GML Autumn 23 - Project Proposal

Jiaqing Xie, Yucheng Sun

October 2023

Choice of paper: *An Equivalence Between Private Classification and Online Prediction*

1 Division of Labor

The proof of the main results is divided into two steps. Each one of us will focus on understanding one step of the proof.

Step 1: Show that every class with a finite littlestone dimension can be learned by a global stable learning algorithm (Jiaqing Xie)

Step 2: Show that it's feasible to obtain a differentially private learner from any global stable learner (Yucheng Sun)

2 Motivation of the Paper

The idea is to prove an equivalence between online learning and differentially private learning, which is equivalent to state that given a class of predictors $\mathcal{H}$, if $\mathcal{H}$ is differentially private learnable, then it must be online learnable, and vice versa. In order to prove this, two iff. conditions are considered.

1. DP-learning $\leftrightarrow$ Littlestone dimension is finite. Previous work has proved that a private PAC learner hinted a corresponding finite littlestone dimension [ALMM19]. The selected paper supplemented the converse direction [BLM20], therefore combining two results suffices to show the equivalence of private learning and finite littlestone dimension. In this project, we mainly focus on the latter part. Global stability is defined in this paper as an intermediate step for proofs. When proving from finite littlestone dimension to global stable learning, Standard Optimal Algorithm (**SOA**) is involved by operating on a pair of samples. We want to prove that such SOA$(\cdot)$ as an algorithm satisfies the definition of global stability that is also generalized well for some finite number of samples. When proving from global stable learning to private learning, stable histograms are involved and we need to construct such a private learner with some privacy/accuracy parameters satisfying stable conditions, as well as satisfying the statement of a generic private learner [KLNRS11].

2. If H is online-learnable $\leftrightarrow$ its Littlestone dimension is finite. Previous works have stated this conclusion with regard to the regret which depends on corresponding littlestone dimension and number of samples [Lit88; BPS09]. In our selected paper, authors also re-stated this conclusion when introducing the relationship between online learning and finite Littlestone dimension [BLM20].

If both iff. conditions are satisfied, use transitive law will lead to the conclusion.

References

[ALMM19] Noga Alon, Roi Livni, Maryanthe Malliaris, and Shay Moran. "Private PAC learning implies finite Littlestone dimension". In: *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*. 2019, pp. 852–860 (cit. on p. 1).

[BLM20] Mark Bun, Roi Livni, and Shay Moran. "An equivalence between private classification and online prediction". In: *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE. 2020, pp. 389–402 (cit. on pp. 1, 2).

[BPS09] Shai Ben-David, Dávid Pál, and Shai Shalev-Shwartz. "Agnostic Online Learning." In: *COLT*. Vol. 3. 2009, p. 1 (cit. on p. 2).

[KLNRS11] Shiva Prasad Kasiviswanathan, Homin K Lee, Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith. "What can we learn privately?" In: *SIAM Journal on Computing* 40.3 (2011), pp. 793–826 (cit. on p. 1).

[Lit88] Nick Littlestone. "Learning quickly when irrelevant attributes abound: A new linear-threshold algorithm". In: *Machine learning* 2 (1988), pp. 285–318 (cit. on p. 2).