Mechanism Design via Differential Privacy

Frank McSherry, Kunal Talwar
Presented by: Lidor Avigad

Weizmann Institute

March 17, 2008

Preliminaries

- **Differential Privacy** : How to disclose general non-specific information, but hide information about a specific participant.
- **Mechanism Design** : The design and analysis of algorithms robust to strategic manipulation of their inputs by self-interested agents.

Preliminaries

- **Differential Privacy** : How to disclose general non-specific information, but hide information about a specific participant.

- **Mechanism Design** : The design and analysis of algorithms robust to strategic manipulation of their inputs by self-interested agents.

Differential Privacy

Definition

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 $S \subseteq Range(\mathcal{M})$:

$$Pr[\mathcal{M}(D_1) \in S] \leq e^{\epsilon} \cdot Pr[\mathcal{M}(D_2) \in S]$$

Note that:

- Any event S is not substantially more of less likely as a result of specific user participation.
- Any event that are unlikely of impossible without a specific user participation remains so after introducing the data to the computation.

Differential Privacy

Definition

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 $S \subseteq Range(\mathcal{M})$:

$$Pr[\mathcal{M}(D_1) \in S] \leq e^{\epsilon} \cdot Pr[\mathcal{M}(D_2) \in S]$$

Note that:

- Any event S is not substantially more of less likely as a result of specific user participation.
- Any event that are unlikely of impossible without a specific user participation remains so after introducing the data to the computation.

Differential Privacy

Definition

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 $S \subseteq Range(\mathcal{M})$:

$$Pr[\mathcal{M}(D_1) \in S] \leq e^{\epsilon} \cdot Pr[\mathcal{M}(D_2) \in S]$$

Note that:

- Any event S is not substantially more of less likely as a result of specific user participation.
- Any event that are unlikely of impossible without a specific user participation remains so after introducing the data to the computation.

Mechanism Design

- Subfield of economics theory, interested in designing economics mechanism.
- The notion of *social choice* - aggregation of the preferences of the different participants toward a single joint decision.
- Implement desired social choices in a strategic settings.
- Agents, often selfish, acts rationally.
- Few examples:
  - **Auctions** - buyers and sellers the social choice: the identity of the winner.
  - **Elections** - voters and candidates the social choice: the outcome of the elections.

Mechanism Design

- Subfield of economics theory, interested in designing economics mechanism.
- The notion of *social choice* - aggregation of the preferences of the different participants toward a single joint decision.
- Implement desired social choices in a strategic settings.
- Agents, often selfish, acts rationally.
- Few examples:
  - **Auctions** - buyers and sellers the social choice: the identity of the winner.
  - **Elections** - voters and candidates the social choice: the outcome of the elections.

Mechanism Design

- Subfield of economics theory, interested in designing economics mechanism.
- The notion of *social choice* - aggregation of the preferences of the different participants toward a single joint decision.
- Implement desired social choices in a strategic settings.
- Agents, often selfish, acts rationally.
- Few examples:
  - **Auctions** - buyers and sellers the social choice: the identity of the winner.
  - **Elections** - voters and candidates the social choice: the outcome of the elections.

Mechanism Design

- Subfield of economics theory, interested in designing economics mechanism.
- The notion of *social choice* - aggregation of the preferences of the different participants toward a single joint decision.
- Implement desired social choices in a strategic settings.
- Agents, often selfish, acts rationally.
- Few examples:
  - **Auctions** - buyers and sellers the social choice: the identity of the winner.
  - **Elections** - voters and candidates the social choice: the outcome of the elections.

Mechanism Design

- Subfield of economics theory, interested in designing economics mechanism.
- The notion of *social choice* - aggregation of the preferences of the different participants toward a single joint decision.
- Implement desired social choices in a strategic settings.
- Agents, often selfish, acts rationally.
- Few examples:
  - **Auctions** - buyers and sellers the social choice: the identity of the winner.
  - **Elections** - voters and candidates the social choice: the outcome of the elections.

Vickrey Auction

Consider the following auction problem.

Example (Vickrey Auction)

Alice would like to sell on auction a picture. But she would like to sell it to the bidder which benefits most of it.

Vickrey Auction Solution

Example (Vickrey Auction - Second Price Auction)

Alice will sell the picture to the highest bidder at the price of the **second highest** bid!

Vickrey Auction Theorem

Theorem

Let $w_1, \ldots, w_n$ be the bids of n bidders. Then for every $w_1, \ldots, w_n$ and every $w_i^{'}$, let u_i be the i's utility if he bids w_i and $u_i^{'}$ his utility if he bids $w_i^{'}$. Then $u_i \geq u_i^{'}$

- The importance of truth telling in mechanism design as a concept.

Vickrey Auction Theorem

Theorem

Let $w_1, \ldots, w_n$ be the bids of n bidders. Then for every $w_1, \ldots, w_n$ and every w_i', let u_i be the i's utility if he bids w_i and u_i' his utility if he bids w_i'. Then $u_i \geq u_i'$

- The importance of truth telling in mechanism design as a concept.

Motivation: Unlimited Supply Auction

- A provider has unlimited number of good that it would like to sell at a given price: pay-per-view, music files etc'.
- The cost of production is almost zero.
- There are n bidders who would like to buy the goods.
- The more cheaper it costs the more items a bidder would buy.

Motivation: Unlimited Supply Auction

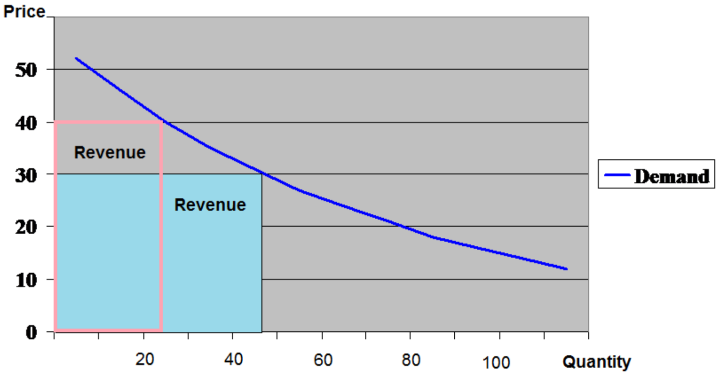
- A provider has unlimited number of good that it would like to sell at a given price: pay-per-view, music files etc'.
- The cost of production is almost zero.
- There are n bidders who would like to buy the goods.
- The more cheaper it costs the more items a bidder would buy.

Motivation: Unlimited Supply Auction

- A provider has unlimited number of good that it would like to sell at a given price: pay-per-view, music files etc'.
- The cost of production is almost zero.
- There are n bidders who would like to buy the goods.
- The more cheaper it costs the more items a bidder would buy.

Motivation: Unlimited Supply Auction

- A provider has unlimited number of good that it would like to sell at a given price: pay-per-view, music files etc'.
- The cost of production is almost zero.
- There are n bidders who would like to buy the goods.
- The more cheaper it costs the more items a bidder would buy.


Price
50
40
30
20
10
0
Revenue
Revenue
Demand
20
40
60
80
100
Quantity

Motivation: Unlimited Supply Auction

- A provider has unlimited number of good that it would like to sell at a given price, pay-per-view, digital goods etc'.
- There are n bidders. Each bidder i has a non-increasing demand curve $b_i : [0, 1] \to \mathbb{R}^+$.
- For price $p \in [0, 1]$ the provider can sell $\sum_i^n b_i(p)$.
- Yielding a profit of $q(b, p) = p \cdot \sum_i^n b_i(p)$ say dollars in revenue.
- Each bidder has limited resources $p \cdot b_i(p) \leq 1$.

Motivation: Unlimited Supply Auction

- A provider has unlimited number of good that it would like to sell at a given price, pay-per-view, digital goods etc'.
- There are n bidders. Each bidder i has a non-increasing demand curve $b_i : [0,1] \to \mathbb{R}^+$.
- For price $p \in [0,1]$ the provider can sell $\sum_i^n b_i(p)$.
- Yielding a profit of $q(b,p) = p \cdot \sum_i^n b_i(p)$ say dollars in revenue.
- Each bidder has limited resources $p \cdot b_i(p) \leq 1$.

Motivation: Unlimited Supply Auction

- A provider has unlimited number of good that it would like to sell at a given price, pay-per-view, digital goods etc'.
- There are n bidders. Each bidder i has a non-increasing demand curve $b_i : [0,1] \to \mathbb{R}^+$.
- For price $p \in [0,1]$ the provider can sell $\sum_i^n b_i(p)$.
- Yielding a profit of $q(b,p) = p \cdot \sum_i^n b_i(p)$ say dollars in revenue.
- Each bidder has limited resources $p \cdot b_i(p) \leq 1$.

Motivation: Unlimited Supply Auction

- A provider has unlimited number of good that it would like to sell at a given price, pay-per-view, digital goods etc'.
- There are n bidders. Each bidder i has a non-increasing demand curve $b_i : [0,1] \to \mathbb{R}^+$.
- For price $p \in [0,1]$ the provider can sell $\sum_i^n b_i(p)$.
- Yielding a profit of $q(b,p) = p \cdot \sum_i^n b_i(p)$ say dollars in revenue.
- Each bidder has limited resources $p \cdot b_i(p) \leq 1$.

Motivation: Unlimited Supply Auction

- A provider has unlimited number of good that it would like to sell at a given price, pay-per-view, digital goods etc'.
- There are n bidders. Each bidder i has a non-increasing demand curve $b_i : [0,1] \rightarrow \mathbb{R}^+$.
- For price $p \in [0,1]$ the provider can sell $\sum_i^n b_i(p)$.
- Yielding a profit of $q(b,p) = p \cdot \sum_i^n b_i(p)$ say dollars in revenue.
- Each bidder has limited resources $p \cdot b_i(p) \leq 1$.

Main Problem

Sensitive to bidder input !

Slight change can send bidders empty handed, thus reducing revenue !

Main Problem

Sensitive to bidder input !

Slight change can send bidders empty handed, thus reducing revenue !

Proposed Solution

Define:

$$q(b, p) = p \cdot \sum_{i}^{n} b_i(p)$$

Theorem

Selecting p according to this distribution yields almost optimal solution:

$$\varepsilon_q^{\epsilon}(b) := \textit{choose } p \textit{ with probability } \propto e^{\epsilon q(b,p)} \cdot p$$

Proposed Solution

Define:

$$q(b, p) = p \cdot \sum_{i}^{n} b_i(p)$$

Theorem

Selecting p according to this distribution yields almost optimal solution:

$$\varepsilon_q^{\epsilon}(b) := \textit{choose } p \textit{ with probability } \propto e^{\epsilon q(b,p)} \cdot p$$

Why ? We will prove general result.

Why ? We will prove general result.

Cut ...

Differential Privacy as a Solution Concept

Assume we have mechanism that provide differential privacy then:

- **Approximate truthfulness**
  ϵ-dominance, no agent has more then ϵ-additive incentive to reply non-truthfully.
- **Collusion resistance**
  resistance to coalitions.
- **Compatibility**
  robust under composition.

Differential Privacy as a Solution Concept

Assume we have mechanism that provide differential privacy then:

- **Approximate truthfulness**
  ϵ-dominance, no agent has more then ϵ-additive incentive to reply non-truthfully.
- **Collusion resistance**
  resistance to coalitions.
- **Compatibility**
  robust under composition.

Differential Privacy as a Solution Concept

Assume we have mechanism that provide differential privacy then:

- **Approximate truthfulness**
  ϵ-dominance, no agent has more then ϵ-additive incentive to reply non-truthfully.
- **Collusion resistance**
  resistance to coalitions.
- **Compatibility**
  robust under composition.

Differential Privacy as a Solution Concept

Assume we have mechanism that provide differential privacy then:

- **Approximate truthfulness**
  ϵ-dominance, no agent has more then ϵ-additive incentive to reply non-truthfully.
- **Collusion resistance**
  resistance to coalitions.
- **Compatibility**
  robust under composition.

Approximate Truthfulness

Theorem

Any mechanism $\mathcal{M}$ giving ϵ-differential privacy make truth telling $(e^{\epsilon} - 1)$-dominant strategy for any utility function $u : Range(\mathcal{M}) \to [0, 1]$.

Approximate Truthfulness - Proof

Following from this lemma:

Lemma (Approximate Truthfulness)

For any mechanism $\mathcal{M}$ giving ϵ-differential privacy and any non-negative function $g : Range(\mathcal{M}) \rightarrow \mathbb{R}^+$, for any D_1 and D_2 differing on single input

$$\mathbb{E}[g(\mathcal{M}(D_1))] \leq e^{\epsilon} \cdot \mathbb{E}[g(\mathcal{M}(D_2))]$$

Collusion Resistance

Theorem

For any mechanism $\mathcal{M}$ giving ϵ-differential privacy and any non-negative function $g : Range(\mathcal{M}) \rightarrow \mathbb{R}^+$, for any D_1 and D_2 differing on at most t inputs

$$\mathbb{E}[g(\mathcal{M}(D_1))] \leq e^{\epsilon t} \cdot \mathbb{E}[g(\mathcal{M}(D_2))]$$

- When g is is the sum of the utility functions of t agents.
- Side payments are irrelevant.

Collusion Resistance

Theorem

For any mechanism $\mathcal{M}$ giving ϵ-differential privacy and any non-negative function $g : Range(\mathcal{M}) \to \mathbb{R}^+$, for any D_1 and D_2 differing on at most t inputs

$$\mathbb{E}[g(\mathcal{M}(D_1))] \leq e^{\epsilon t} \cdot \mathbb{E}[g(\mathcal{M}(D_2))]$$

- When g is is the sum of the utility functions of t agents.
- Side payments are irrelevant.

Collusion Resistance

Theorem

For any mechanism $\mathcal{M}$ giving ϵ-differential privacy and any non-negative function $g : Range(\mathcal{M}) \to \mathbb{R}^+$, for any D_1 and D_2 differing on at most t inputs

$$\mathbb{E}[g(\mathcal{M}(D_1))] \leq e^{\epsilon t} \cdot \mathbb{E}[g(\mathcal{M}(D_2))]$$

- When g is is the sum of the utility functions of t agents.
- Side payments are irrelevant.

Compatibility

Theorem

The sequential application of mechanisms $\{\mathcal{M}_i\}$, each giving $\{\epsilon_i\}$-differential privacy, gives $\sum_i \epsilon_i$-differential privacy.

Agent cannot skew the result effectively over time.

The Goal of Privacy Mechanism

Privacy mechanism $\mathcal{M}$ maps randomly n inputs from domain $\mathcal{D}$ into range $\mathcal{R}$ assuming measure μ on $\mathcal{R}$.

$$\mathcal{M} : \mathcal{D}^n \rightarrow \mathcal{R}$$

Also define a **query function q**

$$q : \mathcal{D}^n \times \mathcal{R} \rightarrow \mathbb{R}$$

The higher, the better.
The goal of $\mathcal{M}$: when given $d \in \mathcal{D}^n$ return $r^* \in \mathcal{R}$ s.t.

$$r^* := max_{r \in \mathcal{R}}\{q(d, r)\}$$

while guaranteeing differential privacy

The Goal of Privacy Mechanism

Privacy mechanism $\mathcal{M}$ maps randomly n inputs from domain $\mathcal{D}$ into range $\mathcal{R}$ assuming measure μ on $\mathcal{R}$.

$$\mathcal{M} : \mathcal{D}^n \to \mathcal{R}$$

Also define a **query function q**

$$q : \mathcal{D}^n \times \mathcal{R} \to \mathbb{R}$$

The higher, the better.

The goal of $\mathcal{M}$: when given $d \in \mathcal{D}^n$ return $r^* \in \mathcal{R}$ s.t.

$$r^* := max_{r \in \mathcal{R}}\{q(d, r)\}$$

while guaranteeing differential privacy

The Goal of Privacy Mechanism

Privacy mechanism $\mathcal{M}$ maps randomly n inputs from domain $\mathcal{D}$ into range $\mathcal{R}$ assuming measure μ on $\mathcal{R}$.

$$\mathcal{M} : \mathcal{D}^n \to \mathcal{R}$$

Also define a **query function q**

$$q : \mathcal{D}^n \times \mathcal{R} \to \mathbb{R}$$

The higher, the better.
The goal of $\mathcal{M}$: when given $d \in \mathcal{D}^n$ return $r^* \in \mathcal{R}$ s.t.

$$r^* := max_{r \in \mathcal{R}}\{q(d, r)\}$$

while guaranteeing differential privacy

Definition

For any function $q : \mathcal{D}^n \times \mathcal{R} \rightarrow \mathbb{R}$, and base measure μ over $\mathcal{R}$ define:

$$\varepsilon_q^\epsilon(d) := \text{choose } r \text{ with probability } \propto e^{\epsilon q(d,r)} \cdot \mu(r)$$

Note that:

- Small additive change to $q(d, r)$ has a limited multiplicative influence (as in differential privacy).
- The probability associated with r increases exponentially biasing the distribution towards the optimum.

Definition

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

$$\varepsilon_q^\epsilon(d) := \text{choose } r \text{ with probability } \propto e^{\epsilon q(d,r)} \cdot \mu(r)$$

Note that:

- Small additive change to $q(d, r)$ has a limited multiplicative influence (as in differential privacy).
- The probability associated with r increases exponentially biasing the distribution towards the optimum.

Definition

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

$$\varepsilon_q^\epsilon(d) := \text{choose } r \text{ with probability } \propto e^{\epsilon q(d,r)} \cdot \mu(r)$$

Note that:

- Small additive change to $q(d, r)$ has a limited multiplicative influence (as in differential privacy).
- The probability associated with r increases exponentially biasing the distribution towards the optimum.

Privacy

Theorem

$\varepsilon_q^\epsilon(d)$ gives $(2\epsilon\Delta q)$ differential privacy, where Δq is the largest possible difference in the query function on inputs that differ on single value.

Proof.

By definition the density of $\varepsilon_q^\epsilon(d)$ at r is:

$$\frac{e^{\epsilon q(d,r)} \cdot \mu(r)}{\int_r e^{\epsilon q(d,r)} \cdot \mu(r) dr} \leq e^{2\epsilon\Delta q} \frac{e^{\epsilon q(d^*,r)} \cdot \mu(r)}{\int_r e^{\epsilon q(d^*,r)} \cdot \mu(r) dr}$$

$$max_r\{q(d_1,r) - q(d_2,r) | \, d_1, \, d_2 \text{ differs on one value}\} = \Delta q$$

The minimum is $-\Delta q$.
Plug into the enumerator and denominator resp. □

Privacy

Theorem

$\varepsilon_q^\epsilon(d)$ gives $(2\epsilon\Delta q)$ differential privacy, where Δq is the largest possible difference in the query function on inputs that differ on single value.

Proof.

By definition the density of $\varepsilon_q^\epsilon(d)$ at r is:

$$\frac{e^{\epsilon q(d,r)} \cdot \mu(r)}{\int_r e^{\epsilon q(d,r)} \cdot \mu(r)dr} \leq e^{2\epsilon\Delta q} \frac{e^{\epsilon q(d^*,r)} \cdot \mu(r)}{\int_r e^{\epsilon q(d^*,r)} \cdot \mu(r)dr}$$

$$max_r\{q(d_1,r) - q(d_2,r) | \, d_1, \, d_2 \text{ differs on one value}\} = \Delta q$$

The minimum is $-\Delta q$.
Plug into the enumerator and denominator resp. □

Accuracy

Define $\mu(A)$ for $A \subseteq \mathcal{R}$ the base measure normalized.
Define $p(A)$ the measure defined by $\varepsilon_q^\epsilon(d)$ normalized.

Lemma

Let $S_t = \{r \mid q(d,r) > OPT - t\}$, then $p(\overline{S}_{2t}) \leq \frac{e^{-\epsilon t}}{\mu(S_t)}$, where OPT is $\max_r\{q(d,r)\}$.

Proof.

$$p(\overline{S}_{2t}) \leq \frac{p(\overline{S}_{2t})}{p(S_t)} = \frac{\int_{\overline{S}_{2t}} e^{\epsilon q(d,r)}\mu(r)dr}{\int_{S_t} e^{\epsilon q(d,r)}\mu(r)dr} \leq e^{-\epsilon t} \cdot \frac{\mu(\overline{S}_{2t})}{\mu(S_t)} \leq \frac{e^{-\epsilon t}}{\mu(S_t)}$$

□

Accuracy

Define $\mu(A)$ for $A \subseteq \mathcal{R}$ the base measure normalized.
Define $p(A)$ the measure defined by $\varepsilon_q^\epsilon(d)$ normalized.

Lemma

Let $S_t = \{r \mid q(d,r) > OPT - t\}$, then $p(\overline{S}_{2t}) \leq \frac{e^{-\epsilon t}}{\mu(S_t)}$, where OPT is $\max_r\{q(d,r)\}$.

Proof.

$$p(\overline{S}_{2t}) \leq \frac{p(\overline{S}_{2t})}{p(S_t)}$$

$$= \frac{\int_{\overline{S}_{2t}} e^{\epsilon q(d,r)} \mu(r) dr}{\int_{S_t} e^{\epsilon q(d,r)} \mu(r) dr} \leq e^{-\epsilon t} \cdot \frac{\mu(\overline{S}_{2t})}{\mu(S_t)} \leq \frac{e^{-\epsilon t}}{\mu(S_t)}$$

□

Accuracy Theorem

Theorem

For those values of t satisfying $t \geq \epsilon^{-1} \ln \frac{OPT}{t\mu(S_t)}$ *we have* $\mathbb{E}[q(d, \varepsilon_q^{\epsilon}(d))] \geq OPT - 3t$.

Proof.

From previous lemma: $p(S_{2t}) > 1 - \frac{e^{-\epsilon t}}{\mu(S_t)}$.
Substitute t: $p(S_{2t}) > 1 - \frac{t}{OPT}$.

$$\mathbb{E}[q(d, \varepsilon_q^{\epsilon}(d))] \geq (1 - \frac{t}{OPT})(OPT - 2t) \geq OPT - 3t$$ □

Accuracy Theorem

Theorem

For those values of t satisfying $t \geq \epsilon^{-1} \ln \frac{OPT}{t\mu(S_t)}$ *we have* $\mathbb{E}[q(d, \varepsilon_q^{\epsilon}(d))] \geq OPT - 3t$.

Proof.

From previous lemma: $p(S_{2t}) > 1 - \frac{e^{-\epsilon t}}{\mu(S_t)}$.
Substitute t: $p(S_{2t}) > 1 - \frac{t}{OPT}$.

$$\mathbb{E}[q(d, \varepsilon_q^{\epsilon}(d))] \geq (1 - \frac{t}{OPT})(OPT - 2t) \geq OPT - 3t$$ □

Accuracy Implications

Recall:

Theorem

For those values of t satisfying $t \geq \epsilon^{-1} \ln \frac{OPT}{t\mu(S_t)}$ *we have* $\mathbb{E}[q(d, \varepsilon_q^{\epsilon}(d))] \geq OPT - 3t$.

The implications are:

- Central parameter: $\mu(S_t)$ defines how large we must take t so our exponential bias can overcome the small size of $\mu(S_t)$.
- In case of discrete $\mathcal{R}$ a uniform μ makes $\mu(S_t) \geq \frac{1}{|\mathcal{R}|}$.

Accuracy Implications

Recall:

Theorem

For those values of t satisfying $t \geq \epsilon^{-1} \ln \frac{OPT}{t\mu(S_t)}$ *we have* $\mathbb{E}[q(d, \varepsilon_q^{\epsilon}(d))] \geq OPT - 3t$.

The implications are:

- Central parameter: $\mu(S_t)$ defines how large we must take t so our exponential bias can overcome the small size of $\mu(S_t)$.
- In case of discrete $\mathcal{R}$ a uniform μ makes $\mu(S_t) \geq \frac{1}{|\mathcal{R}|}$.

Accuracy Implications

Recall:

Theorem

For those values of t satisfying $t \geq \epsilon^{-1} \ln \frac{OPT}{t\mu(S_t)}$ *we have* $\mathbb{E}[q(d, \varepsilon_q^{\epsilon}(d))] \geq OPT - 3t$.

The implications are:

- Central parameter: $\mu(S_t)$ defines how large we must take t so our exponential bias can overcome the small size of $\mu(S_t)$.
- In case of discrete $\mathcal{R}$ a uniform μ makes $\mu(S_t) \geq \frac{1}{|\mathcal{R}|}$.

Proof of Unlimited Supply Auction

Theorem

Taking:

$$q(b, p) = p \cdot \sum_{i}^{n} b_i(p)$$

the mechanism $\varepsilon_q^\epsilon(d)$ *gives* 2ϵ*-differential privacy and has expected revenue at least* $OPT - 3\epsilon^{-1} \ln(e + \epsilon^2 OPTm)$

Privacy:

Proof.
Privacy follows since bidder i can change $q(b, p)$ at most by $p \cdot b_i(p) \leq 1$. Using privacy theorem. □

Revenue:

Proof.
Take $t = \epsilon^{-1} \ln\left(e + \epsilon^2 OPTm\right)$. □

Privacy:

Proof.

Privacy follows since bidder i can change $q(b, p)$ at most by $p \cdot b_i(p) \leq 1$. Using privacy theorem. $\square$

Revenue:

Proof.

Take $t = \epsilon^{-1} \ln(e + \epsilon^2 OPTm)$. $\square$

Privacy:

Proof.

Privacy follows since bidder i can change $q(b, p)$ at most by $p \cdot b_i(p) \leq 1$. Using privacy theorem. □

Revenue:

Proof.

Take $t = \epsilon^{-1} \ln(e + \epsilon^2 OPTm)$. □

Privacy:

Proof.

Privacy follows since bidder i can change $q(b, p)$ at most by $p \cdot b_i(p) \leq 1$. Using privacy theorem. □

Revenue:

Proof.

Take $t = \epsilon^{-1} \ln(e + \epsilon^2 OPTm)$. □

Attribute Auctions

- The bidders has attributes like: age, income etc'.
- The market can be segmented according these properties resulting different pricing policies.
- SEG_k the number of permitted segmentation of n users to k market.
- OPT_k the optimal revenue with the markets segmented into k parts.

Theorem

Taking q to be the revenue function over segmentations into k markets and their prices, $\varepsilon_q^\epsilon(d)$ has expected revenue is at least $OPT_k - 3\epsilon^{-1}\ln\left(e + \epsilon^{k+1} OPT_k SEG_k m^k\right)$

Attribute Auctions

- The bidders has attributes like: age, income etc'.
- The market can be segmented according these properties resulting different pricing policies.
- SEG_k the number of permitted segmentation of n users to k market.
- OPT_k the optimal revenue with the markets segmented into k parts.

Theorem

Taking q to be the revenue function over segmentations into k markets and their prices, $\varepsilon_q^\epsilon(d)$ has expected revenue is at least $OPT_k - 3\epsilon^{-1}\ln\left(e + \epsilon^{k+1} OPT_k SEG_k m^k\right)$

Attribute Auctions

- The bidders has attributes like: age, income etc'.
- The market can be segmented according these properties resulting different pricing policies.
- SEG_k the number of permitted segmentation of n users to k market.
- OPT_k the optimal revenue with the markets segmented into k parts.

Theorem

Taking q to be the revenue function over segmentations into k markets and their prices, $\varepsilon_q^{\epsilon}(d)$ has expected revenue is at least $OPT_k - 3\epsilon^{-1}\ln\left(e + \epsilon^{k+1} OPT_k SEG_k m^k\right)$

Attribute Auctions

- The bidders has attributes like: age, income etc'.
- The market can be segmented according these properties resulting different pricing policies.
- SEG_k the number of permitted segmentation of n users to k market.
- OPT_k the optimal revenue with the markets segmented into k parts.

Theorem

Taking q to be the revenue function over segmentations into k markets and their prices, $\varepsilon_q^{\epsilon}(d)$ has expected revenue is at least $OPT_k - 3\epsilon^{-1}\ln\left(e + \epsilon^{k+1} OPT_k SEG_k m^k\right)$

Attribute Auctions

- The bidders has attributes like: age, income etc'.
- The market can be segmented according these properties resulting different pricing policies.
- SEG_k the number of permitted segmentation of n users to k market.
- OPT_k the optimal revenue with the markets segmented into k parts.

Theorem

Taking q to be the revenue function over segmentations into k markets and their prices, $\varepsilon_q^{\epsilon}(d)$ has expected revenue is at least $OPT_k - 3\epsilon^{-1}\ln\left(e + \epsilon^{k+1} OPT_k SEG_k m^k\right)$

What Did We Cover ?

- **Differential Privacy as a Solution Concept:**
  - "Truthfulness" is solution concept for mechanism design.
  - Helps to design mechanism in complex environment, for example recourse.
  - Simplifies the analysis of mechanism.
  - Differential privacy leads to relaxation of truthfulness. There incentive to misrepresent a value is non-zero, but tightly controlled.
  - Can handle collisions and repeated runs.
  - Address problem that cannot be addressed with strict truthfulness as the unlimited supply pricing problem.

What Did We Cover ?

- **Differential Privacy as a Solution Concept**:
  - "Truthfulness" is solution concept for mechanism design.
  - Helps to design mechanism in complex environment, for example recourse.
  - Simplifies the analysis of mechanism.
  - Differential privacy leads to relaxation of truthfulness. There incentive to misrepresent a value is non-zero, but tightly controlled.
  - Can handle collisions and repeated runs.
  - Address problem that cannot be addressed with strict truthfulness as the unlimited supply pricing problem.

What Did We Cover ?

- **Differential Privacy as a Solution Concept**:
  - "Truthfulness" is solution concept for mechanism design.
  - Helps to design mechanism in complex environment, for example recourse.
  - Simplifies the analysis of mechanism.
  - Differential privacy leads to relaxation of truthfulness. There incentive to misrepresent a value is non-zero, but tightly controlled.
  - Can handle collisions and repeated runs.
  - Address problem that cannot be addressed with strict truthfulness as the unlimited supply pricing problem.

What Did We Cover ?

- **Differential Privacy as a Solution Concept**:
  - "Truthfulness" is solution concept for mechanism design.
  - Helps to design mechanism in complex environment, for example recourse.
  - Simplifies the analysis of mechanism.
  - Differential privacy leads to relaxation of truthfulness. There incentive to misrepresent a value is non-zero, but tightly controlled.
  - Can handle collisions and repeated runs.
  - Address problem that cannot be addressed with strict truthfulness as the unlimited supply pricing problem.

What Did We Cover ?

- **Differential Privacy as a Solution Concept**:
  - "Truthfulness" is solution concept for mechanism design.
  - Helps to design mechanism in complex environment, for example recourse.
  - Simplifies the analysis of mechanism.
  - Differential privacy leads to relaxation of truthfulness. There incentive to misrepresent a value is non-zero, but tightly controlled.
  - Can handle collisions and repeated runs.
  - Address problem that cannot be addressed with strict truthfulness as the unlimited supply pricing problem.

What Did We Cover ?

- **Differential Privacy as a Solution Concept**:
  - "Truthfulness" is solution concept for mechanism design.
  - Helps to design mechanism in complex environment, for example recourse.
  - Simplifies the analysis of mechanism.
  - Differential privacy leads to relaxation of truthfulness. There incentive to misrepresent a value is non-zero, but tightly controlled.
  - Can handle collisions and repeated runs.
  - Address problem that cannot be addressed with strict truthfulness as the unlimited supply pricing problem.

What Did We Cover ?

- **Differential Privacy as a Solution Concept**:
  - "Truthfulness" is solution concept for mechanism design.
  - Helps to design mechanism in complex environment, for example recourse.
  - Simplifies the analysis of mechanism.
  - Differential privacy leads to relaxation of truthfulness. There incentive to misrepresent a value is non-zero, but tightly controlled.
  - Can handle collisions and repeated runs.
  - Address problem that cannot be addressed with strict truthfulness as the unlimited supply pricing problem.

What Did We Cover ?

- **A General Differential Privacy Framework**:
  - Previous approaches to differential privacy focus on real valued insensitive functions.
  - Sensitive functions as in unlimited supply auction. Single bidder can make difference.
  - Other problem domains with non-numeric output: classifiers in machine learning, route flow etc'.
  - The framework will address this issues producing privacy preserving mechanism if given suitable measurable range.

What Did We Cover ?

- **A General Differential Privacy Framework**:
  - Previous approaches to differential privacy focus on real valued insensitive functions.
  - Sensitive functions as in unlimited supply auction. Single bidder can make difference.
  - Other problem domains with non-numeric output: classifiers in machine learning, route flow etc'.
  - The framework will address this issues producing privacy preserving mechanism if given suitable measurable range.

What Did We Cover ?

- **A General Differential Privacy Framework**:
  - Previous approaches to differential privacy focus on real valued insensitive functions.
  - Sensitive functions as in unlimited supply auction. Single bidder can make difference.
  - Other problem domains with non-numeric output: classifiers in machine learning, route flow etc'.
  - The framework will address this issues producing privacy preserving mechanism if given suitable measurable range.

What Did We Cover ?

- **A General Differential Privacy Framework**:
  - Previous approaches to differential privacy focus on real valued insensitive functions.
  - Sensitive functions as in unlimited supply auction. Single bidder can make difference.
  - Other problem domains with non-numeric output: classifiers in machine learning, route flow etc'.
  - The framework will address this issues producing privacy preserving mechanism if given suitable measurable range.

What Did We Cover ?

- **A General Differential Privacy Framework**:
  - Previous approaches to differential privacy focus on real valued insensitive functions.
  - Sensitive functions as in unlimited supply auction. Single bidder can make difference.
  - Other problem domains with non-numeric output: classifiers in machine learning, route flow etc'.
  - The framework will address this issues producing privacy preserving mechanism if given suitable measurable range.

What Did We Cover ?

- **Applications to Digital Goods Auctions**:
  - Unlimited supply auction.
  - Attribute Auctions

What Did We Cover ?

- **Applications to Digital Goods Auctions**:
  - Unlimited supply auction.
  - Attribute Auctions

What Did We Cover ?

- **Applications to Digital Goods Auctions**:
  - Unlimited supply auction.
  - Attribute Auctions

Questions ?

Thank You !

Questions ?

Thank You !