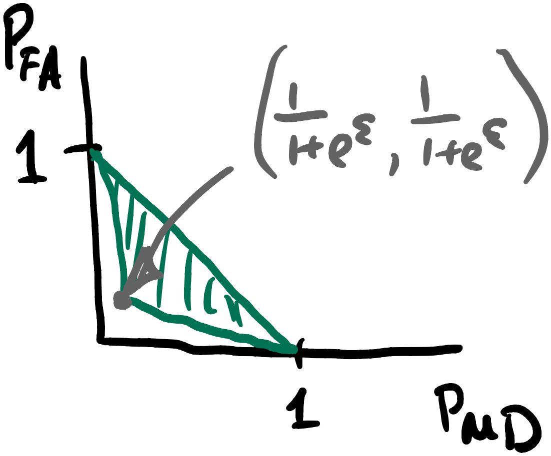
Recall Last time:

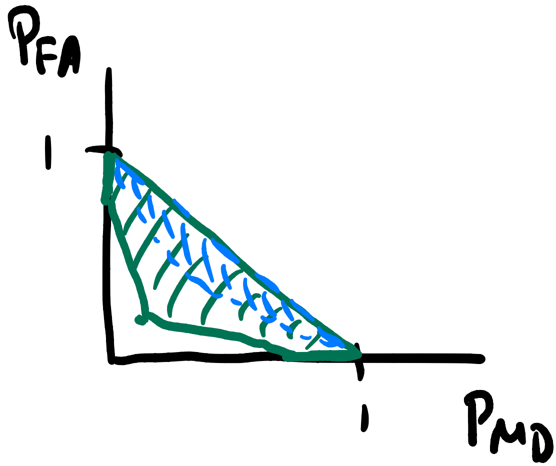
Hypothesis Testing and DP

- Privacy Region

ε-DP



(ε, δ)-DP



- M is (ε, δ)-DP $\Rightarrow$ M is $(\tilde{\varepsilon}, \tilde{\delta})$-DP for any $\hat{\delta} \geq \delta$ and

$$\frac{1-\delta}{1+e^{\varepsilon}} \geq \frac{1-\hat{\delta}}{1+e^{\tilde{\varepsilon}}}$$

Rényi Differential Privacy

Anatomy of the Paper:

I. Introduction

II. DP and its flavors — meaning of (ε,δ)-DP

III. Rényi DP — Def^n & Properties of RDP

IV. RDP & (ε,δ)-DP

(α,ε)-RDP $\Rightarrow$ $(\varepsilon_\delta,\delta)$-DP

V. Advance Composition theorem

VI. Mechanisms

VII & VIII Discussion & Concluding Remarks

Recall:

- ε-DP

Privacy mechanism $f: \mathcal{D} \to \mathcal{R}$

event

$$\mathbb{P}[f(D) \in S] \le e^{\varepsilon}\, \mathbb{P}[f(D') \in S]$$

D & D' are neighboring databases

- (ε, δ)-DP

$$\mathbb{P}[f(D) \in S] \le e^{\varepsilon}\, \mathbb{P}[f(D') \in S] + \delta$$

New def$\underline{^n}$

- Def$\underline{^n}$ 4 [(α, ε)-RDP]: A randomized mechanism $f: \mathcal{D} \to \mathcal{R}$ is said to have ε-RDP of order $\alpha \ge 1$, or (α, ε)-RDP, if for any adjacent $D, D' \in \mathcal{D}$

$$D_\alpha(P \| Q) = \frac{1}{\alpha - 1} \log \mathbb{E}_{x \sim Q}\left[\left(\frac{P(x)}{Q(x)}\right)^{\alpha}\right]$$

$$D_\alpha(f(D) \| f(D')) \le \varepsilon.$$

Rényi divergence of order α

$\approx$ ε-DP for $\alpha = \infty$

$\alpha = 1$: KL-Divergence (Relative Entropy)

$\alpha = \infty$: $$D_\infty(P \| Q) = \sup_{x \in \text{support of } Q} \log \frac{P(x)}{Q(x)}$$

in general $D_\alpha(P \| Q) \le D_\beta(P \| Q)$

$\beta \ge \alpha$

Properties:

- "Bad outcomes" Guarantee

$$e^{-\varepsilon} \mathbb{P}[f(D') \in S]^{\alpha/\alpha-1} \leq \mathbb{P}[f(D) \in S]$$

$$\leq \left(e^{\varepsilon} \mathbb{P}[f(D') \in S]\right)^{\alpha-1/\alpha}$$

- Post-Processing

$$D_\alpha(P \| Q) \geq D_\alpha(g(P) \| g(Q))$$

$g: R \to R'$
a random mechanism

if f is (α, ε)-RDP
so is $g(f(\cdot))$.

- Composition

$f: D \to R_1$ is (α, ε_1)-RDP
and
$g: R_1 \times D \to R_2$ is (α, ε_2)-RDP
then f, g are $(\alpha, \varepsilon_1 + \varepsilon_2)$-RDP.

- Group Privacy

Proposition 2: If $f: \mathcal{D} \to \mathcal{R}$ is (α, ε)-RDP, $g: \mathcal{D} \mapsto \mathcal{D}'$ is 2^c-stable and $\alpha \geq 2^{c+1}$, then $f \circ g$ is $(\alpha/2^c, 3^c\varepsilon)$-RDP

$g: \mathcal{D} \to \mathcal{D}'$ is c-stable means neighbors in $\mathcal{D}'$ are at most c apart in $\mathcal{D}$.

- (α, ε)-RDP and (ε, δ)-DP
  - (∞, ε)-RDP $\Leftrightarrow$ ε-DP

$\Rightarrow$ (α, ε)-RDP $\forall \; 1 \leq \alpha \leq \infty$

Proposition 3: If f is an (α, ε)-RDP then it is also $\left(\varepsilon + \frac{\log 1/\delta}{\alpha - 1}, \delta\right)$-DP for any $0 < \delta < 1$.

Advanced Composition

Corollary 1: Let f be the composition of n ε-DP mechanisms.

$(n\varepsilon)$-DP Let $0<\delta<1$ be s.t $\log(1/\delta) \geq \varepsilon^2 n$

$\Updownarrow$

$(n\varepsilon, 0)$-DP then f satisfies (ε', δ)-DP

where $\varepsilon' = 4\,\varepsilon\sqrt{2n\log(1/\delta)}$.

Comments:

- Comparison to prior work not clear
- No composition for (α,ε)-RDP
- (α,ε)-RDP provides new technical tools to look at DP.