Privacy Odometers and Filters: Pay-as-you-Go Composition

Ryan Rogers, Aaron Roth, Jonathan Ullman, and Salil Vadhan

Differential Privacy [DMNS]

- Outcome of algorithm $A : \mathcal{X}^n \rightarrow \mathcal{O}$ should roughly stay the same if one person's data changes. For all neighboring $x, x'$ and outcomes $O \subseteq \mathcal{O}$,\[ P[A(x) \in O] \leq e^{\delta} P[A(x') \in O] + \delta \]
- Parameter $\epsilon > 0$ measures the privacy loss.
- Parameter $\delta > 0$ is the failure probability where the privacy loss can be much larger than $\epsilon$.

Composition Theorems - Prior Work

- Run algorithm $A_i$ which is $\epsilon_i$-DP on the data $x$ as a function of the outcomes of previous algorithms $A_1, \ldots, A_{i-1}$.
- Basic Composition [DMNS]: $f(\epsilon_1, \ldots, \epsilon_k) = \sum \epsilon_i$.
- Advanced Composition [DRV]: quadratic improvement for $\delta_g > 0$:\[ f(\epsilon_1, \ldots, \epsilon_k) = \tilde{O}\left(\sqrt{\sum \epsilon_i^2}\right) \]
- Optimal Composition [KOV, MV]: complex form.

Our Focus: Adaptive Privacy Parameters

- As the analyst determines what (and how many) analyses to run he will want to allocate his privacy budget adaptively.
- These composition theorems crucially rely on the choice of parameters $\epsilon_i$ and the number of algorithms $k$ to be fixed up front.
- Which composition theorems still apply when we can select the parameters adaptively?
- How can we even define differential privacy in this adaptively parameter setting?

Privacy Loss and the Analyst

- The privacy loss for algorithm $A : \mathcal{X}^n \rightarrow \mathcal{O}$ on neighboring $x, x'$ for outcome $o \in \mathcal{O}$\[ L(o) = \log \frac{P[A(x) = o]}{P[A(x') = o]} \]
- Privacy loss random variable $L(o)$ where $o \sim A(x)$.
- $A$ selects $\epsilon_i \geq 0$ and $A_i$, which is $\epsilon_i$-DP, as a function of previous outcomes in an adversarial way to try to make the privacy loss large.

Privacy Odometer

- Privacy odometer provides a running upper bound on privacy loss.
- A valid privacy odometer is a function $\text{COMP}_{\delta_g} : \mathbb{R}^k \rightarrow \text{HALT, CONT}$ where for any analyst $A$ who selects $\epsilon_1, \ldots, \epsilon_k$ adaptively, then w.p. $1 - \delta_g$, we have $L < \epsilon_g$ and $\text{COMP}_{\epsilon_g, \delta_g}(\epsilon_1, \ldots, \epsilon_k) = \text{HALT}$.
- The mechanism that stops before HALT is $(\epsilon_g, \delta_g)$-DP.

Privacy Filter

- Privacy filter is a stopping rule, so w.h.p. a given privacy budget $\epsilon_g$ will not be exceeded.
- A valid privacy filter $\text{COMP}_{\epsilon_g, \delta_g} : \mathbb{R}^k \rightarrow \{\text{HALT, CONT}\}$ where for any analyst $A$ who selects $\epsilon_1, \ldots, \epsilon_k$ adaptively, then w.p. $1 - \delta_g$, we have $L < \epsilon_g$ and $\text{COMP}_{\epsilon_g, \delta_g}(\epsilon_1, \ldots, \epsilon_k) = \text{HALT}$.
- The mechanism that stops before HALT is $(\epsilon_g, \delta_g)$-DP.

Main Results

- Basic composition still applies in adaptive setting.
- A valid privacy filter is the following $\text{COMP}_{\epsilon_g, \delta_g}(\epsilon_1, \ldots, \epsilon_k) = \text{CONT}$ if $\tilde{O}\left(\sqrt{\epsilon_g^2 + \sum \epsilon_i^2}\right) < \epsilon_g$ and otherwise $\text{COMP}_{\epsilon_g, \delta_g}(\epsilon_1, \ldots, \epsilon_k) = \text{HALT}$.
- A valid privacy odometer is:\[ \text{COMP}_{\delta_g}(\epsilon_1, \ldots, \epsilon_k) = \tilde{O}\left(\sqrt{\sum \epsilon_i^2 \log \log(n)}\right) \]as long as $\sum \epsilon_i^2 > 1/n^2$.
- There is a provable gap between privacy filters and odometers – there is no valid privacy odometer where $\text{COMP}_{\delta_g}(\epsilon_1, \ldots, \epsilon_k)$ is $\tilde{O}\left(\sqrt{\sum \epsilon_i^2 \log \log(n)}\right)$.

Key to Proofs

- The advanced composition theorem used martingale concentration inequalities, like Azuma’s inequality, but they no longer apply when the bounds are random.
- We then apply concentration bounds from self normalizing processes [PnKLL].

References

[DMNS] C. Dwork, F. McSherry, K. Nissim, and A. Smith. In TCC'06.