Approximate Bayesian Computing for Differential Privacy

Jordan Awan

Department of Statistics, Penn State University

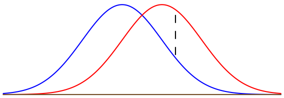
November 27, 2017

Differential Privacy

Definition (DMNS06, WZ10)

- Let $\mathcal{X}$ be a set,
- A *mechanism* $\mathcal{P} = \{P_{\underline{x}} \mid \underline{x} \in \mathcal{X}^n\}$ is a set of probability measures on a space $\mathcal{Z}$
- $\mathcal{P}$ satisfies ϵ-**Differential Privacy** (ϵ - DP) if for all $B \subset \mathcal{Z}$ and all $\underline{x}, \underline{x}'$ differing in one entry, we have

$$P_{\underline{x}}(B) \leq e^{\epsilon} P_{\underline{x}'}(B).$$



Problem Setup

- Collect sensitive data $\underline{X} \in \mathcal{X}^n$
- Output private summary $Z \sim P_{\underline{X}}(z)$

- Model $\underline{X} \sim f_\theta(\underline{x})$, with prior $\theta \sim \pi(\theta)$
- Want to infer about θ, given only Z.

$$\pi(\theta \mid Z) \propto \pi(\theta) \int_{\underline{x} \in \mathcal{X}^n} f_\theta(\underline{x}) P_{\underline{x}}(Z)\, d\underline{x}$$

- This integral is often intractable

Perspective originally from [WM10]

ABC

- Sample (approximately) a posterior distribution
- Does not require evaluating likelihood

Algorithm 1 ABC algorithm [MPR+11]

INPUT: $Z \in \mathcal{Z}$, ρ a pseudo-metric on $\mathcal{Z}$, and $c \geq 0$.

1: Draw $\theta \sim \pi$
2: Draw $Z' \sim f(z \mid \theta)$
3: If $\rho(Z', Z) \leq c$, accept θ, else reject θ,
4: Repeat 1-3 as desired.

OUTPUT: Accepted θ's

- If ρ is a metric, and $c = 0$, then samples are from $\pi(\theta \mid Z)$.

Toy Example

- $\theta \sim U[0,1]$,
- $X \sim \text{Binom}(n,\theta)$,
- $Z = X + \text{DLap}(e^{-\epsilon})$

- Closed form of posterior
- Discrete: can use $c = 0$
- Simulation: $n = 100$, $\theta = .5, \epsilon = .1$
- $\approx 10^4$ accepted samples

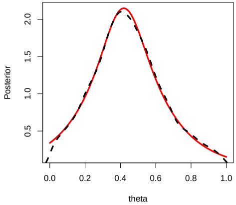


Figure: $c = 0$, AR: 1.7%

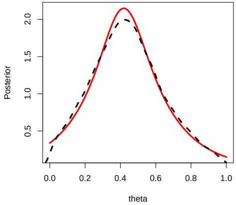
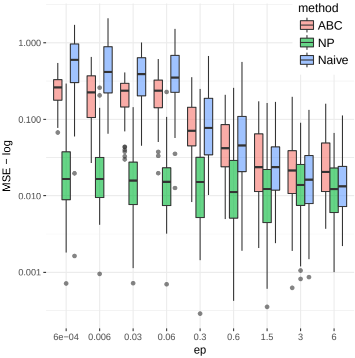


Figure: c as std error, AR: 20%

Problem based on [VS09] and [AS18]

Bigger Example

- Observe n iid copies of $D = (X, Y)$ (feature/class)
- $Y_i \sim \text{Bern}(p)$
- $X_i \mid (Y_i = j) \sim \text{Bern}(p_j)$



- Sufficient statistics:

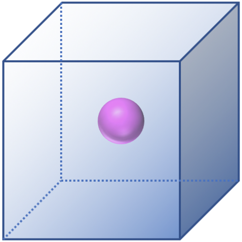
		X	
		1	2
Y	1	n_{11}	n_{12}
	2	n_{21}	n_{22}

- Work with $m_{ij} = n_{ij} + e_{ij}$, where $e_{ij} \overset{\text{iid}}{\sim} \text{Dlap}(e^{-\epsilon/2})$.
- Posterior estimates of p, p_1, and p_2, given uniform priors

Problem based on [KKS16]

Acceptance Rate

- Each proposal in ABC is approximately uniform from $\mathcal{Z}$
- Suppose that $\mathcal{Z} = [a, b]^m$
- Acceptance region is a ball of radius $O\left(\frac{1}{\sqrt{n}}\right)$



- Acceptance rate is ratio of volumes $O\left(\frac{1}{n^{m/2}}\right)$

Image courtesy of Tobia Boschi

Conclusions

- Correct statistical inference by viewing private output as latent variable model
- Likelihood is often **computationally intractable**
- ABC offers an elegant method of sampling from posterior
  - ABC works well when Z is low-dimensional
  - Trade either accuracy, or computational efficiency when Z is higher-dimensional

References

[AS18] J. Awan and A. Slavković. Differentially Private Uniformly Most Powerful Tests for Binomial Data. In *Advances in Neural Information Processing Systems 32*. Curran Associates, Inc., 2018. To Appear.

[DMNS06] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. *Calibrating Noise to Sensitivity in Private Data Analysis*, pages 265–284. Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.

[KKS16] Vishesh Karwa, Dan Kifer, and Aleksandra Slavković. Private posterior distributions from variational approximations. *NIPS 2015 Workshop on Learning and Privacy with Incomplete Data and Weak Supervision*, 2016.

[MPR+11] Jean Michel Marin, Pierre Pudlo, Christian P. Robert, Université Paris Dauphine, Robin J. Ryder, and Université Paris Dauphine. Approximate bayesian computational methods. *Statistics and Computing*, pages 1–14, 2011.

[VS09] Duy Vu and Aleksandra Slavković. Differential privacy for clinical trial data: Preliminary evaluations. In *Proceedings of the 2009 IEEE International Conference on Data Mining Workshops*, ICDMW '09, pages 138–143, Washington, DC, USA, 2009. IEEE Computer Society.

[WM10] Oliver Williams and Frank Mcsherry. Probabilistic inference and differential privacy. In J. D. Lafferty, C. K. I. Williams, J. Shawe-Taylor, R. S. Zemel, and A. Culotta, editors, *Advances in Neural Information Processing Systems 23*, pages 2451–2459. Curran Associates, Inc., 2010.

[WZ10] Larry Wasserman and Shuheng Zhou. A statistical framework for differential privacy. *JASA*, 105:489:375–389, 2010.