User-Specified Local Differential Privacy in Unconstrained Adaptive Online Learning

Dirk van der Hoeven

Abstract

Standard Local Differential Privacy:
• All uses have the same privacy requirements.
• Learner chooses how much privacy users have.

User-Specified Local Differential Privacy:
• All uses have the same privacy requirements.
• Learner chooses how much privacy users have.

Adaptive Unconstrained algorithms:
• Compete with \( u \in \mathbb{R}^d \)
• Adapt to unknown and varying noise.
• Data dependent bounds.

Approach to Unconstrained OCO: Reward Regret Duality

User-Specified Local Differential Privacy in Unconstrained Adaptive Online Learning

Private Unconstrained Online Convex Optimization with Noisy Subgradients

Local Differential Privacy: Let \( A = (X_1, \ldots, X_T) \) be a sensitive dataset where each \( X_t \) corresponds to data about individual \( t \). A randomiser \( R \) which outputs a disguised version of \( S = (U_1, \ldots, U_T) \) of \( A \) is said to provide \( \epsilon \)-local differential privacy to individual \( t \) if for all \( x, x' \in A \) and for all \( S \subseteq \mathcal{S} \),

\[
Pr(U_t \in S | X_t = x) \leq e^\epsilon Pr(U_t \in S | X_t = x').
\]

User specified LDP Unconstrained OCO:

0 for \( t = 1, 2, \ldots, T \) do
1. The learner sends \( w_t \in \mathbb{R}^d \) to the provider of the \( t \)-th subgradient.
2. The provider chooses zero-mean and symmetrical \( \rho_t \) and samples \( \xi_t \sim \rho_t \).
3. The provider computes subgradient \( g_t = \partial L_t(w_t) \), where \( \|g_t\|_1 \leq G \).
4. The provider sends \( \tilde{g}_t = g_t + \xi_t \in \mathbb{R}^d \) to the learner.

Only bounded in \( \mathbb{R} \) Unconstrained comparator

Objective: minimize expected regret w.r.t. oracle parameter \( u \in \mathbb{R} \)

\[
E[R_T(u)] = \sum_{t=1}^T E[\langle u, g_t \rangle - \langle u, \tilde{g}_t \rangle].
\]

Goal: achieve adaptive expected regret bounds with unknown LDP requirements

\[
E[R_T(u)] = O \left( E[\|u\|^2] + \max_{t \in [T]} E[\|\tilde{g}_t\|^2] \ln(1 + \|u\|^2) \right).
\]

Previous work with known \( \rho_t \):

\[
O(\|u\|^2 \sqrt{G^2 + \max_{t \in [T]} E[\|\tilde{g}_t\|^2]} \ln(1 + \|u\|^2)).
\]

Applicaton: Sparse Gradients

We play \( v \xi_t \), where \( v \) is the prediction in (3) and \( \|\xi\| \leq 1 \) comes from a standard OCO algorithm. By using the black-box reduction of Culler and Orabona 2018 we obtain:

\[
E[R_T(u)] = \mathbb{E} \left[ \sum_{t=1}^T \langle v - u, \tilde{g}_t \rangle \right] + \mathbb{E} \left[ \sum_{t=1}^T \langle u, \tilde{g}_t \rangle \right] = 0.
\]

Application: 1d to d Black-Box Reduction

Private expert setting:
1. Learner plays probability distribution \( p_i \) over experts.
2. Experts sample \( \xi_t \sim \rho_t \).
3. Experts receive their losses \( \ell_t \).
4. Experts send their perturbed losses \( \ell_t = \ell_t + \xi_t \) to the learner.

The analysis of recent adaptive expert algorithms is closely related to the analysis in this paper. Using this relationship we can easily derive private and adaptive expert algorithms. Replace \( \gamma_t \) by the instantaneous regret \( \hat{\gamma}_t(i) = (p_i - c_i, \ell_t) \), where \( \ell_t = \ell_t + \xi_t \) and \( \ell_t \) is a vector containing the expert losses. If we play

\[
p_i(i) \propto p_i(i) \mathbb{E} \left[ \exp(- \sum_{t=1}^T \hat{\gamma}_t(i) - (v \xi_t(i))^2) \right],
\]

where \( P_t \) is a prior on \( v \in \{0, 1\} \).

It can be shown that, by using (2) instead of the prod bound in the analysis of quinst, that the expected regret satisfies:

\[
E[R_T(i)] = O \left( \mathbb{E} \left[ \sum_{t=1}^T \hat{\gamma}_t(i)^2 \right] \right).
\]

A More Granular Randomiser

For more control over the privacy we employ the Local Laplace randomiser:

\[
\rho_t(z) = \exp(- \sum_{j=1}^d \tau_j z_j), \text{ where } \sum_{j=1}^d \tau_j = \epsilon, \tau_j \geq 0.
\]