Robust Statistics

March 6, 2022

Contents

1 Part 1

- Can we develop learning algorithms that are robust to a constant fraction of corruptions in the data
- Statistical Learning Problem: Input: sample generated by a **statistical model** with unknown θ^*. Goal is to estimate parameters θ such that $\theta \approx \theta^*$
- Strong contamination model: Let $\mathcal{F}$ be a family of statistical models. We say that a set of N samples is ϵ-corrupted from $\mathcal{F}$ if it is generated as follows:
  - N samples drawn from unknown $F \in \mathcal{F}$
  - omniscient adverdary inspects samples and arbitrarily changees an ϵ-fraction of them
- Example: Parameter estimation
  - Given i.i.d samples from unknown distribution, how do we estimate its parameters?
  - mean: $\frac{1}{N}\sum_{i=1}^{N} X_i \to \mu$, empirical variance: $\frac{1}{N}\sum_{i=1}^{N}(X_i - \bar{X})^2 \to \sigma^2$
- Robust Estimation: One dimension
  - Given **corrupted** samples from a 1-D gaussian, can we accurately estimate its parameters?
  - A single corrupted sample can arbitrarily corrupt empirical mean and variance
  - Median still works: Given N ϵ-corrupted samples from $\mathcal{N}(\mu, \sigma^2)$, with high constant probability $|\hat{\mu} - \mu| \leq O(\epsilon) + \sqrt{\frac{1}{N}}) \cdot \sigma$ where $\hat{\mu} = \text{median}(S)$
- In high dimensions:

- Robust mean estimation: Given ϵ-corrupted set of samples from unkown mean, identity covariance Gaussian $\mathcal{N}(\mu, I)$ in d dimensions, recover $\hat{mu}$ with $\|\hat{\mu}-\mu\|_2 = O(\epsilon) + O(\sqrt{\frac{d}{N}})$
- above convergence rate is optimal
- All known estimators either require exponential time to compute or can tolerate a neglible fraction of outliers

- Robust estimation in high dimensions is algorithmically possible!
- Meta-Theorem: Can obtain dimension-independent error guarantees, if distribtution on inliers has a nice concentration
- Robust mean estimation: Gaussian case
  - Problem: Given ϵ-corrupted set of points $x_1, \ldots, x_N \in \mathbb{R}^d$ from unkown dist. D in known family $\mathcal{F}$, estimate mean μ of D
  - Theorem 1: Let $\epsilon < \frac{1}{2}$. If D is a spherical gaussian, there is an efficient alg. that outputs estimate $\hat{\mu}$ that with high probability satisfies $\|\hat{\mu}-\mu\|_2 = O(\epsilon) + O(\sqrt{\frac{d}{N}})$ in the additive contamination model
  - Note: First term of RHS is independent of d
- Robust mean estimation: Sub-Gaussian case
  - Problem: Given ϵ-corrupted set of points $x_1, \ldots, x_N \in \mathbb{R}^d$ from unkown dist. D in known family $\mathcal{F}$, estimate mean μ of D
  - Theorem 1: Let $\epsilon < \frac{1}{2}$. If D is a spherical sub-gaussian, there is an efficient alg. that outputs estimate $\hat{\mu}$ that with high probability satisfies $\|\hat{\mu}-\mu\|_2 = O(\epsilon\sqrt{\log(\frac{1}{\epsilon})}) + O(\sqrt{\frac{d}{N}})$ in the strong contamination model
  - Note: Information-theoretically optimal error
- Robust mean estimation: Bounded covariance case
  - Problem: Given ϵ-corrupted set of points $x_1, \ldots, x_N \in \mathbb{R}^d$ from unkown dist. D in known family $\mathcal{F}$, estimate mean μ of D
  - Theorem 1: Let $\epsilon < \frac{1}{2}$. If D has covariance $\Sigma \preceq \sigma^2 \cdot I$, there is an efficient alg. that outputs estimate $\hat{\mu}$ that with high probability satisfies $\|\hat{\mu}-\mu\|_2 = O(\sigma\sqrt{\epsilon}) + O(\sqrt{\frac{d}{N}})$ in the strong contamination model
  - Note: Information-theoretically optimal error

References

[1] Tutorial: Recent Advances in High-Dimensional Robust Statistics, ICML 2020 `http://www.iliasdiakonikolas.org/icml-robust-tutorial.html`