Separating the Communication Complexity of Truthful and Non-truthful Combinatorial Auctions*

Sepehr Assadi
Rutgers University
USA

Hrishikesh Khandeparkar
Princeton University
USA

Raghuvansh R. Saxena
Princeton University
USA

S. Matthew Weinberg
Princeton University
USA

ABSTRACT

We prove the first separation in the approximation guarantee achievable by truthful and non-truthful combinatorial auctions with polynomial communication. Specifically, we prove that any truthful auction guaranteeing a $(3/4 - 1/240 + \epsilon)$-approximation for two buyers with XOS valuations over m items requires $\exp(\Omega(\epsilon^2 \cdot m))$ communication whereas a non-truthful auction by Feige [*J. Comput.* 2009] is already known to achieve a $3/4$-approximation in $\text{poly}(m)$ communication.

We obtain our lower bound for truthful auctions by proving that any simultaneous auction (not necessarily truthful) which guarantees a $(3/4-1/240+\varepsilon)$-approximation requires communication $\exp(\Omega(\varepsilon^2 \cdot m))$, and then apply the taxation complexity framework of Dobzinski [FOCS 2016] to extend the lower bound to all truthful auctions (including interactive truthful auctions).

CCS CONCEPTS

• **Theory of computation → Algorithmic mechanism design**.

KEYWORDS

Combinatorial Auctions, Simultaneous Communication, Lower Bounds

ACM Reference Format:
Sepehr Assadi, Hrishikesh Khandeparkar, Raghuvansh R. Saxena, and S. Matthew Weinberg. 2020. Separating the Communication Complexity of Truthful and Non-truthful Combinatorial Auctions. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing (STOC '20), June 22–26, 2020, Chicago, IL, USA.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3357713.3384267

*Part of this work was done while the first author was a postdoctoral researcher at Princeton University and was supported in part by the Simons Collaboration on Algorithms and Geometry. The third author is supported by the National Science Foundation CAREER award CCF-1750443. The fourth author is supported by the National Science Foundation NSF CCF-1717899.

STOC '20, June 22–26, 2020, Chicago, IL, USA

ACM ISBN 978-1-4503-6979-4/20/06…$15.00
https://doi.org/10.1145/3357713.3384267

1 INTRODUCTION

Combinatorial auctions have been at the forefront of Algorithmic Game Theory since the field's inception, owing both to their rich algorithmic theory and their economic relevance. In a combinatorial auction, there are n bidders and a seller selling a set M of items. Each bidder i has a 'value' for all possible subsets of the items. These values are given by a valuation function $v_i : 2^M \to \mathbb{R}_+$. The seller's goal is to find a partition of the M items into disjoint sets $S_1, \cdots, S_n$ such that the *welfare*, $\sum_{i\in[n]} v_i(S_i)$, is maximized.

The main difficulty faced by the seller in computing this partition is the lack of knowledge of the bidders' valuation functions. Indeed, in a combinatorial auction, the seller needs to communicate with the bidders in order to obtain information about their valuation functions. The number of bits communicated between the seller and the bidders is called the communication complexity of the combinatorial auction, and is the main focus of this paper (and many prior works, *e.g.*, [LS05, NS06, Dob07, DN11, MSV08, Fei09, DNS10, KV12, Dob16a, BMW18, EFN+19, AS19])

The actual communication complexity of a combinatorial auction depends on whether the bidders are willing to report information about their valuation functions to the seller truthfully or not. If not, then, in order to compute anything meaningful, the seller needs to appropriately incentivize the bidders so that they report truthfully. When the bidders are incentivized to tell the truth, then the auction is said to be *truthful*. Observe that truthful auctions are at least as complex (require at least as much communication) as non-truthful (or general) auctions where the bidders always report truthfully (even without incentivization).

The main question we study in this paper is the following: Are there instances where truthful combinatorial auctions require strictly more communication than general auctions?

The VCG Mechanism: A Partial Answer. A partial answer to the above question is given by the VCG mechanism due to Vickrey [Vic61], Clarke [Cla71], and Groves [Gro73]. The VCG mechanism implies that if there is a general auction with polynomial (in $|M|$) communication that maximizes the welfare *exactly*, then, there is also a truthful mechanism with polynomial communication that does the same.

It turns out, that in most settings of interest, there are *no* general auctions with polynomial communication that provide the maximum possible welfare, and thus, the above result is vacuously true. Naturally, therefore, researchers turned their attention to auctions that *approximate* the optimal welfare, and studied the above question in this case. The VCG mechanism was powerful

enough to rule out some extreme cases (where the valuation functions may be arbitrary) of the approximation-version of the problem as well, and "VCG-based" schemes were used to show that general auctions require roughly the same amount of communication as truthful auctions [Rag88, LOS02, LS05, NS06] in these cases.

Other than these extreme cases, the problem remains wide open.

Beyond VCG: Gaps in Relevant Cases. As soon as one stops considering arbitrary valuation functions, and restricts attention to a subclass (say submodular, XOS, or subadditive), the state of affairs is drastically different. Not only are there huge gaps in the state of the art approximation guarantees provided by general and truthful auctions [Dob07, Fei09, DNS10, FV10, AS19], but, despite these huge gaps, there are no known (even small constant factor) separations between the approximation guarantees provided by general and truthful auctions.

Our main result provides the first such separation:

Main Result (Informal). *No poly-communication, deterministic truthful auction for two bidders with XOS valuations achieves an approximation guarantee better than $\frac{179}{240}$, whereas general deterministic auctions can do so.*

We note that the part of our main result that deals with general auctions is well known and due to [Fei09]. Our contribution is the lower bound for deterministic truthful auctions. In fact, our result generalizes and even covers randomized auctions, but we defer the formal statement to Theorem 3.12.

1.1 Other Related Work

Communication complexity separations. As mentioned above, there are no known separations between the approximation guarantees provided by general and truthful auctions. However, some limited results in this direction are known.

For example, due to works of [DN11, BDF+10, DSS15], we have a separation between general auctions and truthful "VCG-based" auctions when the valuation functions are from subclasses such as submodular, XOS, or subadditive. Recall that VCG-based auctions also show that there is no such separation from general valuation functions [Rag88, LOS02, LS05, NS06]. On similar lines, the work of [DN15] establishes that a separation between general and truthful "scalable" auctions when valuation functions are from a subclass called multi-unit valuations.

As both the above separations hold only for a subclass of truthful auctions, they are weaker than our unconditional separation. We note that the separation of [DN15] is also weaker as it only separate guarantees achievable with poly-logarithmic communication where as we separate guarantees achievable with polynomial communication.

Other complexity measures. We conclude this related work section with a brief overview of the line of work on the *computational complexity* of combinatorial auctions. In this setting, the resource of interest is the *running-time* of the bidders and the seller during the auction. The story here is similar. The VCG mechanism again shows that poly-time truthful auctions for the *optimal* welfare are as powerful as general auctions. Again, optimal welfare maximization is computationally hard except in very restricted settings and it makes sense to consider approximations. For approximate welfare maximization, just like before, VCG-based schemes show that truthful and general auctions are equally powerful for various 'extreme' cases [DNS10] (unless **P** = **NP**).

When it comes to approximate welfare maximization outside these extreme cases, there is an interesting distinction between the communication and computational complexity regimes. In the computational complexity model, a strong separation between truthful and general auctions is known when the valuation functions are submodular (unless **NP** $\subseteq$ **RP**). Details about this separation can be found in the line of work due to [Von08, MSV08, Dob11, DV11, DV12a, DV12b, DV16].

One can reasonably debate whether the computational or communication model is more relevant, but most researchers tend to view both models as extremely relevant (and the vast amount of prior work in both models supports this view). If anything, we argue that the communication model might be more relevant, owing to odd technicalities associated with evaluating 'demand queries' in 'posted-price auctions'. We refer the reader to [CTW20] or [BMW18] for a deeper comparison of the models, but will not further belabor this comparison and take the position that major open problems in both the communication and computational models are extremely relevant.

1.2 Our Techniques

Our main result is an exponential lower bound on the communication complexity of truthful auctions with two bidders and XOS valuation functions, and we use the framework proposed in the beautiful work of [Dob16b].

In [Dob16b], the authors show that for two bidders and XOS valuations, the existence of a truthful auction with polynomial communication implies the existence of a 'simultaneous' general auction with polynomial communication. An auction is called simultaneous if it involves the bidders sending exactly one message to the seller. Furthermore, the messages sent by the two bidders are not allowed to depend on each other. This is opposed to general auction where the the bidders may send messages to the seller across many rounds, where each message may depend on the messages in all the previous rounds.

This theorem of [Dob16b] constitutes the first step in our result, essentially converting the task of separating truthful auctions from general auctions to the task of separating simultaneous general auctions from general auctions. However, the latter task is still highly non-trivial, and as the work [BMW18] shows, there are provable barriers that such a separation must overcome.

Startlingly, we are able to turn some of the ideas used by [BMW18] to show these barriers into a construction that gets around the same barriers! At a super-high level, our actual construction maintains two copies of the construction of [BMW18] and argues about them simultaneously. A lot of new ideas are needed, as, in particular, simply maintaining two independent copies of the [BMW18] construction does not work, and these copies need to be suitably correlated. Furthermore, these correlations need to be precisely controlled, in order to deal with

the 'cross-terms' originating from having two copies. In fact, these cross-terms are the reason why the parameter $\frac{179}{240}$ that we obtain is slightly weaker than the one in [BMW18].

Describing all these additional ideas that go into our proof would require, at least, a detailed overview of the work of [BMW18], and we defer this to next section, where we give a step by step construction of our lower bound.

2 DETAILED PROOF SKETCH

Our main result is an exponential lower bound on the communication complexity of truthful auctions for two bidders with XOS valuations that achieve an approximation guarantee better than $\frac{179}{240}$. In this section, we gradually build various aspects of this lower bound highlighting the roles they play. It should be noted that the parameter $\frac{179}{240}$ is not critically important, only that $\frac{179}{240} < \frac{3}{4}$, as any number $< \frac{3}{4}$ suffices to separate truthful auctions from general auctions [Fei09].

In the rest of this text, we will use Alice and Bob to refer to the two bidders and denote by $m = |M|$, the number of items on sale. Often, we will refer to a subclass of XOS functions called binary XOS (or BXOS) functions. A valuation function v is called binary XOS if there exists a set $\mathcal{C} \subseteq 2^M$ of subsets of M such that for all subsets $S \subseteq M$, it holds that $v(S) = \max_{C \in \mathcal{C}} |C \cap S|$. The set $\mathcal{C}$ is called the set of clauses of v and each element $C \in \mathcal{C}$ is called a *clause*. We shall sometimes refer to v simply by its set of clauses.

As mentioned in subsection 1.2, using the framework of [Dob16b], to show our lower bound, it is sufficient to show the same lower bound for *simultaneous* (possibly non-truthful) auctions. In other words, it suffices to show that at the end of a simultaneous auction with less than exponential communication, the Seller cannot compute an allocation of items to Alice and Bob with welfare within a factor of $\frac{3}{4}$ of the optimal welfare.

2.1 The [BMW18] Construction

In the beautiful work of [BMW18], the authors consider the related question of *determining* the optimal welfare up to a factor of $\frac{3}{4}$. In general, for simultaneous auctions[1], the question of determining the optimal welfare is incomparable to the question of computing an allocation with welfare close to the optimal. Thus, [BMW18] does not directly imply anything about our problem. However, their construction does serve as a starting point for ours.

In the construction of [BMW18], the valuation functions of Alice and Bob are BXOS with exponentially many *regular* clauses but may or may not include one *special* clause. It holds that the union of a regular clause of Alice and a regular clause of Bob has size $< \frac{3}{4}m$ whereas the union of the special clause of Alice with the special clause of Bob has size m. This means that determining the optimal welfare up to a factor of $\frac{3}{4}$ amounts to determining whether or not Alice and Bob have the special clauses.

However, in the construction of [BMW18], the special clauses of Alice and Bob are indistinguishable from the regular clauses. Thus, determining whether or not one of their exponentially many clauses is special requires exponential communication and the desired lower bound follows.

[1] As is argued in [BMW18], this is true only for simultaneous auctions.

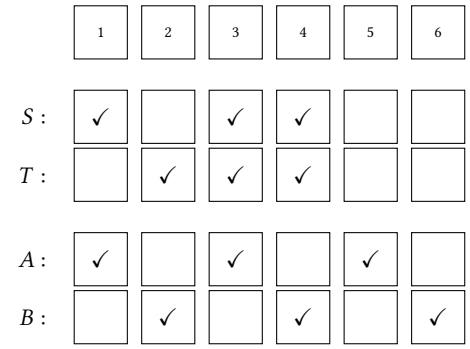

Figure 1: The construction of [BMW18]. Each of the numbers 1 to 6 represents a group of $\frac{m}{6}$ items.

The structure of the clauses in [BMW18]. We now describe how the clauses in [BMW18] are constructed more formally.

Call a pair of sets (S, T) a *basis* if the sets S and T are of size $\frac{m}{2}$ and their intersection is of size $\frac{m}{3}$. In [BMW18], a basis is sampled uniformly at random from all possible bases, and the set S is told to Alice and set T is told to Bob. We provide an illustration of a basis in Figure 1 where each of the six blocks in a row represents a group of $\frac{m}{6}$ items.

Next, Alice's regular clauses are constructed by uniformly sampling sets of size $\frac{m}{2}$ that intersect S in $\frac{m}{3}$ places and Bob's regular clauses are constructed by uniformly sampling sets of size $\frac{m}{2}$ that intersect T in $\frac{m}{3}$ places. Constructing the regular clauses this way satisfies the two main properties needed for the argument in [BMW18] to work:

- Firstly, it holds that the union of a regular clause of Alice and a regular clause of Bob has size strictly less than $\frac{3}{4}m$.
  We explain why. As all regular clauses have size $\frac{m}{2}$, it is equivalent to describe why the intersection of a regular clause of Alice and a regular clause of Bob has size strictly more than $\frac{m}{4}$. This is because if the sets S, T in the basis had an intersection of size $\frac{m}{4}$, the expected size of the intersection of two *independently* random sets of size $\frac{m}{2}$, then, as the regular clauses of Alice and Bob are chosen independently of each other, they will also behave like independently chosen random sets and have an intersection of size $\frac{m}{4}$ in expectation. In actuality, the sets S, T in the basis have an intersection of size $\frac{m}{3}$, more than the expected size of the intersection of two *independently* random sets of size $\frac{m}{2}$. Thus, the regular clauses of Alice and Bob also intersect more than random sets, *i.e.*, in more than $\frac{m}{4}$ places.
- Secondly, such a sampling procedure allows one to 'hide' a special clause inside the exponentially many regular clauses sampled by Alice and Bob.
  To see an illustration of how a special clause is hidden amongst the regular clauses, observe the rows corresponding to the special clauses A and B in Figure 1. The special clauses for Alice and Bob are disjoint and their union is of size m. Additionally, note that A intersects S in $\frac{m}{3}$ places and similarly B intersects T in $\frac{m}{3}$ places, just like all the other regular clauses. As the size of their intersections with S and

T (respectively) are the same, Alice and Bob cannot tell the special clauses (if they are present) apart from the regular clauses.

A small generalization. In the presented construction, we thought of each of the blocks from 1 to 6 in Figure 1 as representing a group of $\frac{m}{6}$ items. However, the exact same arguments (with numerically-different calculations) would also apply to any construction where blocks 1 and 2 represented u items, and blocks 3 through 6 represented v items (for any u, v).

With these additional parameters, it turns out (we omit the calculations), that the size of the intersection of a regular clause of Alice and a regular clause of Bob is:

$$\frac{2v^3 + 2u^2v + 3uv^2}{(u+2v)^3} \cdot m.$$

The expression above is maximized when $u = v$ (as observed in [BMW18]) but is strictly larger than $\frac{m}{4}$ for all u, v such that $u < 2v$ (to get intuition for the breakpoint: when $u = 2v$, $|S \cap T| = \frac{m}{4}$, and S, T behave like independently chosen sets). We will use this idea later in our construction.

2.2 From the Decision Problem to the Allocation Problem

The crucial difference between [BMW18] and our work is that [BMW18] show that the problem of 'deciding' whether or not the optimal welfare is close to m is hard while we wish to show that the problem of 'computing' an allocation with welfare close to the optimal is hard. As [BMW18] emphasize, these problems are incomparable for simultaneous auctions.

Our lower bound is based on the following approach of going from a lower bound for the decision problem to a lower bound for the computation/allocation problem: Consider two copies of the [BMW18] construction, where (a uniformly chosen) one is such that Alice and Bob have the special clauses and the other one is such that Alice and Bob do not have the special clauses. Suppose further that the Seller can only allocate items in one of the two copies.

We claim that the decision lower bound for [BMW18] implies an allocation lower bound for this system. Indeed, the optimal welfare of the copy with the special clauses is much larger than the optimal welfare of the copy without the special clauses. Thus, any allocation that allocates items in only one of the two copies and gets welfare close to optimal must allocate items in the copy with the special clause. But, this requires the Seller to at least determine which copy has the special clause, which is hard owing to [BMW18].

Cross-terms. It remains now to transform the system with two copies and a restriction on the Seller to only allocate items in one of the two copies to a standard unrestricted combinatorial auction. A first approach may be two have two bases (S^1, T^1) and (S^2, T^2) on the same set of items and give Alice and Bob regular clauses generated from both the bases together with a special clause from (a uniformly random) one of the bases.

One would then hope that just like the system described above, computing a good allocation for this system would require the Seller to implicitly determine which basis does the special clause come from, and maybe we can show that determining this is hard *a la* [BMW18].

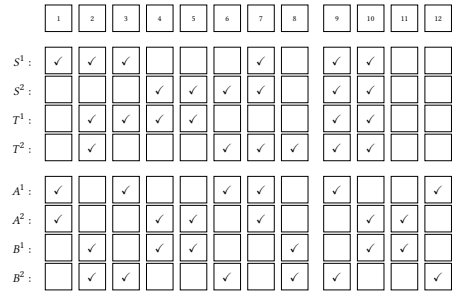

Figure 2: An illustration of two correlated bases. Each column denotes a group of $\frac{m}{12}$ items. This construction works even if columns 1 through 8 denote groups of u items, and columns 9 through 12 denote groups of v items, for any u, v (see subsection 2.3).

A little more thought reveals that this is not actually the case, and the reason is that having two bases on the same set of items gives rise to 'cross-terms'. Specifically, if we have two bases on the same set of items, then not only do we have to argue about the size of the union of regular clauses from basis 1 of Alice and regular clauses from basis 1 of Bob, but we also need to argue about the size of the union of regular clauses from basis 1 of Alice and regular clauses from basis 2 of Bob.

These additional unions, which we call the cross-terms, imply that the two bases must necessarily be correlated in order to avoid the issues described in subsection 2.1. Namely, if the two bases are independent, then S^1 and T^2 intersect in $\frac{m}{4}$ places in expectation (like sets of size $\frac{m}{2}$ chosen independently), implying in turn that the size of the union of regular clauses from basis 1 of Alice and regular clauses from basis 2 of Bob is $\frac{3}{4}m$ in expectation. This is too large for our lower bound, as we need the union to be of size strictly less than $\frac{3}{4}m$ in expectation.

2.3 Finding the Right Correlations

As motivated in the foregoing section, it is essential to have the two bases be suitably correlated to deal with the cross-terms. What is the right way to correlate these bases? It would be ideal if the cross terms coming from the 'cross-pairs' S^1, T^2 and S^2, T^1 behave exactly like the terms coming from two bases (S^1, T^1) and (S^2, T^2). If we can make this happen, then the argument that shows why the size of the union of regular clauses from basis 1 of Alice and regular clauses from basis 1 of Bob is $< \frac{3}{4}m$ would extend to also show that the size of the cross-terms is $< \frac{3}{4}m$.

In order to show that sets S^1, T^2 and S^2, T^1 behave like bases, we need to ensure that their intersections, namely $S^1 \cap T^2$ and $S^2 \cap T^1$ have size $\frac{m}{3}$, just like the intersections of two sets in a basis. Is it possible to have sets that behave in this way?

The answer turns out to be yes, and one such construction is described in Figure 2. In Figure 2, each of the 12 columns denotes a group of $\frac{m}{12}$ items, making a total of m items, and a ✓ in row S^1 and column 1 means that the first $\frac{m}{12}$ items are present in the set S^1. Importantly, note that the tuples (S^1, T^1) and (S^2, T^2) behave

like a [BMW18] basis, and have four columns in their intersection, amounting to $\frac{m}{3}$ items, and so do the cross-terms (S^1, T^2) and (S^2, T^1).

Thus, the construction in Figure 2 has fixed the issue with the cross-terms described in the foregoing section, but there is one more step needed to finish the proof.

Special cross-terms. Just like there are cross terms coming from regular clauses from basis 1 of Alice and regular clauses from basis 2 of Bob, there are also cross terms coming from regular clauses from basis 1 of Alice and *special* clauses from basis 2 of Bob (and vice-versa)[2].

Before we describe how we deal with these 'special cross-terms', we first need to define the special clauses in our system. We omit defining them precisely in this sketch but mention here that the fact that the special clauses need to be indistinguishable from the regular clauses impose a lot of constraints on their structure. In fact, the special clauses need to more or less look like the sets A^1, A^2, B^1, and B^2 in Figure 2, where again a ✓ in a given column indicates that the corresponding group of $\frac{m}{12}$ items is in the set.

With this definition of special clauses, one can calculate the expected intersection of the special cross terms and check if it is $> \frac{m}{4}$ or not. It turn out that with the construction in Figure 2, this size is exactly $\frac{m}{4}$ and work needs to be done to increase it. It is here that we use the generalization of [BMW18] given in subsection 2.1, and let the blocks of items have unequal size. We'll assume that the first 8 columns in Figure 2 denote groups of u items each, and the last 4 columns denote groups of v items each. For general u, v, the intersection of the regular cross terms has size:

$$\frac{5u^2v + u^3 + 6uv^2 + 2v^3}{2(u+2v)^2(2u+v)} \cdot m.$$

On the other hand, the intersection of a special cross terms has size:

$$\frac{16uv + 5u^2 + 6v^2}{12(u+2v)(2u+v)} \cdot m.$$

In fact, the parameter governing our lower bound is the minimum of the two expressions above, and this is maximized when $\frac{v}{u} = 1 + \sqrt{\frac{3}{2}}$. For simplicity sake, we present our main results assuming $\frac{v}{u} = 2$ when the minimum of the two expressions above is $\frac{61m}{240} > \frac{m}{4}$. The value $\frac{61m}{240}$ corresponds to the the parameter $\frac{179}{240}$ in our main result.

3 MODELS AND PRELIMINARIES

All logarithms are to the base 2, unless noted otherwise. We shall denote sequences with a $\vec{}$ on top, *e.g.*, $\vec{S}$. We shall use $\vec{S} \| \vec{S'}$ to denote the concatenation of the sequences $\vec{S}$ and $\vec{S'}$. Similarly, we shall use $\vec{S} \| S''$ to denote the sequence formed by appending the single element S'' to the sequence $\vec{S}$. Let $k > 0$ and $\vec{S} = S_1, S_2, \cdots, S_k$ be a sequence of k sets. For a function f defined on sets, we shall use $f(\vec{S})$ to denote the sequence $f(S_1), \cdots, f(S_k)$. Thus, $|\vec{S}|$ shall denote the sequence $|S_1|, \cdots, |S_k|$ and $\vec{S} \cap A$, for a set A, shall denote the sequence $S_1 \cap A, \cdots, S_k \cap A$, *etc.*

[2]We do not have to deal with cross terms coming from special clauses from basis 1 of Alice and special clauses from basis 2 of Bob as only one of the bases will have a special clause in our construction.

We will use $\mathbb{Z}$ to denote the set of integers and $\mathbb{R}$ to denote the set of all real numbers. We also define $\mathbb{R}_+$ to denote the set of all non-negative real numbers. If S is a set, then 2^S will denote the power set, *i.e.*, the set of all subsets, of S. Additionally, we shall denote using S^* the set $\cup_{i \geq 0} S^i$, where S^i, for $i > 0$, is the set of all strings of length i that can be formed with elements of S, and S^0 is the set containing only ε, the empty string. The length of a string σ will be denoted using $\mathsf{len}(\sigma)$, *e.g.*, $\mathsf{len}(\varepsilon) = 0$.

Let $t \geq 1$ be an integer. We define $[t] = \{1, \cdots, t\}$. For a tuple $X = (X_1, \cdots, X_t)$ and integer $i \in [t]$, we define $X_{<i} = (X_1, \cdots, X_{i-1})$ and $X_{-i} = (X_1, \cdots, X_{i-1}, X_{i+1}, \cdots, X_t)$.

We will use $\mathcal{U}(S)$ to denote the uniform distribution over a finite set S. If X is a random variable, then $\mathsf{dist}(X)$ will denote the distribution of the values taken by X.

Concentration inequalities. We use the following version of Chernoff bound for negatively correlated random variables:

Definition 3.1 (Negatively Correlated Random Variables). *For $n > 0$, let $X_1, \cdots, X_n$ be random variables that take values in $\{0, 1\}$. We say that the random variables $X_1, \cdots, X_n$ are negatively correlated if for all subsets $S \subseteq [n]$, we have $\Pr(\forall i \in S : X_i = 1) \leq \prod_{i \in S} \Pr(X_i = 1)$.*

Lemma 3.2 (Generalized Chernoff Bound; cf. [PS97]). *For $n > 0$, let $X_1, \cdots, X_n$ be negatively correlated random variables that take values in $\{0, 1\}$. Then, for any $\epsilon > 0$, we have (where $\mu = \sum_{i \in [n]} \mathbb{E}[X_i] \leq n$):*

$$\Pr\left(\sum_{i \in [n]} X_i > \mu + \epsilon n\right) \leq \Pr\left(\sum_{i \in [n]} X_i > (1+\epsilon) \cdot \mu\right) \leq \exp(-\varepsilon^2 \cdot \sum_{i \in [n]} \mu/3).$$

3.1 Tools from Information Theory

This section includes a very brief summary of the tools from information theory that we use in this paper. We refer the interested reader to the text by Cover and Thomas [CT06] for an excellent introduction to this field.

3.1.1 Entropy and Mutual Information.

Definition 3.3 (Entropy). *The Shannon Entropy of a discrete random variable X is defined as*

$$\mathbb{H}(X) = \sum_{x \in \mathsf{supp}(X)} \Pr(X = x) \log \frac{1}{\Pr(X = x)},$$

where $\mathsf{supp}(X)$ is the set of all values X can take and $0 \log \frac{1}{0} = 0$ by convention.

Definition 3.4 (Conditional Entropy). *Let X and Y be discrete random variables. The entropy of X conditioned on Y is defined as*

$$\mathbb{H}(X \mid Y) = \mathop{\mathbb{E}}_{y \sim \mathsf{dist}(Y)} \left[\mathbb{H}(X \mid Y = y)\right].$$

Definition 3.5 (Mutual Information). *Let X, Y, and Z be discrete random variables. The mutual information between X and Y is defined as*

$$\mathbb{I}(X; Y) = \mathbb{H}(X) - \mathbb{H}(X \mid Y).$$

The conditional mutual information between X and Y conditioned on Z is defined as:

$$\mathbb{I}(X;Y \mid Z) = \mathbb{H}(X \mid Z) - \mathbb{H}(X \mid YZ).$$

We note that mutual information is symmetric in X and Y, *i.e.* $\mathbb{I}(Y;X \mid Z) = \mathbb{I}(X;Y \mid Z)$ and $\mathbb{I}(X;Y) = \mathbb{I}(Y;X)$.

Fact 3.6. *The following holds for discrete random variables W, X, Y, Z:*

1. *We have $\mathbb{H}(XY) = \mathbb{H}(X) + \mathbb{H}(Y \mid X) \leq \mathbb{H}(X) + \mathbb{H}(Y)$. Equality holds if X and Y are independent.*
2. *If the random variable X takes values in the set Ω, it holds that $0 \leq \mathbb{H}(X) \leq \log|\Omega|$.*
3. *We have $0 \leq \mathbb{I}(X;Y \mid Z) \leq \mathbb{H}(X)$ and $\mathbb{I}(X;Y \mid Z) = 0$ if and only if X is independent of Y given Z.*
4. *If A, B, C, D are random variables, then*
$$\mathbb{I}(WX;Y \mid Z) = \mathbb{I}(W;Y \mid Z) + \mathbb{I}(X;Y \mid WZ).$$

We also use the following technical lemmas about mutual information.

Lemma 3.7. *For discrete random variables W, X, Y, and Z, we have*

$$\max(\mathbb{I}(W;X \mid YZ), \mathbb{I}(Y;X \mid Z)) \leq \mathbb{I}(W;X \mid Z) + \mathbb{I}(Y;X \mid WZ).$$

Proof. Observe that:

$$\begin{aligned}\max(\mathbb{I}(W;X \mid YZ), \mathbb{I}(Y;X \mid Z)) &\leq \mathbb{I}(W;X \mid YZ) + \mathbb{I}(Y;X \mid Z) \\ &\qquad \text{(item 3, Fact 3.6)} \\ &= \mathbb{I}(WY;X \mid Z) \quad \text{(item 4, Fact 3.6)} \\ &= \mathbb{I}(W;X \mid Z) + \mathbb{I}(Y;X \mid WZ). \\ &\qquad \text{(item 4, Fact 3.6)}\end{aligned}$$

□

Lemma 3.8. *Let $n > 0$ and $X = X_1, X_2, \cdots, X_n$ where $X_1, X_2, \cdots, X_n$ are independent and identically distributed discrete random variables. Let I be a random variable distributed uniformly over $[n]$. For all discrete random variables Y such that X is independent of Y and I is independent of (X, Y) and all functions f, we have:*

$$\mathbb{I}(X_I; f(X,Y) \mid Y, I) \leq \frac{1}{n} \cdot \mathbb{I}(X; f(X,Y) \mid Y).$$

Proof. The proof of this lemma can be found in the full version. □

3.1.2 Measures of Distance Between Distributions. We use two main measures of distance (or divergence) between distributions, namely the Kullback-Leibler divergence (KL-divergence) and the total variation distance.

Definition 3.9 (KL-divergence). *For two distributions μ and ν over the same set Ω, the Kullback-Leibler divergence between μ and ν, denoted by $\mathbb{D}(\mu \mid\mid \nu)$, is defined as*

$$\mathbb{D}(\mu \mid\mid \nu) = \sum_{x \in \Omega} \mu(x) \log \frac{\mu(x)}{\nu(x)}.$$

Definition 3.10 (Total Variation Distance). *For two distributions μ and ν over the same set Ω, the total variation distance μ and ν is defined as*

$$\|\mu - \nu\|_{tvd} := \max_{\Omega' \subseteq \Omega} \sum_{x \in \Omega'} \mu(x) - \nu(x).$$

These definitions satisfy the following properties:

Fact 3.11. *The following hold:*

1. *For discrete random variables X, Y, and Z, we have*

$$\mathbb{I}(X;Y \mid Z) = \mathop{\mathbb{E}}_{(y,z) \sim \text{dist}((Y,Z))} \left[\mathbb{D}(\text{dist}(X \mid Y = y, Z = z) \mid\mid \text{dist}(X \mid Z = z))\right].$$

2. (Pinsker's inequality) *For any distributions μ and ν, we have* $\|\mu - \nu\|_{tvd} \leq \sqrt{\frac{1}{2} \cdot \mathbb{D}(\mu \mid\mid \nu)}$.

3.2 Combinatorial Auctions

We now formally define the setting of two player combinatorial auctions. Let $m > 0$ and $\mathcal{V}$ be a non-empty set of functions from $2^{[m]}$ to $\mathbb{R}$. A deterministic, m-item, $\mathcal{V}$-combinatorial auction Π with two bidders and one seller is defined by five functions $\Pi = (f^{\mathsf{A}}, f^{\mathsf{B}}, f^{\mathsf{S}}, \text{alloc}, \text{price})$, of types

$$\begin{aligned} f^{\mathsf{A}}, f^{\mathsf{B}} &: \mathcal{V} \times (\{0,1\}^*)^* \to \{0,1\}^*, \\ f^{\mathsf{S}} &: (\{0,1\}^*)^* \times (\{0,1\}^*)^* \to (\{0,1\}^* \times \{0,1\}^*) \cup \{(\perp, \perp)\}, \\ \text{alloc} &: (\{0,1\}^*)^* \times (\{0,1\}^*)^* \to 2^{[m]} \times 2^{[m]}, \\ \text{price} &: (\{0,1\}^*)^* \times (\{0,1\}^*)^* \to \mathbb{R} \times \mathbb{R}, \end{aligned}$$

where $\perp$ is a special symbol. Furthermore, we require that, for any input to the function alloc, the pair of sets output by alloc are disjoint.

Observe that the output of functions $f^{\mathsf{S}}, \text{alloc}, \text{price}$ is a pair. We shall use $f^{\mathsf{S}\to\mathsf{A}}$ (respectively, $f^{\mathsf{S}\to\mathsf{B}}$) to denote the function, that on every input, outputs the first (resp. second) element in the pair output by f^{S} on the same input. We define the functions $\text{alloc}^{\mathsf{A}}, \text{alloc}^{\mathsf{B}}, \text{price}^{\mathsf{A}}, \text{price}^{\mathsf{B}}$ analogously.

We define a randomized auction to be a distribution over deterministic auctions.

Execution of an auction. A deterministic, m-item, $\mathcal{V}$-combinatorial auction $\Pi = (f^{\mathsf{A}}, f^{\mathsf{B}}, f^{\mathsf{S}}, \text{alloc}, \text{price})$ takes place as follows: At the beginning of the auction, the Seller has m items for sale and Alice and Bob have functions $v^{\mathsf{A}} \in \mathcal{V}$ and $v^{\mathsf{B}} \in \mathcal{V}$ respectively as input. The auction takes place in multiple rounds, where before round i, for $i > 0$, it holds that Alice has received a transcript $\sigma^{\mathsf{A}}_{<i} \in (\{0,1\}^*)^{i-1}$ from the Seller, Bob has received a transcript $\sigma^{\mathsf{B}}_{<i} \in (\{0,1\}^*)^{i-1}$ from the Seller, and the Seller has received transcripts $\sigma^{\mathsf{A}\to\mathsf{S}}_{<i}, \sigma^{\mathsf{B}\to\mathsf{S}}_{<i} \in (\{0,1\}^*)^{i-1}$ from Alice, Bob respectively.

In round i, Alice and Bob send messages $\sigma^{\mathsf{A}\to\mathsf{S}}_i = f^{\mathsf{A}}(v^{\mathsf{A}}, \sigma^{\mathsf{A}}_{<i})$ and $\sigma^{\mathsf{B}\to\mathsf{S}}_i = f^{\mathsf{B}}(v^{\mathsf{B}}, \sigma^{\mathsf{B}}_{<i})$ to the Seller respectively. The Seller appends these to the transcripts $\sigma^{\mathsf{A}\to\mathsf{S}}_{<i}, \sigma^{\mathsf{B}\to\mathsf{S}}_{<i}$ respectively to get transcripts $\sigma^{\mathsf{A}\to\mathsf{S}}_{\leq i}, \sigma^{\mathsf{B}\to\mathsf{S}}_{\leq i} \in (\{0,1\}^*)^i$ (respectively). Thereafter, the seller sends a message $\sigma^{\mathsf{A}}_i = f^{\mathsf{S}\to\mathsf{A}}(\sigma^{\mathsf{A}\to\mathsf{S}}_{\leq i}, \sigma^{\mathsf{B}\to\mathsf{S}}_{\leq i})$ to Alice and a message $\sigma^{\mathsf{B}}_i = f^{\mathsf{S}\to\mathsf{B}}(\sigma^{\mathsf{A}\to\mathsf{S}}_{\leq i}, \sigma^{\mathsf{B}\to\mathsf{S}}_{\leq i})$ to Bob.

If $(\sigma^{\mathsf{A}}_i, \sigma^{\mathsf{B}}_i) \neq (\perp, \perp)$, then Alice (resp. Bob) append σ^{A}_i to $\sigma^{\mathsf{A}}_{<i}$ (resp. $\sigma^{\mathsf{B}}_{<i}$) to get transcript $\sigma^{\mathsf{A}}_{\leq i}$ (resp. $\sigma^{\mathsf{B}}_{\leq i}$) and continue round $i+1$ of the auction. On the other hand, if $(\sigma^{\mathsf{A}}_i, \sigma^{\mathsf{B}}_i) = (\perp, \perp)$, then the auction *terminates* after round i and no further communication

takes place. The Seller outputs an allocation $(O^A, O^B) = \text{alloc}(\sigma^{A\to S}_{\le i}, \sigma^{B\to S}_{\le i})$, and prices $(p^A, p^B) = \text{price}(\sigma^{A\to S}_{\le i}, \sigma^{B\to S}_{\le i})$.

Observe that, if Π is deterministic, then, the values of (O^A, O^B) and (p^A, p^B) are completely determined by Π and the inputs v^A, v^B to Alice and Bob respectively. We sometimes denote these values by $(O^A, O^B) = \text{alloc}_\Pi(v^A, v^B)$ and $(p^A, p^B) = \text{price}_\Pi(v^A, v^B)$. We will also use the shorthand $O^A = \text{alloc}^A_\Pi(v^A, v^B)$, *etc.*

Relevant properties of an auction. In this paper, we will only consider the following parameters of an auction:

- **Rounds:** For a deterministic auction Π, and $v^A, v^B \in \mathcal{V}$, define $R_\Pi(v^A, v^B) = R$ if the execution of Π when Alice and Bob have inputs v^A, v^B respectively terminates after round R. If the execution does not terminate at all, then we define $R_\Pi(v^A, v^B) = \infty$.
  We say that Π has R rounds if, for all $v^A, v^B \in \mathcal{V}$, we have $R_\Pi(v^A, v^B) = R$. A randomized auction has R rounds if all the deterministic auctions in its support have R rounds. If a deterministic or randomized auction has exactly 1 round, then, we say that the auction is *simultaneous*.
- **Communication complexity:** For a deterministic auction Π, and $v^A, v^B \in \mathcal{V}$, we define $\text{CC}_\Pi(v^A, v^B) = \infty$ if $R_\Pi(v^A, v^B) = \infty$. On the other hand, if $R_\Pi(v^A, v^B) = R < \infty$, then we define
$$\text{CC}_\Pi(v^A, v^B) = \sum_{i\le R} \text{len}(\sigma_i^{A\to S}) + \text{len}(\sigma_i^{B\to S}) + \sum_{i<R} \text{len}(\sigma_i^A) + \text{len}(\sigma_i^B).$$
  In the above equation, the values $\sigma_i^{A\to S}$, $\sigma_i^{B\to S}$, *etc.* denote the corresponding values in an execution of Π when Alice has input v^A and Bob has input v^B. These values are well defined as Π is deterministic.
  We define $\text{CC}(\Pi) = \max_{v^A, v^B \in \mathcal{V}} \text{CC}_\Pi(v^A, v^B)$. Finally we define $\text{CC}(\Pi')$, for a randomized auction Π' to be the largest value of $\text{CC}(\Pi)$ for all deterministic auctions Π in its support.
- **Truthfulness:** We say that a deterministic auction Π is truthful if for all $v^A, v^B, v' \in \mathcal{V}$, we have
$$v^A(\text{alloc}^A_\Pi(v^A, v^B)) - \text{price}^A_\Pi(v^A, v^B) \ge v^A(\text{alloc}^A_\Pi(v', v^B)) - \text{price}^A_\Pi(v', v^B)$$
$$v^B(\text{alloc}^B_\Pi(v^A, v^B)) - \text{price}^B_\Pi(v^A, v^B) \ge v^B(\text{alloc}^B_\Pi(v^A, v')) - \text{price}^B_\Pi(v^A, v')$$
  We say that randomized auction is *truthful* if all the deterministic auction in its support are truthful.
- **Approximation guarantee:** For $m, \mathcal{V}$ as above and $v^A, v^B \in \mathcal{V}$, define the function $\text{opt}(v^A, v^B) = \max_{S^A, S^B \subseteq [m]: S^A \cap S^B = \emptyset} v^A(S^A) + v^B(S^B)$. Let ν be a distribution over pairs drawn from $\mathcal{V}$ and $\alpha, p > 0$. We say that a deterministic auction Π is α-approximate over ν with probability p if we have
$$\Pr_{(v^A, v^B)\sim\nu} \left(v^A(\text{alloc}^A_\Pi(v^A, v^B)) + v^B(\text{alloc}^B_\Pi(v^A, v^B)) > \alpha \cdot \text{opt}(v^A, v^B) \right) \ge p.$$
  On the other hand, we say that a randomized auction Π' is α-approximate with probability p if for all $v^A, v^B \in \mathcal{V}$, we have:
$$\Pr_{\Pi} \left(v^A(\text{alloc}^A_\Pi(v^A, v^B)) + v^B(\text{alloc}^B_\Pi(v^A, v^B)) > \alpha \cdot \text{opt}(v^A, v^B) \right) \ge p,$$
  where the probability is over all deterministic auctions Π in the support of Π'.

3.3 The Formal Statement of Our Main Result

We now formalize our main result. For $m > 0$, let $\texttt{BXOS}_m$ be the class of all functions $v : 2^{[m]} \to \mathbb{R}$ such that for some set of sets $C \subseteq 2^{[m]}$, it holds that, for all $S \in 2^{[m]}$, we have $v(S) = \max_{C\in C}\{|S \cap C|\}$. Also, define $\texttt{XOS}_m \supseteq \texttt{BXOS}_m$ to be the class of all functions $v : 2^{[m]} \to \mathbb{R}$ such that for a subset $C \subseteq \mathbb{R}^m_+$, it holds that, for all $S \in 2^{[m]}$, we have $v(S) = \max_{c\in C}\{\sum_{i\in S} c_i\}$.

Theorem 3.12 (Main Result). *There exists a constant $\beta > 0$ such that for all $\epsilon > 0$, there is a constant $m_0 > 0$ satisfying the following: For all $m > m_0$, any randomized, m-item, $\texttt{XOS}_m$-combinatorial auction Π with two bidders and one seller that is truthful and $\left(\frac{3}{4} - \frac{1}{240} + \epsilon\right)$-approximate with probability $\frac{1}{2} + \exp(-\beta\epsilon^2 \cdot m)$ satisfies*
$$\text{CC}(\Pi) \ge \exp(\beta\epsilon^2 \cdot m).$$

To show Theorem 3.12, we use the framework due to [Dob16b]. Formally, we use the following theorem from [Dob16b].

Theorem 3.13 ([Dob16b]). *There exists a polynomial $P(\cdot)$ such that for all $m, p, \alpha > 0$ and all randomized, m-item, $\texttt{XOS}_m$-combinatorial auction Π with two bidders and one seller that is truthful and α-approximate with probability p, there is a randomized, m-item, $\texttt{XOS}_m$-combinatorial auction Π' with two bidders and one seller that is simultaneous and α-approximate with probability p, and satisfies $\text{CC}(\Pi') \le P(\max(\text{CC}(\Pi), m))$.*

It follows from Theorem 3.13 that the following theorem implies Theorem 3.12. We include a proof below for completeness.

Theorem 3.14. *For all $\epsilon > 0$, and all $m > \frac{10^{10}}{\epsilon^2}$, any randomized, m-item, $\texttt{BXOS}_m$-combinatorial auction Π with two bidders and one seller that is simultaneous and $\left(\frac{3}{4} - \frac{1}{240} + \epsilon\right)$-approximate with probability $\frac{1}{2} + \exp\left(-\frac{\epsilon^2 m}{500}\right)$ satisfies*
$$\text{CC}(\Pi) \ge \exp\left(\frac{\epsilon^2 m}{500}\right).$$

Proof of Theorem 3.12 assuming Theorem 3.14. Proof by contradiction. Suppose that Theorem 3.14 is true and Theorem 3.12 is not. Let $P(\cdot)$ be the polynomial promised by Theorem 3.13 and let d be the degree of P. Define $\beta = \frac{1}{500(d+1)}$. Let $\epsilon_\star > 0$ be the constant promised by the negation of Theorem 3.12 for this value of β (recall that we assume that Theorem 3.12 is false). Let m_1 to be large enough so that (1) $P(m') \le m'^{d+1}$ for all $m' > m_1$, (2) $\exp(\beta\epsilon_\star^2 \cdot m') \ge m'$ for all $m' > m_1$, (3) $m_1 > \frac{10^{10}}{\epsilon_\star^2}$.

Using our assumption that Theorem 3.12 is false, we get that there is an $m > m_1$, and a randomized, m-item, $\texttt{XOS}_m$-combinatorial auction Π with two bidders and one seller that is truthful, is $\left(\frac{3}{4} - \frac{1}{240} + \epsilon_\star\right)$-approximate with probability $\frac{1}{2} + \exp(-\beta\epsilon_\star^2 \cdot m)$, and satisfies $\text{CC}(\Pi) < \exp(\beta\epsilon_\star^2 \cdot m)$.

Plugging Π into Theorem 3.13, we get a randomized, m-item, $\texttt{XOS}_m$-combinatorial auction Π' with two bidders and one seller that

is simultaneous and $\left(\frac{3}{4} - \frac{1}{240} + \epsilon_\star\right)$-approximate with probability $\frac{1}{2} + \exp(-\beta\epsilon_\star^2 \cdot m) > \frac{1}{2} + \exp\left(-\frac{\epsilon_\star^2 m}{500}\right)$ and satisfies (using $m > m_1$)

$$\mathrm{CC}(\Pi') < P(\max(\exp(\beta\epsilon_\star^2 \cdot m), m)) \leq \exp\left(\frac{\epsilon_\star^2 m}{500}\right).$$

This contradicts Theorem 3.14 and we are done. □

The rest of this paper is devoted to showing the lower bound in Theorem 3.14. By Yao's minimax principle, in order to a lower bound $\mathrm{CC}(\Pi)$ for randomized m-item simultaneous auctions Π that are α-approximate with probability p (for some m, α, p), it is sufficient to show a distribution ν over pairs of functions in $\mathtt{BXOS}_m$, such that all deterministic simultaneous auctions Π' that are α-approximate over ν with probability p have large $\mathrm{CC}(\Pi')$. We construct ν in section 4 and analyze it in section 5.

4 OUR CONSTRUCTION

For the purposes of this section, we fix $m > 0$. We denote the set $[m]$ using the letter M. If S is a subset of M, then we use $\overline{S}$ to denote $M \setminus S$, *i.e.*, the set of items in M that are *not* in S.

We give a formal definition of our lower bound instance.

In our proof below, we omit the proof of some of the lemmas. The interested reader can find them in the full version of our paper.

4.1 Partitions

Let $k > 0$. We say that a sequence $\vec{P} = P_1, P_2, \cdots, P_k$ of subsets of M forms a partition of M into k sets if the sets $P_1, \cdots, P_k$ are pairwise disjoint and their union is M. Formally, it should hold that $P_i \cap P_j = \emptyset$ for all $i \neq j \in [k]$ and $\cup_{i\in[k]} P_i = M$. For a partition $\vec{P} = P_1, P_2, \cdots, P_k$ of M into k sets, and an element $z \in M$, we define $\vec{P}[z]$ to be the unique $i \in [k]$ such that $z \in P_i$. Observe that our definition of a partition above ensures that $\vec{P}[z]$ is well-defined for all z.

Definition 4.1. *We say that a tuple $(k, \vec{P}, \vec{p})$ is a partition parameter if $k > 0$, $\vec{P} = P_1, \cdots, P_k$ is a partition of M into k sets, and $\vec{p} = p_1, p_2, \cdots, p_k$ is a sequence of integers satisfying $0 \leq p_i \leq |P_i|$ for all $i \in [k]$.*

For a partition parameter $(k, \vec{P}, \vec{p})$, we define $\mathrm{PC}(k, \vec{P}, \vec{p})$ to be the uniform distribution over all sets U satisfying

$$|\vec{P} \cap U| = \vec{p}.$$

Furthermore, define $\text{PC-ally}(k, \vec{P}, \vec{p})$ to be the distribution over subsets of M such that we have $\Pr_{U\sim\text{PC-ally}(D)}(z \in U) = \frac{p_{\vec{P}[z]}}{|\vec{P}_{\vec{P}[z]}|}$ independently for all $z \in M$.

We will need the following technical lemmas about partition parameters

Lemma 4.2. *For any subset $S \subseteq M$ and any partition parameter $(k, \vec{P}, \vec{p})$, it holds that*

$$\Pr_{U\sim\mathrm{PC}(k,\vec{P},\vec{p})}(U \cap S = \emptyset) \leq \Pr_{U\sim\text{PC-ally}(k,\vec{P},\vec{p})}(U \cap S = \emptyset).$$

Corollary 4.3. *For any partition parameter $(k, \vec{P}, \vec{p})$ and any distribution D^* over subsets of M, it holds that*

$$\Pr_{\substack{U\sim\mathrm{PC}(k,\vec{P},\vec{p})\\ U^*\sim D^*}}(U \cap U^* = \emptyset) \leq \Pr_{\substack{U\sim\text{PC-ally}(k,\vec{P},\vec{p})\\ U^*\sim D^*}}(U \cap U^* = \emptyset).$$

Lemma 4.4. *For any partition parameters $(k, \vec{P}, \vec{p})$ and $(k', \vec{P'}, \vec{p'})$, it holds for all $\epsilon > 0$ that*

$$\Pr_{\substack{U\sim\mathrm{PC}(k,\vec{P},\vec{p})\\ U'\sim\mathrm{PC}(k',\vec{P'},\vec{p'})}}(|U \cap U'| < \Delta - \epsilon m) \leq \exp(-\epsilon^2(m-\Delta)/3),$$

where

$$\Delta = \sum_{i\in[k]:|P_i|>0} \sum_{i'\in[k']:|P'_{i'}|>0} p_i p'_{i'} \frac{|P_i \cap P'_{i'}|}{|P_i| \cdot |P'_{i'}|}.$$

4.2 The Function Part

Let $k > 0$. For any sequence $\vec{S} = S_1, \cdots, S_k$ of k subsets of M and any sequence $\vec{b} = b_1, \cdots, b_k$ of bits, we define the set

$$\mathrm{Part}_{\vec{S}}(\vec{b}) = \{z \in M \mid \forall i \in [k] : \mathbf{1}(z \in S_i) = b_i\}.$$

We use $\mathrm{Part}_{\vec{S}}$ to denote the sequence of sets $\{\mathrm{Part}_{\vec{S}}(\vec{b})\}_{\vec{b}\in\{0,1\}^k}$ ordered lexicographically according to $\vec{b}$. Observe that the sequence $\mathrm{Part}_{\vec{S}}$ forms a partition of M into 2^k sets. We will need the following result about Part.

Lemma 4.5. *Let $k, k_1, k_2 > 0$ and consider $\vec{a}_j \in \mathbb{Z}^{2^{k+k_j}}$ for $j \in \{1, 2\}$. Let $\vec{S}$ be a sequence of k subsets of M. For $j \in \{1, 2\}$, define μ_j to be the uniform distribution over all sequences $\vec{S}_j$ of k_j subsets of M satisfying $|\mathrm{Part}_{\vec{S}\|\vec{S}_j}| = \vec{a}_j$.*

For any $\vec{a} \in \mathbb{Z}^{2^{k+k_1+k_2}}$ such that $\Pr_{\vec{S}_1\sim\mu_1, \vec{S}_2\sim\mu_2}\left(|\mathrm{Part}_{\vec{S}\|\vec{S}_1\|\vec{S}_2}| = \vec{a}\right) > 0$, we have for all $j \in \{1, 2\}$ and all sequences $\vec{Z}$ of subsets of M,

$$\Pr_{\vec{S}_j\sim\mu_j}\left(\vec{S}_j = \vec{Z}\right) = \Pr_{\substack{\vec{S}_1\sim\mu_1\\ \vec{S}_2\sim\mu_2}}\left(\vec{S}_j = \vec{Z} \mid |\mathrm{Part}_{\vec{S}\|\vec{S}_1\|\vec{S}_2}| = \vec{a}\right).$$

Corollary 4.6. *Let $k > 0$ and $\vec{a}_1, \vec{a}_2 \in \mathbb{Z}^{2^k}$ be arbitrary. Let $\vec{S}$ be a sequence of k subsets of M. For $j \in \{1, 2\}$, define μ_j to be the uniform distribution over all sets $A \subseteq M$ satisfying $|\mathrm{Part}_{\vec{S}} \cap A| = \vec{a}_j$.*

For any $\vec{a} \in \mathbb{Z}^{2^k}$ such that $\Pr_{A_1\sim\mu_1, A_2\sim\mu_2}\left(|\mathrm{Part}_{\vec{S}} \cap A_1 \cap A_2| = \vec{a}\right) > 0$, we have for all $j \in \{1, 2\}$ and all subsets $Z \subseteq M$,

$$\Pr_{A_j\sim\mu_j}\left(A_j = Z\right) = \Pr_{\substack{A_1\sim\mu_1\\ A_2\sim\mu_2}}\left(A_j = Z \mid |\mathrm{Part}_{\vec{S}} \cap A_1 \cap A_2| = \vec{a}\right).$$

4.3 Bases and Clauses

We next define the notion of a *basis*.

Definition 4.7 (Basis). *A pair $S = (S^1, S^2)$ of subsets of M forms a basis if*

$$|\mathrm{Part}_S| = \left(\frac{5m}{16}, \frac{3m}{16}, \frac{3m}{16}, \frac{5m}{16}\right).$$

We reserve the letters S and T to denote bases. Note that if $S = (S^1, S^2)$ is a basis, then the pair $S^{rev} = (S^2, S^1)$ is also a basis. For notational convenience, we will treat bases as a sequence of two sets, and omit the $\vec{}$ sign. We have the following definition:

Definition 4.8 (Compatible Bases). *We say that basis S is compatible with basis T if*

$$|\mathrm{Part}_{S\|T}| = \left(\frac{4m}{16}, \frac{m}{16}, 0, 0, 0,\right.$$

$$\frac{m}{16}, \frac{2m}{16}, 0, \frac{m}{16}, 0, \frac{m}{16}, \frac{m}{16}, 0, \frac{m}{16}, 0, \frac{4m}{16}\Big) = \vec{\text{cmp}}, \textit{ say.}$$

An example of a basis S that is compatible with T is depicted in Figure 3. We note that Definition 4.8 is not symmetric, *i.e.*, basis S may be compatible with T without basis T being compatible with S. However, it holds that if basis S is compatible with T, then basis T^{rev} is compatible with basis S^{rev}.

We will use ξ_{single} to denote the uniform distribution over all bases and ξ to denote the uniform distribution over pairs of bases S, T such that S is compatible with T.

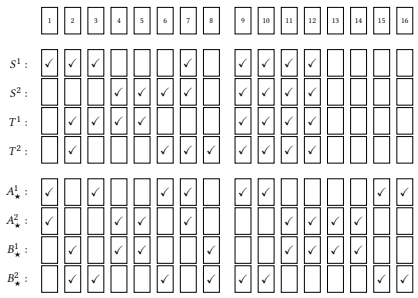

Figure 3: A basis $S = (S^1, S^2)$ that is compatible with another basis $T = (T^1, T^2)$. Also pictured: a pair of sets $(A^1_\star, A^2_\star)$ special with respect to (S, T) (see subsubsection 4.3.2). Observe that $(B^2_\star, B^1_\star) = (\overline{A^2_\star}, \overline{A^1_\star})$ is special with respect to (T^{rev}, S^{rev}). Here, the blocks inside each column correspond to the same $m/16$ elements.

4.3.1 Regular Clauses.

We next define:

Definition 4.9 (Clause). *Let $S = (S^1, S^2)$ be basis. We say that a set $A \subseteq M$ is a clause with respect to S if*

$$|\text{Part}_S \cap A| = \left(\frac{2m}{16}, \frac{m}{16}, \frac{2m}{16}, \frac{3m}{16}\right) = \vec{\text{reg}}, \textit{ say.}$$

We define $\mu_{single}(S)$ to be the uniform distribution over all clauses with respect to S. Observe that the distribution $\mu_{single}(S) = \text{PC}(4, \text{Part}_S, \vec{\text{reg}})$. We also define:

Definition 4.10 (The distribution $\mu(\cdot)$). *Let $S = (S^1, S^2)$ be a basis. A pair (A^1, A^2) of subsets of M is called a clause pair with respect to S if A^1 be a clause with respect to S, A^2 be a clause with respect to S^{rev} and we have*

$$|\text{Part}_S \cap A^1 \cap A^2| = \left(0, 0, \frac{m}{16}, \frac{m}{16}\right) = \vec{\text{regpair}}, \textit{ say.}$$

We define $\mu(S)$ to be the uniform distribution over all clause pairs with respect to S.

Observation 4.11. *Observe that for any basis S, the fact that a pair of sets (A^1, A^2) is a clause pair with respect to S implies that $|\text{Part}_S|$, $|\text{Part}_S \cap A^1|$, $|\text{Part}_S \cap A^2|$, and $|\text{Part}_S \cap A^1 \cap A^2|$ are all fixed functions of m. This means that there exist a vector $\vec{\text{pair}}$ such that (A^1, A^2) is a clause pair with respect to S if and only if*

$$|\text{Part}_{S \| A^1 \| A^2}| = \vec{\text{pair}}.$$

In our lower bound construction, Alice's regular clauses are drawn from the distribution $\mu(S)$ while Bob's regular clauses are drawn from the distribution $\mu(T)$, where S and T are bases such that S is compatible with T. The following lemma shows that the intersection of a regular clause of Alice and a regular clause of Bob has size at least $\frac{51m}{200} > \frac{m}{4}$ (with high probability).

Lemma 4.12. *Consider $\epsilon > 0$ and bases S, T such that S is compatible with T. For all $i, j \in \{1, 2\}$, we have*

$$\Pr_{\substack{(A^1, A^2) \sim \mu(S) \\ (B^2, B^1) \sim \mu(T^{rev})}} \left(|A^i \cap B^j| < \frac{51m}{200} - \epsilon m\right) \leq \exp(-\epsilon^2 m/20).$$

4.3.2 Special Clauses.

Definition 4.13 (Special clauses). *Let S, T be bases such that S is compatible with T. We say that a set $A_\star \subseteq M$ is 1-special with respect to (S, T) if:*

$$|\text{Part}_{S \| T} \cap A_\star| = \Big(\frac{2m}{16}, 0, 0, 0, 0, \frac{m}{16}, 0, 0, \frac{m}{16}, 0, \frac{m}{16}, 0, 0, \frac{m}{16}, 0, \frac{2m}{16}\Big) = \vec{\text{spec}}_1, \textit{ say.}$$

Similarly, we say that $A_\star$ is 2-special with respect to (S, T) if:

$$|\text{Part}_{S \| T} \cap A_\star| = \Big(\frac{2m}{16}, 0, 0, 0, 0, 0, \frac{2m}{16}, 0, \frac{m}{16}, 0, 0, 0, 0, \frac{m}{16}, 0, \frac{2m}{16}\Big) = \vec{\text{spec}}_2, \textit{ say.}$$

For $i \in \{1, 2\}$, we define $\mu^i_{\star, single}(S, T)$ to be the uniform distribution over all sets that are i-special with respect to (S, T). Observe that $\mu^i_{\star, single}(S, T) = \text{PC}\left(16, \text{Part}_{S \| T}, \vec{\text{spec}}_i\right)$ for $i \in \{1, 2\}$. Next, define:

Definition 4.14 (The distribution $\mu_\star(\cdot)$). *Let S, T be bases such that S is compatible with T. We say that a pair of sets $(A^1_\star, A^2_\star)$ is special with respect to (S, T) if $A^1_\star$ is 1-special with respect to (S, T) and $A^2_\star$ is 2-special with respect to (S, T) and*

$$|\text{Part}_{S \| T} \cap A^1_\star \cap A^2_\star| = (0, 0, 0, 0, 0, 0, 0, 0, \frac{m}{16}, 0, 0, 0, 0, \frac{m}{16}, 0, 0) = \vec{\text{specpair}}, \textit{ say.}$$

We define $\mu_\star(S, T)$ to be the uniform distribution over all pairs of sets that are special with respect to (S, T).

Observation 4.15. *Observe that for bases S, T such that S is compatible with T, the fact that a pair of sets $(A^1_\star, A^2_\star)$ is special with respect to (S, T) implies that $|\text{Part}_{S \| T}|$, $|\text{Part}_{S \| T} \cap A^1_\star|$, $|\text{Part}_{S \| T} \cap A^2_\star|$, and $|\text{Part}_{S \| T} \cap A^1_\star \cap A^2_\star|$ are all fixed functions of m. This means that there exist a vector $\vec{\text{opt}}$ such that $(A^1_\star, A^2_\star)$ is special with respect to (S, T) if and only if*

$$|\text{Part}_{S \| T \| A^1_\star \| A^2_\star}| = \vec{\text{opt}}.$$

We reserve $\vec{\text{opt}}$ to denote this vector for the rest of this document. Furthermore, observe that any pair $(A^1_\star, A^2_\star)$ that is special with respect to (S, T) is a clause pair with respect to S. Thus, for all $Z^1, Z^2 \subseteq M$, we have that

$$\Pr_{(A^1_\star, A^2_\star) \sim \mu_\star(S, T)} \left((A^1_\star, A^2_\star) = (Z^1, Z^2)\right) = \Pr_{(A^1, A^2) \sim \mu(S)} \left((A^1, A^2) = (Z^1, Z^2) \mid |\text{Part}_{S \| T \| A^1 \| A^2}| = \vec{\text{opt}}\right).$$

Recall that if S is compatible with T, then T^{rev} is compatible with S^{rev}. It can be verified from Definition 4.14 that $(A^1_\star, A^2_\star)$ is special with respect to (S, T) if and only if $(\overline{A^2_\star}, \overline{A^1_\star})$ is special

with respect to (T^{rev}, S^{rev}). See Figure 3 for a depiction of such a configuration of sets.

Next, we show, in Lemma 4.16, an analogue of Lemma 4.12 for special sets. Just like Lemma 4.12 shows that the intersection of a regular clause of Alice and a regular clause of Bob has size $> \frac{m}{4}$ with high probability, Lemma 4.16 shows that if $(A^1_\star, A^2_\star)$ is special with respect to (S, T), then, intersection of $A^1_\star$ with any clause with respect to T^{rev} and the intersection of $A^2_\star$ with any clause with respect to T has size $> \frac{m}{4}$ with high probability.

We note that Lemma 4.16 does not make similar claims regarding the intersection of $A^1_\star$ and clauses with respect to T and the intersection of $A^2_\star$ and clauses with respect to T^{rev}. This is no coincidence, as these intersections have size $< \frac{m}{4}$ (with high probability).

Lemma 4.16. *Consider $\epsilon > 0$ and bases S, T such that S is compatible with T. For all $i \in \{1, 2\}$, we have*

$$\Pr_{\substack{(A^1_\star, A^2_\star) \sim \mu_\star(S,T) \\ (B^2, B^1) \sim \mu(T^{rev})}} \left(|A^i_\star \cap B^{3-i}| < \frac{61m}{240} - \epsilon m \right) \leq \exp(-\epsilon^2 m/20).$$

4.4 The Distribution ν

We now define a distribution ν over pairs of functions $(v^{\mathsf{A}}, v^{\mathsf{B}}) \in \mathtt{BXOS}_m$ (recall the definition of $\mathtt{BXOS}_m$ from subsection 3.3) that we will use to show Theorem 3.14. Fix $\epsilon > 0$ and define $n = \exp\left(\frac{\epsilon^2 \cdot m}{100}\right)$. We assume for simplicity that n is an integer.

- **Sampling** $(v^{\mathsf{A}}, v^{\mathsf{B}}) \sim \nu$:
  (1) Sample bases $(S, T) \sim \xi$.
  (2) Sample $i_\star \sim \mathcal{U}([n])$ and construct sequences $\vec{A}^1, \vec{A}^2, \vec{B}^1, \vec{B}^2$ of n subsets of M as follows (where $\vec{A}^1 = A^1_1, \cdots, A^1_n$, *etc.*):
    (a) For $i \neq i_\star \in [n]$, sample $(A^1_i, A^2_i) \sim \mu(S)$ and $(B^2_i, B^1_i) \sim \mu(T^{rev})$ independently.
    (b) Sample $(A^1_\star, A^2_\star) \sim \mu_\star(S, T)$ and set $(A^1_{i_\star}, A^2_{i_\star}, B^1_{i_\star}, B^2_{i_\star}) = (A^1_\star, A^2_\star, \overline{A^1_\star}, \overline{A^2_\star})$.
  (3) Sample $\theta \in \mathcal{U}(\{1, 2\})$, and sequences $\vec{r}^{\mathsf{A}} = r^{\mathsf{A}}_1, \cdots, r^{\mathsf{A}}_n \in \{1, 2\}^n$ and $\vec{r}^{\mathsf{B}} = r^{\mathsf{B}}_1, \cdots, r^{\mathsf{B}}_n \in \{1, 2\}^n$ uniformly at random subject to $r^{\mathsf{A}}_{i_\star} = r^{\mathsf{B}}_{i_\star} = \theta$.
  (4) Define $v^{\mathsf{A}}(Z) = \max_{F \in \mathcal{F}^{\mathsf{A}}} |Z \cap F|$ and $v^{\mathsf{B}}(Z) = \max_{F \in \mathcal{F}^{\mathsf{B}}} |Z \cap F|$ where, for all $Z \subseteq M$,
  $$\mathcal{F}^{\mathsf{A}} = \{A^{r^{\mathsf{A}}_i}_i \mid i \in [n]\} \text{ and } \mathcal{F}^{\mathsf{B}} = \{B^{r^{\mathsf{B}}_i}_i \mid i \in [n]\}.$$

For notational convenience, it will be easier to consider ν as the distribution of a random variable $\Upsilon = (S, T, i_\star, \vec{A}^1, \vec{A}^2, \vec{B}^1, \vec{B}^2, \theta, \vec{r}^{\mathsf{A}}, \vec{r}^{\mathsf{B}})$ and consider $v^{\mathsf{A}}, v^{\mathsf{B}}$ as functions of Υ. We will also need shorthand for certain entries of Υ. We will use $\mathcal{A}$ to denote the pair $(\vec{A}^1, \vec{A}^2)$, $\mathcal{B}$ to denote the pair $(\vec{B}^1, \vec{B}^2)$, Υ^{A} to denote $(S, \mathcal{A}, \vec{r}^{\mathsf{A}})$, Υ^{B} to denote $(T, \mathcal{B}, \vec{r}^{\mathsf{B}})$, and finally $\Upsilon_{-\theta}$ to denote $(\Upsilon^{\mathsf{A}}, \Upsilon^{\mathsf{B}}, i_\star)$. Next, using Υ, we define random variables $v^{\mathsf{A}}_j, v^{\mathsf{B}}_j \in \mathtt{BXOS}_m$ for $j \in \{1, 2\}$. To simplify notation, we omit Υ from these random variables even though they are functions of Υ. We define, for $j \in \{1, 2\}$ and $Z \subseteq M$:

$$v^{\mathsf{A}}_j(Z) = \max_{F \in \mathcal{F}^{\mathsf{A}}_j} |Z \cap F| \qquad v^{\mathsf{B}}_j(Z) = \max_{F \in \mathcal{F}^{\mathsf{B}}_j} |Z \cap F|,$$

where

$$\mathcal{F}^{\mathsf{A}}_j = \{A^{j'}_i \mid i \in [n], j' \in [2]\} \setminus \{A^{3-j}_{i_\star}\}$$
$$\mathcal{F}^{\mathsf{B}}_j = \{B^{j'}_i \mid i \in [n], j' \in [2]\} \setminus \{B^{3-j}_{i_\star}\}.$$

Lemma 4.17 and Lemma 4.18 below capture what we need from the distribution ν. We mention that the proof of item 3 of Lemma 4.17 uses the observation that $|A^j_i| = |B^j_i| = \frac{m}{2}$ for all $i \in [n], j \in [2]$. It also crucially leverages the fact that we are taking the minimum over $j \in \{1, 2\}$ (as is captured by $\forall$). In particular, the same statement with the minimum replaced by an average over j is not true. This should be expected, as otherwise it would contradict the auction of [BMW18].

Recall the definition of $\mathrm{opt}(\cdot)$ from subsection 3.2 and that Υ defines $v^{\mathsf{A}}, v^{\mathsf{B}}$.

Lemma 4.17. *We have:*

(1) For all $\Upsilon \sim \nu$, we have $\mathrm{opt}(v^{\mathsf{A}}, v^{\mathsf{B}}) = m$.
(2) For all $\Upsilon \sim \nu$ and $Z \subseteq M$, we have $v^{\mathsf{A}}(Z) \leq v^{\mathsf{A}}_\theta(Z)$ and $v^{\mathsf{B}}(Z) \leq v^{\mathsf{B}}_\theta(Z)$.
(3) It holds that:

$$\Pr_{\Upsilon \sim \nu} \left(\exists Z \subseteq M : \forall j \in \{1, 2\} : v^{\mathsf{A}}_j(Z) + v^{\mathsf{B}}_j(\overline{Z}) > \frac{179m}{240} + \epsilon m \right) \leq 12n^2 \cdot \exp\left(-\frac{\epsilon^2 m}{20}\right).$$

Proof. We show each part in turn:

(1) For the first part, is is enough to show that $\mathrm{opt}(v^{\mathsf{A}}, v^{\mathsf{B}}) \geq m$. We have $\mathrm{opt}(v^{\mathsf{A}}, v^{\mathsf{B}}) \geq v^{\mathsf{A}}(A^\theta_{i_\star}) + v^{\mathsf{B}}(\overline{A^\theta_{i_\star}}) = v^{\mathsf{A}}(A^\theta_{i_\star}) + v^{\mathsf{B}}(B^\theta_{i_\star}) = m$.
(2) For the second part, we only argue for $v^{\mathsf{A}}(Z) \leq v^{\mathsf{A}}_\theta(Z)$ as the other argument is symmetric. This follows by the definition of v^{A} and v^{A}_θ and the fact that $\mathcal{F}^{\mathsf{A}} \subseteq \mathcal{F}^{\mathsf{A}}_\theta$.
(3) For the third part, we define the following events over the randomness in Υ.

$$E_{reg} \equiv \exists i, i' \neq i_\star, j, j' \in \{1, 2\} : |A^j_i \cap B^{j'}_{i'}| < \frac{51m}{200} - \epsilon m.$$
$$E^{\mathsf{A}}_{special} \equiv \exists i \neq i_\star, j \in \{1, 2\} : |A^j_{i_\star} \cap B^{3-j}_i| < \frac{61m}{240} - \epsilon m.$$
$$E^{\mathsf{B}}_{special} \equiv \exists i \neq i_\star, j \in \{1, 2\} : |A^{3-j}_i \cap B^j_{i_\star}| < \frac{61m}{240} - \epsilon m.$$

Finally, define the event $E = E_{reg} \vee E^{\mathsf{A}}_{special} \vee E^{\mathsf{B}}_{special}$. We claim that

Claim. $\Pr(E) \leq 12n^2 \cdot \exp\left(-\frac{\epsilon^2 m}{20}\right)$.

Proof. By the union bound, we have $\Pr(E) \leq \Pr(E_{reg}) + \Pr(E^{\mathsf{A}}_{special}) + \Pr(E^{\mathsf{B}}_{special})$. We next show that each one of $\Pr(E_{reg})$, $\Pr(E^{\mathsf{A}}_{special})$, $\Pr(E^{\mathsf{B}}_{special})$ is at most $4n^2 \cdot \exp\left(-\frac{\epsilon^2 m}{20}\right)$.

We start by showing $\Pr(E_{reg}) \leq 4n^2 \cdot \exp\left(-\frac{\epsilon^2 m}{20}\right)$. We derive using Lemma 4.12:

$$\Pr(E_{reg}) \leq \sum_{i,i' \neq i_\star} \sum_{j,j' \in \{1,2\}} \Pr\left(|A_i^j \cap B_{i'}^{j'}| < \frac{51m}{200} - \epsilon m\right) \leq 4n^2 \cdot \exp\left(-\frac{\epsilon^2 m}{20}\right).$$

We next show that $\Pr(E^{\mathsf{A}}_{special}) \leq 4n^2 \cdot \exp\left(-\frac{\epsilon^2 m}{20}\right)$. We derive using Lemma 4.16:

$$\Pr(E^{\mathsf{A}}_{special}) \leq \sum_{i \neq i_\star} \sum_{j \in \{1,2\}} \Pr\left(|A_{i_\star}^j \cap B_i^{3-j}| < \frac{61m}{240} - \epsilon m\right) \leq 4n^2 \cdot \exp\left(-\frac{\epsilon^2 m}{20}\right).$$

Finally, we show that $\Pr(E^{\mathsf{B}}_{special}) \leq 4n^2 \cdot \exp\left(-\frac{\epsilon^2 m}{20}\right)$. For this part, recall that if a basis S is compatible with T, then T^{rev} is compatible with S^{rev}. Furthermore, a pair $(A^1_\star, A^2_\star)$ is special with respect to (S,T) if and only if $(\overline{A^2_\star}, \overline{A^1_\star})$ is special with respect to (T^{rev}, S^{rev}). We apply Lemma 4.16 on T^{rev}, S^{rev} to get:

$$\Pr(E^{\mathsf{B}}_{special}) \leq \sum_{i \neq i_\star} \sum_{j \in \{1,2\}} \Pr\left(|A_i^{3-j} \cap B_{i_\star}^j| < \frac{61m}{240} - \epsilon m\right) \leq 4n^2 \cdot \exp\left(-\frac{\epsilon^2 m}{20}\right).$$

This finishes the proof that $\Pr(E) \leq 12n^2 \cdot \exp\left(-\frac{\epsilon^2 m}{20}\right)$. □

We next claim that whenever we have a $Z \subseteq M$ such that $v_j^{\mathsf{A}}(Z) + v_j^{\mathsf{B}}(\overline{Z}) > \frac{179m}{240} + \epsilon m$ for all $j \in \{1,2\}$, then E happens. This finishes the proof of the lemma as it follows that:

$$\Pr_{\Upsilon \sim \nu}\left(\exists Z \subseteq M : \forall j \in \{1,2\} : v_j^{\mathsf{A}}(Z) + v_j^{\mathsf{B}}(\overline{Z}) > \frac{179m}{240} + \epsilon m\right) \leq \Pr(E) \leq 12n^2 \cdot \exp\left(-\frac{\epsilon^2 m}{20}\right).$$

We now prove the claim. Let $Z \subseteq M$ be such that $v_j^{\mathsf{A}}(Z) + v_j^{\mathsf{B}}(\overline{Z}) > \frac{179m}{240} + \epsilon m$ for all $j \in \{1,2\}$. Using the definition of v_j^{A} and v_j^{B}, we get that for all $j \in \{1,2\}$, we have $F_j^{\mathsf{A}} \in \mathcal{F}_j^{\mathsf{A}}$ and $F_j^{\mathsf{B}} \in \mathcal{F}_j^{\mathsf{B}}$ such that $|F_j^{\mathsf{A}} \cap Z| + |F_j^{\mathsf{B}} \cap \overline{Z}| > \frac{179m}{240} + \epsilon m$. We proceed via a case analysis on $F_j^{\mathsf{A}}, F_j^{\mathsf{B}}$ for $j \in \{1,2\}$.

- **$\exists j \in [2] : F_j^{\mathsf{A}} \neq A_{i_\star}^j \wedge F_j^{\mathsf{B}} \neq B_{i_\star}^j$:** Let $j_\star$ be such a j. We use the identity $|Z' \cap Z| + |Z'' \cap \overline{Z}| \leq |Z' \cup Z''|$ for any sets Z, Z', Z'' to get:
  $$\frac{179m}{240} + \epsilon m < |F_{j_\star}^{\mathsf{A}} \cap Z| + |F_{j_\star}^{\mathsf{B}} \cap \overline{Z}| \leq |F_{j_\star}^{\mathsf{A}} \cup F_{j_\star}^{\mathsf{B}}|.$$
  Next, as $F_{j_\star}^{\mathsf{A}} \in \mathcal{F}_{j_\star}^{\mathsf{A}}$ and $F_{j_\star}^{\mathsf{B}} \in \mathcal{F}_{j_\star}^{\mathsf{B}}$, we have that $|F_{j_\star}^{\mathsf{A}}| = |F_{j_\star}^{\mathsf{B}}| = \frac{m}{2}$ and we get $|F_{j_\star}^{\mathsf{A}} \cap F_{j_\star}^{\mathsf{B}}| < \frac{61m}{240} - \epsilon m$. As $F_{j_\star}^{\mathsf{A}} \neq A_{i_\star}^{j_\star}$ and $F_{j_\star}^{\mathsf{B}} \neq B_{i_\star}^{j_\star}$, this means that E_{reg} and thus, E happens.
- **If $\exists j \in [2] : F_j^{\mathsf{A}} \in \vec{A}^{3-j} \vee F_j^{\mathsf{B}} \in \vec{B}^{3-j}$:** Let $j_\star$ be such a j and assume that $F_{j_\star}^{\mathsf{A}} \in \vec{A}^{3-j_\star}$. The proof is symmetric when $F_{j_\star}^{\mathsf{B}} \in \vec{B}^{3-j_\star}$. We begin by showing that $\vec{A}^1$ and $\vec{A}^2$ are disjoint. Indeed, all elements of $\vec{A}^1$ are clauses with respect to S whereas all elements of $\vec{A}^2$ are clauses with respect to S^{rev} (Observation 4.15). By Definition 4.9 no set can be a clause with respect to both S and S^{rev} and thus, $\vec{A}^1$ and $\vec{A}^2$ must be disjoint.
  As $\vec{A}^1$ and $\vec{A}^2$ are disjoint, we have that $F_{j_\star}^{\mathsf{A}} \in \vec{A}^{3-j_\star} \implies F_{j_\star}^{\mathsf{A}} \notin \vec{A}^{j_\star} \implies F_{j_\star}^{\mathsf{A}} \neq A_{i_\star}^{j_\star}$. If $F_{j_\star}^{\mathsf{B}} \neq B_{i_\star}^{j_\star}$, then we are done by the previous part, so we assume that $F_{j_\star}^{\mathsf{B}} = B_{i_\star}^{j_\star}$.
  Using the definition of $\mathcal{F}_{j_\star}^{\mathsf{A}}$, we have that $F_{j_\star}^{\mathsf{A}} \notin \vec{A}^{j_\star} \implies F_{j_\star}^{\mathsf{A}} = A_{i^{\mathsf{A}}}^{3-j_\star}$ for some $i^{\mathsf{A}} \neq i_\star$. We use the identity $|Z' \cap Z| + |Z'' \cap \overline{Z}| \leq |Z' \cup Z''|$ for any sets Z, Z', Z'' to get:
  $$\frac{179m}{240} + \epsilon m < |A_{i^{\mathsf{A}}}^{3-j_\star} \cap Z| + |B_{i_\star}^{j_\star} \cap \overline{Z}| \leq |A_{i^{\mathsf{A}}}^{3-j_\star} \cup B_{i_\star}^{j_\star}|.$$
  Next, as $|A_{i^{\mathsf{A}}}^{3-j_\star}| = |B_{i_\star}^{j_\star}| = \frac{m}{2}$ and we get $|A_{i^{\mathsf{A}}}^{3-j_\star} \cap B_{i_\star}^{j_\star}| < \frac{61m}{240} - \epsilon m$. As $i^{\mathsf{A}} \neq i_\star$, this means that $E^{\mathsf{B}}_{special}$ and thus, E happens.
- **Otherwise:** As we are not in case 2, we can assume that for all $j \in [2]$, we have an i_j^{A} and an i_j^{B} such that $F_j^{\mathsf{A}} = A^j_{i_j^{\mathsf{A}}}$ and $F_j^{\mathsf{B}} = B^j_{i_j^{\mathsf{B}}}$. We have that:
  $$|A^1_{i_1^{\mathsf{A}}} \cap Z| + |B^1_{i_1^{\mathsf{B}}} \cap \overline{Z}| + |A^2_{i_2^{\mathsf{A}}} \cap Z| + |B^2_{i_2^{\mathsf{B}}} \cap \overline{Z}| > 2 \cdot \left(\frac{179m}{240} + \epsilon m\right).$$
  By an averaging argument, this means that there exists $j_\star \in [2]$ such that $|A^{j_\star}_{i^{\mathsf{A}}_{j_\star}} \cap Z| + |B^{3-j_\star}_{i^{\mathsf{B}}_{3-j_\star}} \cap \overline{Z}| > \frac{179m}{240} + \epsilon m$. Using $|Z' \cap Z| + |Z'' \cap \overline{Z}| \leq |Z' \cup Z''|$ for any sets Z, Z', Z'' and the fact that $|A^{j_\star}_{i^{\mathsf{A}}_{j_\star}}| = |B^{3-j_\star}_{i^{\mathsf{B}}_{3-j_\star}}| = \frac{m}{2}$, we get that
  $$|A^{j_\star}_{i^{\mathsf{A}}_{j_\star}} \cap B^{3-j_\star}_{i^{\mathsf{B}}_{3-j_\star}}| < \frac{61m}{240} - \epsilon m.$$
  If $i^{\mathsf{A}}_{j_\star} \neq i_\star$ and $i^{\mathsf{B}}_{3-j_\star} \neq i_\star$, then the above inequality implies that E_{reg}, and therefore E happens. If $i^{\mathsf{A}}_{j_\star} = i_\star$ and $i^{\mathsf{B}}_{3-j_\star} \neq i_\star$, then the above inequality implies that $E^{\mathsf{A}}_{special}$, and therefore E happens. If $i^{\mathsf{A}}_{j_\star} \neq i_\star$ and $i^{\mathsf{B}}_{3-j_\star} = i_\star$, then the above inequality implies that $E^{\mathsf{B}}_{special}$, and therefore E happens. Finally, one of these three cases must hold as otherwise, we have $i^{\mathsf{A}}_{j_\star} = i^{\mathsf{B}}_{3-j_\star} = i_\star$, implying
  $$\frac{m}{2} - |A^1_{i_\star} \cap A^2_{i_\star}| = \frac{m}{2} - |A^{j_\star}_{i_\star} \cap A^{3-j_\star}_{i_\star}| = |A^{j_\star}_{i_\star} \cap B^{3-j_\star}_{i_\star}| < \frac{61m}{240} - \epsilon m,$$
  contradicting Definition 4.14.

□

Lemma 4.18. *For the random variable $\Upsilon = (\Upsilon^{\mathsf{A}}, \Upsilon^{\mathsf{B}}, i_\star, \theta)$, it holds that:*

(1) The marginal $i_\star$ is independent of the marginal Υ^{A}.

(2) The marginal $i_\star$ is independent of the marginal Υ^{B}.

5 THE PROOF OF THEOREM 3.14

In this section, we present our proof of Theorem 3.14. Our proof crucially relies on Lemma 4.17 and Lemma 4.18 from section 4.

Proof of Theorem 3.14. Let $\epsilon > 0$ and $m > \frac{10^{10}}{\epsilon^2}$ be arbitrary. By Yao's minimax principle, in order to show Theorem 3.14, it is sufficient to show a distribution ν over pairs of functions from $\texttt{BXOS}_m$ such that any *deterministic* combinatorial auction that is simultaneous and $\left(\frac{3}{4} - \frac{1}{240} + \epsilon\right)$-approximate over ν with probability $\frac{1}{2} + \exp\left(-\frac{\epsilon^2 m}{500}\right)$ satisfies $\mathrm{CC}(\Pi) \geq \exp\left(\frac{\epsilon^2 m}{500}\right)$.

We let ν denote the distribution defined in subsection 4.4 for m, ϵ and let Υ be a random variable denoting a sample from ν as in subsection 4.4. Recall how Υ defines the valuation functions $v^{\mathsf{A}}, v^{\mathsf{B}}$, and also $v_j^{\mathsf{A}}, v_j^{\mathsf{B}}$ for $j \in [2]$. Fix Π to be a simultaneous deterministic auction that is $\left(\frac{3}{4} - \frac{1}{240} + \epsilon\right)$-approximate over ν with probability $\frac{1}{2} + \exp\left(-\frac{\epsilon^2 m}{500}\right)$. We have from subsection 3.2 that

$$\Pr_{\Upsilon \sim \nu}\left(v^{\mathsf{A}}(\mathrm{alloc}_\Pi^{\mathsf{A}}(v^{\mathsf{A}}, v^{\mathsf{B}})) + v^{\mathsf{B}}(\mathrm{alloc}_\Pi^{\mathsf{B}}(v^{\mathsf{A}}, v^{\mathsf{B}})) > \left(\frac{179}{240} + \epsilon\right) \cdot \mathrm{opt}(v^{\mathsf{A}}, v^{\mathsf{B}})\right) \quad (1)$$
$$\geq \frac{1}{2} + \exp\left(-\frac{\epsilon^2 m}{500}\right).$$

To simplify notation, we will henceforth omit $\Upsilon \sim \nu$ with the understanding that all the probabilities and expectations are over the randomness in $\Upsilon \sim \nu$. We use item 1 and item 2 of Lemma 4.17, the fact that the functions v^{A} and v^{B} are monotone, and that $\mathrm{alloc}_\Pi^{\mathsf{A}}(v^{\mathsf{A}}, v^{\mathsf{B}})$ and $\mathrm{alloc}_\Pi^{\mathsf{B}}(v^{\mathsf{A}}, v^{\mathsf{B}})$ are disjoint to get the following from Equation 1:

$$\Pr\left(v_\theta^{\mathsf{A}}(Z(\Upsilon)) + v_\theta^{\mathsf{B}}(\overline{Z(\Upsilon)}) > \left(\frac{179}{240} + \epsilon\right) \cdot m\right) \geq \frac{1}{2} + \exp\left(-\frac{\epsilon^2 m}{500}\right), \quad (2)$$

where $Z(\Upsilon) = \mathrm{alloc}_\Pi^{\mathsf{A}}(v^{\mathsf{A}}, v^{\mathsf{B}})$. Let

$$E_{bad} = \exists Z \subseteq M : \forall j \in \{1, 2\} : v_j^{\mathsf{A}}(Z) + v_j^{\mathsf{B}}(\overline{Z}) > \left(\frac{179}{240} + \epsilon\right) m,$$

be the event from item 3 of Lemma 4.17. By the law to total probability we have

$$\begin{aligned}
&\Pr\left(v_\theta^{\mathsf{A}}(Z(\Upsilon)) + v_\theta^{\mathsf{B}}(\overline{Z(\Upsilon)}) > \left(\frac{179}{240} + \epsilon\right) \cdot m\right) \\
&\leq \Pr\left(E_{bad}\right) + \Pr\left(\overline{E_{bad}} \wedge v_\theta^{\mathsf{A}}(Z(\Upsilon)) + v_\theta^{\mathsf{B}}(\overline{Z(\Upsilon)}) > \left(\frac{179}{240} + \epsilon\right) \cdot m\right) \\
&\leq 12n^2 \cdot \exp\left(-\frac{\epsilon^2 m}{20}\right) \\
&\qquad + \Pr\left(\overline{E_{bad}} \wedge v_\theta^{\mathsf{A}}(Z(\Upsilon)) + v_\theta^{\mathsf{B}}(\overline{Z(\Upsilon)}) > \left(\frac{179}{240} + \epsilon\right) \cdot m\right) \\
&\leq 12n^2 \cdot \exp\left(-\frac{\epsilon^2 m}{20}\right) \\
&\qquad + \Pr\left(v_\theta^{\mathsf{A}}(Z(\Upsilon)) + v_\theta^{\mathsf{B}}(\overline{Z(\Upsilon)}) > v_{3-\theta}^{\mathsf{A}}(Z(\Upsilon)) + v_{3-\theta}^{\mathsf{B}}(\overline{Z(\Upsilon)})\right), \quad (3)
\end{aligned}$$

using item 3 of Lemma 4.17 in the penultimate step. Now, we focus on the second term in the expression above. For every value ω that the tuple $(\mathcal{A}, \mathcal{B}, i_\star)$ can take, we define the event $E_\omega \equiv (\mathcal{A}, \mathcal{B}, i_\star) = \omega$. By the law of total probability, we have

$$\begin{aligned}
&\Pr\left(v_\theta^{\mathsf{A}}(Z(\Upsilon)) + v_\theta^{\mathsf{B}}(\overline{Z(\Upsilon)}) > v_{3-\theta}^{\mathsf{A}}(Z(\Upsilon)) + v_{3-\theta}^{\mathsf{B}}(\overline{Z(\Upsilon)})\right) \\
&\leq \sum_\omega \sum_{Z \subseteq [m]} \sum_{j \in [2]} \Pr(E_\omega \wedge Z(\Upsilon) = Z) \Pr(\theta = j \mid E_\omega, Z(\Upsilon) = Z) \\
&\qquad \times \Pr\left(v_\theta^{\mathsf{A}}(Z(\Upsilon)) + v_\theta^{\mathsf{B}}(\overline{Z(\Upsilon)}) > v_{3-\theta}^{\mathsf{A}}(Z(\Upsilon)) + v_{3-\theta}^{\mathsf{B}}(\overline{Z(\Upsilon)}) \right. \\
&\qquad\qquad \left. \mid E_\omega, Z(\Upsilon) = Z, \theta = j\right).
\end{aligned}$$

Observe that conditioning on $E_\omega, Z(\Upsilon) = Z$ fixes the value of $v_1^{\mathsf{A}}(Z(\Upsilon)) + v_1^{\mathsf{B}}(\overline{Z(\Upsilon)})$ and $v_2^{\mathsf{A}}(Z(\Upsilon)) + v_2^{\mathsf{B}}(\overline{Z(\Upsilon)})$. Thus, the last factor in the summand above is either 0 or 1 and it can be 1 for at most one value of θ. We conclude:

$$\begin{aligned}
&\Pr\left(v_\theta^{\mathsf{A}}(Z(\Upsilon)) + v_\theta^{\mathsf{B}}(\overline{Z(\Upsilon)}) > v_{3-\theta}^{\mathsf{A}}(Z(\Upsilon)) + v_{3-\theta}^{\mathsf{B}}(\overline{Z(\Upsilon)})\right) \\
&\leq \sum_\omega \sum_{Z \subseteq [m]} \Pr(E_\omega \wedge Z(\Upsilon) = Z) \max_{j \in [2]} \Pr(\theta = j \mid E_\omega, Z(\Upsilon) = Z). \quad (4)
\end{aligned}$$

Next, we concentrate on upper bounding the term $\max_{j \in [2]} \Pr(\theta = j \mid E_\omega, Z(\Upsilon) = Z)$. Since θ is chosen independently of $\mathcal{A}, \mathcal{B}, i_\star$ in the distribution ν, we have

$$\begin{aligned}
&\max_{j \in [2]} \Pr(\theta = j \mid E_\omega, Z(\Upsilon) = Z) \\
&= \frac{1}{2} + \max_{j \in [2]} \left(\Pr(\theta = j \mid E_\omega, Z(\Upsilon) = Z) - \frac{1}{2}\right) \\
&= \frac{1}{2} + \max_{j \in [2]} \left(\Pr(\theta = j \mid E_\omega, Z(\Upsilon) = Z) - \Pr(\theta = j \mid E_\omega)\right) \\
&= \frac{1}{2} + \|\mathrm{dist}(\theta \mid E_\omega, Z(\Upsilon) = Z) - \mathrm{dist}(\theta \mid E_\omega)\|_{tvd} \\
&\qquad \text{(Definition 3.10)} \\
&\leq \frac{1}{2} + \sqrt{\frac{1}{2} \cdot \mathbb{D}(\mathrm{dist}(\theta \mid E_\omega, Z(\Upsilon) = Z) \,||\, \mathrm{dist}(\theta \mid E_\omega))} \\
&\qquad \text{(Fact 3.11, item 2)}
\end{aligned}$$

Plugging into Equation 3 and Equation 4 and using concavity of $\sqrt{\cdot}$, we get

$$\begin{aligned}
&\Pr\left(v_\theta^{\mathsf{A}}(Z(\Upsilon)) + v_\theta^{\mathsf{B}}(\overline{Z(\Upsilon)}) > \left(\frac{179}{240} + \epsilon\right) \cdot m\right) \\
&\leq \frac{1}{2} + 12n^2 \cdot \exp\left(-\frac{\epsilon^2 m}{20}\right) + \sqrt{\frac{1}{2} \cdot \mathbb{I}(\theta; Z(\Upsilon) \mid \mathcal{A}, \mathcal{B}, i_\star)}. \quad (5)
\end{aligned}$$

To finish the proof, we claim that

Lemma 5.1. *It holds that* $\mathbb{I}(\theta; Z(\Upsilon) \mid \mathcal{A}, \mathcal{B}, i_\star) \leq 4 \cdot \frac{\mathrm{CC}(\Pi)}{n}$.

We prove Lemma 5.1 later but assuming it for now, we can combine Equation 2 and Equation 5 as

$$\exp\left(-\frac{\epsilon^2 m}{500}\right) \leq 12n^2 \cdot \exp\left(-\frac{\epsilon^2 m}{20}\right) + \sqrt{2 \cdot \frac{\mathrm{CC}(\Pi)}{n}},$$

and Theorem 3.14 follows using $n = \exp\left(\frac{\epsilon^2 m}{100}\right)$. □

We finish this section by showing Lemma 5.1.

Proof of Lemma 5.1. Let Π^{A} and Π^{B} be random variables denoting the message sent by Alice and Bob to the Seller in the first round of Π when inputs to Alice and Bob are drawn from the distribution ν. As Π is simultaneous, it has only one round and $Z(\Upsilon)$

is a function of Π^A and Π^B. We get, invoking Lemma 3.7 multiple times:

$$\begin{aligned}
&\mathbb{I}(\theta; Z(\Upsilon) \mid \mathcal{A}, \mathcal{B}, i_\star) \\
&\leq \mathbb{I}(\theta; \Pi^A \Pi^B \mid \mathcal{A}, \mathcal{B}, i_\star) \\
&= \mathbb{I}(\theta; \Pi^A \mid \mathcal{A}, \mathcal{B}, i_\star) + \mathbb{I}(\theta; \Pi^B \mid \mathcal{A}, \mathcal{B}, i_\star, \Pi^A) \\
&\qquad\qquad \text{(item 4 of Fact 3.6)} \\
&\leq \mathbb{I}(\theta; \Pi^A \mid \mathcal{A}, \mathcal{B}, i_\star) + \mathbb{I}(\theta; \Pi^B \mid \mathcal{A}, \mathcal{B}, i_\star) + \mathbb{I}(\Pi^A; \Pi^B \mid \mathcal{A}, \mathcal{B}, i_\star, \theta) \\
&\leq \mathbb{I}(\theta; \Pi^A \mid \mathcal{A}, i_\star) + \mathbb{I}(\theta; \Pi^B \mid \mathcal{B}, i_\star) \\
&\qquad + \mathbb{I}(\mathcal{B}; \Pi^A \mid \mathcal{A}, i_\star, \theta) + \mathbb{I}(\mathcal{A}; \Pi^B \mid \mathcal{B}, i_\star, \theta) \\
&\qquad\qquad + \mathbb{I}(\Pi^A; \Pi^B \mid \mathcal{A}, \mathcal{B}, i_\star, \theta)
\end{aligned}$$

We now show that the last 3 terms are all 0. To show this, we go term by term using the fact that Π^A is a function of Alice's input v^A, and therefore a function of $\mathcal{A}, \vec{r}^A$. Similarly, Π^B is a function of Bob's input v^B, and therefore a function of $\mathcal{B}, \vec{r}^B$. For the term $\mathbb{I}(\mathcal{B}; \Pi^A \mid \mathcal{A}, i_\star, \theta)$, we get $\mathbb{I}(\mathcal{B}; \Pi^A \mid \mathcal{A}, i_\star, \theta) \leq \mathbb{I}(\mathcal{B}; \mathcal{A}\vec{r}^A \mid \mathcal{A}, i_\star, \theta) = \mathbb{I}(\mathcal{B}; \vec{r}^A_{-i_\star} \mid \mathcal{A}, i_\star, \theta) = 0$ as $\theta = r^A_{i_\star}$ and $\vec{r}^A_{-i_\star}$ is sampled independently of $\mathcal{A}, \mathcal{B}, i_\star, \theta$. Recall that $\vec{r}^A_{-i_\star}$ denotes $\vec{r}^A$ with the coordinate $i_\star$ removed. Similarly, we can deduce that $\mathbb{I}(\mathcal{A}; \Pi^B \mid \mathcal{B}, i_\star, \theta) = 0$. Finally, for the term $\mathbb{I}(\Pi^A; \Pi^B \mid \mathcal{A}, \mathcal{B}, i_\star, \theta)$, we get $\mathbb{I}(\Pi^A; \Pi^B \mid \mathcal{A}, \mathcal{B}, i_\star, \theta) \leq \mathbb{I}(\mathcal{A}\vec{r}^A; \mathcal{B}\vec{r}^B \mid \mathcal{A}, \mathcal{B}, i_\star, \theta) = \mathbb{I}(\vec{r}^A_{-i_\star}; \vec{r}^B_{-i_\star} \mid \mathcal{A}, \mathcal{B}, i_\star, \theta) = 0$ as $\vec{r}^A_{-i_\star}$ is sampled independently of $\vec{r}^B_{-i_\star}, \mathcal{A}, \mathcal{B}, i_\star, \theta$. Combining, we get

$$\mathbb{I}(\theta; Z(\Upsilon) \mid \mathcal{A}, \mathcal{B}, i_\star) \leq \mathbb{I}(\theta; \Pi^A \mid \mathcal{A}, i_\star) + \mathbb{I}(\theta; \Pi^B \mid \mathcal{B}, i_\star).$$

We next show that $\mathbb{I}(\theta; \Pi^A \mid \mathcal{A}, i_\star) \leq 2 \cdot \frac{\mathrm{CC}(\Pi)}{n}$. A similar argument shows that $\mathbb{I}(\theta; \Pi^B \mid \mathcal{B}, i_\star) \leq 2 \cdot \frac{\mathrm{CC}(\Pi)}{n}$ finishing the proof of Lemma 5.1. As $\theta = r^A_{i_\star}$, Π^A is a function of $\mathcal{A}$ and $\vec{r}^A$, and $i_\star$ is sampled from $\mathcal{U}([n])$, we have by Lemma 4.18,

$$\begin{aligned}
\mathbb{I}(\theta; \Pi^A \mid \mathcal{A}, i_\star) &= \mathbb{I}(r^A_{i_\star}; \Pi^A \mid \mathcal{A}, i_\star) \\
&\leq \frac{1}{n} \cdot \mathbb{I}(r^A; \Pi^A \mid \mathcal{A}) \qquad \text{(Lemma 3.8)} \\
&\leq \frac{1}{n} \cdot \mathbb{H}(\Pi^A) \leq \frac{\mathrm{CC}(\Pi) + 1}{n} \leq 2 \cdot \frac{\mathrm{CC}(\Pi)}{n}.
\end{aligned}$$

We note that we lose an extra '+1' in the argument only because, in our model in subsection 3.2, the length of Alice's and Bob's messages can be anywhere from 0 to $\mathrm{CC}(\Pi)$. Thus, the total number of possible messages can be upper bounded by $2^{\mathrm{CC}(\Pi)+1}$ but not $2^{\mathrm{CC}(\Pi)}$.

□

REFERENCES

[AS19] Sepehr Assadi and Sahil Singla. Improved truthful mechanisms for combinatorial auctions with submodular bidders. In *Proceedings of the Sixtieth Annual IEEE Foundations of Computer Science (FOCS)*, 2019.

[BDF+10] David Buchfuhrer, Shaddin Dughmi, Hu Fu, Robert Kleinberg, Elchanan Mossel, Christos H. Papadimitriou, Michael Schapira, Yaron Singer, and Christopher Umans. Inapproximability for VCG-Based Combinatorial Auctions. In *Proceedings of the Twenty-First Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2010.

[BMW18] Mark Braverman, Jieming Mao, and S. Matthew Weinberg. On simultaneous two-player combinatorial auctions. In *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2018, New Orleans, LA, USA, January 7-10, 2018*, pages 2256–2273, 2018.

[Cla71] Edward H. Clarke. Multipart Pricing of Public Goods. *Public Choice*, 11(1):17–33, 1971.

[CT06] Thomas M. Cover and Joy A. Thomas. *Elements of information theory (2. ed.)*. Wiley, 2006.

[CTW20] Linda Cai, Clayton Thomas, and S. Matthew Weinberg. Implementation in advised strategies: Welfare guarantees from posted-price mechanisms when demand queries are np-hard. In *Proceedings of the 11th Innovations in Theoretical Computer Science Conference, (ITCS)*, 2020.

[DN11] Shahar Dobzinski and Noam Nisan. Limitations of vcg-based mechanisms. *Combinatorica*, 31(4):379–396, 2011.

[DN15] Shahar Dobzinski and Noam Nisan. Multi-unit auctions: Beyond roberts. *J. Economic Theory*, 156:14–44, 2015.

[DNS10] Shahar Dobzinski, Noam Nisan, and Michael Schapira. Approximation algorithms for combinatorial auctions with complement-free bidders. *Math. Oper. Res.*, 35(1):1–13, 2010.

[Dob07] Shahar Dobzinski. Two randomized mechanisms for combinatorial auctions. In *Proceedings of the 10th International Workshop on Approximation and the 11th International Workshop on Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 89–103, 2007.

[Dob11] Shahar Dobzinski. An Impossibility Result for Truthful Combinatorial Auctions with Submodular Valuations. In *Proceedings of the 43rd ACM Symposium on Theory of Computing (STOC)*, 2011.

[Dob16a] Shahar Dobzinski. Breaking the logarithmic barrier for truthful combinatorial auctions with submodular bidders. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2016, pages 940–948, New York, NY, USA, 2016. ACM.

[Dob16b] Shahar Dobzinski. Computational efficiency requires simple taxation. In *FOCS*, 2016.

[DSS15] Amit Daniely, Michael Schapira, and Gal Shahaf. Inapproximability of truthful mechanisms via generalizations of the VC dimension. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015*, pages 401–408, 2015.

[DV11] Shaddin Dughmi and Jan Vondrak. Limitations of Randomized Mechanisms for Combinatorial Auctions. In *52nd Annual Symposium on Foundations of Computer Science (FOCS)*, 2011.

[DV12a] Shahar Dobzinski and Jan Vondrák. From query complexity to computational complexity. In *Proceedings of the 44th Symposium on Theory of Computing (STOC)*, 2012.

[DV12b] Shahar Dobzinski and Jan Vondrak. The Computational Complexity of Truthfulness in Combinatorial Auctions. In *Proceedings of the ACM Conference on Electronic Commerce (EC)*, 2012.

[DV16] Shahar Dobzinski and Jan Vondrák. Impossibility results for truthful combinatorial auctions with submodular valuations. *J. ACM*, 63(1):5:1–5:19, 2016.

[EFN+19] Tomer Ezra, Michal Feldman, Eric Neyman, Inbal Talgam-Cohen, and S. Matthew Weinberg. Settling the communication complexity of combinatorial auctions with two subadditive buyers. In *the 60th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2019.

[Fei09] Uriel Feige. On maximizing welfare when utility functions are subadditive. *SIAM J. Comput.*, 39(1):122–142, 2009.

[FV10] Uriel Feige and Jan Vondrák. The submodular welfare problem with demand queries. *Theory of Computing*, 6(1):247–290, 2010.

[Gro73] Theodore Groves. Incentives in Teams. *Econometrica*, 41(4):617–631, 1973.

[KV12] Piotr Krysta and Berthold Vöcking. Online mechanism design (randomized rounding on the fly). In *Automata, Languages, and Programming*, pages 636–647. Springer, 2012.

[LOS02] Daniel Lehmann, Liadan O'Callaghan, and Yoav Shoham. Truth revelation in approximately efficient combinatorial auctions. *J. ACM*, 49(5):577–602, 2002.

[LS05] Ron Lavi and Chaitanya Swamy. Truthful and near-optimal mechanism design via linear programming. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2005.

[MSV08] Vahab S. Mirrokni, Michael Schapira, and Jan Vondrák. Tight information-theoretic lower bounds for welfare maximization in combinatorial auctions. In *Proceedings 9th ACM Conference on Electronic Commerce (EC-2008), Chicago, IL, USA, June 8-12, 2008*, pages 70–77, 2008.

[NS06] Noam Nisan and Ilya Segal. The communication requirements of efficient allocations and supporting prices. *J. Economic Theory*, 129(1):192–224, 2006.

[PS97] Alessandro Panconesi and Aravind Srinivasan. Randomized distributed edge coloring via an extension of the chernoff-hoeffding bounds. *SIAM J. Comput.*, 26(2):350–368, 1997.

[Rag88] Prabhakar Raghavan. Probabilistic construction of deterministic algorithms: Approximating packing integer programs. *J. Comput. Syst. Sci.*, 37(2):130–143, October 1988.

[Vic61] William Vickrey. Counterspeculations, Auctions, and Competitive Sealed Tenders. *Journal of Finance*, 16(1):8–37, 1961.

[Von08] Jan Vondrák. Optimal approximation for the submodular welfare problem in the value oracle model. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*, pages 67–74, 2008.