Calibrating Noise when Coordinates have Different Sensitivity

Christian Janos Lebeda*† and Rasmus Pagh*‡

†IT University of Copenhagen, ‡University of Copenhagen
*Basic Algorithms Research Copenhagen

IT UNIVERSITY OF COPENHAGEN

Problem formulation

Given a dataset x of n real-valued vectors $x_k \in \mathbb{R}^d$, design a differentially private mechanism $\mathscr{M}$ to approximate the coordinate-wise sum:

$$f(x) = \sum_{k=1}^{n} x_k$$

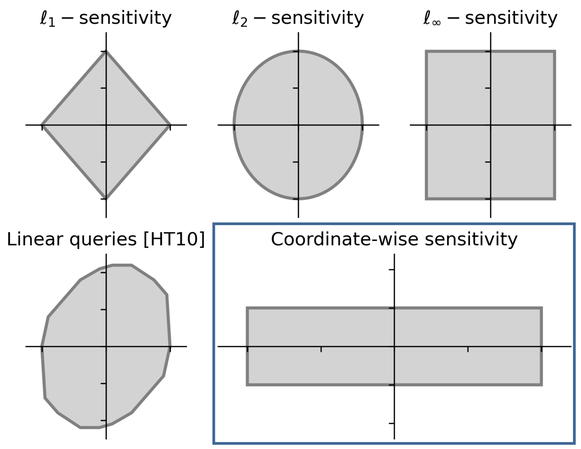
Error measure

For some $p > 0$, the goal is to minimize the pth moment of the error of $\mathscr{M}(x)$:

$$\|\mathscr{M}(x) - f(x)\|_p^p := \sum_{i=1}^{d} |\mathscr{M}(x)_i - f(x)_i|^p$$

Sensitivities

The sensitivity of each coordinate is denoted by $\vec{\Delta} = (\Delta_1, \ldots, \Delta_d)$. That is, $|f(x)_i - f(x')_i| \leq \Delta_i$ when x and x' are neighbors.



Technique

For some fixed $p > 0$, modify standard additive noise mechanisms to minimize

$$\mathbb{E}\left[\|\mathscr{M}(x) - f(x)\|_p^p\right]$$

- Instead of sampling i.i.d. noise, we can scale magnitude of noise based on $\vec{\Delta}$.
- We can reduce noise at coordinates with low sensitivity by increasing noise at coordinates with high sensitivity.

Gaussian Mechanism

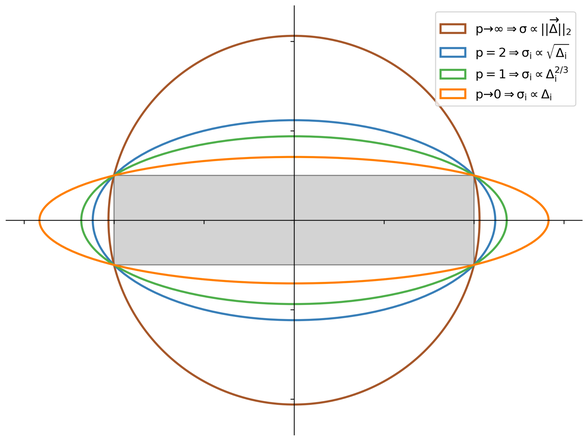
For i.i.d. noise scaled by $\|\vec{\Delta}\|_2$ we have

$$\mathbb{E}\left[\|\text{GaussMech}(x) - f(x)\|_p^p\right] \propto d \cdot \|\vec{\Delta}\|_2^p$$

The error is minimized for $\sigma_i \propto \Delta_i^{2/(p+2)}$.

$$\mathbb{E}\left[\|\mathscr{M}(x) - f(x)\|_p^p\right] \propto \|\vec{\Delta}\|_{2p/(p+2)}^p$$

Improves error by a factor in $[1, d)$.



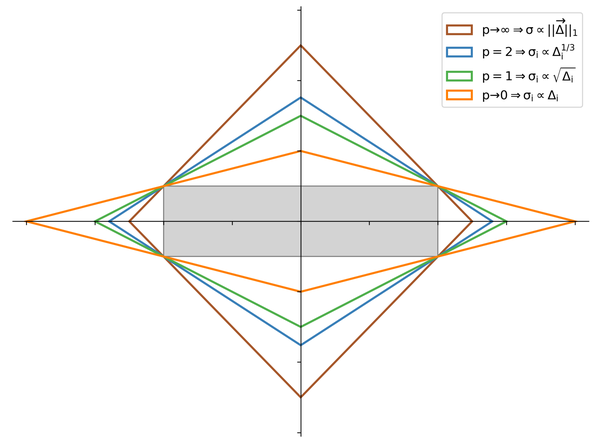
Laplace Mechanism

For i.i.d. noise scaled by $\|\vec{\Delta}\|_1$ we have

$$\mathbb{E}\left[\|\text{Lap}(x) - f(x)\|_p^p\right] \propto d \cdot \|\vec{\Delta}\|_1^p$$

The error is minimized for $\sigma_i \propto \Delta_i^{1/(p+1)}$.

$$\mathbb{E}\left[\|\mathscr{M}(x) - f(x)\|_p^p\right] \propto \|\vec{\Delta}\|_{p/(p+1)}^p$$



Potential Future Work

- Lower bounds on expected error.
- Better comparison with related work ([HT10], [NTZ13], [AS19]).
- Other error metrics e.g. ℓ_2-distance.

References

[DMNS06] Dwork, McSherry, Nissim & Smith. Calibrating Noise to Sensitivity in Private Data Analysis. TCC 2006.
[HT10] Hardt & Talwar. On the Geometry of Differential Privacy. STOC 2010
[NTZ13] Nikolov, Talwar, and Zhang: The Geometry of Differential Privacy: The Sparse and Approximate Cases. STOC 2013.
[AS21] Awan & Slavkovic. Structure and Sensitivity in Differential Privacy: Comparing K-Norm Mechanisms. JASA 2021.
[Online forum] Mark: https://crypto.stackexchange.com/q/85581

Research supported by the VILLUM foundation grant number 16582.

chle@itu.dk pagh@di.ku.dk