SIAM J. COMPUT.
Vol. 51, No. 3, pp. STOC20-75–STOC20-114

SEPARATING THE COMMUNICATION COMPLEXITY OF TRUTHFUL AND NONTRUTHFUL ALGORITHMS FOR COMBINATORIAL AUCTIONS*

SEPEHR ASSADI†, HRISHIKESH KHANDEPARKAR‡, RAGHUVANSH R. SAXENA‡, AND S. MATTHEW WEINBERG‡

Abstract. We provide the first separation in the approximation guarantee achievable by truthful and nontruthful algorithms for combinatorial auctions with polynomial communication. Specifically, we prove that any truthful mechanism guaranteeing a $(3/4 - 1/240 + \varepsilon)$-approximation for two buyers with XOS valuations over m items requires $\exp(\Omega(\varepsilon^2 \cdot m))$ communication, whereas a nontruthful algorithm by Dobzinski and Schapira [*Proceedings of the Seventeenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, SIAM, 2006, pp. 1064–1073] and Feige [*SIAM J. Comput.*, 39 (2009), pp. 122–142] is already known to achieve a $3/4$-approximation in $\text{poly}(m)$ communication. We obtain our separation by proving that any simultaneous protocol (not necessarily truthful) which guarantees a $(3/4 - 1/240 + \varepsilon)$-approximation requires communication $\exp(\Omega(\varepsilon^2 \cdot m))$. The taxation complexity framework of Dobzinski [*Proceedings of the 57th Annual Symposium on Foundations of Computer Science* (FOCS), IEEE, 2016, pp. 209–218] extends this lower bound to all truthful mechanisms (including interactive truthful mechanisms).

Key words. combinatorial auctions, communication complexity, simultaneous communication, fractionally subadditive

AMS subject classification. 91B03

DOI. 10.1137/20M1370021

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 m items. Each bidder i has a value for all possible subsets of the items, given by a valuation function $v_i : 2^M \to \mathbb{R}_+$. The bidders are assumed to have quasi-linear utilities, i.e., the utility of bidder i when given a set $S \subseteq M$ at a price p is $v_i(S) - p$, and the goal of the bidders is to maximize their own utility. The seller's goal is to find a partition of the M items into disjoint sets $S_1, \ldots, S_n$ such that the *welfare*, $\sum_{i \in [n]} v_i(S_i)$, is maximized.

The seller faces two challenges in solving this problem. First, the seller must communicate efficiently with the bidders to find a good allocation. Specifically, the seller hopes to use $\text{poly}(n, m)$ total bits of communication, even though each bidder's full valuation function in principle requires (at least) 2^m bits to describe. Second, the seller must accommodate the bidders' own incentives, i.e., the seller must take into account the fact that bidders are interested in their own utility and will only follow the protocol if it maximizes their utility. In other words, the seller desires a protocol

*Received by the editors September 28, 2020; accepted for publication (in revised form) January 26, 2022; published electronically April 7, 2022.
https://doi.org/10.1137/20M1370021
Funding: The first author was supported in part by National Science Foundation (NSF) CAREER award CCF-2047061 and a gift from Google Research. 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 was supported by NSF CAREER award CCF-1750443. The fourth author was supported by NSF grant CCF-1717899.
†Department of Computer Science, Rutgers University, Piscataway, NJ 08854 USA (sepehr.assadi@rutgers.edu).
‡Department of Computer Science, Princeton University, Princeton, NJ 08540 USA (hrishikesh.khandeparkar@gmail.com, rrsaxena@cs.princeton.edu, smweinberg@princeton.edu).

that each bidder is incentivized to follow—such protocols are called *truthful*.

The main question we study in this paper is the following: Are there settings where nontruthful algorithms are strictly more powerful than truthful mechanisms? More specifically, is it the case that for all valuation classes $\mathcal{V}$ and all α, if a poly-communication algorithm can guarantee an α-approximation when all bidders have valuations in $\mathcal{V}$, then a poly-communication truthful mechanism can also guarantee an α-approximation when all bidders have valuations in $\mathcal{V}$?

Our main result is the first setting for which the answer is no, and in fact we show this separation for the well-studied class of XOS (equivalently, fractionally subadditive) valuation functions.[1] Before detailing our result, we provide some context.

The VCG mechanism. For some valuation classes $\mathcal{V}$, truthful mechanisms are indeed as powerful as nontruthful algorithms, due to the Vickrey–Clarke–Groves (VCG) mechanism [Vic61, Cla71, Gro73]. In theoretical computer science terminology, the VCG mechanism is a black-box reduction from *exact* welfare maximization with a truthful mechanism to *exact* welfare maximization with a non-truthful algorithm. More specifically, the VCG mechanism is truthful, maximizes welfare exactly, and can be implemented using $n+1$ black-box calls to a nontruthful algorithm which maximizes welfare exactly.

There are indeed some restricted settings (e.g., when $\mathcal{V}$ is the set of additive valuations, or unit-demand valuations, and even up to gross substitutes) for which a poly-communication algorithm precisely maximizes welfare, implying that VCG is also poly-communication and precisely maximizes welfare. Still, the cases for which VCG is poly-communication are *very* restrictive and do not include, e.g., submodular[2] valuations, let alone XOS or subadditive.[3]

If one considers *approximate* welfare maximization, then, for general (unrestricted) valuation functions, the best achievable approximation guarantee by a poly-communication algorithm is just $O(1/\sqrt{m})$ [NS06]. Due to the strength of this lower bound, poly-communication "VCG-based" truthful mechanisms actually suffice to match this guarantee [Rag88, LOS02, LS05]. So in these domains too, poly-communication truthful mechanisms are as powerful as poly-communication algorithms. Still, the guarantees achievable without any assumptions are quite weak.

In summary, truthful mechanisms are as powerful as nontruthful algorithms at the extremes. When valuations are heavily restricted, VCG is poly-communication. When valuations are arbitrary, good poly-communication algorithms don't exist. Still, this leaves out the entire intermediate range of valuation classes.

Beyond VCG: Gaps in relevant cases. Consider now this intermediate range of valuations, such as submodular, XOS, or subadditive: these classes are rich enough to contain realistic valuation functions, yet also restrictive enough to admit poly-communication constant-factor approximation algorithms. For these valuation classes, the state of affairs is drastically different. Indeed, there are huge gaps between the best-known poly-communication algorithm (where deterministic, constant-factor approximations are known for all three classes [DS06, Fei09, FV10]) and the best-known poly-communication truthful mechanism (where no randomized constant-factor approximation is known for any class [Dob07, AS19], and the best deterministic mechanism guarantees only an $\Omega(1/\sqrt{m})$-approximation [DNS10]). Yet despite these huge gaps in the state of affairs, it was previously unknown whether *any* gap (even a

[1] A valuation function is XOS if it can be written as a maximum of additive functions—see section 2 for precise definition.

[2] A valuation function is submodular if $v(S)+v(T) \leq v(S \cap T)+v(S \cup T)$.

[3] A valuation function is subadditive if $v(S)+v(T) \leq v(S \cup T)$.

small constant factor) exists in any domain! Our main result provides the first such separation:

> MAIN RESULT (informal). *No poly-communication, deterministic truthful mechanism for two bidders with XOS valuations achieves an approximation guarantee better than* $\frac{179}{240} = \frac{3}{4} - \frac{1}{240}$*, whereas a poly-communication, deterministic nontruthful algorithm guarantees a* $\frac{3}{4}$*-approximation.*

We note that the part of our main result that deals with nontruthful algorithms is well known and due to [DS06, Fei09]. Our contribution is the lower bound for deterministic truthful mechanisms. In fact, our result generalizes to rule out certain randomized mechanisms as well, but we defer the formal statement to Theorem 2.1.

Brief overview of approach: Simultaneous communication. Communication lower bounds which hold for truthful mechanisms *but not algorithms* are notoriously hard to come by. Specifically, only two general approaches are known. The first is to pick a subclass of truthful mechanisms (e.g., VCG-based) and prove lower bounds against these particular mechanisms. The aforementioned prior work successfully provides such bounds, so we now know that VCG-based truthful mechanisms cannot beat an $O(1/m^{1/3})$-approximation for submodular (or XOS, subadditive) valuations [DN11, BDF+10, DSS15]. While VCG-based mechanisms are surprisingly general [LMN03], (deterministic) truthful mechanisms exist which are not VCG-based [DN15, KV12, Dob16a, AS19], and these mechanisms indeed achieve better approximation guarantees than the aforementioned lower bounds. In particular, simple posted-price mechanisms are not VCG-based.[4]

The only alternative framework was recently proposed in [Dob16b], which establishes the following remarkable theorem (stated formally in Theorem 2.2): if there exists a deterministic poly-communication truthful mechanism which achieves an α-approximation for two buyers with XOS valuation functions, then there also exists a deterministic poly-communication *simultaneous* algorithm which achieves an α-approximation for two buyers with XOS valuation functions (that is, the two bidders each send exactly one message, simultaneously, and then the designer allocates based only on these messages).[5] That is, while the existence of interactive poly-communication algorithms generally does not imply the existence of simultaneous poly-communication algorithms (e.g., [PS82, DGS84, NW93, BGKL03, DNO14, ANRW15, Ass17]), the additional structure on interactive *truthful mechanisms* does (at least for two-player combinatorial auctions). Following [Dob16b], the remaining task was "merely" to establish a separation between the approximation guarantees achievable in poly-communication with simultaneous versus interactive communication.

Initially, it seems tempting to conjecture that better than just a 1/2-approximation (which for two bidders is trivial—simply ask each bidder for $v_i(M)$ simultaneously and award M to the highest bidder) would be impossible with poly-communication simultaneous algorithms, due to known lower bounds on "sketching" valuation functions [BDF+12]. However, surprising barriers were discovered on this front: [BMW18] developed a simultaneous, randomized 3/4-approximation with poly-communication

[4] A posted-price mechanism computes prices $p_1, \ldots, p_m$ in poly-time, then visits each buyer one at a time and asks them to purchase their favorite set (the one maximizing $v_i(S) - \sum_{j \in S} p_j$).

[5] Note that [Dob16b] has implications beyond XOS, beyond deterministic protocols, and beyond two bidders, but the implications are tricky to formally state and not relevant for this paper.

for two buyers with binary-XOS valuations,[6] which is tight even for interactive algorithms with poly-communication. In addition, [EFN+19] established that even interactive algorithms with poly-communication cannot beat a $1/2$-approximation for two bidders with subadditive valuations (which is matched by the aforementioned trivial simultaneous protocol, so there cannot possibly be a separation for two subadditive bidders). We prove our main result by establishing a lower bound of $3/4 - 1/240$ on the approximation guarantee of any deterministic simultaneous algorithm for two bidders with binary-XOS valuation functions, thus also providing the first successful instantiation of Dobzinski's framework [Dob16b], despite these barriers.

As the main ideas behind our construction require preliminaries and a detailed overview of prior work (especially [BMW18]), we defer further details of our proof to the technical sections. We conclude with a reminder that our main result is the first separation between approximation guarantees achievable by (deterministic) truthful mechanisms and (deterministic) algorithms with poly-communication, which follows by providing the first separation between approximation guarantees achievable by (deterministic) simultaneous algorithms and (deterministic) interactive algorithms with poly-communication for two bidders, and an application of [Dob16b].

1.1. Related work.

Communication complexity separations. As mentioned above, there are no previously known separations between approximation guarantees provided by poly-communication truthful mechanisms and poly-communication algorithms for combinatorial auctions. However, some partial results are known.

For example, due to the works [DN11, BDF+10, DSS15], we have a separation between poly-communication algorithms and poly-communication "VCG-based" truthful mechanisms when the valuation functions are submodular, XOS, or subadditive. While this rules out a large class of potential mechanisms, we have already noted that (variants of) posted-price mechanisms, which are not VCG-based, outperform these lower bounds. Therefore, more general results (like ours) are necessary to consider these mechanisms.

Along similar lines, [DN15] established that a separation exists between polylogarithmic communication algorithms and polylogarithmic communication "scalable" truthful mechanisms for the special case of multi-unit auctions (where all items are identical, so a buyer's valuation is fully specified by m numbers). Scalability is not a particularly restrictive definition, although the result is still quite specialized because of its focus on multi-unit auctions (where the entire valuation function can be communicated with $\text{poly}(m)$ bits).

Other complexity measures. We conclude with a brief overview of the line of work on *computational complexity* of combinatorial auctions. In this setting, the resource of interest is the *running time* of the bidders and the seller during the mechanism. The VCG mechanism again shows that poly-time truthful mechanisms are as powerful as poly-time algorithms in the restricted settings where precise welfare maximization is poly-time tractable.

Interestingly, welfare-maximization is already inapproximable in poly-time better than $\Theta(1/\sqrt{m})$ for XOS or subadditive valuations (unless $\mathbf{P} = \mathbf{NP}$), and again a VCG-based truthful mechanism matches this guarantee [DNS10]. Note the distinction in the communication model, where XOS and subadditive valuations admit a poly-communication constant-factor approximation.

[6] $v(\cdot)$ is binary-XOS if there exists a collection $\mathcal{C}$ of sets and $v(S) := \max_{T \in \mathcal{C}}\{|S \cap T|\}$. Binary-XOS implies XOS.

In the computational model, submodular valuations are the sweet spot where constant-factor poly-time approximations exist (but not poly-time exact solutions). Specifically, there is a poly-time $(1-1/e)$-approximation [Von08], which is optimal assuming $\mathbf{P} = \mathbf{NP}$ [MSV08]. Yet no (randomized) poly-time truthful mechanism can guarantee an $m^{-1/2+\varepsilon}$-approximation for any $\varepsilon > 0$ (unless $\mathbf{NP} \subseteq \mathbf{RP}$). Details about this separation can be found in [Von08, MSV08, Dob11, DV11, DV12a, DV12b, DV16].

While these works in the computational model are quite impressive, we briefly note one major aspect which is better captured by the communication model. Some algorithms/mechanisms are poly-time as long as the bidders can implement *demand queries*.[7] This includes the $(1-1/e)$-approximation algorithm for XOS valuations [DS06], the $1/2$-approximation algorithm for subadditive valuations [Fei09], and the $1/(\log\log m)^3$-approximation truthful mechanism for XOS valuations [AS19]. However, none of these algorithms/mechanisms is "truly poly-time" (unless $\mathbf{NP} \subseteq \mathbf{RP}$), as demand-queries are **NP**-hard even for submodular valuations.

This means that computational lower bounds *do not* rule out poly-time approximations with demand-queries, and indeed the aforementioned algorithms/mechanisms outperform known computational lower bounds. Put another way, the computational model declares these algorithms/mechanisms to be not poly-time *only because the computational model assumes that bidders cannot choose a set to purchase from a simple pricing scheme in poly-time*. Communication lower bounds do not face this issue, as bidders can clearly *state* the set they wish to purchase with m bits. Along these lines, our results are also the first lower bounds separating what is achievable for algorithms and truthful mechanisms with polynomially many demand queries. We refer the reader to [CTW20] or [BMW18] for a deeper comparison of the two models.

1.2. Road map. In section 2, we provide the minimum preliminaries necessary to state our main result, with a detailed proof overview given in section 3. Afterwards, we provide thorough preliminaries necessary for our proofs in section 4, followed by a complete description of our construction in section 5 and its analysis in section 6. Appendix A contains the basic information theory tools we use in this paper.

2. Problem statement and main result. We formally define two-player combinatorial auctions in subsection 2.1 and state our main result in subsection 2.2. We additionally include an informal description below for readers familiar with the topic.

We shall consider auctions with one seller and two bidders, Alice and Bob. In our formalization, the auction would take place in several rounds of communication. In each round, first Alice and Bob (simultaneously) send messages to the seller, and thereafter the seller either responds by sending one message each to Alice and Bob or terminates the auction. When the auction is terminated, the seller outputs an allocation of the items and the price to be charged from both Alice and Bob. Otherwise, the auction goes on to the next round. Observe that in this definition Alice and Bob cannot communicate with each other directly and can only do so through the seller.

2.1. Two-player combinatorial auctions. We first formally define the setting of two-player combinatorial auctions. Let $m > 0$ denote the number of items, and let $\mathcal{V}$ be a nonempty set of functions from $2^{[m]}$ to $\mathbb{R}$. A deterministic protocol Π for the m-item, $\mathcal{V}$-combinatorial auction problem with two bidders is formally specified by the following five functions:

- f^{A} determines Alice's behavior in the protocol. Specifically, f^{A} takes as input Alice's valuation function $v^{\mathsf{A}} \in \mathcal{V}$, and the transcript $\sigma^{\mathsf{A}} \in (\{0,1\}^*)^*$ of

[7] A demand query takes as input a price vector $\vec{p}$ and outputs the set $\arg\max_S\{v(S) - \sum_{i\in S} p_i\}$.

communication with the seller she has seen so far, and decides which message (in $\{0,1\}^*$) to next send the seller. Alice communicates exclusively with the seller (and not directly with Bob).

- f^{B} determines Bob's behavior in the protocol. Similarly, f^{B} takes as input Bob's valuation function $v^{\mathsf{B}} \in \mathcal{V}$, and the transcript $\sigma^{\mathsf{B}} \in (\{0,1\}^*)^*$ of communication with the seller he has seen so far, and decides which message (in $\{0,1\}^*$) to next send the seller. Bob communicates exclusively with the seller (and not directly with Alice).
- f^{S} determines the seller's behavior in the protocol. f^{S} takes as input the transcripts $\sigma^{\mathsf{A}\to\mathsf{S}}, \sigma^{\mathsf{B}\to\mathsf{S}} \in (\{0,1\}^*)^*$ it has seen so far and selects a pair $\{0,1\}^* \times \{0,1\}^* \cup \{(\perp,\perp)\}$ to send. When $\perp$ is sent to both parties, the communication ends.
- alloc determines how to allocate the items, once the communication has concluded. Specifically, alloc takes as input the entirety of Alice's and Bob's communication with the auctioneer (which is in $(\{0,1\}^*)^* \times (\{0,1\}^*)^*$) and selects a pair of sets $(O^{\mathsf{A}}, O^{\mathsf{B}}) \in 2^{[m]} \times 2^{[m]}$, satisfying $O^{\mathsf{A}} \cap O^{\mathsf{B}} = \emptyset$, to award Alice and Bob, respectively.
- price determines how to charge prices once the communication has concluded. Similarly, price takes as input the entirety of Alice's and Bob's communication with the seller (which is in $(\{0,1\}^*)^* \times (\{0,1\}^*)^*$) and selects a pair of prices $(p^{\mathsf{A}}, p^{\mathsf{B}}) \in \mathbb{R} \times \mathbb{R}$ to charge Alice and Bob, respectively.

Observe that the functions $f^{\mathsf{S}}, \mathsf{alloc}, \mathsf{price}$ output a pair (a message/set/price for Alice, and another for Bob). We shall use $f^{\mathsf{S}\to\mathsf{A}}$ (respectively, $f^{\mathsf{S}\to\mathsf{B}}$) to denote the function that outputs only the message to send to Alice (respectively, the message to send to Bob). We define the functions $\mathsf{alloc}^{\mathsf{A}}, \mathsf{alloc}^{\mathsf{B}}, \mathsf{price}^{\mathsf{A}}, \mathsf{price}^{\mathsf{B}}$ analogously. We also define a randomized protocol to be a distribution over deterministic protocols.

Execution of a protocol. A deterministic, m-item, $\mathcal{V}$-combinatorial auction $\Pi = (f^{\mathsf{A}}, f^{\mathsf{B}}, f^{\mathsf{S}}, \mathsf{alloc}, \mathsf{price})$ takes place as follows: At the beginning of the protocol, 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 protocol 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 and 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 $\sigma^{\mathsf{B}\to\mathsf{S}}_i = f^{\mathsf{B}}(v^{\mathsf{B}}, \sigma^{\mathsf{B}}_{<i})$, respectively, to the seller. The seller appends these to the transcripts $\sigma^{\mathsf{A}\to\mathsf{S}}_{<i}, \sigma^{\mathsf{B}\to\mathsf{S}}_{<i}$ to get transcripts $\sigma^{\mathsf{A}\to\mathsf{S}}_{\le i}, \sigma^{\mathsf{B}\to\mathsf{S}}_{\le i} \in (\{0,1\}^*)^i$. Thereafter, the seller sends a message $\sigma^{\mathsf{A}}_i = f^{\mathsf{S}\to\mathsf{A}}(\sigma^{\mathsf{A}\to\mathsf{S}}_{\le i}, \sigma^{\mathsf{B}\to\mathsf{S}}_{\le i})$ to Alice and a message $\sigma^{\mathsf{B}}_i = f^{\mathsf{S}\to\mathsf{B}}(\sigma^{\mathsf{A}\to\mathsf{S}}_{\le i}, \sigma^{\mathsf{B}\to\mathsf{S}}_{\le i})$ to Bob.

If $(\sigma^{\mathsf{A}}_i, \sigma^{\mathsf{B}}_i) \neq (\perp,\perp)$, then Alice (respectively, Bob) appends σ^{A}_i to $\sigma^{\mathsf{A}}_{<i}$ (respectively, σ^{B}_i to $\sigma^{\mathsf{B}}_{<i}$) to get transcript $\sigma^{\mathsf{A}}_{\le i}$ (respectively, $\sigma^{\mathsf{B}}_{\le i}$) and continue round $i+1$ of the protocol. On the other hand, if $(\sigma^{\mathsf{A}}_i, \sigma^{\mathsf{B}}_i) = (\perp,\perp)$, then the protocol *terminates* after round i and no further communication takes place. The seller outputs an allocation $(O^{\mathsf{A}}, O^{\mathsf{B}}) = \mathsf{alloc}(\sigma^{\mathsf{A}\to\mathsf{S}}_{\le i}, \sigma^{\mathsf{B}\to\mathsf{S}}_{\le i})$ and prices $(p^{\mathsf{A}}, p^{\mathsf{B}}) = \mathsf{price}(\sigma^{\mathsf{A}\to\mathsf{S}}_{\le i}, \sigma^{\mathsf{B}\to\mathsf{S}}_{\le i})$.

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

Properties of a protocol. We consider the following parameters of a protocol:

- **Rounds:** For a deterministic protocol Π and $v^{\mathsf{A}}, v^{\mathsf{B}} \in \mathcal{V}$, define $R_\Pi(v^{\mathsf{A}}, v^{\mathsf{B}}) = R$ if the execution of Π when Alice and Bob have inputs $v^{\mathsf{A}}, v^{\mathsf{B}}$, respectively, terminates after round R. If the execution does not terminate at all, then we define $R_\Pi(v^{\mathsf{A}}, v^{\mathsf{B}}) = \infty$.
  We say that Π has R rounds if, for all $v^{\mathsf{A}}, v^{\mathsf{B}} \in \mathcal{V}$, we have $R_\Pi(v^{\mathsf{A}}, v^{\mathsf{B}}) = R$. A randomized protocol has R rounds if all the deterministic protocols in its support have R rounds. If a deterministic or randomized protocol has exactly one round, then we say that the protocol is *simultaneous*.
  To emphasize, in a simultaneous protocol Alice and Bob each send exactly one message. The seller does not send any messages. Then an allocation is determined only as a function of these messages.
- **Communication complexity:** For a deterministic protocol Π and $v^{\mathsf{A}}, v^{\mathsf{B}} \in \mathcal{V}$, we define $\mathsf{CC}_\Pi(v^{\mathsf{A}}, v^{\mathsf{B}}) = \infty$ if $R_\Pi(v^{\mathsf{A}}, v^{\mathsf{B}}) = \infty$. On the other hand, if $R_\Pi(v^{\mathsf{A}}, v^{\mathsf{B}}) = R < \infty$, then we define
$$\mathsf{CC}_\Pi(v^{\mathsf{A}}, v^{\mathsf{B}}) = \sum_{i \le R} \left(\mathsf{len}(\sigma_i^{\mathsf{A}\to\mathsf{S}}) + \mathsf{len}(\sigma_i^{\mathsf{B}\to\mathsf{S}})\right) + \sum_{i<R} \left(\mathsf{len}(\sigma_i^{\mathsf{A}}) + \mathsf{len}(\sigma_i^{\mathsf{B}})\right).$$
  In the above equation, the values $\sigma_i^{\mathsf{A}\to\mathsf{S}}$, $\sigma_i^{\mathsf{B}\to\mathsf{S}}$, 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 $\mathsf{CC}(\Pi) = \max_{v^{\mathsf{A}}, v^{\mathsf{B}} \in \mathcal{V}} \mathsf{CC}_\Pi(v^{\mathsf{A}}, v^{\mathsf{B}})$. Finally we define $\mathsf{CC}(\Pi')$ for a randomized protocol Π' to be the largest value of $\mathsf{CC}(\Pi)$ for all deterministic protocols Π in its support.
- **Truthfulness:** We say that a deterministic protocol Π is truthful if for all $v^{\mathsf{A}}, v^{\mathsf{B}}, v' \in \mathcal{V}$, following the protocol is an *ex-post Nash*. Formally,
$$v^{\mathsf{A}}(\mathsf{alloc}_\Pi^{\mathsf{A}}(v^{\mathsf{A}}, v^{\mathsf{B}})) - \mathsf{price}_\Pi^{\mathsf{A}}(v^{\mathsf{A}}, v^{\mathsf{B}}) \ge v^{\mathsf{A}}(\mathsf{alloc}_\Pi^{\mathsf{A}}(v', v^{\mathsf{B}})) - \mathsf{price}_\Pi^{\mathsf{A}}(v', v^{\mathsf{B}}),$$
$$v^{\mathsf{B}}(\mathsf{alloc}_\Pi^{\mathsf{B}}(v^{\mathsf{A}}, v^{\mathsf{B}})) - \mathsf{price}_\Pi^{\mathsf{B}}(v^{\mathsf{A}}, v^{\mathsf{B}}) \ge v^{\mathsf{B}}(\mathsf{alloc}_\Pi^{\mathsf{B}}(v^{\mathsf{A}}, v')) - \mathsf{price}_\Pi^{\mathsf{B}}(v^{\mathsf{A}}, v').$$
  We say that a randomized protocol is *universally truthful* if all the deterministic mechanisms in its support are truthful. To clearly emphasize the distinction between protocols which are truthful and not truthful, we will often refer to a truthful protocol as a (truthful) *mechanism*, and one which is not necessarily truthful as an *algorithm*.
- **Approximation guarantee:** For $m, \mathcal{V}$ as above and $v^{\mathsf{A}}, v^{\mathsf{B}} \in \mathcal{V}$, define the function $\mathsf{opt}(v^{\mathsf{A}}, v^{\mathsf{B}}) = \max_{S^{\mathsf{A}}, S^{\mathsf{B}} \subseteq [m] : S^{\mathsf{A}} \cap S^{\mathsf{B}} = \emptyset} v^{\mathsf{A}}(S^{\mathsf{A}}) + v^{\mathsf{B}}(S^{\mathsf{B}})$. Let ν be a distribution over pairs drawn from $\mathcal{V}$ and $\alpha, p > 0$. We say that a deterministic protocol Π is α-approximate over ν with probability p if we have
$$\Pr_{(v^{\mathsf{A}}, v^{\mathsf{B}}) \sim \nu} \left(v^{\mathsf{A}}(\mathsf{alloc}_\Pi^{\mathsf{A}}(v^{\mathsf{A}}, v^{\mathsf{B}})) + v^{\mathsf{B}}(\mathsf{alloc}_\Pi^{\mathsf{B}}(v^{\mathsf{A}}, v^{\mathsf{B}})) > \alpha \cdot \mathsf{opt}(v^{\mathsf{A}}, v^{\mathsf{B}}) \right) \ge p.$$
  We further say that a randomized protocol Π' is α-approximate with probability p if for all $v^{\mathsf{A}}, v^{\mathsf{B}} \in \mathcal{V}$, we have
$$\Pr_{\Pi} \left(v^{\mathsf{A}}(\mathsf{alloc}_\Pi^{\mathsf{A}}(v^{\mathsf{A}}, v^{\mathsf{B}})) + v^{\mathsf{B}}(\mathsf{alloc}_\Pi^{\mathsf{B}}(v^{\mathsf{A}}, v^{\mathsf{B}})) > \alpha \cdot \mathsf{opt}(v^{\mathsf{A}}, v^{\mathsf{B}}) \right) \ge p,$$
  where the probability is over all deterministic protocols Π in the support of Π'.

2.2. Formal statement of our main result. We now formalize our main result. For $m > 0$, let $\texttt{BXOS}_m$ be the class of all binary-XOS functions on m items. That is, $\texttt{BXOS}_m$ denotes the set of all $v : 2^{[m]} \to \mathbb{R}$ such that there exists a collection $\mathcal{C} \subseteq 2^{[m]}$, such that for all $S \in 2^{[m]}$, $v(S) = \max_{C \in \mathcal{C}}\{|S \cap C|\}$. Define also $\texttt{XOS}_m \supseteq \texttt{BXOS}_m$ to be the class of all XOS functions on m items. That is, $\texttt{XOS}_m$ denotes the set of all $v : 2^{[m]} \to \mathbb{R}$ such that there exists a collection $\mathcal{C} \subseteq \mathbb{R}^m_+$, such that for all $S \in 2^{[m]}$, we have $v(S) = \max_{c \in \mathcal{C}}\{\sum_{i \in S} c_i\}$.

THEOREM 2.1 (main result). *There exists a constant $\beta > 0$ such that for all $\varepsilon > 0$, there exists an $m_0 > 0$ 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 universally truthful and $(3/4 - 1/240 + \varepsilon)$-approximate with probability $1/2 + \exp(-\beta\varepsilon^2 \cdot m)$ satisfies*

$$\mathsf{CC}(\Pi) \geq \exp(\beta\varepsilon^2 \cdot m).$$

Note, of course, that deterministic protocols are a special case of randomized protocols, so Theorem 2.1 also applies to deterministic mechanisms. Combining this with the deterministic $3/4$-approximation for $\texttt{XOS}_m$ which uses only $\text{poly}(m)$ communication [DS06, Fei09] separates the achievable guarantees of deterministic truthful mechanisms and deterministic algorithms with poly-communication.

Our proof of Theorem 2.1 makes use of the taxation complexity framework developed by [Dob16b]. This framework is very rich and has implications beyond XOS valuations, and beyond two-player auctions. We state below only the case of the framework necessary for our main results and refer the reader to [Dob16b] for the full framework.

THEOREM 2.2 (see [Dob16b]). *There exists a polynomial $P(\cdot)$ such that for all $m, p, \alpha > 0$ and all randomized, m-item, $\texttt{XOS}_m$-combinatorial auctions Π with two bidders and one seller that are universally 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 $\mathsf{CC}(\Pi') \leq P(\max(\mathsf{CC}(\Pi), m))$.*

Theorem 2.2 provides a poly-communication reduction from simultaneous combinatorial auctions to truthful combinatorial auctions. Our main technical result is a lower bound on the simultaneous communication necessary for a randomized protocol that is $(3/4 - 1/240 + \varepsilon)$-approximate with probability $1/2 + \exp(-\beta\varepsilon^2 \cdot m)$.

THEOREM 2.3. *For all $\varepsilon > 0$ and all $m > \frac{10^{10}}{\varepsilon^2}$, any randomized, m-item, $\texttt{BXOS}_m$-combinatorial auction Π with two bidders and one seller that is simultaneous and $\left(\frac{3}{4} - \frac{1}{240} + \varepsilon\right)$-approximate with probability $\frac{1}{2} + \exp\left(-\frac{\varepsilon^2 m}{500}\right)$ satisfies*

$$\mathsf{CC}(\Pi) \geq \exp\left(\frac{\varepsilon^2 m}{500}\right).$$

We briefly compare Theorem 2.3 to Theorem 1.1 of [BMW18]. Theorem 1.1 of [BMW18] gives a randomized, poly-communication simultaneous algorithm which gets a $3/4$-approximation *in expectation*. Theorem 2.3 rules out randomized, poly-communication simultaneous algorithms which achieve a $3/4$-approximation *with probability nonnegligibly larger than* $1/2$. In particular, this includes deterministic algorithms as they achieve the approximation with probability 1.

For the sake of completeness, we prove Theorem 2.1 assuming Theorems 2.2 and 2.3 in Appendix B. The remainder of the paper is devoted to proving Theorem 2.3.

By Yao's minimax principle, in order to obtain a lower bound $\mathsf{CC}(\Pi)$ for randomized m-item simultaneous mechanisms 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 mechanisms Π' that are α-approximate over ν with probability p have large $\mathsf{CC}(\Pi')$. We construct ν in section 5 and analyze it in section 6. Before this, we give a detailed sketch of our construction and the key aspects that drive it.

3. Detailed proof sketch. In this section, we gradually build various aspects of our main construction and highlight the roles they play. All valuation functions for the rest of the paper will be BXOS. Recall that each binary-XOS valuation v has an associated set $\mathcal{C}$ of *clauses*, such that $v(S) := \max_{T \in \mathcal{C}}\{|S \cap T|\}$. We shall sometimes refer to v simply by its set of clauses.

As mentioned previously, our work builds off of a prior construction of [BMW18], which we first describe in detail.

3.1. The [BMW18] construction. The authors of [BMW18] also study BXOS combinatorial auctions. Their result, which serves as our starting point, is a lower bound on the communication required to *determine* the value of the optimal achievable welfare up to a factor of $3/4$. Importantly, though, observe that for *simultaneous* protocols hardness for the decision problem *does not imply* hardness for finding an approximately optimal allocation (and hardness for the decision problem has no implications in Dobzinski's framework). Indeed, deciding the optimal achievable welfare in the [BMW18] construction better than a $(3/4 - 1/108)$-approximation requires exponential communication, yet an allocation guaranteeing a $3/4$-approximation can be found with polynomial communication! We elaborate on this after presenting their construction.[8]

In the construction of [BMW18], the valuation functions of Alice and Bob are BXOS with exponentially many *regular* clauses and may or may not include one *special* clause. The regular clauses are constructed so that the union of a regular clause of Alice and a regular clause of Bob has size $< 3m/4$ (and therefore the maximum possible welfare of any allocation is $< 3m/4$ as well), while the union of a special clause of Alice and a special clause of Bob has size m (and therefore the optimal allocation has welfare m). This means that determining the optimal welfare up to a factor of $3/4$ (or, in fact, any constant better than $20/27$) amounts to determining whether or not Alice and Bob have special clauses.

However, in the [BMW18] construction, the special clauses of Alice and Bob are indistinguishable from the regular clauses. Intuitively, determining whether or not one of their exponentially many clauses is special *with a simultaneous protocol* then requires exponential communication (and this is true). We now detail the [BMW18] construction.

3.1.1. The structure of the clauses in [BMW18].

Step one: Select a basis. For the [BMW18] construction, a *basis* is a pair of sets (S, T) such that $|S| = |T| = m/2$, and also $|S \cap T| = m/3$. In the [BMW18] construction, a basis (S, T) is sampled uniformly at random from all possible bases.

[8] To get a quick intuition for how this can be possible, consider the trivial reduction establishing that allocation is at least as hard as decision: First, solve the allocation problem. Then ask Alice and Bob to output their value for the allocation chosen, and solve the decision problem. This reduction requires an extra round for Alice and Bob to evaluate the solution, and so it cannot be applied simultaneously. One interpretation of [BMW18] is that this extra round is necessary.

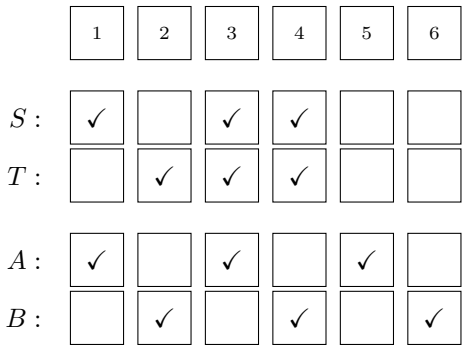

FIG. 1. *The construction of* [BMW18]. *Each of the numbers* 1 *to* 6 *represents a group of* $\frac{m}{6}$ *items.*

Alice knows S and Bob knows T (Alice does not know T, but has a Bayesian posterior conditioned on S and the fact that (S,T) is a uniformly random basis). We provide an illustration of one possible basis in Figure 1 where each of the six blocks in a row represents a group of $m/6$ items.

Step two: Draw regular clauses. Alice's regular clauses are constructed by uniformly sampling sets of size $m/2$ that have intersection exactly $m/3$ with S, and Bob's regular clauses are constructed by uniformly sampling sets of size $m/2$ that have intersection exactly $m/3$ with T. Constructing the regular clauses this way satisfies the following first key property: *The union of a regular clause of Alice and a regular clause of Bob has size strictly less than* $3m/4$ (in fact, at most $20m/27 + \varepsilon m$ except with exponentially small probability).

We briefly explain why (it is $< 3m/4$). As all regular clauses have size $m/2$, it is equivalent to describing why the intersection of a regular clause of Alice and a regular clause of Bob has size strictly more than $m/4$. Intuitively, this is because each regular clause of Alice intersects S more than random, while each regular clause of Bob intersects T more than random, and S and T intersect more than random. Put another way, if the basis (S,T) instead satisfied $|S \cap T| = m/4$, 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 $m/4$ in expectation. In actuality, the basis (S,T) has intersection of size $m/3$, more than the expected size of the intersection of two *independently* random sets of size $m/2$. Thus, the regular clauses of Alice and Bob also intersect more than random sets, i.e., in more than $m/4$ places.

Importantly, observe that if we were to curtail the construction here, the optimal welfare would be $< 3m/4$.

Step three: Special clauses. The second key property of this construction is that we can "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 among 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 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.

Importantly, observe that we can now either add or not add a pair of special clauses to their input. If we do, then the optimal achievable welfare is now m. If we don't, it remains $< 3m/4$. So for Alice and Bob to *simultaneously* decide whether they have a special clause or not, they must somehow send information about each of their exponentially many clauses, which requires exponential communication.

Two observations. We briefly make two observations about the [BMW18] construction (without proof). First, their lower bound holds only for simultaneous protocols. Indeed, Alice and Bob could first communicate S and T to each other in round one, and then they could declare in round two whether they have a special clause or not. In addition, observe that if we simply award to Alice the items corresponding to a uniformly random clause, this allocation achieves a $> 3m/4$-approximation with high probability! We refer the reader to [BMW18] for these calculations, but note that the main idea is that *Bob can have high welfare for a set because of his special clause, without communicating to the seller that a special clause exists.* So if we award Alice a uniformly random clause, if Bob happens to have a special clause, then his welfare is at least $m/4$ (and therefore the achieved welfare is at least $3m/4$, good enough for a $3/4$-approximation). If Bob doesn't have a special clause, then the resulting welfare is nearly optimal. But observe that this approximation is guaranteed *without needing to learn whether Bob has a special clause or not.*

This latter phenomenon is not just an artifact of precise choices in the [BMW18] construction, but a genuine barrier. For example, [BMW18] also designs a randomized, poly-communication simultaneous algorithm that achieves a $3/4$-approximation in expectation. Of course, this algorithm is not deterministic, nor does it guarantee a $3/4$-approximation with good probability (see Theorem 2.1). But it does help convey that the allocation and decision problems are fundamentally different for simultaneous algorithms.

3.1.2. A minor generalization. In the presented construction, we thought of each of the blocks from 1 to 6 in Figure 1 as representing a group of $m/6$ 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 $m/4$ for all u, v such that $u < 2v$ (to get intuition for the breakpoint: when $u = 2v$, then $|S \cap T| = m/4$, and S, T behave like independently chosen sets). We will use this idea later in our construction.

3.2. From the decision problem to the allocation problem. The crucial difference between [BMW18] and our work is that [BMW18] shows that the problem of "deciding" whether or not the optimal welfare is close to m is hard, whereas we wish to show that the problem of "computing" an allocation with welfare close to the optimal is hard. As [BMW18] emphasizes, these problems are incomparable for simultaneous mechanisms.

Our construction is based on the following approach of going from a lower bound for the decision problem to a lower bound for the allocation problem: Consider two

copies of the [BMW18] construction on disjoint sets of items, 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 artificial problem. 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 (by more than a factor of $4/3$). 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. However, this requires the seller to at least determine which copy has the special clause, which is hard due to [BMW18]. The catch, of course, is that we needed to assume that the seller can only allocate items in one of the two copies, so this is not actually an instance of the combinatorial auctions problem.

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 combinatorial auction. A first approach may be to 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 has special clause, and maybe we can show that determining this is hard à la [BMW18].

Unfortunately, this is not actually the case. 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 3.1. Namely, if the two bases are independent, then S^1 and T^2 intersect in $m/4$ places in expectation (like sets of size $m/2$ 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 $3m/4$ in expectation. This is too large for our lower bound, as we need the union to be of size strictly less than $3m/4$ in expectation.

But we do at least have a candidate approach: pick two correlated bases, and hope to find an appropriate correlation so that knowing an allocation which achieves welfare $3m/4$ immediately determines which basis had a special clause.

3.3. Finding the right correlations. As shown in the previous 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 the 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 $< 3m/4$ would extend to also show that the size of the cross-terms is $< 3m/4$.

In order to show that sets S^1, T^2 and S^2, T^1 behave like bases, we need to ensure

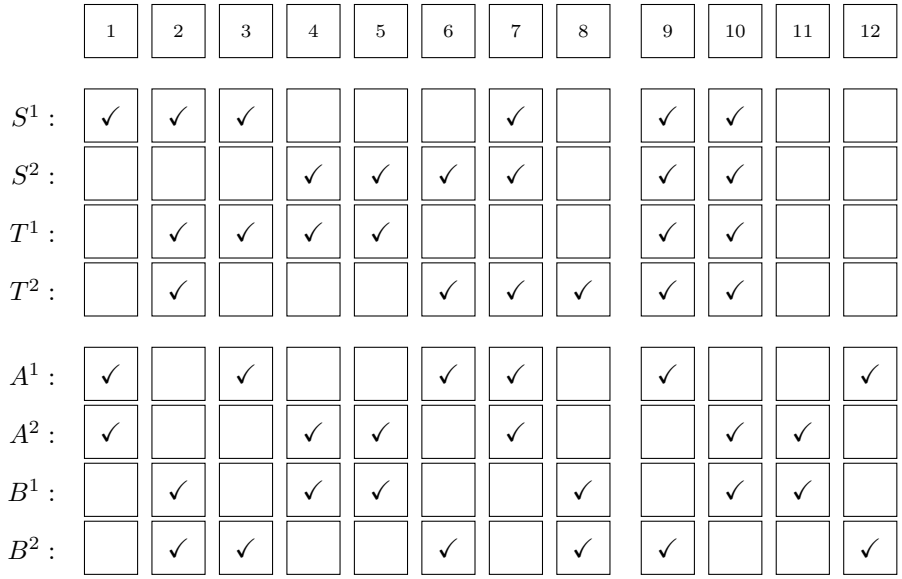

FIG. 2. *An illustration of two correlated bases. Each column denotes a group of $\frac{m}{12}$ items. This construction works even if columns* 1 *through* 8 *denote groups of* u *items, and columns* 9 *through* 12 *denote groups of* v *items, for any* u, v *(see subsection* 3.3*).*

that their intersections, namely, $S^1 \cap T^2$ and $S^2 \cap T^1$, have size $m/3$, 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 $m/12$ items, making a total of m items, and a ✓ in row S^1 and column 1 means that the first $m/12$ 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 $m/3$ 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 previous section. This step is clearly necessary in order to have any hope of a successful construction, but there is one more step to ensure that knowing a $3/4$-approximate allocation reveals which copy is special.

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).[9]

Before we describe how we deal with these special cross-terms, we first need to define the special clauses in our system. We omit a precise definition in this sketch, but mention here that significant structure is imposed by the fact that special clauses need to be indistinguishable from the regular clauses. 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 $m/12$ items is in the set.

With this definition of special clauses, one can calculate the expected intersection

[9] 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.

of the special cross-terms and check if it is $> m/4$ or not. It turns out that with the construction in Figure 2, this size is exactly $m/4$, which means that the construction does *not* suffice. The reason this is problematic is because we can now simply award Alice items corresponding to an arbitrary regular clause, and Bob will get welfare $m/4$ from its complement (using his special clause, *no matter which copy his special clause is from*).

It is here that we use the generalization of [BMW18] given in subsection 3.1, 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 $v/u = 1 + \sqrt{3/2}$. For simplicity's sake, we present our main results assuming $v/u = 2$ when the minimum of the two expressions above is $61m/240 > m/4$. The value $61m/240$ corresponds to the parameter $179/240$ in our main result.

3.4. Summary of outline. So to summarize, our construction takes two correlated bases for a generalized [BMW18] construction. We carefully choose the parameters of both each individual instance, as well as the correlation pattern, so that the following hold:

- The intersection of a regular clause of Alice and regular clause of Bob *within the same copy* is $> m/4$.
- The intersection of a regular clause of Alice and a regular clause of Bob *across different copies* is $> m/4$.
- The intersection of a special clause of Alice and a regular clause of Bob *from the opposite copy* is $> m/4$.
- It is possible to embed disjoint special clauses for both Alice and Bob within either copy, in such a way that they are indistinguishable from regular clauses.

If we can accomplish all four properties, this means that *any allocation guaranteeing welfare* $\geq 3m/4$ *must involve at least one special clause, and a regular or special clause from the same copy.* This sketch omits the calculations, but this property suffices to guarantee that no allocation guarantees welfare $\geq 3m/4$ both when copy one is special and when copy two is special. This in turn means that knowing an allocation which guarantees welfare $\geq 3m/4$ determines which copy is special (and then careful information-theoretic arguments establish that determining the special copy requires exponential communication). This completes our detailed sketch, and the technical sections confirm both that our construction satisfies the properties above and that these properties guarantee the desired conclusion.

4. Technical preliminaries. This section contains notation and preliminaries necessary for our complete proofs. The following notation is standard (and some of it is previously used in our proof sketch and preliminaries), but included for completeness.

Unless otherwise specified, all logarithms are to the base 2. 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 nonnegative 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 the empty string. The length of a string σ will be denoted using $\mathsf{len}(\sigma)$.

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

We will use $\mathcal{U}(S)$ to denote the uniform distribution over a finite set S. If X is a random variable, then $\mathrm{dist}(X)$ will denote the distribution of the values taken by X. Our proofs require careful information-theoretic arguments, and Appendix A contains thorough preliminaries for the notation and facts we use.

4.1. Partitions and notation. Recall that in the [BMW18] construction, one defines a distribution $D(S)$ which is uniform over all sets A such that $|A \cap S| = m/3$. Such a distribution is concise to describe in text and does not merit special notation. Our construction, however, will eventually define a distribution $\mu_\star(\cdot)$ which is uniform over all sets A such that $|A \cap P_i| = p_i$ *for all* $i \in [16]$. We will also frequently discuss the intersection of two sets drawn independently from such distributions and show that it concentrates around its expectation (and compute its expectation). This section provides notation so that we can make concise descriptions and statements of this form, and concludes with a concentration inequality that we will repeatedly use. While this notation does (significantly) help keep statements concise, the reader may wish to refer back to this section for help parsing the precise statements.

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 $\vec{S} = S_1, S_2, \ldots, S_k$ be a sequence of k sets. For a function f defined on sets, we shall use $f(\vec{S})$ to denote the sequence $f(S_1), \ldots, f(S_k)$. Thus, $|\vec{S}|$ shall denote the sequence $|S_1|, \ldots, |S_k|$, and $\vec{S} \cap A$, for a set A, shall denote the sequence $S_1 \cap A, \ldots, S_k \cap A$, etc.

Let $k > 0$. We say that a sequence $\vec{P} = P_1, P_2, \ldots, P_k$ of subsets of M forms a partition of M into k sets if the sets $P_1, \ldots, P_k$ 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 $\vec{P} = P_1, P_2, \ldots, P_k$ 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 defines the class of distributions over sets that we consider frequently throughout our construction.

DEFINITION 4.1. *We say that a tuple $(k, \vec{P}, \vec{p})$ is a partition parameter if $k > 0$, $\vec{P} = P_1, \ldots, P_k$ is a partition of M into k sets, and $\vec{p} = p_1, p_2, \ldots, p_k$ 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 $\mathsf{PC}(k, \vec{P}, \vec{p})$ to be the uniform distribution over all sets U satisfying

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

Recall in our proof sketch that we repeatedly draw regular sets from a distribution of the form $\mathsf{PC}(k, \vec{P}, \vec{p})$ and wish to argue about the size of the intersection of two independently drawn regular sets (from different distributions). The following lemma

states the expected intersection (captured in Δ), and also bounds the probability that the intersection deviates far from Δ. Mapping back to the [BMW18] construction, Lemma 4.2 would help claim that all regular sets have intersection at least $7m/27-\varepsilon m$ with high probability. The proof of Lemma 4.2 is in Appendix B.1.

LEMMA 4.2. *For any partition parameters $(k, \vec{P}, \vec{p})$ and $(k', \vec{P'}, \vec{p'})$, it holds for all $\varepsilon > 0$ that*

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

where

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

4.1.1. The function Part. All of the partition parameters that we consider take a particular form, which enables further concise notation. Specifically, they will arise from the following construction: Let $k > 0$. For any sequence $\vec{S} = S_1, \dots, S_k$ of k subsets of M and any sequence $\vec{b} = b_1, \dots, b_k$ of bits, we define the set

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

We use $\mathsf{Part}_{\vec{S}}$ to denote the sequence of sets $\{\mathsf{Part}_{\vec{S}}(\vec{b})\}_{\vec{b}\in\{0,1\}^k}$ ordered lexicographically according to $\vec{b}$ (i.e., $\mathsf{Part}_{\vec{S}}(0^k)$, followed by $\mathsf{Part}_{\vec{S}}(0^{k-1}1)$, etc.). Observe that the sequence $\mathsf{Part}_{\vec{S}}$ forms a partition of M into 2^k sets. Lemma 4.3 and Corollary 4.4 discuss marginals of distributions drawn jointly (intuitively, Alice and Bob will have inputs drawn jointly, and we will want to reason about the marginal distribution of the input that Alice sees). Applied to the [BMW18] construction, Corollary 4.4 would be useful to claim that when (S, T) are drawn uniformly at random among sets of size $m/2$ which intersect at $m/3$, that S is a uniformly random set of size $m/2$. It would also be useful to claim that Alice's special set is indistinguishable from her regular sets. Lemma 4.3 is a technical generalization of Corollary 4.4 which is necessary for our construction because we sometimes jointly draw tuples of sets (but it has no analogue in [BMW18]).

LEMMA 4.3. *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 $|\mathsf{Part}_{\vec{S}\|\vec{S}_j}| = \vec{a}_j$.*

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

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

COROLLARY 4.4. *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 $\mu_j := \mathsf{PC}(2^k, \mathsf{Part}_{\vec{S}}, \vec{a}_j)$ (which is the uniform distribution over all sets $A \subseteq M$ satisfying $|\mathsf{Part}_{\vec{S}} \cap A| = \vec{a}_j$).*

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

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

5. 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 now give a formal definition of our lower bound instance.

5.1. Bases and clauses. We next define the notion of a *basis*.

DEFINITION 5.1 (basis). *A pair $S = (S^1, S^2)$ of subsets of M forms a basis if*

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

To help parse the notation Part_S, recall that the first term denotes the number of elements which are in neither S^1 nor S^2 (corresponds to $\vec{b} = (0,0)$), the second term is the number of elements which are in S^2 but not S^1 (corresponds to $\vec{b} = (0,1)$), the third term is the number of elements in S^1 but not S^2 (corresponds to $\vec{b} = (1,0)$), and the fourth term is the number of elements which are in $S^1 \cap S^2$ (corresponds to $\vec{b} = (1,1)$).

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. The following definition considers a pair of bases. Recall that $S||T$ is a list of four sets, so $|\mathsf{Part}_{S||T}|$ has sixteen possible $\vec{b}$ to consider (and therefore is a list of sixteen numbers).

DEFINITION 5.2 (compatible bases). *We say that basis S is compatible with basis T if*

$$|\mathsf{Part}_{S\|T}| = \left(\frac{4m}{16}, \frac{m}{16}, 0, 0, 0, \frac{m}{16}, \frac{2m}{16}, 0, \frac{m}{16}, 0, \frac{m}{16}, \frac{m}{16}, 0, \frac{m}{16}, 0, \frac{4m}{16}\right).$$

For short, we refer to $\vec{\mathsf{cmp}} := \left(\frac{4m}{16}, \frac{m}{16}, 0, 0, 0, \frac{m}{16}, \frac{2m}{16}, 0, \frac{m}{16}, 0, \frac{m}{16}, \frac{m}{16}, 0, \frac{m}{16}, 0, \frac{4m}{16}\right)$.

Again, recall that (e.g.) $2m/16$ denotes the number of elements in $\overline{S^1} \cap S^2 \cap T^1 \cap \overline{T^2}$ (and corresponds to $\vec{b} = (0,1,1,0)$). An example of a basis S that is compatible with T is depicted in Figure 3. We note that Definition 5.2 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.

The first step in our construction is the distribution ξ, which defines a distribution over pairs of bases. Mapping back to our proof sketch, (S^1, T^1) denotes the basis for the "first copy," and (S^2, T^2) denotes the basis for the "second copy."

5.1.1. Regular clauses. The next step in our construction is to define how to draw regular clauses once the bases are fixed. In order to have the desired interaction between cross-terms, we need to specify the intersection of each clause not only with the basis "of its copy," but also the basis for the "other copy."

DEFINITION 5.3 (clause). *Let $S = (S^1, S^2)$ be a basis. We say that a set $A \subseteq M$ is a clause with respect to S if*

$$|\mathsf{Part}_S \cap A| = \left(\frac{2m}{16}, \frac{m}{16}, \frac{2m}{16}, \frac{3m}{16}\right).$$

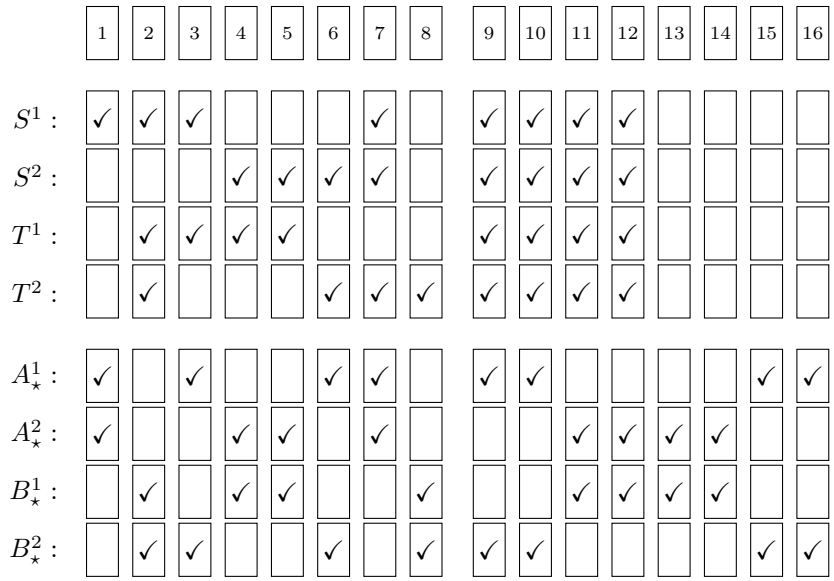

FIG. 3. *A basis $S = (S^1, S^2)$ that is compatible with another basis $T = (T^1, T^2)$. Also pictured: a pair of sets $(A^1_\star, A^2_\star)$ special with respect to (S, T) (see subsection 5.1.2). Observe that $(B^2_\star, B^1_\star) = (\overline{A^2_\star}, \overline{A^1_\star})$ is special with respect to (T^{rev}, S^{rev}). Here, the blocks inside each column correspond to the same $m/16$ elements.*

For short, we denote this by $\vec{\mathsf{reg}} := \left(\frac{2m}{16}, \frac{m}{16}, \frac{2m}{16}, \frac{3m}{16}\right)$.

We define $\mu_{single}(S)$ to be the uniform distribution over all clauses with respect to S. Observe that the distribution $\mu_{single}(S) = \mathsf{PC}(4, \mathsf{Part}_S, \vec{\mathsf{reg}})$ (recall the definition of PC from Definition 4.1). We also define the following.

DEFINITION 5.4 (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 is a clause with respect to S, A^2 is a clause with respect to S^{rev}, and we have*

$$|\mathsf{Part}_S \cap A^1 \cap A^2| = \left(0, 0, \frac{m}{16}, \frac{m}{16}\right).$$

For short, we define $\vec{\mathsf{regpair}} := \left(0, 0, \frac{m}{16}, \frac{m}{16}\right)$.

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

The second step in our construction is the distribution $\mu(\cdot)$, which describes how Alice and Bob draw pairs of regular clauses once their basis is fixed.

Observe that $\mu(S)$ is a distribution over *pairs* of clauses. The first clause in the pair is a clause with respect to S (this corresponds to a regular clause in the "first copy"), and the second is a clause with respect to S^{rev} (this corresponds to a regular clause in the "second copy"). Observation 5.5 below is simple, but key: it states that a pair of sets (A^1, A^2) is a clause pair with respect to S if and only if a sequence of equalities involving the size of sets involving S, A^1, A^2 holds. Because $\mu(S)$ is the uniform distribution clause pairs with respect to S, this means that any (A^1, A^2) satisfying the noted equalities is equally likely to have been drawn from $\mu(S)$ (and this is what lets us later plant an undetectable special clause pair).

OBSERVATION 5.5. *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 $|\mathsf{Part}_S|$, $|\mathsf{Part}_S \cap A^1|$, $|\mathsf{Part}_S \cap A^2|$, and $|\mathsf{Part}_S \cap A^1 \cap A^2|$ are all fixed functions of m. This means that there exist a vector $\vec{\mathsf{pair}}$ such that (A^1, A^2) is a clause pair with respect to S if and only if*

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

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). While the proof requires several steps to be rigorous, the intuition is simple: we first need to argue that each of the sets A^1, A^2, B^1, B^2 is identically distributed to draws from a distribution of the form $\mu_{single}(\cdot)$, which is of the form $\mathsf{PC}(k, \vec{P}, \vec{p})$. This step uses Lemma 4.3. Once we have done this, we can use Lemma 4.2 to argue that the intersection of any two pairs concentrates around its expectation (and that its expectation is $51m/100$).

LEMMA 5.6. *Consider $\varepsilon > 0$ and bases S, T such that S is compatible with T. For all $i, j \in \{1, 2\}$, we have*

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

Proof. We show the lemma assuming $i = j = 1$. The proof for other values of (i, j) is similar (with different calculations), and we discuss necessary modifications at the end. We derive

$$\begin{aligned}
&\Pr_{\substack{(A^1,A^2)\sim\mu(S)\\(B^2,B^1)\sim\mu(T^{rev})}} \left(|A^1 \cap B^1| < \frac{51m}{200} - \varepsilon m \right) \\
&= \sum_{Z,Z' : |Z \cap Z'| < \frac{51m}{200} - \varepsilon m} \Pr_{\substack{(A^1,A^2)\sim\mu(S)\\(B^2,B^1)\sim\mu(T^{rev})}} \left((A^1, B^1) = (Z, Z') \right) \\
&= \sum_{Z,Z' : |Z \cap Z'| < \frac{51m}{200} - \varepsilon m} \Pr_{(A^1,A^2)\sim\mu(S)} (A^1 = Z) \Pr_{(B^2,B^1)\sim\mu(T^{rev})} (B^1 = Z') \\
&= \sum_{Z,Z' : |Z \cap Z'| < \frac{51m}{200} - \varepsilon m} \Pr_{\substack{A^1\sim\mu_{single}(S)\\A^2\sim\mu_{single}(S^{rev})}} (A^1 = Z \mid |\mathsf{Part}_S \cap A^1 \cap A^2| = \vec{\mathsf{regpair}}) \\
&\qquad \times \Pr_{\substack{B^2\sim\mu_{single}(T^{rev})\\B^1\sim\mu_{single}(T)}} (B^1 = Z' \mid |\mathsf{Part}_{T^{rev}} \cap B^2 \cap B^1| = \vec{\mathsf{regpair}}) \\
&= \sum_{Z,Z' : |Z \cap Z'| < \frac{51m}{200} - \varepsilon m} \Pr_{A\sim\mu_{single}(S)} (A = Z) \Pr_{B\sim\mu_{single}(T)} (B = Z') \quad \text{(Corollary 4.4)} \\
&= \sum_{Z,Z' : |Z \cap Z'| < \frac{51m}{200} - \varepsilon m} \Pr_{\substack{A\sim\mu_{single}(S)\\B\sim\mu_{single}(T)}} \left((A, B) = (Z, Z') \right) \\
&= \Pr_{\substack{A\sim\mu_{single}(S)\\B\sim\mu_{single}(T)}} \left(|A \cap B| < \frac{51m}{200} - \varepsilon m \right).
\end{aligned}$$

It is thus sufficient to show that $\Pr_{A\sim\mu_{single}(S),B\sim\mu_{single}(T)}\left(|A\cap B|<\frac{51m}{200}-\varepsilon m\right)\leq \exp(-\varepsilon^2 m/20)$. We show this using Lemma 4.2 as the distributions $\mu_{single}(S)=\mathsf{PC}\left(4,\mathsf{Part}_S,\vec{\mathsf{reg}}\right)$ and $\mu_{single}(T)=\mathsf{PC}\left(4,\mathsf{Part}_T,\vec{\mathsf{reg}}\right)$. By Lemma 4.2, we have

$$\Pr_{\substack{A\sim\mu_{single}(S)\\B\sim\mu_{single}(T)}}(|A\cap B|<\Delta-\varepsilon m)\leq\exp(-\varepsilon^2(m-\Delta)/3),$$

so we just need to compute Δ. Below, recall that $\vec{\mathsf{cmp}}$ lists the size of $S^1\cap S^2\cap T^1\cap T^2$, $S^1\cap S^2\cap T^1\cap\overline{T^2}$, etc., and this is where the terms $\frac{4m}{16}$, $\frac{m}{16}$, etc., come from. Recall that $\vec{\mathsf{reg}}$ lists the size of $A^1\cap S^1\cap S^2$, etc., and also $B^1\cap T^1\cap T^2$, etc. So, for example, $|A^1\cap\overline{S^1}\cap\overline{S^2}|=2m/16$ (according to $\vec{\mathsf{reg}}$), and $|\overline{S^1}\cap\overline{S^2}|=4m/16+m/16+0+0=5m/16$ (according to $\vec{\mathsf{cmp}}$), and therefore A^1 contains $2/5$ of the elements in $\overline{S^1}\cap\overline{S^2}$:

$$\begin{aligned}\Delta&=\frac{2}{5}\cdot\frac{2}{5}\cdot\frac{4m}{16}+\frac{2}{5}\cdot\frac{1}{3}\cdot\frac{m}{16}+\frac{1}{3}\cdot\frac{1}{3}\cdot\frac{m}{16}\\&\quad+\frac{1}{3}\cdot\frac{2}{3}\cdot\frac{2m}{16}+\frac{2}{3}\cdot\frac{2}{5}\cdot\frac{m}{16}+\frac{2}{3}\cdot\frac{2}{3}\cdot\frac{m}{16}\\&\quad+\frac{2}{3}\cdot\frac{3}{5}\cdot\frac{m}{16}+\frac{3}{5}\cdot\frac{1}{3}\cdot\frac{m}{16}+\frac{3}{5}\cdot\frac{3}{5}\cdot\frac{4m}{16}\\&=\frac{51}{200}\cdot m.\end{aligned}$$

Thus, we get

$$\Pr_{\substack{A\sim\mu_{single}(S)\\B\sim\mu_{single}(T)}}\left(|A\cap B|<\frac{51m}{200}-\varepsilon m\right)\leq\exp(-149\varepsilon^2 m/600)<\exp(-\varepsilon^2 m/20),$$

as desired.

To adjust the proof for the other three values of (i,j), the first half of the proof would be identical, but perhaps replacing $\mu_{single}(S)$ with $\mu_{single}(S^{rev})$ and perhaps replacing $\mu_{single}(T)$ with $\mu_{single}(T^{rev})$. This also causes the precise calculations above for Δ to change, but all four calculations result in $\Delta\geq 51m/200$. ∎

Lemma 5.6 *is the first key property of our construction, which establishes that the union of two regular clauses is* $<3m/4$. Note in particular that Lemma 5.6 covers both the "like terms" and the "cross-terms" at once. Note also that if we were to have a construction which draws uniformly random compatible bases from ξ, and then has Alice and Bob draw exponentially many (but not too many) clause pairs with respect to their basis, that the optimal welfare would be at most $149m/200$.

5.1.2. Special clauses. We now describe how to add special clauses to our construction. Again recall that there are three properties we need: First, the special clauses should be indistinguishable from regular clauses. Second, Alice's and Bob's special clauses should be disjoint. Third, a special clause should intersect a regular clause "from the other copy" at slightly more than $m/4$.

DEFINITION 5.7 (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*

$$|\mathsf{Part}_{S\|T}\cap A_\star|=\left(\frac{2m}{16},0,0,0,0,\frac{m}{16},0,0,\frac{m}{16},0,\frac{m}{16},0,0,\frac{m}{16},0,\frac{2m}{16}\right).$$

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

$$|\mathsf{Part}_{S\|T}\cap A_\star|=\left(\frac{2m}{16},0,0,0,0,0,\frac{2m}{16},0,\frac{m}{16},0,0,0,0,\frac{m}{16},0,\frac{2m}{16}\right).$$

For short, we refer to these as $\vec{\mathsf{spec}}_1 := \left(\frac{2m}{16}, 0, 0, 0, 0, \frac{m}{16}, 0, 0, \frac{m}{16}, 0, \frac{m}{16}, 0, 0, \frac{m}{16}, 0, \frac{2m}{16}\right)$ *and* $\vec{\mathsf{spec}}_2 := \left(\frac{2m}{16}, 0, 0, 0, 0, 0, 0, \frac{2m}{16}, 0, \frac{m}{16}, 0, 0, 0, 0, \frac{m}{16}, 0, \frac{2m}{16}\right)$.

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 $\mu^i_{\star,single}(S, T) = \mathsf{PC}\left(16, \mathsf{Part}_{S\|T}, \vec{\mathsf{spec}}_i\right)$ for $i \in \{1, 2\}$. We again define a distribution over a pair of special sets (again intuitively, $A^1_\star$ is special for the "first copy" and $A^2_\star$ is special for the "second copy").

DEFINITION 5.8 (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*

$$|\mathsf{Part}_{S\|T} \cap A^1_\star \cap A^2_\star| = \left(0, 0, 0, 0, 0, 0, 0, 0, \frac{m}{16}, 0, 0, 0, 0, \frac{m}{16}, 0, 0\right).$$

For short, we define $\vec{\mathsf{specpair}} := \left(0, 0, 0, 0, 0, 0, 0, 0, \frac{m}{16}, 0, 0, 0, 0, \frac{m}{16}, 0, 0\right)$. *We define $\mu_\star(S, T)$ to be the uniform distribution over all pairs of sets that are special with respect to (S, T).*

The third step in our construction is the distribution $\mu_\star(\cdot)$, which describes how Alice and Bob draw potential special clauses once their basis is fixed. Observation 5.9 is again simple, but crucial. In particular, it observes that every pair that is special with respect to (S, T) is also a clause pair with respect to S. This means that an independently drawn special pair will be indistinguishable from clause pairs.

OBSERVATION 5.9. *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 $|\mathsf{Part}_{S\|T}|$, $|\mathsf{Part}_{S\|T} \cap A^1_\star|$, $|\mathsf{Part}_{S\|T} \cap A^2_\star|$, and $|\mathsf{Part}_{S\|T} \cap A^1_\star \cap A^2_\star|$ are all fixed functions of m. This means that there exists a vector $\vec{\mathsf{opt}}$ such that $(A^1_\star, A^2_\star)$ is special with respect to (S, T) if and only if*

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

We reserve $\vec{\mathsf{opt}}$ 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

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

Observation 5.9 *is the second key property of our construction, which suggests that special clauses are indistinguishable from regular clauses, prior to any communication.* Recall that if S is compatible with T, then T^{rev} is compatible with S^{rev}. It can be verified from Definition 5.8 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 5.10, an analogue of Lemma 5.6 for special sets. Just like Lemma 5.6 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 5.10 shows that if $(A^1_\star, A^2_\star)$ is special with respect to (S, T), then the 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 5.10 *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). Intuitively, this should be expected: recall from the [BMW18] construction that a special clause for Alice and a regular clause for Bob had intersection $< m/4$. The intersection of $A^1_\star$ with a clause with respect to T is the analogue in our construction. But we still need to make sure that the intersection of a special clause of Alice for one copy and a regular clause for Bob *in the other copy* is large, and this is what Lemma 5.10 states.

LEMMA 5.10. *Consider* $\varepsilon > 0$ *and bases* S, T *such that* S *is compatible with* T. *For all* $i \in \{1,2\}$, *we have*

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

Proof. We show the lemma assuming $i = 1$. The proof for $i = 2$ is similar (with different calculations), and we discuss necessary modifications at the end. We derive

$$\begin{aligned}
&\Pr_{\substack{(A^1_\star,A^2_\star)\sim\mu_\star(S,T)\\(B^2,B^1)\sim\mu(T^{rev})}}\left(|A^1_\star \cap B^2| < \frac{61m}{240} - \varepsilon m\right)\\
&\quad= \sum_{Z,Z':|Z\cap Z'|<\frac{61m}{240}-\varepsilon m} \Pr_{\substack{(A^1_\star,A^2_\star)\sim\mu_\star(S,T)\\(B^2,B^1)\sim\mu(T^{rev})}}\left((A^1_\star, B^2) = (Z, Z')\right)\\
&= \sum_{Z,Z':|Z\cap Z'|<\frac{61m}{240}-\varepsilon m} \Pr_{(A^1_\star,A^2_\star)\sim\mu_\star(S,T)}\left(A^1_\star = Z\right) \Pr_{(B^2,B^1)\sim\mu(T^{rev})}\left(B^2 = Z'\right)\\
&= \sum_{Z,Z':|Z\cap Z'|<\frac{61m}{240}-\varepsilon m} \Pr_{\substack{A^1_\star\sim\mu^1_{\star,single}(S,T)\\A^2_\star\sim\mu^2_{\star,single}(S,T)}}\left(A^1_\star = Z \mid |\mathsf{Part}_{S\|T} \cap A^1_\star \cap A^2_\star| = \vec{\mathsf{spec}}\mathsf{pair}\right)\\
&\qquad\times \Pr_{\substack{B^2\sim\mu_{single}(T^{rev})\\B^1\sim\mu_{single}(T)}}\left(B^2 = Z' \mid |\mathsf{Part}_{T^{rev}} \cap B^2 \cap B^1| = \vec{\mathsf{reg}}\mathsf{pair}\right)\\
&= \sum_{Z,Z':|Z\cap Z'|<\frac{61m}{240}-\varepsilon m} \Pr_{A_\star\sim\mu^1_{\star,single}(S,T)}(A_\star = Z) \Pr_{B\sim\mu_{single}(T^{rev})}(B = Z') \quad \text{(Corollary 4.4)}\\
&= \sum_{Z,Z':|Z\cap Z'|<\frac{61m}{240}-\varepsilon m} \Pr_{\substack{A_\star\sim\mu^1_{\star,single}(S,T)\\B\sim\mu_{single}(T^{rev})}}\left((A_\star, B) = (Z, Z')\right)\\
&= \Pr_{\substack{A_\star\sim\mu^1_{\star,single}(S,T)\\B\sim\mu_{single}(T^{rev})}}\left(|A_\star \cap B| < \frac{61m}{240} - \varepsilon m\right).
\end{aligned}$$

It is thus sufficient to show that $\Pr_{A_\star\sim\mu^1_{\star,single}(S,T),B\sim\mu_{single}(T^{rev})}\left(|A_\star \cap B| < \frac{61m}{240} - \varepsilon m\right) \le \exp(-\varepsilon^2 m/20)$. We show this using Lemma 4.2 as the distribution $\mu^1_{\star,single}(S,T) = \mathsf{PC}\left(16, \mathsf{Part}_{S\|T}, \vec{\mathsf{spec}}_1\right)$ and $\mu_{single}(T^{rev}) = \mathsf{PC}\left(4, \mathsf{Part}_{T^{rev}}, \vec{\mathsf{reg}}\right)$. By Lemma 4.2, we have

$$\Pr_{\substack{A_\star\sim\mu^1_{\star,single}(S,T)\\B\sim\mu_{single}(T^{rev})}}(|A_\star \cap B| < \Delta - \varepsilon m) \le \exp(-\varepsilon^2(m-\Delta)/3),$$

so we just need to compute Δ. Again, recall that the relevant terms come from the vectors $\vec{\mathsf{spec}}_1, \vec{\mathsf{reg}}, \vec{\mathsf{cmp}}$. Expanding the calculations, we get

$$\Delta = \frac{1}{2}\cdot\frac{2}{5}\cdot\frac{4m}{16} + \frac{2}{3}\cdot\frac{m}{16} + \frac{2}{5}\cdot\frac{m}{16} + \frac{1}{3}\cdot\frac{m}{16} + \frac{2}{3}\cdot\frac{m}{16} + \frac{1}{2}\cdot\frac{3}{5}\cdot\frac{4m}{16} = \frac{61}{240}\cdot m.$$

Thus, we get

$$\Pr_{\substack{A_\star\sim\mu^1_{\star,single}(S,T)\\ B\sim\mu_{single}(T^{rev})}}\left(|A_\star\cap B| < \frac{61m}{240} - \varepsilon m\right) \le \exp(-179\varepsilon^2 m/720) < \exp(-\varepsilon^2 m/20),$$

as desired.

Adjusting the proof for $i = 2$ just requires replacing 1 with 2 in the first half of the proof. The calculations for Δ are similar, and also $\ge 61m/240$. ∎

Lemma 5.10 *is the third key property of our construction, which establishes that the union of a special clause for one copy with a regular clause of the other copy is* $< 3m/4$. With the three building blocks and these three properties, we can now define our full construction.

5.2. 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 2.2) that we will use to show Theorem 2.3. Fix $\varepsilon > 0$ and define $n = \exp\left(\frac{\varepsilon^2\cdot m}{100}\right)$. We assume for simplicity that n is an integer. This will be our hard instance for $\mathtt{BXOS}_m$ combinatorial auctions.

- **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 $\vec{A}^1 = A^1_1, \ldots, A^1_n$, etc.):
     (a) For $i \ne i_\star \in [n]$, 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 $\vec{r}^{\mathsf{A}} = r^{\mathsf{A}}_1, \ldots, r^{\mathsf{A}}_n \in \{1,2\}^n$ and $\vec{r}^{\mathsf{B}} = r^{\mathsf{B}}_1, \ldots, r^{\mathsf{B}}_n \in \{1,2\}^n$ 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 $Z \subseteq M$,

$$\mathcal{F}^{\mathsf{A}} = \{A^{r^{\mathsf{A}}_i}_i \mid i \in [n]\} \qquad \text{and} \qquad \mathcal{F}^{\mathsf{B}} = \{B^{r^{\mathsf{B}}_i}_i \mid i \in [n]\}.$$

Before continuing, we briefly elaborate upon each step and connect it to our proof sketch. In (1), we jointly draw a basis for each copy of the modified [BMW18] construction. (S^1, T^1) is the basis for the first copy, and (S^2, T^2) is the basis for the second copy. In step (2), we first draw a uniformly random index in $[n]$ where we will hide the special clauses. Each index i corresponds to *two* clauses for Alice and *two* clauses for Bob. Intuitively, the first clause for Alice is in "copy one" and the second is in "copy two." In (2a), we draw pairs of regular clauses uniformly at random for each nonspecial index for both Alice and Bob. In (2b) we jointly draw

special clauses for Alice and Bob *that are disjoint*. In step (3), we visit each index and pick *one of the two clauses uniformly at random to include*. That is, for each index, there is a "copy one" clause and a "copy two" clause. One of these will be a clause in the defined valuation function in step (4), and one of them will be ignored. Importantly, $r^{\mathsf{A}}_{i^\star} = r^{\mathsf{B}}_{i^\star} = \theta$, meaning that Alice and Bob have a special set from the same copy, and therefore the optimal welfare is m in every instance drawn from ν. This further implies that knowing θ is equivalent to knowing which copy is special. This setup allows us to provide a somewhat clean outline of an information-theoretic proof that learning θ requires exponential communication—$r^{\mathsf{A}}_{i^\star}$ appears indistinguishable from r^{A}_i for all other $i \in [n]$. Therefore, any *simultaneous* algorithm which reveals nontrivial information about $r^{\mathsf{A}}_{i^\star}$ must reveal nontrivial information about all r^{A}_i. We now proceed with analysis of our construction.

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 $v^{\mathsf{A}}_j, v^{\mathsf{B}}_j \in \texttt{BXOS}_m$ 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

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

Intuitively, v^{A}_θ has strictly more clauses than v^{A}; it contains *every* regular clause (but still only one special clause). While of course Alice does not know the valuation v^{A}_θ (because she does not know which clause is special), we can still nonetheless use it to upper bound the value of v^{A} for any set.

5.3. A good allocation determines θ. Two key properties establish ν as a hard distribution. The first property is that θ can be recovered immediately from any allocation which guarantees a $3/4$-approximation. This is captured in Lemma 5.11 below.

We mention that the proof of item 3 of Lemma 5.11 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 randomized simultaneous algorithm of [BMW18] which guarantees a 3/4-approximation in expectation.

In Lemma 5.11 below, item 1 simply states that the optimal welfare is always m. We have given intuition for this immediately following the definition of ν, but the proof below makes this rigorous. Item 2 is straightforward as v^{A}_θ has strictly more clauses than v^{A}. Item 3 is the crucial bullet, which states that (except with exponentially small probability) *no allocation achieves welfare* $3m/4$ *when* $\theta = 1$ *and when* $\theta = 2$. Therefore, learning an allocation which guarantees welfare at least $3m/4$ immediately determines θ.

Recall the definition of $\mathsf{opt}(\cdot)$ from section 2 and that Υ defines $v^{\mathsf{A}}, v^{\mathsf{B}}$.

LEMMA 5.11. *We have the following:*

1. *For all* $\Upsilon \sim \nu$, *we have* $\mathsf{opt}(v^{\mathsf{A}}, v^{\mathsf{B}}) = m$.
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*

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

Proof. We show each part in turn:

1. For the first part, is is enough to show that $\mathsf{opt}(v^{\mathsf{A}}, v^{\mathsf{B}}) \geq m$. We have $\mathsf{opt}(v^{\mathsf{A}}, v^{\mathsf{B}}) \geq v^{\mathsf{A}}(A^{\theta}_{i_\star}) + v^{\mathsf{B}}(\overline{A^{\theta}_{i_\star}}) = v^{\mathsf{A}}(A^{\theta}_{i_\star}) + v^{\mathsf{B}}(B^{\theta}_{i_\star}) = m$.
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:

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

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

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

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 $4n^2 \cdot \exp\left(-\frac{\varepsilon^2 m}{20}\right)$.

We start by showing $\Pr(E_{reg}) \leq 4n^2 \cdot \exp\left(-\frac{\varepsilon^2 m}{20}\right)$. We derive the following using Lemma 5.6:

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

We next show that $\Pr(E^{\mathsf{A}}_{special}) \leq 4n^2 \cdot \exp\left(-\frac{\varepsilon^2 m}{20}\right)$. Using Lemma 5.10, we derive

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

Finally, we show that $\Pr(E^{\mathsf{B}}_{special}) \leq 4n^2 \cdot \exp\left(-\frac{\varepsilon^2 m}{20}\right)$. 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 5.10 to T^{rev}, S^{rev} to get

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

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

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

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

We now prove the claim. Let $Z \subseteq M$ be such that $v_j^{\mathsf{A}}(Z) + v_j^{\mathsf{B}}(\overline{Z}) > \frac{179m}{240} + \varepsilon m$ 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 $|F_j^{\mathsf{A}} \cap Z| + |F_j^{\mathsf{B}} \cap \overline{Z}| > \frac{179m}{240} + \varepsilon m$. We proceed via a case analysis on $F_j^{\mathsf{A}}, F_j^{\mathsf{B}}$ for $j \in \{1,2\}$.

- $\boldsymbol{\exists j \in [2] : F_j^{\mathsf{A}} \neq A_{i_\star}^j \wedge F_j^{\mathsf{B}} \neq B_{i_\star}^j}$**:** Let $j_\star$ be such a j. We use the identity[10] $|Z' \cap Z| + |Z'' \cap \overline{Z}| \leq |Z' \cup Z''|$ for any sets Z, Z', Z'' to get

$$\frac{179m}{240} + \varepsilon m < |F_{j_\star}^{\mathsf{A}} \cap Z| + |F_{j_\star}^{\mathsf{B}} \cap \overline{Z}| \leq |F_{j_\star}^{\mathsf{A}} \cup F_{j_\star}^{\mathsf{B}}|.$$

  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 $|F_{j_\star}^{\mathsf{A}} \cap F_{j_\star}^{\mathsf{B}}| < \frac{61m}{240} - \varepsilon m$. 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** $\boldsymbol{\exists j \in [2] : F_j^{\mathsf{A}} \in \vec{A}^{3-j} \vee F_j^{\mathsf{B}} \in \vec{B}^{3-j}}$**:** 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 5.9). By Definition 5.3 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

$$\frac{179m}{240} + \varepsilon m < |A_{i^{\mathsf{A}}}^{3-j_\star} \cap Z| + |B_{i_\star}^{j_\star} \cap \overline{Z}| \leq |A_{i^{\mathsf{A}}}^{3-j_\star} \cup B_{i_\star}^{j_\star}|.$$

  Next, as $|A_{i^{\mathsf{A}}}^{3-j_\star}| = |B_{i_\star}^{j_\star}| = \frac{m}{2}$, we get $|A_{i^{\mathsf{A}}}^{3-j_\star} \cap B_{i_\star}^{j_\star}| < \frac{61m}{240} - \varepsilon m$. As $i^{\mathsf{A}} \neq i_\star$, this means that $E_{special}^{\mathsf{B}}$, 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 $F_j^{\mathsf{A}} = A_{i_j^{\mathsf{A}}}^j$ and $F_j^{\mathsf{B}} = B_{i_j^{\mathsf{B}}}^j$. We have

[10] To see why this identity holds, note that both the sets $Z', Z'' \subseteq Z' \cup Z''$. This gives $|Z' \cap Z| + |Z'' \cap \overline{Z}| \leq |(Z' \cup Z'') \cap Z| + |(Z' \cup Z'') \cap \overline{Z}|$. As $Z, \overline{Z}$ form a partition of the universe, the latter expression is just $|Z' \cup Z''|$.

that

$$|A^1_{i^{\mathsf{A}}_1} \cap Z| + |B^1_{i^{\mathsf{B}}_1} \cap \overline{Z}| + |A^2_{i^{\mathsf{A}}_2} \cap Z| + |B^2_{i^{\mathsf{B}}_2} \cap \overline{Z}| > 2 \cdot \left(\frac{179m}{240} + \varepsilon m\right).$$

By an averaging argument, this means that there exists $j_\star \in [2]$ such that $|A^{j_\star}_{i^{\mathsf{A}}_{j_\star}} \cap Z| + |B^{3-j_\star}_{i^{\mathsf{B}}_{3-j_\star}} \cap \overline{Z}| > \frac{179m}{240} + \varepsilon m$. 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

$$|A^{j_\star}_{i^{\mathsf{A}}_{j_\star}} \cap B^{3-j_\star}_{i^{\mathsf{B}}_{3-j_\star}}| < \frac{61m}{240} - \varepsilon m.$$

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

$$\begin{aligned}\frac{m}{2} - |A^1_{i_\star} \cap A^2_{i_\star}| &= \frac{m}{2} - |A^{j_\star}_{i_\star} \cap A^{3-j_\star}_{i_\star}| \\ &= |A^{j_\star}_{i_\star} \cap B^{3-j_\star}_{i_\star}| < \frac{61m}{240} - \varepsilon m,\end{aligned}$$

contradicting Definition 5.8. ∎

Again, the key aspects of our construction which we have established so far is that (a) the optimal welfare is always m, and (b) learning an allocation which achieves welfare $\geq 179m/240 + \varepsilon m$ determines θ. Therefore, any algorithm which guarantees a 3/4-approximation also learns θ. It now remains to show that learning θ requires exponential communication.

5.4. Key technical lemma: $i^\star$ is independent of all else. Section 6 contains our final proof that learning θ requires exponential communication. We wrap up this section with one key lemma regarding our construction. Absent any conditioning, $i^\star$ is clearly a uniformly random index in $[n]$. Clearly, $i^\star$ is not uniformly random conditioned on the entire rest of the construction (because it is the only index with a special clause, which can be determined from the rest of the construction). However, we have carefully constructed ν so that $i^\star$ remains a uniformly random index in $[n]$, *even conditioning on Alice's other information* (and ditto for Bob). Lemma 5.12 states this formally.

LEMMA 5.12. *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}.*

Proof. We only show the first claim as the second one is similar. To show that the marginal $i_\star$ is independent of the marginal Υ^{A}, we show that the distribution ν is equivalent to the distribution ν' below. It is clear from the definition of ν' that the marginal $i_\star$ is independent of the marginal Υ^{A}.

- **Sampling** $(v^{\mathsf{A}}, v^{\mathsf{B}}) \sim \nu'$: Recall $n = \exp\left(\frac{\varepsilon^2 \cdot m}{100}\right)$.
  (1) Sample a basis $S \sim \xi_{single}$.
  (2) Construct sequences $\vec{A}^1, \vec{A}^2$ of n subsets of M (where $\vec{A}^1 = A^1_1, \ldots, A^1_n$, etc.) by sampling $(A^1_i, A^2_i) \sim \mu(S)$ independently for $i \in [n]$.
  (3) Sample $i_\star \sim \mathcal{U}([n])$ and let T be sampled uniformly at random such that $|\mathsf{Part}_{S\|T\|A^1_{i_\star}\|A^2_{i_\star}}| = \vec{\mathsf{opt}}$. Observe that any such T is a basis. We show in our proof that at least one such T exists, and therefore this step is well defined.
  (4) Construct sequences $\vec{B}^1, \vec{B}^2$ of n subsets of M (where $\vec{B}^1 = B^1_1, \ldots, B^1_n$, etc.) as follows:
    (a) For $i \neq i_\star \in [n]$, sample $(B^2_i, B^1_i) \sim \mu(T^{rev})$ independently.
    (b) Set $(B^1_{i_\star}, B^2_{i_\star}) = (\overline{A^1_{i_\star}}, \overline{A^2_{i_\star}})$.
  (5) Sample $\theta \in \mathcal{U}(\{1,2\})$ and sequences $\vec{r}^{\mathsf{A}} = r^{\mathsf{A}}_1, \ldots, r^{\mathsf{A}}_n \in \{1,2\}^n$ and $\vec{r}^{\mathsf{B}} = r^{\mathsf{B}}_1, \ldots, r^{\mathsf{B}}_n \in \{1,2\}^n$ uniformly at random subject to $r^{\mathsf{A}}_{i_\star} = r^{\mathsf{B}}_{i_\star} = \theta$.
  (6) 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 $Z \subseteq M$

$$\mathcal{F}^{\mathsf{A}} = \{A^{r^{\mathsf{A}}_i}_i \mid i \in [n]\} \qquad \text{and} \qquad \mathcal{F}^{\mathsf{B}} = \{B^{r^{\mathsf{B}}_i}_i \mid i \in [n]\}.$$

We first show why item (3) in the definition of ν' is well defined. For this, we need to show that for any basis S and any (A^1, A^2) in the support of $\mu(S)$, there exists a T such that $|\mathsf{Part}_{S\|T\|A^1\|A^2}| = \vec{\mathsf{opt}}$. As for any basis S and all (A^1, A^2) in the support of $\mu(S)$, the value of $|\mathsf{Part}_{S\|A^1\|A^2}|$ (Observation 5.5) is the same, by symmetry, it is sufficient to show this for any one (A^1, A^2) in the support of $\mu(S)$ for any one S. But such an $S, (A^1, A^2)$, and T are described in Figure 3

Next, we show why distribution ν is equivalent to distribution ν', proceeding in steps, each time changing the description of ν a little bit so that it eventually becomes ν'. We show that the distributions described in all the steps are equivalent.

- **Step (a):** In this step, we replace line (1) in the definition of ν by the following:
  (1a) Sample a basis $S \sim \xi_{single}$ and basis T uniformly at random such that S is compatible with T. This step is well defined for the same reason as above.

  To show that this does not affect the actual distribution, we use Lemma 4.3. We get that, for all bases Z, Z',

$$\begin{aligned}
\Pr_{(S,T)\sim\xi}((S,T) = (Z,Z')) &= \Pr_{(S,T)\sim\xi}(S = Z) \Pr_{(S,T)\sim\xi}(T = Z' \mid S = Z) \\
&= \Pr_{\substack{S\sim\xi_{single}\\ T\sim\xi_{single}}}\left(S = Z \mid |\mathsf{Part}_{S\|T}| = \vec{\mathsf{cmp}}\right) \Pr_{(S,T)\sim\xi}(T = Z' \mid S = Z) \\
&= \Pr_{S\sim\xi_{single}}(S = Z) \Pr_{(S,T)\sim\xi}(T = Z' \mid S = Z) && \text{(Lemma 4.3)} \\
&= \Pr_{S\sim\xi_{single}}(S = Z) \Pr_{T\sim\xi_{single}}(T = Z' \mid Z \text{ is compatible with } T), \\
& && \text{(Definition of } \xi)
\end{aligned}$$

  as required.
- **Step (b):** In this step, we replace line (1a) from Step (a) and line (2) in the definition of ν by the following:

(1b) Sample a basis $S \sim \xi_{single}$.
(2b) 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 $\vec{A}^1 = A^1_1, \ldots, A^1_n$, etc.):
(a) For $i \neq i_\star \in [n]$, sample $(A^1_i, A^2_i) \sim \mu(S)$ independently.
(b) Sample basis T uniformly at random such that S is compatible with T.
(c) Sample $(A^1_\star, A^2_\star) \sim \mu_\star(S,T)$ and set $(A^1_{i_\star}, A^2_{i_\star}) = (A^1_\star, A^2_\star)$.
(d) For $i \neq i_\star \in [n]$, sample $(B^2_i, B^1_i) \sim \mu(T^{rev})$ independently.
(e) Set $(B^1_{i_\star}, B^2_{i_\star}) = (\overline{A^1_{i_\star}}, \overline{A^2_{i_\star}})$.

This change does not affect the distribution as $i_\star$ and (A^1_i, A^2_i) for $i \neq i_\star$ were picked independently of T and (B^2_i, B^1_i) for $i \neq i_\star$ were picked independently of $(A^1_\star, A^2_\star)$, and thus we can interchange the order in which these are picked.

- **Step (c):** In this step, we replace line (2b) from Step (b) with the following:
(2c) 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 $\vec{A}^1 = A^1_1, \ldots, A^1_n$, etc.):
(a) For $i \in [n]$, sample $(A^1_i, A^2_i) \sim \mu(S)$ independently.
(b) Sample basis T uniformly at random such that $|\mathsf{Part}_{S\|T\|A^1_{i_\star}\|A^2_{i_\star}}| = \vec{\mathsf{opt}}$. Observe that any such T is always a basis.
(c) For $i \neq i_\star \in [n]$, sample $(B^2_i, B^1_i) \sim \mu(T^{rev})$ independently.
(d) Set $(B^1_{i_\star}, B^2_{i_\star}) = (\overline{A^1_{i_\star}}, \overline{A^2_{i_\star}})$.

Before showing that this change does not affect the distribution, we define some helpful notation. For a basis S, we let $\xi_{cmp}(S)$ denote that the uniform distribution over all bases T such that S is compatible with T. Using this notation, we get that for all bases Z and $Z^1, Z^2 \subseteq M$,

$$\begin{aligned}
&\Pr_{T\sim\xi_{cmp}(S)}(T=Z) \Pr_{(A^1_\star,A^2_\star)\sim\mu_\star(S,Z)}\left((A^1_\star,A^2_\star)=(Z^1,Z^2)\right)\\
&\quad= \Pr_{T\sim\xi_{cmp}(S)}(T=Z) \Pr_{(A^1,A^2)\sim\mu(S)}\left((A^1,A^2)=(Z^1,Z^2) \mid |\mathsf{Part}_{S\|Z\|A^1\|A^2}|=\vec{\mathsf{opt}}\right) && \text{(Observation 5.9)}\\
&\quad= \Pr_{T\sim\xi_{cmp}(S)}(T=Z)\\
&\qquad\times \Pr_{\substack{T\sim\xi_{cmp}(S)\\(A^1,A^2)\sim\mu(S)}}\left((A^1,A^2)=(Z^1,Z^2) \mid |\mathsf{Part}_{S\|T\|A^1\|A^2}|=\vec{\mathsf{opt}}, T=Z\right)\\
&\quad= \Pr_{\substack{T\sim\xi_{cmp}(S)\\(A^1,A^2)\sim\mu(S)}}\left((T,A^1,A^2)=(Z,Z^1,Z^2) \mid |\mathsf{Part}_{S\|T\|A^1\|A^2}|=\vec{\mathsf{opt}}\right) && \text{(Observation 5.5, Lemma 4.3)}\\
&\quad= \Pr_{(A^1,A^2)\sim\mu(S)}\left((A^1,A^2)=(Z^1,Z^2)\right)\\
&\qquad\times \Pr_{\substack{T\sim\xi_{cmp}(S)\\(A^1,A^2)\sim\mu(S)}}\left(T=Z \mid |\mathsf{Part}_{S\|T\|A^1\|A^2}|=\vec{\mathsf{opt}}, (A^1,A^2)=(Z^1,Z^2)\right) && \text{(Observation 5.5, Lemma 4.3)}\\
&\quad= \Pr_{(A^1,A^2)\sim\mu(S)}\left((A^1,A^2)=(Z^1,Z^2)\right)\\
&\qquad\times \Pr_{T\sim\xi_{cmp}(S)}\left(T=Z \mid |\mathsf{Part}_{S\|T\|Z^1\|Z^2}|=\vec{\mathsf{opt}}\right),
\end{aligned}$$

as desired.

- **Step (d):** To finish the proof, we claim that ν' is the same as the distri-

bution in Step (c) above. This is because (A_i^1, A_i^2) for $i \in [n]$ were picked independently of $i_\star$ in line (a) of the distribution in Step (c), and thus we can interchange the order in which they are picked. As interchanging this order converts the distribution in Step (c) above to ν', we are done. ∎

6. The proof of Theorem 2.3. In this section, we complete our proof of Theorem 2.3. Our proof crucially relies on Lemmas 5.11 and 5.12 from section 5. Note that the main remaining task is to establish that exponential communication is required to learn nontrivial information about θ.

Proof of Theorem 2.3. Let $\varepsilon > 0$ and $m > \frac{10^{10}}{\varepsilon^2}$ be arbitrary. By Yao's minimax principle, in order to show Theorem 2.3, 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 $\left(\frac{3}{4} - \frac{1}{240} + \varepsilon\right)$-approximate over ν with probability $\frac{1}{2} + \exp\left(-\frac{\varepsilon^2 m}{500}\right)$ satisfies $\mathsf{CC}(\Pi) \geq \exp\left(\frac{\varepsilon^2 m}{500}\right)$.

We let ν denote the distribution defined in subsection 5.2 for m, ε and let Υ be a random variable denoting a sample from ν as in subsection 5.2. Recall how Υ defines the valuation functions v^{A}, v^{B}, and also $v_j^{\mathsf{A}}, v_j^{\mathsf{B}}$ for $j \in [2]$. Fix Π to be a simultaneous deterministic mechanism that is $\left(\frac{3}{4} - \frac{1}{240} + \varepsilon\right)$-approximate over ν with probability $\frac{1}{2} + \exp\left(-\frac{\varepsilon^2 m}{500}\right)$. We have from section 2 that

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

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 5.11, the fact that the functions v^{A} and v^{B} are monotone, and that $\mathsf{alloc}_\Pi^{\mathsf{A}}(v^{\mathsf{A}}, v^{\mathsf{B}})$ and $\mathsf{alloc}_\Pi^{\mathsf{B}}(v^{\mathsf{A}}, v^{\mathsf{B}})$ are disjoint to get the following from equation (1):

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

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

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

be the event from item 3 of Lemma 5.11. By the law to total probability we have

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

using item 3 of Lemma 5.11 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

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

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. In conclusion,

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

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

$$\begin{aligned}
\max_{j \in [2]} \Pr(\theta = j \mid E_\omega, Z(\Upsilon) = Z) &= \frac{1}{2} + \max_{j \in [2]} \left(\Pr(\theta = j \mid E_\omega, Z(\Upsilon) = Z) - \frac{1}{2}\right) \\
&= \frac{1}{2} + \max_{j \in [2]} \left(\Pr(\theta = j \mid E_\omega, Z(\Upsilon) = Z) - \Pr(\theta = j \mid E_\omega)\right) \\
&= \frac{1}{2} + \|\mathrm{dist}(\theta \mid E_\omega, Z(\Upsilon) = Z) - \mathrm{dist}(\theta \mid E_\omega)\|_{tvd} \\
&\qquad \text{(Definition A.8)} \\
&\le \frac{1}{2} + \sqrt{\frac{1}{2} \cdot \mathbb{D}(\mathrm{dist}(\theta \mid E_\omega, Z(\Upsilon) = Z) \mid\mid \mathrm{dist}(\theta \mid E_\omega))}. \\
&\qquad \text{(Fact A.9, item 2)}
\end{aligned}$$

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

$$\begin{aligned}
&\Pr\left(v_\theta^{\mathsf{A}}(Z(\Upsilon)) + v_\theta^{\mathsf{B}}(\overline{Z(\Upsilon)}) > \left(\frac{179}{240} + \varepsilon\right) \cdot m\right) \\
&\quad \le \frac{1}{2} + 12n^2 \cdot \exp\left(-\frac{\varepsilon^2 m}{20}\right) \\
&\qquad + \sqrt{\frac{1}{2} \cdot \sum_{\omega} \sum_{Z \subseteq [m]} \Pr(E_\omega \wedge Z(\Upsilon) = Z) \mathbb{D}(\mathrm{dist}(\theta \mid E_\omega, Z(\Upsilon) = Z) \mid\mid \mathrm{dist}(\theta \mid E_\omega))} \\
&\quad \le \frac{1}{2} + 12n^2 \cdot \exp\left(-\frac{\varepsilon^2 m}{20}\right) + \sqrt{\frac{1}{2} \cdot \mathbb{I}(\theta; Z(\Upsilon) \mid \mathcal{A}, \mathcal{B}, i_\star)}.
\end{aligned} \tag{5}$$

To finish the proof, we make the following claim.

LEMMA 6.1. *It holds that* $\mathbb{I}(\theta; Z(\Upsilon) \mid \mathcal{A}, \mathcal{B}, i_\star) \le 4 \cdot \frac{\mathsf{CC}(\Pi)}{n}$.

We prove Lemma 6.1 later but assuming it for now, we can combine (2) and (5) as

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

and Theorem 2.3 follows using $n = \exp\left(\frac{\varepsilon^2 m}{100}\right)$. ∎

We finish this section by showing Lemma 6.1.

Proof of Lemma 6.1. Let Π^{A} and Π^{B} be random variables denoting the messages 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 A.5 multiple times,

$$\begin{aligned}
&\mathbb{I}(\theta; Z(\Upsilon) \mid \mathcal{A}, \mathcal{B}, i_\star) \leq \mathbb{I}(\theta; \Pi^{\mathsf{A}}\Pi^{\mathsf{B}} \mid \mathcal{A}, \mathcal{B}, i_\star) && \text{(item 5 of Fact A.4)}\\
&= \mathbb{I}(\theta; \Pi^{\mathsf{A}} \mid \mathcal{A}, \mathcal{B}, i_\star) + \mathbb{I}(\theta; \Pi^{\mathsf{B}} \mid \mathcal{A}, \mathcal{B}, i_\star, \Pi^{\mathsf{A}}) && \text{(item 4 of Fact A.4)}\\
&\leq \mathbb{I}(\theta; \Pi^{\mathsf{A}} \mid \mathcal{A}, \mathcal{B}, i_\star) + \mathbb{I}(\theta; \Pi^{\mathsf{B}} \mid \mathcal{A}, \mathcal{B}, i_\star) + \mathbb{I}(\Pi^{\mathsf{A}}; \Pi^{\mathsf{B}} \mid \mathcal{A}, \mathcal{B}, i_\star, \theta)\\
&\leq \mathbb{I}(\theta; \Pi^{\mathsf{A}} \mid \mathcal{A}, i_\star) + \mathbb{I}(\theta; \Pi^{\mathsf{B}} \mid \mathcal{B}, i_\star)\\
&\qquad + \mathbb{I}(\mathcal{B}; \Pi^{\mathsf{A}} \mid \mathcal{A}, i_\star, \theta) + \mathbb{I}(\mathcal{A}; \Pi^{\mathsf{B}} \mid \mathcal{B}, i_\star, \theta) + \mathbb{I}(\Pi^{\mathsf{A}}; \Pi^{\mathsf{B}} \mid \mathcal{A}, \mathcal{B}, i_\star, \theta).
\end{aligned}$$

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 $\mathcal{A}, \vec{r}^{\mathsf{A}}$. Similarly, Π^{B} is a function of Bob's input v^{B}, and therefore a function of $\mathcal{B}, \vec{r}^{\mathsf{B}}$. For the term $\mathbb{I}(\mathcal{B}; \Pi^{\mathsf{A}} \mid \mathcal{A}, i_\star, \theta)$, we get $\mathbb{I}(\mathcal{B}; \Pi^{\mathsf{A}} \mid \mathcal{A}, i_\star, \theta) \leq \mathbb{I}(\mathcal{B}; \mathcal{A}\vec{r}^{\mathsf{A}} \mid \mathcal{A}, i_\star, \theta) = \mathbb{I}(\mathcal{B}; \vec{r}^{\mathsf{A}}_{-i_\star} \mid \mathcal{A}, i_\star, \theta) = 0$ as $\theta = r^{\mathsf{A}}_{i_\star}$ and $\vec{r}^{\mathsf{A}}_{-i_\star}$ is sampled independently of $\mathcal{A}, \mathcal{B}, i_\star, \theta$. Recall that $\vec{r}^{\mathsf{A}}_{-i_\star}$ denotes $\vec{r}^{\mathsf{A}}$ with the coordinate $i_\star$ removed. Similarly, we can deduce that $\mathbb{I}(\mathcal{A}; \Pi^{\mathsf{B}} \mid \mathcal{B}, i_\star, \theta) = 0$. Finally, for the term $\mathbb{I}(\Pi^{\mathsf{A}}; \Pi^{\mathsf{B}} \mid \mathcal{A}, \mathcal{B}, i_\star, \theta)$, we get $\mathbb{I}(\Pi^{\mathsf{A}}; \Pi^{\mathsf{B}} \mid \mathcal{A}, \mathcal{B}, i_\star, \theta) \leq \mathbb{I}(\mathcal{A}\vec{r}^{\mathsf{A}}; \mathcal{B}\vec{r}^{\mathsf{B}} \mid \mathcal{A}, \mathcal{B}, i_\star, \theta) = \mathbb{I}(\vec{r}^{\mathsf{A}}_{-i_\star}; \vec{r}^{\mathsf{B}}_{-i_\star} \mid \mathcal{A}, \mathcal{B}, i_\star, \theta) = 0$ as $\vec{r}^{\mathsf{A}}_{-i_\star}$ is sampled independently of $\vec{r}^{\mathsf{B}}_{-i_\star}, \mathcal{A}, \mathcal{B}, i_\star, \theta$. Combining, we get

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

We next show that $\mathbb{I}(\theta; \Pi^{\mathsf{A}} \mid \mathcal{A}, i_\star) \leq 2 \cdot \frac{\mathsf{CC}(\Pi)}{n}$. A similar argument shows that $\mathbb{I}(\theta; \Pi^{\mathsf{B}} \mid \mathcal{B}, i_\star) \leq 2 \cdot \frac{\mathsf{CC}(\Pi)}{n}$, finishing the proof of Lemma 6.1. As $\theta = r^{\mathsf{A}}_{i_\star}$, Π^{A} is a function of $\mathcal{A}$ and $\vec{r}^{\mathsf{A}}$, and $i_\star$ is sampled from $\mathcal{U}([n])$, we have the following by Lemma 5.12:

$$\begin{aligned}
\mathbb{I}(\theta; \Pi^{\mathsf{A}} \mid \mathcal{A}, i_\star) &= \mathbb{I}(r^{\mathsf{A}}_{i_\star}; \Pi^{\mathsf{A}} \mid \mathcal{A}, i_\star)\\
&\leq \frac{1}{n} \cdot \mathbb{I}(r^{\mathsf{A}}; \Pi^{\mathsf{A}} \mid \mathcal{A}) && \text{(Lemma A.6)}\\
&\leq \frac{1}{n} \cdot \mathbb{H}(\Pi^{\mathsf{A}}) \leq \frac{\mathsf{CC}(\Pi) + 1}{n} \leq 2 \cdot \frac{\mathsf{CC}(\Pi)}{n}.
\end{aligned}$$

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

Appendix A. Tools from information theory. We include 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.

A.1. Entropy and mutual information.

DEFINITION A.1 (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 A.2 (conditional entropy). *Let X and Y be discrete random variables. The entropy of X conditioned on Y is defined as*

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

DEFINITION A.3 (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 A.4. *The following holds for discrete random variables W, X, Y, Z:*

1. *We have $\mathbb{H}(XY) = \mathbb{H}(X) + \mathbb{H}(Y \mid X) \le \mathbb{H}(X) + \mathbb{H}(Y)$. Equality holds if X and Y are independent.*
2. *If the random variable X takes values in the set Ω, it holds that $0 \le \mathbb{H}(X) \le \log|\Omega|$.*
3. *We have $0 \le \mathbb{I}(X; Y \mid Z) \le \mathbb{H}(X)$ and $\mathbb{I}(X; Y \mid Z) = 0$ if and only if X is independent of Y given Z.*
4. *Chain rule of mutual information:*

$$\mathbb{I}(WX; Y \mid Z) = \mathbb{I}(W; Y \mid Z) + \mathbb{I}(X; Y \mid WZ).$$

5. *Data processing inequality: for any deterministic function f,*

$$\mathbb{I}(X; f(Y) \mid Z) \le \mathbb{I}(X; Y \mid Z).$$

We also use the following technical lemmas about mutual information.

LEMMA A.5. *For discrete random variables W, X, Y, and Z, we have*

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

Proof. Observe that

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

∎

LEMMA A.6. *Let $n > 0$ and $X = X_1, X_2, \ldots, X_n$, where $X_1, X_2, \ldots, X_n$ 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. Using the fact that I is distributed uniformly over $[n]$, we get

$$\begin{aligned}
\mathbb{I}(X_I; f(X,Y) \mid Y, I) &= \mathbb{H}(f(X,Y) \mid Y, I) - \mathbb{H}(f(X,Y) \mid X_I, Y, I) && \text{(Definition A.3)} \\
&= \frac{1}{n} \cdot \sum_{i \in [n]} \Bigg(\mathop{\mathbb{E}}_{y \sim \mathrm{dist}(Y)} [\mathbb{H}(f(X,Y) \mid Y = y, I = i)] \\
&\qquad - \mathop{\mathbb{E}}_{y \sim \mathrm{dist}(Y)} \mathop{\mathbb{E}}_{x \sim \mathrm{dist}(X_i)} [\mathbb{H}(f(X,Y) \mid X_i = x, Y = y, I = i)] \Bigg) \\
& && \text{(Definition A.2)} \\
&= \frac{1}{n} \cdot \sum_{i \in [n]} \Bigg(\mathop{\mathbb{E}}_{y \sim \mathrm{dist}(Y)} [\mathbb{H}(f(X,Y) \mid Y = y)] \\
&\qquad - \mathop{\mathbb{E}}_{y \sim \mathrm{dist}(Y)} \mathop{\mathbb{E}}_{x \sim \mathrm{dist}(X_i)} [\mathbb{H}(f(X,Y) \mid X_i = x, Y = y)] \Bigg) \\
& && \text{(independence of } I \text{ and } (X,Y)) \\
&= \frac{1}{n} \cdot \sum_{i \in [n]} \mathbb{H}(f(X,Y) \mid Y) - \mathbb{H}(f(X,Y) \mid X_i, Y) && \text{(Definition A.2)} \\
&= \frac{1}{n} \cdot \sum_{i \in [n]} \mathbb{I}(X_i; f(X,Y) \mid Y) && \text{(Definition A.3)} \\
&\leq \frac{1}{n} \cdot \sum_{i \in [n]} \mathbb{I}(X_i; f(X,Y) \mid Y, X_{<i}) + \mathbb{I}(X_i; X_{<i} \mid Y) && \text{(Lemma A.5)} \\
&= \frac{1}{n} \cdot \sum_{i \in [n]} \mathbb{I}(X_i; f(X,Y) \mid Y, X_{<i}) && \text{(item 3, Fact A.4)} \\
&= \frac{1}{n} \cdot \mathbb{I}(X; f(X,Y) \mid Y). && \text{(Item 4, Fact A.4)}
\end{aligned}$$

∎

A.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 A.7 (KL-divergence). *For two distributions μ and ν over the same set Ω, the KL-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 A.8 (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 A.9. *The following hold:*

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

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

2. (Pinsker's inequality) *For any distributions μ and ν, we have*

$$\|\mu - \nu\|_{tvd} \le \sqrt{\frac{1}{2} \cdot \mathbb{D}(\mu \mid\mid \nu)}.$$

Appendix B. Omitted proofs.

Proof of Theorem 2.1 *assuming Theorem* 2.3. The proof is by contradiction. Suppose that Theorem 2.3 is true and Theorem 2.1 is not. Let $P(\cdot)$ be the polynomial promised by Theorem 2.2, and let d be the degree of P. Define $\beta = \frac{1}{500(d+1)}$. Let $\varepsilon_\star > 0$ be the constant promised by the negation of Theorem 2.1 for this value of β (recall that we assume that Theorem 2.1 is false). Let m_1 be large enough so that (1) $P(m') \le m'^{d+1}$ for all $m' > m_1$, (2) $\exp(\beta\varepsilon_\star^2 \cdot m') \ge m'$ for all $m' > m_1$, and (3) $m_1 > \frac{10^{10}}{\varepsilon_\star^2}$.

Using our assumption that Theorem 2.1 is false, we get that there is an $m > m_1$, and a randomized, m-item, $\mathtt{XOS}_m$-combinatorial auction Π with two bidders and one seller that is truthful, is $\left(\frac{3}{4} - \frac{1}{240} + \varepsilon_\star\right)$-approximate with probability $\frac{1}{2} + \exp(-\beta\varepsilon_\star^2 \cdot m)$, and satisfies $\mathsf{CC}(\Pi) < \exp(\beta\varepsilon_\star^2 \cdot m)$.

Plugging Π into Theorem 2.2, we get a randomized, m-item, $\mathtt{XOS}_m$-combinatorial auction Π' with two bidders and one seller that is simultaneous and $\left(\frac{3}{4} - \frac{1}{240} + \varepsilon_\star\right)$-approximate with probability $\frac{1}{2} + \exp(-\beta\varepsilon_\star^2 \cdot m) > \frac{1}{2} + \exp\left(-\frac{\varepsilon_\star^2 m}{500}\right)$ and satisfies (using $m > m_1$)

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

This contradicts Theorem 2.3 and we are done. ∎

B.1. Omitted proofs from section 4.1.

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

DEFINITION B.1 (negatively correlated random variables). *For $n > 0$, let $X_1, \ldots, X_n$ be random variables taking values in $\{0,1\}$. The random variables $X_1, \ldots, X_n$ are* negatively correlated *if for all subsets $S \subseteq [n]$, we have* $\Pr(\forall i \in S : X_i = 1) \le \prod_{i\in S} \Pr(X_i = 1)$.

LEMMA B.2 (generalized Chernoff bound; cf. [PS97]). *For $n > 0$, let $X_1, \ldots, X_n$ be negatively correlated random variables that take values in $\{0,1\}$. Then, for any $\varepsilon > 0$, we have (where $\mu = \sum_{i\in[n]} \mathbb{E}[X_i] \le n$)*

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

Much of the proofs in this section will follow by connecting $\mathsf{PC}(k, \vec{P}, \vec{p})$ to a related product distribution, defined below.

DEFINITION B.3. *For a partition parameter* $(k, \vec{P}, \vec{p})$*, define* $\mathsf{PC\text{-}ally}(k, \vec{P}, \vec{p})$ *to be the distribution over subsets of* M *such that we have* $\Pr_{U \sim \mathsf{PC\text{-}ally}(D)}(z \in U) = \frac{p_{\vec{P}[z]}}{|P_{\vec{P}[z]}|}$ *independently for all* $z \in M$*.*

We will need the following technical lemmas about partition parameters.

LEMMA B.4. *For any subset* $S \subseteq M$ *and any partition parameter* $(k, \vec{P}, \vec{p})$*, it holds that*

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

Proof. We have

$$\begin{aligned}
\Pr_{U \sim \mathsf{PC}(k,\vec{P},\vec{p})}(U \cap S = \emptyset) &= \frac{|\{U \subseteq \overline{S} \mid |\vec{P} \cap U| = \vec{p}\}|}{|\{U \subseteq M \mid |\vec{P} \cap U| = \vec{p}\}|} \\
&= \frac{\prod_{i \in [k]:|P_i|>0} \binom{|\overline{S} \cap P_i|}{p_i}}{\prod_{i \in [k]:|P_i|>0} \binom{|P_i|}{p_i}} \\
&= \prod_{i \in [k]:|P_i|>0} \frac{(|P_i| - p_i)\,(|P_i| - p_i - 1) \cdots \left(|\overline{S} \cap P_i| - p_i + 1\right)}{|P_i|\,(|P_i| - 1) \cdots \left(|\overline{S} \cap P_i| + 1\right)} \\
&\leq \prod_{i \in [k]:|P_i|>0} \left(1 - \frac{p_i}{|P_i|}\right)^{|S \cap P_i|} = \Pr_{U \sim \mathsf{PC\text{-}ally}(k,\vec{P},\vec{p})}(U \cap S = \emptyset). \qquad \square
\end{aligned}$$

COROLLARY B.5. *For any partition parameter* $(k, \vec{P}, \vec{p})$ *and any distribution* D^* *over subsets of* M*, it holds that*

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

Proof. We have

$$\begin{aligned}
\Pr_{\substack{U \sim \mathsf{PC}(k,\vec{P},\vec{p}) \\ U^* \sim D^*}}(U \cap U^* = \emptyset) &= \sum_{S \subseteq M} \Pr_{\substack{U \sim \mathsf{PC}(k,\vec{P},\vec{p}) \\ U^* \sim D^*}}(U \cap S = \emptyset, U^* = S) \\
&= \sum_{S \subseteq M} \Pr_{U \sim \mathsf{PC}(k,\vec{P},\vec{p})}(U \cap S = \emptyset) \Pr_{U^* \sim D^*}(U^* = S) \\
&\leq \sum_{S \subseteq M} \Pr_{U \sim \mathsf{PC\text{-}ally}(k,\vec{P},\vec{p})}(U \cap S = \emptyset) \Pr_{U^* \sim D^*}(U^* = S) \qquad \text{(Lemma B.4)} \\
&= \sum_{S \subseteq M} \Pr_{\substack{U \sim \mathsf{PC\text{-}ally}(k,\vec{P},\vec{p}) \\ U^* \sim D^*}}(U \cap S = \emptyset, U^* = S) \\
&= \Pr_{\substack{U \sim \mathsf{PC\text{-}ally}(k,\vec{P},\vec{p}) \\ U^* \sim D^*}}(U \cap U^* = \emptyset). \qquad \square
\end{aligned}$$

Proof of Lemma 4.2. Let D denote the partition parameter $(k, \vec{P}, \vec{p})$ and D' denote the parameter $(k', \vec{P'}, \vec{p'})$. Let U and U' be sets sampled from distributions $\mathsf{PC}(D)$ and $\mathsf{PC}(D')$, respectively. For $z \in M$, we define the indicator random variable

X_z to be such that $X_z = 1$ if and only if $z \notin U \cap U'$. We have that

(6)
$$\mathbb{E}[X_z] = \Pr(X_z = 1) = \Pr_{\substack{U\sim\mathsf{PC}(D)\\U'\sim\mathsf{PC}(D')}}(z \notin U \cap U') = 1 - \Pr_{\substack{U\sim\mathsf{PC}(D)\\U'\sim\mathsf{PC}(D')}}(z \in U \cap U')$$
$$= 1 - \Pr_{U\sim\mathsf{PC}(D)}(z \in U) \cdot \Pr_{U'\sim\mathsf{PC}(D')}(z \in U') = 1 - \frac{p_{\vec{P}[z]}}{|P_{\vec{P}[z]}|} \cdot \frac{p'_{\vec{P}'[z]}}{|P'_{\vec{P}'[z]}|},$$

implying $\sum_{z\in[m]} \mathbb{E}[X_z] = m - \sum_{z\in M} \frac{p_{\vec{P}[z]}}{|P_{\vec{P}[z]}|} \cdot \frac{p'_{\vec{P}'[z]}}{|P'_{\vec{P}'[z]}|}. = m - \Delta$. We now show that the random variables $X_1, \ldots, X_m$ are negatively correlated (Definition B.1), whence it follows from Lemma B.2 that

$$\Pr_{\substack{U\sim\mathsf{PC}(D)\\U'\sim\mathsf{PC}(D')}}(|U \cap U'| < \Delta - \varepsilon m) = \Pr\left(\sum_{z\in[m]} X_z > \sum_{z\in[m]} \mathbb{E}[X_z] + \varepsilon m\right)$$
$$\leq \exp(-\varepsilon^2(m-\Delta)/3).$$

In order to show that the random variables $X_1, \ldots, X_m$ are negatively correlated, we pick an arbitrary subset S of M and show that $\Pr(\forall z \in S : X_z = 1) \leq \prod_{z\in S} \Pr(X_z = 1)$. We have

$$\begin{aligned}
\Pr(\forall z \in S : X_z = 1) &= \Pr_{\substack{U\sim\mathsf{PC}(D)\\U'\sim\mathsf{PC}(D')}}(S \cap U \cap U' = \emptyset)\\
&\leq \Pr_{\substack{U\sim\mathsf{PC\text{-}ally}(D)\\U'\sim\mathsf{PC}(D')}}(S \cap U \cap U' = \emptyset) && \text{(Corollary B.5)}\\
&\leq \Pr_{\substack{U\sim\mathsf{PC\text{-}ally}(D)\\U'\sim\mathsf{PC\text{-}ally}(D')}}(S \cap U \cap U' = \emptyset) && \text{(Corollary B.5)}\\
&= \Pr_{\substack{U\sim\mathsf{PC\text{-}ally}(D)\\U'\sim\mathsf{PC\text{-}ally}(D')}}(\forall z \in S : z \notin U \cap U')\\
&= \prod_{z\in S} \Pr_{\substack{U\sim\mathsf{PC\text{-}ally}(D)\\U'\sim\mathsf{PC\text{-}ally}(D')}}(z \notin U \cap U')\\
&= \prod_{z\in S}\left(1 - \frac{p_{\vec{P}[z]}}{|P_{\vec{P}[z]}|} \cdot \frac{p'_{\vec{P}'[z]}}{|P'_{\vec{P}'[z]}|}\right)\\
&= \prod_{z\in S} \Pr(X_z = 1). && \text{(equation (6))}
\end{aligned}$$

∎

Proof of Lemma 4.3. We only argue for the case $j = 1$ as the case $j = 2$ is symmetric. Let $\mathcal{C}$ be the set of all sequences $\vec{Z}'$ of k_1 subsets of M satisfying $|\mathsf{Part}_{\vec{S}\|\vec{Z}'}| = \vec{a}_1$. If $\vec{Z} \notin \mathcal{C}$, then the result holds as both the terms are 0. We thus assume that $\vec{Z} \in \mathcal{C}$. We immediately get $\Pr_{\vec{S}_1\sim\mu_1}(\vec{S}_1 = \vec{Z}) = \frac{1}{|\mathcal{C}|}$.

For $\vec{Z}' \in \mathcal{C}$, define the set $\mathcal{D}(\vec{Z}')$ to be the set of all sequences $\vec{Z}''$ of k_2 subsets of M such that $|\mathsf{Part}_{\vec{S}\|\vec{Z}'\|\vec{Z}''}| = \vec{a}$. Owing to the fact that $\Pr_{\vec{S}_1\sim\mu_1,\vec{S}_2\sim\mu_2}(|\mathsf{Part}_{\vec{S}\|\vec{S}_1\|\vec{S}_2}| =$

$\vec{a}\big) > 0$, we have $|\mathsf{Part}_{\vec{S}\|\vec{Z}''}| = \vec{a}_2$ for all $\vec{Z}'' \in \mathcal{D}(\vec{Z}')$. Furthermore, by symmetry, the value of $|\mathcal{D}(\vec{Z}')|$ is the same for all $\vec{Z}' \in \mathcal{C}$.

It follows that

$$\Pr_{\substack{\vec{S}_1\sim\mu_1\\ \vec{S}_2\sim\mu_2}}\Big(\vec{S}_1 = \vec{Z} \mid |\mathsf{Part}_{\vec{S}\|\vec{S}_1\|\vec{S}_2}| = \vec{a}\Big) = \frac{|\mathcal{D}(\vec{Z})|}{\sum_{\vec{Z}'\in\mathcal{C}}|\mathcal{D}(\vec{Z}')|} = \frac{1}{|\mathcal{C}|},$$

finishing the proof. ∎

Proof of Corollary 4.4. Observe that there exist unique $\vec{a}'_1 = \vec{a}'_1(\vec{S}, \vec{a}_1)$ and $\vec{a}'_2 = \vec{a}'_2(\vec{S}, \vec{a}_2)$, both in $\mathbb{Z}^{2^{k+1}}$ such that, for any $j \in \{1, 2\}$ and $A \subseteq M$,

$$|\mathsf{Part}_{\vec{S}} \cap A| = \vec{a}_j \iff |\mathsf{Part}_{\vec{S}\|A}| = \vec{a}'_j.$$

Similarly, for any $\vec{a}$ such that $\Pr_{A_1\sim\mu_1, A_2\sim\mu_2}\big(|\mathsf{Part}_{\vec{S}} \cap A_1 \cap A_2| = \vec{a}\big) > 0$, there exists a unique $\vec{a}' = \vec{a}'(\vec{S}, \vec{a}_1, \vec{a}_2, \vec{a}) \in \mathbb{Z}^{2^{k+2}}$ such that, for all A_1, A_2 such that $|\mathsf{Part}_{\vec{S}} \cap A_j| = \vec{a}_j$ for $j \in [2]$, we have

$$|\mathsf{Part}_{\vec{S}} \cap A_1 \cap A_2| = \vec{a} \iff |\mathsf{Part}_{\vec{S}\|A_1\|A_2}| = \vec{a}'.$$

The proof then follows by applying Lemma 4.3 with $k_1 = k_2 = 1$. ∎

Acknowledgment. We are grateful to the anonymous referees for their comments, which greatly improved the presentation of this paper.

REFERENCES

[ANRW15] N. Alon, N. Nisan, R. Raz, and O. Weinstein, *Welfare maximization with limited interaction*, in Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2015, pp. 1499–1512.

[AS19] S. Assadi and S. Singla, *Improved truthful mechanisms for combinatorial auctions with submodular bidders*, in Proceedings of the 60th Annual IEEE Foundations of Computer Science (FOCS), 2019, pp. 233–248.

[Ass17] S. Assadi, *Combinatorial auctions do need modest interaction*, in Proceedings of the 2017 ACM Conference on Economics and Computation (EC'17), 2017, pp. 145–162.

[BDF+10] D. Buchfuhrer, S. Dughmi, H. Fu, R. Kleinberg, E. Mossel, C. H. Papadimitriou, M. Schapira, Y. Singer, and C. Umans, *Inapproximability for VCG-based combinatorial auctions*, in Proceedings of the Twenty-First Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), SIAM, 2010, pp. 518–536, https://doi.org/10.1137/1.9781611973075.45.

[BDF+12] A. Badanidiyuru, S. Dobzinski, H. Fu, R. Kleinberg, N. Nisan, and T. Roughgarden, *Sketching valuation functions*, in Proceedings of the Twenty-Third Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), SIAM, 2012, pp. 1025–1035, https://doi.org/10.1137/1.9781611973099.81.

[BGKL03] L. Babai, A. Gál, P. G. Kimmel, and S. V. Lokam, *Communication complexity of simultaneous messages*, SIAM J. Comput., 33 (2003), pp. 137–166, https://doi.org/10.1137/S0097539700375944.

[BMW18] M. Braverman, J. Mao, and S. M. Weinberg, *On simultaneous two-player combinatorial auctions*, in Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), SIAM, 2018, pp. 2256–2273, https://doi.org/10.1137/1.9781611975031.146.

[Cla71] E. H. Clarke, *Multipart pricing of public goods*, Public Choice, 11 (1971), pp. 17–33.

[CT06] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed., Wiley, 2006.

[CTW20] L. Cai, C. Thomas, and S. M. 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), Dagstuhl, 2020, 61.

[DGS84] P. Duris, Z. Galil, and G. Schnitger, *Lower bounds on communication complexity*, in Proceedings of the Sixteenth Annual ACM Symposium on Theory of Computing, STOC '84, ACM, 1984, pp. 81–91.

[DN11] S. Dobzinski and N. Nisan, *Limitations of VCG-based mechanisms*, Combinatorica, 31 (2011), pp. 379–396.

[DN15] S. Dobzinski and N. Nisan, *Multi-unit auctions: Beyond Roberts*, J. Economic Theory, 156 (2015), pp. 14–44.

[DNO14] S. Dobzinski, N. Nisan, and S. Oren, *Economic efficiency requires interaction*, in Proceedings of the 46th Annual ACM Symposium on Theory of Computing (STOC), 2014, pp. 233–242.

[DNS10] S. Dobzinski, N. Nisan, and M. Schapira, *Approximation algorithms for combinatorial auctions with complement-free bidders*, Math. Oper. Res., 35 (2010), pp. 1–13.

[Dob07] S. 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, Springer-Verlag, 2007, pp. 89–103.

[Dob11] S. Dobzinski, *An impossibility result for truthful combinatorial auctions with submodular valuations*, in Proceedings of the 43rd ACM Symposium on Theory of Computing (STOC), 2011, 5.

[Dob16a] S. 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), ACM, 2016, pp. 940–948.

[Dob16b] S. Dobzinski, *Computational efficiency requires simple taxation*, in Proceedings of the 57th Annual Symposium on Foundations of Computer Science (FOCS), IEEE, 2016, pp. 209–218.

[DS06] S. Dobzinski and M. Schapira, *An improved approximation algorithm for combinatorial auctions with submodular bidders*, in Proceedings of the Seventeenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), SIAM, 2006, pp. 1064–1073.

[DSS15] A. Daniely, M. Schapira, and G. 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, pp. 401–408.

[DV11] S. Dughmi and J. Vondrak, *Limitations of randomized mechanisms for combinatorial auctions*, Games Econom. Behav., 92 (2015), pp. 370–400.

[DV12a] S. Dobzinski and J. Vondrák, *From query complexity to computational complexity*, in Proceedings of the 44th Symposium on Theory of Computing (STOC), ACM, 2012, pp. 1107–1116.

[DV12b] S. Dobzinski and J. Vondrak, *The computational complexity of truthfulness in combinatorial auctions*, in Proceedings of the ACM Conference on Electronic Commerce (EC), 2012, pp. 405–422.

[DV16] S. Dobzinski and J. Vondrák, *Impossibility results for truthful combinatorial auctions with submodular valuations*, J. ACM, 63 (2016), 5.

[EFN+19] T. Ezra, M. Feldman, E. Neyman, I. Talgam-Cohen, and S. M. Weinberg, *Settling the communication complexity of combinatorial auctions with two subadditive buyers*, in Proceedings of the 60th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2019, pp. 249–272.

[Fei09] U. Feige, *On maximizing welfare when utility functions are subadditive*, SIAM J. Comput., 39 (2009), pp. 122–142, https://doi.org/10.1137/070680977.

[FV10] U. Feige and J. Vondrák, *The submodular welfare problem with demand queries*, Theory Comput., 6 (2010), pp. 247–290.

[Gro73] T. Groves, *Incentives in teams*, Econometrica, 41 (1973), pp. 617–631.

[KV12] P. Krysta and B. Vöcking, *Online mechanism design (randomized rounding on the fly)*, in Automata, Languages, and Programming (ICALP), Springer, 2012, pp. 636–647.

[LMN03] R. Lavi, A. Mu'alem, and N. Nisan, *Towards a characterization of truthful combinatorial auctions*, in Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2003, pp. 574–583.

[LOS02] D. Lehmann, L. O'Callaghan, and Y. Shoham, *Truth revelation in approximately efficient combinatorial auctions*, J. ACM, 49 (2002), pp. 577–602.

[LS05] R. Lavi and C. Swamy, *Truthful and near-optimal mechanism design via linear programming*, J. ACM, 58 (2011), 25.

[MSV08] V. S. Mirrokni, M. Schapira, and J. Vondrák, *Tight information-theoretic lower*

bounds for welfare maximization in combinatorial auctions, in Proceedings of the 9th ACM Conference on Electronic Commerce (EC), 2008, pp. 70–77.

[NS06] N. Nisan and I. Segal, *The communication requirements of efficient allocations and supporting prices*, J. Economic Theory, 129 (2006), pp. 192–224.

[NW93] N. Nisan and A. Wigderson, *Rounds in communication complexity revisited*, SIAM J. Comput., 22 (1993), pp. 211–219, https://doi.org/10.1137/0222016.

[PS82] C. H. Papadimitriou and M. Sipser, *Communication complexity*, in Proceedings of the 14th Annual ACM Symposium on Theory of Computing (STOC), ACM, 1982, pp. 196–200.

[PS97] A. Panconesi and A. Srinivasan, *Randomized distributed edge coloring via an extension of the Chernoff–Hoeffding bounds*, SIAM J. Comput., 26 (1997), pp. 350–368, https://doi.org/10.1137/S0097539793250767.

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

[Vic61] W. Vickrey, *Counterspeculations, auctions, and competitive sealed tenders*, J. Finance, 16 (1961), pp. 8–37.

[Von08] J. 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 (STOC), 2008, pp. 67–74.