such that $I \subseteq A$.

A CRS is judged by its balance ratio: we say that a contention resolution scheme is c-balanced if for all $e \in E$, $\mathbf{Pr}[e \in I \mid e \in A] \geq c$. Many natural classes of combinatorial constraints, including matroids, matchings, and knapsacks, admit $\Omega(1)$ -balanced contention resolution schemes when the events $\{e \in A\}_{e \in E}$ are jointly independent, and $\mathcal{P}(\mathcal{M})$ is the usual relaxation of the problem.

In the offline model of contention resolution, all inputs — in particular the set A of active elements — are given upfront. This is the most permissive model considered for contention resolution, and serves as the setting of our impossibility results. Our algorithmic results hold for the more restrictive online setting where elements are presented to the algorithm, which we refer to as an online CRS (OCRS), in some order determined by an adversary. When $e \in E$ arrives online, it is then revealed whether e is active (i.e., whether $e \in A$), at which point the algorithm must irrevocably decide whether to select e subject to feasibility. Several adversary models have been considered for online contention resolution, and our algorithmic results hold even for the most restrictive of those: the almighty adversary who determines the order of elements with full knowledge of all inputs including the realization of A, as well as the realization of any internal randomness used by the algorithm.

In this work, we focus on contention resolution for matroids when $\{e \in A\}_{e \in E}$ are only pairwise independent, and $\mathcal{P}(\mathcal{M})$ is simply the matroid polytope. In particular, $\mathcal{M} = (E, \mathcal{I})$ is a matroid and $\mathcal{D} \in \Delta_{pw}(2^E)(\mathbf{x})$ for some $\mathbf{x} \in \mathcal{P}(\mathcal{M})$. When a CRS is c-balanced for all such \mathcal{D} , we say it is a c-balanced pairwise-independent CRS.

Finally, we restate a Theorem from [25] that characterizes the set of distributions which permit balanced contention resolution schemes in the offline setting.

Theorem 2.1 (Theorem 3.6 from [25]). Fix a matroid $\mathcal{M} = (E, \mathcal{I})$, and let \mathcal{D} be a distribution supported on 2^E . The following are equivalent for every $c \in [0, 1]$,

- 1. There exists an offline contention resolution scheme which is c-balanced for D.
- 2. For every weight vector $\mathbf{w} \in \mathbb{R}^{E}_{>0}$, the following holds: $\mathbb{E}_{A \sim \mathcal{D}}[\mathbf{Rank_{\mathbf{w}}}(A)] \geq c \cdot \mathbb{E}_{A \sim \mathcal{D}}[\mathbf{w}(A)]$
- 3. For every $F \subseteq E$, the following holds: $\mathbb{E}_{A \sim \mathcal{D}}[\mathbf{Rank}(A \cap F)] \geq c \cdot \mathbb{E}_{A \sim \mathcal{D}}[|A \cap F|]$.

2.4 Prophet Inequalities

Fix a downwards-closed set system $\mathcal{M}=(E,\mathcal{I})$. In a prophet inequality problem, there are weights (or values) $\mathbf{w} \in \mathbb{R}_{\geq 0}^E$ on the elements that are drawn from a distribution \mathcal{D} , and elements arrive online in some order determined by an adversary. We take the perspective of a gambler who a-priori knows \mathcal{M} and the distribution \mathcal{D} of weights, but not the realized weights \mathbf{w} . When an element e arrives online, the gambler learns $\mathbf{w}(e)$ and must irrevocably decide whether or not to accept e, subject to accepting a feasible set of elements $S \in \mathcal{I}$. The gambler seeks to maximize their utility $\mathbf{w}(S) = \sum_{e \in S} \mathbf{w}(e)$. The goal is to compete — in expectation — with an omniscient prophet who obtains the maximum possible utility $\max\{\mathbf{w}(T): T \in \mathcal{I}\}$. When the gambler's expected utility is an α fraction of the prophet's expected utility, we say that we have an α -competitive prophet inequality for \mathcal{M} and \mathcal{D} .

Our negative results in this paper hold even against the weakest of adversaries considered in the literature on prophet inequality problems: the *oblivious adversary* who determines the order of elements in advance as a function of only \mathcal{M} and \mathcal{D} ; the gambler, therefore, knows the (arbitrary) order at the outset. In contrast, our positive results hold even for the strongest adversary considered in the literature: the *almighty adversary* who determines the order of elements with full knowledge of all inputs, including the realized weights \mathbf{w} as well as any internal randomness of the gambler's algorithm. The gambler therefore only learns the order as elements arrive online.

In this paper, we focus on prophet inequality problems where \mathcal{M} is a matroid and \mathcal{D} is a pairwise independent distribution over weight vectors, i.e. $\mathcal{D} \in \Delta_{pw}\left(\mathbb{R}_{\geq 0}^{|E|}\right)$.

2.5 A Useful Lemma for Pairwise Independent Events

The following lemma, from [19] establishes a lower bound for the probability that at least one event from a collection of pairwise independent events will occur.

Lemma 2.2 (Lemma 1 from [19]). Let \mathcal{D} and ind be pairwise independent and mutually independent distributions over a collection of random events $\{\mathcal{E}_i\}_{i=1}^k$ such that $\mathbf{Pr}_{\mathcal{E}\sim\mathcal{D}}[\mathcal{E}_i] = \mathbf{Pr}_{\mathcal{E}\sim\mathrm{ind}}[\mathcal{E}_i]$. Then,

$$\Pr_{\mathcal{E} \sim \mathcal{D}} \left[\bigvee_{i=1}^{k} \mathcal{E}_{i} \right] \geq \frac{\sum_{i=1}^{k} \mathbf{Pr}[\mathcal{E}_{i}]}{1 + \sum_{i=1}^{k} \mathbf{Pr}[\mathcal{E}_{i}]} \quad and \quad \Pr_{\mathcal{E} \sim \mathcal{D}} \left[\bigvee_{i=1}^{n} E_{i} \right] \geq \frac{1}{1.299} \cdot \Pr_{\mathcal{E} \sim \text{ind}} \left[\bigvee_{i=1}^{n} \mathcal{E}_{i} \right]$$

where $\mathcal{E} \vee \mathcal{F}$ denotes the event that at least one of \mathcal{E} or \mathcal{F} occurs.

3 Overview of Technical Results

In this section, we present an overview of our techniques and results. First we outline our construction of pairwise stochastically independent vector families. We then show how to employ this construction to prove our main impossibility results for pairwise-independent offline matroid contention resolution, and pairwise-independent matroid prophet inequalities against the oblivious adversary. We show that our impossibility results are tight by providing algorithms with matching bounds for both problems, even against the almighty adversary. Finally, we examine matroids satisfying the partition property, which includes most common matroids encountered in combinatorial optimization. We provide constant factor algorithms for pairwise-independent contention resolution and prophet inequalities on such matroids, even against the almighty adversary.

3.1 A Recipe for Pairwise-Independent Vector Families

As our main technical tool, we present a simple and flexible recipe for constructing pairwise independent families of vectors. We instantiate this recipe in different ways for matroid prophet inequalities and contention resolution schemes. Since our construction permits encoding of a rich variety of higher order relationships between the vectors, while maintaining lower-order independence, we hope it might be of independent interest.

There are two versions of our recipe. The first version produces an ordered family (i.e., a tuple) of pairwise independent vectors, and the second turns that into an unordered family (i.e., a set) of labeled vectors wherein membership is pairwise independent. We require the second, unordered, version for our impossibility results. The ordered construction is the most natural, and easily generalizes to k-wise independence for arbitrary k— we present the more general construction in this paper. The unordered construction is built on its ordered counterpart, and is tailored for pairwise independence (i.e., k = 2).

Ordered Families

We begin with our construction of an ordered family of k-wise independent vectors over the field \mathbb{F}_q , where q is a prime. Let $m, n, d \geq k$ be positive integers. Let $\Sigma \in \mathbb{F}_q^{m \times n}$ be a matrix whose columns $\sigma_1, \ldots, \sigma_n \in \mathbb{F}_q^m$ are k-wise linearly independent; i.e., no linear combination of k or fewer of these columns evaluates to the zero vector in \mathbb{F}_q^m . Intuitively, Σ is the input matrix we get to "design" for encoding a "hard instance" of the problem at hand, while respecting k-wise independence. Let $R \in \mathbb{F}_q^{d \times m}$ be drawn uniformly at random; i.e., each entry of the matrix R is a uniformly-random element of \mathbb{F}_q . Let $X = R\Sigma \in \mathbb{F}_q^{d \times n}$ be the output matrix, with columns $\mathbf{x}_1, \ldots, \mathbf{x}_n \in \mathbb{F}_q^d$ where $\mathbf{x}_i = R\sigma_i$.

The key observation here, which we prove in Section 4, is that the columns $\mathbf{x}_1, \dots, \mathbf{x}_n \in \mathbb{F}_q^d$ of X are k-wise stochastically independent, and moreover each is uniformly distributed in \mathbb{F}_q^d . Notably, the uniformly-random linear map R converts linear independence to stochastic independence. Also notably, linearity of R entails that any higher-order (greater than k) linear relationships between the columns of Σ — designed to inject "hardness" as previously described— are preserved as relationships between the corresponding columns of X. In both our applications, the dimension d of the output vectors $\mathbf{x}_1, \dots, \mathbf{x}_n$ is larger than the dimension m of the inputs $\sigma_1, \dots, \sigma_n$, implying that the linear operator R is injective — and the \mathbf{x}_i s are therefore distinct — with high probability.

Unordered Families

Both of our impossibility results require constructing a set of non-zero vectors A where the events $\{\mathbf{v} \in A\}$ are pairwise independent, and yet feature higher-order positive dependencies. This is easiest to see in the case of contention resolution, where we require the set of active elements to be concentrated in a lower-dimensional subspace, as needed to rule out a balanced CRS. This motivates our second, *unordered*, construction, which we describe next.

A natural first attempt would be to invoke our ordered construction to obtain pairwise-independent $[\mathbf{x}_1,\ldots,\mathbf{x}_n]=R\Sigma$, then take $A=\{\mathbf{x}_1,\ldots,\mathbf{x}_n\}\setminus\mathbf{0}$ to be the (unordered) set of non-zero columns. Some thought reveals that this can introduce mild pairwise correlation. This is largely because $\mathbf{u}\in A$ implies one fewer of the n "chances" is available for a different vector \mathbf{v} . Moreover, analyzing the exact magnitude of this correlation is complicated by the event — albeit a low probability one in our applications — that the random linear operator R is non-injective. We circumvent these issues by creating n copies $\mathbf{v}^1,\ldots,\mathbf{v}^n$ of each vector $\mathbf{v}\in\mathbb{F}_q^d$, and including \mathbf{v}^i in A when $\mathbf{x}_i=\mathbf{v}\neq 0$. Therefore, we work in the matroid $\mathbb{F}_q^d\times[n]$, with n parallel copies of each element in the matroid \mathbb{F}_q^d labeled with the positions $1,\ldots,n$. It is now clear that each non-zero \mathbf{u}^i is in A with probability $1/q^d$, and that the events $\mathbf{u}^i\in A$ and $\mathbf{v}^j\in A$ are pairwise-independent so long as $i\neq j$. This leaves the case of \mathbf{u}^i and \mathbf{v}^i for distinct \mathbf{u} and \mathbf{v} , whose membership in A is mutually exclusive and hence negatively correlated. This, however, can be easily corrected by mixing in — with small probability $\frac{1}{q^d}$ — a set which positively correlates vectors with the same label without introducing dependencies across different labels, nor changing the marginals. We describe the details in Section 4.4

3.2 Contention Resolution on Matroids

We use our construction of pairwise independent vector families to rule out a balance ratio better than $\frac{3}{\text{Rank}}$ for pairwise-independent contention resolution on linear matroids, even in the offline setting. For a desired rank d, we instantiate the recipe described in Section 3.1 with $m=2,\ n=d$, and an arbitrary prime $q\geq d$. The input matrix $\Sigma\in\mathbb{F}_q^{2\times d}$ is a fat (rank 2) matrix with d pairwise-linearly-independent columns $\sigma_1,\ldots,\sigma_d\in\mathbb{F}_q^2$ —we show that such a matrix exists whenever $q\geq d$. The random linear operator $R\in\mathbb{F}_q^{d\times 2}$ then maps Σ to $X\in\mathbb{F}_q^{d\times d}$. The d columns $\mathbf{x}_1,\ldots,\mathbf{x}_d\in\mathbb{F}_q^d$ of X are uniformly distributed in \mathbb{F}_q^d , stochastically pairwise independent, and most crucially—since Σ has rank 2—all lie in a subspace of rank at most 2.

We convert $X = [\mathbf{x}_1, \dots, \mathbf{x}_d]$ to a pairwise-independent set $A \subseteq \mathbb{F}_q^d \times [d]$ as described in Section 3.1. Each non-loop element of the matroid $\mathbb{F}_q^d \times [d]$ is in A with probability $\frac{1}{q^d}$, so its marginals lie in the matroid polytope⁵ and $\mathbb{E}[|A|] \approx d$. Moreover, since X has rank at most 2, and A consists of (labeled copies of) the columns of X with probability $1 - \frac{1}{q^d}$, we can bound $\mathbb{E}[\mathbf{Rank}(A)] \leq 2 + \frac{d}{q^d} < 3$. It follows from Theorem 2.1 that no contention resolution scheme has a balance ratio better than

 $^{^{3}}$ It is this step which recovers pairwise, but not necessarily k-wise, independence. A generalization to k-wise independence appears more technically involved, though likely possible.

⁴Our procedure might seem similar to that of Alon et al. [7], where they devise a procedure to convert an almost k-wise independent distribution to a k-wise independent distribution over $\{0,1\}^n$. However, given pairwise independent random variables (or events) X_1, \ldots, X_n , their procedure requires the following: for any $S \subseteq I$ with $|S| \le k$, $\Pr[\bigoplus_{i \in S} X_i = 1] = \frac{1+\epsilon}{2}$ for small $\epsilon > 0$ which is clearly not the case in our setting as $\Pr[\mathbf{v}^i \in A \land \mathbf{u}^i \in A] = 0$ for any distinct $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^d$. Here \oplus denotes the binary sum or XOR of the bits.

⁵To see this, note that a uniformly random base of $\mathbb{F}_q^d \times [d]$ has essentially the same — in fact, very slightly larger — marginals since all the vectors are equally likely to be part of the base and $\mathbf{0}$ is never sampled.

 $\frac{\mathbb{E}[\mathbf{Rank}(A)]}{\mathbb{E}[|A|]} \leq \frac{3}{d}$, as claimed. This holds even in the offline setting of contention resolution.

We show that our bound of $O(1/\mathbf{Rank})$ is essentially tight for general matroids. Given a pairwise-independent distribution with feasible marginals for a matroid of rank d, the contention resolution scheme which greedily selects active elements with probability $\frac{1}{2d}$ is $\frac{1}{4d}$ -balanced, even against the almighty adversary. This follows simply from pairwise independence, as well as the fact that the marginals sum to at most d.

We also note that our CRS impossibility result for linear matroids can easily be adapted to the important special case of binary matroids, while degrading the bound from $O\left(\frac{1}{\text{Rank}}\right)$ to $O\left(\frac{\log \text{Rank}}{\text{Rank}}\right)$. Specifically, we let $\Sigma \in \mathbb{F}_2^{O(\log d) \times d}$ be a fat (rank $O(\log d)$) binary matrix with d pairwise independent columns, which we show always exists. We then proceed in identical fashion with a uniformly random linear map $R \in \mathbb{F}_2^{d \times \log d}$, culminating in a stochastically pairwise-independent family of $\approx d$ vectors in \mathbb{F}_2^d with expected rank $O(\log d)$, as needed.

3.3 Prophet Inequalities on Matroids

Through a somewhat more involved application of our recipe, we rule out a competitive ratio better than $O(\frac{1}{\log d})$ for prophet inequalities on binary matroids of rank d, even against the oblivious adversary. We also show by way of an algorithm that this bound is tight for pairwise-independent prophet inequalities, even for general matroids and against the almighty adversary.

The Impossibility Result

We begin with the following randomized construction. For arbitrarily large d and some $\kappa = \Omega(\log d)$, we define a (random) nested sequence $V_1 \supset V_2 \ldots \supset V_{\kappa}$ of subspaces of \mathbb{F}_2^d , and corresponding independent sets $S_1, \ldots, S_{\kappa} \subseteq \mathbb{F}_2^d$, satisfying the following properties:

- (i) V_{ℓ} has dimension $\frac{d}{2\ell-1}$
- (ii) S_{ℓ} is a linearly independent subset of V_{ℓ} with size n_{ℓ} equal to a constant fraction of its dimension.⁶
- (iii) Let $\ell < \ell' \leq \kappa$. Conditioned on S_1, \ldots, S_ℓ and V_1, \ldots, V_ℓ , a vector $v \in S_\ell$ is in $V_{\ell'}$ with probability $\geq 1/2^{\ell'-\ell}$.
- (iv) The sets S_1, \ldots, S_{κ} are disjoint.

We show the existence of such random S_{ℓ} s and V_{ℓ} s through a highly technical construction, the details of which we defer to Section 6. For now, the reader might be satisfied of its plausibility by noting that it becomes trivial if we drop property ((iv)): Let S_1 be the standard basis vectors, then for each ℓ let $S_{\ell+1}$ be a random half of S_{ℓ} , and let V_{ℓ} be the span of S_{ℓ} . We cannot help but speculate whether our construction, which goes to some pains in order to achieve all four properties simultaneously, can be simplified or elegantly reduced to known linear-algebraic facts.

To motivate this construction, consider the following "hard" instance of the prophet inequality problem on the matroid \mathbb{F}_2^d where elements of each S_ℓ are assigned weight $w_\ell = 2^\ell$, and remaining elements are assigned weight 0. Suppose also that the non-zero weight elements arrive in increasing

⁶In fact, we can guarantee half the dimension, i.e. $n_{\ell} = d/2^{\ell}$.

order of weight, i.e. in the order S_1, \ldots, S_κ , followed by the zero-weight elements at the end. Forgive for a moment that the weights are not pairwise independent, and that guaranteeing this order is beyond the powers of the oblivious adversary — these are issues we will address later. The maximum weight independent set, which can be constructed by running the greedy algorithm on the non-zero weight elements in decreasing order of weights S_κ, \ldots, S_1 , selects a constant fraction of each S_ℓ — this follows easily from the matroid exchange axiom and Property (ii). Therefore, the prophet's reward is $\Omega(\sum_{\ell=1}^{\kappa} w_\ell \cdot n_\ell) = \Omega(d \log d)$. The gambler, in having to choose a subset T_ℓ of each S_ℓ before learning anything about flats $V_{\ell'}$ for $\ell' > \ell$, is not as fortunate. Properties ((i)) and ((iii)) imply that $\mathbb{E}[\sum_{\ell=1}^{\ell'} |T_\ell| \cdot \frac{1}{2\ell'-\ell}] \leq \frac{d}{2\ell'-1}$. Plugging in $w_\ell = 2^\ell$ and multiplying both sides by $2^{\ell'}$, we get $\mathbb{E}[\sum_{\ell=1}^{\ell'} w_\ell |T_\ell|] \leq 2d$. Since this holds for arbitrary ℓ' , we conclude that the gambler's expected total reward is only O(d).

It remains to address two issues with this prophet inequality instance: pairwise independence, and the limited powers of the oblivious adversary. For pairwise independence, we use our recipe described in Section 3.1. We let Σ_{ℓ} be the binary $d \times n_{\ell}$ matrix with S_{ℓ} as its columns, and let the matrix $\Sigma = [\Sigma_1, \ldots, \Sigma_{\kappa}] \in \mathbb{F}_2^{d \times n}$ with $n = \sum_{\ell=1}^{\kappa} n_{\ell}$ be the concatenation of the Σ_{ℓ} s. By property (iv), as well as the fact that we defined each S_{ℓ} as a set (rather than a multiset), the columns of Σ are distinct. Since we are in \mathbb{F}_2 , this is equivalent to the columns being pairwise linearly independent, as required for using Σ in our recipe. For the random linear embedding R, we choose a slightly larger output dimension to guarantee that the mapping is injective with high probability, and therefore preserves the geometry of S_1, \ldots, S_{κ} as captured by properties ((i)) through ((iv)). An output dimension of 2d suffices, so we let R be a uniformly random matrix in $\mathbb{F}_2^{2d \times d}$.

We proceed as described in Section 3.1. We define $X = R\Sigma \in \mathbb{F}_2^{2d \times n}$, or in more detail $X = [X_1, \dots, X_\kappa]$ where $X_\ell = R\Sigma_\ell \in \mathbb{F}_2^{2d \times n_\ell}$ has as its columns the image of S_ℓ under the linear map R. Recall from Section 3.1 that, for a fixed Σ , any pair of columns of X are distributed independently and uniformly in the destination space \mathbb{F}_2^{2d} . It follow that this continues to hold when using our randomly-constructed Σ , and the columns of our matrix X constitute a pairwise-independent ordered family of vectors distributed uniformly in \mathbb{F}_2^{2d} . We then convert X to an unordered family $A \subseteq \mathbb{F}_2^{2d} \times [n]$ wherein membership is stochastically pairwise independent as in Section 3.1. In more detail, with probability $1 - 1/2^d$ we let A_ℓ consist of the the n_ℓ columns of $X_\ell = R\Sigma_\ell$ labeled with the integers L_ℓ from $(\sum_{\ell' < \ell} n_{\ell'}) + 1$ to $\sum_{\ell' \le \ell} n_{\ell'}$, and let A be the (disjoint) union of the A_ℓ s. With remaining probability $1/2^d$ the set A is drawn from a positively-correlated distribution designed to ensure pairwise-independence overall as described in Section 3.1.

In summary, A is an (unordered) family of (labeled) vectors in $\mathbb{F}_2^{2d} \times [n]$ wherein membership is stochastically pairwise independent. Moreover, with high probability A is the disjoint union of A_1, \ldots, A_κ , where A_ℓ is simply S_ℓ transformed by an injective linear map R then distinctly labeled with integers from L_ℓ . By assigning weight $w_\ell = 2^\ell$ to elements with labels in L_ℓ , we obtain what is effectively our original "hard" instance of the matroid prophet inequality transformed by the injective linear operator R. Moreover, since a labeled vector $\mathbf{v}^i \in \mathbb{F}_2^{2d} \times [n]$ with $i \in L_\ell$ has weight $w_\ell = 2^\ell$ when $\mathbf{v}^i \in A$ and weight 0 otherwise, it follows that the weights are stochastically pairwise independent. Therefore, we have converted our original hard instance into one which is stochastically pairwise independent.

But what of the oblivious adversary's power to set the arrival order? Fortunately, now that the weight of $\mathbf{v}^i \in \mathbb{F}_2^{2d} \times [n]$ is either zero or uniquely determined as a non-decreasing function of its label $i \in [n]$, ordering elements in increasing order of label guarantees that vectors in \mathbb{F}_2^{2d} arrive

in non-decreasing order of weight. In particular, after arrival of elements with labels in L_1, \ldots, L_ℓ , the gambler knows the positions in \mathbb{F}_2^{2d} of the vectors with weights up to 2^ℓ — those corresponding with high probability to the original S_1, \ldots, S_ℓ — but nothing else of the positions of vectors with weights exceeding 2^ℓ — corresponding to $S_{\ell'}$ for $\ell' > \ell$. This is a fixed arrival order, and therefore obviously within the power of the oblivious adversary.

The Algorithm

We show that our bound of $O(1/\log \mathbf{Rank})$ is essentially tight for general matroids. Specifically, we obtain an $\Omega(1/\log \mathbf{Rank})$ matroid prophet inequality for pairwise independent distributions, even against the almighty adversary. We necessarily exploit pairwise independence, as no nontrivial guarantee is possible for general correlated distributions even for the rank one matroid.

Our algorithm is based on simple bucketing. Let $\mathcal{M}=(E,\mathcal{I})$ be a matroid with pairwise-independent random weights $w\in\mathbb{R}^{\mathbb{E}}_{\geq 0}$, and let $\mathrm{OPT}=\mathbb{E}[\mathbf{Rank}_w(\mathcal{M})]$ denote the expected reward of the prophet. Weights smaller than $\frac{OPT}{2\mathbf{Rank}}$ contribute at most half the prophet's reward, so can be discarded. Partition the weights between $\frac{OPT}{2\mathbf{Rank}}$ and $3\,\mathrm{OPT}$ into $O(\log\mathbf{Rank})$ "regular" buckets delimited by the integer powers of 2. Weights larger than 3OPT are assigned their own "special" bucket. The algorithm simply chooses the bucket with the largest contribution to the prophet's reward, and greedily selects as many elements as possible from that bucket subject to feasibility.

Clearly, the greedy algorithm applied to any of the regular buckets recovers at least half of that bucket's contribution to the prophet's expected reward. The special bucket B_{∞} requires a more careful analysis which exploits pairwise independence of the events $e \in B_{\infty}$. By Markov's inequality, B_{∞} is non-empty with probability at most 1/3. A Lemma from [19] for pairwise-independent events implies that $\sum_{e \in E} \Pr[e \in B_{\infty}] \leq \frac{\Pr[B_{\infty} \neq \emptyset]}{1-\Pr[B_{\infty} \neq \emptyset]} \leq \frac{1}{2}$. Invoking pairwise independence again, together with the union bound, an element e in B_{∞} is the only element in that bucket with probability at least 1/2, even after conditioning on its weight w_e . It follows that the greedy algorithm applied to B_{∞} recovers half of its contribution to the prophet's reward.

Putting it all together, since our algorithm greedily selects from the bucket contributing most to the prophet's reward, and there are $O(\log \mathbf{Rank})$ buckets, we obtain an $\Omega(1/\log \mathbf{Rank})$ prophet inequality for pairwise-independent distributions on matroids. Since we assumed nothing about the order in which elements are greedily selected, this holds even against the almighty adversary.

3.4 Exploiting the Partition Property

In contrast to our negative results for general matroids, we show that not all is lost for most common matroids in the optimization literature. Such matroids often satisfy the α -partition property for a constant α . Informally, this means that the matroid \mathcal{M} can be approximated by a randomly-chosen simple partition matroid \mathcal{M}' on the same elements, in the sense that the weighted rank of \mathcal{M}' approximates that of \mathcal{M} from below up to a factor of α for every vector of element weights.

For prophet inequalities, we apply the pairwise-independent single-choice prophet inequality of [19] to each part of \mathcal{M}' separately. This gives a $\frac{1}{3}$ prophet inequality for \mathcal{M}' , and therefore a $\frac{\alpha}{3}$ prophet inequality for \mathcal{M} , for pairwise independent distributions. Since the guarantees of [19] hold even against the almighty adversary, so do ours.

For contention resolution, the situation is slightly more involved. First, we show the existence of a balanced offline CRS for pairwise-independent distributions by utilizing Theorem 2.1 and

Lemma 2.2, then we show how to exploit a duality argument as well as the aforementioned prophet inequality to convert it to an online CRS against the almighty adversary.

Let A be a set of elements wherein membership is pairwise-independent with marginals μ feasible for \mathcal{M} . To show the existence of an offline balanced CRS, it suffices by Theorem 2.1 to show, for every set of elements F, that the expected rank of $A \cap F$ is a constant fraction of its expected size $\mu(F)$. We begin by analyzing the set \widetilde{A} where membership is jointly independent with the same marginals μ , and later relate A and \widetilde{A} through Lemma 2.2. It follows from [23] that \widetilde{A} admits a (1-1/e)-balanced CRS with respect to \mathcal{M} , and therefore $\mathbb{E}[\mathbf{Rank}_{\mathcal{M}}(\widetilde{A} \cap F)] \geq (1-1/e) \cdot \mu(F)$ for every set of elements F. Invoking the partition property, we get $\mathbb{E}[\mathbf{Rank}_{\mathcal{M}'}(\widetilde{A} \cap F)] \geq \alpha \cdot (1-1/e) \cdot \mu(F)$. We then observe that the rank function of the partition matroid \mathcal{M}' decomposes additively across its parts E_1, \ldots, E_k , with the i-th part contributing 1 to $\mathbf{Rank}_{\mathcal{M}'}(\widetilde{A} \cap F)$ precisely when at least one of the elements in $E_i \cap F$ is in \widetilde{A} . Lemma 2.2 implies that the probability of a disjunction of pairwise-independent events approximates, up to a factor of 1.299, the same quantity in the jointly independent case. In particular, $\mathbb{E}[\mathbf{Rank}_{\mathcal{M}'}(A \cap F)] \geq \frac{1}{1.299} \cdot \alpha \cdot (1-1/e) \cdot \mu(F)$. Since the rank function of \mathcal{M}' is smaller than that of \mathcal{M} , we can invoke Theorem 2.1 to conclude the existence of an $\frac{1-1/e}{1.299} \cdot \alpha$ -balanced CRS for A with respect to \mathcal{M} .

For good measure, we also show how to turn our offline CRS into an online one, even against the almighty adversary, at a cost of an additional $O(\alpha)$ factor in the balance ratio. We use a duality-based construction essentially identical to that in [25, Theorem 4.1]. At a high level, the problem of maximizing the weighted rank of active elements functions as a dual to contention resolution. An online β -approximation to this dual problem can be converted to an online CRS whose balance ratio is within β of the best possible offline. Our prophet inequality is such an approximation with $\beta = \frac{\alpha}{3}$, even against the almighty adversary. Therefore, we obtain a pairwise-independent online CRS with balance ratio $\frac{1-1/e}{3.897} \cdot \alpha^2$ against the almighty adversary.

We note that our offline CRS for matroids satisfying the partition property, together with the impossibility results for linear and binary matroids in Section 3.2, imply limits on the partition property for these matroids. In particular, for an α -partition property we show that $\alpha = O\left(\frac{1}{d}\right)$ for the full linear matroid, and $\alpha = O\left(\frac{\log d}{d}\right)$ for the full binary matroid, where d denotes the rank. The latter results improves on the bound of $O\left(\frac{1}{d^{1/4}}\right)$ from [1].

4 A Recipe for Pairwise-independent Vector Families

In this section, we devise our main tool to produce a family of pairwise independent (labeled) vectors. Initially, we detail our approach to constructing an ordered family of pairwise independent vectors. Subsequently, we outline the process for transforming an ordered family to an unordered family.

4.1 Ordered Pairwise Independent Vector Families

The construction of an ordered family of pairwise independent vectors naturally extends to the k-wise independence. Therefore, in this section, we present the construction in the most general form. We fix positive integers $m, n, d \geq k$. Let $\Sigma \in \mathbb{F}_q^{m \times n}$ be a matrix with k-wise linearly independent columns $\sigma_1, \sigma_2, \ldots \sigma_n$ and $R \in \mathbb{F}_q^{d \times m}$ be a matrix where each entry is a uniformly random element of \mathbb{F}_q drawn independently. Consider the matrix $X = R\Sigma \in \mathbb{F}_q^{d \times n}$ whose columns are obtained by

linearly transforming each column of Σ via R. In the following lemma, we show that the columns $\mathbf{x}_1, \ldots, \mathbf{x}_n \in \mathbb{F}_q^d$ of X form an ordered family of k-wise stochastically independent vectors., i.e., for each $S \subseteq [n]$ of size at most k the vectors $\{\mathbf{x}_i\}_{i \in S}$ are mutually (stochastically) independent.

Lemma 4.1. Let $\Sigma \in \mathbb{F}_q^{m \times n}$ be a matrix with k-wise linearly independent columns $\sigma_1, \ldots, \sigma_n \in \mathbb{F}_q^m$, $R \in \mathbb{F}_q^{d \times m}$ be a uniformly random matrix with entries $r_{i,j} \sim \text{Unif}(0,1,\ldots,q-1)$, and $X = R\Sigma$ with column vectors $\mathbf{x}_1, \ldots, \mathbf{x}_n$. For any subset $S \subseteq [n]$ of size at most k, the vectors $\{\mathbf{x}_i\}_{i \in S}$ are mutually stochastically independent. Moreover, for any $i \in [n]$ and $\mathbf{v} \in \mathbb{F}_q^d$, $\mathbf{Pr}[\mathbf{x}_i = \mathbf{v}] = \frac{1}{a^d}$.

Proof. First we show that each column $\mathbf{x}_i \in \mathbb{F}_q^d$ of X is uniformly distributed over \mathbb{F}_q^d . For arbitrary $\mathbf{v} \in \mathbb{F}_q^d$, we can express,

$$\begin{aligned} \mathbf{Pr}[\mathbf{x}_i &= \mathbf{v}] = \mathbf{Pr}[R\sigma_i &= \mathbf{v}] \\ &= \mathbf{Pr}\left[\bigwedge_{\ell=1}^d \left\{\sum_{j=1}^m r_{\ell,j} \cdot \sigma_i(j) = \mathbf{v}(\ell)\right\}\right] \\ &= \prod_{\ell=1}^d \mathbf{Pr}\left[\sum_{j=1}^m r_{\ell,j} \cdot \sigma_i(j) = \mathbf{v}(\ell)\right] \end{aligned} \qquad \text{(disjoint set of independent RVs)}.$$

For any fixed $\ell \in [d]$, the set of possible solutions $(r_{\ell,1}, \ldots, r_{\ell,m})$ to the equation $\sum_{j=1}^m r_{\ell,j} \cdot \sigma_i(j) = \mathbf{v}_i(\ell)$, considering σ_i and \mathbf{v} as fixed, forms an affine subspace of rank m-1 which has size of q^{m-1} . As each $r_{i,j}$ is a uniformly random element from \mathbb{F}_q , the probability,

$$\mathbf{Pr}[\mathbf{x}_i = \mathbf{v}] = \prod_{\ell=1}^d \mathbf{Pr} \left[\sum_{j=1}^m r_{\ell,j} \cdot \sigma_i(j) = \mathbf{v}(\ell) \right] = \left(\frac{q^{m-1}}{q^m} \right)^d = \frac{1}{q^d}.$$
 (1)

Next, we prove k-wise stochastic independence of the columns of X. Let $S \subseteq [n]$ be such that $|S| \leq k$. By assumption, the corresponding columns $\{\sigma_i\}_{i \in S}$ of Σ are linearly independent. It follows that

$$\begin{split} \mathbf{Pr}\left[\bigwedge_{i \in S} \{\mathbf{x}_i = \mathbf{v}_i\}\right] &= \mathbf{Pr}\left[\bigwedge_{i \in S} \{R\sigma_i = \mathbf{v}_i\}\right] \\ &= \mathbf{Pr}\left[\bigwedge_{i \in S} \bigwedge_{\ell=1}^d \left\{\sum_{j=1}^m r_{\ell,j} \cdot \sigma_i(j) = \mathbf{v}_i(\ell)\right\}\right] \\ &= \mathbf{Pr}\left[\bigwedge_{\ell=1}^d \bigwedge_{i \in S} \left\{\sum_{j=1}^m r_{\ell,j} \cdot \sigma_i(j) = \mathbf{v}_i(\ell)\right\}\right] \\ &= \prod_{\ell=1}^d \mathbf{Pr}\left[\bigwedge_{i \in S} \left\{\sum_{j=1}^m r_{\ell,j} \cdot \sigma_i(j) = \mathbf{v}_i(\ell)\right\}\right]. \quad \text{(disjoint set of independent RVs)} \end{split}$$

Consider the following system of equations with variables $(r_{\ell,1}, \dots r_{\ell,m})$ for a fixed $\ell \in [d]$:

$$\sum_{j=1}^{m} r_{\ell,j} \cdot \sigma_i(j) = \mathbf{v}_i(\ell) \qquad \forall i \in S.$$
 (2)

Since $\{\sigma_i \mid i \in S\}$ are linearly independent, the set of solutions $(r_{\ell,1}, \dots r_{\ell,m})$ to the system of equations (2) forms an affine subspace of dimension m - |S| containing $q^{m-|S|}$ many vectors. As each $r_{i,j}$ is a uniformly random element from \mathbb{F}_q , the probability,

$$\begin{aligned} \mathbf{Pr} \left[\bigwedge_{i \in S} \{ \mathbf{x}_i = \mathbf{v}_i \} \right] &= \prod_{\ell=1}^d \mathbf{Pr} \left[\bigwedge_{i \in S} \left\{ \sum_{j=1}^m r_{\ell,j} \cdot \sigma_i(j) = \mathbf{v}_i(\ell) \right\} \right] \\ &= \left(\frac{q^{m-|S|}}{q^m} \right)^d \\ &= q^{-d \cdot |S|} \\ &= \prod_{i \in S} \mathbf{Pr}[\mathbf{x}_i = \mathbf{v}_i]. \end{aligned}$$

Above, the second equality follows from the fact that $r_{i,j}$ is a uniformly random element from \mathbb{F}_q and the last equality follows from Equation (1). This proves that the random vectors $\{\mathbf{x}_i\}_{i\in S}$ are mutually independent, as needed.

Next, we present a well-known fact about random matrices defined over finite fields. For the self containment of the paper, we provide its simple proof in Appendix A.

Lemma 4.2. Let $R \in \mathbb{F}_q^{d \times m}$ be a uniformly random matrix with entries $r_{i,j} \sim \text{Unif } (0,1,\ldots,q-1)$. Then, for any m < d, we have $\Pr[\mathbf{Rank}(R) = m] \geq 1 - \frac{1}{q^{d-m}}$. In addition, for any $\Sigma \in \mathbb{F}_q^{m \times n}$ with distinct columns, the columns of $X = R\Sigma$ are distinct with probability $\geq 1 - \frac{1}{q^{d-m}}$.

The last lemma essentially states that when d >> m, the random matrix $R \in \mathbb{F}_q^{d \times m}$ becomes full rank. Therefore, the random linear map under R becomes a random linear "embedding" (or an injective mapping) with high probability. In such a scenario, when a matrix $\Sigma \in \mathbb{F}_q^{m \times n}$ consists of distinct columns, the product $X = R\Sigma$ will have distinct columns with high probability.

4.2 Unordered Pairwise Independent Vector Families

In the context of stochastic selection, we typically focus on probability distributions over sets of elements. This requires us to construct an (unordered) set of vectors A such that for any two distinct vectors \mathbf{u} and \mathbf{v} , the events $\{\mathbf{u} \in A\}$ and $\{\mathbf{v} \in A\}$ are independent.

In the previous section, we introduced a technique for producing a sequence $\mathbf{x}_1, \dots, \mathbf{x}_n \in \mathbb{F}_q^d$ of vectors that exhibit pairwise (indeed k-wise) stochastic independence. To turn this into a set of vectors A, it is tempting to define $A = \{\mathbf{x}_1, \dots, \mathbf{x}_n\}$. However, some thought reveals that membership in this set A can exhibit some slight negative correlation. Even in the (high probability) event that the vectors $\mathbf{x}_1, \dots, \mathbf{x}_n$ are distinct, for distinct $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^d$ we have $\mathbf{Pr}[\mathbf{u} \in A] = \mathbf{Pr}[\mathbf{v} \in A] = \frac{n(n-1)}{q^{2d}} < \mathbf{Pr}[\mathbf{u} \in A] \mathbf{Pr}[\mathbf{v} \in A]$. It might be tempting

Procedure 1. Random Set Generation from Random Matrix (MatrixToSet)

Input: $X \in \mathbb{F}_q^{d \times n}$ with pairwise independent columns $\mathbf{x}_1, \dots \mathbf{x}_n$ and an ordered label set $L = \{\ell_1, \dots, \ell_n\}$,

Output: $A \subseteq \mathbb{F}_q^d \times L$.

Dist - I: \mathcal{D}_1

(1) Construct an unordered set $A := \{\mathbf{x}_i^{\ell_i} : i \in [n]\} \subseteq \mathbb{F}_q^d \times L$.

Dist II: \mathcal{D}_2

(1) Start with $A = \emptyset$. Then, for each label $\ell_i \in [n]$, independently with probability $\frac{1}{q^d}$, include all elements $\{\mathbf{v}^{\ell_i} : \mathbf{v} \in \mathbb{F}_q^d\}$ in A.

Sample $A \subseteq \mathbb{F}_q^d \times L$ from \mathcal{D}_1 w.p $1 - \frac{1}{q^d}$ and \mathcal{D}_2 w.p. $\frac{1}{q^d}$.

to "correct" for this negative correlation in A by slightly mixing with a different set A' featuring positive correlation that is calibrated to "cancel out" the negative correlation in A. However, this is further complicated by the (low probability) event where the random linear map used in our construction is singular, and the vectors $\mathbf{x}_1, \ldots, \mathbf{x}_n$ are therefore not necessarily distinct. This makes it challenging to quantify the exact "amount" of correlation in A in general, and therefore challenging to argue for the existence of a suitable A'. To circumvent these difficulties, we take a somewhat different approach which creates n labeled duplicates for each vector. We describe this approach next.

Recall the construction of ordered families from the previous section: The matrix $\Sigma \in \mathbb{F}_q^{m \times n}$ is comprised of pairwise linearly independent column vectors $\sigma_1, \ldots, \sigma_n$, the matrix $R \in \mathbb{F}_q^{d \times m}$ has its entries $r_{i,j}$ drawn i.i.d. uniformly from \mathbb{F}_q , and the matrix $X = [\mathbf{x}_1, \ldots, \mathbf{x}_n] = R \cdot \Sigma$ is the image of Σ under the linear transformation defined by matrix R. We create n labeled copies $\mathbf{v}^{\ell_1}, \ldots, \mathbf{v}^{\ell_n}$ of each vector $\mathbf{v} \in \mathbb{F}_q^d$, and include $\mathbf{v}^{\ell_i} \in A$ whenever the i-th column of X equals \mathbf{v} , i.e. $\mathbf{x}_i = \mathbf{v}$. This allows the inclusion of each vector \mathbf{v} in the set A multiple times, each occurrence distinguished by a unique label from a set of labels L. A is therefore a subset of $\mathbb{F}_q^d \times L$. Without loss of generality, one can think of L = [n].

Let us proceed to understand correlation structure within this set A. First, we observe that for distinct indices $i, j \in [n]$ and any two (possibly equal) vectors $\mathbf{v}, \mathbf{u} \in \mathbb{F}_q^d$, the events $\{\mathbf{v}^{\ell_i} \in A\}$ and $\{\mathbf{u}^{\ell_j} \in A\}$ are independent as events $\{\mathbf{x}_i = \mathbf{v}\}$ and $\{\mathbf{x}_j = \mathbf{u}\}$ are assured to be independent by Lemma 4.1. Nonetheless, this method introduces correlation between the events $\{\mathbf{v}^{\ell_i} \in A\}$ and $\{\mathbf{u}^{\ell_i} \in A\}$ since $\mathbf{Pr}[\mathbf{u}^{\ell_i} \in A \land \mathbf{v}^{\ell_i} \in A] = 0$ for any two distinct vectors $\mathbf{v}, \mathbf{u} \in \mathbb{F}_q^d$ and index $i \in [n]$ (or label $\ell_i \in L$). To overcome this, we mix A with another distribution that positively correlates the inclusion of labeled vectors with the same label without introducing dependencies across different labels, nor changing the marginals. We describe our procedure of converting ordered families of vectors to unordered families of vectors in Procedure 1.

In the subsequent lemma, we demonstrate that the unordered family of vectors sampled according to Procedure 1 is pairwise independent provided the ordered family of vectors $\mathbf{x}_1, \dots, \mathbf{x}_n$ are pairwise independent and uniformly sampled from \mathbb{F}_q^d . To maintain a smooth and uninterrupted

discussion, we have postponed the detailed technical proof to Appendix A.

Lemma 4.3. Let $X \in \mathbb{F}_q^{d \times n}$ be a random matrix with pairwise independent column vectors $\mathbf{x}_1, \dots \mathbf{x}_n$ for some $n < q^d$ where each vector \mathbf{x}_i is distributed uniformly in \mathbb{F}_q^d . Then a random set $A \subseteq \mathbb{F}_q^d \times L$ generated by Procedure 1 given the inputs of X and $L = \{\ell_1, \dots \ell_n\}$ satisfies:

- (1) For any $\mathbf{v}^{\ell_i} \in \mathbb{F}_q^d \times L$, $\mathbf{Pr}[\mathbf{v}^{\ell_i} \in A] = \frac{1}{q^d}$.
- (2) For any two distinct \mathbf{v}^{ℓ_i} , $\mathbf{u}^{\ell_j} \in \mathbb{F}_q^d \times L$, the events $\{\mathbf{v}^{\ell_i} \in A\}$ and $\{\mathbf{u}^{\ell_j} \in A\}$ are independent.

5 Pairwise-independent Contention Resolution on Matroids

In this section, we utilize the tool devised in the previous section to show the limits of pairwise-independent contention resolution schemes for matroids. In particular, we show that the class of linear matroids does not admit an $\omega(1/\mathbf{Rank})$ -balanced pairwise independent offline CRS. We complement this with a pairwise independent online CRS against the almighty adversary whose balance ratio matches our impossibility result for offline schemes up to a constant factor.

5.1 Limits of Pairwise Independent Contention Resolution

We consider the matroid $\mathcal{M}^{\times d} = (\mathbb{F}_q^d \times [d], \mathcal{I}^{\times d})$ which consists of d labeled copies of each element in the full linear matroid \mathbb{F}_q^d . The following theorem states the limits of pairwise independent offline contention resolution for this matroid.

Theorem 5.1. For any d > 2 and any prime q, the matroid $\mathbb{F}_q^d \times [d]$ does not admit a $\frac{c+1}{d}$ -balanced pairwise independent offline CRS where c is any positive integer satisfying $q^{c-1} \geq d$. In particular,

- 1. $\mathbb{F}_q^d \times [d]$ does not admit a $\frac{3}{d}$ -balanced pairwise independent offline CRS for $q \geq d$.
- 2. $\mathbb{F}_2^d \times [d]$ does not admit a $\frac{3+\log_2 d}{d}$ -balanced pairwise independent offline CRS.

Our construction of a hard offline contention resolution instance utilizes the tool devised in Section 4 to sample pairwise independent unordered family of vectors. This unordered family will serve as the set of active elements for contention resolution. We first form a "fat" matrix $\Sigma \in \mathbb{F}_q^{c \times d}$ (c << d) with pairwise linearly independent columns. The existence of such a matrix can be assured by choosing q and c so that $d \leq q^{c-1}$ as we show in Claim 5.2. Then, linear transformation of Σ via a uniformly random matrix $R \in \mathbb{F}_q^{d \times c}$ yields a matrix $X = R\Sigma$ whose columns $\mathbf{x}_1, \dots \mathbf{x}_d$ are pairwise stochastically independent due to Lemma 4.1. Finally, we use Procedure 1 to turn the sequence $(\mathbf{x}_1, \dots \mathbf{x}_d)$ into the set $A \subseteq \mathbb{F}_q^d \times [d]$ of active elements. Lemma 4.3 ensures that for any two distinct elements $\mathbf{v}^i, \mathbf{u}^i \in \mathbb{F}_q^d \times [d]$, the events $\{\mathbf{v}^i \in A\}$ and $\{\mathbf{u}^j \in A\}$ are pairwise independent. We summarize this construction in Procedure 2.

The following claim together with Lemma 4.3 implies that the output of Procedure 2 follows a pairwise independent distribution over $\mathbb{F}_q^d \times [d]$.

Claim 5.2. Given that $d \leq q^{c-1}$, there exists a matrix $\Sigma^{CRS} \in \mathbb{F}_q^{c \times d}$ which consists of d pairwise linearly independent columns.

Procedure 2. Pairwise Independent Set of Active Elements in $\mathcal{M}^{\times d} = (\mathbb{F}_q^d \times [d], \mathcal{I}^{\times d})$

Input: Positive integers d, c and a prime q satisfying $q^{c-1} \ge d$. Output: $A \subseteq \mathbb{F}_q^d \times [d]$.

- (1) Let $\Sigma^{CRS} \in \mathbb{F}_q^{c \times d}$ be an arbitrary matrix with pairwise linearly independent column vectors.
- (2) Let $R \in \mathbb{F}_q^{d \times c}$ be a matrix where each entry r_{ij} is uniformly and independently sampled from $\{0, \dots q-1\}$.
- (3) Set $A \leftarrow \text{MatrixToSet}(R \cdot \Sigma^{\text{CRS}}, [d])$.

Proof. Notice that there are q^c-1 non-zero vectors in \mathbb{F}_q^c , and linear dependence partitions them into equivalence classes of size q-1. Therefore, by selecting one vector from each equivalence class one can generate $\frac{q^c-1}{q-1} > q^{c-1}$ pairwise linearly independent columns. When $d \leq q^{c-1}$, the matrix Σ^{CRS} always exists.

Before we show that A, the output of Procedure 2, does not admit a $\frac{c+1}{d}$ -balanced contention resolution scheme, we first verify that the marginals of A reside within the matroid polytope $\mathcal{P}(\mathcal{M}^{\times d})$.

Lemma 5.3. Let $\mu \in \mathbb{R}_+^{\mathbb{F}_q^d \times [d]}$ be the marginal probability vector of A where $\mu(\mathbf{v}^i) = \mathbf{Pr}[\mathbf{v}^i \in A]$ when A is sampled according to Procedure 2. Then, $\mu \in \mathcal{P}(\mathcal{M}^{\times d})$.

Proof. By Lemma 4.3 we know that $\mu(\mathbf{v}^i) = \frac{1}{q^d}$ for each $\mathbf{v}^i \in \mathbb{F}_q^d$. Thus, for any subset $S \subseteq \mathbb{F}_q^d \times [d]$, observe that

$$\mu(S) := \sum_{\mathbf{v}^i \in S} \mu(\mathbf{v}^i) = |S| \cdot \frac{1}{q^d} \leq \frac{d \cdot q^{\mathbf{Rank}(S)}}{q^d} = \frac{d \cdot q^{\mathbf{Rank}(S)}}{\mathbf{Rank}(S) \cdot q^d} \cdot \mathbf{Rank}(S) \leq \mathbf{Rank}(S).$$

Above, the first inequality holds because $|S| \leq d \cdot q^{\mathbf{Rank}(S)}$ as we have d copies of each $\mathbf{v} \in \mathbb{F}_q^d$ in $\mathbb{F}_q^d \times [d]$. The last inequality follow from the fact that xq^{-x} is a decreasing function of x and $\mathbf{Rank}(S) \leq d$, hence, $\frac{d \cdot q^{\mathbf{Rank}(S)}}{\mathbf{Rank} \cdot q^d} \leq 1$. Thus, $\mu \in \mathcal{P}(\mathcal{M}^{\times d})$.

Now we are ready to prove Theorem 5.1.

Proof of Theorem 5.1. Let q be any prime, c and d be two integers satisfying $q^{c-1} \ge d$, and A be the random set sampled according to Procedure 2. By Lemma 4.3 and Claim 5.2 we know that A follows a pairwise independent distribution and Lemma 5.3 demonstrates that the set A has marginals inside the matroid polytope $\mathcal{P}(\mathcal{M}^{\times d})$.

The final step of Procedure 2 invokes Procedure 1. Recall that Procedure 1 mixes distributions \mathcal{D}_1 and \mathcal{D}_2 . Then,

$$\begin{split} \mathbb{E}[\mathbf{Rank}(A)] &\leq \mathbb{E}[\mathbf{Rank}(A) \mid A \sim \mathcal{D}_1] \cdot \mathbf{Pr}[A \sim \mathcal{D}_1] + \mathbf{Rank}(\mathcal{M}^{\times d}) \cdot \mathbf{Pr}[A \sim \mathcal{D}_2] \\ &\leq \mathbb{E}[\mathbf{Rank}(A) \mid A \sim \mathcal{D}_1] + \frac{d}{q^d} & & & & & & & & & \\ &\leq c + 1 & & & & & & & & & \\ \end{split}$$

Moreover, due to Lemma 4.3 we know that $\mathbf{Pr}[\mathbf{v}^i \in A] = \frac{1}{q^d}$ for any $\mathbf{v}^i \in \mathbb{F}_q^d \times [d]$. Thus,

$$\mathbb{E}[|A|] = \sum_{\mathbf{v}^i \in \mathbb{F}_q^d \times [d]} \mathbf{Pr}[\mathbf{v}^i \in A] = \frac{1}{q^d} \cdot \left| \mathbb{F}_q^d \times [d] \right| = d.$$

Combining these two facts we obtain:

$$\frac{\mathbb{E}[\mathbf{Rank}(A)]}{\mathbb{E}[|A|]} \le \frac{c+1}{d}.$$

Finally, the characterization of distributions permitting contention resolution from Theorem 2.1 concludes the proof.

5.2 Optimal Pairwise Independent OCRS

Consider a matroid $\mathcal{M}=(E,\mathcal{I})$ and a randomly chosen set of active elements $A\subseteq 2^E$, which is sampled from a pairwise independent distribution $\mathcal{D}\in\Delta_{\mathrm{pw}}(2^E)(\mu)$ with marginals $\mu\in\mathcal{P}(\mathcal{M})$. In online contention resolution, the elements $e\in E$ arrive in some order chosen by an adversary, at which point the CRS algorithm learns whether e is in A and must irrevocably decide whether or not to select e for inclusion in its solution. The algorithm is required to adhere to the feasibility constraints of the matroid during these inclusions. We assume that the arrival order is chosen by the almighty adversary who is aware of the algorithm and all random outcomes, including those internal to the algorithm.

In the previous section we showed that for a class of linear matroids no offline CRS can attain a balance ratio greater than $\frac{3}{\operatorname{rank}(\mathcal{M})}$ for pairwise independent distributions. The following theorem shows the existence a $\frac{4}{\operatorname{rank}(\mathcal{M})}$ -balanced online CRS against the almighty adversary for all matroids.

Theorem 5.4. For any matroid $\mathcal{M} = (E, \mathcal{I})$, an arbitrary vector $\mu \in \mathcal{P}_{\mathcal{I}}$ and distribution $\mathcal{D} \in \Delta_{pw}(2^E)(\mu)$, there exists $\frac{1}{4Rank(\mathcal{M})}$ -balanced pairwise independent online contention resolution scheme against the almighty adversary.

Proof. We use the simple greedy algorithm that selects each active element with a probability of $\frac{1}{2 \cdot \text{rank}(\mathcal{M})}$ unless it violates feasibility. This algorithm internally flips an independent random coin for each element $e \in E$, where each coin lands on "heads" with probability $\frac{1}{2 \cdot \text{rank}(\mathcal{M})}$. We denote the joint occurrence of an element being active and its corresponding coin flip resulting in heads by \mathcal{E}_e , and the complement of this event is denoted by $\overline{\mathcal{E}_e}$.

We note two crucial observations: First, events $\{\mathcal{E}_e\}_{e\in E}$ are pairwise independent since events $\{e\in A\}_{e\in E}$ are pairwise independent. Second, given that the marginal probability vector $\mu(e) := \mathbf{Pr}[e\in A]$ is within the matroid polytope $\mathcal{P}(\mathcal{M})$, the total sum of probabilities $\sum_{e\in E} \mathbf{Pr}[e\in A]$ is at most rank (\mathcal{M}) . Consequently, the sum $\sum_{e\in E} \mathbf{Pr}[\mathcal{E}_e]$ is at most $\frac{1}{2}$. We now bound the balance ratio of the greedy algorithm as follows.

$$\begin{aligned} \mathbf{Pr}[e \text{ is selected}] &\geq \mathbf{Pr}\left[\mathcal{E}_{e} \land \bigwedge_{f \in E \setminus \{e\}} \overline{\mathcal{E}_{f}}\right] & (\mathcal{E}_{e} \text{ solely occurs}) \end{aligned}$$

$$&= \left(1 - \mathbf{Pr}\left[\bigvee_{f \in E \setminus \{e\}} \mathcal{E}_{f} \middle| \mathcal{E}_{e}\right]\right) \cdot \mathbf{Pr}[\mathcal{E}_{e}]$$

$$&\geq \left(1 - \sum_{f \in E \setminus \{e\}} \mathbf{Pr}[\mathcal{E}_{f} \middle| \mathcal{E}_{e}]\right) \cdot \mathbf{Pr}[\mathcal{E}_{e}] & (\text{Union bound})$$

$$&= \left(1 - \sum_{f \in E \setminus \{e\}} \mathbf{Pr}[\mathcal{E}_{f}]\right) \cdot \mathbf{Pr}[\mathcal{E}_{e}] & (\text{Pairwise Independence})$$

$$&\geq \frac{1}{2} \cdot \frac{1}{2\mathbf{Rank}} \cdot \mathbf{Pr}[e \in A] & \left(\sum_{f \in E} \mathbf{Pr}[\mathcal{E}_{f}] \leq \frac{1}{2}\right)$$

$$&= \frac{1}{4\mathbf{Rank}} \cdot \mathbf{Pr}[e \in A]. & \Box$$

6 Pairwise-independent Prophet Inequalities on Matroids

In this section, we explore a specific instance of the pairwise independent prophet inequality problem which demonstrates the impossibility of achieving any $\omega\left(\frac{1}{\log \operatorname{Rank}}\right)$ -competitive algorithm against the oblivious adversary. Our focus is on a complete binary matroid of rank 2d, comprising n labeled copies of each element, represented as $\mathcal{M}^{\times n}=(E^{\times n},\mathcal{I}^{\times n})$. Here, d is an integer power of 2, $n=\Theta(d)$, and $E^{\times n}$ is defined as $\mathbb{F}_2^{2d}\times[n]$. The precise value of n will be determined in subsequent discussions. The hard instance is structured around two main elements: (i) a pairwise independent probability distribution for the weights assigned to $E^{\times n}$ and (ii) a fixed order λ of elements $E^{\times n}$. This setup will ensure that any algorithm adhering to λ for processing elements inevitably fails to select an independent set that offers substantial reward, particularly due to the lack of prior knowledge regarding the weight assignments.

6.1 Construction of Weight Distribution and Arrival Order

We start by outlining the process for constructing a pairwise independent weight distribution for the elements in the matroid $\mathbb{F}_2^{2d} \times [n]$, where $n = \Theta(d)$. Reflecting on the core principles summarized in Section 3.3, our approach for determining weight distribution involves generating $\kappa = \Theta(\log d)$ distinct levels. The elements of $\mathbb{F}_2^{2d} \times [n]$ will be partitioned into these levels based on their respective labels. For elements assigned to the ℓ -th level, we will assign weights, either being 2^{ℓ} or zero, in accordance with a carefully formulated distribution.

For each level $\ell \in [\kappa]$, we fix the size of labels L_{ℓ} of level ℓ as $d/2^{\ell}$. Subsequently, we define n as the cumulative sum of the sizes of these label sets, expressed as $n := \sum_{\ell=1}^{\kappa} |L_{\ell}|$. In particular, we define label set L_{ℓ} as $\left\{\sum_{j=1}^{\ell-1} \frac{d}{2^{j}} + 1, \ldots, \sum_{j=1}^{\ell} \frac{d}{2^{j}}\right\}$. Note that the collection $\{L_{\ell}\}_{\ell \in [\kappa]}$ effectively forms a partition of the set [n]. Consequently, the set of vectors $\mathbb{F}_2^{2d} \times L_{\ell} \subseteq \mathbb{F}_2^{2d} \times [n]$ is categorized as

belonging to the level ℓ . Having established this framework, we now proceed to outline the pairwise independent weight distribution along with a deterministic worst-case arrival order of elements which renders this distribution challenging for a gambler.

First, we describe the weight assignment procedure for elements in the matroid, with an approach akin to the active element distribution for the pairwise independent CRS problem, described in Procedure 2. More formally, for each level $\ell \in [\kappa]$, we begin by constructing a random matrix $\Sigma_{\ell} \in \mathbb{F}_2^{d \times |L_{\ell}|}$ whose columns are pairwise linearly independent with probability one. Subsequent to this, we apply a linear transformation with a matrix R whose entries are sampled independently from $r_{(i,j)} \sim \text{Ber}(1/2)$. This step produces a new random matrix $X_{\ell} := R\Sigma_{\ell}$ for each level $\ell \in [\kappa]$.

Next, X_{ℓ} is converted into a subset A_{ℓ} of $\mathbb{F}_2^{2d} \times L_{\ell}$ by independently applying Procedure 1 across all levels. Each vector \mathbf{v}^i in A_{ℓ} is assigned a weight of 2^{ℓ} . Notice that this process is well defined as $\{L_{\ell}\}_{\ell \in [\kappa]}$ forms a partition of [n]. As we will show in Lemma 6.1, weights sampled according to this process are pairwise independent, provided the matrix $\Sigma := \left[\Sigma_1 \ \Sigma_2 \ \ldots \Sigma_{\kappa}\right]$ comprises pairwise linearly independent columns.

Regarding the deterministic order in the prophet inequality problem, we define an arbitrary fixed sequence λ_{ℓ} for the elements within each level. The worst-case order λ for the matroid $\mathbb{F}_2^{2d} \times [n]$ is then composed by concatenating these individual level sequences in ascending order of levels. This is expressed as $\lambda := \lambda_1, \lambda_2, \dots, \lambda_{\kappa}$. Crucially, this sequence is structured without foreknowledge of the weight realizations, ensuring that any algorithm addressing the prophet inequality will confront elements with nonzero weights in ascending order of their assigned weights.

6.1.1 Properties of Σ matrices

We encode the challenging instance of the prophet inequality problem via a careful selection of the matrices $\Sigma_1, \ldots, \Sigma_\kappa$, each adhering to certain essential properties. At high level, we designate a random subspace for each level ℓ , derived from the span of a randomly chosen subset of principal basis vectors B_ℓ . The matrices Σ_ℓ are then selected in a way that their columns are linearly independent subset within $\mathbf{Span}(B_\ell)$. For convenience, we think of Σ_ℓ interchangeably as a matrix as well as the set of it's columns, and write $e \in \Sigma_\ell$ for $e \in \mathbb{F}_2^d$ if e is a column of Σ_ℓ . The following four properties define critical features of $\{\Sigma_\ell\}_{\ell \in [\kappa]}$ and $\{B_\ell\}_{\ell \in [\kappa]}$ which ensure that our resulting \mathbf{w} and λ constitute a hard instance for the pairwise-independent prophet inequality problem as explained in Section 3.3.

- (i) $B_{\kappa} \subseteq \cdots \subseteq B_2 \subseteq B_1 \subseteq \mathbb{F}_2^d$ is a nested system with size $|B_{\ell}| = \frac{d}{2^{\ell-1}}$.
- (ii) $\Sigma_{\ell} \in \mathbb{F}_2^{d \times d/2^{\ell}}$ is a full column rank matrix with columns from $\mathbf{Span}(B_{\ell})$.

(iii)
$$\mathbf{Pr}[e \in \mathbf{Span}(B_{\ell'}) \mid \{e \in \Sigma_{\ell}\}, \Sigma_1, \dots, \Sigma_{\ell}, B_1, \dots, B_{\ell}] = \frac{1}{2^{\ell'-\ell}} \text{ for all } e \in \mathbb{F}_2^d \text{ and } \ell' \geq \ell.$$

(iv)
$$\Sigma := \left[\Sigma_1 \ \Sigma_2 \ \dots \Sigma_{\kappa} \right]$$
 consists of distinct columns with probability 1.

Let us revisit the roles of these properties, briefly touched upon in Section 3.3. We first set aside for a moment the requirement for the distribution to be pairwise independent. Consider a "hard" instance of a prophet inequality problem on \mathbb{F}_2^d where each column vector in some Σ_ℓ is assigned a weight of 2^ℓ and the rest of the vectors are assigned weight zero. Assume that the vectors

with non-zero weight appear in ascending order of weight, starting with vectors in $\Sigma_1, \Sigma_2, \ldots, \Sigma_{\kappa}$, followed by vectors with weight zero.

A greedy offline algorithm, aiming to select the maximum weight independent set, would process the non-zero-weight vectors in reverse order from Σ_{κ} to Σ_{1} . By utilizing the matroid exchange principle and Property (ii), the algorithm can secure a constant fraction of each set Σ_{ℓ} . This strategy enables the prophet to achieve a total reward of $\Omega(d \cdot \log d)$.

Conversely, a gambler must select a subset T_{ℓ} from the columns of Σ_{ℓ} without prior knowledge of the sets $\Sigma_{\ell'}$ or their corresponding weights, for all $\ell' > \ell$. Roughly speaking, based on Properties (i) and (iii), we can potentially show that if $|T_{\ell}| = c \cdot |\Sigma_{\ell}|$ for some constant c then T_{ℓ} ends up spanning c-fraction of vectors from all the sets $\Sigma_{\ell'}$ for all $\ell' > \ell$. Hence, the gambler can only select c fraction of vectors from $\frac{1}{c}$ many levels. This leads an O(d) upper bound on the total reward of the gambler and rules out $\omega(1/\log d)$ -competitive algorithm for the gambler.

Returning to the aspect of pairwise independence, Property (iv) facilitates the conversion of this "hard" instance into one where weights are pairwise independent, while maintaining the problem's inherent difficulty. This step utilizes the tools developed in Section 4.

6.1.2 Formal description of hard instance

At this stage, we provisionally accept the existence of a random sampling for the sets $\{B_\ell\}_{\ell\in[\kappa]}$ and matrices $\{\Sigma_\ell\}_{\ell\in[\kappa]}$, which adhere to the four specified properties in unison. We postpone the discussion of how this distribution is explicitly constructed to Section 6.3. Now, we are prepared to describe the detailed process for determining the weight assignments and the sequence λ in Procedure 3.

Next, we show that the weight assignment constructed by Procedure 3 is pairwise independent whose proof simply follows from Property (iv) and Lemmas 4.3 and 4.1.

Lemma 6.1. Given any $\kappa \geq 4$ and $d = 2^{2 \cdot \kappa}$, let $n = \sum_{\ell=1}^{\kappa} \frac{d}{2^{\ell}}$ and \mathbf{w} be the random weight assignment of elements of $\mathbb{F}_2^{2d} \times [n]$ sampled according to the Procedure 3. Then, for any distinct pairs of labeled vectors \mathbf{v}^i , $\mathbf{u}^j \in \mathbb{F}_2^{2d} \times [n]$, and $\ell, \ell' \in [\kappa]$ we have

$$\mathbf{Pr}[\mathbf{w}(\mathbf{v}^i) = 2^{\ell} \wedge \mathbf{w}(\mathbf{u}^j) = 2^{\ell'}] = \mathbf{Pr}[\mathbf{w}(\mathbf{v}^i) = 2^{\ell}] \cdot \mathbf{Pr}[\mathbf{w}(\mathbf{u}^j) = 2^{\ell'}].$$

Proof. We consider three cases:

- Case 1 $(i \notin L_{\ell} \text{ or } j \notin L_{\ell'})$: We observe that $\mathbf{Pr}[\mathbf{w}(\mathbf{v}^i) = 2^{\ell} \wedge \mathbf{w}(\mathbf{u}^j) = 2^{\ell'}] = \mathbf{Pr}[\mathbf{w}(\mathbf{v}^i) = 2^{\ell}] \cdot \mathbf{Pr}[\mathbf{w}(\mathbf{u}^j) = 2^{\ell'}] = 0$.
- Case 2 ($\ell = \ell'$ and $i, j \in L_{\ell}$): Property (iv) and Lemma 4.3 ensures that the events $\{\mathbf{v}^i \in A_{\ell}\}$ and $\{\mathbf{v}^i \in A_{\ell}\}$ are independent.

Procedure 3. Pairwise Independent Weight Assignments to Matroid $\mathbb{F}_2^{2d} \times [n]$

Input: Dimension of column vector d, Number of levels κ .

Output: Weight assignment **w** and λ .

- Construction of random matrices with pairwise independent columns.
 - (1) Let $\Sigma_1, \Sigma_2, \dots \Sigma_{\kappa}$ be random matrices satisfying (i), (ii), (iii) (iv).
 - (2) Let matrix $R \in \mathbb{F}_2^{2d \times d}$ to be a random matrix with entries $r_{ij} \sim \text{Ber}(1/2)$ independently.
 - (3) Define $X_{\ell} = R\Sigma_{\ell} \in \mathbb{F}_2^{2d \times d/2^{\ell}}$ for each $\ell \in [\kappa]$.
 - (4) Define $n := \sum_{\ell=1}^{\kappa} \frac{d}{2^{\ell}}$.
- Conversion from matrices to pairwise independent sets and weight assignment.
 - (5) Define labels of level ℓ as $L_{\ell} := \left\{ \sum_{j=1}^{\ell-1} \frac{d}{2^j} + 1, \dots, \sum_{j=1}^{\ell} \frac{d}{2^j} \right\} \subseteq [n].$
 - (6) For each $\ell \in [\kappa]$, call Procedure 1 with X_{ℓ} and L_{ℓ} to obtain $A_{\ell} \leftarrow \text{MatrixToSet}(X_{\ell}, L_{\ell})$.
 - (7) For each $\mathbf{v}^i \in \mathbb{F}_2^{2d} \times L_\ell$, assign weight $\mathbf{w}(\mathbf{v}^i) = \begin{cases} 2^\ell & \text{if } \mathbf{v}^i \in A_\ell, \\ 0 & \text{otherwise.} \end{cases}$
- Definition of a worst-case deterministic order.
 - (10) Let λ_{ℓ} be an arbitrary ordering of elements $\{\mathbf{v}^i : \mathbf{v} \in \mathbb{F}_2^{2d} \text{ and } i \in L_{\ell}\} = \mathbb{F}_2^{2d} \times L_{\ell}$.
 - (11) Concatenate λ_{ℓ} in increasing order of ℓ to form the ordering $\lambda = \lambda_1, \dots \lambda_{\kappa}$ of $\mathbb{F}_2^{2d} \times [n]$
- Case 3 ($\ell \neq \ell'$ and $i \in L_{\ell}$ and $j \in L_{\ell'}$): We have marginal probabilities $\Pr[\mathbf{v}^i = 2^{\ell}] = \Pr[\mathbf{u}^j = 2^{\ell'}] = \frac{1}{2^d}$. Recall that A_{ℓ} sampled according to mixture of two distributions \mathcal{D}_1 and \mathcal{D}_2 in MatrixToSet for each level ℓ . We compute the joint probability as

$$\begin{aligned} \mathbf{Pr}[\mathbf{v}^{i} = & 2^{\ell} \wedge \mathbf{u}^{j} = 2^{\ell'}] \\ = & \mathbf{Pr}[\{\mathbf{x}_{i} = \mathbf{v}\} \wedge \{\mathbf{x}_{j} = \mathbf{u}\} \mid A_{\ell} \sim \mathcal{D}_{1} \wedge A_{\ell'} \sim \mathcal{D}_{1}] \cdot \mathbf{Pr}[A_{\ell} \sim \mathcal{D}_{1} \wedge A_{\ell'} \sim \mathcal{D}_{1}] \\ & + \mathbf{Pr}[\{\mathbf{x}_{i} = \mathbf{v}\} \wedge \{\mathbf{u}^{j} \in A_{\ell'}\} \mid A_{\ell} \sim \mathcal{D}_{1} \wedge A_{\ell'} \sim \mathcal{D}_{2}] \cdot \mathbf{Pr}[A_{\ell} \sim \mathcal{D}_{1} \wedge A_{\ell'} \sim \mathcal{D}_{2}] \\ & + \mathbf{Pr}[\{\mathbf{v}^{i} \in A_{\ell}\} \wedge \{\mathbf{x}_{j} = \mathbf{u}\} \mid A_{\ell} \sim \mathcal{D}_{2} \wedge A_{\ell'} \sim \mathcal{D}_{1}] \cdot \mathbf{Pr}[A_{\ell} \sim \mathcal{D}_{2} \wedge A_{\ell'} \sim \mathcal{D}_{1}] \\ & + \mathbf{Pr}[\{\mathbf{v}^{i} \in A_{\ell}\} \wedge \{\mathbf{u}^{j} \in A_{\ell'}\} \mid A_{\ell} \sim \mathcal{D}_{2} \wedge A_{\ell'} \sim \mathcal{D}_{2}] \cdot \mathbf{Pr}[A_{\ell} \sim \mathcal{D}_{2} \wedge A_{\ell'} \sim \mathcal{D}_{2}] \\ & = \frac{1}{2^{2d}} \left(1 - \frac{1}{2^{d}}\right)^{2} + \frac{1}{2^{3d}} \left(1 - \frac{1}{2^{d}}\right) + \frac{1}{2^{3d}} \left(1 - \frac{1}{2^{d}}\right) + \frac{1}{2^{4d}} = \frac{1}{2^{2d}}. \end{aligned}$$

6.2 Upper Bounding the Approximation Ratio

In this section, we prove the following theorem.

Theorem 6.2. For any integers $\kappa \geq 4$ and $d = 2^{2 \cdot \kappa}$, let $n = \sum_{\ell=1}^{\kappa} \frac{d}{2^{\ell}}$ and $\mathcal{M}^{\times n} = (E^{\times n}, \mathcal{I}^n)$ where $\mathcal{M} = (E, \mathcal{I})$ is the full binary matroid with rank 2d, i.e., $E = \mathbb{F}_2^{2d}$. Then, there is no $\omega(1/\log d)$ -competitive pairwise independent prophet inequality algorithm for matroid $\mathcal{M}^{\times n}$.

In order to prove the above theorem, we show that when the weights \mathbf{w} and the order λ are determined according to Procedure 3, the prophet is able to secure a reward of $\Omega(d \cdot \log d)$, where as any gambler is limited to obtaining a reward at most O(d). To prove this claim, we first identify a high probability event which makes the problem challenging for the gambler. Let $\mathcal{E}_{\text{hard}}$ be the event when the following two events happen together:

- (1) The random matrix R sampled in Step (2) of Procedure 3 has full column rank,
- (2) The set A_{ℓ} constructed in the Step (6) of Procedure 3, is sampled according to \mathcal{D}_1 in Procedure 1 for all $\ell \in [\kappa]$ simultaneously.

Notice that the two described events are mutually independent. The first event occurs with a probability of $1 - \frac{1}{2^d}$, as $R \in \mathbb{F}_q^{2d \times d}$. The second event occurs with a probability of $\left(1 - \frac{1}{2^{2d}}\right)^{\kappa} \ge 1 - \frac{\kappa}{2^{2d}}$. Together, these events imply that $\mathcal{E}_{\text{hard}}$ occurs with a probability of at least $1 - \frac{\kappa + 1}{2^d}$.

Furthermore, when the latter event happens only labeled copies of columns in X_{ℓ} will have a non-zero weight for each $\ell \in [\kappa]$. Additionally, if the first event occurs, at most one labeled copy of each vector will have a non-zero weight. Conceptually, when $\mathcal{E}_{\text{hard}}$ occurs, one can imagine that \mathbf{w} assigns non-zero weights to columns of X_{ℓ} and so vectors of \mathbb{F}_2^{2d} , rather than their labeled copies, since there is only one labeled copy of each item with a non-zero weight.

Next, we demonstrate two lemmas that lower-bound the prophet's reward and upper-bound the any gambler's utility respectively, under the condition that \mathcal{E}_{hard} happens.

Lemma 6.3 (Lower-bound Prophet's Reward). Given $\kappa \geq 4$, $d = 2^{2 \cdot \kappa}$, $n = \sum_{\ell=1}^{\kappa} \frac{d}{2^{\ell}}$ and $\mathcal{M} = \mathbb{F}_2^{2d}$, let \mathbf{w} be the random weight assignment over elements of $\mathcal{M}^{\times n}$ determined according to Procedure 3. Then,

$$\mathbb{E}[reward\ of\ prophet\ |\ \mathcal{E}_{hard}] \geq \frac{\kappa \cdot d}{10}.$$

Lemma 6.4 (Upper-bound Gambler's Reward). Given $\kappa \geq 4$, $d = 2^{2 \cdot \kappa}$, $n = \sum_{\ell=1}^{\kappa} \frac{d}{2^{\ell}}$ and $\mathcal{M} = \mathbb{F}_2^{2d}$, let **w** be the random weight assignment over elements of $\mathcal{M}^{\times n}$ and λ be the order of these elements determined according to Procedure 3. Then,

$$\mathbb{E}[reward\ of\ gambler\ |\ \mathcal{E}_{hard}] \leq 2d.$$

Finally, we utilize these lemmas to prove the main result of this section.

Proof of Theorem 6.2. Due to Lemma 6.3, we have

$$\mathbb{E}[\text{reward of prophet}] \ge \mathbb{E}[\text{reward of prophet} \mid \mathcal{E}_{\text{hard}}] \cdot \mathbf{Pr}[\mathcal{E}_{\text{hard}}]$$
(3)

$$\geq \frac{\kappa \cdot d}{4} \cdot \left(1 - \frac{\kappa + 1}{2^d}\right) \geq \frac{\kappa \cdot d}{5} \tag{4}$$

and due to Lemma 6.4, we have

$$\mathbb{E}[\text{reward of gambler}] \leq \mathbb{E}[\text{reward of gambler} \mid \mathcal{E}_{\text{hard}}] + 2^{\kappa} \cdot \mathbf{Rank}(\mathcal{M}^{\times n}) \cdot (1 - \mathbf{Pr}\left[\mathcal{E}_{\text{hard}}\right])$$

$$\leq 2d + (d \cdot 2^{\kappa}) \cdot \frac{\kappa + 1}{2^{d}} \leq 2d + 1. \qquad (\kappa \geq 4)$$

Therefore, combining two inequalities concludes the desired result.

$$\frac{\mathbb{E}[\text{reward of gambler}]}{\mathbb{E}[\text{reward of prophet}]} \leq \frac{10}{\kappa} = O\left(\frac{1}{\log d}\right).$$

In the remaining part of this section, we condition on the event \mathcal{E}_{hard} and prove the two lemmas.

6.2.1 Proof of Lemma 6.3: Lower-bound for Prophet's Reward

To compute a lower-bound for prophet's reward, or equivalently $\mathbb{E}[\mathbf{Rank_w}(\mathcal{M}^{\times n})]$, we will construct a feasible solution S and show that its expected weight is at least $\frac{\kappa \cdot d}{2}$. Let $A_1, \ldots A_{\kappa}$ be the random sets constructed in Step (6) of Procedure 3. Given that we have conditioned on $\mathcal{E}_{\text{hard}}$, each set A_{ℓ} contains $n_{\ell} = \frac{d}{2^{\ell}}$ vectors, and at most one labeled copy of a vector $\mathbf{v} \in \mathbb{F}_2^{2d}$ appears in any of the sets $\{A_{\ell}\}_{\ell \in [\kappa]}$.

Then, for each level ℓ in decreasing order, let \widetilde{A}_{ℓ} be a maximal subset of A_{ℓ} such that $\bigcup_{i=\ell}^{\kappa} \widetilde{A}_{\ell}$ is an independent set. We form the solution $S := \bigcup_{\ell=1}^{\kappa} \widetilde{A}_{\ell}$. Essentially, S is the outcome of a greedy algorithm that processes elements in descending order of their weights. By construction, S constitutes a feasible set. The matroid exchange property then implies that

$$|\widetilde{A}_{\ell}| = \mathbf{Rank}\left(igcup_{i=\ell}^{\kappa} A_i
ight) - \mathbf{Rank}\left(igcup_{i=\ell+1}^{\kappa} A_i
ight).$$

Consequently, for any $1 \le i \in \lceil \kappa/2 \rceil$,

$$\begin{split} |\widetilde{A}_{2i-1}| + |\widetilde{A}_{2i}| &= \mathbf{Rank} \left(\bigcup_{j=2i-1}^{\kappa} A_j \right) - \mathbf{Rank} \left(\bigcup_{j=2i+1}^{\kappa} A_j \right) \\ &\geq \mathbf{Rank}(A_{2i-1}) - \mathbf{Rank}(B_{2i+1}) \qquad \qquad \left(\bigcup_{j=2i+1}^{\kappa} A_j \subseteq \mathbf{Span}(B_{2i+1}) \right) \\ &= \frac{d}{2^{2i-1}} - \frac{d}{2^{2i}} = \frac{1}{2} \cdot \frac{d}{2^{2i-1}}. \end{split}$$

Therefore, we can bound the weighted rank of the matroid as follows:

$$\mathbf{Rank_{w}}(\mathcal{M}^{\times n}) \geq \mathbf{w}(S) = \sum_{\ell=1}^{\kappa} \mathbf{w}(\widetilde{A}_{\ell}) \geq \sum_{i=1}^{\lceil \kappa/2 \rceil} (|\widetilde{A}_{2i-1}| + |\widetilde{A}_{2i}|) \cdot 2^{2i-1}$$
$$\geq \sum_{i=1}^{\lceil \kappa/2 \rceil} \frac{1}{2} \cdot \frac{d}{2^{2i-1}} \cdot 2^{2i-1} = \sum_{i=1}^{\lceil \kappa/2 \rceil} \frac{d}{2} = \frac{\kappa \cdot d}{4}$$

where the second inequality follows from the fact that $\mathbf{w}(\mathbf{v}^i) \geq 2^{2i-1}$ for any $\mathbf{v}^i \in \widetilde{A}_{2i-1} \cup \widetilde{A}_{2i}$. This concludes the proof of Lemma 6.3.

6.2.2 Proof of Lemma 6.4: Upper-bound for Gambler's Reward

Let S be the set of elements selected by the gambler and define S_{ℓ} as its subset which contains elements from level ℓ , i.e., $S_{\ell} = S \cap \mathbb{F}_q^{2d} \times L_{\ell}$, and let $S_{\leq \ell} = \bigcup_{i=1}^{\ell} S_i$. We assume without loss of generality that the gambler only selects elements with non-zero weight. Recall that λ first presents all elements with first level labels L_1 , then all elements with second level labels L_2 , and so on. Thus, any algorithm visits non-zero-weight elements of the matroid in increasing order of weight. Therefore, S_{ℓ} is a random set which is independent of $B_{\ell+1}, B_{\ell+2}, \ldots, B_{\kappa}$ given the information revealed by the elements up to level ℓ . This independence remains even when conditioned on R.

We define $\rho_{\ell} := |S_{\ell}|$ and $\gamma_{\ell} := |S_{\leq \ell} \cap \mathbf{Span}(RB_{\ell} \times [n])|$ for each $\ell \in [\kappa]$. To simplify the notation and reduce clutter, we will use a shorthand for $\mathbf{Span}(\cdot)$, where $\mathbf{Span}(V)$ will represent $\mathbf{Span}(V \times [n])$, effectively omitting labels for the ease of understanding. The following claim establishes a relationship between the two series $\{\rho_{\ell}\}_{\ell \in [\kappa]}$ and $\{\gamma_{\ell}\}_{\ell \in [\kappa]}$ in expectation.

Claim 6.5.
$$\mathbb{E}[\rho_{\ell}] \leq \mathbb{E}[\gamma_{\ell}] - \frac{\mathbb{E}[\gamma_{\ell-1}]}{2}$$
.

Before we prove the claim, we utilize it to complete the proof of Lemma 6.4. Remember that all expectations are conditioned on the event \mathcal{E}_{hard} .

$$\begin{split} \mathbb{E}[\mathbf{w}(S)] &= \sum_{\ell=1}^{\kappa} \mathbb{E}[2^{\ell} \cdot |S_{\ell}|] \\ &= \sum_{\ell=1}^{\kappa} \mathbb{E}[2^{\ell} \cdot \rho_{\ell}] \\ &\leq 2 \cdot \mathbb{E}[\gamma_{1}] + \sum_{\ell=2}^{\kappa} 2^{\ell} \cdot \left(\mathbb{E}[\gamma_{\ell}] - \mathbb{E}\left[\frac{\gamma_{\ell-1}}{2}\right]\right) \qquad \text{(Claim 6.5)} \\ &= 2^{\kappa} \cdot \mathbb{E}[\gamma_{\kappa}] + \sum_{\ell=1}^{\kappa-1} \left(2^{\ell} \cdot \mathbb{E}[\gamma_{\ell}] - 2^{\ell+1} \cdot \mathbb{E}\left[\frac{\gamma_{\ell}}{2}\right]\right) \\ &\leq 2^{\kappa} \cdot \mathbf{Rank}(RB_{\kappa}) \qquad (S_{\leq \kappa} \cap \mathbf{Span}(RB_{\kappa})) \subseteq \mathbf{Span}(RB_{\kappa})) \\ &= 2^{\kappa} \cdot \frac{d}{2^{\kappa-1}} = 2d. \end{split}$$

We complete the discussion with the following proof of Claim 6.5.

Proof of Claim 6.5. First, we bound ρ_{ℓ} as follows.

$$\rho_{\ell} \leq |S_{\leq \ell} \cap \operatorname{\mathbf{Span}}(RB_{\ell})| - |S_{\leq \ell-1} \cap \operatorname{\mathbf{Span}}(RB_{\ell})| = \gamma_{\ell} - |S_{\leq \ell-1} \cap \operatorname{\mathbf{Span}}(RB_{\ell})|.$$

Here, the inequality follows from the fact that $S_{\ell} \subseteq \mathbf{Span}(RB_{\ell})$ and $S_{<\ell}$ is an independent set.

We re-express the expectation of $|S_{<\ell-1} \cap \mathbf{Span}(RB_{\ell})|$ to complete the proof.

$$\mathbb{E}[|S_{\leq \ell-1} \cap \mathbf{Span}(RB_{\ell})|] = \sum_{\ell'=1}^{\ell-1} \mathbb{E}[|S_{\ell'} \cap \mathbf{Span}(RB_{\ell})|] \qquad (\text{disjoint})$$

$$= \sum_{\ell'=1}^{\ell-1} \mathbb{E}\left[\sum_{e \in S_{\ell'}} \mathbf{Pr}[e \in \mathbf{Span}(RB_{\ell})]\right]$$

$$= \sum_{\ell'=1}^{\ell-1} \mathbb{E}\left[\sum_{e \in S_{\ell'}} \frac{1}{2^{\ell-\ell'}}\right] \qquad (\text{Property (iii)})$$

$$= \sum_{\ell'=1}^{\ell-1} \mathbb{E}\left[\frac{1}{2} \cdot \sum_{e \in S_{\ell'}} \frac{1}{2^{(\ell-1)-\ell'}}\right]$$

$$= \sum_{\ell'=1}^{\ell-1} \mathbb{E}\left[\frac{1}{2} \cdot \sum_{e \in S_{\ell'}} \mathbf{Pr}[e \in \mathbf{Span}(RB_{\ell-1})]\right] \qquad (\text{Property (iii)})$$

$$= \frac{1}{2} \cdot \sum_{\ell'=1}^{\ell-1} \mathbb{E}[|S_{\ell-1} \cap \mathbf{Span}(RB_{\ell-1})|]$$

$$= \frac{1}{2} \cdot \mathbb{E}[\gamma_{\ell-1}]. \qquad (\text{disjoint})$$

Each of our two invocations Property (iii) uses the conditional independence of $S_{\ell'}$ of B_{ℓ} given the information revealed by elements at levels up to ℓ' .

6.3 Construction of Σ

This section is dedicated to presenting a method for constructing a random matrix Σ , along with a nested system of subspaces. Each subspace is defined as the span of a subset of principal basis vectors B_{ℓ} for every level $\ell \in [\kappa]$. The goal is to demonstrate that this construction adheres to Properties (i), (ii), (iii), and (iv) simultaneously. We will prove the following lemma.

Lemma 6.6. The matrices $\Sigma_1, \ldots, \Sigma_{\kappa}$ and sets B_1, \ldots, B_{κ} constructed by Procedure 4 satisfy Properties (i), (ii), (iii), and (iv).

To aid understanding, we now give a brief explanation of our construction. The procedure starts at the first level by defining the "alive" basis vectors as $B_1 = \{\mathbf{e}_1, \dots, \mathbf{e}_d\}$, which are the principal basis vectors in \mathbb{F}_2^d . It then organizes these vectors into consecutive pairs to create the set \mathbf{P}_1 , a partition of B_1 . We use $P_1(j) = \{e_{2j-1}, e_{2j}\}$ to denote the jth pair in \mathbf{P}_1 , for $j \in [d/2]$. We let $\Sigma_1(j) \in \mathbb{F}_2^{d \times 1}$ be a matrix consisting of a single non-zero column, chosen as a linear combination of the two vectors in $P_1(j)$. These matrices are then concatenated to form the $d \times \frac{d}{2}$ matrix $\Sigma_1 = \left[\Sigma_1(1), \dots, \Sigma_1\left(\frac{d}{2}\right)\right]$ with full column rank.

In the second level, the procedure randomly selects half of the elements from $\mathbf{P_1}$ to form $\widetilde{\mathbf{P_1}}$. For simplicity in our discussion, we will renumber the selected parts in $\widetilde{\mathbf{P_1}}$ as $\left\{\widetilde{P}_1(i):i\in[d/4]\right\}$. Following this, we combine consecutive parts in $\widetilde{\mathbf{P_1}}$ to create the second level partition, formally

Procedure 4. Construction of Pairwise Linearly Independent Collection of Vectors Σ

Input: Dimension of column vector d, Number of levels κ .

- (1) Base level $\ell = 1$:
 - (a) $B_1 = \{\mathbf{e}_1, \dots, \mathbf{e}_d\}$ be the principal basis of \mathbb{F}_2^d .
 - (b) $\mathbf{P}_1 = \{P_1(i) : i \in [d/2]\}$ be a partition of B_1 where $P_1(i) = \{\mathbf{e}_{2i-1}, \mathbf{e}_{2i}\}$.
- (2) **Level** $\ell > 1$:
 - (a) Let $\widetilde{\mathbf{P}}_{\ell-1}$ be a uniformly random half of $\mathbf{P}_{\ell-1}$, written $\widetilde{\mathbf{P}}_{\ell-1} := \{\widetilde{P}_{\ell-1}(i) : i \in [d/2^{2\ell-2}]\}$.
 - (b) Define $P_\ell(i) = \widetilde{P}_{\ell-1}(2i-1) \cup \widetilde{P}_{\ell-1}(2i)$ for $i \in \left[\frac{d}{2^{2\ell-1}}\right]$ and let $\mathbf{P}_\ell = \{P_\ell(i) : i \in [d/2^{2\ell-1}]\}$
 - (c) Define $B_{\ell} = \bigcup_{i=1}^{d/2^{2\ell-1}} P_{\ell}(i)$, which we refer to as the alive basis vectors of level ℓ .
- (3) For each $\ell \in [\kappa]$ and $j \in [d/2^{2\ell-1}]$, define $\Sigma_{\ell}(j) \in \mathbb{F}_2^{d \times 2^{\ell-1}}$ as follows. Let $\mathbf{v}_1', \dots \mathbf{v}_{2^{\ell}}'$ be an arbitrary enumeration of $P_{\ell}(j)$, and let the t-th column of $\Sigma_{\ell}(j)$ be $\sigma_t := \sum_{i=t}^{t+2^{\ell-1}-1} \mathbf{v}_i'$.
- (4) Let $\Sigma_{\ell} = \left[\Sigma_{\ell}(1) \ \Sigma_{\ell}(2) \ \dots \ \Sigma_{\ell}(d/2^{2\ell-1}) \right] \in \mathbb{F}_2^{d \times d/2^{\ell}}$.

Output: $[\Sigma_1, \Sigma_2, \dots, \Sigma_{\kappa}].$

denoted as $\mathbf{P_2} = \{P_2(j) : j \in [d/8]\}$, where $P_2(j) = \widetilde{P}_1(2j-1) \cup \widetilde{P}_1(2j)$. The basis vectors appearing in a part of $\mathbf{P_2}$ are designated the "alive" basis vectors at level two, and denoted by B_2 . Note that the B_2 consists of half the vectors in B_1 . In a manner akin to the first level, vectors in each part $P_2(j)$ in $\mathbf{P_2}$ are linearly combined to create a matrix $\Sigma_2(j) \in \mathbb{F}_2^{d \times 2}$, with two linearly-independent columns lying within $\mathbf{Span}(P_2(j))$. Moreover, the procedure ensures that columns of each $\Sigma_2(j)$ are distinct from the columns of Σ_1 . These matrices are then concatenated to form Σ_2 .

For each subsequent level ℓ , the process follows a similar pattern. Given $B_{\ell-1}, \mathbf{P}_{\ell-1}$ and $\Sigma_{\ell-1}$,

- 1. We let $\widetilde{\mathbf{P}}_{\ell-1}$ be the random half of $\mathbf{P}_{\ell-1}$ and then obtain \mathbf{P}_{ℓ} whose parts are formed by merging two consecutive parts from $\widetilde{\mathbf{P}}_{\ell-1}$ after an arbitrary enumeration. We let B_{ℓ} consist of the vectors appearing in \mathbf{P}_{ℓ} . Here, note that $|\mathbf{P}_{\ell}| = \frac{1}{4}|\mathbf{P}_{\ell-1}| = \frac{d}{2^{2\ell-1}}$. Moreover, $|P_{\ell}(j)| = 2^{\ell}$ for any $j \in [d/2^{2\ell-1}]$, and $|B_{\ell}| = \frac{d}{2^{\ell}-1}$. We refer the reader to Figure 1 for a visualization of the construction of B_{ℓ} , \mathbf{P}_{ℓ} , and $\widetilde{\mathbf{P}}_{\ell}$ for the initial three levels.
- 2. For each part $P_{\ell}(j)$ in \mathbf{P}_{ℓ} , a matrix $\Sigma_{\ell}(j) \in \mathbb{F}_2^{d \times |P_{\ell}(j)|/2}$ with full column rank is constructed. Its columns lie within $\mathbf{Span}(P_{\ell}(j))$, and are distinct from the columns of $\Sigma_1, \ldots, \Sigma_{\ell-1}$.
- 3. The matrices $\Sigma_{\ell}(j)$ are concatenated to form Σ_{ℓ} .

Since each $\Sigma_{\ell}(j)$ has linearly-independent columns in $\mathbf{Span}(P_{\ell}(j))$, and P_{ℓ} partitions the linearly-independent set of vectors B_{ℓ} , it follows that each Σ_{ℓ} has full column rank with its columns in $\mathbf{Span}(B_{\ell})$.

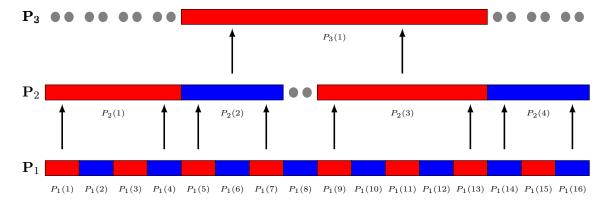


Figure 1: A snapshot of the construction of B_{ℓ} and partition \mathbf{P}_{ℓ} for the initial 3 levels. In this illustration, vertically aligned dots in groups of three represent the same basis vector. At any given level ℓ , vectors indicated in solid colors comprise the alive vectors B_{ℓ} of level ℓ . Furthermore, the colored boxes at each level ℓ , along with their constituent alive basis vectors, represent the parts $P_{\ell}(i)$ of the partition of \mathbf{P}_{ℓ} . Random parts $\widetilde{\mathbf{P}}_{\ell}$ that survive through to the next level are indicated by upward arrows.

$$P_3(j) = \left\{ \begin{array}{cccccc} v'_1, & v'_2, & v'_3, & v'_4, & v'_5, & v'_6, & v'_7, & v'_8 \end{array} \right\}$$

$$\Sigma_3(j) = \left[\begin{array}{cccccc} \sigma_1 = & v'_1 + & v'_2 + & v'_3 + & v'_4 & & & \\ \sigma_2 = & & v'_2 + & v'_3 + & v'_4 + & v'_5 & & \\ \sigma_3 = & & & v'_3 + & v'_4 + & v'_5 + & v'_6 & & \\ \sigma_4 = & & & & v'_4 + & v'_5 + & v'_6 + & v'_7 \end{array} \right]^T$$

Figure 2: Construction of $\Sigma_3(j)$ matrix.

Our construction also guarantees that the columns of all the matrices Σ_{ℓ} , across all the different levels ℓ , are distinct and therefore pairwise linearly-independent in \mathbb{F}_2 . Each column of $\Sigma_{\ell}(j)$ is formulated as a sum of distinct subsets (which may overlap) of vectors from $P_{\ell}(j)$, with each subset containing $2^{\ell-1}$ vectors. Given that the number of columns in $\Sigma_{\ell}(j)$ is half the size $P_{\ell}(j)$, such a construction is possible. In detail, given $P_{\ell}(j) = \{\mathbf{v}'_1, \dots, \mathbf{v}'_{2^{\ell}}\}$, the t-th column of $\Sigma_{\ell}(j)$ is defined as:

$$\sigma_t := \sum_{i=t}^{t+2^{\ell-1}-1} \mathbf{v}_i'.$$

As an illustrative example, we depict the construction of $\Sigma_3(j)$ for $j \in [d/2^{2\ell-1}]$ in Figure 2.

The final matrix Σ is the concatenation of the matrices across all levels, namely $\Sigma := \left[\Sigma_1 \ \Sigma_2 \ \dots \ \Sigma_{\kappa} \right]$. The precise construction is described in Procedure 4.

We now present two essential observations about our construction, which are vital for the proof of Lemma 6.6.

Observation 6.7. For each level $\ell \in [\kappa]$ and part $P_{\ell}(j) \in \mathbf{P}_{\ell}$, there exists level ℓ' such that $\ell \leq \ell' \leq \kappa$ and

- 1. $P_{\ell}(j) \subseteq B_i \text{ for all } i \leq \ell'$,
- 2. $P_{\ell}(j) \cap B_i = \emptyset$ for all $i > \ell'$.

Proof. Considering a specific part $P_{\ell}(j)$ within \mathbf{P}_{ℓ} , it is constructed such that either it becomes part of a subsequent part $P_{\ell+1}(j')$ in $\mathbf{P}_{\ell+1}$, or it does not intersect with any part in $\mathbf{P}_{\ell+1}$. This pattern holds for any two consecutive levels. Therefore, for any two levels $\ell < \ell'$ and a given part $P_{\ell}(j)$, it is either entirely contained within a part $P_{\ell'}(j')$ in $\mathbf{P}_{\ell'}$, or it shares no common elements with any part in $\mathbf{P}_{\ell'}$. Since $\mathbf{P}_{\ell'}$ is a partition of $B_{\ell'}$, this implies that $P_{\ell}(j)$ is either a subset of $B_{\ell'}$ or has no overlap with $B_{\ell'}$. Since $\{B_i\}_{i\in[\kappa]}$ form a nested system, i.e., $B_i\subseteq B_{i+1}$ for each $i\in[\kappa-1]$, the proof is complete.

The following observation directly follows from the fact that each part survives to the next level with probability 1/2 independently.

Observation 6.8. For any level $\ell \in [\kappa - 1]$ and part $P_{\ell}(j) \in \mathbf{P}_{\ell}$ for $j \in [d/2^{2\ell-1}]$,

$$\mathbf{Pr}[P_{\ell}(j) \subseteq B_{\ell+1} \mid P_{\ell}(j) \subseteq B_{\ell}] = \frac{1}{2}.$$

We are now ready to prove the Lemma 6.6.

Proof of Lemma 6.6. We will demonstrate separately that each property is met by the construction:

- (i) At each level, precisely half of the "alive" basis vectors continue to the next level. Initially, at the first level, there are d alive basis vectors, i.e., $|B_1| = d$. We conclude Property (i).
- (ii) By construction, each column of Σ_{ℓ} is a sum of standard basis vectors in B_{ℓ} . It remains to show linear independence. Recall that $\Sigma_{\ell} = [\Sigma_{\ell}(1), \dots, \Sigma_{\ell}(d/2^{2\ell-1})]$, with $\Sigma_{\ell}(j) \subseteq \operatorname{Span}(P_{\ell}(j))$. Also recall that \mathbf{P}_{ℓ} is a partition of B_{ℓ} . Consider an arbitrary column e of Σ_{ℓ} , corresponding to the tth column of a particular $\Sigma_{\ell}(j)$. From Step (3) of Procedure 4, $e = \sum_{i=t}^{s} \mathbf{v}'_{i}$ for $s = t + 2^{\ell-1} 1$, where $\mathbf{v}'_{1}, \dots \mathbf{v}'_{2^{\ell}}$ is a fixed enumeration of $P_{\ell}(j)$. All columns of Σ_{ℓ} to the left of e, whether in $\Sigma_{\ell}(j)$ or otherwise, are orthogonal to v'_{s} , whereas e is not. Therefore, e is linearly independent of all columns to its left. Applying this argument inductively, we conclude that Σ_{ℓ} has full column rank. Therefore, our construction satisfies Property (ii).
- (iii) Fix two levels $\ell, \ell' \in [\kappa]$ such that $\ell' > \ell$. Let $\mathbf{e} \in \Sigma_{\ell}$ be an arbitrary column of Σ_{ℓ} . Let j be such that \mathbf{e} is a column of $\Sigma_{\ell}(j)$. By construction, we have that $\mathbf{e} \in \mathbf{Span}(P_{\ell}(j))$. Then,

$$\begin{split} \mathbf{Pr}[e \in \mathbf{Span}(B_{\ell'}) \mid \{e \in \Sigma_{\ell}(j)\}, \Sigma_{1}, \dots, \Sigma_{\ell}, B_{1}, \dots, B_{\ell}] \\ &= \mathbf{Pr}[P_{\ell}(j) \subseteq \mathbf{Span}(B_{\ell'}) \mid \Sigma_{1}, \dots, \Sigma_{\ell}, B_{1}, \dots, B_{\ell}] \\ &= \prod_{i=\ell+1}^{\ell'} \mathbf{Pr}\left[P_{\ell}(j) \subseteq \mathbf{Span}(B_{i}) \mid P_{\ell}(j) \subseteq \mathbf{Span}(B_{i-1}), \Sigma_{1}, \dots, \Sigma_{\ell}, B_{1}, \dots, B_{\ell}\right] \\ &= \prod_{i=\ell+1}^{\ell'} \mathbf{Pr}\left[P_{\ell}(j) \subseteq \mathbf{Span}(B_{i}) \mid P_{\ell}(j) \subseteq \mathbf{Span}(B_{i-1})\right] \\ &= \left(\frac{1}{2}\right)^{\ell'-\ell}. \end{split}$$

Above, the first equality follows from Observation 6.7. The second one follows from the fact that $\{B_{\ell}\}_{{\ell}\in[\kappa]}$ forms a nested system. The third equality is because $\Sigma_1,\ldots,\Sigma_{\ell}$ and B_1,\ldots,B_{ℓ} are functions of $\mathbf{P}_1,\ldots,\mathbf{P}_{\ell}$, conditionally independent of what transpires at higher levels. The last equality follows from Observation 6.8. Therefore, the construction satisfies Property (iii).

(iv) Each Σ_{ℓ} has full column rank, and therefore it's columns are distinct. It remains to compare columns $\sigma \in \Sigma_{\ell}$ and $\sigma' \in \Sigma_{\ell'}$ for $\ell \neq \ell'$. The vector σ is the sum of $2^{\ell-1}$ principal basis vectors, while σ' is the sum of $2^{\ell'-1}$ principal basis vectors. It follows that σ and σ' are distinct. This confirms Property (iv).

6.4 Optimal Pairwise Independent Matroid Prophet Inequality

In this section, we present an optimal (up to a constant factor) algorithm for the pairwise independent matroid prophet inequality problem against the almighty adversary. It is important to note that although our algorithm is designed to perform against the strongest adversary, the almighty adversary; our impossibility result holds against the weakest adversary, namely the oblivious adversary.

The following theorem is the main result of the section.

Theorem 6.9. There exists an $\Omega\left(\frac{1}{\log Rank}\right)$ -competitive algorithm for the pairwise independent prophet inequality problem against the almighty adversary for any given matroid $\mathcal{M}=(E,\mathcal{I})$. Here, Rank is a shorthand notation for $Rank(\mathcal{M})$.

The algorithm defines the strategy for the gambler by dividing elements into weight buckets. Let $\mathcal{M} = (E, \mathcal{I})$ be a matroid and $\mathbf{w} \sim \mathcal{D}$ be a pairwise independent weight distribution. We use **OPT** to denote the expected value of $\mathbf{Rank_w}(\mathcal{M})$ under \mathcal{D} . To proceed, we set k as the ceiling of $\log(8\mathbf{Rank})$ and introduce k+2 buckets: $B_0, B_1, \ldots B_k$, along with B_{∞} . The buckets are defined as follows:

$$B_0 = \left[0, \frac{\mathbf{OPT}}{2\mathbf{Rank}}\right), B_1 = \left[\frac{\mathbf{OPT}}{2\mathbf{Rank}}, \frac{2\mathbf{OPT}}{2\mathbf{Rank}}\right), \dots, B_k = \left[\frac{2^{k-1}\mathbf{OPT}}{2\mathbf{Rank}}, \frac{2^k\mathbf{OPT}}{2\mathbf{Rank}}\right), B_{\infty} = \left[\frac{2^k\mathbf{OPT}}{2\mathbf{Rank}}, \infty\right).$$

Given any draw of the weights $w \sim \mathcal{D}$, we partition the elements into random sets $E_0, E_1, \ldots E_k$ and E_{∞} based on their realization. We define $E_i = \{e \in E : \mathbf{w}(e) \in B_i\}$ for any $i \in \{0, \ldots, k, \infty\}$, which represents the elements whose weight lies in bucket B_i . It is important to note that the sets E_i for $i \in \{0, \ldots, k, \infty\}$ are random.

We define the expected optimal reward from bucket B_i for any $i \in \{0, 1, \dots, k, \infty\}$ as

$$\mathbf{OPT}(B_i) = \mathbb{E}\left[\max_{S \subseteq E_i, S \in \mathcal{I}} \mathbf{Rank_w}(S)\right].$$

This represents the maximum expected weighted rank of elements belonging to bucket B_i . We further define

$$B^* = \max_{i \in \{1, \dots, k, \infty\}} \mathbf{OPT}(B_i).$$

Note that we ignore bucket B_0 because every element $e \in E_0$ has weight $\mathbf{w}(e) \leq \frac{\mathbf{OPT}}{2 \cdot \mathbf{Rank}}$, and therefore $\mathbf{OPT}(B_0) \leq \frac{\mathbf{OPT}}{2}$. Next, we aim to upper-bound the expected reward of the prophet

Algorithm 1 Pairwise Independent Matroid Prophet Inequality Algorithm.

Input: Matroid $\mathcal{M} = (E, \mathcal{I})$ and pairwise independent joint weight distribution $\mathbf{w} \sim \mathcal{D}$.

Output: S.

Compute \mathbf{OPT} and buckets B_0, \dots, B_{k+1} Let $B^* = \operatorname{argmax}_{B_i \in \{B_1, \dots, B_k, B_\infty\}} \mathbf{OPT}(B_i)$ Set $S \leftarrow \emptyset$ while Visit elements $e \in E$ in given order \mathbf{do} if $\mathbf{w}(e) \in B^*$ and $S \cup \{e\} \in \mathcal{I}$ then

Update $S \leftarrow S \cup \{e\}$ end if
end while

by considering the total expected optimal rewards from each bucket. By invoking the fact that $\mathbf{OPT}(B_0) \leq \frac{\mathbf{OPT}}{2}$, we obtain:

$$\mathbf{OPT} \le \sum_{i=0}^{k} \mathbf{OPT}(B_i) + \mathbf{OPT}(B_{\infty}) \le 2 \cdot \left(\sum_{i=1}^{k} \mathbf{OPT}(B_i) + \mathbf{OPT}(B_{\infty}) \right).$$
 (5)

Based on these observations, we define Algorithm 1.

To prove the competitive ratio of the algorithm, we consider two cases: (i) when $B^* = B_i$ for some $i \in [k]$, and (ii) when $B^* = B_{\infty}$. First, we demonstrate that within each bucket B_i (where $i \in \{1, ..., k\}$), the greedy algorithm obtains a substantial portion of the optimal solution. This is because the weights of items in each bucket differ by at most a factor of 2

Lemma 6.10. Let S be the output of Algorithm 1. If $B^* \in \{B_1, \dots B_k\}$ then

$$\mathbb{E}[\mathbf{w}(S)] \ge \frac{1}{2} \cdot \mathbb{E}[\mathbf{\textit{Rank}}_{\mathbf{w}}(B^*)].$$

Proof. Let $B_i = B^*$ for some $i \in [k]$ and $\ell = 2^{i-1} \cdot \frac{\mathbf{OPT}}{\mathbf{Rank}^2}$. Then, observe that $\ell \leq \mathbf{w}(e) \leq 2 \cdot \ell$ for all $e \in B_i$ and $\mathbf{Rank}_{\mathbf{w}}(E_i) \leq 2 \cdot \ell \cdot \mathbf{Rank}(E_i)$. Since the greedy algorithm guarantees an independent set S such that $|S| = \mathbf{Rank}(E^*)$ with probability 1, we have

$$\operatorname{\mathbf{Rank}}_{\mathbf{w}}(S) \ge \ell \cdot |S| = \ell \cdot \operatorname{\mathbf{Rank}}(E_i) \ge \frac{1}{2} \cdot \operatorname{\mathbf{Rank}}_{\mathbf{w}}(E_i).$$

which completes the proof.

Next, we consider the scenario when $B^* = B_{\infty}$.

Lemma 6.11. Let S be the output of Algorithm 1. If $B^* = B_{\infty}$ then

$$\mathbb{E}[\mathbf{w}(S)] \geq \frac{1}{2} \cdot \mathbb{E}[\mathbf{\textit{Rank}}_{\mathbf{w}}(B^*)].$$

Proof. First of all, observe that $\mathbf{w}(e) \ge \frac{2^k \cdot \mathbf{OPT}}{2} \ge 4 \cdot \mathbf{OPT}$ as $k = \lceil \log(8\mathbf{Rank}) \rceil$. Therefore,

$$\Pr[|E_{\infty}| \geq 1] \cdot 4 \cdot \mathbf{OPT} \leq \mathbb{E}[\mathbf{Rank}_w(E_{\infty})] \leq \mathbf{OPT},$$

and so $\Pr[E_{\infty} \neq \emptyset] \leq \frac{1}{4}$. As we have pairwise independent random weights, we use Lemma 2.2 to obtain

$$\mathbf{Pr}[E_{\infty} \neq \emptyset] = \mathbf{Pr}\left[\bigvee_{e \in E} \{e \in E_{\infty}\}\right] \geq \frac{\sum_{e \in E} \mathbf{Pr}[e \in E_{\infty}]}{1 + \sum_{e \in E} \mathbf{Pr}[e \in E_{\infty}]}.$$

Rearranging terms implies that $\sum_{e \in E} \mathbf{Pr}[e \in E_{\infty}] \leq \frac{\mathbf{Pr}[E_{\infty} \neq \emptyset]}{1 - \mathbf{Pr}[E_{\infty} \neq \emptyset]} \leq \frac{1}{3}$. Thus, by using pairwise independence we obtain that for any element $e \in E$ and value $v \in B_{\infty}$,

$$\mathbf{Pr}[|E_{\infty}| > 1 \mid \mathbf{w}(e) = v] \le \sum_{f \in E \setminus \{e\}} \mathbf{Pr}[f \in E_{\infty} \mid \mathbf{w}(e) = v] = \sum_{f \in E \setminus \{e\}} \mathbf{Pr}[f \in E_{\infty}] \le \frac{1}{3}.$$

Above, the first inequality is due to union bound. The equality follows from pairwise independence of the weights. This imply that for any value $v \in B_{\infty}$, we have $\Pr[E_{\infty} = \{e\} \mid \mathbf{w}(e) = v] \geq \frac{2}{3}$. Finally, we compute the expected weight of S as

$$\begin{split} \mathbb{E}[\mathbf{w}(S)] &= \sum_{e \in E} \mathbb{E}[\mathbf{w}(e) \cdot \mathbb{1}[e \in S]] \\ &\geq \sum_{e \in E} \mathbb{E}[\mathbf{w}(e) \cdot \mathbb{1}[|E_{\infty}| = 1] \cdot \mathbb{1}[\mathbf{w}(e) \in B_{\infty}]] \\ &= \sum_{e \in E} \mathbb{E}[\mathbf{Pr}[|E_{\infty}| = 1 \mid \mathbf{w}(e) \wedge \mathbf{w}(e) \in B_{\infty}] \cdot \mathbf{w}(e) \cdot \mathbb{1}[\mathbf{w}(e) \in B_{\infty}]] \\ &\geq \sum_{e \in E} \mathbb{E}\left[\frac{2}{3} \cdot \mathbf{w}(e) \cdot \mathbb{1}[\mathbf{w}(e) \in B_{\infty}]\right] \\ &= \frac{2}{3} \cdot \mathbb{E}[\mathbf{w}(B_{\infty})] \geq \frac{2}{3} \cdot \mathbb{E}[\mathbf{Rank}_{\mathbf{w}}(B_{\infty})] \end{split}$$

We now complete the proof of Theorem 6.9.

Proof. Let $B^* := \operatorname{argmax}_{B_i \in \{B_1, \dots B_k, B_{\infty}\}} \mathbf{OPT}(B_i)$ as defined in Algorithm 1. We observe that

$$\mathbb{E}[\mathbf{Rank}_w(E^*)] = \max_{i \in \{1, \dots, k, \infty\}} \mathbf{OPT}(B_i) \ge \frac{1}{k+1} \cdot \sum_{i \in \{1, \dots, k, \infty\}} \mathbf{OPT}(B_i) \ge \frac{1}{k+1} \cdot \frac{1}{2} \cdot \mathbf{OPT}.$$

By Lemma 6.10 and Lemma 6.11, we know that $\mathbb{E}[w(S)] \geq \frac{1}{2} \cdot \mathbb{E}[\mathbf{Rank}_w(E^*)] = \frac{1}{2} \cdot \mathbf{OPT}(B^*)$. Thus, $\mathbb{E}[w(S)] \geq \frac{1}{4(k+1)} \cdot \mathbf{OPT}$ completes the proof as $k = \Theta(\log \mathbf{Rank})$. Since our algorithm is deterministic and the probabilistic guarantees are valid regardless of the arrival order, the approximation guarantee holds even against the almighty adversary.

7 The Partition Property and its Implications

In this section, our focus is on matroids that exhibit a *constant partition property*. We demonstrate that such matroids admit constant factor guarantees for both pairwise-independent contention resolution and prophet inequalities. We also state structural implications of these results for the partition property.

A simple partition matroid is the disjoint union of rank one matroids, as defined in Section 2.2. We use the following definition of the partition property from [10].

Constraint	Offline CRS	OCRS	Prophet Inequality	Notes & References
Partition Matroid	$\frac{1}{1.299} \cdot \left(1 - \frac{1}{e}\right)$	$\frac{1}{1.299} \cdot \left(1 - \frac{1}{e}\right) \cdot \frac{1}{3}$	$\frac{1}{3}$	Theorem 7.3 7.4 7.6
Graphic Matroid	$\frac{1}{1.299} \cdot \left(1 - \frac{1}{e}\right) \cdot \frac{1}{2}$	$\frac{1}{1.299} \cdot \left(1 - \frac{1}{e}\right) \cdot \frac{1}{12}$	$\frac{1}{6}$	Theorem 7.3 7.4 7.6 and [10]
Co-Graphic Matroid	$\frac{1}{1.299} \cdot \left(1 - \frac{1}{e}\right) \cdot \frac{1}{3}$	$\frac{1}{1.299} \cdot \left(1 - \frac{1}{e}\right) \cdot \frac{1}{27}$	$\frac{1}{9}$	Theorem 7.3 7.4 7.6 and [51]
Laminar Matroid	$\frac{1}{1.299} \cdot \left(1 - \frac{1}{e}\right) \cdot \frac{1}{3\sqrt{3}}$	$\frac{1}{1.299} \cdot \left(1 - \frac{1}{e}\right) \cdot \frac{1}{3^4}$	$\frac{1}{9\sqrt{3}}$	Theorem 7.3 7.4 7.6 and [37]
Low Density Matroid	$\frac{1}{1.299} \cdot \left(1 - \frac{1}{e}\right) \cdot \frac{1}{2\gamma}$	$\frac{1}{1.299} \cdot \left(1 - \frac{1}{e}\right) \cdot \frac{1}{12\gamma^2}$	$\frac{1}{6\gamma}$	Theorem 7.3 7.4 7.6 and [51], $\gamma = \max_{S \subseteq E} \frac{ S }{\mathbf{Rank}(S)}$
Column k Sparse Matroid	$\frac{1}{1.299} \cdot \left(1 - \frac{1}{e}\right) \cdot \frac{1}{2k}$	$\frac{1}{1.299} \cdot \left(1 - \frac{1}{e}\right) \cdot \frac{1}{12k^2}$	$\frac{1}{6k}$	Theorem 7.3 7.4 7.6 and [51]

Table 1: Summary of our results for matroids that satisfy the partition property.

Definition 7.1 (Partition Property). We say a matroid $\mathcal{M} = (E, \mathcal{I})$ satisfies the α -partition property for $\alpha \in (0, 1]$ if there exists a random simple partition matroid $\mathcal{M}' = (E', \mathcal{I}')$ satisfying

- 1. $E' \subseteq E$ and $\mathcal{I}' \subseteq \mathcal{I}$, and
- 2. $Rank_{\mathbf{w}}(\mathcal{M}) \geq \mathbb{E}_{\mathcal{M}'}[Rank_{\mathbf{w}}(\mathcal{M}')] \geq \alpha \cdot Rank_{\mathbf{w}}(\mathcal{M})$ for every nonnegative weight vector \mathbf{w} .

It is known that many classes of matroids that are frequently encountered in discrete optimization satisfy an α -partition property with $\alpha = O(1)$ [10, 51].

We show that if a matroid \mathcal{M} satisfies the α partition property, then it admits a pairwise independent (i) $\frac{\alpha}{3}$ -competitive prophet inequality against the almighty adversary, (ii) $\frac{\alpha}{1.299} \cdot (1-1/e)$ -balanced offline CRS, and (iii) $\frac{\alpha^2}{3.897} \cdot (1-1/e)$ -balanced OCRS against the almighty adversary. These are proven in Theorem 7.3, 7.4, and 7.6 respectively. Essentially, we demonstrate these results by reducing the stochastic selection problems with pairwise independent priors for such matroids to those of one-uniform matroids, utilizing the partition property. In doing so, we assume our algorithms can sample a simple partition matroid \mathcal{M}' satisfying the conditions of Definition 7.1. We summarize the corollaries derived from our results in Table 1.

7.1 Prophet Inequalities

We now exhibit an $\frac{\alpha}{3}$ -competitive algorithm for pairwise-independent prophet inequalities on matroids satisfying the α -partition property. First, we recall a result from [19] which shows the existence of a $\frac{1}{3}$ -competitive pairwise independent prophet inequality for rank one matroids. The analysis of their threshold-based algorithm can easily be seen to hold even against the almighty online adversary.

Algorithm 2 Partition-Based Algorithm for Pairwise Independent Matroid Prophet Inequalities.

Input: A matroid $\mathcal{M} = (E, \mathcal{I})$ satisfying the α partition property, distribution $\mathcal{D} \in \Delta_{pw}(2^E)$, black-box access to algorithm \mathcal{A} for single-choice pairwise-independent prophet inequalities

Let \mathcal{M}' be a random partition matroid α -approximating \mathcal{M} as in Definition 7.1, and let P_1, \ldots, P_r be its parts.

Separately for each part P_i , invoke \mathcal{A} for the rank one matroid on P_i using the restriction of \mathcal{D} to P_i , and let S_i be its output.

Output: Set $S \leftarrow \bigcup_{i=1}^r S_i$.

Theorem 7.2 ([19]). Given a rank one matroid over elements E and a pairwise independent value distribution $\mathcal{D} \in \Delta_{pw}(2^E)$, there exists a $\frac{1}{3}$ -competitive prophet inequality algorithm against the almighty adversary.

Our algorithm samples a partition matroid \mathcal{M}' as in Definition 7.1, then applies the $\frac{1}{3}$ -competitive prophet inequality to each part of \mathcal{M}' separately. This is shown in Algorithm 2.

Theorem 7.3. For matroids satisfying the α -partition property for some $\alpha \in (0,1]$, there is an $\frac{\alpha}{3}$ -competitive pairwise-independent prophet inequality against the almighty adversary.

Proof. We invoke Algorithm 2 with black box access to a $\frac{1}{3}$ -competitive prophet inequality algorithm \mathcal{A} for rank one matroids and pairwise independent distributions as in Theorem 7.2. Let \mathcal{M} , \mathcal{D} , \mathcal{M}' , $\{P_i\}_{i=1}^r$ and $S = \bigcup_i S_i$ be as in Algorithm 2, and let $\mathbf{w} \sim \mathcal{D}$ be the realized stochastic weights. We have the following guarantee on the weight of the output S conditioned on \mathcal{M}' .

$$\mathbb{E}[\mathbf{w}(S) \mid \mathcal{M}'] = \sum_{i=1}^{r} \mathbb{E}[\mathbf{w}(S_i) \mid \mathcal{M}'] \qquad \text{(Linearity of expectation)}$$

$$\geq \sum_{i=1}^{r} \mathbb{E}\left[\frac{1}{3} \cdot \mathbf{Rank}_{\mathbf{w}}^{\mathcal{M}'}(P_i) \mid \mathcal{M}'\right] \qquad \text{(Theorem 7.2)}$$

$$= \frac{1}{3} \cdot \mathbb{E}\left[\sum_{i=1}^{r} \mathbf{Rank}_{\mathbf{w}}^{\mathcal{M}'}(P_i) \mid \mathcal{M}'\right] \qquad \text{(Linearity of expectation)}$$

$$= \frac{1}{3} \cdot \mathbb{E}\left[\mathbf{Rank}_{\mathbf{w}}(\mathcal{M}') \mid \mathcal{M}'\right] \qquad (\mathcal{M}' \text{ is a partition matroid)} \qquad (6)$$

Next, taking expectations over \mathcal{M}' , we have

$$\mathbb{E}[w(S)] = \mathbb{E}\left[\mathbb{E}[\mathbf{w}(S) \mid \mathcal{M}']\right]$$

$$\geq \mathbb{E}\left[\frac{1}{3} \cdot \mathbb{E}\left[\mathbf{Rank_{w}}(\mathcal{M}') \mid \mathcal{M}'\right]\right] \qquad \text{(Equation 6)}$$

$$= \frac{1}{3} \mathbb{E}\left[\mathbb{E}\left[\mathbf{Rank_{w}}(\mathcal{M}') \mid \mathbf{w}\right]\right]$$

$$\geq \frac{1}{3} \mathbb{E}\left[\alpha \cdot \mathbf{Rank_{w}}(\mathcal{M})\right] \qquad \text{(α-partition property)}$$

$$= \frac{\alpha}{3} \cdot \mathbb{E}\left[\mathbf{Rank_{w}}(\mathcal{M})\right].$$

Above, the second equality holds due to Fubini's theorem since $\mathbf{Rank_w}(\mathcal{M}')$ is a non-negative random variable with a finite expectation. We conclude that Algorithm 2 is $\frac{\alpha}{3}$ -competitive, as needed. We note that since the competitive ratio of \mathcal{A} holds against the almighty adversary, so does ours.

7.2 Contention Resolution

Now, we turn our attention to proving the existence of $O(\alpha)$ -balanced offline and $O(\alpha^2)$ -balanced online pairwise independent CRS for matroids that satisfy α partition property. We begin with the offline result.

Theorem 7.4. For matroids satisfying the α -partition property for some $\alpha \in (0,1]$, there is a $\frac{1}{1.299} \cdot (1 - \frac{1}{e}) \cdot \alpha$ -balanced pairwise-independent offline CRS.

Proof. Consider a matroid $\mathcal{M} = (E, \mathcal{I})$ and a distribution $\mathcal{D} \in \Delta_{\mathrm{pw}}(2^E)(\mu)$ with $\mu \in \mathcal{P}(\mathcal{M})$. Let $\mathcal{M}' = (E', \mathcal{I}')$ be a random partition matroid which α -approximates \mathcal{M} in the sense of Definition 7.1. Let $\widetilde{R} \subseteq E$ be sampled from the product distribution with marginals μ ; i.e., each element $e \in E$ is included in \widetilde{R} independently with probability $\mu(e)$. It was shown in [22] that the class of product distributions with marginals in $\mathcal{P}(\mathcal{M})$ admits a (1 - 1/e)-balanced offline CRS. Therefore, by Theorem 2.1 the following holds for all sets of elements $F \subseteq E$.

$$\mathbb{E}_{\widetilde{R}}[\mathbf{Rank}_{\mathcal{M}}(\widetilde{R}\cap F)] \ge (1 - 1/e) \cdot \mu(F). \tag{7}$$

Moreover, the α -partition property implies that for every fixed \widetilde{R} , $\mathbb{E}_{\mathcal{M}'}[\mathbf{Rank}_{\mathcal{M}'}(\widetilde{R} \cap F)] \geq \alpha \cdot \mathbf{Rank}_{\mathcal{M}}(\widetilde{R} \cap F)$. Combining this with Equation 7, we obtain

$$\mathbb{E}_{\mathcal{M}'|\widetilde{R}}[\mathbf{Rank}_{\mathcal{M}'}(\widetilde{R}\cap F)] \ge (1 - 1/e) \cdot \alpha \cdot \mu(F). \tag{8}$$

Let P_1, \ldots, P_k be the parts of the matroid \mathcal{M}' , and let R be sampled from the pairwise independent distribution \mathcal{D} . We have the following for any $F \subseteq E$.

$$\mathbb{E}[\mathbf{Rank}_{\mathcal{M}}(R \cap F)] \geq \mathbb{E}_{\mathcal{M}'} \left[\mathbb{E}[\mathbf{Rank}_{\mathcal{M}'}(R \cap F)] \right] \qquad (\mathcal{I}' \subseteq \mathcal{I})$$

$$= \mathbb{E}_{\mathcal{M}'} \left[\sum_{i=1}^{k} \mathbf{Pr}_{R} \left[\bigvee_{e \in F \cap P_{i}} e \in R \right] \right] \qquad (Partition matroid)$$

$$\geq \mathbb{E}_{\mathcal{M}'} \left[\sum_{i=1}^{k} \frac{1}{1.299} \cdot \mathbf{Pr}_{\widetilde{R}} \left[\bigvee_{e \in F \cap P_{i}} e \in \widetilde{R} \right] \right] \qquad (Lemma 2.2)$$

$$= \frac{1}{1.299} \cdot \mathbb{E}_{\mathcal{M}',\widetilde{R}}[\mathbf{Rank}_{\mathcal{M}'}(\widetilde{R} \cap F)] \qquad (Partition matroid)$$

$$\geq \frac{1}{1.299} \cdot \left(1 - \frac{1}{e} \right) \cdot \alpha \cdot \mu(F). \qquad (Equation 8)$$

Combining above inequality with the characterization from Theorem 2.1, we conclude that the family of pairwise independent distributions $\Delta_{\text{pw}}(\mu)$ with $\mu \in \mathcal{P}_{\mathcal{M}}$ admits $\left(\frac{1}{1.29} \cdot (1 - 1/e) \cdot \alpha\right)$ -balanced CRS when matroid \mathcal{M} satisfies the α -partition property.

Next, we show how to combine our offline pairwise-independent CRS with our pairwise-independent prophet inequality to obtain an online CRS. We use the following lemma, the proof of which closely mirrors the arguments used in the proof of Theorem 4.1 from [25]. Hence, we omit its detailed presentation here.

Lemma 7.5. If a matroid \mathcal{M} admits a γ -competitive pairwise-independent prophet inequality against the almighty adversary and a β -balanced offline pairwise-independent CRS, then it also admits a $\beta \cdot \gamma$ -balanced OCRS against the almighty adversary.

Combining Lemma 7.5 and Theorem 7.4 and 7.3, we obtain the following theorem.

Theorem 7.6. For matroids satisfying the α -partition property for some $\alpha \in (0,1]$, there is a $\frac{1}{1.299} \cdot \left(1 - \frac{1}{e}\right) \cdot \frac{\alpha^2}{3}$ -balanced pairwise-independent OCRS against the almighty adversary.

7.3 Structural Implications

We now shift our focus to showing that full linear matroids over a finite field do not admit a partition property with strong approximation guarantees. We prove this by combining the offline CRS of Theorem 7.4 with the impossibility result for contention resolution presented in Theorem 5.1.

Corollary 7.7. The full linear matroid \mathbb{F}_q^d of rank d, with $q \geq d$, does not satisfy an α -partition property with $\alpha = \omega\left(\frac{1}{d}\right)$. Moreover, the full binary matroid \mathbb{F}_2^d of rank d does not satisfy an α -partition property with $\alpha = \omega\left(\frac{\log d}{d}\right)$.

Proof. First, we briefly argue that duplicating elements of a matroid preserves the partition property. Suppose that $\mathcal{M}=(E,\mathcal{I})$ satisfies the α -partition property, as witnessed by a random matroid \mathcal{M}' as in Definition 7.1. For a positive integer m, let $\mathcal{M}\times m=(E^{\times m},\mathcal{I}^{\times m})$ be the matroid which includes m parallel duplicates e^1,\ldots,e^m of each element e of \mathcal{M} , as described in Section 2.2. Let $\mathcal{M}'\times m$ be defined similarly. For a weight vector \mathbf{w} indexed by the elements $E^{\times m}$ of $\mathcal{M}^{\times m}$, let $\widetilde{\mathbf{w}}\in\mathbb{R}^E$ be such that $\widetilde{w}(e)=\max_{i=1}^m w(e^i)$. Similarly, for $S\subseteq E^{\times m}$ let $\widetilde{S}=\left\{e\in E:e^i\in S \text{ for some }i\right\}$. It is clear that $\mathbf{Rank}_w^{\mathcal{M}\times m}(S)=\mathbf{Rank}_{\widetilde{\mathbf{w}}}^{\mathcal{M}}(\widetilde{S})$, and similarly $\mathbf{Rank}_w^{\mathcal{M}'\times m}(S)=\mathbf{Rank}_{\widetilde{\mathbf{w}}}^{\mathcal{M}'}(\widetilde{S})$. The following calculation for arbitrary $S\subseteq E^{\times m}$ shows that $\mathcal{M}\times m$ satisfies the α -partition property, as witnessed by $\mathcal{M}'\times m$.

$$\begin{split} \mathbb{E}_{\mathcal{M}'} \left[\mathbf{Rank}_{w}^{\mathcal{M}' \times m}(S) \right] &= \mathbb{E}_{\mathcal{M}'} \left[\mathbf{Rank}_{\widetilde{\mathbf{w}}}^{\mathcal{M}'}(\widetilde{S}) \right] \\ &\geq \alpha \cdot \mathbf{Rank}_{\widetilde{\mathbf{w}}}^{\mathcal{M}}(\widetilde{S}) \\ &= \alpha \cdot \mathbf{Rank}_{\mathbf{w}}^{\mathcal{M} \times m}(S) \end{split}$$

Given that the partition property is invariant to duplicating elements, combining Theorem 5.1 and 7.4 now yields the corollary.

8 Open Questions

Our results indicate that pairwise independence lends insufficient structure for constant approximations to contention resolution and prophet inequalities on matroids. More generally, it is natural to investigate the same questions for k-wise independence, and to quantify the optimal ratios as

a function of k. Our impossibility results rely on the recipe presented in Section 4, which easily generalizes to k-wise independence only for ordered vector families. Generalizing our unordered construction to arbitrary k promises to extend our results to k-wise independence. We conjecture an optimal bound of O(k/rank) for contention resolution, and refrain from such conjecture for prophet inequalities.

Due to the equivalence between the matroid secretary problem and the matroid prophet secretary problem from [26], extending our impossibility result for prophet inequalities to the random order model would disprove the matroid secretary conjecture. In fact, constructions which are k-wise independent might be particularly promising, since they preclude any "learning" from samples of size k. On the flip side, designing secretary algorithms for variants of our construction could stimulate the development of pertinent algorithmic techniques.

References

- [1] Dorna Abdolazimi, Anna R. Karlin, Nathan Klein, and Shayan Oveis Gharan. Matroid partition property and the secretary problem. In 14th Innovations in Theoretical Computer Science Conference (ITCS), volume 251, pages 2:1–2:9, 2023.
- [2] Marek Adamczyk and Michał Włodarczyk. Random order contention resolution schemes. In 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS), pages 790–801. IEEE, 2018.
- [3] Marek Adamczyk, Fabrizio Grandoni, and Joydeep Mukherjee. Improved approximation algorithms for stochastic matching. In *Algorithms-ESA 2015: 23rd Annual European Symposium*, *Patras, Greece, September 14-16, 2015, Proceedings*, pages 1–12. Springer, 2015.
- [4] Saeed Alaei. Bayesian combinatorial auctions: Expanding single buyer mechanisms to many buyers. SIAM Journal on Computing (SICOMP), 43(2):930–972, 2014.
- [5] Noga Alon, László Babai, and Alon Itai. A fast and simple randomized parallel algorithm for the maximal independent set problem. *Journal of Algorithms*, 7(4):567–583, 1986.
- [6] Noga Alon, Oded Goldreich, Johan Håstad, and René Peralta. Simple construction of almost k-wise independent random variables. Proceedings [1990] 31st Annual Symposium on Foundations of Computer Science, pages 544–553 vol.2, 1990.
- [7] Noga Alon, Oded Goldreich, and Yishay Mansour. Almost k-wise independence versus k-wise independence. *Information Processing Letters*, 88(3):107–110, 2003.
- [8] Georgios Askalidis and Edward C. Malthouse. The value of online customer reviews. In *Proceedings of the 10th ACM Conference on Recommender Systems*, page 155–158, 2016.
- [9] Moshe Babaioff, Nicole Immorlica, and Robert Kleinberg. Matroids, secretary problems, and online mechanisms. In *Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, page 434–443, 2007.
- [10] Moshe Babaioff, Michael Dinitz, Anupam Gupta, Nicole Immorlica, and Kunal Talwar. Secretary problems: weights and discounts. In *Proceedings of the twentieth annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1245–1254. SIAM, 2009.

- [11] Moshe Babaioff, Michal Feldman, Yannai A. Gonczarowski, Brendan Lucier, and Inbal Talgam-Cohen. Escaping cannibalization? correlation-robust pricing for a unit-demand buyer. In *Proceedings of the 21st ACM Conference on Economics and Computation*, page 191, 2020.
- [12] Maryam Bahrani, Hedyeh Beyhaghi, Sahil Singla, and S. Matthew Weinberg. Formal barriers to simple algorithms for the matroid secretary problem. In Michal Feldman, Hu Fu, and Inbal Talgam-Cohen, editors, Web and Internet Economics, pages 280–298, 2022.
- [13] MohammadHossein Bateni, Sina Dehghani, MohammadTaghi Hajiaghayi, and Saeed Seddighin. Revenue maximization for selling multiple correlated items. In *Algorithms-ESA 2015: 23rd Annual European Symposium, Patras, Greece, September 14-16, 2015, Proceedings*, pages 95–105. Springer, 2015.
- [14] Alok Baveja, Amit Chavan, Andrei Nikiforov, Aravind Srinivasan, and Pan Xu. Improved bounds in stochastic matching and optimization. *Algorithmica*, 80:3225–3252, 2018.
- [15] Curtis Bechtel and Shaddin Dughmi. Delegated stochastic probing. In 12th Innovations in Theoretical Computer Science Conference, ITCS 2021, January 6-8, 2021, Virtual Conference, volume 185, pages 37:1–37:19, 2021.
- [16] Curtis Bechtel, Shaddin Dughmi, and Neel Patel. Delegated pandora's box. In *Proceedings of the 23rd ACM Conference on Economics and Computation*, pages 666–693, 2022.
- [17] Xiaohui Bei, Nick Gravin, Pinyan Lu, and Zhihao Gavin Tang. Correlation-robust analysis of single item auction. In *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '19, page 193–208, USA, 2019. Society for Industrial and Applied Mathematics.
- [18] Yang Cai and Argyris Oikonomou. On simple mechanisms for dependent items. In *Proceedings* of the 22nd ACM Conference on Economics and Computation, EC '21, page 242–262, 2021.
- [19] Ioannis Caragiannis, Nick Gravin, Pinyan Lu, and Zihe Wang. Relaxing the independence assumption in sequential posted pricing, prophet inequality, and random bipartite matching. In Michal Feldman, Hu Fu, and Inbal Talgam-Cohen, editors, Web and Internet Economics, pages 131–148. Springer International Publishing, 2022.
- [20] J. Lawrence Carter and Mark N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979.
- [21] Shuchi Chawla, Jason D Hartline, David L Malec, and Balasubramanian Sivan. Multi-parameter mechanism design and sequential posted pricing. In *Proceedings of the 42nd Annual ACM Symposium on Theory of Computing (STOC)*, pages 311–320, 2010.
- [22] Chandra Chekuri, Jan Vondrák, and Rico Zenklusen. Multi-budgeted matchings and matroid intersection via dependent rounding. In *Proceedings of the 22nd Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1080–1097, 2011.
- [23] Chandra Chekuri, Jan Vondrák, and Rico Zenklusen. Submodular function maximization via the multilinear relaxation and contention resolution schemes. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 783–792, 2011.

- [24] Michael Dinitz. Recent advances on the matroid secretary problem. ACM SIGACT News, 44 (2):126–142, 2013.
- [25] Shaddin Dughmi. The outer limits of contention resolution on matroids and connections to the secretary problem. In 47th International Colloquium on Automata, Languages and Programming (ICALP), volume 168, pages 42:1–42:18, 2020.
- [26] Shaddin Dughmi. Matroid Secretary Is Equivalent to Contention Resolution. In 13th Innovations in Theoretical Computer Science Conference (ITCS), volume 215, pages 58:1–58:23, 2022.
- [27] Shaddin Dughmi, Yusuf Hakan Kalayci, and Neel Patel. On Sparsification of Stochastic Packing Problems. In 50th International Colloquium on Automata, Languages and Programming (ICALP), volume 261, pages 51:1–51:17, 2023.
- [28] Paul Dütting, Michal Feldman, Thomas Kesselheim, and Brendan Lucier. Prophet inequalities made easy: Stochastic optimization by pricing nonstochastic inputs. SIAM Journal on Computing (SICOMP), 49(3):540–582, 2020.
- [29] Tomer Ezra, Michal Feldman, Nick Gravin, and Zhihao Gavin Tang. Online stochastic maxweight matching: prophet inequality for vertex and edge arrival models. In *Proceedings of the 21st ACM Conference on Economics and Computation (EC)*, pages 769–787, 2020.
- [30] Moran Feldman, Ola Svensson, and Rico Zenklusen. Online contention resolution schemes. In *Proceedings of the 27th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1014–1033, 2016.
- [31] Nick Gravin and Pinyan Lu. Separation in correlation-robust monopolist problem with budget. In *Proceedings of the 2018 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 2069–2080, 2018.
- [32] Nikolai Gravin and Hongao Wang. Prophet inequality for bipartite matching: Merits of being simple and non adaptive. In *Proceedings of the 20th ACM Conference on Economics and Computation (EC)*, pages 93–109, 2019.
- [33] Anupam Gupta, Jinqiao Hu, and Roie Levin Gregory Kehne. Pairwise independent contention resolution. In *The 25th Conference on Integer Programming and Combinatorial Optimization (IPCO)*, 2024.
- [34] Jason D Hartline et al. Bayesian mechanism design. Foundations and Trends® in Theoretical Computer Science, 8(3):143–263, 2013.
- [35] Theodore P Hill and Robert P Kertz. A survey of prophet inequalities in optimal stopping theory. *Contemporary Mathematics*, 125:191–207, 1992.
- [36] Nicole Immorlica, Sahil Singla, and Bo Waggoner. Prophet inequalities with linear correlations and augmentations. In *Proceedings of the 21st ACM Conference on Economics and Computation*, pages 159–185, 2020.

- [37] Patrick Jaillet, José A Soto, and Rico Zenklusen. Advances on matroid secretary problems: Free order model and laminar case. In *The 14th Conference on Integer Programming and Combinatorial Optimization (IPCO)*, pages 254–265. Springer, 2013.
- [38] Joseph, Naor, Aravind Srinivasan, and David Wajc. Online dependent rounding schemes, 2023.
- [39] Howard Karloff and Yishay Mansour. On construction of k-wise independent random variables. In *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing*, page 564–573, 1994.
- [40] Jon Kleinberg and Robert Kleinberg. Delegated search approximates efficient search. In *Proceedings of the 2018 ACM Conference on Economics and Computation*, pages 287–302, 2018.
- [41] Robert Kleinberg and S Matthew Weinberg. Matroid prophet inequalities and applications to multi-dimensional mechanism design. *Games and Economic Behavior*, 113:97–115, 2019.
- [42] Euiwoong Lee and Sahil Singla. Optimal online contention resolution schemes via ex-ante prophet inequalities. In *Proceedings of the 26th Annual European Symposium on Algorithms* (ESA), 2018.
- [43] Michael Luby, Avi Wigderson, et al. Pairwise independence and derandomization. Foundations and Trends® in Theoretical Computer Science, 1(4):237–301, 2006.
- [44] J. Naor and M. Naor. Small-bias probability spaces: Efficient constructions and applications. In Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing, STOC '90, page 213–223, New York, NY, USA, 1990.
- [45] Pranav Nuti and Jan Vondrák. Towards an optimal contention resolution scheme for matchings. In *The 24th Conference on Integer Programming and Combinatorial Optimization (IPCO)*, volume 13904, pages 378–392. Springer, 2023.
- [46] James G Oxley. Matroid theory, volume 3. Oxford University Press, USA, 2006.
- [47] Do-Hyung Park, Jumin Lee, and Ingoo Han. The effect of on-line consumer reviews on consumer purchasing intention: The moderating role of involvement. *International Journal of Electronic Commerce*, 11(4):125–148, 2007.
- [48] Tristan Pollner, Mohammad Roghani, Amin Saberi, and David Wajc. Improved online contention resolution for matchings and applications to the gig economy. In *Proceedings of the 23rd ACM Conference on Economics and Computation*, pages 321–322, 2022.
- [49] Yosef Rinott and Ester Samuel-Cahn. Optimal stopping values and prophet inequalities for some dependent random variables. *Lecture Notes-Monograph Series*, 22:343–358, 1992.
- [50] Aviad Rubinstein and Sahil Singla. Combinatorial prophet inequalities. In Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, pages 1671–1687. SIAM, 2017.
- [51] José A Soto. Matroid secretary problem in the random-assignment model. SIAM Journal on Computing, 42(1):178–211, 2013.

- [52] Salil P. Vadhan. Pseudorandomness. Foundations and Trends® in Theoretical Computer Science, 7(1–3):1–336, 2012.
- [53] Mark N. Wegman and J. Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, 1981.
- [54] Dominic JA Welsh. *Matroid theory*. Courier Corporation, 2010.

A Missing Proofs from Section 4

Lemma 4.2. Let $R \in \mathbb{F}_q^{d \times m}$ be a uniformly random matrix with entries $r_{i,j} \sim \text{Unif } (0,1,\ldots,q-1)$. Then, for any m < d, we have $\Pr[\mathbf{Rank}(R) = m] \geq 1 - \frac{1}{q^{d-m}}$. In addition, for any $\Sigma \in \mathbb{F}_q^{m \times n}$ with distinct columns, the columns of $X = R\Sigma$ are distinct with probability $\geq 1 - \frac{1}{q^{d-m}}$.

Proof. The proof of this lemma proceeds via induction on m. The base case where m=1 is straightforward, as $\mathbf{Rank}(R) \geq 0$, which validates the claim. For the induction step, consider m>1, and let $R \in \mathbb{F}_q^{d \times m}$ be a matrix generated uniformly at random with column denoted by $\mathbf{r}_1, \dots \mathbf{r}_m$. Then, we have the following:

$$\begin{split} &\mathbf{Pr}[\mathbf{Rank}(R) = m] \\ &= \mathbf{Pr}[\mathbf{Rank}(\mathbf{r}_1, \dots \mathbf{r}_{m-1}) = m-1] \cdot \mathbf{Pr}[\mathbf{r_m} \notin \mathbf{Span}(\mathbf{r}_1, \dots \mathbf{r}_{m-1}) \mid \mathbf{Rank}(\mathbf{r}_1, \dots \mathbf{r}_{m-1}) = m-1] \\ &\geq \left(1 - \frac{1}{q^{d-m+1}}\right) \cdot \mathbf{Pr}[\mathbf{r_m} \notin \mathbf{Span}(\mathbf{r}_1, \dots \mathbf{r}_{m-1}) \mid \mathbf{Rank}(\mathbf{r}_1, \dots \mathbf{r}_{m-1}) = m-1] \\ &= \left(1 - \frac{1}{q^{d-m+1}}\right) \cdot \left(1 - \frac{1}{q^{d-m+1}}\right) \geq 1 - \frac{2}{q^{d-m+1}} \\ &\geq 1 - \frac{q}{q^{d-m+1}} = 1 - \frac{1}{q^{d-m}}. \end{split}$$

Above, the first inequality follows from the induction on m. The second equality holds since \mathbf{r}_m is a sampled independent of $\mathbf{r}_1, \dots, \mathbf{r}_{m-1}$ and uniformly from $\mathbb{F}_q^d \setminus \mathbf{Span}(\mathbf{r}_1, \dots, \mathbf{r}_{m-1})$ once conditioned on the event $\mathbf{r}_m \notin \mathbf{Span}(\mathbf{r}_1, \dots, \mathbf{r}_{m-1})$. Hence, $\mathbf{Pr}[\mathbf{r}_m \notin \mathbf{Span}(\mathbf{r}_1, \dots, \mathbf{r}_{m-1}) \mid \mathbf{Rank}(\mathbf{r}_1, \dots, \mathbf{r}_{m-1})] = \left(1 - \frac{1}{q^{d-m+1}}\right)$.

Lemma 4.3. Let $X \in \mathbb{F}_q^{d \times n}$ be a random matrix with pairwise independent column vectors $\mathbf{x}_1, \dots \mathbf{x}_n$ for some $n < q^d$ where each vector \mathbf{x}_i is distributed uniformly in \mathbb{F}_q^d . Then a random set $A \subseteq \mathbb{F}_q^d \times L$ generated by Procedure 1 given the inputs of X and $L = \{\ell_1, \dots \ell_n\}$ satisfies:

- (1) For any $\mathbf{v}^{\ell_i} \in \mathbb{F}_q^d \times L$, $\mathbf{Pr}[\mathbf{v}^{\ell_i} \in A] = \frac{1}{q^d}$.
- (2) For any two distinct \mathbf{v}^{ℓ_i} , $\mathbf{u}^{\ell_j} \in \mathbb{F}_q^d \times L$, the events $\{\mathbf{v}^{\ell_i} \in A\}$ and $\{\mathbf{u}^{\ell_j} \in A\}$ are independent.

Proof. First we fix any $\mathbf{v}^i \in \mathbb{F}_q^d \times [n]$. We can express,

$$\begin{aligned} \mathbf{Pr}[\mathbf{v}^{i} \in A] &= \left(1 - \frac{1}{q^{d}}\right) \cdot \mathbf{Pr}[\mathbf{v}^{i} \in A \mid A \sim \mathcal{D}_{1}] + \frac{1}{q^{d}} \cdot \mathbf{Pr}[\mathbf{v}^{i} \in A \mid A \sim \mathcal{D}_{2}] \\ &= \left(1 - \frac{1}{q^{d}}\right) \cdot \mathbf{Pr}[\mathbf{x}_{i} = \mathbf{v}] + \frac{1}{q^{d}} \cdot \frac{1}{q^{d}} \\ &= \left(1 - \frac{1}{q^{d}}\right) \cdot \frac{1}{q^{d}} + \frac{1}{q^{d}} \cdot \frac{1}{q^{d}} = \frac{1}{q^{d}}. \end{aligned}$$

Above the second equality follows from the definition of the distribution \mathcal{D}_1 and \mathcal{D}_2 . The second equality follows because each \mathbf{x}_i is sampled uniformly from \mathbb{F}_q^d . This concludes the proof of the first part of the lemma.

Next, we fix any two distinct elements $\mathbf{v}^i, \mathbf{u}^j \in \mathbb{F}_q^d$. We compute the joint probability of $\mathbf{Pr}[\mathbf{v}^i \in A \wedge \mathbf{u}^j \in A]$ for two cases separately. First, we consider the case when $i \neq j$. We have,

$$\begin{aligned} \mathbf{Pr}[\mathbf{v}^i \in A \wedge \mathbf{u}^j \in A] &= \left(1 - \frac{1}{q^d}\right) \cdot \mathbf{Pr}[\mathbf{v}^i \in A \wedge \mathbf{u}^j \in A \mid A \sim \mathcal{D}_1] + \frac{1}{q^d} \cdot \mathbf{Pr}[\mathbf{v}^i \in A \wedge \mathbf{u}^j \in A \mid A \sim \mathcal{D}_2] \\ &= \left(1 - \frac{1}{q^d}\right) \cdot \mathbf{Pr}[\mathbf{x}_i = \mathbf{v} \wedge \mathbf{x}_j = \mathbf{u}] + \frac{1}{q^d} \cdot \frac{1}{q^{2d}} \\ &= \left(1 - \frac{1}{q^d}\right) \cdot \frac{1}{q^{2d}} + \frac{1}{q^d} \cdot \frac{1}{q^{2d}} = \frac{1}{q^{2d}}. \end{aligned}$$

Above the second equality follows from the definition of the distribution \mathcal{D}_1 and \mathcal{D}_2 . The second equality follows because the ordered family of vectors $\mathbf{x}_1, \ldots, x_n$ are pairwise independent and $i \neq j$. Second, we consider the case when i = j. We have

$$\mathbf{Pr}[\mathbf{v}^{i} \in A \wedge \mathbf{u}^{i} \in A] = \left(1 - \frac{1}{q^{d}}\right) \cdot \mathbf{Pr}[\mathbf{v}^{i} \in A \wedge \mathbf{u}^{i} \in A \mid A \sim \mathcal{D}_{1}] + \frac{1}{q^{d}} \cdot \mathbf{Pr}[\mathbf{v}^{i} \in A \wedge \mathbf{u}^{i} \in A \mid A \sim \mathcal{D}_{2}]$$
$$= \frac{1}{q^{d}} \cdot \frac{1}{q^{d}} = \frac{1}{q^{2d}}.$$

Above the second equality follows from the definition of the distribution \mathcal{D}_1 and \mathcal{D}_2 . This concludes the proof of the lemma.