Gaussian Noise Mechanism

Sensitivity, again

The ℓ_2 *sensitivity* of $f : \mathcal{X}^n \to \mathbb{R}^k$ is

$$\Delta_2 f = \max_{X \sim X'} \|f(X) - f(X')\|_2 = \max_{X \sim X'} \left(\sum_{i=1}^{k} |f(X)_i - f(X')_i|^2 \right)^{1/2}$$

$\forall z \in \mathbb{R}^k \quad \|z\|_2 \leq \|z\|_1$

$\Rightarrow \quad \Delta_2 f \leq \Delta_1 f$

Sensitivity of a workload of counting queries, again

$q_1, \ldots, q_k$ are counting queries

$$Q(X) = \begin{pmatrix} q_1(X) \\ \vdots \\ q_k(X) \end{pmatrix} \qquad \Delta_2 Q \le \frac{\sqrt{k}}{n}$$

$$\Delta_2 Q = \max_{X \sim X'} \underbrace{\left(\sum_{i=1}^{k} \underbrace{|q_i(X) - q_i(X')|^2}_{\le 1/n^2} \right)}_{\le \frac{k}{n^2}}^{1/2} \le \frac{\sqrt{k}}{n}$$

Gaussian noise mechanism

The Gaussian noise mechanism $\mathcal{M}_{\text{Gauss}}$ (for a function $f : \mathcal{X}^n \to \mathbb{R}^k$) outputs

$$\mathcal{M}_{\text{Gauss}}(X) = f(X) + Z,$$

$Z_1, \ldots, Z_k$ are independent Gaussians

where $Z \in \mathbb{R}^k$ is sampled from $\mathrm{N}\left(0, \frac{(\Delta_2 f)^2}{\rho} \cdot \underline{I}\right)$.

ρ is a parameter, to be decided

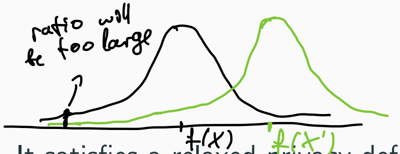
I identity matrix $\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}$

$\mathrm{N}(\mu, \Sigma)$ is the *Gaussian distribution* on $\mathbb{R}^k$ with expectation $\mu \in \mathbb{R}^k$ and covariance matrix Σ.

When $\Sigma = \sigma^2 I$, it has pdf

$$p(z) = \frac{1}{(2\pi)^{k/2}\sigma^k} e^{-\|z-\mu\|_2^2/(2\sigma^2)} = \frac{1}{(2\pi)^{k/2}\sigma^k} \exp\left(-\frac{1}{2\sigma^2}\sum_{i=1}^{k} |z_i - \mu_i|^2\right)$$

Problem: Gaussian tails drop off too fast! $\mathcal{M}_{\text{Gauss}}$ is not ε-DP for any $\varepsilon < \infty$.



It satisfies a relaxed privacy definition.

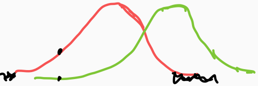
Definition

A mechanism $\mathcal{M}$ is (ε, δ)-*differentially private* if, for any two neighbouring datasets X, X', and any set of outputs S

$$\mathbb{P}(\mathcal{M}(X) \in S) \leq e^{\varepsilon}\mathbb{P}(\mathcal{M}(X') \in S) \underline{+ \delta}$$

We will ask that $\delta \ll \frac{1}{n}$, so that we do not allow "name and shame" mechanism

Privacy of the Gaussian noise mechanism



$$\mathcal{M}_{\text{Gauss}}(X) = f(X) + \underset{\in \mathbb{R}^k}{Z}, \quad \underset{\in \mathbb{R}^k}{Z} \sim \mathrm{N}\left(0, \frac{(\Delta_2 f)^2}{\rho} \cdot I\right)$$

To get (ε,δ)-DP
$\rho \approx \frac{\varepsilon^2}{\log(1/\delta)}$

→ For any $\delta > 0$, $\mathcal{M}_{\text{Gauss}}$ is (ε, δ)-DP for $\varepsilon = \frac{\sqrt{\rho}}{2}(\sqrt{\rho} + 2\sqrt{2\ln(1/\delta)}) \approx \sqrt{\rho \ln(1/\delta)}$

$X \sim X'$: $p(z)$ pdf of $\mathcal{M}_{\text{Gauss}}(X)$; $p'(z)$ pdf of $\mathcal{M}_{\text{Gauss}}(X')$

Claim: enough to show that, for $T = \{z \in \mathbb{R}^k : \frac{p(z)}{p'(z)} > e^{\varepsilon}\}$, $\mathbb{P}(\mathcal{M}_{\text{Gauss}}(X) \in T) \leq \delta$.

↳ "bad set of outputs" (reveal too much)

$S \subseteq \mathbb{R}^k$

$$\mathbb{P}(\mathcal{M}_{\text{Gauss}}(X) \in S) = \mathbb{P}(\mathcal{M}_{\text{Gauss}}(X) \in S \setminus T) + \underbrace{\mathbb{P}(\mathcal{M}_{\text{Gauss}}(X) \in S \cap T)}_{\leq \delta}$$

$$\leq \int_{S \setminus T} p(z)\,dz + \delta \leq e^{\varepsilon} \int_{S\setminus T} p'(z)\,dz + \delta$$

$$= e^{\varepsilon} \overbrace{\mathbb{P}(\mathcal{M}_{\text{Gauss}}(X') \in S \setminus T)}^{\leq \mathbb{P}(\mathcal{M}_{\text{Gauss}}(X') \in S)} + \delta$$

$T = \{ z : \ln \frac{p(z)}{p'(z)} > \varepsilon \}$

$u, v \in \mathbb{R}^k$ $\quad \langle u, v \rangle = \sum_{i=1}^{k} u_i v_i = u^T v = v^T u$

$$\ln \frac{p(z)}{p'(z)} = \frac{\rho \cdot \overbrace{\|f(X) - f(X')\|_2^2}^{\le (\Delta_2 f)^2}}{2(\Delta_2 f)^2} + \frac{\rho \cdot \overbrace{\langle z - f(X), f(X) - f(X') \rangle}}{(\Delta_2 f)^2}$$

$$\le \frac{\rho}{2} + \frac{\rho \langle z - f(X), f(X) - f(X') \rangle}{(\Delta_2 f)^2}$$

$\varepsilon = \frac{\rho}{2} + \sqrt{2 \rho \ln(1/\delta)}$

$$T \subseteq \left\{ z : \frac{\rho \langle z - f(X), f(X) - f(X') \rangle}{(\Delta_2 f)^2} > \sqrt{2\rho \ln 1/\delta} \right\}$$

Privacy of the Gaussian noise mechanism

$\sum v_i Z_i$ $\qquad$ $\sum v_i^2$

1. For any $v \in \mathbb{R}^k$, and $Z \sim \mathrm{N}(0, \sigma^2 I)$, $\qquad \langle Z, v\rangle \sim \mathrm{N}(0, \sigma^2 \|v\|_2^2)$.
2. $Z \sim \mathrm{N}(0, \sigma^2)$, then $\qquad \mathbb{P}(Z > t) < e^{-t^2/(2\sigma^2)}$.

$Z \sim N\left(0, \frac{(\Delta_2 f)^2}{\rho} I\right)$

Then $\qquad \mathcal{M}_{Gauss}(X) = f(X) + Z$

$$\underbrace{\mathbb{P}(\mathcal{M}_{\mathrm{Gauss}}(X) \in T)}_{\wedge\delta} \le \mathbb{P}\left(\underbrace{\boxed{\frac{\rho \cdot \langle Z, f(X) - f(X')\rangle}{(\Delta_2 f)^2}}}_{\sim N(0,\sigma^2)} > \frac{\sqrt{2\rho \ln(1/\delta)}}{\cancel{\rho}}\right)$$

$\sigma^2 = \frac{\rho^2}{\cancel{(\Delta_2 f)^2}} \cdot \frac{\|f(X) - f(X')\|_2^2 \; \cancel{(\Delta_2 f)^2}}{\cancel{\rho}}$

$\sigma^2 \le \rho$

$\mathbb{P}(G > \sqrt{2\rho \ln(1/\delta)}) < \delta$

$G \sim N(0, \sigma^2) \qquad \sigma^2 \le \rho$

Accuracy of the Gaussian noise mechanism

$Z \sim \mathrm{N}(\mu, \sigma^2)$, then $\qquad \mathbb{P}(|Z-\mu| > t) < 2e^{-t^2/(2\sigma^2)}$.

Exercise: for k counting queries, with ρ set s.t. $\mathcal{M}_{Gauss}$ satisfies (ε, δ)-DP, we have

$$\mathbb{P}(\max \text{ error} \geq \alpha) \leq \beta$$

if $\quad n \gg \dfrac{\sqrt{k \log 1/\delta}}{\varepsilon \alpha}$