Quantum Communication Complexity of Classical Auctions

Aviad Rubinstein
Department of Computer Science, Stanford University, CA, USA

Zixin Zhou
Department of Computer Science, Stanford University, CA, USA

Abstract

We study the fundamental, classical mechanism design problem of single-buyer multi-item Bayesian revenue-maximizing auctions under the lens of communication complexity between the buyer and the seller. Specifically, we ask whether using quantum communication can be more efficient than classical communication. We have two sets of results, revealing a surprisingly rich landscape – which looks quite different from both quantum communication in non-strategic parties, and classical communication in mechanism design.

We first study the expected communication complexity of approximately optimal auctions. We give quantum auction protocols for buyers with unit-demand or combinatorial valuations that obtain an arbitrarily good approximation of the optimal revenue while running in exponentially more efficient communication compared to classical approximately optimal auctions. However, these auctions come with the caveat that they may require the seller to charge exponentially large payments from a deviating buyer. We show that this caveat is necessary - we give an exponential lower bound on the product of the expected quantum communication and the maximum payment.

We then study the worst-case communication complexity of exactly optimal auctions in an extremely simple setting: additive buyer's valuations over two items. We show the following separations:

- There exists a prior where the optimal classical auction protocol requires infinitely many bits, but a one-way message of 1 qubit and 2 classical bits suffices.
- There exists a prior where no finite one-way quantum auction protocol can obtain the optimal revenue. However, there is a barely-interactive revenue-optimal quantum auction protocol with the following simple structure: the seller prepares a pair of qubits in the EPR state, sends one of them to the buyer, and then the buyer sends 1 qubit and 2 classical bits.
- There exists a prior where no multi-round quantum auction protocol with a finite bound on communication complexity can obtain the optimal revenue.

2012 ACM Subject Classification Theory of computation → Algorithmic mechanism design; Theory of computation → Communication complexity; Theory of computation → Quantum computation theory

Keywords and phrases Mechanism design, Communication complexity, Quantum computing

Digital Object Identifier 10.4230/LIPIcs.ITCS.2025.84

Related Version *Full Version*: https://arxiv.org/abs/2311.12444

Funding *Aviad Rubinstein*: Supported by NSFCCF-1954927, and a David and Lucile Packard Fellowship.
Zixin Zhou: Supported by NSFCCF-1954927, and the Stanford interdisciplinary graduate fellowship.

1 Introduction

We study the quantum communication complexity of classical problems with strategic constraints. The communication problems we study differ from traditional ("cooperative") problems in communication complexity like Set Disjointness due to Incentive Compatibility

16th Innovations in Theoretical Computer Science Conference (ITCS 2025).
Editor: Raghu Meka; Article No. 84; pp. 84:1–84:27
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

(IC) constraints. Informally speaking, one can think of the goal of a traditional communication problem is to design a protocol for both parties that optimizes some common objective function.

For instance, in Set Disjointness, the common goal is to maximize the probability of outputing the correct answer. By contrast, in strategic communication, each party optimizes a different objective; we seek protocols that are communication-efficient, and at the same time don't expect strategic parties to take actions that are mis-aligned with their objectives.

Specifically, we study the quantum communication complexity of a fundamental setting in mechanism design: a monopolistic, revenue-maximizing seller with Bayesian prior auctioning n items to a single buyer; this setting has proved very attractive to researchers in theoretical computer science (e.g. [6, 18, 5, 40, 44, 70] and references therein).

It is known that even with seemingly benign Bayesian priors, revenue-optimality requires complex auctions, e.g. ones that allow the buyer to choose among lotteries [73, 55, 16, 62, 48]. This realization has sparked a fruitful line of work on the simplicity-vs-complexity of (approximately) optimal auctions. Understanding the tradeoffs of simplicity vs. complexity requires formal definitions of complexity.

Perhaps the most well-studied notion of complexity for this problem is the number of distinct lotteries offered to the buyer ("menu-size complexity" [47]). The measure exactly characterizes the *deterministic communication* complexity of the interaction between a buyer and seller who both know the rules of the auction[1] [5].

We study the communication complexity of auctions subject to an Incentive Compatibility (IC) constraint: it is crucial that a strategic buyer must not be able to gain from deviating from the protocol. (As is standard in the literature, we assume that the seller is non-strategic and follows the protocol faithfully. See Section 4 for formal definition, and e.g. [34, 29, 70, 69] for further discussion.) Under this IC constraint, [70] show that it is possible to obtain dramatic savings in communication by considering (classical) *randomized communication*. The main question we ask in this work is whether *quantum communication* can be even more efficient than classical randomized communication complexity for this problem:

Can quantum auction protocols achieve super-classical performance?

Specifically, [70] show that even though randomized auction protocols can be much more efficient than deterministic ones, they still have limitations:

- **Worst-case vs expected CC barrier:** [70] improve the communication complexity in expectation (over the randomness of the protocol), but the worst-case communication complexity of randomized protocols is still characterized by the menu-size complexity.
- **Combinatorial valuations barrier:** For buyers with combinatorial valuations over the items, [70] prove exponential lower bounds even for the expected communication of randomized auction protocols. These lower bounds hold even for approximately optimal mechanisms, and even against restricted classes of valuations (e.g. monotone submodular valuations).

In this paper, we investigate to what extent quantum communication can break these classical barriers.

[1] Specifically, deterministic-CC $= \log\Big(\lceil\text{menu-size complexity}\rceil\Big)$.

1.1 Our Contributions

We formalize a model of *quantum auction protocols* (Definition 7) that extends the randomized auction protocols of [70] by allowing the buyer and seller to send, receive, operate on, and measure qubits. We then provide two sets of results, centered around the two barriers for classical auction protocols mentioned above.

1.1.1 (Un)expected Quantum CC with Combinatorial Valuations

Our first result is an exponential quantum speed-up for auction protocols. It is stated in a general form for a mechanism that chooses an allocation among B possible allocations. Specifically, it gives a near-equivalent IC quantum auction protocol that uses only $O(\log(B))$ qubits – matching the cost of naively encoding the allocation (without strategic considerations).

▶ **Theorem 1** (Efficient in-expectation quantum auction protocols). *Let $\mathcal{D}$ be a prior over buyer's combinatorial valuations over n items; assume all valuations are in the range*[2] $[0, U]$*. Let $\mathcal{M}$ be any mechanism that can only possibly allocate one of B subsets of the items. Finally, let $\delta > 0$ be any parameter (δ may be a function of n or B). Then there is an IC quantum auction protocol that guarantees a $(1 - \delta)$-fraction of $\mathcal{M}$'s expected revenue using $O(\log(B))$ qubits in expectation.*

As a corollary, we only need $O(\log(n))$ qubits for unit-demand, or $O(n)$ qubits for arbitrary combinatorial valuations. On the contrary, [70] shows that any randomized classical communication protocol requires at least $\Omega(n)$ bits for unit-demand, and $\Omega(2^n)$ bits for combinatorial valuations. To the best of our knowledge, this is the first exponential separation of quantum and classical communication in algorithmic game theory.

The positive result in Theorem 1 has a caveat: the protocol may require large payments. Specifically, we need the ability to inflict a large penalty on buyers who deviate from the intended quantum strategy. However, the probability of catching deviating buyers may be exponentially small, so we use exponentially large payments. Even though buyers who follow the protocol can never be penalized, to be accountable for a potentially large payment the buyer may need significant collateral to participate in the auction. Our second result shows that unfortunately without exponentially large payments all the lower bounds from [70] extend to quantum communication.

▶ **Theorem 2** (Efficient protocols require large payments - short version). *Let n be the number of items, P be an upper bound on the payments in the quantum auction protocol (when the valuations are normalized to $[0, 1]$), and $\hat{K}$ an upper bound on the expected communication complexity. Then for a buyer with combinatorial (XOS) valuations, any quantum auction protocol that obtains $\Omega(1)$-approximation to the optimal revenue must satisfy $\hat{K}P = 2^{\Omega(n)}$. See Theorem 8 for full statement and additional results.*

Interestingly, we are not aware of any classical analogs of such tradeoffs between maximum payment and communication complexity. In particular, the exponential lower bounds against classical auction protocols in [70] hold even with arbitrarily large payments.

[2] Our protocol assumes that we're given some finite upper bound U on valuations, but the communication complexity does not depend on U.

1.1.2 Worst-Case Quantum CC with Two Items

Our second set of results focuses on the particularly simple case of a buyer with additive valuations over only two items, and the Bayesian prior for these values is independent. In this case, classical protocols of [70] already achieve $O(1)$ expected communication, but their worst-case communication is infinite. Note that this is for exactly optimal mechanisms – for approximately optimal mechanisms, worst-case can be reduced to expected communication.

We show that on one hand, a *single qubit* can sometimes replace an *infinite* stream of classical bits.

▶ **Theorem 3** (Separating one-way quantum vs classical)**.** *For the problem of auctioning two items to a single buyer, there is a Bayesian prior over independent item values, such that there is a revenue-optimal and IC one-way quantum auction protocol where the buyer sends 1 qubit and 2 classical bits; yet no finite classical auction protocol can achieve the optimal revenue.*

Furthermore, interactive quantum protocols are even more powerful:

▶ **Theorem 4** (Separating interactive quantum vs one-way quantum)**.** *For the problem of auctioning two items to a single buyer, there is a Bayesian prior over independent item values, such that there is an IC revenue-optimal quantum auction protocol where the seller sends 1 qubit to the buyer, who replies with 1 qubit and 2 classical bits; yet no finite classical or one-way quantum auction protocol can achieve the optimal revenue.*

However, in the worst case, even fully interactive quantum auction protocols cannot achieve optimal revenue in finite worst-case communication.

▶ **Theorem 5** (Limitations of finite interactive quantum auction protocols)**.** *For the problem of auctioning two items to a single buyer, there is a Bayesian prior over independent item values, such that there is a revenue-optimal classical auction protocol that requires a constant number of bits* in exepctation*; yet no worst-case finite IC quantum auction protocol can achieve the optimal revenue.*

1.2 Key Takeaway: Thinking About Quantum and Incentives Together

Communication complexity in game-theoretic setting and quantum communication complexity have each been studied extensively over the past few decades, but in separate lines of work, and to a large extent in disjoint communities. The key takeaway from our work is that we can unlock significant advantages by thinking of both together - advantages that are not possible by composing disjoint results for classical-strategic communication and quantum-cooperative communication.

In particular, it is important to note that our quantum speed-ups are not achievable by a generic quantum speed-up on communication (for example, Holevo's theorem states that an n-qubit quantum state, even with infinite precision, can only carry up to n classical bits accessible information [49]). In fact, they cannot be derived from a quantum speed-up on any non-strategic communication problem.

We further note that our infinite separations require quantum operations with infinite precision. While this is clearly not practical, it is the standard textbook model of quantum computing, and, to the best of our knowledge, no previous work on quantum-cooperative communication complexity exhibits infinite separations[3].

[3] Compared with quantum advantages in interactive proofs, e.g. the celebrated $\mathsf{MIP}^* = \mathsf{RE}$ [51], it is

Surprises for the quantum side:

- **Exponential quantum speedup on a natural problem (Theorem 1).** For combinatorial and unit-demand auctions, we find quantum protocols that are exponentially more efficient than any classical protocol. Existing exponential quantum-classical separations (in cooperative communication complexity) are for problems like Hidden Matching Problem [10] that were designed for the purpose of exhibiting a separation. In contrast, the strategic communication problem we study here was considered before in classical algorithmic game theory [5, 70].
- **Infinite 1-way vs. 1-way + entanglement separation (Theorem 4).** Specifically, we show that a one-way protocol with pre-shared entanglement (an EPR pair) is infinitely more efficient than any one-way protocol with no shared entanglement. This unique separation does not exist in the cooperative quantum communication environment as the honest sender can always prepare the EPR pair and send one half through the channel.
- **Infinite quantum-classical separation (Theorem 3).** We construct an example where we can implement the optimal auction with a one-way quantum communication protocol with 3 qubits in the worst case. However, no worst-case finite classical protocol can implement it.

Figure 1 Summary of most surprising aspects of our results from quantum perspective.

We highlight some of the ways in which our results are distinct from previous work in either line of work in Figure 1 and Figure 2.

Core conceptual idea: Efficient, samplable and verifiable distribution encodings

At a high level, the communication protocol of Bayesian auction boils down to the following task: The seller has a set $\mathcal{S}$ consisting of valid distributions of auction outcomes (allocation and payment). The buyer then selects a distribution D from $\mathcal{S}$ that maximizes his utility. Subsequently, the seller draws a sample from the chosen distribution D and outputs it as the outcome. In general, the complexity of describing a distribution is exponentially higher than specifying an outcome. It is worth noting that this task is completely trivial in a fully cooperative environment as the buyer can simply draw the outcome himself and send only this outcome to the seller. A natural quantum solution to this problem is that the buyer can efficiently encode D in state $\sum_x \sqrt{D_x}\,|x\rangle$. To draw an element from the distribution, the seller only needs to measure this quantum state in the computational basis. However, this simple approach has a caveat – in general it is information theoretically impossible for the seller to verify that this quantum state indeed encodes a valid distribution in set $\mathcal{S}$. To overcome this issue, our paper proposes two solutions. The first one is a general spot-check method – with a small probability, after receiving the quantum state, the seller asks the buyer to send the whole classical description of the distribution; the seller verifies that the classical description is valid and the quantum state is close enough to this classical description. By imposing an exponentially large penalty, we ensure that the buyer is always

worth noting that the latter is only an "unbounded" separation, i.e. that separation still needs the complexity of the MIP* provers to go to infinity. In contrast, we show separation of 3 qubits vs infinitely many classical bits.

Surprises for the AGT side:

- **Infinite 1-way vs. interactive separation (Theorem 4).** We show an example where an interactive two-way quantum protocol is infinitely better than any one-way quantum protocol. This unique separation does not exist in the classical setting. Since with a trusted party (the seller in our setting), any classical protocol can be "flattened" to a one-way protocol incurring an exponential overhead in the worst-case communication complexity, yet this overhead remains finite.
- **Exponential lower bound on CC × payment (Theorem 8).** We prove that our exponentially more efficient quantum protocol in Theorem 1 necessitates an exponentially large payment, by establishing an exponential lower bound on the product of payment and communication complexity. This characteristic is distinctive to the quantum setting, as the exponential lower bounds for classical protocols [70] apply even with arbitrarily large payments.

Figure 2 Summary of most surprising aspects of our results from AGT perspective.

incentivized to prepare a quantum state corresponding to a valid distribution while keeping the *expected* communication complexity low. The other solution works for the worst case communication complexity under some specific assumptions on the set of valid distribution of auction outcomes. These assumptions are satisfied for example by the canonical classically-hard example of [24], but not in general (see Theorem 5). By carefully tailoring the quantum protocol to the desired auction, we can ensure that the space of distributions that the buyer can encode coincides with the desired valid space.

1.3 Additional Related Works

Our work extends a rich tradition of studying mechanism design and game theory under the lens of communication complexity – including auctions [61, 12, 4, 31, 28, 26, 27, 14, 2, 15, 33, 3, 5, 76], and also stable matching [41], voting rules [22, 64, 17, 71], fair division [13, 63], computation of equilibria [21, 46, 68, 43, 35, 7, 8, 36, 9], and interdomain routing [53]. In particular, the communication complexity of IC implementing a mechanism vs that of (non-IC) computing the outcome was the focus of [34, 29, 69, 30].

We show exponential separations (and for worst-case complexity – infinite separations) between quantum and classical communication complexity of auctions. Earlier works on separating the two measures (in non-strategic settings) include general boolean functions (constructed for obtaining separations) [65, 10, 37, 38, 66], sampling [1, 57], and very recently also linear regression [58, 72].

Our work is also related to works on quantum game theory – including nonlocal games [19, 20], quantization of classical games [32, 56], quantum equilibria [25, 75], and quantum interactive games [45]. In particular, quantum interactive strategies are also studied in quantum interactive proofs [74, 11, 50, 59, 51].

1.4 Organization

We begin with a review of the quantum communication model and mechanism design in Section 2 and 3, and then introduce our main model of quantum auction protocols in Section 4. Part I brings our results for expected communication: Our quantum auction protocol for combinatorial valuations in Section 5, and our lower bound against quantum auction protocols with bounded maximum payment in Section 6. Part II focuses on worst-case communication: we begin with preliminaries of optimal 2-item auctions in Section 7; in Section 9 we construct an example separating one-way quantum auction protocols from finite classical; in Sections 8 and 10 we separate interactive quantum auction protocols from one-way; and finally in Section 11 we show that in general no finite quantum auction protocol can guarantee optimal revenue.

2 Preliminaries I: Quantum

Bra-ket notation

In this paper, we may occasionally use bra-ket notation. Specifically, within an N-dimensional complex vector space, we represent each unit-length column vector as a ket, denoted as $|\phi\rangle$. Correspondingly, for every unit-length vector $|\phi\rangle$, a bra $\langle\phi|$ is defined as an N-dimensional row vector that is the conjugate transpose of $|\phi\rangle$.

Moreover, we use the notation $|a\rangle$ for $a \in \{1, \dots, N\}$ to indicate the column vector with a value of 1 at the a-th coordinate and 0 in all other positions. We refer to $|1\rangle, \dots, |N\rangle$ as the computational basis.

We employ the notation $|\phi\rangle$ to represent a pure quantum state associated with the density matrix $|\phi\rangle\langle\phi|$. Inversely, a quantum state described by the density matrix ρ is considered a pure state if there exists a $|\phi\rangle \in \mathbb{C}^N$ such that $\rho = |\phi\rangle\langle\phi|$.

Closeness of states

Given two positive semidefinite matrices $\rho, \sigma \in \mathbb{C}^{N\times N}$, the trace distance between them is defined as

$$T(\rho,\sigma) = \max_F \frac{1}{2} \sum_\ell \left|\mathrm{Tr}(F_\ell \rho) - \mathrm{Tr}(F_\ell \sigma)\right|,$$

where $\{F_\ell\}$ is maximized over all possible POVMs[4].

In particular, when ρ and σ are density matrices, $T(\rho,\sigma)$ is equal to the total variation distance between classical distributions obtained by measuring two states maximized over all possible measurements.

Below is an important property of the trace distance:

$$T(\rho,\sigma) \le \sqrt{1 - \mathrm{Tr}(\rho\sigma)}. \tag{1}$$

2.1 (Non-Strategic) Quantum Communicatiom Protocols

We give an overview of multi-party quantum communication protocols. For readers who are familiar with quantum communication, this model is equivalent to the ones used in the literature (e.g. [77]). A formal description of two-party strategic communication model is given in Section 4. A multi-party quantum communication protocol is defined over a system of qubits, that are initially partitioned between the parties. The protocol proceeds in rounds; in each round, one party can locally manipulate or measure her qubits, and then send a

[4] a positive operator-valued measure (POVM) is a finite set of positive semidefinite Hermitian matrices that sum to identity.

subset of them to other parties. The *communication complexity* of a protocol is the total number of qubits sent by parties across all rounds. We now provide more detail on each of those components.

Quantum systems

Let m be an upper bound on the number of qubits in the system.[5] The state $\rho^{(r)}$ of the system at the beginning of round r can be mathematically represented as a *density matrix*[6] $\rho^{(r)} \in (\mathbb{C}^{2\times 2})^{\otimes m}$. Note that $(\mathbb{C}^{2\times 2})^{\otimes m} = \mathbb{C}^{2^m \times 2^m}$, i.e. it is just a 2^m-by-2^m complex matrix; however, the former tensor product notation will be useful when we consider the qubits held by each party.

Initial state of the system

Initially, each party holds $m_i^{(0)}$ qubits ($\sum_i m_i^{(0)} = m$). Because we're concerned with quantum protocols for mechanisms with classical inputs, we assume that initially all the qubits are not entangled (e.g. the initial state is $\rho^{(0)} = (|0\rangle\langle 0|)^{\otimes m}$). In particular, it is important that qubits held by different parties are initially non-entangled.

Local histories

A party's local history consists of the number of qubits that she sent and received in each round so far in the protocol, as well as the outcomes of measurements that she locally performed on her qubits (see more on measurements below).

Local manipulations: unitary operators and measurements

In each round, before sending any qubits, the active party can locally apply quantum operations and measurements to the qubits that she currently holds. If $m_i^{(r)}$ is the number of qubits held by party i at the beginning of round r, we can represent the state $\rho^{(r)}$ as a density matrix in $(\mathbb{C}^{2\times 2})^{\otimes m_i^{(r)}} \otimes (\mathbb{C}^{2\times 2})^{\otimes m - m_i^{(r)}}$. Party i's operations can transform the state into

$$\rho^{(r+1/2)} = (U \otimes I_{2^{m-m_i^{(r)}}})^{\dagger} \rho^{(r)} (U \otimes I_{2^{m-m_i^{(r)}}}),$$

where $I_{2^{m-m_i^{(r)}}}$ is the identity operator on qubits held by other parties, U is a unitary operator of i's choice, acting only on i's qubits, and $\rho^{(r+1/2)}$ is the new state of the quantum system after applying the operator (but before the measurement).

Similarly, party i can measure her qubits. A POVM is defined by L matrices $\{A_\ell\}_{\ell=1}^{L} \in \mathbb{C}^{2^{m_i^{(r)}} \times 2^{m_i^{(r)}}}$ such that $\sum_\ell A_\ell^\dagger A_\ell = I_{2^{m_i^{(r)}}}$. After applying the measurement, with probability

$$\mathrm{Tr}\left(\left(A_\ell \otimes I_{2^{m-m_i^{(r)}}}\right)^{\dagger}\left(A_\ell \otimes I_{2^{m-m_i^{(r)}}}\right)\rho^{(r+1/2)}\right),$$

[5] We assume for simplicity of notation that there is a finite upper bound on the total number of qubits. Our results can be generalized e.g. to a setting where each party can add qubits in each round of the protocol, and a setting where local operators are defined by general quantum channels.

[6] A matrix is a *density matrix* if it is a positive semidefinite, trace 1 Hermitian matrix. *Hermitian* means that $A^\dagger = A$, where $A^\dagger$ is the conjugate transpose of A.

the state of the system is updated to

$$\rho^{(r+1)} = \frac{\left(A_\ell \otimes I_{2^{m-m_i^{(r)}}}\right)^\dagger \rho^{(r+1/2)} \left(A_\ell \otimes I_{2^{m-m_i^{(r)}}}\right)}{\operatorname{Tr}\left(\left(A_\ell \otimes I_{2^{m-m_i^{(r)}}}\right)^\dagger \left(A_\ell \otimes I_{2^{m-m_i^{(r)}}}\right) \rho^{(r+1/2)}\right)}.$$

It is wlog for each party to perform the measurement after all the unitary operators in a given round.

Sending and receiving qubits

After applying local operations, the active party sends exactly one of the qubits she holds to another party. Sending qubits does not change the state of the quantum system, but it changes which party can operate on the sent qubits.

Note that it is wlog to send e.g. the last qubit, because locally qubits can be swapped by unitary operators.

Termination of the protocol

The protocol may terminate after a pre-determined number of rounds, or by any party as a function of her private inputs and/or local history.

Complexity of the protocol

The main metric of complexity of the protocol that we use is the total number of qubits sent by different parties. We give bounds for the complexity of both in-expectation (over the outcome of quantum measurements) and worst-case communication. In addition to the total number of qubits, we will show that: (i) In some cases it is possible to simplify protocols by replacing some qubits with classical bits, and (ii) we also consider the effect of restricting the number of rounds of the protocol.

2.1.1 Conventions

We make the following conventions to simplify both our notation and analysis:

- There is no seperate channel for classical information. For convenience, when we say a message is intended to be classical, it means the receiver immediately measures the qubit in the computational basis ($\left|0\right\rangle, \left|1\right\rangle$).
- For convenience, in a 2-party protocol, when we mention that the a player sends m consecutive qubits to the other, it technically means that this player sends these qubit over m rounds and the other player responds with a dummy qubit in each round.

2.1.2 Choi-Jamiołkowski representation of protocols and strategies

Consider a quantum protocol with a fixed number of rounds R and a fixed number of qubits sent in each round. A *strategy* s_i of a party i who is active in R_i rounds is a sequence of R_i mappings applied to the qubits that it holds at each round, together with a measurement of its qubits at the end of the protocol. A *co-strategy* s_{-i} is a sequence of mappings by other parties at their rounds (and finally a measurement). Notice that the tuple of protocol, strategy, and co-strategy, fully determine the distribution of measurement realizations at the end of the protocol.

Suppose that party i's measurements have L_i possible outcomes and the other parties have L_{-i} possible outcomes. [45] show that any strategy (resp, co-strategy) can be represented as L_i (resp. L_{-i}) matrices of dimension that depend only on the communication complexity, and not on the additional (possibly very large) quantum memory of the parties. For ease of presentation, we state only the simplest form of the theorem that we need; in particular, we avoid the notation necessary for actually defining the Choi-Jamiołkowski representation.

▶ **Theorem 6** (Choi-Jamiołkowski representation of strategies in interactive quantum protocols [45]). *Consider any R-round quantum protocol with communication complexity K, a party i in the protocol, and strategy s_i for i and co-strategy s_{-i} for the rest of the parties. Let $\Phi^{(s_i)}, \Psi^{(s_{-i})}$ denote the respective Choi-Jamiołkowski representation. Then the probability of measuring outcome (a_i, a_{-i}) is given by*

$$2^K \cdot \mathrm{Tr}\left(\Phi^{(s_i)}_{a_i} \Psi^{(s_{-i})}_{a_{-i}}\right).$$

Moreover, each of $\Phi^{(s_i)}_{a_i}$, $\Psi^{(s_{-i})}_{a_{-i}}$ is a 2^{2K} by 2^{2K} positive semidefinite Hermitian matrix, and $\sum_{a_i=1}^{L_i} \mathrm{Tr}\left(\Phi^{(s_i)}_{a_i}\right) = \sum_{a_{-i}=1}^{L_{-i}} \mathrm{Tr}\left(\Phi^{(s_{-i})}_{a_{-i}}\right) = 1$[7].

3 Preliminaries II: Mechanism Design

We consider the mechanism (auction) design for selling n indivisible items to a single risk-neutral buyer. A buyer has a *type* (valuation function) $v : 2^{[n]} \to \mathbb{R}_{\geq 0}$ specifying his value for each bundle (subset). We use X to denote the type set, which contains all possible types of the buyer. For our purposes, it is important to define the two simplest and most widely studied class valuations:

- **Additive** If there exists a value of each item $v_1, \dots, v_n$ such that $v(S) = \sum_{i \in S} v_i$.
- **Unit-demand** If there exists a value of each item $v_1, \dots, v_n$ such that $v(S) = \max_{i \in S} v_i$.

Some of our results also hold for more general classes of valuations[8], which satisfy the following hierarchy of increasing generality:

additive, unit-demand ⊂ gross-substitutes ⊂ submodular ⊂ XOS ⊂ subadditive ⊂ combinatorial.

In addition to satisfying these structures, valuations are usually assumed to be monotone; our results hold for both monotone and non-monotone valuations.

Without loss of generality, we consider direct mechanisms. The buyer reports a type $v' \in X$ to the mechanism, and the mechanism then allocates a (randomized) bundle to the buyer and charges the buyer a price. $\mathcal{M}$ consists of two functions.

- An allocation function $\mathcal{A} : X \to [0,1]^{2^{[n]}}$ gives the probability of allocating each bundle to the buyer declares to have each possible type.
- A payment function $\mathcal{Q} : X \to \mathbb{R}_{\geq 0}$ gives the price the buyer needs to pay for each declared type of the buyer.

Let D be a distribution over bundles. With a slight abuse of notation, we denote by $v(D) = \mathbb{E}_{S \sim D} v(S)$ the expected value of the buyer with type v.

[7] In the original definition of [45], Choi-Jamiołkowski representations $\Phi^{(s_i)}, \Psi^{(s_{-i})}$ are not normalized. Here, we normalize all Choi-Jamiołkowski representations (now they are all density matrices), that is why we have an additional 2^K factor in the probability of outcome compared to the original paper.

[8] See e.g. [52] for definitions; they are not necessary for understanding our paper.

We say a mechanism $\mathcal{M} = (\mathcal{A}, \mathcal{Q})$ is *incentive compatible* (IC) if

$$v(\mathcal{A}(v)) - \mathcal{Q}(v) \geq v(\mathcal{A}(v')) - \mathcal{Q}(v') \quad \forall v, v' \in X.$$

We say a mechanism $\mathcal{M} = (\mathcal{A}, \mathcal{Q})$ is *ε-incentive compatible* (ε-IC) if

$$v(\mathcal{A}(v)) - \mathcal{Q}(v) \geq v(\mathcal{A}(v')) - \mathcal{Q}(v') - \varepsilon \quad \forall v, v' \in X.$$

We say a mechanism $\mathcal{M} = (\mathcal{A}, \mathcal{Q})$ is *individually rational* (IR) if

$$v(\mathcal{A}(v)) - \mathcal{Q}(v) \geq 0 \quad \forall v \in X.$$

We say a mechanism $\mathcal{M} = (\mathcal{A}, \mathcal{Q})$ is *ε-individually rational* (ε-IR) if

$$v(\mathcal{A}(v)) - \mathcal{Q}(v) \geq -\varepsilon \quad \forall v \in X.$$

For a mechanism $\mathcal{M} = (\mathcal{A}, \mathcal{Q})$, we denote by $u : X \to \mathbb{R}$ the expected utility of the buyer when he truthfully reports the valuation function. It follows from the definition that $u(v) = v(\mathcal{A}(v)) - \mathcal{Q}(v)$.

Revenue Maximization

In this paper, we primarily focus on the revenue-optimal Bayesian mechanism design. In this setting, the buyer knows his type v for sure. However, the seller only knows the probability distribution over X. Let $f : X \to \mathbb{R}$ be the probability density function of this distribution.

The goal of revenue-optimal Bayesian mechanism design is to find an IC and IR mechanism $\mathcal{M} = (\mathcal{A}, \mathcal{Q})$ that maximizes the revenue of the seller:

$$Rev = \int_X \mathcal{Q}(v) f(v) \mathrm{d}v.$$

4 Quantum Communication Model with a Strategic Player

We now introduce the main strategic communication model of this work, which formally defines the elements of a two-player quantum communication protocol subject to strategic manipulation. In essence, when the length of the protocol is fixed, this model is equivalent to the one used in the literature of quantum games and quantum interactive proofs (see e.g. [45]). The communication is between one strategic player (we call it the buyer), and a truthful player (we call it the seller). In this setup, the seller initially possesses n qubits, while the buyer has m qubits, with S representing the finite set of possible communication outcomes. Initially, the joint state is $|0\rangle^{\otimes(n+m)}$. The communication proceeds in rounds (or steps). Since we will cover protocols with infinite worst-case communication complexity (but bounded expected communication), we do not specify the total number of rounds in our model. In each round, one of the player performs a local operation on qubits in their hand and then sends *one* qubit to the other player. Or you can alternatively think there is a one-qubit register shared by both players. We assume the seller takes the first round and then they alternate in the following rounds.

The seller's operations

Without loss of generality, we assume the seller only performs general measurements in her rounds[9]. For round i, let $\{A^i_x\}_{x \in S \cup \{\perp\}}$, such that $\sum_{x \in S \cup \{\perp\}} (A^i_x)^\dagger A^i_x = I_{2^n}$, be the seller's

[9] If the seller simply want to apply a unitary U, she can do it by letting $A^i_\perp = U$, and $A^i_x = 0$ for any $x \in S$.

measurements. Let $h_i \in S \cup \{\perp\}$ be the measurement outcome of round i. For each round i, if $h_i = \perp$ then communication continues, otherwise the seller terminates the communication and outputs h_i as the outcome[10].

The buyer's operations

In our model, only seller can terminate the protocol and output an outcome. Therefore, by the principle of deferred measurement (see e.g. Chapter 4.4 of [60]), we wlog assume the buyer makes no measurement[11], and his only local operation in round i is a unitary U_i with dimension 2^{m+1}, for $i = 2, 4, \ldots$.

The seller's strategy

A seller's strategy includes the following elements:

- Set of communication outcomes: S.
- The size of initial local quantum memory: n.
- General measurements: $\{A_x^i\}_{x \in S \cup \{\perp\}}$, for $i = 1, 3, 5, \ldots$.

The buyer's strategy

A buyer's strategy s^{buy} includes the following elements:

- The size of initial local quantum memory: m.
- Unitary operators: U_i, for $i = 2, 4, 6, \ldots$.

Quantum auction protocols

Our objective is to implement an auction using the strategic quantum communication model previously outlined. Our quantum auction protocols are a generalization of classical auction protocols defined in [70]. The classical auction protocols are also a special case of Bayesian incentive compatibility (BIC)-incentivizable binary dynamic mechanism (BDM) defined in [34]. For simplicity, here we only define the quantum analog for auctions, but exploring the quantum communication complexity of mechanisms more broadly is an interesting direction for future work.

▶ **Definition 7** (Quantum auction protocols). *A* quantum auction protocol $\mathcal{P}$ *that sells* n *items to a single buyer with type space* X *consists of:*

- *A seller's strategy* $s^{\mathcal{P}}_{seller}$ *such that the outcomes in the outcome set* S *are in the form* (B, p)*, where* $B \subseteq [n]$ *is a subset of items and* $p \in \mathbb{R}_{\geq 0}$ *is the price.*
- *A suggested strategy function* $s^{\mathcal{P}}_*$ *that maps each valuation in the type space* X *to a buyer's strategy.*

[10] By the principle of deferred measurement (see e.g. Chapter 4.4 of [60]), any non-terminating measurements outcomes can be removed by adding more qubits to the system. Therefore, it is wlog to only consider measurement with at most one non-terminiating outcome($\perp$) each round.

[11] By the principle of deferred measurement, the buyer can always obtain the same outcome distribution by adding more qubits to his local memory and removing measurements. Since the buyer is allowed to choose an arbitrarily large memory size m (we will discuss it later), it is wlog not to consider buyer's measurement.

Given a seller's strategy s_{seller}, and a buyer's strategy s_{buyer} let $D(s_{\text{seller}}, s_{\text{buyer}})$ be the outcome distribution of the communication[12]. Let $\mathcal{A}(s_{\text{seller}}, s_{\text{buyer}})$ be the marginal distribution of the first component of $D(s_{\text{seller}}, s_{\text{buyer}})$. So, $\mathcal{A}(s_{\text{seller}}, s_{\text{buyer}})$ is a distribution over subsets of $[n]$. Let $\mathcal{Q}(s_{\text{seller}}, s_{\text{buyer}})$ be the expected value of the second component (price) of $D(s_{\text{seller}}, s_{\text{buyer}})$.

With definitions above, we say a quantum auction protocol $\mathcal{P}$ *implements* the mechanism

$$\mathcal{M}^{\mathcal{P}} = \left(\mathcal{A}(s^{\mathcal{P}}_{\text{seller}}, s^{\mathcal{P}}_{*}(\cdot)), \mathcal{Q}((s^{\mathcal{P}}_{\text{seller}}, s^{\mathcal{P}}_{*}(\cdot))\right).$$

Further, we say a quantum auction protocol $\mathcal{P}$ is ε-IC if for any type $v \in X$, and any buyer's strategy $\hat{s}$, the following holds,

$$v\left(\mathcal{A}(s^{\mathcal{P}}_{\text{seller}}, s^{\mathcal{P}}_{*}(v))\right) - \mathcal{Q}(s^{\mathcal{P}}_{\text{seller}}, s^{\mathcal{P}}_{*}(v)) \geq v\left(\mathcal{A}(s^{\mathcal{P}}_{\text{seller}}, \hat{s})\right) - \mathcal{Q}(s^{\mathcal{P}}_{\text{seller}}, \hat{s}) - \varepsilon.$$

By definition, the mechanism implemented by an ε-IC quantum auction protocol is an ε-IC mechanism.

We say quantum auction protocol $\mathcal{P}$ is ε-IR if for any type $v \in X$ the following holds,

$$v\left(\mathcal{A}(s^{\mathcal{P}}_{\text{seller}}, s^{\mathcal{P}}_{*}(v))\right) - \mathcal{Q}(s^{\mathcal{P}}_{\text{seller}}, s^{\mathcal{P}}_{*}(v)) \geq -\varepsilon.$$

By definition, the mechanism implemented by an ε-IR quantum auction protocol is an ε-IR mechanism.

Exactly IC and IR quantum protocols are defined similarly.

The main goal of our paper is to find an (ε-)IC and (ε-)IR quantum auction protocol that implements the revenue-optimal mechanism.

Part I

Expected communication

5 ε-IC Quantum Protocols for General Valuations

Consider selling n items to a single buyer with combinatorial valuations drawn from prior $\mathcal{D}$. We will show that for any direct IC mechanism $\mathcal{M}$ that only ever allocates B different deterministic bundles, there is an ε-IC quantum protocol with the same expected payment for every type using $O(\log B)$ qubits of communication in expectation. Note that our protocol holds for arbitrarily small ε, and the constant factor in $O(\log B)$ does not depend on ε.

Moreover, by employing a standard ε-IC-to-IC reduction that discounts all the payments by $(1-\sqrt{\varepsilon})$-factor, we can transform an ε-IC quantum protocol into an exactly IC quantum protocol that has the same expected communication complexity, while incurring only a negligible loss in revenue (see e.g. [42, Theorem 7]).

▶ **Theorem** (Theorem 1 restated). *Let $\mathcal{D}$ be a prior over buyer's combinatorial valuations over n; assume all valuations are in the range $[0, U]$. Let $\mathcal{M}$ be any mechanism that can only possibly allocate one of B subsets of the items. Finally, let $\delta > 0$ be any parameter (δ may be a function of n or B). Then there is an IC auction quantum protocol that guarantees a $(1-\delta)$-fraction of $\mathcal{M}$'s expected revenue using $O(\log(B))$ qubits in expectation.*

[12] Throughout the paper we only consider seller's strategies which guarantee termination within finite steps with probability 1 for any buyer's strategy.

We first present a modification of an $O(B\log(B))$-bits classical protocol given in [70]. Then, we augment it with a single quantum message from the buyer to the seller that gives an exponential improvement in the expected communication.

5.1 Warm-up: An Inefficient Classical Protocol [70]

First note that if the maximum value of the buyer over any bundle is at most U, any IC and IR direct mechanism $\mathcal{M}$ that only ever allocates B different bundles can be converted into an equivalent direct mechanism $\mathcal{M}'$ that only ever allocates B different bundles and always charges either 0 or U. This implies the new mechanism $\mathcal{M}'$ has $2B$ different deterministic outcomes (each deterministic outcome is a bundle-payment pair). Suppose B different bundles allocated in $\mathcal{M}$ are $\pi_1,\ldots,\pi_B$, then $\mathcal{M}'$ creates 2 outcomes $(\pi_j,0),(\pi_j,U)$ for each bundle in $\mathcal{M}$. For each type, v, $\mathcal{M}$ has a distribution over B bundles and an expected payment P (by IR, $P\leq U$). Then $\mathcal{M}'$ defines a distribution over $2B$ outcomes for each type v: suppose in $\mathcal{M}$ the proability of receiving π_j is p_j, $\mathcal{M}'$ gives outcome (π_j,U) with probability $p_j\cdot\frac{P}{U}$ and outcome $(\pi_j,0)$ with probability $p_j\cdot(1-\frac{P}{U})$.

We first present a classical (randomized) IC protocol that implements $\mathcal{M}'$ with $O(B\log B)$ expected communication complexity. This protocol differs slightly from the one in [70] and serves as a more straightforward foundation for constructing a quantum protocol. A probability distribution over $2B$ outcomes can be represented by $2B$ non-negative real numbers $p_1,\ldots,p_{2B}$ such that $\sum_{i=1}^{2B}p_j=1$. We call a distribution *feasible* if it is a distribution over $2B$ outcomes for some type in mechanism $\mathcal{M}'$. At each round, the buyer sends $2B$ bits, and the seller either terminates the protocol with an allocation and a payment or continues by moving to the next round and letting the buyer send more bits.

Buyer's suggested strategy

Given the buyer's type and mechanism $\mathcal{M}'$, we denote by $p_1,\ldots,p_{2B}$ the probability of each outcome. The buyer sends $2B$ bits each round. The suggested strategy is to send, in the r-th Buyer round, the r-th bit of the binary representation of $p_1,\ldots,p_{2B}$, respectively.

Seller's strategy

After receiving each bit, the seller first checks if all buyer's messages so far are consistent with some feasible distributions, which means messages are binary prefixes of probabilities corresponding to some feasible distributions. When there is only one possible value for the next bit that is consistent with some feasible distribution, then the seller sets the value of the next bit of the message to be the only feasible value and ignores the original bit of the message.

Let $m_j^{(r)}$ be the j-th bit of message receives at round r. For round r, we denote by $\tau^{(r)}$ the total probability revealed so far.

In addition, we define $\tau^{(0)}=0$. After receiving all $2B$ bits of message at round r, the protocol terminates with probility $\frac{\tau^{(r)}-\tau^{(r-1)}}{1-\tau^{(r-1)}}$. Conditioned on terminating, the protocol assigns allocation and payment of outcome j of $\mathcal{M}'$ with probability $\frac{m_j^{(r)}\cdot 2^{-r}}{\tau^{(r)}-\tau^{(r-1)}}$ for each j. Finally, with probability $1-\frac{\tau^{(r)}-\tau^{(r-1)}}{1-\tau^{(r-1)}}$, the protocol continues. It is important to note that the protocol terminates in no longer than r rounds with probability $\tau^{(r)}$.

IC

The suggested strategy is optimal for the buyer.

Communication complexity

The overall expected communication complexity is $O(B \log B)$.

5.2 Quantum Protocol

The idea of our quantum protocol is to replace all classical bits the buyer sends in the first $2 \log B$ rounds (total of $O(B \log B)$ bits) with a single message with $\log(B) + 1$ qubits and $2 \log B$ classical bits. Note that $\log(B) + 1$ qubits can encode an arbitrary distribution with support size $2B$ (see details below). The buyer is supposed to encode the distribution associated with his type into a quantum state. Then the seller can measure the quantum state and decide the allocation and payment according to the outcome. Here, the problem with this approach is that the buyer might encode an infeasible distribution (not associated with any type), and the seller has no way to tell if a quantum state encodes a feasible distribution.

To overcome this challenge, the seller will, with high probability, blindly trust the buyer and determine the allocation and payment according to the measurement outcome. However, with a small probability, rather than measuring the qubits, the seller asks the buyer to reveal the probability distribution he encoded by sending its full description classically. Subsequently, the seller can perform a measurement to verify if the quantum state accurately encodes the given distribution. Specifically, any quantum state that unfaithfully encodes the distribution will fail the test with a non-zero probability. As a result, the protocol can penalize the buyer with a big payment once she observes that the test has failed.

Seller's strategy

In the first round, the seller expects a quantum message of $(\log(B) + 1)$ qubits, which we denote by m_Q, and a $\log(B + 1)$-bit classical message that represents an integer $\hat{\tau} \in [0, B]$.

With probability $\gamma(\hat{\tau}) = 1 - \frac{1}{2B} - (1 - \frac{1}{2B})\frac{\hat{\tau}}{B^2}$, the seller measures the quantum message m_Q in the computational basis $(|1\rangle, |2\rangle, \ldots, |2B\rangle)$ and terminates the protocol. Suppose the measurement outcome is $|a\rangle \in \{|1\rangle, |2\rangle, \ldots, |2B\rangle\}$, the allocation and payment are determined according to outcome a of mechanism $\mathcal{M}'$.

With probability $1 - \gamma(\hat{\tau}) = \frac{1}{2B} + (1 - \frac{1}{2B})\frac{\hat{\tau}}{B^2}$, the seller asks the buyer to send $4B \log B$ classical bits to represent $2B$ binary numbers, $\widehat{p_1}, \ldots, \widehat{p_{2B}}$, each consisting of $2 \log B$ bits (we denote by m_C this classical message). Applying the same correction procedure as described in Subsection 5.1, we can assume that $\widehat{p_1}, \ldots, \widehat{p_{2B}}$ is the rounding-down to nearest multiple of $1/B^2$ of a feasible distribution $p_1, \ldots, p_{2B}$. The seller then verifies that $\hat{\tau} = B^2 \cdot (1 - \sum_i \widehat{p_i})$; if it isn't, the protocol terminates with the empty allocation and payment $2BU^3\varepsilon^{-2}$. Next, the seller measures the quantum message she receives earlier m_Q in a way such that the measurement has two outcomes $0, 1$, and the probability of outcome 1 is given by $\mathrm{Tr}(\rho |\psi\rangle\langle\psi|)$, where ρ is the reduced density matrix that represents the state of m_Q at the time of measurement, and $|\psi\rangle$ is the canonical state of classical message m_C that is given by $|\psi\rangle = \frac{B}{\sqrt{B^2 - \hat{\tau}}} \sum_{i=1}^{2B} \sqrt{\widehat{p_i}} |i\rangle$.

If the measurement outcome is 0, the protocol terminates with empty allocation and payment $2BU^3\varepsilon^{-2}$. Otherwise, the protocol continues as a purely classical protocol in the following manner: for each $i \in \{1, \ldots, 2B\}$, with probability $\frac{1}{2B(1-\gamma(\hat{\tau}))}\widehat{p_i}$, the protocol terminates with outcome i of mechanism $\mathcal{M}'$. Finally, with probability $1 - \frac{1}{2B(1-\gamma(\hat{\tau}))} \sum_i \widehat{p_i}$, the seller starts to run the classical protocol from round $2 \log B + 1$ and let $\widehat{p_1}, \ldots, \widehat{p_{2B}}$ be the message she received in the first $2 \log B$ rounds.

Buyer's suggested strategy

Given the buyer's type and mechanism $\mathcal{M}'$, we denote by $p_1, \dots, p_{2B}$ the probability of each outcome. Let $\widetilde{p_1}, \dots, \widetilde{p_{2B}}$ be the numbers such that for any i, the binary representation of $\widetilde{p_i}$ consists of first $2\log B$ bits of the binary representation of p_i. The suggested strategy is to send, for quantum message m_Q whose density matrix is given by $|\varphi\rangle\langle\varphi|$, where $|\varphi\rangle$ is defined as $|\varphi\rangle = \frac{B}{\sqrt{B^2-\tilde{\tau}}}\sum_{i=1}^{2B}\sqrt{\widetilde{p_i}}\,|i\rangle$, and send integer $\tilde{\tau} = B^2(1-\sum_i \widetilde{p_i})$. In addition, when the protocol asks the buyer to send classical message m_C, the suggested strategy sends $\widetilde{p_1}, \dots, \widetilde{p_{2B}}$. Finally, as for the classical protocol part, for round corresponding to the r-th round of the classical protocol, the suggested strategy is to send the r-th bit of the binary representation of $p_1, \dots, p_{2B}$, respectively.

ε-IC

We demonstrate that this protocol is ε-IC.

Communication complexity

The overall expected communication complexity is $O(\log B)$.

6 Lower Bounds for Quantum Protocols with Small Payments

Throughout this section, we normalize the valuations so that the upper bound on the highest value is $U = 1$.

▶ **Theorem 8** (Full version of Theorem 2). *Let n be the number of items, P be the upper bound on the payments and in the quantum auction protocol, and $\hat{K}$ an upper bound on the expected communication complexity. Then we have the following lower bounds on $\hat{K}P$:*

- *For unit-demand valuations, any quantum auction protocol that obtains $\Omega(1)$-approximation to the optimal revenue must satisfy $\hat{K}P = \Omega(n)$.*
- *For Gross-substitutes valuations, any quantum auction protocol that obtains $\Omega(1)$-approximation to the optimal revenue must satisfy $\hat{K}P = 2^{\Omega(n^{1/3})}$.*
- *For XOS valuations, any quantum auction protocol that obtains $\Omega(1)$-approximation to the optimal revenue must satisfy $\hat{K}P = 2^{\Omega(n)}$.*
- *For XOS valuations over independent items, any quantum auction protocol that obtains $4/5 + \Omega(1)$-approximation to the optimal revenue must satisfy $\hat{K}P = 2^{\Omega(n)}$.*

6.1 A List-Decodable Code of Bayesian Priors

The lower bounds of [70] against approximately optimal classical auction protocols construct, for each valuation class (unit-demand, submodular, etc.), a family of Bayesian priors over valuations from this class. Each family has the following "list-decodability" guarantee: no mechanism can simultaneously obtain high revenue on a "list" of $\omega(1)$ priors from the family. We now state the results from [70], with different parameters for family size and approximability for different valuation classes.

▶ **Lemma 9** (Family of hard priors [70]). *For each of the following combinations of valuation class X over n items, family size ζ, and approximability factor γ, there exists a family of ζ Bayesian priors over valuations from X, and a small constant $\varepsilon > 0$ such that no single ε-IC and ε-IR mechanism can simultaneously obtain a γ-approximation of the optimal revenue from $\omega(1)$ distinct priors from the family.*

- X = *unit-demand;* $\zeta = 2^{2^{\Omega(n)}}$*;* $\gamma =$ *arbitrarily small constant.*
- X = *gross-substitute;* $\zeta = 2^{2^{2^{o(n^{1/3})}}}$*;* $\gamma =$ *arbitrarily small constant.*
- X = *XOS;* $\zeta = 2^{2^{2^{\Omega(n)}}}$*;* $\gamma =$ *arbitrarily small constant.*
- X = *XOS over independent items;* $\zeta = 2^{2^{2^{\Omega(n)}}}$*;* $\gamma = 4/5 + \tau$ *for arbitrarily small constant* τ*.*

6.2 Approximate Cover over Efficient Quantum Auction Protocols

Our next objective is to demonstrate the existence of a finite set of protocols capable of approximating any (almost) IC and (almost) IR quantum protocol with bounded worst-case communication complexity. Formally speaking, we have the following lemma.

▶ **Lemma 10** (Approximate cover over efficient quantum auction protocols)**.** *Let* X *be a type space with* n *items,* B *an upper bound of number of feasible bundles,* P *an upper bound of payments and values of types in* X*,* $\varepsilon > 0$ *as an approximation parameter, and* K *an upper bound on the communication complexity, there exists a set* $\mathcal{S} = \mathcal{S}(n, B, P, \varepsilon, K)$ *of mechanisms such that the following hold:*

- *Small cover:* $|\mathcal{S}| = 2^{2^{O(K+\log B+\log\log P+\log n)}}$.
- *Mechanisms in* $\mathcal{S}$ *are* $2\sqrt{\varepsilon}$*-IC and* $2\sqrt{\varepsilon}$*-IR.*
- *Approximate covering property: For any* ε*-IC and* ε*-IR quantum protocol* $\mathcal{P}$ *with a worst-case communication complexity bounded by* K*, let* $\mathcal{M}_{\mathcal{P}} = (\mathcal{A}_{\mathcal{P}}, \mathcal{Q}_{\mathcal{P}})$ *be the mechanism induced by* $\mathcal{P}$*. Then there exists a mechanism* $\mathcal{M} = (\mathcal{A}, \mathcal{Q}) \in \mathcal{S}$ *such that for every type* $v \in X$*, we have*

$$\mathcal{Q}(v) \geq (1 - \sqrt{\varepsilon})\mathcal{Q}_{\mathcal{P}}(v).$$

Part II
Worst-case communication

7 Preliminaries III: Optimal Mehchanisms for Selling 2 Items

In this section, we introduce a special case of framework of [24, 39] to characterize optimal auctions for selling two goods to a single additive buyer with independent valuations. We will first give a picture of their framework and then discuss how to apply duality theory to show that infinite menu complexity (aka infinite worst-case classical communication complexity) is inevitable for the optimal mechanisms of some prior distributions.

For simplicity, we only consider the case where the buyer's type space X is $[0, 1]^2$, and each coordinate represents the buyer's value of each good. We assume the prior distribution has a density function $f(x, y) = f_1(x)f_2(y)$. Further, we assume f_1, f_2 are continuous and differentiable with bounded derivatives.

It is well-known (see e.g. [67, 54], that for any IC and IR mechanism the utility function $u : [0, 1]^2 \to \mathbb{R}$ is convex, non-negative, non-decreasing, and 1-Lipschitz with respect to the ℓ_1 norm. Also, given any $u : [0, 1]^2 \to \mathbb{R}$ with these conditions, the utility function uniquely[13] defines an IC and IR mechanism $\mathcal{M}$ with allocation function $\mathcal{A}(v) = \nabla u(v)$ and payment function $\mathcal{Q}(v) = \mathcal{A}(v) \cdot v - u(v)$.

[13] Up to measure zero.

At a high level, the mechanisms established in [24, 39] partition $[0,1]^2$ into 4 regions $Z, \mathcal{A}, \mathcal{B}, \mathcal{W}$ induced by a convex area Z defined by two concave functions s_1, s_2 and a straight line $x+y=P_{\text{crit}}$ for some $P_{\text{crit}} \in [0,2]$. Moreover, [24] calls $Z, \mathcal{A}, \mathcal{B}, \mathcal{W}$ *the canonical partition with respect to* Z, and P_{crit} *the critical price.* For ease of exposition, we only consider the case that the line $x+y=P_{\text{crit}}$ intersects both curves $x=s_1(y)$ and $y=s_2(x)$.

More precisely, let $s_1, s_2 : [0,1] \to [0,1]$ be two 1-Lipschitz, concave and non-increasing function, and $P_{\text{crit}} \in [0,2]$. Let x_{crit} be the solution to $s_2(x) = P_{\text{crit}} - x$, and y_{crit} be the solution to $s_1(y) = P_{\text{crit}} - y$. We can always find such solutions since we assume the line $x+y=P_{\text{crit}}$ intersects both curves.

Region $Z \subseteq [0,1]^2$ is defined as the region enclosed by s_1, s_2, and line $x+y=P_{\text{crit}}$. Formally, $Z = \{(x,y) \in [0,1]^2 : x \le s_1(y), y \le s_2(x), x+y \le P_{\text{crit}}\}$. The other three regions are defined as follows:

$$\mathcal{A} = \{(x,y) \in [0,1]^2 : x < x_{\text{crit}}\} \backslash Z; \quad \mathcal{B} = \{(x,y) \in [0,1]^2 : y < y_{\text{crit}}\} \backslash Z; \quad \mathcal{W} = [0,1]^2 \backslash (Z \cup \mathcal{A} \cup \mathcal{B}).$$

▶ **Definition 11** (GK conditions [39]). *Let* $\mu(x,y) = 3f_1(x)f_2(y) + xf_1'(x)f_2(y) + yf_2'(y)f_1(x)$. *Given a canonical partition of* $[0,1]^2$ *induced by* s_1, s_2, *and* P_{crit}, *we say that it satisfies* GK conditions *with respect to* f_1, f_2 *if it satisfies the following conditions:*

- $\mu(x,y) > 0$ *for all* $(x,y) \in [0,1]^2$, *and*
- $\int_Z \mu(x,y) = 1$, *and*
- $\int_{s_1(y)}^1 \mu(x,y) \mathrm{d}x = f_1(1)f_2(y)$, *for all* $y \in [0, y_{crit}]$, *and*
- $\int_{s_2(x)}^1 \mu(x,y) \mathrm{d}y = f_1(x)f_2(1)$, *for all* $x \in [0, x_{crit}]$.

Finally by [39] (specifically, their Theorem 1 and duality discussions in Section 2.2), we have the following characterization of the optimal mechanism.

▶ **Theorem 12** (Uniqueness and characterization of optimal auction [39]). *Given probability density functions* f_1, f_2 *over* $[0,1]$. *Suppose that canonical partition* $(Z, \mathcal{A}, \mathcal{B}, \mathcal{W})$ *induced by* 1*-Lipschitz, concave and non-increasing functions* s_1, s_2, *and* $P_{\text{crit}} \in [0,2]$ *satisfies the GK conditions. The utility function* $u(x,y)$ *of the optimal IC and IR mechanism for selling two items to a single additive buyer with independent prior distributions* f_1, f_2 *is given by*

$$u(x,y) = \max(0, x - s_1(y), y - s_2(x), x + y - P_{\text{crit}}).$$

Specifically,

- *if* $(x,y) \in Z$, $u(x,y) = 0$;
- *if* $(x,y) \in \mathcal{A}$, $u(x,y) = y - s_2(x)$;
- *if* $(x,y) \in \mathcal{B}$, $u(x,y) = x - s_1(y)$;
- *if* $(x,y) \in \mathcal{W}$, $u(x,y) = x + y - P_{\text{crit}}$.

Moreover, the optimal utility function $u(x,y)$ *is unique in regions* $\mathcal{A}, \mathcal{B}, Z$.

8 Limitations of One-Way Quantum Protocols

[24] studies the optimal auction of selling two items to a single additive buyer with i.i.d. valuations from Beta$(1,2)$. It characterizes the unique utility function $u(\cdot)$ for any optimal mechanism. In particular they show that in the region $y=1$ and $x \in [0, 0.06]$, the unique utility function for optimal mechanism is given by $u(x,1) = \frac{2-2x}{4-5x}$.

In this section, we show that no finite one-way quantum mechanism can implement this utility function for $x \in [0, 0.06]$ and $y = 1$. It it worth noting that, although only one qubit is exchanged in a single round per definition of our main model, the following negative result applies to any one-way quantum protocol with an arbitrarily large (but finite) message size.

▶ **Theorem 13.** *Given the two-item additive type space $[0,1]^2$, for any non-linear rational function $R(x)$, for any $r > 0$, there is no IC quantum one-way protocol $\mathcal{P}$ has utility function $u(x,1) = R(x)$ for $x \in [0,r)$.*

9 A Quantum One-Way Mechanism for An Uncountable Menu

In this section, we are going to construct an example of a prior over two additive, independent items, where the corresponding optimal auction can: (i) be implemented by a one-way protocol in 1 qubit and 2 classical bits; but (ii) requires an uncountably infinite menu.

▶ **Theorem** (Theorem 3 restated)**.** *For the problem of auctioning two items to a single buyer, there is a Bayesian prior over independent item values, such that there is a revenue-optimal one-way quantum auction protocol where the buyer sends 1 qubit and 2 classical bits; yet no finite classical auction protocol can achieve the optimal revenue.*

At a high level, we construct the example in the following steps:

1. First, we want to apply Theorem 12 to identify the utility function for optimal mechanisms. To simplify the verification of GK conditions, we choose $f_1(x) = 1$, for $x \in [0,1]$, aka the value for item 1 is drawn uniformly from $[0,1]$. By choosing $f_1(x) = 1$, the measure $\mu(x,y)$ defined in GK conditions can be simplified to $\mu(x,y) = 3f_2(y) + yf_2'(y)$.
2. Next, we choose a non-increasing, 1-Lipschitz, concave function s_1. In addition, we require s_1 to be a non-piecewise-linear function, so the utility function in the region $\mathcal{B}$ of the canonical partition $u(x,y) = x - s_1(y)$ is non-piecewise-linear, which implies no finite menu can characterize it. Moreover, as we discussed in the last section, to be able to be implemented by a one-way quantum protocol, $s_1(y)$ has to be a function in the form $\|Ay + B\|$ for some Hermitian matrices A and B. After some trial and error, it turns out that $s_1(y) = \frac{49}{24} - \frac{1}{4}(3y + \sqrt{121/4 - 10y + y^2})$ is a good idea.
3. With the chosen s_1, the next step is to reverse-engineer Theorem 12 to obtain a probability density function $f_2(y)$, function s_2 and critical price P_{crit} such that the canonical partition induced by $s_1, s_2, P_{\text{crit}}$ satisfies GK conditions. In particular, By the third bullet of Definition 11, $f_2(y)$ has to satisfy the following ODE:
$$(1 - s_1(y))\,(3f_2(y) + yf_2'(y)) = f_2(y).$$
4. Finally, we construct a one-way quantum protocol whose utility function is exactly the one given by Theorem 12.

By solving the ODE in bullet 2, we obtain

$$f_2(y) = \frac{c \cdot \left(-6g(y) + 12y + \sqrt{5737} + 5\right)^{-\frac{75}{58} - \frac{7551}{58\sqrt{5737}}} (g(y) - 2y + 10)^3 \left(6g(y) - 12y + \sqrt{5737} - 5\right)^{\frac{7551}{58\sqrt{5737}} - \frac{75}{58}}}{(11 - 2y + g(y))^{99/29}}, \qquad (2)$$

where $g(y) = \sqrt{4y^2 - 40y + 121}$, and c is the normalization factor such that

$$\int_0^1 f_2(y)\,\mathrm{d}y = 1.$$

9.1 Optimal Mechanisms

In this subsection, we will further define another non-increasing, 1-Lipschitz, concave function s_2 and critical price $P_{\text{crit}} \in [0,2]$. Next, we verify the canonical partition induced by s_1, s_2, and P_{crit} satisfy GK conditions and give the characterization of the optimal mechanism by applying Theorem 12.

First, one can verify that $\mu(x, y) = 3f_2(y) + yf_2'(y)$ is negative for all $(x, y) \in [0, 1]^2$.

Next, given $f_1(x) = 1$, by the last bullet of Definition 11, we set $s_2(x) \approx 0.558$ as a constant function such that $\int_{s_2(x)}^{1}(3f_2(y) + yf_2'(y))\mathrm{d}y = f_2(1)$.

Finally, we set $P_{\text{crit}} \approx 0.669$ such that $\int_Z(3f_2(y)+yf_2'(y)) = 1$. Moreover, line $x+y = P_{\text{crit}}$ intersects both curves $x = s_1(y)$ and $y = s_2(x)$. With s_1, s_2 and P_{crit} we now have $x_{\text{crit}} \approx 0.111$ and $y_{\text{crit}} \approx 0.005$. By definition, the canonical partition induced by s_1, s_2 and P_{crit} satisfies GK conditions. Therefore, by Theorem 12, we give the following characterization of the optimal mechanism for selling two items to a single additive buyer with values independently distributed according to $f_1 = 1$ and f_2 given by (2).

▶ **Lemma 14.** *The optimal mechanism for selling two items to a single additive buyer with values independently distributed according to $f_1 = 1$ and f_2 defined by (2) is given by the utility function*

$$u(x, y) = \max(0, x - s_2(y), y - s_1(x), x + y - P_{\text{crit}}).$$

Specifically, $u(x, y) = x - s_2(y)$ in region B is not a piecewise linear function, and it is the unique utility function for all optimal mechanisms in region B.

9.2 Exact One-Way Quantum Protocol

In this subsection, we give an IC one-way quantum protocol with exactly the same utility as the one characterized in Lemma 14.

Protocol implementation

In the first (and the only) round, the buyer send a single qubit with reduced density matrix ρ, and two classical bits b_1, b_2. If $b_1 = b_2 = 0$, then the seller terminates the protocol with empty allocation and payment 0. If $b_1 = b_2 = 1$, then the seller terminates the protocol with allocation $\{1, 2\}$ and payment $P_{\text{crit}} \approx 0.669$. If $b_1 = 0, b_2 = 1$, then the seller terminates the protocol with alloation $\{2\}$ and payment $s_2(0) \approx 0.558$. Finally, if $b_1 = 1, b_2 = 0$, the seller measures the qubit using the following POVM and terminates the protocol with allocation and payment associated with each measurement outcome.

$$A_1 = \begin{pmatrix} 2/5 & \sqrt{21}/16 \\ \sqrt{21}/16 & 1/4 \end{pmatrix}, \quad a_1 = \{1, 2\}, \quad p_1 = 2,$$
$$A_2 = \begin{pmatrix} 2/5 & -\sqrt{21}/16 \\ -\sqrt{21}/16 & 1/4 \end{pmatrix}, \quad a_2 = \{1, 2\}, \quad p_2 = 0,$$
$$A_3 = \begin{pmatrix} 1/5 & 0 \\ 0 & 0 \end{pmatrix}, \quad a_3 = \{1, 2\}, \quad p_3 = \frac{299}{24},$$
$$A_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1/2 \end{pmatrix}, \quad a_4 = \{1\}, \quad p_4 = \frac{7}{12}.$$

We define the buyer's suggested strategy as the optimal response to the seller's strategy, given his private value x and y.

10 (Barely) interactive one-way quantum auction protocols

In Section 8 we see an example of a prior whose optimal mechanism cannot be implemented by a finite one-way quantum auction protocol. In this section, we introduce a barely interactive multi-round quantum auction protocol which is optimal for this example, i.e. $f_1(x) = 2(1 - x), f_2(y) = 2(1 - y)$ for $(x, y) \in [0, 1]^2$.

▶ **Theorem 15** (Theorem 4). *For the problem of auctioning two items to a single buyer, there is a Bayesian prior over independent item values, such that there is a revenue-optimal quantum auction protocol where the seller sends 1 qubit to the buyer, who replies with 1 qubit and 2 classical bits; yet no finite classical or one-way quantum auction protocol can achieve the optimal revenue.*

Due to [24] Section 8.2.1, the (unique) optimal mechanism for this example can be characterized by the following lemma.

Protocol implementation

The seller's strategy is as follows.

In this protocol, the seller first prepares an EPR pair: $\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$ and sends one qubit of the EPR pair to the buyer.

The density matrix of an EPR pair is $\rho_{\text{EPR}} = \begin{pmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{pmatrix}$.

Next, the seller receives one qubit from the buyer (and two classical bits). We denote by b_1, b_2 the two classical bits. If $b_1 = b_2 = 0$, the protocol terminates with empty allocation and payment 0. If $b_1 = b_2 = 1$ the protocol terminates with allocation $\{1, 2\}$ and payment $P_{\text{crit}} \approx 0.5535$ defined in [24]. If $b_1 \neq b_2$, the seller measures the joint state (two qubits) of his half of the EPR pair and the qubit she receives from the buyer. The seller will use the following POVM and corresponding allocation and payments. For convenience, we define bundle $\pi = \{1\}$ if $b_1 = 1$, and $\pi = \{2\}$ if $b_2 = 1$.

$$A_1 = \begin{pmatrix} \frac{3}{20} & 0 & 0 & \frac{1}{10} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{2}{5} & 0 \\ \frac{1}{10} & 0 & 0 & \frac{2}{5} \end{pmatrix}, \quad a_1 = \pi, \quad p_1 = 3,$$

$$A_2 = \begin{pmatrix} \frac{23}{80} & 0 & 0 & -\frac{1}{10} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{3}{5} & 0 \\ -\frac{1}{10} & 0 & 0 & \frac{3}{5} \end{pmatrix}, \quad a_2 = \pi, \quad p_2 = 0,$$

$$A_3 = \begin{pmatrix} \frac{9}{16} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad a_3 = \{1, 2\}, \quad p_3 = 0.$$

We can verify by calculation that this is a valid POVM as all three matrices are positive semidefinite and $A_1 + A_2 + A_3 = I$.

We define the buyer's suggested strategy as the optimal response to the seller's strategy, given his private value x and y.

11 Limitations of finite-round quantum protocols

In this section we give an example where no finite IC and IR protocol obtains optimal revenue.

▶ **Theorem** (Theorem 5 restated). *For the problem of auctioning two items to a single buyer, there is a Bayesian prior over independent item values, such that there is a revenue-optimal classical auction protocol that requires a constant number of bits* in exepctation*; yet no finite quantum auction protocol can achieve the optimal revenue.*

Below are definitions of semialgebraic sets and semialgebraic functions. (See e.g. [23] for reference.)

▶ **Definition 16** (semialgebraic sets). *A subset of $\mathbb{R}^n$ is semialgebraic if it can be represented as a finite union of sets of the form:*

$$\{x \in \mathbb{R}^n : f(x) = 0, g_1(x) > 0, \ldots, g_m(x) > 0\},$$

where f and g_is are real polynomials in x.

▶ **Definition 17** (Semialgebraic functions). *A function $f : \mathbb{R}^n \to \mathbb{R}$ is semialgebraic if its graph $\{(x, y) \in \mathbb{R}^{n+1} : f(x) = y\}$ is a semialgebraic set.*

11.1 The utility function of finite round IC protocol is semialgebraic

▶ **Lemma 18.** *Given an IC an IR finite-round quantum auction protocol, its utility function $u(x)$ is semialgebraic.*

11.2 A mechanism with a non-semialgebraic utility function

[39] characterizes the optimal mechanism for selling two items to an additive buyer with i.i.d. priors $\frac{e^{-x}}{1-1/e}$ (i.e. $f_1(x) = \frac{e^{-x}}{1-1/e}$ and $f_2(y) = \frac{e^{-y}}{1-1/e}$). In particular, they show that the utility function of the optimal mechanism satisfies $u(x, 1) = 2x + W(e^{1-x}(2 - x)) - 1$ for $x \in [0, 0.1]$, where $W(\cdot)$ is the Lambert W function[14]. Furthermore, by Theorem 12, we also know this utility function is unique in this region ($y = 1, x \in [0, 0.1]$).

Next, we show that the unique utility function $g(x) = 2x + W(e^{1-x}(2 - x)) - 1$ is not a semialgebraic function. Together with Lemma 18, this implies that no finite quantum IC protocol achieves exactly optimal revenue (aka completing the proof of Theorem 5).

▶ **Lemma 19.** *Let $f : \mathbb{R} \to \mathbb{R}$ be a semialgebraic function. $f(x)$ cannot be equal to $g(x) = 2x + W(e^{1-x}(2 - x)) - 1$ on $[0, r)$ for any $r > 0$.*

References

1 Andris Ambainis, Leonard J Schulman, Amnon Ta-Shma, Umesh Vazirani, and Avi Wigderson. The quantum communication complexity of sampling. *SIAM Journal on Computing*, 32(6):1570–1585, 2003. doi:10.1137/S009753979935476.

2 Sepehr Assadi. Combinatorial auctions do need modest interaction. In *Proceedings of the 2017 ACM Conference on Economics and Computation, EC '17, Cambridge, MA, USA, June 26-30, 2017*, pages 145–162, 2017. doi:10.1145/3033274.3085121.

3 Sepehr Assadi, Hrishikesh Khandeparkar, Raghuvansh R Saxena, and S Matthew Weinberg. Separating the communication complexity of truthful and non-truthful combinatorial auctions. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on theory of computing*, pages 1073–1085, 2020. doi:10.1145/3357713.3384267.

4 Moshe Babaioff, Liad Blumrosen, and Michael Schapira. The communication burden of payment determination. *Games and Economic Behavior*, 77(1):153–167, 2013. doi:10.1016/j.geb.2012.08.007.

[14] Defined as the inverse function of $f(w) = w \cdot e^w$. Moreover, by the Lagrange inversion theorem, W is analytic everywhere on $(-1/e, \infty)$.

5 Moshe Babaioff, Yannai A. Gonczarowski, and Noam Nisan. The menu-size complexity of revenue approximation. *Games Econ. Behav.*, 134:281–307, 2022. doi:10.1016/j.geb.2021.03.001.

6 Moshe Babaioff, Nicole Immorlica, Brendan Lucier, and S. Matthew Weinberg. A simple and approximately optimal mechanism for an additive buyer. *J. ACM*, 67(4):24:1–24:40, 2020. URL: https://dl.acm.org/doi/10.1145/3398745, doi:10.1145/3398745.

7 Yakov Babichenko, Shahar Dobzinski, and Noam Nisan. The communication complexity of local search. In Moses Charikar and Edith Cohen, editors, *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, STOC 2019, Phoenix, AZ, USA, June 23-26, 2019*, pages 650–661. ACM, 2019. doi:10.1145/3313276.3316354.

8 Yakov Babichenko and Aviad Rubinstein. Communication complexity of nash equilibrium in potential games (extended abstract). In Sandy Irani, editor, *61st IEEE Annual Symposium on Foundations of Computer Science, FOCS 2020, Durham, NC, USA, November 16-19, 2020*, pages 1439–1445. IEEE, 2020. doi:10.1109/FOCS46700.2020.00137.

9 Yakov Babichenko and Aviad Rubinstein. Communication complexity of approximate nash equilibria. *Games Econ. Behav.*, 134:376–398, 2022. doi:10.1016/j.geb.2020.07.005.

10 Ziv Bar-Yossef, T. S. Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In *Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing*, STOC '04, pages 128–137, New York, NY, USA, 2004. Association for Computing Machinery. doi:10.1145/1007352.1007379.

11 Salman Beigi, Peter Shor, and John Watrous. Quantum interactive proofs with short messages. *Theory of Computing*, 7, April 2010. doi:10.4086/toc.2011.v007a007.

12 Liad Blumrosen, Noam Nisan, and Ilya Segal. Auctions with severely bounded communication. *J. Artif. Intell. Res.*, 28:233–266, 2007. doi:10.1613/jair.2081.

13 Simina Brânzei and Noam Nisan. Communication complexity of cake cutting. In *Proceedings of the 2019 ACM Conference on Economics and Computation, EC 2019, Phoenix, AZ, USA, June 24-28, 2019.*, page 525, 2019. doi:10.1145/3328526.3329644.

14 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 2016, Arlington, VA, USA, January 10-12, 2016*, pages 1444–1457, 2016. doi:10.1137/1.9781611974331.ch99.

15 Mark Braverman, Jieming Mao, and S. Matthew Weinberg. On simultaneous two-player combinatorial auctions. In *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2018, New Orleans, LA, USA, January 7-10, 2018*, pages 2256–2273, 2018. doi:10.1137/1.9781611975031.146.

16 Patrick Briest, Shuchi Chawla, Robert Kleinberg, and S. Matthew Weinberg. Pricing randomized allocations. In *Proceedings of the Twenty-First Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2010, Austin, Texas, USA, January 17-19, 2010*, pages 585–597, 2010. doi:10.1137/1.9781611973075.49.

17 Ioannis Caragiannis and Ariel D. Procaccia. Voting almost maximizes social welfare despite limited communication. *Artif. Intell.*, 175(9-10):1655–1671, 2011. doi:10.1016/j.artint.2011.03.005.

18 Xi Chen, Ilias Diakonikolas, Anthi Orfanou, Dimitris Paparas, Xiaorui Sun, and Mihalis Yannakakis. On the complexity of optimal lottery pricing and randomized mechanisms. In *IEEE 56th Annual Symposium on Foundations of Computer Science, FOCS 2015, Berkeley, CA, USA, 17-20 October, 2015*, pages 1464–1479, 2015. doi:10.1109/FOCS.2015.93.

19 John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical review letters*, 23(15):880, 1969.

20 Richard Cleve, Peter Hoyer, Benjamin Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, CCC '04, pages 236–249, USA, 2004. IEEE Computer Society. doi:10.1109/CCC.2004.1313847.

21 Vincent Conitzer and Tuomas Sandholm. Communication complexity as a lower bound for learning in games. In *Proceedings of the twenty-first international conference on Machine learning*, page 24. ACM, 2004.

22 Vincent Conitzer and Tuomas Sandholm. Communication complexity of common voting rules. In *Proceedings 6th ACM Conference on Electronic Commerce (EC-2005), Vancouver, BC, Canada, June 5-8, 2005*, pages 78–87, 2005. doi:10.1145/1064009.1064018.

23 Michel Coste. An introduction to semialgebraic geometry, 2000.

24 Constantinos Daskalakis, Alan Deckelbaum, and Christos Tzamos. Strong duality for a multiple-good monopolist. *Econometrica*, 85(3):735–767, 2017.

25 Alan Deckelbaum. Quantum correlated equilibria in classical complete information games. *arXiv preprint*, 2011. arXiv:1101.3380.

26 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. doi:10.1145/2897518.2897569.

27 Shahar Dobzinski. Computational efficiency requires simple taxation. In *FOCS*, 2016.

28 Shahar Dobzinski, Noam Nisan, and Sigal Oren. Economic efficiency requires interaction. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 233–242, 2014. doi:10.1145/2591796.2591815.

29 Shahar Dobzinski and Shiri Ron. The communication complexity of payment computation. In Samir Khuller and Virginia Vassilevska Williams, editors, *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*, pages 933–946. ACM, 2021. doi:10.1145/3406325.3451083.

30 Shahar Dobzinski, Shiri Ron, and Jan Vondrák. On the hardness of dominant strategy mechanism design. In Stefano Leonardi and Anupam Gupta, editors, *STOC '22: 54th Annual ACM SIGACT Symposium on Theory of Computing, Rome, Italy, June 20 - 24, 2022*, pages 690–703. ACM, 2022. doi:10.1145/3519935.3520013.

31 Shahar Dobzinski and Jan Vondrák. Communication complexity of combinatorial auctions with submodular valuations. In Sanjeev Khanna, editor, *Proceedings of the Twenty-Fourth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2013, New Orleans, Louisiana, USA, January 6-8, 2013*, pages 1205–1215. SIAM, 2013. doi:10.1137/1.9781611973105.87.

32 Jens Eisert, Martin Wilkens, and Maciej Lewenstein. Quantum games and quantum strategies. *Phys. Rev. Lett.*, 83:3077–3080, October 1999. doi:10.1103/PhysRevLett.83.3077.

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

34 Ronald Fadel and Ilya Segal. The communication cost of selfishness. *Journal of Economic Theory*, 144(5):1895–1920, 2009. doi:10.1016/J.JET.2007.09.015.

35 Anat Ganor and Karthik C. S. Communication complexity of correlated equilibrium with small support. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2018, August 20-22, 2018 - Princeton, NJ, USA*, pages 12:1–12:16, 2018. doi:10.4230/LIPIcs.APPROX-RANDOM.2018.12.

36 Anat Ganor, Karthik C. S., and Dömötör Pálvölgyi. On communication complexity of fixed point computation. *ACM Trans. Economics and Comput.*, 9(4):25:1–25:27, 2021. doi:10.1145/3485004.

37 Dmitry Gavinsky. Classical interaction cannot replace a quantum message. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, pages 95–102, New York, NY, USA, 2008. Association for Computing Machinery. doi:10.1145/1374376.1374393.

38 Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. Exponential separation for one-way quantum communication complexity, with applications to cryptography. *SIAM Journal on Computing*, 38(5):1695–1708, 2009. doi:10.1137/070706550.

39 Yiannis Giannakopoulos and Elias Koutsoupias. Selling two goods optimally. *Information and Computation*, 261:432–445, 2018. doi:10.1016/J.IC.2018.02.016.

40 Yannai A. Gonczarowski. Bounding the menu-size of approximately optimal auctions via optimal-transport duality. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 123–131, 2018. doi:10.1145/3188745.3188786.

41 Yannai A. Gonczarowski, Noam Nisan, Rafail Ostrovsky, and Will Rosenbaum. A stable marriage requires communication. *Games Econ. Behav.*, 118:626–647, 2019. doi:10.1016/j.geb.2018.10.013.

42 Yannai A. Gonczarowski and S. Matthew Weinberg. The sample complexity of up-to-ε multidimensional revenue maximization. In *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS*, 2018. doi:10.1109/FOCS.2018.00047.

43 Mika Göös and Aviad Rubinstein. Near-optimal communication lower bounds for approximate nash equilibria. In *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*, pages 397–403, 2018. doi:10.1109/FOCS.2018.00045.

44 Chenghao Guo, Zhiyi Huang, and Xinzhi Zhang. Settling the sample complexity of single-parameter revenue maximization. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, STOC 2019, Phoenix, AZ, USA, June 23-26, 2019.*, pages 662–673, 2019. doi:10.1145/3313276.3316325.

45 Gus Gutoski and John Watrous. Toward a general theory of quantum games. In David S. Johnson and Uriel Feige, editors, *Proceedings of the 39th Annual ACM Symposium on Theory of Computing, San Diego, California, USA, June 11-13, 2007*, pages 565–574. ACM, 2007. doi:10.1145/1250790.1250873.

46 Sergiu Hart and Yishay Mansour. How long to equilibrium? the communication complexity of uncoupled equilibrium procedures. *Games and Economic Behavior*, 69(1):107–126, 2010. doi:10.1016/J.GEB.2007.12.002.

47 Sergiu Hart and Noam Nisan. Selling multiple correlated goods: Revenue maximization and menu-size complexity. *J. Econ. Theory*, 183:991–1029, 2019. doi:10.1016/j.jet.2019.07.006.

48 Sergiu Hart and Philip J. Reny. Maximizing Revenue with Multiple Goods: Nonmonotonicity and Other Observations. *Theoretical Economics*, 10(3):893–922, 2015.

49 Alexander S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3), 1973.

50 Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. Qip = pspace. *Communications of the ACM*, 53(12):102–109, 2010. doi:10.1145/1859204.1859231.

51 Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. Mip* = re. *Commun. ACM*, 64(11):131–138, October 2021. doi:10.1145/3485628.

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

53 Hagay Levin, Michael Schapira, and Aviv Zohar. Interdomain routing and games. *SIAM J. Comput.*, 40(6):1892–1912, 2011. doi:10.1137/080734017.

54 A. M. Manelli and D. R. Vincent. Multidimensional Mechanism Design: Revenue Maximization and the Multiple-Good Monopoly. *Journal of Economic Theory*, 137(1):153–185, 2007. doi:10.1016/J.JET.2006.12.007.

55 A. M. Manelli and D. R. Vincent. Bayesian and Dominant-Strrategy Implementation in the Independent Private-Values Model. *Econometrica*, 78(6):1905–1938, 2010.

56 David A Meyer. Quantum games and quantum algorithms. *arXiv preprint*, 2000. arXiv:quant-ph/0004092.

57 Ashley Montanaro. Quantum states cannot be transmitted efficiently classically. *Quantum*, 3:154, 2019.

58 Ashley Montanaro and Changpeng Shao. Quantum communication complexity of linear regression. *arXiv preprint arXiv:2210.01601*, 2022. doi:10.48550/arXiv.2210.01601.

59 Anand Natarajan and John Wright. Neexp is contained in mip. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 510–518. IEEE, 2019. doi:10.1109/FOCS.2019.00039.

60 Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*, volume 2. Cambridge university press Cambridge, 2001.

61 Noam Nisan and Ilya Segal. The communication requirements of efficient allocations and supporting prices. *J. Economic Theory*, 129(1):192–224, 2006. doi:10.1016/j.jet.2004.10.007.

62 Gregory Pavlov. Optimal mechanism for selling two goods. *The B.E. Journal of Theoretical Economics*, 11(3), 2011.

63 Benjamin Plaut and Tim Roughgarden. Communication complexity of discrete fair division. In *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2019, San Diego, California, USA, January 6-9, 2019*, pages 2014–2033, 2019. doi:10.1137/1.9781611975482.122.

64 Ariel D. Procaccia and Jeffrey S. Rosenschein. The communication complexity of coalition formation among autonomous agents. In *5th International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS 2006), Hakodate, Japan, May 8-12, 2006*, pages 505–512, 2006. doi:10.1145/1160633.1160727.

65 Ran Raz. Exponential separation of quantum and classical communication complexity. In *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing*, STOC '99, pages 358–367, New York, NY, USA, 1999. Association for Computing Machinery. doi:10.1145/301250.301343.

66 Oded Regev and Bo'az Klartag. Quantum one-way communication can be exponentially stronger than classical communication. In *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing*, STOC '11, pages 31–40, New York, NY, USA, 2011. Association for Computing Machinery. doi:10.1145/1993636.1993642.

67 Jean-Charles Rochet and Philippe Chone. Ironing, sweeping, and multidimensional screening. *Econometrica*, 66(4):783–826, 1998.

68 Tim Roughgarden and Omri Weinstein. On the communication complexity of approximate fixed points. In *Electronic Colloquium on Computational Complexity (ECCC)*, volume 23, page 55, 2016.

69 Aviad Rubinstein, Raghuvansh R. Saxena, Clayton Thomas, S. Matthew Weinberg, and Junyao Zhao. Exponential communication separations between notions of selfishness. In Samir Khuller and Virginia Vassilevska Williams, editors, *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*, pages 947–960. ACM, 2021. doi:10.1145/3406325.3451127.

70 Aviad Rubinstein and Junyao Zhao. The randomized communication complexity of optimal randomized auctions. In *Symposium on Theory of Computing, STOC 2021*. ACM, 2021.

71 Travis C. Service and Julie A. Adams. Communication complexity of approximating voting rules. In *International Conference on Autonomous Agents and Multiagent Systems, AAMAS 2012, Valencia, Spain, June 4-8, 2012 (3 Volumes)*, pages 593–602, 2012. URL: http://dl.acm.org/citation.cfm?id=2343781.

72 Hao Tang, Boning Li, Guoqing Wang, Haowei Xu, Changhao Li, Ariel Barr, Paola Cappellaro, and Ju Li. Communication-efficient quantum algorithm for distributed machine learning. *arXiv preprint*, 2022. arXiv:2209.04888.

73 John Thanassoulis. Haggling over substitutes. *Journal of Economic Theory*, 117:217–245, 2004. doi:10.1016/J.JET.2003.09.002.

74 John Watrous. Pspace has constant-round quantum interactive proof systems. *Theoretical Computer Science*, 292(3):575–588, 2003. doi:10.1016/S0304-3975(01)00375-9.

75 Zhaohui Wei and Shengyu Zhang. Full characterization of quantum correlated equilibria. *Quantum Inf. Comput.*, 13(9-10):846–860, 2013. doi:10.26421/QIC13.9-10-7.

76 S. Matthew Weinberg and Zixin Zhou. Optimal multi-dimensional mechanisms are not locally-implementable. In *Proceedings of the 23rd ACM Conference on Economics and Computation*, EC '22, pages 875–896, New York, NY, USA, 2022. Association for Computing Machinery. doi:10.1145/3490486.3538334.

77 A Chi-Chih Yao. Quantum circuit complexity. In *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*, pages 352–361. IEEE, 1993. doi:10.1109/SFCS.1993.366852.