1 Strong Composition

In this lecture, we show that \((\epsilon, \delta)\)-differential privacy satisfies a “strong composition” theorem, in which the \(\epsilon\) parameter increases only with the square root of the number of stages of the composition.

**Theorem 1 (Strong Composition)** For all \(\epsilon, \delta \geq 0\) and \(\delta' > 0\), the adaptive composition of \(k\) algorithms, each of which is \((\epsilon, \delta)\)-differentially private, is \((\tilde{\epsilon}, \tilde{\delta})\)-differentially private where 
\[
\tilde{\epsilon} = \epsilon\sqrt{2k \ln(1/\delta')} + k\epsilon\frac{e^{\epsilon - 1}}{e^\epsilon + 1} \quad \text{and} \quad \tilde{\delta} = k\delta + \delta'.
\]

If \(X\) and \(Y\) are random variables taking values in the same set (and with probabilities defined for the same collection of events), we say \(X \approx_{\epsilon, \delta} Y\) if for every event \(E\): 
\[
P_X(E) \leq e^\epsilon P_Y(E) + \delta \quad \text{and} \quad P_Y(E) \leq e^\epsilon P_X(E) + \delta.
\]

We would like to characterize this relation in simpler terms. As a starting point, let’s try to imagine the simplest pair of random variables that satisfies the relationship. It seems like we need one type of outcome to capture the \(\delta\) additive difference in probabilities, and another type that captures the \(e^\epsilon\) multiplicative change. Consider the following two special random variables, \(U\) and \(V\), taking values in the set \(\{0, 1, \text{"I am U"}, \text{"I am V"}\}\) with the probabilities:

<table>
<thead>
<tr>
<th>Outcome</th>
<th>(P_U)</th>
<th>(P_V)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(\frac{e^\epsilon (1-\delta)}{e^\epsilon + 1})</td>
<td>(\frac{1-\delta}{e^\epsilon + 1})</td>
</tr>
<tr>
<td>1</td>
<td>(\frac{1-\delta}{e^\epsilon + 1})</td>
<td>(\frac{e^\epsilon (1-\delta)}{e^\epsilon + 1})</td>
</tr>
<tr>
<td>&quot;I am U&quot;</td>
<td>(\delta)</td>
<td>0</td>
</tr>
<tr>
<td>&quot;I am V&quot;</td>
<td>0</td>
<td>(\delta)</td>
</tr>
</tbody>
</table>

**Lemma 2** For every pair of random variables \(X, Y\) such that \(X \approx_{\epsilon, \delta} Y\), there exists a randomized map \(F\) such that \(F(U) \sim X\) and \(F(V) \sim Y\).

We leave this proof as a homework problem, but provide the following pictorial hint:

![Figure 1: The “proof” of Lemma 2](image)

The first step of the proof is to show that the areas of the regions \(A\) and \(B\) are both bounded by \(\delta\). The rest is the homework problem! It is ok to assume, for the sake of the homework problem, that \(X\) and \(Y\) take values in a discrete set.

We can now proceed to the proof of Strong Composition (Theorem 1).

**Proof** Fix a sequence of \(k\) mechanisms \(M_j\), each of which takes a data set in \(X^n\) as well as a partial transcript \(a_1, ..., a_{j-1}\) (abbreviated \(a_1^{j-1}\)) such that, for every partial transcript, \(M_j(\cdot; a_1^{j-1})\) is \((\epsilon, \delta)\)-differentially private. Also, fix two data sets \(s, s'\) that differ in one entry.

13-1
For every partial transcript $a_j^{i-1}$, we have $M_j(s; a_j^{i-1}) \approx_{\epsilon, \delta} M_j(s'; a_j^{i-1})$ and so there exists a randomized map $F_{a_j^{i-1}}$ such that $F_{a_j^{i-1}}(U)$ and $F_{a_j^{i-1}}(V)$ have the same distributions as $M_j(s; a_j^{i-1})$ and $M_j(s'; a_j^{i-1})$, respectively.

This allows us to show the first important claim:

**Claim 3** There is a randomized map $F^*$ such that the composed mechanism $M$ satisfies:

$$M(s) \sim F^*(U_1, ..., U_k) \text{ where } U_1, ..., U_k \sim_{i.i.d.} U$$

$$M(s') \sim F^*(V_1, ..., V_k) \text{ where } V_1, ..., V_k \sim_{i.i.d.} V.$$  \hspace{1cm} (1)

**Proof** [of claim] Consider the algorithm:

**Algorithm 1:** $F^*(z_1, ..., z_k)$:

1. for $j = 1$ to $k$
2. \hspace{1cm} $a_j \leftarrow F_{a_j^{i-1}}(z_j)$
3. return $(a_1, ..., a_k)$.

Since $F_{a_j^{i-1}}(U_j)$ has the same distribution as $M_j(s; a_j^{i-1})$ for each stage $j$, the overall distribution of $F^*(U_1, ..., U_k)$ is the same as $M(s)$ (and similarly for $s'$ when the inputs are i.i.d. copies of $V$).

To prove that $M$ is $\tilde{\epsilon}, \tilde{\delta}$-differentially private, it suffices, by closure under postprocessing, to prove that $(U_1, ..., U_k) \approx_{\tilde{\epsilon}, \tilde{\delta}} (V_1, ..., V_k)$.

We'll 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 $U$:

$$B_1 = \{ z : \text{at least one } z_j \text{ is } \text{"I am U"} \}. \hspace{1cm} (3)$$

Under $z$ is distributed according to either $U_1, ..., U_k$ or $V_1, ..., v_k$, the probability of $B_1$ is exactly $1 - (1 - \delta)^k \leq k\delta$.

If $z \sim U_1, ..., U_k$, then conditioned on $B_1$, not occurring, we have $z \in \{0, 1\}^k$. The probability of $z$ is nonzero under both $U$ and $V$, and we can compute the odds ratio by taking advantage of independence:

$$\ln \left( \frac{P_U(z)}{P_V(z)} \right) = \sum_j \ln \left( \frac{P_U(z_j)}{P_V(z_j)} \right) = \sum_j \ln \left( \frac{(1 - \delta) e^{\epsilon(1-z_j)}/(e^{\epsilon} + 1)}{(1 - \delta) e^{\epsilon z_j}/(e^{\epsilon} + 1)} \right) = \sum_j (1-\epsilon)^z_j.$$  \hspace{1cm} (4)

This log odds ratio is thus a sum of bounded, independent random variables under distribution $U$, with expectation

$$\mathbb{E}_{z \sim \{U_1, ..., U_k\}} \left( \ln \left( \frac{P_U(z)}{P_V(z)} \right) \right| B_1 \right) = k\epsilon \cdot \mathbb{E} \left( (1-\epsilon) U \mid U \in \{0, 1\} \right) = k\epsilon e^{\epsilon} \frac{e^{\epsilon} - 1}{e^{\epsilon} + 1}.$$  \hspace{1cm} (5)

By the Chernoff bound (Lemma 1), for any $t > 0$ we have

$$P_{z \sim U_1, ..., U_k} \left( 2^{\sum_{\text{event } B_2} \ln \left( \frac{P_U(z)}{P_V(z)} \right) > \epsilon} \left| B_1 \right. \right) \leq e^{-\epsilon^2/2} \text{ where } \epsilon \triangleq k\epsilon \frac{e^{\epsilon} - 1}{e^{\epsilon} + 1} + t\epsilon \sqrt{k}.$$  \hspace{1cm} (6)

Let $B_2$ be the event that $\{ z \in \{0, 1\}^k : \ln \left( \frac{P_U(z)}{P_V(z)} \right) > \epsilon \frac{e^{\epsilon} - 1}{e^{\epsilon} + 1} + t\epsilon \sqrt{k} \}$. Note that conditioned on $B_1 \cap B_2$, the ratio of $P_U(z)$ to $P_V(z)$ is bounded. Hence, for any event $E$,

$$P_U(E \cap \bar{B_1} \cap \bar{B_2}) \leq e^\epsilon P_V(E \cap \bar{B_1} \cap \bar{B_2}) \leq e^\epsilon P_V(E).$$

13-2
This allows us to show the indistinguishability condition we want:

\[
P_U(E) \leq P_U(E \cap \bar{B}_1 \cap \bar{B}_2) + P_U(B_1) + P_U(B_2 | \bar{B}_1)P_U(\bar{B}_1)
\leq e^\epsilon P_V(E) + k\delta + e^{-t^2/2}.
\]

Setting \( t = \sqrt{2\ln(1/\delta')} \) yields the theorem statement. ■

**Exercise 1** Use the proof strategy from the previous theorem to show that the composition of an \((\epsilon_1, \delta_1)\)-DP algorithm with a \((\epsilon_2, \delta_2)\)-DP algorithm is \((\epsilon_1 + \epsilon_2, \delta_1 + \delta_2)\)-DP.

**Exercise 2** Using Lemma 2, show that if \( X \approx_{\epsilon, 0} Y \), then \( D_{KL}(P_X \parallel P_Y) \leq \epsilon \frac{e^{\epsilon - 1}}{e^{\epsilon} + 1} \) (which is a tighter bound than the one we derived in earlier lectures).

## 2 Notes

The first version of the strong composition theorem appeared in [?]. Our presentation is based on Kairouz et al. [KOV17], as well as Dwork and Roth [DR14, Sections 3.5.1–2]. The characterization of \( \epsilon, \delta \) indistinguishability of Lemma 2 is due to [KOV17]. Their proof is based on a much more general result of Blackwell (1953). The homework problem asks students to provide a direct proof of this special case.

## References
