1/30/25:

Exponential Mechanism:

Previous setup: utility was directly connected to noise added.

- Not always the case! Sometimes utility very complicated fn of noise, or not even numeric in first place!

Ex from last: auctions.

Want to set price, but keep bids private. (max revenue)

Four bidders A, B, C, D.

A, B, C: $1

D: $3.01

utility (revenue): $x \leq 3.01$: x

> 3.01: 0

Exponential mechanism: queries w/ arbitrary utilities, possibly non-numeric range, DP.

Start from some setup: database $\mathcal{D}$, want to output something from range R.

What is "something"?

$u : \mathcal{D} \times R \to \mathbb{R}$ utility function

- If our database is D, and output $\in R$,
  $u(D, r)$ is how happy we are.
  So want to output $\operatorname{argmax}_{r \in R} u(D, r)$

Sensitivity: only measured for database parameter

$$\Delta u = \max_{r \in R} \max_{D \sim D'} |u(D, r) - u(D', r)|$$

Def (Exponential mechanism): $M_\varepsilon(D, u, R)$:

output $r \in R$ with probability proportional to $\exp\left(\frac{\varepsilon u(D, r)}{2\Delta u}\right)$

Thm: Exponential mechanism is ε-DP.

Pf: Let $D \sim D' \in \mathcal{D}$, $r \in R$.

$$\frac{\Pr[M_\varepsilon(D, u, R) = r]}{\Pr[M_\varepsilon(D', u, R) = r]} = \frac{\frac{\exp\left(\frac{\varepsilon u(D, r)}{2\Delta u}\right)}{\sum_{r' \in R} \exp\left(\frac{\varepsilon u(D, r')}{2\Delta u}\right)}}{\frac{\exp\left(\frac{\varepsilon u(D', r)}{2\Delta u}\right)}{\sum_{r' \in R} \exp\left(\frac{\varepsilon u(D', r')}{2\Delta u}\right)}}$$

$$= \frac{\exp\left(\frac{\varepsilon \cdot u(D,r)}{2\Delta u}\right)}{\exp\left(\frac{\varepsilon \cdot u(D',r)}{2\Delta u}\right)} \cdot \frac{\sum_{r' \in R} \exp\left(\frac{\varepsilon \cdot u(D',r')}{2\Delta u}\right)}{\sum_{r' \in R} \exp\left(\frac{\varepsilon \cdot u(D,r')}{2\Delta u}\right)}$$

$$= \exp\left(\frac{\varepsilon (u(D,r) - u(D',r))}{2\Delta u}\right) \cdot \frac{\sum_{r' \in R} \exp\left(\frac{\varepsilon \cdot u(D',r')}{2\Delta u}\right)}{\sum_{r' \in R} \exp\left(\frac{\varepsilon \cdot u(D,r')}{2\Delta u}\right)}$$

$$\leq \exp\left(\frac{\varepsilon}{2}\right) \cdot \frac{\sum_{r' \in R} \exp\left(\frac{\varepsilon \cdot u(D',r')}{2\Delta u}\right)}{\sum_{r' \in R} \exp\left(\frac{\varepsilon \cdot u(D,r')}{2\Delta u}\right)}$$

$$\leq \exp\left(\frac{\varepsilon}{2}\right) \cdot \frac{\sum_{r' \in R} \exp\left(\frac{\varepsilon \left(u(D,r') + \Delta u\right)}{2\Delta u}\right)}{\sum_{r' \in R} \exp\left(\frac{\varepsilon \cdot u(D,r')}{2\Delta u}\right)}$$

$$= \exp\left(\frac{\varepsilon}{2}\right) \cdot \frac{\sum_{r' \in R} \exp\left(\frac{\varepsilon}{2}\right) \exp\left(\frac{\varepsilon \cdot u(D,r')}{2\Delta u}\right)}{\sum_{r' \in R} \exp\left(\frac{\varepsilon \cdot u(D,r')}{2\Delta u}\right)}$$

$$= \exp\left(\frac{\varepsilon}{2}\right) \cdot \exp\left(\frac{\varepsilon}{2}\right) = \exp(\varepsilon) \qquad \checkmark$$

Quality: Is exponential mechanism "good"?

Intuition: probability drops exponentially w/ utility, so might be pretty good quality!

Def: Let $OPT_u(D) = \max_{r \in R} u(D,r)$ be max achievable utility.

Let $R_{OPT}(D) = \{r \in R : u(D,r) = OPT_u(D)\}$ be outputs with max utility

Thm: $\Pr[u(M_E(D,u,R)) \leq OPT_u(D) - \frac{2\Delta u}{\varepsilon}\left(\ln\left(\frac{|R|}{|R_{OPT}(D)|}\right) + t\right)]$

$\leq e^{-t}$

Pf: Fix some c. Let $S_c = \{r \in R : u(D,r) \leq c\}$

$$\Pr[u(M_E(D,u,R)) \leq c] = \Pr[M_E(D,u,r) \in S_c]$$

$$= \frac{\sum_{r \in S_c} \exp\left(\frac{\varepsilon u(D,r)}{2\Delta u}\right)}{\sum_{r \in R} \exp\left(\frac{\varepsilon u(D,r)}{2\Delta u}\right)} \leq \frac{\sum_{r \in S_c} \exp\left(\frac{\varepsilon c}{2\Delta u}\right)}{\sum_{r \in R_{OPT}(D)} \exp\left(\frac{\varepsilon \cdot OPT_u(D)}{2\Delta u}\right)}$$

$$\leq \frac{|S_c| \exp\left(\frac{\varepsilon c}{2\Delta u}\right)}{|R_{OPT}(D)| \exp\left(\frac{\varepsilon OPT_u(D)}{2\Delta u}\right)}$$

$$\leq \frac{|R|}{|R_{OPT}(D)|} \cdot \exp\left(\frac{\varepsilon(c - OPT_u(D))}{2\Delta u}\right)$$

Set $c = OPT_u(D) - \frac{2\Delta u}{\varepsilon}\left(\ln\left(\frac{|R|}{|R_{OPT}(D)|}\right) + t\right)$:

$$\leq \frac{|R|}{|R_{OPT}(D)|} \cdot \exp\left(\frac{\varepsilon\left(-\frac{2\Delta u}{\varepsilon}\left(\ln\left(\frac{|R|}{|R_{OPT}(D)|}\right) + t\right)\right)}{2\Delta u}\right)$$

$$= \frac{|R|}{|R_{OPT}(D)|} \cdot \exp\left(-\ln\left(\frac{|R|}{|R_{OPT}(D)|}\right) - t\right)$$

$$= \exp(-t) \quad \checkmark$$

(Note: other, more refined versions. See, e.g., Vadhan (?).)

(Corollary: $\Pr[u(M_\varepsilon(D, u, R)) \leq OPT_u(D) - \frac{2\Delta u}{\varepsilon}(\ln|R| + t)]$

$$\leq e^{-t}$$

Pf: $|R_{OPT}(D)| \geq 1$ $\checkmark$

Ex: Best of 2.

Two medical conditions, A and B. which more common?

Sps true count of B = true count of A + C.

$u(B) = u(A) + C$ (utilities are true counts).

$$\Pr[\text{Count}_{\text{out}} A] = \Pr[u(M_\varepsilon(D,u)) \le OPT_u(D) - C$$

$$C = \frac{2\Delta u}{\varepsilon}(\ln|R| + t) \le \frac{2}{\varepsilon}(t+1)$$

$$\Rightarrow t \ge C\frac{\varepsilon}{2} - 1$$

$$\Rightarrow \Pr[\text{Count}_{\text{out}} A] \le e^{1 - \frac{C\varepsilon}{2}}$$

Ex: Laplace Mechanism!

Sps $f: \mathcal{D} \to \mathbb{R}$, sensitivity Δf

Laplace: add $Lap(\frac{\Delta f}{\varepsilon})$ noise, i.e.

$$\Pr[M_L(f, D) = x] \propto \exp\left(-\frac{\varepsilon|x - f(D)|}{\Delta u}\right)$$

Exponential: use $R = \mathbb{R}$, $u(D, r) = |r - f(D)|$

$$\Rightarrow \Pr[M_E(D, u, r) = x) \propto \exp\left(-\frac{\varepsilon|x - f(D)|}{2\Delta u}\right)$$

Discussion: Exponential Mechanism super powerful!

Main downside: how do we actually implement?

Naive version: enumerate R, write down all probabilities, sample.

works, but requires enumerating R!

often don't want to enumerate full range: way too slow.

Ex: Synthetic database.

Say given D, want to output synthetic database that looks "similar" to D: for some class of queries, answers similar.

Idea: $d(D, \hat{D})$ = how close is $\hat{D}$ to D in terms of query class?

$\Rightarrow$ exponential mechanism works!

But need to enumerate all possible synthetic databases...