Thesis Propsal
Market Algorithms: Incentives, Learning and Privacy

Jamie Morgenstern

April 28, 2014

Abstract

This thesis is a collection of work in the broad area of *mechanism design.* A centralized planner, or an algorithm, aims to solve an algorithmic problem, maximizing some objective function. In the classical algorithms literature, it is assumed that the planner has exact, perfect access to all of the input to this optimization problem, and that the interesting questions lie in whether or not the problem is computationally tractable: can one compute the optimal solution in polynomial time? If this is not possible, what is the best approximation which can be achieved in polynomial time? Mechanism design, on the other hand, does not assume all input data for the optimization problem is directly accessible to the central planner. On the contrary, it is assumed that the input is held by a collection of agents acting in their own best interest, and that the central planner has to extract the relevant input from these agents. The agents may have preferences over the output of the mechanism, or simply value their data as *private*: in either case, the planner's optimization task becomes more difficult. She needs to ensure that it is in the best interest of the agents to provide her accurate information.

In the case of self-interested agents, the planner needs to ensure that if an agent misreports her data, she does not get a more preferred outcome from the planner: the planner should design *truthful* mechanisms. Alternatively, she might aim to design mechanisms which are not truthful but have good objective value when players act strategically. In this domain, we discuss work aimed at selling heterogeneous goods to combinatorial bidders [8] and constructing mechanisms for peer review of grant proposals [18].

In the case of privacy-aware agents, the planner's outcome should not depend too heavily on any one agent's data, or the agents may not choose to share their data. In this context, we discuss work in providing private information to help players coordinate in online decision-making contexts [3]. Finally, we discuss ongoing work in which we design a privacy-preserving mechanism which computes an approximately school-optimal stable matching: by virtue of the mechanism being private in the student's data, it provides the first known nontrivial truthfulness guarantees for the student side of the matching market.

1 Introduction

Classical theoretical computer science has focused on coordinated optimization, where a particular problem has a well-defined set of optimal solutions, and the goal of the researcher is to design efficient algorithms to construct (near) optimal-solutions. This setting is well-motivated by settings where a single, central coordinator has full information about the problem parameters, e.g. when an individual wishes to sort his files in order of most to least recently used, or when a single person wishes to compute the most efficient allocation of his jobs to a set of jobs he alone can access. However, many decentralized settings arise where such assumptions may not hold, and a new issues arises: how can an algorithm designer incentivise people to give up their data? The algorithms designed in such a setting need to be aware of the *incentives* and also *privacy* concerns of the individuals from which they solicit information.

We begin by motivating the study of *incentive-aware* algorithms. If a system administrator is scheduling jobs for various other parties, some parties may misreport the size or importance of their job so as to expedite the completion of their job over others. In a very different context, bidders in an auction may misreport their values for certain items, in hopes of paying less for those items. It has been observed that airlines intentionally submit erroneous flight plans to manipulate airspace, only to alter those plans last-minute. These and many other examples motivate the study of *strategyproof* mechanisms, or, at the least, the study of systems when the individuals participating are self-interested. The past decade has seen an increased focus on such decentralized settings, where self-interested agents are attempting to optimize some objective (e.g., their own wait-time) while a central authority is attempting to optimize another objective (for example, social welfare), where the authority must solicit information from the agents about their objective functions. The area of *algorithmic game theory* works in the area of this tension.

Even if players are not trying to optimize their own objective explicitly via misreporting their data to an algorithm, there may be concerns that the algorithm will leak too much of their personal information, leading to concerns about a player's privacy. If a collection of scientists wishes to do a statistical study of the correlation between exercise and heart disease, an individual may worry about his health insurance premiums rising if the scientist gives that data to the person's insurance company. In another context, a collection of competing firms may have profits which depend on the other firm's marketing strategies; it would be helpful for all firms to have some idea about the aggregate marketing strategy of other firms, but no individual firm wishes for her marketing strategy to be freely available for other firms to peruse. We study algorithms which guarantee *differential privacy* of the individual participant's data: the outcome of the algorithm shouldn't reveal too much about any individual.

This thesis proposal is organized as follows. In Sections 2.1, 2.3 and 2.4, we provide the formal notation and definitions necessary for the rest of the proposal. Section 3 describes our results on a new, sequential auction for combinatorial bidders. Section 4 describes our new mechanism for impartial peer review. Section 5 contains an overview of our private coordination mechanism and the results it gives for online matching problems. In Section 6, we describe a private version of the deferred acceptance algorithm, and show that the school-optimal version of this mechanism is approximately truthful for the student side of the market. Finally, Section 7 states several open problems and Section 8 details a timeline for completion of this thesis.

2 Definitions and Preliminaries

Throughout this work, the following shorthand will be used

- $i, j \in [n]$ will refer to agents, or players, of a game with n players
- Each player i has an allowable action space $\mathcal{A}_i$
- Each player has utility $u_i(a_1, \ldots, a_n)$ which depends on the action of each other player.
- The pair $(A_i, u_i) = \tau_i$ is the *type* of player i

A mechanism $\mathcal{M}$[1] defines a (multi-stage) game in the following way. $\mathcal{M}$ takes as input some information about the players: i may reveal her type τ_i; some function $s_{i,1}$ of her type (for example, in the case of an auction, she may submit a bid for a given item, or submit her most preferred public project); or some function of her type and other players' actions to this stage of the mechanism. This input to $\mathcal{M}$ is the first action $a_{i,1}$ made by the player. As a result of $(a_{1,1}, \ldots, a_{n,1})$, $\mathcal{M}$ will either output some result (for example, $\mathcal{M}$ may output an allocations and payments) or solicit more information ($\mathcal{M}$ may request bids on a second item, or ask players to pick items subject to prices), or do some combination thereof ($\mathcal{M}$ may output who won the first item and charge them some payment and then ask for bids on a second item).

For ease of notation, let $a_{\cdot,i} = (a_{1,i}, \ldots, a_{t,i})$ (the actions of player i from time 1 to t) and $a_{t,\cdot} = (a_{1,t}, \ldots, a_{n,t})$ (the actions of all players at time t), and $a$denote the joint actions for each player, for each time. We define player i's *strategy* at time t, $d_{t,i}$, as a map from the partial outcome prior to round t to an action at time t : $d_{t,i}(\mathcal{M}(a_{1,\cdot}, \ldots, a_{t-1,\cdot})) = a_{t,i}$. Each player has some utility for the final output of the mechanism:

$$u_i(a) = u'_i(\mathcal{M}(a)).$$

[1] In general, $\mathcal{M} = (\mathcal{M}_0, \ldots, \mathcal{M}_T)$ is a T-stage mechanism, but for ease of notation, we will refer to each of these when the stage of computation is clear.

In general, both the strategies and $\mathcal{M}$ might be randomized. In that case, the actions a and the output of $\mathcal{M}$ are random variables, and rather than utility u_i we discuss expected utility:

$$\mathbb{E}_{\mathcal{M},a_{\cdot,1},\ldots,a_{\cdot,n}}[u_i(a_{\cdot,1},\ldots,a_{\cdot,n})] = \mathbb{E}_{\mathcal{M},a_{\cdot,1},\ldots,a_{\cdot,n}}[u'_i(\mathcal{M}(a_{\cdot,1},\ldots,a_{\cdot,n}))]$$

2.1 Truthfulness, Dominant and Undominated Strategies

In some settings (in particular, in Section 4), we will focus on mechanisms for which *truthful* reporting is always a weakly dominant strategy, or so-called *truthful* mechanisms. Depending on the information requested by $\mathcal{M}$, this may mean slightly different things. Suppose that each round t of a mechanism $\mathcal{M}$ asks a question $q_{t,i}$ of a player i. Then, the following definition is sufficiently general

Definition 2.1 (Truthful Mechanisms). *Consider a mechanism $\mathcal{M}$ which asks questions $q_{t,i}$ of player i in round t. Let $\bar{a}_{t,i} = q_{t,i}(u_i, A_i)$ be the* truthful answer of $q_{t,i}$. *Then, $\mathcal{M}$ is said to be* truthful *if, for all players i, all actions $a_{\cdot,i}, a_{\cdot,-i}$, and for all questions $q_{t,i}$ asked by the mechanism,*

$$u_i(a_{\cdot,-i}, \bar{a}_{\cdot,i}) = u'_i(\mathcal{M}(a_{\cdot,-i}, \bar{a}_{\cdot,i})) \geq u'_i(\mathcal{M}(a_{\cdot,-i}a_{\cdot,i})) = u_i(a_{\cdot,-i}a_{\cdot,i}).$$

Informally, if $\mathcal{M}$ is truthful, each player i would maximize their own utility answering $\mathcal{M}$'s questions honestly. In general, these answers depend on the type of a player i.

We also consider a slightly weaker definition of truthfulness, where a player has little (but perhaps nonzero) incentive to misreport.

Definition 2.2 (ζ-Approximate Truthfulness). *$\mathcal{M}$ is ζ-approximately truthful if for all players i, all actions $a_{\cdot,i}, a_{\cdot,-i}$, and for all questions $q_{t,i}$ asked by the mechanism,*

$$u_i(a_{\cdot,-i}, \bar{a}_{\cdot,i}) = u'_i(\mathcal{M}(a_{\cdot,-i}, \bar{a}_{\cdot,i})) \geq u'_i(\mathcal{M}(a_{\cdot,-i}a_{\cdot,i})) - \zeta = u_i(a_{\cdot,-i}a_{\cdot,i}) - \zeta$$

Definition 2.3 (Dominant and Undominated Strategies in Multi-Stage settings). *Suppose there are two strategies $d_{\cdot,i}, d'_{\cdot,i}$. For $j \neq i$, let $a_{t,j} = d_{t,j}(\mathcal{M}(a_{t-1,\cdot}))$, $a'_{t,j} = d_{t,j}(\mathcal{M}(a'_{t-1,\cdot}))$ be the actions taken by j denoted by their strategies and the partial output of the mechanism until time t, in the case where i plays $d_{t,i}$ or $d'_{t,i}$, respectively. Furthermore, let $a_{t,i} = d_{t,i}(\mathcal{M}(a_{t-1,\cdot}))$ and $a'_{t,i} = d'_{t,i}(\mathcal{M}(a'_{t-1,\cdot}))$ denote the actions i will take following $d_{\cdot,i}, d'_{\cdot,i}$, respectively.*

A strategy $d_{\cdot,i}$ is said to strictly **dominate** *$d'_{\cdot,i}$ if, for all $j \neq i$ and $d_{\cdot,j}$:*

$$u_i(a_{\cdot,-i}, a_{\cdot,i}) \geq u_i(a'_{\cdot,-i}, a'_{\cdot,i})$$

and for at least one $a_{\cdot,-i}$:

$$u_i(a_{\cdot,-i}, a_{\cdot,i}) > u_i(a'_{\cdot,-i}, a'_{\cdot,i}).$$

If there is no strategy $d_{\cdot,i}$ which strictly dominates $d'_{\cdot,i}$, $d'_{\cdot,i}$ is said to be an **undominated** *strategy. If $d_{\cdot,i}$ dominates all $d'_{\cdot,i}$, then $d_{\cdot,i}$ is called a* **dominant** *strategy.*

As usual, dominant strategies do not always exist, but undominated strategies always do (when the strategy space is closed and bounded).[2] It is worth emphasizing a subtle point about this definition: the only actions $a_{\cdot,-i}$ for which the d dominating d' is well-defined are those which are *consistent with the mechanism's partial outputs.* In particular, in Section 5, when the partial outputs are signals describing the actions of other players, a strategy d dominates d' if, for all a_{-i}'s *consistent with those signals*, the utility for d is higher than for d' (d need give higher utility than d' only on states consistent with the signals). In the case where $\mathcal{M}$ is randomized, consistence of a_{-i} with a signal just means that $\mathcal{M}(a_{-i})$ could produce the signal with nonzero probability. This definition is a weakening of the normal definition of one strategy dominating another in the one-shot game, where the inequality would need to hold for all $a_{-i} \in \mathcal{A}_{-i}$.

[2] To see this, consider a strategy. If it is undominated, then you have an example of an undominated strategy. If not, consider a strategy which dominates it *by the largest amount in terms of the strict inequality*; if that strategy is undominated, that is an example of an undominated strategy, otherwise consider the strategy which dominates it, and so on. Since two strategies cannot strictly dominate each other, the limit of this process will lead to an undominated strategy (if the strategy space is closed and bounded, the utility of a player must be bounded).

2.2 Equilibrium Concepts

In a **Bayesian setting**, each $\tau_i = (u_i, A_i)$ is drawn independently from a distribution $\mathcal{T}_i$ on a set of possible types T_i, all $\mathcal{T}_i$s are public knowledge and τ_is are private information. In each round t, $\mathcal{M}$ reveals some information, denoted as $\mathcal{M}(a_{t-1,\cdot})$. The **complete information** setting is a special case where each player knows the type of all the other players.[3]

Observe that a strategy actually also contains information about *what might have happened*, i.e., they specify the result of possible deviations from the actual outcome, which becomes important in the definitions of equilibria. We now define the most basic equilibrium concept, that of a Nash equilibrium.

Definition 2.4. *A* **pure (resp. mixed) Bayes-Nash** *equilibrium is a pure (resp. mixed) strategy tuple d such that no player can unilaterally deviate to obtain a better utility. In other words, for $j \neq i$, let $a_{t,j} = d_{t,j}(\mathcal{M}(a_{t-1,\cdot}))$, $a'_{t,j} = d_{t,j}(\mathcal{M}(a'_{t-1,\cdot}))$ be the actions taken by j denoted by their strategies and the partial output of the mechanism until time t, in the case where i plays $d_{t,i}$ or $d'_{t,i}$, respectively. Furthermore, let $a_{t,i} = d_{t,i}(\mathcal{M}(a_{t-1,\cdot}))$ and $a'_{t,i} = d'_{t,i}(\mathcal{M}(a'_{t-1,\cdot}))$ denote the actions i will take following $d_{\cdot,i}, d'_{\cdot,i}$, respectively.*

$$\forall i \in [n], \forall u_i \in U_i, \forall d'_i \in D_i, \mathbb{E}_{\tau_{-i}}[u_i(a_{\cdot,i}, a_{\cdot,-i})] \geq \mathbb{E}_{\tau_{-i}}[u_i(a'_{\cdot,i}, a'_{\cdot,-i})]$$

A Nash equilibrium in sequential games allows for *irrational threats*, where an equilibrium strategy of a bidder could be suboptimal beyond a certain round. A standard refinement of the Nash equilibrium for extensive form games is the *subgame perfect equilibrium*, that allows only for strategies that constitute an equilibrium of any subgame, conditional on any possible history of play (see [11] for a formal definition and a more comprehensive treatment.) Our results also extend to complete-information correlated equilibria.

Definition 2.5. Correlated equilibrium *A correlated equilibrium is a distribution X over joint strategy profiles such that, for each player i, following the suggestion s_i drawn from the distribution X is a best-response, in expectation over the suggestions s_{-i}, not known to i and assuming everyone else plays according to their suggestion:*

$$\mathbb{E}_{\mathbf{s}_{-i},\mathbf{v}}[u_i(\mathbf{s}(\mathbf{v})) \mid s_i] \geq \mathbb{E}_{s_{-i},\mathbf{v}}[u_i\left(s'_i(v_i), \mathbf{s}_{-i}(\mathbf{v}_{-i})\right) \mid s_i]$$

Note that the deviation is allowed to depend on the suggestion (in the event that s'_i is required to be independent of s_i for all i, we call s a coarse correlated equilibrium).

$$\text{Subgame perfect } \subseteq \text{ Nash } \subseteq \text{Correlated Equilibria}$$

2.3 Price of Anarchy

The price of anarchy may be defined w.r.t any of the equilibrium concepts in the previous section; the larger (by inclusion) classes have higher price of anarchy. In the Bayesian setting the price of anarchy is defined as the worst-case ratio of the expectations, over the random values, of the social welfare at the optimum $\mathbb{E}_{\vec{\tau}}[SW(\textsc{Opt}(\vec{\tau}))]$ and at an equilibrium $\mathbb{E}_{\vec{\tau}}[SW(d(\vec{\tau}))]$. The Price of Anarchy provides a quantitative scale with which we can measure the inherent inefficiency of a game[4]; the larger the Price of anarchy, the more social welfare is inherently lost by strategic agents playing the game when compared to some central authority forcing players to cooperate for the common good.

To be precise, for a given tuple of types $\vec{\tau}$, let $SW(\textsc{Opt}(\vec{\tau}))$ be the optimal social welfare, which is the highest social welfare obtainable over all possible choices of actions by players of types $\tau_1, \ldots, \tau_n$, that is:

$$SW(\textsc{Opt}(\vec{\tau})) := \max_{a \in A_1 \times \ldots \times A_n} \sum_{i=1}^{n} u_i(a).$$

Then, the price of anarchy of a set of equilibria T is defined as

$$PoA(T) := \max_{s \in T} \frac{SW(\textsc{Opt}(\vec{\tau}))}{SW(s)}.$$

The price of anarchy defined above is for a given instance; it can be generalized to a *Bayesian* setting, which formalizes the notion that players have probabilistic beliefs about each others types:[5] each type τ_i

[3] It is the case where $\mathcal{T}_i$ is τ_i with probability 1.

[4] Analogous to an approximation factor for approximation algorithms or a competitive ratio for online algorithms.

[5] What we call the *Bayesian* setting here is also called the *incomplete information* setting.

is drawn independently from a probability distribution $\mathcal{T}_i$ for all $i \in [n]$. The $\mathcal{T}_i$s are public knowledge, but v_i is bidder i's private information. $\mathcal{T}_i$ represents the belief about player i's utility and available actions based on publicly available information. The price of anarchy is then defined as a ratio of expectations, expectation of $SW(\textsc{Opt})$ and expectation of $SW(s)$. The expectations are taken over the draws of τ_i from $\mathcal{T}_i$ for each i. The *complete information* setting where all players know all of one another's utility functions is a special case of the Bayesian setting.

2.4 Differential Privacy

In this section, we outline the basic definitions relating to differential privacy.

Definition 2.6. *An offline mechanism $\mathcal{M}$ is (ϵ, δ)-differentially private if, for all a_{-i}, a_i, a'_i, and for any event S:*

$$\mathbb{P}[\mathcal{M}(a_{-i}, a_i) \in S] \leq e^{\epsilon}\mathbb{P}[\mathcal{M}(a_{-i}, a'_i) \in S] + \delta$$

Definition 2.6 makes sense in settings where the mechanism solicits information all at once, from all players, without the players being provided information by the mechanism, and without further interaction with the mechanism. If, on the other hand, the mechanism is collecting player's data in an online, streaming fashion, and outputting signals over time, a slight generalization of this definition is appropriate, called *d*ifferential privacy under continual observation [5, 9].

Definition 2.7. *A mechanism $\mathcal{M}$, which operates over streams of input $X \in B^n$, is (ϵ, δ)-differentially private under continual observation if, for two streams X, X' which differ in at most one coordinate, for all events S*

$$\mathbb{P}[\mathcal{M}(X') \in S] \leq e^{\epsilon}\mathbb{P}[\mathcal{M}(X) \in S] + \delta$$

In several settings, we will be particularly interested in privacy-preserving mechanisms whose outputs will be used by future players to determine future inputs (in this case, actions). For this, we define a more specialized form of differential privacy under adaptive continual observation.

Definition 2.8. *An announcement mechanism $\mathcal{M}$ is (ϵ, δ)-differentially private under adaptive*[6] *continual observation in the strategies of the players if, for each player i, each pair of strategies d, d'_i, and every subset S of events in the output announcement space H^n:*

$$\mathbb{P}[(m_1, \ldots, m_n) \in S] \leq e^{\epsilon}\mathbb{P}[(m_1, \ldots, m_i, m'_{i+1} \ldots, m'_n) \in S] + \delta$$

where $m_j \sim \mathcal{M}_j(a_1, \ldots, a_{j-1})$ and $m'_j \sim \mathcal{M}_j(a_1, \ldots, a_{i-1}, a'_i, a'_{i+1}, \ldots, a'_{j-1})$. Here $a_j = d_j(m_1, \ldots, m_j)$, and $a'_i = d'_i(m_1, \ldots, m_i)$, and for all $j > i$, $a'_j = d_j(m_1, \ldots, m_{i-1}, m_i, m'_{i+1}, \ldots, m'_j)$.

2.4.1 Relationship between privacy and truthfulness

There has been a long line of work exploring the formal connections between truthfulness and privacy [19, 32, 15, 12, 26, 23, 22, 6]. In particular, McSherry and Talwar [19] were the first to point out the following connection between privacy and truthfulness, which will be the most relevant for the purpose of this proposal: any mechanism which is differentially private automatically satisfies approximate truthfulness.

Theorem 2.9. *[([19])] Suppose $\mathcal{M}$ is (ϵ, δ)-differentially private. Then, a given player can affect the outcome of the mechanism with probability at most $e^{\epsilon} + \delta$. Thus, if players have utilities which are bounded $\in [0, 1]$, then $\mathcal{M}$ is also $e^{\epsilon} + \delta$-approximately truthful.*

2.5 Valuation Classes

In this section, we describe several important restrictions of valuation classes that we will use in Section 3. An *auction* mechanism outputs an allocation $X_1, \ldots, X_n$ of goods and a payment for each player $P_1, \ldots, P_n$. Bidders in the auction are generally assumed to have utilities which are *quasilinear* in their valuation function, e.g. $u_i(X_i, P_i) = v_i(X_i) - P_i$. We will be considering the following restricted forms of valuation functions v.

Perhaps the simplest combinatorial structure a valuation function might have is to be additive.

[6] Adaptivity is needed in this case because the announcements are arguments to the actions of players: when a particular action changes, this modifies the distribution over the future announcements, which in turn changes the distribution over future selected actions.

Definition 2.10. *A monotone valuation function is* **additive** *if it can be written as a sum of values for individual items:*

$$\forall\ S,\ v(S) = \sum_{i \in S} v(i)$$

This sort of valuation implies that there is some value each item has to a bidder, and their value for a bundle is just the sum of those individual values per item in the bundle.

Another simple class of valuation functions are unit-demand valuations.

Definition 2.11. *A monotone valuation function is* **unit-demand** *if it can be written as a maximum of values for individual items:*

$$\forall\ S,\ v(S) = \max_{i \in S} v(i)$$

Unit-demand valuations also have per-item values, but rather than adding them together to determine the value of a bundle, one takes the maximum. This may be a reasonable class of valuations in the case of people purchasing housing or refrigerators for personal use.

Both unit-demand and additive valuations are subsets of a more general class of valuations, that of gross-substitutes.

Definition 2.12. *Valuations with the* **gross substitutes** *property are defined in terms of the corresponding* demand *function. Given prices p_j for all $j \in [m]$, the demand correspondence is*

$$x(p_j)_{j \in [m]} := \arg \max_{S \subseteq [m]} \{v(S) - \sum_{j \in S} p_j\}.$$

A demand function satisfies gross-substitutes if increasing the price of one item does not decrease the demand for any other item. If the demand function is a correspondence, then it satisfies the gross-substitute condition when the following holds: if an item j is in some demand set under price $p = (p_1, \ldots, p_m)$, then after increasing the price of item j and keeping the rest of the prices the same, there exists a demand set under the new prices that contains j.

A yet more general class of valuations is the class of submodular valuation functions, which captures the concept of decreasing marginal return in settings with discrete, heterogeneous goods.

Definition 2.13. *A monotone valuation function is* **submodular** *if it exhibits the diminishing marginal value property, which to be precise is that*

$$\forall\ S \subseteq T, \forall\ i \notin T, v(S \cup \{i\}) - v(S) \geq v(T \cup \{i\}) - v(T).$$

In the case of identical items, submodularity reduces to a simpler form, concavity of the valuation function in the number of items given.

Definition 2.14. *A monotone valuation function is* **concave** *in the number of items if, for some monotonic, concave function $f : \mathbb{N} \to \mathbb{R}_+$,*

$$\forall\ S v(S) = f(|S|).$$

Finally, we define the yet more general class of valuation profiles XOS.

Definition 2.15. *A valuation function f is XOS if f can be represented as the maximum of some k additive functions:*

$$f(S) = \max \left(\sum_{j \in S} v_{1j}, \ldots, \sum_{j \in S} v_{kj} \right)$$

We note the following well-known hierarchy of valuation classes:

$$\text{unit-demand} \ \cup \ \text{additive} \ \subseteq \ \text{gross substitutes} \ \subseteq \ \text{submodular} \ \subseteq \text{XOS} \subseteq \ \text{subadditive}.$$

3 Draft Auctions

Consider the scenario where several indivisible items are to be auctioned off to bidders with *combinatorial* valuations, i.e., valuations that depend on the entire set of items obtained. In practice, simple auctions such as *sequential item auctions* are commonly used for such purposes. As a motivating example, the *Indian Premiere League*[7] conducts an "IPL player auction" annually, an auction where the teams in the league recruit players [30, 33, 7]. The format is a sequential auction: the players are considered one after the other in some order. When a player is up for auction the teams participate in an ascending price auction and the highest bidding team "wins" the player. The winning bid is the salary of the player for a given period.[8] The process is repeated with the next player.

It is known that sequential item auctions could lead to a highly inefficient allocation of items, as measured by the *price of anarchy*, even for very simple combinatorial valuations. We introduce a natural and simple alternative called a *draft auction* which has a much (exponentially) better price of anarchy for the very general class of subadditive valuation functions. We discuss why this makes a strong case for the following message of the paper: *if you are running a sequential item auction, then replace it with a draft auction.*

We now define the model formally: an instance of a *combinatorial auction* consists of m *items* that are to be auctioned off, n *bidders* wishing to obtain these items, and a *valuation* function $v_i : 2^{[m]} \to \mathbb{R}_+$ for each bidder i. (We identify the set of items and the set of bidders with $[m]$ and $[n]$ respectively.) We assume that the v_is are monotone and non-decreasing. The *result* of an auction is an allocation of items to bidders and payments of bidders: bidder i gets a set $S_i \subseteq [m]$ of items, and makes a payment P_i, with the S_is forming a partition of $[m]$. Bidders are selfish and try to maximize their utility from the auction, which is assumed to be *quasi-linear*, i.e., $u_i(S_i, P_i) = v_i(S_i) - P_i$. The valuation $v_i(S)$ can then be interpreted as how much the set of items S is worth to i, in terms of the *numeraire* in which the payments are made. Suppose that the objective of the auction designer is to maximize the *social welfare* of the resulting allocation, which is defined as $SW := \sum_{i\in[n]} v_i(S_i)$.

An example of such an auction that is commonly seen in practice is what is called a *sequential item auction*: items are auctioned off one after the other (in some arbitrary order), using a simple auction such as an ascending price auction or a sealed bid first or second price auction. To be precise, consider a sequential, sealed-bid first price auction which is formally defined as follows. There are m rounds, and in each round $j \in [m]$ each bidder $i \in [n]$ submits a bid b_{ij}. Item j is sold to the highest bidder $i^* = \arg\max_{i\in[n]}\{b_{ij}\}$, at the price equal to her bid, b_{i^*j}, breaking ties arbitrarily. The winner's identity i^* and the winning bid b_{i^*j} are publicly revealed before proceeding to the next round.

Notice that the allocation of items in this auction is a function of the bids, and each bidder strategizes to maximize her own utility. The bid of a bidder in any round could be a function of her own valuation, the information the bidder has about other bidders' valuations, and the observed history until that time, which includes the winners and their bids in all previous rounds. In general there is no single utility-maximizing strategy for a bidder since her utility also depends on other bidders' strategies, thus setting up a *game* among the bidders.

Rational players are assumed to play *equilibrium* strategies, where each bidder's strategy is a "best response" to the strategies of all the other bidders. There are many equilibrium definitions in the same spirit as above but differing in technical details; see Section 2.2 for precise definitions.

Bounding the inefficiency at equilibrium via the price of anarchy Equilibria of certain auctions lead to allocations that are not welfare optimal. It is standard practice to analyze this inefficiency by bounding the ratio of welfares of the optimal allocation and the welfare-minimizing equilibrium of the auction. Such a bound is called the **Price of Anarchy** (*PoA*).

It was recently shown by [10] that for sequential first price auctions, when bidders may have *either* additive or unit-demand valuations, **the price of anarchy could be** $\Omega(m)$ for the set of pure Nash equilibria in the complete information setting.[9] Since the class of additive/unit-demand valuations are among the simplest valuations and the set of pure Nash equilibria in the complete information setting is among the smallest set of equilibria, the price of anarchy for this case should be among the lowest. Yet

[7] A professional league for the sport of cricket

[8] The salaries for the most demanded players are in the range of a few million dollars, for playing about 6 weeks a year for 3 years. This is substantially higher than the player incomes prior to the auction.

[9] See Section 2.2 for formal definitions of equilibria and the complete information setting.

the lower bound of $\Omega(m)$ is nearly as bad as it gets since it is easy to show an upper bound of $O(m)$ for a much more general class of valuations (subadditive valuations) and a much bigger set of equilibria.

Our Contributions

We propose a natural and simple variant of the sequential item auction which we call a **draft auction**. Draft auctions also proceed in rounds: each round is a sealed-bid first price auction. The difference is that there is no designated item in any round; instead, the winner decides which items she wishes to purchase in that round, paying her bid for *each* such item. Formally, a draft auction is as follows.

```
1. Initialize, for all $i \in [n]$, $S_i = \emptyset, P_i = 0$. The set of remaining items $I = [m]$.
2. While $I \neq \emptyset$,
3.         Each bidder $i \in [n]$ submits a sealed bid $b_i$ and a set $X_i \subseteq I$.
4.         Allocate set $X_{i^*}$ to $i^* = \arg\max_{i\in[n]}\{b_i\}$, i.e., $S_{i^*} = S_{i^*} \cup X_{i^*}$. Break ties arbitrarily.
5.         Bidder $i^*$ pays her bid for each item in $X_{i^*}$, i.e., $P_{i^*} = P_{i^*} + b_{i^*}|X_{i^*}|$.
6.         The winner $i^*$, winning bid $b_{i^*}$ and allocated bundle $X_{i^*}$ is announced.
7. End While.
```

We show that draft auctions have a much better price of anarchy than sequential item auctions, for the very general class of subadditive valuation functions. **Subadditive** valuations are those v that satisfy the property $v(S \cup T) \leq v(S) + v(T)$ for all $S, T \subseteq [m]$. The class of subadditive valuations, which are also called complement-free valuations, contains other well-studied classes of valuations such as submodular, gross substitutes (see Section 2.5 for formal definitions), additive and unit-demand valuations. We show the following price of anarchy bound for draft auctions for subadditive valuations.

Theorem 3.1. *The price of anarchy for draft auctions for subadditive valuations with respect to Nash equilibria (Definition 2.4) in the Bayesian setting or correlated equilibria (Definition 2.5) in the complete information setting is $O(\log^2 m)$.*

We show a slightly better bound for the class of XOS valuations, which is the class of valuations that are representable as a maximum of linear functions (see Section 2.5 for a formal definition).

Theorem 3.2. *The price of anarchy for draft auctions for XOS valuations with respect to Nash equilibria in the Bayesian setting or correlated equilibria in the complete information setting is $O(\log m)$.*

When compared to the $\Omega(m)$ lower bound on the price of anarchy for sequential item auctions for the class unit-demand $\cup$ additive [10], our results above give an exponential improvement.

We also show constant factor upper and lower bounds for the price of anarchy for unit-demand valuations as well as for symmetric concave valuations (where the valuation is a concave function of only the *number* of items; see Section 2.5 for a precise definition).

Theorem 3.3. *The price of anarchy for draft auctions for unit demand bidders with respect to Nash equilibria in the Bayesian setting or correlated equilibria in the complete information setting is at most 4, and w.r.t. pure Nash equilibria in the complete information setting is at most 2.*

Theorem 3.4. *The price of anarchy for draft auctions for unit demand bidders w.r.t. pure Nash equilibria in the complete information setting is at least 1.22. Further there are instances where no equilibrium achieves a welfare within $1 + \epsilon$ of the optimum, for some small universal constant $\epsilon > 0$.*

Theorem 3.5. *The price of anarchy for draft auctions for bidders with symmetric concave valuations with respect to Nash equilibria in the Bayesian setting or correlated equilibria in the complete information setting is at most 8.*

The price of anarchy bounds we show are exponentially better than those for sequential item auctions. In fact, it is possible that draft auctions have a constant price of anarchy for subadditive valuations. We use this contrast to advocate the use of draft auctions in place of sequential item auctions in practice.

To prove our upper bounds, we use the smoothness approach introduced by [28] and extended to auctions by [29]. It boils down to the following main technique: for every equilibrium, construct a deviating strategy for each player which gets at least some fraction of her value in the social-welfare maximizing allocation, while paying at most a small multiple of the revenue in equilibrium. The deviations we construct are more involved than those for sequential item auctions; see [8] for more details.

On a separate note, we show that efficiency bounds proven via the smoothness approach for a very special class of valuations directly extend with only a polylogarithmic degradation to the whole class of subadditive valuations and with no degradation to the class of symmetric concave valuations. Specifically, we show that it suffices to analyze settings where the value of a player is simply proportional to the number of items he acquired from a specific interest set of items. Then we show that smoothness for these simple constrained, cardinality valuations directly implies smoothness for concave symmetric valuations (i.e. identical items) with no loss, for submodular valuations with only a $\log(m)$ loss and for subadditive valuations with a $\log^2(m)$ loss. Our approach may have potential applications to the analysis of other simple mechanisms for combinatorial auction settings.

Illustrative example To illustrate the advantages of draft auctions over sequential item auctions, we revisit an instance introduced by [24], that shows that inefficiency is bound to arise at the unique subgame perfect equilibrium in undominated strategies of sequential item auctions with unit-demand bidders: Consider an instance with 4 bidders, a, b, c, d and 3 items A, B, C. Bidder a has value $v_a = \epsilon$ only for item A, bidder b has value α for either A or B, bidder c has value α for either B or C and bidder d has value $\alpha - \epsilon$ for C. It is shown by [24] that assuming that auctions occur in order A, C, B then in the unique equilibrium, bidder b will let the ϵ-valued bidder a, win the auction, so that he gets the last auction for item B for free. The reasoning being that bidder c will go for item C and will not bid in the last auction. This yields a price of anarchy of 3/2.

However, observe that the latter behavior is very much tied to the ordering of the item auctions. If the auctioneer were to run a draft auction in the same setting then it is easy to see that the optimal allocation can arise at equilibrium: bidders b, c, d all bid ϵ^+ at every iteration until they get allocated. If bidder b wins he gets item A, if bidder c wins then he gets item B and if bidder d wins he gets item C. It is easy to see that no bidder has an incentive to deviate.

Right to choose auctions A simpler variant of the draft auction is obtained by restricting each bidder to only pick one item when she wins a round. This auction format has been studied and used previously, under the names of "right to choose" (RTC) auctions or "pooled auctions". Intuitively, the two formats should not differ much; if a bidder wins a round at a certain price in an RTC auction, then she should be able to win subsequent rounds at the same price too, thus simulating a draft auction. The reason that our results don't readily extend to this format is that the deviations we construct in our proofs need the ability to win multiple items at once. The same deviation for RTC auctions would occur over multiple rounds and necessarily involve reasoning about "off-equilibrium" paths, which is perhaps the biggest technical hurdle in proving price of anarchy bounds for sequential settings. In fact, we believe that the draft vs. RTC auctions might prove to be a good training ground where this technical hurdle could be crossed.

3.0.1 Coauthors

This work is joint with Nikhil Devanur and Vasilis Syrgkanis.

4 Impartial Peer Review

Motivated by a radically new peer review system currently under evaluation by the National Science Foundation, we study peer review systems in which proposals are reviewed by PIs who have submitted proposals themselves. An (m, k)-selection mechanism asks each PI to review m proposals, and uses these reviews to select (at most) k proposals. We are interested in *impartial* mechanisms, which guarantee that the ratings given by a PI to others' proposals do not affect the likelihood of the PI's own proposal being selected. Impartiality is the analogue of truthfulness in a setting where player's utilities are 0 if they are not selected, and 1 if they are selected[10]. We design an impartial mechanisms that selects a k-subset of proposals that is essentially as highly rated as the one selected by the non-impartial (abstract version

[10] In this setting, players will simply play to maximize their probability of being selected. Thus, for a mechanism to be truthful, the probability of any player being selected must be independent of her report, else there will be some state from which she could improve her probability of being selected by misreporting

of) the NSF pilot mechanism, even when the latter mechanism has the "unfair" advantage of eliciting honest reviews.

The Sensors and Sensing Systems (SSS) program of the National Science Foundation (NSF) is currently trying out a revolutionary peer review method. Traditionally, grant proposals submitted to a specific program are evaluated by a panel of reviewers. Potential conflicts of interest play a crucial role in composing the panel; most importantly, principal investigators (PIs) whose proposal is being evaluated by the panel cannot serve on the panel. In stark contrast, the new peer review method — originally designed by Merrifield and Saari [20] for the review of proposals for telescope time — requires the PIs themselves to review each other's proposals! A "dear colleague letter" [14] explains the potential merits of the new process:

> *"This pilot is an attempt to find an alternative proposal review process that can preserve the ability of investigators to submit multiple proposals at more than one opportunity per year while encouraging high quality and collaborative research, placing the burden of proposal review onto the reviewer community in proportion to the burden each individual imposes on the system, simplifying the internal NSF review process, ameliorating concerns of conflict-of-interest, maintaining high quality in the review process, and substantially reducing proposal review costs."*

Under the Saari-Merrifield mechanism, each PI must review m proposals submitted by other PIs; in the NSF pilot, $m = 7$. The PI then ranks the m proposals according to their quality. To aggregate these rankings, the Borda count voting rule is used, so, essentially, each PI awards $m - i$ points to the proposal she ranks in position i. A proposal's overall rating is the average over the points awarded by the m PIs who reviewed it. An intriguing innovation is that a PI's own proposal receives a small bonus based on the similarity between the PI's submitted ranking and the aggregate ranking of proposals; this is meant to encourage PIs to make an effort to produce accurate reviews.

The NSF pilot sparked a lively debate among researchers in mechanism design and social choice, which also took place in the blogosphere [25, 31, 21]. While most researchers seem to agree that the NSF should be commended for trying out an ambitious peer review method, serious concerns have been raised regarding the pilot mechanism itself. Perhaps most strikingly, while the NSF announcement [14] states that the "theoretical basis for the proposed review process lies in an area of mathematics referred to as mechanism design", the pilot mechanism provides no theoretical guarantees. In particular, the mechanism is susceptible to strategic manipulation: PIs will often be able to advance their own proposals by giving low scores to competitive proposals (even though they may forfeit some of the small bonus for accurate reviewing). Indeed, while most researchers who sit on NSF panels are well-respected, the pilot mechanism cannot control the quality of PIs who submit proposals and therefore conduct reviews — leaving open the very real possibility of game-theoretic mayhem.

In this paper, we wish to rigorously study the design of peer review mechanisms where each reviewer is also associated with a proposal or a paper. These mechanisms must be *impartial*: reviewers must not be able to affect the chances of their own proposals being selected. Our research challenge is therefore to

> ... *design provably impartial peer review mechanisms that provide formal quality guarantees.*

We believe that solutions to this problem truly matter. The NSF plays a huge role in enabling scientific research in the United States, and its consideration of alternative peer review methods may transform how scientific funding is allocated in the US. The need to build sound foundations for these methods therefore provides a timely and unique opportunity for the economics and computation community.

4.1 Our Approach

In our setting there are n PIs, each associated with a proposal. Each PI i has a hypothetical (honest) evaluation of the quality of the proposal j, which is the rating i would give j if she were asked to review that proposal. The *score* of a proposal is the average rating given to it by other PIs. As NSF program directors, if our budget is sufficient to fund k proposals, we would ideally want to select a set of k proposals with maximum score. Thus we distill the strategic aspects of the NSF reviewing setting and abstract away some other practical aspects, such as the fact that PIs may submit multiple proposals to the same program. However, our model and results easily extend. Even under the simplified formulation, there are two obstacles we must overcome: we cannot possibly ask each PI to review all other proposals, and the reviews may not be honest.

To address the first problem, we restrict our mechanisms to m reviews per PI (much like the NSF pilot). We therefore define an (m, k)-*selection mechanism* as follows. First, the mechanism asks each PI to review m proposals, in a way that each proposal is reviewed by exactly m PIs; for every such pair (i, j), PI i's evaluation for proposal j is revealed. Based on these elicited reviews, the mechanism selects k vertices. The most natural (m, k)-selection mechanism is an abstract version of the NSF pilot mechanism, which we fondly refer to as the Vanilla mechanism; it chooses m reviews per PI uniformly at random (subject to the constraint that each proposal is reviewed by m PIs), and then selects the k vertices with highest average rating, based only on the sampled reviews.

Returning to the second problem — dishonest reviewing — we say that a selection mechanism is *impartial* if the probability of proposal i being selected is independent of the ratings given by PI i. The motivation for our work stems from the observation that the Vanilla mechanism is not impartial: we seek mechanisms that are.

But how should we evaluate the impartial mechanisms we design? When m is small compared to n, the sampled reviews are likely to be a poor proxy for the underlying scores, even for the Vanilla mechanism, and even when reviewers are truthful. In fact, no (m, k)-selection mechanism can hope to select a subset of proposals with high expected score. We therefore use the Vanilla mechanism as our performance benchmark; this idea is one of the main conceptual contributions of this work. Since the Vanilla Mechanism is an abstraction of the NSF pilot mechanism, our choice of benchmark allows us to quantify how much the NSF must sacrifice to achieve impartiality. We also note that designing impartial mechanisms which compete with the Vanilla mechanism is nontrivial: we give Vanilla the "unfair" advantage of assuming that reviews are honest, even though it is not impartial. Specifically, we say that an impartial mechanism α-*approximates* Vanilla if, in the worst case over reviews, the ratio between the expected score (based on the largely unseen set of all possible reviews) of the set of proposals selected by the impartial mechanism, and the expected score of the set of proposals selected by Vanilla, is at most α.

4.2 Our Results

We present a simple, impartial (m, k)-selection mechanism, the Credible Subset Mechanism which approximates the Vanilla Mechanism to a factor of $\frac{k}{k+m}$. We think of m, the number of reviews per PI, as being a small constant, and we would like to think of k, the number of proposals to be selected, as significantly larger (here we are being somewhat optimistic about NSF funding!). We view Credible Subset as practical, as it modifies Vanilla in a rather minimal way while guaranteeing impartiality. Indeed, instead of selecting the top k proposals, it (usually) selects k proposals at random from a slightly larger pool (of size $k + m$) of eligible, high-quality proposals. We also show that the bound given by Credible Subset is asymptotically tight when $k = m^2$ is a constant and the number of PIs n grows.

4.2.1 Coauthors

This work is joint with David Kurokawa, Omer Lev, and Ariel Procaccia.

5 Privacy-Preserving public information for Sequential Games

Suppose a collection of strategic agents are trying to make some decision. For example, a collection of investment banks are trying to decide how to invest their money. The payoffs of the players will depend upon the actions of the other players; as more people choose a particular investment, the value to investors who are "later to the game" will be smaller than the value for earlier investors. If players make these decisions in some order, and have perfect information about earlier players' decisions, one can analyze the social welfare of various strategies or equilibrium concepts. In particular, if the utility of a player does not depend on later players, only upon the decisions made by earlier players, the greedy strategy is a dominant strategy (and the only undominated strategy). On the other hand, banks may not want their investment decisions to be public knowledge for their competition, which motivates looking into what happens if players are only provided approximate, *private* information regarding previous players' actions. In our work, we ask how well different strategies perform with respect to this approximate information.

To illustrate this idea, consider the classical online optimization problem of vertex-weighted matching. Suppose n nodes on side U of a bipartite graph arrive online. These nodes arrive with unweighted edges to some subset of the m weighted vertices on the V side of the bipartite graph. Let the weight of a perfect matching be the sum of the weighted vertices in V who are matched to a vertex in U.

We identify the nodes on the right-hand side of the bipartite graph with the investment opportunities, or resources, that the players might select. Suppose that a given resource r has k_r "copies", that is, the first k_r people to select r get utility v_r, and no other players get utility from choosing r. In our work, we that approximate information about how many people have selected a given resource or investment is enough for players to approximate Opt with greedy behavior, for arbitrary v_r, k_r. In fact, all of the results in this section actually apply in much more general settings, where each resource r has diminishing value for each subsequent "copy" of the resource chosen by a player, when players may choose multiple (fractional copies of) resources, and even when players are only restricted to playing undominated strategies (see the full paper [3] for more details).

Let Opt refer to the optimal matching in the offline optimization setting: when all nodes and their respective edges are visible, there is a well-defined largest weight any perfect matching can achieve. There is a well-known argument showing that the online greedy matching algorithm 2-approximates the maximum weight matching.

Theorem 5.1 ([16]). *The online matching algorithm which matches vertices in U greedily with weighted vertices in V is a 2-approximation to the optimal matching.*

This theorem can easily be extended to the approximately greedy algorithm: suppose vertices u_i which arrive online choose to match with a v_j such that $w(v_j) \geq \frac{1}{\alpha}w(g_j)$, where g_j is the greedy choice for player j. Call the set of strategies which satisfy this constraint α-approximately greedy. Then, we have the following theorem.

Remark 5.2. *This result actually extends to players being allowed to pick* subsets *of their edges, so long as the sets they are allowed to pick are downward closed (e.g., if X is an allowed set of neighbors for a node, then $X' \subseteq X$ is also allowed), losing another factor of 2 in the approximation. Roughly speaking, either half of the utility from a set X was already taken by some other nodes, or half the utility still remains for X. The union of these facts implies a 4-approximation.*

Remark 5.3. *This actually holds for the continuous version of this problem, where nodes can take fractional pieces of nodes on the other side of the graph.*

Notice that, with no information, "greedy behavior" with respect to initial values can do quite poorly (there can be $\Omega(n)$ ratio between OPT and this behavior). We ask what one can do with private information.

It is interesting to note that, while the counts are approximate, the value each individual player is getting isn't well-approximated. That is, an individual might have an unbounded ratio between her perceived utility from picking resource r (if no more copies exist but the counters say there are still copies available). The welfare approximation is only true when summed over all players' utilities.

Before presenting the theorem for this section, we need a definition of *approximate counters* in the continual observation setting. We will say a mechanism $\vec{s}$ provides an (α, β, γ)-approximate counter vector with respect to an input stream $\vec{a} = (\vec{a}^1, \dots, \vec{a}^n)$ where $\vec{a}^i = (a^i_1, \dots, a^i_m)$ if, with probability $1-\gamma$, for all i, for all r, it is the case that

$$\frac{1}{\alpha}x^i_r - \beta \leq y^i_r \leq \alpha x^i_r + \beta$$

where $x^i_r \sum_{j=1}^{i-1} a^i_r$ is the partial sum for resource r. That is, the guarantee is that all the approximate partial sums are correct up to an additive factor β and a multiplicative factor α within the true partial sum values.

The main theorem we will prove for the simpler case of k_r identical copies of r each with value v_r, is the following.

Theorem 5.4. *Suppose y is (α, β, γ)-approximate counter vector which only underestimates x^i_r for all i, r. Then, the social welfare resulting from players play greedily with respect to y in the online vertex-weighted matching setting is at least an $\frac{1}{4\alpha(\beta+1)}$-fraction of the social welfare of OPT, with probability $1-\gamma$.*

The crux of the proof of Theorem 5.4 lies in the following claim.

Claim 5.5. *Suppose k players select r according to greedy behaviour with respect to an $(\alpha, \beta, 0)$-approximate counter vector and expect to get nonzero utility. Then,*

$$\frac{k}{\min(k_r, k)} = \frac{\textit{Perceived utility from } r}{\textit{Actual welfare from } r} \leq \alpha(1 + \beta)$$

5.1 A better Privacy-preserving mechanism

Theorem 5.4 motivates looking for counter schemes that can get slightly better additive approximations at the expense of a small multiplicative loss in accuracy; the guarantees of the theorem degrade linearly with respect to $\alpha\beta$. So, if $\alpha = O(1)$, then $\beta = o(log^2(n))$ would give a better approximation guarantee than the best-known counter mechanism (Chan et al or Dwork et al's binary tree-sum protocol). Here, we present a mechanism with improved additive guarentees at the expense of an (arbitrarily small) multiplicative loss in accuracy.

Recall the basic counter problem: given a stream $\vec{a} = (a_1, a_2, ..., a_n)$ of numbers $a_i \in [0, 1]$, we wish to release at every time step t the partial sum $x_t = \sum_{i=1}^{t} a_i$.

We require a generalization, where one maintains a vector of m counters. Each player's update contribution is now a vector $a_i \in [0, 1]^m$, with the constraint that $\|a_i\|_1 \leq 1$. That is, a player can add non-negative values to all counters, but the total value of her updates is at most 1. The partial sums x_t then lie in $(\mathbb{R}^+)^m$ (with ℓ_1 norm bounded by t).

Given an algorithm $\mathcal{A}$, we define the output stream $(s_1, s_2, ..., s_n) = \mathcal{A}(\vec{a})$ where $s_i = \mathcal{A}(t, a_1, ..., a_{i-1})$. The original works on differentially private counters [9, 4] concentrated on minimizing the additive error of the estimated sums, that is, they sought to minimize $\|x_t - s_t\|_\infty$. Both papers gave a binary tree-based mechanism, which we dub "TreeSum", with additive error approximately $(\log^2 n)/\epsilon$. Some of our algorithms use TreeSum, and others use a new mechanism (FTSum, described below) which gets a better additive error guarantee at the price of introducing a small multiplicative error. We capture a mixed approximation guarantee as follows:

Definition 5.6. *The algorithm $\mathcal{A}$ provides an (α, β, γ)-approximation to partial sums if for every (adaptively defined) sequence $\vec{a} \in ([0, 1]^m)^n$, with probability at least $1 - \gamma$ over the coins of $\mathcal{A}$, for all times $i \in [n]$ and counters $r \in [m]$, the reported value $x_{t,r}$ satisfies:*

$$\frac{1}{\alpha} \cdot x_{i,r} - \beta \leq s_{i,r} \leq \alpha \cdot x_{i,r} + \beta\,.$$

Proofs of all the results in this section can be found in the full paper [3].

Lemma 5.7. *For every $m \in \mathbb{N}$ and $\gamma \in (0, 1)$: Running m independent copies of TreeSum [9, 4] is $(\epsilon, 0)$-differentially private and provides an $(1, C_{tree} \cdot \frac{(\log n)(\log(nm/\gamma))}{\epsilon}, \gamma)$-approximation to partial vector sums, where $C_{tree} > 0$ is an absolute constant.*

Even for $m = 1, \alpha = 1$, this bound is slightly tighter than those in [4] and [9]; however, it follows directly from the tail bound in [4].

Our new algorithm, FTSum (for Flag/Tree Sum), is described in Algorithm 1. For small m ($m = o(log(n))$), it provides lower additive error at the expense of introducing an arbitrarily small constant multiplicative error.

Lemma 5.8. *For every $m \in \mathbb{N}$, $\alpha > 1$ and $\gamma \in (0, 1)$, FTSum (Algorithm 1) is $(\epsilon, 0)$-differentially private and $(\alpha, \tilde{O}_\alpha(\frac{m \log(n/\gamma)}{\epsilon}), \gamma)$-approximates partial sums (where $\tilde{O}_a(\cdot)$ hides polylogarithmic factors in its argument, and treats α as constant).*

FTSum proceeds in two phases. In the first phase, it increments the reported output value only when the underlying counter value has increased significantly. Specifically, the mechanism outputs a public signal, which we will call a "flag", roughly when the true counter achieves the values $\log n$, $\alpha \log n$, $\alpha^2 \log n$ and so on, where α is the desired *multiplicative* approximation. The reported estimate is updated each time a flag is raised (it starts at 0, and then increases to $\log n$, $\alpha \log n$, etc). The privacy analysis for this phase is based on the "sparse vector" technique of [13], which shows that the cost to privacy is proportional to the number of times a flag is raised (but not the number of time steps between flags).

When the value of the counter becomes large (about $\frac{\alpha \log^2 n}{(\alpha-1)\epsilon}$), the algorithm switches to the second phase and simply uses the TreeSum protocol, whose additive error (about $\frac{\log^2 n}{\epsilon}$) is low enough to provide an α multiplicative guarantee (without need for the extra space given by the additive approximation).

If the mechanism were to raise a flag *exactly* when the true counter achieved the values $\log n$, $\alpha \log n$, $\alpha^2 \log n$, etc, then the mechanism would provide a $(\alpha, \log n, 0)$ approximation during the first phase, and a $(\alpha, 0, 0)$ approximation thereafter. The rigorous analysis is more complicated, since flags are raised only near those thresholds.

Algorithm 1: FTSum — A Private Counter with Low Multiplicative Error

```
Input: Stream $\vec{a} = (a_1, ..., a_n) \in ([0,1]^m)^n$, parameters $m, n \in \mathbb{N}$, $\alpha > 1$ and $\gamma > 0$
Output: Noisy partial sums $s_1, ..., s_n \in \mathbb{R}^m$
$k \leftarrow \lceil \log_\alpha(\frac{\alpha}{\alpha-1} \cdot C_{tree} \cdot \frac{\log(nm/\gamma)}{\epsilon}) \rceil$;
/* $C_{tree}$ is the constant from Lemma 5.7 */
$\epsilon' \leftarrow \frac{\epsilon}{2m(k+1)}$;
for $r = 1$ to $m$ do
    $\text{flag}_r \leftarrow 0$;
    $x_{0,r} \leftarrow 0$;
    $\tau_r \leftarrow (\log n) + \mathsf{Lap}(2/\epsilon')$;
for $i = 1$ to $n$ do
    for $r = 1$ to $m$ do
        if $flag_r \leq k$ then (First phase still in progress for counter $r$)
            $x_{i,r} \leftarrow x_{i-1,r} + a_{i,r}$;
            $\tilde{x_{i,r}} \leftarrow x_{i,r} + \mathsf{Lap}(\frac{2}{\epsilon'})$;
            if $\tilde{x_{i,r}} > \tau_r$ then (Raise a new flag for counter $r$)
                $\text{flag}_r \leftarrow \text{flag}_r + 1$;
                $\tau_r \leftarrow (\log n) \cdot \alpha^{\text{flag}_r} + \mathsf{Lap}(2/\epsilon')$;
            Release $s_{i,r} = (\log n) \cdot \alpha^{\text{flag}_r - 1}$ ;
        else (Second phase has been reached for counter $r$)
            Release $s_{i,r} = r$-th counter output from TreeSum$(\vec{a}, \epsilon/2)$);
```

Proposition 5.9. *If $\mathcal{A}$ is (ϵ, δ)-private and (α, β, γ)-accurate, then one can modify $\mathcal{A}$ to obtain an algorithm $\mathcal{A}'$ with the same efficiency that is $(\epsilon, \delta + \gamma)$-private and $(\alpha, \beta, 0)$-accurate.*

Corollary 5.10. *Algorithm 1 is an (ϵ, δ)-differentially private vector counter algorithm providing a*

1. $(1, O(\frac{(\log n)(\log(nm/\delta))}{\epsilon}), 0)$*-approximation (using modified TreeSum); or*
2. $(\alpha, \tilde{O}_\alpha(\frac{m \log n \log\log(1/\delta)}{\epsilon}), 0)$*-approximation for any constant $\alpha > 1$ (using FTSum).*

5.1.1 Coauthors

This work is joint with Avrim Blum, Adam Smith, and Ankit Sharma.

6 Private and Truthful Deferred Acceptance

Suppose there are m schools and n students. Each student i has a linear ordering which represents her preferences over schools, denoted $\succ_i$. Simlarly, each school s has a linear preference over the students, denoted $\succ_s$. Each school is also accompanied by a capacity c_s, representing the total number of students the school wishes to admit. $\succ_s$ can also be interpreted as assigning scores to the individual students, e.g. the results of a school-specific entrance exam. For the purposes of this work, we assume each school Y has assigned a unique number $score(s, Y)$ (e.g., a ranking which might be thought of as a test score) to each student s, and that the student knows this test score for each school.

A classical problem in economics is that of computing stable matchings in such a setting. It is well-known [27] that no mechanism can compute stable matchings and be truthful simultaneously for both sides (e.g., for students and schools) of the market. Furthermore, while any mechanism which computes the student-optimal stable matching is truthful for the student side of the market, the mechanism which computes the school-optimal stable matching is (in general) truthful for neither side of the market. In our work, we aim to devise mechanisms which are (approximately) school-optimal, (approximately) truthful for the student side of the market, and (approximately) stable. To the best of our knowledge, this is the first work in the worst-case model to show nontrivial truthfulness guarantees for (approximately) school-optimal matchings.

We use two main tools for this task: the well-known deferred acceptance algorithm, and Theorem 2.9. Our assumption is that the number of seats at each school is large (polynomial in the number of schools) for the school optimality guarantee to kick in. We make a few definitions in order to be able to state the main result of this section. First, we define what it means for a particular empty seat at a school to be blocking.

Definition 6.1. *Given μ with $e_Y > 0$, we say an empty seat is blocking if there exists a student s such that $Y \succ_s \mu(s)$. We say there are k empty blocking seats if there $e_Y \geq k$ and there are k students which block with empty seats for Y.*

Definition 6.2. *Given μ with $e_Y > 0$, we say a school Y and student s form a* **full seat blocking pair** *if there exists a student s' such that $s \notin \mu(Y)$, $s' \in \mu(Y)$, but $Y \succ_s \mu(s)$ and $s \succ_Y s'$.*

With these definition in hand, we define our notion of approximate stability.

Definition 6.3. *Consider a many-to-one matching $\mu : n \to 2^{[m]}$. We say that μ is k-stable if there are at most k empty blockings seats at any school, there are no full-seat blocking pairs, and no school has more than its capacity of students.*

Now, we have all the ingredients we need to define what it means for a matching to be approximately school optimal.

Definition 6.4. *Suppose μ is the school-optimal stable matching. A matching μ' is a school-dominant matching if, for each school Y, for each $s \in \mu(Y) \setminus \mu'(Y)$, $s' \in \mu'(Y) \setminus \mu(Y)$, that $s' \succ_Y s$.*

Formally, we will use a variant of the deferred acceptance algorithm which is (ϵ, δ)-differentially private under adaptive continual observation, to prove the following theorem.

Theorem 6.5. *There exists a mechanism which allows students to compute an $\frac{\sqrt{8m}\ln^2(1/\delta)}{\epsilon}$-approximately stable matching which is school-dominant, where a student who misreports can improve which school she attends with probability at most $e^\epsilon + \delta$.*

The mechanism's informal description is simple. In each round, each school will post a "threshold score", and any student with that score or above can choose to tell that school they (tentatively) wish to attend. Once all students have decided where they tentatively wish to attend, each school determines whether or not they are (approximately) at capacity. If a school is not full, they will lower their threshold score in the following round. If a school is full, their threshold will remain the same for the next round. In all future rounds, students will look at the current thresholds, and determine whether they wish to change schools (in which case they tell their current tentative match and their new school), or stay put (in which they do nothing).

Algorithm 2: School proposing, where $noisy(d(Y))$ is an implementation of the tree-sum counting protocol [5, 9]

```
For each school $Y$, start a DP counter $d(Y)$
For each school $Y$, set a threshold $m(Y) = max$
For each student, begin unmatched $\mu(s) = \emptyset$
while Some school $Y$ has $c(Y) - noisy(d(Y)) > 0$ and $m(Y) > 0$ do
    for each $Y$ with $c(Y) - d(Y) > 0$ do
        set $m(Y) = m(Y) - 1$
    for each student $s$ do
        if $\mu(s) = \emptyset$ then
            If $score(s, Y) > m(Y)$, then match $s$ to her favorite such $Y$
            Increment $d(Y)$
        else
            if $\mu(s) \neq fav(s, m(1), \ldots, m(k))$ then
                Decrement $d(\mu(s))$
                Set $\mu(s) = fav(s, m(1), \ldots, m(k))$
                Increment $d(\mu(s))$
            else
                Do nothing
```

The approximate truthfulness guarantee can be proven by the following line of reasoning. Since the entire run of the mechanism is differentially private, any deviation on the part of a student (e.g., by choosing to tentatively choose or reject a school which does not signify her true preferences) can change the final thresholds (and thus, the set of schools available to her) with probability more than $e^{\epsilon} + \delta$.

6.0.2 Coauthors

This work is joint with Aaron Roth, Steven Wu, and Sampath Kannan.

7 Future Work and Open Questions

There are several directions which I am planning to pursue in the coming months to complete this thesis. I will roughly order them by topic.

7.1 Draft Auctions

Is it possible to improve the $O(\log(m))$ and $O(log^2(m))$ upper bounds on the price of anarchy from this paper? If not, what about lower bounds? I have several ideas for how a better upper bound might come about, perhaps via the $O(\log(m))$-approximations for subadditive valuations in single-item bidding in [2], or [1]. I would also be interested in whether or not there is some formal reduction from draft auctions to the right-to-choose auctions: the RTC auctions are simpler conceptually and it would be great if some of the analysis carried over. Finally, it would be interesting to know some reasonable strategy for a bidder to employ which would be approximately best-response; we have no idea about the computational or communicational complexity of these auctions so any result in this direction would be interesting.

7.2 Private Public Signals

I have started work thinking about whether our results regarding greedy play could extend to Bayes-Nash equilibria: namely, if players computed consistent estimates of the world as a function of the data we provide, and played optimally with respect to that computation, can we get similar welfare guarantees? This project was originally inspired by the idea of private equilibrium computation (much akin in spirit to [17]), and it would be interesting to prove something about equilibria of this setting.

It would also be interesting to prove things in terms of counters that are "soft": rather than using a bound on their accuracy which holds with high probability, using one which talks about the expected amount of noise would allow us to have more accurate on average while preserving privacy. It would also be useful to reduce the linear dependence on m (the number of resources) that the accuracy guarantee of our new counter mechanism currently has: we have no reason to believe it is necessary to preserve privacy, but haven't been able to prove that it is extraneous.

7.3 Impartial Peer Review

There are several open problems relating to this paper. First, to better motivate the use of Vanilla as a benchmark, can we show that no mechanism can do much better (with respect to Opt), when the number of reviews m is much smaller than n, the total number of proposals? In particular, we would like to show that no mechanism can do better than $\frac{\max\{m,k\}}{n}$-approximate Opt for appropriately chosen ranges of m, k as n grows (since Vanilla $\frac{m}{n}$-approximates Opt, and randomly choosing k proposals $\frac{k}{n}$-approximates Opt, this is the strongest lower bound we could hope for). It would also be interesting to understand slightly weaker models, where reviewers' opinions are not worst-case, or whether reviewers have finite weight they can place on their opinions.

7.4 Private Deferred Acceptance

We know that it is impossible to compute exactly-school-optimal stable matchings with a differentially private mechanism. Furthermore, it is impossible to compute a stable matching with zero empty seats when differential privacy is a hard constraint. However, we do not know whether there is a lower bound stating we need $\Omega(\sqrt{m}/\epsilon)$ empty seats at each school to ensure privacy on the part of the student's data. Such a lower bound would be very interesting, and may have interesting implications for the possibility of student-truthful mechanisms which compute approximately school-optimal matchings.

7.5 Learning from Auction Data

In ongoing work, we ask the following question. Given limited information (e.g., the winner and the price paid) about the outcome of a sequence of independent auctions or pricing mechanisms, is it possible to learn back data about the players' valuations, or to predict outcomes of future auctions? The first setting we have considered, and for which we have made the most progress, is the following. Suppose each player has a fixed, deterministic valuation function over the set of available items. In each round, a set of players arrive along with a price for each item. One by one, in a fixed order, the players choose from the remaining set of items at their prices to maximize their quasilinear utility. The label for an example is the allocation of items to players. In this setting, for several classes of valuations, we are able to learn the allocations for all subsets of players in a mistake bound model, with a number of mistakes which is polynomial in the number of possible bidders and items (rather than needing to see examples from all 2^n subsets of bidders).

We are also considering several models where players draw independent, private values from some distribution, and bid such a value in a second-priced auction. If the label for an example is who won and what price they paid, we ask the question as to whether this gives us sufficient information to (approximately) reconstruct the players' valuation distributions?

7.5.1 Coauthors

This work is joint with Avrim Blum and Yishay Mansour.

8 Timeline

1. Submit papers on Sections 4 to 6 to SODA (July 2014)
2. Submit paper on Section 7.5 to WINE (August 2014)
3. Continue working on open questions (September 2014-Feb 2015)
4. Write thesis draft (Feb 2015-April 2015)

5. Defend (May-August 2015)

References

[1] Maria-Florina Balcan, Avrim Blum, and Yishay Mansour. Item pricing for revenue maximization. In *Proceedings of the 9th ACM conference on Electronic commerce*, pages 50–59. ACM, 2008.

[2] 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*, pages 700–709. SIAM, 2011.

[3] Avrim Blum, Jamie Morgenstern, Ankit Sharma, and Adam Smith. Privacy-preserving public information for sequential games. *CoRR*, abs/1402.4488, 2014.

[4] T.-H. Hubert Chan, Elaine Shi, and Dawn Song. Private and continual release of statistics. *ACM Trans. Inf. Syst. Secur.*, 14(3):26, 2011.

[5] Yiling Chen, Stephen Chong, Ian A. Kash, Tal Moran, and Salil Vadhan. Truthful mechanisms for agents that value privacy. EC '13, pages 215–232, 2013.

[6] Yiling Chen, Stephen Chong, Ian A. Kash, Tal Moran, and Salil Vadhan. Truthful mechanisms for agents that value privacy. In *Proceedings of the Fourteenth ACM Conference on Electronic Commerce*, EC '13, pages 215–232, New York, NY, USA, 2013. ACM.

[7] cricinfo.com. Mumbai unhappy with change in auction norms. `http://www.espncricinfo.com/indian-premier-league-2011/content/story/498498.html`. Accessed: 2013-10-30.

[8] Nikhil R. Devanur, Jamie Morgenstern, and Vasilis Syrgkanis. Draft auctions. *CoRR*, abs/1311.2820, 2013.

[9] Cynthia Dwork, Moni Naor, Toniann Pitassi, and Guy N Rothblum. Differential privacy under continual observation. STOC '10, pages 715–724. ACM, 2010.

[10] Michal Feldman, Brendan Lucier, and Vasilis Syrgkanis. Limits of efficiency in sequential auctions. In *Proceedings of the 9th Workshop on Internet and Network Economics*, WINE, 2013.

[11] Drew Fudenberg and Jean Tirole. *Game Theory*. MIT Press, 1991.

[12] Arpita Ghosh and Aaron Roth. Selling privacy at auction. *Games and Economic Behavior*, 2013.

[13] Moritz Hardt and Guy N. Rothblum. A multiplicative weights mechanism for privacy-preserving data analysis. In *FOCS '10*, 2010.

[14] G. A. Hazelrigg. Dear colleague letter: Information to principal investigators (PIs) planning to submit proposals to the Sensors and Sensing Systems (SSS) program October 1, 2013, deadline. `http://www.nsf.gov/pubs/2013/nsf13096/nsf13096.jsp?WT.mc_id=USNSF_25#reference1`. Retrieved on January 7, 2014., 2013.

[15] Zhiyi Huang and Sampath Kannan. The exponential mechanism for social welfare: Private, truthful, and nearly optimal. In *Foundations of Computer Science (FOCS), 2012 IEEE 53rd Annual Symposium on*, pages 140–149. IEEE, 2012.

[16] Richard M. Karp, Umesh V. Vazirani, and Vijay V. Vazirani. An optimal algorithm for on-line bipartite matching. In *STOC '90*, pages 352–358, 1990.

[17] Michael Kearns, Mallesh M. Pai, Aaron Roth, and Jonathan Ullman. Mechanism design in large games: Incentives and privacy. *CoRR*, abs/1207.4084, 2012.

[18] David Kurokawa, Omer Lev, Jamie Morgenstern, and Ariel Procaccia. Impartial peer review. In submission, February 2014.

[19] Frank McSherry and Kunal Talwar. Mechanism design via differential privacy. In *Foundations of Computer Science, 2007. FOCS'07. 48th Annual IEEE Symposium on*, pages 94–103. IEEE, 2007.

[20] M. Merrifield and D. Saari. Telescope time without tears: a distributed approach to peer review. *Astronomy and Geophysics*, 50(4):2–6, 2009.

[21] M. Mitzenmacher. NSF reviewing trial run. `http://mybiasedcoin.blogspot.com/2013/06/nsf-reviewing-trial-run.html`. Retrieved on January 7, 2014., 2013.

[22] Kobbi Nissim, Claudio Orlandi, and Rann Smorodinsky. Privacy-aware mechanism design. In *Proceedings of the 13th ACM Conference on Electronic Commerce*, EC '12, pages 774–789, New York, NY, USA, 2012. ACM.

[23] Kobbi Nissim, Rann Smorodinsky, and Moshe Tennenholtz. Approximately optimal mechanism design via differential privacy. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, ITCS '12, pages 203–213, New York, NY, USA, 2012. ACM.

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

[25] Ariel D. Procaccia. NSF (actually) reviewing via social choice. `http://agtb.wordpress.com/2013/06/10/nsf-actually-reviewing-via-social-choice/`. Retrieved on January 7, 2014., 2013.

[26] Aaron Roth and Grant Schoenebeck. Conducting truthful surveys, cheaply. In *Proceedings of the 13th ACM Conference on Electronic Commerce*, EC '12, pages 826–843, New York, NY, USA, 2012. ACM.

[27] Alvin E Roth. The economics of matching: Stability and incentives. *Mathematics of Operations Research*, 7(4):617–628, 1982.

[28] T. Roughgarden. Intrinsic robustness of the price of anarchy. In *STOC*, 2009.

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

[30] thehindu.com. Ipl auction day 1 - as it happened - the hindu. `http://www.thehindu.com/sport/cricket/ipl-auction-day-1-as-it-happened/article1072914.ece`. Accessed: 2013-10-30.

[31] R. V. Vohra. A mechanism design approach to peer review. `http://theoryclass.wordpress.com/2013/06/06/a-mechanism-design-approach-to-peer-review/`. Retrieved on January 7, 2014., 2013.

[32] David Xiao. Is privacy compatible with truthfulness? *IACR Cryptology ePrint Archive*, 2011:5, 2011.

[33] youtube.com. Ipl 2013 player auction ipl 6. `http://www.youtube.com/watch?v=QYARd23PPPQ`. Accessed: 2013-10-30.