Local DP

All privacy problems discussed so far were based on an assumption:

A private dataset is held by a trusted central entity (such as hospital or bank).

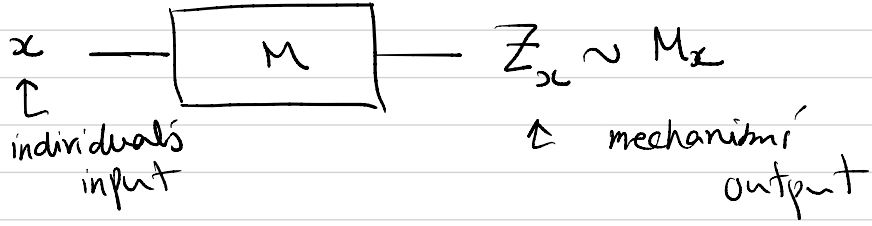
What if there can't be such central entity that's trusted by all individuals?

Example: we wish to find how many women in North Carolina have undergone abortion? We take a sample of women there & ask them. this is what statistician have been doing

for decades. The caveat here in North Carolina, it is a crime to do abortion. So no body answer the question truthfully !

To address problem like this, we need to let each individual randomize their data before they release it publicly.

Consider the following the mechanism:



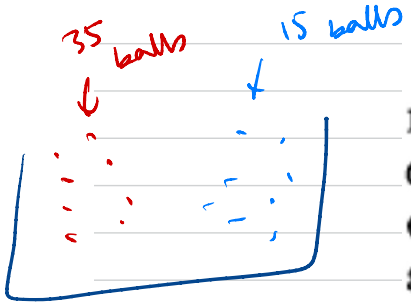
Estimate of Abortion Rate

* In 1955, there was a conference "Conference on Abortion". Somehow, they "guessed" there are 200k of Abortion / year.
* In 1970, 3 statisticiens wanted to have a better estimate

I was pregnant at some time during the past 12 months and had an abortion which ended the pregnancy. — Red

I was born in the month of April. — Blue

* "Estimates of Induced Abortion in Urban North Carolina" by Abernathy, Greenberg & Horvitz



The first printed question had a small red ball in front of it while the second question had a blue ball in the same location. Inside the box there were 35 red and 15 blue balls. The respondent was asked to shake the box of balls thoroughly, and to tip the box allowing one of the freely moving balls to appear in a "window" which was clearly visible to the respondent. The color of the ball which appeared in the window determined which of the two questions the respondent was supposed to answer. If a red ball appeared, she answered the abortion question; if a blue ball appeared, she answered the other question.

Suppose we have λ as the number of ppls who said "Yes".

$$\lambda = E[\text{"Number of Yes"}] = \text{"ppl who had abortion"} \times \Pr(\text{"red ball"}) + \text{"ppl born in April"} \times \Pr(\text{"blue ball"})$$

$\Pr(\text{"red ball"}) = 35/50$

$\Pr(\text{"blue ball"}) = 15/50$

$=$

* They showed that the abortion rate $\approx$ 32%

In 1973, SC passed a remarkable ruling, "Roe v Wade" that legalized federal abortion [14th amendment of constitution]

* In 2022, "Roe v Wade" was overturned.

Suppose we get λ number of "Yes"

$$E[\text{"Number of Yes"}] = \lambda$$

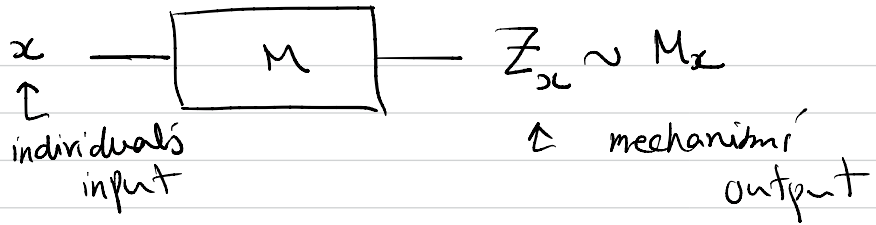
$$\#\text{ ppl who had abortion} \times \Pr(\text{"answer first question"}) + \#\text{ ppl born April} \times \Pr(\text{"answer second question"}) = \lambda$$

$$\Rightarrow \left(\#\text{ ppl with abortion}\right)\cdot\frac{35}{50} + \left(\#\text{ ppl born in April}\right)\frac{15}{50} = \lambda \qquad = \lambda$$

they showed that the abortion rate $\approx$ 32%.

In 1973, S.C passed a landmark ruling, "Roe v Wade"

In 2022, this was over turned!



Def. We say mechanism M is ε-locally DP (or ε-LDP for short) if

$$E_{e^\varepsilon}(M_x \| M_{x'}) = 0 \qquad \forall\ x \& x' \text{ possible inputs}.$$

Example. Randomized-response mechanism:



$Z \sim \text{Ber}(r)$ if $x=0$ & $Z \sim \text{Ber}(1-r)$ if $x=1$

In fact, r indicates the lying probability.

* Show that this mechanism is ε-LDP if $r = \frac{1}{1+e^\varepsilon}$.

Theorem. A mechanism M is ε-LDP if & only if

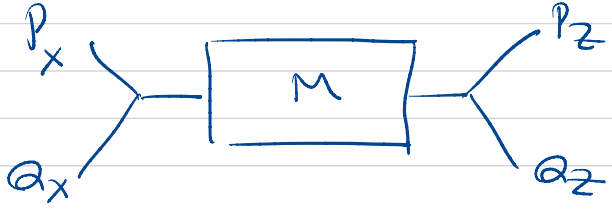
$$\eta_{e^\varepsilon}(M) = 0$$

Proof: HW4

In other word, an ε-LDP mechanism always satisfied:

$$E_{e^\varepsilon}(P_Z \| Q_Z) = 0 \quad \forall\ P_X \& Q_X$$

where P_Z & Q_Z are the output distributions of M when input distributions are P_X & Q_X.



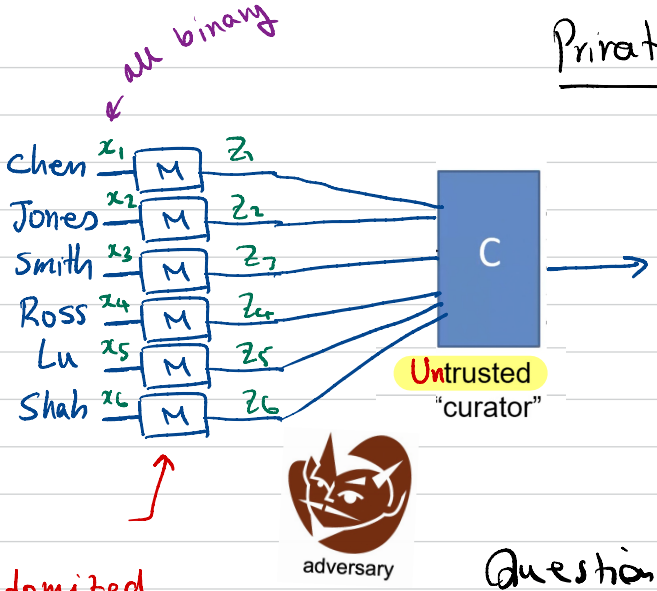
Example: Prove that the following mechanism is ε-LDP:

$$P_{Z|X}(z|x) = \begin{cases} \frac{e^{\varepsilon}}{e^{\varepsilon}+k-1} & z = x \in \{1,2,\cdots,k\} \\ \frac{1}{e^{\varepsilon}+k-1} & z \neq x \\ 0 & z \notin \{1,2,\cdots,k\} \end{cases}$$

* In HW1, we already proved that $\eta_{e^{\varepsilon}}(P_{Z|X}) = 0$, showing that this mechanism is ε-LDP.

* this mechanism is known as k-ary randomized response, because both input & output take values in $\{1,2,\cdots,k\}$.

Private estimation: Binary case



ε-DP Randomized response

We are interested in

$\frac{1}{n}\sum x_i \equiv$ Proportion of "Yes"

But we need to estimate this using z_i

Question: Is $\sum z_i$ a good estimate for $\sum x_i$? No!

Let's look at one example:

$$E[z_1] = x_1 \cdot Pr(z_1 = x_1) + (1-x_1) \cdot Pr(z_1 \neq x_1) = \dots$$

$$\Rightarrow x_1 = \frac{e^{\varepsilon}+1}{e^{\varepsilon}-1} \cdot E[z_1] - \frac{1}{e^{\varepsilon}-1}$$

Thus, Z_1 is not an unbiased estimate of x, but:

$$\tilde{Z}_1 := \frac{e^{\varepsilon}+1}{e^{\varepsilon}-1} \cdot Z_1 - \frac{1}{e^{\varepsilon}-1} \quad \text{is an unbiased estimate}$$

$\Rightarrow$ Therefore,

$$\frac{1}{n}\,\frac{e^{\varepsilon}+1}{e^{\varepsilon}-1} \cdot \sum_{i=1}^{n} Z_i - \frac{1}{e^{\varepsilon}-1} \quad \text{is an unbiased estimate of } \frac{1}{n}\sum x_i.$$

Comparison with Central DP:

ε-DP CDP: $Z := \frac{1}{n}\sum x_i + N \longrightarrow E\left[\left(Z - \frac{1}{n}\sum x_i\right)^2\right] = \mathrm{Var}(N) = \frac{2}{n^2\varepsilon^2}$, where $N \sim \mathcal{L}(0, 1/n\varepsilon)$

ε-DP LDP: $\tilde{Z} := \frac{1}{n}\,\frac{e^{\varepsilon}+1}{e^{\varepsilon}-1} \sum Z_i - \frac{1}{e^{\varepsilon}-1} \longrightarrow E\left[\left(\tilde{Z} - \frac{1}{n}\sum x_i\right)^2\right] = \mathrm{Var}(\tilde{Z})$

$$\leq \frac{1}{4n}\left(\frac{e^{\varepsilon}+1}{e^{\varepsilon}-1}\right)^2$$

For small ε: $\frac{e^{\varepsilon}+1}{e^{\varepsilon}-1} \approx \frac{1}{\varepsilon} \Rightarrow \quad Var(\tilde{z}) \leq \frac{1}{4n\varepsilon^2}$

The error in CDP is $O(n)$ smaller!

A more flexible notion of utility is:

$$Pr\left(\left| \tilde{z} - \frac{1}{n}\sum x_i \right| \geq t \right)$$

using Chebyshev's inequality, it can be shown that $Var(\tilde{z})$ gives an upper bound:

Chebyshev: $$Pr\left(\left| \tilde{z} - \frac{1}{n}\sum x_i \right| \geq t \right) \leq \frac{Var(\tilde{z})}{t^2}$$

Exercise: Suppose n users have binary (Private) inputs $x_i \in \{0,1\}$. Each employs the following mechanism:

x_i: 0 → NO, 1 → Yes

toss a fair coin → Heads: Truth

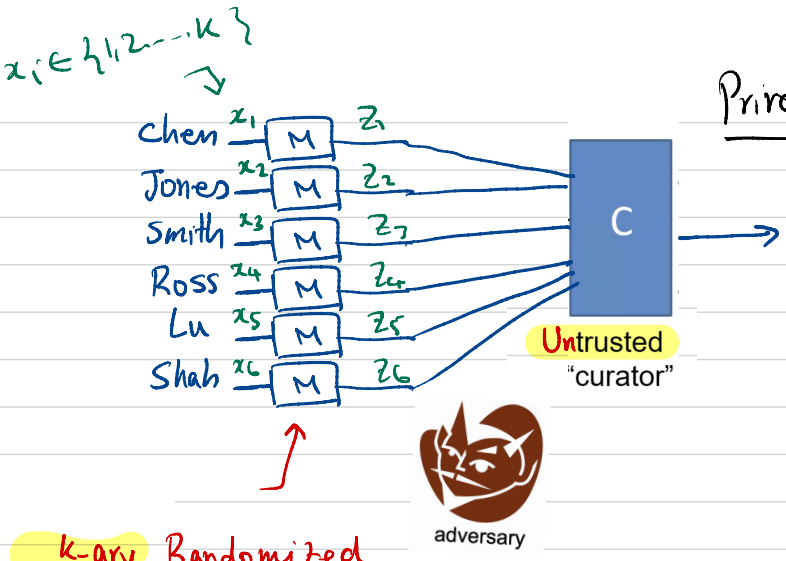
→ Tail: Toss the coin again → Heads: Truth

→ Tail: Lie

What is the privacy guarantee?

Let Y be the proportion of 1's received. Prove that the actual proportion of 1's is $2(Y - 0.25)$.

Private estimation: Non-binary case



we wish to estimate

$$p_j := \frac{1}{n} \#\{i : x_i = j\}$$

Proportion of people whose response was j

Theorem. An unbiased estimator for p_j is

$$\hat{p}_j := \frac{e^\varepsilon + k - 1}{e^\varepsilon - 1}\left[N_j^\varepsilon - \frac{1}{e^\varepsilon + k - 1}\right]$$

N_j^ε: $\frac{1}{n} \#\{i : z_i = j\}$

Proof. $E[N_j^\varepsilon] = E\left[\frac{1}{n}\sum_{i=1}^{n} \mathbb{1}\{z_i = j\}\right] = \frac{1}{n}\sum_{i=1}^{n} \Pr\{z_i = j\}$

$$= \frac{1}{n}\sum_{i=1}^{n} \frac{e^\varepsilon}{k-1+e^\varepsilon}\mathbb{1}\{x_i = j\} + \frac{1}{k-1+e^\varepsilon}\mathbb{1}\{x_i \neq j\}$$

$$= \frac{e^\varepsilon}{k-1+e^\varepsilon}\underbrace{\frac{1}{n}\sum_{i=1}^{n}\mathbb{1}\{x_i = j\}}_{p_j} + \frac{1}{k-1+e^\varepsilon}\underbrace{\frac{1}{n}\sum_{i=1}^{n}\mathbb{1}\{x_i \neq j\}}_{1-p_j}$$

$$\Rightarrow \quad E[N_j^\varepsilon] = \frac{e^\varepsilon}{k-1+e^\varepsilon}p_j + \frac{1}{k-1+e^\varepsilon}(1-p_j)$$

Thus, $\hat{p}_j = \frac{k-1+e^\varepsilon}{e^\varepsilon-1}N_j^\varepsilon - \frac{1}{e^\varepsilon-1}$ is an unbiased estimator for p_j, with ε-LDP guarantee.

□

Utility:

$$\Pr\left(|\hat{P}_j - P_j| \geq t \right) \leq \frac{\mathrm{Var}(\hat{P}_j)}{t^2}$$

↑ Chebyshev's inequality

so we need to compute $\mathrm{Var}(\hat{P}_j)$.

$\hat{P}_j = \frac{1}{n} \sum 1\{z_i = j\}$

$$\mathrm{Var}(\hat{P}_j) = \mathrm{Var}\left(\frac{e^{\varepsilon}+k-1}{e^{\varepsilon}-1} \hat{N}_j^{\varepsilon} \right) = \left(\frac{e^{\varepsilon}+k-1}{e^{\varepsilon}-1} \right)^2 \mathrm{Var}\left(\hat{N}_j^{\varepsilon} \right)$$

$$= \frac{1}{n^2} \left(\frac{e^{\varepsilon}+k-1}{e^{\varepsilon}-1} \right)^2 \sum \underbrace{\mathrm{Var}(1\{z_i = j\})}_{\leq \frac{1}{4}}$$

$$\leq \frac{1}{4n} \left(\frac{e^{\varepsilon}+k-1}{e^{\varepsilon}-1} \right)^2.$$

$$\Rightarrow \text{Utility: } \Pr\left(|\hat{P}_j - P_j| \geq t \right) \leq \frac{\mathrm{Var}(\hat{P}_j)}{t^2} \leq \frac{1}{4nt^2} \left(\frac{e^{\varepsilon}+k-1}{e^{\varepsilon}-1} \right)^2.$$