CSC2419:Algorithms and Complexity in Private Data Analysis Winter 2017

Lecture 5 — February 14, 2017

Aleksandar Nikolov *Scribe: Assimakis Kattis*

Advanced Composition

Theorem 1 (Simple Composition). *If $M_1, ..., M_k$ are ϵ-DP and $M(x) = M_k(x, M_{k-1}(x, M_{k-2}(x, ...)))$, then it follows that $M(x)$ is $k\epsilon$-DP.*

Note that we say M_i is ϵ-DP if $\forall y \in$
$Range(M_{i-1})$, $M_i(\cdot, y)$ is ϵ-DP.

Theorem 2 (Advanced Composition). *If $M_1, ..., M_k$ are ϵ-DP and $M(x) = M_k(x, M_{k-1}(x, M_{k-2}(x, ...)))$, then $M(x)$ is (ϵ', δ)-DP for all δ and $\epsilon' = \sqrt{2k \log 1/\delta} + k(e^\epsilon - 1)$.*

To prove the advanced composition theorem, we will start with some preliminary definitions.

Definition 3. *Let X, Y be random variables taking values in $\mathcal{R}$, then we can define the Kullback-Leibler divergence as:*

$$D_{KL}(X\|Y) = \sum_{r \in \mathcal{R}} \mathbb{P}(X = r) \log \left(\frac{\mathbb{P}(X = r)}{\mathbb{P}(Y = r)} \right). \tag{1}$$

We also define the max-KL divergence in an analogous way:

$$D_\infty(X\|Y) = \max_{r \in \mathcal{R}} \log \left(\frac{\mathbb{P}(X = r)}{\mathbb{P}(Y = r)} \right). \tag{2}$$

Divergences can be seen as measures of “distance” between distributions. However, it should be noted that they are not metrics, in particular, they are not symmetric with respect to switching the distributions, and they do not satisfy the triangle inequality.

The following proposition is immediate from the definitions.

Proposition 4. *If M is ϵ-DP, then for any two databases x and x' differing in one element, it holds that $D_\infty(M(x)\|M(x')) \leq \epsilon$.*

Below, we use the notation $p_i = \mathbb{P}(X = i)$ and $q_i = \mathbb{P}(Y = i)$ for simplicity. The first proposition we prove shows that KL-divergencce does have at least one property in common with metrics: it is non-negative, and takes value 0 only when $X = Y$ almost everywhere.

Proposition 5. *For all distributions X, Y, $D_{KL}(X\|Y) \geq 0$, and equality is achieved only when $X = Y$ with probability 1.*

Proof. By definition, we have that:

$$D_{KL}(X\|Y) = -\sum_r p_r \log(\frac{q_r}{p_r}) \geq -\log(\sum_r p_r q_r/p_r) = -\log(\sum_r q_r) = 0, \tag{3}$$

where we used Jensen's inequality and the convexity of the function$\phi(x) = -\log(x)$. The equality case follows from the strong convexity of ϕ. □

The following is the main technical lemma that we need in the proof. It says, roughly, that if the max-KL-divergence of X and Y is small in both directions, then the KL-divergence is even smaller. For an intuitive picture of why that should be true observe that the max KL-divergence is the maximum of $\log \frac{p_r}{q_r}$, while the KL-divergence is the average. In order for the average to be close to the maximum, we would need that p_r is bigger than q_r except for a set with very small probability under p. But then q must give much larger mass to this set than p, which contradicts the fact that both max-KL-divergencies are bounded. The formal proof follows.

Lemma 6. *For X, Y random variables, let $D_\infty(X\|Y) \leq \epsilon$ and $D_\infty(Y\|X) \leq \epsilon$. It follows that $D_{KL}(X\|Y) \leq \epsilon(e^\epsilon - 1) \approx \epsilon^2$.*

Proof. By the previous proposition, and using Hölder's inequality with $p = 1$ and $q = \infty$, we can show that

$$\begin{aligned}
D_{KL}(X\|Y) &\leq D_{KL}(Y\|X) + D_{KL}(X\|Y) \\
&= \sum_r \left(p_r \log \frac{p_r}{q_r} + q_r \log \frac{q_r}{p_r} \right) \\
&= \sum_r p_r \left(\log \frac{p_r}{q_r} + \log \frac{q_r}{p_r} \right) + \sum_r (q_r - p_r) \log \frac{q_r}{p_r} \\
&= \sum_r (q_r - p_r) \log \frac{q_r}{p_r} \leq \left(\sum_r |q_r - p_r| \right) \cdot \max_r \left| \log \frac{q_r}{p_r} \right| \\
&\leq \epsilon \sum_r \max\{q_r, p_r\} - \min\{q_r, p_r\} \leq \epsilon \sum_r (e^\epsilon - 1) \cdot \min\{q_r, p_r\} \leq \epsilon(e^\epsilon - 1)
\end{aligned}$$

□

Theorem 7 (Azuma)**.** *Let $Z_1, ..., Z_k \in \mathbb{R}$ be random variables such that $\forall i\ |Z_i| \leq \alpha$ and $\mathbb{E}[Z_i | Z_1 = z_1, ..., Z_{i-1} = z_{i-1}] \leq \beta$. Then :*

$$\mathbb{P}\left(\sum_i Z_i > k\beta + t\sqrt{k}\alpha \right) \leq \exp\left(-\frac{t^2}{2} \right) \tag{4}$$

We are now ready to prove the advanced composition theorem using the above ingredients.

Proof of Theorem 2. Fix two arbitrary neighboring databases x, x' , and define $y_i = M_i(x, y_{i-1})$, $y'_i = M_i(x', y_{i-1})$ with $y_1 = M(x)$, $y'_1 = M(x')$. Define the random variable Z_i as:

$$Z_i = \log \left(\frac{\mathbb{P}(y_i | y_{i-1}, ..., y_1)}{\mathbb{P}(y'_i = y_i | y'_{i-1} = y_{i-1}, ..., y'_1 = y_1)} \right),$$

which, by using the chain rule, gives us that:

$$\sum_{i=1}^{k} Z_i = \log\left(\frac{\prod_{i=1}^{k} \mathbb{P}(y_i|y_{i-1} =, ..., y_1)}{\prod_{i=1}^{k} \mathbb{P}(y_i' = y_i|y_{i-1}' = y_{i-1}, ..., y_1' = y_1)}\right)$$
$$= \log\left(\frac{\mathbb{P}(y_k, y_{k-1}, ..., y_1)}{\mathbb{P}(y_k' = y_k, y_{k-1}' = y_{k-1}, ..., y_1' = y_1)}\right).$$

Fix $r_1, ..., r_{i-1}$ and set the random variables X and Y to:

$$X = y_i|y_{i-1} = r_{i-1}, ..., y_1 = r_1;$$
$$Y = y_i'|y_{i-1}' = r_{i-1}, ..., y_1' = r_1;$$

Because M_i is ϵ-DP for all i, we get that $D_\infty(X\|Y) \leq \epsilon$ and $D_\infty(Y\|X) \leq \epsilon$, implying that $|Z_i| \leq \epsilon$ and, by our main lemma, that:

$$\mathbb{E}[Z_i|y_{i-1} = r_{i-1}, ..., y_1 = r_1] \leq \epsilon(e^\epsilon - 1). \tag{5}$$

Finishing off the proof, we use Azuma's inequality with $t = \sqrt{2\log 1/\delta}$, $\alpha = \epsilon$ and $\beta = \epsilon(e^\epsilon - 1)$ to arrive at the fact that:

$$\mathbb{P}\left(\sum_{i=1}^{k} Z_i > k\epsilon(e^\epsilon - 1) + \epsilon\sqrt{2\log 1/\delta k}\right) < \delta, \tag{6}$$

or that $\exists B \subseteq \text{Range}(M_1) \times ... \times \text{Range}(M_k) = \mathcal{R}^k$ for which:

1. $\mathbb{P}((y_1, ..., y_k) \in B) < \delta$.
2. $\forall(r_1, ..., r_k) \in \mathcal{R}^k \backslash B$, we have:

$$\log\left(\frac{\mathbb{P}(y_k = r_k, y_{k-1} = r_{k-1}, ..., y_1 = r_1)}{\mathbb{P}(y_k' = r_k, y_{k-1}' = r_{k-1}, ..., y_1' = r_1)}\right) < \epsilon'. \tag{7}$$

As we saw in the privacy analysis of the Gaussian noise mechanism, this is sufficient to prove (ϵ', δ)-DP. □