A Differentially Private Linear-Time fPTAS for the Minimum Enclosing Ball Problem

Bar Mahpud and Or Sheffet
{mahpudb, or.sheffet}@biu.ac.il

Neural Information Processing Systems Foundation, November 2022

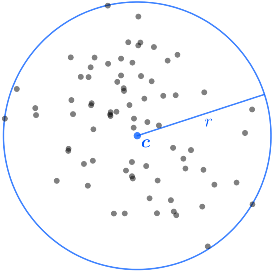
Tradition of Excellence

BIU
Center for Research in Applied Cryptography and Cyber Security

1-Cluster Problem

Minimum Enclosing Ball (MEB) Problem

Given a set P of n points in $\mathbb{R}^d$, the MEB problem is to find a ball with minimum radius that covers all points in P.
The resulting ball center and its radius are denoted by $c_{opt}(P)$ and $r_{opt}(P)$, respectively.



Differential Privacy

(ϵ, δ)-differential privacy [DR14]

A randomized algorithm $\mathcal{A} : \mathcal{U}^n \to \mathcal{O}$ is (ϵ, δ)-differentially private if for all $\mathcal{S} \subseteq \mathcal{O}$ and for all $D, D' \in \mathcal{U}^n$ such that $||D - D'||_1 \leq 1$:

$$\Pr[\mathcal{A}(D) \in \mathcal{S}] \leq e^{\epsilon} \Pr[\mathcal{A}(D') \in \mathcal{S}] + \delta$$

where the probability space is over the coin flips of the algorithm $\mathcal{A}$.
If $\delta = 0$, we say that $\mathcal{A}$ is ϵ-differentially private.

Differentially Private MEB:

- Locating a small cluster privately [NSV16]
- Clustering algorithms for the centralized and local models [NS18]
- Differentially private clustering: Tight approximation ratios [GKM20]

Our Work

Our result:

- $(1+\gamma)$ DP-MEB approximation
- Running time $\tilde{O}(n/\gamma^2)$ - fPTAS
- $\tilde{O}(\sqrt{d}/\gamma\epsilon)$ Points uncovered

Main Algorithm(θ^0, r)

Gets θ^0, r where $\|\theta^0 - \theta_{opt}\| \leq 10 r_{opt}$ and $r_{opt} \leq r \leq 4 r_{opt}$ (from [NS18])
Outputs θ s.t. $\|\theta - \theta_{opt}\| \leq \gamma r_{opt}$

Analysis

Main ALG(θ^0, r):

- Repeat:
  - Compute the mean μ of the points uncovered by the current $B(\theta^t, r)$
  - Update in a Perceptron-like style: $\theta^{t+1} \leftarrow \theta^t - \frac{\gamma^2}{2}(\mu - \theta^t)$
- Until $\tilde{O}({}^1/_{\gamma^2})$ repetitions

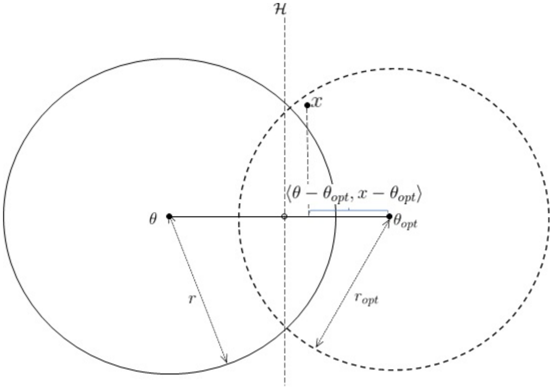
Making a $\tilde{O}(1/\gamma^2)$-size step towards this μ must push us significantly in the $\theta^t - \theta_{opt}$ direction.

$$\|\theta^{t+1} - \theta_{opt}\|^2 \leq (1 - \frac{\gamma^2}{2})\|\theta^t - \theta_{opt}\|^2 + \frac{\gamma^4}{4} r_{opt}^2$$

Thus $O(\frac{1}{\gamma^2} \log({}^1/_{\gamma^2}))$ steps exceed $\|\theta^{t+1} - \theta_{opt}\| \leq \gamma r_{opt}$

Intuition

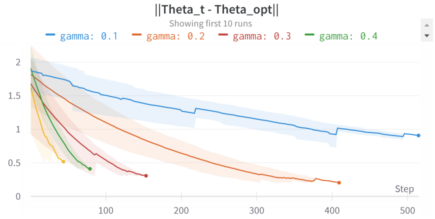
Any uncovered point has large projection on the "right" direction $\theta_{opt} - \theta^t$.

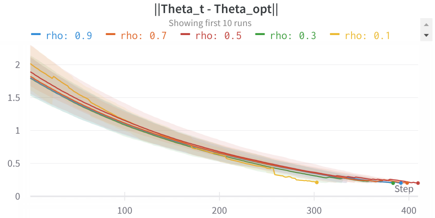


$$\langle \theta_{opt} - \theta^t, x - \theta_{opt} \rangle \geq \frac{1}{2} \|\theta^t - \theta_{opt}\|^2$$

Summary

- An iterative simple DP-algorithm
- Linear-time approximation scheme
- Empirically applicable





https://arxiv.org/abs/2206.03319

Questions?

Cynthia Dwork and Aaron Roth.
The algorithmic foundations of differential privacy.
Found. Trends Theor. Comput. Sci., 9(3–4):211–407, August 2014.

Badih Ghazi, Ravi Kumar, and Pasin Manurangsi.
Differentially private clustering: Tight approximation ratios.
In *NeurIPS*, 2020.

Kobbi Nissim and Uri Stemmer.
Clustering algorithms for the centralized and local models.
ArXiv, abs/1707.04766, 2018.

Kobbi Nissim, Uri Stemmer, and Salil Vadhan.
Locating a small cluster privately.
Proceedings of the 35th ACM SIGMOD-SIGACT-SIGAI Symposium on Principles of Database Systems, Jun 2016.