yesterday

DP definition, properties

Randomized Response

Laplace Mechanism

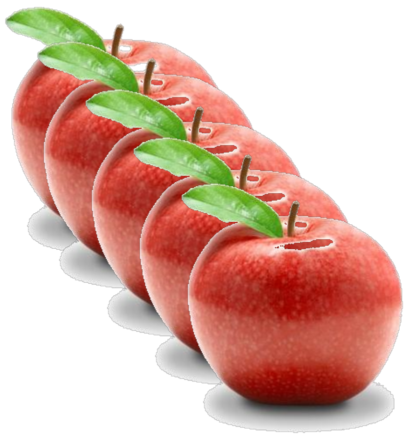
reportNoisyMax

Ok, but I wanted to use my data for a scenario where direct noise addition doesn't make sense

selecting from among discrete set of alternatives

small perturbation in outcome space could be disastrous for outcome quality

Example: Items for sale



$1.00

$1.00

$1.00

$4.01

Could set the price of apples at $1.00 for profit: $4.00

Could set the price of apples at $4.01 for profit $4.01

Best price: $4.01
2nd best price: $1.00
Profit if you set the price at $4.02: $0
Profit if you set the price at $1.01: $1.01

The Exponential Mechanism

- A mechanism $M: \mathbb{N}^{|X|} \to R$ for some abstract range R.
  - i.e. $R = \{\text{Red, Blue, Green, Brown, Purple}\}$
  - $R = \{\$1.00, \$1.01, \$1.02, \$1.03, \dots\}$
- Paired with a *quality score:*

$$q: \mathbb{N}^{|X|} \times R \to \mathbb{R}$$

$q(D, r)$ represents how good output r is for database D.

The Exponential Mechanism

- Relative parameters for privacy, solution quality:
  - Sensitivity of q:
  $$GS(q) = \max_{r \in R, D, D' : ||D - D'||_1 \leq 1} |q(D, r) - q(D', r)|$$
  - Size and structure of R.
    - How many elements of R are high quality? How many are low quality?

The Exponential Mechanism

Exponential$(D, R, q: \mathbb{N}^{|X|} \rightarrow R, \epsilon)$:

1. Let $\Delta = GS(q)$.
2. Output $r \sim R$ with probability proportional to:

$$\Pr[r] \sim \exp\left(\frac{\epsilon q(D,r)}{2\Delta}\right)$$

$$\Pr[r] = \frac{\exp(\frac{\epsilon q(D,r)}{2\Delta})}{\sum_{r' \in R} \exp(\frac{\epsilon q(D,r')}{2\Delta})}$$

The Exponential Mechanism

Exponential$(D, R, q: \mathbb{N}^{|X|} \to R, \epsilon)$:

1. Let $\Delta = GS(q)$.
2. Output $r \sim R$ with probability proportional to:

$$\Pr[r] \sim \exp\left(\frac{\epsilon q(D, r)}{2\Delta}\right)$$

Idea: Make high quality outputs exponentially more likely at a rate that depends on the sensitivity of the quality score (and the privacy parameter)

Thm. The exponential mechanism preserves $(\varepsilon, 0)$-differential privacy.

The Exponential Mechanism

Exponential$(D, R, q: \mathbb{N}^{|X|} \rightarrow R, \epsilon)$:

1. Let $\Delta = GS(q)$.
2. Output $r \sim R$ with probability proportional to:

$$\Pr[r] \sim \exp\left(\frac{\epsilon q(D,r)}{2\Delta}\right)$$

Theorem: The Exponential Mechanism preserves $(\epsilon, 0)$-differential privacy.

Proof: Fix any $D, D' \in \mathbb{N}^{|X|}$ with $\left|\left|D, D'\right|\right|_1 \leq 1$ and any $r \in R$…

$$\frac{\Pr[\text{Exponential}(D, R, q, \epsilon) = r]}{\Pr[\text{Exponential}(D', R, q, \epsilon) = r]} =$$

$$\frac{\left(\frac{\exp(\frac{\epsilon q(D,r)}{2\Delta})}{\sum \exp(\frac{\epsilon q(D,r')}{2\Delta})}\right)}{\left(\frac{\exp(\frac{\epsilon q(D',r)}{2\Delta})}{\sum \exp(\frac{\epsilon q(D',r')}{2\Delta})}\right)} = \left(\frac{\exp(\frac{\epsilon q(D,r)}{2\Delta})}{\exp(\frac{\epsilon q(D',r)}{2\Delta})}\right)\left(\frac{\sum_{r'} \exp(\frac{\epsilon q(D',r')}{2\Delta})}{\sum_{r'} \exp(\frac{\epsilon q(D,r')}{2\Delta})}\right)$$

The Exponential Mechanism

Exponential$(D, R, q\colon \mathbb{N}^{|X|} \to R, \epsilon)$:

1. Let $\Delta = GS(q)$.
2. Output $r \sim R$ with probability proportional to:

$$\Pr[r] \sim \exp\left(\frac{\epsilon q(D,r)}{2\Delta}\right)$$

Theorem: The Exponential Mechanism preserves $(\epsilon, 0)$-differential privacy.

Proof:

$$\bigstar \;=\; \left(\frac{\exp(\frac{\epsilon q(D,r)}{2\Delta})}{\exp(\frac{\epsilon q(D',r)}{2\Delta})}\right) =$$

$$\exp\left(\frac{\epsilon(q(D,r) - q(D',r))}{2\Delta}\right) \leq$$

$$\exp\left(\frac{\epsilon\Delta}{2\Delta}\right) = \exp\left(\frac{\epsilon}{2}\right)$$

The Exponential Mechanism

Exponential$(D, R, q: \mathbb{N}^{|X|} \to R, \epsilon)$:
1. Let $\Delta = GS(q)$.
2. Output $r \sim R$ with probability proportional to:

$$\Pr[r] \sim \exp\left(\frac{\epsilon q(D,r)}{2\Delta}\right)$$

Theorem: The Exponential Mechanism preserves $(\epsilon, 0)$-differential privacy.

Proof:

$$\bigstar\bigstar = \left(\frac{\sum_{r'} \exp(\frac{\epsilon q(D',r')}{2\Delta})}{\sum_{r'} \exp(\frac{\epsilon q(D,r')}{2\Delta})}\right) \le$$

$$\left(\frac{\sum_{r'} \exp(\frac{\epsilon (q(D,r') + \Delta)}{2\Delta})}{\sum_{r'} \exp(\frac{\epsilon q(D,r')}{2\Delta})}\right) =$$

$$= \left(\frac{\exp(\frac{\epsilon}{2}) \sum_{r'} \exp(\frac{\epsilon q(D,r')}{2\Delta})}{\sum_{r'} \exp(\frac{\epsilon q(D,r')}{2\Delta})}\right) = \exp(\frac{\epsilon}{2})$$

The Exponential Mechanism

Exponential$(D, R, q: \mathbb{N}^{|X|} \to R, \epsilon)$:

1. Let $\Delta = GS(q)$.
2. Output $r \sim R$ with probability proportional to:

$$\Pr[r] \sim \exp\left(\frac{\epsilon q(D, r)}{2\Delta}\right)$$

Theorem: The Exponential Mechanism preserves $(\epsilon, 0)$-differential privacy.

Proof: Recall:

$$\frac{\Pr[\text{Exponential}(D, R, q, \epsilon) = r]}{\Pr[\text{Exponential}(D', R, q, \epsilon) = r]} =$$

$$\leq \exp\left(\frac{\epsilon}{2}\right) \exp\left(\frac{\epsilon}{2}\right)$$

$$= \exp(\epsilon)$$

The Exponential Mechanism

Exponential$(D, R, q: \mathbb{N}^{|X|} \rightarrow R, \epsilon)$:

1. Let $\Delta = GS(q)$.
2. Output $r \sim R$ with probability proportional to:

$$\Pr[r] \sim \exp\left(\frac{\epsilon q(D, r)}{2\Delta}\right)$$

But is the answer any good?

The Exponential Mechanism

Exponential$(D, R, q: \mathbb{N}^{|X|} \rightarrow R, \epsilon)$:

1. Let $\Delta = GS(q)$.
2. Output $r \sim R$ with probability proportional to:

$$\Pr[r] \sim \exp\left(\frac{\epsilon q(D, r)}{2\Delta}\right)$$

But is the answer any good?

It depends…

The Exponential Mechanism

Define:

$$OPT_q(D) = \max_{r \in R} q(D, r)$$
$$R_{OPT} = \{r \in R : q(D, r) = OPT_q(D)\}$$
$$r^* = \text{Exponential}(D, R, q, \epsilon)$$

Theorem:

$$\Pr\left[q(r^*) \le OPT_q(D) - \frac{2\Delta}{\epsilon}\left(\log\left(\frac{|R|}{|R_{OPT}|}\right) + t\right)\right] \le e^{-t}$$

The Exponential Mechanism

Theorem:

$$\Pr\left[q(r^*) \leq OPT_q(D) - \frac{2\Delta}{\epsilon}\left(\log\left(\frac{|R|}{|R_{OPT}|}\right) + t\right)\right] \leq e^{-t}$$

Corollary:

$$\Pr\left[q(r^*) \leq OPT_q(D) - \frac{2\Delta}{\epsilon}(\log(|R|) + t)\right] \leq e^{-t}$$

Proof:

$|R_{OPT}| \geq 1$ by definition.

The Exponential Mechanism

Theorem:

$$\Pr\left[q(r^*) \leq OPT_q(D) - \frac{2\Delta}{\epsilon}\left(\log\left(\frac{|R|}{|R_{OPT}|}\right) + t\right)\right] \leq e^{-t}$$

Corollary:

$$\mathrm{E}[q(r^*)] \geq OPT_q(D) \ - \frac{2\Delta}{\epsilon}\left(\log(|R|) + \log\left(OPT_q(D)\right)\right) - 1$$

Proof:

$$\Pr\left[q(r^*) \leq OPT_q(D) - \frac{2\Delta}{\epsilon}\left(\log(|R|) + \log(OPT_q(D)\right)\right] \leq \frac{1}{OPT_q(D)}$$

$$\Pr\left[q(r^*) \geq OPT_q(D) - \frac{2\Delta}{\epsilon}\left(\log(|R|) + \log(OPT_q(D)\right)\right] \geq 1 - \frac{1}{OPT_q(D)}$$

The Exponential Mechanism

Theorem:

$$\Pr\left[q(r^*) \leq OPT_q(D) - \frac{2\Delta}{\epsilon}\left(\log\left(\frac{|R|}{|R_{OPT}|}\right) + t\right)\right] \leq e^{-t}$$

Corollary:

$$\mathrm{E}[q(r^*)] \geq OPT_q(D) \; - \frac{2\Delta}{\epsilon}\left(\log(|R|) + \log\left(OPT_q(D)\right)\right) - 1$$

Proof:

$E[q(r^*)] \geq (x \cdot \Pr[q(r^*) \geq x])$

$\geq \left(OPT_q(D) \; - \frac{2\Delta}{\epsilon}\left(\log(|R|) + \log\left(OPT_q(D)\right)\right)\right) \cdot \left(1 - \frac{1}{OPT_q(D)}\right)$

$> OPT_q(D) \; - \frac{2\Delta}{\epsilon}\left(\log(|R|) + \log\left(OPT_q(D)\right)\right) - 1$