Mechanism Design via Differential Privacy

Aaron Roth

University of Pennsylvania

April 22 2021

Overview

- We'll have one final lecture using digital goods auctions as a testbed for techniques in mechanism design.

Overview

- We'll have one final lecture using digital goods auctions as a testbed for techniques in mechanism design.
- Recall two lectures ago: we designed a dominant strategy truthful auction that for any vector of valuations v, obtained revenue:

$$Rev(v) \geq \mathrm{OPT}(v) - O(\sqrt{n})$$

where $\mathrm{OPT}_v = \max_{p \in [0,1]} p \cdot |\{i : v_i \geq p\}|$.

Overview

- We'll have one final lecture using digital goods auctions as a testbed for techniques in mechanism design.
- Recall two lectures ago: we designed a dominant strategy truthful auction that for any vector of valuations v, obtained revenue:
$$Rev(v) \geq \mathrm{OPT}(v) - O(\sqrt{n})$$
where $\mathrm{OPT}_v = \max_{p \in [0,1]} p \cdot |\{i : v_i \geq p\}|$.
- This class: we will relax our solution concept to *asymptotic* dominant strategy truthfulness, and try to obtain a better revenue guarantee.

Overview

- We'll have one final lecture using digital goods auctions as a testbed for techniques in mechanism design.
- Recall two lectures ago: we designed a dominant strategy truthful auction that for any vector of valuations v, obtained revenue:
$$Rev(v) \geq \mathrm{OPT}(v) - O(\sqrt{n})$$
where $\mathrm{OPT}_v = \max_{p\in[0,1]} p \cdot |\{i : v_i \geq p\}|$.
- This class: we will relax our solution concept to *asymptotic* dominant strategy truthfulness, and try to obtain a better revenue guarantee.
- Our tool: Differential privacy, a technique developed for protecting user privacy in data analysis.

Approach

- Recall: Why can we not simply compute the price $p^* = \arg\max_{p \in [0,1]} p \cdot |\{i : v_i \geq p\}|$ and charge that?

Approach

- Recall: Why can we not simply compute the price $p^* = \arg\max_{p \in [0,1]} p \cdot |\{i : v_i \geq p\}|$ and charge that?
- This price will be highly manipulable by (at least) one of the bidders – $p^* = v_{i^*}$ for some bidder i^*, who will have strong incentive to change his bid.

Approach

- Recall: Why can we not simply compute the price $p^* = \arg\max_{p\in[0,1]} p \cdot |\{i : v_i \geq p\}$ and charge that?
- This price will be highly manipulable by (at least) one of the bidders – $p^* = v_{i^*}$ for some bidder i^*, who will have strong incentive to change his bid.
- So to get dominant strategy truthfulness, we needed to compute prices that were independent of bidder reports.

Approach

- Recall: Why can we not simply compute the price $p^* = \arg\max_{p \in [0,1]} p \cdot |\{i : v_i \geq p\}|$ and charge that?
- This price will be highly manipulable by (at least) one of the bidders – $p^* = v_{i^*}$ for some bidder i^*, who will have strong incentive to change his bid.
- So to get dominant strategy truthfulness, we needed to compute prices that were independent of bidder reports.
- But what if we could compute a price p that is *almost* independent of the reported valuation v_i for every buyer i?

Approach

- Recall: Why can we not simply compute the price $p^* = \arg\max_{p \in [0,1]} p \cdot |\{i : v_i \geq p\}|$ and charge that?
- This price will be highly manipulable by (at least) one of the bidders – $p^* = v_{i^*}$ for some bidder i^*, who will have strong incentive to change his bid.
- So to get dominant strategy truthfulness, we needed to compute prices that were independent of bidder reports.
- But what if we could compute a price p that is *almost* independent of the reported valuation v_i for every buyer i?
- Will this yield in some sense an approximate truthfulness guarantee? This will be the idea behind our approach.

Privacy Definitions

Definition

Two bid vectors $v, v' \in [0,1]^n$ are *neighbors* if they differ in just a single agent's bid: i.e. if there exists an index i such that $v_j = v'_j$ for every index $j \neq i$.

Privacy Definitions

Definition

Two bid vectors $v, v' \in [0,1]^n$ are *neighbors* if they differ in just a single agent's bid: i.e. if there exists an index i such that $v_j = v'_j$ for every index $j \neq i$.

We can now define differential privacy:

Definition

A mechanism $M : [0,1]^n \to \mathcal{O}$ is ϵ-differentially private if for every pair of neighboring bid vectors $v, v' \in [0,1]^n$, and for every outcome $x \in \mathcal{O}$:

$$\Pr[M(v) = x] \leq \exp(\epsilon) \Pr[M(v') = x]$$

.

Privacy Definitions

Definition

Two bid vectors $v, v' \in [0,1]^n$ are *neighbors* if they differ in just a single agent's bid: i.e. if there exists an index i such that $v_j = v'_j$ for every index $j \neq i$.

We can now define differential privacy:

Definition

A mechanism $M : [0,1]^n \to \mathcal{O}$ is ϵ-differentially private if for every pair of neighboring bid vectors $v, v' \in [0,1]^n$, and for every outcome $x \in \mathcal{O}$:

$$\Pr[M(v) = x] \leq \exp(\epsilon) \Pr[M(v') = x]$$

.

Here you should think of $\epsilon < 1$ as a small constant, and think of $\exp(\epsilon) \approx (1+\epsilon)$. For $\epsilon \leq 1$ we have:

$$1 + \epsilon \leq \exp(\epsilon) \leq 1 + 2\epsilon$$

Approximate Truthfulness

We can also define what we mean by *approximate* dominant strategy truthfulness:

Approximate Truthfulness

We can also define what we mean by *approximate* dominant strategy truthfulness:

Definition

A mechanism $M : [0,1]^n \rightarrow \mathcal{O}$ is ϵ-approximately dominant strategy truthful if for every bidder i, every utility function $u_i : [0,1] \times \mathcal{O} \rightarrow [0,1]$, every vector of valuations $v \in [0,1]^n$, and every deviation $v'_i \in [0,1]$, if we write $v' = (v_{-i}, v'_i)$, then:

$$\mathrm{E}_{o \sim M(v)}[u_i(v_i, o)] \geq \mathrm{E}_{o \sim M(v')}[u_i(v_i, o)] - \epsilon$$

Approximate Truthfulness

We can also define what we mean by *approximate* dominant strategy truthfulness:

Definition

A mechanism $M : [0,1]^n \rightarrow \mathcal{O}$ is ϵ-approximately dominant strategy truthful if for every bidder i, every utility function $u_i : [0,1] \times \mathcal{O} \rightarrow [0,1]$, every vector of valuations $v \in [0,1]^n$, and every deviation $v'_i \in [0,1]$, if we write $v' = (v_{-i}, v'_i)$, then:

$$\mathrm{E}_{o \sim M(v)}[u_i(v_i, o)] \geq \mathrm{E}_{o \sim M(v')}[u_i(v_i, o)] - \epsilon$$

In other words, we require that no bidder can *substantially* (by more than ϵ) increase his utility by mis-reporting his valuation.

The Connection

Differential privacy will be useful for us because differentially private mechanisms are automatically ϵ-approximately dominant strategy truthful.

The Connection

Differential privacy will be useful for us because differentially private mechanisms are automatically ϵ-approximately dominant strategy truthful.

Theorem

If a mechanism $M : [0,1]^n \to \mathcal{O}$ *is* ϵ*-differentially private, then* M *is also* ϵ*-approximately dominant strategy truthful.*

The Connection: Proof

Fix any buyer i, valuation vector v, and utility function $u_i : [0,1] \times \mathcal{O} \to [0,1]$.

The Connection: Proof

Fix any buyer i, valuation vector v, and utility function $u_i : [0,1] \times \mathcal{O} \to [0,1]$.

$$\mathrm{E}_{o \sim M(v)}[u_i(v_i, o)] \quad = \quad \sum_{o \in \mathcal{O}} u_i(v_i, o) \cdot \Pr[M(v) = o]$$

The Connection: Proof

Fix any buyer i, valuation vector v, and utility function $u_i : [0,1] \times \mathcal{O} \to [0,1]$.

$$\begin{aligned} \mathrm{E}_{o \sim M(v)}[u_i(v_i, o)] &= \sum_{o \in \mathcal{O}} u_i(v_i, o) \cdot \Pr[M(v) = o] \\ &\geq \sum_{o \in \mathcal{O}} u_i(v_i, o) \cdot \exp(-\epsilon) \Pr[M(v') = o] \end{aligned}$$

The Connection: Proof

Fix any buyer i, valuation vector v, and utility function $u_i : [0,1] \times \mathcal{O} \to [0,1]$.

$$\begin{aligned}
\mathrm{E}_{o \sim M(v)}[u_i(v_i, o)] &= \sum_{o \in \mathcal{O}} u_i(v_i, o) \cdot \Pr[M(v) = o] \\
&\geq \sum_{o \in \mathcal{O}} u_i(v_i, o) \cdot \exp(-\epsilon) \Pr[M(v') = o] \\
&= exp(-\epsilon) \mathrm{E}_{o \sim M(v')}[u_i(v_i, o)]
\end{aligned}$$

The Connection: Proof

Fix any buyer i, valuation vector v, and utility function $u_i : [0,1] \times \mathcal{O} \rightarrow [0,1]$.

$$
\begin{aligned}
\mathrm{E}_{o \sim M(v)}[u_i(v_i, o)] &= \sum_{o \in \mathcal{O}} u_i(v_i, o) \cdot \Pr[M(v) = o] \\
&\geq \sum_{o \in \mathcal{O}} u_i(v_i, o) \cdot \exp(-\epsilon) \Pr[M(v') = o] \\
&= exp(-\epsilon) \mathrm{E}_{o \sim M(v')}[u_i(v_i, o)] \\
&\geq \mathrm{E}_{o \sim M(v')}[u_i(v_i, o)] - \epsilon
\end{aligned}
$$

The Connection: Proof

Fix any buyer i, valuation vector v, and utility function $u_i : [0,1] \times \mathcal{O} \rightarrow [0,1]$.

$$\begin{aligned}
\mathrm{E}_{o \sim M(v)}[u_i(v_i, o)] &= \sum_{o \in \mathcal{O}} u_i(v_i, o) \cdot \Pr[M(v) = o] \\
&\geq \sum_{o \in \mathcal{O}} u_i(v_i, o) \cdot \exp(-\epsilon) \Pr[M(v') = o] \\
&= exp(-\epsilon) \mathrm{E}_{o \sim M(v')}[u_i(v_i, o)] \\
&\geq \mathrm{E}_{o \sim M(v')}[u_i(v_i, o)] - \epsilon
\end{aligned}$$

The last inequality follows because for $\epsilon < 1$, $\exp(-\epsilon) \geq 1 - \epsilon$, and $u_i(v_i, o) \leq 1$.

Exploiting the Connection

- So: to design an approximately truthful mechanism that guarantees high revenue, it is sufficient to design a differentially private mechanism with high revenue.

Exploiting the Connection

- So: to design an approximately truthful mechanism that guarantees high revenue, it is sufficient to design a differentially private mechanism with high revenue.
- Lets try a straightforward approach: directly picking a price that approximately maximizes revenue for the reported bidder valuations.

Exploiting the Connection

- So: to design an approximately truthful mechanism that guarantees high revenue, it is sufficient to design a differentially private mechanism with high revenue.
- Lets try a straightforward approach: directly picking a price that approximately maximizes revenue for the reported bidder valuations.
- As in the last two lectures, lets pick a finite subset of prices $P \subset [0, 1]$ to select from.

Consider the following mechanism (an instantiation of what is called “the exponential mechanism” in its more general form):

Consider the following mechanism (an instantiation of what is called "the exponential mechanism" in its more general form):
ExpMech(v, ϵ, P):

Define $\mathrm{Rev}(p, v) = p \cdot |\{i : v_i \geq p\}|$.
Output each $p \in P$ according to the following probability distribution:

$$\Pr[p] = \frac{1}{\phi(v)} \exp\left(\frac{\epsilon \cdot Rev(p, v)}{2}\right)$$

where

$$\phi(v) = \sum_{p \in P} \exp\left(\frac{\epsilon \cdot Rev(p, v)}{2}\right)$$

Privacy/Truthfulness

Theorem

For any ϵ, P: ExpMech$(\cdot, \epsilon, P)$ is ϵ-differentially private.

Privacy/Truthfulness

Theorem

For any ϵ, P: ExpMech$(\cdot, \epsilon, P)$ is ϵ-differentially private. (and thus ϵ-approximately dominant strategy truthful)

Proof

Fix any pair of neighboring bid vectors v, v' and any output p. We have:

Proof

Fix any pair of neighboring bid vectors v, v' and any output p. We have:

$$\Pr[EM(v, \epsilon, P) = p] = \frac{1}{\phi(v)} \exp\left(\frac{\epsilon \cdot Rev(p, v)}{2}\right)$$

Proof

Fix any pair of neighboring bid vectors v, v' and any output p. We have:

$$\begin{aligned}
\Pr[EM(v, \epsilon, P) = p] &= \frac{1}{\phi(v)} \exp\left(\frac{\epsilon \cdot Rev(p, v)}{2}\right) \\
&\leq \frac{1}{\phi(v)} \exp\left(\frac{\epsilon \cdot (Rev(p, v') + 1)}{2}\right)
\end{aligned}$$

Proof

Fix any pair of neighboring bid vectors v, v' and any output p. We have:

$$\begin{aligned}
\Pr[EM(v,\epsilon,P)=p] &= \frac{1}{\phi(v)}\exp\left(\frac{\epsilon\cdot Rev(p,v)}{2}\right)\\
&\leq \frac{1}{\phi(v)}\exp\left(\frac{\epsilon\cdot(Rev(p,v')+1)}{2}\right)\\
&= \frac{1}{\phi(v)}\exp\left(\frac{\epsilon}{2}\right)\exp\left(\frac{\epsilon\cdot Rev(p,v')}{2}\right)
\end{aligned}$$

Proof

Fix any pair of neighboring bid vectors v, v' and any output p. We have:

$$
\begin{aligned}
\Pr[EM(v, \epsilon, P) = p] &= \frac{1}{\phi(v)} \exp\left(\frac{\epsilon \cdot Rev(p, v)}{2}\right) \\
&\leq \frac{1}{\phi(v)} \exp\left(\frac{\epsilon \cdot (Rev(p, v') + 1)}{2}\right) \\
&= \frac{1}{\phi(v)} \exp\left(\frac{\epsilon}{2}\right) \exp\left(\frac{\epsilon \cdot Rev(p, v')}{2}\right) \\
&\leq \exp\left(\frac{\epsilon}{2}\right) \frac{1}{\phi(v')} \exp\left(\frac{\epsilon}{2}\right) \exp\left(\frac{\epsilon \cdot Rev(p, v')}{2}\right)
\end{aligned}
$$

Proof

Fix any pair of neighboring bid vectors v, v' and any output p. We have:

$$
\begin{aligned}
\Pr[EM(v, \epsilon, P) = p] &= \frac{1}{\phi(v)} \exp\left(\frac{\epsilon \cdot Rev(p, v)}{2}\right) \\
&\leq \frac{1}{\phi(v)} \exp\left(\frac{\epsilon \cdot (Rev(p, v') + 1)}{2}\right) \\
&= \frac{1}{\phi(v)} \exp\left(\frac{\epsilon}{2}\right) \exp\left(\frac{\epsilon \cdot Rev(p, v')}{2}\right) \\
&\leq \exp\left(\frac{\epsilon}{2}\right) \frac{1}{\phi(v')} \exp\left(\frac{\epsilon}{2}\right) \exp\left(\frac{\epsilon \cdot Rev(p, v')}{2}\right) \\
&= \exp(\epsilon) \Pr[EM(v', \epsilon, P) = p]
\end{aligned}
$$

And Revenue...

Theorem

For any P, v, ϵ, δ, with probability $1-\delta$, ExpMech(v, ϵ, P) outputs a price p such that:

$$Rev(p, v) \geq \max_{p^* \in P} Rev(p^*, v) - \frac{2}{\epsilon} \cdot \ln\left(\frac{|P|}{\delta}\right)$$

Proof

Let $p^* = \max_{p^* \in P} Rev(p^*, v)$. For any value x, we have:

Proof

Let $p^* = \max_{p^* \in P} Rev(p^*, v)$. For any value x, we have:

$$\Pr_p[Rev(p, v) \leq x] \quad \leq \quad \frac{\Pr_p[Rev(p, v) \leq x]}{\Pr_p[Rev(p, v) = Rev(p^*, v)]}$$

Proof

Let $p^* = \max_{p^* \in P} Rev(p^*, v)$. For any value x, we have:

$$\begin{aligned}
\Pr_p[Rev(p, v) \leq x] &\leq \frac{\Pr_p[Rev(p, v) \leq x]}{\Pr_p[Rev(p, v) = Rev(p^*, v)]} \\
&\leq \frac{|P| \cdot \exp(\epsilon x/2)}{\exp(\epsilon Rev(p^*, v)/2)}
\end{aligned}$$

Proof

Let $p^* = \max_{p^* \in P} Rev(p^*, v)$. For any value x, we have:

$$\begin{aligned}
\Pr_p[Rev(p,v) \le x] &\le \frac{\Pr_p[Rev(p,v) \le x]}{\Pr_p[Rev(p,v) = Rev(p^*,v)]} \\
&\le \frac{|P| \cdot \exp(\epsilon x/2)}{\exp(\epsilon Rev(p^*,v)/2)} \\
&= |P| \cdot \exp\left(\frac{\epsilon \cdot (x - Rev(p^*,v))}{2}\right)
\end{aligned}$$

Proof

Let $p^* = \max_{p^* \in P} Rev(p^*, v)$. For any value x, we have:

$$\begin{aligned}
\Pr_p[Rev(p, v) \le x] &\le \frac{\Pr_p[Rev(p, v) \le x]}{\Pr_p[Rev(p, v) = Rev(p^*, v)]} \\
&\le \frac{|P| \cdot \exp(\epsilon x/2)}{\exp(\epsilon Rev(p^*, v)/2)} \\
&= |P| \cdot \exp\left(\frac{\epsilon \cdot (x - Rev(p^*, v))}{2}\right)
\end{aligned}$$

Now choose $x = Rev(p^*, v) - \frac{2}{\epsilon} \cdot \ln\left(\frac{|P|}{\delta}\right)$. Plugging that in above, we get:

Proof

Let $p^* = \max_{p^* \in P} Rev(p^*, v)$. For any value x, we have:

$$
\begin{aligned}
\Pr_p[Rev(p,v) \le x] &\le \frac{\Pr_p[Rev(p,v) \le x]}{\Pr_p[Rev(p,v) = Rev(p^*,v)]} \\
&\le \frac{|P| \cdot \exp(\epsilon x/2)}{\exp(\epsilon Rev(p^*,v)/2)} \\
&= |P| \cdot \exp\left(\frac{\epsilon \cdot (x - Rev(p^*,v))}{2}\right)
\end{aligned}
$$

Now choose $x = Rev(p^*, v) - \frac{2}{\epsilon} \cdot \ln\left(\frac{|P|}{\delta}\right)$. Plugging that in above, we get:

$$
\Pr_p[Rev(p,v) \le x] \le |P| \cdot \exp\left(-\ln\left(\frac{|P|}{\delta}\right)\right)
$$

Proof

Let $p^* = \max_{p^* \in P} Rev(p^*, v)$. For any value x, we have:

$$\begin{aligned}
\Pr_p[Rev(p,v) \le x] &\le \frac{\Pr_p[Rev(p,v) \le x]}{\Pr_p[Rev(p,v) = Rev(p^*,v)]} \\
&\le \frac{|P| \cdot \exp(\epsilon x/2)}{\exp(\epsilon Rev(p^*,v)/2)} \\
&= |P| \cdot \exp\left(\frac{\epsilon \cdot (x - Rev(p^*,v))}{2}\right)
\end{aligned}$$

Now choose $x = Rev(p^*, v) - \frac{2}{\epsilon} \cdot \ln\left(\frac{|P|}{\delta}\right)$. Plugging that in above, we get:

$$\begin{aligned}
\Pr_p[Rev(p,v) \le x] &\le |P| \cdot \exp\left(-\ln\left(\frac{|P|}{\delta}\right)\right) \\
&= |P| \cdot \frac{\delta}{|P|}
\end{aligned}$$

Proof

Let $p^* = \max_{p^* \in P} Rev(p^*, v)$. For any value x, we have:

$$\begin{aligned}
\Pr_p[Rev(p, v) \leq x] &\leq \frac{\Pr_p[Rev(p, v) \leq x]}{\Pr_p[Rev(p, v) = Rev(p^*, v)]} \\
&\leq \frac{|P| \cdot \exp(\epsilon x/2)}{\exp(\epsilon Rev(p^*, v)/2)} \\
&= |P| \cdot \exp\left(\frac{\epsilon \cdot (x - Rev(p^*, v))}{2}\right)
\end{aligned}$$

Now choose $x = Rev(p^*, v) - \frac{2}{\epsilon} \cdot \ln\left(\frac{|P|}{\delta}\right)$. Plugging that in above, we get:

$$\begin{aligned}
\Pr_p[Rev(p, v) \leq x] &\leq |P| \cdot \exp\left(-\ln\left(\frac{|P|}{\delta}\right)\right) \\
&= |P| \cdot \frac{\delta}{|P|} \\
&= \delta
\end{aligned}$$

Putting it all Together

- We have: an approximately truthful way to select a revenue maximizing price from a finite set of prices P, with revenue guarantees with respect to the best price in P that degrade with $|P|$.

Putting it all Together

- We have: an approximately truthful way to select a revenue maximizing price from a finite set of prices P, with revenue guarantees with respect to the best price in P that degrade with $|P|$.
- This is a familiar tradeoff.

Putting it all Together

- We have: an approximately truthful way to select a revenue maximizing price from a finite set of prices P, with revenue guarantees with respect to the best price in P that degrade with $|P|$.
- This is a familiar tradeoff.
- Now our dependence on $|P|$ is only logarithmic...

Putting it all Together

- We have: an approximately truthful way to select a revenue maximizing price from a finite set of prices P, with revenue guarantees with respect to the best price in P that degrade with $|P|$.
- This is a familiar tradeoff.
- Now our dependence on $|P|$ is only logarithmic...
- Lets again see what happens when we take the natural discretization:

$$P = \{\alpha, 2\alpha, 3\alpha, \ldots, 1\}$$

Putting it all Together

- We have: an approximately truthful way to select a revenue maximizing price from a finite set of prices P, with revenue guarantees with respect to the best price in P that degrade with $|P|$.
- This is a familiar tradeoff.
- Now our dependence on $|P|$ is only logarithmic...
- Lets again see what happens when we take the natural discretization:

$$P = \{\alpha, 2\alpha, 3\alpha, \ldots, 1\}$$

- Just as before, $|P| = 1/\alpha$, and that we have the guarantee that for all v:

$$\max_{p \in P} Rev(p, v) \geq \max_{p \in [0,1]} Rev(p, v) - \alpha n$$

Putting it all Together

- Combining our bounds we see that if we discretize the price space by α, with probability 0.99, we obtain revenue:

$$Rev(p, v) \geq \mathrm{OPT} - \alpha \cdot n - O\left(\frac{1}{\epsilon}\ln\left(\frac{1}{\alpha}\right)\right)$$

Putting it all Together

- Combining our bounds we see that if we discretize the price space by α, with probability 0.99, we obtain revenue:

$$Rev(p, v) \geq \mathrm{OPT} - \alpha \cdot n - O\left(\frac{1}{\epsilon} \ln\left(\frac{1}{\alpha}\right)\right)$$

- Choosing $\alpha = 1/n$, we find that for any ϵ, we can obtain an ϵ-approximately dominant strategy truthful mechanism which obtains revenue:

$$Rev(p, v) \geq \mathrm{OPT} - O\left(\frac{\log n}{\epsilon}\right)$$

Putting it all Together

- Combining our bounds we see that if we discretize the price space by α, with probability 0.99, we obtain revenue:

$$Rev(p, v) \geq \mathrm{OPT} - \alpha \cdot n - O\left(\frac{1}{\epsilon} \ln\left(\frac{1}{\alpha}\right)\right)$$

- Choosing $\alpha = 1/n$, we find that for any ϵ, we can obtain an ϵ-approximately dominant strategy truthful mechanism which obtains revenue:

$$Rev(p, v) \geq \mathrm{OPT} - O\left(\frac{\log n}{\epsilon}\right)$$

- If we take e.g. $\epsilon = O(1/\log(n))$, then we have an *asymptotically truthful* mechanism (in the sense that it becomes exactly truthful as $n \to \infty$) that improves by an exponential factor on the revenue guarantee that we were able to obtain with an exactly truthful mechanism for the same problem.

Thanks!

See you next class — stay healthy, and get vaccinated!