CS 325: Private Data Analysis **Fall 2022**

Lecture 6: Advanced Composition Theorem

Lecturer: Di Wang *Scribes: Di Wang*

Note: *LaTeX template courtesy of UC Berkeley EECS dept.*

Disclaimer: *These notes have not been subjected to the usual scrutiny reserved for formal publications. They may be distributed outside this class only with the permission of the Instructor.*

6.1 Advanced Composition Theorem

Theorem 6.1 (Composition Theorem for ϵ-DP) *Let $\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_k$ be a sequence of randomized algorithms, where $\mathcal{A}_1 : \mathcal{X}^n \mapsto \mathcal{Y}_1$, $\mathcal{A}_2 : \mathcal{Y}_1 \times \mathcal{X}^n \mapsto \mathcal{Y}_2, \cdots, \mathcal{A}_k : \mathcal{Y}_1 \times \mathcal{Y}_2 \times \mathcal{Y}_{k-1} \times \mathcal{X}^n \mapsto \mathcal{Y}_k$. Suppose for every $i \in [k]$ and $a_1 \in \mathcal{Y}_1, a_2 \in \mathcal{Y}_2, \cdots, a_k \mathcal{Y}_k$ we have $\mathcal{A}_i(a_1, \cdots, a_{i-1}, \cdot) : \mathcal{X}^n \mapsto \mathcal{Y}_i$ is ϵ_i-DP. Then the algorithm $\mathcal{A} : \mathcal{X} \mapsto \mathcal{Y}_1 \times \mathcal{Y}_2 \times \cdots \mathcal{Y}_k$ that runs the algorithms $\mathcal{A}_i$ sequentially is ϵ-DP for $\epsilon = \sum_{i=1}^k \epsilon_i$.*

Theorem 6.2 (Composition Theorem for (ϵ, δ)-DP) *Let $\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_k$ be a sequence of randomized algorithms, where $\mathcal{A}_1 : \mathcal{X}^n \mapsto \mathcal{Y}_1$, $\mathcal{A}_2 : \mathcal{Y}_1 \times \mathcal{X}^n \mapsto \mathcal{Y}_2, \cdots, \mathcal{A}_k : \mathcal{Y}_1 \times \mathcal{Y}_2 \times \mathcal{Y}_{k-1} \times \mathcal{X}^n \mapsto \mathcal{Y}_k$. Suppose for every $i \in [k]$ and $a_1 \in \mathcal{Y}_1, a_2 \in \mathcal{Y}_2, \cdots, a_k \mathcal{Y}_k$ we have $\mathcal{A}_i(a_1, \cdots, a_{i-1}, \cdot) : \mathcal{X}^n \mapsto \mathcal{Y}_i$ is (ϵ_i, δ_i)-DP. Then the algorithm $\mathcal{A} : \mathcal{X} \mapsto \mathcal{Y}_1 \times \mathcal{Y}_2 \times \cdots \mathcal{Y}_k$ that runs the algorithms $\mathcal{A}_i$ sequentially is (ϵ, δ)-DP for $\epsilon = \sum_{i=1}^k \epsilon_i$ and $\delta = \sum_{i=1}^k \delta_i$.*

Thus, if each algorithm is (ϵ, δ)-DP, then the whole algorithm will be $(k\epsilon, k\delta)$-DP. In today's lecture, we will show that we can improve this guarantee.

Theorem 6.3 (Advanced Composition Theorem) *For all $\epsilon, \delta \geq 0$ and $\delta' > 0$, the adaptive composition of k algorithms, each of which is (ϵ, δ)-DP, is $(\tilde{\epsilon}, \tilde{\delta})$-DP where*

$$\tilde{\epsilon} = \epsilon\sqrt{2k \ln \frac{1}{\delta'}} + k\epsilon \frac{e^\epsilon - 1}{e^\epsilon + 1}, \tilde{\delta} = k\delta + \delta' \tag{6.1}$$

When ϵ is not too big (say at most 1), the quantity $\frac{e^\epsilon - 1}{e^\epsilon + 1}$ is close to $\frac{\epsilon}{2}$, so the final privacy parameter $\tilde{\epsilon}$ is $\Theta(\epsilon\sqrt{k \ln(1/\delta)} + k\epsilon^2)$ if we take $\delta' = \delta$. Moreover, suppose we want the final privacy guarantee to be at most 1, then we need $\epsilon^2 k < 1$. In that range we have $\sqrt{k}\epsilon > \epsilon^2 k$, so

$$\tilde{\epsilon} = \Theta(\epsilon\sqrt{k \ln(1/\delta)}). \tag{6.2}$$

Corollary 6.4 *Given target privacy parameters $0 < \epsilon < 1$ and $0 < \delta < 1$, to ensure $(\epsilon, k\delta' + \delta)$-DP over k mechanisms, it suffices that each mechanism is (ϵ', δ')-DP, where $\epsilon' = \frac{\epsilon}{2\sqrt{2k \ln(2/\delta)}}$ and $\delta' = \frac{\delta}{2k}$.*

Now consider we have k-adaptive count queries $f_i : \mathcal{X}^n \mapsto \mathbb{R}$ with $\Delta_i = 1$. Then compare with the four composition theorems:

- Laplace+Basic Composition: Noise should be $O(\frac{k}{\tilde{\epsilon}})$.

- Laplace+Advanced Composition: Noise should be $O(\frac{\sqrt{k\ln(1/\tilde{\delta})}}{\tilde{\epsilon}})$.
- Gaussian+Basic Composition: Noise should be $O(\frac{k\sqrt{\ln(k/\tilde{\delta})}}{\tilde{\epsilon}})$.
- Gaussian+Advanced Composition: Noise should be $O(\frac{\sqrt{k\ln(k/\tilde{\delta}\ln(1/\tilde{\delta})}}{\tilde{\epsilon}})$.

6.2 Proof

Recall in the previous lecture we define the privacy loss as a random variable. For a neighboring datasets $D \sim D'$, if we denote $p_{A(D)}(y)$ and $p_{A(D')}(y)$ as the density function of $A(D)$ and $A(D')$ respectively. And we denote the privacy loss as $\ell_{D,D'}(y) = \ln(\frac{p_{A(D)}(y)}{p_{A(D')}(y)})$. We could think $L_{D,D'} = \ell_{D,D'}(Y)$ as the transformation of the output random variable $Y = A(D)$.

For the whole composite algorithm $A : \mathcal{X}^n \mapsto \mathcal{Y}_1 \times \cdots \mathcal{Y}_k$, if we can show that

$$\mathbb{P}_{Y\sim A(D)}(L_{D,D'}(Y) > \tilde{\epsilon}) \leq \tilde{\delta}. \tag{6.3}$$

Then by Lemma 6.14, we can see A is $(\tilde{\epsilon}, \tilde{\delta})$-DP.

Now we denote $y = (y_1, y_2, \cdots, y_k) \in \mathcal{Y}_1 \times \cdots \mathcal{Y}_k$. Then we have

$$p_{A(D)}(y) = p_{A_1(D)}(y_1) \times p_{A_2(D,y_1)}(y_2) \times \cdots \times p_{A_k(D,y_1,\cdots,y_{k-1})}(y_k). \tag{6.4}$$

Thus,

$$L_{D,D'}(y) = \ln\frac{p_{A_1(D)}(y_1)}{p_{A_1(D')}(y_1)} + \ln\frac{p_{A_2(D,y_1)}(y_2)}{p_{A_2(D',y_1)}(y_2)} + \cdots + \ln\frac{p_{A_k(D,y_1,\cdots,y_{k-1})}(y_k)}{p_{A_k(D',y_1,\cdots,y_{k-1})}(y_k)}. \tag{6.5}$$

We can see each of them is a privacy loss. Denote $L_{D,D'}(y_1,\cdots,y_{k-1}) = \frac{p_{A_k(D,y_1,\cdots,y_{k-1})}(y_k)}{p_{A_k(D',y_1,\cdots,y_{k-1})}(y_k)}$.

To prove the strong composition theorem for (ϵ, δ)-DP, we want to take advantage of the fact that there is some cancelation in this sum. We know that each term is contained in the interval $[-\epsilon, \epsilon]$ with high probability. But it turns out that their average is generally at most ϵ^2. When many of them are added, that is the behavior which dominates.

To get a sense of that, we can compute this privacy loss for a few example of mechanisms and how it is distributed.

Gaussian Noise: Suppose each A_i is an instance of the Gaussian Mechanism from the last lecture, we have that $L_{D,D'}(Y) \sim \mathcal{N}(\frac{\Delta^2}{2\sigma^2}, \frac{\Delta^2}{\sigma^2})$ where $\Delta = \|f(D) - f(D')\|_2$. We choose $\sigma = O(\frac{\Delta\sqrt{\ln\frac{1}{\delta}}}{\epsilon})$. Thus, the privacy loss for this mechanism has expectation $O(\epsilon^2)$.

Randomized Response: In this mechanism, each data record $x_i \in \{0, 1\}$ is randomized with a value

$$Y_i = \begin{cases} x_i, \text{ w.p. } \frac{e^\epsilon}{e^\epsilon+1} \\ 1 - x_i, \text{ w.p. } \frac{1}{e^\epsilon+1}. \end{cases} \tag{6.6}$$

For every two neighboring data D, D', the privacy loss $L_{D,D'}$ is ϵ with probability $\frac{e^\epsilon}{e^\epsilon+1}$, and $-\epsilon$ with probability $\frac{1}{e^\epsilon+1}$. Its expectation is $\epsilon\frac{e^\epsilon-1}{e^\epsilon+1} = \Theta(\epsilon^2)$.

We have seen two examples, but how can we show for all the privacy losses? We will actually show that once we fix two neighboring datasets, every (ϵ, δ)-DP algorithm's behavior is captured by a very "leaky" variant of randomized response.

If X and Y are random variables, and taking values in the same set, we denote $X \approx_{\epsilon,\delta} Y$ if for every event E, $\mathbb{P}_X(E) \leq e^\epsilon \mathbb{P}_Y(E) + \delta$ and $\mathbb{P}_Y(E) \leq e^\epsilon \mathbb{P}_X(E) + \delta$.

As a starting point, we imagine the simplest pair of random variables that satisfies the relationship. It seems like we need one type of outcome to capture the δ additive difference in probabilities, and another type that captures the e^ϵ multiplicative change. Consider the following two special random variables, U and V taking values in the set $\{0, 1,$ "I am U" , "I am V" $\}$ with probabilities:

Outcome	P_U	P_V
0	$\frac{e^\varepsilon(1-\delta)}{e^\varepsilon+1}$	$\frac{1-\delta}{e^\varepsilon+1}$
1	$\frac{1-\delta}{e^\varepsilon+1}$	$\frac{e^\varepsilon(1-\delta)}{e^\varepsilon+1}$
"I am U"	δ	0
"I am V"	0	δ

Now, we claim that this simple pair of random variables is sufficient to express any pair of random variables with a bounded privacy loss.

Lemma 6.5 ([1]) *For every pair of random variables X, Y such that $X \approx_{\epsilon,\delta} Y$, then there exists a randomized map F such that $F(U) \sim X$ and $F(V) \sim Y$.*

For every fixed vector $y_{1:i-1} = (y_1, \cdots, y_{i-1})$ we have $A_i(D, y_{1:i-1}) \approx_{\epsilon,\delta} A_i(D', y_{1:i-1})$. Thus, there exists a map F_i such that $A_i(D, y_{1:i-1}) \sim F_i(U)$ and $A_i(D', y_{1:i-1}) \sim F_i(V)$. This allow us to show the following lemma

Lemma 6.6 *There is a randomized map F^* such that the composed algorithms A satisfies*

$$A(D) \sim F^*(U_1, \cdots, U_k), \text{ where } U_1, \cdots U_k \sim_{i.i.d.} U \tag{6.7}$$

$$A(D') \sim F^*(V_1, \cdots, V_k), \text{ where } V_1, \cdots V_k \sim_{i.i.d.} V \tag{6.8}$$

Proof: For $z_1, \cdots, z_k$, we define $(y_1, \cdots, y_k) = F^*(z_1, \cdots, z_k)$ where $y_i = F_i(z_i)$. Since $F_i(U_i)$ has the same distribution as $A_i(D, y_{1:i-1})$, the overall distribution of $F^*(U_1, \cdots, U_k)$ is the same as $A(D)$. ■

Thus, to prove A is $(\tilde{\epsilon}, \tilde{\delta})$-DP, it is suffice, by closure under postprocessing, to prove that $(U_1, U_2, \cdots, U_k) \approx_{\tilde{\epsilon},\tilde{\delta}} (V_1, V_2, \cdots, V_k)$.

Lemma 6.7 $(U_1, U_2, \cdots, U_k) \approx_{\tilde{\epsilon},\tilde{\delta}} (V_1, V_2, \cdots, V_k)$.

Proof: We consider two bad events: B_1 and B_2. The first B_1 is when we see a clear signal that the input was drawn according to U:

$$B_1 = \{z : \text{ at least one } z_j \text{ is "I am U" } \}. \tag{6.9}$$

From the definition of U we can see $\mathbb{P}_U(B_1) = 1 - (1-\delta)^k \leq k\delta$.

If $z \sim (U_1, \cdots, U_k)$ conditioned on $\bar{B}_1$, then we have $z \in \{0,1\}^k$. The probability of z is non-zero under both U and V, and we can compute the density ratio by taking the advantage of independence:

$$\ln \frac{P_{(U_1,\cdots,U_k)}(z)}{P_{(V_1,\cdots,V_k)}(z)} = \sum_{j=1}^{k} \ln \frac{P_U(z_j)}{P_V(z_j)} = \sum_{j=1}^{k} \ln \frac{\frac{(1-\delta)\exp(\epsilon(1-z_j))}{\exp(\epsilon)+1}}{\frac{(1-\delta)\exp(\epsilon(z_j))}{\exp(\epsilon)+1}} = \sum_{j=1}^{k} \epsilon(1-2z_j). \tag{6.10}$$

■

Thus

$$\mathbb{E}[\ln \frac{P_{(U_1,\cdots,U_k)}(z)}{P_{(V_1,\cdots,V_k)}(z)} | \bar{B}_1] = k\epsilon\mathbb{E}[(1-2z)|z=\{0,1\}] = k\epsilon\frac{e^\epsilon - 1}{e^\epsilon + 1}. \tag{6.11}$$

Now we recall the Chernoff Lemma

Lemma 6.8 *For k independent random variables $Z_1, Z_2, \cdots, Z_k$ in the range of $[l,u]$, we have*

$$\mathbb{P}(\sum_{i=1}^{k} Z_i \geq \sum_{i=1}^{k} \mathbb{E}[Z_i] + t) \leq \exp(-\frac{2t^2}{k(u-l)^2}). \tag{6.12}$$

Since for each $\ln \frac{P_U(z_j)}{P_V(z_j)} \in [-\epsilon, \epsilon]$ conditioned on $\bar{B}_1$ and $\mathbb{E}[\ln \frac{P_U(z_j)}{P_V(z_j)} | \bar{B}_1] = \epsilon\frac{e^\epsilon-1}{e^\epsilon+1}$. we have

$$\mathbb{P}(\ln \frac{P_{(U_1,\cdots,U_k)}(z)}{P_{(V_1,\cdots,V_k)}(z)} > k\epsilon\frac{e^\epsilon - 1}{e^\epsilon + 1} + t\epsilon\sqrt{k} | \bar{B}_1) \leq \exp(-\frac{t^2}{2}). \tag{6.13}$$

Denote the event $B_2 = \{z \in \{0,1\}^k | \ln \frac{P_{(U_1,\cdots,U_k)}(z)}{P_{(V_1,\cdots,V_k)}(z)} > k\epsilon\frac{e^\epsilon-1}{e^\epsilon+1} + t\epsilon\sqrt{k}\}$, then we have $\mathbb{P}(\bar{B}_1 \cap B_2) \leq \exp(-\frac{t^2}{2})$. Note that conditioned on $\bar{B}_1 \cap \bar{B}_2$ we have ration of $P_U(z)$ and $P_V(z)$ is bounded. Thus, for every event E we have

$$\begin{aligned}
P_U(E) &\leq P_U(E \cap \bar{B}_1 \cap \bar{B}_2) + P_U(E \cap B_1) + P_U(E \cap \bar{B}_1 \cap B_2) \\
&\leq P_U(E \cap \bar{B}_1 \cap \bar{B}_2) + P_U(B_1) + P_U(\bar{B}_1 \cap B_2) \\
&=\leq P_U(E \cap \bar{B}_1 \cap \bar{B}_2) + P_U(B_1) + P_U(B_2|\bar{B}_1)P_U(\bar{B}_1) \\
&\leq e^{\tilde{\epsilon}} P_V(E \cap \bar{B}_1 \cap \bar{B}_2) + k\delta + \exp(-\frac{t^2}{2}) \\
&\leq e^{\tilde{\epsilon}} P_V(E) + k\delta + \exp(-\frac{t^2}{2}).
\end{aligned}$$

Take $t = \sqrt{2\ln(\frac{1}{\delta'})}$ we complete the proof.

References

[1] Cynthia Dwork, Guy N Rothblum, and Salil Vadhan. Boosting and differential privacy. In *2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, pages 51–60. IEEE, 2010.