CS 325: Differential Privacy **Fall 2022**

Lecture 7: Relaxations of Differential Privacy

Lecturer: Di Wang *Scribes: Di Wang*

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

7.1 Rényi Differential Privacy

In the previous lecture, we showed that for $k(\epsilon, \delta)$-DP algorithms $A_1, \cdots, A_k$, there (adaptive) composition will be $(\tilde{\epsilon}, \tilde{\delta})$-DP with $\tilde{\epsilon} = O(\epsilon\sqrt{k})$ and $\tilde{\delta} = O(k\delta)$. The question is, is this bound tight? Yes, but just a little [2]. Thus the previous bound is near optimal. However, that is only for homogeneous case (each algorithm A_i has the same privacy budget). The question is how about general case? That is if each A_i is (ϵ_i, δ_i), then what is the privacy for their composition. Actually, [4] shows that the problem is #P-hard![1] Thus, later, there were several relaxations of ϵ-DP rather than the approximate DP. In this section, we will mainly focus on one of them, i.e., Rényi-DP [3].

To show the motivation of Rényi Differential Privacy (RDP), we first go back to ϵ-DP. Recall that ϵ-DP means $\max_{y\in\mathcal{Y}} \ln \frac{\mathbb{P}(A(D)=y)}{\mathbb{P}(A(D')=y)} \leq \epsilon$. Actually, this "closeness" could be think as the Rényi divergence of the distribution of $A(D)$ and $A(D')$ at ∞!

Definition 7.1 *For two distributions P and Q, the Rényi divergence of order ∞ is defined as*

$$D_\infty(P\|Q) = \max_{x\in supp(Q)} \ln \frac{P(x)}{Q(x)}.$$

Thus, ϵ-DP is equivalent to $D_\infty(A(D)\|A(D')) \leq \epsilon$.

Rényi divergence of order ∞ is a quite strong "measurement", we can relax it to Rényi divergence of order α for some $\alpha > 1$:

Definition 7.2 *For two distributions P and Q, the Rényi divergence of order α with $\alpha > 1$ is defined as*

$$D_\alpha(P\|Q) = \frac{1}{\alpha - 1} \ln \mathbb{E}_{x\sim Q}(\frac{P(x)}{Q(x)})^\alpha.$$

When $\alpha \to 1$, $D_\alpha(P\|Q)$ will be the KL-divergence, $D_1(P\|Q) = \mathbb{E}_{x\sim P} \ln \frac{P(x)}{Q(x)}$.

Thus, based on the D_∞, it motivates exploring a relaxation of differential privacy based on the Rényi divergence of order α.

[1] A polynomial-time algorithm for solving a #P-complete problem, if it existed, would solve the P versus NP problem by implying that P and NP are equal.

Definition 7.3 *A randomized algorithm $A : \mathcal{X}^n \mapsto \mathcal{Y}$ is said to have ϵ-Rényi Differential Privacy of order α, or (α, ϵ)-RDP, if for every neighboring dataset D, D'*

$$D_\alpha(A(D)\|A(D') \leq \epsilon. \tag{7.1}$$

Theorem 7.4 *(α, ϵ)-RDP is closed under post-processing.*

Theorem 7.5 (Group Privacy) *If A is (α, ϵ)-RDP, D and D' differs in $k = 2^c$ records for some $c \geq 0$, and $\alpha \geq 2^{c+1}$ then*

$$D_{\frac{\alpha}{2^c}}(f(D)\|f(D')) \leq 3^c\epsilon.$$

Theorem 7.6 (Composition Theorem) *Let $A : \mathcal{X}^n \mapsto \mathcal{Y}_1 \times \mathcal{Y}_2$ be a randomized algorithm that outputs $A(D) = (a_1, a_2)$, where $a_1 = A_1(D)$ and $a_2 = A_2(a_1, D)$. If $A_1 : \mathcal{X}^n \mapsto \mathcal{Y}_1$ is (α, ϵ_1)-RDP and $A_2 : \mathcal{Y} \times \mathcal{X}^n \mapsto \mathcal{Y}_2$ is (α, ϵ_2)-RDP for any fixed $a_1 \in \mathcal{Y}_1$. Then A is $(\alpha, \epsilon = \epsilon_1 + \epsilon_2)$-RDP.*

Proof: We denote the density function of $A_1(D)$ and $A_2(y, D)$ as $p_{A_1(D)}$ and $p_{A_2(D)}$, respectively.

$$\begin{aligned}
&\exp[(\alpha-1)D_\alpha(A(D)\|A(D'))] \\
&= \int_{\mathcal{Y}_1\times\mathcal{Y}_2} p^\alpha_{A(D)}((x,y))p^{1-\alpha}_{A(D')}((x,y))dxdy \\
&= \int_{\mathcal{Y}_1}\int_{\mathcal{Y}_2} p^\alpha_{A_2(D,x)}(y)p^\alpha_{A_1(D)}(x)p^{1-\alpha}_{A_2(D',x)}(y)p^{1-\alpha}_{A_1(D')}(x)dxdy \\
&= \int_{\mathcal{Y}_1} p^\alpha_{A_1(D)}(x)p^{1-\alpha}_{A_1(D')}(x)(\int_{\mathcal{Y}_2} p^\alpha_{A_2(D,x)}(y)p^{1-\alpha}_{A_2(D',x)}(y)dy)dx \\
&\leq \int_{\mathcal{Y}_1} p^\alpha_{A_1(D)}(x)p^{1-\alpha}_{A_1(D')}(x)\exp(\epsilon_2(\alpha-1))dx \\
&\leq \exp((\alpha-1)(\epsilon_1+\epsilon_2).
\end{aligned}$$

■

Corollary 7.7 *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 (α, ϵ_i)-RDP. 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 (α, ϵ)-RDP for $\epsilon = \sum_{i=1}^k \epsilon_i$.*

In above, we have already showed the postprocessing, composition and group privacy, which are quite similar to ϵ-DP. Below we will show the sub-sampling property of RDP:

Theorem 7.8 (Subsampling Property: Without replacement [5]) *Given a dataset of n points drawn from a domain $\mathcal{X}$ and a mechanism A that takes an input from $\mathcal{X}^n$, for $m \leq n$, let the randomized algorithm $M \circ$ subsample be defined as: (1)* **subsample without replacement** *m datapoints of the dataset (sampling parameter $q = \frac{m}{n}$), and (2) apply M to the subsampled dataset. For all integers $\alpha \geq 2$, if M is $(\alpha, \epsilon(\alpha))$-RDP, then the subsampled mechanism $M \circ$ subsample obey $\alpha, \tilde{\epsilon}(\alpha)$-RDP where*

$$\epsilon(\alpha) \leq \frac{1}{\alpha-1}\ln(1+\gamma^2\binom{\alpha}{2}\min\{4(\epsilon^{\epsilon(2)}-1), e^{\epsilon(2)}\min\{2, (e^{\epsilon(\infty)}-1)^2\}\}+\sum_{j=3}^{\alpha}\gamma^j\binom{\alpha}{j}e^{(j-1)\epsilon(j)}\min\{2, (e^{\epsilon(\infty)}-1)^j\}) \tag{7.2}$$

For the **Poison subsampling** of RDP, see [6] for details.

Next, we will see the relationship between RDP, DP and Approximate DP. The first result tells Pure DP is stronger than RDP.

Theorem 7.9 *If the randomized algorithm A is ϵ-DP, then it is (α, ϵ)-RDP for any $\alpha > 1$.*

Proof: This is by the monotonicity of the Rényi divergence: For any pairs of distribution P, Q, we have $D_\alpha(P\|Q) \leq D_\beta(P\|Q)$ if $1 \leq \alpha < \beta \leq \infty$. ■

The following theorem tells us an (α, ϵ)-RDP mechanism implies $(\epsilon_\delta, \delta)$-DP.

Theorem 7.10 *If the randomized algorithm A is (α, ϵ)-RDP, then it is $(\epsilon' = \epsilon + \frac{\ln \frac{1}{\delta}}{\alpha - 1}, \delta)$-DP for any $0 < \delta < 1$.*

Proof: To show the theorem we need the following lemma:

Lemma 7.11 *Let $\alpha > 1$, P and Q be two distributions with identical support, let E be any event. Then*

$$\mathbb{P}(P \in E) \leq (\exp[D_\alpha(P\|Q)]\mathbb{P}(Q \in E))^{\frac{\alpha-1}{\alpha}}.$$

Thus, for any event E we have $\mathbb{P}(A(D) \in E) \leq (\exp(\epsilon)\mathbb{P}(A(D') \in E))^{\frac{\alpha-1}{\alpha}}$. Denote $Q = \mathbb{P}(A(D') \in E)$ We now consider two cases:

Case:1 $e^\epsilon Q > \delta^{\frac{\alpha}{\alpha-1}}$ we have

$$\mathbb{P}(A(D) \in E) \leq e^\epsilon Q(e^\epsilon Q)^{-\frac{1}{\alpha}} \leq \epsilon Q \delta^{-\frac{1}{\alpha-1}} = \exp(\epsilon + \frac{\ln \frac{1}{\delta}}{\alpha - 1})Q.$$

Case:2 $e^\epsilon Q \leq \delta^{\frac{\alpha}{\alpha-1}}$, then

$$\mathbb{P}(A(D) \in E) \leq (\exp(\epsilon)\mathbb{P}(A(D') \in E))^{\frac{\alpha-1}{\alpha}} \leq \delta. \tag{7.3}$$

■

Corollary 7.12 *For given privacy budget ϵ, δ, if the mechanism is $(\frac{2\ln \frac{1}{\delta}}{\epsilon} + 1, \frac{\epsilon}{2})$-RDP, then it is (ϵ, δ)-DP.*

7.1.1 Basic Mechanisms

Next, we will show some mechanisms that satisfy RDP.

Lemma 7.13 *The Randomized Response Mechanism is $(\alpha, \frac{1}{\alpha-1}\ln p^\alpha(1-p)^{1-\alpha} + (1-p)^\alpha p^{1-\alpha})$-RDP. Where p is the probability that $y = x$ for record x.*

Lemma 7.14 *For the query $f : \mathcal{X}^n \mapsto \mathbb{R}$ with global sensitivity 1 and its Laplacian mechanism $A(D) = f(D) + Lap(\lambda)$, then the Laplacian mechanism is $(\alpha, \tilde{\epsilon})$-RDP with*

$$\tilde{\epsilon} = \frac{1}{\alpha - 1}\ln\{\frac{\alpha}{2\alpha - 1}\exp(\frac{\alpha - 1}{\lambda}) + \frac{\alpha - 1}{2\alpha - 1}\exp(-\frac{\alpha}{\lambda})\} < \frac{1}{\lambda}.$$

Proof: We just need to calculate $\mathbb{E}_{x\sim\mathcal{A}(D')}(\frac{A(D)}{A(D')})^\alpha = \int_{-\infty}^{+\infty} p_{A(D)}(x)^\alpha p_{A(D')}(x)^{1-\alpha}dx$:

$$\begin{aligned}
&\int_{-\infty}^{+\infty} p_{A(D)}(x)^\alpha p_{A(D')}(x)^{1-\alpha}dx = \frac{1}{2\lambda}\int_{-\infty}^{+\infty}\exp(-\frac{\alpha|x|}{\lambda}-\frac{(1-\alpha)|x-1|}{\lambda})dx\\
&=\frac{1}{2\lambda}\int_{-\infty}^{0}\exp(\frac{\alpha x}{\lambda}+\frac{(1-\alpha)(x-1)}{\lambda})dx+\frac{1}{2\lambda}\int_{0}^{1}\exp(\frac{(1-\alpha)(x-1)}{\lambda}-\frac{\alpha x}{\lambda})dx\\
&+\frac{1}{2\lambda}\int_{1}^{+\infty}\exp(-\frac{(1-\alpha)(x-1)}{\lambda}-\frac{\alpha x}{\lambda})dx\\
&=\frac{\alpha}{2\alpha-1}\exp(\frac{\alpha-1}{\lambda})+\frac{\alpha-1}{2\alpha-1}\exp(-\frac{\alpha}{\lambda})
\end{aligned}$$

■

Lemma 7.15 *For the query $f:\mathcal{X}^n\mapsto\mathbb{R}^k$ with global ℓ_2-norm sensitivity Δ and its Gaussian mechanism $A(D)=f(D)+\mathcal{N}(0,\sigma^2\mathbb{I}_k)$, then the Gaussian mechanism is $(\alpha,\tilde{\epsilon})$-RDP with $\tilde{\epsilon}=\frac{\alpha\Delta^2}{2\sigma^2}$.*

Proof: For convenience we assume $f(D)=0$ then it is suffice to calculate

$$\mathbb{E}_{x\sim\mathcal{A}(D')}(\frac{A(D)}{A(D')})^\alpha = \int_{-\infty}^{+\infty} p_{A(D)}(x)^\alpha p_{A(D')}(x)^{1-\alpha}dx$$

$$\begin{aligned}
&\int_{-\infty}^{+\infty} p_{A(D)}(x)^\alpha p_{A(D')}(x)^{1-\alpha}dx = \frac{1}{(2\pi\sigma^2)^{\frac{k}{2}}}\exp(-\frac{\alpha\|x\|_2^2}{2\sigma^2}-\frac{(1-\alpha)\|x-f(D')\|_2^2}{2\sigma^2})\\
&=\frac{1}{(2\pi\sigma^2)^{\frac{k}{2}}}\int_{-\infty}^{+\infty}\exp(-\frac{\|x\|_2^2+2(1-\alpha)x\cdot f(D')+(\alpha-1)\|f(D')\|_2^2}{2\sigma^2})dx\\
&=\frac{1}{(2\pi\sigma^2)^{\frac{k}{2}}}\int_{-\infty}^{+\infty}\exp(-\frac{\|x-(1-\alpha)f(D')\|_2^2+(\alpha^2-\alpha)\|f(D'\|_2^2}{2\sigma^2})dx\\
&=\exp(\frac{(\alpha^2-\alpha)\|f(D'\|_2^2}{2\sigma^2})
\end{aligned}$$

Thus, $D_\alpha(A(D)\|A(D'))=\frac{\alpha\|f(D'\|_2^2}{2\sigma^2}\le\frac{\alpha\Delta^2}{2\sigma^2}$. ■

Now consider k Gaussian mechanisms $A_1,\cdots,A_k$ where each mechanism adds Gaussian $\mathcal{N}(0,\sigma^2\mathbb{I}_d)$. And our goal is to ensure (ϵ,δ)-DP for their composition. If we use the advanced composition theorem, each one should be $(\frac{\epsilon}{2\sqrt{2k\log\frac{2}{\delta}}},\frac{\delta}{2k})$-DP. Thus, by the Gaussian mechanism $\sigma^2_{ACT}=\frac{16k\Delta^2\log\frac{2.5k}{\delta}\log\frac{2}{\delta}}{\epsilon^2}$.

If we use the composition theorem and RDP, to ensure (ϵ,δ)-DP, by Corollary 8.12, it is sufficient to ensure the composite algorithm is $(\frac{2\ln\frac{1}{\delta}}{\epsilon}+1,\frac{\epsilon}{2})$-RDP. Thus, each one need to be $(\frac{2\ln\frac{1}{\delta}}{\epsilon}+1,\frac{\epsilon}{2k})$-RDP. By the Gaussian mechanism of RDP, we just need $\frac{(\frac{2\ln\frac{1}{\delta}}{\epsilon}+1)\Delta^2}{2\sigma^2}\le\frac{\epsilon}{2k}$. Thus, $\sigma^2_{rdp}\ge\frac{k(\frac{2\ln\frac{1}{\delta}}{\epsilon}+1)\Delta^2}{\epsilon}$. Thus we can see it is less the noise of the Gaussian mechanism.

7.2 Zero Concentrated Differential Privacy

Concurrent to Rényi DP, [1] introduced the zero concentrated DP. Generally speaking a mechanism is called ρ-zCDP if it is $(\alpha,\alpha\rho)$-RDP for any $\alpha>1$.

Definition 7.16 *A randomized algorithm $A : \mathcal{X}^n \mapsto \mathcal{Y}$ is ρ zero concentrated Differential Privacy, or ρ-zCDP, if for every neighboring dataset D, D' and every $\alpha > 1$*

$$D_\alpha(A(D)\|A(D') \leq \alpha\rho. \tag{7.4}$$

Why it is called zero concentrated DP? That is due to from the previous inequality we have

$$\mathbb{E}[e^{(\alpha-1)Z}] \leq e^{(\alpha-1)\rho\alpha}, \tag{7.5}$$

where $Z = \log \frac{p_{A(D)}}{p_{A(D)}}$ is the privacy loss. And this indicates that for all $\alpha > 1$ we have

$$\Pr(Z > \lambda+\rho) = \Pr(\exp((\alpha-1)Z) > \exp((\alpha-1)(\lambda+\rho)) \leq \frac{\exp((\alpha-1)Z)}{\exp((\alpha-1)(\lambda+\rho))} \leq \exp((\alpha-1)\alpha\rho-(\alpha-1)(\lambda+\rho)) \tag{7.6}$$

Thus

$$\Pr(Z > \lambda+\rho) \leq \inf_{b>0} \exp(b^2\rho - b\lambda) = \exp(-\frac{\lambda^2}{4\rho}) \tag{7.7}$$

Thus zCDP requires that the privacy loss random variable is concentrated around zero hence the name). That is, Z is small with high probability, with larger deviations from zero becoming increasingly unlikely. Note that the randomness of the privacy loss random variable is taken only over the randomnesss of the mechanism

Theorem 7.17 *zCDP satisfies composition and postprocessing, group properties. However, it does not have the subsampling property!!*

Theorem 7.18 *If A is ρ-zCDP, then it is (ϵ, δ)-DP with $(\epsilon = \rho + \sqrt{4\rho \log 1/\delta}, \delta)$ for all $\delta > 0$.*

Proof: By (7.7) we have $\Pr(Z > \lambda + \rho) \leq \inf_{b>0} \exp(b^2\rho - b\lambda) = \exp(-\frac{\lambda^2}{4\rho})$. Take $\lambda = \epsilon - \rho > 0$ we have $\Pr(Z > \epsilon) < \exp(-\frac{(\epsilon-\rho)^2}{4\rho}) \leq \delta$. ■

Thus to achieve a given (ϵ, δ)-DP guarantee it suffices to satisfy ρ-zCDP with

$$\rho = (\sqrt{\epsilon + \log 1/\delta} - \sqrt{\log 1/\delta})^2 \approx \frac{\epsilon^2}{4 \log 1/\delta}$$

.

Theorem 7.19 *From Lemma 7.15 we can see Gaussian mechanism is $\frac{\Delta}{2\sigma^2}$-CDP.*

References

[1] Mark Bun and Thomas Steinke. Concentrated differential privacy: Simplifications, extensions, and lower bounds. In *Theory of Cryptography Conference*, pages 635–658. Springer, 2016.

[2] Peter Kairouz, Sewoong Oh, and Pramod Viswanath. The composition theorem for differential privacy. In *International conference on machine learning*, pages 1376–1385. PMLR, 2015.

[3] Ilya Mironov. Rényi differential privacy. In *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, pages 263–275. IEEE, 2017.

[4] Jack Murtagh and Salil Vadhan. The complexity of computing the optimal composition of differential privacy. In *Theory of Cryptography Conference*, pages 157–175. Springer, 2016.

[5] Yu-Xiang Wang, Borja Balle, and Shiva Prasad Kasiviswanathan. Subsampled rényi differential privacy and analytical moments accountant. In *The 22nd International Conference on Artificial Intelligence and Statistics*, pages 1226–1235. PMLR, 2019.

[6] Yuqing Zhu and Yu-Xiang Wang. Poission subsampled rényi differential privacy. In *International Conference on Machine Learning*, pages 7634–7642. PMLR, 2019.