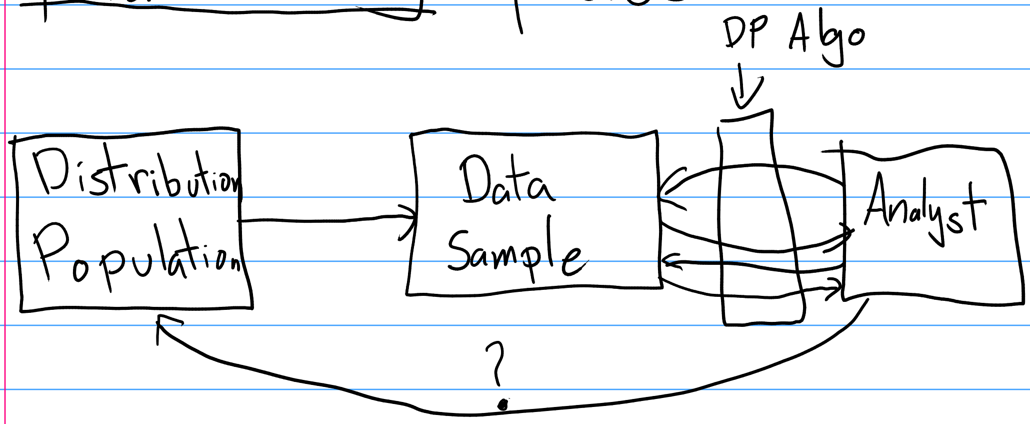
Lecture 16

Adaptive Data Analysis

Setup and Motivation

<u>p-Value hacking</u> $p<0.05$



Dist $\mathcal{D}$ on $\mathcal{X}$

$$q_1, \ldots, q_k : \mathcal{X} \to \{0,1\}$$

$$q_i(\mathcal{D}) := \mathbb{E}_{x\sim \mathcal{D}}[q_i(x)], \ \forall i \in [k]$$

$$X = (X_1, \ldots, X_n) \in \mathcal{X}^n, \quad X_j \sim \mathcal{D}$$

$$q_i(X) = \frac{1}{n}\sum_{j=1}^{n} q_i(X_j) \qquad q_i(\mathcal{D}) \approx q_i(X).$$

$$\forall i \ \Pr[|q_i(X) - q_i(\mathcal{D})| \geq \alpha] \leq 2\exp(-2\alpha^2 n)$$

$$\Pr[\exists i : |q_i(X) - q_i(\mathcal{D})| \geq \alpha] \leq 2k\exp(-2\alpha^2 n) \leq \beta$$

$$2\cancel{n}k/\beta \leq \exp(2\alpha^2 n) \Leftrightarrow n \geq \frac{\log(2k/\beta)}{2\alpha^2}$$

$$n \geq \log k \Leftrightarrow k \leq e^n$$

<u>Independence</u>

Bad new w/ adaptivity

What goes wrong adaptively?

$\mathcal{X} = \{1, \dots, k\}$

$q_i : \mathcal{X} \to \{0,1\}$

$q_i(x) = \begin{cases} 1 & \text{if } x = i \\ 0 & \text{else} \end{cases}$

Ask queries $q_1(X), \dots, q_k(X)$

Learn dataset X

$q_{k+1}(x) = \begin{cases} 1 & \text{if } x \in X \\ 0 & \text{else} \end{cases}$

$q_{k+1}(X) = 1$ but $q_{k+1}(D) \le n/k$

Unless $n = \Omega(k)$, no "generalization"

A naive Solution

Sample splitting

Split X into k parts $X^{(1)}, \dots, X^{(k)}$

Run ith query on ith part

$q_i(X^{(i)}) \simeq q_i(D)$ if $n^{(i)} \gtrsim \frac{\log(k/\beta)}{\alpha^2}$

Need $n > \frac{k \log(k/\beta)}{\alpha^2}$ (naive)

advanced composition

Today

$n \gtrsim \frac{\sqrt{k} \log(2k/\beta) \log(1/\alpha\beta)}{\alpha^2}$ ($\approx$optimal)

$\log(k)$ (nonadaptive)

$n \gtrsim \frac{\sqrt{\log|\mathcal{X}| \log(k/\beta) \log(1/\alpha\beta)}}{\alpha^3}$ ($\approx$optimal)

PMW

McSherry

Dwork Feldman Hardt Pitassi Reingold Roth '15

Bassily Nissim Smith Steinke Stemmer Ullman '16?

A "Transfer" Theorem

Theorem 1 ***(Transfer Theorem)*** *Suppose that the mechanism $\mathcal{M}$ takes n iid samples X from $\mathcal{D}$, and answers* ~~n~~ k *(adaptive) queries $q_1, \dots, q_k$ on X such that,*

i) $\forall X \in \mathcal{X}^n, \mathbb{P}_{\mathcal{M}}(\exists i : |q_i(X) - \mathcal{M}(X)_i| > \alpha) \leq \beta$, *where $\mathcal{M}(X)_i$ is the answer given by $\mathcal{M}$ to the i-th query;* M is accurate on dataset

ii) $\mathcal{M}$ *is $(\alpha, \alpha\beta)$-DP.* M is private

Then,

M generalizes

$$\mathbb{P}_{\mathcal{D},\mathcal{M}}(\exists i : |\cancel{q_i}\mathcal{M}_i(X) - q_i(\mathcal{D})| > C\alpha) \leq C\beta, \tag{1}$$

for some constant C.

Jung Ligett Neel Roth Sharifi-Malvajerdi Shenfeld '20

A Simpler Transfer Theorem

Theorem 3 (Easier Transfer Theorem) *Let $X \sim \mathcal{D}^n$ and let $\mathcal{M}$ be (ϵ, δ)-DP such that for every adaptive $q_1, \dots, q_k$ and for all $X \in \mathcal{X}^n$,* ← Private

$$\mathbb{E}_{\mathcal{M},X}[\max_i |q_i(X) - \mathcal{M}(X)_i|] \leq \alpha.$$ ← Accurate

Then,

$$\mathbb{E}_{\mathcal{M},X}[\max_i |q_i(\mathcal{D}) - \mathcal{M}(X)_i|] \leq \alpha + e^\epsilon - 1 + \delta. \quad \simeq \alpha + \varepsilon + \delta$$

Proof of Easier Transfer Theorem

Theorem 3 (Easier Transfer Theorem) *Let $X \sim \mathcal{D}^n$ and let $\mathcal{M}$ be (ϵ, δ)-DP such that for every adaptive $q_1, \ldots, q_k$ and for all $X \in \mathcal{X}^n$,*

$$\mathbb{E}_{\mathcal{M},X}[\max_i |q_i(X) - \mathcal{M}(X)_i|] \le \alpha.$$

Then,

$$\mathbb{E}_{\mathcal{M},X}[\max_i |q_i(\mathcal{D}) - \mathcal{M}(X)_i|] \le \alpha + e^\epsilon - 1 + \delta.$$

Key Lemma

Lemma 2 *Suppose $\mathcal{W}$ is (ϵ, δ)-DP and on input $X \in \mathcal{X}^n$, it outputs a counting query q. Let $X \sim \mathcal{D}^n$ (independent rows). Then,*

$$|\mathbb{E}_{X,\mathcal{W}}[q(D)|q = \mathcal{W}(X)] - \mathbb{E}_{X,\mathcal{W}}[q(X)|q = \mathcal{W}(X)]| \le e^\epsilon - 1 + \delta.$$

$$E[q(X)|q=W(X)] = \frac{1}{n}\sum E[q(X_i)|q=W(X)]$$
$$= \frac{1}{n}\sum \Pr[q(X_i)=1|q=W(X)]$$

$X_i' \sim D$, $X' = (X_1, \ldots, X_i', \ldots, X_n)$

$$\Pr[q(X_i)=1|q=W(X)] \le e^\varepsilon \Pr[q(X_i)=1|q=W(X')] + \delta$$

$$\Pr[q(X_i) = 1|q=W(X')] = \Pr[q(X_i')=1|q=W(X)]$$
$$= E[q(D)|q=W(X)]$$

$$E[q(X)|q=W(X)] \le e^\varepsilon \cdot E[q(D)|q=W(X)] + \delta$$

$$|E[q(X)|q=W(X)] - E[q(D)|q=W(X)]|$$
$$\le (e^\varepsilon - 1) E[q(D)|q=W(X)] + \delta \le e^\varepsilon - 1 + \delta \quad \square$$

Proof

Theorem 3 (Easier Transfer Theorem) *Let $X \sim \mathcal{D}^n$ and let $\mathcal{M}$ be (ϵ, δ)-DP such that for every adaptive $q_1, \ldots, q_k$ and for all $X \in \mathcal{X}^n$,*

$$\mathbb{E}_{\mathcal{M},X}[\max_i |q_i(X) - \mathcal{M}(X)_i|] \leq \alpha.$$

Then,

$$\mathbb{E}_{\mathcal{M},X}[\max_i |q_i(\mathcal{D}) - \mathcal{M}(X)_i|] \leq \alpha + e^\epsilon - 1 + \delta.$$

W: Choose q_i maximizing $|q_i(X) - M(X)_i|$

Double # of queries. $2k$ queries

$q_1, \ldots, q_k$ $\quad$ $(1-q_1), \ldots, (1-q_k)$

$M_1(X)$ $\quad$ $1-M_1(X)$

$$\max_i |q_i(D) - M(X)_i| = \max_i q_i(D) - M(X)_i$$

$+q_i(X) - q_i(X)$

$$E[\max_i q_i(D) - M(X)_i] = E[q_i(D) - M(X)_i \mid q_i = W(X)]$$

$$= E[q_i(D) - q_i(X) \mid q_i = W(X)] + E[q_i(X) - M(X) \mid q_i = W(X)]$$

$$\leq (e^\varepsilon - 1 + \delta) + (\alpha)$$

$\boxtimes$