Efficient Online Learning using A Private Oracle

Alon Gonen, UCSD
Shay Moran, Princeton
Elad Hazan, Princeton
Private & Online Learning

- Differential private learning: learning in differentially private manner
- Online learning: sequential decision making against adversarial environments
- What’s the connection?
Common Theme: Stability

“As stability is also increasingly understood to be a key necessary and sufficient condition for learnability, we observe a tantalizing moral equivalence between learnability, differential privacy, and stability.” [Dwork & Roth, 2014]
Main Result

Open Question:

“Can every differentially private learning algorithm be used in a black box manner to efficiently obtain a no-regret learning algorithm?” [Neel, Roth, Wu, 2018]

**Theorem.** [Gonen, Hazan, Moran - NeurIPS ‘19]

Any pure-DP learner for $\mathcal{H}$ can be **efficiently** transformed to an online learner for $\mathcal{H}$
Previous Non-constructive Reductions

- Pure DP $\rightarrow$ Online Learning (Feldman, Xiao, 2014): via communication complexity
- Approximate DP $\rightarrow$ Online Learning (Alon, Livni, Malliaris, Moran, 2018): via Ramsey Theory
Open Questions

Agnostic setting

Approximate DP

Efficient reduction from approximate DP to online learning
Thank You!