On Simultaneous Two-player Combinatorial Auctions *

Mark Braverman † Jieming Mao ‡ S. Matthew Weinberg §

Abstract

We consider the following communication problem: Alice and Bob each have some valuation functions $v_1(\cdot)$ and $v_2(\cdot)$ over subsets of m items, and their goal is to partition the items into $S, \bar{S}$ in a way that maximizes the *welfare*, $v_1(S)+v_2(\bar{S})$. We study both the *allocation problem*, which asks for a welfare-maximizing partition and the *decision problem*, which asks whether or not there exists a partition guaranteeing certain welfare, for binary XOS valuations. For interactive protocols with poly(m) communication, a tight 3/4-approximation is known for both [29, 23].

For interactive protocols, the allocation problem is provably *harder* than the decision problem: any solution to the allocation problem implies a solution to the decision problem with one additional round and $\log m$ additional bits of communication via a trivial reduction. Surprisingly, the allocation problem is provably *easier* for simultaneous protocols. Specifically, we show:

- There exists a simultaneous, randomized protocol with polynomial communication that selects a partition whose expected welfare is at least 3/4 of the optimum. This matches the guarantee of the best interactive, randomized protocol with polynomial communication.
- For all $\varepsilon > 0$, any simultaneous, randomized protocol that decides whether the welfare of the optimal partition is ≥ 1 or $\leq 3/4 - 1/108 + \varepsilon$ correctly with probability $> 1/2 + 1/\text{poly}(m)$ requires exponential communication. This provides a separation between the attainable approximation guarantees via interactive (3/4) versus simultaneous ($\leq 3/4 - 1/108$) protocols with polynomial communication.

In other words, this trivial reduction from decision to allocation problems provably requires the extra round of communication. We further discuss the implications of our results for the design of truthful combinatorial auctions in general, and extensions to general XOS valuations. In particular, our protocol for the allocation problem implies a new style of truthful mechanisms.

1 Introduction

Intuitively, search problems (find the optimal solution) are considered "strictly harder" than decision problems (does a solution with quality $\geq Q$ exist?) for the following (formal) reason: once you find the optimal solution, you can simply evaluate it and check whether its quality is $\geq Q$ or not. The same intuition carries over to approximation as well: once you find a solution whose quality is within a factor α of optimal, you can distinguish between cases where solutions with quality $\geq Q$ exist and those where all solutions have quality $\leq \alpha Q$. The easy conclusion one then draws is that the communication (resp. runtime) required for an α-approximation to any decision problem is upper bounded by the communication (resp. runtime) required for an α-approximation to the corresponding search problem plus the communication (resp. runtime) required to evaluate the quality of a proposed solution.

Note though that for communication problems, in addition to the negligible increase in communication (due to evaluating the quality of the proposed solution), this simple reduction might also require (at least) an extra round of communication (because the parties can evaluate a solution's quality only after it is found). Still, it seems hard to imagine that this extra round is really necessary, and that somehow protocols exist that guarantee an (approximately) optimal solution without (approximately) learning their quality. The surprising high-level takeaway from our main results is that *this extra round of communication is provably necessary*: Theorems 1.1 and 1.2 provide a natural communication problem (combinatorial auctions) such that a 3/4-approximation for the search problem can be found by

*Full version of this paper can be found at https://arxiv.org/abs/1704.03547

†Department of Computer Science, Princeton University, email: mbraverm@cs.princeton.edu. Research supported in part by an NSF CAREER award (CCF-1149888), NSF CCF-1215990, NSF CCF-1525342, a Packard Fellowship in Science and Engineering, and the Simons Collaboration on Algorithms and Geometry.

‡Department of Computer Science, Princeton University, email: jiemingm@cs.princeton.edu.

§Department of Computer Science, Princeton University, email: smweinberg@princeton.edu. Research completed in part while the author was a Research Fellow at the Simons Institute for the Theory of Computing.

a simultaneous protocol[1] with polynomial communication, but every simultaneous prootcol guaranteeing a $(3/4 - 1/108 + \varepsilon)$-approximation for the decision problem requires $\exp(m)$ communication.

At this point, we believe our results to have standalone interest, regardless of how we wound up at this specific communication problem. But there is a rich history related to the design of truthful combinatorial auctions motivating our specific question, which we overview below.

1.1 Combinatorial Auctions - how did we get here? In a combinatorial auction, a designer with m items wishes to allocate them to n bidders so as to maximize the *social welfare*. That is, if bidder i has a monotone valuation function $v_i : 2^{[m]} \to \mathbb{R}_+$,[2] the designer wishes to find disjoint sets $S_1, \ldots, S_n$ maximizing $\sum_i v_i(S_i)$. The history of combinatorial auctions is rich, and the problem has been considered with and without incentives, with and without Bayesian priors, and in various models of computation (see Appendix A for brief overview). The overarching theme in all of these works is to try and answer the following core question: *Are truthful mechanisms as powerful as (not necessarily truthful) algorithms?*[3]

For many instantiations of the above question, the answer is surprisingly yes. For example, without concern for computational/communication complexity, the celebrated Vickrey-Clarke-Groves auction is a truthful mechanism that always selects the welfare-maximizing allocation (and therefore achieves welfare equal to that of the best algorithm) [53, 12, 34]. Of course, the welfare maximization problem is NP-hard and also requires exponential communication between the bidders, even to guarantee a $1/\sqrt{m}$-approximation. A poly-time algorithm (with polynomial communication) is known to match this guarantee [49, 37, 8], and interestingly, a poly-time truthful mechanism (with polynomial communication) was later discovered as well [40].

The state of affairs gets even more interesting if we restrict to proper subclasses of monotone valuations such as *submodular* valuations.[4] Here, a very simple greedy algorithm is known to find a 1/2-approximation in both $\text{poly}(n, m)$ black-box value queries to each $v_i(\cdot)$, and polynomial runtime (in n, m, and the description complexity of each $v_i(\cdot)$) [41], and a series of improvements provides now a (1-1/e)-approximation, which is tight [54, 42, 24]. Yet, another series of works also proves that any truthful mechanism that runs in polynomial time (in n, m, and the description complexity of each $v_i(\cdot)$), or makes only $\text{poly}(n, m)$ black-box value queries to each $v_i(\cdot)$ achieves at best an $1/m^{\Omega(1)}$-approximation [14, 17, 27, 25]. So while poly-time algorithms, or algorithms making $\text{poly}(n, m)$ black-box value queries can achieve constant-factor approximations, poly-time truthful mechanisms and truthful mechanisms making $\text{poly}(n, m)$ black-box value queries can only guarantee an $1/m^{\Omega(1)}$-approximation, and there is a separation.

But this is far from the whole story: already ten years ago, quite natural truthful mechanisms were developed that achieved an $1/O(\log^2 m)$-approximation [22], which were subsequently improved to $1/O(\sqrt{\log m})$ [16, 38, 18], and even hold for the much broader class of XOS valuations.[5] As these approximation guarantees are better than the lower bounds referenced in the previous paragraph, it seems that perhaps there should be some kind of contradiction: any reasonable definition of "natural" should imply "poly-time," right? The catch is that each of these mechanisms are essentially posted-price mechanisms: they (essentially) offer each bidder a price p_j for item j, and let the buyer choose any subset of items they want to purchase. These prices can be computed in poly-time, but the barrier is that deciding which subset of items the bidder wishes to purchase, called a *demand query*, is in general NP-hard (assuming a succinct representation of the valuation function is given), or requires exponentially many black-box value queries. So the only reason these mechanisms don't fall victim to the strong lower bounds of the previous paragraph is because they get to ask each bidder to compute a single demand query, and this query is used to select exactly the set of items that bidder receives.

The point is that while these existing separations are major results, and rule out certain classes of natural truthful mechanisms from achieving desirable approximation ratios, they are perhaps not addressing "the right" model if posted-price mechanisms with poly-time computable prices provide approximation guarantees that significantly outperform known lower bounds. Therefore, it seems that communication is really the right complexity measure to consider, if one wants the

[1] A simultaneous protocol has one round of communication: Alice and Bob each simultaneously send a message and then no further communication takes place.

[2] By monotone, we mean that $v_i(S) \geq v_i(T)$ for all $T \subseteq S$.

[3] Note that combinatorial auctions is not the only literature to study this question, see Appendix A for very brief discussion of other examples such as combinatorial public projects [47] and job scheduling [43]. We just note here that combinatorial auctions remain the core testbed for this line of work.

[4] A function is submodular if $v(S)+v(T) \geq v(S \cup T)+v(S \cap T)$.

[5] A valuation is XOS if there exists a matrix of item valuations v_{ij} and $v_i(S) = \max_j\{\sum_{i \in S} v_{ij}\}$. XOS valuations are also called fractionally subadditive, and are a proper subclass of subadditive valuations (where $v(S \cup T) \leq v(S) + v(T)$).

resulting lower bounds to hold against all "natural" mechanisms. Unfortunately, the state-of-affairs for communication complexity of combinatorial auctions lags pretty far behind the aforementioned complexity measures. For instance, existing literature doesn't provide a single lower bound against truthful mechanisms that doesn't also hold against algorithms. That is, wherever it's known that no truthful mechanism with communication at most C obtains an approximation ratio better than α when buyers have valuations in class V, it's because it's also known that no algorithm/protocol with communication at most C obtains an approximation ratio better than α when buyers have valuations in class V. On the other hand, the best known truthful mechanisms with polynomial communication for (say) XOS bidders achieve an $1/O(\sqrt{\log m})$ approximation [18], while the best known algorithms with polynomial communication obtain a $(1-1/e)$-approximation [23, 29, 30]. Even for the case of just two bidders, the best known truthful mechanisms with polynomial communication achieve a 1/2-approximation (which is trivial - just give the grand bundle of all items to whoever values it most), while the best known algorithms with polynomial communication achieve a 3/4-approximation (which is tight). It's fair to say that determining whether or not there's a separation in what approximation guarantees are possible for algorithms with polynomial communication and truthful mechanisms with polynomial communication for any class of valuations between submodular and subadditive is one of the core, concrete open problems in Algorithmic Mechanism Design.

Progress on this front had largely been stalled until very recent work of Dobzinski provided a clear path to possibly proving a separation (and it seems to be an accepted conjecture that indeed a separation exists) [19]. Without getting into details of the complete result, one implication is the following: if there exists a truthful mechanism with polynomial communication for 2-player combinatorial auctions with XOS (/submodular/subadditive) valuations that guarantees an approximation ratio of α, then there exists a *simultaneous* protocol with polynomial communication for 2-player combinatorial auctions with XOS (/submodular/subadditive) valuations that guarantees an approximation ratio of α as well. Let us emphasize this point again: in general, interactive protocols with polynomial communication *do not* imply simultaneous protocols with polynomial communication, and numerous well-known problems have polynomial interactive protocols, but require exponential simultaneous communication [48, 28, 44, 21, 1, 2]. But, Dobzinski's result asserts that because of the extra conditions on *truthful* (interactive) mechanisms, their existence indeed implies a simultaneous (not necessarily truthful) protocol of comparable communication complexity. So "all" one has to do to prove lower bounds against truthful mechanisms for 2-player combinatorial auctions is prove lower bounds against simultaneous protocols, motivating the study of simultaneous 2-player combinatorial auctions.

At first glance, it perhaps seems obvious that achieving strictly better than a 1/2-approximation via a simultaneous protocol should be impossible, and it's just a matter of finding the right tools to prove it.[6] This is because quite strong lower bounds are known for "sketching" valuation functions, that is, finding a succinct representation of a function that allows for *approximate* evaluation of value queries. For example, it's known that any sketching scheme for XOS valuations that allows for evaluation of value queries to be accurate within a $o(m)$-factor requires superpoly(m) size [4]. So if somehow a $1/(2-\varepsilon)$-approximation could be guaranteed with a poly(m)-communication simultaneous protocol, it is *not* because enough information is transmitted to evaluate value queries within any non-trivial error. At first glance, it perhaps seems unlikely that such a protocol can possibly exist. Surprisingly, our work shows not only that a $1/(2-\varepsilon)$-approximation is achievable with poly(m) simultaneous communication, but (depending on exactly the question asked) poly(m) simultaneous communication suffices to achieve the same approximation guarantees as the best possible interactive protocol with poly(m) communication.

1.2 Simultaneous Protocols for Welfare Maximization In this work, we specifically study the welfare maximization problem for two bidders with *binary XOS valuations*.[7] Binary XOS valuations are a natural starting point since welfare maximization is especially natural when phrased as a communication problem. Depending on whether one wants to decide the quality of the welfare-optimal allocation, or actually find an allocation inducing the optimal welfare, welfare maximization for binary XOS bidders is equivalent to one of the following:[8]

Definition 1.1. (BXOS Decision Problem) *Alice is given as input a subsets of* $[m]$, $A_1, \ldots, A_a$. *Bob is given as input* b *subsets of* $[m]$, $B_1, \ldots, B_b$, *and both*

[6] Indeed, that is what the authors conjectured at the onset of this work.

[7] A function is binary XOS if all v_{ij} in the matrix representation are 0 or 1.

[8] Equivalent definitions are given in Section 1.4 which are stated more in the language of welfare maximization. We pose these statements here since these formulations make for an especially natural communication problem.

see input X. Determine whether or not there exists an i, j such that $|A_i \cup B_j| \geq X$. A protocol is an α-approximation if whenever there exists an i, j such that $|A_i \cup B_j| \geq X$, it answers yes, and whenever $\max_{i,j}\{|A_i \cup B_j|\} < X/\alpha$ it answers no, but may have arbitrary behavior in between.

DEFINITION 1.2. (BXOS ALLOCATION PROBLEM) *Alice is given as input a subsets of $[m]$, $A_1, \ldots, A_a$. Bob is given as input b subsets of $[m]$, $B_1, \ldots, B_b$. Output a partition of items $S, \bar{S}$ maximizing $\max_{i,j}\{|A_i \cap S| + |B_j \cap \bar{S}|\}$ (over all partitions).*[9]

Recall that typically we think of decision problems as being "easier" than allocation/search problems: certainly if you can find a welfare maximizing allocation, you can also determine its welfare (and this claim is formal for interactive protocols with poly(m) communication). Our main result asserts that this intuition breaks down for simultaneous protocols: the decision problem is strictly harder than the allocation/search problem. To the best of our knowledge, this is the first instance of such a separation.

THEOREM 1.1. *There exists a randomized, simultaneous protocol with* poly(m) *communication that obtains a 3/4-approximation for the BXOS allocation problem. This is the best possible, as even randomized, interactive protocols require $2^{\Omega(m)}$ communication to do better.*

THEOREM 1.2. *For all $\varepsilon > 0$, any randomized, simultaneous protocol that obtains a $(3/4 - 1/108 + \varepsilon)$-approximation for the BXOS decision problem with probability larger than $1/2 + 1/\text{poly}(m)$ requires $2^{\Omega(m)}$ communication.*

Future sections contain more precise versions (that reference the protocols achieving them) of Theorems 1.1 (Theorem 4.1) and 1.2 (Theorem 5.1).

1.3 Extensions and Implications for Truthful Combinatorial Auctions Part of the analysis of our protocols actually makes use of the binary assumption (as opposed to holding for general XOS). Part of the analysis, however, does not. In particular, our same protocols when applied to general XOS functions yield a deterministic, simultaneous $(3/4-1/32-\varepsilon)$-approximation for both problems, and a deterministic 2-round $(3/4-\varepsilon)$-approximation for both problems for general XOS functions.

We are also able to show that a modification of our protocol yields a 1/2-approximation for any number of binary XOS bidders, and that this protocol implies a *strictly* truthful mechanism.[10] The mechanism is quite different from existing approaches, and could inspire better truthful mechanisms in domains where previous molds provably fail. Essentially, the designer offers a menu of lotteries to each bidder and the cost of each lottery depends on how "flexible" the option is. So for instance, taking item one deterministically will be more expensive than taking a single item uniformly at random. The pricing scheme is designed exactly so that each bidder is strictly incentivized to follow our simultaneous protocol.

Finally, while our results have standalone merit outside the scope of truthful combinatorial auctions, it is important to properly quantify their impact in this direction. Dobzinski's recent reduction shows that truthful combinatorial auctions with polynomial communication imply simultaneous algorithms for the *allocation problem*. So Theorem 1.2 *does not* rule out the possibility of a truthful mechanism for two XOS bidders that requires polynomial communication and guarantees a 3/4-approximation (more on this in Section 6).

1.4 Brief Preliminaries and Roadmap Below we give some brief preliminaries. Section 2 provides a toy setting to help develop intuition for where the gap between allocation and decision problem comes from. Section 3 provides a warmup for our protocols via a 2/3-approximation for the allocation problem and a 3/5-approximation for the decision problem. Sections 4 and 4.1 contain our positive results, and Section 5 contains details on our lower bound.

In a combinatorial auction, there are n players and m items. In 2-party case, we call the first player Alice and the second player Bob. Each player i has a valuation function $v_i : 2^{[m]} \to \mathbb{R}^+$. (We require $v_i(\emptyset) = 0$.) The goal for the auctioneer is to find an allocation $S_1, ..., S_n$ $(S_1 \cap \cdots \cap S_n = \emptyset)$ to maximize the social welfare $\sum_{i=1}^{n} v_i(S_i)$.

1. When we use "**protocol**", it means that players honestly follow the protocol and the challenge is to make the protocol have good approximation ratio, polynomial communication cost and possibly small number of rounds. In this paper, we use the standard communication complexity model and we allow public randomness and private randomness.

[9] A protocol is an α-approximation if it outputs a partition $S, \bar{S}$ guaranteeing $\alpha \cdot \max_{i,j}\{|A_i \cap S| + |B_j \cap \bar{S}|\} \geq \max_{i,j,T}\{|A_i \cap T| + |B_j \cap T|\}$.

[10] By this we mean it is a *strongly* dominant strategy for bidders to follow the protocol, and not just that they are indifferent between following and not following.

For details, we refer the reader to [39]. We want to emphasize two relevant properties of the communication protocols here:

(a) We care about the number of rounds of a protocol. In each round, all the messages need to be sent simultaneously. We use "simultaneous protocols" to denote protocols with only one round of communication.

(b) All the protocols discussed in this paper are in the "blackboard model." In the blackboard model, each message is broadcasted. Or in other words, each message is written on a blackboard for all players and the auctioneer to see. In some protocol, we don't really need broadcast, we will specify where is the message from and sent to in those protocols.

2. When we use "**mechanism**," it means that players might not tell the truth and we need to incentivize the players to cooperate. A mechanism in this paper can be considered as a protocol together with an allocation rule and a payment rule. Let the protocol be π and the transcript be Π. For $i = 1, ..., n$, let S_i be the allocation rule and p_i be the payment of player i. Player i's utility is defined as $u_i(\Pi) = v_i(S_i(\Pi)) - p_i(\Pi)$. Player i's goal is to maximize her expected utility $\mathbb{E}[u_i(\Pi)]$. The expectation is over the randomness of the mechanism.

We further define the truthful mechanism as the following. Let m_i be the message sent by player i. m_i is a function of v_i and the history of the protocol. Here we only make the definition for the case when each player sends at most one message in the protocol and all the mechanisms in this paper are in this case. We say that m_i is a **dominant strategy** (in expectation) for player i, if for all $v_1, ..., v_n$, player i's other strategy m_i' and other players' strategy m_{-i},

$$\begin{aligned} & \mathbb{E}\left[v_i(S_i(\Pi(m_i, m_{-i})) - p_i(\Pi(m_i, m_{-i}))\right] \\ \geq \quad & \mathbb{E}\left[v_i(S_i(\Pi(m_i', m_{-i})) - p_i(\Pi(m_i', m_{-i}))\right]. \end{aligned}$$

We say that a mechanism is a **truthful mechanism** if there exist dominant strategies for all players.

One of our goals in this paper is to find an allocation that achieves good approximation of the maximum social welfare $\mathcal{SW}^*(v_1, ..., v_n)$ (defined as allocation problem in Section 1). We say a protocol is α-approximation if for all $v_1, ..., v_n$,

$$\mathbb{E}[\sum_{i=1}^{n} v_i(S_i(\Pi))] \geq \alpha \cdot \mathcal{SW}^*(v_1, ..., v_n).$$

We say a truthful mechanism is α-approximation if for all $v_1, ..., v_n$ there exist dominant strategies $m_1, ..., m_n$ for player $1, ..., n$ guaranteeing:

$$\mathbb{E}[\sum_{i=1}^{n} v_i(S_i(\Pi(m_1, ..., m_n))] \geq \alpha \cdot \mathcal{SW}^*(v_1, ..., v_n).$$

Below are definitions of the valuation classes used in the paper. These are equivalent to the definitions used in Section 1, but more apt for proofs and less apt for posing easy-to-parse communication problems.

DEFINITION 1.3. *We consider the following classes of valuations:*

- *A valuation function v is **additive** if for every bundle S, $v(S) = \sum_{i \in S} v(\{i\})$.*
- *A valuation function v is **XOS** if there exist additive valuations $a_1, ..., a_t$ such that for every bundle S, $v(S) = \max_{i=1}^{t} a_i(S)$. Each a_i is called a **clause** of v.*
- *A valuation function v is **binary additive** if v is additive and for every item i, $v(\{i\}) \in \{0, 1\}$. We will sometimes refer to a binary additive valuation as a **set**, referring to $\{i | v(\{i\}) = 1\}$.*
- *A valuation function v is **binary XOS** if v is XOS and all v's clauses are binary additive valuations. Again, we will sometimes refer to v's clauses as **sets** to make it more natural to talk about unions/intersections/etc.*

2 Intuition for the Gap: an Extremely Toy Setting

Consider the following very toy setting: Alice and Bob each have some valuation function $v(\cdot)$ such that $v([m]) \in [1, M]$, and $v(\cdot)$ is monotone (no other assumptions).[11]

OBSERVATION 1. *In the very toy setting, Alice and Bob can guarantee the following tight approximation guarantees with zero communication:*

- *A 1/2-approximation for the allocation problem with a randomized protocol: give all the items either to Alice or Bob uniformly at random.*
- *A $1/(M+1)$-approximation for the allocation problem with a deterministic protocol: give all the items to Alice.*
- *A $1/(2M)$-approximation for the decision problem (decide if social welfare $\geq X$ or $\leq X/(2M)$, arbitrary behavior allowed in-between): If $X > 2M$ output "$\leq X/(2M)$" If $X \leq 2M$, "$\geq X$."*

[11] If one wishes, one could further restrict attention to submodular, XOS, etc., but this section is just supposed to be a toy model to provide some intuition, and we will not belabor this point.

Since this example is just to provide intuition, we omit a complete proof. The first bullet should be fairly clear: the optimal welfare is clearly upper bounded by $v_1([m]) + v_2([m])$, and the protocol guarantees exactly half of this. The third bullet should also be clear: the optimal welfare is always between 1 and $2M$. Moreover, any value in the range is possible ($2M$ if, for instance, $v_1(\{1\}) = M = v_2(\{2\})$. 1 if, for instance, $v_1(S) = v_2(S) = 1$ iff $S \ni 1$, and $v_1(S) = v_2(S) = 0$ otherwise). So with zero communication, better than $1/(2M)$ is not possible. The middle bullet is perhaps the only tricky one. If we give all of the items to Alice, we guarantee welfare $v_1([m]) \geq 1$, and the optimum is upper bounded by $v_1([m]) + M$.

Again, the purpose of this example is just to provide intuition as to where this gap might come from, and we do not consider it a "result." Of course, one should not expect the gaps to stay quite so drastic as we dial up the communication: with just $\log M$ bits in the above example, a deterministic protocol for the allocation problem and decision problem can both guarantee a 1/2-approximation (output $v([m])$). But this example still captures some of the intuition as to where the gap comes from.

3 Warmup: Beating a 1/2-Approximation

Before explaining our protocol, consider the following thought experiment: say instead Alice and Bob are asked to just report a single clause from their valuation. What clause should they choose and how well will this protocol solve the allocation/decision problem? It's not too hard to see that the best they can do is to just report the largest clause in their list (maximizes $b_i([m])$ over all clauses b_j), which will obtain just a 1/2-approximation for each problem. Now, what if they each report *two* clauses from their valuations, can they do something more clever? Well, they should certainly try to report clauses that are large, as this lets the other know which sets they value the most. But they should also try to report clauses that are different, as this allows for more flexibility in an allocation that both parties value highly. It's perhaps not obvious what the right tradeoff is between large/different (or even exactly what "different" should formally mean), but it turns out that a good approach is for Alice and Bob to each output the two clauses in their list with the largest union (i.e. output b_i, b_j maximizing $\mathcal{SW}^*(b_i, b_j)$). Subject to figuring out how to translate this information into solutions, a slight variant of this protocol guarantees a 2/3-approximation for the allocation problem, and a 3/5-approximation for the decision problem, and the proof is actually quite simple. Note below that Theorem 3.1 holds only for BXOS, whereas Theorem 3.2 holds for general XOS. We'll provide both proofs below first, followed by a brief discussion.

Protocol 1 Simultaneous randomized warmup protocol for 2-party combinatorial auctions with binary XOS valuations

1: Alice finds b_1, b_2, b_3 among clauses of her valuation v_1 such that b_1 maximizes $b_1([m])$ and b_2, b_3 maximize $\mathcal{SW}^*(b_2, b_3)$. Then she picks j uniformly at random from $\{1, 2, 3\}$ and sends b_j to the auctioneer.
2: For each item i, the auctioneer allocates it to Alice if $b_j(\{i\}) = 1$; otherwise allocate it to Bob.

THEOREM 3.1. *Protocol 1 gives a 2/3-approximation to the 2-party BXOS allocation problem.*

Proof. First, we want to claim that if Alice sents b_j to the auctioneer, then the resulting welfare is at least $\mathcal{SW}^*(b_j, v_2)$. This is actually an instantiation of a claim we will want to reference later, so we'll state a more general form below:

CLAIM 1. *Let b_1 be a binary additive valuation and v_2 be a binary XOS valuation. Then the allocation that awards to Alice all items such that $b_1(\{i\}) = 1$ achieves welfare equal to $\mathcal{SW}^*(b_1, v_2)$.*

Proof. Let A denote the set of items for which $b_1(\{i\}) = 1$, and consider any other allocation $(B, \bar{B})$. We first reason that we can remove from B all items $\notin A$ without hurting $b_j(B) + v_2(\bar{B})$. This is trivial to see, as b_j has value 0 for all items $\notin A$. Next, we reason that we can add to B any item $\in A$ without hurting $b_j(B) + v_2(\bar{B})$. To see this, observe that we are certainly increasing $b_j(B)$ by 1 when we make this change, as b_j is just additive and $b_j(\{i\}) = 1$ for all $i \in A$. In addition, we can't possibly decrease $v_2(\bar{B})$ by more than 1, as all of the clauses in v_2 are binary additive (and therefore have value at most 1 for any item). So again, the total change is only positive. At the end of these changes, observe that we have now transitioned from $(B, \bar{B})$ to $(A, \bar{A})$ without losing any welfare, and therefore $(A, \bar{A})$ is indeed optimal.

Claim 1 immediately lets us conclude that the expected welfare guaranteed by Protocol 1 is at least $\frac{1}{3} \cdot \sum_{j=1}^{3} \mathcal{SW}^*(b_j, v_2)$. Now, let S and T be the optimal allocation to achieve $\mathcal{SW}^*(v_1, v_2)$. Let a be the clause of v_1 such that $a(S) = v_1(S)$. Let a' be the clause of v_2 such that $a'(T) = v_2(T)$. So $\mathcal{SW}^*(v_1, v_2) = a(S) + a'(T)$. From the protocol, we know that $b_1([m]) \geq a([m]) \geq a(S)$. Moreover, if U and U' are the allocation

that achieves $\mathcal{SW}^*(b_2, b_3)$, then we know that $b_2(U) + b_3(U') = \mathcal{SW}^*(b_2, b_3) \geq \mathcal{SW}^*(a, b_1) \geq a(S) + b_1(T)$ (by definition of b_2, b_3). In expectation, the social welfare we get in the protocol is at least:

$$\begin{aligned}
& \frac{1}{3} \cdot \sum_{j=1}^{3} \mathcal{SW}^*(b_j, v_2) \\
\geq\ & \frac{1}{3} \cdot (b_1(S) + a'(T) + b_2(U) + a'(U') + b_3(U') + a'(U)) \\
\geq\ & \frac{1}{3} \cdot (b_1(S) + a'(T) + a(S) + b_1(T) + a'([m])) \\
\geq\ & \frac{1}{3} \cdot (b_1([m]) + a(S) + 2a'(T)) \\
\geq\ & \frac{1}{3} \cdot (2a(S) + 2a'(T)) = \frac{2}{3} \cdot \mathcal{SW}^*(v_1, v_2).
\end{aligned}$$

Protocol 2 Simultaneous deterministic warmup protocol for 2-party combinatorial auctions with XOS valuations

1: Alice finds b_1, b_2, b_3 among clauses of her valuation v_1 such that b_1 maximizes $b_1([m])$ and b_2, b_3 maximize $\mathcal{SW}^*(b_2, b_3)$. Bob finds b_4, b_5, b_6 among clauses of his valuation v_2 such that b_4 maximizes $b_4([m])$ and b_5, b_6 maximize $\mathcal{SW}^*(b_5, b_6)$. Alice sends b_1, b_2, b_3 to the auctioneer and Bob sends b_4, b_5, b_6 to the auctioneer simultaneously.

2: **For allocation problem:** Auctioneer finds $j \in \{1, 2, 3\}, j' \in \{4, 5, 6\}$ that maximizes $\mathcal{SW}^*(b_j, b'_{j'})$ and allocate items according to it.

3: **For decision problem:** Let X be the parameter in the decision problem. Auctioneer finds $j \in \{1, 2, 3\}, j' \in \{4, 5, 6\}$ that maximizes $\mathcal{SW}^*(b_j, b'_{j'})$. If $\mathcal{SW}^*(b_j, b'_{j'}) \geq 3X/5$, say "yes" ($\mathcal{SW}^*(v_1, v_2) \geq X$). If $\mathcal{SW}^*(b_j, b'_{j'}) < 3X/5$, say "no".

THEOREM 3.2. *Protocol 2 gives a* 3/5*-approximation to the 2-party XOS allocation problem and the 2-party XOS decision problem.*[12]

Proof. Let S and T be the optimal allocation to achieve $\mathcal{SW}^*(v_1, v_2)$. Let a be the clause of v_1 such that $a(S) = v_1(S)$. Let a' be the clause of v_2 such that $a'(T) = v_2(T)$. So $\mathcal{SW}^*(v_1, v_2) = a(S) + a'(T)$. From the protocol, we know that $b_1([m]) \geq a([m]) \geq a(S)$ and $b_4([m]) \geq a'([m]) \geq a'(T)$. Let U and U' be the allocation to achieve $\mathcal{SW}^*(b_2, b_3)$. We know that $b_2(U) + b_3(U') \geq a(S) + b_1(T)$. Let W and W' be the allocation to achieve $\mathcal{SW}^*(b_5, b_6)$. We know that $b_5(W) + b_6(W') \geq a'(T) + b_4(S)$. Then we have

$$\begin{aligned}
& \mathcal{SW}^*(b_1, b_5) + \mathcal{SW}^*(b_1, b_6) \\
\geq\ & b_1(W') + b_5(W) + b_1(W) + b_6(W') \\
\geq\ & b_1([m]) + b_5(W) + b_6(W') \geq a(S) + a'(T) + b_4(S).
\end{aligned}$$

Similarly we have

$$\mathcal{SW}^*(b_2, b_4) + \mathcal{SW}^*(b_3, b_4) \geq a(S) + a'(T) + b_1(T).$$

The social welfare we get in the protocol is at least

$$\begin{aligned}
& \mathcal{SW}^*(b_j, b'_{j'}) \\
\geq\ & \frac{1}{5} \cdot (\mathcal{SW}^*(b_1, b_4) + \mathcal{SW}^*(b_1, b_5) + \\
& \mathcal{SW}^*(b_1, b_6) + \mathcal{SW}^*(b_2, b_4) + \mathcal{SW}^*(b_3, b_4)) \\
\geq\ & \frac{1}{5} \cdot (b_1(S) + b_4(T) + 2a(S) + 2a'(T) + b_4(S) + b_1(T)) \\
\geq\ & \frac{1}{5} \cdot (b_1([m]) + b_4([m]) + 2a(S) + 2a'(T)) \\
\geq\ & \frac{3}{5} (a(S) + a'(T)) = \frac{3}{5} \mathcal{SW}^*(v_1, v_2).
\end{aligned}$$

From this, it is easy to check that Protocol 2 gives a 3/5-approximation to both the 2-party XOS allocation problem and the 2-party XOS decision problem.

So now there are two remaining questions: first, how does one generalize the reasoning in Protocols 1 and 2 to multiple clauses? And second, why the heck is there a difference between their guarantees for the allocation and decision problem for binary XOS valuations? For the first question, we'll postpone the details to Section 4, but just note here that our full protocols indeed makes use of similar reasoning. For the second, observe that Claim 1 is somewhat magical: if Alice's valuation is binary additive, and Bob's is binary XOS, then it is possible to allocate the items optimally *without any input from Bob* (other than the knowledge that his valuation is indeed binary XOS). While it's not obvious that Claim 1 should necessarily be quite so helpful (given that we do, in fact, get input from Bob), this turns out to be the crucial difference between the allocation and decision problem. At a high level, there is necessarily some information lost between Alice's valuation and her message (ditto for Bob). The decision problem requires us to deal with both losses, but Claim 1 lets certain kinds of protocols only worry about the loss from Alice.

4 Developing Good Summaries

In this section, we define "summaries" in some specific forms for binary XOS valuations. They are the main

[12] XOS allocation problem and XOS decision problem are the obvious extensions of BXOS allocation problem and BXOS decision problem for non-binary clauses.

ingredients in our protocols and mechanisms. At a high level, the summaries are trying to simultaneously maximize the size of the reported clauses, while also keeping on eye on reporting "different" clauses. One can interpret the negative term as a "regularizer" that achieves this goal. The total size of the reported clauses corresponds to term $\sum_{i=1}^{m} x_i$ and we encourage reporting "different" clauses by having the term $-\sum_{i=1}^{m} \alpha \cdot x_i^2$.

DEFINITION 4.1. (SUMMARIES OF BINARY XOS VALUATIONS) *For a binary XOS valuation v, define its (k,α)-summary $(b_1, ..., b_k)$ as* $\text{argmax}_{b_1,...,b_k \in \{a_1,...,a_t\}} \sum_{i=1}^{m} \left(x_i - \alpha \cdot x_i^2\right)$, *where $a_1, ..., a_t$ are the clauses of v and $x_i = \frac{b_1(\{i\})+\cdots+b_k(\{i\})}{k}$.*

REMARK 4.1. *For the summaries defined above, there might be multiple $(b_1, ..., b_k)$'s maximize the term. When we use a (k,α)-summary in some protocol, we will use an arbitrary one. Additionally, note that our warm-up protocols from Section 3 ask Alice and Bob to output both their $(1, 1/2)$-summary and their $(2, 2/3)$-summary, see examples below.*

EXAMPLE 1. *For a $(1, 1/2)$-summary of some binary XOS valuation v, we will find b_1 among clauses of v that maximizes*

$$\sum_{i=1}^{m} \left(b_1(\{i\}) - \frac{1}{2} \cdot (b_1(\{i\}))^2 \right) = \sum_{i=1}^{m} b_1(\{i\})/2 = \frac{1}{2} b_1([m]).$$

EXAMPLE 2. *For a $(2, 2/3)$-summary of some binary XOS valuation v, we will find b_1, b_2 among clauses of v that maximize*

$$\begin{aligned} & \sum_{i=1}^{m} \left(\frac{b_1(\{i\}) + b_2(\{i\})}{2} - \frac{2}{3} \cdot \left(\frac{b_1(\{i\}) + b_2(\{i\})}{2} \right)^2 \right) \\ = \; & \frac{1}{3} \sum_{i=1}^{m} \left(b_1(\{i\}) + b_2(\{i\}) - b_1(\{i\}) b_2(\{i\}) \right) \\ = \; & \frac{1}{3} \mathcal{SW}^*(b_1, b_2). \end{aligned}$$

In Appendix C, we prove some simple properties of these summaries, and an extension of the definition to non-binary XOS valuations. Essentially, what the lemmas are stating is that for any set A, the summaries defined above do a "good enough" job capturing Alice's (/Bob's) value for A. Note that "good enough" doesn't mean "captures $v(A)$ within a constant factor," as this is impossible with a sketch [4]. "Good enough" simply means that the summary can be used inside a similar approach to Section 3.

Once summaries from Alice and Bob are in hand, there are a couple natural ways to "wrap up" the allocation/decision problem. We'll formally name these and refer to them in future protocols:

- **Alice-Only Allocation (randomized):** Pick a clause uniformly at random from Alice's summary, award to Alice items for which that clause values at 1, and the rest to Bob.
- **Best Known Allocation (deterministic):** If Alice reports clauses $a_1, \ldots, a_k$, and Bob reports clauses $b_1, \ldots, b_k$, find i, j maximizing $\mathcal{SW}^*(a_i, b_j)$. Allocate items according to the allocation that yields $\mathcal{SW}^*(a_i, b_j)$.
- **Best Known Decision(α, X) (deterministic):** If Alice reports clauses $a_1, \ldots, a_k$, and Bob reports clauses $b_1, \ldots, b_k$, find i, j maximizing $\mathcal{SW}^*(a_i, b_j)$. If $\mathcal{SW}^*(a_i, b_j) \geq \alpha X$ say "yes" (guess that $\mathcal{SW}^*(v_1, v_2) \geq X$). Otherwise, guess "no" (guess that $\mathcal{SW}^*(v_1, v_2) < \alpha X$).

4.1 Our Protocols and Mechanisms In this section, we'll describe all protocols used to provide our positive results. All protocols involve Alice and Bob reporting a (k,α)-summary, and then using the Alice-Only or Best Known Allocation, or making the Best Known Decision. All proofs are in Appendix D and the appendices in the full version. We make two remarks before proceeding:

1. All of the high-level intuition for why the protocols work is captured by the summaries. Many of the actual proofs are different, but at a high level everything comes down to the fact that this class of summaries selects "the right" clauses to report for welfare maximization.
2. Any protocol that eventually uses the Alice-Only Allocation doesn't require Alice to report her entire summary (she can just draw the random clause herself as in Protocol 1 (and have communication m for any choice of k). While we state the guarantees for such protocols for a fixed k, one can actually take $k \to \infty$ without increasing the communication at all.

THEOREM 4.1. *The following protocols achieve the following guarantees:*

Alice's summary	*Bob's summary*	*Wrap-up*
$(k, 1/2)$	$\perp$	*Alice-Only*
$(k, 1/3)$	$(k, 1/3)$	*Best Known Allocation*
$(k, 1/3)$	$(k, 1/3)$	*Best Known Decision*

Approximation	*Problem*	*Valuations*
$3/4 - 1/k$	*Allocation*	*BXOS*
$23/32 - 1/k$	*Allocation*	*XOS*
$23/32 - 1/k$	*Decision*	*XOS*

Each line in the first table corresponds to each line in the second table. For a better table, check the full version of this paper.

Before continuing, we briefly remark the following:

- The 3/4-approximation guaranteed by the protocol in the first row is tight: [23] showed that randomized, interactive protocols require exponential communication to beat a 3/4-approximation.
- The second and third protocols also work for general XOS (subject to updating the summary definition as in Appendix C).
- It is still open whether it is possible to beat 23/32 with a deterministic protocol for the allocation problem, but 23/32 is optimal for any protocol using the Best Known Allocation after Alice and Bob each report a (k, α_i)-summary (see the full version of this paper).

Additional applications of our summaries appear in the full version of this paper, including a 2-round protocol guaranteeing a 3/4-approximation for general XOS valuations, and our strictly truthful mechanism. The strictly truthful mechanism essentially visits bidders one at a time, asks for a $(k, 1/2)$-summary on the remaining items, awards them the "Alice-Only Allocation" for their reported summary, and charges payments to ensure strict truthfulness.

5 Lower Bounds

Finally, we overview our lower bound for the BXOS decision problem (which implies Theorem 1.2). We begin with some intuition: Alice and Bob will each get exponentially many clauses of size $m/2$. These sets will be random, but not uniformly random.[13] Instead, they are drawn in such a way that the union of two random clauses of Alice and Bob has size $(3/4-1/108)m$ in expectation. At this point, the optimal welfare is $(3/4 - 1/108)m$ if we don't further adjust their inputs. Finally, we modify the construction either by hiding or not hiding a_0 within Alice's input and b_0 within Bob's input such that $a_0 \cup b_0 = [m]$, in a matter so that these sets are indistinguishable from the rest. Therefore, the answer to the decision problem rests on whether or not Alice and Bob each have this hidden set, but they have no means by which to convey this information as this set looks indistinguishable from the rest. This description captures all of the intuition for our construction, which appears in Appendix E along with a proof of Theorem 5.1 below.

[13] If they were uniformly random, then Alice and Bob can guarantee $3m/4$ in expectation by just reporting a single arbitrary clause, because two uniformly random sets of size $m/2$ have union $3m/4$ in expectation.

THEOREM 5.1. *For any constant $\varepsilon > 0$, there exists a distribution over binary XOS valuations such that no simultaneous, randomized protocol with less than $e^{2Cm/9}$ communication can guarantee an α-approximation to the 2-party BXOS decision problem with probability larger than $\frac{1}{2} + 2e^{-Cm/9}$. Here $\alpha = 3/4 - 1/108 + \varepsilon$ and $C = 2\varepsilon^2$.*

6 Discussion and Future Work

Our main result shows a simultaneous protocol guaranteeing a 3/4-approximation for the BXOS allocation problem, and a lower bound of $3/4 - 1/108$ for for the BXOS decision problem. The bigger picture behind these results, even without consideration of truthful combinatorial auctions, is the following:

- It is surprising that the decision problem is strictly *harder* than the allocation/search problem. To the best of our knowledge, this is the first instance of such a separation.
- It is surprising that a ($> 1/2$)-approximation for either the allocation or decision problem is possible at all, given the strong lower bounds already known on sketching valuation functions, but we are able to get a tight 3/4-approximation for the allocation problem.
- A 3/4-approximation for the decision problem now serves as a new example of what can be achieved in polynomial interactive communication (in fact, two rounds by a theorem in the full version), but requires exponential simultaneous communication. While such problems are already known, this has a very different flavor than previous constructions, and will likely be a useful tool for this reason.

The most obvious question is to resolve whether or not there is a 3/4-approximation for the allocation problem with general XOS functions. If there isn't, this would provide the first separation between truthful and non-truthful protocols with polynomial communication via Dobzinski's reduction [19]. Additionally, whether or not our protocol can be de-randomized is an enticing open question: if no matching deterministic protocol can be found (implying a lower bound of $< 3/4$ for deterministic protocols for the allocation problem), this would provide the first separation between truthful and non-truthful deterministic protocols (Dobzinski's reduction preserves determinism). If our protocol can in fact be de-randomized, this would be fascinating, as this protocol would *deterministically* guarantee a 3/4-approximation without learning the welfare it achieves.[14]

[14] It somehow seems tempting to conjecture both that our protocol can be de-randomized and that it can't - a random clause

Finally, while we have provided simultaneous protocols for the allocation problem with approximation guarantees strictly better than 1/2 when bidders have XOS valuations, it still remains open whether or not a truthful mechanism can obtain a $(> 1/2)$-approximation for two-player combinatorial auctions with XOS bidders.

A Background on Related Work

There is an enormous literature of related work on combinatorial auctions. The state-of-the-art without concern for incentives is a 1/2-approximation for any number of subadditive bidders [29], and numerous improvements for special cases, such as submodular bidders [23, 29, 30]. With concern for incentives, the state-of-the-art (for worst-case approximation ratios and dominant strategy truthfulness) is an $1/O(\sqrt{\log m})$-approximation for XOS bidders, again with improvements for further special cases [26]. The problem has also been studied in Bayesian settings, where a generic black-box reduction is known if the designer only desires *Bayesian* truthfulness[15] [36, 35, 5]. If the designer desires dominant strategy truthfulness but is okay with an average-case welfare guarantee, then a 1/2-approximation is known for XOS bidders [33]. Combinatorial auctions have also been studied through the lens of *Price of Anarchy*, but a deeper discussion of this is outside the scope of this paper [6, 45, 51, 52, 32, 9, 20, 15, 41, 11, 7, 31].

The direction of "truthful mechanisms versus algorithms" is also studied through other topics. For example, [47] introduces the *combinatorial public projects* problem, and characterize truthful mechanisms via a Roberts-like theorem [50]. They further show a separation between what is achievable by communication-efficient truthful mechanisms and communication-efficient algorithms, owing to this characterization. In contrast, such a characterization is not known (and not believed to exist) for combinatorial auctions, with Dobzinski's recent reduction being the only progress in this direction [19]. Nisan and Ronen's seminal paper also attacked this question through the problem of truthful job scheduling on unrelated machines [43]. Here, the specific question studied is fundamentally different: they ask whether or not any truthful mechanism (regardless of computation/communication) can achieve makespan guarantees competitive with the best possible (whereas for combinatorial auctions, the VCG mechanism guarantees that truthful mechanisms can achieve the first-best without concern for computation/communication [53, 12, 34]).

On the topic of simultaneous versus interactive communication, [55] proposed the 2-party simultaneous communication model when communication complexity was introduced. [48], [28], [44] showed that in the 2-party case, there is an exponential gap between k and $(k-1)$-round deterministic/randomized communication complexity of an explicit function. In the multiparty number-on-forehead communication model [10], [3] showed an exponential gap between simultaneous communication complexity and communication complexity for up to $(\log n)^{1-\varepsilon}$ players for any $\varepsilon > 0$. [21] recently showed that in combinatorial auctions with unit demand bidders/subadditive bidders, there is an exponential gap (exponential in the number of players) between simultaneous communication complexity and communication complexity. In comparison to these works, our separation between simultaneous and interactive communication for the 2-player BXOS decision problem is of a quite different flavor, and makes the available toolkit for future results more diverse.

B Tools for proofs

B.1 Information Theory Here we briefly review some facts and definitions from information theory that will be used in this paper. For a more detailed introduction, we refer the reader to [13].

Throughout this paper, we use log to refer to the base 2 logarithm and use ln to refer to the natural logarithm.

Definition B.1. *The* entropy *of a random variable X, denoted by $H(X)$, is defined as $H(X) = \sum_x \Pr[X = x] \log(1/\Pr[X = x])$.*

If X is drawn from Bernoulli distributions $\mathcal{B}(p)$, we use $H(p) = -(p \log p + (1-p)(\log(1-p))$ to denote $H(X)$.

Definition B.2. *The* conditional entropy *of random variable X conditioned on random variable Y is defined as $H(X|Y) = \mathbb{E}_y[H(X|Y = y)]$.*

Fact B.1. *$H(XY) = H(X) + H(Y|X)$.*

Definition B.3. *The* mutual information *between two random variables X and Y is defined as $I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$.*

of Alice's does well on average with no input from Bob, so to derandomize we just need Bob to tell us *something* that identifies a clause performing better than average. At the same time it seems extremely unlikely that a deterministic protocol will somehow provide an approximation guarantee better than $3/4 - 1/108$ for the allocation problem without violating Theorem 5.1.

[15] A mechanism is Bayesian truthful if it is in every bidder's interest to tell the truth, assuming all other bidders tell the truth and have values drawn from the correct Bayesian prior.

DEFINITION B.4. *The* conditional mutual information *between X and Y given Z is defined as $I(X;Y|Z) = H(X|Z) - H(X|YZ) = H(Y|Z) - H(Y|XZ)$.*

FACT B.2. *Let X_1, X_2, Y, Z be random variables, we have $I(X_1X_2;Y|Z) = I(X_1;Y|Z) + I(X_2;Y|X_1Z)$.*

FACT B.3. *Let X, Y, Z, W be random variables. If $I(Y;W|X,Z) = 0$, then $I(X;Y|Z) \geq I(X;Y|ZW)$.*

FACT B.4. *Let X, Y, Z, W be random variables. If $I(Y;W|Z) = 0$, then $I(X;Y|Z) \leq I(X;Y|ZW)$.*

B.2 Concentration Bound

DEFINITION B.5. (NEGATIVE CORRELATION) *Let $X_1, ..., X_n$ be n random variables supported on $\{0,1\}$. We say $X_1, ..., X_n$ are negatively correlated if for all $S \subseteq [n]$,*

$$\Pr\left[\bigwedge_{i\in S}(X_i = 1)\right] \leq \prod_{i\in S} Pr[X_i = 1].$$

LEMMA B.1. (GENERALIZED CHERNOFF BOUND[46]) *Let $X_1, ..., X_n$ be n random variables supported on $\{0,1\}$ and they are negatively correlated. Then for any $a > 0$,*

$$\Pr\left[\sum_{i=1}^{n} X_i \geq a + \mathbb{E}[\sum_{i=1}^{n} X_i]\right] \leq e^{-2a^2/n}.$$

C Missing Definitions and Proofs of Section 4

Here we give an extension of Definition 4.1 to non-binary XOS valuations. It is easy to verify that Definition 4.1 and Definition C.1 are equivalent for binary XOS valuations.

DEFINITION C.1. (SUMMARIES OF XOS VALUATIONS) *For a XOS valuation v, define its (k,α)-summary $(b_1, ..., b_k)$ as*

$$\text{argmax}_{b_1,...,b_k\in\{a_1,...,a_t\}} \sum_{i=1}^{m}\left(\int_0^{+\infty}(x_{i,u} - \alpha\cdot x_{i,u}^2)du\right).$$

Here $a_1, ..., a_t$ are the clauses of v and $x_{i,u} = \frac{\sum_{j=1}^{k}\mathbb{1}_{b_j(\{i\})\geq u}}{k}$.

Now we prove some simple properties of these summaries.

LEMMA C.1. *Let $(b_1, ..., b_k)$ be the (k,α)-summary of some binary XOS valuation v. Let $\alpha \leq 1/2$. Let a be a clause of v and $A \subseteq \{i|a(\{i\} = 1\}$. We have*

$$\sum_{i=1}^{m}(x_i - 2\alpha\cdot x_i^2) + 2\alpha\cdot\sum_{i\in A} x_i \geq |A| - \frac{2\alpha\cdot v([m])}{k}.$$

Here $x_i = \frac{b_1(\{i\})+\cdots+b_k(\{i\})}{k}$.

Proof. Because $x_i \leq 1$ and $\alpha \leq 1/2$, we have

$$2\alpha\cdot\sum_{i\in\{i|a(\{i\}=1\}\setminus A} x_i \leq |\{i|a(\{i\} = 1\}\setminus A|.$$

So if we can prove the lemma for the case when $A = \{i|a(\{i\} = 1\}$, it will directly imply the lemma for the case when $A \subsetneq \{i|a(\{i\} = 1\}$. From now on, we will assume $A = \{i|a(\{i\} = 1\}$. By Definition 4.1, $(b_1, ..., b_k)$ are some clauses of v that maximize $\sum_{i=1}^{m}(x_i - \alpha\cdot x_i^2)$.

For $1 \leq j \leq m$, if we replace b_j with a, then $\sum_{i=1}^{m}(x_i - \alpha\cdot x_i^2)$ will not increase. So we have

$$\begin{aligned}
&\sum_{i=1}^{m}(x_i - \alpha\cdot x_i^2)\\
\geq\ &\sum_{i=1}^{m}((x_i - b_j(\{i\})/k + a(\{i\})/k)\\
&-\alpha\cdot(x_i - b_j(\{i\})/k + a(\{i\}/k))^2).
\end{aligned}$$

This implies

$$\begin{aligned}
&\sum_{i=1}^{m}(\frac{b_j(\{i\}) - a(\{i\})}{k} +\\
&2\alpha\cdot\frac{k\cdot x_i(a(\{i\}) - b_j(\{i\})) + \alpha(b_j(\{i\}) - a(\{i\}))^2}{k^2})\\
&\geq 0.
\end{aligned}$$

Summing over all $j \in [k]$, we get

$$\begin{aligned}
&\sum_{i=1}^{m}(x_i - 2\alpha\cdot x_i^2) + 2\alpha\cdot\sum_{i\in A} x_i\\
\geq\ &|A| - \sum_{i=1}^{m}\sum_{j=1}^{k}\alpha\cdot\frac{(b_j(\{i\}) - a(\{i\}))^2}{k^2}\\
\geq\ &|A| - \sum_{i=1}^{m}\sum_{j=1}^{k}\alpha\cdot\frac{b_j(\{i\}) + a(\{i\})}{k^2}\\
=\ &|A| - \frac{\alpha\cdot(|A| + \sum_{i=1}^{m} x_i)}{k}\\
\geq\ &|A| - \frac{2\alpha\cdot v([m])}{k}.
\end{aligned}$$

LEMMA C.2. *Let $(b_1, ..., b_k)$ be the (k,α)-summary of some XOS valuation v. Let $\alpha \leq 1/2$. Let a be a clause of v. a' is an additive valuation and for all i, $a(\{i\}) \geq a'(\{i\})$. We have*

$$\begin{aligned}
&\sum_{i=1}^{m}\left(\int_0^{+\infty}(x_{i,u} - 2\alpha\cdot x_{i,u}^2)du + 2\alpha\cdot\int_0^{a'(\{i\})} x_{i,u}du\right)\\
&\geq a'([m]) - \frac{2\alpha\cdot v([m])}{k}.
\end{aligned}$$

Here $x_{i,u} = \frac{\sum_{j=1}^{k}\mathbb{1}_{b_j(\{i\})\geq u}}{k}$.

Proof. Because $x_{i,u} \le 1$ and $\alpha \le 1/2$, similarly as Lemma C.1, it suffices to prove the case when $a' = a$. By Definition C.1, for $1 \le j \le m$, if we replace b_j with a, $\sum_{i=1}^{m}\left(\int_0^{+\infty}(x_{i,u} - \alpha \cdot x_{i,u}^2)du\right)$ will not decrease. Let $y_{i,j,u} = (\mathbb{1}_{b_j(\{i\})\ge u} - \mathbb{1}_{a(\{i\})\ge u})/k$. We get

$$\begin{aligned}&\sum_{i=1}^{m}\left(\int_0^{+\infty}(x_{i,u} - \alpha \cdot x_{i,u}^2)du\right)\\ \ge &\sum_{i=1}^{m}\left(\int_0^{+\infty}\left(x_{i,u} - y_{i,j,u} - \alpha \cdot (x_{i,u} - y_{i,j,u})^2\right)du\right)\end{aligned}$$

This implies

$$\begin{aligned}&\sum_{i=1}^{m}\int_0^{+\infty}(y_{i,j,u} - 2\alpha \cdot x_{i,u} \cdot y_{i,j,u})\,d_u\\ \ge\ & -\alpha \cdot \sum_{i=1}^{m}\int_0^{+\infty} y_{i,j,u}^2 d_u\\ \ge\ & -\alpha \cdot \sum_{i=1}^{m}\int_0^{\max(a(\{i\}),b_j(\{i\}))}\frac{1}{k^2}\cdot d_u\\ =\ & -\alpha \cdot \sum_{i=1}^{m}\frac{\max(a(\{i\}),b_j(\{i\}))}{k^2} \ge -\frac{2\alpha \cdot v([m])}{k^2}.\end{aligned}$$

Notice that $\sum_{j=1}^{k} y_{i,j,u} = x_{i,u} - \mathbb{1}_{a(\{i\})\ge u}$. Summing over all $j \in [m]$, we get

$$\begin{aligned}&\sum_{i=1}^{m}\int_0^{+\infty}\left(x_{i,u} - 2\alpha \cdot x_{i,u}^2\right)d_u\\ \ge\ & \sum_{i=1}^{m}\int_0^{+\infty}\left(\mathbb{1}_{a(\{i\})\ge u} - 2\alpha \cdot x_{i,u} \cdot \mathbb{1}_{a(\{i\})\ge u}\right)d_u\\ & -\frac{2\alpha \cdot v([m])}{k}\\ =\ & a([m]) - \frac{2\alpha \cdot v([m])}{k} - \sum_{i=1}^{m} 2\alpha \cdot \int_0^{a(\{i\})} x_{i,u}du.\end{aligned}$$

D Protocols for BXOS parties

Protocol 3 Simultaneous protocol for 2-party combinatorial auctions with binary XOS valuations

1: Alice computes the $(k, 1/2)$-summary $(b_1, ..., b_k)$ of her valuation v_1. Then she picks j uniformly randomly from $\{1, ..., k\}$ and sends b_j to the auctioneer.
2: For each item i, the auctioneer allocates it to Alice if $b_j(\{i\}) = 1$; otherwise allocate it to Bob.

D.1 Simultaneous protocol for two BXOS parties (implies Theorem 1.1)

THEOREM D.1. *Protocol 3 gives a $(3/4 - 1/k)$-approximation in expectation to the 2-party BXOS allocation problem.*

Proof. Let S and $T = [m]\backslash S$ be the allocation that achieves the optimal social welfare between v_1 and v_2 (if there are multiple such allocations, just pick an arbitrary one). Let a be some clause of v_1 such that $v_1(S) = a(S)$ and a' be some clause of v_2 such that $v_2(T) = a'(T)$. Let $A = \{i|a(\{i\}) = 1\} \cap S$ and $A' = \{i|a'(\{i\}) = 1\} \cap T$. We have $A \cap A' = \emptyset$. The optimal social welfare is

$$\mathcal{SW}^*(v_1, v_2) = v_1(S) + v_2(T) = a(S) + a'(T) = |A| + |A'|.$$

Let $x_i = \frac{b_1(\{i\})+\cdots+b_k(\{i\})}{k}$. By Lemma C.1, we have

$$\sum_{i=1}^{m}(x_i - x_i^2) + \sum_{i\in A} x_i \ge |A| - \frac{v_1([m])}{k}.$$

Therefore,

$$\begin{aligned}\sum_{i\notin A'} x_i &\ge -\sum_{i\in A\cup A'} x_i + \sum_{i=1}^{m} x_i^2 + |A| - \frac{v_1([m])}{k}\\ &\ge -\sum_{i\in A\cup A'} x_i + \sum_{i\in A\cup A'} x_i^2 + |A| - \frac{v_1([m])}{k}\\ &= \sum_{i\in A\cup A'}\left((x_i - \frac{1}{2})^2 - \frac{1}{4}\right) + |A| - \frac{v_1([m])}{k}\\ &\ge \sum_{i\in A\cup A'}\left(-\frac{1}{4}\right) + |A| - \frac{v_1([m])}{k}\\ &= -\frac{|A| + |A'|}{4} + |A| - \frac{v_1([m])}{k}.\end{aligned}$$

Define $B_j = \{i|b_j(\{i\}) = 1\}$ and $\overline{B_j} = [m]\backslash B_j$. By Claim 1, the expected social welfare Protocol 3 gets is

$$\begin{aligned}&\frac{1}{k}\cdot\sum_{j=1}^{k}\mathcal{SW}^*(b_j, v_2) \ge \frac{1}{k}\cdot\sum_{j=1}^{k}\left(b_j(B_j) + a'(\overline{B_j})\right)\\ \ge\ & \frac{1}{k}\cdot\sum_{j=1}^{k}\left(|B_j| + |\overline{B_j} \cap A'|\right)\\ =\ & \frac{1}{k}\cdot\sum_{j=1}^{k}\left(|B_j| - |A' \cap B_j| + |A'|\right)\\ =\ & |A'| + \frac{1}{k}\cdot\sum_{j=1}^{k}\sum_{i\notin A'} b_j(\{i\})\\ =\ & |A'| + \sum_{i\notin A'} x_i\\ \ge\ & |A'| - \frac{|A| + |A'|}{4} + |A| - \frac{v_1([m])}{k}\\ =\ & \frac{3}{4}\cdot(|A| + |A'|) - \frac{v_1([m])}{k}.\end{aligned}$$

As $v_1([m]) \leq \mathcal{SW}^*(v_1, v_2) = |A| + |A'|$, Protocol 3 gives a $(3/4 - 1/k)$ approximation in expectation to the problem.

Protocol 4 Sequential protocol for multi-party combinatorial auctions with binary XOS valuations

1: **for** $l = 1, ..., n-1$ **do**
2: The l-th player computes the $(k, 1/2)$-summary $(b_1^l, ..., b_k^l)$ of her valuation v_l for items that are left. Then she picks j uniformly randomly from $\{1, ..., k\}$ and broadcasts b_j^l.
3: For each item i left, the auctioneer allocates it to the l-th player if $b_j^l(\{i\}) = 1$.
4: **end for**
5: Allocate the left items to the n-th player.

D.2 Sequential protocol for multiple BXOS parties

THEOREM D.2. *Protocol 4 gives a $(1/2 - 1/k)$-approximation in expectation to the n-party BXOS allocation problem.*

Proof. Let $C(n) - 1/k$ be the approximation ratio of Protocol 4 on n players. We prove the theorem by induction on n. By Theorem 3, $C(2) \geq 3/4$. For any $n \geq 3$, let $S_1, S_2, ..., S_n$ be the allocation that achieves the optimal social welfare. For $l \in [n]$, let a_l be the clause of v_l such that $a_l(S_l) = v_l(S_l)$ and $A_l = \{i : a_l(\{i\}) = 1\} \cap S_l$. Therefore $\mathcal{SW}^*(v_1, ..., v_n) = |A_1| + \cdots + |A_n|$.

Let $x_i = \frac{b_1^1(\{i\}) + \cdots + b_k^1(\{i\})}{k}$. By Lemma C.1, we have

$$\sum_{i=1}^{m}(x_i - x_i^2) + \sum_{i \in A_1} x_i \geq |A_1| - \frac{|A_1| + \sum_{i=1}^m x_i}{2k}.$$

Notice this not exactly from the statement of Lemma C.1, but it is explicit from the proof of Lemma C.1.

Let $B_j = \{i | b_j^1(\{i\}) = 1\}$. In Protocol 4, player 1 will get welfare $\frac{1}{k} \cdot \sum_{j=1}^k |B_j| = \sum_{i=1}^m x_i$ in expectation. Let $A' = A_2 \cup \cdots \cup A_n$. After player 1 takes all the items in B_j, the other players can at least get welfare $|A' \backslash B_j|$ if we allocate items optimally. By induction, in Protocol 4, players 2 to n will get welfare $(C(n-1) - 1/k) \cdot |A' \backslash B_j|$ conditioned on player 1 gets B_j. So in expectation, players 2 to n will get welfare at least $\frac{1}{k} \cdot \sum_{j=1}^k (C(n-1) - 1/k) \cdot |A' \backslash B_j| = (C(n-1) - 1/k) \cdot (|A'| - \sum_{i \in A'} x_i)$. So in expectation, Protocol 4 gets welfare at least

$$\begin{aligned}
& \sum_{i=1}^m x_i + (C(n-1) - 1/k) \cdot (|A'| - \sum_{i \in A'} x_i) \\
\geq\ & \sum_{i=1}^m x_i + (C(n-1) - 1/k) \cdot (|A'| - \sum_{i \in A'} x_i) \\
& + C(n-1)(|A_1| - \frac{|A_1| + \sum_{i=1}^m x_i}{2k} \\
& - \sum_{i=1}^m (x_i - x_i^2) - \sum_{i \in A_1} x_i) \\
=\ & C(n-1) \cdot (|A'| + |A_1|) \\
& + \sum_{i \in A_1 \cup A'} \left((1 - 2C(n-1))\, x_i + C(n-1) x_i^2\right) \\
& + \sum_{i \notin A_1 \cup A'} \left((1 - C(n-1)) x_i + C(n-1) x_i^2\right) \\
& - \frac{1}{k}\left(|A'| - \sum_{i \in A'} x_i + C(n-1) \cdot \frac{|A_1| + \sum_{i=1}^m x_i}{2}\right) \\
\geq\ & C(n-1) \cdot (|A'| + |A_1|) + \sum_{i=1}^m C(n-1) \\
& \cdot \left(\left(x_i - \frac{2C(n-1) - 1}{2C(n-1)}\right)^2 - \frac{(2C(n-1) - 1)^2}{4C(n-1)}\right) \\
& + 0 - \frac{(|A_1| + |A'|) + (\sum_{i \notin A'} x_i + |A'|)}{2k} \\
\geq\ & \left(C(n-1) - \frac{(2C(n-1) - 1)^2}{4C(n-1)} - \frac{1}{k}\right) \\
& \cdot \mathcal{SW}^*(v_1, ..., v_n) \\
=\ & \left(1 - \frac{1}{4C(n-1)} - \frac{1}{k}\right) \cdot \mathcal{SW}^*(v_1, ..., v_n).
\end{aligned}$$

So we have

$$C(n) \geq 1 - \frac{1}{4C(n-1)} = \frac{1}{2} + \frac{C(n-1) - \frac{1}{2}}{2C(n-1)}.$$

This means $C(n-1) \geq 1/2$ would imply $C(n) \geq 1/2$. As $C(2) \geq 3/4$, we know that $C(n) \geq 1/2$ for all $n \geq 2$.

E Missing Proof of Section 5

We now provide a little more detail for the construction. Any claims in the first six bullets are straight-forward without any background in information theory. Formalizing the final bullet is the only tricky part, but will probably appear straight-forward to experts in information theory. The real interest lies in the construction itself.

- First, draw S to be a uniformly random set of size $m/2$. Draw T uniformly random among all sets of

size $m/2$ with $S \cap T = m/3$. Alice will know S (but not T, only that $S \cap T = m/3$), and Bob will know T (but not S).

- Each of Alice's (exponentially many) clauses a_i are drawn uniformly random among sets such that $|a_i \cap S| = m/3$ and $|a_i \cap \bar{S}| = m/6$. In other words, Alice's sets are all of size $m/2$, and all intersect S more than a uniformly random set.
- Each of Bob's (exponentially many) clauses b_i are drawn uniformly random among sets such that $|b_i \cap T| = m/3$ and $|b_i \cap \bar{T}| = m/6$.
- At this point, with very high probability, the optimal welfare is $(3/4 - 1/108)m$.
- Now, notice that there exist (many possible) a_0^0 such that $|a_0^0 \cap S| = m/3 = |a_0^0 \cap T|$. There also exist (many possible) a_0^1 such that $|a_0^1 \cap S| = m/3 = |\bar{a}_0^1 \cap T|$. So with probability $1/2$, add the clause a_0^0 to both Alice and Bob's input. With probability $1/2$, add the clause a_0^1 to Alice's clauses and $b_0^1 = \bar{a}_0^1$ to Bob's.
- We can prove that in case 0, we haven't improved the welfare at all, while in case 1 the welfare has improved to m. So in order to obtain better than a $(3/4 - 1/108)$ approximation for the decision problem, Alice and Bob must figure out whether they are in case 0 or case 1.
- But doing so requires someone to communicate useful information about either a_0 or b_0, which is impossible since all sets appear a priori indistinguishable and there are exponentially many of them.

THEOREM E.1. (RESTATEMENT OF THEOREM 5.1) *For any constant $\varepsilon > 0$, there exists a distribution over binary XOS valuations such that no simultaneous protocol with communication cost less than $e^{2Cm/9}$ can have an α-approximation to the 2-party BXOS decision problem with probability larger than $\frac{1}{2} + 2e^{-Cm/9}$. Here $\alpha = 3/4 - 1/108 + \varepsilon$ and $C = 2\varepsilon^2$.*

Proof. This proof uses mutual information (Definition B.3) and other information theory tools. We also use generalized Chernoff bound for negatively correlated random variables. We mention these tools in Appendix B.

To start the proof, we sample Alice and Bob's valuations v_1 and v_2 from the below procedure. It's basically following the ideas above. Sampling in this specific way will make the later part of the proof easier. Here M is the bit we want to hide in Alice and Bob's inputs. Later we will show M is equal to the output of the decision problem with high probability.

1. Sample S and T uniformly randomly from all the pairs of sets that satisfy $S, T \subseteq [m]$, $|S| = |T| = m/2$, $|S \cap T| = m/3$.
2. Sample bit M uniformly randomly from $\{0, 1\}$. Let $S^c = [m] \backslash S$ and $T^c = [m] \backslash T$.
   (a) If $M = 1$ then sample U_1 uniformly randomly from all the sets that satisfy $S \cap T^c \subseteq U_1$, $|U_1 \cap (S \cap T)| = m/6$, $|U_1 \cap (S^c \cap T^c)| = m/6$ and $|U_1 \cap (T \cap S^c)| = 0$. And let $U_2 = [m] \backslash U_1$.
   (b) If $M = 0$ then sample U_1 uniformly randomly from all the sets that satisfy $S \cap T \subseteq U_1$, $|U_1 \cap (S^c \cap T^c)| = m/6$, $|U_1 \cap (S \cap T^c)| = 0$ and $|U_1 \cap (T \cap S^c)| = 0$. And let $U_2 = U_1$.
3. Let $l = e^{4Cm/9}$. Sample J_1, J_2 uniformly randomly from $[l]$. Set $A_{J_1} = U_1$ and $B_{J_2} = U_2$.
   (a) Define D_S to be the uniform distribution over all sets X such that $X \subseteq [m]$, $|X \cap S| = m/3$ and $|X \cap S^c| = m/6$. For $j = 1, ..., l$ and $j \neq J_1$ sample A_j from D_S.
   (b) Similarly define D_T to be the uniform distribution over all sets X such that $X \subseteq [m]$, $|X \cap T| = m/3$ and $|X \cap T^c| = m/6$. For $j = 1, ..., l$ and $j \neq J_2$ sample B_j from D_T.
4. Finally we set v_1 and v_2 as following:
   (a) For $j = 1, ..., l$, define a_j to be the binary additive valuation such that $a_j(\{i\}) = \mathbb{1}_{i \in A_j}$ for all $i \in [m]$. And set v_1 to be the binary XOS valuation with clauses $a_1, ..., a_l$.
   (b) For $j = 1, ..., l$, define b_j to be the binary additive valuation such that $b_j(\{i\}) = \mathbb{1}_{i \in B_j}$ for all $i \in [m]$. And set v_2 to be the binary XOS valuation with clauses $b_1, ..., b_l$.

Since we are working on a specific distribution, wlog we can assume the simultaneous protocol is deterministic. Let Π_1 be the message sent by Alice and Π_2 be the message sent by Bob in the simultaneous protocol. The rest of the proof proceeds in two steps. We will first show that Π_1 and Π_2 together convey very little information about M to the auctioneer using information theoretic argument. After that, we will show that if the auctioneer has very little information about M, she cannot solve BXOS decision problem with large probability.

For the first step, we prove the following lemma. It's basically stating that $I(\Pi_1\Pi_2; M)$ - the mutual information (Definition B.3) between $\Pi_1\Pi_2$ (messages sent by Alice and Bob) and the bit M is no more than the length of messages over the number of sets Alice/Bob has in its input. Here's an overview of the proof. The proof can be broken down into two parts. In the first part we show $I(\Pi_1\Pi_2; M)$ is upper bounded by $I(\Pi_1; U_1|S) + I(\Pi_2; U_2|T)$. As defined above, U_1 and U_2 are special sets which contain information about M. The proof of the first part is roughly just to use

independence of random variables and the fact that M is a function of U_1 and U_2 to transit through mutual information terms. In the second part of the proof, we show $I(\Pi_1; U_1|S) \leq \frac{|\Pi_1|}{l}$. The idea is that when only S is given, U_1 looks similar to other sets in Alice's input. We can prove that the amount of information Π_1 conveys about U_1 is the same as the amount of information Π_1 conveys about some other set in Alice's input. As Π_1's entropy is at most its length, we can conclude $I(\Pi_1; U_1|S) \leq \frac{|\Pi_1|}{l}$.

LEMMA E.1.

$$I(\Pi_1\Pi_2; M) \leq \frac{|\Pi_1| + |\Pi_2|}{l} = e^{-2Cm/9}.$$

Proof. Since M is independent with S and T, we have

$$\begin{aligned} & I(\Pi_1\Pi_2; M) \leq I(\Pi_1\Pi_2 ST; M) \\ = \; & I(ST; M) + I(\Pi_1\Pi_2; M|ST) \\ = \; & 0 + I(\Pi_1\Pi_2; M|ST). \end{aligned}$$

Since M is a function of U_1 and U_2 ($M = \mathbb{1}_{U_1=U_2}$), we have

$$\begin{aligned} & I(\Pi_1\Pi_2; M|ST) \leq I(\Pi_1\Pi_2; U_1U_2|ST) \\ = \; & I(\Pi_1; U_1U_2|ST) + I(\Pi_2; U_1U_2|ST\Pi_1). \end{aligned}$$

Notice that

$$\begin{aligned} & I(\Pi_2; U_1U_2|ST\Pi_1) \\ = \; & I(\Pi_2; U_1U_2\Pi_1|ST) - I(\Pi_2; \Pi_1|ST) \\ \leq \; & I(\Pi_2; U_1U_2\Pi_1|ST) \\ = \; & I(\Pi_2; U_1U_2|ST) + I(\Pi_2; \Pi_1|STU_1U_2) \\ \leq \; & I(\Pi_2; U_1U_2|ST) + I(v_2; v_1|STU_1U_2) \\ = \; & I(\Pi_2; U_1U_2|ST). \end{aligned}$$

The second last step is because Π_1 is a function of v_1 and Π_2 is a function of v_2. The last step is because after S, T, U_1, U_2 are sampled, v_1 and v_2 are sampled using independent randomness.

It's easy to check that when S, T are given, U_2 is a function of U_1. So we have

$$\begin{aligned} I(\Pi_1; U_1U_2|ST) &= I(\Pi_1; U_1|ST) \\ &= I(\Pi_1; U_1T|S) - I(\Pi_1; T|SU_1) \\ &\leq I(\Pi_1; U_1T|S) \\ &= I(\Pi_1; U_1|S) + I(\Pi_1; T|SU_1) \\ &\leq I(\Pi_1; U_1|S) + I(v_1; T|SU_1) \\ &= I(\Pi_1; U_1|S). \end{aligned}$$

The second last step is because Π_1 is a function of v_1. The last step is because when fixing S and U_1, v_1 is independent with T. Similarly we also get

$$I(\Pi_2; U_1U_2|ST) \leq I(\Pi_2; U_2|T).$$

So far, we get

$$\begin{aligned} & I(\Pi_1\Pi_2; M) \\ \leq \; & I(\Pi_1\Pi_2; M|ST) \\ \leq \; & I(\Pi_1; U_1U_2|ST) + I(\Pi_2; U_1U_2|ST\Pi_1) \\ \leq \; & I(\Pi_1; U_1U_2|ST) + I(\Pi_2; U_1U_2|ST) \\ \leq \; & I(\Pi_1; U_1|S) + I(\Pi_2; U_2|T). \end{aligned}$$

Finally, we just need to bound $I(\Pi_1; U_1|S)$ and $I(\Pi_2; U_2|T)$. First it's easy to check that when S is fixed, A_{J_1} is also distributed as D_S. Therefore given S, fixing J_1 does not change v_1's distribution . So $I(v_1; J_1|S) = 0$. As Π_1 is a function of v_1, we also have $I(\Pi_1; J_1|S) = 0$. Therefore,

$$\begin{aligned} & I(\Pi_1; U_1|S) = I(\Pi_1; A_{J_1}|S) \leq I(\Pi_1; A_{J_1}J_1|S) \\ = \; & I(\Pi_1; J_1|S) + I(\Pi_1; A_{J_1}|SJ_1) = I(\Pi_1; A_{J_1}|SJ_1). \end{aligned}$$

We also have

$$I(\Pi_1; A_1A_2...A_l|S) \leq H(\Pi_1|S) \leq |\Pi_1|.$$

On the other hand, we know that for all $j = 1, ..., l-1$, $I(A_1...A_j; A_{j+1}|S) = 0$. By Fact B.4, we have

$$\begin{aligned} & I(\Pi_1; A_1A_2...A_l|S) \\ = & \sum_{j=1}^{l} I(\Pi_1; A_j|SA_1...A_{j-1}) \geq \sum_{j=1}^{l} I(\Pi_1; A_j|S). \end{aligned}$$

Then we have

$$I(\Pi_1; U_1|S) \leq I(\Pi_1; A_{J_1}|SJ_1) = \frac{1}{l} \cdot \sum_{j=1}^{l} I(\Pi_1; A_j|S) \leq \frac{|\Pi_1|}{l}.$$

Similarly we have

$$I(\Pi_2; U_2|T) \leq \frac{|\Pi_2|}{l}.$$

To sum up, we get

$$I(\Pi_1\Pi_2; M) \leq I(\Pi_1; U_1|S) + I(\Pi_2; U_2|T) \leq \frac{|\Pi_1| + |\Pi_2|}{l}.$$

Now we are going to show that the auctioneer cannot solve the decision problem with large probability based on Lemma E.1. Let D be the output from the auctioneer for the BXOS decision problem. ($D = 1$ if the answer is "yes", $D = 0$ if the answer is no.) Since D is a function of Π_1 and Π_2, we have

$$I(D; M) \leq I(\Pi_1\Pi_2; M) \leq e^{-2Cm/9}.$$

Let $e = \Pr[D \neq M]$. By Fano's inequality ,

$$\begin{aligned} & 1 - (e - 1/2)^2 \geq H(e) \geq H(M|D) \\ & = H(M) - I(M; D) \geq 1 - e^{-2Cm/9}. \end{aligned}$$

So $e \geq 1/2 - e^{-Cm/9}$. This basically states that if mutual information between M and D is small, then the probability of $M \neq D$ is large.

Finally we will show that since $\Pr[D \neq M]$ is large, the algorithm fails to solve the decision problem with large probability. Let W be the indicator variable such that $W = 1$ if the one of the following three events happens and $W = 0$ otherwise:

1. $\alpha m \leq \mathcal{SW}^*(v_1, v_2) < m$.
2. $\mathcal{SW}^*(v_1, v_2) < \alpha m$ and $M = 1$.
3. $\mathcal{SW}^*(v_1, v_2) \geq m$ and $M = 0$.

We know that if $W = 0$, then M is the unique correct output of the decision problem. So the probability that auctioneer fails to solve the decision problem is at least $\Pr[M \neq D] - \Pr[W = 1]$.

Now we need to upper bound $Pr[W = 1]$.

1. When $M = 1$, we know that $\mathcal{SW}^*(v_1, v_2) \geq \mathcal{SW}^*(a_{J_1}, b_{J_2}) = |U_1 \cup U_2| = m$. So $\Pr[W = 1|M = 1] = 0$.
2. When $M = 0$, we know that $\mathcal{SW}^*(v_1, v_2) = \max_{j_1, j_2 \in [l]} \mathcal{SW}^*(a_{j_1}, b_{j_2})$. Therefore,

$$\Pr[W = 1|M = 0] \leq \Pr[\mathcal{SW}^*(v_1, v_2) > \alpha m|M = 0] \leq \sum_{j_1, j_2 \in [l]} \Pr[\mathcal{SW}^*(a_{j_1}, b_{j_2}) \geq \alpha m|M = 0].$$

Define $X_i = \mathbb{1}_{i \in A_{j_1} \cup B_{j_2}}$. We are going to upper bound $\Pr[\mathcal{SW}^*(a_{j_1}, b_{j_2}) \geq \alpha m|M = 0]$ in four different cases.

(a) When $j_1 = J_1$, $j_2 = J_2$: $\mathcal{SW}^*(a_{j_1}, b_{j_2}) = |U_1| = m/2$. In this case $\Pr[\mathcal{SW}^*(a_{j_1}, b_{j_2}) \geq \alpha m|M = 0] = 0$.

(b) When $j_1 = J_1$ and $j_2 \neq J_2$: Fix S and T. We know $X_i = 1$ when $i \in U_1$. $\mathbb{E}[X_i] = 2/3$ when $i \in T \cap S^c$. $\mathbb{E}[X_i] = 1/3$ when $i \in T^c \backslash U_1$. So

$$\mathbb{E}[\mathcal{SW}^*(a_{j_1}, b_{j_2})] = \mathbb{E}[\sum_{i=1}^{m} X_i] = m/2 + (2/3) \cdot (m/6) + (1/3) \cdot (m/3) = 13m/18.$$

Although X_i's are not independent, but it is easy to check that they are negatively correlated. By generalized chernoff bound for negative correlated random variables, we get

$$\Pr[\sum_{i=1}^{m} X_i \geq \alpha m] \leq exp(-2(\alpha - 13/18)^2 m) \leq e^{-Cm}.$$

Thus in this case, we have $Pr[\mathcal{SW}^*(a_{j_1}, b_{j_2}) \geq \alpha m|M = 0] \leq e^{-Cm}$.

(c) When $j_2 = J_2$ and $j_1 \neq J_1$: This is similar to the previous case, we can get $\Pr[\mathcal{SW}^*(a_{j_1}, b_{j_2}) \geq \alpha m|M = 0] \leq e^{-Cm}$.

(d) When $j_1 \neq J_1$ and $j_2 \neq J_2$: Fix S and T. We know $\mathbb{E}[X_i] = 8/9$ when $i \in S \cap T$. $\mathbb{E}[X_i] = 7/9$ when $i \in (T \cap S^c) \cup (S \cap T^c)$. $\mathbb{E}[X_i] = 5/9$ when $i \in S^c \cap T^c$. So

$$\mathbb{E}[\mathcal{SW}^*(a_{j_1}, b_{j_2})] = \mathbb{E}[\sum_{i=1}^{m} X_i] = 20m/27.$$

Although X_i's are not independent, but it is easy to check that they are negatively correlated. By generalized chernoff bound for negative correlated random variables, we get

$$\Pr[\sum_{i=1}^{m} X_i \geq \alpha m] \leq exp(-2(\alpha - 20/27)^2 m) = e^{-Cm}.$$

Thus in this case, we have $\Pr[\mathcal{SW}^*(a_{j_1}, b_{j_2}) \geq \alpha m|M = 0] \leq e^{-Cm}$.

Therefore, we have

$$\Pr[W = 1|M = 0] \leq l^2 \cdot e^{-Cm} = e^{-Cm/9}.$$

To sum up, the auctioneer fails with probability at least

$$\Pr[M \neq D] - \Pr[W = 1] = 1/2 - 2e^{-Cm/9}.$$

References

[1] Noga Alon, Noam Nisan, Ran Raz, and Omri Weinstein. Welfare maximization with limited interaction. In *IEEE 56th Annual Symposium on Foundations of Computer Science, FOCS 2015, Berkeley, CA, USA, 17-20 October, 2015*, pages 1499–1512, 2015.

[2] Sepehr Assadi. Combinatorial auctions do need modest interaction. *manuscript*, 2017.

[3] László Babai, Anna Gál, Peter G. Kimmel, and Satyanarayana V. Lokam. Communication complexity of simultaneous messages. *SIAM J. Comput.*, 33(1):137–166, 2003.

[4] Ashwinkumar Badanidiyuru, Shahar Dobzinski, Hu Fu, Robert Kleinberg, Noam Nisan, and Tim Roughgarden. Sketching valuation functions. In *Proceedings of the Twenty-third Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '12, pages 1025–1035, Philadelphia, PA, USA, 2012. Society for Industrial and Applied Mathematics.

[5] Xiaohui Bei and Zhiyi Huang. Bayesian Incentive Compatibility via Fractional Assignments. In *the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2011.

[6] Kshipra Bhawalkar and Tim Roughgarden. Welfare guarantees for combinatorial auctions with item bidding. In *Proceedings of the Twenty-second Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '11, pages 700–709, Philadelphia, PA, USA, 2011. Society for Industrial and Applied Mathematics.

[7] Mark Braverman, Jieming Mao, and S. Matthew Weinberg. Interpolating between truthful and non-truthful mechanisms for combinatorial auctions. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '16, pages 1444–1457, Philadelphia, PA, USA, 2016. Society for Industrial and Applied Mathematics.

[8] Patrick Briest, Piotr Krysta, and Berthold Vöcking. Approximation techniques for utilitarian mechanism design. In *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing*, STOC '05, pages 39–48, New York, NY, USA, 2005. ACM.

[9] Yang Cai and Christos H. Papadimitriou. Simultaneous bayesian auctions and computational complexity. In *ACM Conference on Economics and Computation, EC '14, Stanford , CA, USA, June 8-12, 2014*, pages 895–910, 2014.

[10] Ashok K. Chandra, Merrick L. Furst, and Richard J. Lipton. Multi-party protocols. In *Proceedings of the 15th Annual ACM Symposium on Theory of Computing, 25-27 April, 1983, Boston, Massachusetts, USA*, pages 94–99, 1983.

[11] George Christodoulou, Annamária Kovács, and Michael Schapira. Bayesian combinatorial auctions. In *ICALP*, 2008.

[12] Edward H. Clarke. Multipart pricing of public goods. *Public Choice*, pages 17–33, 1971.

[13] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, 2006.

[14] Amit Daniely, Michael Schapira, and Gal Shahaf. Inapproximability of truthful mechanisms via generalizations of the vc dimension. In *Proceedings of the Forty-seventh Annual ACM Symposium on Theory of Computing*, STOC '15, pages 401–408, New York, NY, USA, 2015. ACM.

[15] Nikhil Devanur, Jamie Morgenstern, Vasilis Syrgkanis, and S. Matthew Weinberg. Simple auctions with simple strategies. *Manuscript*, 2015. http://www.cs.cmu.edu/ jamiemmt/papers/draft.pdf.

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

[17] Shahar Dobzinski. An impossibility result for truthful combinatorial auctions with submodular valuations. In *Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011, San Jose, CA, USA, 6-8 June 2011*, pages 139–148, 2011.

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

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

[20] Shahar Dobzinski, Hu Fu, and Robert Kleinberg. On the complexity of computing an equilibrium in combinatorial auctions. In *the 26th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2015.

[21] Shahar Dobzinski, Noam Nisan, and Sigal Oren. Economic efficiency requires interaction. In *the 46th annual ACM symposium on Theory of computing (STOC)*, 2014.

[22] Shahar Dobzinski, Noam Nisan, and Michael Schapira. Truthful randomized mechanisms for combinatorial auctions. In *Proceedings of the thirty-eighth annual ACM symposium on Theory of computing*, pages 644–652. ACM, 2006.

[23] Shahar Dobzinski and Michael Schapira. An improved approximation algorithm for combinatorial auctions with submodular bidders. In *Proceedings of the Seventeenth Annual ACM-SIAM Symposium on Discrete Algorithm*, SODA '06, pages 1064–1073, Philadelphia, PA, USA, 2006. Society for Industrial and Applied Mathematics.

[24] Shahar Dobzinski and Jan Vondrák. The computational complexity of truthfulness in combinatorial auctions. In *ACM Conference on Electronic Commerce, EC '12, Valencia, Spain, June 4-8, 2012*, pages 405–422, 2012.

[25] Shahar Dobzinski and Jan Vondrák. From query complexity to computational complexity. In *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 1107–1116, 2012.

[26] Shaddin Dughmi, Tim Roughgarden, and Qiqi Yan. From convex optimization to randomized mechanisms: toward optimal combinatorial auctions. In *Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011, San Jose, CA, USA, 6-8 June 2011*, pages 149–158, 2011.

[27] Shaddin Dughmi and Jan Vondrák. Limitations of randomized mechanisms for combinatorial auctions. In *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*, pages 502–511, 2011.

[28] Pavol Duris, Zvi Galil, and Georg Schnitger. Lower bounds on communication complexity. In *Proceedings of the Sixteenth Annual ACM Symposium on Theory of Computing*, STOC '84, pages 81–91, New York, NY, USA, 1984. ACM.

[29] Uriel Feige. On maximizing welfare when utility functions are subadditive. In *Proceedings of the Thirty-eighth Annual ACM Symposium on Theory of Computing*, STOC '06, pages 41–50, New York, NY, USA, 2006. ACM.

[30] Uriel Feige and Jan Vondrak. The allocation problem

with submodular utility functions. In *In Proc. of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS*, 2006.

[31] Michal Feldman, Ophir Friedler, Jamie Morgenstern, and Guy Reiner. Simple mechanisms for agents with complements. In *Proceedings of the 2016 ACM Conference on Economics and Computation*, EC '16, pages 251–267, New York, NY, USA, 2016. ACM.

[32] Michal Feldman, Hu Fu, Nick Gravin, and Brendan Lucier. Simultaneous auctions are (almost) efficient. In *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*, pages 201–210. ACM, 2013.

[33] Michal Feldman, Nick Gravin, and Brendan Lucier. Combinatorial auctions via posted prices. In *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '15, pages 123–135, Philadelphia, PA, USA, 2015. Society for Industrial and Applied Mathematics.

[34] Theodore Groves. Incentives in teams. *Econometrica*, pages 617–623, 1973.

[35] Jason D. Hartline, Robert Kleinberg, and Azarakhsh Malekian. Bayesian Incentive Compatibility via Matchings. In *the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2011.

[36] Jason D. Hartline and Brendan Lucier. Bayesian Algorithmic Mechanism Design. In *the 42nd ACM Symposium on Theory of Computing (STOC)*, 2010.

[37] Stavros G. Kolliopoulos and Clifford Stein. *Approximating Disjoint-Path Problems Using Greedy Algorithms and Packing Integer Programs*, pages 153–168. Springer Berlin Heidelberg, Berlin, Heidelberg, 1998.

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

[39] Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, New York, NY, USA, 1997.

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

[41] Benny Lehmann, Daniel Lehmann, and Noam Nisan. Combinatorial auctions with decreasing marginal utilities. In *the 3rd Annual ACM Conference on Electronic Commerce (EC)*, 2001.

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

[43] Noam Nisan and Amir Ronen. Algorithmic Mechanism Design (Extended Abstract). In *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing (STOC)*, 1999.

[44] Noam Nisan and Avi Wigderson. Rounds in communication complexity revisited. *SIAM J. Comput.*, 22(1):211–219, February 1993.

[45] Renato Paes Leme, Vasilis Syrgkanis, and Éva Tardos. Sequential auctions and externalities. In *SODA*, 2012.

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

[47] Christos H. Papadimitriou, Michael Schapira, and Yaron Singer. On the hardness of being truthful. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2008.

[48] Christos H. Papadimitriou and Michael Sipser. Communication complexity. In *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing*, STOC '82, pages 196–200, New York, NY, USA, 1982. ACM.

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

[50] Kevin Roberts. The characterization of implementable choice rules. *Jean-Jacques Laffont, editor, Aggregation and Revelation of Preferences*, page 321349, 1979. Papers presented at the 1st European Summer Workshop of the Econometric Society, North-Holland.

[51] Vasilis Syrgkanis and Eva Tardos. Bayesian sequential auctions. In *Proceedings of the 13th ACM Conference on Electronic Commerce*, pages 929–944. ACM, 2012.

[52] Vasilis Syrgkanis and Eva Tardos. Composable and efficient mechanisms. In *STOC*, 2013.

[53] William Vickrey. Counterspeculation, auctions and competitive sealed tenders. *Journal of Finance*, pages 8–37, 1961.

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

[55] Andrew Chi-Chih Yao. Some complexity questions related to distributive computing(preliminary report). In *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing*, STOC '79, pages 209–213, New York, NY, USA, 1979. ACM.