Lecture 6
Advanced Composition

Dwork, Rothblum, Vadhan '10 Adam Smith

Theorem 1 (Advanced Composition). *For all $\varepsilon, \delta, \delta' > 0$, let $M = (M_1, \dots, M_k)$ be a sequence of (ε, δ)-differentially private algorithms, where the M_i's are potentially chosen sequentially and adaptively. Then M is $(\tilde{\varepsilon}, \tilde{\delta})$-differentially private, where* $\tilde{\varepsilon} = \underbrace{\varepsilon\sqrt{2k\log(1/\delta')}}_{\approx \varepsilon\sqrt{k} \quad \varepsilon k} + \underbrace{k\varepsilon\frac{e^{\varepsilon}-1}{e^{\varepsilon}+1}}_{\approx k\varepsilon^2}$ *and* $\tilde{\delta} = k\delta + \delta'$.

Kairouz Oh Vishwanath '15

$\frac{1}{n}\sum X_i \quad X_i \in \{0,1\}^d$

Gauss. vs Lap.

$\frac{d}{\varepsilon n}$ (apprx) $\quad \frac{d^{3/2}}{\varepsilon n}$ (pure) $\rightarrow \frac{d}{\varepsilon n}$ (apprx)

1. Reduction to Binary(ish) Mechanisms

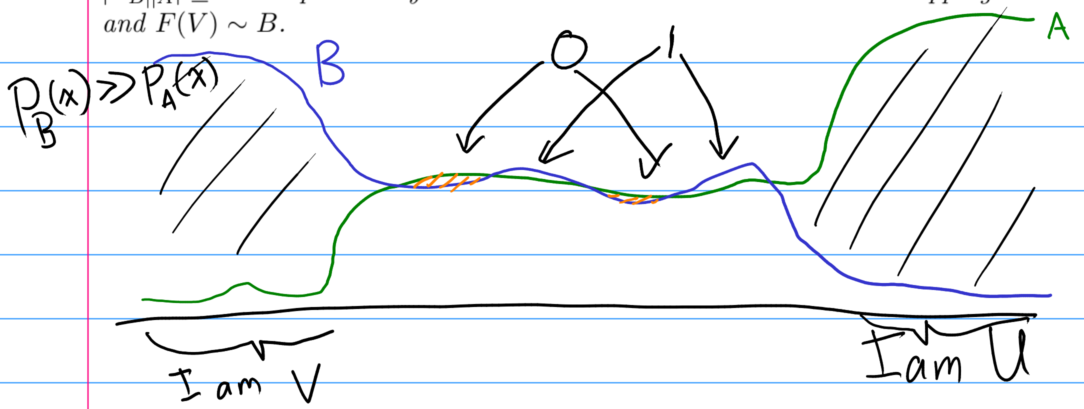
U, V rv's, "simple"

$|L_{U\|V}| \le \varepsilon$ w.p. $1-\delta$, $|L_{V\|U}| \le \varepsilon$ w.p. $1-\delta$

$t \sim A$, $L_{A\|B} = \ln\left(\frac{\Pr[A=t]}{\Pr[B=t]}\right)$

t	$\Pr[U=t]$	$\Pr[V=t]$
0	$\frac{e^{\varepsilon}(1-\delta)}{1+e^{\varepsilon}}$	$\frac{(1-\delta)}{1+e^{\varepsilon}}$
1	$\frac{(1-\delta)}{1+e^{\varepsilon}}$	$\frac{e^{\varepsilon}(1-\delta)}{1+e^{\varepsilon}}$
I am U	δ	0
I am V	0	δ

Theorem 2. *Let A and B be random variables such that $|L_{A\|B}| \le \varepsilon$ with probability $1-\delta$ and $|L_{B\|A}| \le \varepsilon$ with probability $1-\delta$. Then there exists a randomized mapping F such that $F(U) \sim A$ and $F(V) \sim B$.*



$M_1(x), M_2(x, M_1(x))$

$\forall a_1^{j-1}$

$M_1, \ldots, M_k : X^n \to Y$ $\quad M_j(X, a_1^{j-1})$ (ε, δ)-DP

X, X' nbrs

$Z_1, \ldots, Z_k \sim U$ or V

$F_1 : F_1(U) \sim M_1(X), \; F_1(V) \sim M_1(X')$

$F_2 : F_{2,a_1^i}(U) \sim M_2(X, a_1^i), \; F_2(V) \sim M_2(X', a_1^i)$

$F^* = F_1, \ldots, F_k$

Theorem 3. *There exists a randomized mapping $F*$ such that the algorithm M defined by the composition of $M_1, \ldots, M_k$ has the following two properties:*

- $M(X) \sim F^*(U_1, \ldots, U_k)$ *where $U_1, \ldots, U_k$ are drawn i.i.d. from U*
- $M(X') \sim F^*(V_1, \ldots, V_k)$ *where $V_1, \ldots, V_k$ are drawn i.i.d. from V*

2. Composition of Binary-ish Mechanisms

$(U_1, \dots, U_k)$ vs $(V_1, \dots, V_k)$

$|\text{Privacy loss RV}_{U \| V}| \le \tilde{\varepsilon}$ w.p. $1-\tilde{\delta}$

$\tilde{\delta} = \boxed{\delta k} + \delta'$

$\tilde{\varepsilon} = \varepsilon\sqrt{2k\log(1/\delta')} + \varepsilon k \cdot \frac{e^{\varepsilon}-1}{e^{\varepsilon}+1}$

$z \in \{0, 1, \text{I am } U\}^k$, $z_j \sim U$

$E_1 = \{z : \exists_j \ z_j = \text{"I am U"}\}$

$\Pr[E_1] = 1-(1-\delta)^k \le \boxed{\delta k}$

$z \in \{0,1\}^k$

$$\ln\left(\frac{\Pr[(U_1,\dots,U_n)=z]}{\Pr[(V_1,\dots,V_n)=z]}\right) = \sum_{j=1}^{k} \ln\left(\frac{\Pr[U_j = z_j]}{\Pr[V_j = z_j]}\right)$$

$$= \sum \ln\left(\frac{\cancel{(1-\delta)} e^{\varepsilon(1-z_i)} \cancel{/(e^{\varepsilon}+1)}}{\cancel{(1-\delta)} e^{\varepsilon z_j} \cancel{/(e^{\varepsilon}+1)}}\right) = \boxed{\sum_{j=1}^{k} (\varepsilon(1-2z_j))}$$

$z_j = 0$ w.p. $\frac{e^{\varepsilon}(1-\delta)}{1+e^{\varepsilon}}$

Cond on $\bar{E}_1$

$k\varepsilon \underline{E[1-2z_j]}$ $-\varepsilon$ or ε $\left\{ \text{sum} \perp \text{bounded} \right.$

$$\mathop{E}_{z \sim (U_1,\dots,U_k)}\left[\ln\left(\frac{\Pr[(U_1,\dots,U_k)=z]}{\Pr[(V_1,\dots,V_k)=z]}\right) \Big| \bar{E}_1\right] = k\varepsilon \cdot \frac{e^{\varepsilon}-1}{e^{\varepsilon}+1}$$

$(1-2z_j) = 1$ w.p. $\frac{e^{\varepsilon}}{1+e^{\varepsilon}}$

$= -1$ w.p. $\frac{1}{1+e^{\varepsilon}}$

$$E_2 = \left\{z \in \{0,1\}^k, \ln\left(\frac{\Pr[\vec{U}=z]}{\Pr[\vec{V}=z]}\right) > k\varepsilon \cdot \frac{e^{\varepsilon}-1}{e^{\varepsilon}+1} + t\varepsilon\sqrt{k}\right\}$$

Hoeffding bound: $Z_1, \dots, Z_k$ independent, bounded $[\ell, u]$

$$\Pr\left[\sum Z_j \ge E\left[\sum Z_j\right] + \tau\right] \le \exp\left(-\frac{2\tau^2}{k(u-\ell)^2}\right)$$

$[\ell, u] = [-\varepsilon, \varepsilon]$, $\tau = t\varepsilon\sqrt{k}$

$$\Pr\left[\ln\left(\frac{\Pr[\vec{U}=z]}{\Pr[\vec{V}=z]}\right) \geq k\varepsilon \cdot \frac{e^{\varepsilon}-1}{e^{\varepsilon}+1} + t\varepsilon\sqrt{k}\right] \leq \exp\left(-\frac{2(t\varepsilon\sqrt{k})^2}{k(2\varepsilon)^2}\right) = \exp\left(\frac{-t^2}{2}\right)$$

$$\Pr[E_2 \mid \bar{E}_1] \leq \exp(-t^2/2)$$

$$\Pr[U=z \cap \bar{E}_1 \cap \bar{E}_2] \leq e^{\hat{\varepsilon}} \Pr[V=z \cap \bar{E}_1 \cap \bar{E}_2] \leq e^{\hat{\varepsilon}} \Pr[V=z]$$

$$\Pr[U=z] = \Pr[U=z \cap \underline{\bar{E}_1 \cap \bar{E}_2}] + \Pr[\underline{U=z \cap E_1}] + \Pr[U=z \cap \bar{E}_1 \cap E_2]$$

$$\leq e^{\hat{\varepsilon}} \Pr[V=z] + \Pr[E_1] + \Pr[E_2 \mid \bar{E}_1] \cdot \Pr[\bar{E}_1]$$

$$\leq e^{\hat{\varepsilon}} \Pr[V=z] + \delta k + \exp(-t^2/2) \cdot 1$$

$t = \sqrt{2\log(1/\delta')}$

$$\leq e^{\hat{\varepsilon}} \Pr[V=z] + \overbrace{\delta k + \delta'}^{\tilde{\delta}}$$