CS208: Applied Privacy for Data Science
DP Foundations: the Laplace Mechanism

James Honaker & Salil Vadhan
School of Engineering & Applied Sciences
Harvard University

February 22, 2019
Differential Privacy

M is $\epsilon$-DP if

$$Pr[M(D, q) \in T] \leq (1 + \epsilon)Pr[M(D', q) \in T], \quad \forall T, q.$$
Differential Privacy

$M$ is $\epsilon$-DP if

$$Pr[M(D, q) \in T] \leq (1 + \epsilon)Pr[M(D', q) \in T], \quad \forall \ T, q.$$  

- $D, D'$ Neighbouring datasets
Differential Privacy

$M$ is $\epsilon$-DP if

$$ \Pr[M(D, q) \in T] \leq e^\epsilon \Pr[M(D', q) \in T], \quad \forall T, q. $$

- $D, D'$ Neighbouring datasets
- $M$ Mechanism that Maps from data to result
Differential Privacy

M is $\epsilon$-DP if

$$Pr[M(D, q) \in T] \leq e^\epsilon Pr[M(D', q) \in T], \quad \forall T, q.$$ 

- $D, D'$ Neighbouring datasets
- $M$ Mechanism that Maps from data to result
- $q$ Query
- $T$ Set providing a decision rule
$e^\epsilon$ vs. $(1 + \epsilon)$

see `expEpsilon.r`
\[ x_i = x_{\text{min}} \]

\[ \bar{X}(x_i) = \sum_{j \neq i} \frac{x_j}{N-1} + \frac{x_{\text{min}}}{N} \]
\[ x_i = x_{\text{min}} \]
\[ \bar{X}(x_i) = \sum_{j \neq i} \frac{x_j}{N-1} + \frac{x_{\text{min}}}{N} \]
\[ \bar{X}(x'_i) = \sum_{j \neq i} \frac{x_j}{N-1} + \frac{x_{\text{max}}}{N} \]
\[ x'_i = x_{\text{max}} \]
The Laplace has density over $y$:

$$f_{\text{Laplace}}(y|s, \mu) = \text{Lap}(s, \mu) = \frac{1}{2s} \exp\left(-\frac{|y - \mu|}{s}\right)$$
The Laplace has density over $y$:

$$f_{\text{Laplace}}(y|s) = \text{Lap}(s) = \frac{1}{2s} \exp\left(-\frac{|y|}{s}\right)$$

We were given the theorem:

$$M(x, q) = q(x) + \text{Lap}(\text{GS}_q/\epsilon)$$
The Laplace has density over $y$:

$$f_{\text{Laplace}}(y|s) = \text{Lap}(s) = \frac{1}{2s} \exp\left(-\frac{|y|}{s}\right)$$

We were given the theorem:

$$M(x, q) = q(x) + \text{Lap}(GS_q/\epsilon)$$

So our differentially private mean, $M(X)$, which combines the "true" sample mean with Laplace noise, becomes:

$$M(x) = \bar{x} + Z; \quad Z \sim \text{Lap}(s = GS_q/\epsilon)$$
see laplaceDistributions.r
\[ \frac{\text{pr}[M(x) = t]}{\text{pr}[M(x') = t]} = e^{\frac{-\epsilon|\bar{x} - t|}{G_{S_q}}} = e^{\frac{\epsilon|x' - t| - \epsilon|\bar{X} - t|}{G_{S_q}}} = e^{\frac{\epsilon|x' - \bar{x}|}{G_{S_q}}} \leq e^\epsilon \]

since we know \( G_{S_q} \geq |\bar{x}' - \bar{x}| \) by the def. of sensitivity. Thus we meet the original definition:

\[ Pr[M(x) = t] \leq e^\epsilon Pr[M(x') = t] \]
Two Laplace distributions, for two adjacent datasets $x$ and $x'$. The definition of $\epsilon$-differential privacy requires the ratio of $M(x)/M(x')$ is not greater than $e^\epsilon$ for all points along the $x$-axis. Thus for any realized output $z$ (for example here, $z = 1.3$) we can not determine that $x$ or $x'$ were more likely to have produced $z$. 
Exponential Distribution

Survivor Function, Conditional on $t$

$S(t|t>k)$
Exponential Distribution

Survivor Function, Conditional on $t$
see laplaceMeanRelease.r