Mechanism Design via Differential Privacy

Frank McSherry
Microsoft Research
Silicon Valley Campus
mcsherry@microsoft.com

Kunal Talwar
Microsoft Research
Silicon Valley Campus
kunal@microsoft.com

Abstract

We study the role that privacy-preserving algorithms, which prevent the leakage of specific information about participants, can play in the design of mechanisms for strategic agents, which must encourage players to honestly report information. Specifically, we show that the recent notion of differential privacy [15, 14], in addition to its own intrinsic virtue, can ensure that participants have limited effect on the outcome of the mechanism, and as a consequence have limited incentive to lie. More precisely, mechanisms with differential privacy are approximate dominant strategy under arbitrary player utility functions, are automatically resilient to coalitions, and easily allow repeatability.

We study several special cases of the unlimited supply auction problem, providing new results for digital goods auctions, attribute auctions, and auctions with arbitrary structural constraints on the prices. As an important prelude to developing a privacy-preserving auction mechanism, we introduce and study a generalization of previous privacy work that accommodates the high sensitivity of the auction setting, where a single participant may dramatically alter the optimal fixed price, and a slight change in the offered price may take the revenue from optimal to zero.

1 Introduction

The problem of analyzing sensitive data with an eye towards maintaining its privacy has existed for some time. Problems faced by the Census Bureau, among other examples, helped to develop the study of "disclosure limitation mechanisms"[1], which aim to limit the amount or nature of specific information that leaks out of a data set. Techniques emerged in which the sensitive input data is randomized, aggregated, anonymized, and generally contorted to remove any concrete implications about its original form, and thereby constrain the disclosures that might result.

As might be expected, a common part of most (but not all) disclosure limitation mechanisms is a precise understanding of what constitutes an unacceptable disclosure. Generally, disclosing specific information about a participant is unacceptable, whereas non-specific, general information about a population is acceptable, even desirable. Specific guarantees given by different techniques are, naturally, different, and the tendency is to formally characterize privacy as protection from the disclosures prevented by the mechanism at hand, rather than aiming for any specific privacy goal.

Recent work [15, 14] avoids the difficulties of formally characterizing disclosures through a definition that imposes *relative* bounds the change in the probability of *any* event. Rather than bound the probability that any event does or does not happen, the definition bounds the relative change in probability of events as a result of changes in any one user's data.

Definition 1 (Differential Privacy) *A randomized function $\mathcal{M}$ gives* ϵ-differential privacy *if for all data sets D_1 and D_2 differing on a single user, and all $S \subseteq Range(\mathcal{M})$,*

$$\mathbf{Pr}[\mathcal{M}(D_1) \in S] \leq \exp(\epsilon) \times \mathbf{Pr}[\mathcal{M}(D_2) \in S] . \quad (1)$$

A natural consequence is that any event (perhaps an unwanted disclosure of private information) as defined by a subset S of $Range(\mathcal{M})$, is not substantially more or less likely as a result of any one user's participation. Events that are unlikely (or impossible) without a specific user's data remain so even after introducing the data to the computation.

The field of Mechanism Design studies the design and analysis of algorithms robust to strategic manipulation of their inputs by self-interested agents. One can view privacy concerns as a form of strategic play: participants are concerned that the specific values of their inputs may result in noticeably different outcomes, of noticeably different utilities. While results from Mechanism Design can potentially

[1] The reuse of the term "mechanism" is not our choice, but we will see that it is not entirely inappropriate either.

provide interesting privacy-preserving algorithms, the subject of this note is to develop the converse: that strong privacy guarantees, such as given by differential privacy, can inform and enrich the field of Mechanism Design.

1.1 Statement of Results and Comparison with Related Work

The contributions of this note fall into three parts. We introduce the use of differential privacy as a solution concept for mechanisms design, we expand the applicability of differential privacy by presenting a mechanism that can be applied in a substantially larger set of contexts than previous work, and we study the particular case of unlimited supply auctions, providing substantially improved regret bounds using this solution concept.

Differential Privacy as a Solution Concept Perhaps the most common solution concept for mechanism design is "truthfulness", where the mechanism is designed so that truthfully reporting one's value is a dominant strategy for each user. Designing mechanisms that are truthful simplifies their analysis by removing the need to worry about potential gaming that the users might apply in order to raise their expected utility. For this reason, the comfort of truthfulness as a solution concept is very appealing.

The mechanisms are normally proved truthful in the setting where collusion among multiple players is prohibited, where the utility functions of the bidders are constrained to simple classes, and where the mechanisms are executed once, with limited possibility of recourse. Additionally, the mechanisms may need provide large payments to some users or offer goods to different users at different prices or not at all. Such strong assumptions can limit the domains in which the mechanisms can be faithfully implemented and the benefits of truthfulness fully realized.

As we will develop in Section 2, differential privacy leads to a relaxation of truthfulness where the incentive to misrepresent a value is non-zero, but tightly controlled. More importantly, the approximate truthfulness that results gives *immediate* guarantees in the presence of collusion, for arbitrary utility functions, and under repeated runs of the mechanism. Owing to recent work of Chaudhuri et al. [12], such mechanisms can be implemented to be truthful with high probability. Moreover, it will allow us to develop mechanisms for problems that cannot be addressed with strict truthfulness, a notable example being the *unlimited supply pricing problem*, where an unlimited supply of goods must be made available to all at a single price.

A General Differential Privacy Framework Previous approaches to differential privacy focus on real valued functions whose values are relatively insensitive to the change in the data of a single individual *and* whose usefulness is relatively unaffected by additive perturbations. Many statistical quantities fit these requirements, as do several other more computational quantities. Most work has focused on the goal of reducing the magnitude of additive perturbation, either by studying properties of the function, or more recently by taking advantage of non-uniformity in the sensitivity of the function [33].

What the approaches have not discussed is how to expand their methods to domains where the above assumptions do not hold. Taking the example of unlimited supply auctions, the function "optimal fixed price to sell at" is neither insensitive – a single bidder has the potential to shift the optimal price arbitrarily – nor robust to additive noise, as increasing the offered price even slightly has the potential to send all bidders home empty-handed. While the recent work of Nissim et al. [33] may address those instances where the optimal price is insensitive, it does not address sensitive instances or the issue of additive perturbations, which we will.

A larger issue, which our general mechanism will also address, is the design of mechanisms for problems where the output is non-numeric. For example, in machine learning one produces models or classifiers; in optimization one may want to activate facilities or route flow. While these solutions may contain numbers in them, a large component of the output is structural information that is not easily "perturbed". Our general framework will permit an arbitrary measurable range, and allow us to tackle problems like those mentioned above in a privacy-preserving manner. In fact, the framework captures *any* mechanism that gives differential privacy, but does not necessarily expose the computational benefits possible in special settings.

Applications to Digital Goods Auctions The *digital goods auction problem* involves a set of n bidders, each of which has a private utility for a good at hand, of which the auctioneer has an unlimited supply. The bidders submit bids in $[0, 1]$, and the auctioneer determines who receives the good and at what prices. We write OPT for the optimal fixed price revenue the auctioneer could extract from the submitted bids.

Theorem 1 *There is a mechanism for the digital goods auction problem giving ϵ-differential privacy and with expected revenue at least $OPT - 3\ln(e + \epsilon^2 OPTn)/\epsilon$.*

This can be compared with the recent work of Balcan et al. [6] who use machine learning applied to random samples of users to arrive at a *truthful* mechanism that gives $OPT - O(\sqrt{OPT})$ revenue in expectation. Our approach trades strict adherence to truthfulness for the exponentially smaller deficit from the optimal revenue. Moreover, in this

exchange our mechanism collects the strong properties discussed in Section 2, which are not present in the work of [6]. In addition, our mechanism offers the same price to all users, and is therefore *envy-free*.

As an extension of the digital goods auction problem, the *digital goods attribute auction problem* adds public, immutable attributes to each participant. The output of mechanisms for this problem describe a market segmentation (*i.e.* a partitioning) of the attribute space, and prices for each market segment. It is common to constrain the possible segmentations, thereby constraining the optimal solution to a manageable space. We write OPT_k for the optimal revenue over segmentations into k markets, and SEG_k for the number of segmentations of the specific bidders at hand into k markets.

Theorem 2 *There is a mechanism for the digital goods attribute auction problem giving ϵ-differential privacy and with expected revenue at least*

$$\max_k (OPT_k - 3\ln(e + \epsilon^{k+1} OPT_k SEG_k n^{k+1})/\epsilon).$$

This can be compared with Theorem 5 in [6] which gives a structural risk minimization based bound, guaranteeing revenue at least

$$\max_k (OPT_k - O((OPT_k^2 \ln(k^2 SEG_k))^{1/3}))$$

with high probability. Again, we give up strong truthfulness in exchange for the additional revenue as well as the properties outlined in Section 2, and the single-price offer.

We also provide new results for constrained pricing problems, as well as the problem of selecting and applying the best of a set of truthful algorithms.

1.1.1 Previous Work in Privacy

Several mechanisms that give differential privacy have been detailed in prior work, mostly for tasks in data mining, machine learning, and statistics. A large class of mechanisms take advantage of the fact that the outputs of interest are robust to small additive noise, and consequently additive perturbations chosen to preserve privacy do not compromise their usefulness. Specifically, in [9, 15] the addition of symmetric, exponentially distributed noise to functions satisfying a Lipschitz condition is shown to ensure differential privacy.

Recent work of Nissim et al [33] shows how to take advantage of non-uniformity in the sensitivity of functions whose worst-case sensitivity may be large, while the "local sensitivity" is small. These results can often substantially reduce the amount of noise that is added to such computed quantities.

Other disclosure limitation techniques involve input perturbation, scrambling the data that is received from the users, and query restriction, in which certain questions are not answered if it is determined that their outputs would compromise privacy. Research in these areas have aimed to prevent disclosures in the absolute sense, typically folding assumptions on the adversary into the definition of disclosure. Indeed, [14] shows that absolute disclosure limitation is impossible without limiting the prior knowledge of the adversary. We refer the reader to [1] for a good survey of related work.

1.1.2 Previous Work in Mechanism Design

The field of mechanism design has been an active area of research in game theory and economics for several years, starting with the Vickrey auction and generalizations of it to social choice theory (see *e.g.* the book by Mas-Colell, Whinston, and Green [30]). Algorithmic mechanism design, starting with the work of Nisan and Ronen [32], has mostly concentrated on designing truthful mechanisms. Some examples include work on auctions for digital goods, scheduling problems, and combinatorial auctions.

However, in many settings, truthfulness appears to be too strong an assumption, preventing the mechanism from having other very desirable properties. For example, Archer and Tardos [4] and Elkind, Sahai and Steiglitz [16] show that any truthful mechanism for buying a shortest path in a graph must overpay by a lot. For the combinatorial auction problem, the work of Lavi, Mu'alem, and Nisan [27] shows that under fairly natural assumptions, no truthful and computationaly efficient mechanism can give a good approximation to the social welfare. While truthful mechanisms for single parameter agents are reasonably well-understood, the characterization of truthful mechanisms for multi-dimensional agents [8, 35] is more recent.

Thus relaxations to strong truthfulness are natural to consider, and have been extensively studied. Implementation in Bayes-Nash equilibria is fairly common in auction theory (see e.g. [30]). Archer et al. [3] considered mechanisms that are strongly truthful with high probability, in the setting of combinatorial auctions for single-minded bidders. Babaioff, Lavi, and Pavlov [5] designed mechanisms where truthtelling is undominated for single-value combinatorial auctions. For the case of shortest path auctions, Elkind et al. [16] look at Bayes-Nash equilibria, while Czumaj and Ronen [13] propose implementations in Nash equilibria and Myopic equilibria. Immorlica *et al.* [24] look at ϵ-Nash implementations in the same setting. Lavi and Nisan [28] introduce the notion of set Nash and give a mechanism implementing this notion, for auctioning items that have expiry times. Finally, myopic equilibria is also commonly used as a solution concept in the setting of ascending auctions (see

e.g. [34]).

Schummer [37] defined the notion of ϵ-dominant strategy implementation, and showed how relaxing truthfulness by a small amount allows one to bypass impossibility results in the context of 2-agent exchange economies with two goods. Kothari, Parkes, and Suri [26] use this notion to design mechanisms for multi-unit auctions. Feigenbaum and Shenker [18] mention investigating study of approximate notions of truthfulness, including ϵ-dominance, as a major open problem.

There has been a lot of work on the unlimited supply auction problem [21, 19, 6, 2, 17, 23]. The online variant of this problem has also been extensively studied [7, 11, 25, 10]. Attribute auctions have been studied in [10, 6]. The work on consensus auctions for digital good auctions by Goldberg and Hartline [19, 20] is close in spirit to our work, in that a summary value is randomly perturbed to limit manipulability; they get collusion resistance, but lose a constant fraction of the revenue.

1.2 Paper Outline

We start in Section 2 with an articulation of the game theoretic consequences of differential privacy. In Section 3 we develop a mechanism that provides differential privacy and generalizes the additive noise mechanisms of [9, 15]. Along with the proof of differential privacy, we prove a theorem about the usefulness of the mechanism, showing that it is very unlikely to produce undesirable outputs. In Section 4 we apply this general mechanism to the problem of single-commodity pricing, attributes auctions, and structurally constrained pricing problems. Finally, we conclude with open problems and directions for further research.

2 Differential Privacy as a Solution Concept

We translate some implications of differential privacy into language more familiar in the mechanism design space.

2.1 Approximate Truthfulness

Several notions of approximate truthfulness have been proposed and studied; one that we will highlight is called ϵ-dominance, proposed and studied by Schummer [37], in which no agent has more than an ϵ additive incentive to reply non-truthfully. We note that this is a stronger notion than that of ϵ-Nash.

Mechanisms satisfying ϵ-differential privacy make truthtelling an $(\exp(\epsilon) - 1)$-dominant strategy for any utility function mapping $Range(\mathcal{M})$ to $[0, 1]$. This follows from a more general guarantee: that no user can cause a *relative* change of more than $\exp(\epsilon)$ in their utility.

Lemma 3 (Approximate Truthfulness) *For any mechanism $\mathcal{M}$ giving ϵ-differential privacy and any non-negative function g of its range, for any D_1 and D_2 differing on a single input*

$$E[g(\mathcal{M}(D_1))] \quad \leq \quad \exp(\epsilon) \times E[g(\mathcal{M}(D_2))] \; . \quad (2)$$

Proof: For any non-negative function g, we can rewrite

$$E[g(\mathcal{M}(x))] \quad = \quad \int_c g(c) \times p_x(c). \quad (3)$$

Differential privacy bounds, via (1), the change from p_{D_1} to p_{D_2} by a factor of $\exp(\epsilon)$, concluding the proof. ■

We have made no assumptions on the nature of the function g, other than its non-negativity. This serves differential privacy well in avoiding *a priori* definitions of privacy violations, and will serve us equally well accommodating non-quasilinear utilities, risk-averse players, the temptations of side payments, and certain other externalities. Of course, the bound on the change in expectation is drawn from the bound on the change in the distribution, which provides even stronger guarantees, such as bounds on the relative change in higher moments.

Remark: In recent work, Chaudhuri et al. [12] show that any mechanism $\mathcal{M}$ with ϵ-differential privacy can be implemented so that for all D_1, with probability at least $1 - 2\epsilon$, $\mathcal{M}(D_1) = \mathcal{M}(D_2)$ for all D_2 differing from D_1 on a single user. In the mechanism design context, this corresponds to *truthfulness with high probability* [3]: starting from the vector of private values, for most tosses of the random coins of the mechanism, there is zero incentive for a user to misreport her private value. The approach uses a generalization of min-wise independent sampling to non-uniform distributions, one implementation of which can be found in [29].

2.2 Collusion Resistance

Many truthful mechanisms suffer from the defect that although no single player has incentive to lie for their own benefit, groups of players can collude to improve each of their utilities, even in the absence of side payments. One fortunate property of differential privacy is that it degrades smoothly with the number of changes in the data set.

Corollary 4 (Collusion Resistance) *For any mechanism $\mathcal{M}$ giving ϵ-differential privacy and any non-negative function g of its range, for any D_1 and D_2 differing on at most t inputs*

$$E[g(\mathcal{M}(D_1))] \quad \leq \quad \exp(\epsilon t) \times E[g(\mathcal{M}(D_2))] \; . \quad (4)$$

Corollary 4 applies to the notable case that g is the sum of the utility functions of t players, ensuring that their collective utility does not increase by much, making the issue of side payments between them irrelevant.

Clearly, $\exp(\epsilon t)$ is larger than $\exp(\epsilon)$, and the resistance to collusions deteriorates as the size of the coalition increases. For coalitions of size less than $1/\epsilon$, the gain is essentially linear in their size. For larger coalitions the change in distribution can be substantial, which we view as a good thing: we will want our mechanisms to react differently to different populations.

Remark: Goldberg and Hartline[19] define t-truthful mechanisms as those for which any group of t agents can not increase their utility by submitting inputs other than their true values. The implementation of Chaudhuri et al. [12] for mechanisms that are truthful with high probability has the more general property of being t-truthful[19] with probability $1 - 2\epsilon t$ for all t.

2.3 Composability

Many mechanisms suffer from problems of repeated application: participants may misrepresent their utilities hoping to influence early rounds so as to lead to more favorable later rounds. As a concrete example, imagine an unlimited supply auction that is rerun daily: clever participants may underbid, hoping to lower the early prices and causing the wealthier bidders to drop out faster, leaving less competition in later rounds. However, any mechanism with differential privacy is robust under composition.

Corollary 5 (Composability) *The sequential application of mechanisms $\{\mathcal{M}_i\}$, each giving $\{\epsilon_i\}$-differential privacy, gives $(\sum_i \epsilon_i)$-differential privacy.*

In the auction above, assuming each instance of the auction mechanism gives ϵ-differential privacy, a single user can skew the seven prices of the week ahead by at most $\exp(7\epsilon)$, even if each instance of the mechanism reacts to the results of previous instances, for example ignoring bidders who have won the good. This assumes the same user data is used for each mechanism. To permit the users to change their bids in each instance of the mechanism, we would need to incorporate the result of Corollary 4.

3 A General Differential Privacy Mechanism

The goal of a privacy mechanism is to map, randomly, a set of n inputs each from a domain $\mathcal{D}$ to some output in a range $\mathcal{R}$. We will make no specific assumptions about the nature of $\mathcal{D}$ or $\mathcal{R}$ other than a base measure μ on $\mathcal{R}$.

The general mechanism we design is driven by an input query function $q : \mathcal{D}^n \times \mathcal{R} \to \mathbb{R}$ that assigns a real valued score to any pair (d, r) from $\mathcal{D}^n \times \mathcal{R}$, with the understanding that higher scores are more appealing.

Given a $d \in \mathcal{D}^n$ the goal of the mechanism is to return an $r \in \mathcal{R}$ such that $q(d, r)$ is (approximately) maximized while guaranteeing differential privacy. We will start from the base measure μ, commonly uniform, and amplify the probability associated with each output by a factor of $\exp(\epsilon q(d, r))$:

Definition 2 *For any function $q : (\mathcal{D}^n \times \mathcal{R}) \to \mathbb{R}$, and base measure μ over $\mathcal{R}$, we define*

$$\mathcal{E}_q^\epsilon(d) \quad := \quad \textit{Choose } r \textit{ with probability proportional to } \exp(\epsilon q(d, r)) \times \mu(r) \ .$$

Intuitively, a small additive change to $q(d, r)$, as might be caused by a single participant, has a limited multiplicative influence on the density of any output, guaranteeing differential privacy. Nonetheless, the probability associated with an output r increases exponentially with its score on the input d, substantially biasing the distribution towards high scoring outputs and bringing the expected score close to the optimum.

Remark: For $\mathcal{E}_q^\epsilon(d)$ to be properly defined we will require $\int_r \exp(\epsilon q(d, r))\mu(r)$ to be bounded. This needn't be the case for general q, ϵ, but in this note all mechanisms will have q bounded by n, bounding the integral by $\exp(\epsilon n)$.

Remark: The work of [15, 14], in which Laplace noise is added to the result of a function $f : \mathcal{D}^n \to \mathbb{R}$, can be captured by taking $q(d, r) = -|f(d) - r|$. Technically, $\mathcal{E}_q^\epsilon$ can capture any differential privacy mechanism M by taking $q(d, r)$ to be the logarithm of the probability density of $M(d)$ at r. While such a transformation does not necessarily provide any additional information about M, except perhaps the function we should expect it to maximize, it assures us that we have captured the full class of differential privacy mechanisms.

3.1 Privacy

For any query function q, we define Δq to be the largest possible difference in the query function when applied to two inputs that differ only on a single user's value, for all r.

Theorem 6 (Privacy) *$\mathcal{E}_q^\epsilon$ gives $(2\epsilon\Delta q)$-differential privacy.*

Proof: The density of $\mathcal{E}_q^\epsilon(d)$ at r is equal to

$$\frac{\exp(\epsilon q(d, r))\mu(r)}{\int \exp(\epsilon q(d, r))\mu(r)dr} \ . \tag{5}$$

A single change in d can change q by at most Δq, giving a factor of at most $\exp(\epsilon\Delta q)$ in the numerator and at least $\exp(-\epsilon\Delta q)$ in the denominator, giving $\exp(2\epsilon\Delta q)$. ■

This result highlights the fact that our mechanisms will be the most useful when Δq is limited. This is a natural assumption in many contexts, described in the coming section. Looking ahead, we will commonly choose q with $\Delta q \leq 1$ so that $\mathcal{E}_q^\epsilon$ ensures (2ϵ)-differential privacy.

Remark: In several cases, such as the unit demand auction settings of the introduction, any change to $\exp(\epsilon q(d,r))\mu(r)$ will necessitate a change in the same direction (increase/decrease) for the normalization factor, strengthening the bound to $(\epsilon\Delta q)$-differential privacy.

3.2 Accuracy

We would like the expected score of a configuration drawn according to $\mathcal{E}_q^\epsilon(d)$ to achieve some value that is nearly the maximum. Intuitively, the exponential bias of $\mathcal{E}_q^\epsilon(d)$ puts configurations with high score at a substantial advantage. Nonetheless, the base measure of high score configurations may be low, counteracting this advantage. Recall the notation $\mu(A)$ for the base measure of set $A \subseteq \mathcal{R}$, normalized so that $\mathcal{R}$ has unit measure, and write $p(A)$ for the measure defined by $\mathcal{E}_q^\epsilon(d)$, again normalized. We write OPT for $\max_r q(d,r)$.

Lemma 7 *Letting $S_t = \{r : q(d,r) > OPT - t\}$, we have $p(\overline{S}_{2t})$ is at most $\exp(-\epsilon t)/\mu(S_t)$.*

Proof: The probability $p(\overline{S}_{2t})$ is at most $p(\overline{S}_{2t})/p(S_t)$, as the new denominator is at most one. As the two probabilities have the same normalizing term, we can write

$$\frac{p(\overline{S}_{2t})}{p(S_t)} = \frac{\int_{\overline{S}_{2t}} \exp(\epsilon q(d,r))\mu(r)dr}{\int_{S_t} \exp(\epsilon q(d,r))\mu(r)dr} \quad (6)$$

$$\leq \exp(-\epsilon t)\frac{\mu(\overline{S}_{2t})}{\mu(S_t)} . \quad (7)$$

As $\mu(\overline{S}_{2t})$ is at most one, we can discard it, arriving at the statement of the theorem. ■

This lemma gives a very strong bound on the probability that the score is less than any given level. Ignoring for the moment the matter of division by $\mu(S_t)$, the deficit from OPT exhibits an exponential tail, and is very unlikely to be substantial.

To lower bound the expected score, we multiply the probability that the output $\mathcal{E}_q^\epsilon(d)$ lies in S_{2t} times $OPT-2t$, a lower bound on its score.

Theorem 8 (Accuracy) *For those values of t satisfying $t \geq \ln(OPT/t\mu(S_t))/\epsilon$, we have $E[q(d,\mathcal{E}_q^\epsilon(d))] \geq OPT - 3t$.*

Proof: Lemma 7 assures score at least $OPT-2t$ with probability at least $1 - \exp(-\epsilon t)/\mu(S_t)$. Our assumption on t makes this probability at least $1-t/OPT$. Multiplying this with $OPT - 2t$ yields the stated bound. ■

This theorem highlights a central parameter: the size of $\mu(S_t)$ as a function of t defines how large we must take t before our exponential bias can overcome the small size of $\mu(S_t)$. In the case of discrete $\mathcal{R}$, a uniform μ makes $\mu(S_t) \geq 1/|\mathcal{R}|$. For continuous $\mathcal{R}$, we must take advantage of the structure of q to provide non-trivial results. In Section 4 we will see several examples that yield interesting results.

4 Applications to Pricing and Auctions

In this section we apply our general mechanism to several problems in unlimited supply auctions and pricing. Although auctions permit offering different prices to different players, all of our results will be single price, and envy-free. Unless otherwise stated, we will assume that μ is uniform over the output space.

4.1 Unlimited Supply Auctions

Imagine we as auctioneers have access to a endless supply of an appealing good, desired by some set of bidders. Each bidder has a demand curve $b_i : [0,1] \to \mathbb{R}^+$ in mind, describing how much of the item they would like at any given price p. We require that the demand be non-increasing with price, and we limit the resources of any one bidder, requiring $pb_i(p) \leq 1$ for all i, p. Note that unit demand is a special case of non-increasing demand.

For each price p, we can sell $\sum_i b_i(p)$ items, yielding $q(b,p) = p\sum_i b_i(p)$ dollars in revenue.

Theorem 9 *Taking $q(b,p) = p\sum_i b_i(p)$, the mechanism $\mathcal{E}_q^\epsilon$ gives 2ϵ-differential privacy, and has expected revenue at least $OPT - 3\ln(e+\epsilon^2 OPT m)/\epsilon$, where m is the number of items sold in OPT.*

Proof: Privacy is seen from Theorem 6, as a bidder can change $q(b,p)$ by at most $pb_i(p) \leq 1$. To prove the bound on expected revenue we will apply Theorem 8 using $t = \ln(e+\epsilon^2 OPT m)/\epsilon$, and must verify that

$$\ln(e+\epsilon^2 OPT m)/\epsilon > \ln(OPT/t\mu(S_t))/\epsilon . \quad (8)$$

First, notice that $t \geq 1/\epsilon$, which implies that

$$\ln(e+\epsilon^2 OPT m)/\epsilon > \ln(OPT m/t^2)/\epsilon . \quad (9)$$

Second, assume without loss of generality that $OPT > t$, as otherwise the bound of $OPT - 3t$ holds trivially. All prices at most t/m less than the optimal price continue to sell at least the same m items (non-increasing demand), at a loss of at most t/m per item. Introducing $\mu(S_t) \geq t/m$ into (9) allows to conclude (8), completing the proof. ■

Theorem 1 follows, as the unit demand case is a special case of a non-increasing demand curve. The factor of two in the privacy guarantee is removed via the reasoning of the remark of Section 3.1.

Remark: There are demand curves in which an agent might like to purchase as many items as possible provided the total cost does not exceed a fixed budget. This challenges the bound above, as there is no *a priori* limit to the number of items sold. We can impose a limit s if we like, as the regret depends only logarithmically on m or impose a minimum price δ, so that no agent wins more than $1/\delta$ items.

4.2 Attribute Auctions

A natural and common extension to the standard auction setting, in which all bidders are *a priori* indistinguishable, is the introduction of public attributes about each of the bidders. For example, bidders may be associated with public information about their state of residence, age, gender, etc. This information can be used to segment the market, offering different prices to different demographics and leading to a larger optimal revenue. This increased flexibility in the optimal solutions leads to challenges for competitive auctions, which must compete with higher revenue over a more complex solution space.

It is not difficult to extend our auction framework to handle attribute auctions: we can still design an output space, consisting of a partitioning of the labels and associated prices for each part, and a revenue function that computes how much each possible set of prices would yield. If there are not terribly many possible segmentations of the bidders, perhaps as guaranteed by a low VC-dimension, and we do not segment into terribly many markets, our mechanism will be assured to find a configuration with nearly optimal revenue.

In the results that follow, we write OPT_k for the optimal revenue with the markets segmented into k parts and SEG_k for the number of permitted segmentations of the n users into k markets. Sauer's Lemma[36] bounds $SEG_k \leq n^{kVC}$, where VC denotes the VC dimension of the permissable segmentations of the attribute space, but we stay with the use of SEG_k as a more accurate bound. Note that μ is now the uniform measure over the permitted segmentations and offered prices.

Theorem 10 *Taking q to be the revenue function over segmentations into k markets and their prices, $\mathcal{E}_q^\epsilon$ has expected revenue is at least $OPT_k - 3(\ln(e + \epsilon^{k+1} OPT_k SEG_k m^k))/\epsilon$.*

Proof: As the attributes are public and available *a priori*, our mechanism can restrict itself to the SEG_k possible segmentations of users. The base measure of S_t is then at least the measure in the optimal segmentation, which is $(t/m)^k$ divided by the number of segmentations SEG_k. The bound follows in the same manner as for the $k = 1$ case, taking $t = \ln(e + \epsilon^{k+1} OPT_k SEG_k m^k)/\epsilon$. ■

Rather than fix a number of markets beforehand, we can let this parameter change as needed, taking care to be suspicious of large values of k. By setting the base measure of each segmentation proportional to $1/nSEG_k$, we arrive at a result with the flavor of structural risk minimization:

Theorem 11 *Taking q to be the revenue function over segmentations into arbitrary markets and their prices, $\mathcal{E}_q^\epsilon$, and taking the base measure of each segmentation into k markets to be $1/nSEG_k$, the expected revenue is at least $\max_k(OPT_k - 3(\ln(e + \epsilon^{k+1} OPT_k SEG_k n m^k))/\epsilon)$.*

Proof: The optimal segmentation, say into k markets, has base measure exactly $1/nSEG_k$. S_t restricted to this segmentation has base measure at least $(t/m)^k/nSEG_k$, and taking $t = \ln(e+\epsilon^{k+1} OPT_k SEG_k n m^k)/\epsilon$ gives the stated bound. ■

Theorem 2 follows, as the unit demand case is a special case of a non-increasing demand curve. The factor of two is removed via the reasoning of the remark of Section 3.1.

4.3 Constrained Pricing Problems

Other types of auctions problems have been proposed whose solutions have somewhat delicate structures. Consider the problem of the independent film theater, who must choose which single film of many to run each weekend. The theater can solicit bids from its patrons on different films, but is ultimately constrained to run only a single film, and can only expect to collect revenue from bids for that film.

This is a special case of a multi-parameter problem, where bidders come in with a bid for each of k different kinds of items, and the mechanism is constrained to sell at most one kind of item at a fixed price. Each bidder has a demand curve $b_i^j : [0,1] \to \mathbb{R}^+$ for each item $j \in [k]$. As in the case of single item auction, we require that the demand be non-increasing with price and limit the endowment of each bidder so that $pb_i^j(p) \leq 1$ for each i, j, p. Here $\mathcal{R}$ is $[k] \times \mathbb{R}$. For each item j, at price p, we can sell $\sum_i b_i^j(p)$ items, yielding a revenue $q(b,(j,p)) = p \sum_i b_i^j(p)$.

Theorem 12 *Taking $q(b,(j,p)) = p \sum_i b_i^j(p)$, $\mathcal{E}_q^\epsilon$ gives 2ϵ-differential privacy, and has expected revenue at least $OPT - 3\ln(e + \epsilon^2 OPT km)/\epsilon$, where m is the number of items sold in OPT.*

Proof: Privacy is seen from Theorem 6, as a bidder can change $q(b,(j,p))$ by at most $pb_i^j(p) \leq 1$. The bound on expected revenue follows using the same ideas from the proof of Theorem 9. ■

We note that more general constraints can be easily accommodated: one can imagine settings where a small number of items may be produced, and priced differently, or

different items could be made available to different market segments. Hard constraints of this form are naturally accommodated by restricting the space of solutions (eg: to prices where all but one are infinite), and defining a revenue function on this space. Other approaches such as cross training [6], where the bidders are partitioned and the optimal strategy for each group is applied to the other, do not necessarily meet the hard structural constraint.

4.4 General Mechanism Design Problems

It is natural to expect that this general mechanism can be applied more broadly to other mechanism design problems. Pricing problems have the property that their outcome space is of low dimensionality, which leads to non-trivial base measure around the optimal solution. In other contexts where there are many near-optimal solutions relative to the number of total solutions, the logarithm of the base measure will be small, and the revenue will be nearly optimal.

Notice that the revenue can be replaced with any other objective function; for example social welfare is a natural choice in certain settings.

As shown by Mu'alem and Nisan [31], an algorithm that takes the MAX of one or more monotone algorithms is not necessarily monotone, and thus not truthful. They show certain conditions under which the MAX operator is monotone, and use it to design truthful approximately efficient mechanisms for certain combinatorial auctions. We can model this as the problem of selecting one algorithm from a discrete set, and apply the mechanisms $\mathcal{E}_q^\epsilon$ where $q(d, r)$ is the revenue/welfare of algorithm r on d. Thus the MAX operator can in fact be implemented (approximately) truthfully, with strong guarantees on the efficiency of the outcome.

5 Conclusions and Future Research

We have seen how Differential Privacy extends beyond disclosure limitation to give broad game theoretic guarantees, including approximate truthfulness, collusion resistance, and repeatable play. These guarantees come with the caveat that they are approximate: incentives are present, though arbitrarily small as controlled by the parameter ϵ.

We have also introduced a new general mechanism with differential privacy that comes with guarantees about the quality of the output, even for functions that are not robust to additive noise, and those whose output may not even permit perturbation. This mechanism skews a base measure to the largest degree possible while ensuring differential privacy, focusing probability on the outputs of highest value.

Finally, we applied this general mechanism to several auction problems, yielding revenue that is within an additive logarithmic term of optimal. We stress that unlike some previous work, eg [6], our mechanism is not strictly truthful. On the other hand, we have shown several constrained pricing settings where our mechanism can be applied directly, but prior works such as [6] are unable to maintain the hard structural constraints.

Future Directions One direction that went underdeveloped in this work is the issue of efficiently sampling from the exponentially weighted distributions we define. We are only aware of efficient algorithms in the case where the query function q has very constrained structure, *e. g.* piecewise linear, or in the cases where the output space can be effectively discretized. Even managing the weights once constructed taxes modern computers, which restrict their values to roughly 10^{100}, whereas we can quite casually define distributions using much larger values. We refer the reader to [29] for an algorithmic approach that operates strictly with logarithms, and implements the strong truthfulness of [12], but still uses brute-force examination of each element in the range.

An additional computational challenge we face is the exact computation of $q(d, r)$ in cases where the optimization is not known to be computationally efficient. In such settings, we would like to use approximation algorithms in place of the inefficient exact computation, but we face the challenge of finding approximation algorithms that have small values of Δq. That is, the approximations themselves should also be insensitive to changes in the values of few inputs. Most natural approximation algorithms do not seem to have this property. Halevi et al. [22] show that private approximation can be hard, but use a stronger privacy requirement than we need: that instances with the same set of optimal solutions yield the same output.

Of course, extending the scope of our mechanisms to other mechanisms design settings remains an interesting challenge whose potential is unknown.

6 Acknowledgements

The authors would like to graciously acknowledge Jason Hartline, who several years back asserted that there must be a connection between truth-telling and privacy-preserving, and more recently highlighted constrained pricing problems as one of the notable applications of our work. We would also like to thank Udi Wieder, whose comments helped to substantially improve this paper's presentation.

References

[1] N. R. Adam and J. C. Wortmann. Security-control methods for statistical databases: A comparative study. *ACM Comput. Surv.*, 21(4):515–556, 1989.

[2] G. Aggarwal, A. Fiat, A. V. Goldberg, J. D. Hartline, N. Immorlica, and M. Sudan. Derandomization of auctions. In H. N. Gabow and R. Fagin, editors, *STOC*, pages 619–625. ACM, 2005.

[3] A. Archer, C. Papadimitriou, K. Talwar, and É. Tardos. An approximate truthful mechanism for combinatorial auctions with single parameter agents. In *SODA '03: Proceedings of the fourteenth annual ACM-SIAM symposium on Discrete algorithms*, pages 205–214, Philadelphia, PA, USA, 2003. Society for Industrial and Applied Mathematics.

[4] A. Archer and É. Tardos. Frugal path mechanisms. In *SODA '02: Proceedings of the thirteenth annual ACM-SIAM symposium on Discrete algorithms*, pages 991–999, Philadelphia, PA, USA, 2002. Society for Industrial and Applied Mathematics.

[5] M. Babaioff, R. Lavi, and E. Pavlov. Single-value combinatorial auctions and implementation in undominated strategies. In *SODA '06: Proceedings of the seventeenth annual ACM-SIAM symposium on Discrete algorithm*, pages 1054–1063, New York, NY, USA, 2006. ACM Press.

[6] M.-F. Balcan, A. Blum, J. D. Hartline, and Y. Mansour. Mechanism design via machine learning. In *FOCS*, pages 605–614. IEEE Computer Society, 2005.

[7] Z. Bar-Yossef, K. Hildrum, and F. Wu. Incentive-compatible online auctions for digital goods. In *SODA*, pages 964–970, 2002.

[8] S. Bikhchandani, S. Chatterji, R. Lavi, A. Mu'alem, N. Nisan, , and A. Sen. Weak monotonicity characterizes deterministic dominant strategy implementation. *Econometrica*, 74(4):1109–1132, 2006.

[9] A. Blum, C. Dwork, F. McSherry, and K. Nissim. Practical privacy: the SuLQ framework. In C. Li, editor, *PODS*, pages 128–138. ACM, 2005.

[10] A. Blum and J. D. Hartline. Near-optimal online auctions. In *SODA*, pages 1156–1163, 2005.

[11] A. Blum, V. Kumar, A. Rudra, and F. Wu. Online learning in online auctions. *Theor. Comput. Sci.*, 324(2-3):137–146, 2004.

[12] K. Chaudhuri, S. Kale, F. McSherry, and K. Talwar. From differential privacy to privacy with high probability. Manuscript, 2007.

[13] A. Czumaj and A. Ronen. On the expected payment of mechanisms for task allocation. In S. Chaudhuri and S. Kutten, editors, *PODC*, pages 98–106. ACM, 2004.

[14] C. Dwork. Differential privacy. In M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, editors, *ICALP (2)*, volume 4052 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2006.

[15] C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In S. Halevi and T. Rabin, editors, *TCC*, volume 3876 of *Lecture Notes in Computer Science*, pages 265–284. Springer, 2006.

[16] E. Elkind, A. Sahai, and K. Steiglitz. Frugality in path auctions. In *SODA '04: Proceedings of the fifteenth annual ACM-SIAM symposium on Discrete algorithms*, pages 701–709, Philadelphia, PA, USA, 2004. Society for Industrial and Applied Mathematics.

[17] U. Feige, A. Flaxman, J. D. Hartline, and R. D. Kleinberg. On the competitive ratio of the random sampling auction. In X. Deng and Y. Ye, editors, *WINE*, volume 3828 of *Lecture Notes in Computer Science*, pages 878–886. Springer, 2005.

[18] J. Feigenbaum and S. Shenker. Distributed algorithmic mechanism design: Recent results and future directions. In *Proceedings of the 6th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications*, pages 1–13. ACM Press, 2002.

[19] A. V. Goldberg and J. D. Hartline. Competitiveness via consensus. In *SODA*, pages 215–222, 2003.

[20] A. V. Goldberg and J. D. Hartline. Collusion-resistant mechanisms for single-parameter agents. In *SODA*, pages 620–629, 2005.

[21] A. V. Goldberg, J. D. Hartline, and A. Wright. Competitive auctions and digital goods. In *SODA*, pages 735–744, 2001.

[22] S. Halevi, R. Krauthgamer, E. Kushilevitz, and K. Nissim. Private approximation of NP-hard functions. In *ACM Symposium on Theory of Computing*, pages 550–559, 2001.

[23] J. D. Hartline and R. McGrew. From optimal limited to unlimited supply auctions. In J. Riedl, M. J. Kearns, and M. K. Reiter, editors, *ACM Conference on Electronic Commerce*, pages 175–182. ACM, 2005.

[24] N. Immorlica, D. Karger, E. Nikolova, and R. Sami. First-price path auctions. In *EC '05: Proceedings of the 6th ACM conference on Electronic commerce*, pages 203–212, New York, NY, USA, 2005. ACM Press.

[25] R. D. Kleinberg and F. T. Leighton. The value of knowing a demand curve: Bounds on regret for online posted-price auctions. In *FOCS*, pages 594–605. IEEE Computer Society, 2003.

[26] A. Kothari, D. C. Parkes, and S. Suri. Approximately-strategyproof and tractable multiunit auctions. *Decis. Support Syst.*, 39(1):105–121, 2005.

[27] R. Lavi, A. Mu'alem, and N. Nisan. Towards a characterization of truthful combinatorial auctions. In *FOCS '03: Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science*, page 574, Washington, DC, USA, 2003. IEEE Computer Society.

[28] R. Lavi and N. Nisan. Online ascending auctions for gradually expiring items. In *SODA '05: Proceedings of the sixteenth annual ACM-SIAM symposium on Discrete algorithms*, pages 1146–1155, Philadelphia, PA, USA, 2005. Society for Industrial and Applied Mathematics.

[29] M. Manasse, F. McSherry, and K. Talwar. Consistent weighted sampling. Submitted, 2008.

[30] A. Mas-Colell, M. D. Whinston, and J. R. Green. *Microeconomic Theory*. Oxford University Press, 1995.

[31] A. Mu'alem and N. Nisan. Truthful approximation mechanisms for restricted combinatorial auctions. In *AAAI/IAAI*, pages 379–384, 2002.

[32] N. Nisan and A. Ronen. Algorithmic mechanism design (extended abstract). In *STOC*, pages 129–140, 1999.

[33] K. Nissim, S. Raskhodnikova, and A. Smith. Smooth sensitivity and sampling in private data analysis. In D. S. Johnson and U. Feige, editors, *STOC*, pages 75–84. ACM, 2007.

[34] D. C. Parkes. ibundle: an efficient ascending price bundle auction. In *EC '99: Proceedings of the 1st ACM conference on Electronic commerce*, pages 148–157, New York, NY, USA, 1999. ACM Press.

[35] M. Saks and L. Yu. Weak monotonicity suffices for truthfulness on convex domains. In *EC '05: Proceedings of the 6th ACM conference on Electronic commerce*, pages 286–293, New York, NY, USA, 2005. ACM Press.

[36] N. Sauer. On the density of families of sets. *J. Combinatorial Theory (A)*, 13:145–147, 1972.

[37] J. Schummer. Almost-dominant strategy implementation. *Games and Economic Behavior*, 48:154–170, 2004.