Oneshot Differentially Private Top-k Selection Supplementary Material

Gang Qiao [1] Weijie J. Su [2] Li Zhang [3]

1. Proof of Theorem 2.1

Proof of Theorem 2.1. We prove this theorem with a standard coupling argument. Without loss of generality, we assume $s_f = 1$. Let $x = (x_1, \ldots, x_m)$ and $x' = (x'_1, \ldots, x'_m)$ be adjacent, i.e., $\|x - x'\|_\infty \leq 1$. Let S be an arbitrary k-subset of $\{1, \ldots, m\}$ and $\mathcal{G}$ consist of all $(g_1, \ldots, g_m)$ such that $\mathcal{M}^{\mathrm{os}}$ with input x reports S. Similarly we have $\mathcal{G}'$ for x'. It is clear that $\mathcal{G} - 2 \cdot \mathbb{1}_S \subset \mathcal{G}'$, where $\mathbb{1}_S \in \{0,1\}^m$ satisfies $\mathbb{1}_S(i) = 1$ if and only if $i \in S$. Here $\{0,1\}^m$ stands for the set of m-elements sets which only contain 0 and 1 as elements. Therefore, the standard coupling argument gives

$$
\begin{aligned}
&\mathbb{P}(\mathcal{M}^{\mathrm{os}}(x) = S) = \int_{\mathcal{G}} \frac{1}{2^m \lambda^m} \mathrm{e}^{-\frac{\|g\|_1}{\lambda}} dg \\
&\geq \int_{\mathcal{G}' + 2\cdot\mathbb{1}_S} \frac{1}{2^m \lambda^m} \mathrm{e}^{-\frac{\|g\|_1}{\lambda}} dg = \int_{\mathcal{G}'} \frac{1}{2^m \lambda^m} \mathrm{e}^{-\frac{\|g + 2\cdot\mathbb{1}_S\|_1}{\lambda}} dg \\
&\geq \int_{\mathcal{G}'} \frac{\mathrm{e}^{-2k/\lambda}}{2^m \lambda^m} \mathrm{e}^{-\frac{\|g\|_1}{\lambda}} dg = \mathrm{e}^{-\varepsilon} \mathbb{P}(\mathcal{M}^{\mathrm{os}}(x') = S) .
\end{aligned}
$$

On the opposite side, we have $\mathbb{P}(\mathcal{M}^{\mathrm{os}}(x) = S) \leq \mathrm{e}^{\varepsilon} \mathbb{P}(\mathcal{M}^{\mathrm{os}}(x') = S)$, which completes the proof since S is arbitrary. □

2. Proof of Theorem 2.3

We begin by proving the following lemma.

Lemma 2.1. *Let X and Y be independent identically $\mathrm{Lap}(\lambda)$ distributions and $Z = X - Y$, then the density function of random variable Z has the form*

$$
f_Z(z) = \frac{\lambda + |z|}{4\lambda^2} \cdot \exp\left(-\frac{|z|}{\lambda}\right).
$$

Proof of Lemma 2.1. Notice that

$$
f_Z(z) = \int_{-\infty}^{\infty} f_X(x) f_Y(x - z) dx,
$$

by applying the convolution formula above, when $z \geq 0$ we have

$$
\begin{aligned}
& 4\lambda^2 f_Z(z) \\
&= \int_{-\infty}^{\infty} \exp\left(-\frac{|x|}{\lambda}\right) \exp\left(-\frac{|x - z|}{\lambda}\right) dx \\
&= \int_{-\infty}^{0} \exp\left(\frac{x}{\lambda}\right) \exp\left(\frac{x - z}{\lambda}\right) dx + \\
&\quad \int_{0}^{z} \exp\left(-\frac{x}{\lambda}\right) \exp\left(\frac{x - z}{\lambda}\right) dx + \\
&\quad \int_{z}^{\infty} \exp\left(-\frac{x}{\lambda}\right) \exp\left(-\frac{x - z}{\lambda}\right) dx + \\
&= \frac{\lambda}{2} \exp\left(-\frac{z}{\lambda}\right) + z \exp\left(-\frac{z}{\lambda}\right) + \frac{\lambda}{2} \exp\left(-\frac{z}{\lambda}\right) \\
&= (\lambda + z) \exp\left(-\frac{z}{\lambda}\right) .
\end{aligned}
$$

Therefore, with $z \geq 0$, we have

$$
f_Z(z) = \frac{\lambda + z}{4\lambda^2} \exp\left(-\frac{z}{\lambda}\right) .
$$

Since the pdfs of random variables X and Y are symmetric around the origin, the pdf of Z must be symmetric around the origin. From this we get that

$$
f_Z(z) = \frac{\lambda + |z|}{4\lambda^2} \exp\left(-\frac{|z|}{\lambda}\right) .
$$

□

With the lemma above, we start to prove Theorem 2.3. Let $g_1, g_2, \cdots, g_m$ be i.i.d. $\mathrm{Lap}(\lambda)$ distributions. We define the event

$$
A = \{\mathcal{M}_{oneshot} \text{ reports the index set of true top-}k \text{ elements}\}
$$

and consider the extreme case when y_i's follow the exact same order as $f_i(D)$'s, i.e.,

$$
f_{(1)}(D) + g_1 \leq f_{(2)}(D) + g_2 \leq \cdots \leq f_{(m)}(D) + g_m .
$$

[1] Department of Statistics, University of Michigan, Ann Arbor, MI, USA. [2] The Wharton School, University of Pennsylvania, Philadelphia, PA, USA. [3] Google Research, Mountain View, CA, USA. Correspondence to: <qiaogang@umich.edu, suw@wharton.upenn.edu, liqzhang@google.com>.

Proceedings of the 38th International Conference on Machine Learning, PMLR 139, 2021. Copyright 2021 by the author(s).

Thus we can lower bound $P(A)$ by the extreme case above,

$$\begin{aligned}\mathbb{P}(A) &\geq \mathbb{P}(f_{(1)}(D)+g_1 \leq \cdots \leq f_{(m)}(D)+g_m)\\ &= \mathbb{P}(f_{(1)}(D)+g_1 \leq f_{(2)}(D)+g_2,\\ &\quad f_{(2)}(D)+g_2 \leq f_{(3)}(D)+g_3, \cdots,\\ &\quad f_{(m-1)}(D)+g_{m-1} \leq f_{(m)}(D)+g_m)\\ &= \mathbb{P}(g_1-g_2 \leq f_{(2)}(D)-f_{(1)}(D),\\ &\quad g_2-g_3 \leq f_{(3)}(D)-f_{(2)}(D), \cdots,\\ &\quad g_{m-1}-g_m \leq f_{(m)}(D)-f_{(m-1)}(D))\\ &\geq \mathbb{P}(g_1-g_2 \leq \Delta, g_2-g_3 \leq \Delta, \cdots,\\ &\quad g_{m-1}-g_m \leq \Delta)\,.\end{aligned}$$

Recall the Bonferroni lower bound that for events $X_1, \cdots, X_n$, we have

$$\mathbb{P}(X_1, \cdots, X_n) \geq \max\left\{0, 1-\sum_{i=1}^{m}(1-\mathbb{P}(X_i))\right\}.$$

Combining the calculation above, we have

$$\begin{aligned}\mathbb{P}(A) &\geq 1-\sum_{i=1}^{m-1}(1-\mathbb{P}(g_i-g_{i+1} \leq \Delta))\\ &= 1-\sum_{i=1}^{m-1}\mathbb{P}(g_i-g_{i+1} \leq -\Delta)\\ &= 1-\sum_{i=1}^{m-1}\int_{-\infty}^{-\Delta} f_Z(z)dz\\ &= 1-\frac{(m-1)(2\lambda+\Delta)\mathrm{e}^{-\Delta/\lambda}}{4\lambda}\,,\end{aligned}$$

this completes the proof of Theorem 2.3.

3. Proof of Theorem 3.5

Proof of Theorem 3.5. We only need to prove the sensitivity part $s = \frac{2}{dL(1-\rho)}$. For two adjacent databases D, D' where they only differ in only one data item, we assume their corresponding sufficient statistics are $\boldsymbol{y}$ and $\tilde{\boldsymbol{y}}$. To capture the definition of adjacent databases, we assume one sample $y_{i_0,j_0}^{(l_0)}$ of the edge (i_0, j_0) in database D and D' is different. Without loss of generality, we assume that $y_{i_0,j_0}^{(l_0)} = 0$ in D and $\tilde{y}_{i_0,j_0}^{(l_0)} = 1$ in D'. Note that

$$P_{ij} = \begin{cases}\frac{1}{d}y_{i,j} & \text{if } (i,j) \in E,\\ 1-\frac{1}{d}\sum_{k:(i,k)\in E} y_{i,k} & \text{if } i = j,\\ 0 & \text{otherwise,}\end{cases}$$

two transition matrices $\boldsymbol{P}$ and $\tilde{\boldsymbol{P}}$ only differ in four elements in positions (i_0, j_0), (j_0, i_0), (i_0, i_0) and (j_0, j_0). To find the maximum possible value of $||\boldsymbol{P}-\tilde{\boldsymbol{P}}||_\infty$, for $i \neq i_0$ and $i \neq j_0$,

$$\sum_{j=1}^{m}|P_{ij}-\tilde{P}_{ij}| = 0\,.$$

In the case when $i = i_0$,

$$\begin{aligned}&\sum_{j=1}^{m}|P_{ij}-\tilde{P}_{ij}|\\ &= \frac{|y_{i_0,j_0}-\tilde{y}_{i_0,j_0}|}{d} + |P_{i_0i_0}-\tilde{P}_{i_0i_0}|\\ &= \frac{|y_{i_0,j_0}-\tilde{y}_{i_0,j_0}|}{d} +\\ &\left|\left(1-\frac{1}{d}\sum_{k:(i_0,k)\in E} y_{i_0,k}\right)-\left(1-\frac{1}{d}\sum_{k:(i_0,k)\in E}\tilde{y}_{i_0,k}\right)\right|\\ &= \frac{|y_{i_0,j_0}-\tilde{y}_{i_0,j_0}|}{d} + \frac{1}{d}|y_{i_0,j_0}-\tilde{y}_{i_0,j_0}|\\ &= \frac{2}{d}|y_{i_0,j_0}-\tilde{y}_{i_0,j_0}|\\ &= \frac{2}{dL}\,.\end{aligned}$$

When $i = j_0$, we can follow the exact same calculation and get $\sum_{j=1}^{m}|P_{ij}-\tilde{P}_{ij}| = \frac{2}{dL}$. Therefore,

$$||\boldsymbol{P}-\tilde{\boldsymbol{P}}||_\infty = \max_{1\leq i\leq m}\sum_{j=1}^{m}|P_{ij}-\tilde{P}_{ij}| = \frac{2}{dL}\,.$$

By the definition of sensitivity, we have $s = \frac{2}{dL(1-\rho)}$. □

4. Proof of Lemma 4.3

Proof of Lemma 4.3. By mean value theorem, there exists a point $\tilde{z}$ between z and z' such that

$$|g(\tilde{z})| = \left|\frac{G(z')-G(z)}{z'-z}\right|\,,$$

where g denotes the density function of the standard Laplace distribution. Hence, we only need to prove

$$\frac{|g(\tilde{z})|}{G(z)(1-G(z))} \leq 2\mathrm{e}^{|z'-z|}\,.$$

Now we prove this inequality in different cases.

Case 1: when $\max(z, z') \leq 0$. In this case,

$$\frac{|g(\tilde{z})|}{G(z)(1-G(z))} = \frac{\mathrm{e}^{\tilde{z}-z}}{1-\frac{1}{2}\mathrm{e}^{z}} \leq 2\mathrm{e}^{|\tilde{z}-z|} \leq 2\mathrm{e}^{|z'-z|}\,.$$

Case 2: when $\min(z, z') \geq 0$. With a similar argument in Case 1, we have

$$\frac{|g(\tilde{z})|}{G(z)(1-G(z))} = \frac{\mathrm{e}^{z-\tilde{z}}}{1-\frac{1}{2}\mathrm{e}^{-z}} \leq 2\mathrm{e}^{|z-\tilde{z}|} \leq 2\mathrm{e}^{|z'-z|}\,.$$

Case 3: when $\min(z, z') < 0 < \max(z, z')$. The triangle inequality gives

$$\frac{|g(\tilde{z})|}{G(z)(1-G(z))} = \frac{\mathrm{e}^{|z|-|\tilde{z}|}}{1-\frac{1}{2}\mathrm{e}^{-|z|}} \le 2\mathrm{e}^{|z-\tilde{z}|} \le 2\mathrm{e}^{|z'-z|}\,.$$

In summary, combining all the cases above gives the lemma. □

5. Proof of Lemma 4.5

The proof of the Lemma 4.5 is based on the classical Bennett's inequality stated below.

Bennett's inequality: Let $Z_1 \ldots, Z_n$ be independent random variables with all means being zero. In addition, assume $|Z_i| \le a$ almost surely for all i. Denoting by $\sigma^2 = \sum_{i=1}^n \mathrm{Var}(Z_i)$, we have

$$\mathbb{P}\left(\sum_{i=1}^n Z_i > t\right) \le \exp\left(-\frac{\sigma^2 h(at/\sigma^2)}{a^2}\right)$$

for any $t \ge 0$, where $h(u) = (1+u)\log(1+u) - u$.

Proof of Lemma 4.5. By the Bennett's inequality stated above, we have

$$\begin{aligned}&\mathbb{P}(\sum_i Z_i \le k)\\ =\ &\mathbb{P}\left(\sum_i Z_i - \sum_i q_i \le -tk\right) \le \mathrm{e}^{-\sigma^2 h\left(tk/\sigma^2\right)},\end{aligned}$$

Note that $\mathbb{P}(\sum_i Z_i \le k)$ is a decreasing function with respect to $\sum_{i=1}^m q_i$, hence we can assume $\sum_{i=1}^m q_i = (1+t)k$. In this case, we have $\sigma^2 = \sum_{i=1}^m q_i(1-q_i) \le (1+t)k$. Making use of the fact that $\sigma^2 h(tk/\sigma^2)$ is a monotonically decreasing function with respect to σ^2 gives

$$\begin{aligned}\mathbb{P}(\sum_i Z_i \le k) &\le \mathrm{e}^{-\sigma^2 h\left(tk/\sigma^2\right)}\\ &\le \exp\left(-(1+t)kh\left(\frac{t}{t+1}\right)\right).\end{aligned}$$

Hence, the first part of Lemma 4.5 is proved. In order to prove the second part of the lemma, we need to take advantage of the conclusion from the first part. Note that $h(u)/u^2$ is a decreasing function of u, by setting $t = c\sqrt{\frac{\log(m/\delta)}{k}} \le \frac{c}{\sqrt{C_0}}$, we get

$$\begin{aligned}&(1+t)kh\left(\frac{t}{t+1}\right)\\ \ge\ &(1+t)k\left(\frac{t}{t+1}\right)^2 \frac{h(\frac{c}{c+\sqrt{C_0}})}{(\frac{c}{c+\sqrt{C_0}})^2}\\ \ge\ &k\left(c\sqrt{\frac{\log(m/\delta)}{k}}\right)^2 \frac{1}{1+\frac{c}{\sqrt{C_0}}} \frac{h(\frac{c}{c+\sqrt{C_0}})}{(\frac{c}{c+\sqrt{C_0}})^2}\\ \ge\ &1.099\log\left(\frac{m}{\delta}\right)\\ >\ &\log\left(\frac{m}{\delta}\right).\end{aligned}$$

Therefore, when $\sum_{i=1}^m q_i \ge (1+t)k$, we have

$$\mathbb{P}(\sum_i Z_i \le k) \le \exp\left(-(1+t)kh\left(\frac{t}{t+1}\right)\right) \le \frac{\delta}{m}\,.$$

□