Delving into Bootstrapping for Differential Privacy

Anonymous Authors[1]

Abstract

In this paper, we propose a bootstrapping-based method to release private datasets with differential privacy (DP) guarantees. Bootstrapping has long been considered helpful for mitigating disclosure risks. However, it is challenging to provide worst-case privacy guarantees by pure bootstrapping because the presence of an individual in a dataset might completely alter bootstrapped samples. We address this issue by properly smoothing the data before bootstrapping and further establish DP for this composite procedure which we call the *bootstrapping mechanism*. We exhibit its connection to the exponential mechanism, and analyze its utility for density estimation.

1. Introduction

Recent progress in machine learning has catalyzed successes in a wide range of applications, including image classification (Taigman et al., 2014), speech recognition (Hinton et al., 2012), medical diagnosis (Rajpurkar et al., 2017) among others. These advances are due in no small part to the availability of large and representative datasets. These datasets are often crowdsourced and may contain sensitive information. A key question is, therefore, "How can we construct high-performing models while preserving the privacy of individuals?" DP has emerged as a dominant privacy definition that allows ones to understand privacy-utility tradeoff via formal and provable guarantees. The idea of DP is to carefully randomize the algorithm so that the output does not depend too much on any individuals' data.

Differentially-private machine learning has thus far mostly been focused on the scenario where a trusted curator holds sensitive data of the individuals and releases differentially-private models to untrusted third parties. However, oftentimes, those with the expertise to learn from datasets are not the same as those who administer the datasets. Particularly, as Machine Learning as a Service becomes increasingly popular, it is desirable to publish a privatized dataset which allows data analysts to conduct different data analysis *ad infinitum* without impacting privacy.

The goal of this paper is to design simple and practical differentially private data publishing algorithms. The promise made by our algorithms is that the published dataset cannot help ascertain whether a person contributes his/her information to the private dataset. Work on differentially private data publishing has focused on analyzing and improving utility of published datasets for a set of simple queries such as counting (Xiao et al., 2011) and predicate queries (Blum et al., 2013). Existing algorithms largely include sampling from a properly calibrated distribution over datasets (Blum et al., 2013) or publishing private data synopsis such as histograms (Leoni, 2012) and coresets (Feldman et al., 2009).

In this paper, we propose a new technique, termed *bootstrapping mechanism*, for releasing differentially private datasets. Despite its rich history in statistics, bootstrapping has not seen widespread use in privacy preservation; to the best of our knowledge, the work closest to ours is (Muralidhar et al., 2015), which uses bootstrapping to randomize responses to database queries and shows that bootstrapping mitigates the risk of inferential disclosure. However, we show that pure bootstrapping is not adequate to offer DP, as it is difficult to hide an individual who has attributes different from anyone else in a dataset. We address this challenge by showing that we can retain DP by adding proper smoothing to private datasets before bootstrapping. We provide details on how to set the smoothing parameter and bootstrap size. This new technique is simple to implement. We show both theoretically and empirically that it releases data that are useful for different data mining tasks.

In summary, we make the following contributions: (1) We propose the bootstrapping mechanism, which allows for publishing private datasets with DP guarantees; (2) We build connection between the bootstrapping mechanism and the exponential mechanism; (3) We analyze the the convergence rate of private data distribution estimation based on the released data by the bootstrapping mechanism.

[1] Anonymous Institution, Anonymous City, Anonymous Region, Anonymous Country. Correspondence to: Anonymous Author <anon.email@domain.com>.

Preliminary work. Under review by the International Conference on Machine Learning (ICML). Do not distribute.

2. Related Work

Our work is in part inspired by (Chaudhuri and Mishra, 2006), which connects random sampling to DP. Random sampling refers to including each private record in the published dataset with a fixed probability. Chaudhuri and Mishra (2006) notes that limited number of samples can be published especially when there are "rare" values in the private dataset. Instead, our work adopts a resampling approach which can lead to published data of any size at the price of the increased bias due to smoothing. Our work is also connected to posterior sampling (Machanavajjhala et al., 2008; Dimitrakakis et al., 2017), as the smoothed dataset can be treated as the expected value of the posterior distribution using a Dirichlet prior. Exponential mechanism (McSherry and Talwar, 2007) is another sampling paradigm to synthesize datasets. It randomly selects datasets according to a pre-defined utility function. Blum et al. (2013) makes use of the exponential mechanism to publish datasets that achieve provable usefulness for range queries. We show that the bootstrapping mechanism is an instance of the exponential mechanism but nevertheless more efficient since it does not require an explicit utility function in order to perform sampling. Nissim et al. (2007) presents a subsample-and-aggregate mechanism that first runs a non-private function on subsamples of the original database, then aggregates the results with additive noise calibrated to the sensitivity of the aggregator. By far the most similar paper to this work is that of Wasserman and Zhou (2010) who employs sampling from a smoothed histogram to achieve differential privacy and presents a bound on the accuracy in approximating the private data distribution. However, their method only applies to pure differential privacy.

3. Problem Statement

Let $D = \{x_j | x_j \in \Sigma, j = 1, \cdots, n\}$ be a set of private records of n individuals. Assume that a data curator holds D and wishes to release a synthetic dataset $D^* = \{x_j^* | x_j^* \in \Sigma, j = 1, \cdots, m\}$ to the public. Let $\mathcal{M} : \Sigma^n \to \Sigma^m$ be a randomized data publishing algorithm such that $D^* = \mathcal{M}(D)$. Our goal is to design simple algorithms that can publish useful datasets while protecting the privacy of individuals. The privacy notion used herein is DP. Informally, it requires that an individual's data has a bounded effect on the algorithm's output. The formal definition of DP requires reasoning about all pairs of adjacent datasets which differ only in one individual. We denote the adjacency of two datasets D and D' by $D \sim D'$.

Definition 1 (DP). *$\mathcal{M} : \Sigma^n \to \Sigma^m$ is (ϵ, δ)-differentially private if for all $S \subseteq \Sigma^m$ and for all $D, D' \in \Sigma^n$ such that $D \sim D'$: $P[\mathcal{M}(D) \in S] \leq e^\epsilon P[\mathcal{M}(D') \in S] + \delta$.*

Differentially private algorithms are immune to post-processing. This property ensures that any computation on the dataset published by a differentially private algorithm cannot weaken the privacy guarantee.

Proposition 1 (Post-processing (Dwork et al., 2014))**.** *Let $\mathcal{M} : \Sigma^n \to \Sigma^m$ be an (ϵ, δ)-differentially private algorithm and let $g : \Sigma^m \to \mathcal{R}$ be an arbitrary function. Then $g \circ \mathcal{M}$ is also (ϵ, δ)-differentially private.*

4. Challenges of Privacy via Bootstrapping

Bootstrapping refers to random sampling with replacement. Given the original dataset $D = (x_1, \cdots, x_n)$, a bootstrapped dataset contains i.i.d. samples drawn from the empirical distribution $\hat{Q} = \frac{1}{n}\sum_{j=1}^n \delta_{x_j}$, where δ_{x_j} assigns full probability to the point x_j and zero probability elsewhere. Intuitively, bootstrapping is a randomized algorithm per se and thereby can be potentially used as a privacy mechanism for releasing datasets. In this section, we describe roadblocks that prevent pure bootstrapping from achieving differentially private data publishing.

We illustrate the roadblocks via a toy example. Suppose each entry in the private datasets is a binary number, i.e., $\Sigma = \{0, 1\}^n$, and suppose that synthetic datasets are generated via bootstrapping the private datasets. The privacy loss is defined by $c_{\mathcal{M}}(D^*; D, D') = \log \frac{P[\mathcal{M}(D)=D^*]}{P[\mathcal{M}(D')=D^*]}$. DP requires that the above privacy loss is bounded by ϵ with probability at least $1 - \delta$ for all $D \sim D'$.

Difficulty in masking population uniques. Assume that D contains $n - 1$ zeros and a single one and D' is a vector of all zeros. Then, $c_{\mathcal{M}}(D^*; D, D') = \infty$ if we release a dataset D^* which contains one and this happens with probability $1 - (1 - \frac{1}{n})^m$. To ensure (ϵ, δ)-DP, m must be chosen such that $m \leq \log(1 - \delta)/\log(1 - \frac{1}{n})$. Typically, we are interested in values of δ that are less than the inverse of any polynomial in the size of the dataset (Dwork et al., 2014). It is, therefore, difficult to bootstrap a dataset of reasonable size without violating DP.

The individuals that are unlike anyone else in a dataset are often called population uniques. In effect, population uniques are known to be at comparatively high risk of identification disclosure (Manrique-Vallier and Reiter, 2012). On the contrary, if each value in the data domain appears at least k ($k \geq 2$) times in the private dataset, then the privacy loss will always be bounded. This motivates us to apply smoothing to the private dataset before bootstrapping.

Large worst-case privacy loss. Even if population uniques are smoothed out, it remains challenging to bound the worst-case privacy loss. Suppose that we smooth D and D' by adding k zeros and k ones, denoting the corresponding smoothed datasets by $\tilde{D}$ and $\tilde{D}'$, respectively. Then, we perform bootstrapping on the smoothed datasets. Consider the privacy loss when D^* has all ones:

$\log\left(\frac{k+1}{n+2k}/\frac{k}{n+2k}\right)^m = \log\left(\frac{k+1}{k}\right)^m$. If $(\epsilon, 0)$-DP is desired, we must ensure that $m \leq \epsilon/\log(\frac{k+1}{k})$. For small privacy budget (e.g., $\epsilon < \log(\frac{k+1}{k})$), it is impossible to achieve $(\epsilon, 0)$-DP via bootstrapping.

However, bootstrapping becomes appealing if $\delta > 0$ is allowed. Returning to the above example, we note that "D^* has all ones" is a rare event given that D consists of $k+1$ ones and $n+k-1$ zeros. In fact, according to the law of large numbers, it is highly probable (e.g., with probability at least $1-\delta$) that the bootstrapped dataset D^* has around $\frac{k+1}{n+2k}m$ ones and $\frac{n+k-1}{n+2k}m$ zeros when m is sufficiently large. Then, the privacy loss we need to bound is approximately $\log\left(\left(\frac{k+1}{k}\right)^{\frac{k+1}{n+2k}m}\cdot\left(\frac{n+k-1}{n+k}\right)^{\frac{n+k-1}{n+2k}m}\right)$. We can see that it is now possible to confine the privacy loss to arbitrarily small values by properly choosing m and k (e.g., setting m to be 1 and k to be a very large value). The bootstrapped datasets that have the same empirical distribution as the original dataset are called "typical bootstrapped datasets" due to the high probability of their occurrence. If we can guarantee small privacy loss for all typical bootstrapped datasets, then we can achieve small privacy loss for all possible bootstrapped datasets with high probability. The above derivation provides an intuitive view of privacy loss when m approaches infinity. The formal proof, described in the next section, will accommodate the uncertainty of occurrences of zeros and ones in the bootstrapped dataset when m is finite.

5. Bootstrapping Mechanism

In this section, we describe the bootstrapping mechanism (BM), sketch the proof of its privacy guarantee and elucidate the connection to some existing differentially private mechanisms.

5.1. Algorithm and Main Results

We focus on the discrete data domain and assume $\Sigma = \{d_1, \cdots, d_{|\Sigma|}\}$. Inspired by previous discussion, we combine the idea of smoothing and bootstrapping and propose the following bootstrapping mechanism:

1. Smoothing: Apply additive smoothing with the pseudocount k to the private dataset D. More specifically, we add k fictitious records to each value in the domain Σ. The augmented dataset is denoted by $\tilde{D} = (\tilde{x}_1, \ldots, \tilde{x}_{n+k|\Sigma|})$ and $|\tilde{D}| = n + k|\Sigma|$.

2. Bootstrapping: Sample m records from $\tilde{D}$ with replacement. The bootstrapped dataset is denoted by $D^* = (x_1^*, \ldots, x_m^*)$.

In the sequel, we will use $\mathcal{M}$ to represent the bootstrapping mechanism, and denote the smoothing and bootstrapping step in the mechanism by $\mathcal{M}_S$ and $\mathcal{M}_B$, respectively.

Theorem 2. *The bootstrapping mechanism preserves (ϵ, δ)-DP if the private dataset size n, data domain size $|\Sigma|$, pseudocount $k \geq 2$, bootstrap size $m > 0$, and privacy parameters ϵ and δ satisfy the following inequalities for some $\gamma \in (0, 1)$:*

$$m \geq \frac{2}{\gamma^2}\log(\frac{2}{\delta}) \triangleq L \qquad (1)$$

$$m \leq \frac{\epsilon}{(\frac{1}{n+k|\Sigma|} + 2\gamma)\log\frac{k+1}{k}} \triangleq U \qquad (2)$$

The proof of Theorem 2 is inspired by the method of types in information theory (Csiszár, 1998). The key idea of our privacy analysis is to divide all bootstrapped datasets into two sets: a typical set which contains a randomly bootstrapped dataset with probability $1-\delta$ and its complement. We identify the requirements for bootstrap size and pseudocount such that the privacy loss of observing the same typical bootstrapped dataset conditioned on the dataset being D and D' is bounded by ϵ. Since an atypical dataset is very unlikely to be observed (with probability at most δ), we can achieve (ϵ, δ)-DP. We leave the detailed proof to the appendix.

Given the size and domain of a private dataset, Theorem 2 provides sufficient conditions on the free parameters of the bootstrapping mechanism for achieving desired privacy guarantees. The following corollary specifies the constraint on k such that we can find a bootstrap size m satisfying the lower and upper bound established in Theorem 2.

Corollary 3. *Given target privacy parameters ϵ and δ, dataset size n and domain size $|\Sigma|$, to ensure there exists some m that satisfies (1)-(2), it suffices to fix an arbitrary $\gamma \in (0, 1)$ and choose $k \geq k_0$. k_0 is the positive root of $a_2k^2 + a_1k + a_0 = 0$, where $a_2 = \epsilon|\Sigma|$, $a_1 = \epsilon n - 2|\Sigma|\gamma L$, and $a_0 = (-2n\gamma - 1)L$.*

Ideally, we want k to be small and m to be large in order to maximally retain the information in the private dataset. Corollary 3 suggests that we can set the free parameters for the bootstrapping mechanism by taking the following steps: (1) Set γ to some value in $(0, 1)$; (2) Set k to its minimum allowable value $\lceil k_0 \rceil$ defined in Corollary 3; (3) Set m to its maximum allowable value $\lfloor U \rfloor$ at $k = \lceil k_0 \rceil$.

5.2. Connection to Exponential Mechanism

We connect the bootstrapping mechanism to the exponential mechanism (McSherry and Talwar, 2007). The canonical exponential mechanism is often used for preserving $(\epsilon, 0)$-DP. Herein, we consider a relaxed version (Mir, 2013), which can adapt to (ϵ, δ)-DP.

Definition 2 (Relaxed Exponential Mechanism)**.** *Suppose that $D = (x_1, \cdots, x_n)$ and each $x_i \in \Sigma$. Given some arbitrary range $\mathcal{R}$ and utility function $u : \Sigma \times \mathcal{R} \to \mathbb{R}$*

which maps database/output pairs to utility scores, we define the sensitivity of u *at response* r *to be* $\Delta u(r) = \max_{D\sim D'} |u(D,r) - u(D',r)|$. *The relaxed exponential mechanism* $\mathcal{M}_E(D,u,\mathcal{R})$ *selects and outputs an element* $r \in \mathcal{R}$ *with probability proportional to* $\exp(\frac{\epsilon u(D,r)}{2\Delta u_\delta})$ *where* Δu_δ *represents the sensitivity of* u *for high probability outputs, i.e.,* $u_\delta = \max_{r\in\mathcal{R}_\delta} u(r)$*, where* $\mathcal{R}_\delta$ *is any subset of* $\mathcal{R}$ *such that* $P[M_E(D,u,\mathcal{R}) \in \mathcal{R}_\delta] \geq 1-\delta$.

Theorem 4. *The relaxed exponential mechanism preserves* (ϵ,δ)*-DP.*

We can capture the bootstrapping mechanism by choosing proper utility functions in the relaxed exponential mechanism.

Theorem 5. *The bootstrapping mechanism is equivalent to the relaxed exponential mechanism with utility function* $u(D,D^*) = -[\mathcal{H}(h^{D^*}) + \mathcal{KL}(h^{D^*}||h^{\tilde{D}})]$ *where* $D^* \in \Sigma^m$, $m = \frac{\epsilon}{2(\frac{1}{n+k|\Sigma|}+2\gamma)\log\frac{k+1}{k}}$, $\tilde{D} = \mathcal{M}_S(D)$. $\mathcal{H}(\cdot)$ *is the entropy function and* $\mathcal{KL}(h^{D^*}||h^{\tilde{D}})$ *denotes the Kullback-Leibler divergence between* h^{D^*} *and* $h^{\tilde{D}}$*, where the ith element of* h^{D^*} *contains the fraction of occurrences of* d_i *in* D *and* $h^{\tilde{D}}$ *is similarly definied.*

Theorem 5 indicates that the bootstrapping mechanism can be obtained if we sample bootstrapped datasets that have the same type as the smoothed dataset with highest probability and sample other types with the exponential decay rate $\mathcal{KL}(h^{D^*}||h^{\tilde{D}})$.

5.3. Utility for Estimating Data Distribution

We study the accuracy of estimating the private data distribution using the data released by the bootstrapping mechanism. We consider the Kolmogorov-Smirnov (KS) distance, $\rho(F,\hat{F}) = \sup_{x\in\mathcal{X}} |F(x) - \hat{F}(x)|$, where $F(x)$ and $\hat{F}(x)$ are the cumulative density functions (cdf). We use the KS distance to measure the estimation accuracy.

Assume that each data instance in the dataset lies in a continuous domain $\mathcal{X} = [0,1]^d = [0,1]\times\cdots\times[0,1]$ for some integer $d \geq 1$. Assume that the data $X_1,\ldots,X_n$ are drawn from $p(x)$. We first discretize the data space $\mathcal{X}$ into s bins $\{B_1,\ldots,B_s\}$ where each bin B_j is a cube with sides of length b. The binwidth b is chosen such that $s = 1/b^d$ is an integer. Let $\hat{p}(x) = \sum_{j=1}^s \frac{\hat{h}_j}{b^d}\mathbb{1}[x \in B_j]$ denote the histogram estimator on $\mathcal{X}$, where $\hat{h}_j = \sum_{i=1}^s \mathbb{1}[x_i \in B_j]/n$. Recall that $\hat{p}$ is a consistent estimator of $p(x)$ if $b \to 0$ and $nb^d \to \infty$.

We now construct a differentially private histogram estimator based on the bootstrapping mechanism. Define the bootstrapping-based (BS-based) estimator $\hat{p}^*(x) = \sum_{j=1}^s \frac{h_j^*}{b^d}\mathbb{1}[x \in B_j]$, where $h^* = \mathcal{M}(n\hat{h})/m$ is the normalized histogram after applying the bootstrapping mechanism to $n\hat{h}$ and m is the number of bootstrapped samples.

Table 1. Comparison of error rate for different differentially private density estimators.

Minimax rate	**BS-based histogram**	**Smoothed histogram**	**Perturbed histogram**	**Exponential mechanism**
$n^{-1/2}$	$\sqrt{\log n}n^{-4/(d+4)}$	$\sqrt{\log n}n^{-2/(d+6)}$	$\sqrt{\log n}n^{-2/(2+d)}$	$n^{-1/3}$

Note that h^* is a biased estimator of $\hat{h}$, because $\mathbb{E}[h_i^*] = \frac{n\hat{h}_i+k}{n+k|\Sigma|} \neq \hat{h}_i$. To eliminate the bias, we post-process h^* as follows: $\hat{h}_i^c = \frac{n+k|\Sigma|}{n}h_i^* - \frac{k}{n}$. It can be verified that $\hat{h}^c$ is unbiased. By Proposition 1, $\hat{h}^c$ will be differentially private if h^* is DP. The estimator induced by h^c is

$$\hat{p}^c(x) = \sum_{j=1}^s \frac{\hat{h}_j^c}{b^d}\mathbb{1}[x \in B_j] \tag{3}$$

Let F and $\hat{F}^c$ be the cdfs corresponding to p and $\hat{p}^c$, respectively. Now we consider how to choose m, k, s to minimize $\mathbb{E}[\rho(F,\hat{F}^c)]$ while ensuring differential privacy. Here, $\mathbb{E}$ is the expectation under the randomness due to sampling from p and due to the privacy mechanism $\mathcal{M}$.

The following theorem shows the inference accuracy in the KS distance using the estimator constructed from the data released by the bootstrapping mechanism.

Theorem 6. *Consider the density estimator in (3). Then choosing* $m \sim n^{8/(d+4)}$, $s \sim n^{2d/(d+4)}$ *and* k *satisfying (2) minimizes* $\mathbb{E}\rho(F,\hat{F}^c) = \mathcal{O}(\frac{\sqrt{\log n}}{n^{4/(d+4)}})$.

An application of the Markov inequality to $\mathbb{E}\sup_{x\in[0,1]^d}|\hat{F}^c(x) - F(x)|$ indicates that $\hat{F}^c$ is a consistent estimator. However, the rate is lower that the minimax rate of convergence for density estimators in the KS distance, which is $n^{-1/2}$. In Table 1, we compare with other DP density estimators in (Wasserman and Zhou, 2010), where the BS-based histogram refers to our bootstrapping-based estimator. Note that the other estimators in the table are only applicable to $(\epsilon,0)$-differential privacy. We can see that the BS-based histogram can achieve a better rate than the smoothed and perturbed histogram (Wasserman and Zhou, 2010) by allowing (ϵ,δ)-differential privacy.

Due to the space limit, we will leave the evaluation of the utility of the bootstrapping mechanism for estimating data distribution to the appendix.

6. Conclusion

We introduce the bootstrapping mechanism as a simple method to release private data and establish its differential privacy guarantees. Moreover, we analyze the utility of the bootstrapping mechanism for estimating data distribution.

References

Avrim Blum, Katrina Ligett, and Aaron Roth. A learning theory approach to noninteractive database privacy. *Journal of the ACM (JACM)*, 60(2):12, 2013.

Kamalika Chaudhuri and Nina Mishra. When random sampling preserves privacy. In *Annual International Cryptology Conference*, pages 198–213. Springer, 2006.

Imre Csiszár. The method of types [information theory]. *IEEE Transactions on Information Theory*, 44(6):2505–2523, 1998.

Christos Dimitrakakis, Blaine Nelson, Zuhe Zhang, Aikateirni Mitrokotsa, and Benjamin Rubinstein. Differential privacy for bayesian inference through posterior sampling. *Journal of Machine Learning Research*, 18 (11):1–39, 2017.

Cynthia Dwork, Aaron Roth, et al. The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, 9(3–4):211–407, 2014.

Dan Feldman, Amos Fiat, Haim Kaplan, and Kobbi Nissim. Private coresets. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 361–370. ACM, 2009.

Geoffrey Hinton, Li Deng, Dong Yu, George E Dahl, Abdelrahman Mohamed, Navdeep Jaitly, Andrew Senior, Vincent Vanhoucke, Patrick Nguyen, Tara N Sainath, et al. Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups. *IEEE Signal Processing Magazine*, 29(6):82–97, 2012.

David Leoni. Non-interactive differential privacy: a survey. In *Proceedings of the First International Workshop on Open Data*, pages 40–52. ACM, 2012.

Ashwin Machanavajjhala, Daniel Kifer, John Abowd, Johannes Gehrke, and Lars Vilhuber. Privacy: Theory meets practice on the map. In *Proceedings of the 2008 IEEE 24th International Conference on Data Engineering*, pages 277–286. IEEE Computer Society, 2008.

Daniel Manrique-Vallier and Jerome P Reiter. Estimating identification disclosure risk using mixed membership models. *Journal of the American Statistical Association*, 107(500):1385–1394, 2012.

Frank McSherry and Kunal Talwar. Mechanism design via differential privacy. In *Foundations of Computer Science, 2007. FOCS'07. 48th Annual IEEE Symposium on*, pages 94–103. IEEE, 2007.

Darakhshan J Mir. *Differential privacy: an exploration of the privacy-utility landscape*. PhD thesis, Rutgers University-Graduate School-New Brunswick, 2013.

Krishnamurty Muralidhar, Christine M O'Keefe, and Rathindra Sarathy. A bootstrap mechanism for response masking in remote analysis systems. *Decision Sciences*, 46(6): 1199–1226, 2015.

Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith. Smooth sensitivity and sampling in private data analysis. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 75–84. ACM, 2007.

Pranav Rajpurkar, Jeremy Irvin, Kaylie Zhu, Brandon Yang, Hershel Mehta, Tony Duan, Daisy Ding, Aarti Bagul, Curtis Langlotz, Katie Shpanskaya, et al. Chexnet: Radiologist-level pneumonia detection on chest x-rays with deep learning. *arXiv preprint arXiv:1711.05225*, 2017.

Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato, and Lior Wolf. Deepface: Closing the gap to human-level performance in face verification. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 1701–1708, 2014.

Larry Wasserman and Shuheng Zhou. A statistical framework for differential privacy. *Journal of the American Statistical Association*, 105(489):375–389, 2010.

Xiaokui Xiao, Guozhang Wang, and Johannes Gehrke. Differential privacy via wavelet transforms. *IEEE Transactions on Knowledge and Data Engineering*, 23(8):1200–1214, 2011.

A. Proof of Theorem 2

We now discuss the proof of Theorem 2, which is inspired by the method of types in information theory (Csiszár, 1998). The key idea of our privacy analysis is to divide all bootstrapped datasets into two sets: a typical set which contains a randomly bootstrapped dataset with probability $1-\delta$ and its complement. We identify the requirements for bootstrap size and pseudocount such that the privacy loss of observing the same typical bootstrapped dataset conditioned on the dataset being D and D' is bounded by ϵ. Since an atypical dataset is very unlikely to be observed (with probability at most δ), we can achieve (ϵ, δ)-DP.

Let $\tilde{D}$ and $\tilde{D}'$ denote the augmented datasets corresponding to D and D', respectively. Assume $D \sim D'$. We first define the type of a dataset and then rigorously state the meaning of a "typical" bootstrapped dataset.

Definition 3. *The type h^D of a dataset $D \in \Sigma^n$ is the empirical measure induced by this dataset. Explicitly, $h^D = (h^D(d_1), \cdots, h^D(d_{|\Sigma|}))$ is a probability measure defined on Σ where $h^D(d_i) = \frac{1}{n}\sum_{j=1}^{n} \mathbb{1}_{d_i}(x_j), i = 1, \cdots, |\Sigma|$, i.e., $h^D(d_i)$ is the fraction of occurrences of d_i in D.*

Definition 4. *The typical set $T^m_{[\tilde{D}],\gamma}$ with respect to $\tilde{D}$ is the set of datasets bootstrapped from $\tilde{D}$ such that for any $D^* = (D^*_1, \cdots, D^*_m) \in T^m_{[\tilde{D}],\gamma}$ the inequality*

$$\max_{i=1,\cdots,|\Sigma|} |h^{D^*}(d_i) - h^{\tilde{D}}(d_i)| \leq \gamma \tag{4}$$

holds, where $h^{D^*}(d_i)$ and $h^{\tilde{D}}(d_i)$ are types of D^* and $\tilde{D}$, respectively.

The following theorem establishes a lower bound on the bootstrap size such that a randomly bootstrapped dataset belongs to the typical set with high probability.

Theorem 7. *Let D^* be a bootstrapped dataset from $\tilde{D}$ and $|D^*| = m$. If $m \geq \frac{2}{\gamma^2}\log\frac{2}{\delta}$, then $P[D^* \in T^m_{[\tilde{D}],\gamma}] \geq 1-\delta$.*

We will present the proof of Theorem 7 in Appendix B.

By Theorem 7, if we can establish

$$\left|\log\left(\frac{P[\mathcal{M}(D) = D^*]}{P[\mathcal{M}(D') = D^*]}\right)\right| \leq \epsilon \quad \forall D^* \in T^m_{[\tilde{D}],\gamma} \tag{5}$$

for all $D \sim D'$ and $\tilde{D} = \mathcal{M}_S(D)$, then (ϵ, δ)-DP is satisfied.

Since $P[\mathcal{M}(D) = D^*] = P[\mathcal{M}_B(\tilde{D}) = D^*]$ and similarly $P[\mathcal{M}(D') = D^*] = P[\mathcal{M}_B(\tilde{D}') = D^*]$, we can bound $-\epsilon \leq \log\frac{P[\mathcal{M}_B(\tilde{D}) = D^*]}{P[\mathcal{M}_B(\tilde{D}') = D^*]} \leq \epsilon$ instead. We will sketch the proof of the upper bound in the sequel, and the lower bound can be derived in a similar fashion.

Proof of Theorem 2. Without loss of generality, we assume that D and D' differ in nth entry, i.e., $x'_n \neq x_n$ and $x'_j = x_j$ for $j \in \{1, \cdots, n-1\}$. Suppose $x_n = d_{i_1}$ and $x'_n = d_{i_2}$. Then, $h^{\tilde{D}}$ and $h^{\tilde{D}'}$ differ in the two elements corresponding to d_{i_1} and d_{i_2}'s fraction of occurrences:

$$h^{\tilde{D}'}(d_i) = \begin{cases} h^{\tilde{D}}(d_i) - \frac{1}{n+k|\Sigma|}, & i = i_1 \\ h^{\tilde{D}}(d_i) + \frac{1}{n+k|\Sigma|}, & i = i_2 \\ h^{\tilde{D}}(d_i), & i \in \{1, \cdots, |\Sigma|\} \setminus \{i_1, i_2\} \end{cases} \tag{6}$$

In addition, we have for any $D^* \in T^m_{[\tilde{D}]}$ and for all $i \in \{1, \cdots, |\Sigma|\}$,

$$h^{\tilde{D}}(d_i) - \gamma \leq h^{D^*}(d_i) \leq h^{\tilde{D}}(d_i) + \gamma \tag{7}$$

Combining (6) and (7), we obtain an upper bound on the privacy loss:

$$\begin{aligned} &\log\frac{P[\mathcal{M}_B(\tilde{D}) = D^*]}{P[\mathcal{M}_B(\tilde{D}') = D^*]} \\ &\leq -m(h^{\tilde{D}}(d_{i_1}) + \gamma)\log\left(\frac{h^{\tilde{D}}(d_{i_1}) - \frac{1}{n+k|\Sigma|}}{h^{\tilde{D}}(d_{i_1})}\right) - m(h^{\tilde{D}}(d_{i_2}) - \gamma)\log\left(\frac{h^{\tilde{D}}(d_{i_2}) + \frac{1}{n+k|\Sigma|}}{h^{\tilde{D}}(d_{i_2})}\right) \end{aligned} \tag{8}$$

One can verify that the above upper bound is a monotonically decreasing function of both $h^{\tilde{D}}(d_{i_1})$ and $h^{\tilde{D}}(d_{i_2})$. Recall the definition of $h^{\tilde{D}}$ and we have

$$\frac{k+1}{k|\Sigma|+n} \leq h^{\tilde{D}}(d_i) \leq \frac{k+n}{k|\Sigma|+n} \tag{9}$$

$$\frac{k}{k|\Sigma|+n} \leq h^{\tilde{D}}(d_i) \leq \frac{k+n}{k|\Sigma|+n-1} \tag{10}$$

We can use (9) and (10) to further bound (8) by an expression that depends only on n, k, $|\Sigma|$ and γ:

$$(8) \leq m(\frac{1}{n+k|\Sigma|} + 2\gamma)\log\frac{k+1}{k} \tag{11}$$

Combining (11) and Theorem 7 yields the bounds in Theorem 2. □

B. Proof of Theorem 7

The proof of Theorem 7 relies on the following Lemma, which characterizes the convergence of empirical distributions to the underlying probability mass function.

Lemma 1. *Suppose that $X_1, \cdots, X_n$ are i.i.d. samples drawn from the probability mass function f and the domain of X_j ($j = 1, \cdots, n$) is $\mathcal{X} = \{x_1, \cdots, x_{|\mathcal{X}|}\}$. Define the empirical probability mass function as $f_n(x_i) = \frac{1}{n}\sum_{j=1}^{n} \mathbb{1}_{X_j}(x_i)$, then we have*

$$P\left[\max_{x\in\{x_1,\cdots,,x_{|\mathcal{X}|}\}} |f(x) - f_n(x)| > t\right] \leq 2\exp(-\frac{nt^2}{2}) \tag{12}$$

Proof. By the Dvoretzky-Kiefer-Wolfowitz (DKW) inequality, for every $t > 0$

$$P\left[\max_{x\in\{x_1,\cdots,,x_{|\mathcal{X}|}\}} |F(x) - F_n(x)| > t\right] \leq 2\exp(-2nt^2) \tag{13}$$

where $F(x_i) = \sum_{k=1}^{i} f(x_k)$ and $f(x_i) = F(x_i) - F(x_{i-1})$.

If we can prove that

$$\left\{\max_{i=1,\cdots,|\mathcal{X}|} |F(x_i) - F_n(x_i)| > \frac{t}{2}\right\} \supset \left\{\max_{i=1,\cdots,|\mathcal{X}|} |f(x_i) - f_n(x_i)| > t\right\} \tag{14}$$

then

$$P\left[\max_{i=1,\cdots,|\mathcal{X}|} |f(x_i) - f_n(x_i)| > t\right] \tag{15}$$

$$\leq P\left[\max_{i=1,\cdots,|\mathcal{X}|} |F(x_i) - F_n(x_i)| > \frac{t}{2}\right] \tag{16}$$

$$\leq 2\exp\left(-\frac{nt^2}{2}\right) \tag{17}$$

We will prove (14) by contradiction. Suppose that

$$\max_{i=1,\cdots,|\mathcal{X}|} |F(x_i) - F_n(x_i)| \leq \frac{t}{2} \tag{18}$$

Then,

$$\max_{i=1,\cdots,|\mathcal{X}|} |f(x_i) - f_n(x_i)| \tag{19}$$

$$= \max_{i=1,\cdots,|\mathcal{X}|} |F(x_i) - F(x_{i-1}) - F_n(x_i) + F_n(x_{i-1})| \tag{20}$$

$$\leq \max_{i=1,\cdots,|\mathcal{X}|} |F(x_i) - F_n(x_i)| + \max_{i=1,\cdots,|\mathcal{X}|} |F(x_{i-1}) - F_n(x_{i-1})| \tag{21}$$

$$\leq t \tag{22}$$

Hence, we have

$$\{\max_{i=1,\cdots,|\mathcal{X}|} |F(x_i) - F_n(x_i)| \leq \frac{t}{2}\} \subseteq \{\max_{i=1,\cdots,|\mathcal{X}|} |f(x_i) - f_n(x_i)| \leq t\} \tag{23}$$

which implies (14). □

Proof of Theorem 7. Since $h^{\tilde{D}}$ is the true probability mass function that generates the bootstrapped samples and h^{D^*} is the empirical probability mass function, we know from Lemma 1 that

$$P\left[\max_{i=1,\cdots,|\Sigma|} |h^{D^*}(d_i) - h^{\tilde{D}}(d_i)| > \gamma\right] \leq 2\exp(-\frac{m\gamma^2}{2}) \tag{24}$$

Let $\delta = 2\exp(-\frac{m\gamma^2}{2})$. Then, for any $m \geq \frac{2}{\gamma^2}\log\frac{2}{\delta}$,

$$P\left[\max_{i=1,\cdots,|\Sigma|} |h^{D^*}(d_i) - h^{\tilde{D}}(d_i)| > \gamma\right] \leq \delta \tag{25}$$

□

C. Proof of Corollary 3

The free parameters in the bootstrapping mechanism include the pseudo count k, γ and the bootstrap size m. Corollary 3 presents the constraints on k and γ such that there always exists some m such that differential privacy is achieved, i.e., $L \leq U$.

Proof of Corollary 3. Since the expression of U is difficult to analyze, we consider a lower bound of U which enjoys simpler expression.

$$U = \frac{\epsilon}{(\frac{1}{n+k|\Sigma|} + 2\gamma)\log\frac{k+1}{k}} \tag{26}$$

$$\geq \frac{\epsilon}{(\frac{1}{n+k|\Sigma|} + 2\gamma)\frac{1}{k}} \triangleq U_L \tag{27}$$

where the last step follows from an inequality for logarithm functions: $\log(1+x) \leq x$.

We can guarantee $L \leq U$ by ensuring $L \leq U_L$:

$$U_L \geq L \tag{28}$$

$$\iff \frac{\epsilon}{L} \geq (\frac{1}{n+k|\Sigma|} + 2\gamma)\frac{1}{k} \tag{29}$$

$$\iff \epsilon|\Sigma|k^2 + (\epsilon n - 2\gamma L|\Sigma)k - (2\gamma L n + L) \geq 0 \tag{30}$$

□

D. Proof of Theorem 4

In the main paper, we present the extended exponential mechanism, which is a surrogate for the canonical exponential mechanism for achieving (ϵ, δ)-differential privacy. We now present the privacy analysis of the extended exponential mechanism.

Proof of Theorem 4. We divide $\mathcal{R}$ into $\mathcal{R} = \mathcal{R}_\delta \cup \mathcal{R}_\delta^c$ where $\mathcal{R}_\delta$ represents a set of typical outputs of $\mathcal{M}_E$ such that $P[\mathcal{M}_E(D,u,\mathcal{R}) \in \mathcal{R}_\delta] \geq 1-\delta$ and $\mathcal{R}_\delta^c$ is $\mathcal{R}_\delta$'s complement. Hence, $P[\mathcal{M}_E(D,u,\mathcal{R}) \in \mathcal{R}_\delta^c] \leq \delta$.

For any $r \in \mathcal{R}_\delta$ and any two adjacent datasets $D' \sim D$,

$$\frac{P[\mathcal{M}_E(D,u,\mathcal{R})=r]}{P[M_E(D',u,\mathcal{R})=r]} = \left(\frac{\exp\frac{\epsilon u(D,r)}{2\Delta u_\delta}}{\sum_{r'\in\mathcal{R}_\delta}\exp\frac{\epsilon u(D,r')}{2\Delta u_\delta}}\right)\Big/\left(\frac{\exp\frac{\epsilon u(D',r)}{2\Delta u_\delta}}{\sum_{r'\in\mathcal{R}_\delta}\exp\frac{\epsilon u(D',r')}{2\Delta u_\delta}}\right) \tag{31}$$

$$= \left(\frac{\exp\frac{\epsilon u(D,r)}{2\Delta u_\delta}}{\exp\frac{\epsilon u(D',r)}{2\Delta u_\delta}}\right)\left(\frac{\sum_{r'\in\mathcal{R}_\delta}\exp\frac{\epsilon u(D,r')}{2\Delta u_\delta}}{\sum_{r'\in\mathcal{R}_\delta}\exp\frac{\epsilon u(D',r')}{2\Delta u_\delta}}\right) \tag{32}$$

$$= \exp\left(\frac{\epsilon(u(D,r)-u(D',r))}{2\Delta u_\delta}\right)\cdot\left(\frac{\sum_{r'\in\mathcal{R}_\delta}\exp\frac{\epsilon u(D,r')}{2\Delta u_\delta}}{\sum_{r'\in\mathcal{R}_\delta}\exp\frac{\epsilon u(D',r')}{2\Delta u_\delta}}\right) \tag{33}$$

$$\leq \exp\left(\frac{\epsilon}{2}\right)\exp\left(\frac{\epsilon}{2}\right)\left(\frac{\sum_{r'\in\mathcal{R}_\delta}\exp\frac{\epsilon u(D',r')}{2\Delta u_\delta}}{\sum_{r'\in\mathcal{R}_\delta}\exp\frac{\epsilon u(D',r')}{2\Delta u_\delta}}\right) = \exp(\epsilon) \tag{34}$$

Similarly, $\frac{P[\mathcal{M}_E(D,u,\mathcal{R})=r]}{P[\mathcal{M}_E(D',u,\mathcal{R})=r]} \geq \exp(-\epsilon)$ by symmetry.

Consider any $\mathcal{S} \subseteq \mathcal{R}$. Let $\mathcal{S}_T = \mathcal{R}_\delta \cap \mathcal{S}$ and $\mathcal{S}_{AT} = \mathcal{R}_\delta^c \cap \mathcal{S}$. Then,

$$P[\mathcal{M}_E(D,u,\mathcal{R}) \in \mathcal{S}] \tag{35}$$

$$= P[\mathcal{M}_E(D,u,\mathcal{R}) \in \mathcal{S}_T] + P[\mathcal{M}_E(D,u,\mathcal{R}) \in \mathcal{S}_{AT}] \tag{36}$$

$$\leq \exp(\epsilon)P[\mathcal{M}_E(D',u,\mathcal{R}) \in \mathcal{S}_T] + \delta \tag{37}$$

Therefore, $\mathcal{M}_E(D,u,\mathcal{R})$ can achieve (ϵ,δ)-differential privacy. □

E. Proof of Theorem 5

Theorem 5 connects the extended exponential mechanism and the bootstrapping mechanism. The proof of the connection requires the following lemma.

Lemma 2. *If $D^* = \mathcal{M}_b(\tilde{D})$, then the probablity of D^* depends only on the type of D^*, i.e.,*

$$P[\mathcal{M}_b(\tilde{D}) = D^*] = \exp(-m(\mathcal{H}(h^{D^*}) + \mathcal{KL}(h^{D^*}||h^{\tilde{D}}))) \tag{38}$$

where $\mathcal{H}(\cdot)$ is the entropy function

$$\mathcal{H}(h^{D^*}) = -\sum_{i=1}^{|\Sigma|} h^{D^*}(d_i)\log h^{D^*}(d_i) \tag{39}$$

and $\mathcal{KL}(h^{D^*}||h^{\tilde{D}})$ denotes the KL divergence between h^{D^*} and $h^{\tilde{D}}$

$$\mathcal{KL}(h^{D^*}||h^{\tilde{D}}) = \sum_{i=1}^{|\Sigma|} h^{D^*}(d_i)\log\left(\frac{h^{D^*}(d_i)}{h^{\tilde{D}}(d_i)}\right) \tag{40}$$

The proof of Lemma 2 can be found in “Large Deviations, Techniques, and Applications” by Amir Dembo. Now we provide the proof of Theorem 5.

Proof of Theorem 5. By Theorem 7, we can set $\mathcal{R}_\delta$ to be $T^m_{[\tilde{D}],\gamma}$ as long as $m \geq \frac{2}{\gamma^2}\log\frac{2}{\delta}$. Using Lemma 2, we can represent the sensitivity of u for high probability outputs as

$$\Delta u_\delta = \max_{D^*\in T^m_{[\tilde{D}],\gamma}}\ \max_{D\sim D'} |u(D,D^*) - u(D',D^*)| \tag{41}$$

$$= \max_{D^*\in T^m_{[\tilde{D}],\gamma}}\ \max_{D\sim D'} |D(h^{D^*}||h^{\tilde{D}}) - D(h^{D^*}||h^{\tilde{D}'})| \tag{42}$$

$$= \max_{\substack{\frac{k+1}{k|\Sigma|+n}\leq x_1\leq\frac{k+n}{k|\Sigma|+n}\\ \frac{k}{k|\Sigma|+n}\leq x_2\leq\frac{k+n-1}{k|\Sigma|+n}}} \left|\gamma\log\frac{(x_1-\frac{1}{n+k|\Sigma|})x_2}{(x_2+\frac{1}{n+k|\Sigma|})x_1} + x_1\log\left(1-\frac{1}{x_1(n+k|\Sigma|)}\right) + x_2\log\left(1+\frac{1}{x_2(n+k|\Sigma|)}\right)\right| \tag{43}$$

Denote the expression inside the modulus function as $f(x_1, x_2)$ and it can be decomposed as $f(x_1, x_2) = f_1(x_1) + f_2(x_2)$, where

$$f_1(x_1) = (x_1 + \gamma)\log(1 - \frac{a}{x_1}) \tag{44}$$

$$f_2(x_2) = (x_2 - \gamma)\log(1 + \frac{a}{x_2}) \tag{45}$$

$$a = \frac{1}{n + k|\Sigma|} \tag{46}$$

f_1 and f_2 are both monotonically increasing functions for $x_1 \in [\frac{k+1}{k|\Sigma|+n}, \frac{k+n}{k|\Sigma|+n}]$, $x_2 \in [\frac{k}{k|\Sigma|+n}, \frac{k+n-1}{k|\Sigma|+n}]$, because

$$\frac{df_1}{dx_1} = (x_1 + \gamma)\frac{a}{x_1(x_1 - a)} + \log\frac{x_1 - a}{x_1} \tag{47}$$

$$\geq (x_1 + \gamma)\frac{a}{x_1(x_1 - a)} - \frac{a}{x_1} \tag{48}$$

$$\geq \frac{a}{x_1 - a} - \frac{a}{x_1} \geq 0 \tag{49}$$

and

$$\frac{df_2}{dx_2} = (x_2 - \gamma)\frac{-a}{x_2(x_2 + a)} + \log\frac{x_2 + a}{x_2} \tag{50}$$

$$\tag{51}$$

If $x_2 \leq \gamma$, then it is evident that $\frac{df_2}{dx_2} > 0$. When $x_2 > \gamma$,

$$\frac{df_2}{dx_2} \geq \frac{-a}{x_2 + a} + \log\frac{x_2 + a}{x_2} \tag{52}$$

$$\geq \log(1 - \frac{a}{x_2 + a}) + \log\frac{x_2 + a}{x_2} \geq 0 \tag{53}$$

Hence, $f = f_1 + f_2$ is also a monotonically increasing function. Since

$$\max f(x_1, x_2) \tag{54}$$

$$= f(\frac{n+k}{n+k|\Sigma|}, \frac{n+k-1}{n+k|\Sigma|}) \tag{55}$$

$$\leq f(\frac{n+k}{n+k|\Sigma|}, \frac{n+k}{n+k|\Sigma|}) \tag{56}$$

$$= (\frac{n+k}{n+k|\Sigma|} + \gamma)\log\frac{n+k-1}{n+k} + (\frac{n+k}{n+k|\Sigma|} - \gamma)\log\frac{n+k+1}{n+k} \tag{57}$$

$$= \frac{n+k}{n+k|\Sigma|}\log\frac{(n+k)^2 - 1}{(n+k)^2} + \gamma\log\frac{n+k-1}{n+k+1} \leq 0 \tag{58}$$

we have

$$\Delta u_\delta = \max_{\substack{x_1 \in [\frac{k+1}{k|\Sigma|+n}, \frac{k+n}{k|\Sigma|+n}] \\ x_2 \in [\frac{k}{k|\Sigma|+n}, \frac{k+n-1}{k|\Sigma|+n}]}} |f(x_1, x_2)| \tag{59}$$

$$= -f(\frac{k+1}{n+k|\Sigma|}, \frac{k}{n+k|\Sigma|}) \tag{60}$$

$$= -\left[(\frac{k+1}{n+k|\Sigma|} + \gamma)\log\frac{k}{k+1} + (\frac{k}{n+k|\Sigma|} - \gamma)\log\frac{k+1}{k}\right] \tag{61}$$

$$= (2\gamma + \frac{1}{n+k|\Sigma|})\log\frac{k+1}{k} \tag{62}$$

The extended exponential mechanism will therefore select D^* with probability

$$P[\mathcal{M}_E(D, u, \Sigma^m) = D^*] = \exp\left(\frac{-\epsilon[H(h^{D^*}) + D(h^{D^*}||h^{\tilde{D}})]}{2(2\gamma + \frac{1}{n+k|\Sigma|})\log\frac{k+1}{k}}\right) \tag{63}$$

If we set the size of the sampled database to be $m = \frac{\epsilon}{2(\frac{1}{n+k|\Sigma|}+2\gamma)\log\frac{k+1}{k}}$, then

$$P[\mathcal{M}_E(D, u, \Sigma^m) = D^*] = \exp\left(- m[H(h^{D^*}) + D(h^{D^*}||h^{\tilde{D}})]\right) \tag{64}$$

which yields the bootstrapping mechanism. □

F. Proof of Theorem 6

Proof. Let $\tilde{h}$ denote the normalized histogram of the output of the smoothing step in the bootstrapping mechanism, i.e., $\tilde{h} = \mathcal{M}_S(n\hat{h})/(n + ks)$, where k denotes the pseudocount. Let the estimator induced by $\tilde{h}$ be denoted by

$$\tilde{p}(x) = \sum_{j=1}^{s} \frac{\tilde{h}_j}{b^d} \mathbb{1}[x \in B_j] \tag{65}$$

Let $\hat{F}$, $\tilde{F}$ and $\hat{F}^*$ denote the cdf of $\hat{p}$, $\tilde{p}$, and $\hat{p}^*$, respectively. We use the triangle inequality to analyze $\mathbb{E}\rho(F, \hat{F}^c)$:

$$\begin{aligned} &\mathbb{E} \sup_{x\in[0,1]^d} |\hat{F}^c(x) - F(x)| \\ &\le \mathbb{E} \sup_{x\in[0,1]^d} |\hat{F}^c(x) - \hat{F}(x)| + \mathbb{E} \sup_{x\in[0,1]^d} |\hat{F}(x) - F(x)| \end{aligned} \tag{66}$$

By the Vapnik-Chervonenkis bound, we have for $t > 0$ that

$$P[\sum_{x\in[0,1]^d} |\hat{F}^*(x) - \tilde{F}(x)| > t] \le 8m^d \exp(-\frac{mt^2}{32})$$

for large n. Hence, $\mathbb{E}\sup_{x\in[0,1]^d} |\hat{F}^*(x) - \tilde{F}(x)| = \mathcal{O}(\sqrt{\frac{d\log m}{m}})$. Since $\hat{h}^c = \frac{n+ks}{n}h^* - \frac{k}{n}$ and $\hat{h} = \frac{n+ks}{n}\tilde{h} - \frac{k}{n}$, we obtain

$$\begin{aligned} &\mathbb{E} \sup_{x\in[0,1]^d} |\hat{F}^c(x) - \hat{F}(x)| \\ &= \frac{n+ks}{n}\mathbb{E} \sup_{x\in[0,1]^d} |\hat{F}^*(x) - \tilde{F}(x)| \\ &= \mathcal{O}(\frac{n+ks}{n}\sqrt{\frac{d\log m}{m}}) \end{aligned} \tag{67}$$

In (Wasserman and Zhou, 2010), it is shown that

$$\mathbb{E} \sup_{x\in[0,1]^d} |\hat{F}(x) - F(x)| = \mathcal{O}(\sqrt{\frac{d\log n}{n}}) + Ld^{3/2}s^{-2/d} \tag{68}$$

where L is the Lipschitz constant of $p(x)$. Thus we have by (66), (67), and (68)

$$\begin{aligned} &\mathbb{E} \sup_{x\in[0,1]^d} |\hat{F}^c(x) - F(x)| = \mathcal{O}(\frac{n+ks}{n}\sqrt{\frac{d\log m}{m}}) \\ &+ \mathcal{O}(\sqrt{\frac{d\log n}{n}}) + Ld^{3/2}s^{-2/d} \end{aligned} \tag{69}$$

Setting $s \sim n^{2d/(d+4)}$, $m \sim n^{8/(d+4)}$, and k such that (2) holds, we get for all n large enough, $\mathbb{E}\sup_{x\in[0,1]^d} |\hat{F}^c(x) - F(x)| = \mathcal{O}(\frac{\sqrt{\log n}}{n^{4/(d+4)}})$. □

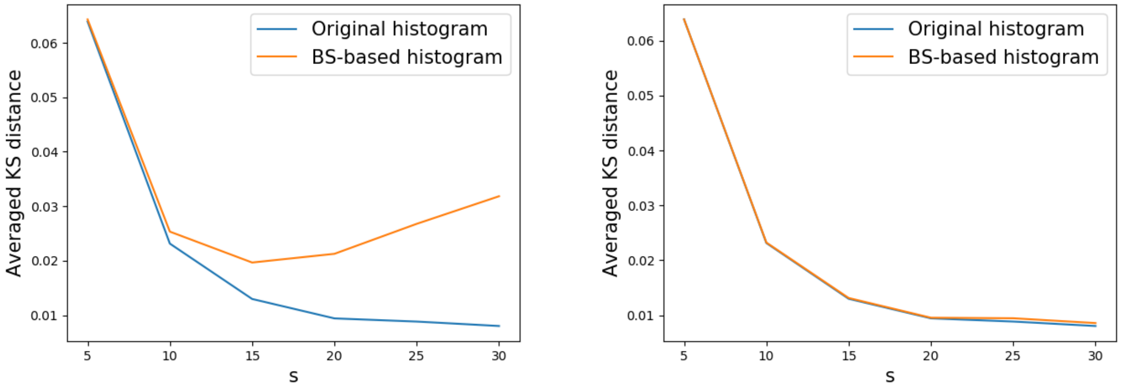

Figure 1. Comparison of the error for different DP data release methods in approximating the orginal data distribution. $n = 10000$, $\delta = 0.01$, $\epsilon = 0.5$ in (a) and $\epsilon = 5$ in (b).

G. Experiments

We examine the utility of the bootstrapping mechanism for estimating the private data distribution. We take the true density of X to be a $\texttt{Beta}(10{,}10)$ density. Figure 1 shows the results of 100 simulations for various numbers of bins s. As expected, smaller values of ϵ induce a large information loss.