Privately Solving Linear Programs

Hsu, Roth, Roughgarden, Ullman
Discussed by Andy Haupt

MIT Hamsa Group

July 2020

Some (Re)View

$\mathcal{M}$ is (ε, δ)-DP if for neighboring "Databases"

$$\mathbb{P}[\mathcal{M}(D) \in S] \le e^{\varepsilon}\mathbb{P}[\mathcal{M}(D') \in S] + \delta.$$

Laplace Mechanism

Assume $|\mathcal{M}(D) - \mathcal{M}(D')| \le \Delta$.
Then, $D \mapsto \mathcal{M}(D) + \nu$, $\nu \sim \text{Laplace}(\frac{\varepsilon}{\Delta})$ is ε-DP.

Exponential Mechanism

Let $Q\colon (r, D) \to \mathbb{R}$ give loss of solution r with data D. Assume $|Q(r, D) - Q(r, D')| \le \Delta$. Then $\mathcal{M}$ with

$$\mathbb{P}[\mathcal{M}(D) = r] \propto e^{\frac{\varepsilon Q(r,D)}{2\Delta}}$$

is ε-DP and approximates loss-minimization in PAC sense.

Goals and Prereqs

After this, you are able to...

- ...define and give an example of High- and Low-Sensitivity Differential Privacy (DP).
- ...identify DP-relevant parts in an algorithm.
- ...illustrate with an example why High-Sensitivity DP might be incompatible with accuracy.

Motivation

$$\max_{x \in \mathbb{R}_+^d} c(D)^\intercal x$$
$$\text{s.t. } A(D)x \leq b(D)$$

- How to get a private output of x?
  - Laplace Mechanism does not like $\mathbb{R}^d$
  - Exponential Mechanism does not like exp. large search space
  - Perturbing the objective/output cannot recognize constraints
- When are the efficient, DP approximation algorithms
- (. . . which do not necessarily return feasible outputs)?

Differential Privacy for LPs

$$\max_{x \in \mathbb{R}^d_+} c(D)^\intercal x$$
$$\text{s.t. } A(D)x \leq b(D)$$

Definition (DP4LPs)

A randomized algorithm $\mathcal{M}\colon D := (c, A, b) \mapsto x \in \mathbb{R}^d$ is (ε, δ)-DP if for any $S \in \mathbb{R}^d$ and D, D' neighboring LPs

$$\mathbb{P}[\mathcal{M}(D) \in S] \leq e^\varepsilon \mathbb{P}[\mathcal{M}(D') \in S] + \delta.$$

- high-sensitivity neighboring LPs: ≤ 1 entry in (c, A, b) differs
- low-sensitivity neighboring LPs: $\|D - D'\| \leq \frac{1}{n}$ in some norm $\| \bullet \|$ (either $\| \bullet \|_1$ or $\| \bullet \|_\infty$)

Overview of Results

Location of change	High sensitivity	Low sensitivity
Objective c	No (Section 5)	Yes (Section 4.5)
Scalar b	No (Section 5)	Yes (Folklore, Section 4.2)
Row/All of A	Yes* (Section 3)	Yes (Section 4.4)
Column of A	No (Section 5)	Yes (Section 4.4)

1. High Sensitivity: DP and accuracy are incompatible
2. Low sensitivity: There are efficient algorithms
3. Constraint Matrix, High Sensitivity: There is an efficient algorithm, if we may violate small number of constraints

- I will givyou the case for DP in the right hand side of equations and for the constraint matrix.
  - Similar techniques apply to the other ones
  - Easiest impossibility result

DP and Non-Reconstructability

Theorem (Reconstruction)

Assume that there is a function $\mathcal{M}\colon \{0,1\}^n \to [0,1]^n$ *that is* (ε,δ)*-DP and* $\|\mathcal{M}(D) - D\|_1 \leq \alpha n$. *Then*

$$\alpha \geq \frac{1}{2} - \frac{e^{\varepsilon} + \delta}{2(1+e^{\varepsilon})(1-\beta)}.$$

- Blackboard

Incompatibility

- Databases are bit strings

$$\begin{aligned} &\text{find } x \\ &\text{s.t. } x_i = D_i, \quad \forall i \in [m] \end{aligned}$$

- Changes of one bit yield neighboring databases.
- Call x^* α-feasible if $Ax^* \leq b + \alpha\mathbb{1}$.
- D, D' neighboring in high sensitivity regime for b if they differ in at most one entry.

Theorem

If $\mathcal{M}$ is (ε, δ)-high sensitivity DP in b and finds an α-feasible distribution with probability at least $\frac{e^\varepsilon+\delta}{e^\varepsilon+1}$, then $\alpha \geq \frac{1}{2}$.

Efficient Approximation Algorithms

- Assume only b depends on RHS and that D, D' are neighboring if $\|b(D) - b(D')\|_\infty \leq \Delta_\infty$
- Find ε-private (α, γ)-dual oracle/apx. strongest violation, i.e.
  - Input: A, b, x
  - Output: $i \in [m]$ s.th. $A_i x \geq \max_j A_j x - b_j - \alpha$ w.p. $\geq 1 - \gamma$.
- (Reduce optimization to feasibility)
- Write down a generic (Multiplicative-Weights) Algorithm that uses a dual oracle
- Show existence of dual oracle
- Use composition to prove DP for complete algorithm
- Use a known performance bound for approximate dual oracles to prove performance in PAC sense.

Generic Multiplicative Weights

Algorithm 3 The Multiplicative Weights Algorithm, MW_η

Let $\widetilde{A}^1$ be the uniform distribution on $\mathcal{A}$

For $t = 1, 2, \ldots, T$:

  Receive loss vector ℓ^t (may depend on $A^1, \ldots, A^t$)

  For each $a \in \mathcal{A}$**:**

    Update $A_a^{t+1} = e^{-\eta \ell_a^t} \widetilde{A}_a^t$ for every $a \in \mathcal{A}$

  Normalize $\widetilde{A}^{t+1} = A^{t+1} / |A_{t+1}|$

Feasibility Algorithm using (α, γ)-dual oracle

- Input: A, b
- Output: x
- Initialization: $\rho = \|A\|_\infty$, η, T parameters depending on d, T, ρ, α

For $t = 1, \ldots, T$:
  Find $p^t = Oracle(A, b, \widetilde{x}^t)$
  Compute losses $\ell_i^t := (1/\rho) A_{p^t i}$
  Update $\widetilde{x}^{t+1}$ from $\widetilde{x}^t$ and ℓ^t via multiplicative weights.
Output $\overline{x} = (1/T) \sum_{t=1}^{T} \widetilde{x}^t$

And what is the Oracle?

- Use exponential mechanism on set $[m]$
- $Q(i, D) = A_i x - b_i$

Exponential Mechanism

Let $Q \colon (r, D) \to \mathbb{R}$ give loss of solution r with data D. Assume $|Q(r, D) - Q(r, D')| \leq \Delta$. Then $\mathcal{M}$ with

$$\mathbb{P}[\mathcal{M}(D) = r] \propto e^{\frac{\varepsilon Q(r,D)}{2\Delta}}$$

and approximates loss-minimization in PAC sense.

- Δ needs to be controlled from A, b
- Approximate optimality via PAC bound.

What is different for High Sensitivity?

- If the distribution we get from MWU is too sparse, there might be higher sensitivity for changes in a few entries
- We hence should densify the input
- This is done via Bregman projections
- The Bregman projections are not too bad if the LP has bounded width
- . . . but we have to sacrifice that all constraints might be satisfied.

Discussion

- When is DP (and not joint DP) the correct approach?
- When is low sensitivity a fair assumption?
- How do fairness and DP interact in the light of these results?