Today: DP covariance estimation

Last class (FriendlyCore for mean estimation)

- Preprocess & remove outliers with soft weights $w \in [0, 1]$
- Check that not too many outliers removed (ie $\|w\|_1 \approx n$)
- Stable non-private estimator
- Add noise

Same formula today, more complex.

Bibliography

Presentation based on Brown, Hopkins & Smith 23

https://arxiv.org/abs/2301.12250

Similar techniques used in concurrent work of Duchi, Haque & Kuditipudi 23

https://arxiv.org/abs/2301.07078

Gaussian Sampling Mechanism is from Albi et al. 2023

https://arxiv.org/abs/2212.08018

Gaussian sampling mechanism

Alg 1 GSampling

Input: $\hat{\Sigma} \in \mathbb{R}^{d \times d}$, $m \in \mathbb{N}$

Output: $\tilde{\Sigma}$

(1) Sample $y_1, \dots, y_m \overset{iid}{\sim} \mathcal{N}(0, \hat{\Sigma})$

(2) Return $\tilde{\Sigma} = \frac{1}{m} \sum_{i=1}^{m} y_i y_i^T$

$$d_M(\Sigma_1, \Sigma_2) = \dots$$

Claim Fix $\varepsilon, \delta \in (0,1)$ and positive definite Σ_1, Σ_2.

If Σ_1, Σ_2 satisfy

~~$\max\{\|\Sigma_2^{-1/2}(\Sigma_1 - \Sigma_2)\Sigma_2^{-1/2}\|_F, \|\Sigma_1^{-1/2}(\Sigma_1 - \Sigma_2)\Sigma_1^{-1/2}\|_F\}$~~

$$d_M(\Sigma_1, \Sigma_2) \le \Delta \le \frac{\varepsilon}{8 \log 1/\delta},$$

then for any $m \le \frac{\varepsilon^2}{8\Delta^2 \log(1/\delta)}$ Alg 1's output satisfies $\tilde{\Sigma}_1 \approx_{(\varepsilon,\delta)} \tilde{\Sigma}_2$

Leverage Filtering

Approach: on input $X = x_1, \ldots, x_n$, produce $\hat{\Sigma}(X)$ s.t. $\forall x \sim x'$, $\hat{\Sigma}(x) \approx \hat{\Sigma}(x')$ as above

If $x \sim x'$ & $d_M(\Sigma_1, \Sigma_2)$ big, then one contains an outlier

Def $\ell(i) = x_i^T (X^T X)^{-1} x_i$

$\ell_S(i) = x_i^T (X_S^T X_S)^{-1} x_i$

like rescaled ℓ_2 norm, write $X^T X = A$,

expect for Gaussian data? $\frac{d}{n}$.

$\ell(i) = \|A^{-1/2} x_i\|^2$

Alg 2: Greedy Leverage Filtering

Input: $x_1, \dots, x_n \in \mathbb{R}^d$, $L > 0$

Output: $S \subseteq [n]$

(1) $S \leftarrow [n]$

(2) Repeat

(3) $\quad OUT \leftarrow \{i \in S : \ell_S(i) > L\}$

(4) $\quad S \leftarrow S \setminus OUT$

(5) Until $OUT = \emptyset$

(6) Return S

Good news: always exists unique largest

Bad news: highly unstable.

Stable Covariance

Put a wrapper around greedy filtering

Alg 3 Stable Covariance

Input: $x = x_1, \dots, x_n \in \mathbb{R}^d$, $L_0 > 0$, $k \in \mathbb{N}$

Output: $\hat{d} \in \mathbb{N}$, $w \in [0,1]^n$

(1) For $j = 0, 1, \dots, 2k$

(2) $\quad S_j \leftarrow \text{GreedyLeverageFilter}(x, e^{j/k} L_0)$

(3) $\hat{d} = \min\{k, \min_{0 \le j \le k} \{n - |S_j| - j\}\}$

(4) $\forall i \in [n]$, $w_i \leftarrow \frac{1}{k} \sum_{j=k+1}^{2k} \mathbb{1}\{i \in S_j\}$

(5) Return $\hat{d}, w$

"safe" data $\Leftrightarrow$ no leverage outliers

$\hat{d} \approx$ distance to safety

Prove four properties:

① $\forall x \sim x'$, $\left|\hat{d}(x) - \hat{d}(x')\right| \le 2$

② Completeness: if $\ell(i) \le L_0$ $\forall i$, then $\hat{d}(x) = 0$ and $\vec{w}(x) = 1$

③ Soundness: if $w_i > 0$, then $\ell_{\vec{w}}(i) = x_i^T \left(\sum_{i=1}^{n} w_i x_i x_i^T\right)^{-1} x_i \le 20 \cdot L_0$

④ Stability for $x \sim x'$, if $\hat{d}(x), \hat{d}(x') < k$, then $\|w(x) - w(x')\|_1 \le 2$

Proving ① + ④

Fix x.

Claim: Suppose $\forall i \in S$, $\ell_S(i) \le L$. Then $\forall i, j \in S$, $\ell_{S \setminus \{j\}}(i) \le e^L \ell_S(i)$

Proof Sherman-Morrison formula:

$$\left(A + uv^T\right)^{-1} = A^{-1} - \frac{A^{-1}uv^TA^{-1}}{1 + v^TA^{-1}u}$$

$$\ell_{S\setminus\{i\}}(i) = x_i^T \Big(\overbrace{\sum_{k\in S} x_k x_k^T}^{A} - x_j x_j^T\Big) x_i$$

$$= x_i^T A^{-1} x_i + \frac{x_i^T A^{-1} x_j \, x_j^T A^{-1} x_i}{1 + x_j^T A^{-1} x_i}$$

$$\left| x_i^T A^{-1} x_j \right|^2 = \left| \langle A^{-1/2} x_i, A^{-1/2} x_j \rangle \right|^2$$

$$\le \|A^{-1/2} x_i\|_2^2 \cdot \|A^{-1/2} x_j\|_2^2$$

$$\le \ell_S(i) \cdot L$$

$$\ell_{S\setminus\{i\}}(i) \le \ell_S(i)\left(1 + L\right) \le e^L \ell_S(i)$$

$\boxtimes$

Prove score stable

Prove weight w_i is stable