Adaptive Composition Property of Summary Statistic Privacy

In this document, we take a first step towards analyzing the adaptive composition property of the summary statistic privacy. We focus on the setting where the distribution parameter θ belongs to a finite set, there is only one summary statistic secret, and the tolerance range ϵ is 0. We also assume that $\sup_\theta \mathbb{P}\left(\theta\right) = a < 1$ and $\inf_\theta \mathbb{P}\left(\theta\right) = b > 0$. Under such setting, the summary statistic privacy of a mechanism $\mathcal{M}$ can be written as

$$\Pi_{\omega_\Theta}^{\mathcal{M}} \triangleq \sup_{\hat{g}} \mathbb{P}\left(\hat{g}\left(\theta'\right) = g\left(\theta\right)\right).$$

The following theorem shows the adaptive composition guarantee of the summary statistic privacy under such setting.

Theorem 0.1 (Adaptive Composition)**.** *Consider a data holder sequentially applies m data release mechanisms to the original dataset. For the i-th mechanism $\mathcal{M}_i$, $\forall i \in [m]$, it takes the original distribution parameter θ and all previous released parameters $\theta'_1, \ldots, \theta'_{i-1}$ as input and output θ'_i. Suppose the summary statistic privacy of mechanism $\mathcal{M}_i$ is $\Pi_{\omega_\Theta}^{\mathcal{M}_i}$, $\forall i \in [m]$. Let $\boldsymbol{\mathcal{M}}$ be the composition of these m mechanisms, and suppose the adversary can get access to all released parameters $\theta'_1, \ldots, \theta'_m$. The summary statistic privacy of $\boldsymbol{\mathcal{M}}$ can be bounded as $\Pi_{\omega_\Theta}^{\boldsymbol{\mathcal{M}}} \leq a \cdot \prod_{i\in[m]} \frac{\Pi_{\omega_\Theta}^{\mathcal{M}_i}}{b}$.*

Proof. For the summary statistic privacy of $\boldsymbol{\mathcal{M}}$, we can get that

$$\begin{aligned}
\Pi_{\omega_\Theta}^{\boldsymbol{\mathcal{M}}} &= \sup_{\hat{g}} \mathbb{P}\left(\hat{g}\left(\theta'_1, \ldots, \theta'_m\right) = g\left(\theta\right)\right) \\
&= \sum_{\theta'_1,\ldots,\theta'_m} \mathbb{P}\left(\theta'_1, \ldots, \theta'_m\right) \cdot \left(\sup_{\mathrm{g}} \sum_{\theta: g(\theta)=\mathrm{g}} \mathbb{P}\left(\theta | \theta'_1, \ldots, \theta'_m\right)\right) \\
&= \sum_{\theta'_1,\ldots,\theta'_m} \sup_{\mathrm{g}} \sum_{\theta: g(\theta)=\mathrm{g}} \mathbb{P}\left(\theta, \theta'_1, \ldots, \theta'_m\right) \\
&= \sum_{\theta'_1,\ldots,\theta'_m} \sup_{\mathrm{g}} \sum_{\theta: g(\theta)=\mathrm{g}} \mathbb{P}\left(\theta\right) \cdot \mathbb{P}\left(\theta'_1, \ldots, \theta'_m | \theta\right) \\
&\leq a \cdot \sum_{\theta'_1,\ldots,\theta'_m} \sup_{\mathrm{g}} \sum_{\theta: g(\theta)=\mathrm{g}} \mathbb{P}\left(\theta'_1, \ldots, \theta'_m | \theta\right) \\
&= a \cdot \sum_{\theta'_1,\ldots,\theta'_m} \sup_{\mathrm{g}} \sum_{\theta: g(\theta)=\mathrm{g}} \prod_{i\in[m]} \mathbb{P}\left(\theta'_i | \theta, \theta'_1, \ldots, \theta'_{i-1}\right) \\
&\leq a \cdot \sum_{\theta'_1,\ldots,\theta'_m} \sup_{\mathrm{g}} \prod_{i\in[m]} \sum_{\theta: g(\theta)=\mathrm{g}} \mathbb{P}\left(\theta'_i | \theta, \theta'_1, \ldots, \theta'_{i-1}\right) \\
&\leq a \cdot \sum_{\theta'_1,\ldots,\theta'_m} \prod_{i\in[m]} \sup_{\mathrm{g}} \sum_{\theta: g(\theta)=\mathrm{g}} \mathbb{P}\left(\theta'_i | \theta, \theta'_1, \ldots, \theta'_{i-1}\right) \\
&\leq a \cdot \prod_{i\in[m]} \sum_{\theta'_1,\ldots,\theta'_i} \sup_{\mathrm{g}} \sum_{\theta: g(\theta)=\mathrm{g}} \mathbb{P}\left(\theta'_i | \theta, \theta'_1, \ldots, \theta'_{i-1}\right) \\
&= a \cdot \prod_{i\in[m]} \sum_{\theta'_1,\ldots,\theta'_i} \sup_{\mathrm{g}} \sum_{\theta: g(\theta)=\mathrm{g}} \frac{\mathbb{P}\left(\theta'_i\right) \mathbb{P}\left(\theta | \theta'_1, \ldots, \theta'_i\right)}{\mathbb{P}\left(\theta\right)} \\
&\leq a \cdot \prod_{i\in[m]} \frac{\Pi_{\omega_\Theta}^{\mathcal{M}_i}}{b}.
\end{aligned}$$

$\square$