Lecture 8

Private Multiplicative Weights

Linear Queries

$\mathcal{X} = \{s_1, \ldots, s_{|\mathcal{X}|}\}$.

$q : \mathcal{X} \to [0,1]$

$X \in \mathcal{X}^n$ $q(X) = \frac{1}{n} \sum_{i \in [n]} q(X_i)$

Set Q of queries

$M : \mathcal{X}^n \to [0,1]^{|Q|}$

$\forall q_j \in Q$, $|M_j(X) - q_j(X)| \le \alpha$, M is DP

Histograms

$|Q_{Hist}| = |\mathcal{X}|$

$q_s(x) = \begin{cases} 1 & \text{if } x = s \\ 0 & \text{o.w.} \end{cases}$

Marginal q's

$\mathcal{X} = \{0,1\}^d$

$|Q_{Marg}| = d$

$q_j(x) = x_j$

Some Algorithms

Laplace: $M_j(X) = q_j(X) + \text{Lap}\left(\frac{|Q|}{\varepsilon n}\right)$, $\forall q_j \in Q$. $n \ge \frac{c|Q| \log|Q|}{\alpha \varepsilon} \to \boxed{\frac{c|Q|}{\alpha\varepsilon}}$ ε-DP

Gaussian: $n \ge c\frac{\sqrt{|Q| \log|Q| \log(1/\delta)}}{\alpha \varepsilon} \to \boxed{c\frac{\sqrt{|Q| \log\log|Q| \log(1/\delta)}}{\alpha\varepsilon}}$ (ε, δ)-DP

$n \ge \boxed{c\frac{\sqrt{|\mathcal{X}| \log|Q|}}{\alpha\varepsilon}}$ Thm 2.9 Vadhan 17 ε-DP

SmallDB ε-DP

$n \ge \boxed{\tilde{O}\left(\frac{\log|Q| \log|\mathcal{X}|}{\alpha^3 \varepsilon}\right)}$ running time $|\mathcal{X}|^{O\left(\frac{\log|Q|}{\alpha^2}\right)}$

Private Multiplicative Weights

$n \ge \tilde{O}\left(\frac{\log|Q| \sqrt{\log|\mathcal{X}| \log(1/\delta)}}{\alpha^2 \varepsilon}\right)$ $\tilde{O}\left(\frac{|Q| n |\mathcal{X}|}{\alpha^2}\right)$ r.t.

Non-Private Multiplicative Weights

A Perfect Expert

- Setting

N experts

$t = 1, \ldots, T$

expert i's prediction $p_i^t = U$ or D

You make prediction p^t U or D

$s^t = U$ or D

If $p^t \neq s^t$, mistake

Claim 2. *There is an algorithm that always makes at most* $\log N$ *mistakes.*

Algorithm 1: An algorithm with a perfect expert

Set $S^1 = [N]$
for $t = 1$ *to* T **do**
  Let $S^t_U = \{i : p^t_i = U\}$ be the set of experts who picked U, and similarly $S^t_D = \{i : p^t_i = D\}$
  If $|S^t_U| > |S^t_D|$ then predict U, otherwise predict D
  Set $S^{t+1} = S^t_{s^t}$
end

Mistake at t. $|S^{t+1}| \leq |S^t|/2$

$\Rightarrow$ # of mistakes $\leq \log N$

Regret: Error of real algo − Error of best in hindsight

A Best Expert

best exp. makes OPT mistakes

Diffs: - down weighting
- weighted majority

Claim 3. *There is an algorithm that makes at most* $2.4(OPT + \log N)$ *mistakes.*

Algorithm 2: Weighted Majority Algorithm

Set $w_i^1 = 1$ for all $i \in [N]$
for $t = 1$ *to* T **do**
  Let $W_U^t = \sum_{i:p_i^t=U} w_i^t$ be the weight of experts who picked U, and similarly $W_D^t = \sum_{i:p_i^t=D} w_i^t$
  If $W_U^t > W_D^t$ then predict U, otherwise predict D
  For all i such that $p_i^t \neq s^t$, set $w_i^{t+1} = \frac{1}{2} w_i^t$
end

$W^T = \sum_{i=1}^{N} w_i^T$ $\qquad$ $M = \#$ of alg's mistakes

Lower: $W^T \geq (1/2)^{OPT}$

Upper: $W^T \leq N(3/4)^M = (\underbrace{\tfrac{1}{2}}_{\text{right}} + \underbrace{\tfrac{1}{2}\cdot\tfrac{1}{2}}_{\text{wrong}})^M N$

$(1/2)^{OPT} \leq N(3/4)^M$

$\Rightarrow (4/3)^M \leq N 2^{OPT} \Rightarrow M \log(4/3) \leq \log N + OPT$

$M \leq \dfrac{OPT + \log N}{\log(4/3)} \leq 2.4(OPT + \log N)$ ☒

Multiplicative Weights Algorithm

-Setting

Seq of T rounds, $l_i^t \in [-1,1]$

In each:

- Algo chooses $i^t \in [N]$
- Expert i experiences loss l_i^t.

Algo's loss $l_A^t = l_{i^t}^t$

$L_A^T = \sum_{t=1}^{T} l_A^t$, $L_i^T = \sum l_i^t$. regret: $L_A^T - \min_i L_i^T$

Algorithm 3: Polynomial Weights Algorithm

Set $w_i^1 = 1$ for all $i \in [N]$
for $t = 1$ *to* T **do**
  Let $W^t = \sum_{i=1}^{N} w_i^t$
  Select expert i with probability w_i^t / W^t
  Update $w_i^{t+1} = w_i^t(1 - \gamma \ell_i^t)$, where γ is some parameter to be set.
end

Theorem 4. *For an arbitrary sequence of losses, and any expert i,*

$$\mathbf{E}[L_A^T] \le L_i^T + 2\sqrt{T \ln N}$$

In particular, this holds for the best expert.

A Rephrasing

Seq of T rounds

- Alg chooses dist p^t over $[N]$
- Algo experiences loss $l_A^t = l^t \cdot p^t = \sum p_i^t l_i^t$

- Setting

Arora Hazan Kale

Algorithm 4: Polynomial Weights Algorithm - Distributional Phrasing

Set $w_i^1 = 1$ for all $i \in [N]$
for $t = 1$ *to* T **do**
  Let $W^t = \sum_{i=1}^N w_i^t$
  Select p^t to have $p_i^t = w_i^t / W^t$
  Update $w_i^{t+1} = w_i^t(1 - \gamma \ell_i^t)$, where γ is some parameter to be set.
end

Theorem 5. *For an arbitrary sequence of loss functions:*

$$\sum_{t=1}^T \ell^t \cdot p^t \leq \sum_{t=1}^T \ell^t \cdot p + 2\sqrt{T \ln N},$$

where p is any fixed distribution over $[N]$.

Proof: UB + LB on W^t

$$W^t = \sum_{i \in [N]} w_i^t$$

UB: $$W^{t+1} = \sum w_i^t (1 - \gamma \ell_i^t) = W^t (1 - \gamma \ell^t \cdot p^t)$$

$$W^{T+1} = N \prod_{t=1}^T (1 - \gamma \ell^t \cdot p^t)$$

log, $\ln(1-x) \leq -x$:

$$\ln W^{T+1} = \ln N + \sum_{t=1}^T \ln(1 - \gamma \ell^t \cdot p^t)$$

$$\leq \ln N - \gamma \sum_{t=1}^T \ell^t \cdot p^t$$

$$\boxed{\ln W^{T+1} \leq \ln N - \gamma \sum \ell^t \cdot p^t}$$

Fix some expert i.

$$\ln(1-x) \geq -x - x^2 \quad -\tfrac{1}{2} \leq x \leq \tfrac{1}{2}$$

$$\ln W^{T+1} \geq \ln w_i^{T+1} \rightarrow$$

$$= \sum_{t=1}^{T} \ln(1-\gamma l_i^t) = -\sum \gamma l_i^t - \sum (\gamma l_i^t)^2$$

$$\ln W^{T+1} \geq -\gamma L_i^T - \gamma^2 T$$

$$-\gamma(p \cdot L^T) - \gamma^2 T = -\gamma \sum_{t=1}^{T} p \cdot l_i^t - \gamma^2 T \leq \ln W^{T+1}$$

$$-\gamma \sum_{t=1}^{T} p \cdot l^t - \gamma^2 T \leq \ln W^{T+1} \leq \ln N - \gamma \sum p^t \cdot l^t$$

$$\gamma \sum p^t \cdot l^t \leq \gamma \sum p \cdot l^t + \gamma^2 T + \ln N$$, Divide by γ

$$\gamma = \sqrt{\frac{\ln N}{T}}$$

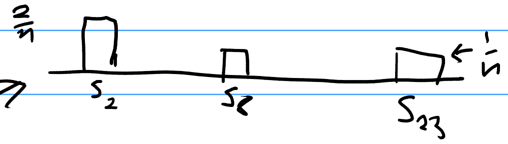
$$\sum p^t \cdot l^t \leq \sum p \cdot l^t + 2\sqrt{T \ln N}$$ ▨

$$\gamma^2 T + \ln N$$

Multiplicative Weights for Queries

- Setting

$Q \;,\quad q(X) = \frac{1}{n}\sum_{k\in[n]} q(X_k)$



$$\begin{bmatrix} X_1 = S_2 \\ X_2 = S_8 \\ \dots \\ X_{n-1} = S_2 \\ X_n = S_{23} \end{bmatrix} \qquad \mathcal{X} = \{S_1, \dots, S_{|\mathcal{X}|}\}$$

$\xrightarrow{\text{Histogram}}$ $p_i = \frac{|\{k : X_k = i\}|}{n}$

empirical distribution

$$q(X) = \sum_{i\in\mathcal{X}} q(i)\,p_i \triangleq \langle q, p\rangle$$

T rounds
- Adversary picks $q^t \in Q$
- Algo picks p^t over $\mathcal{X}$

$$\text{regret} = \sum_{t=1}^{T} |\langle q^t, p^t\rangle - \langle q^t, p\rangle| \triangleq \sum_{t=1}^{T} f^t(p^t)$$

$\langle q^t, p\rangle$

Ideas and Derivations

$$f^t(p^t) = |\langle q^t, p^t\rangle - \langle q^t, p\rangle|$$

$$f(p^t) + \nabla f(p^t)\cdot(p - p^t) \le f(p)$$

$f(p) = 0$, rearrange

$$f(p^t) \le \nabla f(p^t)\cdot(p^t - p)$$

$$\sum \ell^t\cdot(p^t - p) < 2\sqrt{T\ln N}$$

$$\sum f^t(p^t) \le \sum \nabla f^t(p^t)\cdot(p^t - p)$$

$$\sum |\langle q^t, p^t\rangle - \langle q^t, p\rangle| \le \sum \nabla f^t(p^t)\cdot(p^t - p)$$

$$\ell^t = \nabla|\langle q^t, p^t\rangle - \langle q^t, p\rangle| \Rightarrow \underset{[-1,1]^{|\mathcal{X}|}}{\ell_i^t} = \begin{cases} q^t(i) & \text{if } \langle q^t, p^t\rangle \ge \langle q^t, p\rangle \\ -q^t(i) & \text{o.w.} \end{cases}$$

Theorem 6. *Given an arbitrary sequence of T queries, we have the following regret bound:*

$$\sum_{t=1}^{T} |\langle q^t, p^t \rangle - \langle q^t, p \rangle| \le 2\sqrt{T \ln |\mathcal{X}|}.$$

Regret → Mistake Bound

p^{T+1}. Mistake at t: $|\langle q^t, p^t \rangle - \langle q^t, p \rangle| > \alpha$

Suppose q^t always causes a mistake

regret $\geq \alpha T$, regret $\leq 2\sqrt{T \ln|\mathcal{X}|}$

$T \leq \frac{4 \ln|\mathcal{X}|}{\alpha^2}$.

Algorithm 5: A non-private multiplicative weights algorithm for answering linear queries

Set $p^1_i = 1/|\mathcal{X}|$ for all $i \in \mathcal{X}$
for $t = 1$ *to* T **do**
  Choose a query $q^t \in \mathcal{Q}$ such that $|\langle q^t, p^t \rangle - \langle q^t, p \rangle| \geq \alpha$
  Compute $s = \text{sign}(\langle q^t, p^t \rangle - \langle q^t, p \rangle)$
  Update $p^{t+1}_i \propto p^t_i \left(1 - s\left(\sqrt{\frac{\ln|\mathcal{X}|}{T}}\right) q^t_i\right)$
end

Corollary 7. *Algorithm 5 can only run for at most $4 \ln|\mathcal{X}|/\alpha^2$ timesteps, until it is no longer able to select a $q \in \mathcal{Q}$ which causes a mistake. Consequently, we have that p^{T+1} correctly answers all queries $q \in \mathcal{Q}$ to accuracy $\leq \alpha$.*

Private Multiplicative Weights

Diffs: Exp Mech.
Lap mech.

Algorithm 6: Private multiplicative weights

Set $p_i^1 = 1/|\mathcal{X}|$ for all $i \in \mathcal{X}$
for $t = 1$ *to* T **do**
  Use the exponential mechanism to choose a query $q^t \in \mathcal{Q}$ with ε_0-DP, using score function $|\langle q^t, p^t\rangle - \langle q^t, p\rangle|$
  Compute $y^t = \langle q^t, p^t\rangle - \langle q^t, p\rangle + \text{Laplace}(1/\varepsilon_0 n)$ $\boxed{\ll \frac{\alpha}{100}}$
  If $|y^t| \le 2\alpha$, return p^t
  Otherwise, compute $s = \text{sign}(y^t)$
  Update $p_i^{t+1} \propto p_i^t \left(1 - s\sqrt{\frac{\ln|\mathcal{X}|}{T}} q_i^t\right)$
end

Privacy Analysis

$2\varepsilon_0$-DP. ~~$2\varepsilon_0 T$-DP $\Rightarrow$ Basic comp~~

$\hookrightarrow$ Adv comp $\left(O\left(\varepsilon_0\sqrt{T\log(1/\delta)}\right), \delta\right)$-DP.

$\varepsilon_0 = O\left(\frac{1}{\sqrt{T\log(1/\delta)}}\right) \Rightarrow (\varepsilon, \delta)$-DP

$T \le O\left(\frac{\log|\mathcal{X}|}{\alpha^2}\right)$

Accuracy Analysis

Lap: $\frac{1}{\varepsilon_0 n} \ll \frac{\alpha}{100}$. $n \ge \frac{1}{\alpha\varepsilon_0} \overset{T,\varepsilon_0}{\ge} \Omega\left(\frac{\sqrt{\log|\mathcal{X}|\log(1/\delta)}}{\alpha^2\varepsilon}\right)$

Exp: $\approx \frac{\log|Q|}{n\varepsilon_0} \ll \frac{\alpha}{100}$. $n \ge \frac{\log|Q|}{\varepsilon_0\alpha} \ge \Omega\left(\frac{\log|Q|\sqrt{\log|\mathcal{X}|\log(1/\delta)}}{\alpha^2\varepsilon}\right)$

$n \ge \tilde{\Omega}\left(\frac{\log|Q|\sqrt{\log|\mathcal{X}|\log(1/\delta)}}{\alpha^2\varepsilon}\right)$

p^{T+1} "synthetic dataset"